Cisco VPN 3000 Concentrator Series Security Policy

Introduction

This non-proprietary Cryptographic Module Security Policy describes how the VPN 3000 Series Concentrator meets the security requirements of FIPS 140-2, and how to operate a VPN 3000 Concentrator using IPSec encryption in secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the VPN 3000 Series Concentrator, referred to in this document as the VPN Concentrator.

Note The VPN 3000 Series Concentrator comprises models 3005, 3015, 3030, 3060, and 3080.

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:

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

References

This document describes the operations and capabilities of the VPN Concentrator only in the technical terms of FIPS 140-2 cryptographic module security policy. More information is available on VPN 3000 Concentrator Series in the following documents:

VPN 3000 Series Concentrator Getting Started, Release 3.6—explains how to unpack and install the VPN Concentrator and how to configure the minimal parameters.

VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 3.6—explains how to start and use the VPN Concentrator Manager and how to configure your device beyond the minimal parameters you set during quick configuration.

VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring, Release 3.6—explains and defines all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager.

Release Notes for Cisco VPN 3000 Series Concentrator, Release 3.6 through 3.6.7.F

Release Notes for Cisco VPN 3000 Series Concentrator, FIPS Release 3.6

You can find this documentation as well as information on the complete line of products from Cisco Systems at the website http://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 modules.

Document Organization

The Security Policy document is one document in a complete FIPS-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 and is releasable only under appropriate non-disclosure agreements. For access to these documents, contact Cisco Systems.

Cisco VPN 3000 Series Concentrator

This section presents an overview of the VPN Concentrator, its interfaces, roles and services, authentication mechanisms, cryptographic key management, design assurance, and mitigation of attacks.

Overview

Cisco VPN 3000 Series Concentrator comprises a family of hardware appliances that operate as concentrators in Virtual Private Networking (VPN) environments. They combine the best features of a software concentrator, including scalability and easy deployment, with the stability and independence of a hardware platform. The VPN Concentrator connects a remote user to a corporate network. The user connects to a local Internet service provider (ISP), then to the VPN device Internet IP address. The VPN Concentrator encrypts the data and encapsulates it into a routable IPSec packet, creating a secure tunnel between the remote user and the corporate network. The corporate server authenticates the user, decrypts and authenticates the IPSec packet, and translates the source address in the packets to an address recognized on the corporate network. This address is used for all traffic sent from the corporate network to the remote user for the duration of the connection. The VPN Concentrator distinguishes between tunneled and non-tunneled traffic and, depending on your server configuration, allows simultaneous access to the corporate network and to Internet resources. It supports RADIUS and TACACS+ for remote authentication.

Module Interfaces

The VPN Concentrator is a multi-chip stand-alone module and the cryptographic boundary of the module is defined by its metal enclosure. The module provides a number of physical and logical interfaces to the device.

The physical interfaces that the module provides are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their module mapping are described in Table 1.

Table 1 FIPS 140-2 Logical Interface

FIPS 140-2 Logical Interfaces	VPN Concentrator's Physical Interfaces
Data input	10/100BASE-TX LAN ports
Data output	10/100BASE-TX LAN ports
Control input sequence	10/100BASE-TX LAN ports Console port Power button Reset button

Table 1 FIPS 140-2 Logical Interface (continued)

FIPS 140-2 Logical Interfaces	VPN Concentrator's Physical Interfaces
Status output	LEDs 10/100BASE-TX LAN ports Console port
Power	A DC Input 19V/3.16A 60W power input

Roles and Services

The VPN Concentrator supports role-based authentication. To perform tasks on the VPN Concentrator, users must enter a password and authenticate to the system. Users can access the VPN Concentrator in one of the following ways:

- Serial Port
- HTTP
- HTTPS
- Telnet
- Telnet over SSL
- SSH

In a FIPS approved mode of operation, only the interfaces through the serial port, HTTPS (using TLS) and SSH are enabled.

There are two main roles in the VPN Concentrator (as required by FIPS 140-2) that operators may assume: a *crypto officer* role and a *user* role. The VPN Concentrator also supports an *administrator* role and up to four additional administrative roles with the restricted privileges.

Table 2 shows how the VPN Concentrator roles map to the crypto officer and user roles.

:

Table 2 FIPS Mapping of Roles

Role	FIPS Mapping
Admin user	Crypto-Officer
Four administrative accounts (config, isp, mis, user)	Crypto-Officer
User	User

Admin Role

The admin user is responsible for configuring the VPN Concentrator properly. The admin can access all the services available via the management interfaces. This section lists these services.

The non-crypto services include show status commands and user establishment and authentication initialization. The various non-crypto services available to the administrator role include the following:

- Performing general configuration (for example, defining IP addresses, enabling interfaces, enabling network services, and configuring routing protocols)
- Reloading and shutting down the VPN Concentrator
- Displaying full status of the VPN Concentrator

- Shutting down and restarting network services
- Displaying the configuration stored in memory, and also the version saved in flash, which is used to initialize the VPN Concentrator following a reboot
- Configuring all administrative roles and privileges
- Managing the event log
- Monitoring operations

The crypto services include key generation, encryption/decryption, and the power-up self-tests. Some of the specific crypto services available to the admin role include the following:

- Managing certificate enrollment
- Configuring authentication policy
- Managing the accounts of the other administrators
- Managing remote user address pools
- Configuring authentication servers
- Configuring LAN to LAN tunnels including policy management (public key algorithm, encryption, authentication)
- Configuring filters and access lists for interfaces and users
- Configuring administrator privileges
- Configuring RADIUS and TACACS+ authentication

Admin users may not configure static session keys for encrypted tunnels, nor are they allowed to enter static keys for certificate enrollment. These keys are all generated dynamically via the appropriate mechanism (IKE, RSA, DSA).

For information on the specific administrator commands, see the section "Administration | Access Rights | Access Settings" in the *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* user guide.

Other Administrator Roles

For FIPS, the administrator role is also the crypto officer delegated for specific tasks such as taking backups or managing users. The VPN Concentrator implements four roles called *config*, *isp*, *mis*, and *user*. These roles have limited rights on the system and are configured by the Admin user. These roles are disabled by default and the admin user has to enable them if needed. These roles are accessed through an Ethernet port using the Web-based administration tool or by connecting through the console port. All administrator roles are entered by supplying the correct username/password combination and passing the appropriate IP address checks. All administrators are responsible for ensuring that the VPN Concentrators are configured properly to meet all FIPS 140-2 requirements.

At some permission levels, an administrator can access only the configuration and monitoring functions that the administrator with the highest level of permissions selects. It is possible to give other administrators the highest level privileges. For more detailed information on the subset descriptions, see the section "Administration | Access Rights | Access Settings" in the *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* user guide.

User Role

Users are the people or entities that wish to send data or traffic through the VPN Concentrator. Users comprise devices, concentrators, and anyone passing data through the VPN Concentrators. All user roles are entered by supplying the correct authentication information. Users are authenticated to the VPN Concentrators based on the authentication protocol established by the administrator (for example, security association ID or IP address and preshared secret key combination).

Authentication Mechanisms

The VPN Concentrator supports the username-password combination or digital certificates for authenticating IPSec users. An operator must log on to the VPN Concentrator to connect to the module through one of the management interfaces (Serial Port, SSH, HTTPS over TLS in FIPS mode) and provide a username and password.

Table 3 Estimated Strength of Authentication Mechanisms

Authentication Type	Strength
Username-Password mechanism	The module implements a minimum length requirement for the password. The minimum length is 6 characters. The length of the password makes the probability of getting a random guess correct, less than 1 in 1000000. This argument is also valid for RADIUS or TACACS+ shared secret keys when a RADIUS or a TACACS+ server authenticates to the module.
Certificate-based authentication	The module supports a public key based authentication. It supports 512, 768 and 1024 bit keys. The signature on each certificate is 128-bits. Thus the probability of getting a random guess correct is much less than 1 in 1000000. This is used to authenticate the client when creating an IPSec tunnel.

Physical Security

The VPN Concentrator is a multi-chip stand-alone cryptographic module.

Cryptographic Key Management

The module uses the following FIPS-approved algorithms.

- Symmetric Key Algorithms

Algorithm	Modes Implemented	Key Sizes
DES (FIPS 46-3)	CBC	56 bits
Triple DES (FIPS 46-3)	CBC	168 bits
AES (FIPS 197)	CBC	128, 196, 256 bits

- Hashing Algorithms
  - SHA-1 (FIPS 180-1)

  - HMAC with SHA-1
- MAC Algorithms
  - DES MAC
  - TDES MAC
- Public Key Algorithms
  - RSA (PKCS#1)
  - DSA (FIPS 186-1)

It also uses the SSL/TLS protocol, SSH protocol and HTTPS. It uses the PKCS 1.0 algorithm for encrypting and signing using the RSA public-key crypto system.

Cryptographic Keys Used by the VPN Concentrator

The VPN concentrator uses a variety of keys during its operation. Table 4 lists the keys used by various services and protocols.

Only the crypto officer (administrator) can log on to the box directly through the console or the web interface. Normal users of the module access it only through the services. So the CSPs are accessed directly only by the crypto officer. All other users access them through protocol.

Note PKCS #5 format is not FIPS approved and for FIPS, files stored encrypted in the PKCS#5 format are considered to be stored in plain text.

Table 4 VPN Concentrator Keys

Key	Description	Storage and Zeroization
Key Encryption Key 1 (KEK1)	An ephemeral triple DES key used to protect all traffic keys, HMAC keys, Diffie-Hellman private keys. KEK1 is used to decrypt the appropriate cryptographic key prior to use.	KEK1 is stored in RAM in plaintext form. It is zeroized by resetting/restarting the module.
Key Encryption Key 2 (KEK2)	An ephemeral DES key used to protect DSA private keys, RSA private keys, and the Diffie-Hellman shared secret (g^{xy}) private keys. KEK2 is used to decrypt the appropriate cryptographic keys prior to use by the module.	KEK2 is stored in RAM in plaintext form. It is zeroized by resetting/restarting the module.
RSA public/private keys	Identity certificates for the module itself and also used in IPSec negotiations. The module supports 512, 768 and 1024 bit key sizes.	The RSA private key is stored encrypted with KEK2 in the RAM memory. In the Flash they are stored encrypted with a PKCS#5 based encryption mechanism. The pass phrase used for the PKCS#5 encryption is derived from hardware. The keys are zeroized by overwriting them with new keys.

Table 4 VPN Concentrator Keys (continued)

DSA public/private keys	Identity certificates for the module itself and also used in IPSec negotiations.	The DSA private key is stored encrypted with KEK2 in the RAM memory. In the Flash file system they are stored encrypted with a PKCS#5 password based encryption mechanism. The pass phrase used for the PKCS#5 encryption is derived from hardware. These keys are zeroized by overwriting them with new keys.
Diffie-Hellman Key Pairs	Used by VPN Concentrator devices for key agreement during the IKE session establishment process.	Diffie-Hellman private keys and shared secrets (g^{xy}) are stored in RAM and protected by encryption using either KEK1 or KEK2. Resetting or rebooting the module zeroizes them.
Public keys	The module stores public keys of peers (for example client systems that use the VPN 3002 Hardware Client). It also receives the public key of the VPN Client.	These can be either deleted or overwritten with a new value of the certificate from the client.
TLS Traffic Keys	Used in HTTPS connections to configure the system and also in SSH host keys.	These are ephemeral keys stored in RAM encrypted using KEK1 and are zeroized once the TLS session is closed.
SSH Host keys and Session Keys	The SSH keys for the VPN module. The keys from clients, from where the operator is connecting are also stored.	The SSH session keys are ephemeral keys stored in RAM encrypted using KEK1. They are zeroized once the SSH session is closed. The SSH host keys are zeroized by either deleting them or by overwriting them with a new value of the key.
IPSec traffic keys	Exchanged using the IKE protocol and the public/private key pairs. These are DES/3DES or AES keys.	They are ephemeral keys stored in RAM encrypted with KEK1 in and are zeroized when the IPSec tunnel is closed.
IKE pre-shared keys	Entered by the Crypto-Officer in plain-text form over the HTTPS(TLS) web interface and are stored in plaintext form.	They are used for authentication during IKE. They are zeoized by either deleting them or by replacing them with new ones.

Table 4 VPN Concentrator Keys (continued)

RADIUS and TACACS+ shared secret keys.	Entered by the Crypto-Officer in plain-text form over the HTTPS (TLS) web interface and stored in plain-text form.	Used for authenticating the RADIUS or TACACS+ server to the concentrator and vice versa. They are zeroized by either deleting them or by replacing them with new ones.
Password table	Critical security parameters used to authenticate the user/crypto-officer logging in on to the machine.	They are stored in NVRAM in plaintext and are zeroized by overwriting the passwords with new ones.
Group and User passwords	Critical security parameters used to authenticate the Users of the module	They are stored in flash memory using a PKCS#5 derived key. They are zeroized when the passwords are changed.
Certificates of Certificate Authorities (CAs)	Necessary to verify certificates issued by them. So the CA's certificate should be installed before installing the certificate issued by it.	They are stored in the file system and are signed by the CA to prevent modification.

The VPN Concentrator uses PKCS10 format for certificate requests. It also supports the Simple Certificate Enrollment Protocol (SCEP).

Key Generation

The VPN Concentrator uses a FIPS-approved random number generator. The VPN Concentrator generates all keys using the pseudo random number generator defined in the ANSI X9.31 standard.

Key Entry and Output

All the keys are entered through the administrative interface. Keys are never output from the VPN module.

Key Storage

All cryptographic keys are stored in encrypted form using Key Encryption Keys (KEKs). The only keys stored in plain-text form are the KEKs and IPSec pre-shared keys. KEKs are accessible only to the crypto officer. Also a user thread cannot access shared keys of other users.The RAS/DSA keys are stored encrypted in the flash using a PKCS#5-based pass-phrase.

Key destruction

As required by FIPS 140-2, all keys can be destroyed and the VPN zeroizes all keys prior to their destruction. Also performing a hardware or software reboot zeroizes all the ephemeral session keys.

Self-Tests

The VPN Concentrator provides the following power-up self-tests automatically each time it starts:

- Software/firmware test
- DSA (sign/verify test)
- RSA KAT
- DES KAT
- TDES KAT
- AES KAT
- SHA-1 KAT
- HMAC SHA1 KATs

All power-up self-tests must be passed before allowing any operator to perform any cryptographic services. The power-up 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-up self-test failure. In the unlikely event a power-up self-test fails, an event is displayed indicating the error and then the module logs the error. In this state, the module does not a perform any operations. The only way the operator can try to clear the error is to check the logs and cycle the power.

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

- Pair-wise Consistency test for DSA key pair generation
- RSA pair wise consistency test
- Continuous Random Number Generator Test for the FIPS-approved RNG.

In the unlikely event a conditional self-test fails, an event is displayed indicating the error and then the VPN Concentrator logs the error. In this state, the module does not a perform any operations. The only way the operator can try to clear the error is to check the logs and cycle the power.

The module does not allow a bypass mode of operation.

Design Assurance

Cisco Systems uses the Perforce Configuration Management System. Perforce is used in software and document version control, code sharing and build management.

The configuration management system is used for Software Lifecycle Modeling. Software life-cycle modeling is the business of tracking source code as it goes through various stages throughout its life, from development, to testing, release, reuse, and retirement. Cisco Systems also uses Perforce Configuration Management to effectively perform the following processes:

- Workspaces - where developers build, test, and debug
- Codelines - the canonical sets of source files
- Branches - variants of the codeline
- Change propagation - getting changes from one codeline to another
- Builds - turning source files into products

Cisco Systems follows established software engineering principles to design, develop, track and document software and hardware modules.

Mitigation of Other Attacks

The VPN Concentrator does not claim to mitigate any attacks in a FIPS approved mode of operation.

Secure Operation

The Cisco VPN Concentrator meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

Admin (Crypto-Officer) Guidance

The following are instructions to the admin (crypto officer) to run the module in a FIPS approved mode of operation.

Initial Setup

The following list is a summary of the security rules that the administrator must configure and enforce on the VPN Concentrators:

- Only FIPS-approved cryptographic algorithms to be used
- TFTP administrative access method must not be allowed
- Only the IPSec protocol may be enabled for protection of traffic; all other protocols for protecting data must be disabled.
- When using HTTPS to protect administrative functions, only the TLS protocol may be used for key derivation. The SSL protocol is not compliant with the FIPS 140-2 standard.
- The crypto officer must change the default password and choose a password that is at least 6 characters long.
- The crypto officer must not perform firmware upgrades in a FIPS mode of operation.
- The crypto officer must define RADIUS and TACACS+ shared secret keys that are at least 6 characters long.

Cryptographic Algorithms

VPN Concentrators support many different cryptographic algorithms. However, to properly use VPN Concentrators in FIPS mode, only the FIPS-approved algorithms may be used. The following cryptographic algorithms are to be used for encrypting traffic, hashing, or signing/verifying digital signatures:

- DES encryption/decryption

Note Use the DES algorithm only for protecting low sensitivity information. Cisco recommends that you use Triple DES to protect highly sensitive information.

- Triple DES encryption/decryption
- AES encryption/decryption

- SHA-1 hashing
- DSA signing and verifying
- RSA digital signature signing and verifying

Administrators must configure VPN Concentrators to use only the cryptographic algorithms listed above for all services that they provide.

Security Relevant Data Items

VPN Concentrators store many security relevant data items, such as authentication keys (Pre-shared keys, DSA or RSA private keys, etc.) and traffic encryption keys. All security data items are stored and protected within the VPN Concentrator tamper evident enclosure (see section “Tamper Evidence” for details on applying tamper evident labels). In addition, most security data items are stored encrypted on VPN Concentrators.

Security Protocols

VPN Concentrators, by design, support many Internet security tunneling protocols for protecting data transfer. However, to ensure that the device operates in FIPS mode, the administrator must ensure that the VPN Concentrator is configured such that only the IPSec protocol is used to protect data transmission. All other tunneling protocols supported by a VPN Concentrator may not be used if compliance with the FIPS 140-2 standard is required.

Services

To operate in FIPS crypto officer mode, you must configure the VPN Concentrator as follows:

- Configure the minimum password length for all users to 6.
- The crypto officer should change the default password on module initialization. The minimum length of the changed password is 6.
- The crypto officer must define RADIUS and TACACS+ shared secret keys that are at least 6 characters long.
- Enable HTTPS only. Disable HTTP for performing system management
- Configure SSL to use only FIPS-approved encryption algorithms (DES, 3DES, or SHA-1) and set SSL version to TLS V1.
- Configure the Event subsystem to avoid sending events to the console.
- Disable the Telnet server.
- Disable the FTP server.
- Disable the TFTP server.
- Disable PPTP.
- Disable L2TP.
- Deactivate any IKE proposals using algorithms that are not FIPS compliant.
- Ensure that installed digital certificates are signed using FIPS-compliant algorithms (SHA-1).
- Configure digital certificates to require FIPS-compliant algorithms.

User Guidance

The user has to choose passwords responsibly and should safeguard them properly without disclosing them.

Tamper Evidence

The VPN Concentrator protects all critical security parameters through the use of tamper evident labels. The administrator is responsible for properly placing all tamper evident labels. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit (CVPN3000FIPS/KIT), which you can order for any validated model. These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

The following sections describe where to apply the tamper evident labels to the VPN Concentrators.

VPN Concentrator Model 3005

VPN Concentrator Model 3005 has a smaller and more compact encasing (1U) than that of the VPN Concentrator models 3015-3080. The main encasing of the VPN Concentrator Model 3005 may be removed like the encasing of a personal computer. The VPN Concentrator's encasing is attached with four screws at the rear of the device. In addition, the VPN Concentrator also has a removable front panel.

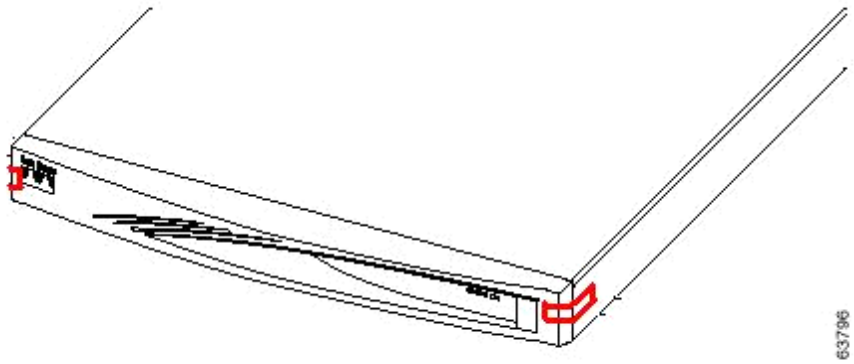
Both the main encasing and front panel of the VPN Concentrator must be protected through the use of tamper evident labels. Apply the serialized tamper-evidence labels as follows:

Step 1 Turn off and unplug the system before cleaning the chassis and applying labels.

Step 2 Clean the chassis of any grease, dirt, or oil before applying the tamper-evident labels. Alcohol-based cleaning pads are recommended for this purpose.

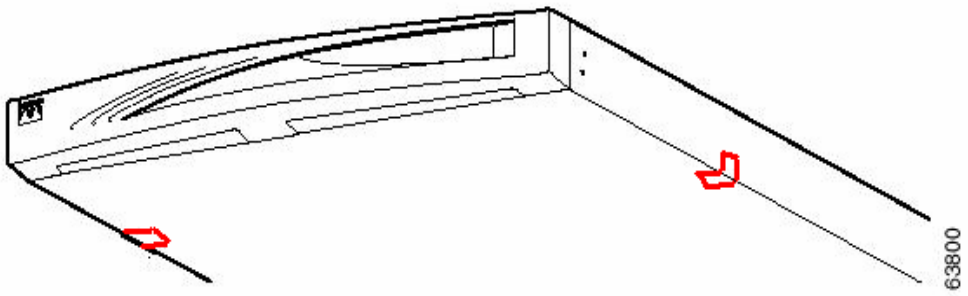
Step 3 Apply two tamper-evident labels one on the front of the box such that the label covers the side of the encasing and the front removable plate (see Figure 1).

Figure 1 Applying Tamper-evident Labels on VPN Concentrator 3005



Step 4 Apply two tamper evident labels on the sides of the box (see Figure 2).

Figure 2 Applying Labels on Sides of VPN Concentrator 3005



Step 5 Record the serial numbers of the labels applied to the system in a security log.

Step 6 Allow a minimum of 12 hours for the labels to cure properly before using the module in a secure mode of operation.

VPN Concentrator Models 3015-3080

The encasing of the VPN Concentrator Models 3015-3080 is very similar to that of the VPN Concentrator Model 3005. The 3015-3080 models have a larger encasing (2U) and use Scalable Encryption Processing modules (SEPs). The main encasing of the VPN Concentrator models 3015-3080 may be removed like the encasing of a personal computer. The VPN Concentrator encasing is attached with four screws at the rear of the device. In addition, the VPN Concentrator also has a removable front panel.

The main encasing, front panel, and side panel of the VPN Concentrator must be protected through the use of tamper evident labels.

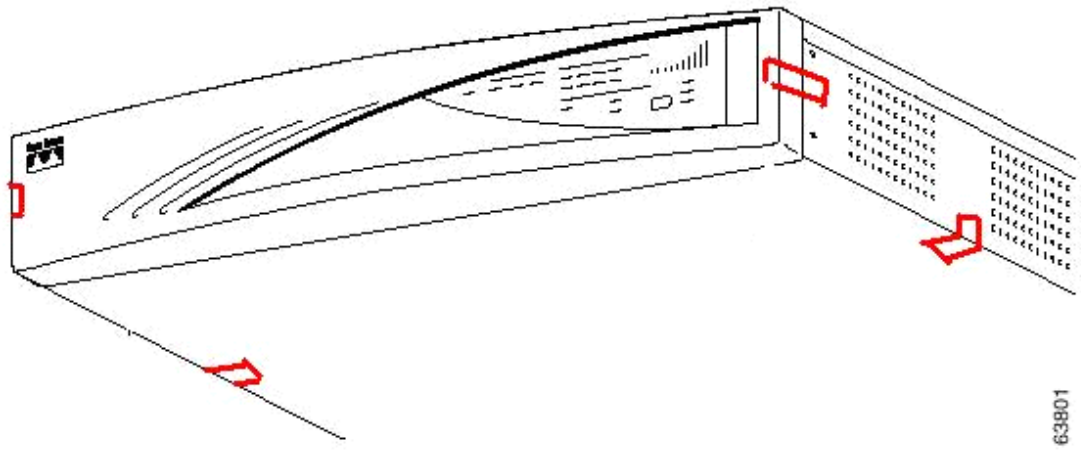
In addition, VPN Concentrator Models 3015-3080 employ SEPs to accelerate IPSec cryptographic operations. The SEPs are located at the back panel of the VPN Concentrators. The SEP devices are attached to the VPN Concentrator by two screws. Security labels must be applied across the SEPs to ensure that these devices are not tampered with. Apply tamper evident labels according to the instructions below.

Step 1 Turn off and unplug the system before cleaning the chassis and applying labels.

Step 2 Clean the chassis of any grease, dirt, or oil before applying the tamper-evident labels. Alcohol-based cleaning pads are recommended for this purpose.

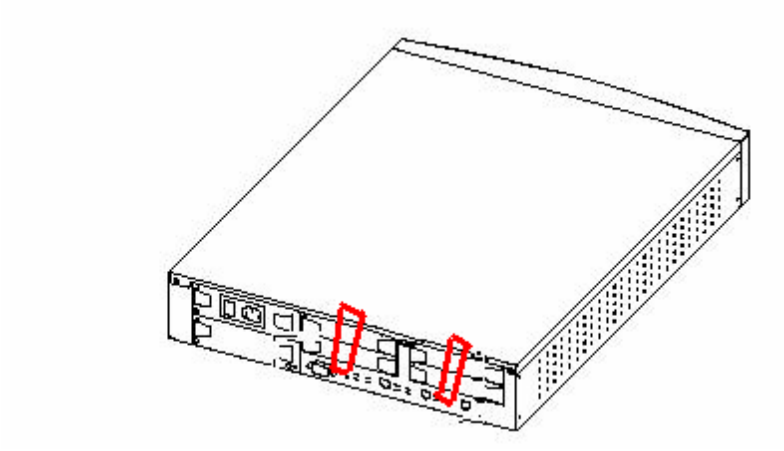
Step 3 Apply four tamper evident labels to the module (see Figure 3). Apply two of the labels to the front removable plate and two to the encasing.

Figure 3 Applying Tamper-evident Labels on VPN Concentrator Models 3015—3080



Step 4 Apply tamper evident labels over the SEP modules at the back of the module. Be careful not to cover the other hardware interface ports with the tamper evidence labels (see Figure 4).

Figure 4 Applying Labels over SEP Modules



Step 5 Record the serial numbers of the labels applied to the system in a security log.

Step 6 Allow a minimum of 12 hours for the labels to cure properly before using the module in a secure mode of operation.

Non-FIPS Approved Cryptographic Algorithms

The following cryptographic algorithms are not FIPS-compliant algorithms.

Symmetric Key Algorithms

- RC4 algorithm

- CBC mode implemented
- 40 and 128 key sizes

Hashing/Authentication Algorithms

- MD5
- HMAC with MD5

Public Key Algorithms

- RSA Encrypt/Decrypt (Key Wrapping) (PKCS#1) allowed for use in FIPS mode
- Diffie-Hellman allowed for use in FIPS mode

Acronyms

ANSI	American National Standards Institute
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HTTP	Hyper Text Transfer Protocol
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
RAM	Random Access Memory
RSA	Rivest Shamir and Adleman
SCEP	Simple Certificate Enrollment Protocol
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security

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