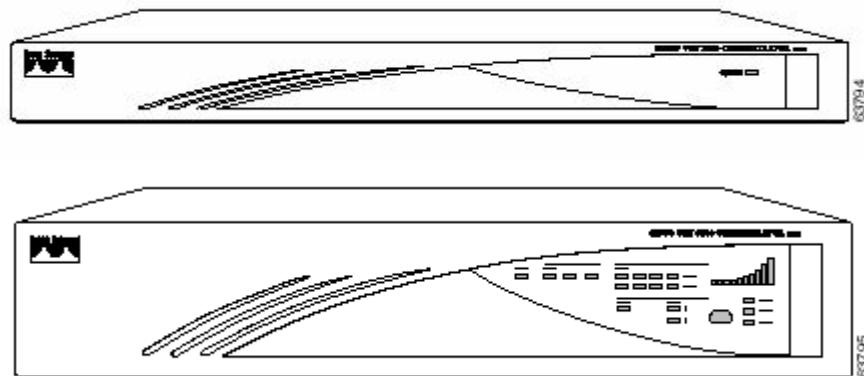




Cisco VPN 3000 Series Concentrators® 3005, 3015, 3030, 3060, 3080



FIPS 140-2 Non-Proprietary Security Policy

**Level 2 Validation
Version 1.4**

April 8, 2004

Table of Contents

INTRODUCTION.....	3
PURPOSE	3
REFERENCES	3
DOCUMENT ORGANIZATION	3
CISCO VPN 3000 SERIES CONCENTRATOR.....	4
OVERVIEW	4
MODULE INTERFACES	4
ROLES AND SERVICES.....	5
<i>Admin Role.....</i>	5
<i>Other Administrator Roles</i>	6
<i>User Role</i>	6
<i>Authentication Mechanisms</i>	6
PHYSICAL SECURITY	7
CRYPTOGRAPHIC KEY MANAGEMENT	7
<i>Cryptographic Keys used by module.....</i>	8
<i>Key Generation</i>	10
<i>Key Entry and Output.....</i>	10
<i>Key Storage</i>	10
<i>Key destruction.....</i>	11
SELF-TESTS.....	11
DESIGN ASSURANCE.....	12
MITIGATION OF OTHER ATTACKS.....	12
SECURE OPERATION.....	12
ADMIN (CRYPTO-OFFICER) GUIDANCE	12
<i>Initial Setup</i>	12
<i>Cryptographic Algorithms</i>	13
<i>Security Relevant Data Items.....</i>	13
<i>Security Protocols</i>	13
<i>Services</i>	13
USER GUIDANCE	14
TAMPER EVIDENCE	14
NON-FIPS APPROVED ALGORITHMS.....	17
ACRONYMS	17

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco VPN 3000 Series Concentrator (3005, 3015, 3030, 3060 and 3080), referred to in this document and the VPN Concentrator. This security policy describes how this VPN Concentrator meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

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 Validated Modules 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 and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

CISCO VPN 3000 SERIES CONCENTRATOR

Overview

The Cisco VPN 3000 Series Concentrators are 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 standalone 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 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 module mapping are described in the following table:

Logical Interface	Physical Interface Mapping
Data Input Interface	10/100BASE-TX LAN Ports, WAN Port
Data Output Interface	10/100BASE-TX LAN Ports, WAN Port
Control Input Sequence	10/100BASE-TX LAN Ports, WAN Port, Console Port, Power Button, Reset Button
Status Output Interface	LEDs, 10/100BASE-TX LAN Ports, WAN Port, Console Port
Power Interface	A DC Input 19V/3.16A 60W power input.

Table 1 – FIPS 140-2 Logical Interfaces

Roles and Services

The module supports role-based authentication. The users are required to enter a password and authenticate to the system in order to perform tasks on it. The module can be accessed 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 module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer role and User role. The module also supports an administrative role and up to four additional administrative roles with restrictive privileges.

The various roles supported by the module are mapped to the Crypto-Officer and User roles as shown below:

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

Each of these roles is described and discussed below.

Admin Role

The Admin user is responsible for configuring the module properly. The Admin can access all the services available via the management interfaces. Descriptions of the services available to the Admin role are provided below.

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

- Performing general configuration (for example, defining IP addresses, enabling interfaces, enabling network services, and configuring IP 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 file 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. The specific crypto services available to the Admin role include:

- Managing certificate enrollment
- Configuring authentication policy
- Managing the accounts of the other administrative accounts
- 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
- 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, and DSA).

Other Administrator Roles

For FIPS, the administrator role is also the crypto-officer. The administrator is a crypto-officer delegated for specific tasks, such as taking backups or managing users. The concentrators implement 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 assumed by supplying the correct username/password combination and passing the appropriate IP address checks. All administrators are responsible for ensuring, that the VPN Concentrator is 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.

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 Concentrator. All user roles are assumed by supplying the correct authentication information. Users are authenticated to the VPN Concentrator based on the authentication protocol established by the administrator (for example, security association ID or IP address and pre-shared secret key combination, identity certificate).

Authentication Mechanisms

The module supports either a username password combination or digital certificates for authenticating IPSec users. To log on to the VPN Concentrators for management

purposes, an operator (Crypto-Officer) must connect to it through one of the management interfaces (Serial Port, SSH, HTTPS over TLS in FIPS mode) and provide a username and password.

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 is also valid for RADIUS or TACACS+ shared secret keys
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.

Table 2 – Estimated Strength of Authentication Mechanisms

Physical Security

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

Cryptographic Key Management

The module uses the following FIPS approved cryptographic algorithms.

- *Symmetric Key Algorithms*

Algorithm	Modes Implemented	Key Sizes
DES (FIPS 46-3)	CBC	56 bits
Triple DES (FIPS 46-3)	CBC	168bits
AES (FIPS 197)	CBC	128, 192, 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 key exchange using the RSA public-key cryptosystem.

Cryptographic Keys used by module

The VPN Concentrator uses a variety of keys during its operation. Below is a complete list of 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 box only access it 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 purposes files stored encrypted in the PKCS#5 format are considered to be stored in plain text.

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.
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 filesystem 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 the 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 VPN3002 module). 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	They are used for authentication during

	HTTPS(TLS) web interface and are stored in plaintext form.	IKE. They are zeroized by either deleting them or by replacing them with new ones.
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 module 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. All keys are generated 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 passwords are stored in clear text format. The RSA/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 will zeroize all the ephemeral session keys.

Self-Tests

The module provides the following power-up self-tests:

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

The VPN Concentrator performs all power-up self-tests automatically each time it starts. 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 in the error log indicating the error and then the module logs the error. In this state the module does not perform any operations. The only way to clear the error by the operator is to check the logs and cycle the power to attempt to clear the error.

In addition, the module 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 in the error log indicating the error and then the module logs the error. In this state the module disables all data output. The operator has to check the logs and cycle the power to attempt to clear the error.

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 system 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 module does not claim to mitigate any attacks in a FIPS approved mode of operation.

SECURE OPERATION

The Cisco VPN3000 Hardware 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 for legacy use: Use the DES algorithm only for protecting low sensitivity information. Cisco recommends that the Triple DES or AES algorithms be used to protect sensitive information

-
- Triple DES encryption/decryption
 - AES encryption/decryption
 - SHA-1 hashing
 - DSA signing and verifying
 - RSA digital signature signing and verifying

The administrator 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.) 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. The VPN 3000 Concentrators do not support software upgrades in a FIPS mode of operation.

Services

To operate in FIPS mode, the Admin (Crypto-Officer) must configure the VPN 3000 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 AES) 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 approved.
- Ensure that installed digital certificates are signed using FIPS approved algorithms (SHA-1).
- Configure digital certificates to require FIPS approved 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.

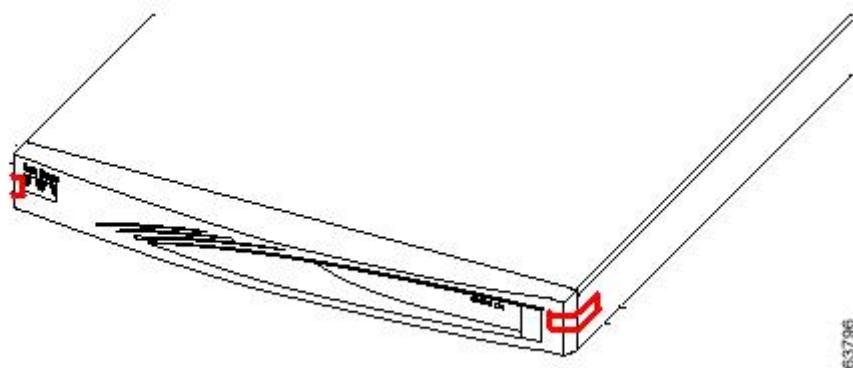
The Crypto-Officer should inspect the tamper evidence labels periodically to verify they are intact.

VPN Concentrator Model 3005

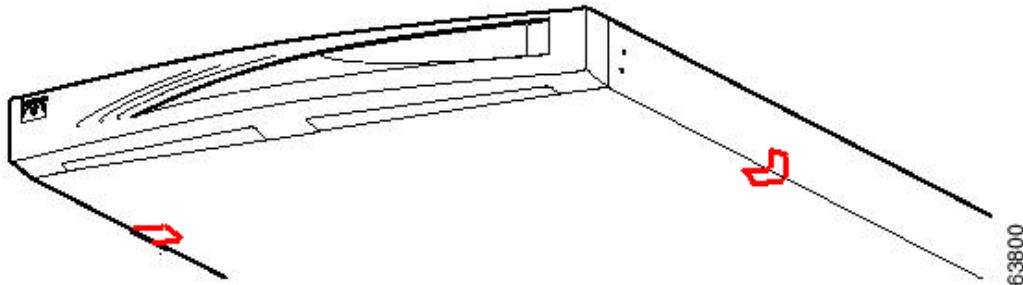
VPN Concentrator Model 3005 has a smaller and more compact encasing (1U) than that of the VPN Concentrator models 3015-3080. The main encasing of the VPN Concentrator Model 3005 may be removed like the encasing of a personal computer. The VPN Concentrator's encasing is attached with four screws at the 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. Application of the serialized tamper-evidence labels is as follows:

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

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. This is illustrated in the following



4. Apply two tamper evident labels on the sides of the box as illustrated in the figure below.



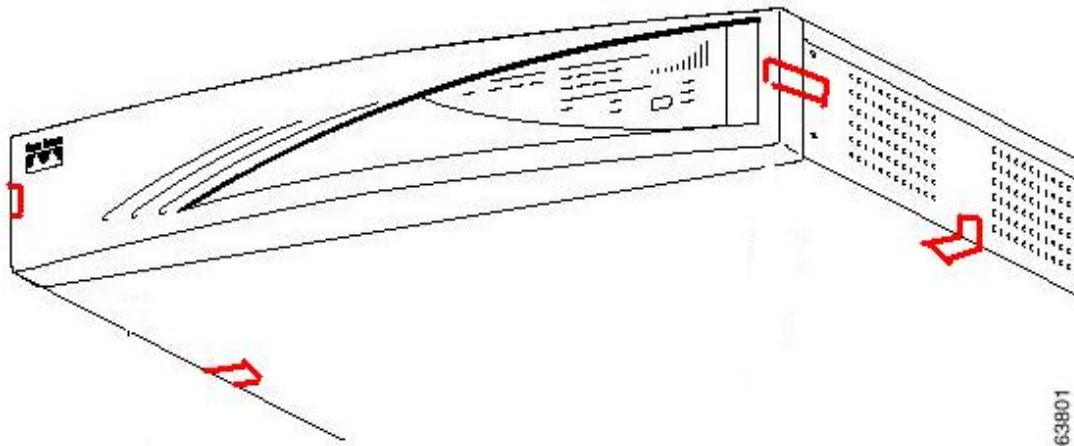
5. Record the serial numbers of the labels applied to the system in a security log.
6. A minimum of 12 hours is required for the labels to cure properly before the module can be used in a secure mode of operation.

VPN Concentrator Models 3015, 3030, 3060 and -3080

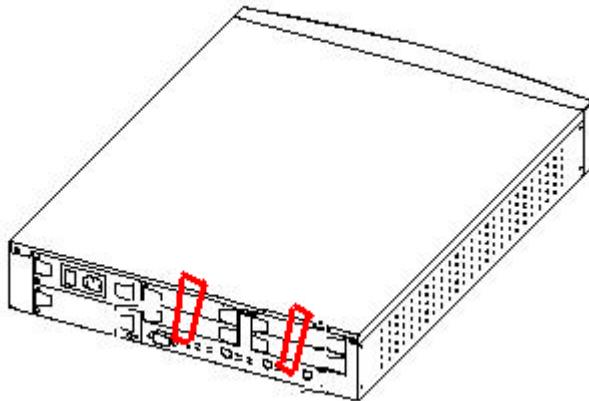
The encasing of the VPN Concentrator Models 3015, 3030, 3060 and 3080 is very similar to that of the VPN Concentrator Model 3005. The 3015, 3030, 3060 and 3080 models have a larger encasing (2U) and use Scalable Encryption Processing modules (SEPs). The main encasing of the VPN Concentrator models 3015, 3030, 3060 and 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, 3030, 3060 and 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. Tamper evident labels are to be applied as described below:

1. Turn off and unplug the system before cleaning the chassis and applying labels.
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.
3. Apply four tamper evident labels to the module as shown in the figure below. Two of the labels are to be applied to the front removable plate and two to the encasing.



4. Tamper evident labels need to be applied over the SEP modules at the back of the module. Care should be taken not to cover the other hardware interface ports with the tamper evidence labels.



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

- A minimum of 12 hours is required for the labels to cure properly before the module can be used in a secure mode of operation.

Non-FIPS Approved Algorithms

The VPN 3000 concentrators uses the following non-FIPS-approved cryptographic algorithms:

- Symmetric Key Algorithms*

<i>Algorithm</i>	<i>Modes Implemented</i>	<i>Key Sizes</i>
<i>RC4</i>	<i>CBC</i>	<i>40, 128</i>

- Hashing Algorithms*

<i>MD5</i>	<i>HMAC MD5</i>
------------	-----------------

- Public Key Algorithms*

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

ACRONYMS

Edit this with acronyms that relate to the module

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