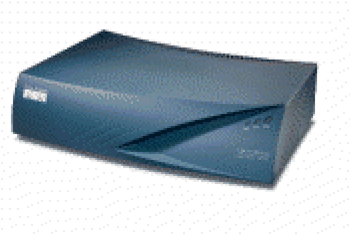
CISCO VPN 3002 and 3002-8E Hardware Clients



FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation
Version 1.3

February 25, 2004

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security policy for the Cisco VPN 3002 and 3002 8E Hardware Client (Firmware version FIPS 3.6.7.F) from Cisco Systems. This security policy describes how the VPN 3002 Hardware clients meet the security requirements of FIPS 140-2 and how to run the module in an approved mode of operation. This module was prepared as part of the Level 2 FIPS 140-2 validation of the VPN 3002.

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 VPN 3002 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the VPN 3002 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 VPN 3002.

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 3002 HARDWARE CLIENT

Overview

The Cisco VPN 3002 and 3002-8E Hardware Client, referred to in this document, as the VPN 3002 is a small hardware appliance that operates as a client in Virtual Private Networking (VPN) environments. It combines the best features of a software client, including scalability and easy deployment, with the stability and independence of a hardware platform. The VPN 3002 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 3002 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 3002 distinguishes between tunneled and non-tunneled traffic and, depending on your server configuration, allows simultaneous access to the corporate network and to Internet resources.

VPN 3002 Interfaces

The VPN 3002 is a multi-chip standalone module and the cryptographic boundary of the module is defined by its metal enclosure. The VPN 3002 provides a number of physical and logical interfaces to the device.

The physical interfaces provided by the VPN 3002 are mapped to the FIPS 140-2 defined logical interfaces: data input, data output, control input, 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	3.3 VDC, 4.55 A power inlet

Table 1 – FIPS 140-2 Logical Interfaces

Roles and Services

The VPN 3002 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 VPN 3002 can be accessed in one of the following ways.

- Serial Port
- Hyper Text Transfer Protocol (HTTP)
- HTTPS (over TLS or SSL)
- Telnet
- Telnet over SSL (Secure Socket Layers)
- SSH

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

The module supports three roles by default. These are mapped to the Crypto-Officer and User roles as shown below:

Role	*FIPS Mapping*
Admin role	Crypto-Officer
Config & Monitor roles	Crypto-Officer
User	User

Each of these roles is described and discussed below.

Admin Role

The Admin is responsible for configuring the VPN 3002 properly, and is considered to be a Crypto-officer role. 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 3002
- Displaying full status of the VPN 3002
- 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 3002 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 crypto services available to the Admin role include:

- Managing certificate enrollment
- Configuring group authentication policy
- Configuring management protocols (public key algorithm, encryption, authentication)
- Configuring filters and access lists for interfaces and users
- Configuring administrator passwords

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 (e.g. IKE negotiations or RSA and DSA digital signatures).

The VPN 3000 Concentrator, in conjunction with which the 3002 hardware client is working, is also considered to be a Crypto Officer role of it. The 3002 hardware client uses the following services from the 3000 concentrator:

- The 3000 Concentrator “pushes” the split tunneling policy to the VPN 3002 over an IPsec tunnel.
- The Concentrators perform the authentication of Users of 3002 on behalf of the 3002. If a User tries to login to the VPN 3002 the authentication information is passed onto the Concentrator over the IPSec tunnel, which verifies the information and sends back the status.

The Concentrator and the hardware client authenticate to each other using public key certificates during IPSec tunnel negotiation.

Config and Monitor Roles

The VPN 3002 supports two additional Administrator roles with restrictive privileges. The Administrator roles are also Crypto-Officers but with lesser privileges. These two roles are called ‘Config’ and ‘Monitor’ and are created by default on the module. The Admin user can disable them or change their passwords.

For FIPS purposes the administrator role is also considered to be a crypto-officer role. The ‘Config’ administrator is a crypto-officer with access rights to Quick Configuration and monitoring. The Monitor administrator is a Crypto Officer with rights to monitoring management options only.

The administrator role is accessed through an Ethernet port using the Web-based administration tool, or by connecting through the console port. All administrator roles are authenticated by the correct username/password combination and passing the appropriate IP address checks.

User Role

Users are the people or entities that wish to send data or traffic through the VPN 3002. Users comprise devices, clients, and anyone passing data through the VPN 3002. Users are authenticated to the VPN 3002 based on the authentication protocol established by the administrator (for example, digital certificates or username and password combination).

Authentication Mechanisms

The VPN 3002 supports either a username password combination or digital certificates for authenticating Users for IPSec tunnel negotiation. To log on to the VPN 3002 for management purposes, an operator (Admin) must connect to the VPN 3002 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 VPN 3002 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.
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

Cisco VPN 3002 Hardware Client is a multi-chip stand-alone cryptographic module.

Cryptographic Key Management

The VPN 3002 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

- *Public Key Algorithms*

RSA (PKCS#1)	DSA (FIPS 186-1)

The VPN 3002 also implements the Diffie-Hellman Key exchange algorithm.
It also uses the TLS protocol, SSH protocol and HTTPS for system management.

Cryptographic Keys used by VPN 3002

The VPN 3002 client uses a variety of keys during its operation. Below is a complete list of keys used by various services and protocols.

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 restarting/resetting 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 restarting/resetting the module.
RSA public/private keys	Identity certificates for the module itself and also used in IPSec negotiations.	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. For FIPS purposes this is considered plain text storage. They are stored in Flash memory and no one can access the Flash to access these keys. They can be zeroized by overwriting them with new keys by storing under the same filename.

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. For FIPS purposes this is considered plain text storage. They are stored in Flash memory and no one can access the Flash to access these keys. They can be zeroized by overwriting them with new keys by storing under the same filename.
Diffie-Hellman Key Pairs	Used by the VPN 3002 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. They are zeroized by resetting/rebooting the module.
Public keys	The VPN 3002 stores public keys of client systems that use the VPN 3002. It also receives the public key of the VPN 3002.	These can be either deleted by the Admin 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 using KEK1 and are zeroized when the 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 zeroized by resetting/changing the user passwords.
Password table	Critical security parameters used to authenticate the Crypto-Officer logging in on to the machine.	They are stored in NVRAM and are zeroized by overwriting the password with a new one.
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 3002 uses PKCS10 format for certificate requests. It also supports the Simple Certificate Enrollment Protocol (SCEP).

Only the Crypto-Officer can logon to the module through an administrative interface (console or web interface). All users access only the services provided by the module. Hence the CSPs stored on the disk are accessed directly only by the Crypto-Officer.

Key Generation

The VPN 3002 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 3002.

Key Storage

All cryptographic keys are stored in encrypted form using Key Encryption Keys (KEKs). The only keys that are stored in plain-text form are the KEKs and IPSec pre-shared keys. KEKs are not accessible to anyone and are stored in flash. 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. Keys encrypted with a pass-phrase based PKCS#5 are considered plain text for FIPS purposes.

Key Destruction

As required by FIPS 140-2, all keys can be destroyed and the VPN 3002 zeroizes all keys prior to their destruction. Also performing a hardware or software reboot will zeroize all the ephemeral session keys.

Self-Tests

The VPN 3002 provides the following power-up self-tests:

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

The VPN 3002 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 message. In this state the module does not perform any operations. The operator has 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 for RSA key pair generation, and
- Continuous Random Number Generator Test for the FIPS-approved RNG.

In the unlikely event that 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.

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 VPN 3002 doesn't claim to mitigate any attacks in a FIPS approved mode of operation.

SECURE OPERATION

The Cisco VPN 3002 Hardware Client meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the VPN 3002 in FIPS-approved mode of operation (FIPS mode).

Crypto-Officer Guidance

The following are instructions to the 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 crypto-officer must configure
and enforce on the VPN 3002s:

- Only FIPS approved cryptographic algorithms to be used
- Only the IPSec protocol may be enabled for protection of traffic.
- 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 has to make sure the corresponding Concentrator is also operating in a FIPS mode.

Cryptographic Algorithms

VPN 3002s support many different cryptographic algorithms. However, to properly use VPN 3002s 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 3002s to use only the cryptographic algorithms listed above for all services that they provide.

Security Relevant Data Items

VPN 3002s 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 3002 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 3002s.

Services

To operate in FIPS mode, the Crypto-Officer must configure the VPN 3002 Client as follows:

- Enable HTTPS only. Disable HTTP for performing system management.
- Configure SSL to use only FIPS compliant encryption algorithms (DES, 3DES, AES, 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.
- Ensure that installed digital certificates are signed using FIPS compliant algorithms (SHA-1).
- Configure SSH to use only the FIPS approved encryption algorithms.
- Firmware upgrades are not to be performed in a FIPS mode of operation.

User Guidance

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

Tamper Evidence Labels

The VPN 3002 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 main encasing of the VPN 3002 may be removed like the encasing of a personal computer. The VPN 3002's encasing is attached with four screws at the bottom of the device. 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 each side of the box such that the label covers the side of the encasing and the bottom of the box.
4. Record the serial numbers of the labels applied to the system in a security log.
5. 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.

The Crypto-Officer should inspect the tamper evidence labels periodically.

Non-FIPS Approved Algorithms

The VPN 3002 uses the following non-FIPS-approved cryptographic algorithms:

- *Symmetric Key Algorithms*

Algorithm	*Modes Implemented*	*Key Sizes*
RC4	*CBC*	*40, 128*

- *Hashing Algorithms*

MD5	*HMAC MD5*

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
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL
IKE	Internet Key Exchange
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
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security