Cisco VPN 3002 Hardware Client Security Policy

Introduction

This security policy describes how the VPN 3002 Hardware Client meets the security requirements of FIPS 140-1, and how to operate a VPN 3002 using IPSec encryption in secure FIPS 140-1 mode. This policy was prepared as part of the Level 2 FIPS 140-1 validation of the VPN 3002 Hardware Client, sometimes referred to in this document as the VPN 3002.

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

FIPS 140-1 (Federal Information Processing Standards Publication 140-1—Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available in the following document:

Security Requirements for Cryptographic Modules, FIPS Publication 140-1 (http://csrc.nist.gov/publications/fips/fips140-1/fips1401.htm).

For information about the FIPS 140-1 validation program, see the following NIST website:

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 3002 only in the technical terms of FIPS 140-1 cryptographic module security policy. More information is available on the VPN 3002 Hardware Client in the following documents:

VPN 3002 Hardware Client Getting Started, Release 3.1, August 2001—explains how to unpack and install the VPN 3002 and how to configure the minimal parameters.

VPN 3002 Hardware Client Reference, Release 3.1, August 2001—explains how to start and use the VPN 3002 Hardware Client Manager and how to configure your device beyond the minimal parameters you set during quick configuration. This guide also explains and defines all functions available in the Administration and Monitoring screens of the VPN 3002 Hardware Client Manager.

VPN 3002 Hardware Client Quick Start card summarizes information for quick configuration.

VPN 3002 Hardware Client Basic Information sticky label summarizes information for installing the VPN 3002 and beginning configuration.

Release Notes for Cisco VPN 3002 Hardware Client, FIPS Release 3.1.3

Terminology

This document uses the following terminology.

AH	Authentication header.
ESP	Encapsulation security payload.
FIPS 140-1	*Federal Information Processing Standards Publication 140-I—Security Requirements for Cryptographic Modules* details the U.S. Government requirements for cryptographic modules.
FIPS Mode	A configuration of the VPN 3002 Hardware Client that allows users to use the VPN 3002 in a way that is compliant with the government standard FIPS 140-1.
IPSec	A family of IETF protocols that provide network layer encryption.
IKE	A key management protocol used by IPSec for authentication and secret key derivation.

VPN 3000 Series Concentrators and the Cisco VPN 3002 Hardware Client

Cisco VPN 3000 Series Concentrators comprise a family of purpose-built, remote access Virtual Private Network (VPN) platforms that incorporate high availability, high performance, and scalability with the most advanced encryption and authentication techniques available today.

The VPN 3002 Hardware Client communicates with a VPN 3000 Series Concentrator to create a virtual private network across a TCP/IP network (such as the Internet). The VPN 3002 provides an alternative to deploying the software VPN Client at remote locations.

FIPS 140-1 Applicability

The VPN 3002 is a Multiple-Chip Standalone Cryptographic Module as defined in *Security Requirements for Cryptographic Modules*, FIPS publication 140-1. The cryptographic boundary for each VPN 3002 module is the actual physical embodiment of each device.

This security policy pertains to the VPN 3002 Hardware Client (3002 and 3002-8E), Release Version 3.1 FIPS. The VPN 3002 is intended to meet the overall requirements for FIPS-140 Level 2 security as defined in FIPS-140-1. Table 1 shows the security level requirements met for the VPN 3002:

Table 1 Security Level Requirements

Security Requirements Section	FIPS-140 Security Level
Cryptographic Module	2
Module Interfaces	2
Roles & Services	2
Finite State Machines	2
Physical Security	2
Software Security	3
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	3
Self Tests	2

Roles and Services

The VPN 3002 implements a role-based authentication mechanism. Up to three administrative roles can be defined with the restriction that at least one administrator must serve as a superuser (an administrator with the highest level of privileges). The highest level administrator is also known as the Crypto-officer in FIPS 140-1 terminology.

There can be multiple simultaneous administrative sessions active in the VPN 3002 at one time. The access methods for the administrative roles as well as the services available for each role are listed below. For detailed descriptions on configuration, see the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

Administrator (Superuser) Role

For the VPN 3002, the superuser is the highest level administrator. To access the administrator role, connect through an Ethernet port and use the web-based administration tool or connect through the console port.

The administrator must enter the correct username/password combination and pass the appropriate IP address checks. The administrator role can access all the services accessible via any management interface. Administrators are responsible for ensuring that VPN 3002s are configured properly to meet all FIPS 140-1 requirements.

Warning **There is no way to recover your system if you forget the Administrator password. Take appropriate measures to safeguard your password and remember it. If you forget the Administrator password, you cannot log in to your system and you will have to return the VPN 3002 to be recovered.**

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 enabling 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 stored in memory, and also the version saved in NVRAM, 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. Some of these are policies that the administrator configures on the VPN Concentrator at the central-site. The VPN Concentrator then pushes these policies to the VPN 3002 Hardware Client. Some of the specific crypto services available to the administrator role include:

- Managing certificate enrollment
- Configuring remote access users including groups, user accounts, authentication policy, and encryption policy
- Managing remote user address pools
- Configuring authentication servers
- Policy management (public key algorithm, encryption, authentication)
- Configuring filters and access lists for interfaces and users
- Configuring administrator privileges

Administrators 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” in the *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* user guide.

Administrator Role (Non-Superuser)

You also access the non-superuser administrator role through an Ethernet port using the web-based administration tool or connect 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 3002s are configured properly to meet all FIPS 140-1 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 | Administrators” in the *VPN 3002 Hardware Client Reference*.

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. All user roles are entered by supplying the correct authentication information. Users are authenticated to the VPN 3002 based on the authentication protocol established by the administrator (for example, security association ID or IP address and preshared secret key combination).

Table 2 Services by Module and Role

Services	Roles	Description
Encryption/Decryption	Crypto-officer/User	The module encrypts data being sent by both the crypto-officer and user. Crypto-officer services and data sent are encrypted through HTTPS (TLS) sessions. User-sent data is encrypted/decrypted as defined by the IPSec standard.
Show Status	Crypto-officer	The crypto-officer can view the module status through the module’s administrative interface.
Self-Tests	Crypto-officer	The crypto-officer can perform self-tests and review self-test results.
System Configuration	Crypto-officer	The crypto-officer can configure user and administrator privileges, and other system parameters.
Key Entry	Crypto-officer	The crypto-officer must enter all IPSec preshared keys.

Module Interfaces

As mentioned above, the cryptographic boundary encompasses the physical encasing of the VPN 3002. Table 3 maps the FIPS 140 logical interfaces to the physical interfaces of the VPN 3002.

Table 3 FIPS 140-1 Logical Interfaces

FIPS 140-1 Logical Interfaces	VPN 3002 Physical Interfaces
Data input	Ethernet ports, Console port
Data output	Ethernet ports, Console port
Control input	Ethernet ports, Console port
Status output	Ethernet ports, LEDs

Security Relevant Data Items

The following is a list of all security relevant data items used by the VPN 3002. This section describes all keys that the VPN 3002 uses.

Key Encryption Keys

The VPN 3002 uses Key Encryption Keys (KEK) to protect all persistent and ephemeral cryptographic keys that the VPN 3002 stores. The VPN 3002 uses two KEKs (KEK_1 and KEK_2).

KEK_1 is a triple DES key that protects all traffic keys, HMAC keys, and Diffie-Hellman private keys. KEK_1 is used to decrypt the appropriate cryptographic key prior to use. KEK_1 is stored in RAM in plaintext form.

KEK_2 is a DES key that protects DSA private keys, RSA private keys, and the Diffie-Hellman shared secret (g^{xy}) private keys. KEK_2 is used to decrypt the appropriate cryptographic keys prior to use by the module. KEK_2 is stored in RAM in plaintext form.

Authentication Keys

This section describes authentication keys.

DSA Key Pair

The VPN 3002 uses DSA key pairs for authentication in establishing an IKE session. DSA key pairs are stored encrypted with KEK_2.

RSA Key Pairs

The VPN 3002 uses RSA key pairs for authentication in establishing an IKE session. RSA key pairs are stored encrypted with KEK_2.

IKE—Preshared Keys

The VPN 3002 uses IKE preshared keys for authentication in establishing an IKE session. IKE preshared keys are stored in plaintext form.

HMAC Keys

The VPN 3002 uses HMAC keys for authenticating and verifying the integrity of packets as a part of the IPSec protocol. These keys, generated during IKE negotiation, are used when the AH or ESP is chosen and are stored encrypted with KEK_1.

Diffie-Hellman Key Pairs

The VPN 3002 uses Diffie-Hellman key pairs for authentication in establishing an IKE session. Diffie-Hellman private keys and shared secrets (g^{xy}) are encrypted and stored using KEK_2.

Traffic Keys

All traffic keys are encrypted with KEK_1.

IPSec DES/3DES Keys

The IPSec DES/3DES keys are the traffic encryption keys that protect information passing through the VPN 3002. These keys are generated during the IKE negotiation process. Once these keys are no longer in use for encrypting/decrypting traffic, they are zeroized.

TLS Traffic Keys

TLS traffic keys provide protection of data during administration of the VPN 3002 via HTTPS. These keys are generated ephemerally and are zeroized after the TLS session has ceased.

SSL Traffic Keys

SSL traffic keys provide protection of data during administration of the VPN 3002 via HTTPS. These keys are generated ephemerally and are zeroized after the SSL session has ceased.

PPP Traffic Keys

PPP traffic keys are traffic keys that provide protection of information passing through the VPN 3002. These keys are generated ephemerally during the PPTP negotiation process, and discarded after they are used.

Public Keys

The following public keys are stored within a VPN 3002. All public keys used by the VPN 3002 are stored within a certificate and signed by the issuing authority, thus protecting certificates from modification.

Issuing/Root Certificate Authority

The VPN 3002 might be loaded with the root CA certificate and any subordinate CA's within a PKI. These public keys verify the identity of any certificates issued within a particular PKI.

SSL Server

An SSL certificate might also be loaded onto the VPN 3002. The SSL certificate authenticates the VPN 3002 when an administrator establishes a secure connection (HTTPS) for configuration.

Server Identity

A Server identity certificate binds the public key(s) to the VPN 3002. This certificate authenticates the VPN 3002 during the IKE process.

Cryptographic Algorithms

For a list of all cryptographic algorithms supported by the VPN 3002, see Appendix A.

Security Rules (FIPS Mode of Operation)

This section defines how to use and configure the VPN 3002 to ensure compliance with the FIPS 140-1 standard. The administrators are jointly responsible for configuring the VPN 3002 in FIPS mode. The following list is a summary of the security rules that the administrator must configure and enforce on the VPN 3002:

- Only FIPS approved cryptographic algorithms are to be used
- 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 140-1 standard.

The following sections describe in more detail the security rules summarized above.

Cryptographic Algorithms

The VPN 3002 supports many different cryptographic algorithms. However, to properly use the VPN 3002 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[1]
- Triple DES encryption/decryption
- SHA-1 hashing
- DSA signing and verifying
- RSA digital signature signing and verifying

The administrator must configure the VPN 3002 to use only the cryptographic algorithms listed above for all services that they provide.

Security Relevant Data Items

The VPN 3002 stores many security relevant data items, such as authentication keys (Preshared keys, DSA or RSA private keys, etc.) 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 the VPN 3002.

The superuser or administrator can zeroize all critical security parameters by issuing the zeroize command through the administrative interface.

1. The DES algorithm should only be used for the protection of low sensitivity information. It is recommended that Triple DES be used for protection of highly sensitive information.

Security Protocols

The VPN 3002, by design, supports only the IPSec tunneling protocol for protecting data transfer.

The VPN 3002 has the capability to update the firmware in a secure manner. The administrator must first zeroize all critical security parameters prior to loading new firmware. Because the VPN 3002 stores two images of firmware, the administrator must load the firmware successfully twice to ensure that both images stored contain the firmware that is being loaded.

Please note that the administrator is responsible for acquiring the firmware image from a valid Cisco distribution center and for ensuring that this firmware is a FIPS 140-1 validated module.

Administration Management Access Methods

The VPN 3002 allows the following administrative access methods:

- HTTP
- Console/TELNET (clear text password)
- HTTPS (SSL protocol or TLS protocol)
- SSH

Each access method requires that the administrator enter a password for access. The password is checked against a clear-text password stored in RAM on the VPN 3002.

The VPN 3002 also can restrict access based on the IP address of the administrator. For the protocol-based access methods, the source IP address is checked against a configured list of addresses stored on the VPN 3002.

In addition, the VPN 3002 can be administered remotely. An administrator can manage the VPN 3002 through a direct connection to the console port or through any of the Ethernet interfaces. The administrator can administer and configure the VPN 3002 through either a command-line interface or through the web-based administration application.

Although all of the access modes listed above are supported, based on the rules of the FIPS 140-1 standard, the only access method that may be used to provide encrypted protection of all data and configuration information is HTTPS (using the TLS protocol). All other access methods supported by the VPN 3002 either use nonFIPS approved cryptographic algorithms for encryption (HTTPS (SSL) or SSH) or do not support any encryption mechanism at all (Telnet/Console).

Therefore to operate in FIPS mode, you must configure the VPN 3002 as follows:

- Enable HTTPS only.
- Configure SSL to use only FIPS compliant encryption algorithms (DES, 3DES) and set SSL version to TLS V1.
- Configure the Event subsystem to avoid sending events to the console.
- Disable Telnet server.
- Disable all external authentication servers such as RADIUS, TACACS, and so on (configured on the central-site VPN Concentrator).
- Deactivate any IKE proposals using algorithms that are not FIPS compliant (configured on the central-site VPN Concentrator).
- Ensure that installed digital certificates are signed using FIPS compliant algorithms (DSA/RSA).
- Configure digital certificates to require FIPS compliant algorithms.

Once configured, in the web-based administration application, click Configuration > FIPS Compliance to learn whether the VPN 3002 is operating in FIPS mode.

Tamper Evidence

The VPN 3002 Hardware Client is significantly smaller than the VPN 3000 Series Concentrators, with a removable plastic cover. The VPN 3002 Hardware Client protects all critical security parameters through the use of tamper evident labels.The security labels recommended for FIPS 140-1 compliance are provided in the FIPS Kit (CVPN3000FIPS/KIT), which can be ordered for any validated model. These security labels are very fragile and can not be removed without clear signs of damage to the labels.

The administrator is responsible for properly placing all tamper evident labels on the plastic cover of the VPN 3002 Hardware Client.

Self-Tests

A VPN 3002 implements both power-up and conditional self-tests to ensure that the module is functioning properly at all times.

Power-up Tests

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 indicating the error and then the module transitions into the FAILURE state. This state does not allow the module to perform any additional operations. The operator may power cycle the module to attempt to clear the error.

Each VPN 3002 performs the following power-up self-tests as defined in the FIPS 140-1 standard:

- DES/TDES Known Answer Test
- SHA-1 Known Answer Test
- DSA Algorithm Test
- RSA Algorithm Test
- Software/Firmware Test

Conditional Tests

Each VPN 3002 also performs the following conditional self-tests:

- Pairwise Consistency Test (DSA and RSA)
- Continuous Random Number Generator Test

In the unlikely event a conditional self-test fails, an event is displayed indicating the error and then the module transitions into the HALTED state. This state does not allow the module to perform any additional operations. The operator may power cycle the module to attempt to clear the error.

Appendix A—Cryptographic Algorithms

This appendix lists cryptographic algorithms that are approved for FIPS and others that are not FIPS approved.

FIPS Approved Cryptographic Algorithms

The following cryptographic algorithms are approved for FIPS operation.

Encryption Algorithms

- 56-bit DES – Certificate #147
- 168-bit Triple DES – Certificate #86

Hashing/Authentication Algorithms

- SHA-1 – Certificate #73
- HMAC with SHA-1 – Certificate #73 (Vendor Affirmed)

Digital Signature Algorithms

- DSA – Certificate #54
- RSA (Vendor affirmed)

Non-FIPS Approved Cryptographic Algorithms

The following cryptographic algorithms are not FIPS compliant algorithms.

Encryption Algorithms

- 40- and 128-bit RC4

Hashing/Authentication Algorithms

- MD5
- HMAC with MD5
- Diffie-Hellman