1C - FIPS 140-2 Cisco VPN Client Security Policy

This document describes the Cisco VPN Client security policy.

Introduction

This non-proprietary cryptographic module security policy describes how version 3.6.5 of the Cisco software VPN Client meets the security requirements of FIPS 140-2, and how to run the VPN Client in secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the VPN Client. The Cisco Software VPN Client is referred to in this document as the VPN Client, the software client, and 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/

This document contains the following sections:

References

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

The Cisco Systems Inc. website (http://www.cisco.com) contains information on the full line of products from Cisco Systems Inc.

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.

*Cisco VPN Client User Guid*e, *Release 3.6*—explains how to install, configure, and use the VPN Client. The VPN Client lets a remote client use the IPSec tunneling protocol for secure connection to a private network through the VPN device.

Cisco VPN Client Administrator Guide, Release 3.6—tells how to configure a VPN 3000 Concentrator for remote user connections using the VPN Client, how to automate remote user profiles, how to customize VPN Client software, how to use the VPN Client command-line interface, and how to get troubleshooting information.

Release Notes for Cisco VPN Client, FIPS Release 3.6 Through 3.6.5

You can find this documentation at the website http://www.cisco.com.

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.

Software VPN Client

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

Overview

The Cisco Software VPN Client is a set of software applications that runs on a Microsoft ® Windows ® -based PC configured in a single-user mode. The VPN Client running on a remote PC and communicating with a Cisco VPN device at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user. This secure connection is a Virtual Private Network (VPN).

Some of the features of the VPN Client are:

- Support for ASA and PIX firewalls, VPN 3000 Series Concentrator Release 3.0 and above, and IOS devices (VPN Client Release 3.0 and above will not work with Releases 2.x of the VPN 3000 Concentrator.)
- Command-line interface to the VPN Dialer
- Local LAN access—The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN server (if the central site grants permission)
- Automatic VPN Client configuration option—the ability to import a configuration file
- Log Viewer—An application that collects events for viewing and analysis
- Set MTU size—The VPN Client automatically sets a size that is optimal for your environment
- Automatic connection using Microsoft Dial-Up Networking or any other third-party remote access dialer
- NAT Transparency (NAT-T), which lets the VPN Client and the VPN Concentrator automatically detect when to use IPSec over UDP to work properly in Port Address Translation environments
- Support for Dynamic and Split DNS (DDNS hostname population)
- Certificate Manager—An application that lets you manage your identity certificates
- Ability to use Entrust Entelligence certificates
- Peer Certificate Domain Name Verification—A feature that prevents a client from connecting to an invalid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the client connection also fails.

Note For a complete list of features, see *VPN Client User Guide, Release 3.6.*

VPN Client Interfaces

The VPN Software Client is a software module that runs on the Windows platform. It runs on the following Operating Systems:

- Windows 2000
- Windows XP

The cryptographic boundary of the software client supports the physical interfaces of the standard PC. The physical interfaces include the computer keyboard port, CDROM drive, floppy disk, mouse, network port, monitor port and power plug. The PC network port includes the serial ports, parallel ports, Ethernet ports and NIC cards. The functional module interface exists in the software.

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Table 1 VPN Client Physical Interfaces and Logical 140-02 Interfaces

VPN Client Physical Interface	FIPS 140-2 Logical Interface
PC network port, keyboard interface, mouse port, floppy drive, CDROM drive	Data input interface
PC network port	Data output interface

Table 1 VPN Client Physical Interfaces and Logical 140-02 Interfaces (continued)

PC network port, keyboard port, mouse port, PC power button	Control input interface
LEDs, PC monitor, PC network port	Status output interface
PC power interface	Power interface

The physical interfaces are mapped to the logical interfaces in the following way:

Table 2 FIPS 140-2 Logical Interfaces

Logical Interface	Program Mapping
Control Input	The VPN Dialer (ipsecdialer.exe) and Set MTU (setmtu.exe) programs control input. A network administrator uses the VPN Dialer program to configure tunnel parameters and establish security associations and the Set MTU program to set the network packet parameters, if necessary. The VPN device pushes security policies and parameters to the VPN Client. In addition, the following programs also control input: certmgrgui.exe, cvpnd.exe, ipseclog.exe, ipsxauth.exe, ppptool.exe, vpnclient.exe, cvpndrv.sys, and csgina.dll.
Data Input	The data input is all data coming into the network port. Programs providing this interface are: cvpnd.exe, ppptool.exe, cvpndrv.sys.
Data Output	The data output is any data sent through the network stack. This includes all application data (mail, browser, telnet etc). Programs providing this interface: cvpnd.exe, ppptool.exe, cvpndrv.sys
Status Output	The status output comprises all messages either logged by the module or returned by the module. The error messages from IKE negotiations are also status output. To view the logged error messages, use the log viewer program. Programs providing this interface are: certmgrgui.exe, cvpnd.exe, ipsecdialer.exe, ipseclog.exe, ipsxauth.exe, ppptool.exe, setmtu.exe, vpnclient.exe, cvpndrv.sys, and csgina.dll

The VPN Client provides programs with Graphical User Interfaces to configure and interact with the module. The following is a list of executables that the module uses.

Table 3 VPN Client Executables

Executable	Description
VPNClient.exe	Command line version of the VPN Client, opens VPN tunnels and looks at tunnel statistics
CertMgrGUI.exe	GUI manager for certificates; imports, requests, enrolls, and exports certificates
cvpnd.exe	VPN Client service; handles communication between all aspects of VPN client, performs IKE, and keeps track of all connection statistics
ipsecdialer.exe	GUI for VPN Client; connects/disconnects VPN tunnels, creates profiles, and gets statistics

Table 3 VPN Client Executables (continued)

ipsxauth.exe	Authentication program; performs XAuth, executes XAuth for cvpnd.exe
ppptool.exe	Creates dialup connections
SetMTU.exe	Sets MTUs for Ethernet and dialup adapters
vpnclient.ini	Provides the main configuration file of the VPN Client, containing all the global parameters and parameter settings
cvpndrv.sys	The VPN device driver
Csgina.dll	The DLL supports that the Start Before Logon feature

Roles and Services

As required by FIPS 140-2, there are two main roles in the module that operators may assume: *crypto officer* and *user*. These roles are logically separated. The VPN Client does not implement authentication mechanisms for any role. Also the module does not allow concurrent operators.

The operators can access all keys and services in the module, because they are separated only logically.

Crypto Officer Role

The crypto officer can start the VPN service, install identity certificates and import user/tunnel certificates. All the services available to the user are also available to the crypto officer. For descriptions of the services available to the crypto officer and user roles, see Table 4.

Configuring, managing and monitoring the VPN Concentrator, with which the client is working, is also considered to be a crypto officer role. The VPN Concentrator pushes the split tunneling policy to the VPN Client software over an IPsec tunnel and is responsible for assuring that only FIPS-Approved algorithms are used for IPSec negotiations.

User Role

A user can access the VPN service provided by the module and create tunnels with the proper authentication. Service descriptions and inputs/outputs are listed in the following table:

Table 4 Services that Crypto Officers and Users Can Perform

Service	Authorized Roles	Description, Inputs and Outputs
Installing and Uninstalling the module	crypto officer	Installs and uninstalls the VPN Client.
Starting and stopping the VPN service	crypto officer	Starts the VPN service (IPSec daemon) through the windows services interface. The VPN Client displays an error message if the IPSec module fails to load successfully. The inputs to the service are the various configuration files in the module that contain keys and security association (SA) information.

Table 4 Services that Crypto Officers and Users Can Perform (continued)

Installing the CA certificate	crypto officer	Installs the CA certificate through the Certificate Manager application. The CA certificate is imported into the module through the Certificate Manager. Input to this service is the CA certificate. No keys are output here. The module displays an error message if the certificate is corrupted or is in an unexpected format/encoding.
Generating identity keys for Users/Tunnels	crypto officer	Identity keys used in tunnel establishment are generated through the Certificate Manager. Invoking the Certificate Manager and making a certificate request are the inputs to this service. The module outputs the public key generated in the certificate request.
Importing identity keys for Users/Tunnels	crypto officer	Identity keys in the form of certificates used in tunnel establishment can be imported into the module through the Certificate Manager. The module displays an error message if the certificate is corrupted or is in an unexpected format/encoding. Inputs to the service are the identity keys imported into the module.
Configuring user/tunnel characteristics (Group Id and Password or Digital Certificates for Authentication)	crypto officer	Used in creating IPSec tunnels. Inputs are the group ids, passwords and/or digital certificates to the service. The module displays an error message if the password entries (entered twice to check for correctness) do not match or if the certificate is corrupted or is in an unexpected format/encoding.
Creating IPSec tunnels	user, crypto officer	Both users and a crypto officer can create tunnels. Input is the SA information stored previously and the corresponding keys. If the SA configuration information is wrong the module displays error.
Setting the MTU for packet transfer	crypto officer	The crypto officer configures the maximum transferable packet length through the Set MTU program interface.
Showing status; performing Self-Tests	crypto officer	The crypto officer can view the log files through the View Log program interface. The current status of the module including the self-test-output information can be seen in the log files.

Physical Security

Cisco Software VPN Client is a multi-chip-standalone cryptographic module. The module’s physical boundary is the PC case in which it is running. The module is enclosed in a removable PC cover, which is an industry standard, production grade covering on all standard PCs.

Cryptographic Key Management

The module uses the following FIPS-approved algorithms.

- Symmetric Key Algorithms

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

- Hashing Algorithm
  - SHA-1 (FIPS 180-1)
- Message Authentication Algorithms
  - HMAC SHA-1 (FIPS-198)
  - DES MAC (FIPS-113)
  - Triple DES MAC (FIPS-113)
- Public Key Algorithm
  - RSA sign/verify (PKCS#1)

The certificate numbers of the algorithms are as follows:

- SHA-1: Cert.# 153
- DES: Cert.# 212
- Triple DES: Cert.# 169
- AES: Cert.# 58
- RSA (PKCS #1) digital signature verification (vendor affirmed)
- HMAC SHA-1: Cert.# 153, vendor affirmed
- DES MAC: Cert.# 212, vendor affirmed
- Triple DES MAC: Cert.# 169, vendor affirmed

The module supports the following non-FIPS approved algorithms:

- MD5
- HMAC-MD5
- Diffie-Hellman Algorithm

The VPN Client supports only logical separation of users and operates in a single user mode. Hence the files (containing keys) in the module have read, write access permissions for all users. The operating system principles of file locking and open file access restriction (no other process can write/delete a file opened by another process) prevent unwanted modification or deletion of files. As an exception, operators do not have read and write access to the IPSec session keys, which are stored in RAM, but can zeroize (Delete) them by closing the VPN tunnel.

The VPN Client supports the following critical security parameters:

Table 5 Security Parameters that the VPN Client Supports

Cryptographic Key	Description	Key Type	Storage and Zeroization
RSA public/private keys	Identity certificates for the module itself and also in IPSec negotiations	RSA public/private keys (1024/2048 bits)	Stored encrypted using a password-based encryption based on PKCS#5 standard. The private key is zeroized by deleting the corresponding identity certificate using Certificate Manager.
Group ID and passwords	Group id and passwords corresponding to the VPN Concentrator at the other end; established by the crypto officer	An alphanumeric string with a minimum length of 6 characters	Stored in files in plain text form; zeroized when the crypto officer overwrites passwords to change them.
Pre-shared keys	Used in IPSec negotiations; derived from the group id and password at the other end of the VPN tunnel	A string derived from the group id and password	Derived from the group id and password for each tunnel whenever required. The memory location that stores a pre-shared key (they are stored in RAM) is freed when an IPSec tunnel is terminated and cannot be accessed
IPSec Session Keys	Generated in IPSec transactions to encrypt tunnels; destroyed when the tunnel is destroyed	Either DES, AES or 3DES keys depending on the negotiated algorithm	Stored only in volatile memory (RAM); zeroized once an IPSec tunnel is terminated.
Certificates of Certification Authorities	Certificates that verify certificates that CAs issue; should be installed before installing the certificate issued by the CA	CA Certificates imported into the module	Stored in files in plain text form. They are not CSPs for FIPS purposes as they are essentially public keys.

The VPN Client supports X.509, PKCS #7 and PKCS#12 formats for certificates. It supports the Simple Certificate Enrollment Protocol (SCEP) and also Entrust Entelligence to obtain Entrust Identity Certificates.

Key Generation

The VPN Client generates Diffie-Hellman keys for the Diffie-Hellman key agreements and RSA keys for identity certificates. IPSec session keys are negotiated by IKE. All other keys are generated outside of the module. The module implements the FIPS approved PRNG specified in ANSI X9.62 (A.4).

Key Storage

All private keys are stored in encrypted form using a password-based encryption mechanism (PKCS#5), which is considered plaintext for FIPS purposes. The RSA public/private keys are stored in the hard disk of the PC.

Key destruction

All keys can be zeroized by uninstalling the module and reformatting the hard drive. The RSA key pairs are zeroized by deleting the files where they are stored. The pre-shared keys are zeroized by changing the group id and password. Restarting the module or rebooting the PC zeroizes all session keys.

Self-Tests

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

- Software integrity test
- PRNG KAT
- DES KAT
- TDES KAT+
- AES KAT
- SHA-1 KAT
- HMAC-SHA1 KAT
- RSA Sign/Verify KAT

The VPN Client performs all power-up self-tests automatically each time it starts. It also performs the power-up self-tests at system boot. 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 reading any security associations and creating network connections. 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, the VPN Client displays a message indicating the error and terminates.

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

- Continuous Random Number Generator Test for the PRNG and for the non-Approved RNG that generates the seed for the PRNG
- Alternating Bypass Mode Test
- RSA Sign/Verify Pairwise Consistency Test

In the unlikely event a PRNG test or RSA pairwise consistency conditional self-test fails, the VPN Client displays an error message and logs a message in the log file. For the bypass self-test failure, the module displays an error message and the system terminates.

Design Assurance

Cisco Systems Inc. uses the Perforce Configuration Management System. The Perforce source control system is used for 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 the best practices for configuration management to 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 Inc. follows best software engineering principles in designing, developing, tracking and documenting software and hardware modules.

The FIPS submission documentation is maintained and tracked using Visual Source Safe.

Mitigation of Other Attacks

The VPN Client does not claim to mitigate any attacks.

Secure Operation

The Cisco VPN Client meets Level 1 requirements for FIPS 140-2. The section below describes how to place and keep the module in FIPS-approved mode of operation.

Initial Setup

To ensure that the VPN Client operates in FIPS mode, configure the corresponding VPN Concentrator to use only FIPS approved algorithms during IPSec negotiations.

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
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
PC	Personal Computer
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RSA	Rivest Shamir and Adleman
RNG	Random Number Generator
SA	Security Association
SHA	Secure Hash Algorithm

Cisco VPN Client Security Policy

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.