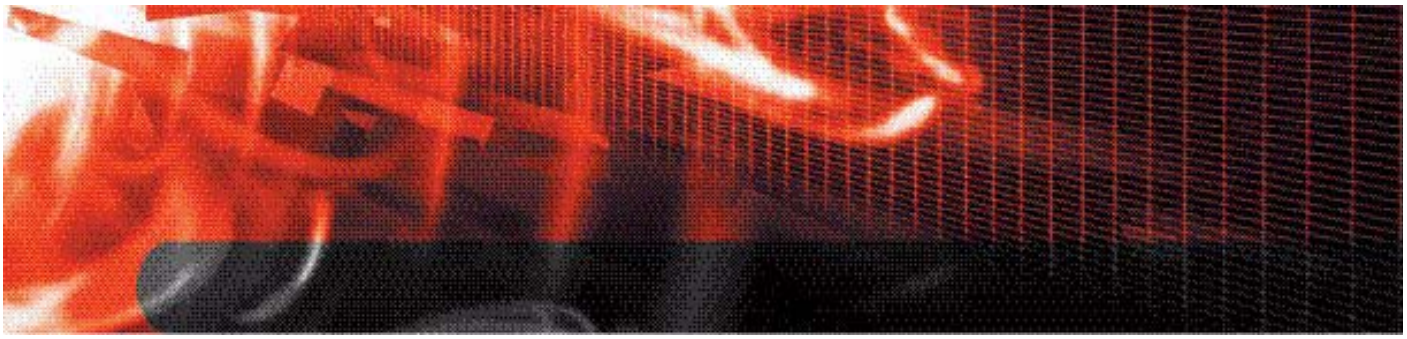


FortiClient Crypto Module FIPS 140-2 Level 1 Security Policy

FortiClient Crypto Module FIPS 140-2 Level 1 Security Policy	
Document Version:	1.3
Publication Date:	May 13, 2008
Description:	Documents FIPS 140-2 Security Policy issues, compliancy and requirements for FIPS compliant operation of the FortiClient product.
Software Version:	3.0.470

FORTINET™
www.fortinet.com

FortiClient Crypto Module FIPS 140-2 Level 1 Security Policy
v1.3

May 13, 2008

04-30000-0476-20080513

Trademarks

Contents

This document is a non-proprietary, FIPS 140-2 Security Policy for Fortinet Incorporated's FortiClient Crypto Module, which is a component of Fortinet's FortiClient software product. This policy describes how the FortiClient Crypto Module (hereafter referred to as the 'module') meet the FIPS 140-2 security requirements and how to operate the module in a FIPS compliant manner. This policy was created as part of the Level 1 FIPS 140-2 validation of the module.

This document contains the following sections:

Fortinet References

This policy deals specifically with operation and implementation of the module in the technical terms of the FIPS 140-2 standard and the associated validation program. Additional information on the module and the entire Fortinet product line can be obtained from the following sources:

- Find general product information in the product section of the Fortinet corporate website at http://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at http://www.fortinet.com/support
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at http://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at http://www.fortinet.com/FortiGuardCenter.

Third Party References

- The Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules* (FIPS 140-2) http://csrc.nist.gov/cryptval/
- Microsoft Windows 2003/XP Security Target, Version 1.0, 28 September 2005 http://niap.bahialab.com/cc-scheme/st/?vid=4025

Security Level Summary

The module meets the overall requirements for a Level 1 FIPS 140-2 validation.

Table 1: Summary of FIPS Security Requirements and Compliance Levels

Security Requirement	Compliance Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

FIPS Mode of Operation

To operate the module in a FIPS compliant manner, the module must be configured to run in the FIPS mode of operation. Enabling the FIPS mode of operation sets default values, disables some features and performs additional configuration procedures to meet FIPS 140-2 Level 1 as specified in Table 1.

See “FIPS 140-2 Compliant Operation” on page 14 for complete details on configuring the module in the FIPS mode of operation.

Cryptographic Module Description

The FortiClient Crypto Module is classified as a multi-chip standalone cryptographic module. The module consists of the following components:

- A commercially available, general purpose, Intel compatible computer
- A commercially available Operating System
- The FortiClient Crypto Module software

This section contains the following information:

- Cryptographic Key Management

Physical Specification

The general purpose, Intel compatible computer consists of the following devices:

- CPU (microprocessor, Intel x86 compatible)
- Memory (RAM) including working memory (input/output buffers, plaintext/ciphertext buffers and control buffers) and program memory
- Hard disk (or disks)
- Display controller
- Keyboard interface
- Mouse interface
- Network interface (Ethernet)
- Serial port
- Parallel port
- Power supply

Computer Hardware and Operating System

To achieve an overall FIPS 140-2 Level 1 certification, the module was tested on the following operating system:

- Microsoft Windows XP, Professional; Service Pack (SP) 2

Software Specification

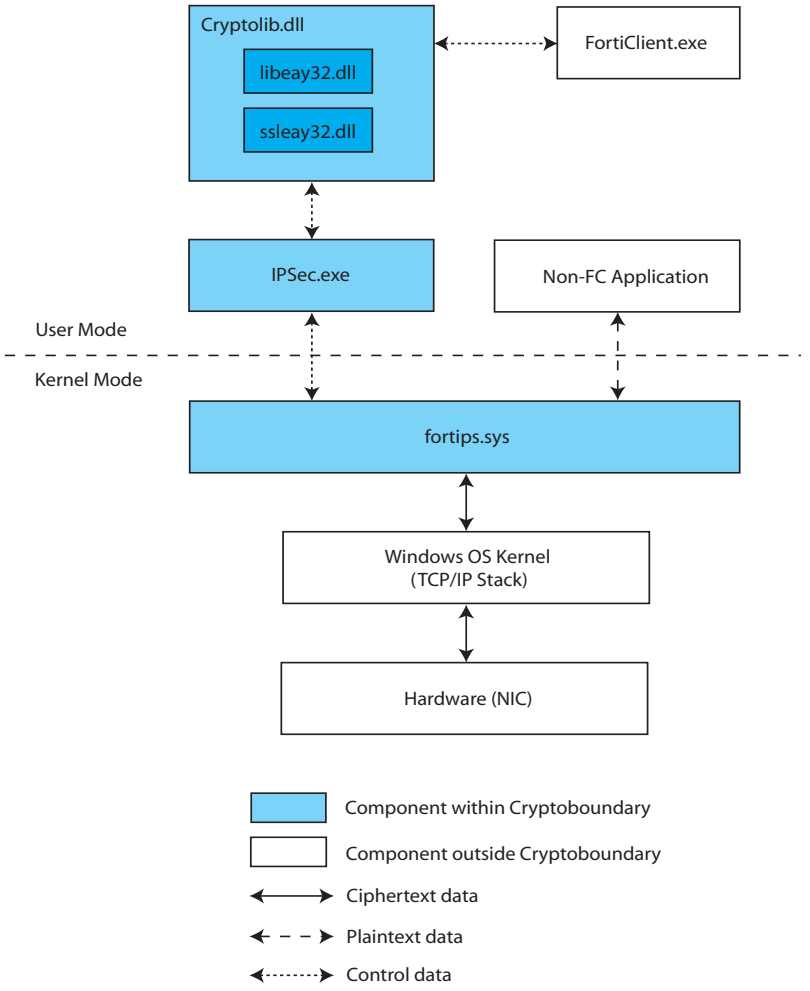
The module provides cryptographic services for the FortiClient product. The primary purpose of the module is providing cryptographic support for FortiClient's IPSec secure communications feature. The module also provides cryptographic support for protecting FortiClient's critical security parameters, passwords and configuration information. The module is distributed as part of the FortiClient software package.

The cryptographic boundary of the module includes the following software binaries:

- CryptoLib.dll, which serves as a wrapper for:
  - libeay32.dll
  - ssleay32.dll
- IPSEC.exe
- fortips.sys

Figure 1 shows a logical block diagram of the module and its relation to the hardware and operating system. FortiClient.exe provides the FortiClient GUI and is used for control input. Status output is sent to the Windows GUI and/or the Windows Command Prompt (not shown). See "Self-test status indicators" on page 15 for more details on status output.

Figure 1: Module software block diagram



Module Interfaces

The module physical and logical interfaces are described in Table 2.

Table 2: Module Logical and Physical Interfaces

I/O	Logical Interface	Physical Interface
Data Input	API	Ethernet port
Data Output	API	Ethernet port
Control Input	API	Keyboard and mouse
Control Output	Return Code	Display
Power Input	API	The power supply is the power interface

Roles, Services and Authentication

Roles

When configured in FIPS mode, the modules provide a **Crypto Officer** role and a **User** role.

An operator assumes the Crypto Officer role by unlocking the FortiClient configuration with a password. An operator assuming the Crypto Officer role has read/write access to all of the administrative functions and services of the module, including configuring IPSec encrypt/decrypt services, executing manual self-tests and shutting down the module.

Users can make use of the IPSec encrypt/decrypt services, but cannot access the modules for administrative purposes. Users authenticate through the Windows authentication mechanism.

Refer to the next section on Services for detailed information on what functions and services each role has access to.

The module does not provide a Maintenance role.

Services

The following tables detail the services available to each role and the types of access for each role.

The following abbreviations are used in the tables:

Crypto Officer	CO
User	U
Read	R
Write	W
Execute	E

Table 3: Services available by role via the CLI

Service	CO	U
Connect/disconnect IPSec tunnel	E	E
Execute self-tests on demand	E	E

Table 4: Services available by role via the GUI

Service	CO	U
Install/Uninstall FortiClient software	E	N/A
Authenticate to module (lock/unlock configuration)	E	N/A
Enable/Disable FIPS Mode	RWE	No
Shutdown FortiClient	E	No
Set/unset CO password	WE	No
Add/delete/configure IPSec tunnel	RWE	No
Connect/disconnect IPSec tunnel	E	E
View status	R	R

Authentication

The minimum Crypto Officer password length is 8 characters when in FIPS mode. Using a strong password policy, where the Crypto Officer password is at least 8 characters in length and use a mix of alphanumeric (printable) characters from the ASCII character set, the odds of guessing a password is 1 in 96^8.

Crypto Officer authentication is not subject to a failed authentication limit, but a 1 second interval between authentication attempts is enforced, limiting the authentication attempts to 60 in 1 minute.

For Users invoking the IPSec encrypt/decrypt services, the module acts on behalf of the User and negotiates an IPSec connection with a remote module using an IPSec policy previously defined by the Crypto Officer. The strength of authentication for IPSec services is based on the authentication method used in the selected IPSec policy: either pre-shared key or RSA certificate.

The minimum permitted IPSec pre-shared key length is 8 characters in FIPS mode and a strong password policy (as described previously) must be enforced. The RSA certificate key size is 1024 bits. Therefore the odds of guessing an IPSec authentication key are at least 1 in 96^8.

Physical Security

This section is not applicable to the module.

Operational Environment

The module must be run on a general purpose PC where the operating system is configured to run in single user mode. To ensure the operating system is running in single user mode, all operator accounts, other than the Windows Administrator account, but including remote login accounts, as well as any services that may allow remote access or login, such as terminal services, SSH, telnet service, remote desktop and remote assistance services, must be disabled.

By default, the FortiClient software is configured to load automatically during the Windows boot process. In order to allow the Crypto Officer or User to view the results of the startup self-tests, automatic loading of FortiClient must be disabled. To disable automatic loading of FortiClient, set the Fortinet Service Scheduler service Startup Type to “Manual”.

Cryptographic Key Management

Random Number Generation

The module uses a software based, deterministic random number generator that conforms to ANSI X9.31 Appendix A.2.4.

Key Zeroization

All keys and CSPs are zeroized when the FortiClient software (and module) is uninstalled by the Crypto Officer. Uninstalling FortiClient will cause the Windows Installer to erase (zeroize) all FortiClient keys from the Registry. See Table 7 on page 14 for a complete list of keys and CSPs.

Algorithms

Table 5: FIPS Approved or Allowed Algorithms

Algorithm	CAVP Certificate Number
RNG (ANSI X9.31 Appendix A.2.4)	396
Triple-DES	621, 622
AES	679, 680
SHA-1	709, 710
HMAC SHA-1	360, 361
Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 110 bits of encryption strength; non-compliant less than 80-bits of encryption strength)	
RSA PKCS1 (digital signature creation and verification)	317

Table 6: Non-FIPS Approved Algorithms

Algorithm
DES (disabled in FIPS mode)
MD5 (disabled in FIPS mode)
HMAC MD5 (disabled in FIPS mode)

Cryptographic Keys and Critical Security Parameters

The following table lists all of the cryptographic keys and critical security parameters used by the module. The following definitions apply to the table:

Key or CSP	The key or CSP description.
Storage	Where and how the keys are stored
Usage	How the keys are used

Table 7: Cryptographic Keys and Critical Security Parameters

Key or CSP	Storage	Usage/Description
Diffie-Hellman Keys	RAM Plaintext	Key agreement and key establishment
IPSEC Encryption Key	RAM Plaintext	IPSec traffic encryption/decryption using Triple-DES or AES
IPSEC Authentication Key	Windows Registry AES encrypted	Electronic key used for IPSec peer-to-peer authentication
IPSec Pre-Shared Key	Windows Registry AES encrypted	Electronic key used to generate IPSec session encryption key and authentication key
IKE Authentication Key	RAM Plain-text	IKE peer-to-peer authentication using HMAC SHA-1 (SKEYID_A)
IKE Key Generation Key	RAM Plain-text	IPSEC SA keying material (SKEYID_D)
IKE Session Encryption Key	RAM Plain-text	Encryption of IKE peer-to-peer key negotiation using Triple-DES or AES (SKEYID_E)
IKE RSA Key	Windows Registry AES encrypted	X.509 certificates used for IKE peer-to-peer authentication
Software Integrity Key	RAM Plain-text	X.509 certificate used to sign and verify crypto module binaries
RNG Seed (ANSI X9.31 Appendix A.2.4)	RAM Plain-text	Seed used for initializing the RNG
RNG AES Key (ANSI X9.31 Appendix A.2.4)	RAM Plain-text	AES seed key used with the RNG
Crypto Officer Password	Windows Registry AES encrypted	Password used to authenticate Crypto Officer access to the module
Registry Encryption Key	RAM Plain-text	AES key used to encrypt configuration information and CSPs stored in the Windows Registry.

FIPS 140-2 Compliant Operation

To operate the module in a FIPs compliant manner, organizations must follow the procedures explained in this section of the Security Policy.

This section contains the following information:

Downloading the FortiClient documentation

Before downloading and installing the FortiClient software, download and read the FortiClient documentation. The documentation can be found at http://docs.forticare.com.

The following is a list of the relevant documentation:

- FortiClient 3.0 MR5 Administration Guide
- FortiClient 3.0 MR5 User's Guide
- FortiClient 3.0 MR5 IPSec User Guide
- FortiClient 3.0 MR5 FIPS Technical Note

Downloading and installing the FIPS certified software

Note: The Crypto Officer must create an account on the Fortinet support site and register the FortiClient product before continuing. Follow the instructions on the Fortinet Support site at https://support.fortinet.com to create an account and register the product.

The FortiClient Crypto Module is distributed as part of the overall FortiClient software package. Installing the FortiClient software package also installs the FortiClient Crypto Module. The FortiClient software package is available from the Fortinet support site at https://support.fortinet.com.

After logging in to the support site, select Firmware Images, then FortiClient, then v3.0, then FIPS Certified. The build information is listed in Table 8. The FortiClient version information is found on the General tab of the FortiClient GUI.

Table 8: FortiClient build information

Filename	Version
FortiClientSetup_3.0.013.exe	3.0.470

Installing the software

Follow the normal instructions for installing the FortiClient software as explained in the FortiClient Administration Guide.

Enabling FIPS mode

After installing the FortiClient software, the Crypto Officer enables the FIPS mode of operation by selecting the 'FIPS Mode' checkbox on the General tab of the FortiClient GUI. The Crypto Officer will immediately be prompted to enter the Crypto Officer Password, which is used to lock the configuration.

To make changes to the configuration once FIPS mode has been enabled and the configuration locked, the Crypto Officer must first unlock the configuration by using the 'Unlock Settings' button on the General tab of the FortiClient GUI and entering the Crypto Officer Password.

Enabling FIPS mode locks the registry configuration and prevents the FortiClient services from being stopped or unloaded unless the Crypto Officer unlocks the configuration.

Self-Tests

The module implements startup, on-demand and conditional self-tests.

Self-test status indicators

Results of the self-tests are logged in the FortiClient log file and output to the FortiClient console. A Microsoft Windows Command Prompt window must be open to display console messages and the self-test results.

If any of the startup, on-demand or conditional self-tests fail, the following indicators are displayed:

- An error message is output to the console that includes the affected binary and algorithm information
- A result of false (0) is output to the console
- An error message is logged
- The affected binary will terminate (shut down)

The on-demand self-tests are run as a batch and a result of true (1) is returned if the tests pass.

Startup Self-Tests

The module executes the following self-tests on startup:

- Integrity test of the binary files that comprise the module using digital signatures
- Triple-DES, CBC mode, encrypt/decrypt known answer test
- AES, ECB and CBC modes, encrypt/decrypt known answer test
- HMAC SHA-1 known answer test
- RSA signature generation/verification known answer test
- RNG known answer test (ANSI X9.31 Appendix A.2.4)

If an integrity test fails on startup, depending on the nature of the failure and how the binary was modified, it is possible that FortiClient will terminate and exit back to the Windows desktop. If the kernel driver (fortips.sys) is modified, a hard crash may result requiring the Crypto Officer to recover the Windows installation.

The startup self-tests terminate at the first test that fails.

On-Demand Self-Tests

The startup self-tests, including the integrity and algorithm tests, can also be initiated on-demand using the FortiClient Command Line Interface (CLI) and the command **ipsec.exe -f 1**

The FortiClient CLI is accessible from the Microsoft Windows Command Prompt. The FortiClient software installation directory must be in the path or the command must be executed from the installation directory.

The on-demand self-tests terminate at the first test that fails.

Conditional Self-Tests

The module executes the following conditional tests when the related service is invoked:

- Continuous RNG test (ANSI X9.31 Appendix A.2.4)
- RSA pairwise consistency test

Disabling FIPS mode

To disable FIPS mode, the Crypto Officer must first unlock the FortiClient configuration by selecting the “Unlock Settings” button on the General tab of the FortiClient GUI and entering the Crypto Officer password when prompted. FIPS mode can then be disabled by de-selecting the ‘FIPS Mode’ checkbox on the General tab of the FortiClient GUI. The CO will be prompted to enter the Crypto Officer password again to disable FIPS mode.

Mitigation of Other Attacks

The module does not mitigate against other attacks.