FIPS 140-2 Level 2 Security Policy

FortiClient 5.0 VPN Client

FortiClient 5.0 VPN Client FIPS 140-2 Level 2 Security Policy	
Document Version:	1.9
Publication Date:	January 22, 2016
Description:	Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.
software Version:	FortiClient 5.0, build0367, 151201

FortiClient 5.0 VPN Client: FIPS 140-2 Level 2 Security Policy

04-500-267323-20150219

for FortiClient 5.0

Trademarks

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Contents

Overview

This document is a non-proprietary, FIPS 140-2 Security Policy for Fortinet Incorporated's FortiClient 5.0 VPN Client. This policy describes how the FortiClient 5.0 VPN Client (hereafter referred to as the 'module') meet the FIPS 140-2 security requirements and how to operate the module in a FIPS compliant manner. The module provides IPSec and SSL VPN client services. This policy was created as part of the Level 2 FIPS 140-2 validation of the module.

This document contains the following sections:

- Security Level Summary
- Cryptographic Module Description
- Mitigation of Other Attacks
- FIPS 140-2 Compliant Operation
- Self-Tests
- Non-FIPS Approved Services

The Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules* (FIPS 140-2) details the United States Federal Government requirements for cryptographic modules. Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

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. Other Fortinet product manuals, guides and technical notes can be found at the Fortinet technical documentation website at http://docs.fortinet.com.

Additional information on 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 7 and Windows Server 2008 Security Target, Version 1.0, 28 March 2011 https://www.commoncriteriaportal.org/files/epfiles/st_vid10390-st.pdf.

Security Level Summary

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

Table 1: Summary of FIPS security requirements and compliance levels

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

Cryptographic Module Description

The module is classified as a multi-chip standalone cryptographic module. The module consists of the FortiClient 5.0 VPN Client software and requires the following components:

- A commercially available, general purpose, Intel compatible computer
- A commercially available Operating System

Computer Hardware and Operating System Specification

To achieve an overall FIPS 140-2 Level 2 validation, the module was tested on (and must be run on) the following combinations of hardware and operating system:

- Dell Optiplex 755
- Fortinet entropy token (FTR-ENT-1)
- Microsoft Windows 7 Enterprise Edition

The following security updates and patches must be applied, as a minimum, to the Windows 7 installation:

- All security updates as of September 14, 2010 as well as the updates associated with security bulletins MS10-073 and MS10-085
- Hotfix KB2492505

Software Specification

The primary purpose of the module is providing IPSec and SSL VPN client services. The cryptographic boundary of the module includes the following software binaries:

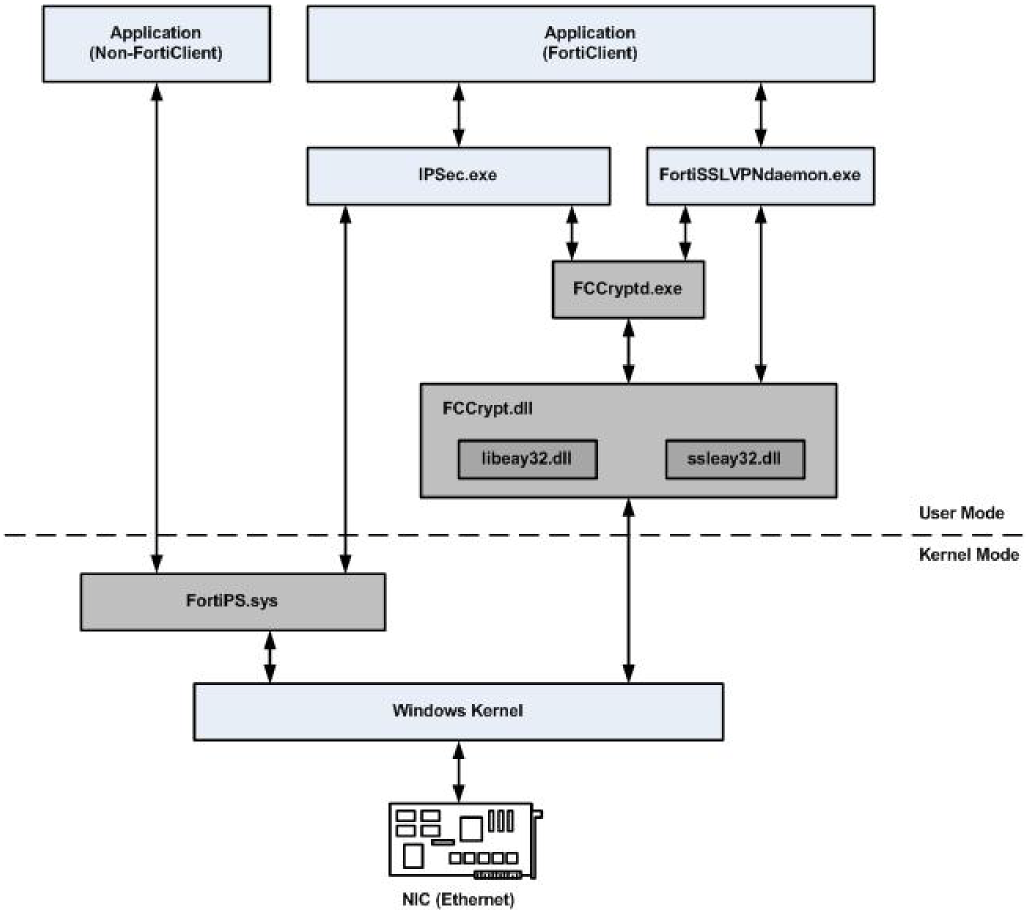
- FCCrypt.dll, which serves as a wrapper for:
  - libeay32.dll
  - ssleay32.dll
- FCCryptd.exe
- fortips.sys

All other FortiClient binaries are specifically excluded from the boundary as they provide no cryptographic services.

The validated software version is FortiClient 5.0, build0367,151201.

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). The binaries highlighted in dark grey are within the cryptographic boundary of the module.

Figure 1: Module software block diagram



Module Interfaces

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

Table 2: FortiOS logical interfaces and physical ports

FIPS 140 Interface	Logical Interface	Physical Port
Data Input	API input parameters	Network interface.
Data Output	API output parameters	Network interface.
Control Input	API function calls	Keyboard, mouse, entropy token.
Status Output	API return values	Display.
Power Input	N/A	The power supply is the power interface.

Roles, Services and Authentication

Roles

The module provides a **Crypto Officer** role and a **User** role. The module supports a Crypto Officer role and a user role. Crypto Officers and Users authenticate through the Windows authentication mechanism. A user with Windows administrative privileges assumes the "Crypto Officer Role". A user without Windows administrative privileges assumes the "User Role" role. Multiple accounts can be logged in to the Windows PC, but only one account can be active at a time through Windows user switching.

Crypto Officers have read/write access to all of the administrative functions and services of the module, including configuring SSL/IPSec VPN encrypt/decrypt services, using the SSL/IPSec VPN encrypt/decrypt services, executing the self-tests and shutting down the module.

Users can make use of the SSL/IPSec VPN encrypt/decrypt services, but cannot access the module for administrative purposes.

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 to Crypto Officers

Service	Access	Key/CSP
show system status	R	N/A
show FIPS mode enabled	R	N/A
enable/disable use of entropy token	RWE	N/A
execute on-demand self-tests	E	Configuration Integrity Key, Firmware Integrity Key
view/set/delete/modify module configuration	RWE	N/A
view/set/delete/modify IPSec/SSL VPN configuration	RWE	IPSec Pre-Shared Key, IKE RSA Key
connect/disconnect IPSec/SSL VPN tunnel*	E	IPSec: IKE Pre-Shared Key, IKE RSA Key, IKE Authentication Key, IKE Key Generation Key, IKE Session Encryption Key SSL: TLS RSA Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS SSH Session Encryption Key
backup/restore configuration file	WE	Configuration Encryption Key, Configuration Backup Key
export/clear log data	WE	N/A
view/clear alerts	E	N/A
view connection status	E	N/A
view module details	E	N/A

Table 4: Services available to Users

Service	Access	Key/CSP
connect/disconnect IPSec/SSL VPN tunnel*	E	IPSec: IKE Pre-Shared Key, IKE RSA Key, IKE Authentication Key, IKE Key Generation Key, IKE Session Encryption Key SSL: TLS RSA Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS SSH Session Encryption Key
execute on-demand self-tests	E	Configuration Integrity Key, Firmware Integrity Key
view/clear alerts	E	N/A
view connection status	E	N/A
view module details	E	N/A

Authentication

The authentication mechanism is provided by the Windows operating system. The Windows Security Policy must be configured so that the minimum password length is 8 characters. Using a strong password policy, where the Crypto Officer and Users passwords are 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.

Assuming that no password lockout settings are configured and an attacker could perform 100 password attempts in a minute, the odds of guessing a password in one minute are 100 in 96^8, which is far less than 1 in 100,000.

Physical Security

This section is not applicable to the module. The module is completely comprised of software.

Cryptographic Key Management

Random Number Generation

The module uses a firmware based, deterministic random bit generator (DRBG) that conforms to NIST Special Publication 800-90A. The module generates cryptographic keys whose strengths are modified by available entropy. There is no assurance of the minimum strength of generated keys.

Entropy Token

The modules use an entropy token to seed the DRBG during the module's boot process and to periodically reseed the DRBG. The entropy token is not included in the boundary of the module and therefore no assurance can be made for the correct operation of the entropy token nor is there a guarantee of stated entropy.

The default reseed period is once every 24 hours (1440 minutes). The token must be installed to complete the boot process and to reseed of the DRBG. The entropy token is responsible for loading a minimum of 256 bits of entropy.

The entropy gathered from the token is conditioned to a strength of 256 bits following the guidelines of Section 6.4.2.1.1 in NIST SP 800-90B. As a result, all keys generated in the module using the seeded NIST SP 800-90A DRBG contain their commensurate encryption strength.

Key Zeroization

Key zeroization is performed by:

1. Uninstalling the module.
2. Reformatting and overwriting, at least once, the mass storage device the module is installed on.
3. Power cycle the host computer.

Algorithms

Table 5: FIPS Approved Algorithms

Algorithm	NIST Certificate Number
DRBG (NIST SP 800-90)	538
Triple-DES	1728, 1737
AES	2912, 2924
SHA-1	2451, 2460
SHA-256	2451, 2460
HMAC SHA-1	1842,1851
HMAC SHA-256	1842, 1851
RSA PKCS1 (digital signature creation and verification)	1533
CVL (IKE v1)	329
CVL (IKE v2)	329
CVL (TLS)	329
PBKDF (Based on NIST SP 800-132)	Vendor Affirmed

Table 6: FIPS Allowed Algorithms

Algorithm
RSA (key wrapping; key establishment methodology provides 112 or 144 bits of encryption strength)
Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 196 bits of encryption strength)

Table 7: Non-FIPS Approved Algorithms

Algorithm
NDRNG
SHA-384 (non-compliant)*
SHA-512 (non-compliant)*
HMAC SHA-384 (non-compliant)*
HMAC SHA-512 (non-compliant)*
RSA is non-compliant when keys of less that 2048 bits are used, since such keys do not provide the minimum required 112 bits of encryption strength.
Diffie-Hellman is non-compliant when keys of less that 2048 bits are used, since such keys do not provide the minimum required 112 bits of encryption strength.

Note that the IKE and TLS protocols have not been reviewed or tested by the CMVP or CAVP. Also, the module is operating in a non-approved mode when algorithms marked with an asterisk (*) in Table 7 are used. SHA-384, SHA-512, HMAC-SHA-384 and HMAC-SHA-512 are non-compliant, as they are not self-tested during the module's power-up sequence.

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 8: Cryptographic Keys and Critical Security Parameters used in FIPS Mode

Key or CSP	Storage	Usage
Diffie-Hellman Keys	SDRAM Plain-text	Key agreement and key establishment
IPSec Session Authentication Key	SDRAM Plain-text	IPSec peer-to-peer authentication using HMAC SHA-1 or HMAC SHA-256
IPSec Session Encryption Key	SDRAM Plain-text	VPN traffic encryption/decryption using Triple-DES or AES
IKE Pre-Shared Key	Registry AES encrypted	Used to generate IKE protocol keys
IKE Authentication Key	SDRAM Plain-text	IKE peer-to-peer authentication using HMAC SHA-1 or HMAC SHA-256 (SKEYID_A)
IKE Key Generation Key	SDRAM Plain-text	IPSec SA keying material (SKEYID_D)
IKE Session Encryption Key	SDRAM Plain-text	Encryption of IKE peer-to-peer key negotiation using Triple-DES or AES (SKEYID_E)
IKE RSA Key	Registry AES encrypted	RSA key used to generate IKE protocol keys
DRBG output	SDRAM Plain-text	Random numbers used in cryptographic algorithms
DRBG v and key values	SDRAM Plain-text	Internal state values for the DRBG
Firmware Integrity Key	Mass storage Plain-text	Verification of firmware integrity using RSA public key
TLS RSA Key	Registry AES encrypted	RSA key used for client authentication.
TLS Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 or HMAC SHA-256 key used for HTTPS/TLS session authentication
TLS Session Encryption Key	SDRAM Plain-text	AES or Triple-DES key used for HTTPS/TLS session encryption
Configuration Integrity Key	Registry AES encrypted	HMAC SHA-256 key used for configuration integrity test
Configuration Encryption Key	SDRAM Plain-text	AES key used to encrypt CSPs in the registry and backup configuration file
Configuration Backup Key	SDRAM Plain-text	AES key used to encrypt the backup configuration file

Mitigation of Other Attacks

The module does not mitigate against any other attacks.

FIPS 140-2 Compliant Operation

FIPS 140-2 compliant operation requires that the Crypto Officer follow secure procedures for installation of the module. The Crypto Officer must ensure that the FortiClient software (the module) is installed as per the FortiClient Administration Guide. The Crypto Officer must be logged in to Windows 7 Enterprise Edition with Administrator privileges in order to install the module.

During installation, the Crypto Officer must ensure that:

- The entropy token is installed and enabled.
- Crypto Officer and User passwords are at least 8 characters long.
- Crypto Officer and User passwords are changed regularly.
- Crypto Officer and User passwords must have the following characteristics:
  - One (or more) of the characters must be capitalized
  - One (or more) of the characters must be numeric
  - One (or more) of the characters must be non alpha-numeric (e.g. punctuation mark)
- The Microsoft security updates and hotfixes are applied as described in "Computer Hardware and Operating System Specification" on page 3.
- The non-approved algorithms listed in Table 7 on page 8 are not used. Backup the FortiClient configuration file and use an XML viewer to verify the configuration. Refer to the FortiClient 5.0 XML Reference guide for more information.

Once the module is installed and configured, the CO or Network Users can log in to Windows 7 Enterprise to execute (run) the module (FortiClient.exe) and access its services.

Self-Tests

The module executes the following self-tests during startup and initialization:

- Software integrity test using RSA signatures
- Configuration integrity test using HMAC SHA-256
- Triple-DES, CBC mode, encrypt known answer test
- Triple-DES, CBC mode, decrypt known answer test
- AES, CBC mode, encrypt known answer test
- AES, CBC mode, decrypt known answer test
- HMAC SHA-1 known answer test
- SHA-1 known answer test (tested as part of HMAC SHA-1 known answer test)
- HMAC SHA-256 known answer test
- SHA-256 known answer test (tested as part of HMAC SHA-256 known answer test)
- RSA signature generation known answer test
- RSA signature verification known answer test
- DRBG known answer test

The results of the startup self-tests are displayed in a Windows taskbar notification message during the module's startup process. The message displayed is:

```
FortiClient FIPS Startup Tests
  All self-tests passed
```

The startup self-tests can also be initiated on demand using the Windows command prompt. The syntax is **FCCryptd.exe fips kat all** (to initiate all self-tests) or **FCCryptd.exe fips kat <test>** (to initiate a specific self-test).

When the self-tests are run, each implementation of an algorithm is tested - e.g. when the AES self-test is run, all AES implementations are tested.

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

- Continuous NDRNG test
- Continuous DRBG test
- RSA pairwise consistency test
- Configuration integrity test using HMAC SHA-256

If any of the self-tests or conditional tests fail, the module enters an error state as shown in a FortiClient message window:

```
  FIPS: Running FIPS self-test ...
  FIPS Error: <Test> self-test failed.
  FIPS Error: Running FIPS self-test --> failed.
```

All of the module’s data output and cryptographic services are inhibited in the error state.

Non-FIPS Approved Services

Services marked with an asterisk (*) in Table 3 and Table 4 are considered non-approved when using the following algorithms:

- SHA-384
- SHA-512
- HMAC SHA-384
- HMAC SHA-512