FIPS 140-2 Security Policy

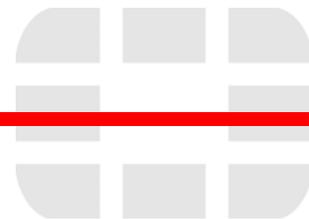| FortiMail 5.2 FIPS 140-2 Security Policy	
Document Version:	1.7
Publication Date:	January 4, 2016
Description:	Documents FIPS 140-2 Level 1 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Firmware Version:	FortiMailOS 5.2, build0460,150922

FortiMail 5.2: FIPS 140-2 Security Policy
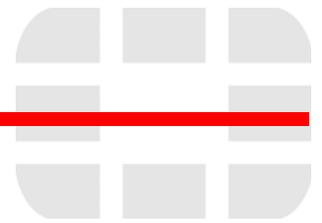
06-520-241428 -20140509

for FortiMail 5.2

Contents

Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiMail 5.2 firmware, which runs on the FortiMail family of security appliances. This policy describes how the FortiMail 5.2 firmware (hereafter referred to as the 'module') meets 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.

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.

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.forticare.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.

Introduction

The FortiMail family of message security appliances provide an effective barrier against the ever-rising volume of spam, maximum protection against sophisticated message-based attacks, and features designed to facilitate regulatory compliance. FortiMail 5.2 offers both inbound and outbound scanning, advanced antispam and antivirus filtering capabilities, IP address black/white listing functionality, and extensive quarantine and archiving capabilities. Three deployment modes offer maximum versatility: transparent mode for seamless integration into existing networks with no IP address changes, gateway mode as a proxy Mail Transfer Agent (MTA) for existing messaging gateways, or server mode to act as a mail server with functionality for small businesses (SMBs) and remote offices.

Note: The server mode of operation is not a FIPS approved mode of operation.

Security Level Summary

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

Table 1: Summary of FIPS security requirements and compliance levels

Security Requirement	Compliance Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Module Description

The module is a firmware operating system that runs exclusively on the FortiMail line of appliances. The firmware consists of multiple object files. The FortiMail appliances are purpose built, PC based, multiple chip, standalone cryptographic modules consisting of production grade components contained in a physically protected enclosure.

Figure 1:   FortiMail Cryptographic Boundary
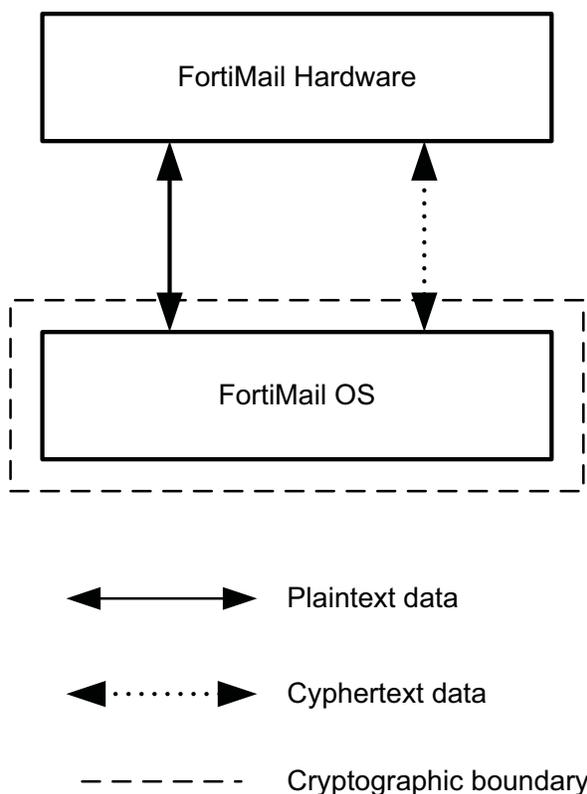
FortiMail Hardware

FortiMail OS

Plaintext data

Cyphertext data

Cryptographic boundary

For the purposes of FIPS 140-2 conformance testing, the module was tested on the FortiMail-3000D appliance and used a Fortinet entropy token (part number FTR-ENT-1) as the entropy source.

The validated firmware version is FortiMailOS 5.2, build0460,150922.

The module can also be executed on any of the following FortiMail appliances and remain vendor affirmed FIPS-compliant. Note the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

- FortiMail-200D
- FortiMail-200E
- FortiMail-400E
- FortiMail-1000D
- FortiMail-2000B
- FortiMail-3000C
- FortiMail-3000D
- FortiMail-5002B

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, USB interface.
Data Output	API output parameters	Network interface.
Control Input	API function calls	Network interface, serial interface, USB interface.
Status Output	API return values	Network interface, serial interface, USB interface, status LEDs, Power LEDs, network port LEDs.
Power Input	N/A	The power supply is the power interface.

Web-Based Manager

The FortiMail web-based manager provides GUI based access to the module and is the primary tool for configuring the module. The manager requires a web browser on the management computer and an Ethernet connection between the FortiMail unit and the management computer.

A web-browser that supports Transport Layer Security (TLS) 1.0 is required for remote access to the web-based manager when the module is operating in FIPS-CC mode. HTTP access to the web-based manager is not allowed in FIPS-CC mode and is disabled.

Figure 2:   The FortiMail web-based manager

Command Line Interface

The FortiMail Command Line Interface (CLI) is a full-featured, text based management tool for the module. The CLI provides access to all of the possible services and configuration options in the module. The CLI uses a console connection or a network (Ethernet) connection between the FortiMail unit and the management computer. The console connection is a direct serial connection. Terminal emulation software is required on the management computer using either method. For network access, a Telnet or SSH client that supports the SSH v2.0 protocol is required (SSH v1.0 is not supported in FIPS-CC mode). Telnet access to the CLI is not allowed in FIPS-CC mode and is disabled.

Roles, Services and Authentication

Roles

When configured in FIPS mode, the module provides the following roles:

• Crypto Officer
• User

The Crypto Officer role is initially assigned to the default 'admin' operator account. The Crypto Officer role has read-write access to all of the module's administrative services. The initial Crypto Officer can create additional operator accounts. These additional accounts are assigned the Crypto Officer role and can be assigned a range of read/write or read only access permissions including the ability to create operator accounts.

The User role can make use of the encrypt/decrypt services, but cannot access the module for administrative purposes. The User role has access to the quarantine and email relay services as defined by a Crypto Officer.

The module does not provide a Maintenance role.

FIPS Approved Services

The following tables detail the types of FIPS approved services available to each role, the types of access for each role and the CSPs they affect.

The role names are abbreviated as follows:

Crypto Officer	CO
User	U

The access types are abbreviated as follows:

Read Access	R
Write Access	W
Execute Access	E

Table 3: Services available to Crypto Officers

Service	Access	Key/CSP
authenticate to module*	WE	Operator Password, Operator LDAP password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS Session Encryption Keys, DRBG Output
show system status	E	N/A
show FIPS mode enabled/disabled (console only)	E	N/A
enable FIPS mode of operation (console only)	WE	Configuration Integrity Key
key zeroization	WE	All keys
execute factory reset (disable FIPS-CC mode)	WE	All keys except firmware update key, configuration integrity key, configuration backup key
execute FIPS on-demand self-tests (console only)	WE	N/A
add/delete operators and users	RWE	Operator Password, User Password
set/reset operator and user passwords	WE	Operator Password, User Password
modify user preferences	RWE	N/A

Table 3: Services available to Crypto Officers

Service	Access	Key/CSP
backup / restore configuration file	WE	Configuration Encryption Key, Configuration Backup Key
read/set/delete/modify module configuration	RWE	N/A
enable/disable alternating bypass mode	RWE	N/A
execute firmware update	WE	Firmware Update Public Key
read log data (GUI only)	R	N/A
delete log data (GUI only)	WE	N/A
format log disk (CLI only)	WE	N/A

Table 4: Services available to Users

Service/CSP	Access	Key/CSP
authenticate to module*	E	User Password, User LDAP password, Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, DRBG Output
access to quarantined email	RE	N/A
modify user preferences	E	N/A

Non-FIPS Approved Services

The module also provides the following non-FIPS approved services:

• Configuration backups using password protection

If the above services are used, the module is not considered to be operating in the FIPS approved mode of operation.

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

• Non-compliant-strength Diffie-Hellman

• Non-compliant-strength RSA key wrapping

• DES

• HMAC-MD5

Refer to Table 6 for descriptions of the minimum required encryption strengths for compliance.

Authentication

The module uses identity based authentiction. By default, operators and users authenticate with a username and password combination to access the module. The username/password can be stored in the local database or in a remote LDAP database. Remote operator authentication is done over HTTPS (TLS) or SSH. Local operator authentication is done over the console connection. Remote user authentication is done over HTTPS (TLS). Password entry is obfuscated using asterisks.

Operator authentication over HTTPS/SSH and user authentication over HTTPS are subject to a limit of 3 failed authentication attempts in 1 minute. Operator authentication using the console is not subject to a failed authentication limit, but the number of authentication attempts per minute is limited by the bandwidth available over the serial connection.

Note that the user's username and password are not stored on the module. The module operates as a proxy for user authentication to a backend server (typically a mail server). User authentication is done over HTTPS, POP3S, or IMAPS. HTTPS, POP3S and IMAPS all use the underlying TLS protocol to protect user data between the client and the module and the module and the back end server during the authentication process.

The minimum password length is 8 characters when in FIPS mode (maximum password length is 32 characters). The password may contain any combination of upper- and lower-case letters, numbers, and printable symbols; allowing for 94 possible characters. The odds of guessing a password are 1 in 94^8 which is significantly lower than one in a million. Recommended procedures to increase the password strength are explained in "FIPS 140-2 Compliant Operation" on page 11.

Physical Security

The physical security for the module is provided by the FortiMail hardware which uses production grade components and an opaque enclosure.

Operational Environment

The module constitutes the entire firmware operating system for a FortiMail unit and can only be installed and run on a FortiMail appliance. The module provides a proprietary and non-modifiable operating system and does not provide a programming environment.

For the purposes of FIPS 140-2 conformance testing, the module was tested on the FortiMail-3000D appliance.

Cryptographic Key Management

Random Number Generation

The modules use 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.

Key Zeroization

The zeroization process must performed under the direct control of the operator. The operator must be present to observe that the zeroization method has completed successfully.

All keys and CSPs are zeroized by erasing the module's flash memory and then power cycling the module. To erase the flash memory, execute the following command from the CLI:

```
execute erase-filesystem 0
```

Algorithms

Table 5: FIPS Approved Algorithms

Algorithm	NIST Certificate Number
DRBG (NIST SP 800-90A) with AES 256 bit keys	873
Triple-DES in CBC mode with 168-bits	1971
AES in CBC mode (128-, 192-, 256-bits)	3500
SHA-1	2892
SHA-256	2892
HMAC SHA-1	2239
HMAC SHA-256	2239
RSA PKCS1 - Signature Generation: 2048 and 3072-bit - Signature Verification: 1024, 1536, 2048 and 3072-bit - Key Generation: 1024, 1536 and 2048-bit	1801
CVL (SSH) with TDES, AES-128, AES256-CBC (using SHA1)	574
CVL (TLS) - TLS1.0/1.1 and TLS1.2 (using SHA 256)	574

Table 6: FIPS Allowed Algorithms

Algorithm
RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)
Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)

Table 7: Non-FIPS Approved Algorithms

Algorithm
DES (disabled in FIPS-CC mode)
MD5 (disabled in FIPS-CC mode except for use in the TLS protocol)
HMAC MD5 (disabled in FIPS-CC mode)
NDRNG
RSA is non-compliant when keys less than 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 less than 2048 bits are used, since such keys do not provide the minimlm required 112 bits of encryption strength.

Note that the TLS protocol has not been tested by the CMVP or CAVP.

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	Zeroization
DRBG output	Flash memory Plain-text	Random numbers used in cryptographic algorithms	By erasing the flash memory and power cycling the module
DRBG v and key values	Flash memory Plain-text	Internal state values for the DRBG	By erasing the flash memory and power cycling the module
Diffie-Hellman Key	SDRAM Plaintext	Key agreement and key establishment	By erasing the flash memory and power cycling the module
Firmware Update Key	Flash memory Plain-text	Verification of firmware integrity for download of new firmware versions using RSA 2048 public key	By erasing the flash memory and power cycling the module
HTTPS/TLS Server/Host Key	Flash memory Plain-text	RSA 2048 private key used in the HTTPS/TLS protocols	By erasing the flash memory and power cycling the module
HTTPS/TLS Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 or HMAC SHA-256 key used for HTTPS/TLS session authentication	By erasing the flash memory and power cycling the module
HTTPS/TLS Session Encryption Key	SDRAM Plain-text	AES 128, 256 or Triple-DES key used for HTTPS/TLS session encryption	By erasing the flash memory and power cycling the module
SSH Server/Host Key	Flash memory Plain-text	RSA 2048 private key used in the SSH protocol	By erasing the flash memory and power cycling the module
SSH Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 or HMAC SHA-256 key used for SSH session authentication	By erasing the flash memory and power cycling the module
SSH Session Encryption Key	SDRAM Plain-text	AES 128, 256 or Triple-DES key used for SSH session encryption	By erasing the flash memory and power cycling the module
Configuration Integrity Key	Flash memory Plain-text	HMAC SHA-256 hash used for configuration and firmware integrity (bypass) tests	By erasing the flash memory and power cycling the module
Configuration Encryption Key	Flash memory Plain-text	AES 128 key used to encrypt CSPs on the flash storage and in the backup configuration file (except for operator passwords in the backup configuration file)	By erasing the flash memory and power cycling the module
Configuration Backup Key	Flash memory Plain-text	HMAC SHA-256 key used to encrypt operator passwords in the backup configuration file	By erasing the flash memory and power cycling the module

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

Key or CSP	Storage	Usage	Zeroization
Operator Password	Flash memory SHA-256 hash	Used during operator authentication	By erasing the flash memory and power cycling the module
User Password	SDRAM Plain-text	Used during user authentication	By erasing the flash memory and power cycling the module

Alternating Bypass Feature

The primary cryptographic function of the module is encrypting/decrypting email messages sent/received using SMTP over TLS (SMTPS). The module can also send/receive plain-text email messages using SMTP. The module implements an alternating bypass feature based on the module's configuration and the direction of traffic. If the traffic is sent/received using SMTPS, the module is operating in a non-bypass state. If the traffic is sent/received using SMTP, the module is operating in a bypass state.

Incoming traffic is processed according to the protocol used and the domain configuration. An SMTPS message received by the module is decrypted before being processed. Once processed, if the specified domain is configured to use SMTPS, the message is encrypted before being sent to the mail server (non-bypass state). If the specified domain is configured to use SMTP, then the message is sent to the mail server in plain-text (bypass state).

Outgoing traffic is processed according to the message delivery configuration. If the destination domain is configured to use SMTPS, then the message is encrypted before it is sent (non-bypass state). If the destination domain is configured to use SMTP, then the message is sent in plain-text (bypass state).

Use of SMTPS for incoming traffic is enabled/disabled by checking/unchecking the "Use SMTPS" checkbox in the domain configuration.

Use of SMTPS for outgoing traffic is enabled/disabled by creating a delivery policy with valid TLS and encryption profiles.

Key Archiving

The module supports key archiving to a management computer or USB token as part of a module configuration file backup. Operator entered keys are archived as part of the module configuration file. The configuration file is stored in plain text, but keys in the configuration file are either AES encrypted using the Configuration Encryption Key or stored as a keyed hash using HMAC-SHA-1 using the Configuration Backup Key.

Mitigation of Other Attacks

The module does not mitigate against any other attacks.

FIPS 140-2 Compliant Operation

FIPS 140-2 compliant operation requires both that you use the module in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the FortiMail unit. You must ensure that:

- The FortiMail unit is configured in the FIPS-CC mode of operation.
- The FortiMail unit is installed in a secure physical location.

- The Fortinet entropy token is installed and enabled.
- Physical access to the FortiMail unit is restricted to authorized operators.
- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Administrator account 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)
- Administration of the module is permitted using only validated administrative methods. These are:
  - Console connection
  - Web-based manager via HTTPS
  - Command line interface (CLI) access via SSH
- Diffie-Hellman groups of less than less than 2048 bits are not used.
- Client side RSA certificates must use 2048 bit or greater key sizes.
- LDAP based authentication must use secure LDAP (LDAPS).
- Only approved and allowed algorithms are used (see "Algorithms" on page 9).
- The module can be configured to operate in either gateway or transparent mode. The module cannot be configured in server mode.

Enabling FIPS-CC mode

To enable the FIPS 140-2 compliant mode of operation, the operator must execute the following command from the Local Console:

```
config system fips-cc
  set entropy-token enable
  set status enable
end
```

The Operator is required to supply a password for the admin account which will be assigned to the Crypto Officer role.

The supplied password must be at least 8 characters long and correctly verified before the system will restart in FIPS-CC mode.

Upon restart, the module will execute self-tests to ensure the correct initialization of the module's cryptographic functions.

After restarting, the Crypto Officer can confirm that the module is running in FIPS-CC mode by executing the following command from the CLI:

```
get system status
```

If the module is running in FIPS-CC mode, the system status output will display the line:

```
FIPS-CC mode: enable
```

Note that enabling/disabling the FIPS-CC mode of operation will automatically invoke the key zeroization service. The key zeroization is performed immediately after FIPS-CC mode is enabled/disabled.

Self-Tests

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

- Firmware 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 on the console during the startup process. The startup self-tests can also be initiated on demand using the CLI command **execute fips kat all** (to initiate all self-tests) or **execute 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
- Firmware load test using RSA signatures

If any of the self-tests or conditional tests fail, the module enters an error state as shown by the console output below:

```
Self-tests failed
Entering error mode...
The system is going down NOW !!
The system is halted.
```

All data output and cryptographic services are inhibited in the error state.

Non-FIPS Approved Services

The module also provides the following non-FIPS approved services:

- Configuration backups using password protection

If the above services are used, the module is not considered to be operating in the FIPS approved mode of operation.

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

- Non-compliant-strength Diffie-Hellman
- Non-compliant-strength RSA key wrapping

- DES
- HMAC-MD5