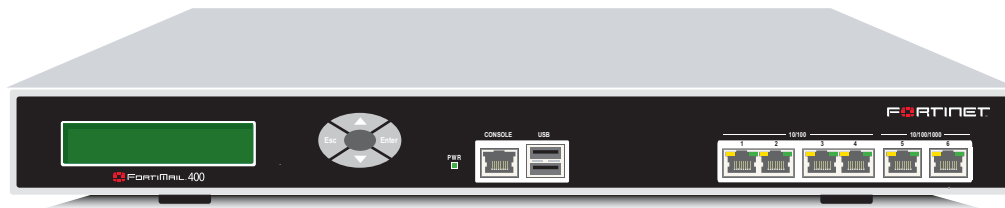


FIPS 140-2 Security Policy

FortiMail OS v3.00



<i>FortiMail OS v3.00 FIPS 140-2 Security Policy</i>	
Document Version:	v1.4
Publication Date:	August 10, 2010
Description:	Documents FIPS 140-2 Level 1 Security Policy issues, compliance and requirements for FIPS compliant operation.
Firmware Version:	FortiMail OS v3.00, build 529, 091029

FortiMail OS v3.00 FIPS 140-2 Security Policy
v1.4

August 10, 2010

06-30MR5-109331-20090831

This document may be copied without Fortinet Incorporated's explicit permission provided that it is copied in its entirety without any modification.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, v3.00, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

References	3
Introduction.....	3
Security Level Summary	4
Module Description	4
Module Interfaces.....	5
Web-Based Manager	6
Command Line Interface	6
Roles, Services and Authentication	6
Physical Security	9
Operational Environment	9
Cryptographic Key Management.....	10
Alternating Bypass Feature	11
Key Archiving	12
Mitigation of Other Attacks.....	12
FIPS 140-2 Compliant Operation	12
Enabling FIPS Mode	13
Self-Tests.....	13
Non-FIPS Approved Services	14

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiMail OS v3.00 firmware, which runs on the FortiMail family of security appliances. This policy describes how the FortiMail OS v3.00 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.

This document contains the following sections:

- [Introduction](#)
- [Security Level Summary](#)
- [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>.

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 provides 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 OS 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 certification.

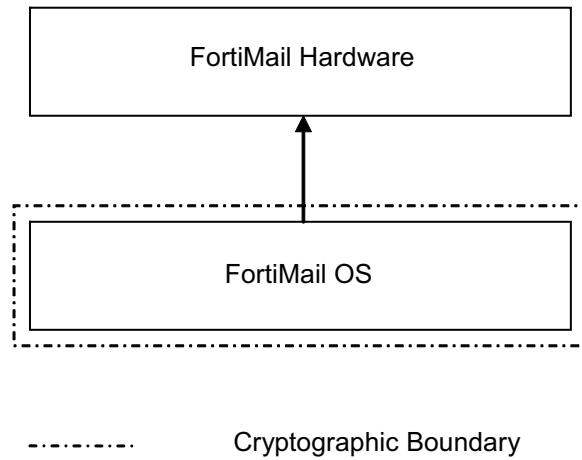
Table 1: Summary of FIPS security requirements and compliance levels

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 constitutes the entire firmware based operating system for a FortiMail appliance 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.

Figure 1: FortiMail Cryptographic Boundary



For the purposes of FIPS 140-2 conformance testing, the module was tested on the following FortiMail appliances:

- FortiMail-100
- FortiMail-400
- FortiMail-400B
- FortiMail-2000A
- FortiMail-4000A

The module can also be executed on any of the following FortiMail appliances and remain FIPS-compliant:

- FortiMail-2000
- FortiMail-2000B
- FortiMail-4000
- FortiMail-5001A

Module Interfaces

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

Table 2: FortiMail OS logical interfaces and physical ports

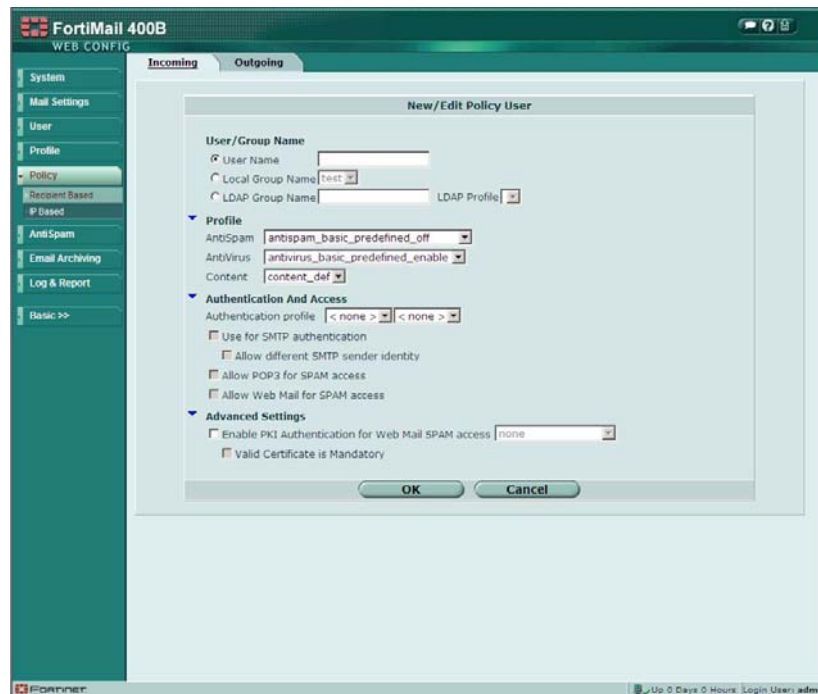
I/O	Logical Interface	Physical Ports
Data Input	API input parameters	Network interface
Data Output	API output parameters	Network interface
Control Input	API function calls	Network interface, serial interface
Status Output	API return values	Network interface, serial interface
Power Input	N/A	The power supply is the power interface

Web-Based Manager

The FortiMail OS web-based manager provides GUI 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 mode. HTTP access to the web-based manager is not allowed in FIPS mode and is disabled.

Figure 2: The FortiMail web-based manager



Command Line Interface

The FortiMail OS 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 mode).

Roles, Services and Authentication

Roles

When configured in FIPS mode, the module provides the following roles for Crypto Officers (hereafter referred to as operators):

- Crypto Officer,
- Senior Crypto Officer,
- Junior Crypto Officer
- Read-only 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.

Only the Crypto Officer has access to the Crypto Officer account.

Senior and Junior Crypto Officer roles are not initially assigned to an operator account. The Crypto officer can create operators and assign them to either Senior or Junior Crypto officer roles:

- The Senior Crypto Officer role has full Read-Write to the entire module, except it does not have access to the Crypto Officer account.
- The Junior Crypto Officer role has full Read-Write to the entire module, except for access to operator accounts. An operator assigned to the Junior Crypto Officer can only manage its own account.
- The Read-only Crypto Officer role has read-only access to the entire module except for access to operator accounts. An operator assigned to the User role can only manage its own account.

The Crypto Officer and Senior Crypto Officer roles are able to create additional operators and users with customized access to the module.

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 or Senior 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. Note that the roles are implicitly assumed based on the service requested by the firmware.

The role names are abbreviated as follows:

Crypto Officer	CO
Senior Crypto Officer	SCO
Junior Crypto Officer	JCO
Read-only Crypto Officer	RCO
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	CO	SCO	JCO	RCO	Key/CSP
authenticate to module	WE	WE	WE	WE	Operator Username, Operator Password
show system status	E	E	E	E	N/A
show FIPS mode enabled/disabled (console only)	E	E	E	E	N/A
enable FIPS mode of operation (console only)	WE	-	-	-	Configuration Integrity Key
execute factory reset (zeroize keys, disable FIPS mode)	WE	WE	-	-	All keys stored in Flash RAM
execute FIPS on-demand self-tests (console only)	WE	WE	WE	WE	N/A
add/delete operators and users	RWE	RWE	-	-	Operator Username, User Username
set/reset Crypto Officer passwords	WE	-	-	-	Operator Password, User Password
set/reset operator and user passwords	WE	WE	-	-	Operator Password, User Password
set/reset own operator password	WE	WE	WE	WE	Operator Password, User Password
backup / restore configuration file	WE	WE	WE	-	Configuration Encryption Key, Configuration Backup Key, all keys stored in Flash RAM
read/set/delete/modify module configuration	RWE	RWE	R	R	N/A
enable/disable alternating bypass mode	RWE	RWE	-	-	N/A
execute firmware update	WE	WE	-	-	Firmware Update Public Key
read log data	R	R	R	R	N/A
delete log data (GUI only)	WE	WE	WE	-	N/A
format log disk (CLI only)	WE	WE	WE	-	N/A

Table 4: Services available to Users

Service/CSP	U	Key/CSP
authenticate to module	WE	User Username, User Password
Access to quarantine email and user preferences	RWE	SSL Server/Host Key, RNG keys, Diffie-Hellman Keys, SSL session keys
Encrypt/decrypt mail messages using SMTPS protocol	E	SSL Server/Host Key, RNG keys, Diffie-Hellman Keys, SSL session keys

Authentication

Operators must authenticate with a user id and password combination to access the modules. Remote operator authentication is done over HTTPS (TLS) or SSH. Local authentication is done over the console connection.

Users must authenticate with a user-id and password combination to access the modules. User authentication is done over HTTPS, POP3S, or IMAPS. HTTPS, POP3S and IMAPS all use the underlying TLS protocol to protect user data.

Note that 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.

Using a strong password policy, where operator and user 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 are 1 in 96^8 .

Physical Security

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

Operational Environment

The module constitutes the entire firmware-based operating system for a FortiMail appliance 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 following FortiMail appliances:

- FortiMail-100
- FortiMail-400
- FortiMail-400B
- FortiMail-2000A
- FortiMail-4000A

Cryptographic Key Management

Random Number Generation

The module uses a firmware-based deterministic random number generator that conforms to the FIPS 186-2 standard, Appendix 3.1, modified as per Change Notice 1.

Key Zeroization

All keys and CSPs, except the RNG Seed Key, are zeroized when the operator executes a factory reset via the web-manager, CLI or console, and when enabling or disabling the FIPS mode of operation via the console. The RNG Seed Key is zeroized by executing a factory reset followed by a firmware update. See [Table 7 on page 11](#) for a complete list of keys and CSPs.

Algorithms

Table 5: FIPS Approved or Allowed Algorithms

Algorithm	NIST Certificate Number
RNG (ANSI X9.31 Appendix A)	682
Triple-DES	884
AES	1231
SHA-1	1131
HMAC SHA-1	718
RSA PKCS1 (digital signature creation and verification)	591

Table 6: Non-FIPS Approved Algorithms

Algorithm
DES (disabled in FIPS mode)
MD5 (disabled in FIPS mode except for use in the TLS protocol)
HMAC MD5 (disabled in FIPS mode)
Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 201 bits of encryption strength; non-compliant less than 80-bits of encryption strength)
RSA PKCS1 - key wrapping; key establishment method provides 80 to 112 bits of encryption strength (1024 to 2048 bit certificates are supported)

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 used in FIPS Mode

Key or CSP	Storage	Usage
Diffie-Hellman Key	SDRAM Plain-text	Key agreement and key establishment
RNG Seed (ANSI X9.31 Appendix A.2.4)	SDRAM Plain-text	Seed used for initializing the RNG
RNG AES Key (ANSI X9.31 Appendix A.2.4)	Flash RAM Plain-text	AES Seed key used with the RNG
Firmware Update Key	Flash RAM Plain-text	Verification of firmware integrity for download of new firmware versions using RSA public key
Firmware Integrity Key	Flash RAM Plain-text	Verification of firmware integrity during firmware integrity testing using RSA public key
HTTPS/TLS Server/Host Key	Flash RAM Plain-text	RSA private key used in the HTTPS/TLS protocols
HTTPS/TLS Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 key used for HTTPS/TLS session authentication
HTTPS/TLS Session Encryption Key	SDRAM Plain-text	AES or Triple-DES key used for HTTPS/TLS session encryption
SSH Server/Host Key	Flash RAM Plain-text	RSA private key used in the SSH protocol
SSH Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 key used for SSH session authentication
SSH Session Encryption Key	SDRAM Plain-text	AES or Triple-DES key used for SSH session encryption
Configuration Integrity Key	Flash RAM Plain-text	HMAC SHA-1 key used for configuration and firmware integrity (bypass) tests
Configuration Encryption Key	Flash RAM Plain-text	AES key used to encrypt CSPs on the flash RAM and in the backup configuration file (except for operator passwords in the backup configuration file)
Configuration Backup Key	Flash RAM Plain-text	HMAC SHA-1 key used to hash operator passwords in the backed up configuration file
Operator Password	Flash RAM SHA-1 hash	Used during operator authentication
Operator Public Key	Flash RAM, Plain-text	RSA public key used for operator authentication
User Password	Flash RAM AES encrypted	Used during user authentication

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).

Key Archiving

The module supports key archiving to a management computer or USB token as part of a module configuration file backup. Passwords and non-hard-coded keys are archived as part of the module configuration file. The configuration file is stored in plain text, but passwords and keys in the configuration file are AES encrypted.

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 mode of operation and that you follow secure procedures for installation and operation of the FortiMail unit. You must ensure that:

- The FIPS mode of operation is enabled
- The FortiMail unit is installed in a secure physical location.
- 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 should be capitalized
 - One (or more) of the characters should be numeric
 - One (or more) of the characters should 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 (using TLS)
 - Command line interface (CLI) access via SSH
- Diffie-Hellman key sizes of less than less than 1024 bits (Group 5) are not used.

To remain FIPS 140-2 compliant, the module can only be configured to operate in either gateway or transparent mode.

Enabling FIPS Mode

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

```
set system fips status enable
```

Note: FIPS mode of operation cannot be enabled when the module is configured to be in server mode.

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 compliant 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 compliant mode by executing the following command from the CLI:

```
get system status
```

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

```
FIPS status: enabled
```

Self-Tests

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

- Firmware integrity test using RSA 1024-bit signature verification
- Configuration bypass test using HMAC SHA-1 (Configuration table integrity test)
- Triple-DES, CBC mode, encrypt/decrypt known answer test
- AES, CBC mode, encrypt/decrypt known answer test
- HMAC SHA-1 known answer test
- RSA signature generation/verification known answer test
- RNG 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:

- to initiate all self-tests:

```
execute fips kat all
```

- To initiate a specific self-test:

```
execute fips kat <test>
```

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

- Continuous RNG test
- RSA pairwise consistency test
- Configuration bypass test using HMAC SHA-1 (Configuration table integrity test)

- Firmware download integrity test using RSA signatures

Non-FIPS Approved Services

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

- Server Mode of operation

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