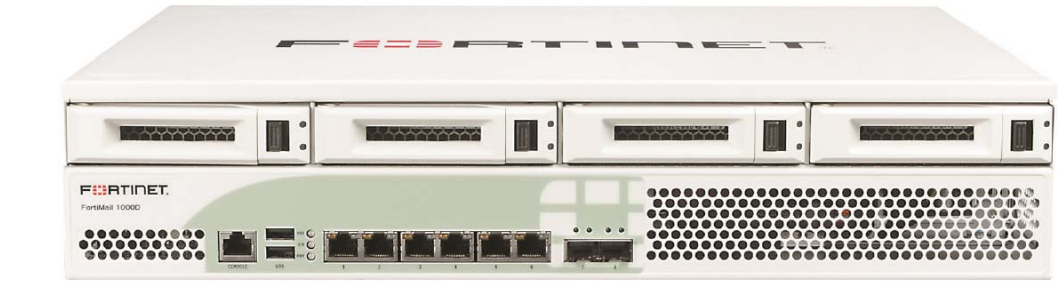
FIPS 140-2 Security Policy

FortiMail-1000D/3000D



FortiMail-1000D/3000D FIPS 140-2 Security Policy	
Document Version:	1.7
Publication Date:	January 4, 2016
Description:	Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Firmware Version:	FortiMailOS 5.2, build0460,150922
Hardware Version:	FortiMail-1000D (C1AA85) with disk trays (SP-D2000) and power supplies (SP-FXX1000D-PS)
	FortiMail-3000D (C1AA63) with disk trays (SP-D2TC) and power supplies (D750E-S1)

FortiMail-1000D/3000D: FIPS 140-2 Security Policy

06-520-244996-20140611

for FortiMail 5.2

Contents

Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiMail-1000D and 3000D message security appliances. This policy describes how the FortiMail 1000D and 3000D appliances (hereafter referred to as the 'modules') meet the FIPS 140-2 security requirements and how to operate the modules in a FIPS compliant manner. This policy was created as part of the Level 2 FIPS 140-2 validation of the modules.

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 appliances offer 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 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	3
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Module Description

The FortiMail-1000D and 3000D are multiple chip, standalone cryptographic modules consisting of production grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 2 requirements.

The modules have a similar appearance and perform the same functions, but have different numbers and types of network interfaces in order to support different network configurations:

- The FortiMail-1000D has 8 network interfaces with a status LED for each network interface (2x 1GB SFP, 6x 10/100/1000 Base-T)
- The FortiMail-3000D has 6network interfaces with a status LED for each network interface (2x 1GB SFP, 4x 10/100/1000 Base-T)

The FortiMail-1000D has one, 4 core, x86 compatible CPU, 4 removable hard drives, 2 removable power supplies and is a 2u rackmount device.

The FortiMail-3000D has two, 6 core, x86 compatible CPUs, 8 removable hard drives, 2 removable power supplies and is a 2u rackmount device.

The modules have ventilation fans on the back panel of the chassis.

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

The modules use a Fortinet entropy token (part number FTR-ENT-1) as the entropy source.

Figure 1 and Figure 2 are representative of the modules tested.

The FortiMail-3000D hardware includes several components that are not supported by the FortiMail firmware and therefore are not part of the evaluated configuration:

- Control panel with LCD
- DVD drive
- 2 VGA ports

Cryptographic Module Ports and Interfaces

FortiMail-1000D Chassis Module

Figure 1: FortiMail-1000D Front and Rear Panels

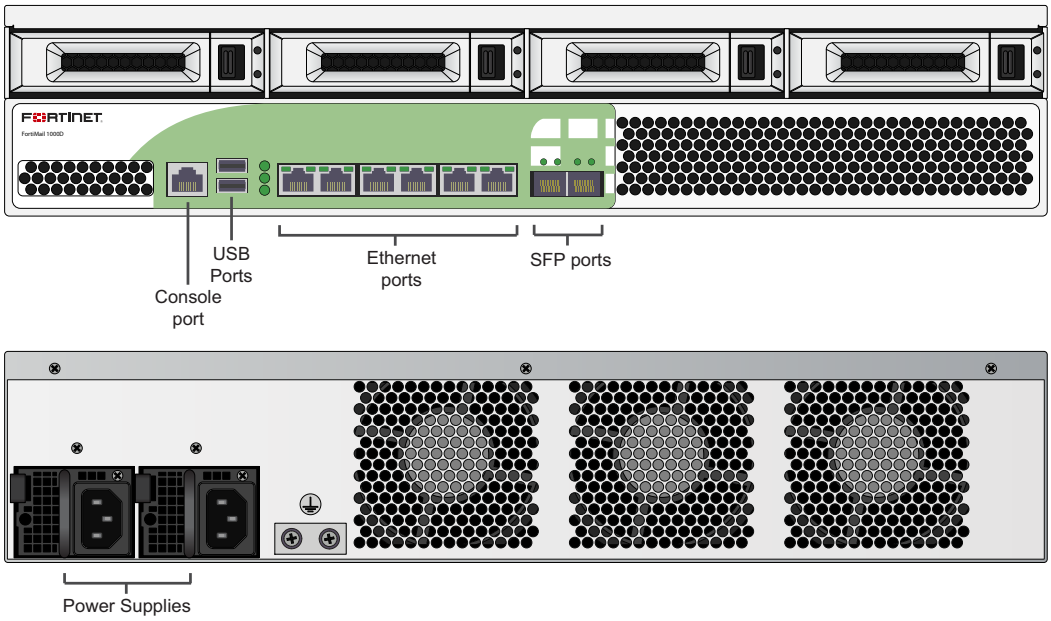


Table 2: FortiMail-1000D Status LEDs

LED		State	Description
HDD		N/A	Not used.
Power		Green	The module is powered on.
		Off	The module is powered off.
Status		Green	The module is running normally.
		Off	The module is powered off.
Hard Disks	Power	Blue	Hard drive installed and powered.
		Off	The module is powered off.
	Status	Flashing Green	Hard drive activity.
		Red	Hard drive failure.
		Off	Hard drive is idle.
SFP Ports	Link	Orange	Port is online.
		Flashing Orange	Port is receiving or sending data.
	Activity	Yellow	Port is active
		Flashing Yellow	Port is receiving or sending data.
		Off	Port is not in use.

Ethernet Ports	Link	Green	Port is online.
		Flashing Green	Port is receiving or sending data.
	Activity	Green	Connected at 1000 Mbps.
		Amber	Connected at 100 Mbps.
		Off	Connected at 10Mbps.
AC Power		Green	Power supply is running.
		Flashing Green	Power supply is functional, but but not running.
		Flashing Red	The power supply has failed.
		Flashing Red/Green	Power supply warning.
		Off	Power is not connected.

Table 3: FortiMail-1000D Front Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ethernet Ports 1-6	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Copper gigabit connection to 10/100/1000 copper networks.
SFP Ports 7-8	SFP	1Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
CONSOLE	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB	USB A	N/A	Data input, data output	Key loading and archiving, entropy input.

Table 4: FortiMail-1000D Rear Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
POWER	N/A	N/A	Power	120/240VAC power connection.

FortiMail-3000D Chassis Module

Figure 2: FortiMail-3000D Front and Rear Panels

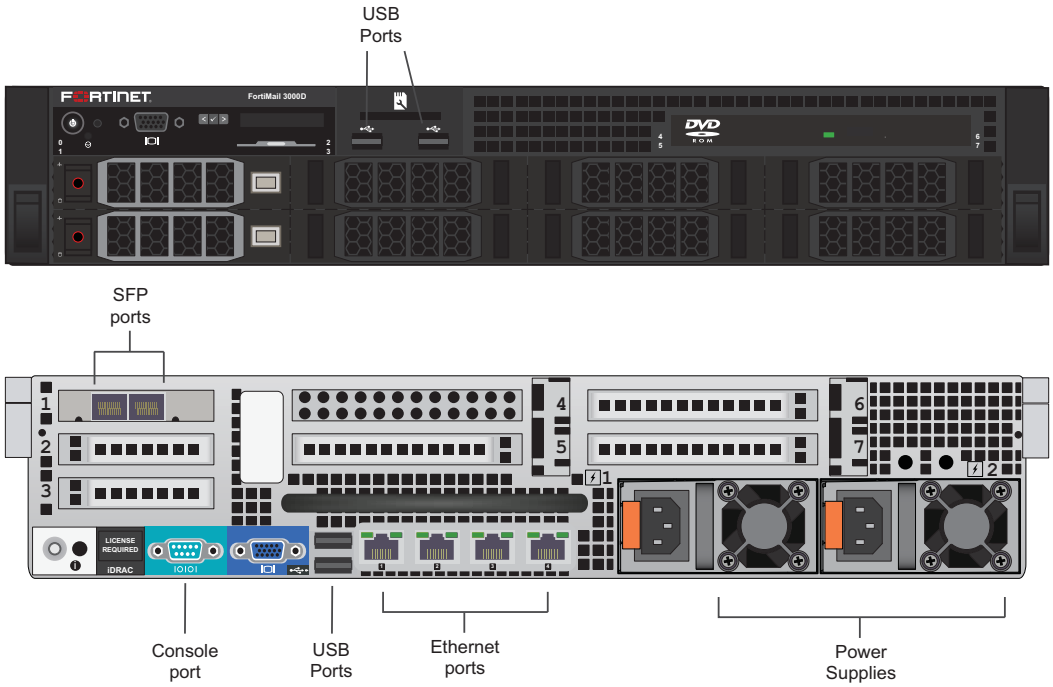


Table 5: FortiMail-3000D Status LEDs

LED		State	Description
Power		Green	The module is powered on.
		Off	The module is powered off.
Status		Flashing Green	The module is starting up.
		Green	The module is running normally.
		Off	The module is powered off.
Hard Disks		Green	Drive is online.
		Flashing Amber	Drive has failed
		Flashing Gree/Amber/Off	Drive is predicted to fail.
		Flashing Green	Drive is rebuilding.
		Off	Drive is ready for insertion or removal.
SFP Ports		Amber	Port is connected at 1Gbps.
		Green	Port is connected at 10/100Mbps.
		Off	Port is not in use.
Ethernet Ports	Link	Green	Port is online.
		Flashing Green	Port is receiving or sending data.
	Activity	Green	Port is connected at 1Gbps.
		Amber	Port is connected at 10/100Mbps.
		Off	Port is not in use.

AC Power	Green	Power supply is operational.
	Flashing Amber	Power supplies are mismatched.
	Off	Power is not connected.

Table 6: FortiMail-3000D Front Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
USB	USB A	N/A	Data input, data output	Key loading and archiving, entropy input.
VGA	N/A	N/A	N/A	Not supported.
Flash Media	N/A	N/A	N/A	Not supported.

Table 7: FortiMail-3000D Rear Panel Connectors and Ports

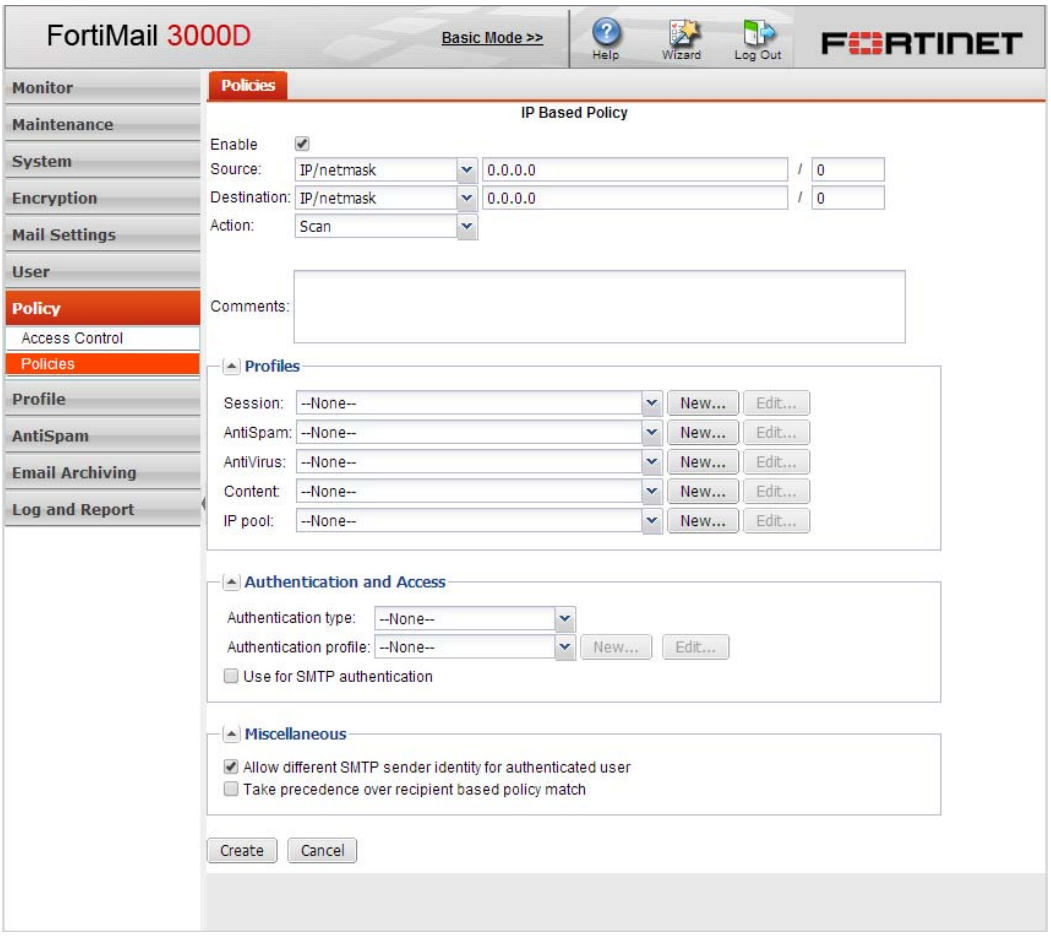
Connector	Type	Speed	Supported Logical Interfaces	Description
Ethernet Ports 1-4	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Copper gigabit connection to 10/100/1000 copper networks.
SFP Ports 5 to 6	QSFP +	40Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
USB	USB A	N/A	Data input, data output	Key loading and archiving, entropy input.
CONSOLE	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
VGA	N/A	N/A	N/A	Not supported.
iDRAC	N/A	N/A	N/A	Not supported.
POWER	N/A	N/A	Power	120/240VAC power connection.

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 3: 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 8: 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 8: 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 9: 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

Note: Services marked with an asterisk (*) may use non-compliant encryption strengths for Diffie-Hellman and RSA. Refer to Table 11 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 16.

Physical Security

The modules meet FIPS 140-2 Security Level 2 requirements by using production grade components and an opaque, sealed enclosure. Access to the enclosure is restricted through the use of tamper-evident seals to secure the overall enclosure.

The seals are serialized red wax/plastic with black lettering that reads “Fortinet Security Seal”.

The tamper seals are not applied at the factory prior to shipping. It is the responsibility of the Crypto Officer to apply the seals before use to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the modules and the tamper seals have not been damaged or tampered with in any way. The Crypto Officer is also responsible for securing and controlling any unused seals.

The surfaces should be cleaned with 99% Isopropyl alcohol to remove dirt and oil before applying the seals. Ensure the surface is completely clean and dry before applying the seals. If a seal needs to be re-applied, completely remove the old seal and clean the surface with an adhesive remover before following the instructions for applying a new seal. The seals require a curing time of 24 hours to ensure proper adhesion.

Additional seals can be ordered through your Fortinet sales contact. Reference the following SKU when ordering: FIPS-SEAL-RED. Specify the number of seals required based on the specific module as described below.

The FortiMail-1000D uses 1 seal to secure:

- tthe external enclosure (1 seal, see Figure 4)

The FortiMail-3000D uses 2 seals to secure:

- the external enclosure (1 seal, see Figure 5)
- the front faceplate (1 seal, see Figure 6)

Figure 4: FortiMail-1000D external enclosure seal, top, left

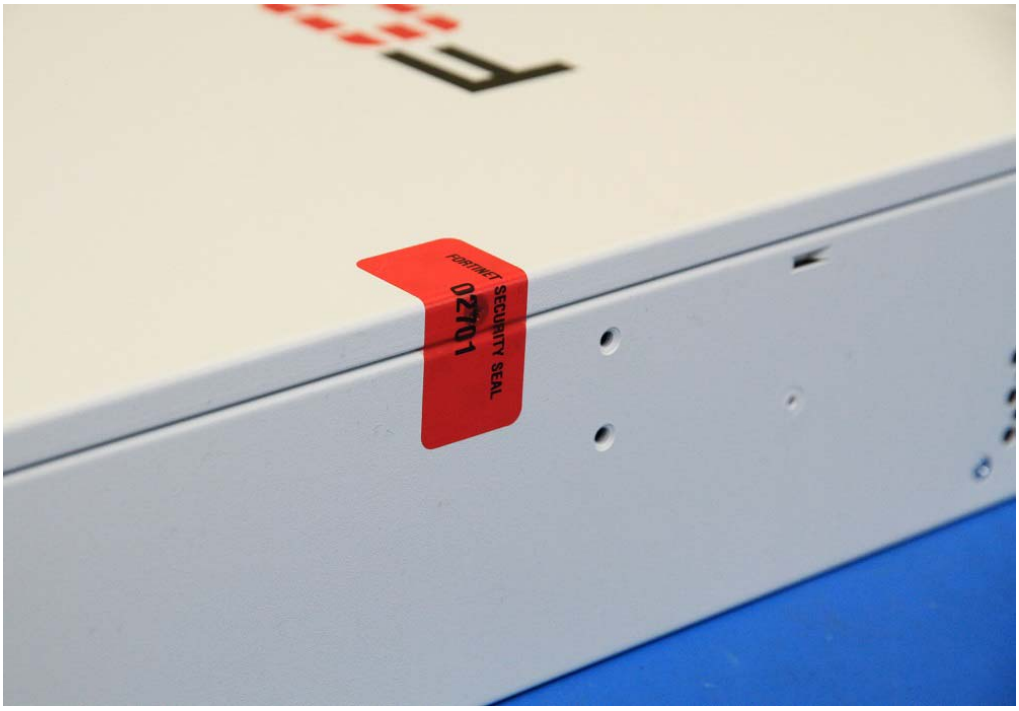


Figure 5: FortiMail-3000D Enclosure Seal, top

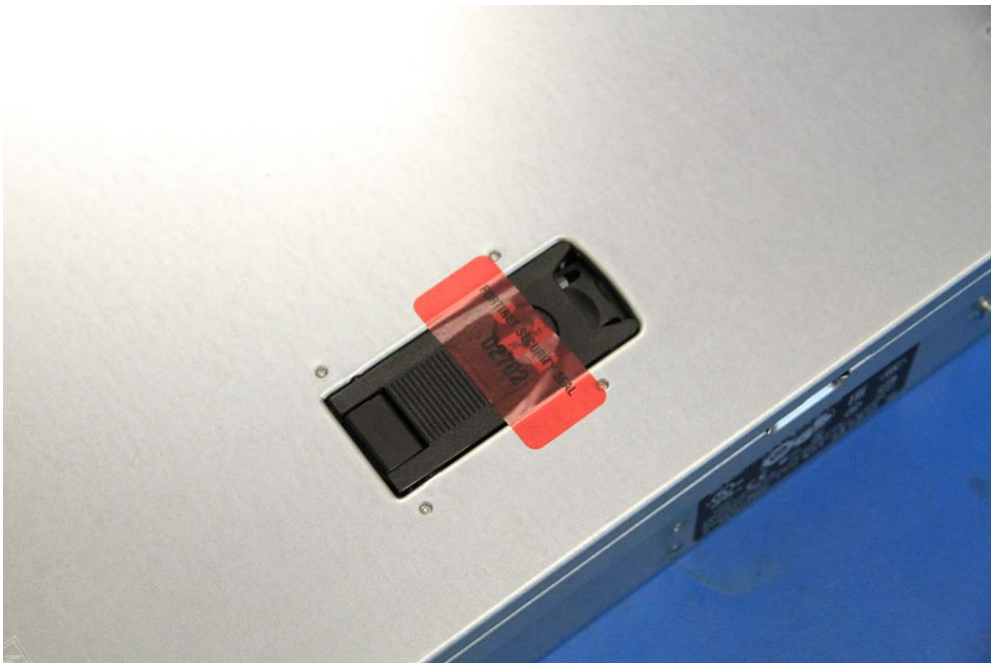


Figure 6: FortiMail-3000D Front Faceplate seal

Operational Environment

The module consists of the combination of the FortiMail firmware and the FortiMail appliance. The FortiMail firmware can only be installed, and run, on a FortiMail appliance. The FortiMail firmware provides a proprietary and non-modifiable operating system.

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 10: 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-, AES128-, AES256-CBC (using SHA1)	574
CVL (TLS) - TLS1.0/1.1 and TLS1.2 (using SHA 256)	574

Table 11: 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 12: 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 minimum 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 13: Cryptographic Keys and Critical Security Parameters used in FIPS Mode

Key or CSP	Storage	Usage	Zeroization
DRBG output	Flash RAM Plain-text	Random numbers used in cryptographic algorithms	By erasing the flash memory and power cycling the module
DRBG v and key values	Flash Ram 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 RAM Plain-text	Verification of firmware integrity for download of new firmware versions using RSA public key	By erasing the flash memory and power cycling the module
HTTPS/TLS Server/Host Key	Flash RAM Plain-text	RSA 2048bit private key used in the HTTPS/TLS protocols	By erasing the flash memory and power cycling the module

Table 13: Cryptographic Keys and Critical Security Parameters used in FIPS Mode

Key or CSP	Storage	Usage	Zeroization
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-128/192/256 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 RAM Plain-text	RSA 2048bit 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-128/192/256 key used for SSH session encryption	By erasing the flash memory and power cycling the module
Configuration Integrity Key	Flash RAM 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 RAM Plain-text	AES-128 key used to encrypt CSPs on the flash RAM 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 RAM 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
Operator Password	Flash RAM SHA-1 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 13).
- 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-1
- 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 (test as part of HMAC SHA-1 known answer test)
- HMAC SHA-256 known answer test
- SHA-256 known answer test (test 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).

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 8 and Table 9 are considered non-approved when using the following algorithms:

- Non-compliant-strength Diffie-Hellman
- Non-compliant-strength RSA key wrapping
- DES
- HMAC-MD5