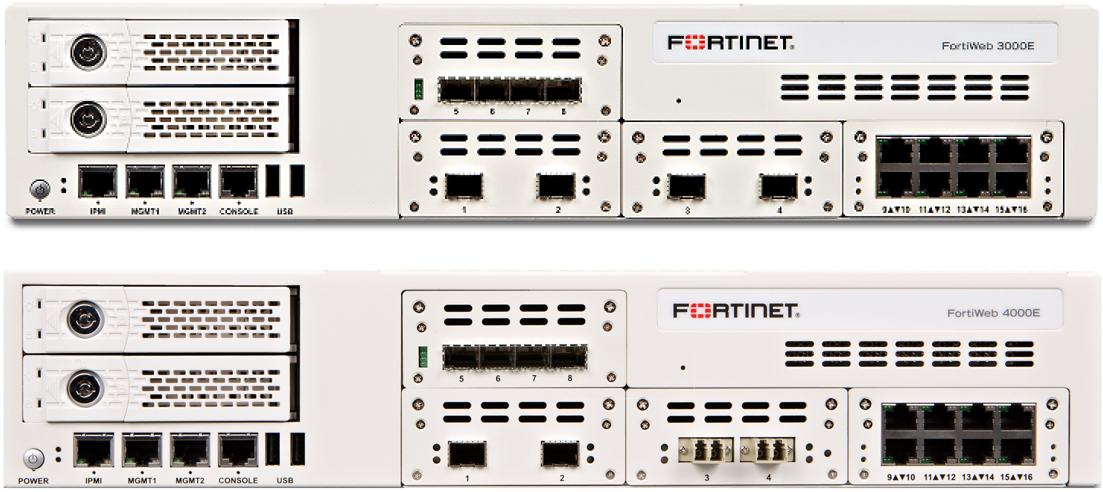
FORTINET

High Performance Network Security

FIPS 140-2 Non-Proprietary Security Policy

FortiWeb-3000E/4000E



FortiWeb-3000E/4000E FIPS 140-2 Security Policy			
Document Version:	2.3		
Publication Date:	Thursday, January 04, 2018		
Description:	Documents FIPS 140-2 Non-Proprietary Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.		
Firmware Version:	v5.6.0, build 6180,170928		
Hardware Version:	FortiWeb-3000E (C1AD49)	FortiWeb-4000E (C1AF19)	

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

FORTINET®

Thursday, January 04, 2018

FortiWeb-3000E/4000E FIPS 140-2 Non-Proprietary Level 2 Security Policy

01-560-0418200-20170410

TABLE OF CONTENTS

Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiWeb-3000E and 4000E Web Application Firewall appliances. This policy describes how the FortiWeb-3000E and 4000E (hereafter referred to as the 'modules') meet the FIPS 140-2 security requirements and how to operate the module in a FIPS compliant manner. This policy was created as part of the FIPS 140-2 Level 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 modules 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://fortiguard.com.

Introduction

The FortiWeb Web Application Firewall provides specialized, layered application threat protection for medium and large enterprises, application service providers, and SaaS providers. FortiWeb Web Application Firewall protects your web-based applications and internet-facing data from attack and data loss. Using advanced techniques to provide bidirectional protection against malicious sources, application layer DoS Attacks and Sophisticated Threats like SQL injection and Cross-site scripting.

FortiWeb platforms help you prevent identity theft, financial fraud and denial of service. It delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal policies.

Security Level Summary

The modules 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 Descriptions

The FortiWeb- 3000E and FortiWeb- 4000E 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:

FortiWeb-3000E specifications:

- 16 network interfaces (4x 1GB SFP, 4x 10G SFP+, 8x 10/100/1000 Base-T)
- Two x86 compatible CPUs
- 2U rackmount device
- 4TB (2TB x 2) hard disk drives

FortiWeb-4000E specifications:

- 16 network interfaces (4x 1GB SFP, 2x 10G SFP+, 2x SFP+ paired bypass ports, 8x 10/100/1000 Base-T)
- Two x86 compatible CPUs
- 2U rackmount device
- 4TB (2TB x 2) hard disk drives

The validated firmware version is FortiWeb v5.6.0, build 6180,170928

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

The FortiWeb-4000E module also has 2 bypass interfaces (SFP+ ports 3 and 4) that are paired with SFP+ ports 1 and 2. If bypass is enabled, these interfaces provide a physical bypass of the paired port if the module fails, hangs or power is lost. Use of the bypass capability is a non-FIPS approved service.

Cryptographic Module Ports and Interfaces

FortiWeb- 3000E

Figure 1: FortiWeb-3000E Front and Rear Panels

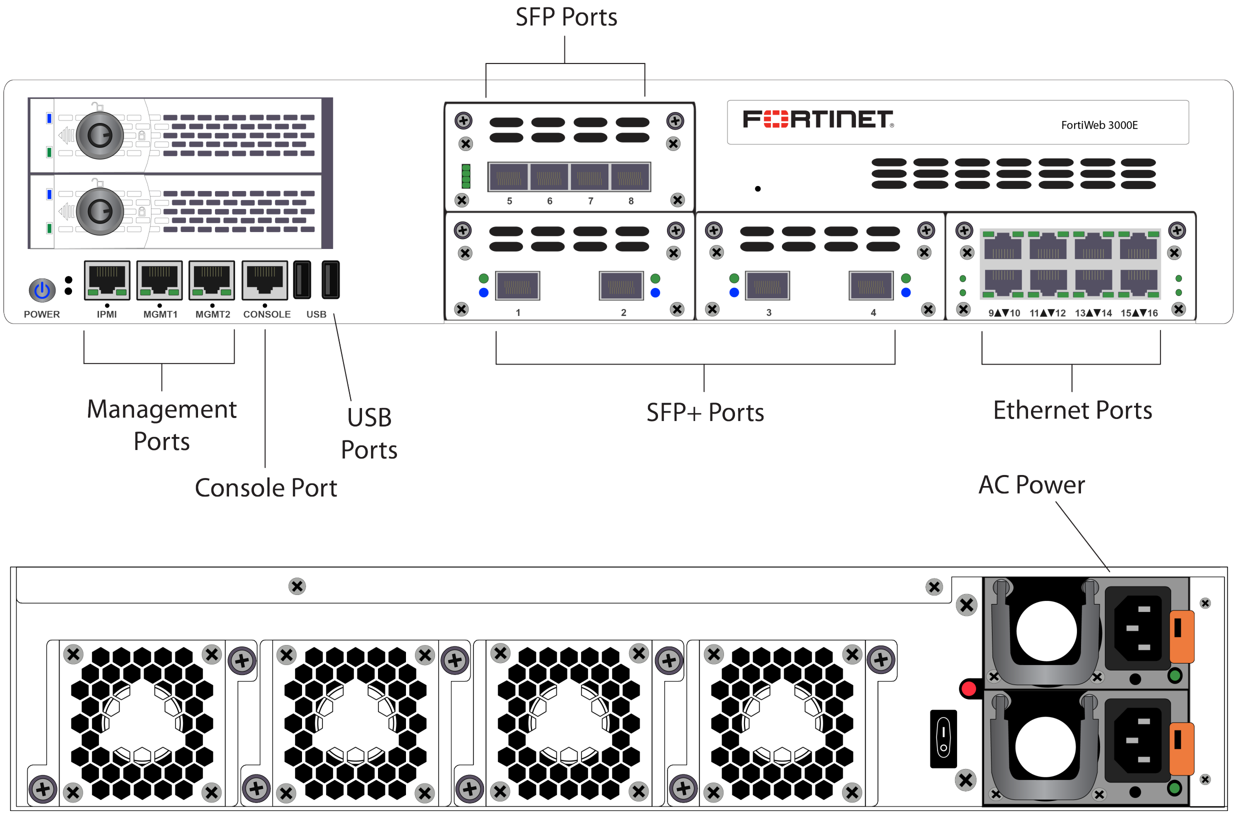


Table 2: FortiWeb-3000E Status LEDs

LED	State	Description
Power	Blue	The module is powered on.
	Off	The module is powered off.

LED		State	Description
Power Connections		Green	Power supply operating normally, power on
		Flashing Green	Power supply operating normally, system standby
		Flashing Yellow	Power supply malfunction
		Off	Power not connected
HDD Power		Blue	HDD power on
		Off	HDD power off
HDD Activity		Flashing Green	HDD read/write
		Off	HDD power off
IPMI,MGMT,SFP+ 1- 4, SFP 5-8, RJ-45 9-16	Link/ACT	Green	Port is online.
		Flashing Green	Port is receiving or sending data.
		Off	Port is not in use.
	Speed	Blue	Connected at 10 Gbps.
		Yellow	Connected at 1 Gbps.
		Green	Connected at 1000 Mbps.
		Off	Connected at 10Mbps or not in use
RJ-45 LAN Bypass Ports 9 & 10, 11 & 12, 13 & 14, 15 & 16		Green	Normal
		Red	Bypass
		Off	Bypass disabled

Table 3: FortiWeb-3000E Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1 - 4	SFP+	10 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 5 - 8	SFP	1 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 9 -16	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.
Management Ports (IMPI & MGMT 1 - 2)	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.
USB	USB-A	N/A	Key loading and archiving, entropy input	Optional USB token and entropy token.
Console	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
Power	N/A	N/A	Power	120/240VAC power connection

FortiWeb-4000E

Figure 2: FortiWeb-4000E Front and Rear Panels

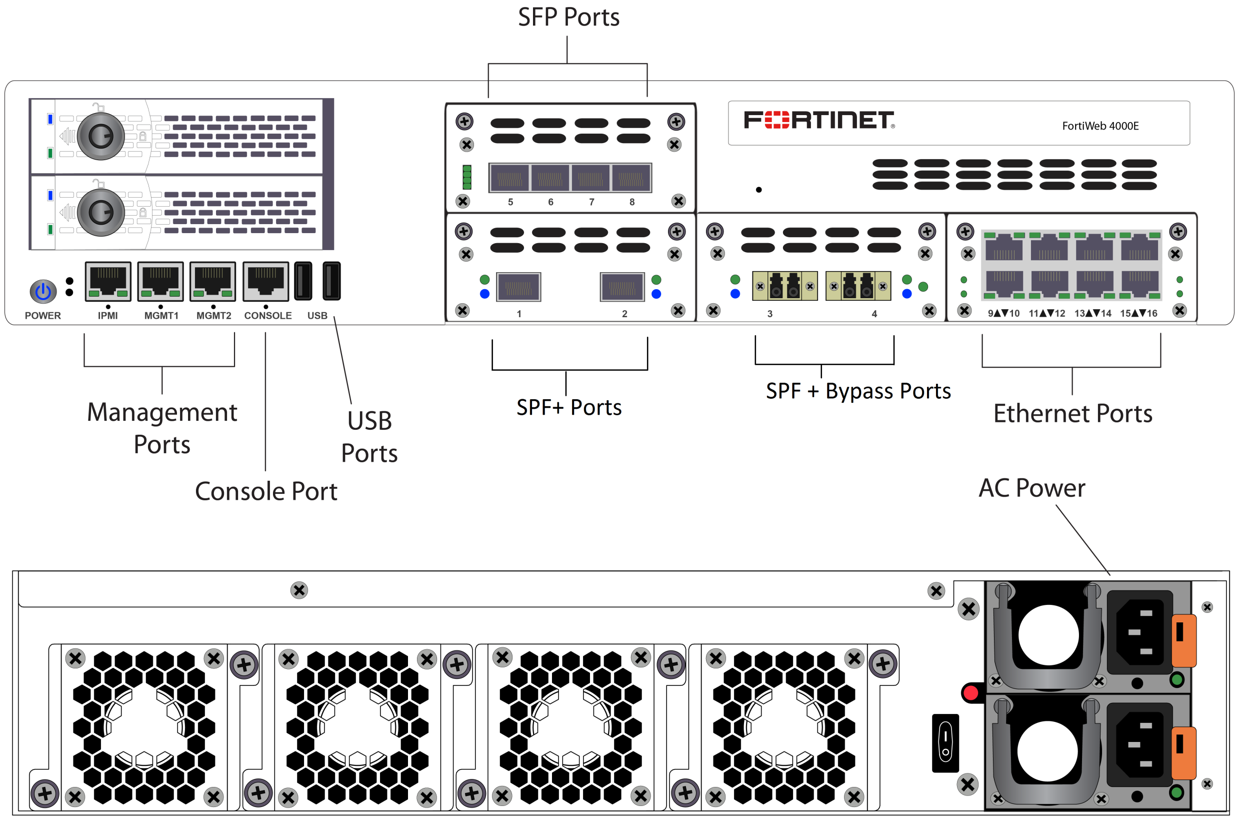


Table 4: FortiWeb-4000E Status LEDs

	State	Description
Power	Blue	The module is powered on.
	Off	The module is powered off.
Power Connections	Green	Power supply operating normally, power on
	Flashing Green	Power supply operating normally, system standby
	Flashing Yellow	Power supply malfunction
	Off	Power not connected

		State	Description
HDD Power		Blue	HDD power on
		Off	HDD power off
HDD Activity		Flashing Green	HDD read/write
		Off	HDD power off
IPMI,MGMT1 - 2,SFP+ 1- 2, SFP 5-8, RJ-45 9-16	Link/ACT	Green	Port is online.
		Flashing Green	Port is receiving or sending data.
		Off	Port is not in use.
	Speed	Blue	Connected at 10 Gbps.
		Yellow	Connected at 1 Gbps.
		Green	Connected at 1000 Mbps.
		Off	Connected at 10Mbps or not in use
SFP+ LAN Bypass Ports 3 & 4 RJ-45 LAN Bypass Ports 9 & 10, 11 & 12, 13 & 14, 15 & 16		Green	Normal
		Red	Bypass
		Off	Bypass disabled

Table 5: FortiWeb-4000E Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1-2	SFP+	10 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 3-4	SFP+	10Gbps	Data input, data output, control input, and status output	Paired bypass ports. Multimode fiber optic connections to gigabit optical networks.
Ports 5 - 8	SFP	1 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.

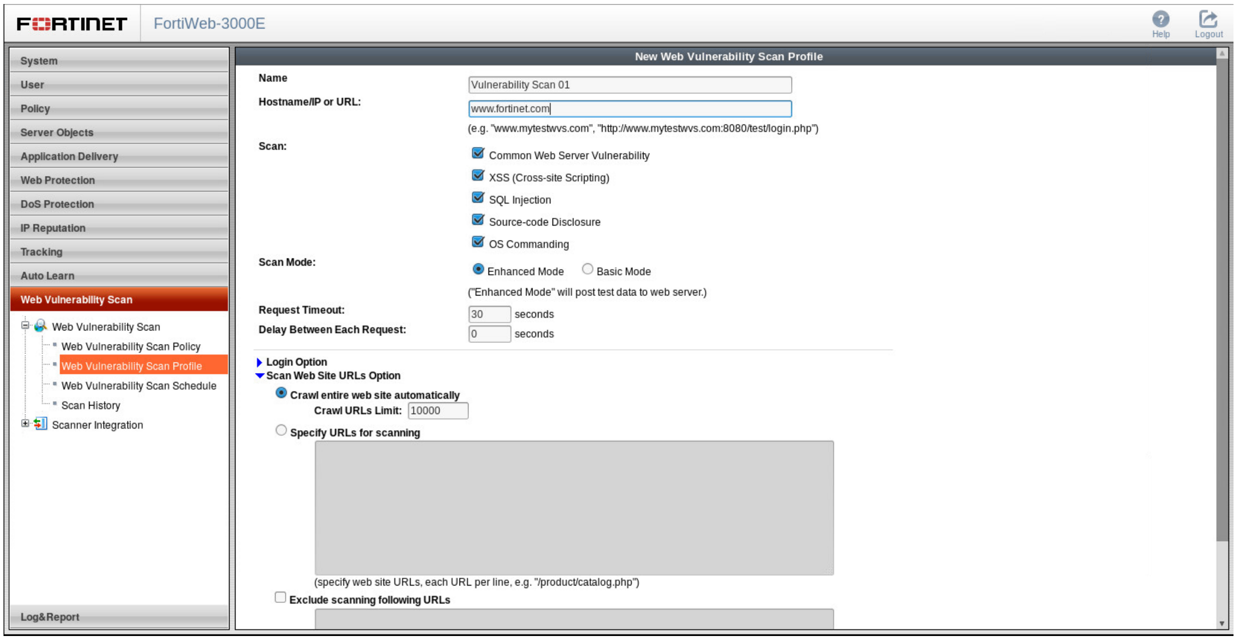
Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 9 -16	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
Management Ports (IMPI & MGMT 1 - 2)	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
USB	USB-A	N/A	Key loading and archiving, entropy input	Optional USB token and entropy token.
Console	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
Power	N/A	N/A	Power	120/240VAC power connection

Web-Based Manager

The FortiWeb 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 FortiWeb unit and the management computer.

A web-browser that supports Transport Layer Security (TLS) 1.2 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 mode and is disabled.

Figure 3: The FortiWeb web-based manager



New Web Vulnerability Scan Profile

Name: Vulnerability Scan 01

Hostname/IP or URL: www.fortinet.com

(e.g. "www.mytestwvs.com", "http://www.mytestwvs.com:8080/test/login.php")

Scan:

☑ Common Web Server Vulnerability
☑ XSS (Cross-site Scripting)
☑ SQL Injection
☑ Source-code Disclosure
☑ OS Commanding

Scan Mode: ● Enhanced Mode ○ Basic Mode

("Enhanced Mode" will post test data to web server.)

Request Timeout: 30 seconds

Delay Between Each Request: 0 seconds

▶ Login Option

▼ Scan Web Site URLs Option

● Crawl entire web site automatically

Crawl URLs Limit: 10000

○ Specify URLs for scanning

(specify web site URLs, each URL per line, e.g. "/product/catalog.php")

□ Exclude scanning following URLs

Command Line Interface

The FortiWeb 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 FortiWeb 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
- Network 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 modules also provide a **Network User** role for end-users (Users). Network Users can make use of the encrypt/decrypt services, but cannot access the modules for administrative purposes.

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 in each mode of operation, the types of access for each role and the Keys or CSPs they affect.

The access types are abbreviated as follows:

Read Access	R
Write Access	W
Execute Access	E

Table 6: Services available to Crypto Officers

Service	Access	Key/CSP
authenticate to module*	WE	Crypto Officer Password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Authentication Keys, and HTTPS/TLS and SSH Session Encryption Keys, DRBG Output, DRBG Seed, NDRNG Output String, DRBG v and key values
show system status	N/A	N/A
show FIPS-CC mode enabled/disabled (console/CLI only)	N/A	N/A
enable FIPS-CC mode of operation (console only)	WE	Configuration Integrity Key
key zeroization	W	All Keys
execute factory reset (disable FIPS-CC mode, console/CLI only)	W	All keys stored in Flash RAM
execute FIPS-CC on-demand self-tests (console only)	E	Configuration Integrity Key, Firmware Integrity Key

Service	Access	Key/CSP
add/delete Crypto Officer and network users	WE	Crypto Officer Password, Network User Password
set/reset Crypto Officer and network user passwords	WE	Crypto Officer Password, Network User Password
backup/restore configuration file	RWE	Configuration Encryption Key, Configuration Backup Key
read/set/delete/modify module configuration	N/A	N/A
modify user preferences	N/A	N/A
execute firmware update	WE	Firmware Update Key
read log data (GUI only)	N/A	N/A
delete log data (GUI only)	N/A	N/A
execute system diagnostics (console/CLI only)	N/A	N/A
format log disk (CLI only)	WE	N/A
enable/disable alternating bypass mode	WE	N/A

Table 7: Services available to Network Users in FIPS-CC mode

Service/CSP	Access	Key/CSP
authenticate to module*	E	Network User Password, Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, DRBG Output, DRBG Seed, NDRNG Output String, DRBG v and key values,

Non-FIPS Approved Services

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

- Configuration backups using password protection
- Services marked with an asterisk (*) Table 4 and Table 5 are considered non-approved when using the following algorithms:

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

The above services shall not be used in the FIPS approved mode of operation.

Authentication

The module uses identity based authentication. By default, operators and users authenticate with a username and password combination to access the module. 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.

The minimum password length is 8 characters when in FIPS-CC 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 .

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 tamper-evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. All Networking devices need tamper-evident seals to meet the Physical Security requirements

The seals are 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. Upon viewing any signs of tampering, the Crypto Officer must assume that the device has been fully compromised. The Crypto Officer is required to zeroize the cryptographic module by following the steps in the Key Zeroization section of the SP. 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 Crypto Officer is also responsible for the direct control and observation of any changes to the modules such as reconfigurations where the tamper-evident labels are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS approved state. Additional seals can be requested through your Fortinet sales contact. Reference the ‘FIPS-SEAL-RED’ SKU when ordering. Specify the number of seals required based on the specific model as described below:

The FortiWeb-3000E and FortiWeb-4000E use seven seals in the exact same location to secure:

- The front plates (2 seals, see Figure 4)
- The external enclosure (1 seal, see Figure 5)
- The internal fans (4 seals, see Figure 6)

Figure 4: FortiWeb-3000E and FortiWeb-4000E Front Plate Seals

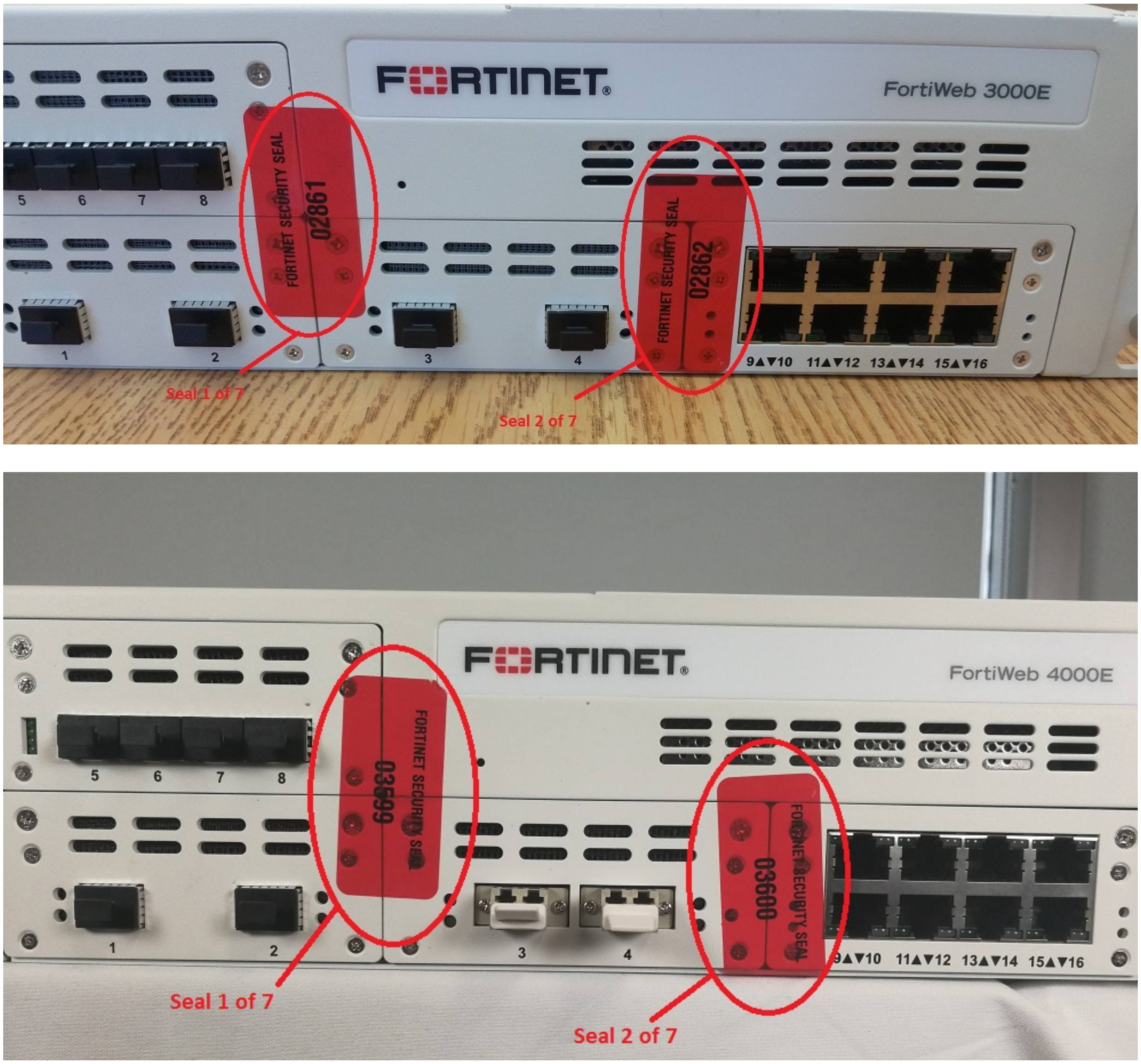


Figure 5: FortiWeb-3000E and FortiWeb-4000E External Enclosure seal

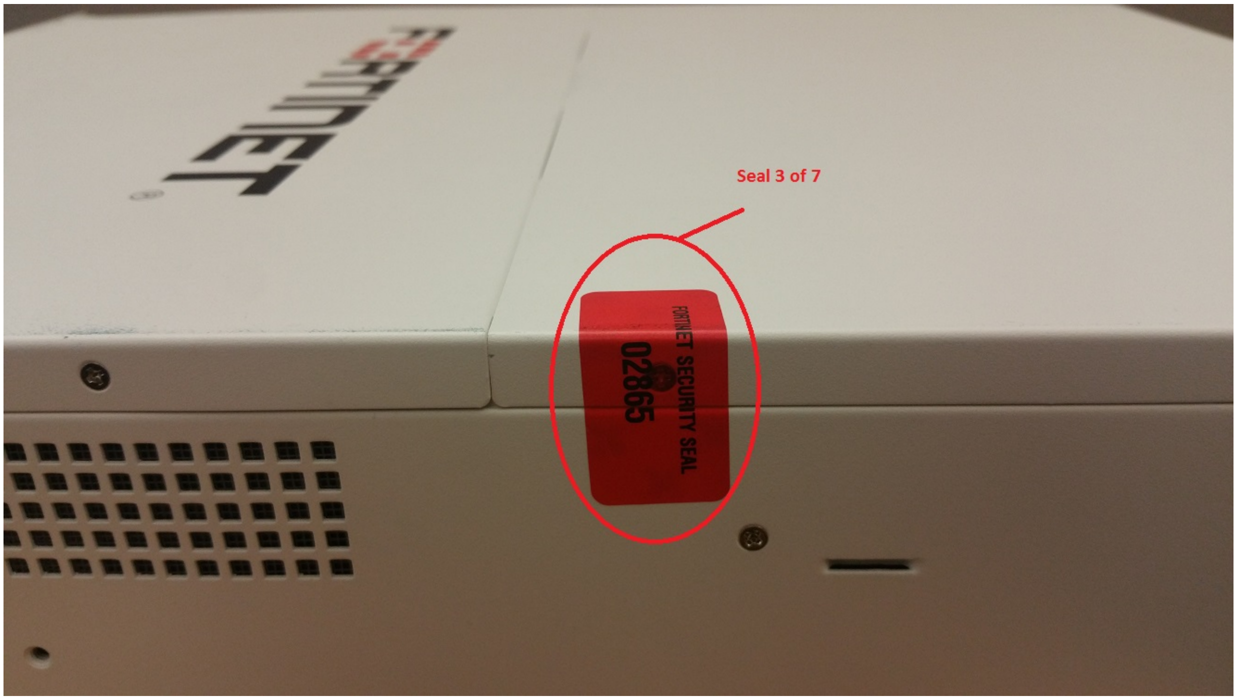
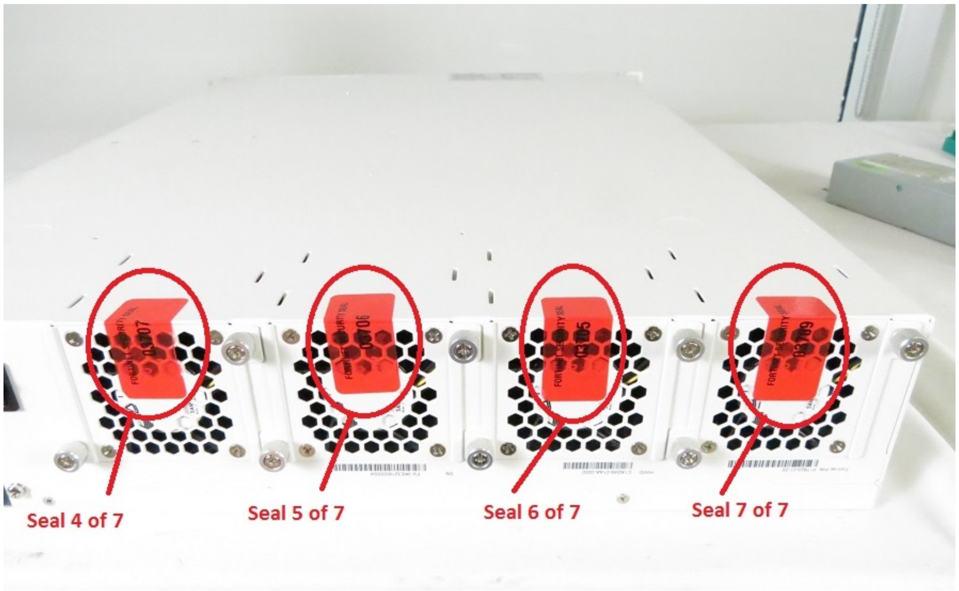


Figure 6: FortiWeb-3000E and FortiWeb-4000E Internal Fans Seals



Operational Environment

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

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.

Entropy

The module uses a Fortinet entropy token (part number FTR-ENT-1 or part number FTR-ENT-2) to seed the DRBG during the modules' 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.

Entropy Strength

The entropy loaded into the approved AES-256 bit DRBG is 256 bits. The entropy source is over-seeded and then an HMAC-SHA-256 post-conditioning component (as per section 6.4.2 of SP 800-90B) is applied.

Reseed Period

The RBG is seeded from the entropy token during the boot process and then reseeded periodically. The default reseed period is once every 24 hours (1440 minutes) and is configurable (1 to 1440 minutes). The entropy token must be installed to complete the boot process and to reseed the DRBG.

Key Zeroization

The zeroization process must be 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 boot device and then power cycling the FortiGate unit. To erase the boot device, execute the following command from the CLI:

```
execute erase-disk <boot device>
```

The boot device ID may vary depending on the FortiGate module. Executing the following command will output a list of the available internal disks:

```
execute erase-disk ?
```

Algorithms

Table 8: FIPS Approved Algorithms

Algorithm	NIST Certificate Number
CTR DRBG (NIST SP 800-90A) with AES 256-bits	1434
AES in CBC mode (128-, 256-bits)	4461
SHA-1	3673
SHA-256	3673
HMAC SHA-1	2960
HMAC SHA-256	2960
RSA PKCS1 • Key Pair Generation: 2048 and 3072 bit • Signature Generation: 2048 and 3072-bit • Signature Verification: 1024, 2048 and 3072-bit • For legacy use, the module supports 1024-bit RSA keys and SHA-1 for signature verification	2437
CVL (SSH) AES 128-bit, AES 256-bit CBC (using SHA1)	1169
CVL (TLS 1.0 and 1.1)	1169
CKG (NIST SP 800-133)	Vendor Affirmed

KTS (AES Cert. #4461 and HMAC Cert. #2960; key establishment methodology provides between 128 and 256 bits of encryption strength).

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG)as per SP800-133 (vendor affirmed). The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

There are algorithms, modes, and keys that have been CAVs tested but are not available when the module is configured for FIPS compliant operation. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are supported by the module in the FIPS validated configuration.

Table 9: FIPS Allowed Algorithms

Algorithm
RSA (CVL Cert. #1169, key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)
Diffie-Hellman (CVL Cert. #1169, key agreement; key establishment methodology provides 112 bits of encryption strength)
NDRNG (Entropy Token)
MD5 (only used as part of the TLS protocol)

Table 10: Non-FIPS Approved Algorithms

Algorithm
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 SSH and TLS protocols, other than the KDF, have not been tested by the CMVP or CAVP as per FIPS 140-2 Implementation Guidance D.11.

Cryptographic Keys and Critical Security Parameters

The following table lists all of the cryptographic keys and critical security parameters used by the modules. The following definitions apply to the tables below.

Table 11: Cryptographic Keys and Critical Security Parameters Descriptions

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

Table 12: Cryptographic Keys and Critical Security Parameters used in FIPS-CC mode

Key or CSP	Generation	Storage	Usage	Zeroization
NDRNG output string	Automatic	Flash RAM Plain-text	Input string for the entropy pool (5120 bits)	By erasing the flash memory and power cycling the module
DRBG seed	Automatic	Flash RAM Plain-text	256-bit seed used by the DRBG (output from NDRNG)	By erasing the flash memory and power cycling the module
DRBG output	Automatic	Flash RAM Plain-text	Random numbers used in cryptographic algorithms (256-bits)	By erasing the flash memory and power cycling the module
DRBG v and key values	Automatic	Flash RAM Plain-text	Internal state values for the DRBG 128 and 256	By erasing the flash memory and power cycling the module
Diffie-Hellman Keys	Automatic	SDRAM Plain-text	Key agreement and key establishment	By erasing the flash memory and power cycling the module
Firmware Update Key	Preconfigured	Flash RAM Plain-text	Verification of firmware integrity when updating to new firmware versions using RSA public key (firmware load test, 2048-bit signature)	By erasing the flash memory and power cycling the module
Firmware Integrity Key	Preconfigured	Flash RAM Plain-text	Verification of firmware integrity in the firmware integrity test using RSA public key (firmware integrity test, 2048-bit signature)	By erasing the flash memory and power cycling the module
HTTPS/TLS Server/Host Key	Preconfigured	Flash RAM Plain-text	RSA private key used in the HTTPS/TLS protocols (key establishment, 2048-bit signature)	By erasing the flash memory and power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
HTTPS/TLS Session Authentication Key	Automatic	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	Automatic	SDRAM Plain-text	AES (128-, 256- bit) key used for HTTPS/TLS session encryption	By erasing the flash memory and power cycling the module
SSH Server/Host Key	Preconfigured	Boot device Plain-text	RSA private key used in the SSH protocol (key establishment, 2048-bit signature)	By erasing the flash memory and power cycling the module
SSH Session Authentication Key	Automatic	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	Automatic	SDRAM Plain-text	AES (128-, 256- bit) key used for SSH session encryption	By erasing the flash memory and power cycling the module
Crypto Officer Password	Manual	Flash RAM SHA-256 hash	Used to authenticate operator access to the module	By erasing the flash memory and power cycling the module
Configuration Integrity Key	Preconfigured	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	Preconfigured	Flash RAM Plain-text	AES 256-bit key used to encrypt CSPs on the Boot device and in the backup configuration file (except for crypto officer passwords in the backup configuration file)	By erasing the flash memory and power cycling the module
Configuration Backup Key	Preconfigured	Flash RAM Plain-text	HMAC SHA-256 key used to encrypt crypto officer passwords in the backup configuration file	By erasing the flash memory and power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
Network User Password	Manual	Flash RAM SHA-256 hash	Used during user authentication	By erasing the flash memory and power cycling the module

The Generation column lists all of the keys/CSPs and their entry/generation methods. Manual entered keys are entered by the operator electronically (as defined by FIPS) using the console or a management computer. Pre-configured keys are set as part of the firmware (hardcoded) and are not operator modifiable. Automatic keys are generated as part of the associated protocol.

Alternating Bypass Feature

The primary cryptographic function of the module is encrypting/decrypting web application traffic sent using HTTPS. The module can also send/receive plain-text web traffic using HTTP. The module implements an alternating bypass feature based on the module's configuration. If the traffic from the client is sent/received using HTTPS , the module is operating in a non-bypass state. If traffic from the client is passed directly to the backend webserver using HTTP, the module is operating in bypass state.

Two independent actions must be taken by a CO to create the bypass HTTPs policy: the CO must select HTTPS and then specifically save that policy.

Incoming traffic is processed according to the module configuration. If HTTPS option is selected, the module handles SSL negotiations and encryption/decryption, instead of the web servers. Connections between the client and the module are encrypted using TLS (non-bypass state). If HTTP option is selected the module accepts connections to the web servers in plain-text (bypass state).

Outgoing traffic is processed according to the HTTP service configured on the module. If HTTPS is selected, web traffic will be encrypted using TLS (non-bypass state). If HTTP is configured, web traffic is sent in plain-text (bypass state).

Use of HTTPS for incoming/outgoing traffic is enabled by selecting " HTTPS" as the HTTPS Service via Server Policy configuration.

Key Archiving

The module supports key archiving to a directly attached management computer as part of the 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-256 using the Configuration Backup Key.

Mitigation of Other Attacks

The module does not mitigate against any other attacks.

Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The modules comply with EMI/EMC requirements for Class A or B devices as specified by Part 15, Subpart B, of the FCC rules. The following table lists the specific lab and report information for the modules.

FCC Report Information

Module	Lab Information	FCC Report Number
FWB-3000E	Xindian lab. Compliance Certification Services Inc. No.163-1, Jhongsheng Rd., Xindian Dist., New Taipei City, 23151 Taiwan. +886-2-22170894	T160304D09-F
FWB-4000E	Xindian lab. Compliance Certification Services Inc. No.163-1, Jhongsheng Rd., Xindian Dist., New Taipei City, 23151 Taiwan. +886-2-22170894	T160304D09-F

FIPS 140-2 Compliant Operation

The Fortinet hardware is shipped in a non-FIPS 140-2 compliant configuration. The following steps must be performed to put the module into a FIPS compliant configuration:

1. Download the model specific FIPS validated firmware image from the Fortinet Support site athttps://support.fortinet.com/
2. Verify the integrity of the firmware image
3. Install the FIPS validated firmware image
4. Install the entropy token
5. Enable the FIPS-CC mode of operation

These steps are described in detail in the "FIPS 140-2 and Common Criteria Compliant Operation for FortiWeb 5.6" document that can be found on the Fortinet Technical Documentation website.

In addition, FIPS 140-2 compliant operation requires that you follow secure procedures for installation and operation of the FortiWeb unit. You must ensure that:

- The FortiWeb unit is configured in the FIPS-CC mode of operation.
- The FortiWeb unit is installed in a secure physical location.
- The Fortinet entropy token is enabled.
- The Fortinet entropy token remains in the USB port during opration.
- Physical access to the FortiWeb 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.
- Only approved and allowed algorithms are used (see “Algorithms” on page 12).
- The module is configured in reverse proxy mode.

Once the FIPS validated firmware has been installed and the module properly configured in the FIPS-CC mode of operation, the module is running in a FIPS compliant configuration. It is the responsibility of the CO to ensure the module only uses approved algorithms and services to maintain the module in a FIPS-CC Approved mode of operation. Using any of the non-approved algorithms and services switches the module to a non-FIPS mode of operation. Prior to switching between modes the CO should ensure all keys and CSPs are zeroized to prevent sharing of keys and CSPs between the FIPS Approved and non-FIPS mode of operation.

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: enabled
```

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

Startup and Initialization Self-tests

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

- Firmware integrity test using RSA 2048-bit 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
- RBG Instantiate test
- RBG Generate test
- RBG Reseed 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 output for successful self-tests is shown below:

```
FIPS-CC mode: Starting self-tests.
Running Configuration Integrity test... passed
Running AES test... passed
Running SHA1 HMAC test... passed
Running SHA256 HMAC test... passed
Running 3DES test... passed
Running RSA test... passed
Running Firmware integrity test... passed
Running RBG instantiate test... passed
Running RBG reseed test... passed
Running RBG generate test... passed
Self-tests passed
```

Conditional Self-tests

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

Critical Function Self-tests

The module also performs the following critical function self-tests appicable to the DRBG, as per NIST SP 800-90A Section 11:

- Instantiate test
- Generate test
- Reseed test
- Uninstantiate test

Error State

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.

FORTINET®

High Performance Network Security