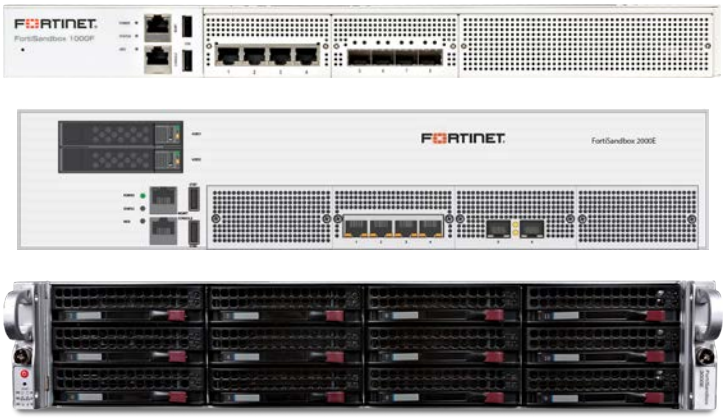
FIPS 140-2 Non-Proprietary Security Policy

FortiSandbox-1000F/2000E/3000E



FortiSandbox-1000F/2000E/3000E FIPS 140-2 Security Policy		
Document Version:	2.3	
Publication Date:	Monday, December 13, 2021	
Description:	Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.	
Firmware Version:	FortiSandbox 3.1, build 5166	
Hardware Version:	FortiSandbox-2000E (C1AG28)	FortiSandbox-1000F (C1AH16)
	FortiSandbox-3000E (C1AF74)	

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://www.fortinet.com/support/contact.html

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

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

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

FEEDBACK

Email: techdoc@fortinet.com

FORTINET

Monday, December 13, 2021

FortiSandbox-1000F/2000E/3000E FIPS 140-2 Non-Proprietary Security Policy

34-310-0637309-20201102

TABLE OF CONTENTS

Overview

This document is a FIPS 140-2 Security Policy for Fortinet's FortiSandbox-1000F, 2000E and 3000E. This policy describes how the FortiSandbox-1000F, 2000E and 3000E (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 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.

FortiSandbox utilizes advanced detection, dynamic antivirus scanning, and threat scanning technology to detect viruses and Advanced Persistent Threats. FortiSandbox leverages the FortiGuard web filtering database to inspect and flag malicious URL requests, and works with devices such as FortiGate, FortiWeb, FortiClient and FortiMail to identify malicious and suspicious files and network traffic. It executes suspicious files in a VM host to determine risk based on the behavior observed.

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 https://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at https://www.fortinet.com/support.
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at https://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at https://wwww.fortiguard.com.

Security Level Summary

The modules meet the overall requirements for a FIPS 140-2 Level 2 validation.

Table 1: Summary of FIPS security requirements and compliance levels

Security Requirement	Compliance Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Module Descriptions

The FortiSandbox-1000F, 2000E and 3000E 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 extent of the cryptographic boundary for all modules is the outer metal chassis.

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 FortiSandbox-1000F has 8 network interfaces with status LEDs for each network interface (4x GbE RJ45, 4x GbE SFP).
- The FortiSandbox-2000E has 6 network interfaces with status LEDs for each network interface (4x 10/100/1000 RJ45, 2x 1GbE SFP+)
- The FortiSandbox-3000E has 6 network interfaces status LEDs for each network interface (4x 10/100/1000 RJ45, 2x 10GbE SFP+).

The FortiSandbox-1000F and 2000E modules each have one x86 compatible CPU.

The FortiSandbox-3000E has two x86 compatible CPUs.

The FortiSandbox-1000F module is a 1u rackmount device.

FortiSandbox-2000E and 3000E are 2u rackmount devices.

The modules each have 2 removable power supplies. These power supplies are excluded from the requirements of FIPS 140-2, as they perform no security relevant function.

The FortiSandbox-3000E has a rear panel VGA and IPMI port that are not supported or used by the FortiSandbox firmware.

The validated firmware version is FortiSandbox 3.1, build 5166. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Figures 1 to 3 are representative of the modules tested.

Cryptographic Module Ports and Interfaces

The modules have status LEDs as described in the following table:

Table 2: FortiSandbox-1000F Status LEDs

LED		State	Description
Power		Green	The module is powered on
		Off	The module is powered off
Status		Red	Major alarm or system failure
		Off	Normal operation
Ethernet Ports	Link/ACT	Flashing Amber	Port is sending/receiving data
		Off	No link established
	Speed	Green	Connected at 100 Mbps
		Amber	Connected at 1000 Mbps
		Off	Connected at 10 Mbps or not in use
SFP Ports	Speed	Amber	Connected at 1000 Mbps
		Off	Not in use
	Link/ACT	Flashing Amber	Port is sending/receiving data
		Off	No link established

Table 3: FortiSandbox-2000E Status LEDs

LED		State	Description
Power		Green	The module is powered on
		Off	The module is powered off
Ethernet Ports	Link/ACT	Flashing Amber	Port is sending/receiving data
		Off	No link established
	Speed	Green	Connected at 100 Mbps
		Amber	Connected at 1000 Mbps
		Off	Connected at 10 Mbps or not in use

LED		State	Description
SFP/SFP+ Ports	Link/ACT	Amber	Connected
		Flashing Amber	Port is sending/receiving data
		Off	No link established

Table 4: FortiSandbox-3000E Status LEDs

LED		State	Description
Power		Green	Power supply normal
		Off	Power supply disconnected
Information		Red	Overheat condition has occured
		Flashing Red (1Hz)	Fan failure
		Flashing Red (0.25 Hz)	Power failure
		Off	System normal
Power Fail		Red	A power supply has failed
		Off	Power supply normal
Ethernet Ports	Link/ACT	Flashing Amber	Port is sending/receiving data
		Off	No link established
	Speed	Green	Connected at 100 Mbps
		Amber	Connected at 1000 Mbps
		Off	Connected at 10 Mbps or not connected
	Front Panel LED	Green	Connected
		Flashing Green	Port is sending/receiving data
		Off	No link established
SFP/SFP+ Ports	Speed	Green	Connected at 10 Gbps
		Off	No link established
	Link/ACT	Flashing Green	Port is sending/receiving data

FortiSandbox-1000F

Figure 1 - FortiSandbox-1000F Front and Rear Panels

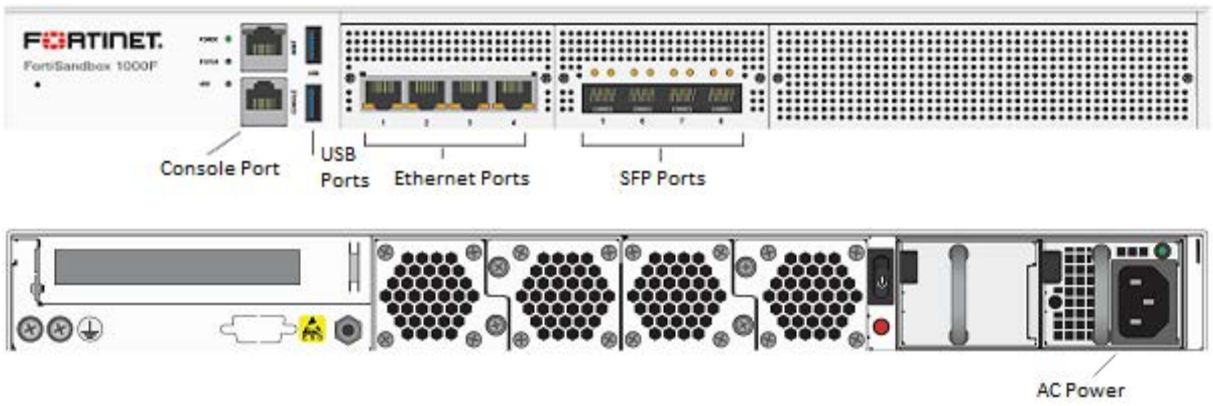


Table 5: FortiSandbox-1000F Connectors and Ports

Connector	Type	Qty	Speed	Supported Logical Interfaces	Description
Ethernet Ports 1-4	RJ-45	4	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 5-8	SFP	4	1 Gbps	Data input, data output, control input, and status output	Multinode fiber optic connections to gigabit optical networks
USB Ports	USB-A	2	N/A	Entropy input	Entropy token
Console Port	RJ-45	1	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI)
AC Power	N/A	1	N/A	Power, Control Input	120/240VAC power connection

FortiSandbox-2000E

Figure 2 - FortiSandbox-2000E Front and Rear Panels

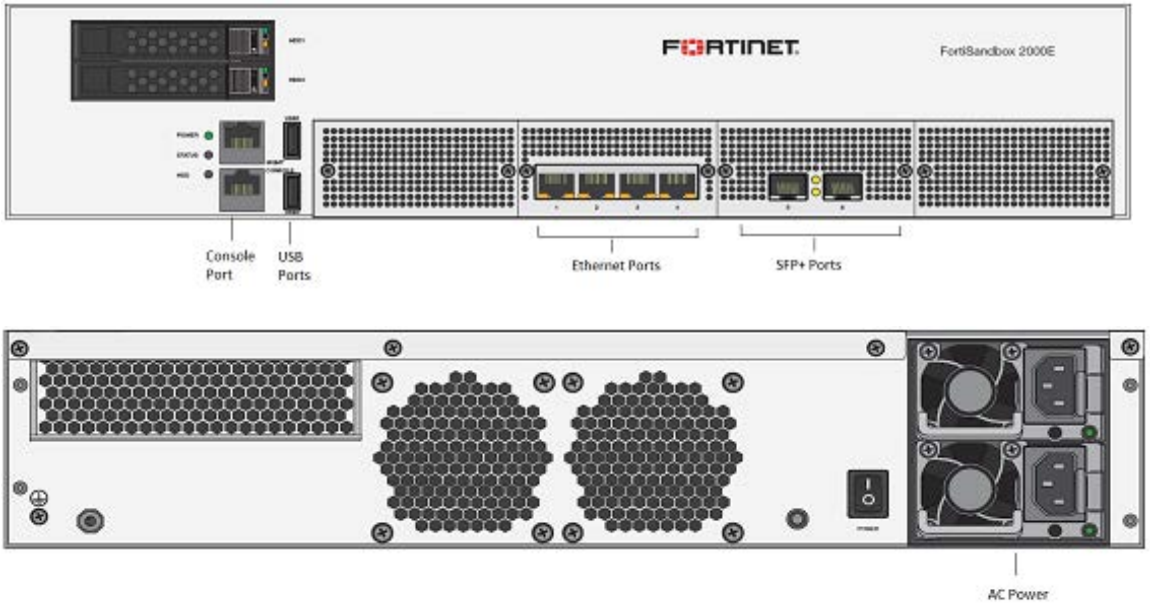


Table 6: FortiSandbox-2000E Connectors and Ports

Connector	Type	Qty	Speed	Supported Logical Interfaces	Description
Ports 1-4	RJ-45	4	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks
Ports 5-6	SFP+	2	10 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks
USB Ports	USB-A	2	N/A	Entropy input	Entropy token
Console Port	RJ-45	1	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI)
AC Power	N/A	2	N/A	Power	120/240VAC power connection

FortiSandbox-3000E

Figure 3 - FortiSandbox-3000E Front and Rear Panels

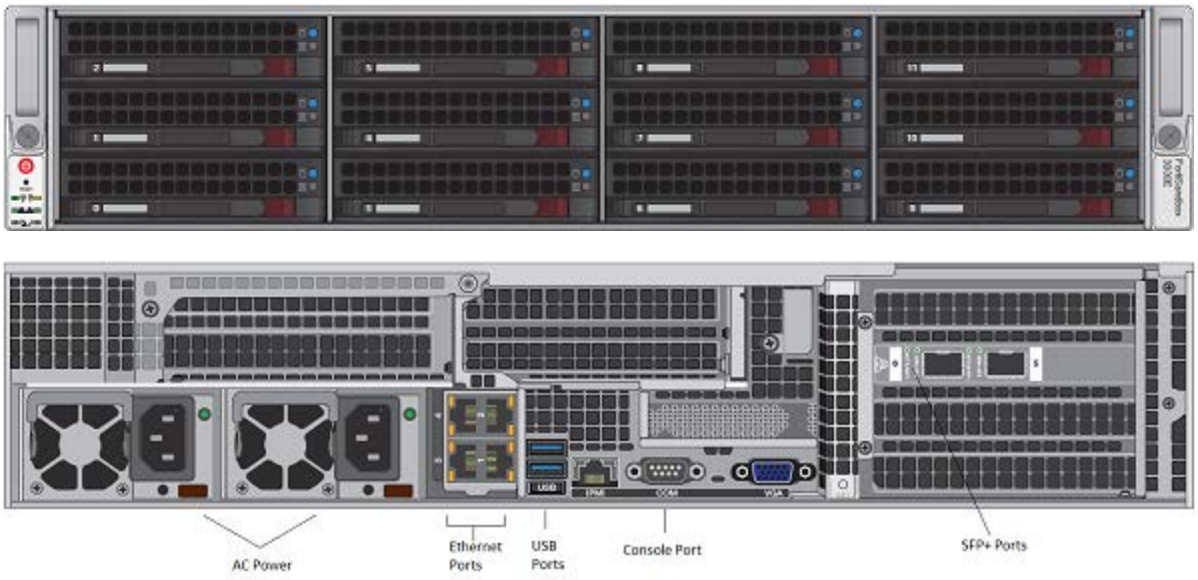


Table 7: FortiSandbox-3000E Connectors and Ports

Connector	Type	Qty	Speed	Supported Logical Interfaces	Description
Ethernet Ports 1-4	RJ-45	4	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks
Ports 5-6	SFP+	2	10 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks
USB Ports	USB-A	2	N/A	Entropy input	Entropy token
Console Port	DB-9	1	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI)
AC Power	N/A	2	N/A	Power	120/240VAC power connection

Web-Based Manager

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

A web-browser that supports Transport Layer Security (TLS) 1.1 or 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.

Command Line Interface

The FortiSandbox Command Line Interface (CLI) is a full-featured, text based management tool for the module. The CLI provides access to services and configuration options in the module. The CLI uses a console connection or a network (Ethernet) connection between the FortiSandbox 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). Telnet access to the CLI is not allowed in FIPS 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 8: Services available to Crypto Officers

Service	Access	Key/CSP
connect to module locally using the console port	WE	N/A
connect to module remotely using TLS*	WE	Diffie-Hellman Keys, EC Diffie Hellman Keys,TLS Premaster Secret, TLS Master Secret, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, and HTTPS/TLS Session Encryption Key, DRBG v and key values, DRBG Output, DRBG Seed, NDRNG Output String
connect to module remotely using SSH*	WE	Diffie-Hellman Keys, SSH Server/Host Key, SSH Session Authentication Key, SSH Session Encryption Key, DRBG v and key values, DRBG Output, DRBG Seed, NDRNG Output String
authenticate to module	WE	Crypto Officer Password
show system status	R	N/A
show FIPS mode enabled/disabled (console/CLI only)	R	N/A
enable FIPS mode of operation (console only)	WE	Configuration Integrity Key
key zeroization	W	All Keys

execute factory reset (disable FIPS mode, console/CLI only)	W	N/A
execute FIPS on-demand self-tests (console only)	E	Configuration Integrity Key, Firmware Integrity Key
add/delete crypto officers and network users	WE	Crypto Officer Password, Network User Password
set/reset crypto officers and network user passwords	WE	Crypto Officer Password, Network User Password
backup/restore configuration file	RWE	Configuration Encryption Key
read/set/delete/modify module configuration*	N/A	N/A
execute firmware update	WE	Firmware Update Key
read log data	N/A	N/A
delete log data (console/CLI only)	N/A	N/A
execute system diagnostics (console/CLI only)	N/A	N/A
log offloading to remote FortiAnalyzer device*	E	OFTP Client Key, Diffie-Hellman Keys, EC Diffie-Hellman Keys, TLS Premaster Secret, TLS Master Secret, HTTPS/TLS Session Integrity Key, HTTPS/TLS Session Encryption Key, DRBG v and key values, DRBG Output, DRBG Seed, NDRNG Output String

Table 9: Services available to Network Users in FIPS-CC mode

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

Non-FIPS Approved Services

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

- Configuration backups using password protection
- RADIUS authentication
- Services marked with an asterisk (*) in Tables 8 and 9 are considered non-approved when using the following algorithms:
  - Non-compliant-strength Diffie-Hellman

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

Authentication

The module implements identity based authentication. Operators must authenticate with a user-id and password combination to access the modules remotely or locally via the console. Remote operator authentication is done over HTTPS (TLS) or SSH. The password entry feedback mechanism does not provide information that could be used to guess or determine the authentication data.

By default, Network User access to the modules is based on firewall policy and authentication by IP address or fully qualified domain names. Network User authentication is done over HTTPS and does not allow access to the modules for administrative purposes.

Note that operator authentication over HTTPS/SSH and Network User authentication over HTTPS are subject to a limit of 3 failed authentication attempts in 1 minute; thus, the maximum number of attempts in one minute is 3. Therefore the probability of a success with multiple consecutive attempts in a one-minute period is 3 in 94^8 which is less than 1/100,000.

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 which is a maximum of 115,200 bps which is 6,912,000 bits per minute. An 8 byte password would have 64 bits, so there would be no more than 108,000 passwords attempts per minute. Therefore the probability of success would be 1/(94^8/108,000) which is less than 1/100,000.

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.

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 FIPS 140-2 Level 2 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 responsible for securing and controlling any unused seals. 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 seals are removed or installed to ensure the security of the module is maintained during such changes and ensuring the module is returned to a FIPS approved state.

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.

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 FortiSandbox-1000F uses five seals to secure the external enclosure (see Figure 4,5,6).
- The FortiSandbox-2000E uses five seals to secure the external enclosure (see Figure 7,8,9).
- The FortiSandbox-3000E uses three seals to secure the external enclosure (see Figure 10,11,12).

Figure 4 - FortiSandbox-1000F external enclosure seal, bottom, front

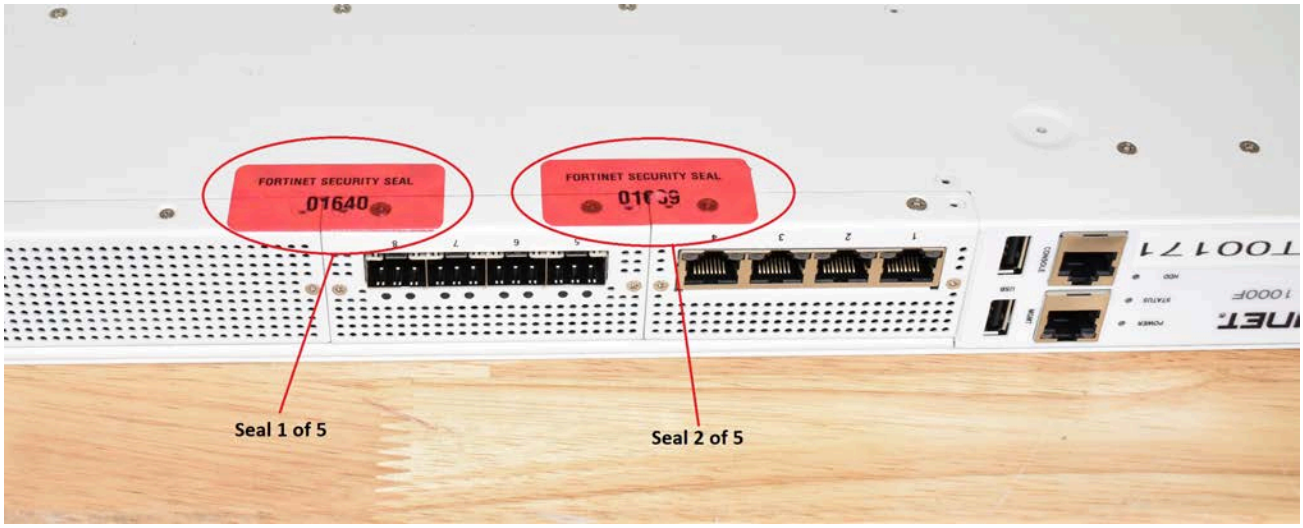


Figure 5 - FortiSandbox-1000F external enclosure seal, top, rear side

Figure 6 - FortiSandbox-1000F external enclosure seal, top, rear back

Figure 7 - FortiSandbox-2000E external enclosure seal, bottom, front

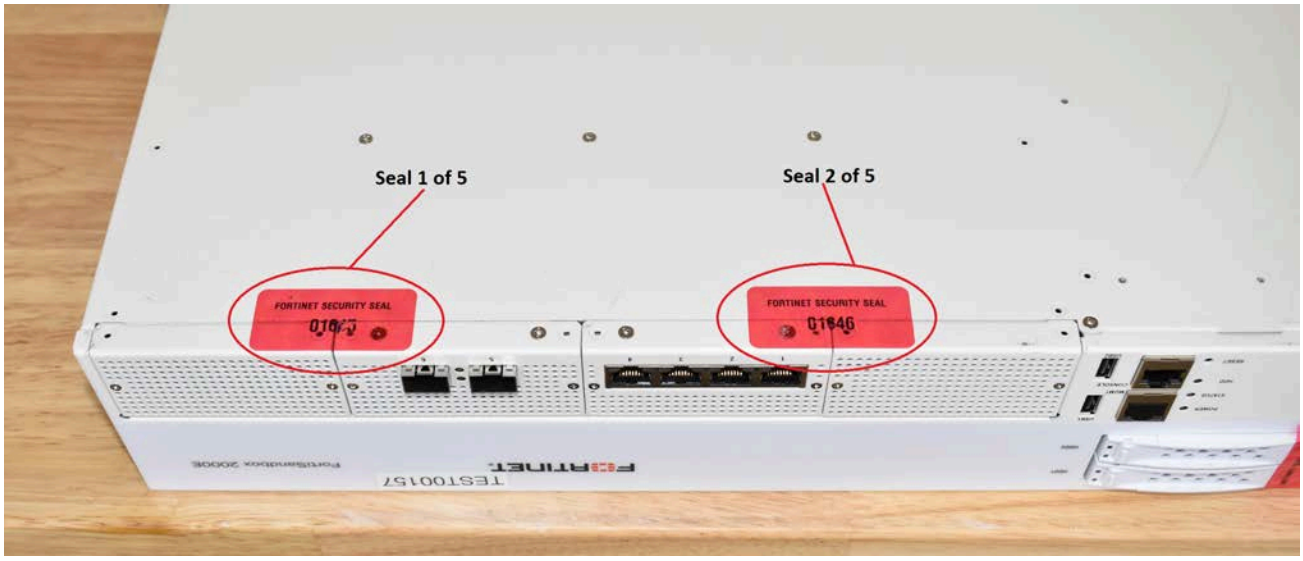


Figure 8 - FortiSandbox-2000E external enclosure seal, top, rear back

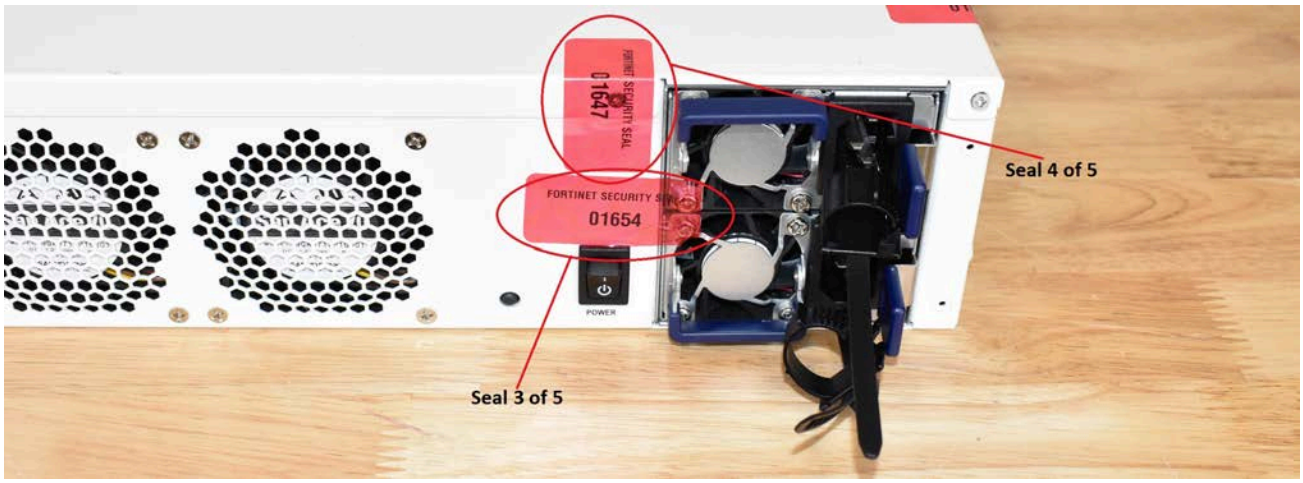


Figure 9 - FortiSandbox-2000E external enclosure seal, front panel

Figure 10 - FortiSandbox-3000E external enclosure seal, top, left

Figure 11 - FortiSandbox-3000E external enclosure seal, top, front

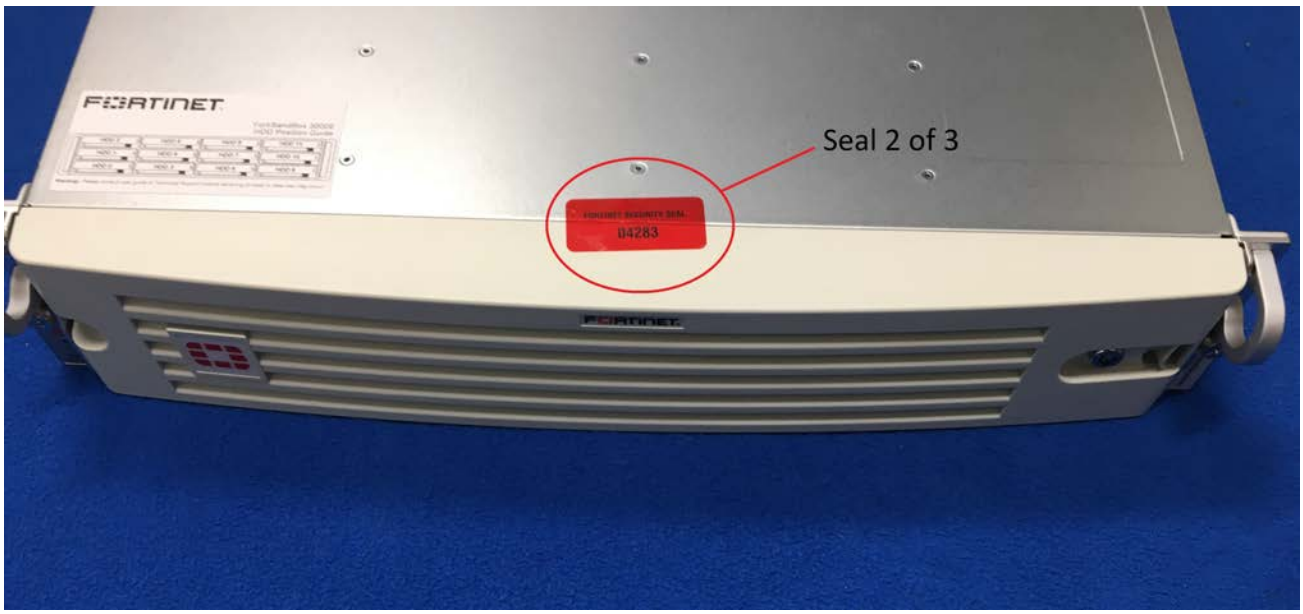
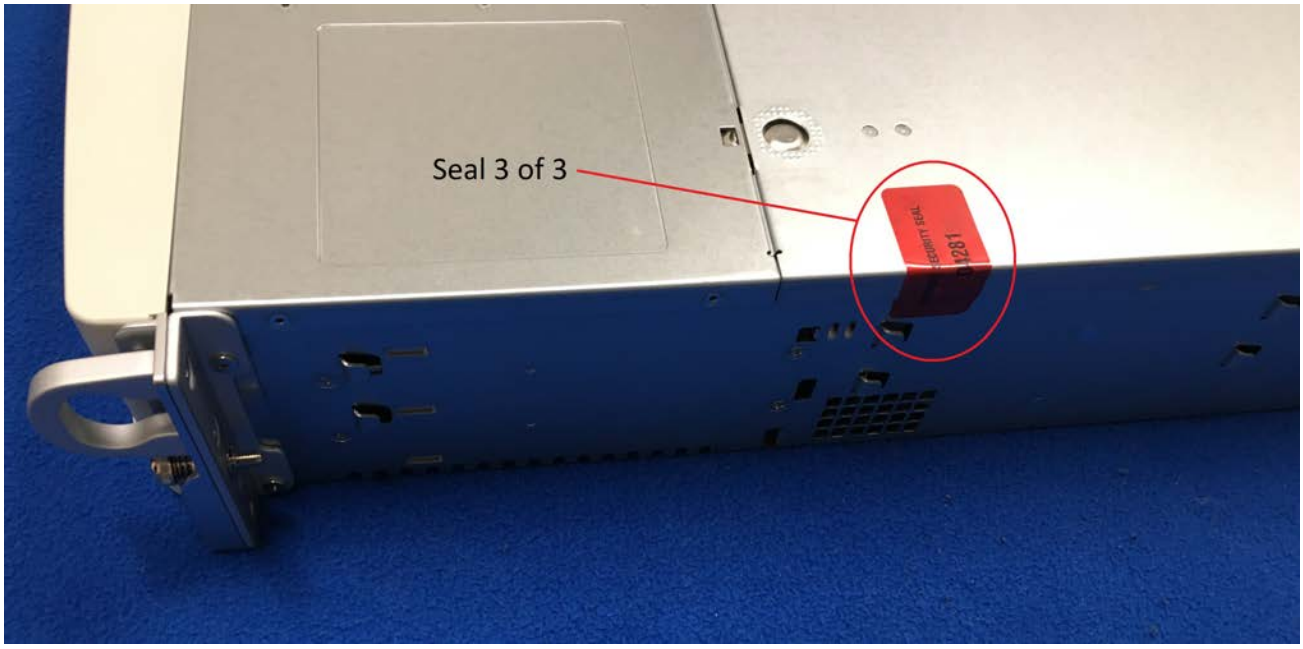


Figure 12 - FortiSandbox-3000E external enclosure seal, top, right



Operational Environment

The modules consist of the combination of the FortiSandbox operating system and the FortiSandbox appliances. The FortiSandbox operating system can only be installed, and run, on a FortiSandbox appliance. The FortiSandbox

operating system 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.

Entropy

The modules use an entropy token (Araneus Alea II) 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 HDD. To erase the boot device, execute the following command from the CLI:

```
factory-reset
```

Executing the following command will wipe all HDD's:

```
erase-all-disks
```

Algorithms

Table 10: FIPS approved algorithms

Algorithm	NIST Certificate Number
CTR DRBG (NIST SP 800-90A) with AES 256-bits	C1986

Algorithm	NIST Certificate Number
AES in CBC mode (128, 256 bits)	C1909
AES in GCM mode (128 , 256 bits)	C1988, C1989
SHA-1	C1988, C1989
SHA-256	C1988, C1989
SHA-384	C1988, C1989
SHA-512	C1988, C1989
HMAC SHA-1	C1988, C1989
HMAC SHA-256	C1988, C1989
HMAC SHA-384	C1988, C1989
HMAC SHA-512	C1988, C1989
RSA PKCS1.5 Signature Generation: 2048 and 3072 bit (186-4) Signature Verification: 1024, 2048 and 3072 bit (186-4) For legacy use, the module supports 1024-bit RSA keys and SHA-1 for signature verification	C1988
CVL (SSH) - AES 128 bit, AES 256 bit -CBC (using SHA-1 and SHA-256))	C1988
CVL (TLS 1.0/1.1 and 1.2 (SHA-256 and SHA-384))	C1988
CVL (KAS-FFC Component) - FB: SHA2-256 | FC: SHA2-256	C1988, C1989
CVL (KAS-ECC Component) - EC: SHA2-256, Curve: P-256 | ED: SHA2-384, Curve: P-384 | EE: SHA2-512, Curve: P-521	C1988

KTS (AES Cert. #C1909 and HMAC Cert. #C1988; key establishment methodology provides 128 or 256 bits of encryption strength); and

KTS (AES Cert. #C1988; key establishment methodology provides 128 or 256 bits of encryption strength)

*(The former KTS utilizes AES-CBC with HMAC. The latter uses AES-GCM only.)

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 11: FIPS allowed algorithms

Algorithm
Diffie-Hellman (CVL Certs. #C1988, and #C1989, key agreement; key establishment methodology provides 112 bits of encryption strength)
EC Diffie-Hellman (CVL Cert. #C1988, key agreement; key establishment methodology provides 128 bits of encryption strength)
NDRNG (Araneus Alea II entropy token is not part of the validation)

Table 12: Non-FIPS approved algorithms

Algorithm
brainpoolP256r1, brainpoolP384r1, and brainpoolP512r1
4096-bit RSA signature generation is non-compliant.
SNMP (The SNMP KDF has not undergone CAVP testing in accordance with NIST SP 800-135, Rev1, and thus SNMP shall not be used in the Approved mode. Any use of SNMP will cause the module to operate in a non-Approved mode.)

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.

The module is compliant to IG A.5: GCM is used in the context of TLS only.

For TLS, the GCM implementation is used in a manner compliant with SP 800-52, and in accordance with RFC 5246 for TLS key establishment. The AES GCM IV generation is in compliance with RFC 5288 and shall only be used for the TLS protocol version 1.2. The cipher suites implemented in the module that utilize AES-GCM are consistent with those specified in Section 3.3.1.1.2 of [SP800-52, Rev2]. During operational testing, the module was tested against an independent version of TLS and found to behave correctly.

In case the module's power is lost and then restored, the key used for the AES GCM encryption or decryption shall be re-distributed.

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 table.

Table 13: Cryptographic Keys and Critical Security Parameters used in FIPS-CC mode

Key or CSP	Generation	Storage	Usage	Zeroization
NDRNG output string	NDRNG	HDD Plain-text	Input string for the entropy pool	By factory-reset and erase-all-disks commands
DRBG seed	Internally generated	SDRAM Plain-text	256 bit seed used by the DRBG (output from NDRNG)	By factory-reset and erase-all-disks commands
DRBG output	Internally generated	SDRAM Plain-text	Random numbers used in cryptographic algorithms (256 bits)	By factory-reset and erase-all-disks commands
DRBG v and key values	Internally generated	SDRAM Plain-text	Internal state values for the DRBG 128 and 256	By factory-reset and erase-all-disks commands
Diffie-Hellman Keys	Internally generated using DRBG	SDRAM Plain-text	Key agreement and key establishment (Public key size of 2048 to 8192 bits with Private key size of 224 to 400 bits)	By factory-reset and erase-all-disks commands
EC Diffie-Hellman Keys	Internally generated using DRBG	SDRAM Plain-text	Key agreement and key establishment (key pairs on the curves secp256r1, secp384r1 and secp521r1)	By factory-reset and erase-all-disks commands
Firmware Update Key	Preconfigured	Boot device Plain-text	Verification of firmware integrity when updating to new firmware versions using RSA public key (firmware load test, 2048 bit signature)	By factory-reset and erase-all-disks commands

Key or CSP	Generation	Storage	Usage	Zeroization
Firmware Integrity Key	Preconfigured	Boot device Plain-text	Verification of firmware integrity in the firmware integrity test using RSA public key (firmware integrity test, 2048 bit signature)	By factory-reset and erase-all-disks commands
TLS Premaster Secret	Internally generated via DH or ECDH KAS	SDRAM Plain-text	HTTPS/TLS keying material	By factory-reset and erase-all-disks commands
TLS Master Secret	Internally generated from the TLS Premaster Secret	SDRAM Plain-text	384 bit master key used in the HTTPS/TLS protocols	By factory-reset and erase-all-disks commands
HTTPS/TLS Server/Host Key	Preconfigured	Boot device and HDD Plain-text	RSA private key used in the HTTPS/TLS protocols (key establishment, 2048 or 3072 bit)	By factory-reset and erase-all-disks commands
HTTPS/TLS Session Authentication Key	Internally generated using DRBG	SDRAM Plain-text	HMAC SHA-1, -256 or -384 key used for HTTPS/TLS session authentication	By factory-reset and erase-all-disks commands
HTTPS/TLS Session Integrity Key	Internally generated using DRBG	SDRAM HDD Plain-text	HMAC SHA-1, -256 or -384 key used for HTTPS/TLS session integrity	By factory-reset and erase-all-disks commands
HTTPS/TLS Session Encryption Key	Internally generated via DH or ECDH KAS	SDRAM HDD Plain-text	AES (128, 256 bit) key used for HTTPS/TLS session encryption	By factory-reset and erase-all-disks commands
SSH Server/Host Key	Preconfigured	Boot device Plain-text	RSA private key used in the SSH protocol (key establishment, 2048 or 3072 bit)	By factory-reset and erase-all-disks commands

Key or CSP	Generation	Storage	Usage	Zeroization
SSH Session Authentication Key	Internally generated using DRBG	SDRAM HDD Plain-text	HMAC SHA-1 or HMAC SHA-256 key used for SSH session authentication	By factory-reset and erase-all-disks commands
SSH Session Encryption Key	Generated using DH or ECDH KAS	SDRAM HDD Plain-text	AES (128, 256 bit) key used for SSH session encryption	By factory-reset and erase-all-disks commands
Crypto Officer Password	Electronic key entry	Boot device SHA-1 hash	Used to authenticate operator access to the module	By factory-reset and erase-all-disks commands
Configuration Integrity Key	Preconfigured	Boot device Plain-text	HMAC SHA-256 hash used for configuration integrity test	By factory-reset and erase-all-disks commands
Configuration Encryption Key	Preconfigured	Boot device Plain-text	AES 256 bit key used to encrypt configuration backup	By factory-reset and erase-all-disks commands
Network User Password	Electronic key entry	Boot device SHA-1 hash	Used to authenticate network access to the module	By factory-reset and erase-all-disks commands
OFTP Client Key	Externally generated	Boot device HDD Plain-text	RSA private key used in the OFTP/TLS protocol (key establishment, 2048 bit signature)	By factory-reset and erase-all-disks commands

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.

Restrictions on TLS Cipher Suites

The browser used to access the administrative interface over HTTPS must be configured to disallow the use of TLS cipher suites and server signatures that utilize security functions that are not approved or not allowed.

For example, Mozilla Firefox 82.0.2 can be configured by entering "about:config" in the URL window and selecting the security.ssl parameters.

The TLS cipher specifications that are disallowed are:

- Server signature algorithms other than rsa_pkcs1_sha256, ecdsa_secp256r1_sha256, rsa_pkcs1_sha384, ecdsa_secp384r1_sha384, rsa_pkcs1_sha512, ecdsa_secp521r1_sha512

Key Archiving

The module supports key archiving to a 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 AES encrypted using the Configuration Encryption 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 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
FSA-1000F	BTL Inc. No. 18, Ln. 171, Sec. 2, Jiuzong Rd., Neihu Dist. Taipei City 114, Taiwan	BTL-FCCE-1-1804T103A
FSA-2000E	BTL Inc. B1, No.37, Lane 365, Yang Guang St., Nei-Hu Dist. Taipei City 114, Taiwan	BTL-FCCE-1-1706035
FSA-3000E	Bay Area Compliance Laboratories Corp. 1274 Anvilwood Ave. Sunnyvale, CA 94086	R1801177-15

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 and checksum from the Fortinet Support site at https://support.fortinet.com/
2. Use a hashing utility on the downloaded firmware image to compare and verify the output against the result from the checksum listing.
3. Install the FIPS validated firmware image from a TFTP server using the BIOS boot menu. To access the BIOS boot menu, use the console connection and press any key when the "Press any key to display the configuration menu" option is displayed during the boot process. Then select "[G]: Get firmware image from TFTP server" and follow the instructions to complete the installation of the firmware image.
4. Install the entropy token (Araneus Alea II, available at https://www.araneus.fi/products/alea2/en)
5. Enable the FIPS-CC mode of operation as per the "Enabling FIPS-CC Mode" section.

In addition, 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 FortiSandbox unit. You must ensure that:

- The FortiSandbox unit is configured in the FIPS-CC mode of operation.
- The FortiSandbox unit is installed in a secure physical location.
- Physical access to the FortiSandbox unit is restricted to authorized operators.
- The entropy token is enabled.
- The entropy token remains in the USB port during operation.
- 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 2048 bits are not used.
- Client side RSA certificates must use 2048 bit or greater key sizes.
- Only approved and allowed algorithms are used.

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 insert the entropy token in the USB port and execute the following command from the Local Console:

```
fips-conf -e -tenable

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:

```
fips-conf -l
```

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

```
FIPS mode is enabled.
Entropy Token is enabled.
Entropy Token reseed interval: 1440
```

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
- AES, CBC mode, encrypt known answer test
- AES, CBC mode, decrypt known answer test
- AES, GCM mode, encrypt known answer test
- AES, GCM 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)
- HMAC SHA-384 known answer test
- SHA-384 known answer test (tested as part of HMAC SHA-384 known answer test)
- HMAC SHA-512 known answer test
- SHA-512 known answer test (tested as part of HMAC SHA-512 known answer test)
- Configuration integrity test
- ECDHE test (Primitive-Z)
- DHE test (Primitive-Z)
- RSA 2048-bit signature generation known answer test
- RSA 2048-bit 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 **`fips-kats -tall`**(to initiate all self-tests) or **`fips-kats -t<test>`** (to initiate a specific self-test).

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

Conditional Self-tests

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

- Continuous NDRNG test
- Continuous DRBG test
- Firmware load test using RSA signatures

Critical Function Self-tests

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

- Instantiate test
- Generate test
- Reseed 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:

```
FIPS error: self-tests failed
Entered FIPS error mode
Requesting system halt
System halted
```

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