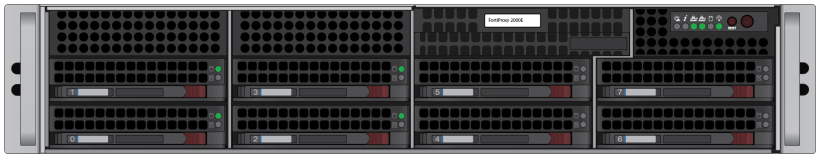
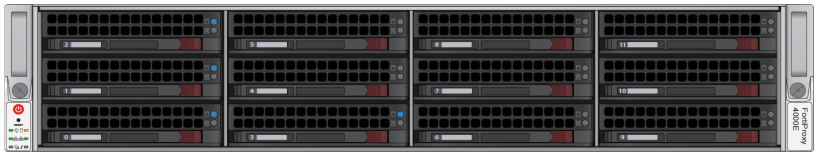
FIPS 140-2 Non-Proprietary Security Policy

FortiProxy-400E/2000E/4000E





FortiProxy-400E/2000E/4000E FIPS 140-2 Security Policy		
Document Version:	2.3	
Publication Date:	Tuesday, January 28, 2020	
Description:	Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.	
Firmware Version:	FortiProxy 1.0, b0066, 190423	
Hardware Version:	FortiProxy-400E (C1AG57)	FortiProxy-2000E (C1AD93)
	FortiProxy-4000E (C1AG58)	

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

Tuesday, January 28, 2020

FortiProxy-400E/2000E/4000E FIPS 140-2 Non-Proprietary Security Policy

45-100-522730-20181106

TABLE OF CONTENTS

Overview

This document is a FIPS 140-2 Security Policy for Fortinet's FortiProxy-400E, 2000E and 4000E. This policy describes how the FortiProxy-400E, 2000E and 4000E (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.

FortiProxy is a secure web/application proxy that protects employees against internet-borne attacks by incorporating multiple detection techniques such as web filtering, DNS filtering, data loss prevention, antivirus, intrusion prevention and advanced threat protection. It helps enterprises enforce internet compliance using granular application control.

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://www.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	3
Mitigation of Other Attacks	2

Module Descriptions

The FortiProxy-400E, 2000E and 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 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 FortiProxy-400E has 4 network interfaces with status LEDs for each network interface (4x 10/100/1000 Base-T).
- The FortiProxy-2000E has 8 network interfaces with status LEDs for each network interface (4x 10/100/1000 Base-T, 2x 1GB SFP, 2x 10GB SFP+).
- The FortiProxy-4000E has 12 network interfaces status LEDs for each network interface (6x 10/100/1000 Base-T, 2x 1GB SFP, 4x 10GB SFP+).

The FortiProxy-400E and 2000E modules each have one x86 compatible CPU.

The FortiProxy-4000E has two x86 compatible CPUs.

The FortiProxy-400E module is a 1u rackmount devices.

FortiProxy-2000E and 4000E 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 FortiProxy-2000E and 4000E have rear panel VGA and IPMI ports that are not supported or used by the FortiProxy firmware.

The validated firmware version is FortiProxy 1.0, b0066, 190423. 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: FortiProxy-400E Status LEDs

LED		State	Description
Power		Green	The module is powered on
		Off	The module is powered off
Status		Green	Minor alarm
		Red	Major alarm or system failure
		Off	Normal operation
HDD		Flashing	Hard disk in use
		Off	No disk activity
Ethernet Ports	Link/ACT	Green	Port is connected
		Flashing	Port is sending/receiving data
		Off	No link established
	Speed	Green	Connected at 1000 Mbps
		Amber	Connected at 100 Mbps
		Off	Connected at 10 Mbps

Table 3: FortiProxy-2000E and 4000E Status LEDs

LED	State	Description
Power	Green	The module is powered on
	Off	The module is powered off
Information	Flashing	Fan failure
	Off	Normal operation
Power Fail	Flashing	A power supply has failed
	Off	Normal operation

LED		State	Description
Ethernet Ports	Link/ACT	Green	Port is connected
		Flashing	Port is sending/receiving data
		Off	No link established
	Speed	Green	Connected at 1000 Mbps
		Amber	Connected at 100 Mbps
		Off	Connected at 10 Mbps
	Bypass	Green	Bypass mode enabled
		Off	Bypass mode disabled
	Disconnect	Green	Disconnect mode enabled
		Off	Disconnect mode disabled
SFP/SFP+ Ports	Speed	Amber	Connected at 10 GBps
		Green	Connected at 10/100 MBps
		Off	No link established
	Link/ACT	Green	Link established
		Flashing	Port is sending/receiving data
		Off	No link activity

FortiProxy-400E

Figure 1 - FortiProxy-400E Front and Rear Panels

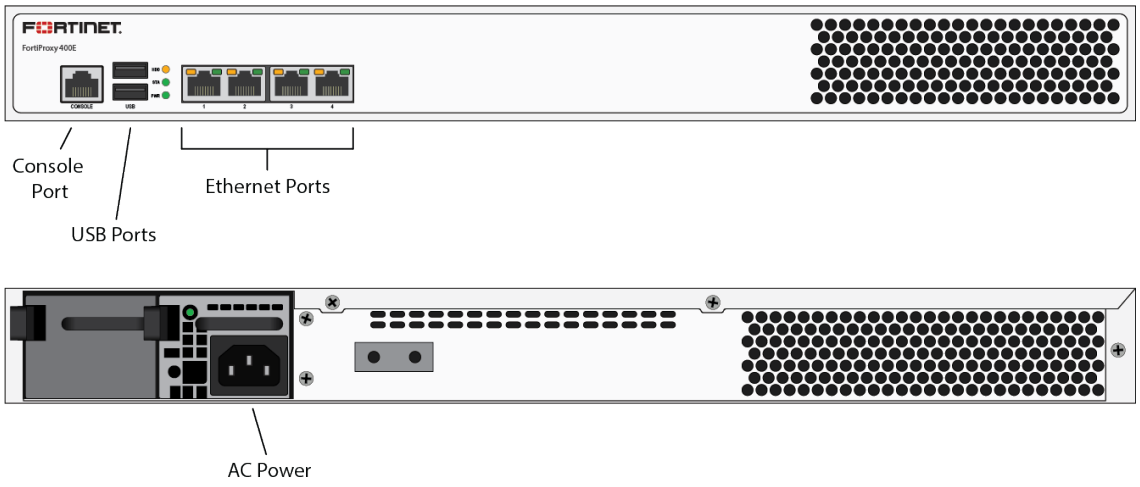


Table 4: FortiProxy-400E Connectors and Ports

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
USB Ports	USB-A	2	N/A	Control input, data output	Configuration loading and archiving
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	120/240VAC power connection

FortiProxy-2000E

Figure 2 - FortiProxy-2000E Front and Rear Panels

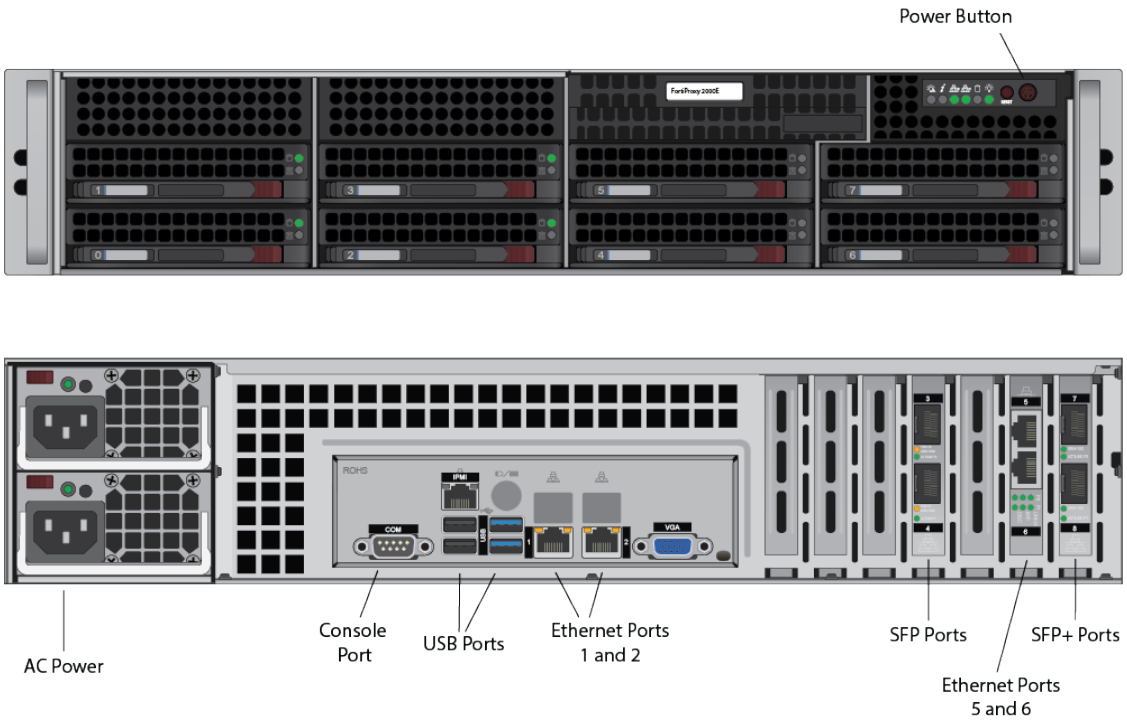


Table 5: FortiProxy-2000E Connectors and Ports

Connector	Type	Qty	Speed	Supported Logical Interfaces	Description
Ports 1-2 and 5-6	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 3-4	SFP	2	1 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks
Ports 7-8	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	Control input, data output	Configuration loading and archiving
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	1	N/A	Power	120/240VAC power connection

FortiProxy-4000E

Figure 3 - FortiProxy-4000E Front and Rear Panels

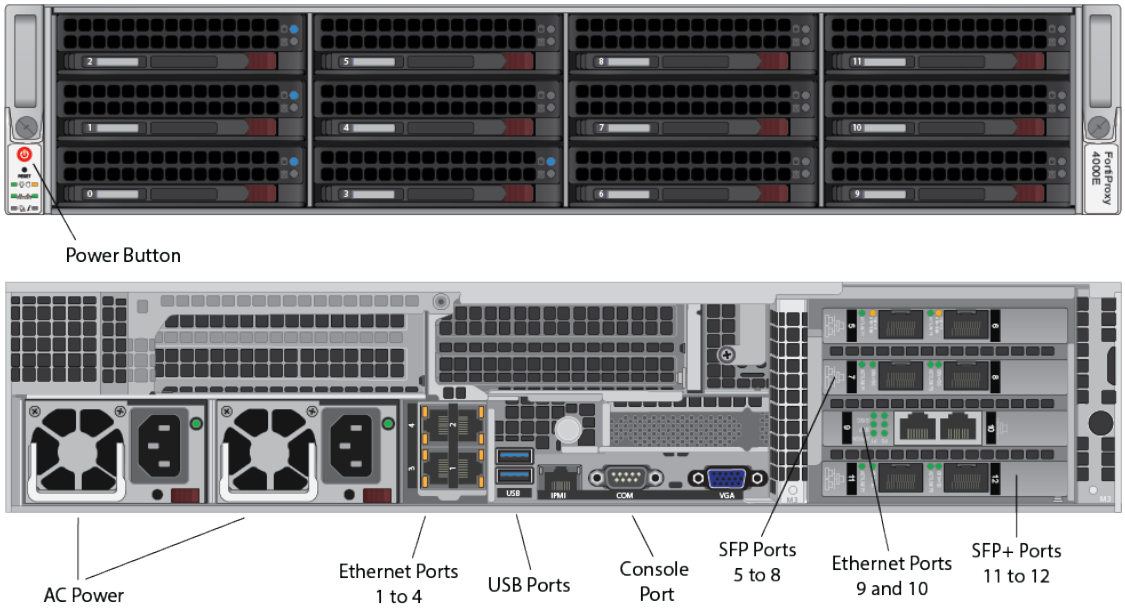


Table 6: FortiProxy-4000E Connectors and Ports

Connector	Type	Qty	Speed	Supported Logical Interfaces	Description
Ports 1-4 and 9-10	RJ-45	6	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks
Ports 5-8	SFP	4	1 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks
Ports 11-12	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	Control input, data output	Configuration loading and archiving
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	1	N/A	Power	120/240VAC power connection

Web-Based Manager

The FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy e 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 7: Services available to Crypto Officers

Service	Access	Key/CSP
authenticate to module*	WE	Crypto Officer Password, Diffie-Hellman Key, EC Diffie Hellman Keys, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS and SSH Session Encryption Keys, DRBG v and key values, DRBG Output, DRBG Seed, NDRNG Output String
show system status	R	N/A
show FIPS-CC mode enabled/disabled (console/CLI only)	R	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
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, Configuration Backup Key
read/set/delete/modify module configuration*	RW	N/A
execute firmware update	WE	Firmware Update Key

Service	Access	Key/CSP
read/set/delete/modify local and remote log configuration	RW	OFTP Client Key
read log data	R	N/A
delete log data (console/CLI only)	W	N/A
execute system diagnostics (console/CLI only)	E	N/A
enable/disable alternating bypass mode	RW	N/A
read/set/delete/modify proxy policy configuration*	W	HTTPS/TLS and SSH Server/Host Key
read/set/modify HA configuration	W	HA Password, HA Encryption Key

Table 8: 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
proxy services controlled by policy*	E	Network User Password, Diffie-Hellman Keys, EC Diffie-Hellman Keys, HTTPS/TLS and SSH Server/Host Key, HTTPS/TLS and SSH Session Authentication Key, HTTPS/TLS and SSH 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
- SNMP
- Services marked with an asterisk (*) in Tables 7 and 8 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 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 Office 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 FortiProxy-400E uses one seal to secure the external enclosure (see Figure 7).
- The FortiProxy-2000E and 4000E use one seal to secure the eternal enclosure (see Figure 8).

Figure 4 - FortiProxy-400E external enclosure seal, top, rear

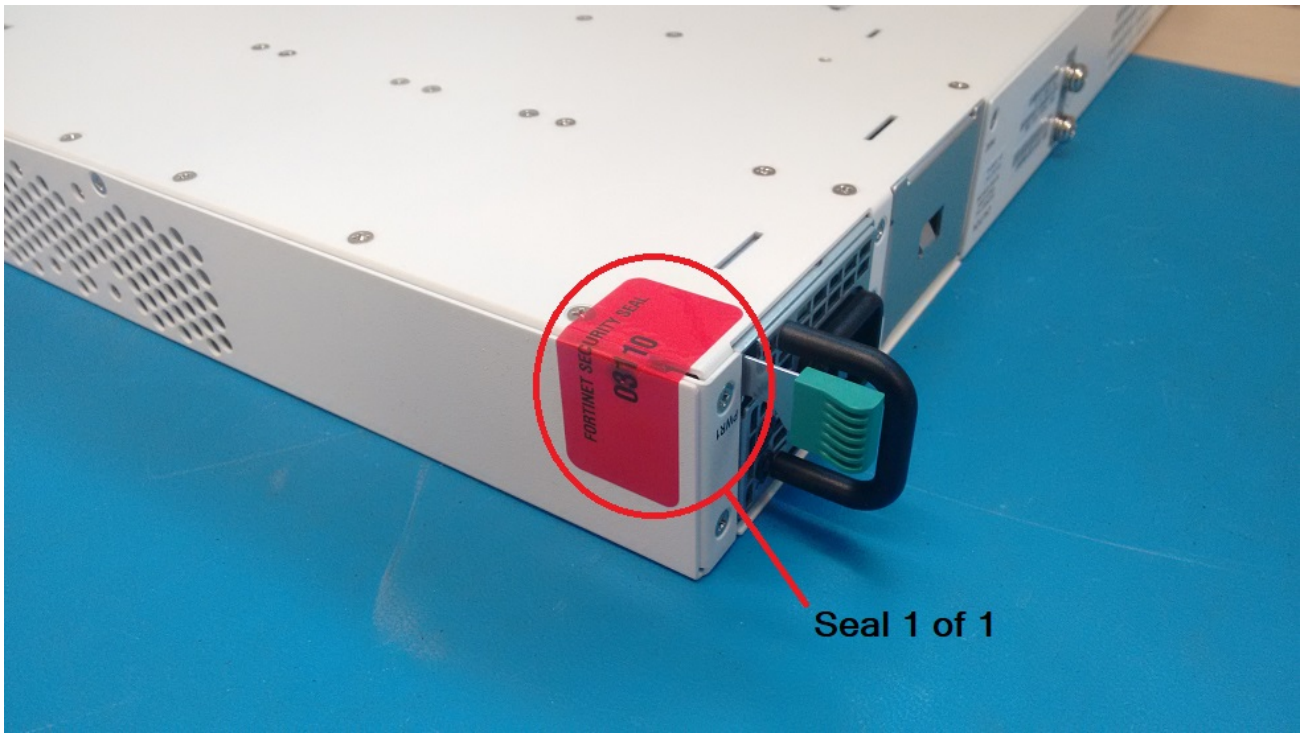
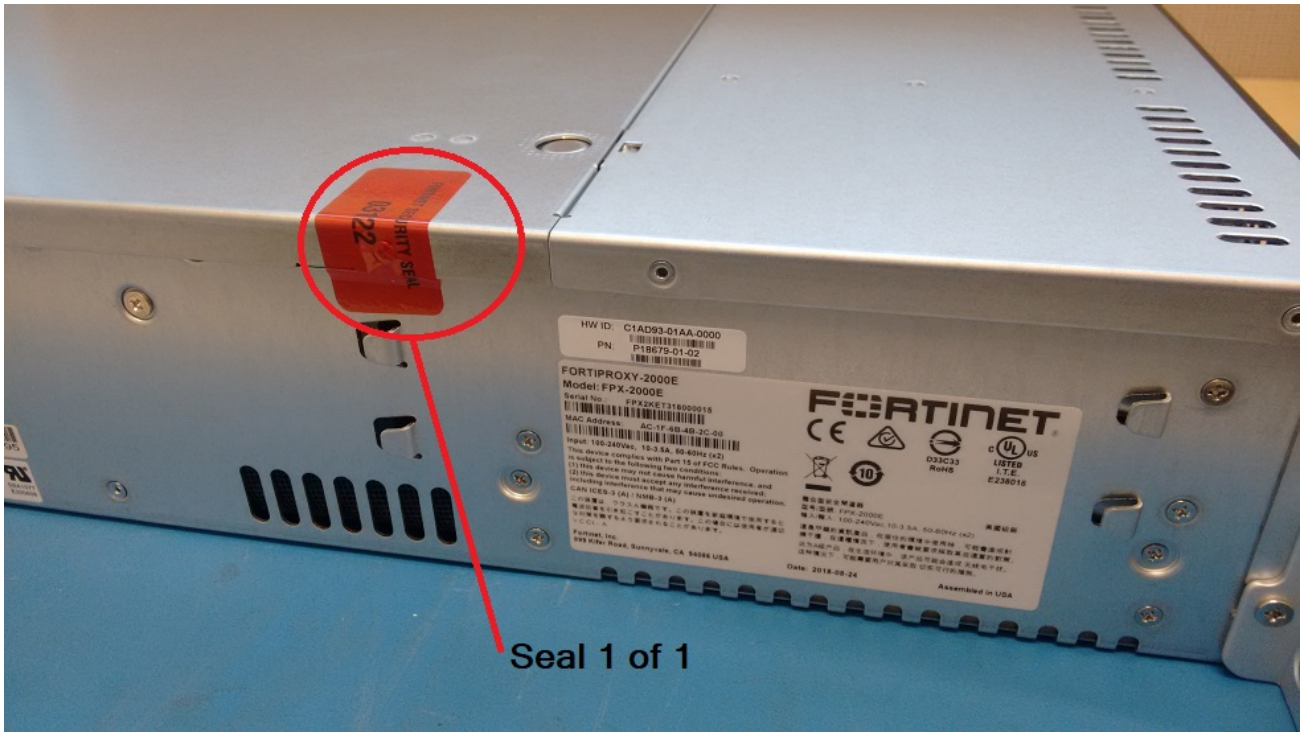


Figure 5 - FortiProxy-2000 and 4000E external enclosure seal, bottom, rear side



Operational Environment

The modules consist of the combination of the FortiProxy operating system and the FortiProxy appliances. The FortiProxy operating system can only be installed, and run, on a FortiProxy appliance. The FortiProxy 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 Fortinet's CP9 Security Processor to seed the DRBG during the modules' boot process and to periodically reseed the DRBG. The CP9 is used by default as the FortiOS entropy source - i.e. no configuration changes are required.

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 CP9 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).

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 FortiProxy 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 FortiProxy module. Executing the following command will output a list of the available internal disks:

```
execute erase-disk ?
```

Algorithms

Table 9: FIPS approved algorithms

Algorithm	NIST Certificate Number
CTR DRBG (NIST SP 800-90A) with AES 256-bits	C658, C799
AES in CBC mode (128-, 256-bits)	C655, C703, C787, C813, C832
AES in GCM mode (128-, 256-bits)	C702, C703, C806, C813, C832
SHA-1	C702, C703, C806, C813, C832
SHA-256	C702, C703, C806, C813, C832
SHA-384	C702, C703, C806, C813, C832
SHA-512	C702, C703, C806, C813, C832
HMAC SHA-1	C702, C703, C806, C813, C832
HMAC SHA-256	C702, C703, C806, C813, C832

Algorithm	NIST Certificate Number
HMAC SHA-384	C702, C703, C806, C813, C832
HMAC SHA-512	C702, C703, C806, C813, C832
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	• C702, C806 • C702, C806, C813 • C702, C806, C813
ECDSA • Key Pair Generation: curves P-256, P-384 and P-521 • Signature Generation: curves P-256, P-384 and P-521 • Signature Verification: curves P-256, P-384 and P-521	C702, C703, C806, C813, C832
CVL (SSH) - AES 128 bit-, AES 256 bit -CBC (using SHA1)	C702, C806
CVL (TLS 1.1 and 1.2)	C702, C806
CVL (ECDSA SigGen Component: Curves P-256, P-384 and P-521)	C813
CVL (KAS-FFC Component) - FB: SHA2-256 | FC: SHA2-256	C702, C703, C806, C832
CVL (KAS-ECC Component) - EC: SHA2-256, Curve: P-256 | ED: SHA2-384, Curve: P-384 | EE: SHA2-512, Curve: P-521	C702, C806

KTS (AES Certs. #C655 and #C787 and HMAC Certs. #C702 and #C806; key establishment methodology provides 128 or 256 bits of encryption strength).

KTS (AES Certs. #C702 and #C806; key establish.ment methodology provides 128 or 256 bits of encryption strength).

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 10: FIPS allowed algorithms

Algorithm
Diffie-Hellman (CVL Certs. #C702, #C703, #806 and #C832, key agreement; key establishment methodology provides between 112 and 196 bits of encryption strength)
EC Diffie-Hellman (CVL Certs. #C702 and #C806, key agreement; key establishment methodology provides 128 bits of encryption strength)

Algorithm
RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
NDRNG (FortiASIC CP9)

Table 11: Non-FIPS approved algorithms

Algorithm
DES (disabled in FIPS-CC mode)
MD5 (disabled in FIPS-CC mode)
HMAC MD5 (disabled in FIPS-CC mode)
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.
4096-bit RSA signature generation is non-compliant.
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.
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 meets Option 1 of IG A.5: it 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 to be compliant with FIPS140-2 IG A.5, Option 1 (“TLS protocol IV generation”); thus, those 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.

While Diffie-Hellman and EC Diffie-Hellman are both compliant with CAVP component validation, please be advised that neither scheme is tested at power-up.

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

Key or CSP	Generation	Storage	Usage	Zeroization
NDRNG output string	NDRNG	Boot device Plain-text	Input string for the entropy pool	By erasing the Boot device and power cycling the module
DRBG seed	Internally generated	Boot device Plain-text	256-bit seed used by the DRBG (output from NDRNG)	By erasing the Boot device and power cycling the module
DRBG output	Internally generated	Boot device Plain-text	Random numbers used in cryptographic algorithms (256-bits)	By erasing the Boot device and power cycling the module
DRBG v and key values	Internally generated	Boot device Plain-text	Internal state values for the DRBG 128 and 256	By erasing the Boot device and power cycling the module
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 erasing the boot device and power cycling the module
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 erasing the boot device and power cycling the module
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 erasing the boot device and power cycling the module
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 erasing the boot device and power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
TLS Premaster Secret	Internally generated via DH or ECDH KAS	SDRAM Plain-text	HTTPS/TLS keying material	By erasing the boot device and power cycling the module
TLS Master Secret	Internally generated from the TLS Premaster Secret	SDRAM Plain-text	384-bit master key used in the HTTPS/TLS protocols	By erasing the boot device and power cycling the module
HTTPS/TLS Server/Host Key	Preconfigured	Boot device Plain-text	RSA private key used in the HTTPS/TLS protocols (key establishment, 2048- or 3072-bit)	By erasing the boot device and power cycling the module
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 erasing the boot device and power cycling the module
HTTPS/TLS Session Encryption Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	AES (128-, 256-bit) key used for HTTPS/TLS session encryption	By erasing the boot device 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- or 3072-bit)	By erasing the boot device and power cycling the module
SSH Session Authentication Key	Internally generated using DRBG	SDRAM Plain-text	HMAC SHA-1 or HMAC SHA-256 key used for SSH session authentication	By erasing the boot device and power cycling the module
SSH Session Encryption Key	Generated using DH or ECDH KAS	SDRAM Plain-text	AES (128-, 256-bit) key used for SSH session encryption	By erasing the boot device and power cycling the module
Crypto Officer Password	Electronic key entry	Boot device SHA-1 hash	Used to authenticate operator access to the module	By erasing the boot device and power cycling the module
Configuration Integrity Key	Preconfigured	Boot device Plain-text	HMAC SHA-256 hash used for configuration bypass test	By erasing the boot device and power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
Configuration Encryption Key	Preconfigured	Boot device 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 boot device and power cycling the module
Configuration Backup Key	Preconfigured	Boot device Plain-text	HMAC SHA-256 key used to encrypt crypto officer passwords in the backup configuration file	By erasing the boot device and power cycling the unit
Network User Password	Electronic key entry	Boot device SHA-1 hash	Used to authenticate network access to the module	By erasing the boot device and power cycling the unit
HA Password	Electronic key entry	Boot device AES encrypted	Used to authenticate FortiGate units in an HA cluster	By erasing the boot device and power cycling the unit
HA Encryption Key	Externally generated	Boot device AES encrypted	Encryption of traffic between units in an HA cluster using AES 128-bit key	By erasing the boot device and power cycling the unit
OFTP Client Key	Externally generated	Boot device Plain-text	RSA private key used in the OFTP/TLS protocol (key establishment, 2048-bit signature)	By erasing the boot device 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.

Alternating Bypass Feature

The primary cryptographic function of the module is as a secure web/application proxy (including caching) for both encrypted and unencrypted network traffic. Two main types of policies can be created: explicit proxy policies and transparent proxy policies. Policies can be created to receive/send the traffic from/to the same network interface or from/to different network interfaces. In both cases the module implements alternating bypass for proxied traffic based on the policy configuration.

If SSL/SSH Inspection is enabled for a policy, the module is operating in non-bypass mode: i.e. the module is operating as a proxy for SSL/SSH traffic and decrypting/encrypting the traffic.

If SSL/SSH Inspection is disabled for a policy, the module is operating in bypass mode: i.e. the module is simply receiving and sending the traffic without performing any SSL/SSH decryption/encryption of the traffic.

At least two independent actions are required to create and enable both bypass and non-bypass policies. The operator must create the policy, configure the desired parameters (SSL/SSH Inspection is enabled by default) and then apply (save) the policy.

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 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 includes a real-time Intrusion Prevention System (IPS) as well as antivirus protection, web content filtering, DNS filtering, application control and data leak prevention. Use of these capabilities is optional.

The FortiProxy IPS uses signatures to detect attacks embedded in proxied traffic. Functionally, signatures are similar to virus definitions, with each signature designed to detect a particular type of attack. The IPS signatures are updated through the FortiGuard IPS service. The IPS engine can also be updated through the FortiGuard IPS service.

FortiProxy antivirus protection removes and optionally quarantines files infected by viruses from web (HTTP), file transfer (FTP), and email (POP3, IMAP, and SMTP) content embedded in proxied traffic. Antivirus protection also controls the blocking of oversized files and supports blocking by file extension. Virus signatures are updated through the FortiGuard antivirus service. The antivirus engine can also be updated through the FortiGuard antivirus service.

FortiProxy web filtering can be configured to provide web (HTTP/HTTPS) content filtering. FortiProxy web filtering uses methods such as banned words, address block/exempt lists, and the FortiGuard managed content service.

FortiProxy DNS filtering can be configured to provide web content (HTTP/HTTPS) content filtering based on DNS domain lookup. FortiProxy DNS filtering uses the FortiGuard DNS database.

FortiProxy application control can detect and take action against network traffic depending on the application generating the traffic. FortiProxy application control uses the FortiGuard application control database.

FortiProxy data leak prevention is used to prevent sensitive data from leaving your network. After sensitive data patterns are defined, data matching the patterns will either be blocked or logged and then allowed.

Whenever a IPS, antivirus, or other filtering event occurs, the modules can record the event in the log and/or send an alert email to an operator.

For complete information refer to the FortiProxy Administration Guide.

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
FPX-400E	Bay Area Compliance Laboratories Corp. 1274 Anvilwood Ave. Sunnyvale, CA 94086	R1803064-15
FPX-2000E	Bay Area Compliance Laboratories Corp. 1274 Anvilwood Ave. Sunnyvale, CA 94086	R1801176-15
FPX-4000E	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 md5sum.txt file 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 md5sum.txt file.
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. 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 FortiProxy unit. You must ensure that:

- The FortiProxy unit is configured in the FIPS-CC mode of operation.
- The FortiProxy unit is installed in a secure physical location.
- Physical access to the FortiProxy 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 2048 bits are not used.
- Client side RSA certificates must use 2048 bit or greater key sizes.
- Only approved and allowed algorithms are used.

The module can be used in either of its two operation modes: NAT/Route or Transparent. NAT/Route mode applies security features between two or more different networks (for example, between a private network and the Internet). Transparent mode applies security features at any point in a network. The current operation mode is displayed on the web-based manager status page and in the output of the `get system status` CLI command.

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 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
```

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 bypass test using HMAC SHA-256
- 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)
- RSA signature generation known answer test
- RSA signature verification known answer test
- ECDSA pairwise consistency test with P-256 curve
- DRBG known answer test

The results of the startup self-tests are displayed on the console during the startup process.

The startup self-tests can also be initiated on demand using the CLI command **`execute fips kat all`**(to initiate all self-tests) or **`execute fips kat <test>`** (to initiate a specific self-test).

When the self-tests are run, each implementation of an algorithm is tested - 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
- RSA pairwise consistency test
- ECDSA pairwise consistency test with P-256 curve
- Configuration bypass 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 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:

```
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.