FireEye FX Series: FX-5400, FX-8400

FireEye, Inc.
FIPS 140-2 Non-Proprietary Security Policy
Document Version: 0.4

Prepared By:
Acumen Security
18504 Office Park Dr
Montgomery Village, MD 20886

www.acumensecurity.net

Table of Contents

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for the FireEye FX Series: FX-5400, FX-8400. Below are the details of the product validated:

Hardware Version: FX-5400, FX-8400
Software Version #: 7.6.0
FIPS 140-2 Security Level: 1

1.1 Purpose

This document was prepared as Federal Information Processing Standard (FIPS) 140-2 validation evidence. The document describes how the FireEye FX Series: FX-5400, FX-8400 meets the security requirements of FIPS 140-2. It also provides instructions to individuals and organizations on how to deploy the product in a secure FIPS-approved mode of operation. Target audience of this document is anyone who wishes to use or integrate this product into a solution that is meant to comply with FIPS 140-2 requirements.

1.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Acumen Security, LLC. under contract to FireEye, Inc. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to FireEye, Inc. and is releasable only under appropriate non-disclosure agreements.

1.3 Notices

This document may be freely reproduced and distributed in its entirety without modification.

2. FireEye FX Series: FX-5400, FX-8400

The FireEye FX Series: FX-5400, FX-8400 (the module) is a multi-chip standalone module validated at FIPS 140-2 Security Level 1. Specifically, the module meets the following security levels for individual sections in the FIPS 140-2 standard:

Table 1 - Security Level for Each FIPS 140-2 Section

#	Section Title	Security Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurances	3
11	Mitigation Of Other Attacks	N/A

2.1 Cryptographic Module Specification

The FireEye FX series is a group of threat prevention platforms that protect content against attacks originating in a wide range of file types. Web mail, online file transfer tools, the cloud, and portable file storage devices can introduce malware that can spread to file shares and content repositories. The FireEye FX platform analyzes network file shares and enterprise content management stores to detect and quarantine malware brought in by employees and others that bypass next-generation firewalls, IPS, AV, and gateways.

2.1.1 Cryptographic Boundary

The cryptographic boundary for the module is defined as encompassing the "top," "front," "left," "right," and "bottom" surfaces of the case and all portions of the "backplane" of the case. The following figures provide a physical depiction of the cryptographic module. The following images depict the FX-5400 and FX-8400

Figure 1: FireEye FX 5400

Figure 2: FireEye FX 8400

2.2 Cryptographic Module Ports and Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following table:

Table 2 - Module Interface Mapping – FX-5400/FX-8400

FIPS Interface	Physical Interface
Data Input	(2x) 10/100/1000 BASE-T Ports PS/2 Keyboard and Mouse Ports (2x) USB Ports Serial Port (2x)10/100/1000 BASE-T Ports (Management)
Data Output	(2x) 10/100/1000 BASE-T Ports DB15 VGA Port (2x) USB Ports Serial Port (2x)10/100/1000 BASE-T Ports (Management)
Control Input	(2x) 10/100/1000 BASE-T Ports PS/2 Keyboard and Mouse Ports (2x) USB Ports Serial Port (2x)10/100/1000 BASE-T Ports (Management)
Status Output	(2x) 10/100/1000 BASE-T Ports DB15 VGA Port (2x) USB Ports Serial Port (2x)10/100/1000 BASE-T Ports (Management)
Power Interface	Power Port

2.3 Roles, Services, and Authentication

The following sections provide details about roles supported by the module, how these roles are authenticated and the services the roles are authorized to access.

2.3.1 Authorized Roles

The module supports several different roles, including multiple Cryptographic Officer roles and a User role.

Configuration of the module can occur over several interfaces and at different levels depending upon the role assigned to the user. There are multiple types of Cryptographic Officers that may configure the module, as follows:

- **Admin:** The system administrator is a "super user" who has all capabilities. The primary function of this role is to configure the system.
- **Monitor:** The system monitor has read-only access to some things the admin role can change or configure.
- **Operator:** The system operator has a subset of the capabilities associated with the admin role. Its primary function is configuring and monitoring the system.
- **Analyst:** The system analyst focuses on data plane analysis and possesses several capabilities, including setting up alerts and reports.
- **Auditor:** The system auditor reviews audit logs and performs forensic analysis to trace how events occurred.
- **SNMP:** The SNMP role provides system monitoring through SNMPv3.

The Users of the module are the remote IT devices and remote management clients accessing the module via cryptographic protocols. These protocols include, SSH, TLS, and SNMPv3.

Unauthenticated users are only able to access the module LEDs and power cycle the module.

2.3.2 Authentication Mechanisms

The module supports identity-based authentication. Module operators must authenticate to the module before being allowed access to services, which require the assumption of an authorized role. The module employs the authentication methods described in the table below to authenticate Crypto-Officers and Users.

Table 3 - Authentication Mechanism Details

Role	Type Of Authentication	Authentication Strength
Admin **Monitor** **Operator** **Analyst** **Auditor**	Password/Username	All passwords must be between 8 and 32 characters. If (8) integers are used for an eight digit password, the probability of randomly guessing the correct sequence is one (1) in 100,000,000 (this calculation is based on the assumption that the typical standard

Role	Type Of Authentication	Authentication Strength
SNMP		American QWERTY computer keyboard has 10 integer digits. The calculation should be 10 ^ 8 = 100,000,000). Therefore, the associated probability of a successful random attempt is approximately 1 in 100,000,000, which is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 1,666,666 guesses per second, which far exceeds the operational capabilities of the module.
User	Password/Username or RSA Asymmetric Authentication	All passwords must be between 8 and 32 characters. If (8) integers are used for an eight digit password, the probability of randomly guessing the correct sequence is one (1) in 100,000,000 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 integer digits. The calculation should be 10 ^ 8 = 100,000,000). Therefore, the associated probability of a successful random attempt is approximately 1 in 100,000,000, which is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 1,666,666 guesses per second, which far exceeds the operational capabilities of the module. When using RSA based authentication, RSA key pair has modulus size of 2048 bit, thus providing 112 bits of strength. Therefore, an attacker would have a 1 in 2^112 chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. For RSA-based authentication, to exceed a 1 in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 3.25X10^32 attempts per minute, which far exceeds the operational capabilities of the modules to support.

2.3.3 Services

The services that are available to unauthenticated entities and the services that require operators to assume an authorized role (Crypto-Officer or User) are listed in the table below.

Please note that the keys and Critical Security Parameters (CSPs) listed below use the following indicators to show the type of access required:

- **R (Read):** The CSP is read
- **W (Write):** The CSP is established, generated, or modified
- **Z (Zeroize):** The CSP is zeroized

Table 4 - Services

Service	Description	Role	Key/CSP and Type of Access
SSH to external IT device	Secure connection between a FX and other FireEye appliances using SSH.	User	• DRBG entropy input (R) • DRBG Seed (R) • DRBG V (R/W/Z) • DRBG Key (R/W/Z) • Diffie-Hellman Shared Secret (R/W/Z) • Diffie Hellman private key (R/W/Z) • Diffie Hellman public key (R/W/Z) • SSH Private Key (R/W/Z) • SSH Public Key (R/W/Z) • SSH Session Key (R/W/Z) • SSH Integrity Key (R/W/Z)
Administrative access over SSH	Secure remote command line appliance administration over an SSH tunnel.	Admin, Monitor, Operator, Analyst, Auditor	• Admin Password (R/W/Z) • Monitor Password (R/W/Z) • Operator Password (R/W/Z) • Analyst Password (R/W/Z) • Auditor Password (R/W/Z) • DRBG entropy input (R) • DRBG Seed (R) • DRBG V (R/W/Z) • DRBG Key (R/W/Z) • Diffie-Hellman Shared Secret (R/W/Z) • Diffie Hellman private key (R/W/Z) • Diffie Hellman public key (R/W/Z) • SSH Private Key (R/W/Z) • SSH Public Key (R/W/Z) • SSH Session Key (R/W/Z) • SSH Integrity Key (R/W/Z)
Administrative access over webGUI	Secure remote GUI appliance administration over a TLS tunnel.	Admin, Monitor, Operator, Analyst, Auditor	• Admin Password (R/W/Z) • Monitor Password (R/W/Z) • Operator Password (R/W/Z) • Analyst Password (R/W/Z) • Auditor Password (R/W/Z)

Service	Description	Role	Key/CSP and Type of Access
			• DRBG entropy input (R) • DRBG Seed (R) • DRBG V (R/W/Z) • DRBG Key (R/W/Z) • Diffie-Hellman Shared Secret (R/W/Z) • Diffie Hellman private key (R/W/Z) • Diffie Hellman public key (R/W/Z) • TLS Private Key (R/W/Z) • TLS Public Key (R/W/Z) • TLS Pre-Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z)
Administrative access over serial console and VGA	Directly connected command line appliance administration.	Admin, Monitor, Operator, Analyst, Auditor	• Admin Password (R/W/Z) • Monitor Password (R/W/Z) • Operator Password (R/W/Z) • Analyst Password (R/W/Z) • Auditor Password (R/W/Z)
SNMPv3	Secure remote SNMPv3-based system monitoring.	SNMP	• SNMP Session Key (R/W/Z) • SNMPv3 password (R/W/Z)
DTI connection	TLS-based connection used to upload data to the FireEye cloud.	User	• DRBG entropy input (R) • DRBG Seed (R) • DRBG V (R/W/Z) • DRBG Key (R/W/Z) • Diffie-Hellman Shared Secret (R/W/Z) • Diffie Hellman private key (R/W/Z) • Diffie Hellman public key (R/W/Z) • TLS Private Key (R/W/Z) • TLS Public Key (R/W/Z) • TLS Pre-Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z)
LDAP over TLS	Secure remote authentication via TLS protected LDAP	User	• Admin Password (R/W/Z) • Monitor Password (R/W/Z) • Operator Password (R/W/Z) • Analyst Password (R/W/Z) • Auditor Password (R/W/Z) • DRBG entropy input (R) • DRBG Seed (R) • DRBG V (R/W/Z)

Service	Description	Role	Key/CSP and Type of Access
			• DRBG Key (R/W/Z) • Diffie-Hellman Shared Secret (R/W/Z) • Diffie Hellman private key (R/W/Z) • Diffie Hellman public key (R/W/Z) • TLS Private Key (R/W/Z) • TLS Public Key (R/W/Z) • TLS Pre-Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z)
Secure log transfer	TLS-based connection with a remote audit server.	User	• DRBG entropy input (R) • DRBG Seed (R) • DRBG V (R/W/Z) • DRBG Key (R/W/Z) • Diffie-Hellman Shared Secret (R/W/Z) • Diffie Hellman private key (R/W/Z) • Diffie Hellman public key (R/W/Z) • TLS Private Key (R/W/Z) • TLS Public Key (R/W/Z) • TLS Pre-Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z)
Show Status	View the operational status of the module	Admin, Monitor, Operator, Analyst, Auditor	• N/A
Zeroization via “"compliance declassify zeroize” Command	Perform zeroization of all persistent CSPs within the module	Admin	• Admin Password (Z) • Monitor Password (Z) • Operator Password (Z) • Analyst Password (Z) • Auditor Password (Z) • SSH Private Key (Z) • SSH Public Key (Z) • SNMPv3 password (Z) • TLS Private Key (Z) • TLS Public Key (Z)
Status LED Output	View status via the Modules LEDs.	Un-auth	• N/A
Cycle Power/ Perform Self-Tests	Reboot of appliance.	Admin, Monitor, Operator,	• DRBG entropy input (Z) • DRBG Seed (Z)

Service	Description	Role	Key/CSP and Type of Access
		Analyst, Auditor, Un-auth	• DRBG V (Z) • DRBG Key (Z) • Diffie-Hellman Shared Secret (Z) • Diffie Hellman private key (Z) • Diffie Hellman public key (Z) • SSH Session Key (Z) • SSH Integrity Key (Z) • SNMPv3 session key (Z) • TLS Pre-Master Secret (Z) • TLS Session Encryption Key (Z) • TLS Session Integrity Key (Z)

R – Read, W – Write, Z – Zeroize

2.4 Physical Security

The modules are production grade multi-chip standalone cryptographic modules that meet Level 1 physical security requirements.

2.5 Cryptographic Key Management

The following table identifies each of the CSPs associated with the module. For each CSP, the following information is provided:

- The name of the CSP/Key
- The type of CSP and associated length
- A description of the CSP/Key
- Storage of the CSP/Key
- The zeroization for the CSP/Key

Table 5 - Details of Cryptographic Keys and CSPs

Key/CSP	Type	Description	Storage	Zeroization
DRBG entropy input	CTR 256-bit	This is the entropy for SP 800-90 RNG.	DRAM	Device power cycle.
DRBG Seed	CTR 256-bit	This DRBG seed is collected from the onboard hardware entropy source.	DRAM	Device power cycle.
DRBG V	CTR 256-bit	Internal V value used as part of SP 800-90 CTR_DRBG.	DRAM	Device power cycle.
DRBG Key	CTR 256-bit	Internal Key value used as part of SP 800-90 CTR_DRBG.	DRAM	Device power cycle.
Diffie-Hellman Shared Secret	DH 2048 – 4096 bits	The shared exponent used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	DRAM	Device power cycle.
Diffie Hellman private key	DH 2048 – 4096 bits	The private exponent used in Diffie-Hellman (DH) exchange.	DRAM	Device power cycle.
Diffie Hellman public key	DH 2048 – 4096 bits	The p used in Diffie-Hellman (DH) exchange.	DRAM	Device power cycle.
SSH Private Key	RSA (Private Key) 2048 – 3072 bits	The SSH private key for the module used for session authentication.	NVRAM	Overwritten w/ “00” prior to replacement.
SSH Public Key	RSA (Public Key) 2048 – 3072 bits	The SSH public key for the module used for session authentication.	NVRAM	Overwritten w/ “00” prior to replacement.
SSH Session Key	Triple-DES 192-bits	The SSH session key. This key is created through SSH key establishment.	DRAM	Device power cycle.

Key/CSP	Type	Description	Storage	Zeroization
	AES 128, 256 bits			
SSH Integrity Key	HMAC-SHA1, HMAC-SHA-256 HMAC-512	The SSH data integrity key. This key is created through SSH key establishment.	DRAM	Device power cycle.
SNMPv3 password	Shared Secret, at least eight characters	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	NVRAM	Overwritten w/ “00” prior to replacement.
SNMPv3 session key	AES 128 bits	SNMP symmetric encryption key used to encrypt/decrypt SNMP traffic.	DRAM	Device power cycle.
TLS Private Key	RSA (Private Key) 2048 – 3072 bits ECDSA (224 – 512 bits)	This private key is used for TLS session authentication.	NVRAM	Overwritten w/ “00” prior to replacement.
TLS Public Key	RSA (Private Key) 2048 – 3072 bits ECDSA (224 – 512 bits)	This public key is used for TLS session authentication.	NVRAM	Overwritten w/ “00” prior to replacement.
TLS Pre-Master Secret	Shared Secret, 384 bits	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created.	DRAM	Device power cycle.
TLS Session Encryption Key	Triple-DES 192-bits AES 128, 256 bits	Key used to encrypt/decrypt TLS session data.	DRAM	Device power cycle.
TLS Session Integrity Key	HMAC SHA-1 160 bits	HMAC-SHA-1 used for TLS data integrity protection.	DRAM	Device power cycle.
Admin Password	Shared Secret, 8+ characters	Authentication password for the Admin user role.	NVRAM	Overwritten w/ “00” prior to replacement.
Monitor Password	Shared Secret,	Authentication password for the Monitor user role.	NVRAM	Overwritten w/ “00”

Key/CSP	Type	Description	Storage	Zeroization
	8+ characters			prior to replacement.
Operator Password	Shared Secret, 8+ characters	Authentication password for the Operator user role.	NVRAM	Overwritten w/ “00” prior to replacement.
Analyst Password	Shared Secret, 8+ characters	Authentication password for the Analyst user role.	NVRAM	Overwritten w/ “00” prior to replacement.
Auditor Password	Shared Secret, 8+ characters	Authentication password for the Audit user role.	NVRAM	Overwritten w/ “00” prior to replacement.

2.6 Cryptographic Algorithm

2.6.1 FIPS-approved Algorithms

The following table identifies the FIPS-approved algorithms included in the module for use in the FIPS mode of operation.

Table 6 – FIPS-approved Algorithms

Cryptographic Algorithm	CAVP Cert. #	Usage
Triple-DES	1941	Used for encryption of SSH and TLS sessions.
AES	3447	Used for encryption of SSH, SNMP, and TLS sessions. Used in support of FIPS-approved DRBG. Note: The module use of AES GCM complies with the Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations defined in SP 800-52.
HMAC-SHS	2195	Used for SSH and TLS traffic integrity. Used in support of SSH, SNMP, and TLS key derivation.
SHS	2837, 2836	Used for SSH, SNMP, and TLS traffic integrity. Used in support of SSH, SNMP, and TLS key derivation. Firmware load test.
RSA	1759, 1758	Used for SSH and TLS Session authentication. Firmware load test.
ECDSA	696	Used for TLS Session authentication. Supported curves include, P-256 P-384 P-521.
DRBG	843	Used in support of SSH and TLS sessions. Used to seed RSA key generation.
CVL	533	SSH, TLS, and SNMP Key Derivation. Note: The TLS, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.

2.6.2 Non-Approved Algorithms allowed for use in FIPS-mode

The cryptographic module implements the following non-Approved algorithms that are allowed for use in FIPS-mode:

- Diffie-Hellman – provides between 112 and 150-bits of encryption strength. Diffie-Hellman with less than 112-bits of security strength is non-compliant and may not be used.
- Elliptic Curve Diffie-Hellman – provides between 112 and 256-bits of encryption strength. Supported curves, include, P-256 P-384 P-521. Elliptic Curve Diffie-Hellman with less than 112-bits of security strength is non-compliance and may not be used.
- RSA Key Wrapping – provides between 112 and 150 bits of encryption strength. RSA with less than 112-bits of security strength is non-compliant and may not be used.
- Non-approved NDRNG for seeding the DRBG.

2.6.3 Non-Approved Algorithms

The cryptographic module implements the following non-approved algorithms that are not permitted for use in FIPS 140-2 mode of operations:

Table 7 – Non-Approved Algorithms

Service	Non-Approved Algorithm
SSH*	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
TLS*	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
SNMP*	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman

Note: Services marked with a single asterisk (*) may use non-compliant cryptographic algorithms. Use of these algorithms are prohibited in a FIPS-approved mode of operation.

2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

All FX appliances are FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI (Class A) certified.

2.8 Self-Tests

Self-tests are health checks that ensure that the cryptographic algorithms within the module are operating correctly. The self-tests identified in FIPS 140-2 broadly fall within two categories

- Power-On Self-Tests
- Conditional Self-Tests

2.8.1 Power-On Self-Tests

The cryptographic module performs the following self-tests at Power-On:

- Software integrity (SHA-256)
- HMAC-SHA1 Known Answer Test
- HMAC-SHA224 Known Answer Test
- HMAC-SHA256 Known Answer Test
- HMAC-SHA384 Known Answer Test
- HMAC-SHA512 Known Answer Test
- AES-128 ECB Encrypt Known Answer Test
- AES-128 ECB Decrypt Known Answer Test
- AES-GCM-256 Encrypt Known Answer Test
- AES-GCM-256 Decrypt Known Answer Test
- TRIPLE-DES Encrypt Known Answer Test
- TRIPLE-DES Decrypt Known Answer Test
- RSA Known Answer Test
- ECDSA Known Answer Test
- DRBG Known Answer Test

2.8.2 Conditional Self-Tests

The cryptographic module performs the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for FIPS-approved DRBG
- Continuous Random Number Generator (CRNGT) for Entropy Source
- Firmware Load Test (2048-bit RSA, SHA-256)
- Pairwise Consistency Test (PWCT) for RSA Key Generation
- Pairwise Consistency Test (PWCT) for ECDSA Key Generation

2.8.3 Self-Tests Error Handling

If any of the identified POSTs fail, the module will not enter an operational state and will instead provide an error message and reboot. If either of the CRNGTs fail, the repeated random numbers are discarded and another random number is requested. If either of the PWCTs fail, the key pair or signature is discarded and another key pair or signature is generated. If the Firmware Load Test fails, the new firmware is not loaded.

Both during execution of the self-tests and while in an error state, data output is inhibited.

2.9 Mitigation of Other Attacks

The module does not claim to mitigate any other attacks beyond those specified in FIPS 140.

3. Secure Operation

The following steps are required to put the module into a FIPS-approved mode of operation.

3.1 Installation

There are no FIPS 140 specific hardware installation steps required.

3.2 Initialization

3.2.1 Enable Trusted Platform Module

Enable the on board TPM which is used as an entropy source for the implemented FIPS-approved DRBG.

1. Enter the CLI configuration mode:
   hostname > enable
   hostname # configure terminal
2. Check if the TPM is present and enabled.
   hostname (config) # show tpm
3. Enable the TPM:
   hostname (config) # tpm enable
4. After reading the warning, select yes to continue.
5. Restart the appliance.

3.2.2 Enable compliance configuration options

Perform the following steps to enable FIPS 140-2 configuration options on the webUI.

1. Enter the CLI configuration mode:
   hostname > enable
   hostname # configure terminal
2. Enable the compliance configuration options on the webUI:
   compliance options webui enable

3.2.3 Enable FIPS 140-2 compliance

There are two methods to enable FIPS 140-2 compliance on the appliance. Compliance may be enabled either through the webUI or through the CLI. Perform the following to enable FIPS 140-2 compliance through the webUI.

1. On the Web UI, select the Settings tab.
2. Select Compliance on the sidebar.
3. Click Enable FIPS Compliance.
4. Click Save changes to continue.
5. Click Reboot Now

Alternatively, perform the following to enable FIPS 140-2 compliance through the CLI.

1. Enable the CLI configuration mode:
   hostname > enable
   hostname # configure terminal
2. Bring the system into FIPS 140-2 compliance:
   hostname (config) # compliance apply standard fips
3. Save your changes:
   hostname (config) # write memory
4. Restart the appliance:
   hostname (config) # reload
5. Verify that the appliance is compliant:
   hostname (config) # show compliance standard fips

3.3 Management

3.3.1 SSH Usage

When in FIPS 140-2 compliance mode, only the following algorithms may be used for SSH communications,

3.3.1.1 Symmetric Encryption Algorithms:

1. 3DES_CBC
2. AES_128_CBC
3. AES_128_GCM
4. AES_256_CBC
5. AES_256_GCM

3.3.1.2 KEX Algorithms:

1. diffie-hellman-group14-sha1

3.3.1.3 Message Authentication Code (MAC) Algorithms:

1. hmac-sha1
2. hmac-sha2-256
3. hmac-sha2-512

3.3.2 TLS Usage

When in FIPS 140-2 compliance mode, only the following ciphersuites may be used for TLS communications,

1. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
2. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
3. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
4. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
5. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
6. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
7. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

8. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
9. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
10. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
11. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
12. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
13. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
14. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
15. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
16. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
17. TLS_DHE_RSA_WITH_AES_256_CBC_SHA
18. TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
19. TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
20. TLS_RSA_WITH_AES_128_GCM_SHA256
21. TLS_RSA_WITH_AES_256_GCM_SHA384
22. TLS_RSA_WITH_AES_128_CBC_SHA256
23. TLS_RSA_WITH_AES_256_CBC_SHA256
24. TLS_RSA_WITH_AES_128_CBC_SHA
25. TLS_RSA_WITH_AES_256_CBC_SHA
26. TLS_RSA_WITH_3DES_EDE_CBC_SHA

When the module’s power is lost and then restored, a new TLS key for use with the AES GCM encryption/decryption is established.

3.4 Additional Information

For additional information regarding FIPS 140-2 compliance, see the “FireEye FIPS 140-2 and Common Criteria Addendum, Release 1.0.”

Appendix A: Acronyms

This section describes the acronyms used throughout the document.

Table 8 - Acronyms

Acronym	Definition
CMVP	Cryptographic Module Validation Program
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CVL	Component Validation List
FIPS	Federal Information Processing Standard
KDF	Key Derivation Function
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
POST	Power-On Self-Test
PWCT	Pairwise Consistency Test