FireEye HX Series: HX4402, HX4502, HX4502D

FireEye, Inc.
FIPS 140-2 Non-Proprietary Security Policy
Document Version: 1.0

Prepared By:
Acumen Security
2400 Research Blvd, Suite 395
Rockville, MD 20850

www.acumensecurity.net

Table of Contents

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for the FireEye HX Series: HX4402, HX4502 and HX4502D. Below are the details of the product validated:

- Hardware Version: HX4402, HX4502, HX4502D
- Firmware Version #: 5.0.4
- 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 HX Series: HX4402, HX4502, and HX4502D 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 HX Series: HX4402, HX4502, and HX4502D

The FireEye HX Series: HX4402, HX4502, and HX4502D (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 HX series appliances enable security operations teams to correlate network and endpoint activity. Organizations can automatically investigate alerts generated by FireEye Threat Prevention Platforms, log management, and network security products, apply intelligence from FireEye to continuously validate Indicators of Compromises on the endpoints and identify if a compromise has occurred and assess the potential risk. Further, organizations can quickly triage the incident to understand the details and contain compromised endpoints with a single click and contain compromised devices within a single click workflow.

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.

1) Power Button	4) NIC Activity LED
2) Power LED	5) HDD LED
3) System Health Indicator LED	

Figure 1: FireEye HX4402 (Front Panel)

1) Power Port	6) Serial Console Port
2) PS/2 Mouse Port	7) Video Port
3) PS/2 Keyboard Port	8) ether1 (RJ45) Management 1 Port
4) IPMI/Serial over Ethernet Port	9) ether2 (RJ45) Management 2 Port
5) USB Ports	

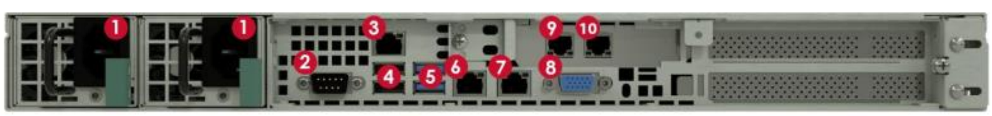
Figure 2: FireEye HX4402 (Rear Panel)

1) Bezel Release	4) LAN 2 LED
2) Universal Information LED	5) Device Activity LED
3) LAN 1 LED	6) Power LED

Figure 3: FireEye HX4502 (Front Panel)

1) Disk Drive Carrier	3) Reset Button
2) Unit Identifier Button	4) Power Button

Figure 4: FireEye HX4502 Chassis (Front Panel without Bezel)



1) Power Port	6) ether1 (RJ45) Management 1 Port
2) Serial Console Port	7) ether2 (RJ45) Management 2 Port
3) IPMI/Serial over Ethernet Port	8) Video Port
4) USB 2.0 Ports	9) Disabled Port
5) USB 3.0 Ports	10) Disabled Port

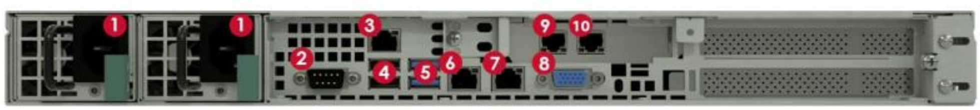
Figure 5: FireEye HX4502 (Rear Panel)

1) Bezel Release	4) LAN 2 LED
2) Universal Information LED	5) Device Activity LED
3) LAN 1 LED	6) Power LED

Figure 6: FireEye HX4502D (Front Panel)

1) Disk Drive Carrier	3) Reset Button
2) Unit Identifier Button	4) Power Button

Figure 7: FireEye HX4502D (Front Panel without Bezel)



1) Power Port	6) ether1 (RJ45) Management 1 Port
2) Serial Console Port	7) ether2 (RJ45) Management 2 Port
3) IPMI/Serial over Ethernet Port	8) Video Port
4) USB 2.0 Ports	9) Disabled Port
5) USB 3.0 Ports	10) Disabled Port

Figure 8: FireEye HX4502D (Rear Panel)

2.1.2 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 – HX4402/4502/4502D

FIPS Interface	Physical Interface
Data Input	(2x) 10/100/1000 BASE-T Management Port (1x) 100 BASE-T Management Port (IPMI) (2x) USB 2.0 Ports (2x) USB 3.0 Ports (HX4502, HX4502D) (1x) PS/2 Mouse Port (HX4402) (1x) PS/2 Keyboard Port (HX4402) (1x) Serial Port
Data Output	(2x) 10/100/1000 BASE-T Management Port (1x) 100 BASE-T Management Port (IPMI) (1x) Video Port (2x) USB 2.0 Ports (2x) USB 3.0 Ports (HX4502, HX4502D) (1x) Serial Port
Control Input	(2x) 10/100/1000 BASE-T Management Port (1x) 100 BASE-T Management Port (IPMI) (2x) USB 2.0 Ports (2x) USB 3.0 Ports (HX4502, HX4502D) (1x) PS/2 Mouse Port (HX4402) (1x) PS/2 Keyboard Port (HX4402) (1x) Serial Port (1x) Power Button (1x) Reset Button (HX4502, HX4502D) (4x) LCD Panel Buttons (HX4402)
Status Output	(2x) 10/100/1000 BASE-T Management Port (1x) 100 BASE-T Management Port (IPMI) (1x) Video Port (2x) USB 2.0 Ports (2x) USB 3.0 Ports (HX4502, HX4502D) (1x) Serial Port LEDs (HX4402 (4x), HX4502 (5x), HX4502D (5x))
Power Interface	(2x) Power Ports

2.2 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.

2.2.1 Authorized Roles

The module supports several different roles, including multiple Cryptographic Officer roles and a User role. The module does not support a maintenance role and/or bypass capability.

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

The Users of the module are the remote IT devices (user role) 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.

2.2.2 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**	Password/Username	All passwords must be between 8 and 32 characters. The passwords can consist of alphanumeric values, {a-z, A-Z, 0-9, and special characters}, the characters can thus be chosen from the 94 human readable ASCII characters on

Role	Type Of Authentication	Authentication Strength
Analyst **Auditor** **SNMP**		an American QWERTY computer keyboard. Thus, the probability of a successful random attempt is 1/94^8 , which is less than 1 in 1,000,000. In the worst-case scenario, 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 again is less than 1 in 1,000,000 required by FIPS 140-2. The module enforces a timed access mechanism as follows: For the first five failed attempts (assuming 0 time to process), no timed access is enforced. Upon the sixth attempt, the module enforces a 15-second delay. For the seventh and eight attempts again, no timed access is enforced. Thereafter this cycle repeats, i.e., every third failed attempt, the module enforces a 15-second delay. This would allow the attacker to perform roughly 15 attempts per minute. The probability of a success with multiple consecutive attempts in a one-minute period is 15/(94^8) (or 15/(10^8) in the worst case), which is less than 1/1,000,000.
User	Password/Username or Asymmetric Authentication	All passwords must be between 8 and 32 characters. The passwords can consist of alphanumeric values, {a-z, A-Z, 0-9, and special characters}, the characters can thus be chosen from the 94 human readable ASCII characters on an American QWERTY computer keyboard. Thus, the probability of a successful random attempt is 1/94^8 , which is less than 1 in 1,000,000. In the worst-case scenario, 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.

Role	Type Of Authentication	Authentication Strength
		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 again is less than 1 in 1,000,000 required by FIPS 140-2. The module enforces a timed access mechanism as follows: For the first five failed attempts (assuming 0 time to process), no timed access is enforced. Upon the sixth attempt, the module enforces a 15-second delay. For the seventh and eight attempts again, no timed access is enforced. Thereafter this cycle repeats, i.e., every third failed attempt, the module enforces a 15-second delay. This would allow the attacker to perform roughly 15 attempts per minute. The probability of a success with multiple consecutive attempts in a one-minute period is 15/(94^8) (or 15/(10^8) in the worst case), which is less than 1/1,000,000. 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 5.19x10^28 attempts per minute. In the worst-case scenario, an operator can make 60 failed attempts per minute.

2.2.3 Services

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, modified, or zeroized
- **Z (Zeroize):** The CSP is zeroized

Table 4 – Services

Service	Description	Role	Key/CSP and Type of Access
SSH to external IT device	Secure SSH connection between a CM and other FireEye appliances using SSH.	User	• DRBG entropy input (W/R) • DRBG Seed (W/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.	CO	• 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 (W/R) • DRBG Seed (W/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.	CO	• 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 (W/R) • DRBG Seed (W/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)

Service	Description	Role	Key/CSP and Type of Access
			• TLS Private Key (R/W/Z) • TLS Public Key (R/W/Z) • TLS Pre-Master Secret (R/W/Z) • TLS Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z) • TLS Session Integrity Key (R/W/Z)
Administrative access over serial console and VGA	Directly connected command line appliance administration.	CO	• 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.	CO	• 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 (W/R) • DRBG Seed (W/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 Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z) • TLS Session Integrity 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 (W/R) • DRBG Seed (W/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)

Service	Description	Role	Key/CSP and Type of Access
			• TLS Public Key (R/W/Z) • TLS Pre-Master Secret (R/W/Z) • TLS Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z) • TLS Session Integrity Key (R/W/Z)
SAML over TLS (Web GUI)	Secure remote authentication to the Web GUI via TLS protected SAML	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 (W/R) • DRBG Seed (W/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 Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z) • TLS Session Integrity Key (R/W/Z)
Secure log transfer	TLS-based connection with a remote audit server.	User	• DRBG entropy input (W/R) • DRBG Seed (W/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 Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z) • TLS Session Integrity Key (R/W/Z)
TLS to external IT device	Secure connection between a CM and other FireEye appliances using TLS.	User	• DRBG entropy input (W/R) • DRBG Seed (W/R) • DRBG V (R/W/Z) • DRBG Key (R/W/Z)

Service	Description	Role	Key/CSP and Type of Access
			• 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 Master Secret (R/W/Z) • TLS Session Encryption Key (R/W/Z)
Show Status	View the operational status of the module	CO	N/A
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand	CO	N/A
Status LED Output	View status via the Modules LEDs.	Un-auth	N/A
Cycle Power	Reboot of appliance.	Un-auth	• DRBG entropy input (Z) • DRBG Seed (Z) • 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 Master Secret (Z) • TLS Session Encryption Key (Z) • TLS Session Integrity Key (Z)
Zeroization via "compliance declassify zeroize" Command	Perform zeroization of all persistent CSPs within the module	CO	• 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)

R – Read, W – Write, Z – Zeroize

2.3 Physical Security

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

2.4 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,HMAC-SHA-512	This is the entropy for SP 800-90 RNG.	DRAM	Device power cycle.
DRBG Seed	CTR 256-bit, HMAC-SHA-512	Seed material used to seed or reseed the DRBG.	DRAM	Device power cycle.
DRBG V	CTR 256-bit, HMAC-SHA-512	Internal V value used as part of SP 800-90 CTR_DRBG, HMAC_DRBG.	DRAM	Device power cycle.
DRBG Key	CTR 256-bit, HMAC-SHA-512	Internal Key value used as part of SP 800-90 CTR_DRBG, HMAC_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 (DSA) 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.
EC Diffie-Hellman Shared Secret	ECDH P-256, P-384, P-521	The shared secret used in the EC Diffie-Hellman (ECDH) exchange.	DRAM	Device power cycle.
EC Diffie Hellman private key	ECDH P-256, P-384, P-521	The private key used in EC Diffie-Hellman (DH) exchange.	DRAM	Device power cycle.

Key/CSP	Type	Description	Storage	Zeroization
EC Diffie Hellman public key	ECDH P-256, P-384, P-521	The public key used in EC 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	AES 128, 256 bits	The SSH session key. This key is created through SSH key establishment.	DRAM	Device power cycle.
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 (Private Key) P-256 P-384 P-521	This private key is used for TLS session authentication.	NVRAM	Overwritten w/ “00” prior to replacement.
TLS Public Key	RSA (Public Key) 2048 – 3072 bits ECDSA (Public Key) P-256 P-384 P-521	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 the TLS Master Secret can be derived.	DRAM	Device power cycle.

Key/CSP	Type	Description	Storage	Zeroization
TLS Master Secret	Shared Secret, 384 bits	Shared Secret created using the TLS Pre-Master Secret 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-SHA1 HMAC-SHA256 HMAC-SHA384	HMAC-SHA 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, 8+ characters	Authentication password for the Monitor user role.	NVRAM	Overwritten w/ “00” 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.

2.5 Cryptographic Algorithm

2.5.1 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

Algorithm	CAVP Cert. #	Options	Usage
Triple-DES[1]	C1720	**TECB**(KO 1 e/d), **TCBC**(KO 1 e/d) **KTS** 112-bits (paired with HMAC Cert. #C1720) Per SP800-67 rev2, the user is responsible for ensuring the module's limit to 2^20 encryptions with the same Triple-DES key while being used in the TLS protocol	Used for encryption of TLS sessions.
		TCFB1(KO 1 e/d); **TCFB8** (KO 1 e/d); **TCFB64**(KO 1 e/d); **TOFB**(KO 1 e/d)	Implemented within the module however never used by any service
AES	C1720	**ECB** (e/d 128, 256); **CBC** (e/d 128, 256); **OFB** (e/d 128); **CTR** (ext only; 128, 256) **GCM**[2] **(KS: AES_128**(e/d) Tag Length(s): 128 120 112 104 96 64 32) **(KS: AES_256**(e/d) Tag Length(s): 128 120 112 104 96 64 32) **IV Generated:** (Internal (using Section 8.2.1)) ; **PT Lengths Tested:** (0 , 1024) ; **AAD Lengths tested:** (1024) ; **96BitIV_Supported GMAC_Supported**	Used for encryption of SSH, SNMP, and TLS sessions. Used in support of FIPS-approved DRBG.

[1] The operator shall ensure that the number of 64-bit blocks encrypted by the same key does not exceed 2^20 with a single Triple-DES key when Triple-DES is the encryption algorithm for TLS.

[2] The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS and RFC 5647 for SSH. Per RFC 5246, if the module is the party that encounters this condition it will trigger a handshake to establish a new encryption key. Per RFC 5647 the module ensures that if the invocation counter reaches its maximum value 2^64 – 1, the next AES GCM encryption is performed with the invocation counter set to either 0 or 1, with a maximum of 2^64 – 1 encryptions per session.

		KTS 128, 256-bits (paired with HMAC Cert. # C1720) AES GCM is used as part of TLS 1.2 cipher suites conformant to IG A.5, RFC 5288 and SP 800-52 and as part of SSHv2 cipher suites conformant to IG A.5 and RFCs 4252, 4253 and 5647.	
		ECB (e/d 192); **CBC** (e/d 192); **CFB1** (e/d 128, 192, 256); **CFB8** (e/d 128, 192, 256); **OFB** (e/d 192, 256); **CTR** (ext only; 192) **CCM (KS: 128 , 192 , 256**) **(Assoc. Data Len Range**: 0 - 32) **(Payload Length Range**: 0 - 32 (**Nonce Length(s)**: 7 13 **(Tag Length(s)**: 4 16) **GCM (KS: AES_192**(e/d) Tag Length(s): 128 120 112 104 96 64 32)	Implemented within the module however never used by any service
HMAC-SHS	C1720	**HMAC-SHA1 (Key Sizes Ranges Tested:**KS=BS, KS> BS, KS < BS) **HMAC-SHA256 (Key Size Ranges Tested:** KS=BS, KS> BS, KS < BS) **HMAC-SHA384 (Key Size Ranges Tested:** KS=BS, KS> BS, KS < BS) **HMAC-SHA512 (Key Size Ranges Tested:** KS=BS, KS> BS, KS < BS) **KTS** HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 (paired with either AES cert. #C1720 or Triple-DES Cert. # C1720)	Used for SSH and TLS traffic integrity. Used in support of SSH, SNMP, and TLS key derivation.
		HMAC-SHA224 (Key Size Ranges Tested: KS=BS, KS> BS, KS < BS)	Implemented within the module however never used by any service
	C1934	**HMAC-SHA1 (Key Sizes Ranges Tested:**KS=BS, KS> BS, KS < BS) **HMAC-SHA256 (Key Size Ranges Tested:** KS=BS, KS> BS, KS < BS) **HMAC-SHA384 (Key Size Ranges Tested:** KS=BS, KS> BS, KS < BS) **HMAC-SHA512 (Key Size Ranges Tested:** KS=BS, KS> BS, KS < BS)	Used in support of random bit generation.

SHS	C1720	**SHA-1** (BYTE-only) **SHA-256** (BYTE-only) **SHA-384** (BYTE-only) **SHA-512** (BYTE-only)	Used for SSH, SNMP, and TLS traffic integrity. Used in support of SSH, SNMP, and TLS key derivation.
		SHA-224 (BYTE-only)	Implemented within the module however never used by any service
	C1720	**SHA-256** (BYTE-only)	Firmware load test
	C1934	**SHA-1** (BYTE-only) **SHA-256** (BYTE-only) **SHA-384** (BYTE-only) **SHA-512** (BYTE-only)	Used in support of random bit generation.
RSA	C1720	**FIPS186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (10001) ; **PGM(ProvPrimeCondition)** (2048 SHA(256)) (3072 SHA(256)) **ALG[ANSIX9.31]** Sig(Gen): (3072 SHA(256 , 384 , 512)) Sig(Ver): (1024 SHA(1 , 256 , 384 , 512)) (2048 SHA(1 , 256 , 384 , 512)) (3072 SHA(1, 256 , 384 , 512) **ALG[RSASSA-PKCS1_V1_5]** SIG(gen) (2048 SHA(256 , 384 , 512)) (3072 SHA(256 , 384 , 512)) SIG(Ver) (1024 SHA(1, 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512))	Used for SSH and TLS Session authentication.
	C1720	**FIPS186-4:** **ALG[RSASSA-PKCS1_V1_5]** SIG(Ver) (2048 SHA(256))	Firmware load test
ECDSA	C1720	**FIPS186-4:** **PKG: CURVES**(P-256 ExtraRandomBits TestingCandidates) **PKV: CURVES**(P-256) **SigGen: CURVES**(P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) *SIG(gen) with SHA-1 allowed for use with protocols only.* **SigVer: CURVES**(P-256: (SHA-1, 224, 256, 384) P-384: (SHA-1, 224, 256, 384) P-521: (SHA-1, 224, 256, 384)	Used for TLS Session authentication.

		PKG: CURVES(P-384 P-521 ExtraRandomBits TestingCandidates) **PKV: CURVES**(P-384 P-521)	Implemented within the module however never used by any service
DSA	C1720	**FIPS186-4:** **KeyPairGen:** [(2048,256) ; (3072,256)]	Used for Diffie-Hellman Key Generation
DRBG	C1720	**CTR_DRBG**: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-128, AES-192, AES-256)] BlockCipher_No_df: (AES-128, AES-192, AES-256)]	Used in support of SSH and TLS sessions. Used to seed RSA key generation.
DRBG	C1934	**HMAC_DRBG**: [Prediction Resistance Tested: Enabled; Reseed Supported; Modes: SHA-1, SHA-256, SHA-384, SHA-512]	Used to generate the requested random bits.
CVL	C1720	**TLS**(TLS1.0/1.1 TLS1.2 (SHA 256, 384)) **SSH** (SHA 1 , 256 , 512) **SNMP** SHA1	SSH, TLS, and SNMP Key Derivation.
KAS-SSC	Vendor Affirmed	[56Arev3] **FFC** **SCHEME: Ephem:** (KARole: Initiator / Responder) Safe Primes per Appendix D **ECC** **SCHEME: EphemUnified:** (KARole: Initiator / Responder) EC: P-256 , P-384, P-521	Diffie-Hellman, EC Diffie-Hellman Key Agreement
CKG	Vendor Affirmed	[133rev2] Section 5.1 Asymmetric signature key generation using unmodified DRBG output	Key Generation
		[133rev2] Section 5.2 Asymmetric key establishment key generation using unmodified DRBG output	
		[133rev2] Section 6.1 Direct symmetric key generation using unmodified DRBG output	
		[133rev2] Section 6.2.1 Derivation of symmetric keys from a key agreement shared secret	

2.5.2 Non-Approved Algorithms Allowed for Use With FIPS-approved services

The module implements the following non-Approved algorithms that are allowed for use with FIPS-approved services:

- RSA Key Wrapping – provides 112 or 128 bits of encryption strength.
- NDRNG - Internal entropy source providing 256-bits of entropy to the DRBG.

Note: No parts of the SNMP, SSH, and TLS protocols, other than the KDF, have been tested by the CAVP.

2.5.3 Non-Approved Algorithms Disallowed for Use With FIPS-approved services

The same set of services are supported by the module in the non-FIPS mode as in the FIPS mode.

In addition to the list of SSH ciphers supported in the FIPS mode (Section 3.4.1), the module also implements the following non-Approved symmetric algorithm that is allowed for use in the non-FIPS mode alone:

1. rijndael-cbc@lysator.liu.se

For TLS, the ciphers supported in the FIPS mode (Section 3.4.2) are available except for the following two ciphers:

1. TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
2. TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

2.6 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

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

2.7 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

2.7.1 Power-On Self-Tests

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

- Firmware 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
- TDES ECB Encrypt Known Answer Test
- TDES ECB Decrypt Known Answer Test
- RSA (mod 2048) Sign and Verify Known Answer Tests
- ECDSA (P-256) Sign and Verify Known Answer Tests
- DRBG (CTR) Known Answer Tests
  - Generate, Reseed, Instantiate KATs
- DRBG (HMAC) Known Answer Tests
  - Generate, Reseed, Instantiate KATs
- DSA Pairwise Consistency Test
- Primitive “Z” Known Answer Tests
  - KAS FFC (dhEphem)
  - KAS ECC (Ephemeral Unified)

2.7.2 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
- Pairwise Consistency Test (PWCT) for ECDSA
- Pairwise Consistency Test (PWCT) for DSA

2.7.3 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.

2.8 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 the FIPS-approved mode of operation. Prior to performing the steps below, the module is in the non-FIPS mode of operation. The cryptographic officer shall verify that the firmware image to be loaded on the module is a FIPS validated image. If any non-validated firmware image is loaded the module will no longer be a FIPS validated module. Any firmware versions other than version 5.0.4, loaded into the modules are out of the scope of this validation and require a separate FIPS 140-2 validation.

3.1 Modes of Operation

The module supports one FIPS Approved mode of operation and a non-Approved mode i.e., a non-FIPS mode of operation. The module must always be zeroized when switching between the FIPS Approved mode of operation and the non-Approved mode of operation and vice versa. Prior to performing the steps outlined below, the module will operate in the non-FIPS mode. All services available in the non-FIPS mode are identical to those in the FIPS approved mode besides key generation services.

3.2 Installation

There are no FIPS 140 specific hardware installation steps required.

3.3 Initialization

3.3.1 Default Authentication

During initial setup, the CO will be prompted to change the default authentication credentials. These credentials must be changed at this point.

3.3.2 Enable compliance configuration options

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

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

3.3.3 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.

- On the Web UI, select the Settings tab.
- Select Compliance on the sidebar.
- Click Enable FIPS Compliance.
- Click Save changes to continue.
- Click Reboot Now

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

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

3.4 Management

3.4.1 SSH Usage

When in FIPS 140-2 compliance mode, only the following algorithms may be used for SSH communications. Note: The module itself restricts access to algorithms. No other algorithms are available.

3.4.1.1 Symmetric Encryption Algorithms:

1. AES_128_CBC
2. AES_128_CTR
3. AES_256_CBC
4. AES_256_CTR
5. AES_128_GCM
6. AES_256_GCM

3.4.1.2 KEX Algorithms:

1. diffie-hellman-group14-sha1

3.4.1.3 Message Authentication Code (MAC) Algorithms:

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

3.4.2 TLS Usage

When in FIPS 140-2 compliance mode, only the following ciphersuites may be used for TLS communications. Note: The module itself restricts access to algorithms. No other algorithms are available.

1. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
2. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

3. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
4. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
5. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
6. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
7. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
8. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
9. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
10. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
11. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
12. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
13. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
14. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
15. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
16. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
17. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
18. TLS_DHE_RSA_WITH_AES_256_CBC_SHA
19. TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
20. TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
21. TLS_RSA_WITH_AES_128_GCM_SHA256
22. TLS_RSA_WITH_AES_256_GCM_SHA384
23. TLS_RSA_WITH_AES_128_CBC_SHA256
24. TLS_RSA_WITH_AES_256_CBC_SHA256
25. TLS_RSA_WITH_AES_128_CBC_SHA
26. TLS_RSA_WITH_AES_256_CBC_SHA

Note: In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

Note: The module is compatible with TLSv1.2 and supports the GCM ciphersuites defined SP 800-52 Rev 1, Section 3.3.1. The module implements nonce management logic that ensures when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key a new encryption key is established.

3.4.3 SNMP Usage

When in FIPS 140-2 compliance mode, only AES_128_OFB may be used for SNMPv3 communications. Note: The module itself restricts access to algorithms. No other algorithms are available.

3.5 Secure Delivery

The product is delivered via commercial carrier (either FedEx or UPS). The product will contain a packing slip with the serial numbers of all shipped devices. The Cryptographic Officer must verify that the hardware serial numbers match the serial numbers listed in the packing slip. Additionally, the Cryptographic Officer must verify that there are no signs of damage/tampering within the delivered package. Any sign of damage/tampering must be reported to FireEye for guidance.

3.6 Switching Modes of operation

To switch between the FIPS mode and the non-FIPS mode, the “reset factory” command can be used which essentially resets the module to its factory default configuration i.e., the non-FIPS mode. Prior to switching between FIPS mode and non-FIPS mode of operation, the CO must perform the zeroization operation via the “compliance declassify zeroized” command.

3.7 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 7 - Acronyms

Acronym	Definition
CMVP	Cryptographic Module Validation Program
CRNGT	Continuous Random Number Generator Test
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