FireEye EX Series: EX-3500, EX-5500, EX-8500

FireEye, Inc.
FIPS 140-2 Non-Proprietary Security Policy
Document Version: 1.3

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 EX Series: EX-3500, EX-5500, EX-8500. Below are the details of the product validated:

- Hardware Version: EX-3500, EX-5500, EX-8500
- Firmware Version #: 8.0
- 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 EX Series: EX-3500, EX-5500, EX-8500 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 EX Series: EX-3500, EX-5500, EX-8500

The FireEye EX Series: EX-3500, EX-5500, EX-8500 (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 EX series secures against advanced email attacks. As part of the FireEye Threat Prevention Platform, the FireEye EX uses signature-less technology to analyze every email attachment and successfully quarantine spear-phishing emails used in advanced targeted attacks.

With all the personal information available online, a cybercriminal can socially engineer almost any user into clicking a URL or opening an attachment. The FireEye EX series provides real-time threat prevention for spear-phishing attacks that evade traditional defenses. The EX also delivers a new level of threat prevention against blended attacks by working with the FireEye NX platform to quarantine emails with malicious URLs and trace Web-based attacks back to the original spear-phishing email.

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.

Figure 1: FireEye EX Series

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 – EX-3500/EX-5500/EX-8500

FIPS Interface	Physical Interface
Data Input	(2x) 1GigE BaseT Ports (Network Monitoring) (EX-3500/EX-5500) (4x) SFP+ Ports (Network Monitoring) (EX-8500) (2x) 1GigE BaseT Ports (Management) PS/2 Keyboard and Mouse Ports (2x) USB Ports Serial Port
Data Output	(2x) 1GigE BaseT Ports (Network Monitoring) (EX-3500/EX-5500) (4x) SFP+ Ports (Network Monitoring) (EX-8500) (2x) 1GigE BaseT Ports (Management) DB15 VGA Port (2x) USB Ports Serial Port
Control Input	(2x) 1GigE BaseT Ports (Management) PS/2 Keyboard and Mouse Ports (2x) USB Ports Serial Port
Status Output	(2x) 1GigE BaseT Ports (Management) DB15 VGA Port (2x) USB Ports Serial Port
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.
- **WSAPI:** The WSAPI role supports system administration via a TLS authenticated interface.

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.

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.

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

Table 3 - Authentication Mechanism Details

Role	Type Of Authentication	Authentication Strength
Admin **Monitor** **Operator** **Analyst**	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

Role	Type Of Authentication	Authentication Strength
Auditor **SNMP** **WSAPI**		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.
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 5.19x10^28 attempts per minute, which far exceeds the operational capabilities of the modules to support.

2.3.3 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 connection between an EX 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	CO	• Admin Password (R/W/Z) • Monitor Password (R/W/Z) • Operator Password (R/W/Z)

Service	Description	Role	Key/CSP and Type of Access
	administration over a TLS tunnel.		• 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 Session Encryption Key (R/W/Z) • TLS Session Integrity Key (R/W/Z)
Administrative access over WSAPI	Secure remote appliance administration over a TLS tunnel.	CO	• WSAPI Password (R/W/Z) • DRBG entropy input (R/W) • DRBG Seed (R/W) • 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) • 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)

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 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) • TLS Public Key (R/W/Z) • TLS Pre-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 Session Encryption Key (R/W/Z) • TLS Session Integrity Key (R/W/Z)
Show Status	View the operational status of the module	CO	• N/A

Service	Description	Role	Key/CSP and Type of Access
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 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 ECDH P-256	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 ECDH P-256	The private exponent used in Diffie-Hellman (DH) exchange.	DRAM	Device power cycle.
Diffie Hellman public key	DH 2048 – 4096 bits ECDH P-256	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		DRAM	Device power cycle.

Key/CSP	Type	Description	Storage	Zeroization
	AES 128, 256 bits	The SSH session key. This key is created through SSH key establishment.		
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 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-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.

Key/CSP	Type	Description	Storage	Zeroization
Monitor Password	Shared Secret, 8+ characters	Authentication password for the Monitor user role.	NVRAM	Overwritten w/ “00” prior to replacement.
Operator Password	Shared Secret, at least eight 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.
WSAPI Password	Shared Secret, 8+ characters	Authentication password for the WSAPI 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

Algorithm	CAVP Cert. #	Options	Usage
Triple-DES	2531	**TECB**(KO 1 e/d), **TCBC**(KO 1 e/d) **KTS** (SP 800-38F) 112-bits (paired with HMAC cert. # 3172) Per SP800-67 rev1, the user is responsible for ensuring the module's limit to 2^32 encryptions with the same Triple-DES key while being used in SSH and/or TLS protocols	Used for encryption of SSH and 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	4761	**ECB** (e/d 128, 256); **CBC** (e/d 128, 256); **OFB** (e/d 128); **CTR** (ext only; 128, 256) **GCM (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** **KTS** (SP 800-38F) 128, 256-bits (paired with HMAC cert. # 3172) AES GCM is used as part of TLS 1.2 cipher suites conformant to IG A.5, RFC 5288 and SP 800-52	Used for encryption of SSH, SNMP, and TLS sessions. Used in support of FIPS-approved DRBG.
		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)	Implemented within the module

		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)	however never used by any service
HMAC-SHS	3172	**HMAC-SHA1 (Key Sizes Ranges Tested:**KS=BS) **HMAC-SHA256 (Key Size Ranges Tested:**KS=BS) **HMAC-SHA384 (Key Size Ranges Tested:**KS=BS) **HMAC-SHA512 (Key Size Ranges Tested:**KS=BS) **KTS** HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 (paired with either AES cert. # 4761 or Triple-DES cert. #2531)	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)	Implemented within the module however never used by any service
SHS	3904	**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
	3903	**SHA-256** (BYTE-only)	Firmware load test
RSA	2605	**FIPS186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (10001) ; **PGM(ProvPrimeCondition)** (2048 SHA(256)) (3072 SHA(256)) **ALG[ANSIX9.31]** Sig(Gen): (2048 SHA(256 , 384 , 512)) (3072 SHA(256 , 384 , 512)) Sig(Ver): (1024 SHA(1 , 256 , 384 , 512)) (2048 SHA(1 , 256 , 384 , 512)) (3072 SHA(256 , 384)) **ALG[RSASSA-PKCS1_V1_5]** SIG(gen) (2048 SHA(256 , 384 , 512)) (3072 SHA(256 , 384 , 512)) SIG(Ver) (1024 SHA(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.

	2604	**FIPS186-4:** **ALG[RSASSA-PKCS1_V1_5]** SIG(Ver) (2048 SHA(256))	Firmware load test
ECDSA	1193	**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 affirmed 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	1281	**FIPS186-4:** **KeyPairGen:** [(2048,256) ; (3072,256)]	Used for Diffie-Hellman Key Generation
DRBG	1638	**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.
CVL	1407	**TLS**(TLS1.0/1.1 TLS1.2 (SHA 256)) **SSH** (SHA 1 , 256 , 512) **SNMP** SHA1	SSH, TLS, and SNMP Key Derivation.
CVL	1406	**FFC:** (FUNCTIONS INCLUDED IN IMPLEMENTATION: KPG) **SCHEMES: Ephem:** (KARole: Initiator / Responder) FB **ECC:** (FUNCTIONS INCLUDED IN IMPLEMENTATION: KPG) **SCHEMES: EphemUnified:** (KARole: Initiator / Responder) EC: P-256	Diffie-Hellman, EC Diffie-Hellman Key Agreement
CKG	N/A	The vendor affirms generated seeds for private keys are generated per SP 800-133 (unmodified output from a DRBG)	

2.6.1 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:

- Diffie-Hellman – provides between 112 and 150-bits of encryption strength.
- Elliptic Curve Diffie-Hellman – provides 128-bits of encryption strength.
- RSA Key Wrapping – provides 112 or 128 bits of encryption strength.
- NDRNG - Internal entropy source providing 256-bits of entropy to the DRBG.

2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

All EX 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:

- 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 Encrypt Known Answer Test
- TDES Decrypt Known Answer Test
- RSA Known Answer Test
- ECDSA Known Answer Test
- DRBG Known Answer Test
- DSA Pairwise Consistency Test
- Primitive "Z" 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
- Pairwise Consistency Test (PWCT) for ECDSA
- Pairwise Consistency Test (PWCT) for DSA

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. Prior to performing the steps below, the module is in a non-FIPS mode of operation.

3.1 Non-FIPS mode of Operation

Prior to performing the steps outlined below, the module will operate in "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 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.

3.3.2 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

3.3.3 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.

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

3.4 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. 3DES_CBC
2. AES_128_CBC
3. AES_128_CTR
4. AES_128_GCM
5. AES_256_CBC
6. AES_256_CTR
7. 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
27. TLS_RSA_WITH_3DES_EDE_CBC_SHA

3.4.3 SNMP Usage

When in FIPS 140-2 compliance mode, only AES_128_OFB may be used for SNMP v3 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 is 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

When 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
CSEC	Communications Security Establishment Canada
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