



# FireEye NX Series: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500

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](http://www.acumensecurity.net)

*Table of Contents*

---

- 1. Introduction ..... 4
  - 1.1 Purpose..... 4
  - 1.2 Document Organization..... 4
  - 1.3 Notices..... 4
- 2. FireEye NX Series: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500 ..... 5
  - 2.1 Cryptographic Module Specification..... 6
    - 2.1.1 Cryptographic Boundary..... 6
  - 2.2 Cryptographic Module Ports and Interfaces ..... 13
  - 2.3 Roles, Services, and Authentication..... 15
    - 2.3.1 Authorized Roles ..... 15
    - 2.3.2 Authentication Mechanisms..... 15
    - 2.3.3 Services ..... 17
  - 2.4 Physical Security ..... 23
  - 2.5 Cryptographic Key Management ..... 24
  - 2.6 Cryptographic Algorithm ..... 27
    - 2.6.1 FIPS-approved Algorithms ..... 27
    - 2.6.2 Non-Approved Algorithms Allowed for Use With FIPS-approved services ..... 31
    - 2.6.3 Non-Approved Algorithms Disallowed for Use With FIPS-approved services..... 31
  - 2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC) ..... 32
  - 2.8 Self-Tests ..... 33
    - 2.8.1 Power-On Self-Tests ..... 33
    - 2.8.2 Conditional Self-Tests ..... 33
    - 2.8.3 Self-Tests Error Handling ..... 33
  - 2.9 Mitigation of Other Attacks ..... 35
- 3. Secure Operation ..... 36
  - 3.1 Modes of Operation ..... 36
  - 3.2 Installation..... 36
  - 3.3 Initialization ..... 36
    - 3.3.1 Default Authentication..... 36

## FIPS 140-2 Security Policy

3.3.2	Enable compliance configuration options .....	36
3.3.3	Enable FIPS 140-2 compliance.....	36
3.4	Management .....	37
3.4.1	SSH Usage .....	37
3.4.1.1	Symmetric Encryption Algorithms: .....	37
3.4.1.2	KEX Algorithms: .....	37
3.4.1.3	Message Authentication Code (MAC) Algorithms: .....	37
3.4.2	TLS Usage .....	37
3.4.3	SNMP Usage.....	38
3.5	Secure Delivery .....	38
3.6	Switching Modes of operation.....	39
3.7	Additional Information .....	39
Appendix A: Acronyms .....		40

## 1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for the FireEye NX Series: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500. Below are the details of the product validated:

Hardware Version: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500

Firmware Version #: 9.0.3

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 NX Series: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500 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 NX Series: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500

The FireEye NX Series: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500 (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 Network Threat Prevention Platform identifies and blocks zero-day Web exploits, droppers (binaries), and multi-protocol callbacks to help organizations scale their advanced threat defenses across a range of deployments, from the multi-gigabit headquarters down to remote, branch, and mobile offices. FireEye Network with Intrusion Prevention System (IPS) technology further optimizes spend, substantially reduces false positives, and enables compliance while driving security across known and unknown threats.

### 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.

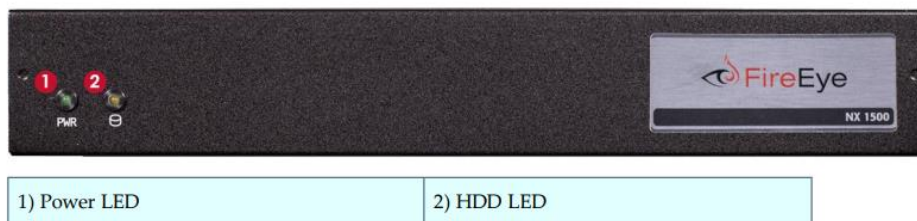


Figure 1: FireEye NX1500 (Front Panel)

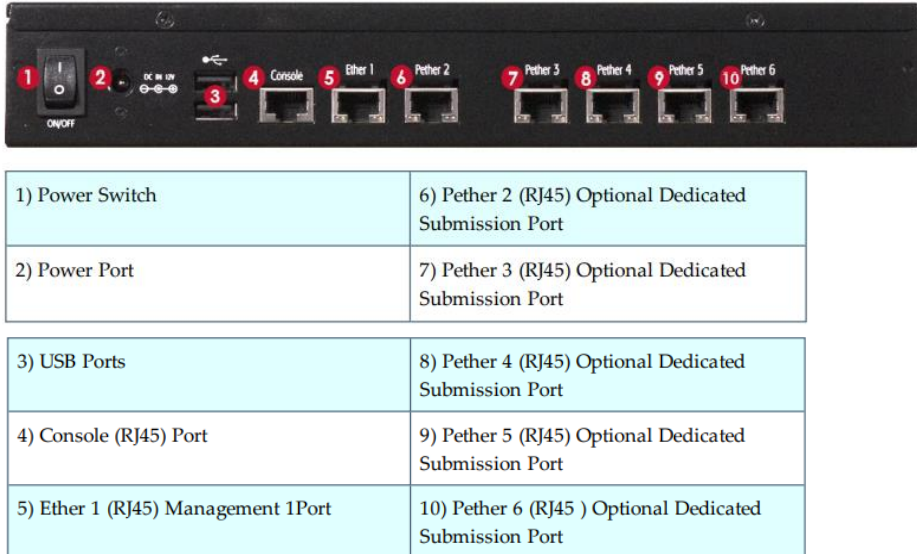


Figure 2: FireEye NX1500 (Rear Panel)

# FIPS 140-2 Security Policy



1) Power LED	6) Ether 1 (RJ45) Management 1 Port
2) HDD LED	7) Pether 3 (RJ45) Monitoring 3 Port
3) Console (RJ45) Port	8) Pether 4 (RJ45) Monitoring 4 Port
4) USB Ports	9) Pether 5 (RJ45) Monitoring 5 Port
5) Disabled Port	10) Pether 6 (RJ45) Monitoring 6 Port

Figure 3: FireEye NX2500 (Front Panel)



1) pether2 (RJ45) Optional Dedicated Submission Port or Dedicated Out-of-Band Blocking Port	3) Power Port
2) Power Switch	

Figure 4: FireEye NX2500 (Rear Panel)



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

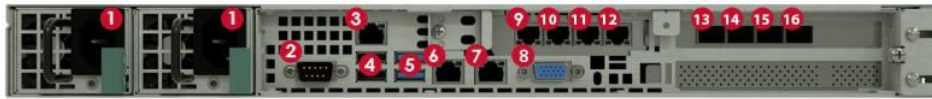
Figure 5: FireEye NX2550 (Front Panel)



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

Figure 6: FireEye NX2550 Chassis (Front Panel without Bezel)

## FIPS 140-2 Security Policy



1) Power Port	9) pether3 (RJ45) Monitoring 3 Port
2) Serial Console Port	10) pether4 (RJ45) Monitoring 4 Port
3) IPMI/Serial over Ethernet Port	11) pether5 (RJ45) Monitoring 5 Port
4) USB 2.0 Ports	12) pether6 (RJ45) Monitoring 6 Port
5) USB 3.0 Ports	13) pether7 (SFP+) Monitoring 7 Port
6) ether1 (RJ45) Management 1 Port	14) pether8 (SFP+) Monitoring 8 Port
7) pether2 (RJ45) Optional Dedicated Out-of-Band Blocking 2 Port	15) pether9 (SFP+) Monitoring 9 Port
8) Video Port	16) pether10 (SFP+) Monitoring 10 Port

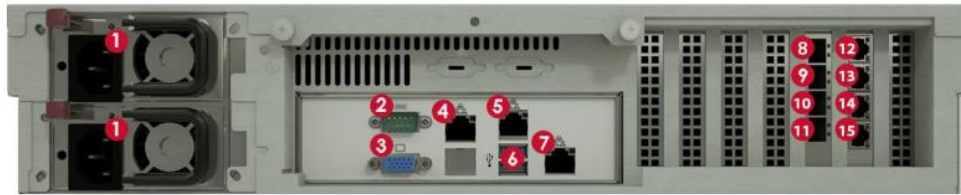
Figure 7: FireEye NX2550 (Rear Panel)



1) USB 2.0 Ports	6) Information LED
2) Bezel Release	7) ether1 LED
3) Power Button	8) IPMI LED
4) HDD LED	9) Reset Button
5) Power LED	

Figure 8: FireEye NX3500 (Front Panel)





1) Power Port	9) pether4 (SFP+) Monitoring 4 Port
2) Serial Console Port	10) pether5 (SFP+) Monitoring 5 Port
3) Video Port	11) pether6 (SFP+) Monitoring 6 Port
4) pether2 (RJ45) Optional Dedicated Out-of-Band Blocking 2 Port	12) pether7 (RJ45) Monitoring 7 Port
5) ether1 (RJ45) Management 1 Port	13) pether8 (RJ45) Monitoring 8 Port
6) USB 3.0 Ports	14) pether9 (RJ45) Monitoring 9 Port
7) IPMI Port	15) pether10 (RJ45) Monitoring 10 Port
8) pether3 (SFP+) Monitoring 3 Port	

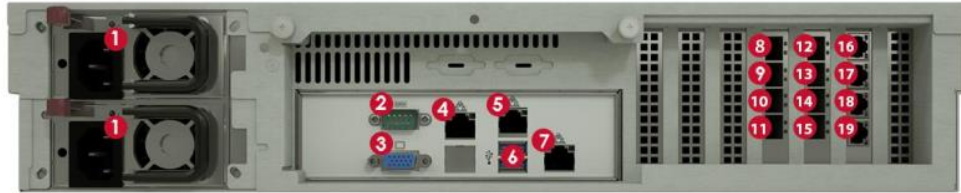
Figure 9: FireEye NX3500 (Rear Panel)



1) USB 2.0 Ports	6) Information LED
2) Bezel Release	7) ether1 LED
3) Power Button	8) IPMI LED
4) HDD LED	9) Reset Button
5) Power LED	

Figure 10: FireEye NX4500 (Front Panel)

# FIPS 140-2 Security Policy



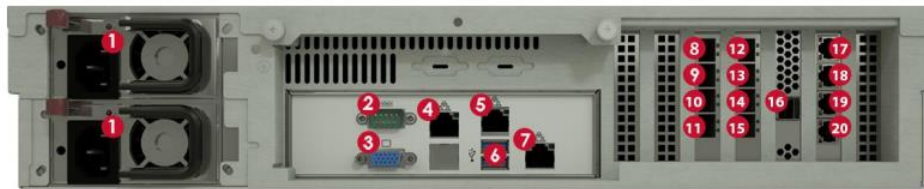
1) Power Port	11) pether6 (SFP+) Monitoring 6 Port
2) Serial Console Port	12) pether7 (SFP+) Monitoring 7 Port
3) Video Port	13) pether8 (SFP+) Monitoring 8 Port
4) pether2 (RJ45) Optional Dedicated Out-of-Band Blocking 2 Port	14) pether9 (SFP+) Monitoring 9 Port
5) ether1 (RJ45) Management 1 Port	15) pether10 (SFP+) Monitoring 10 Port
6) USB 3.0 Ports	16) pether11 (RJ45) Monitoring 11 Port
7) IPMI Port	17) pether12 (RJ45) Monitoring 12 Port
8) pether3 (SFP+) Monitoring 3 Port	18) pether13 (RJ45) Monitoring 13 Port
9) pether4 (SFP+) Monitoring 4 Port	19) pether14 (RJ45) Monitoring 14 Port
10) pether5 (SFP+) Monitoring 5 Port	

Figure 11: FireEye NX4500 (Rear Panel)



1) USB 2.0 Ports	6) Information LED
2) Bezel Release	7) ether1 LED
3) Power Button	8) IPMI LED
4) HDD LED	9) Reset Button
5) Power LED	

Figure 12: FireEye NX5500 (Front Panel)



1) Power Port	11) pether6 (SFP+) Monitoring 6 Port
2) Serial Console Port	12) pether7 (SFP+) Monitoring 7 Port
3) Video Port	13) pether8 (SFP+) Monitoring 8 Port
4) pether2 (RJ45) Optional Dedicated Out-of-Band Blocking 2 Port	14) pether9 (SFP+) Monitoring 9 Port
5) ether1 (RJ45) Management 1 Port	15) pether10 (SFP+) Monitoring 10 Port
6) USB 3.0 Ports	16) Disabled Port
7) IPMI Port	17) pether11 (RJ45) Monitoring 11 Port
8) pether3 (SFP+) Monitoring 3 Port	18) pether12 (RJ45) Monitoring 12 Port
9) pether4 (SFP+) Monitoring 4 Port	19) pether13 (RJ45) Monitoring 13 Port
10) pether5 (SFP+) Monitoring 5 Port	20) pether14 (RJ45) Monitoring 14 Port

Figure 13: FireEye NX5500 (Rear Panel)



1) Power Button	5) Power Fail LED
2) Reset Button	6) HDD LED
3) Power LED	7) NIC LED
4) NIC LED	8) Information LED

Figure 14: FireEye NX6500 (Front Panel)



1) Power Port 1	11) pether4 (SFP+) Monitor/TAP/SPAN ports
2) Power Port 2	12) pether5 (SFP+) Monitor/TAP/SPAN ports
3) Disabled	13) pether6 (SFP+) Monitor/TAP/SPAN ports
4) ether1(RJ45)	14) pether7 (SFP+) Monitor/TAP/SPAN ports
5) pether2 (RJ45) Management 2 Port	15) pether8 (SFP+) Monitor/TAP/SPAN ports
6) USB 3.0 ports	16) pether9 (SFP+) Monitor/TAP/SPAN ports
7) IPMI 10/100/1Gbase-T port	17) pether10 (SFP+) Monitor/TAP/SPAN ports
8) Serial Console Port	18) pether11 (QSFP+) 40G Monitor/TAP/SPAN ports
9) Video Port	19) pether12 (QSFP+) 40G Monitor/TAP/SPAN ports
10) pether3 (SFP+) Monitor/TAP/SPAN ports	

Figure 15: FireEye NX6500 (Rear Panel)

## 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

FIPS Interface	Physical Interface
<b>Data Input</b>	10/100/1000 BASE-T Management Port (NX1500 (1x), NX2500 (1x), NX2550 (1x), NX3500 (1x), NX4500 (1x), NX5500 (1x)), NX6500 (2x)) 10/100/1000 BASE-T Monitoring Ports (NX1500 (5x), NX2500 (5x), NX2550 (5x), NX3500 (4x), NX4500 (5x), NX5500 (5x)) (1x) 10/100/1000 BASE-T IPMI Management Port (NX2550, NX3500, NX4500, NX5500, NX6500) SFP+ Ports (NX2550 (4x), NX3500 (4x), NX4500 (8x), NX5500 (8x), NX6500 (10x)) (2x) USB 2.0 Ports (2x) USB 3.0 Ports (NX2550, NX3500, NX4500, NX5500, NX6500) (1x) Serial Port
<b>Data Output</b>	10/100/1000 BASE-T Management Port (NX1500 (1x), NX2500 (1x), NX2550 (1x), NX3500 (1x), NX4500 (1x), NX5500 (1x)), NX6500 (2x)) 10/100/1000 BASE-T Monitoring Ports (NX1500 (5x), NX2500 (5x), NX2550 (5x), NX3500 (4x), NX4500 (5x), NX5500 (5x)) (1x) 10/100/1000 BASE-T IPMI Management Port (NX2550, NX3500, NX4500, NX5500, NX6500) SFP+ Ports (NX2550 (4x), NX3500 (4x), NX4500 (8x), NX5500 (8x), NX6500 (10x)) (2x) USB 2.0 Ports (2x) USB 3.0 Ports (NX2550, NX3500, NX4500, NX5500, NX6500) (1x) Video Port (NX2550, NX3500, NX4500, NX5500, NX6500) (1x) Serial Port
<b>Control Input</b>	10/100/1000 BASE-T Management Port (NX1500 (1x), NX2500 (1x), NX2550 (1x), NX3500 (1x), NX4500 (1x), NX5500 (1x)), NX6500 (2x)) (1x) 10/100/1000 BASE-T IPMI Management Port (NX2550, NX3500, NX4500, NX5500, NX6500) (2x) USB 2.0 Ports (2x) USB 3.0 Ports (NX2550, NX3500, NX4500, NX5500, NX6500) (1x) Serial Port (1x) Power Button/Switch (1x) Reset Button (NX2550, NX3500, NX4500, NX5500, NX6500)

<p><b>Status Output</b></p>	<p>10/100/1000 BASE-T Management Port (NX1500 (1x), NX2500 (1x), NX2550 (1x), NX3500 (1x), NX4500 (1x), NX5500 (1x)), NX6500 (2x))                  (1x) 10/100/1000 BASE-T IPMI Management Port (NX2550, NX3500, NX4500, NX5500, NX6500)                  (2x) USB 2.0 Ports                  (2x) USB 3.0 Ports (NX2550, NX3500, NX4500, NX5500, NX6500)                  (1x) Serial Port                  (1x) Video Port (NX2550, NX3500, NX4500, NX5500, NX6500)                  LEDs (NX1500 (2x), NX2500 (2x), NX2550 (5x), NX3500 (5x), NX4500 (5x), NX5500 (5x), NX6500 (6x))</p>
<p><b>Power Interface</b></p>	<p>Power Port (NX1500 (1x), NX2500 (1x), NX2550 (1x), NX3500 (2x), NX4500 (2x), NX5500 (2x), NX6500 (2x))</p>

### 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. 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:** 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	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 an American QWERTY computer keyboard. Thus,
Monitor		
Operator		
Analyst		

Role	Type Of Authentication	Authentication Strength
<b>Auditor</b>		<p>the probability of a successful random attempt is <math>1/94^8</math>, 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 <math>10^8 = 100,000,000</math>). 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.</p> <p>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 <math>15/(94^8)</math> (or <math>15/(10^8)</math> in the worst case), which is less than <math>1/1,000,000</math>.</p>
<b>SNMP</b>		
<b>WSAPI</b>		
<b>User</b>	Password/Username or Asymmetric Authentication	<p>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 <math>1/94^8</math>, 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 <math>10^8 = 100,000,000</math>).</p>



Role	Type Of Authentication	Authentication Strength
		<p>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.</p> <p>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 <math>15/(94^8)</math> (or <math>15/(10^8)</math> in the worst case), which is less than 1/1,000,000.</p> <p>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 <math>2^{112}</math> chance of randomly obtaining the key, which is much stronger than the one in a million chance, required by FIPS 140-2.</p> <p>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 <math>5.19 \times 10^{28}</math> attempts per minute. In the worst-case scenario, an operator can make 60 failed attempts per minute.</p>

### 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
<b>SSH to external IT device</b>	Secure SSH connection between a CM and other FireEye appliances using SSH.	User	<ul style="list-style-type: none"> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> <li>• SSH Private Key (R/W/Z)</li> <li>• SSH Public Key (R/W/Z)</li> <li>• SSH Session Key (R/W/Z)</li> <li>• SSH Integrity Key (R/W/Z)</li> </ul>
<b>Administrative access over SSH</b>	Secure remote command line appliance administration over an SSH tunnel.	CO	<ul style="list-style-type: none"> <li>• Admin Password (R/W/Z)</li> <li>• Monitor Password (R/W/Z)</li> <li>• Operator Password (R/W/Z)</li> <li>• Analyst Password (R/W/Z)</li> <li>• Auditor Password (R/W/Z)</li> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> <li>• SSH Private Key (R/W/Z)</li> <li>• SSH Public Key (R/W/Z)</li> <li>• SSH Session Key (R/W/Z)</li> <li>• SSH Integrity Key (R/W/Z)</li> </ul>
<b>Administrative access over webGUI</b>	Secure remote GUI appliance administration over a TLS tunnel.	CO	<ul style="list-style-type: none"> <li>• Admin Password (R/W/Z)</li> <li>• Monitor Password (R/W/Z)</li> <li>• Operator Password (R/W/Z)</li> <li>• Analyst Password (R/W/Z)</li> <li>• Auditor Password (R/W/Z)</li> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> </ul>

Service	Description	Role	Key/CSP and Type of Access
			<ul style="list-style-type: none"> <li>• TLS Private Key (R/W/Z)</li> <li>• TLS Public Key (R/W/Z)</li> <li>• TLS Pre-Master Secret (R/W/Z)</li> <li>• TLS Master Secret (R/W/Z)</li> <li>• TLS Session Encryption Key (R/W/Z)</li> <li>• TLS Session Integrity Key (R/W/Z)</li> </ul>
<b>Administrative access over WSAPI</b>	Secure remote appliance administration over a TLS tunnel.	CO	<ul style="list-style-type: none"> <li>• WSAPI Password (R/W/Z)</li> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> <li>• TLS Private Key (R/W/Z)</li> <li>• TLS Public Key (R/W/Z)</li> <li>• TLS Pre-Master Secret (R/W/Z)</li> <li>• TLS Master Secret (R/W/Z)</li> <li>• TLS Session Encryption Key (R/W/Z)</li> <li>• TLS Session Integrity Key (R/W/Z)</li> </ul>
<b>Administrative access over serial console and VGA</b>	Directly connected command line appliance administration.	CO	<ul style="list-style-type: none"> <li>• Admin Password (R/W/Z)</li> <li>• Monitor Password (R/W/Z)</li> <li>• Operator Password (R/W/Z)</li> <li>• Analyst Password (R/W/Z)</li> <li>• Auditor Password (R/W/Z)</li> </ul>
<b>SNMPv3</b>	Secure remote SNMPv3-based system monitoring.	CO	<ul style="list-style-type: none"> <li>• SNMP Session Key (R/W/Z)</li> <li>• SNMPv3 password (R/W/Z)</li> </ul>
<b>DTI connection</b>	TLS-based connection used to upload data to the FireEye cloud.	User	<ul style="list-style-type: none"> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> <li>• TLS Private Key (R/W/Z)</li> <li>• TLS Public Key (R/W/Z)</li> <li>• TLS Pre-Master Secret (R/W/Z)</li> <li>• TLS Master Secret (R/W/Z)</li> <li>• TLS Session Encryption Key (R/W/Z)</li> </ul>

Service	Description	Role	Key/CSP and Type of Access
			<ul style="list-style-type: none"> <li>• TLS Session Integrity Key (R/W/Z)</li> </ul>
<b>LDAP over TLS</b>	Secure remote authentication via TLS protected LDAP	User	<ul style="list-style-type: none"> <li>• Admin Password (R/W/Z)</li> <li>• Monitor Password (R/W/Z)</li> <li>• Operator Password (R/W/Z)</li> <li>• Analyst Password (R/W/Z)</li> <li>• Auditor Password (R/W/Z)</li> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> <li>• TLS Private Key (R/W/Z)</li> <li>• TLS Public Key (R/W/Z)</li> <li>• TLS Pre-Master Secret (R/W/Z)</li> <li>• TLS Master Secret (R/W/Z)</li> <li>• TLS Session Encryption Key (R/W/Z)</li> <li>• TLS Session Integrity Key (R/W/Z)</li> </ul>
<b>SAML over TLS (Web GUI)</b>	Secure remote authentication to the Web GUI via TLS protected SAML	User	<ul style="list-style-type: none"> <li>• Admin Password (R/W/Z)</li> <li>• Monitor Password (R/W/Z)</li> <li>• Operator Password (R/W/Z)</li> <li>• Analyst Password (R/W/Z)</li> <li>• Auditor Password (R/W/Z)</li> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> <li>• TLS Private Key (R/W/Z)</li> <li>• TLS Public Key (R/W/Z)</li> <li>• TLS Pre-Master Secret (R/W/Z)</li> <li>• TLS Master Secret (R/W/Z)</li> <li>• TLS Session Encryption Key (R/W/Z)</li> <li>• TLS Session Integrity Key (R/W/Z)</li> </ul>
<b>Secure log transfer</b>	TLS-based connection with a remote audit server.	User	<ul style="list-style-type: none"> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> </ul>

Service	Description	Role	Key/CSP and Type of Access
			<ul style="list-style-type: none"> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> <li>• TLS Private Key (R/W/Z)</li> <li>• TLS Public Key (R/W/Z)</li> <li>• TLS Pre-Master Secret (R/W/Z)</li> <li>• TLS Master Secret (R/W/Z)</li> <li>• TLS Session Encryption Key (R/W/Z)</li> <li>• TLS Session Integrity Key (R/W/Z)</li> </ul>
<b>TLS to external IT device</b>	Secure connection between a CM and other FireEye appliances using TLS.	User	<ul style="list-style-type: none"> <li>• DRBG entropy input (W/R)</li> <li>• DRBG Seed (W/R)</li> <li>• DRBG V (R/W/Z)</li> <li>• DRBG Key (R/W/Z)</li> <li>• Diffie-Hellman Shared Secret (R/W/Z)</li> <li>• Diffie Hellman private key (R/W/Z)</li> <li>• Diffie Hellman public key (R/W/Z)</li> <li>• TLS Private Key (R/W/Z)</li> <li>• TLS Public Key (R/W/Z)</li> <li>• TLS Pre-Master Secret (R/W/Z)</li> <li>• TLS Master Secret (R/W/Z)</li> <li>• TLS Session Encryption Key (R/W/Z)</li> </ul>
<b>Show Status</b>	View the operational status of the module	CO	N/A
<b>Perform Self-Tests</b>	Perform the FIPS 140 start-up tests on demand	CO	N/A
<b>Status LED Output</b>	View status via the Modules LEDs.	Un-auth	N/A
<b>Cycle Power</b>	Reboot of appliance.	Un-auth	<ul style="list-style-type: none"> <li>• DRBG entropy input (Z)</li> <li>• DRBG Seed (Z)</li> <li>• DRBG V (Z)</li> <li>• DRBG Key (Z)</li> <li>• Diffie-Hellman Shared Secret (Z)</li> <li>• Diffie Hellman private key (Z)</li> <li>• Diffie Hellman public key (Z)</li> <li>• SSH Session Key (Z)</li> <li>• SSH Integrity Key (Z)</li> <li>• SNMPv3 session key (Z)</li> <li>• TLS Pre-Master Secret (Z)</li> </ul>

Service	Description	Role	Key/CSP and Type of Access
			<ul style="list-style-type: none"> <li>• TLS Master Secret (Z)</li> <li>• TLS Session Encryption Key (Z)</li> <li>• TLS Session Integrity Key (Z)</li> </ul>
<b>Zeroization via “compliance declassify zeroize” Command</b>	Perform zeroization of all persistent CSPs within the module	CO	<ul style="list-style-type: none"> <li>• Admin Password (Z)</li> <li>• Monitor Password (Z)</li> <li>• Operator Password (Z)</li> <li>• Analyst Password (Z)</li> <li>• Auditor Password (Z)</li> <li>• WSAPI Password (Z)</li> <li>• SSH Private Key (Z)</li> <li>• SSH Public Key (Z)</li> <li>• SNMPv3 password (Z)</li> <li>• TLS Private Key (Z)</li> <li>• TLS Public Key (Z)</li> </ul>

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
<b>DRBG entropy input</b>	CTR 256-bit,HMAC-SHA-512	This is the entropy for SP 800-90 RNG.	DRAM	Device power cycle.
<b>DRBG Seed</b>	CTR 256-bit, HMAC-SHA-512	Seed material used to seed or reseed the DRBG.	DRAM	Device power cycle.
<b>DRBG V</b>	CTR 256-bit, HMAC-SHA-512	Internal V value used as part of SP 800-90 CTR_DRBG, HMAC_DRBG.	DRAM	Device power cycle.
<b>DRBG Key</b>	CTR 256-bit, HMAC-SHA-512	Internal Key value used as part of SP 800-90 CTR_DRBG, HMAC_DRBG.	DRAM	Device power cycle.
<b>Diffie-Hellman Shared Secret</b>	DH 2048 – 4096 bits	The shared exponent used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	DRAM	Device power cycle.
<b>Diffie Hellman private key</b>	DH (DSA) 2048 – 4096 bits	The private exponent used in Diffie-Hellman (DH) exchange.	DRAM	Device power cycle.
<b>Diffie Hellman public key</b>	DH 2048 – 4096 bits	The p used in Diffie-Hellman (DH) exchange.	DRAM	Device power cycle.
<b>EC Diffie-Hellman Shared Secret</b>	ECDH P-256, P-384, P-521	The shared secret used in the EC Diffie-Hellman (ECDH) exchange.	DRAM	Device power cycle.
<b>EC Diffie Hellman private key</b>	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
<b>EC Diffie Hellman public key</b>	ECDH P-256, P-384, P-521	The public key used in EC Diffie-Hellman (DH) exchange.	DRAM	Device power cycle.
<b>SSH Private Key</b>	RSA (Private Key) 2048 – 3072 bits	The SSH private key for the module used for session authentication.	NVRAM	Overwritten w/ “00” prior to replacement.
<b>SSH Public Key</b>	RSA (Public Key) 2048 – 3072 bits	The SSH public key for the module used for session authentication.	NVRAM	Overwritten w/ “00” prior to replacement.
<b>SSH Session Key</b>	AES 128, 256 bits	The SSH session key. This key is created through SSH key establishment.	DRAM	Device power cycle.
<b>SSH Integrity Key</b>	HMAC-SHA1, HMAC-SHA-256 HMAC-512	The SSH data integrity key. This key is created through SSH key establishment.	DRAM	Device power cycle.
<b>SNMPv3 password</b>	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.
<b>SNMPv3 session key</b>	AES 128 bits	SNMP symmetric encryption key used to encrypt/decrypt SNMP traffic.	DRAM	Device power cycle.
<b>TLS Private Key</b>	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.
<b>TLS Public Key</b>	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.
<b>TLS Pre-Master Secret</b>	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
<b>TLS Master Secret</b>	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.
<b>TLS Session Encryption Key</b>	Triple-DES 192-bits	Key used to encrypt/decrypt TLS session data.	DRAM	Device power cycle.
	AES 128, 256 bits			
<b>TLS Session Integrity Key</b>	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384	HMAC-SHA used for TLS data integrity protection.	DRAM	Device power cycle.
<b>Admin Password</b>	Shared Secret, 8+ characters	Authentication password for the Admin user role.	NVRAM	Overwritten w/ "00" prior to replacement.
<b>Monitor Password</b>	Shared Secret, 8+ characters	Authentication password for the Monitor user role.	NVRAM	Overwritten w/ "00" prior to replacement.
<b>Operator Password</b>	Shared Secret, 8+ characters	Authentication password for the Operator user role.	NVRAM	Overwritten w/ "00" prior to replacement.
<b>Analyst Password</b>	Shared Secret, 8+ characters	Authentication password for the Analyst user role.	NVRAM	Overwritten w/ "00" prior to replacement.
<b>Auditor Password</b>	Shared Secret, 8+ characters	Authentication password for the Audit user role.	NVRAM	Overwritten w/ "00" prior to replacement.
<b>WSAPI Password</b>	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
<b>Triple-DES<sup>1</sup></b>	C1720	<b>TECB</b> (KO 1 e/d), <b>TCBC</b> (KO 1 e/d)  <b>KTS</b> 112-bits (paired with HMAC Cert. #C1720)  Per SP800-67 rev2, the user is responsible for ensuring the module’s limit to 2 <sup>20</sup> encryptions with the same Triple-DES key while being used in the TLS protocol	Used for encryption of TLS sessions.
		<b>TCFB1</b> (KO 1 e/d); <b>TCFB8</b> (KO 1 e/d); <b>TCFB64</b> (KO 1 e/d); <b>TOFB</b> (KO 1 e/d)	Implemented within the module however never used by any service
<b>AES</b>	C1720	<b>ECB</b> (e/d 128, 256); <b>CBC</b> (e/d 128, 256); <b>OFB</b> (e/d 128); <b>CTR</b> (ext only; 128, 256 )  <b>GCM<sup>2</sup></b> ( <b>KS: AES_128</b> ( e/d ) Tag Length(s): 128 120 112 104 96 64 32 ) ( <b>KS: AES_256</b> ( e/d ) Tag Length(s): 128 120 112 104 96 64 32 ) <b>IV Generated:</b> ( Internal (using Section 8.2.1 ) ) <b>; PT Lengths Tested:</b> ( 0 , 1024 ) ; <b>AAD Lengths tested:</b> ( 1024 ) <b>; 96BitIV_Supported GMAC_Supported</b>	Used for encryption of SSH, SNMP, and TLS sessions. Used in support of FIPS-approved DRBG.

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

<sup>2</sup> 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<sup>64</sup> – 1, the next AES GCM encryption is performed with the invocation counter set to either 0 or 1, with a maximum of 2<sup>64</sup> – 1 encryptions per session.

		<p><b>KTS 128, 256-bits (paired with HMAC Cert. # C1720)</b></p> <p>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.</p>	
		<p><b>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)</b></p> <p><b>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 )</b></p> <p><b>GCM (KS: AES_192( e/d ) Tag Length(s): 128 120 112 104 96 64 32 )</b></p>	<p>Implemented within the module however never used by any service</p>
<b>HMAC-SHS</b>	C1720	<p><b>HMAC-SHA1 (Key Sizes Ranges Tested:KS=BS, KS&gt; BS, KS &lt; BS)</b></p> <p><b>HMAC-SHA256 ( Key Size Ranges Tested: KS=BS, KS&gt; BS, KS &lt; BS)</b></p> <p><b>HMAC-SHA384 ( Key Size Ranges Tested: KS=BS, KS&gt; BS, KS &lt; BS)</b></p> <p><b>HMAC-SHA512 ( Key Size Ranges Tested: KS=BS, KS&gt; BS, KS &lt; BS)</b></p> <p><b>KTS HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 (paired with either AES cert. #C1720 or Triple-DES Cert. # C1720)</b></p>	<p>Used for SSH and TLS traffic integrity. Used in support of SSH, SNMP, and TLS key derivation.</p>
		<p><b>HMAC-SHA224 ( Key Size Ranges Tested: KS=BS, KS&gt; BS, KS &lt; BS)</b></p>	<p>Implemented within the module however never used by any service</p>
	C1934	<p><b>HMAC-SHA1 (Key Sizes Ranges Tested:KS=BS, KS&gt; BS, KS &lt; BS)</b></p> <p><b>HMAC-SHA256 ( Key Size Ranges Tested: KS=BS, KS&gt; BS, KS &lt; BS)</b></p> <p><b>HMAC-SHA384 ( Key Size Ranges Tested: KS=BS, KS&gt; BS, KS &lt; BS)</b></p> <p><b>HMAC-SHA512 ( Key Size Ranges Tested: KS=BS, KS&gt; BS, KS &lt; BS)</b></p>	<p>Used in support of random bit generation.</p>

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

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

### 2.6.2 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.

### 2.6.3 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

## **2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)**

All NX 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 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)

### 2.8.2 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

## FIPS 140-2 Security Policy

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 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 9.0.3, 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.

#### 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.

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. 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 must 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
<b>CMVP</b>	Cryptographic Module Validation Program
<b>CRNGT</b>	Continuous Random Number Generator Test
<b>CVL</b>	Component Validation List
<b>FIPS</b>	Federal Information Processing Standard
<b>KDF</b>	Key Derivation Function
<b>NIST</b>	National Institute of Standards and Technology
<b>NVRAM</b>	Non-Volatile Random Access Memory
<b>POST</b>	Power-On Self-Test
<b>PWCT</b>	Pairwise Consistency Test