Network Security Platform Sensor NS3500

FIPS 140-2 Non-Proprietary Security Policy

Firmware Version 10.1.17.1

Date: January 12, 2021

McAfee, LLC
6220 America Center Drive
San Jose, CA 95002
888.847.8766
http://www.mcafee.com

Table of Contents

1 Module Overview

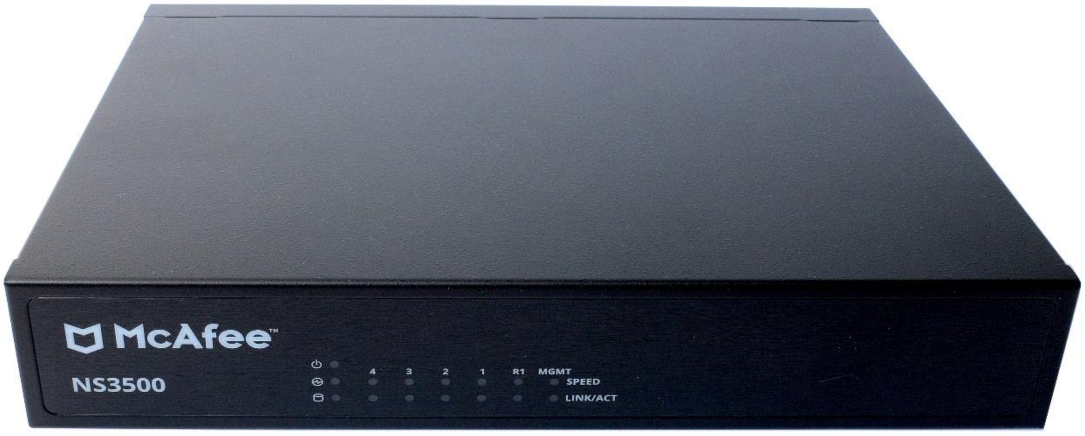
The Network Security Platform Sensor NS3500 (H/W P/N IPS-NS3500 Version 1.10 and FW Version 10.1.17.1) is a multi-chip standalone cryptographic module as defined in FIPS 140-2.

The NS3500 is an Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) designed for network protection against zero-day, DoS/DDoS, encrypted and SYN Flood attacks, and real-time prevention of threats like spyware, malware, VoIP vulnerabilities, phishing, botnets, network worms, Trojans, and peer-to-peer applications. The NSP Sensors connect with the Network Security Manager (NSM). The NSM is used to manage and push configuration data and policies to the Sensors. Communication between NSM and Sensors uses secure channels that protect the traffic from disclosure and modification. Authorized administrators may access the NSM via a GUI (over HTTPS) or a CLI (via SSH or a local connection). Sensors may be accessed via CLI (via SSH or a local connection) for initial setup. Once initial setup is complete, all management occurs via the NSM.

The cryptographic boundary of each platform is the outer perimeter of the enclosure, excluding the removable power supplies, as they are non-security relevant. The removable fan trays are protected by tamper seals.

Figure 1 shows the module configuration and the cryptographic boundary.

Figure 1 – Images of NS3500



2 Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2. Table 1 specifies the levels met for specific FIPS 140-2 areas.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Mode of Operation

3.1 FIPS Approved Mode of Operation

The module only supports a FIPS Approved mode of operation. An operator can obtain the FIPS mode indicator by executing the "show" or "status" CLI command, which returns the module's firmware version, HW version, etc. The firmware and hardware versions must match the FIPS validated versions located on the CMVP website.

The operator must also follow the rules outlined in Sections 8 and 9 of this Security Policy and consult FIPS 140-2 IG 1.23 for further understanding of the use of functions where no security is claimed. **Approved Algorithms**

The module supports the following FIPS Approved algorithms:

- AES CBC and ECB mode with 128 & 256 bits for encryption and decryption (Cert. #C1556)

  (Note: CBC mode is tested but not used.)
- AES GCM mode with 128 bits for encryption and decryption use within TLS 1.2 (Cert. #C1556)
- AES GCM mode with 128 & 256 bits for encryption and decryption use within SSH v2 (Cert. #C1556)
- KTS AES (Cert. #C1556) encryption to transport keys and authentication using HMAC (Cert. #C1556) within TLS 1.2 and SSH
- KTS AES (Cert. #C1556) encryption to transport keys and authentication using GCM (Cert. #C1556) within TLS 1.2 and SSH
- FIPS 186-4 RSA with 2048-bit keys for key generation and RSA PSS with 2048-bit keys for signature generation with SHA-256, and signature verification with SHA-256 (Cert. #C1556)
- SHA-1, SHA-256, SHA-384 and SHA-512 for hashing (Cert. #C1556)
- HMAC SHA-256 and HMAC SHA-512 for message authentication (Cert. #C1556)

  (Note: The minimum HMAC key size is 20 bytes. HMAC SHA-1 and HMAC SHA-384 were CAVP tested but are not used.)
- Block Cipher (CTR) DRBG using AES 256 (Cert. #C1556)
- KAS-SSC (vendor affirmed)
- ECDSA Key Generation and Key Verification using P-256, P-384 and P-521 (Cert. #C1556)
- FIPS 186-4 XYSSL RSA PKCS #1 V1.5 SigVer with 2048 bit keys using SHA-256 for image verification (Cert. #C1555)

  (Note: SHA-1 is CAVP tested but not used.)
- XYSSL SHA-256 for hashing and for use with image verification (Cert. #C1555)

  (Note: SHA-1 is CAVP tested but not used.)
- TLS v1.2 KDF for TLS session key derivation CVL (Cert. #C1558)
- SSH KDF for SSH session key derivation CVL (Cert. #C1557)
- SP 800-133 CKG (Vendor Affirmed)
  - Asymmetric Key Generation (SP 800-133 § 5)
  - Symmetric Key Generation (SP 800-133 § 6)

(Note: The resulting symmetric keys and generated seeds are unmodified output from the DRBG)

Allowed Algorithms

The module supports the following FIPS allowed algorithms and protocols:

- RSA with 2048-bit keys for (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (internal entropy source) for seeding the Block Cipher (CTR) DRBG. The module generates a minimum of 256 bits of entropy for key generation.

Protocols

- TLS v1.2 with the following algorithm tested cipher suites. The protocol algorithms have been tested by the CAVP (see certificate #s above) but no parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 for communication with Network Security Manager (NSM)
    (Note: This is restricted to RSA-2048)
- SSH v2 with the following algorithm tested cipher suites. The protocol algorithms have been tested by the CAVP (see certificate #s above) but no parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.
  - Key Exchange methods (i.e., key establishment methods): EC Diffie-hellman-256-SHA2
  - Public Key methods (i.e., authentication methods): SSH-ECDSA
    (Note: This is restricted to ECDSA P-256)
  - Encryption methods: AES128-GCM, AES256-GCM
  - MAC methods: HMAC-256, HMAC-512

AES GCM is used as part of TLS 1.2 cipher suite conformant to IG A.5 Scenario 1, RFC 5288 and SP 800-52 Rev2 Section 3.3.1. The construction of the 64-bit nonce_explicit part of the IV is deterministic via a monotonically increasing counter. The module ensures that that when the deterministic part of the IV uses the maximum number of possible values and new session key is established. The module generates new AES-GCM keys if the module loses power.
AES GCM is also used as part of the SSHv2 cipher suites conformant to the IG A.5 Scenario 1 and RFCs 4252, 4253 and RFC 5647. The GCM re-key limit is set to 1 hour or 1 GB of payload traffic set as the threshold. Therefore, the invocation counter maximum of $2^{64} – 1$ is never reached nor are that many encryptions performed in a single session. When a session is terminated for any reason, a new key and new initial IV shall be derived.

Non-Approved Algorithms and Protocols with No Security Claimed

The module supports the following algorithms and protocols in the Approved mode for which no security is claimed (per FIPS IG 1.23):

- MD5 used to identify “fingerprint” of potential malware using Global Threat Information (GTI) database (used internal to the module only). Non-Approved algorithms (no security claimed): MD5

- SNMPv3 is used as a transport mechanism between the NSM and the sensor with no security claimed. All non-CSP content is transported within SNMPv3. All CSP content is additionally encrypted by NSM and decrypted in sensor using the sensor TLS private key. In addition, the SNMPv3 protocol between NSM and Sensor is encapsulated within TLS when adopting CA-signing is turned on (TLS–ECDHE-RSA-AES128_GCM-SHA256). Non-Approved algorithms (no security claimed): HMAC (non-compliant), SHA (non-compliant), AES (non-compliant) and SNMP KDF (non-compliant).
- SNMPv3 is used as a Read Only connection and responses to non CSP objects for 3rd Part Clients with no security claimed.
- The following algorithms are implemented independently from all other cryptographic code in the module and are used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. For the reasoning stated above, this functionality is allowed in the FIPS Approved mode of operation.
    - Decryption - SSLv2
        - Cipher suites:
            - SSL_CK_RC4_128_WITH_MD5
            - SSL_CK_RC4_128_EXPORT40_WITH_MD5
            - SSL_CK_DES_64_CBC_WITH_MD5
            - SSL_CK_DES_192_EDE3_CBC_WITH_MD5
        - Non-Approved algorithms: Triple-DES (non-compliant), HMAC (non-compliant), RC4, MD5, DES
    - Decryption - SSLv3/TLS
        - Cipher suites:
            - SSL/TLS_NULL_WITH_NULL_NULL
            - SSL/TLS_RSA_WITH_NULL_MD5
            - SSL/TLS_RSA_WITH_NULL_SHA
            - SSL/TLS_RSA_WITH_RC4_128_MD5
            - SSL/TLS_RSA_WITH_RC4_128_SHA
            - SSL/TLS_RSA_WITH_DES_CBC_SHA
            - SSL/TLS_RSA_WITH_3DES_EDE_CBC_SHA
            - SSL/TLS_RSA_WITH_AES_128_CBC_SHA
            - SSL/TLS_RSA_WITH_AES_256_CBC_SHA
        - Non-Approved algorithms (no security claimed): AES (non-compliant), RSA (non-compliant), SHA (non-compliant), Triple-DES (non-compliant), HMAC (non-compliant), RC4, MD5, DES

4 Ports and Interfaces

Figures 2 and 3 show the modules' front and rear panels and Tables 2 and 3 list the modules' ports and interfaces.

Figure 2 – NS3500 Front Panel

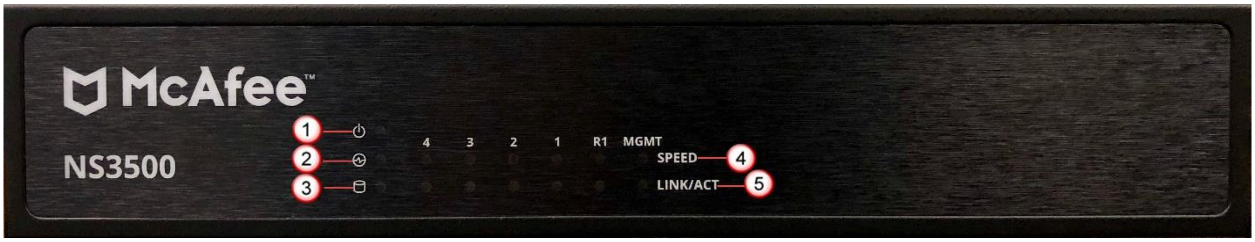


Table 2 – NS3500 Front Panel Ports and Connectors

Item	Description	Input/Output Type
1	Power LED	Status Output
2	Status LED	Status Output
3	Compact Flash Memory LED	Status Output
4	Speed LED for each ethernet port	Status Output
5	Link LED for each ethernet port	Status Output

Figure 3 – NS3500 Rear Panel

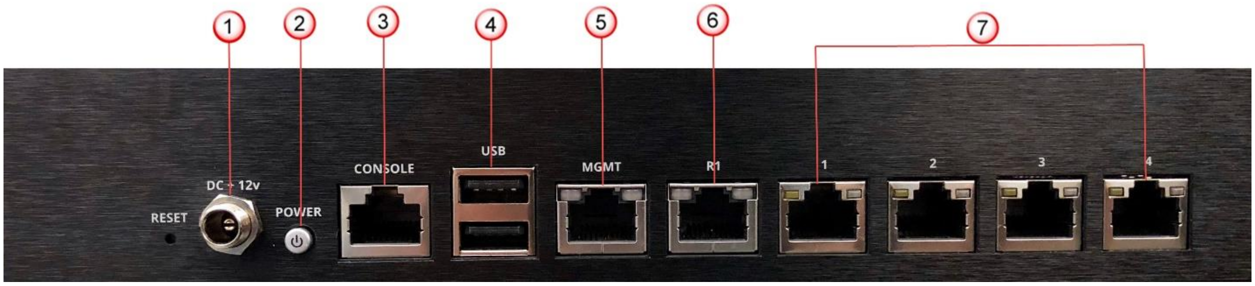


Table 3 – NS3500 Rear Panel Ports and Connectors

Item	Description	Input/Output Type
1	Power Port (2) –(12V DC IN)	Power Input
2	Power Switch	Control Input
3	RJ-45 Console Port (1)	Control Input, Status Output
4	USB ports (2)	Data Input
5	RJ-45 10/100/1000 Management port (MGMT) (1)	Control Input, Data Output, Status Output
6	RJ-45 10/100/1000 Response port (R1) (1 -currently not supported)	N/A
7	RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (4)	Data Input/Output

The module supports the following communication channels with the Network Security Platform (NSP) Manager:

- Install channel: Only used to associate a Sensor with the NSM. They use a "shared secret". NSM listening on port 8501 (Self-signed certificates) or port 8506 (CA signed certificates).
- Trusted Alert/Control channel (TLS): NSM listening on port 8502 (Self-signed certificates) or port 8507 (CA signed certificates).
- Trusted Packet log channel (TLS): NSM listening on port 8503 (Self-signed certificates)

or port 8508 (CA signed certificates).

- Command channel (SNMPv3, plaintext): Sensor listening to NSM and 3rd Party SNMP clients on port 8500 (Self-signed certificates).
- Command channel (TLS): Sensor listening to NSM SNMPv3 client encapsulated in TLS on port 18500 (CA signed certificates).
- Bulk transfer channel (encrypted): NSM listening on port 8504 (CA signed certificates)
- Bulk transfer channel (TLS): NSM listening on port 8509
- Trusted Authentication Gateway channel (TLS): uses same crypto context as Alert/Control channel. NSM listening on port 8502 (Self-signed certificates) or port 8507 (CA signed certificates).

5 Identification and Authentication Policy

The cryptographic module supports three (3) distinct "User" roles (Admin, Sensor Operator(s), and 3rd Party SNMP Client(s)) and one (1) "Cryptographic Officer" role (Network Security Platform Manager). Table 4 lists the supported operator roles along with their required identification and authentication techniques. Table 5 outlines each authentication mechanism and the associated strengths.

Table 4 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin	Role-based operator authentication	Username and Password
Sensor Operator(s)	Role-based operator authentication	Username and Password
Network Security Platform Manager (Cryptographic Officer)	Role-based operator authentication	Digital Signature or Username, Privacy and Authentication Key
3rd Party SNMP Client(s)	Role-based operator authentication	Username, Privacy and Authentication key

Table 5 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The password is an alphanumeric string of a minimum of fifteen (15) characters chosen from the set of ninety-three (93) printable and human-readable characters. Whitespace and "?" are not allowed. New passwords are required to include two (2) uppercase characters, two (2) lowercase characters, two (2) numeric characters, and two (2) special characters. The fifteen (15) character minimum is enforced by the module. The probability that a random attempt will succeed or a false acceptance will occur is 1/{(10^2)*(26^4)*(31^2)*(93^7)} which is less than 1/1,000,000. After three (3) consecutive failed authentication attempts, the module will enforce a one (1) minute delay prior to allowing retry. Additionally, the module only supports five (5) concurrent SSH sessions. Thus, the probability of successfully authenticating to the module within one minute through random attempts is (3*5)/{(10^2)*(26^4)*(31^2)*(93^7)}, which is less than 1/100,000.

Authentication Mechanism	**Strength of Mechanism**
Digital Signature	RSA 2048-bit keys using SHA-256 are used for the signing (in isolated McAfee laboratory or by Certificate Authority (CA)) and verification (by sensor) of digital signatures. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^112, which is less than 1/1,000,000. The module can only perform one (1) digital signature verification per second. The probability of successfully authenticating to the module within one minute through random attempts is 60/2^112, which is less than 1/100,000.
Username, Privacy and Authentication key	The privacy key and authentication key together make an alphanumeric string of a minimum of sixteen (16) characters chosen from the set of sixty-two (62) numbers, lower case letters, and upper case letters. The probability that a random attempt will succeed or a false acceptance will occur is 1/62^16, which is less than 1/1,000,000. The module will allow approximately one (1) attempt per millisecond, meaning that 60,000 attempts can be made per minute. The probability of successfully authenticating to the module within one minute through random attempts is 60,000/62^16, which is less than 1/100,000.

6 Access Control Policy

6.1 Roles and Services

Table 6 lists each operator role and the services authorized for each role.

For additional information of operation of the module, NSP documentation is at docs.mcafee.com:

1. Go to McAfee Documentation Portal (https://docs.mcafee.com/).
2. Scroll to the **Products A-Z** section at the bottom of the landing page (do not select Network Security Platform via the pull-down menu).
3. Click **Network Security Platform**. The NSP documentation list displays.
4. Using the **Product** filter in the left pane, click **NSP 10.1.x** to display a list of NSP 10.1 documentation.

Table 6 – Services Authorized for Roles

Authorized Services	Admin	Sensor Operator(s)	NSP Manager	3rd Party SNMP Client(s)
Show Status: Provides the status of the module, usage statistics, log data, and alerts.	X	X	X	
Sensor Operator Management: Allows Admin to add/delete Sensor Operators, set their service authorization level, set their session timeout limit, and unlock them if needed.	X			
Network Configuration: Establish network settings for the module or set them back to default values.	X	X*	X	
Administrative Configuration: Other various services provided for admin, private, and support levels.	X	X*	X	
Firmware Update: Install an external firmware image through SCP or USB.	X	X*	X	
Install with NSM: Configures module for use. This step includes establishing trust between the module and the associated management station.	X	X*		
Install with 3rd Party SNMP Client: Configures module for 3rd Party SNMPv3 use. This step includes establishing trust between the module and the associated 3rd Party SNMP Client. Trust is provided by NSM.			X	
Change Passwords: Allows Admin and Sensor Operators to change their associated passwords. Admin can also change/reset Sensor Operators passwords.	X	X*		

Zeroize: Destroys all plaintext secrets contained within the module. The “Reset Config” command is used, followed by a reboot.	X	X*		
Intrusion Detection/Prevention Management: Management of intrusion detection/prevention policies and configurations through SNMPv3 and TLS.			X	
Intrusion Detection/Prevention Monitoring: Limited monitoring of Intrusion Detection/Prevention configuration, status, and statistics through SNMPv3.			X	X
Disable SSH/Console Access: Disables SSH/Console access.	X	X*		

* Depending on the authorization level granted by the Admin

<u>Unauthenticated Services:</u>

Table 7 lists the unauthenticated services supported by the module.

Table 7 – Unauthenticated Services

Unauthenticated Services
Self-Tests: This service executes the suite of self-tests required by FIPS 140-2. Self-tests can be initiated by power cycling the module or through the CLI.
Intrusion Prevention Services: Offers protection against zero-day, DoS/DDoS, encrypted and SYN Flood attacks, and real-time prevention of threats like spyware, malware, VoIP vulnerabilities, phishing, botnets, network worms, Trojans, and peer-to-peer applications. *Note:* This service utilizes the no security claimed algorithms listed above. This includes an MD5 hash to identify the “fingerprint” of malware and decryption of SSL-encrypted streams for the purpose of detecting malware and network attacks. See the list above.
Zeroize: Destroys all plaintext secrets contained within the module. The Internal Rescue process is used.

6.2 Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- **Administrator Passwords**: Password used for authentication of the “admin” role through Console and SSH login. Extended permissions are given to the “admin” role by using the “support” or “private” passwords.
- **Sensor Operator Passwords**: Passwords used for authentication of “user” accounts through Console and SSH login. Extended permissions are given to the “user” account by using the “support” or “private” passwords.
- **NSM Initialization Secret (i.e., NSM Shared Secret)**: Password used for mutual authentication of the sensor and NSM during initialization.
- **Bulk Transfer Channel Session Key**: AES 128-bit key used to encrypt data packages across the bulk transfer channel.

- **SSH Host Private Keys**: ECDSA P-256-bit key used for authentication of sensor to remote terminal for CLI access, generated during initialization
- **SSH Session Keys**: Set of ephemeral EC Diffie-Hellman P-256, AES 128/256 bit, and HMAC (SHA-256/512) keys created for each SSH session.
- **TLS Sensor Private Key (for NSM)**: RSA 2048-bit key used for authentication of the sensor to NSM.
- **TLS Session Keys (for NSM)**: Set of ephemeral EC Diffie Hellman P-256, P-384 or P-521, AES 128 bit and HMAC (SHA-256bit) keys created for each TLS session with the NSM.
- **Entropy Input String:** 8192-bit input string from the hardware NDRNG.
- **Seed for DRBG**: 384-bit seed created by NDRNG and used to seed the Block Cipher (CTR) DRBG.
- **DRBG Internal State:** *V* and *Key* used by the DRBG to generate pseudo-random numbers.

(Note: The SNMP authentication data is not considered to be a CSP since the SNMP connection is tunneled within TLS)

6.3 Definition of Public Keys

The following are the public keys contained in the module:

- **McAfee FW Verification Key**: RSA 2048 bit key used to authenticate firmware images loaded into the module.
- **SSH Session Public Key:** EC Diffie-Hellman P-256 session key created for each SSH session
- **SSH Host Public Key**: ECDSA P-256 bit key used to authenticate the sensor to the remote client during SSH.
- **SSH Remote Client Public Key**: ECDSA P-256 bit key used to authenticate the remote client to the sensor during SSH.
- **TLS Sensor Public Key (for NSM):** RSA 2048 bit key used to authenticate the sensor to NSM during TLS connections.
- **TLS NSM Public Key**: RSA 2048 bit key used to authenticate NSM to sensor during TLS connections.
- **TLS Session Public Key:** EC Diffie-Hellman P-256, P-384 or P-521 session key created for each TLS session

6.4 Definition of CSPs Modes of Access

Table 8 defines the relationship between access to keys/CSPs and the different module services. The types of access used in the table are Use (U), Generate (G), Input (I), Output (O), Store (S), and Zeroize (Z). Z* is used to denote that only the plaintext portion of the CSP is zeroized (i.e., the CSP is also stored using an Approved algorithm, but that portion is not zeroized).

Table 8 – Key and CSP Access Rights within Services

	Administrator Passwords	Sensor Operator Passwords	NSM Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	SSH Session Keys	TLS Sensor Private Key (for NSM)	TLS Session Keys (for NSM)	Entropy Input String	Seed for DRBG	DRBG Internal State	McAfee FW Verification Key	SSH Session Public Key	SSH Host Public Key	SSH Remote Client Public Key	TLS Sensor Public Key (for NSM)	TLS NSM Public Key	TLS Session Public Key
Authentication – Admin, Sensor Operator	U	U			U	U G					U G			O	I U			
Authentication – NSP Manager –Digital Signature			U				U	U G			U G					O	U	
SNMP Authentication – NSP Manager to Sensor - Username, Privacy, and Authentication Key																		U
Authentication – 3rd Party SNMP Client(s)																		U
Show Status	U	U			U									U	U			
Sensor Operator Management						U		U										
Network Configuration						U		U										
Administrative Configuration			I		UG	U		U						UG				
Firmware Update				I U		U		U				U I						
Install with NSM				I U			G	U	UG	U G	U G	U	G			G		G
Install with 3rd Party SNMP Client				I U								U						
Change Passwords	I S	I S																
Zeroize (Authenticated)	Z*	Z*	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Zeroize (Unauthenticated)	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Intrusion Detection/ Prevention Management				U			U	U								U	U	U
Intrusion Detection/ Prevention Monitoring																		
Disable SSH/Console Access	U																	

	Administrator Passwords	Sensor Operator Passwords	NSM Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	SSH Session Keys	TLS Sensor Private Key (for NSM)	TLS Session Keys (for NSM)	Entropy Input String	Seed for DRBG	DRBG Internal State	McAfee FW Verification Key	SSH Session Public Key	SSH Host Public Key	SSH Remote Client Public Key	TLS Sensor Public Key (for NSM)	TLS NSM Public Key	TLS Session Public Key
Self Tests																		
Intrusion Prevention Services																		

7 Operational Environment

The device supports a limited operational environment.

8 Security Rules

The cryptographic module's design corresponds to the module's security rules. This section requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module provides four distinct operator roles: Admin, Sensor Operator(s), Network Security Platform Manager, and 3rd Party SNMP Client(s).
2. The cryptographic module provides role-based authentication and each change of operator roles is authenticated and previous authentication results are cleared when the module transitions to a power-off state.
3. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services that could cause modification to the module's CSPs.
4. The cryptographic module performs the following tests:

   A. <u>Power up Self-Tests are performed without operator input:</u>

   1. Firmware Integrity Test: XYSSL RSA 2048 (Cert. #C1555) using SHA-256 (Cert. #C1555) for hashing
   2. Cryptographic algorithm known answer tests (KATs) and pairwise consistency tests (PCT):

      a. AES ECB 128 Encryption KAT and Decryption KAT (AES Cert. #C1556)

      b. AES GCM 128 Encryption KAT and Decryption KAT (AES Cert. #C1556)

      c. RSA 2048 PSS Key Generation/Sign/Verify with SHA-256 Pairwise Consistency Test (RSA Cert. #C1556)

      d. SHA-1 KAT (SHS Cert. #C1556)

      e. SHA-256 KAT (SHS Cert. #C1556)

      f. SHA-512 KAT (SHS Cert. #C1556)

      g. Block Cipher (CTR) DRBG KAT and SP 800-90A DRBG Section 11.3 Health Checks (DRBG Cert. #C1556)

      h. HMAC SHA-256 KAT (HMAC Cert. #C1556)

      i. HMAC SHA-512 KAT (HMAC Cert. #C1556)

      j. XYSSL RSA 2048 Signature Verification KAT (RSA Cert. #C1555)

      (SHA-256 based signatures)

      k. XYSSL SHA-256 KAT (SHS Cert. #C1555)

      l. TLS 1.2 KDF KAT (CVL Cert. #C1558)

      m. SSH KDF KAT (CVL Cert. #C1557)

      n. EC Diffie-Hellman Shared Secret Primitive KAT (vendor affirmed)

      o. ECDSA PCT (ECDSA Cert. #C1556)

      p. SP 800-90A DRBG Section 11.3 Health Checks

If any of these tests fail the following message will be displayed:
!!! CRITICAL FAILURE !!!

```
FIPS 140-2 POST and KAT...Failed
REBOOTING IN 15 SECONDS
```

3. Critical Functions Tests: N/A

B. Conditional Self-Tests:

a. Block Cipher (CTR) DRBG Continuous Test

b. NDRNG Continuous Test

c. RSA KeyGen/Sign/Verify Pairwise Consistency Test

d. ECDSA KeyGen Pairwise Consistency Test

e. External Firmware Load Test – XYSSL RSA 2048 (Cert. #C1555) using SHA-256 (Cert. #C1555) for hashing

If the firmware load test fails the following message will be displayed: "Load Image with SCP Failed."

5. At any time the cryptographic module is in an idle state, the operator is capable of commanding the module to perform the power up self-test by power cycling.
6. Data output is inhibited during self-tests and error states.
   a. All Power Up Self-Test are run before data output ports are initialized.
   b. In the case of failed Self Tests, the module enters an error state, and reboots.
7. Data output is logically disconnected during key generation and zeroization.
8. For both Zeroize services (authenticated and unauthenticated), the operator must remain in control of the module or be physically present with the module to assure that the entire zeroization process completes successfully. This may take up to one (1) minute.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.
11. The module only supports five (5) concurrent SSH operators when SSH is enabled.
12. The cryptographic module shall not be configured to transmit files to McAfee Advanced Threat Detection.
13. During initial configuration of the module via its Console Port, the default admin password should be changed to a password with characteristics as listed in Table 5. Once the default password has been changed the module must be rebooted.

9 Physical Security Policy

The module's physical embodiment is that of a multi-chip stand-alone device that meets Level 1 Physical Security requirements. The module is completely enclosed in a rectangular metal enclosure made from production grade material.

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

11 Glossary

Acronym	**Definition**
AES	Advanced Encryption Standard
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSP	Critical Security Parameter
CVL	Component Validation List
DRBG	Deterministic Random Number Generator
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
IG	Implementation Guidance
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
KAT	Known Answer Test
KDF	Key Derivation Function
KTS	Key Transport Scheme
NDRNG	Non-Deterministic Random Number Generator
NSM	Network Security Manager
NSP	Network Security Platform
PCT	Pairwise Consistency Test
RSA	Rivest, Shamir, Adleman algorithm
SHA/SHS	Secure Hash Algorithm/Standard
SCP	Secure Copy