McAfee, Inc.
Network Security Platform Sensor
M-8000 P

Non-Proprietary Security Policy

Version 3.1

March 25, 2016

TABLE OF CONTENTS

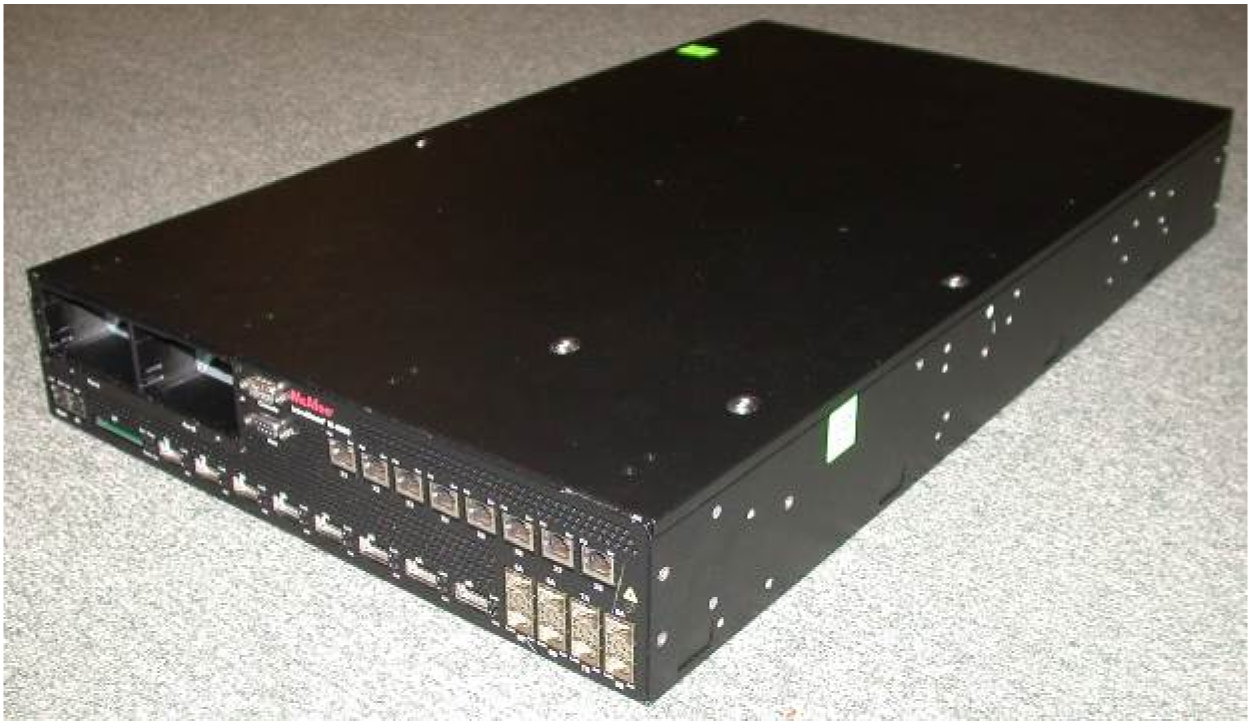
1 Module Overview

The Network Security Platform (NSP) Sensor M-8000 P (HW P/N M-8000 P, Version 1.40; FIPS Kit P/N IAC-FIPS-KT8; FW Version 8.1.15.14) is a multi-chip standalone cryptographic module as defined by FIPS 140-2. It is an Intrusion Prevention System (IPS) and Intrusion Detection System (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 cryptographic boundary is the outer perimeter of the enclosure, including the removable power supplies and fan trays. (The power supplies and fan trays are excluded from FIPS 140-2 requirements, as they are not security relevant.)

The McAfee M-8000 product consists of the M-8000 P cryptographic module physically connected with the M-8000 S cryptographic module. This security policy describes the M-8000 P only.

Figure 1 shows the module and its cryptographic boundary.

Figure 1 – Image of the Cryptographic Module (with Power Supply Trays Unpopulated)



2 Security Level

The cryptographic module meets the overall requirements applicable to Level 2 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	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Modes 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.

Approved Algorithms

The module supports the following FIPS Approved algorithms:

- AES CBC and ECB mode with 128 & 256 bits for encryption and decryption (Cert. #3155)
- Block Cipher (CTR) DRBG using AES 256 (Cert. #648)
- HMAC SHA-1, SHA-256, and SHA-512 for message authentication (Cert. #1988)

  (Note: The minimum HMAC key size is 20 bytes.)
- FIPS 186-4 RSA PSS with 2048 bit keys for key generation, signature generation with SHA-256 and SHA-512, and signature verification with SHA-1, SHA-256, and SHA-512 (Cert. #1598)
- SHA-1, SHA-256, and SHA-512 for hashing (Cert. #2610)

  (Note: SHA-1 validated for use in TLS and verification-purposes only.)
- FIPS 186-4 XYSSL RSA PKCS #1 1.5 SigVer with 2048 bit keys using SHA-1 and SHA-256 for image verification (Cert. #1824)
- XYSSL SHA-1 and SHA-256 for hashing and for use with image verification (Cert. #2922)
- TLS v1.0/1.1 KDF for TLS session key derivation (CVL Cert. #407)
- SSH KDF for SSH session key derivation (CVL Cert. #598)

Allowed Algorithms and Protocols

The module supports the following FIPS allowed algorithms and protocols:

- NDRNG for seeding the Block Cipher (CTR) DRBG.
- RSA with 2048-bit keys for key wrapping (key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman with 2048-bit keys for key agreement (key establishment methodology provides 112 bits of encryption strength)
- TLS v1.0 with the following algorithm tested cipher suites. The protocol algorithms have been tested by the CAVP (see certificate #s above) but the protocol implementation itself has not been reviewed or tested by the CAVP or CMVP.
  - TLS_RSA_WITH_AES_128_CBC_SHA for communication with Network Security Platform (NSP) Manager

    (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 the protocol implementation itself has not been reviewed or tested by the CAVP or CMVP.
    - Key Exchange methods (i.e., key establishment methods): Diffie-hellman-group14-SHAl
    - Public Key methods (i.e., authentication methods):SSH-RSA

      (Note: This is restricted to RSA-2048)
    - Encryption methods: AES128-CBC, AES256-CBC
    - MAC methods: HMAC-SHA1, HMAC-SHAl-96, HMAC-SHA256, HMAC-SHA-512

Non-Approved Algorithms and Protocols with No Security Claimed

The module supports the following non-Approved but allowed algorithms and protocols with no security claimed:

- 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 plaintext transport mechanism with no security claimed. All CSP content in this SNMPv3 channel is additionally key wrapped and signed by NSM to ensure integrity and decrypted in sensor using the sensor TLS private key. Non-CSP SNMPv3 content is deemed plaintext. Non-Approved algorithms (no security claimed): HMAC (non-compliant), SHA (non-compliant), AES (non-compliant), Triple-DES (non-compliant), MD5, DES, SNMP KDF (non-compliant)
- The following algorithms are implemented independently from all validated 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 (no security claimed): 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): RSA (non-compliant), SHA (non-compliant), Triple-DES (non-compliant), HMAC (non-compliant), RC4, MD5, DES

4 Ports and Interfaces

Figure 2 – M 8000 P Front Panel (with Power Supply Trays Populated)

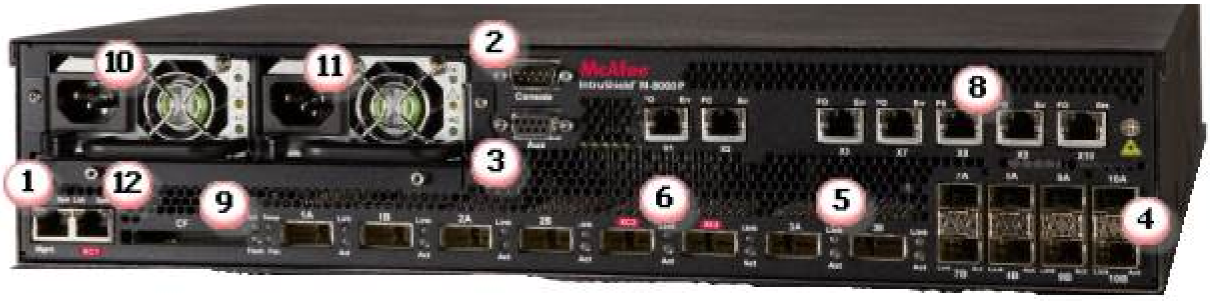


Table 2 provides the cryptographic module’s ports and interfaces.

Table 2 – Ports and Interfaces

Item	Physical Ports	Logical Interfaces	Qty.
1	GigE Management Port	Control Input, Data Output, Status Output	1
2	RS232 Console Port	Control Input, Status Output	1
3	RS232 Auxiliary Port	Control Input, Status Output	1
4	SFP 1-Gig Monitoring Ports	Data Input/Data Output	8
5	XFP 10-GigE Monitoring Ports	Data Input/Data Output	6
6	XFP Interconnect Ports	Data Input/Data Output	2
8	RJ-11Fail-Open Control Ports	Data Input, Power Output	7
9	Compact Flash	Data Input	1
10/11	Power Ports	Power Input	2
12	RJ-45 10/100/1000 Interconnect Port	Data Input/Data Output	1
N/A	LEDs	Status Output	many

Notes:

1. Two 10-GigE ports (out of eight) are used to connect to the peer M-8000 S unit. The other six are used to monitor external traffic.
2. The GigE Management Port is connected directly to the peer M-8000 S unit’s GigE Response Port.

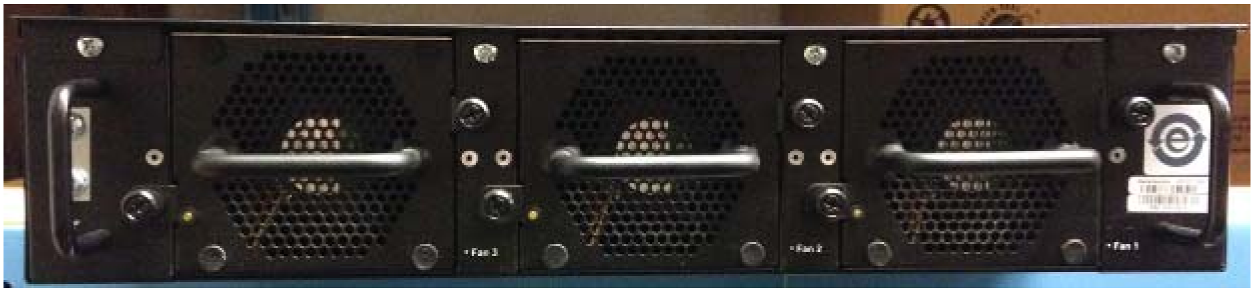
The module supports the following communication channels with the Network Security Platform (NSP) Manager (aka NSM):

- Install channel: Only used to associate a Sensor with the NSM (i.e., NSP Manager, see

Table 3). They use a “shared secret”. NSM listening on port 8501.

- Trusted Alert/Control channel (TLS): NSM listening on port 8502
- Trusted Packet log channel (TLS): NSM listening on port 8503
- Command channel (SNMP, plaintext): Sensor listening to 3rd Party SNMP Clients on port 8500
- Bulk transfer channel (All output is encrypted): NSM listening on port 8504

Figure 3 - Rear Panel of M-8000 P (No Ports)



5 Identification and Authentication Policy

The cryptographic module shall support four distinct “User” roles (Admin, Sensor Operator(s), M-8000 S, and 3rd Party SNMP Client(s)) and one “Cryptographic Officer” (CO) role (Network Security Platform Manager). Table 3 lists the supported operator roles along with their required identification and authentication techniques. Table 4 outlines each authentication mechanism and the associated strengths.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin	Role-based authentication	Username and Password
Sensor Operator(s)	Role-based authentication	Username and Password
Network Security Platform Manager (CO)	Role-based authentication	Digital Certificate
M-8000 S	Role-based authentication	Shared Secret
3rd Party SNMP Client(s)	Role-based authentication	Username, Privacy and Authentication key

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password (Admin and Sensor Operator(s))	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 2 uppercase characters, 2 lowercase characters, 2 numeric characters, and 2 special characters. 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 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
Shared Secret (M-8000 S)	The Shared Secret is an alphanumeric string of a minimum of six (6) characters chosen from the set of ninety-three (93) printable and human-readable characters. Whitespace and “?” are not allowed. The probability that a random attempt will succeed or a false acceptance will occur is 1/93^6 which is less than 1/1,000,000. After setting the Shared Secret, the module requires a reboot in order to authenticate. The reboot takes longer than one minute before authentication is achieved, and if authentication fails, the module automatically reboots a second time. The probability of successfully authenticating to the module within one minute through random attempts is 1/93^6 which is less than 1/100,000.
Digital Certificate	RSA 2048-bit keys using SHA-256 are used for the signing (in isolated McAfee laboratory) 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 certificate 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 5 lists each operator role and the services authorized for each role. Following Table 5, all unauthenticated services are listed.

Table 5 – Services Authorized for Roles

Role					**Authorized Services**
Admin	Sensor Operator(s)	NSP Manager	M-8000 S	3rd Party SNMP Client(s)	
X	X	X	X		**Show Status**: Provides module status, usage statistics, log data, and alerts.
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	X*	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 compact flash.
X	X*				**Install with NSM**: Configures module for use. This step includes establishing trust between the module and the associated management station.
		X			**Install with 3rd Party SNMP Client:** Configures module for 3rd Party SNMP use. This step includes establishing trust between the module and the associated 3rd Party SNMP Client. Trust is provided by NSM.
X	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.
		X			**Intrusion Detection/Prevention Management**: Management of intrusion detection/prevention policies and configurations through SNMPv3 and TLS.

Role					Authorized Services
Admin	Sensor Operator(s)	NSP Manager	M-8000 S	3rd Party SNMP Client(s)	
				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 and Console access.

* Depending on the authorization level granted by the Admin

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- **Self-Tests**: This service executes the suite of self-tests required by FIPS 140-2.
- **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 non-Approved algorithms listed above with no security claims. 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

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.
- **3rd Party SNMP Client Privacy and Authentication Keys**: Passwords used for authentication of 3rd Party SNMP Clients.
- **M-8000 Shared Secret:** Shared secret used for authentication of M-8000 S.
- **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**: RSA 2048 bit key used for authentication of sensor to remote terminal for CLI access.
- **SSH Session Keys**: Set of ephemeral Diffie-Hellman, AES, and HMAC 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 AES and HMAC keys created for each TLS session with the NSM.
- **Seed for RNG**: 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
- **Server Private Keys (for SSL network stream analysis):** Set of up to 64 Private Keys of servers within the environment protected by the IPS Services. Used to decrypt and analyze incoming network traffic.

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 Host Public Key**: RSA 2048 bit key used to authenticate the sensor to the remote client during SSH.
- **SSH Remote Client Public Key**: RSA 2048 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.

6.4 Definition of CSPs Modes of Access

Table 6 defines the relationship between access to keys/CSPs and the different module services. The types of access used in the table are Read (R), Write (W), 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 6 – Key/CSP Access Rights within Services

	Administrator Passwords	Sensor Operator Passwords	3rd Party SNMP Client P and A Keys	M-8000 Password	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)	Seed for RNG	DRBG Internal State	Server Private Keys (for SSL network stream analysis)	McAfee FW Verification Key	SSH Host Public Key	SSH Remote Client Public Key	TLS Sensor Public Key (for NSM)	TLS NSM Public Key
Show Status	R				R	R	R		R	R					R	R	R	R
Sensor Operator Management		R W																
Network Configuration					R		R		R	R					R	R	R	R
Administrative Configuration					R		R		R	R					R	R	R	R
Firmware Update					R		R		R	R					R	R	R	R
Install with NSM					W		R		R W	RW	R W	RW			R	R	R W	R W
Install with 3rd Party SNMP Client			RW															
Change Passwords	R W			R W			R								R	R		
Zeroize	Z*	Z*	Z	Z	Z	Z	R Z	Z	Z	Z	Z	Z	Z	Z	R	R		
Intrusion Detection/Prevention Management						R			R	R							R	R
Intrusion Detection/Prevention Monitoring			R															
Disable SSH/Console Access																		
Self-Tests																		
Intrusion Prevention Services													W R					

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment.

8 Security Rules

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

1. The cryptographic module shall provide five distinct operator roles: Admin, Sensor Operator(s), Network Security Platform Manager, M-8000 S, and 3rd Party SNMP Client(s).
2. The cryptographic module shall provide role-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

      1. Firmware Integrity Test: XYSSL RSA 2048 using SHA-1 for hashing
         (Future versions of this Cryptographic Module will validate integrity with a SHA-256 based hash.)
      2. Cryptographic algorithm known answer tests (KATs):
         a. AES ECB 128 Encryption KAT and Decryption KAT
         b. RSA 2048 Key Generation KAT (Cert. #1598)
         c. RSA 2048 Signature Generation KAT (Cert. #1598)
         d. RSA 2048 Signature Verification KAT (Cert. #1598)
         e. SHA-1 KAT (Cert. #2610)
         f. SHA-256 KAT (Cert. #2610)
         g. SHA-512 KAT (Cert. #2610)
         h. Block Cipher (CTR) DRBG KAT
         i. HMAC SHA-1 KAT
         j. HMAC SHA-256 KAT
         k. HMAC SHA-512 KAT
         l. XYSSL RSA 2048 Signature Verification KAT (Cert. #1824)
            (SHA-1 and SHA-256 based signatures)
         m. XYSSL SHA-1 KAT (Cert. #2922)
         n. XYSSL SHA-256 KAT (Cert. #2922)
         o. TLS 1.0/1.1 KDF KAT
         p. SSH KDF KAT

         If any of these tests fail the following message will be displayed:
         !!! CRITICAL FAILURE !!!
         FIPS 140-2 POST and KAT...
         REBOOTING IN 15 SECONDS

      3. Critical Functions Tests: N/A

   B. Conditional Self-Tests:

      1. Block Cipher (CTR) DRBG Continuous Test
      2. SP 800-90A DRBG Section 11.3 Health Checks

3. NDRNG Continuous Test
4. RSA Sign/Verify Pairwise Consistency Test
5. External Firmware Load Test – XYSSL RSA 2048 using SHA-256 for hashing

   If the firmware load test fails the following message will be displayed: "Load image with SCP failed." If the pairwise consistency test fails the following message will be displayed: “Pairwise Test Failed”. If the DRBG CRNGT test fails the following message will be displayed: “DRBG stuck”. If the NDRNG CRNGT fails the following message will be displayed: “Entropy source stuck”.

5. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power up self-test by power cycling.

6. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.

7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

8. If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.

9. The module shall only support five concurrent SSH operators when SSH is enabled.

9. The use of the Aux ports shall be restricted to the initialization of the cryptographic module.

10. The use of the Compact Flash Port shall be restricted to loading McAfee signed firmware.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Production-grade opaque enclosure with tamper evident seals. Tamper evident seals and further instructions are obtained in the FIPS Kit with the part number: IAC-FIPS-KT8.

9.2 Operator Required Actions

For the module to operate in a FIPS Approved mode, the tamper seals shall be placed by the Admin role as specified below. The Admin must clean the chassis of any dirt before applying the labels. Per FIPS 140-2 Implementation Guidance (IG) 14.4, the Admin role is also responsible for the following:

- Securing and having control at all times of any unused seals
- Direct control and observation of any changes to the module, such as reconfigurations, where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

The Admin is also required to periodically inspect tamper evident seals. Table 7 outlines the recommendations for inspecting/testing physical security mechanisms of the module. If evidence of tamper is found during the periodic inspection, the operator should zeroize the module and modify Administrator Passwords upon start up. The operator should contact McAfee for new tamper labels, if necessary.

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	As specified per end user policy	Visually inspect the labels for tears, rips, dissolved adhesive, and other signs of malice.
Opaque Enclosure	As specified per end user policy	Visually inspect the enclosure for broken screws, bent casing, scratches, and other questionable markings.

Figure 4 depicts the tamper label locations on the cryptographic module. There are 6 tamper labels and they are circled in yellow.

Figure 4 – Tamper Label Placement

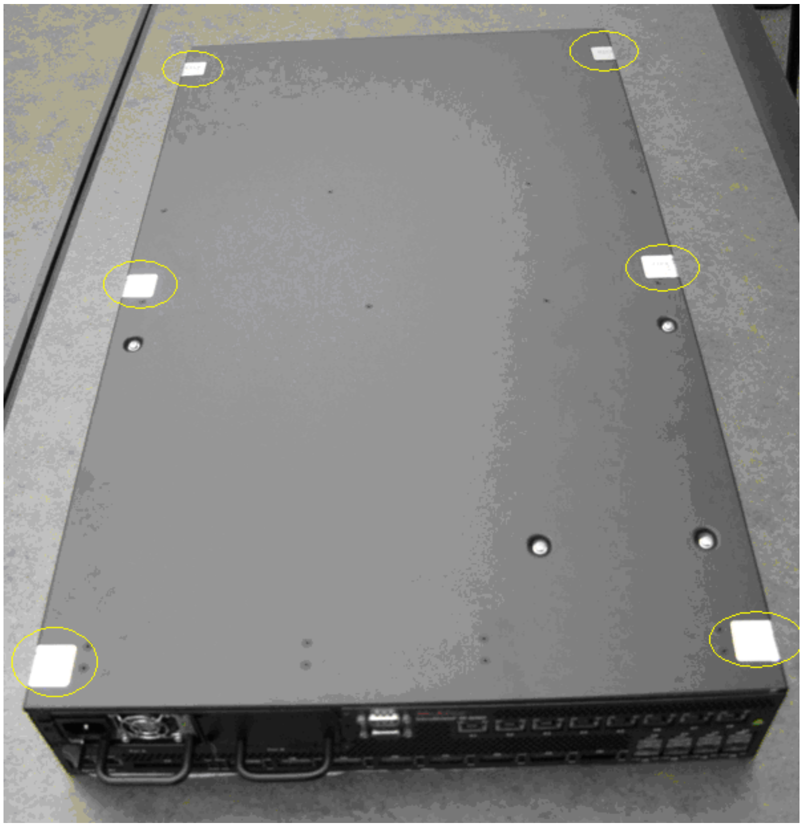
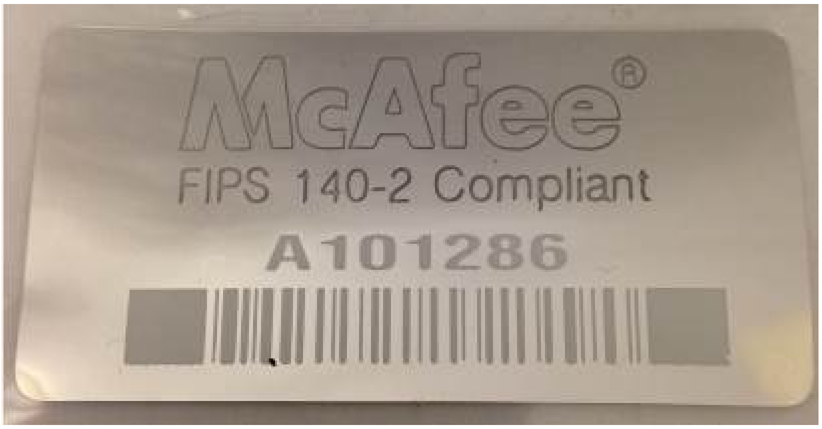


Figure 5 shows a sample Tamper Label.

Figure 5 - Tamper Label



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.