McAfee, Inc.
Network Security Platform Sensor M-1250, M-1450, M-2750, M-2850, M-2950, M-3050, M-4050, and M-6050

Security Policy

Version 1.20

NOVEMBER 7, 2014

NOTICE: Documentation only modifications have been made retroactively to this Security Policy after the January 1, 2014 SP 800-131A transition date per CMVP guidelines. These modifications add a non-FIPS Approved mode of operation which many of the algorithms, services, and keys now fall under due to the transitions.

TABLE OF CONTENTS

1 Module Overview

The Network Security Platform Sensor M-1250, M-1450, M-2750, M-2850, M-2950, M-3050, M-4050, and M-6050 consists of the following multi-chip standalone platforms/configurations:

- M-1250 (HW P/N M-1250 Version 1.10; FIPS Kit P/N IAC-FIPS-KT2)
- M-1450 (HW P/N M-1450 Version 1.10; FIPS Kit P/N IAC-FIPS-KT2)
- M-2750 (HW P/N M-2750 Version 1.50; FIPS Kit P/N IAC-FIPS-KT2)
- M-2850 (HW P/N M-2850 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2)
- M-2950 (HW P/N M-2950 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2)
- M-3050 (HW P/N M-3050 Version 1.20; FIPS Kit P/N IAC-FIPS-KT2)
- M-4050 (HW P/N M-4050 Version 1.20; FIPS Kit P/N IAC-FIPS-KT7)
- M-6050 (HW P/N M-6050 Version 1.40; FIPS Kit P/N IAC-FIPS-KT7)

All module configurations include FW Version 7.1.15.4.

They are all 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 cryptographic boundary of each platform is the outer perimeter of the enclosure, including the power supplies and fan trays (removable and non-removable), as described below:

- M-1250/M-1450: The power supplies and fan trays are non-removable.
- M-2750/M-2850/M-2950: The removable fan trays are protected with tamper seals (see Figure 8). The removable power supplies are excluded from FIPS 140-2 requirements, as they are non-security relevant.
- M-3050/M-4050/M-6050: The removable power supplies and fan trays are excluded from FIPS 140-2 requirements, as they are non-security relevant.

Figures 1 through 5 show the module configurations and their cryptographic boundaries.

Figure 1 – Image of the M-1250/M-1450

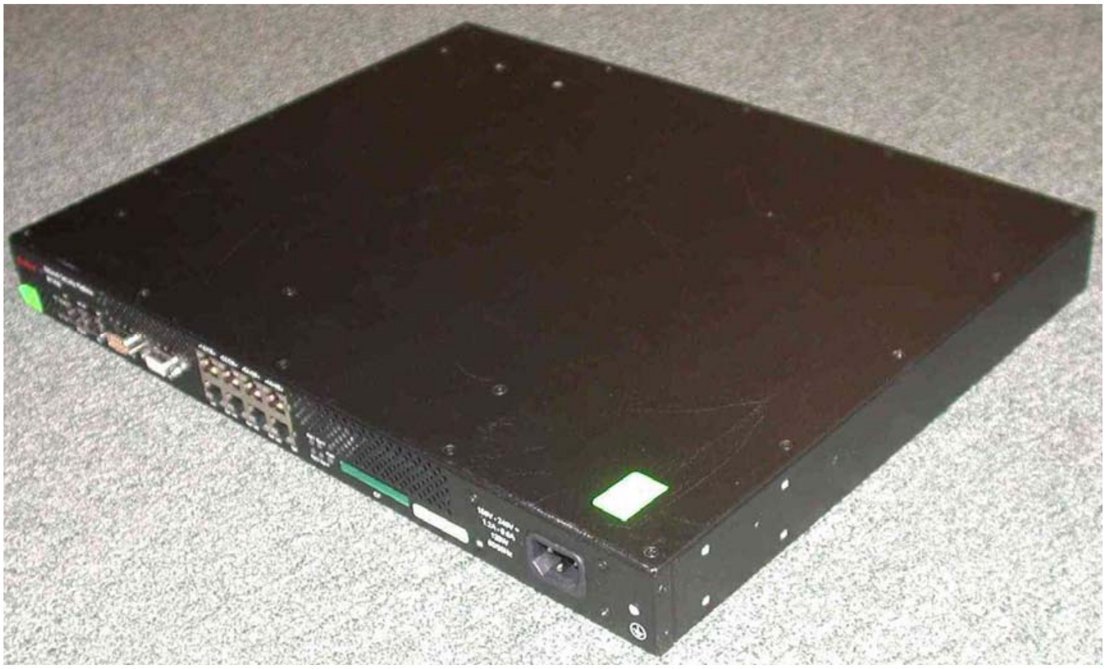


Figure 2 – Image of the M-2750

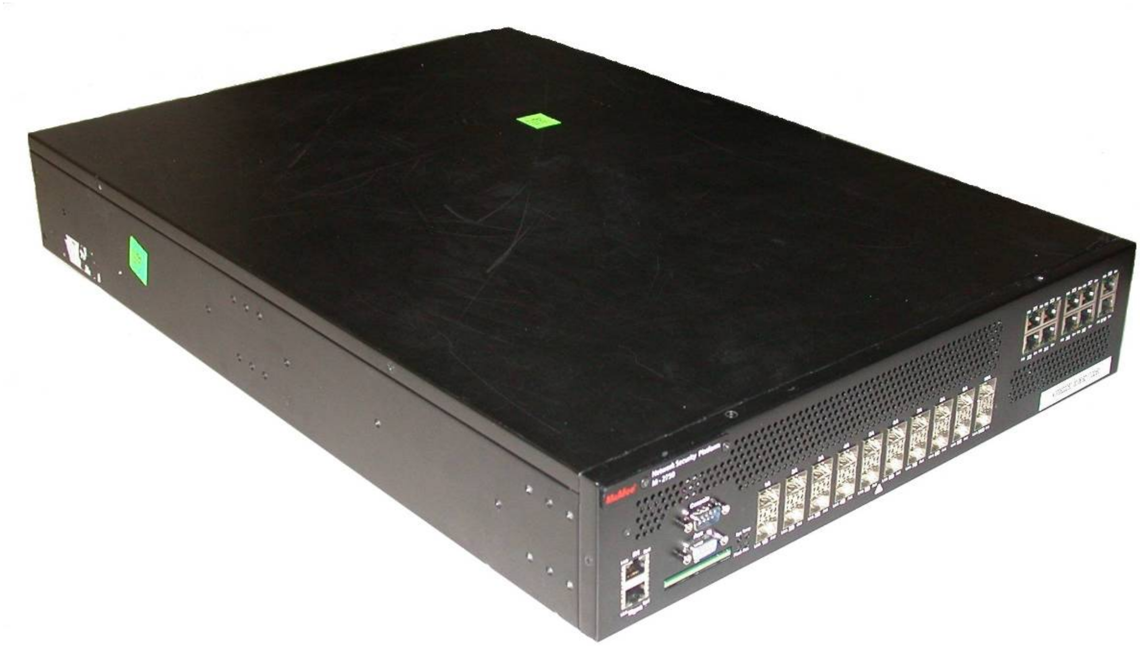


Figure 3 – Image of the M-2850/M-2950

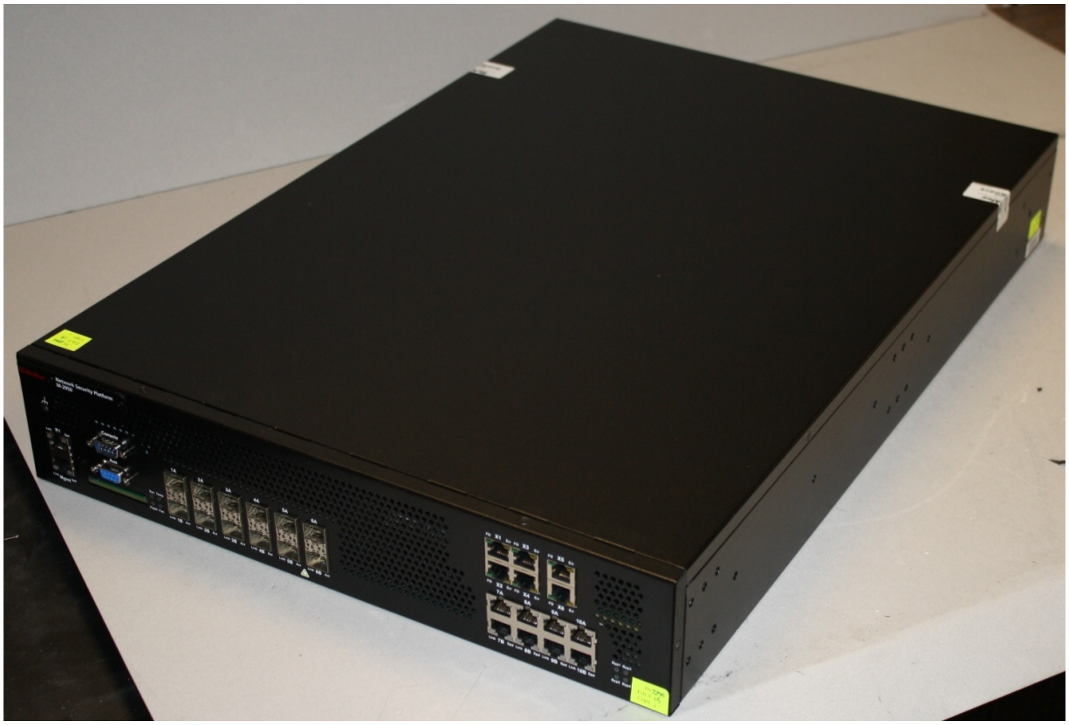


Figure 4 – Image of the M-3050/M-4050

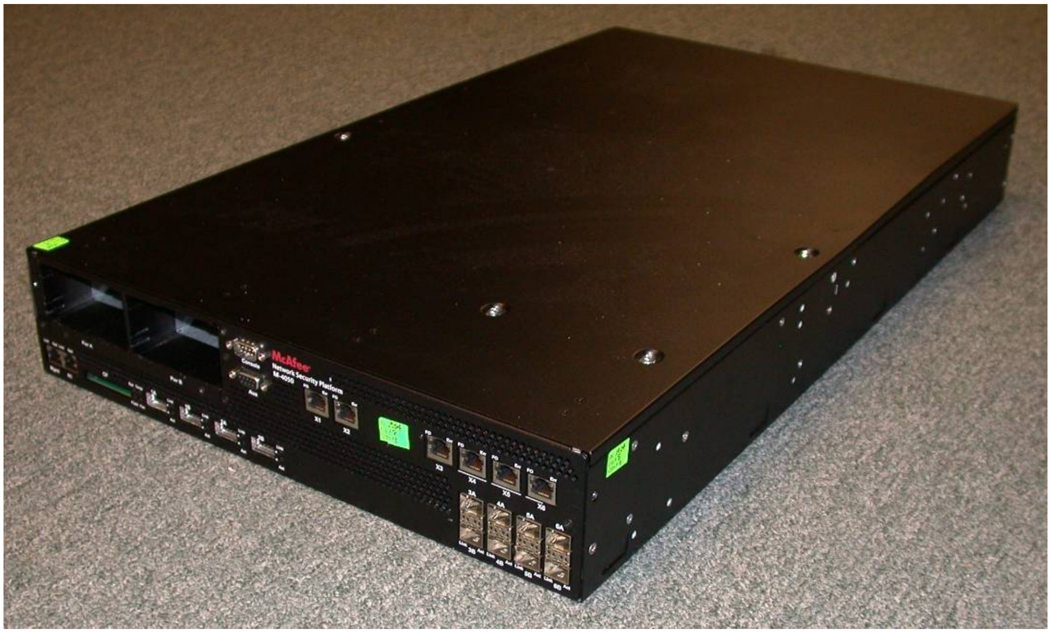
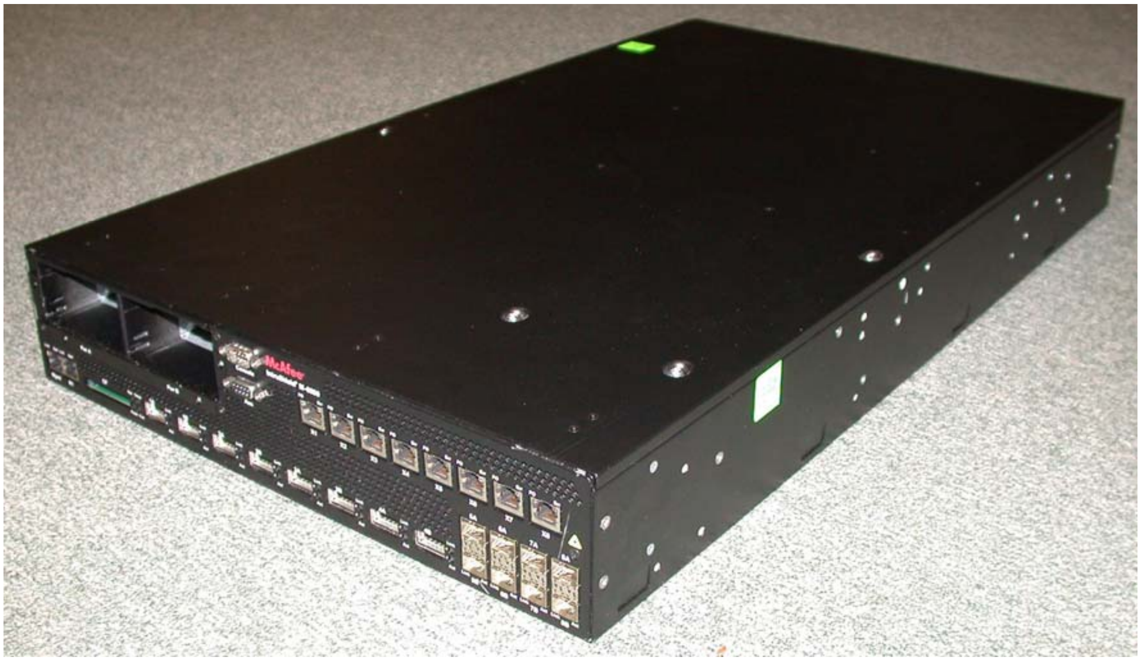


Figure 5 – Image of the M-6050



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 Mode of Operation

3.1 FIPS Approved Mode of Operation

The FIPS Approved mode of operation is defined by the use of only the FIPS Approved and allowed algorithms, modes, and key sizes listed below. It is the responsibility of the operator of the module to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Section 3.2). The operator must also follow the rules outlined in Sections 8 and 9 of this Security Policy.

The module supports the following FIPS Approved algorithms:

- FIPS 186-2 RSA with 1024 and 2048 bit keys for signature verification (Cert. #425)
  (Note: RSA signature verification with 1024 bit keys and 2048 bit keys with SHA-1 is acceptable for Legacy-use per SP 800-131A.)
- FIPS 186-2 DSA with 1024 bit keys for signature verification (Cert. #345)
  (Note: DSA signature verification with 1024 bit keys is acceptable for Legacy-use per SP 800-131A.)
- SHA-1 and SHA-256 for hashing (Cert. #871)
- ANSI X9.31 RNG with 2-Key Triple-DES (Cert. #505)
  (Note: ANSI X9.31 RNG is Deprecated per SP 800-131A and will be Disallowed in 2016.)
- HMAC SHA-256 for message authentication (Cert. #971)
- FIPS 186-2 XYSSL RSA with 2048 bit keys for image verification (Cert. #830)
  (Note: RSA signature verification with 2048 bit keys and SHA-1 will continue to be allowed for Legacy use per SP 800-131A.)
- XYSSL SHA-1 for hashing and for use with image verification (Cert. #970)
- TLS v1.0/1.1 KDF for TLS session key derivation (CVL Cert. #57)
- SSH KDF for SSH session key derivation (CVL Cert. #58)

The module supports the following FIPS allowed algorithms and protocols:

- NDRNG for seeding the ANSI X9.31 RNG
- MD5 used to identify "fingerprint" of potential malware using Artemis database (used internal to the module only*;* no security claimed)

3.2 Non-Approved Mode of Operation

The module supports the following algorithms and options which are Disallowed as of January 1, 2014 per the NIST SP 800-131A algorithm transitions:

- TLS v1.0 with the following cipher suites and algorithms (*Note: Uses RSA with 1024 for key establishment so entire protocol has been moved to non-Approved.*):
  - TLS_RSA_WITH_AES_128_CBC_SHA for communication with Network Security Platform (NSP) Manager
    - RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength; non-compliant)
    - FIPS 186-2 RSA signature generation with 1024 and 2048 bit keys using SHA-1 (non-compliant)
    - AES CBC mode with 128 bits for encryption and decryption (non-compliant; all keys used only have 80 bits of security)

        - HMAC SHA-1 for message authentication (non-compliant; all keys used only have 80 bits of security)
        - Still uses Approved SHA-1, TLS KDF, and RSA signature verification

- SSH v2 with the following cipher suites and algorithms *(Note: Uses DH with 1024 for key establishment so entire protocol has been moved to non-Approved.):*
    - Key Exchange methods (i.e., key establishment methods): Diffie-hellman-group-exchange-SHAl, Diffie-hellman-group1-SHAl
        - Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant)
    - Public Key methods (i.e., authentication methods): SSH-DSS, SSH-RSA
        - FIPS 186-2 RSA signature generation with 1024 and 2048 bit keys using SHA-1 (non-compliant)
        - FIPS 186-2 DSA with 1024 bit keys for key generation and signature generation (non-compliant)
        - Still uses Approved SHA-1, DSA signature verification, RSA signature verification
    - Encryption methods: 3DES-CBC, AES128-CBC
        - AES CBC mode with 128 bits for encryption and decryption (non-compliant; all keys used only have 80 bits of security)
        - Triple-DES CBC mode with 2 and 3 keys for encryption and decryption (non-compliant; all keys used only have 80 bits of security)
    - MAC methods: HMAC-SHA1, HMAC-SHAl-96
        - HMAC SHA-1 for message authentication (non-compliant; all keys used only have 80 bits of security)
        - Still uses Approved SHA-1 and SSH KDF

Use of any Disallowed algorithm, mode, or key size will place the module in the non-Approved mode of operation.

The following CSPs, public keys and services are affected if the above listed Disallowed algorithms/options are used (see Sections 6.1, 6.2 and 6.3):

<u>CSPs</u>

- Bulk Transfer Channel Session Key
- SSH Host Private Keys
- SSH Session Keys
- TLS Sensor Private Key (for ISM)
- TLS Session Keys (for ISM)

<u>Public Keys</u>

- SSH Host Public Key
- SSH Remote Client Public Key
- TLS Sensor Public Key (for ISM)
- TLS ISM Public Key

Services

- Show Status
- Sensor Operator Management
- Network Configuration
- Administrative Configuration
- Firmware Update
- Install with ISM
- Install with 3rd Party SNMP Client
- Change Passwords
- Zeroize
- Intrusion Detection/Prevention Management
- Disable SSH/Console Access

Note: This section and the non-Approved mode were added to the Security Policy retroactively in 2014 due to SP 800-131A transitions and CMVP guidelines. This is strictly a documentation update.

4 Ports and Interfaces

Table 2 provides the cryptographic module's port quantities per platform.

Table 2 – Ports per Platform

Ports ***(Input/Output Type)***	**Platforms and Port Quantities**							
	M-1250	**M-1450**	**M-2750**	**M-2850**	**M-2950**	**M-3050**	**M-4050**	**M-6050**
10-Gig Monitoring Ports *(Data Input/Output)*	0	0	0	0	0	8	8	8
1-GigE Monitoring Ports *(Data Input/Output)*	8	8	20	20	20	8	8	8
GigE Management Port *(Control Input, Data Output, Status Output)*	1	1	1	1	1	1	1	1
GigE Response Port *(Data Output)*	1	1	1	1	1	1	1	1
RS232 Console/Aux Ports *(Control Input, Status Output)*	2	2	2	2	2	2	2	2
Compact Flash *(Data Input)*	1	1	1	1	1	1	1	1
Power Ports *(Power Input)*	1	1	2	2	2	2	2	2
RJ11 Control Port *(Data Input, Power Output)*	0	0	10	6	6	8	8	8
LEDs *(Status Output)*	many	many	many	many	many	many	many	many

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

- Install channel: Only used to associate a Sensor with the ISM. They use a "shared secret". ISM listening on port 8501.
- Trusted Alert/Control channel (TLS): ISM listening on port 8502
- Trusted Packet log channel (TLS): ISM listening on port 8503
- Command channel (SNMPv3, plaintext): Sensor listening to 3rd Party SNMP clients on port 8500
- Bulk transfer channel (All output is encrypted): ISM listening on port 8504
- Trusted Authentication Gateway channel (TLS): uses same crypto context as Alert/Control channel. ISM listening on port 8502.

5 Identification and Authentication Policy

The cryptographic module supports three distinct "User" roles (Admin, Sensor Operator(s), and 3rd Party SNMP Client(s)) and one "Cryptographic Officer" 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 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
3rd Party SNMP Client(s)	Role-based operator authentication	Username, Privacy and Authentication key

Table 4 – 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 (90) printable and human-readable characters. The probability that a random attempt will succeed or a false acceptance will occur is 1/90^15, 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)/90^15, which is less than 1/100,000.
Digital Signature	RSA 1024 and 2048-bit keys 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 1/2^80, 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 60/2^80, which is less than 1/100,000.

Authentication Mechanism	Strength of Mechanism
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.

Note: With the SP 800-131A transitions, many of these services are defined to be allowed to run in the non-Approved and Approved modes of operation. This is allowed because if the services are performed over a plaintext channel (i.e., TLS and SSH with non-Approved algorithms), they are not breaking any FIPS rules. The affected services are marked in Table 5 as follows:

[1] If a plaintext datastream is acceptable to the module end user, the service is allowed in the Approved mode.

[2] If a ciphertext datastream is required by the module end user, the service is *not* allowed in the Approved mode.

Table 5 – Services Authorized for Roles

Admin	Sensor Operator(s)	NSP Manager	3rd Party SNMP Client(s)	Authorized Services	*End User Requirement	Approved Mode	Non-Approved Mode
X	X	X		**Show Status**: Provides the status of the module, usage statistics, log data, and alerts.	[1]	X	
					[2]		X
X				**Sensor Operator Management:** Allows Admin to add/delete Sensor Operators, set their session timeout limit, and unlock them if needed.	[1]	X	
					[2]		X
X		X		**Network Configuration**: Establish network settings for the module or set them back to default values.	[1]	X	
					[2]		X
X	X	X		**Administrative Configuration:** Other various services provided for admin, private, and support levels.	[1]	X	
					[2]		X
X		X		**Firmware Update**: Install an external firmware image through TFTP or compact flash.	[1]	X	
					[2]		X
X				**Install with ISM**: Configures module for use. This step includes establishing trust between the module and the associated management station.	[1]	X	
					[2]		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 ISM.	[1]	X	
					[2]		X

Admin	Sensor Operator(s)	NSP Manager	3rd Party SNMP Client(s)	Authorized Services	*End User Requirement	Approved Mode	Non-Approved Mode
X	X			**Change Passwords**: Allows Admin and Sensor Operators to change their associated passwords. Admin can also change/reset Sensor Operators passwords.	[1]	X	
					[2]		X
X				**Zeroize**: Destroys all plaintext secrets contained within the module. The “Reset Config” command is used, followed by a reboot.	[1]	X	
					[2]		X
		X		**Intrusion Detection/Prevention Management**: Management of intrusion detection/prevention policies and configurations through SNMPv3 and TLS.	[1]	X	
					[2]		X
			X	**Intrusion Detection/Prevention Monitoring:** Limited monitoring of Intrusion Detection/Prevention configuration, status, and statistics through SNMPv3. *Always a plaintext datastream.*	N/A	X	
X				**Disable SSH/Console Access:** Disables SSH and Console access.	[1]	X	
					[2]		X

<u>Unauthenticated Services:</u>

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:* The only cryptography performed during this service is an MD5 hash to identify the “fingerprint” of malware.
- **Zeroize**: Destroys all plaintext secrets contained within the module. The “NetBoot” process is used.

6.2 Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Approved Mode	Non-Approved Mode	CSPs
X		**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.
X		**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.
X		**3rd Party SNMP Client Privacy and Authentication Keys**: Passwords used for authentication of 3rd Party SNMP Clients.
X		**ISM Initialization Secret (i.e., ISM Shared Secret)**: Password used for mutual authentication of the sensor and ISM during initialization.
	X	**Bulk Transfer Channel Session Key**: AES 128 bit key used to encrypt data packages across the bulk transfer channel.
	X	**SSH Host Private Keys**: DSA or RSA 1024 bit key used for authentication of sensor to remote terminal for CLI access.
	X	**SSH Session Keys**: Set of ephemeral Diffie-Hellman, Triple-DES or AES, and HMAC keys created for each SSH session.
	X	**TLS Sensor Private Key (for ISM)**: RSA 1024 bit key used for authentication of the sensor to ISM.
	X	**TLS Session Keys (for ISM)**: Set of ephemeral AES and HMAC keys created for each TLS session with the ISM.
X		**Seed for RNG**: Seed created by NDRNG and used to seed the ANSI X9.31 RNG.
X		**Seed Key for RNG**: Seed created by NDRNG and used as the Triple DES key in the ANSI X9.31 RNG.

6.3 Definition of Public Keys:

The following are the public keys contained in the module:

Approved Mode	**Non-Approved Mode**	**Public Keys**
X		**McAfee FW Verification Key**: RSA 2048 bit key used to authenticate firmware images loaded into the module.
	X	**SSH Host Public Key**: DSA or RSA 1024 bit key used to authenticate the sensor to the remote client during SSH.
	X	**SSH Remote Client Public Key**: DSA or RSA 1024 bit key used to authenticate the remote client to the sensor during SSH.
	X	**TLS Sensor Public Key (for ISM):** RSA 1024 bit key used to authenticate the sensor to ISM during TLS connections.
	X	**TLS ISM Public Key**: RSA 1024 bit key used to authenticate ISM 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 and CSP Access Rights within Services

	Administrator Passwords	Sensor Operator Passwords	3rd Party SNMP Client P and A Keys	ISM Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	SSH Session Keys	TLS Sensor Private Key (for ISM)	TLS Session Keys (for ISM)	Seed for RNG	Seed Key for RNG	McAfee FW Verification Key	SSH Host Public Key	SSH Remote Client Public Key	TLS Sensor Public Key (for ISM)	TLS ISM Public Key
Show Status	R			R	R	R		R	R				R	R	R	R
Sensor Operator Management		R W				R							R	R		
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 ISM						R		R W	R W	R W	R W		R	R	R W	R W
Install with 3rd Party SNMP Client			R W					R	R						R	R
Change Passwords	R W					R							R	R		
Zeroize	Z*	Z*	Z	Z	Z	R 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						R							R	R		
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 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 four distinct operator roles: Admin, Sensor Operator(s), Network Security Platform Manager, 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. Cryptographic algorithm known answer tests (KATs):
         - a. AES CBC 128 Encryption KAT and Decryption KAT
         - b. Triple-DES CBC Encryption KAT and Decryption KAT
         - c. RSA 1024 Signature Generation KAT and Signature Verification KAT
         - d. RSA 2048 Signature Generation KAT and Signature Verification KAT
         - e. DSA 1024 Signature Generation KAT and Signature Verification KAT
         - f. SHA-1 KAT
         - g. SHA-256 KAT
         - h. ANSI X9.31 RNG KAT
         - i. RSA 1024 Decrypt KAT
         - j. HMAC SHA-1 KAT
         - k. HMAC SHA-256 KAT
         - l. XYSSL RSA 2048 Signature Verification KAT
         - m. XYSSL SHA-1 KAT
         - n. TLS 1.0/1.1 KDF KAT
         - o. SSH KDF KAT
      2. Firmware Integrity Test: XYSSL RSA 2048 used
      3. Critical Functions Tests: N/A

   B. Conditional Self-Tests:

      - a. ANSI X9.31 RNG Continuous Test
      - b. NDRNG Continuous Test
      - c. RSA Sign/Verify Pairwise Consistency Test
      - d. DSA Sign/Verify Pairwise Consistency Test
      - e. External Firmware Load Test – XYSSL RSA 2048 used

6. 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.

7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.
10. The module shall only support five concurrent SSH operators when SSH is enabled.
11. The use of the Console Port/Aux ports shall be restricted to the initialization of the cryptographic module.
12. The use of the Compact Flash Port shall be restricted to loading McAfee signed firmware.
13. The “SSL Decryption” service shall be disabled.
14. An MNAC license shall not be installed or used with a FIPS validated module.

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 Kits with the following part numbers:
    - M-1250/M-1450/M-2750/M-2850/M-2950/M-3050: IAC-FIPS-KT2
    - M-4050/M-6050: IAC-FIPS-KT7

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.

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 6 depicts the tamper label locations on the cryptographic module for the M-3050, M-4050, and M-6050 platforms. There are 6 tamper labels and they are circled in yellow.

Figure 6 – Tamper Label Placement (M-3050, M-4050, and M-6050)

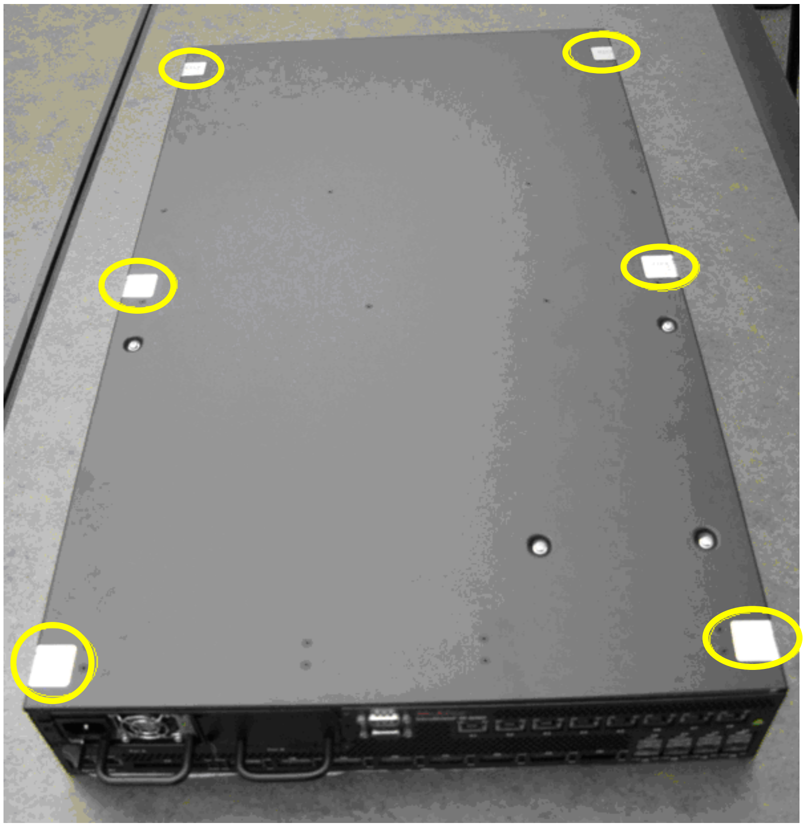


Figure 7 depicts the tamper label locations on the cryptographic module for the M-1250 and M-1450 platforms. There are 8 tamper labels and they are circled in yellow.

Figure 7 – Tamper Label Placement (M-1250 and M-1450)

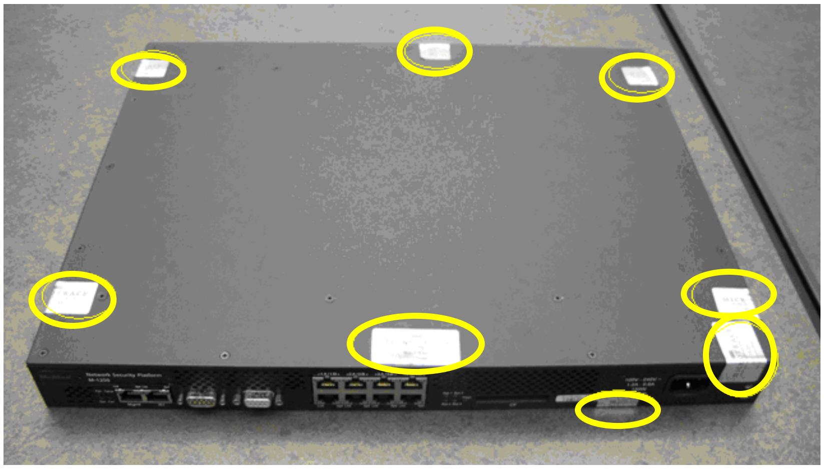
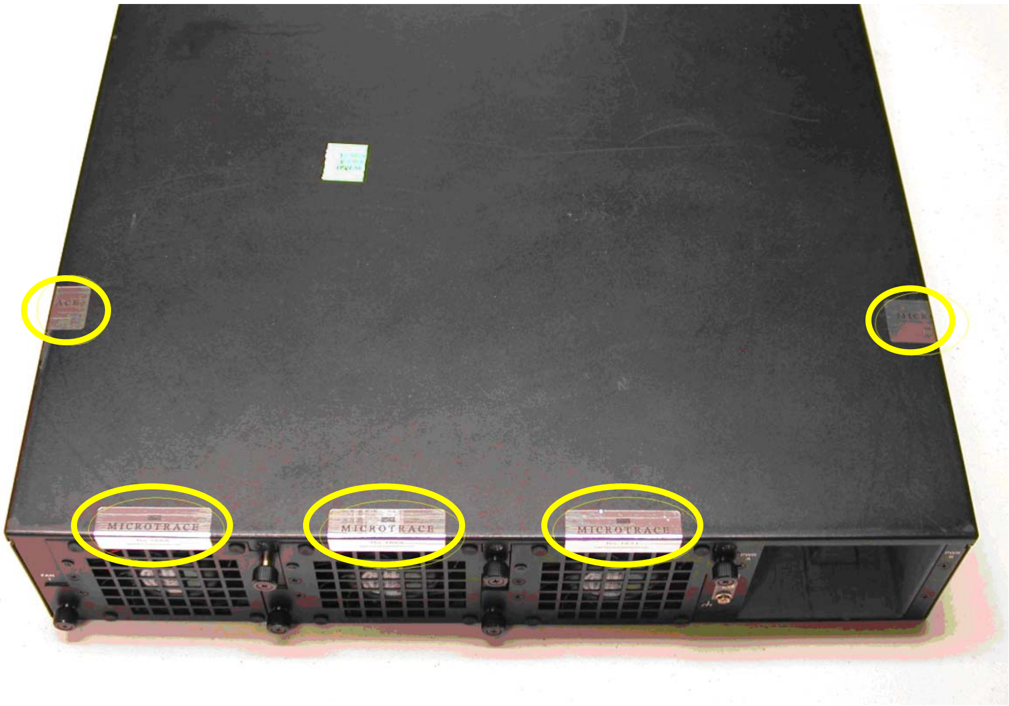


Figure 8 depicts the tamper label locations on the cryptographic module for the M-2750, M-2850, and M-2950 platforms. There are 5 tamper labels and they are circled in yellow.

Figure 8 – Tamper Label Placement (M-2750, M-2850, and M-2950)



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.