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 1.11

November 28, 2011

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 6.1.15.35.

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. Additionally, all platforms can be enabled as Network Access Control (NAC) devices.

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

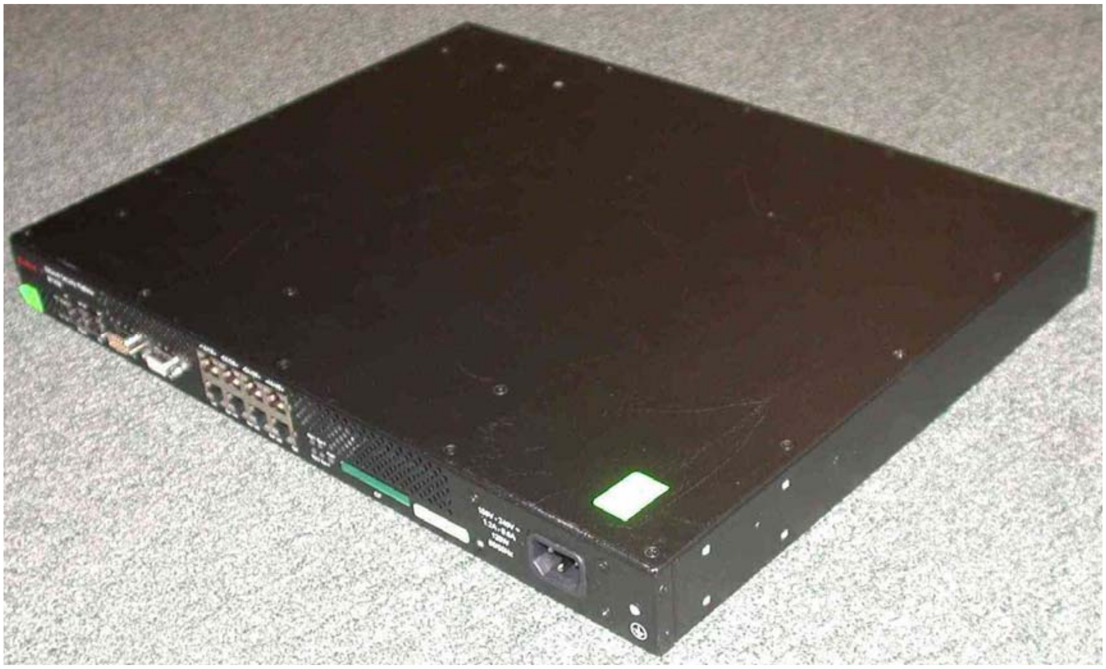


Figure 2 – Image of the M-2750

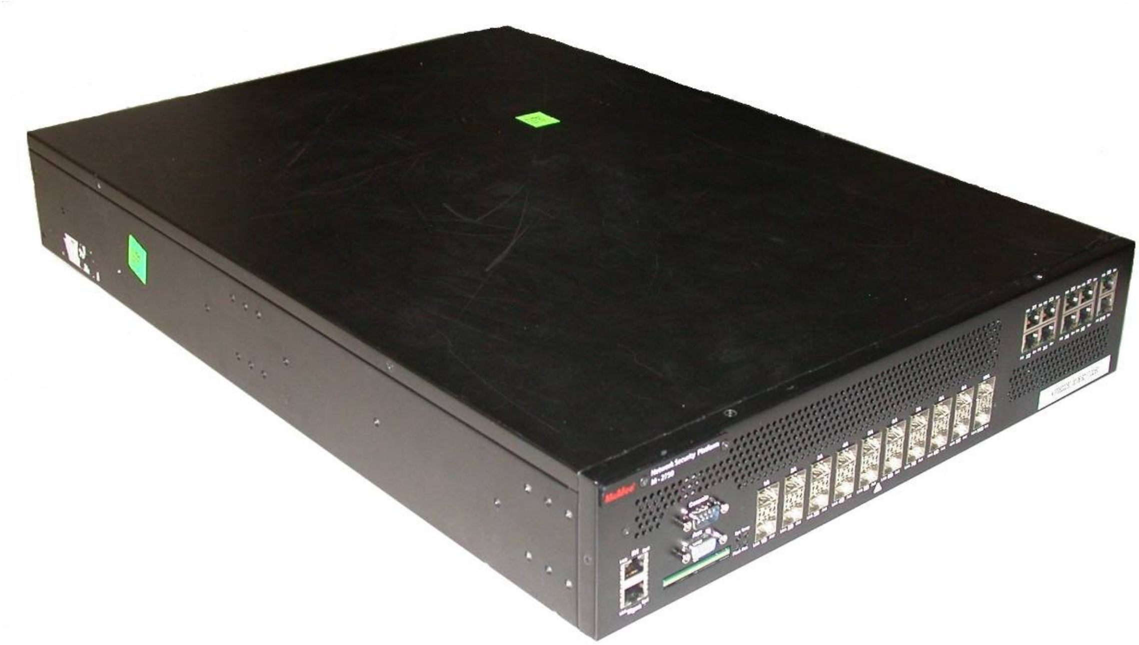


Figure 3 – Image of the M-2850/M-2950

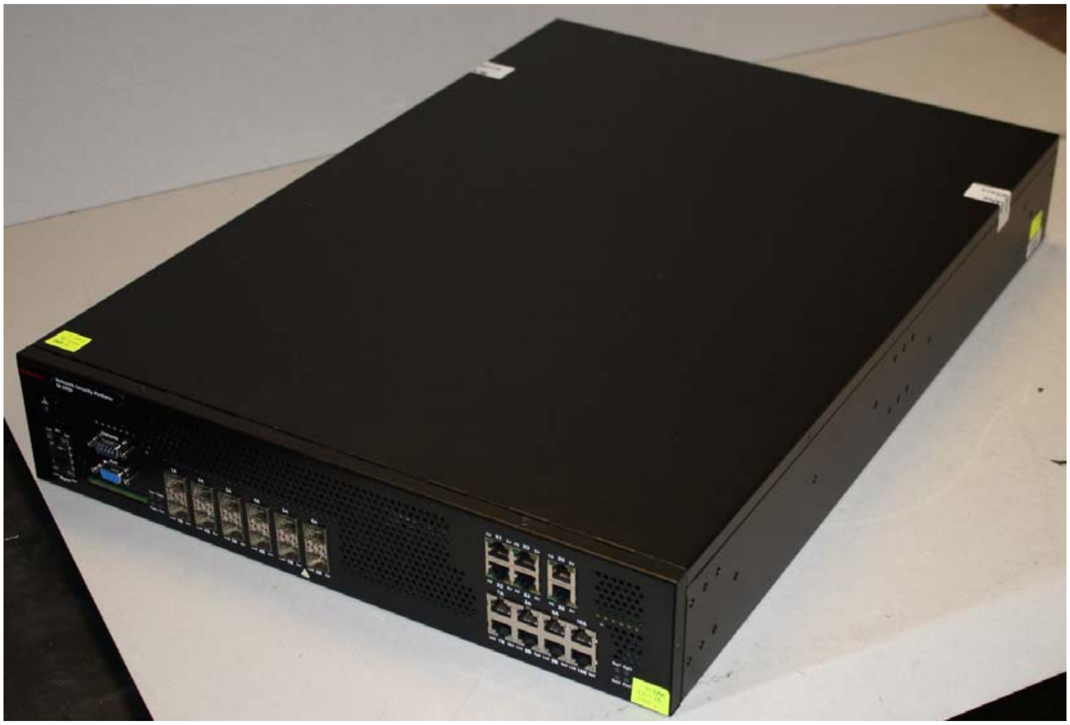


Figure 4 – Image of the M-3050/M-4050

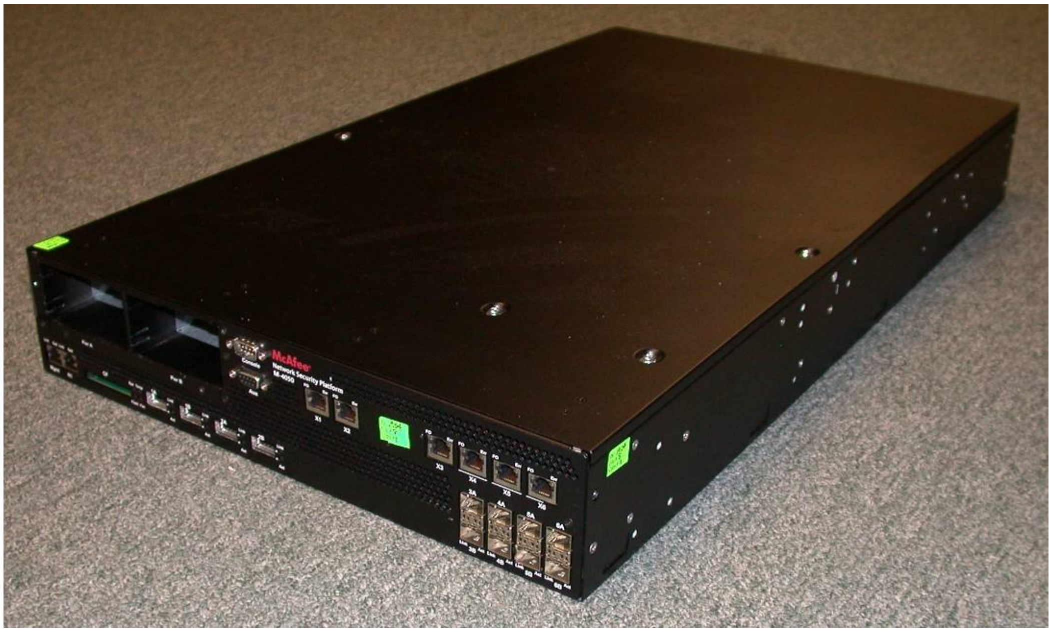
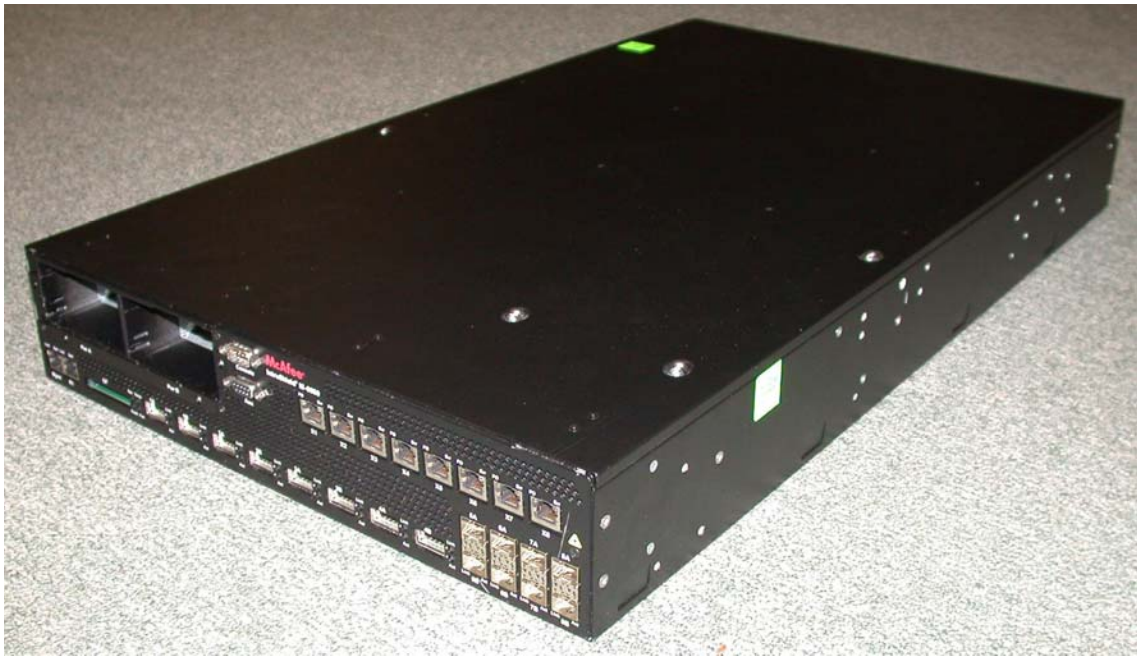


Figure 5 – Image of the M-6050



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 Modes 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 module supports the following FIPS Approved algorithms:

- AES CBC mode with 128 bits for encryption and decryption (Cert. #880)
- Triple-DES CBC mode with 2 and 3 keys for encryption and decryption (Cert. #781) *(Note: 2-key Triple-DES encryption is Restricted per SP 800-131A and will be Disallowed in 2016. 2-key Triple-DES decryption will continue to be acceptable for Legacy-use.)*
- RSA with 1024 and 2048 bit keys for signature generation/verification (Cert. #425) *(Note: RSA signature generation with 1024 bit keys and 2048 bit keys with SHA-1 is Deprecated per SP 800-131A and will be Disallowed in 2014. RSA signature verification with 1024 bit keys and 2048 bit keys with SHA-1 will continue to be acceptable for Legacy-use.)*
- DSA with 1024 bit keys for key generation, signature generation/verification (Cert. #345) *(Note: DSA key and signature generation with 1024 bit keys is Deprecated per SP 800-131A and will be Disallowed in 2014. DSA signature verification with 1024 bit keys will continue to be acceptable for Legacy-use.)*
- 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-1 and SHA-256 for message authentication (Cert. #971)
- 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)

The module supports the following FIPS allowed algorithms and protocols:

- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength) *(Note: Non SP 800-56B Key Transport Schemes providing < 112 bits of strength are Deprecated per SP 800-131A and will be Disallowed in 2014.)*
- Diffie-Hellman (key agreement; key establishment methodology provides 80 of encryption strength) *(Note: Non SP 800-56A Key Agreement Schemes providing < 112 bits of strength are Deprecated per SP 800-131A and will be Disallowed in 2014.)*
- NDRNG for seeding the ANSI X9.31 RNG
- TLS v1.0 with the following cipher suites:
  - TLS_RSA_WITH_AES_128_CBC_SHA for communication with Network Security Platform (NSP) Manager

  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA for communication with McAfee Network Access Control (MNAC) Server

- SSH v2 with the following cipher suites:
  - Key Exchange methods (i.e., key establishment methods): Diffie-hellman-group-exchange-SHAl, Diffie-hellman-group1-SHAl, Diffie-hellman-group14-SHAl
  - Public Key methods (i.e., authentication methods): SSH-DSS, SSH-RSA
  - Encryption methods: 3DES-CBC, AES128-CBC
  - MAC methods: HMAC-SHA1, HMAC-SHAl-96
- SSLv2/3 in addition to TLS used by web portal (no security claimed)
- HMAC MD5 for verifying MNAC Agent UDP messages (no security claimed)
- MD5 used to identify “fingerprint” of potential malware using Artemis database (no security claimed)

4 Ports and Interfaces

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

Table 2 – Ports Quantities 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 (SNMP, 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.

The module supports the following communication channels with the McAfee Network Access Control (MNAC) Server:

- Install channel: Only used to associate a Sensor with the MNAC Server. They use a “shared secret”. This is not manually provided by user on CLI, but comes via Command channel setup with ISM used to get shared secret to install this channel. MNAC Server listening on port 8443.
- Trusted channel (TLS): MNACserver listening on port 8444.
- Asynchronous MNAC Server Message channel (TLS): Service spawned after setup of MNAC Server ‘Trusted channel’ is complete. The MNAC Agent UID response is an example of such a message to the sensor. Sensor listening on port 8554.

5 Identification and Authentication Policy

The cryptographic module supports four distinct "User" roles (Admin, Sensor Operator(s), MNAC Server, 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
MNAC Server	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. The probability of successfully authenticating to the module within one minute is 3/90^15 which is less than 1/100,000.

Authentication Mechanism	Strength of Mechanism
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 a single digital signature verification per second. The probability of successfully authenticating to the module within one minute is 60/2^80 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, 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 attempt per millisecond, meaning that 60,000 attempts can be made per minute. The probability of successfully authenticating to the module within one minute 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.

Table 5 – Services Authorized for Roles

Admin	Sensor Operator(s)	NSP Manager	MNAC Server	3rd Party SNMP Client(s)	**Authorized Services**
X	X	X	X		**Show Status**: Provides the status of the module, usage statistics, log data, and alerts.
X					**Sensor Operator Management:** Allows Admin to add/delete Sensor Operators, 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			**NAC Network Configuration**: Establish network settings for each traffic monitoring port prior to enabling NAC.
X	X	X			**Administrative Configuration:** Other various services provided for admin, private, and support levels.
		X			**NAC Administrative Configuration:** Other various services provided for admin, private, and support levels Matrix MNACserver responsible for ensuring crypto aspects of secure channels between sensor and MNACserver.
X	X	X			**Firmware Update**: Install an external firmware image through TFTP or compact flash.
X	X				**Install with ISM**: Configures module for use. This step includes establishing trust between the module and the associated management station.
		X	X		**Install with MNAC Server:** Configures module for NAC use. This step includes establishing trust between the module and the associated MNAC server station. Shared key provided by ISM not by Admin via CLI.
		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 ISM.

Admin	Sensor Operator(s)	NSP Manager	MNAC Server	3rd Party SNMP Client(s)	**Authorized Services**
X	X				**Change Passwords**: Allows Admin and Sensor Operators to change their associated passwords. Admin can also change/reset Sensor Operators passwords.
		X			**NAC Certificate Management:** Provides the Admin/ISM/MNACserver the ability to install and export certificates.
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.
				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.
			X		**Process asynchronous NAC Agent Messages:** Process messages regarding health levels and status changes of MNAC Agents. The MNAC Server provides the shared secret used as key for HMAC

<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.
- **MNAC Agent Messages:** Receive UDP based messages from MNAC Agents. Traffic from the particular MNAC Agent. The data identifies the end host information and health as broadcast by MNACAgent running on it. *Note:* The only cryptography performed during this service is an MD5 hash.
- **Web Portal Usage:** Allows a pass through of SSL based HTTPS sessions. *Note:* No cryptography or FIPS Approved functions are performed on the Sensor during this service.

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.
- **ISM Initialization Secret (i.e., ISM Shared Secret)**: Password used for mutual authentication of the sensor and ISM during initialization.
- **Bulk Transfer Channel Session Key**: AES 128 bit key used to encrypt data packages across the bulk transfer channel.
- **MNAC Initialization Secret (i.e., MNAC Shared Secret)**: Password used for mutual authentication parameter for the Sensor and MNAC server during initialization.
- **SSH Host Private Keys**: DSA or RSA 1024 bit key used for authentication of sensor to remote terminal for CLI access.
- **SSH Session Keys**: Set of ephemeral Diffie-Hellman, Triple-DES or AES, and HMAC keys created for each SSH session.
- **TLS Sensor Private Key (for ISM)**: RSA 1024 bit key used for authentication of the sensor to ISM.
- **TLS Session Keys (for ISM)**: Set of ephemeral AES and HMAC keys created for each TLS session with the ISM.
- **TLS Sensor Private Key (for MNAC)**: RSA 1024 bit key used for authentication of the sensor to MNAC server.
- **TLS Session Keys (for MNAC)**: Set of ephemeral Diffie-Hellman, AES, and HMAC keys created for each TLS session with the MNAC Server.
- **Seed for RNG**: Seed created by NDRNG and used to seed the ANSI X9.31 RNG.
- **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:

- **McAfee FW Verification Key**: RSA 2048 bit key used to authenticate firmware images loaded into the module.

- **SSH Host Public Key**: DSA or RSA 1024 bit key used to authenticate the sensor to the remote client during SSH.
- **SSH Remote Client Public Key**: DSA or RSA 1024 bit key used to authenticate the remote client to the sensor during SSH.
- **TLS Sensor Public Key (for ISM):** RSA 1024 bit key used to authenticate the sensor to ISM during TLS connections.
- **TLS ISM Public Key**: RSA 1024 bit key used to authenticate ISM to sensor during TLS connections.
- **TLS Sensor Public Key (for MNAC):** RSA 1024 bit key used to authenticate the sensor to MNAC Server during TLS connections.
- **TLS MNAC Server Public Key**: RSA 1024 bit key used to authenticate MNAC Server to sensor during TLS connections.
- **Root MNAC Public Key**: RSA 1024 bit key used to verify the authenticity of the MNAC Server.

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	MNAC Initialization Secret	SSH Host Private Keys	SSH Session Keys	TLS Sensor Private Key (for ISM)	TLS Session Keys (for ISM)	TLS Sensor Private Key (for MNAC)	TLS Session Keys (for MNAC)	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	TLS Sensor Public Key (for MNAC)	TLS MNAC Server Public Key	Root MNAC Public Key
Show Status	R			R	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			
NAC Network Configuration						R	R		R	R						R	R			R	R	R
Administrative Configuration				R			R		R	R						R	R	R	R			
NAC Administrative Configuration						R	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 MNAC Server						R W					R W	R W	R W	R W						R W	R W	R W
Install with 3rd Party SNMP Client			R W																			
Change Passwords	R W						R									R	R					
NAC Certificate Management									R	R	R W									R W	R W	R W
Zeroize	Z*	Z*	Z	Z	Z	Z	R Z	Z	Z	Z	Z	Z	Z	Z	Z	R	R					
Intrusion Detection/Prevention Management					R				R	R								R	R			
Intrusion Detection/Prevention Monitoring			R			R																

	Administrator Passwords	Sensor Operator Passwords	3rd Party SNMP Client P and A Keys	ISM Initialization Secret	Bulk Transfer Channel Session Key	MNAC Initialization Secret	SSH Host Private Keys	SSH Session Keys	TLS Sensor Private Key (for ISM)	TLS Session Keys (for ISM)	TLS Sensor Private Key (for MNAC)	TLS Session Keys (for MNAC)	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	TLS Sensor Public Key (for MNAC)	TLS MNAC Server Public Key	Root MNAC Public Key
Process asynchronous NAC Agent Messages											R	R								R	R	R
Disable SSH/Console Access																						
Self Tests																						
Intrusion Prevention Services																						
MNAC Agent Message																						
Web Portal Usage																						

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, MNAC Server, 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:
         - a. AES CBC 128 encryption/decryption Known Answer Tests
         - b. Triple-DES CBC encryption/decryption Known Answer Tests
         - c. RSA 1024 and 2048 Sign/Verify Known Answer Test
         - d. DSA 1024 Sign/Verify Known Answer Test
         - e. SHA-1 Known Answer Test
         - f. SHA-256 Known Answer Test
         - g. ANSI X9.31 RNG Known Answer Test
         - h. RSA 1024 Decrypt Known Answer Test
         - i. HMAC SHA-1 Known Answer Test
         - j. HMAC SHA-256 Known Answer Test
         - k. XYSSL RSA 2048 Verify Known Answer Test
         - l. XYSSL SHA-1 Known Answer Test
      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.

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)

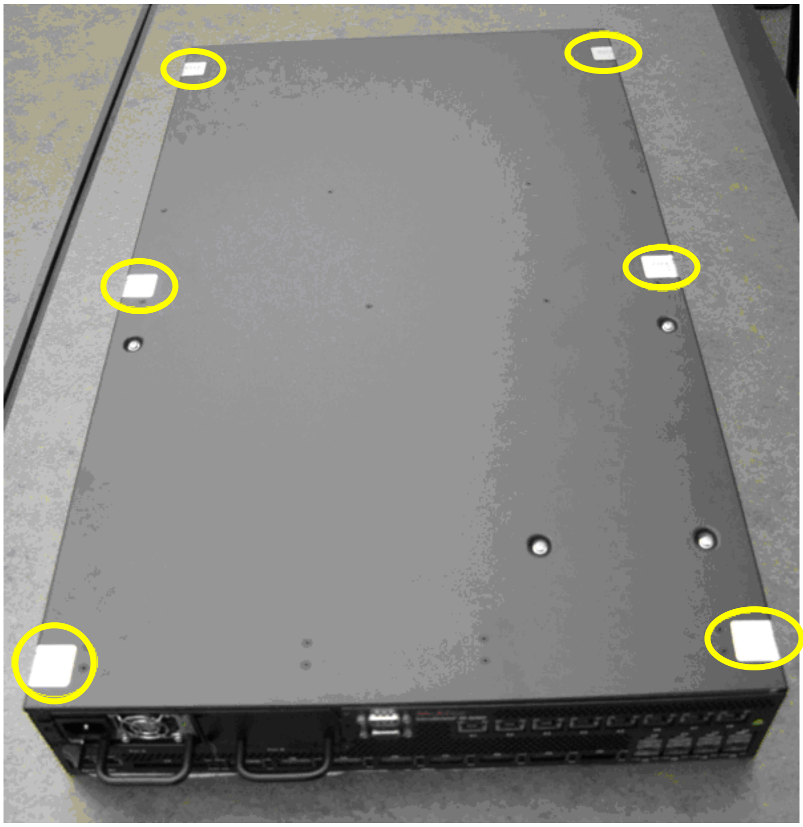


Figure 7 depicts the tamper label locations on the cryptographic module for the M-1250 and M-1450 platforms. There are 8 tamper labels and they are circled in yellow.

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

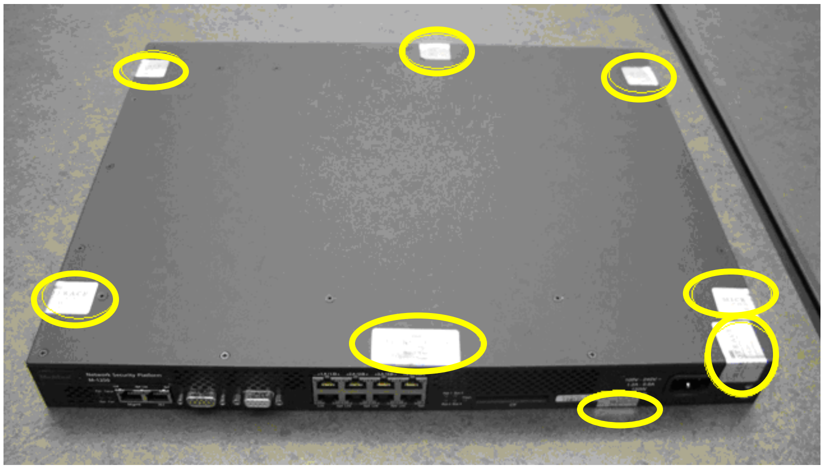
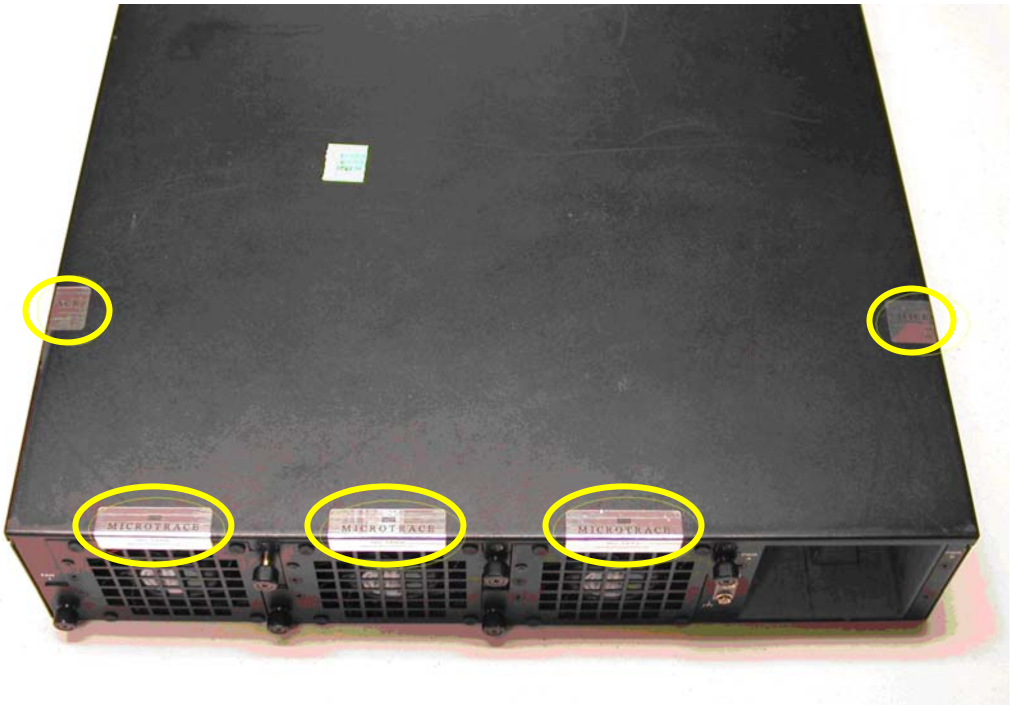


Figure 8 depicts the tamper label locations on the cryptographic module for the M-2750, M-2850, and M-2950 platforms. There are 5 tamper labels and they are circled in yellow.

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.