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

Security Policy

Version 1.9

January 22, 2010

TABLE OF CONTENTS

1 Module Overview

The Network Security Platform Sensor M-1250, M-1450, M-2750, M-3050, M-4050, and M-6050 (HW P/Ns M-1250 Version 1.10, M-1450 Version 1.10, M-2750 Version 1.50, M-3050 Version 1.20, M-4050 Version 1.20, and M-6050 Version 1.40; FW Version 5.1.15.12) consists of the following multi-chip standalone platforms/configurations: M-1250, M-1450, M-2750, M-3050, M-4050, and M-6050. They are all Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) designed for network protection. Both will offer 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: The removable fan trays are protected with tamper seals (see Figure 7). 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 4 show the module configurations and their cryptographic boundaries.

Figure 1 – Image of the M-1250/M-1450

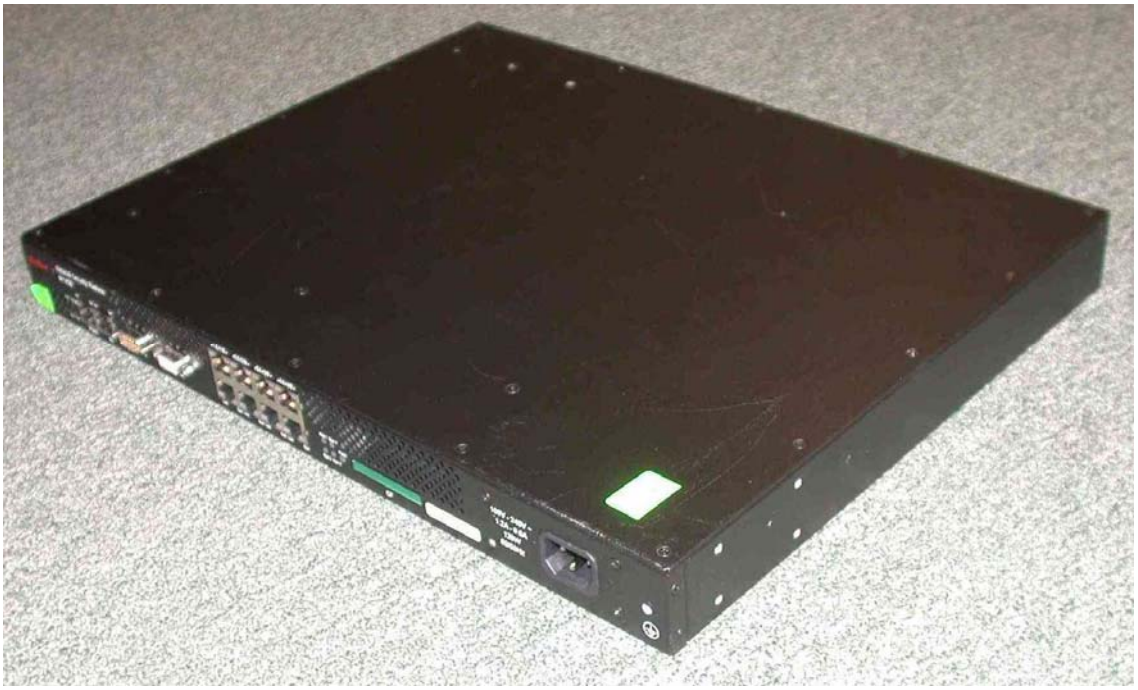


Figure 2 – Image of the M-2750

Figure 3 – Image of the M-3050/M-4050

Figure 4 – 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	3
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 versions will need to match the FIPS validated versions located on the CMVP website.

3.1 FIPS Approved Mode of Operation

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)
- RSA with 1024 and 2048 bit keys for signature generation/verification (Cert. #425)
- DSA with 1024 bit keys for key generation, signature generation/verification (Cert. #345)
- SHA-1 and SHA-256 for hashing (Cert. #871)
- ANSI X9.31 RNG with 2-Key Triple-DES ECB (Cert. #505)
- XYSSL RSA with 2048 bit keys for image verify (Cert. #486)
- XYSSL SHA-1 for hashing (Cert. #970)

The module supports the following FIPS allowed algorithms and protocols:

- RSA with 1024 bit keys for key wrap decryption only (of bulk channel encryption/decryption key) – key wrapping; key establishment methodology provides 80 bits of encryption strength
- NDRNG for seeding the ANSI X9.31 RNG
- TLS v1.0 (with algorithm tested ciphers)
- SSH v2 (with algorithm tested ciphers)
- SSLv2/3 in addition to TLS used by web portal (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-3050**	**M-4050**	**M-6050**
10-Gig Monitoring Ports *(Data Input/Output)*	0	0	0	8	8	8
1-GigE Monitoring Ports *(Data Input/Output)*	8	8	20	8	8	8
GigE Management Port *(Control Input, Data Output, Status Output)*	1	1	1	1	1	1
GigE Response Port *(Data Output)*	1	1	1	1	1	1
RS232 Console/Aux Ports *(Control Input, Status Output)*	2	2	2	2	2	2
Compact Flash *(Data Input)*	1	1	1	1	1	1
Power Ports *(Power Input)*	1	1	2	2	2	2
RJ11 Control Port *(Data Input, Power Output)*	0	0	10	8	8	8
LEDs *(Status Output)*						

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): SNMP master agent listening on port 8500
- Bulk transfer channel (All is encrypted output): 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 shall support two distinct operator roles (Admin and Network Security Platform Manager). The cryptographic module shall enforce the separation of roles using role-based operator authentication. 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 (User)	Role-based operator authentication	Username and Password
Network Security Platform Manager (Cryptographic Officer)	Role-based operator authentication	Digital Signature (TLS), SNMPv3 Shared Secret

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 characters chosen from the set of 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 failed authentication attempts, the module will enforce a 1 minute delay prior to allowing retry. The probability of successfully authenticating to the module within one minute is also 3/90^15 which are 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 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.

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

Authorized Services		
Admin	NSP Manager	
X	X	**Show Status**: Provides the status of the module, usage statistics, log data, and alerts.
X	X	**Network Configuration**: Establish network settings for the module or set them back to default values.
X	X	**Administrative Configuration:** Other various services provided for admin, private, and support levels.
X	X	**Firmware Update**: Install an external firmware image through TFTP or compact flash.
X		**Install with ISM**: Configures module for use. This step includes establishing trust between the module and the associated management station.
X		**Change Passwords**: Allows the Admin to change their associated passwords.
X		**Certificate Management**: Provides the Admin the ability to install and export certificates.
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		**Disable Admin:** Disables SSH and Console.

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:* No crypto is performed 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 services are given to the "admin" role by using the "support" or "private" passwords.
- **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.
- **SSH Host Private Keys**: DSA or RSA 1024 bit key used for authentication of sensor to remote terminal for CLI access.
- **TLS Sensor Private Key (for ISM)**: RSA 1024 bit key used for authentication of the sensor to ISM.
- **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.

.

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).

Table 6 – Key and CSP Access Rights within Services

	Administrator Passwords	ISM Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	TLS Sensor Private Key (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
Network Configuration		R		R	R				R	R	R	R
Administrative Configuration		R		R	R				R	R	R	R
Firmware Update		R		R	R				R	R	R	R
Install with ISM				R	R W	R W	R W		R	R	R W	R W
Change Passwords	R W			R					R	R		
Certificate Management				R				R W	R W	R W	R W	R W
Zeroize		Z	Z	R Z	Z	Z	Z		R	R		
Intrusion Detection/Prevention Management			R		R						R	R
Disable Admin												
Self Tests												
Intrusion Prevention Services												

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 two distinct operator roles: Admin, and Network Security Platform Manager.
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. XYSSL RSA 2048 Verify Known Answer Test
         j. 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. The module shall only support five concurrent SSH operators when SSH is enabled.
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 use of the Console Port 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.

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 (Note: Tamper evident seals are obtained in the FIPS Kit)

9.2 Operator Required Actions

For the module to operate in a FIPS Approved mode, the tamper seals shall be placed by the Admin as specified below. 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 5 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 5 – Tamper Label Placement (M-3050, M-4050, and M-6050)

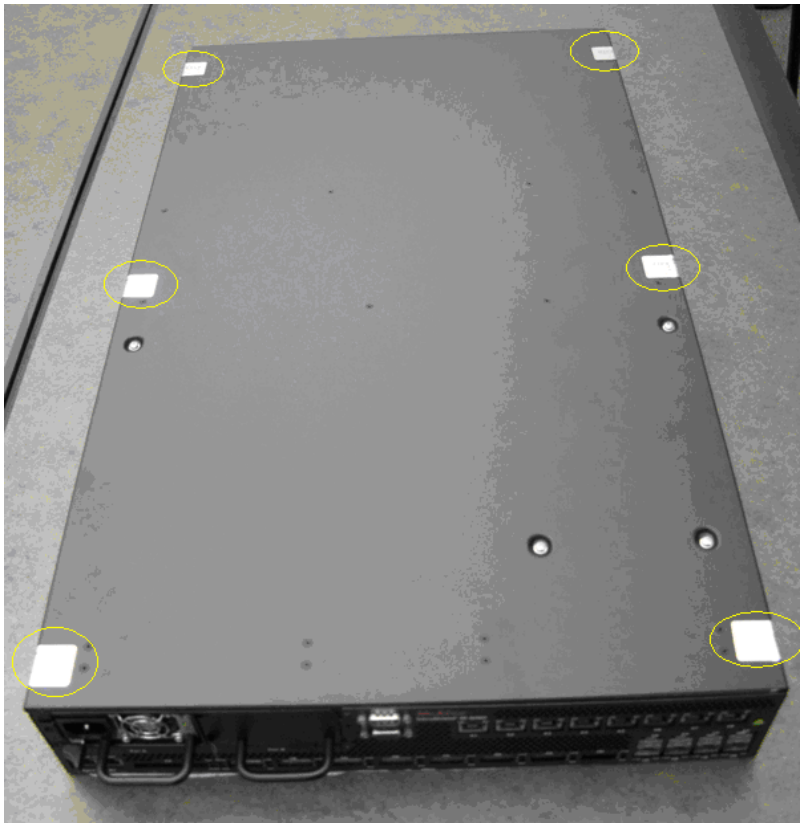
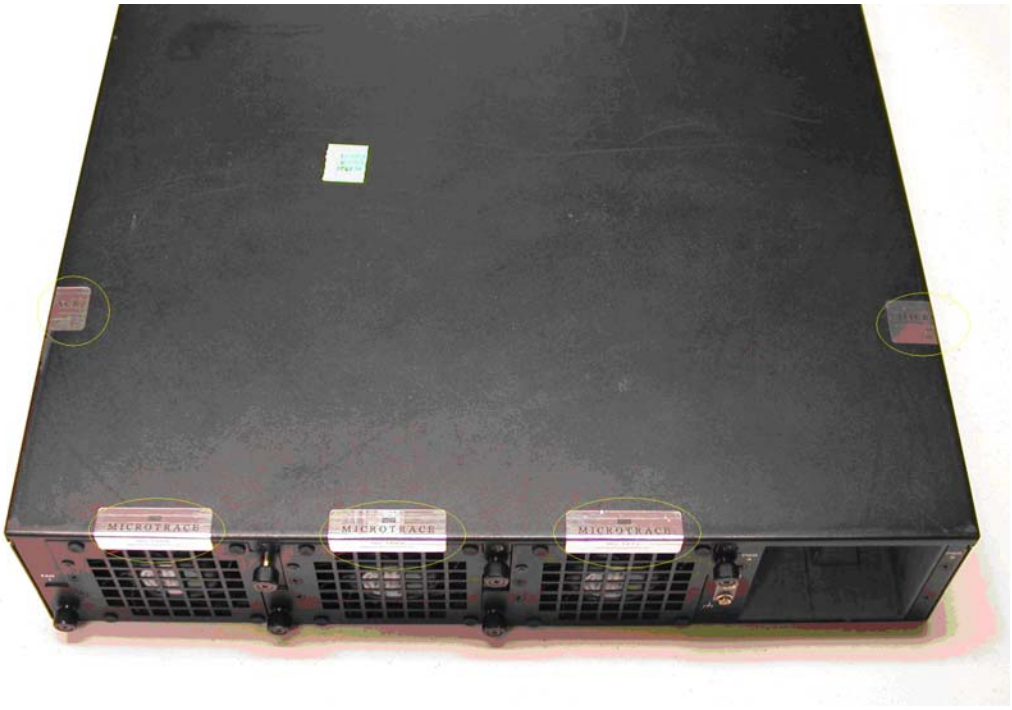


Figure 6 depicts the tamper label locations on the cryptographic module for the M-1250 and M-1450 platforms. There are 8 tamper labels and they are circled in yellow.

Figure 6 – Tamper Label Placement (M-1250 and M-1450)

Figure 7 depicts the tamper label locations on the cryptographic module for the M-2750 platform. There are 5 tamper labels and they are circled in yellow.

Figure 7 – Tamper Label Placement (M-2750)



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.