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

Security Policy
Version 1.17

March 20, 2014

TABLE OF CONTENTS

1 MODULE OVERVIEW 3

2 SECURITY LEVEL 4

3 MODES OF OPERATION 5

3.1 FIPS APPROVED MODE OF OPERATION 5
3.2 NON-APPROVED MODE OF OPERATION 6

4 PORTS AND INTERFACES 7

5 IDENTIFICATION AND AUTHENTICATION POLICY 8

6 ACCESS CONTROL POLICY 9

6.1 ROLES AND SERVICES 9
6.2 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 10
6.3 DEFINITION OF PUBLIC KEYS: 10
6.4 DEFINITION OF CSPS MODES OF ACCESS 10

7 OPERATIONAL ENVIRONMENT 12

8 SECURITY RULES 12

9 PHYSICAL SECURITY POLICY 13

9.1 PHYSICAL SECURITY MECHANISMS 13
9.2 OPERATOR REQUIRED ACTIONS 13

10 MITIGATION OF OTHER ATTACKS POLICY 14

1 Module Overview

The Network Security Platform (NSP) Sensor M-8000 S (HW P/N M-8000 S, Version 1.40; FW Version 7.1.15.4; FIPS Kit P/N IAC-FIPS-KT8) 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 S only.

Figure 1 shows the module and its cryptographic boundary.

Figure 1 – Image of the Cryptographic Module

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 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 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.)
- 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-1 and HMAC-SHA-256 for message authentication (Cert. #971)
- FIPS 186-2 XYSSL RSA with 2048 bit keys for signature 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 verify (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
- SSH v2 (used during Initialization Process with the M-8000 P only) 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
- 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 which are Disallowed as of January 1, 2014 per the NIST SP 800-131A algorithm transitions:

- FIPS 186-2 RSA signature generation with 1024 and 2048 bit keys using SHA-1 (Cert. #425)
- FIPS 186-2 DSA with 1024 bit keys for key generation and signature generation (Cert. #345)
- Diffie-Hellman key agreement (key establishment methodology provides 80 bits of encryption strength; non-compliant)

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 are used (see Sections 6.1, 6.2 and 6.3):

<u>CSPs</u>

- SSH Host Private Keys
- SSH Session Keys

<u>Public Keys</u>

- SSH Host Public Key
- SSH Remote Client Public Key

<u>Services</u>

- Show Status
- Network Configuration
- Administrative Configuration
- Firmware Update
- Change Passwords
- Zeroize
- Intrusion Detection/Prevention Management

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 ports and interfaces.

Table 2 – Ports and Interfaces

Physical Ports	Logical Interfaces	Qty.
10-Gig Monitoring Ports	Data Input/Output	8
1-GigE Monitoring Ports	Data Input/Output	8
GigE Management Port	Control Input, Data Output, Status Output	1
GigE Response Port	Data Output	1
RS232 Console/Aux Ports	Control Input, Status Output	2
Compact Flash	Data Input	1
Power Ports	Power Input	2
RJ11 Control Port	Data Input, Power Output	8
LEDs	Status Output	many

Notes:

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

5 Identification and Authentication Policy

The cryptographic module shall support two distinct operator roles (Admin and M-8000 P). 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
M-8000 P (Cryptographic Officer)	Role-based operator authentication	Username and Password

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password (Admin)	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.
Username and Password (M-8000 P)	The password is an alphanumeric string of a minimum of eight (8) 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 1/90^8 which is less than 1/1,000,000. After one (1) failed authentication attempt, the module requires a reboot prior to allowing retry which takes longer than one minute. The probability of successfully authenticating to the module within one minute through random attempts is 1/90^8 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	M-8000 P	
X	X	**Show Status**: Provides the status of the module, usage statistics, log data, and alerts.
X		**Network Configuration**: Establish network settings for the module or set them back to default values.
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		**Change Passwords**: Allows the Admin to change their associated passwords and the M-8000 Password.
X		**Zeroize**: Destroys all plaintext secrets contained within the module.
	X	**Intrusion Detection/Prevention Management**: Management of intrusion detection/prevention policies and configurations.

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:* The only cryptography performed during this service is an MD5 hash to identify the "fingerprint" of malware

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. Extended services are given to the "admin" role by using the "support" or "private" passwords.
- **M-8000 Password:** Password used for authentication of M-8000 P.
- **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.
- **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 used in the ANSI X9.31 RNG.

6.3 Definition of Public Keys:

The following public key is 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.

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	M-8000 Password	SSH Host Private Keys	SSH Session Keys	Seed for RNG	Seed Key for RNG	McAfee FW Verification Key	SSH Host Public Key	SSH Remote Client Public Key
Initialization Process (*not a service*)			R, W	R, W	R, W	R, W		R, W	R, W
Show Status									
Network Configuration									
Administrative Configuration									
Firmware Update							R		
Change Passwords	R, W	R, W							
Zeroize	Z*	Z	Z	Z	Z	Z			
Intrusion Detection/Prevention Management									
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 M-8000 P.
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. HMAC-SHA-1 KAT
         j. HMAC-SHA-256 KAT
         k. XYSSL RSA 2048 Signature Verification KAT
         l. XYSSL SHA-1 KAT
         m. TLS 1.0/1.1 KDF KAT
         n. SSH KDF KAT
      2. Firmware Integrity Test: XYSSL RSA 2048 used
      3. Critical Functions Tests: N/A

   B. Conditional Self-Tests:

      1. ANSI X9.31 RNG Continuous Test
      2. NDRNG Continuous Test
      3. RSA Sign/Verify Pairwise Consistency Test
      4. DSA Sign/Verify Pairwise Consistency Test
      5. External Firmware Load Test – XYSSL RSA 2048 used

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 use of the Console Port/Aux port 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.

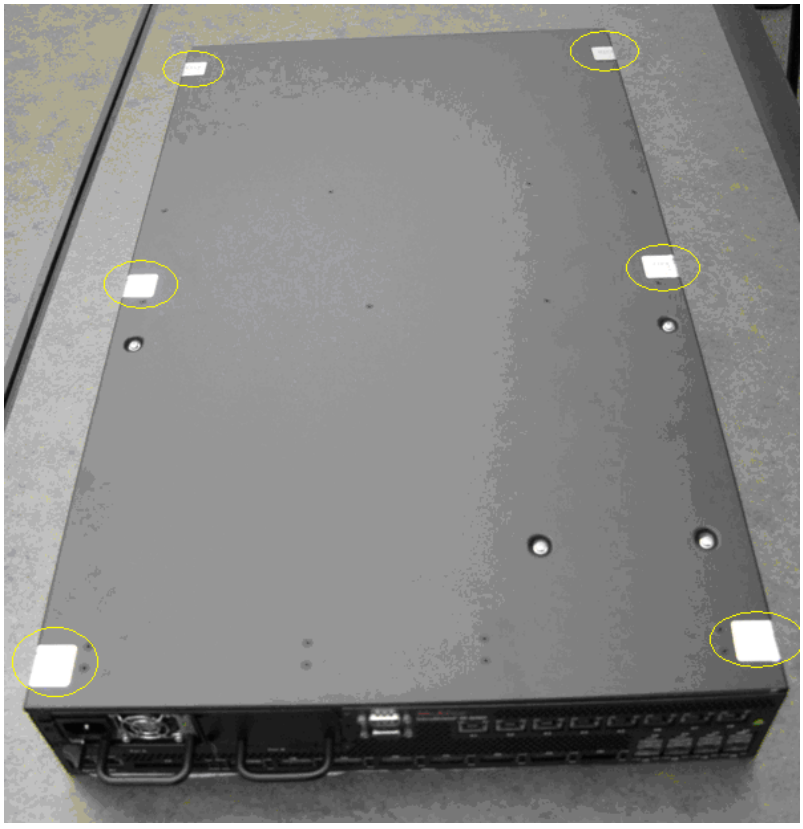
The Admin is also required to periodically inspect tamper evident seals. Table 7 outlines the recommendations for inspecting/testing physical security mechanisms of the module. If evidence of tamper is found during the periodic inspection, the operator should zeroize the module and modify Administrator 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 2 depicts the tamper label locations on the cryptographic module. There are 6 tamper labels and they are circled in yellow.

Figure 2 - Tamper Label Placement for M-8000 S



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.