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

Security Policy
Version 1.9

June 4, 2010

TABLE OF CONTENTS

1 Module Overview

The Network Security Platform (NSP) Sensor M-8000 S (HW P/N M-8000 S, Version 1.40; FW Version 5.1.15.12) 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. The M-8000 S 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. 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	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 modules 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 signature verification (Cert. #486)

- XYSSL SHA-1 for hashing (Cert. #970)

The module supports the following FIPS allowed algorithm:

- NDRNG for seeding the ANSI X9.31 RNG

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 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

Note: 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.

The module also contains multiple LEDs for status output.

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	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 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		**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. 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.

- **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.

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/CSP Access Rights within Services

	Administrator Passwords	M-8000 Password	Seed for RNG	Seed Key for RNG	McAfee FW Verification Key
Show Status					
Network Configuration					
Administrative Configuration					
Firmware Update					
Change Passwords	R, W	R, W			
Certificate Management					R, W
Zeroize		Z	Z	Z	
Intrusion Detection/Prevention Management					
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 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:

         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.   XYSSL RSA 2048 Verify Known Answer Test
         i.   XYSSL SHA-1 Known Answer Test

      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 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 (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. 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
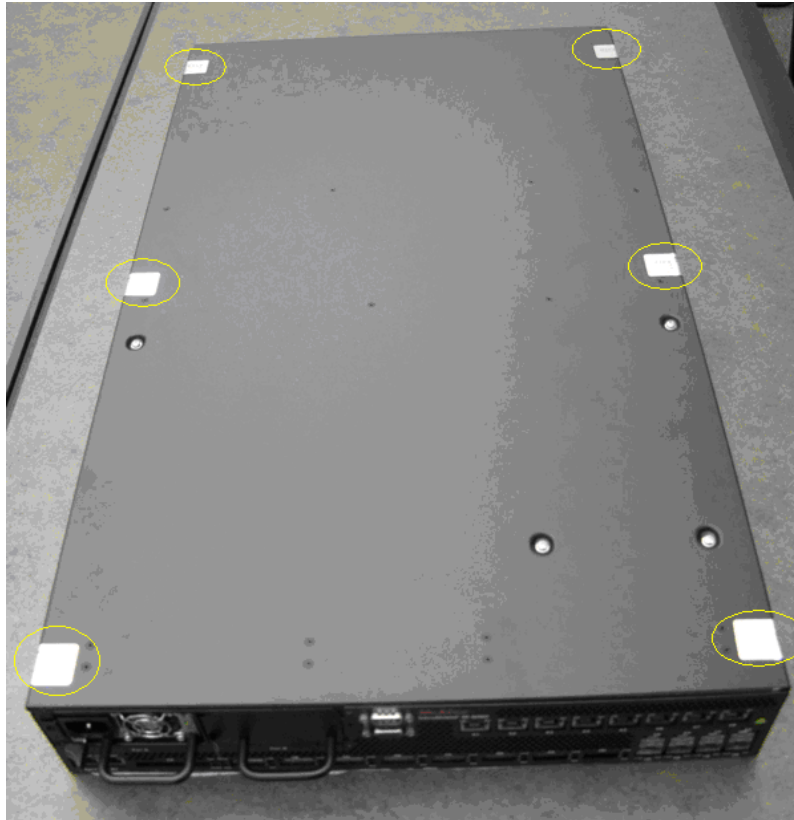
10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.