McAfee, Inc.
Network Security Platform Sensor
N-450

Security Policy
Version 1.7

March 29, 2010

TABLE OF CONTENTS

1 Module Overview

The Network Security Platform Sensor N-450 (HW P/N N-450, Version 1.50; FW Version 5.1.15.2) is a multi-chip standalone module that functions as a Network Access Control (NAC) device. The cryptographic boundary is the outer perimeter of the enclosure, including the power supplies and fan trays.

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 supports both a FIPS Approved and non-FIPS Approved mode of operation. If the module is to switch between the FIPS Approved and non-FIPS Approved mode of operation, the module will zeroize all CSPs and reboot. The cryptographic module may be configured for FIPS mode via execution of the "fips mode enable" command on the Command Line Interface (CLI) and operating the device per the Security Rules in Section 8. The cryptographic module may be configured for non-FIPS mode via execution of the "fips mode disable" command on the CLI. The user can determine if the module is running in FIPS vs. non-FIPS mode by executing the "show fips mode status" CLI command. The module provides additional status information when the "show" or "status" CLI commands are called (e.g., FW version, HW version, health, FIPS violations, etc.).

3.1 FIPS Approved Mode of Operation

In FIPS mode, 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)

In FIPS mode, 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)
- HMAC MD5 for verifying MNAC Agent UDP messages (no security claimed)

3.2 Non-FIPS Approved Mode of Operation

In non-FIPS mode, the module supports the following non-FIPS Approved algorithms:

- Blowfish for encryption
- DES for encryption/decryption
- MD5
- TACACS

4 Ports and Interfaces

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

Table 2 – Port Quantities per Platform

Ports*(Input/Output Type)*	**Port Quantities**
1-GigE Monitoring Ports *(Data Input/Output)*	20
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 Port *(Power Input)*	2
RJ11 Control Port *(Data Input, Power Output)*	10

The module also contains multiple LEDs for 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.

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 shall support three distinct operator roles (Admin, Network Security Platform Manager, and MNAC Server). 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
MNAC Server	Role-based operator authentication	Digital Signature (TLS), RSA key wrap

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The password is an alphanumeric string of a minimum of eight characters chosen from the set of 62 printable and human-readable characters. The probability that a random attempt will succeed or a false acceptance will occur is 1/62^8 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 through random attempts is 3/62^8 which is less than 1/100,000.
Digital Signature and RSA key wrap	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 through random attempts 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. Following Table 5, all unauthenticated services are listed.

Table 5 – Services Authorized for Roles

Role			Authorized Services
Admin	NSP Manager	MNAC Server	
X	X	X	**Show Status**: Provides 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		**NAC Network Configuration**: Establish network settings for each traffic monitoring port prior to enabling NAC.
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		**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	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			**Change Passwords**: Allows the Admin to change their associated passwords.
X			**Certificate Management**: Provides the Admin the ability to install and export certificates.
	X		**NAC Certificate Management:** Provides the Admin/ISM/MNACserver the ability to install and export certificates.
X			**Zeroize**: Destroys all plaintext secrets contained within the module.
		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.

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.
- **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 tunning on it. This data is hashed with MD5 and signed with HMAC using a mutual shared-secret (by sensor and agent).
- **Web Portal Usage:** SSL based HTTPS session (for end user/host redirected to web portal). Connection type and cipher determined by client end browser.

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.
- **MNAC Initialization Secret (i.e., MNAC Shared Secret)**: Password used for mutual authentication parameter for the Sensor and MNAC server during initialization.
- **TLS Sensor Private Key (for ISM)**: RSA 1024 bit key used for authentication of the sensor to ISM.
- **TLS Sensor Private Key (for MNAC)**: RSA 1024 bit key used for authentication of the sensor to 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 used 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 and 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	ISM Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	MNAC Initialization Secret	TLS Sensor Private Key (for ISM)	TLS Sensor Private Key (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			
Network Configuration		R		R		R					R	R	R	R			
NAC Network Configuration				R	R		R				R	R			R	R	R
Administrative Configuration		R		R		R					R	R	R	R			
NAC Administrative Configuration				R	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			
Install with MNAC Server					R W		R W	R W	R W						R W	R W	R W

	Administrator Passwords	ISM Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	MNAC Initialization Secret	TLS Sensor Private Key (for ISM)	TLS Sensor Private Key (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
Change Passwords	R W			R							R	R					
Certificate Management				R						R W	R W	R W	R W	R W			
NAC Certificate Management					R W		R W								R W	R W	R W
Zeroize		Z	Z	R Z	Z	Z	Z	Z	Z		R	R			Z	Z	Z
Process asynchronous NAC Agent Messages					R		R								R	R	R
Self Tests																	
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 three distinct operator roles: Admin, Network Security Platform Manager, and MNAC Server.
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.
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

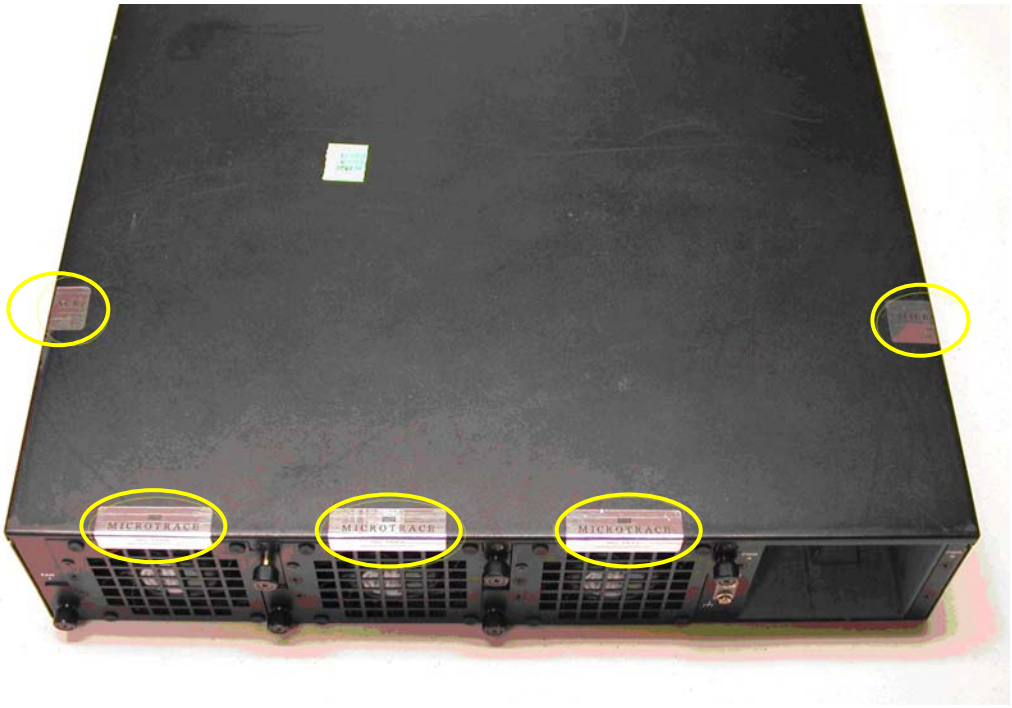
For the module to operate in a FIPS Approved mode, the tamper evident seals shall be placed by the Admin as specified below. The Admin is also required to periodically inspect tamper evident seals. Table 7 outlines the recommendations for inspecting/testing physical security mechanisms of the module.

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 seals 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 evident seal locations on the cryptographic module for the N-450 platform. There are 5 tamper evident seals and they are circled in yellow.

Figure 2 – Tamper Evident Seal Placement (N-450)



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.