McAfee, Inc.
Network Security Platform Sensor

NS-9100 and NS-9200

Non-Proprietary Security Policy
Version 1.2

April 8, 2016

TABLE OF CONTENTS

1 Module Overview

The Network Security Platform Sensor NS-9100 and NS-9200 consists of the following multi-chip standalone platforms/configurations:

- NS-9100 (HW P/N NS-9100 Versions 1.2 and 1.3; FIPS Kit P/N IAC-FIPS-KT2)
- NS-9200 (HW P/N NS-9200 Versions 1.2 and 1.3; FIPS Kit P/N IAC-FIPS-KT2)

The following minor differences exist between the hardware configurations:

- P/Ns NS-9100 and NS-9200 differ only in memory capacity (64GB for NS-9100, 128GB for NS-9200).
- HW Version 1.2 was updated to HW Version 1.3 due to replacement of a non-security relevant internal component that was end of life. The component does not affect physical security.

All module configurations include FW Version 8.1.17.16.

They are 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.

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:

- NS-9100/NS-9200: The optional network I/O modules are not included in the module boundary. The removable fan trays are protected by tamper seals. The removable power supplies are excluded from FIPS 140-2 requirements, as they are non-security relevant.

Figure 1 shows the module configuration and the cryptographic boundaries.

Figure 1 – Image of NS-9100/NS-9200

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 Mode of Operation

3.1 FIPS Approved Mode 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.

Approved Algorithms

The module supports the following FIPS Approved algorithms:

- AES CBC and ECB mode with 128 & 256 bits for encryption and decryption (Cert. #3156)
- FIPS 186-4 RSA PSS with 2048 bit keys for key generation, signature generation with SHA-256 and SHA-512, and signature verification with SHA-1, SHA-256, and SHA-512 (Cert. #1600)

  *(*SHA-1, SHA-256, and SHA-512 for hashing (Cert. #2612)

  (Note: SHA-1 validated for use in TLS and verification-purposes only.)
- HMAC SHA-1, SHA-256, and SHA-512 for message authentication (Cert. #1989)

  (Note: The minimum HMAC key size is 20 bytes.)
- Block Cipher (CTR) DRBG using AES 256 (Cert. #649)
- FIPS 186-4 XYSSL RSA PKCS #1 1.5 SigVer with 2048 bit keys using SHA-1 and SHA-256 for image verification (Cert. #1825)
- XYSSL SHA-1 and SHA-256 for hashing and for use with image verification (Cert. #2923)
- TLS v1.0/1.1 KDF for TLS session key derivation (CVL Cert. #409)
- SSH KDF for SSH session key derivation (CVL Cert. #599)

Allowed Algorithms and Protocols

The module supports the following FIPS allowed algorithms and protocols:

- RSA with 2048-bit keys for key wrapping (key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman with 2048-bit keys for key agreement (key establishment methodology provides 112 bits of encryption strength)
- NDRNG for seeding the Block Cipher (CTR) DRBG.
- TLS v1.0 with the following algorithm tested cipher suites. The protocol algorithms have been tested by the CAVP (see certificate #s above) but the protocol implementation itself has not been reviewed or tested by the CAVP or CMVP.
  - TLS_RSA_WITH_AES_128_CBC_SHA for communication with Network Security Platform (NSP) Manager

    (Note: This is restricted to RSA-2048)
- SSH v2 with the following algorithm tested cipher suites. The protocol algorithms have been tested by the CAVP (see certificate #s above) but the protocol implementation itself has not been reviewed or tested by the CAVP or CMVP.
  - Key Exchange methods (i.e., key establishment methods): Diffie-hellman-group14-SHAl

- Public Key methods (i.e., authentication methods): SSH-RSA
  (Note: This is restricted to RSA-2048)
- Encryption methods: AES128-CBC, AES256-CBC
- MAC methods: HMAC-SHA1, HMAC-SHAl-96, HMAC-256, HMAC-512

Non-Approved Algorithms and Protocols with No Security Claimed

The module supports the following non-Approved but allowed algorithms and protocols with no security claimed:

- MD5 used to identify "fingerprint" of potential malware using Global Threat Information (GTI) database (used internal to the module only). Non-Approved algorithms (no security claimed): MD5
- SNMPv3 is used as a plaintext transport mechanism with no security claimed. All CSP content in this SNMPv3 channel is additionally key wrapped and signed by NSM to ensure integrity and decrypted in sensor using the sensor TLS private key. Non-CSP SNMPv3 content is deemed plaintext. Non-Approved algorithms (no security claimed): HMAC (non-compliant), SHA (non-compliant), AES (non-compliant), Triple-DES (non-compliant), MD5, DES, SNMP KDF (non-compliant)
- The following algorithms are implemented independently from all other cryptographic code in the module and are used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. For the reasoning stated above, this functionality is allowed in the FIPS Approved mode of operation.
  - Decryption - SSLv2
    - Cipher suites:
      - SSL_CK_RC4_128_WITH_MD5
      - SSL_CK_RC4_128_EXPORT40_WITH_MD5
      - SSL_CK_DES_64_CBC_WITH_MD5
      - SSL_CK_DES_192_EDE3_CBC_WITH_MD5
    - Non-Approved algorithms (no security claimed): Triple-DES (non-compliant), HMAC (non-compliant), RC4, MD5, DES
  - Decryption - SSLv3/TLS
    - Cipher suites:
      - SSL/TLS_NULL_WITH_NULL_NULL
      - SSL/TLS_RSA_WITH_NULL_MD5
      - SSL/TLS_RSA_WITH_NULL_SHA
      - SSL/TLS_RSA_WITH_RC4_128_MD5
      - SSL/TLS_RSA_WITH_RC4_128_SHA
      - SSL/TLS_RSA_WITH_DES_CBC_SHA
      - SSL/TLS_RSA_WITH_3DES_EDE_CBC_SHA
      - SSL/TLS_RSA_WITH_AES_128_CBC_SHA
      - SSL/TLS_RSA_WITH_AES_256_CBC_SHA
    - Non-Approved algorithms (no security claimed): AES (non-compliant), RSA (non-compliant), SHA (non-compliant), Triple-DES (non-compliant), HMAC (non-compliant), RC4, MD5, DES

4 Ports and Interfaces

Table 2 provides the cryptographic module's fixed port configuration.

Table 2 – Fixed Ports

Fixed Ports	Number of ports	Input/Output Type
40-Gig Monitoring Ports	2	Data Input/Output
1-GigE Monitoring Ports	8	Data Input/Output
Network I/O slots	2	Data Input/Output
GigE Management Port	1	Control Input, Data Output, Status Output
GigE Response Port	1	Data Output
GigE Aux Port	1	Data Output
RS232 Console	1	Control Input, Status Output
USB Ports	2	Data Input
Power Ports	2	Power Input
LEDs	Many	Status Output

The Network IO Slots each accept interface modules which provide additional monitoring ports. The interface modules are not included in the cryptographic boundary.

Figure 2 – NS-9100/9200 Front Panel

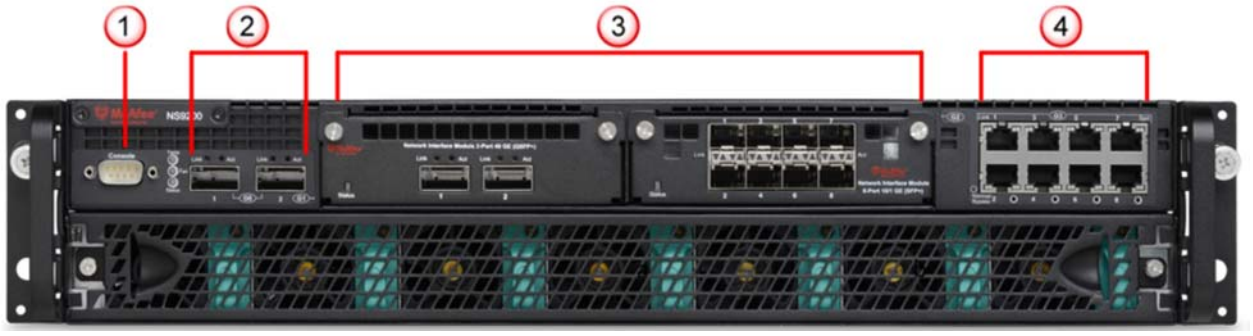

Figure 3 - Front panel with no Network I/O Modules or cover plate

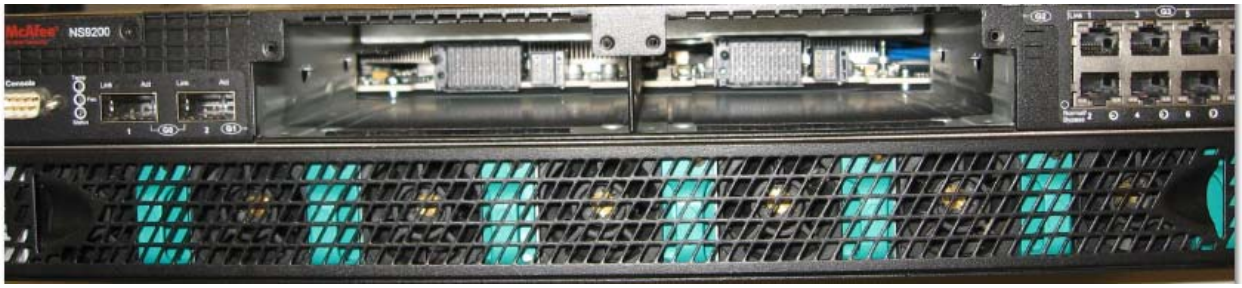

Table 3 – NS-9100/9200 Front Panel Ports and Connectors

Item	Description
1	Console port (1)
2	QSFP+ 40 Gigabit Ethernet ports (2)
3	Two slots for Network I/O modules The Network I/O modules are outside of the cryptographic boundary. There is no security relevance to using the following Network I/O modules in any combination. • QSFP+ 40 Gigabit Ethernet ports (4) • QSFP+ 40 Gigabit Ethernet ports (2) • SFP/SFP+ 1/10 Gigabit Ethernet Monitoring ports (8) • RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (6)
4	RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (8)

Figure 4 – NS-9100/9200 Rear Panel

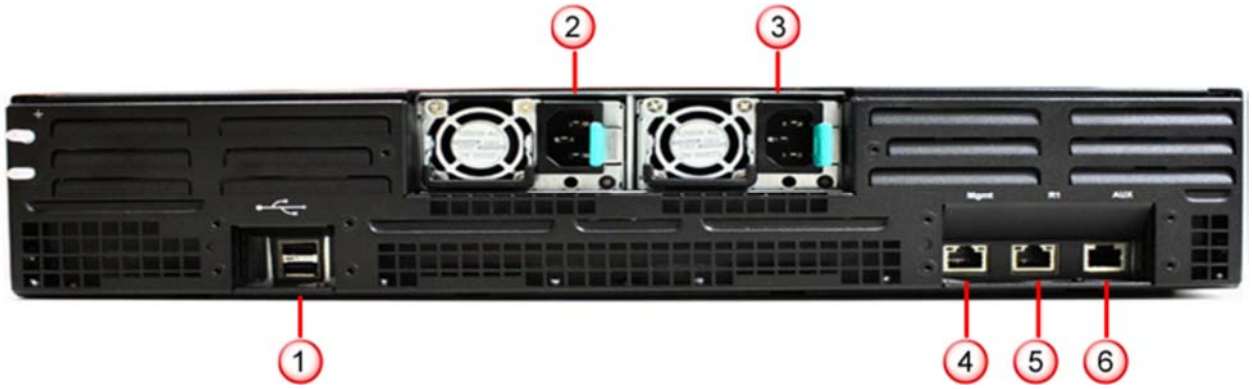

Table 4 – NS-9100/9200 Rear Panel Ports and Connectors

Item	Description
1	USB ports (2)
2	Power supply A (Pwr A)
3	Power supply B (Pwr B) (optional on NS9100)
4	RJ-45 100/1000/10000 Management port (Mgmt) (1)
5	RJ-45 100/1000/10000 Response port (R1) (1)
6	RJ-45 Auxiliary port (Aux) (1)

Figure 5 - Rear panel with Power supplies removed

The module supports the following communication channels with the Network Security Platform (NSP) Manager:

- Install channel: Only used to associate a Sensor with the NSM. They use a "shared secret". NSM listening on port 8501.
- Trusted Alert/Control channel (TLS): NSM listening on port 8502
- Trusted Packet log channel (TLS): NSM listening on port 8503
- Command channel (SNMPv3, plaintext): Sensor listening to 3rd Party SNMP clients on port 8500
- Bulk transfer channel (All output is encrypted): NSM listening on port 8504
- Trusted Authentication Gateway channel (TLS): uses same crypto context as Alert/Control channel. NSM listening on port 8502.

5 Identification and Authentication Policy

The cryptographic module supports three distinct "User" roles (Admin, Sensor Operator(s), and 3rd Party SNMP Client(s)) and one "Cryptographic Officer" role (Network Security Platform Manager). Table 5 lists the supported operator roles along with their required identification and authentication techniques. Table 6 outlines each authentication mechanism and the associated strengths.

Table 5 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin (User)	Role-based operator authentication	Username and Password
Sensor Operator(s) (User)	Role-based operator authentication	Username and Password
Network Security Platform Manager (Cryptographic Officer)	Role-based operator authentication	Digital Signature
3rd Party SNMP Client(s) (User)	Role-based operator authentication	Username, Privacy and Authentication key

Table 6 – 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-three (93) printable and human-readable characters. Whitespace and "?" are not allowed. New passwords are required to include 2 uppercase characters, 2 lowercase characters, 2 numeric characters, and 2 special characters. The probability that a random attempt will succeed or a false acceptance will occur is 1/{(10^2)*(26^4)*(31^2)*(93^7)} 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)/{(10^2)*(26^4)*(31^2)*(93^7)}, which is less than 1/100,000.

Authentication Mechanism	Strength of Mechanism
Digital Signature	RSA 2048-bit keys using SHA-256 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 1/2^112, which is less than 1/1,000,000. The module can only perform one (1) digital signature verification per second. The probability of successfully authenticating to the module within one minute through random attempts is 60/2^112, 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 letters, 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 (1) attempt per millisecond, meaning that 60,000 attempts can be made per minute. The probability of successfully authenticating to the module within one minute through random attempts is 60,000/62^16, which is less than 1/100,000.

6 Access Control Policy

6.1 Roles and Services

Table 7 lists each operator role and the services authorized for each role.

Table 7 – Services Authorized for Roles

Admin	Sensor Operator(s)	NSP Manager	3rd Party SNMP Client(s)	Authorized Services
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 service authorization level, 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	X*	X		**Administrative Configuration:** Other various services provided for admin, private, and support levels.
X	X*	X		**Firmware Update**: Install an external firmware image through SCP or USB
X	X*			**Install with NSM**: Configures module for use. This step includes establishing trust between the module and the associated management station.
		X		**Install with 3rd Party SNMP Client:** Configures module for 3rd Party SNMPv3 use. This step includes establishing trust between the module and the associated 3rd Party SNMP Client. Trust is provided by NSM.
X	X*			**Change Passwords**: Allows Admin and Sensor Operators to change their associated passwords. Admin can also change/reset Sensor Operators passwords.
X	X*			**Zeroize**: Destroys all plaintext secrets contained within the module. The "Reset Config" command is used, followed by a reboot.
		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/Console access.

* Depending on the authorization level granted by the Admin

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:* This service utilizes the non-Approved algorithms listed above with no security claims. This includes an MD5 hash to identify the "fingerprint" of malware and decryption of SSL-encrypted streams for the purpose of detecting malware and network attacks. See the list above.
- **Zeroize**: Destroys all plaintext secrets contained within the module. The "NetBoot" or rescue process is used.

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.
- **NSM Initialization Secret (i.e., NSM Shared Secret)**: Password used for mutual authentication of the sensor and NSM 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**: RSA 2048 bit key used for authentication of sensor to remote terminal for CLI access.
- **SSH Session Keys**: Set of ephemeral Diffie-Hellman, AES, and HMAC keys created for each SSH session.
- **TLS Sensor Private Key (for NSM)**: RSA 2048 bit key used for authentication of the sensor to NSM.
- **TLS Session Keys (for NSM)**: Set of ephemeral AES and HMAC keys created for each TLS session with the NSM.
- **Seed for RNG**: Seed created by NDRNG and used to seed the Block Cipher (CTR) DRBG.
- **DRBG Internal State:** *V* and *Key* used by the DRBG to generate pseudo-random numbers

- **Server Private Keys (for SSL network stream analysis):** Set of up to 64 Private Keys of servers within the environment protected by the IPS Services. Used to decrypt and analyze incoming network traffic.

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**: RSA 2048 bit key used to authenticate the sensor to the remote client during SSH.
- **SSH Remote Client Public Key**: RSA 2048 bit key used to authenticate the remote client to the sensor during SSH.
- **TLS Sensor Public Key (for NSM):** RSA 2048 bit key used to authenticate the sensor to NSM during TLS connections.
- **TLS NSM Public Key**: RSA 2048 bit key used to authenticate NSM to sensor during TLS connections.

6.4 Definition of CSPs Modes of Access

Table 8 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 8 – Key and CSP Access Rights within Services

	Administrator Passwords	Sensor Operator Passwords	3rd Party SNMP Client P and A Keys	NSM Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	SSH Session Keys	TLS Sensor Private Key (for NSM)	TLS Session Keys (for NSM)	Seed for RNG	DRBG Internal State	Server Private Keys	McAfee FW Verification Key	SSH Host Public Key	SSH Remote Client Public Key	TLS Sensor Public Key (for NSM)	TLS NSM Public Key
Show Status	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
Administrative Configuration				R		R		R	R					R	R	R	R
Firmware Update				R		R		R	R					R	R	R	R
Install with NSM						R		R W	R W	R W	R W			R	R	R W	R W
Install with 3rd Party SNMP Client			R W														
Change Passwords	R W					R								R	R		
Zeroize	Z*	Z*	Z	Z	Z	R Z	Z	Z	Z	Z	Z	Z	Z	R	R		
Intrusion Detection/ Prevention Management					R			R	R			W				R	R
Intrusion Detection/ Prevention Monitoring			R														
Disable SSH/Console Access																	
Self Tests																	
Intrusion Prevention Services												R					

7 Operational Environment

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 four distinct operator roles: Admin, Sensor Operator(s), Network Security Platform Manager, 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. Firmware Integrity Test: XYSSL RSA 2048 using SHA-1 for hashing
      (Future versions of this Module will validate integrity with a SHA-256 based hash.)
   2. Cryptographic algorithm known answer tests (KATs):
      a. AES ECB 128 Encryption KAT and Decryption KAT
      b. RSA 2048 Key Generation KAT
      c. RSA 2048 Signature Generation KAT
      d. RSA 2048 Signature Verification KAT
      e. SHA-1 KAT
      f. SHA-256 KAT
      g. SHA-512 KAT
      h. Block Cipher (CTR) DRBG KAT
      i. HMAC SHA-1 KAT
      j. HMAC SHA-256 KAT
      k. HMAC SHA-512 KAT
      l. XYSSL RSA 2048 Signature Verification KAT
         (SHA-1 and SHA-256 based signatures)
      m. XYSSL SHA-1 KAT
      n. XYSSL SHA-256 KAT
      o. TLS 1.0/1.1 KDF KAT
      p. SSH KDF KAT

   If any of these tests fail the following message will be displayed:
   !!! CRITICAL FAILURE !!!
   FIPS 140-2 POST and KAT...
   REBOOTING IN 15 SECONDS

   3. Critical Functions Tests: N/A

B. Conditional Self-Tests:

a. Block Cipher (CTR) DRBG Continuous Test
b. SP 800-90A DRBG Section 11.3 Health Checks
c. NDRNG Continuous Test
d. RSA KeyGen/Sign/Verify Pairwise Consistency Test
e. External Firmware Load Test – XYSSL RSA 2048 using SHA-256 for hashing

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 module shall only support five concurrent SSH operators when SSH is enabled.
10. The use of the Aux ports shall be restricted to the initialization of the cryptographic module.

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:
  - NS-9100/NS-9200: IAC-FIPS-KT2

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 9 outlines the recommendations for inspecting/testing physical security mechanisms of the module.

Table 9 – 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 NS-9100 and NS-9200 platforms. There are 9 tamper labels and they are outlined in red.

Figure 6 – Tamper Label Placement (NS-9100 and NS-9200)

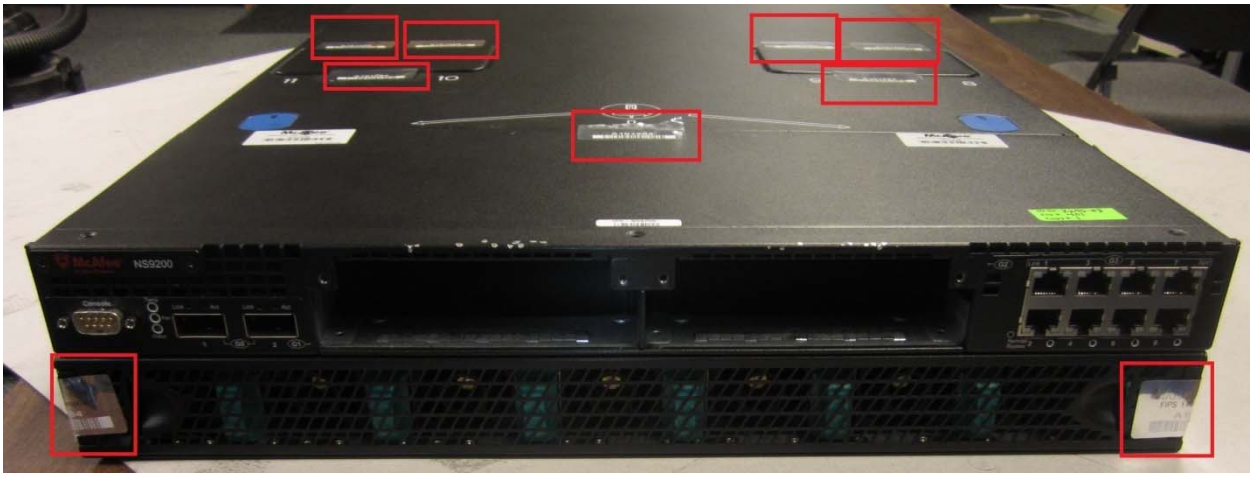

Figure 7 – Tamper Label

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.