McAfee LLC
Network Security Platform Sensor

NS9300 S

Non-Proprietary Security Policy
Version 1.0

November 2019

TABLE OF CONTENTS

1 Module Overview

The Network Security Platform Sensor NS-9300 S (HW P/N IPS-NS9300 S Version 1.30 and Firmware Version 9.1.17.100; FIPS Kit P/N IAC-FIPS-KT2) is a multi-chip standalone cryptographic module as defined in FIPS 140-2.

The NS9300 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.) Optional network I/O modules are not included in the module boundary.

The McAfee NS-9300 product consists of the NS-9300 P cryptographic module physically connected with the NS-9300 S cryptographic module. This Security Policy describes the NS9300 S only.

Figure 1 shows the module configuration and the cryptographic boundary.

Figure 1 – Image of NS9300 S

Figure 2 – Image of the Cryptographic Module connected to its peer NS-9300 P

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.

The operator must also follow the rules outlined in Sections 8 and 9 of this Security Policy and consult FIPS 140-2 IG 1.23 for further understanding of the use of functions where no security is claimed.

Approved Algorithms

The module supports the following FIPS Approved algorithms:

- AES CBC and ECB mode with 128 & 256 bits for encryption and decryption (Cert. #C409)
  (Note: CBC mode is tested but not used.)
- AES GCM mode with 128 & 256 bits for encryption and decryption use within SSH v2 (Cert. #C409)
- KTS AES (Cert. #C409) encryption to transport keys and authentication using HMAC (Cert. #C409) within SSH
- KTS AES (Cert. #C409) encryption to transport keys using GCM (Cert. #C409) within SSH
- FIPS 186-4 RSA with 2048 bit keys for key generation and RSA PSS with 2048 bit keys for signature generation with SHA-256, and signature verification with SHA-256 (Cert. #C409)
- SHA-1, SHA-256 and SHA-512 for hashing (Cert. #C409)
  (Note: SHA-1 is CAVP tested but not used.)
- HMAC SHA-256, and SHA-512 for message authentication (Cert. #C409)
  (Note: The minimum HMAC key size is 20 bytes. HMAC SHA-1 is CAVP tested but not used.)
- Block Cipher (CTR) DRBG using AES 256 (Cert. #C409)
- FIPS 186-4 XYSSL RSA PKCS #1 1.5 SigVer with 2048 bit keys using SHA-256 for image verification (Cert. #2638).
  (Note: SHA-1 is CAVP tested but not used.)
- XYSSL SHA-256 for hashing and for use with image verification (Cert. #3960)
  (Note: SHA-1 is CAVP tested but not used.)
- SSH KDF for SSH session key derivation (CVL Cert. #C410)
- SP 800-133 CKG (Vendor Affirmed)
  - Asymmetric Key Generation (SP 800-133 § 6)
  - Symmetric Key Generation (SP 800-133 § 7.1, 7.2, 7.3)

  (Note: The resulting symmetric keys and generated seeds are unmodified output from the DRBG)

(Note: TLS KDF was CAVP tested but is not used by the module)

Allowed Algorithms and Protocols

The module supports the following FIPS allowed algorithms and protocols:

- EC Diffie-Hellman using P-256 for key agreement (CVL Cert. #C410, key establishment

methodology provides 128 bits of encryption strength)

- NDRNG (internal entropy source) for seeding the Block Cipher (CTR) DRBG. The module generates a minimum of 256 bits of entropy for key generation.
- 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): EC Diffie-hellman-P-256 SHA2
    - Public Key methods (i.e., authentication methods): SSH-RSA
      (Note: This is restricted to RSA-2048)
    - Encryption methods: AES128-GCM, AES256-GCM
    - MAC methods: HMAC-256, HMAC-512

AES GCM is only used as part of the SSHv2 cipher suites conformant to the Draft IG A.5 and RFCs 4252, 4253 and RFC 5647. The GCM re-key limit is set to 1 hour or 1 GB of payload traffic set as the threshold. Therefore, the invocation counter maximum of $2^{64} - 1$ is never reached nor are that many encryptions performed in a single session. When a session is terminated for any reason, a new key and new initial IV shall be derived.

Non-Approved Algorithms and Protocols with No Security Claimed

The module supports the following non-Approved but allowed algorithms with no security claimed (per FIPS IG 1.23):

- 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

Use of any non-Approved/non-allowed algorithm, mode, or key size will place the module in the non-Approved mode of operation.

4 Ports and Interfaces

Table 2 provides the cryptographic module's ports and interfaces.

Table 2 – Fixed Ports

Fixed Ports	Number of ports	Input/Output Type
40-Gig QSFP+ 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

Fixed Ports	Number of ports	Input/Output Type
Power Ports	2	Power Input
LEDs	Many	Status Output

Notes:

1. The Two fixed QSFP+ 40-GigE ports are used to connect to the peer NS-9300 S unit
2. The GigE Management Port is connected directly to the peer NS-9300 P unit's GigE Response Port (peer not shown).
3. The Network IO Slots each accept interface modules which provide additional monitoring ports. The interface modules are not included in the cryptographic boundary.

Figure 3 - Front Panels of NS-9300 S

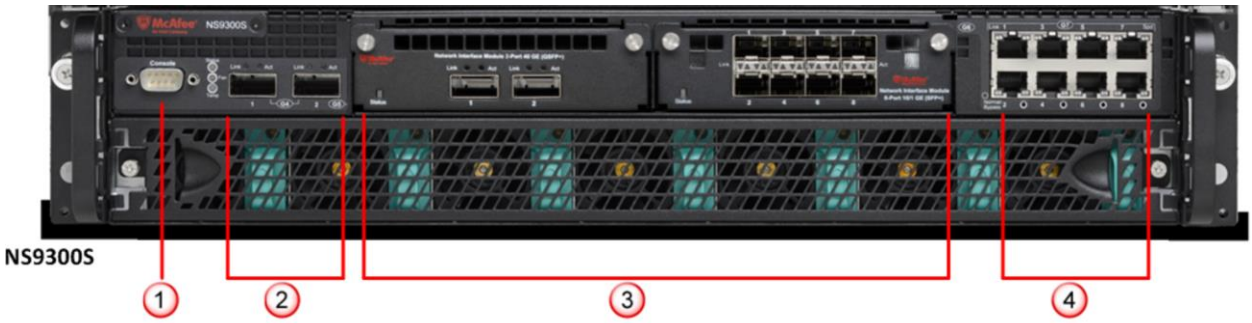

Table 3 – NS-9300 S Front Panel Ports and Connectors

Item	Description
1	Console ports on the NS-9300 S Sensors (1)
2	QSFP+ 40 Gigabit Ethernet Interconnect ports (4). G4/1 and G4/2 on NS-9300 S Sensor.
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 (2) • QSFP+ 40 Gigabit Ethernet ports (1) • SFP/SFP+ 1/10 Gigabit Ethernet Monitoring ports (4) • RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (3)
4	RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (8)

Figure 4 - Rear Panels of NS-9300 S

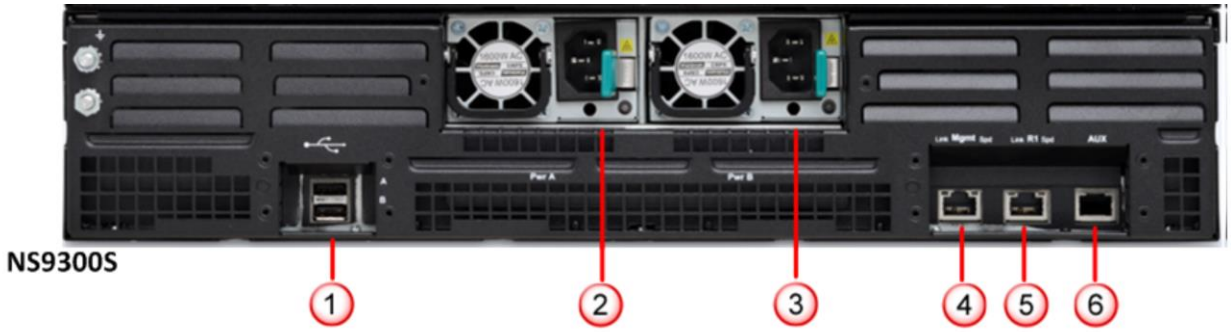

Table 4 – NS-9300 S Rear Panel Ports and Connectors

Item	Description
1	USB ports (2)
2	Power supply A (Pwr A)
3	Power supply B (Pwr B)
4	RJ-45 100/1000/10000 Management port (Mgmt) (1). Mgmt on NS-9300 S Sensor is used as an interconnect port.
5	RJ-45 100/1000/10000 Response port (R1) (1). R1 on NS-9300 P Sensor is used as an interconnect port.
6	RJ-45 Auxiliary port (Aux) (1)

Figure 5 - Rear Panel with Power Supplies Removed

5 Identification and Authentication Policy

The cryptographic module supports one "User" role (Admin) and one "Cryptographic Officer" roles (NS-9300 P). 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
NS-9300 P (Cryptographic Officer)	Role-based operator authentication	Shared Secret

Table 6 – 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-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 fifteen (15) character minimum is enforced by the module. 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.
Shared Secret (NS-9300 P)	The Shared Secret is an alphanumeric string of a minimum of six (6) characters chosen from the set of ninety-three (93) printable and human-readable characters. Whitespace and "?" are not allowed. The probability that a random attempt will succeed or a false acceptance will occur is 1/93^6 which is less than 1/1,000,000. After setting the Shared Secret, the module requires a reboot in order to authenticate. The reboot takes longer than one minute before authentication is achieved, and if authentication fails, the module automatically reboots a second time. The probability of successfully authenticating to the module within one minute through random attempts is 1/93^6 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.

For additional information of operation of the module, see the Network Security Platform 9.1 CLI Guide.

Table 7 – Services Authorized for Roles

Approved Mode	Authorized Services	Admin	NS-9300 P
X	**Show Status**: Provides the status of the module, usage statistics, log data, and alerts.	X	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 SCP or USB	X	X
X	**Change Passwords**: Allows Admin to change their associated passwords and the NS-9300 Password.	X	
X	**Zeroize**: Destroys all plaintext secrets contained within the module. The "Reset Config" command is used, followed by a reboot.	X	X
X	**Intrusion Detection/Prevention Management**: Propagation of management of intrusion detection/prevention policies and configurations through a direct connection to NS-9300 P cryptographic module		X
X	**Disable SSH/Console Access:** Disables SSH/Console access.	X	

* Depending on the authorization level granted by the Admin

Unauthenticated Services:

Table 8 lists the unauthenticated services supported by the module.

Table 8 – Unauthenticated Services

Approved Mode	Unauthenticated Services
X	**Authentication:** This service is associated with an unauthorized operator making a request in order to authenticate themselves to the module.
X	**Self-Tests**: This service executes the suite of self-tests required by FIPS 140-2. Self-tests can be initiated by power cycling the module or through the CLI.
	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. 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.
X	**Zeroize**: Destroys all plaintext secrets contained within the module. The Internal 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.
- **NS-9300 Password:** Password used for authentication of NS-9300 P.
- **SSH Host Private Keys**: RSA 2048 bit key used for authentication of sensor to remote terminal for CLI access, generated during initialization
- **SSH Session Keys**: Set of EC Diffie-Hellman private key P-256, AES 128/256 bit, and HMAC (SHA-256/512 bit) keys created for each SSH session.
- **Seed for DRBG**: Seed created by NDRNG and used to seed the Block Cipher (CTR) DRBG. The Nonce is 128 bits and the Entropy Input is 256 bits for a total seed size of 384 bits.
- **DRBG Internal State:** *V* and *Key* used by the DRBG to generate pseudo-random numbers

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 Session Public Key:** EC Diffie-Hellman P-256 session key created for each SSH session
- **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.

6.4 Definition of CSPs Modes of Access

Table 9 defines the relationship between access to keys/CSPs and the different module services. The types of access used in the table are Use (U), Generate (G), Input (I), Output (O), Store (S), 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 9 – Key and CSP Access Rights within Services

	Administrator Passwords	NS-9300 Password	SSH Host Private Keys	SSH Session Keys	Seed for DRBG	DRBG Intemal State	McAfee FW Verification Key	SSH Host Public Key	SSH Remote Client Public Key
Authentication – Admin, NS-9300 P	U	U	U	U G S					U
Show Status	U	U	U					U	U
Network Configuration			U					U G S	U I S
Administrative Configuration			U					U	U
Firmware Update			U					U	U
Change Passwords	U I S	U G I S	U G S					U	U
Zeroize (Authenticated)	Z*	Z	Z	Z	Z	Z	Z	Z	Z
Zeroize (Unauthenticated)	Z	Z	Z	Z	Z	Z	Z	Z	Z
Intrusion Detection/ Prevention Management									
Disable SSH/Console Access	U								
Self Tests									
Intrusion Prevention Services									

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 requirements of this FIPS 140-2 Level 2 module.

- The cryptographic module shall provide two distinct operator roles: Admin and NS-9300 P.
- The cryptographic module shall provide role-based authentication and each change of operator roles shall be authenticated and previous authentication results are cleared when the module transitions to a power-off state.
- When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
- The cryptographic module shall perform the following tests:
    - Power up Self-Tests are performed without operator input:
        - Firmware Integrity Test: XYSSL RSA 2048 (Cert. #2638) using SHA-256 (Cert. #3960) for hashing
        - Cryptographic algorithm known answer tests (KATs) and pairwise consistency tests (PCT):
            - AES ECB 128 Encryption KAT and Decryption KAT (Cert. #C409)
            - AES GCM Encryption KAT and Decryption KAT (Cert. #C409)
            - RSA 2048 PSS Key Generation/Sign/Verify Pairwise Consistency Test (Cert. #C409)
            - SHA-1 KAT (Cert. #C409)
            - SHA-256 KAT (Cert. #C409)
            - SHA-512 KAT (Cert. #C409)
            - Block Cipher (CTR) DRBG KAT and SP 800-90A DRBG Section 11.3 Health Checks (Cert. #C409)
            - HMAC SHA-256 KAT (Cert. #C409)
            - HMAC SHA-512 KAT (Cert. #C409)
            - XYSSL RSA 2048 Signature Verification KAT (Cert. #2638) (SHA-256 based signatures)
            - XYSSL SHA-256 KAT (Cert. #3960)
            - SSH KDF KAT (CVL Cert. #C410)

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

    - Conditional Self-Tests:
        - Block Cipher (CTR) DRBG Continuous Test
        - SP 800-90A DRBG Section 11.3 Health Checks

        - NDRNG Continuous Test
        - RSA KeyGen/Sign/Verify Pairwise Consistency Test (Cert. #C409)
        - External Firmware Load Test – XYSSL RSA 2048 (Cert. #2638) using SHA-256 (Cert. #3960) for hashing

          If the firmware load test fails the following message will be displayed: "Load Image with SCP Failed."

- 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.
- Data output shall be inhibited during self-tests and error states.
    - All Power Up Self-Test are run before data output ports are initialized.
    - In the case of failed Power Up Self Tests, the module enters an error state, and reboots.
- Data output shall be logically disconnected during key generation and zeroization.
- If the module loses power and then it is restored, then a new key shall be established for use with the AES GCM encryption/decryption processes.
- For both Zeroize services (authenticated and unauthenticated), the operator must remain in control of the module or be physically present with the module to assure that the entire zeroization process completes successfully. This may take up to one minute.
- Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.
- The module shall only support five concurrent SSH operators when SSH is enabled.
- The cryptographic module shall not be configured to transmit files to McAfee Advanced Threat Detection.

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:
    - NS9300 S: 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 10 outlines the recommendations for inspecting/testing physical security mechanisms of the module. If the Admin finds evidence of tampering, then the module is no longer FIPS compliant.

Table 10 – 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, annually at a minimum	Visually inspect the labels for tears, rips, dissolved adhesive, and other signs of malice.
Opaque Enclosure	As specified per end user policy, annually at a minimum	Visually inspect the enclosure for broken screws, bent casing, scratches, and other questionable markings.

Figure 6 and

Figure 7 depicts the tamper label locations on the cryptographic module for the NS9300 S platform. There are 9 tamper labels and they are numbered in red. An example tamper label is shown in Figure 9.

Figure 6 – Tamper Label Placement Top (9300 S)

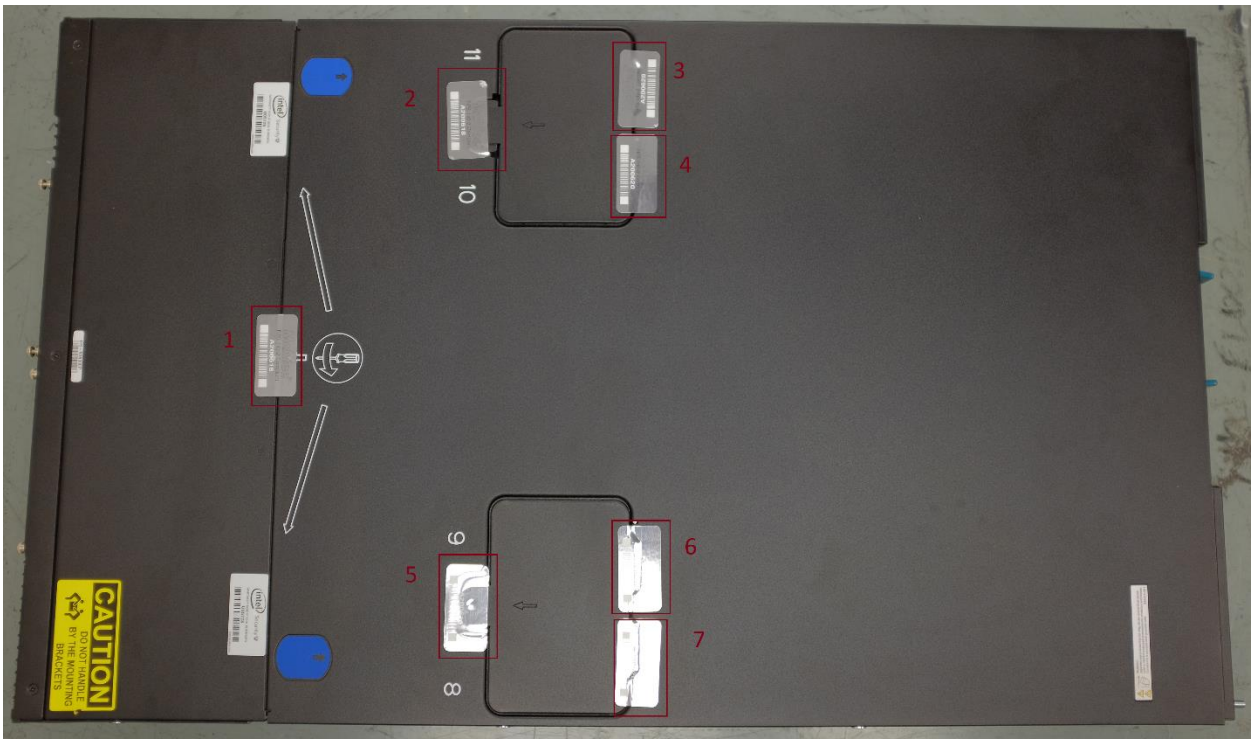

Figure 7 – Tamper Label Placement Front (9300 S)

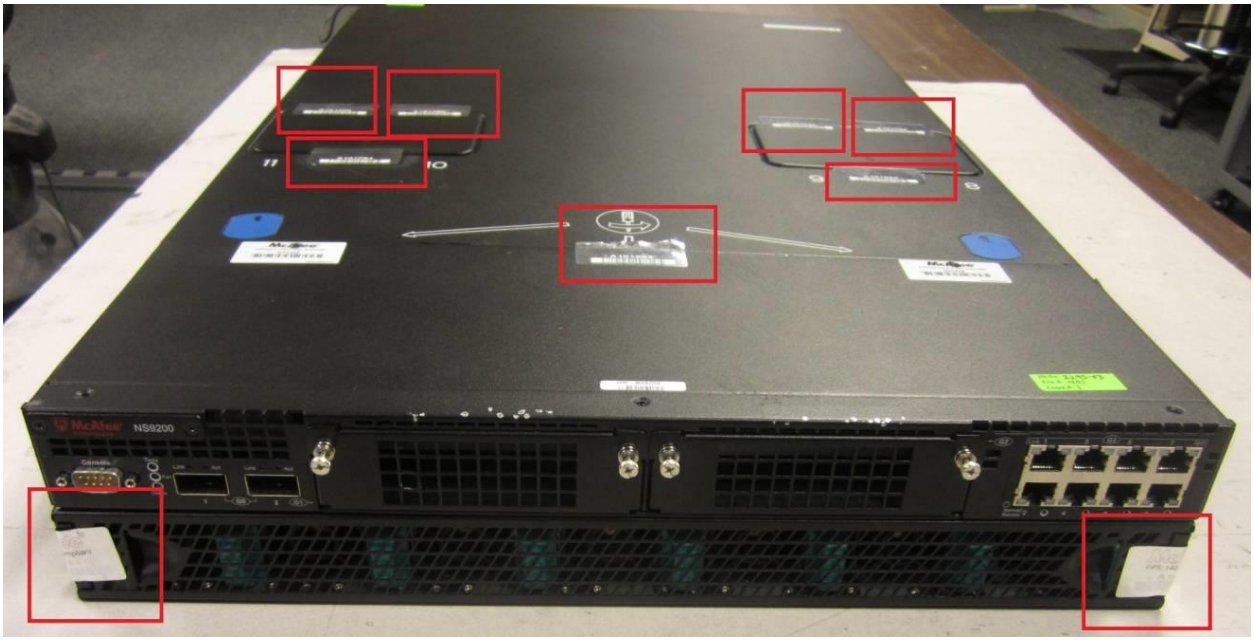

Figure 8 – Tamper Label Placement Front (NS9300 P with NS9300 S)

Figure 9 – 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.

11 Glossary

Acronym	Definition
AES	Advanced Encryption Standard
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSP	Critical Security Parameter
CVL	Component Validation List
DRBG	Deterministic Random Number Generator

FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
IG	Implementation Guidance
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
KAT	Known Answer Test
KDF	Key Derivation Function
KTS	Key Transport Scheme
NDRNG	Non-Deterministic Random Number Generator
NSM	Network Security Manager
NSP	Network Security Platform
PCT	Pairwise Consistency Test
RSA	Rivest, Shamir, Adleman algorithm
SHA/SHS	Secure Hash Algorithm/Standard
SCP	Secure Copy