FIPS 140-2 Non-Proprietary Security Policy

IBM Security Network Intrusion Prevention System Version 4.6.2

Document Version 2.7

March 3, 2016

Prepared For:

IBM Security

6303 Barfield Road

Atlanta, GA 30328

www.ibm.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the Network Intrusion Prevention System Version 4.6.2.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140-2

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) runs the Cryptographic Module Validation Program (CMVP). The National Voluntary Laboratory Accreditation Program (NVLAP) accredits independent testing labs to perform FIPS 140-2 testing; the CMVP validates test reports for products meeting FIPS 140-2 validation. *Validated* is the term given to a product that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Network Intrusion Prevention System Version 4.6.2 from IBM Security provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The IBM Security Network Intrusion Prevention System Version 4.6.2 may also be referred to as the "module" in this document.

1.3 External Resources

The IBM Security website (http://www.ibm.com) contains information on the full line of products from IBM Security, including a detailed overview of the Network Intrusion Prevention System Version 4.6.2 solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/) contains links to the FIPS 140-2 certificate and IBM Security contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DTR	Derived Testing Requirement
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
GPOS	General Purpose Operating System
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
IBM	International Business Machines
ISS	Internet Security Systems
KAT	Known Answer Test
NDRNG	Non-deterministic Random Number Generator
NIM	Network Interface Module
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security
Triple-DES	Triple-Data Encryption Standard

Table 1 – Acronyms and Terms

2 IBM Security Network Intrusion Prevention System Version 4.6.2

2.1 Product Overview

The Network Intrusion Prevention System (IPS) automatically blocks malicious attacks while preserving network bandwidth and availability. The Network IPS appliances are purpose-built, Layer 2 network security appliances that you can deploy either at the gateway or the network to block intrusion attempts, denial of service (DoS) attacks, malicious code, backdoors, spyware, peer-to-peer applications, and a growing list of threats without requiring extensive network reconfiguration.

The Network Intrusion Prevention System Version 4.6.2 can be securely managed via the following interfaces:

- NIPS Manager, which offers a browser-based graphical user interface (GUI) for local, single appliance management.
- SiteProtector, which is a central management console for managing appliances, monitoring events, and scheduling reports

2.2 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	2
Cryptographic 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
Electromagnetic Interference / Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Overall Validation Level	**2**

Table 2 – Validation Level by DTR Section

The “Mitigation of Other Attacks” section is not relevant as the module does not implement any countermeasures towards special attacks.

2.3 Cryptographic Algorithms

2.3.1 Approved Algorithms and Implementation Certificates

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	CAVP Certificate	Use
Asymmetric Key	RSA FIPS 186-2: [ANSIX9.31]: SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096. [PKCS1_V1_5]: SIG(ver): 1024 , 1536 , 2048 , 3072 , 4096 FIPS 186-4: 186-4KEY(gen): PGM(ProbRandom): 2048, 3072 [ANSIX9.31] Sig(Ver): 1024, 2048, 3072 [RSASSA-PKCS1_V1_5] SIG(gen): 2048, 3072 SIG(Ver): 1024, 2048, 3072	1633	Sign / verify operations Sig Ver 1024-bit for legacy use only

Algorithm Type	Algorithm	CAVP Certificate	Use
	ECDSA FIPS186-4: PKG: CURVES (P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571) PKV: CURVES (ALL-P ALL-K ALL-B) SigGen: CURVES (P-224, P-256, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) SigVer: CURVES (P-192, P-224, P-256, P-384 P-521, K-163, K-233, K-283, K-409, K-571, B-163, B-233, B-283, B-409, B-571)	588	
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS 180-3)	2651	Message digest in TLS sessions Module integrity via SHA256
Keyed Hash	HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS 198-1)	2018	Message verification
Symmetric Key	AES-128-CMAC, AES-192-CMAC, AES-256-CMAC. ECB, CBC, CFB1, CFB8, CFB128, OFB, and CTR. AES_CCM 128, 192, or 256 bit keys (SP800-38C). AES_GCM 128, 192, or 256 bit keys (FIPS 197, SP800-38D)	3204	Data encryption / decryption
	Triple-DES (Three key Triple-DES) 192-bit keys in ECB, CBC, CFB64, and OFB mode. CMAC	1825	

Algorithm Type	Algorithm	CAVP Certificate	Use
DRBG	DRBG HMAC_DRBG, HASH_DRBG, CTR_DRBG (SP800-90A)	679	DRBG

Table 3 – Algorithm Certificates (OpenSSL)

Algorithm Type	Algorithm	CAVP Certificate	Use
Asymmetric Key	RSA FIPS 186-2: [PKCS1_V1_5]: SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096. FIPS 186-4: 186-4KEY(gen): PGM(ProbRandom): 2048, 3072 [RSASSA-PKCS1_V1_5] : SIG(gen): 2048, 3072 SIG(Ver): 1024, 2048, 3072	1635	Sign / verify operations Sig Ver 1024-bit for legacy use only
	ECDSA FIPS186-4: P: 224, 256, 384, 521 K: 233, 283, 409, 571 B: 233, 283, 409, 571 ECDSA PKV CURVES(ALL-P) ECDSA Signature Generation P: 224, 256, 384, 521 K: 233, 283, 409, 571 B: 233, 283, 409, 571 ECDSA Signature Verification P: 192, 224, 256, 384, 521 K: 163, 233, 283, 409, 571 B: 163, 233, 283, 409, 571	591	Sign / verify operations

Algorithm Type	Algorithm	CAVP Certificate	Use
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS 180-3)	2657	Message digest in TLS sessions Module integrity via SHA256
Keyed Hash	HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 (FIPS 198-1)	2023	Message verification
Symmetric Key	AES-128-CMAC, AES-192-CMAC, AES-256-CMAC. ECB, CBC, CFB1, CFB8, CFB128, OFB, and CTR. AES_CCM 128, 192, or 256 bit keys (SP800-38C). AES_GCM 128, 192, or 256 bit keys (FIPS 197, SP800-38D)	3210	Data encryption / decryption
	Triple-DES (Three key Triple-DES) 192-bit keys in ECB, CBC, CFB64, and OFB mode.	1827	Data encryption / decryption
DRBG	DRBG HMAC_DRBG, HASH_DRBG, CTR_DRBG (SP800-90A)	682	DRBG

Table 4 – Algorithm Certificates (GSKit)

The TLS, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP. Please see NIST document SP800-131A for guidance regarding the use of non FIPS-approved algorithms.

2.3.2 Non-Approved but Allowed Algorithms

The module implements the following non-FIPS approved but allowed algorithms:

- True Random Number Generator (TRNG), a non-deterministic RNG (NDRNG) used to seed the DRBG.
  - The minimum number of bits of entropy requested per each GET function is 256 bits.
  - The NDRNG is outside the logical boundary but is within the physical boundary.

- RSA Key Wrapping Encrypt / Decrypt (2048, 3072 bits) Allowed to be used in FIPS mode (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

2.4 Cryptographic Module Specification

The modules are the IBM Security GX4004, GX5008C, GX5008SFP, GX5208C, GX5208SFP, GX7412 and GX7800 running firmware version 4.6.2. Each module is classified as a multi-chip standalone cryptographic module and contains a cryptographic module to manage secure communications with NIPS Manager and SiteProtector Management System. The physical cryptographic boundary is defined as the module case (shown in Figure 1).

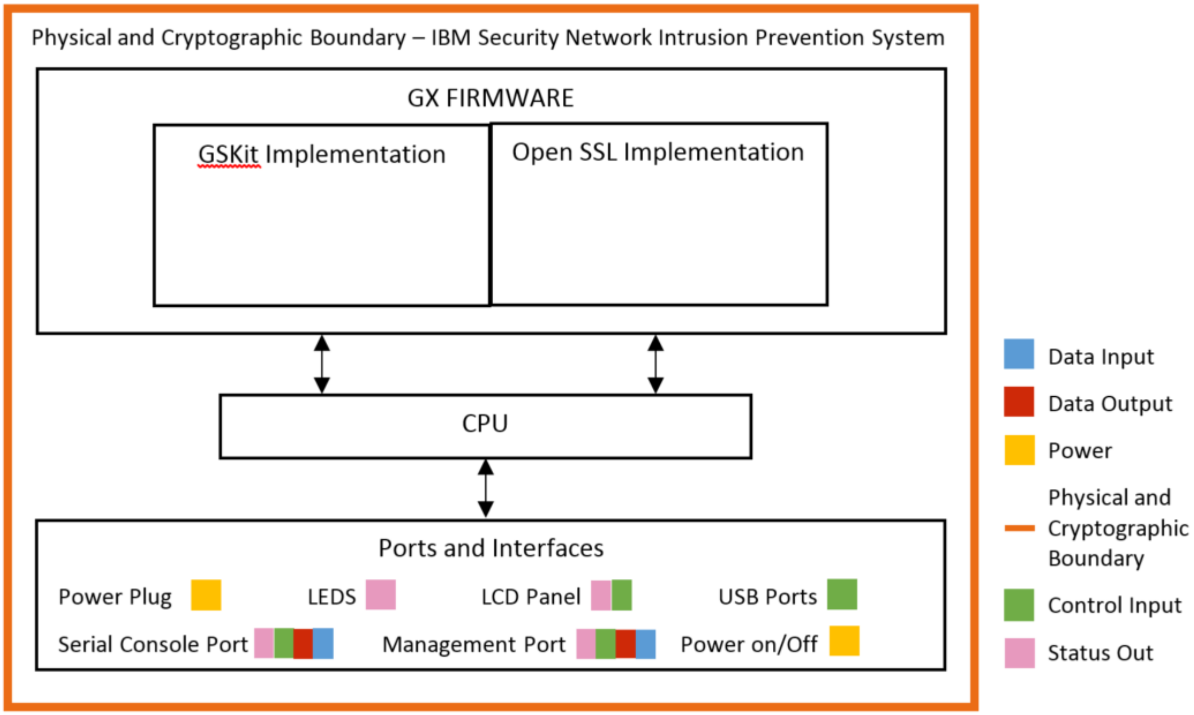


Figure 1 - Block Diagram

2.4.1 Excluded Components

Excluded components include the following:

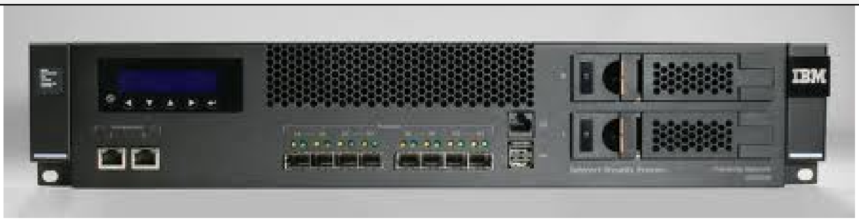
- Monitoring Ports (Ports 0 to 3 on GX4004)
    - These ports accept and pass data traffic that is analyzed by the internal IDS analysis engine. The traffic is not security relevant and does not interact with the cryptographic processing of the appliance.
- Management Port 2 (Port 4 on GX4004)

  - This port is not security relevant and does not interact with the cryptographic processing of the appliance.

- Network Card on GX5008C, GX5008SFP, GX5208C and GX5208SFP
  - The network card provides input/output functionality from the motherboard to the exterior network to accept and pass data traffic that is analyzed by the internal IDS analysis engine. The traffic is not security relevant and does not interact with the cryptographic processing of the appliance.

Although the actual data over these interfaces is excluded, the appliances do provide analysis of data. These scan results are sent to the management interfaces (i.e., NIPS Manager and/or SiteProtector) for review via TLS. The traffic on these ports is not security relevant and does not interact with the cryptographic processing of the appliance.

The module illustrations are provided in the table below:

MODULE	MODULE ILLUSTRATION
GX4004	
GX5008C, GX5008SFP, GX5208C, and GX5208SFP	
GX7412	

MODULE	MODULE ILLUSTRATION
GX7800	

Table 5 – Module Illustrations

2.4.2 FIPS Mode

The module can only be enabled for FIPS mode at the time of initial configuration. Additionally, if the module enters an error state (e.g., a known answer test fails), the module must be powered off and reimaged to FIPS mode of operation.

2.5 Module Interfaces

Each appliance runs the same version of firmware and has the same basic physical interfaces; the main difference is the number of Monitoring Ports (i.e., traffic monitoring interfaces) and the processing speed. The table below describes the main interface on each module:

Physical Interface	Description / Use
LCD	Initial network configuration, restarting or shutting down the appliance
Monitoring Ports (excluded)	Either inline intrusion prevention (IPS mode) or passive intrusion detection (IDS mode). Inline prevention uses a pair of ports per segment. Passive detection uses a single port per segment. IDS traffic is excluded from the validation.
Serial Console Port	Optional terminal-based setup and recovery
USB Ports	Connection to a CD-ROM or similar peripheral for loading images
Management Port 1	Communication with NIPS Manager and SiteProtector Management System
Management Port 2 (excluded)	Communication with SiteProtector Management System and for sending TCP Reset responses. This interface is excluded from the validation when configured for TCP Reset processing otherwise it is identical to Management Port #1.

Table 6 – Interface Descriptions

Each module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	Management 1 Serial Console Port
Data Output	Management 1 Serial Console Port
Control Input	Management 1 Serial Console Port USB Ports LCD Panel
Status Output	Management 1 Serial Console Port LCD Panel LEDs
Power	Power Plug On/Off Switch

Table 7 – Logical Interface / Physical Interface Mapping

2.6 Roles, Services, and Authentication

The module is accessed via Command Line Interface (CLI) NIPS Manager, or the SiteProtector management application. The CLI is used only for installation and initial configuration of the module. The module supports basic management via the LCD panel. This unauthenticated service is used to define basic network configuration, such as system name, IP address, firmware version, etc., allowing an operator to initialize the module for FIPS mode of operation. The LCD Management is unauthenticated but requires physical access and only offers the following services:

- View System Name
- View the IP address
- View Firmware Version
- View XPU Version
- View the Serial Number
- Restart the appliance
- Shutdown the appliance
- Set IP Address (only first-time, cannot change if previously set)

As required by FIPS 140-2, there are two roles (a Crypto Officer Role and User Role) in the module that operators may assume. The module supports identity-based authentication, and the respective services for each role are described in the following sections.

2.6.1 Management Options[1]

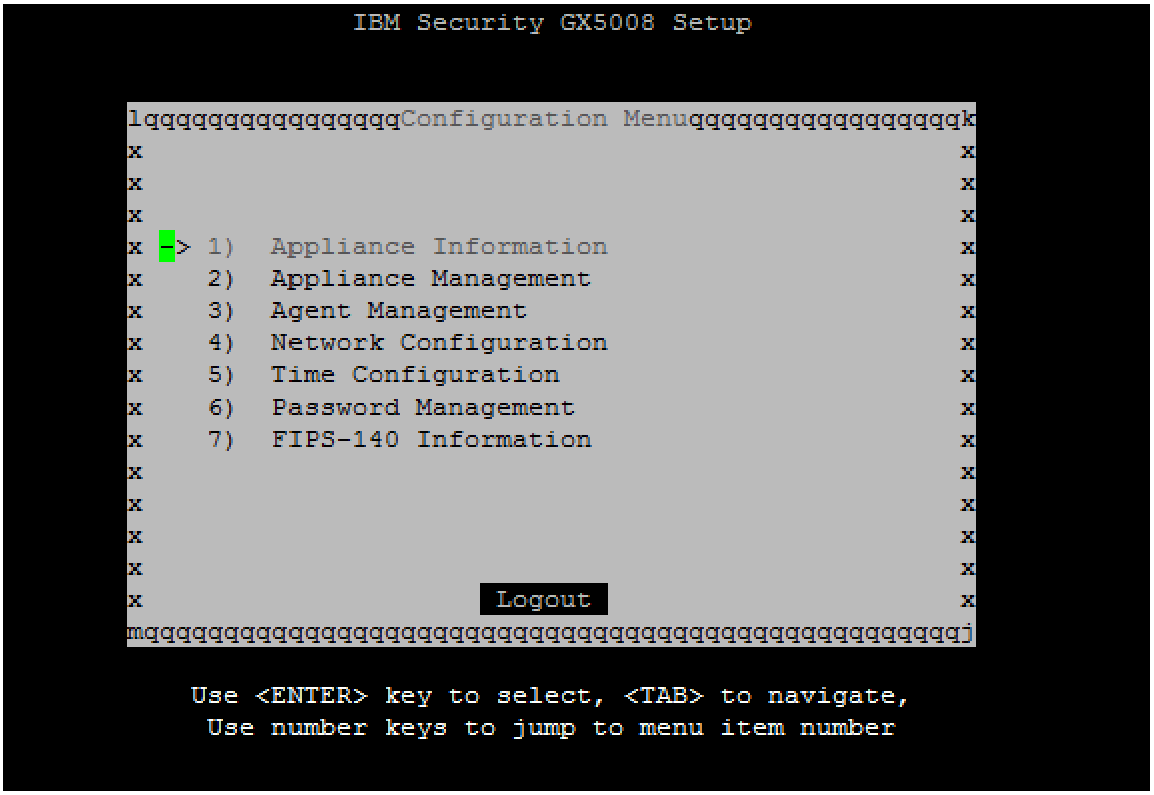
2.6.1.1 Command Line Interface

The command line interface offers the Crypto Officer Role basic functions for installation and initial configuration. An authorized operator can use the CLI to initially configure the following functions:

- Change Password
- Network Configuration Information
- Host Configuration
- Time Zone/Data/Time Configuration
- Agent Name Configuration
- Port Link Configuration
- Adapter Mode Configuration.

Additional CLI options are below:

[1] Please note that NIPS Manager and SiteProtector are outside of the module boundary and only the module interface to these applications are relevant to the validation.



```
                     IBM Security GX5008 Setup


       lqqqqqqqqqqqqqqqqConfiguration Menuqqqqqqqqqqqqqqqqqk
       x                                                   x
       x                                                   x
       x                                                   x
       x -> 1)  Appliance Information                      x
       x    2)  Appliance Management                       x
       x    3)  Agent Management                           x
       x    4)  Network Configuration                      x
       x    5)  Time Configuration                         x
       x    6)  Password Management                        x
       x    7)  FIPS-140 Information                       x
       x                                                   x
       x                                                   x
       x                                                   x
       x                                                   x
       x                      Logout                       x
       mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

           Use <ENTER> key to select, <TAB> to navigate,
            Use number keys to jump to menu item number
```

Figure 2 - Additional CLI Commands

2.6.1.2 NIPS Manager

NIPS Manager offers the Crypto-Officer Role a browser-based graphical user interface (GUI) for local, single appliance management. An authorized operator can use NIPS Manager to manage the following functions:

- Monitor appliance status
- View log files
- Register SiteProtector
- Configure password

This connection is secured via TLS.

2.6.1.3 SiteProtector

SiteProtector is the IBM ISS central management console. SiteProtector can manage appliances, monitor events, and schedule reports. By default, the appliances are configured to be managed through NIPS Manager. If managing a group of appliances along with other sensors, the centralized management capabilities of SiteProtector may be preferred. SiteProtector controls the following management functions of the appliance:

- Monitor appliance status
- View log files
- Configure password

2.6.2 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service	Description	Service Input / Output (API)	Interface	Key/CSP Access	Roles
Configure	Initializes the module for FIPS mode of operation	Configuration Parameters / Module configured	Serial Console Port USB Ports LCD Panel	None	Crypto Officer
Self Test	Performs self tests on critical functions of module	Initiate self tests / Self tests run	Management Port Power switch	None	Crypto Officer User
Decrypt	Decrypts a block of data	Initiate decryption / data decrypted	Management Port	AES Session Key Triple-DES Session Key Private Key SNMP AES Key	Crypto Officer User
Encrypt	Encrypts a block of data	Initiate encryption/ data encrypted	Management Port	AES Session Key Triple-DES Session Key Public Key External Entity Public Key SNMP AES Key	Crypto Officer User

Service	Description	Service Input / Output (API)	Interface	Key/CSP Access	Roles
Establish Session	Provides a protected session for establishment of encryption keys with peers	Initiate session establishment / session established	Management Port	Private Key Public Key HMAC Key Premaster Secret (48 Bytes) Master Secret (48 Bytes) Session Key Symmetric Key External Entity Public Key Session Key DRBG Seed Key Entropy Input String Hash_DRBG mechanism HMAC_DRBG mechanism CTR_DRBG mechanism	Crypto Officer User
Zeroize CSPs	Clear CSPs from memory	Terminate Session / CSPs cleared	Management Port	None	Crypto Officer User
	Clear CSPs from disk	Reimage module / CSPs cleared and module restored to factory settings	USB Serial	None	Crypto Officer
Show Status	Shows status of the module	Show status commands / Module status	Management Port Serial Console Port USB Ports LCD Panel LEDs	None	Crypto Officer User

Table 8 – Operator Services and Descriptions

2.6.3 Operator Authentication

The CO role authentication via CLI (when initially configuring the module for FIPS mode) is over SSH. The LMI connection is over HTTPS/TLS in FIPS mode. Other than status functions available by viewing LEDs, the services described in the table above are available only to authenticated operators.

The operator authenticates via username/password, and passwords are stored on the module. The module checks these parameters before allowing access. The module enforces a minimum password length of 6 characters (see Guidance and Secure Operation section of this document). The password can consist of alphanumeric values, {a-zA-Z0-9], yielding 62 choices per character. The probability of a successful random attempt is $1/62^6$, which is less than 1/1,000,000.[2]

Per the Configuration Guidance, the module will lock an account after 3 failed authentication attempts; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of a success with multiple consecutive attempts in a one minute period is $3/62^6$ which is less than 1/100,000.

For authentication of SiteProtector sessions (i.e., the User Role), the module supports a public key based authentication with 2048 bit keys via RSA. A 2048-bit RSA key has 112-bits of equivalent strength. The probability of a successful random attempt is 1/2^112, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one minute period is 60/2^112 which is less than 1/100,000.

2.7 Physical Security

Each module is a multiple-chip standalone module and conforms to Level 2 requirements for physical security. The modules' production-grade enclosure is made of a hard metal, and the enclosures contain a removable cover. The baffles installed by IBM Security satisfy FIPS 140-2 Level 2 requirements for module opacity. For details on tamper evidence, please see Section 3.1.4 – Placement of Tamper Evidence Labels.

2.8 Operational Environment

The modules operate in a limited operational environment and do not implement a General Purpose Operating System.

The modules meet Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

[2] The password complexity rules are configurable; users can have stricter password rules. The minimum password length can be configured to be 6 to 15 characters and can be configured to require special, numeric, upper and lower case characters. The default minimum password length is 6 characters, and the account should be locked after 3 unsuccessful attempts.

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privileges
GSKIT Implementation						
AES Session Key	AES 128, 192, 256 encryption & decryption of management traffic	Internal generation at installation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: Via secure TLS tunnel **Entry**: NA **Output**: NA	Decrypt Encrypt	Crypto Officer R W D User R W D
Triple-DES Session Key	Triple-DES 192 encryption & decryption of management traffic	Internal generation at installation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: Via secure TLS tunnel **Entry**: NA **Output**: NA	Decrypt Encrypt	Crypto Officer R W D User R W D
HMAC key	HMAC-SHA1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA384,	Internal generation at installation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer R W D

	HMAC-SHA-512 for message verification		**Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: None		User R W D
Crypto Officer Password	Alphanumeric passwords externally generated by a human user for authentication to the operating system.	Not generated by the module; defined by the human user of the workstation	**Storage**: on disk/obfuscated **Type:** Static **Association**: controlled by the operating system	**Agreement**: NA **Entry**: Manual entry via operating system **Output**: NA	Configure	Crypto Officer R W D User None
User Password	Alphanumeric passwords externally generated by a human user for authentication to the operating system.	Not generated by the module; defined by the human user of the workstation	**Storage**: on disk/obfuscated **Type:** Static **Association**: controlled by the operating system	**Agreement**: NA **Entry**: Manual entry via operating system **Output**: NA	Configure	Crypto Officer D User R W
DRBG Seed Key	256-bit value to seed the FIPS-approved DRBG	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
Entropy Input String	Input value for entropy calculation	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer None

			Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: NA		User None
Hash_DRBG mechanism	V and C values	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
HMAC_DRBG mechanism	V and Key values	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
CTR_DRBG mechanism	V and Key values	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None

Private Key	RSA Private Key for sign / verify operations and key establishment[3] for SiteProtector to security devices over TLS	Internal generation	**Storage**: RAM plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: Key handle from API request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
Public Key	RSA Public Key for sign / verify operations and key establishment[4] for SiteProtector to security devices over TLS. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation	**Storage**: RAM plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Agreement**: NA **Entry**: NA **Output**: Key handle from API request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
ECDSA Private Key	Private key for sign / verify operations and key establishment[5]for GX TLS connections	Internal generation	**Storage**: On disk in plaintext **Type:** Static	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer R W D

[3] Key establishment methodology provides 112 or 128-bits of encryption strength

[4] Key establishment methodology provides 112 or 128-bits of encryption strength

			Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Output**: None		User R
ECDSA Public Key	Public key for sign / verify operations and key establishment for GX TLS connections	Internal generation	**Storage**: On disk in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Agreement**: NA **Entry**: NA **Output**: : plaintext during TLS negotiation	Establish Session	Crypto Officer R W D User R
OpenSSL Implementation						
Session Key	AES CBC 256-bit key for encryption / decryption of management traffic	Derived from the Master Secret	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: Via secure TLS tunnel **Entry**: NA **Output**: NA	Decrypt Encrypt	Crypto Officer R W D User R W D
DRBG Seed	160-bit system Entropy seed the DBRG	Use dev / urandom to gather bytes from several areas of system data (including	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer None

		time/date), concatenate them together and hash via SHA-1	**Association:** The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: NA		User None
Private Key	RSA Private for sign / verify operations and key establishment[6] for SiteProtector to GX appliances over TLS	Internal generation at installation by DRBG	**Storage**: On disk in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R W D
GX Public Key	RSA Public for sign / verify operations and key establishment[7] for external entities (such as SiteProtector) to GX appliances over TLS. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation at installation by DRBG	**Storage**: On disk in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Agreement**: NA **Entry**: NA **Output**: plaintext during TLS negotiation	Establish Session	Crypto Officer R W D User R
External Entity Public Key	RSA Public key associated with remote entities (such as the browser or	External generation by FIPS-approved technique	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: Plaintext	Establish Session	Crypto Officer R W D

[6] Key establishment methodology provides 112 or 128-bits of encryption strength

[7] Key establishment methodology provides 112 or 128-bits of encryption strength

	SiteProtector)		**Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Output**: NA		User R W D
Premaster Secret (48 Bytes)	RSA-Encrypted Premaster Secret Message	Internal generation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: Input during TLS negotiation **Output**: Output to server encrypted by Public Key	Establish Session	Crypto Officer None User None
Master Secret (48 Bytes)	Used for computing the Session Key	Internal generation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
SNMP AES Key	AES CBC 256-bit key for encryption / decryption of SNMP traffic	Internal generation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Encrypt	Crypto Officer R W D User R W D

HMAC key	HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 for message verification	Internal generation at installation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R W D
DRBG Seed Key	256-bit value to seed the FIPS-approved DRBG	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
Entropy Input String	Input value for entropy calculation	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
Hash_DRBG mechanism	V and C values	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer None

			Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: NA		User None
HMAC_DRBG mechanism	V and Key values	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
CTR_DRBG mechanism	V and Key values	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
ECDSA Private Key	Private key for sign / verify operations and key establishment for GX TLS connections	Internal generation	**Storage**: On disk in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Agreement**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R

ECDSA Public Key	Public key for sign / verify operations and key establishment for GX TLS connections	Internal generation	**Storage**: On disk in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Agreement**: NA **Entry**: NA **Output**: plaintext during TLS negotiation	Establish Session	Crypto Officer R W D
						User R

R = Read W = Write D = Delete

Table 9 - Key/CSP Management Details

All secret keys, public/private keys, and CSPs are protected from unauthorized disclosure, modification and substitution. The module ensures only authenticated operators have access to keys and functions that can generate keys. Unauthenticated operators to not have write access to modify, change, or delete a public key. Ephemeral CSPs are zeroized by the RAM clearing processes, and static CSPs are zeroized by reimaging the module.

2.10 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the modules will output an error dialog and will shutdown. When a module is in an error state, no keys or CSPs will be output and the module will not perform cryptographic functions.

The module does not support a bypass function.

The following sections discuss the modules' self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of each module and do not require operator intervention to run. If any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. Each module implements the following power-on self-tests:

- Module integrity check via RSA 3072 w/ SHA-256
- Critical functions test: Checks, identifies, and initializes system devices such as the CPU, RAM, interrupt and DMA controllers and other parts of the chipset, BIOS FW integrity, video display memory, Storage drive, PCIe bus, network cards. System high-level POST issues are reported to the BMC, where the events are logged into the SEL.
- OpenSSL Implementation
    - RSA pairwise consistency (signing and signature verification) KAT
    - ECDSA pairwise consistency (signing and signature verification) KAT
    - AES KAT (encryption and decryption)
    - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
    - HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
    - Triple-DES KAT (encryption and decryption)
    - DRBG 800-90A KAT
- GSKIT Implementation
    - RSA signing and signature verification KAT

- Primitive “Z” Computation KAT
- ECDSA pairwise consistency and signature verification KAT
- AES KAT (encryption and decryption)
- Triple-DES KAT (encryption and decryption)
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- DRBG 800-90A KAT

Each module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation.

2.10.2 Conditional Self-Tests

Conditional self-tests are test that run continuously during operation of each module. If any of these tests fail, the module will enter an error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. Each module performs the following conditional self-tests:

- OpenSSL Implementation
  - Pairwise consistency test for RSA implementation (signing and signature verification)
  - Pairwise consistency test for ECDSA implementation
  - Continuous RNG test run on output of DRBG
  - Continuous test on output of DRBG seed mechanism (NDRNG)
  - DRBG 800-90A Health Tests compliant with SP 800-90A Section 11.3
- GSKIT Implementation
  - Pairwise consistency test for RSA (signing and signature verification)
  - Pairwise consistency test for ECDSA
  - DRBG 800-90A
    - Health Tests compliant with SP 800-90A – Section 11.3.

    - The DRBG 800-90A generates a minimum of 8 bytes per request. If less than 8 bytes are requested, the rest of the bytes is discarded and the next request will generate new random data.
    - The first 8 bytes of every request is compared with the last 8 bytes requested, if the bytes match an error is generated.
    - For the first request made to any instantiation of a DRBG 800-90A, two internal 8 byte cycles are performed.
    - The DRBG 800-90A relies on the environment (i.e. proper shutdown of the shared libraries) for resistance to retrospective attacks on data.
    - The DRBG 800-90A performs known answer tests when first instantiated and health checks at intervals as specified in the standard.
- True Random Number Generator (TRNG)
    - A non-deterministic RNG (NDRNG) is used to seed the DRBG. Every time a new seed or n bytes is required (either to initialize the DRBG, reseed the DRBG periodically or reseed the DRBG by user's demand), the cryptographic module performs a comparison between the SHA-256 message digest using the new seed and the previously calculated digest. If the values match, the TRNG generates a new stream of bytes until the continuous DRBG test passes.

The modules do not perform a firmware load test because no additional firmware can be loaded in the module while operating in FIPS-approved mode. Please see Section 3 for guidance on configuring and maintaining FIPS mode.

2.11 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

This section describes how to configure the modules for FIPS-approved mode of operation. Operating a module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Firmware Installation

To install the appliance firmware, please follow these steps:

1. Log in to the ISS support site at https://ibmss.flexnetoperations.com/,
2. Select **My Software | Download** from the menu
3. Choose **IBM Security Network IPS (GV/GX Series)** and then the specific GX Series.
4. Select the appropriate firmware and recovery images from the **New Versions** dropdown menu
5. Accept the End User License by clicking **"I Agree"**
6. Select the appropriate Recovery image type (USB or ISO image)
7. Download the ***.usbimg** or ***.iso** image and follow the installation instructions.
8. Follow the instructions below to copy the update to the appliance:

    1) Using an SCP tool such as WinSCP, copy

    4.6.2.0-ISS-ProvG-FIPS-FP0001.tgz

    to the "/root" folder on your Proventia GX appliance.

    2) Use a serial console application such as PuTTY to log into your Proventia G or GX

    appliance as 'root'.

    3) Execute the following commands:

    ```
    tar -xvzf 4.6.2.0-ISS-ProvG-FIPS-FP0001.tgz
    cd 4.6.2.0-ISS-ProvG-FIPS-FP0001
    ```

    To install the update, execute

    ```
    ./install.sh
    ```

To uninstall the update, execute

```
./install.sh -r
```

3.1.2 Enabling FIPS Mode

When first powering on the module, the operator will be guided through a configuration wizard. In the CLI, the following will appear:

```
Enable FIPS mode [y/N]
```

To initialize the module for FIPS mode, the Crypto Officer must select **Y** at this prompt.

Note: The module can only be enabled for FIPS mode at the time of initial configuration. Additionally, if the module enters an error state (e.g., a known answer test fails), the module must be powered off and reimaged to FIPS mode of operation.

The Cryptographic Officer must follow the General Guidance (Section 3.1.3) to place the module in FIPS mode by removing root privileges to the GX Linux-based operating system.

3.1.3 General Guidance

The Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

- Verify that the firmware version of the module is Version 4.6.2. No other version can be loaded or used in FIPS mode of operation.
- Apply tamper evidence labels as specified in Section 3.1.4 – Placement of Tamper Evidence Labels. The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation.
- Ensure any unused labels are secure at all times.
- Inspect the tamper evidence labels periodically to verify they are intact.
- Do not disclose passwords and store passwords in a safe location and according to his/her organization's systems security policies for password storage.
    - Ensure root privileges via SSH are disabled while in FIPS approved mode. Execute the following commands:
        - service sshd stop
        - chkconfing sshd off
        - chkconfig sshd-iss off

- Configure the module to lock accounts after 3 unsuccessful authentication attempts.

3.1.4 Placement of Tamper Evidence Labels

To meet Physical Security Requirements for Level 2, each module enclosure must be protected with tamper evidence labels. The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation. The Crypto Officer is responsible for applying the labels; IBM Security does not apply the labels at time of manufacture. Once applied, the Crypto Officer shall not remove or replace the labels unless the module has shown signs of tampering, in which case the Crypto Officer shall reimage the module and follow all Guidance to place the module in FIPS mode.

Please note that if additional labels need to be ordered, the Crypto Officer shall contact IBM Security support and request part number *00VM255*.

The Crypto Officer is responsible for:

- Securing and having control at all times of any unused seals, and
- Maintaining the 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.

3.1.4.1 GX4004

A total of two tamper evidence labels are required and are included with the appliance. Application of the tamper evidence labels is as follows:

1. Turn off and unplug the system.
2. Clean the enclosure before applying the tamper evidence labels.
3. Place Label #1 the right side/bottom of the enclosure as shown in Figure 3 - GX4004 Tamper Evidence Label Placement (Front/Right)
4. Place Label #2 the left side/bottom of the enclosure as shown in Figure 4 - GX4004 Tamper Evidence Label Placement (Front/Left)

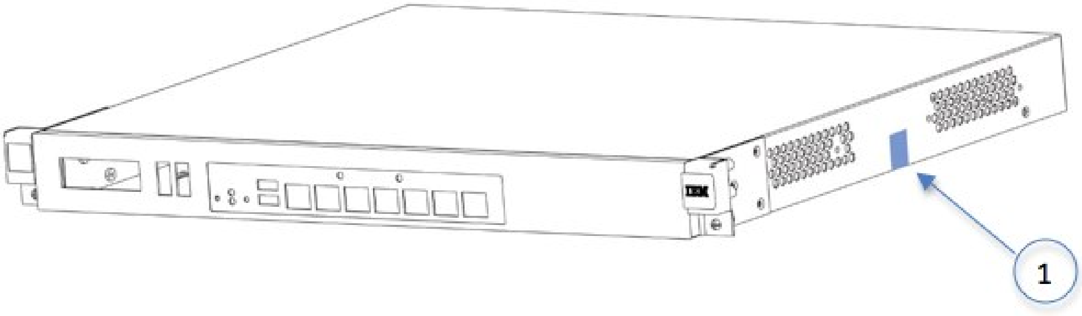


Figure 3 - GX4004 Tamper Evidence Label Placement (Front/Right)

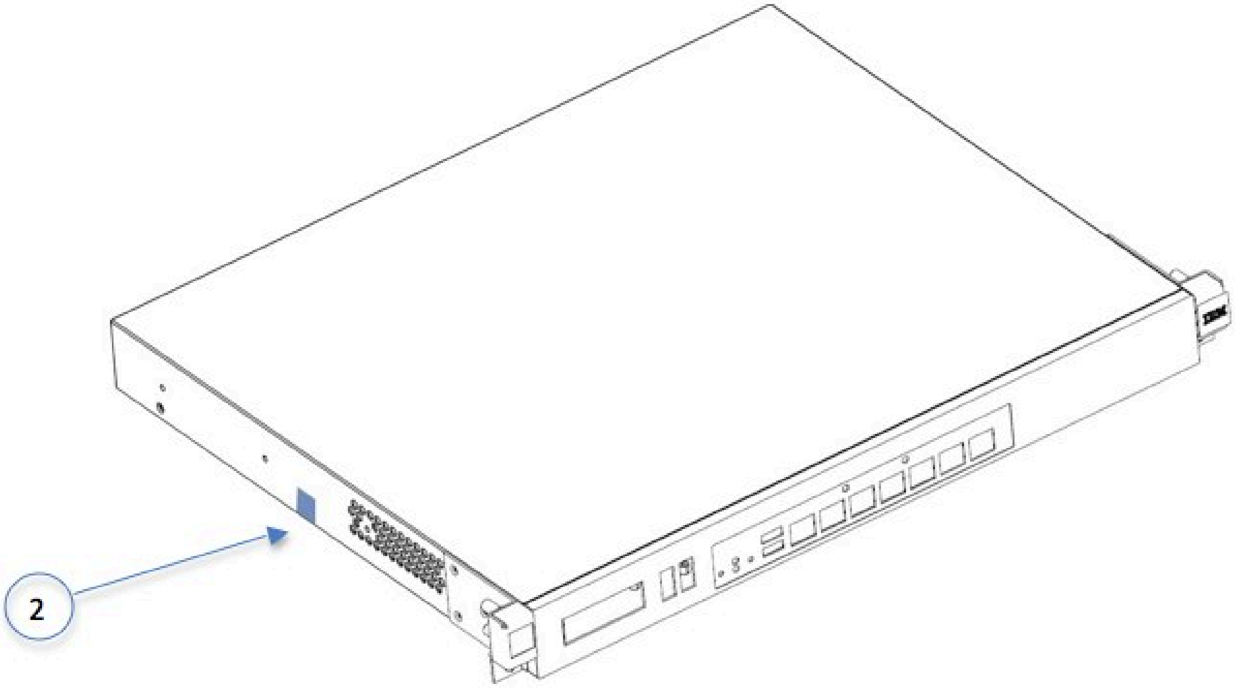


Figure 4 - GX4004 Tamper Evidence Label Placement (Front/Left)

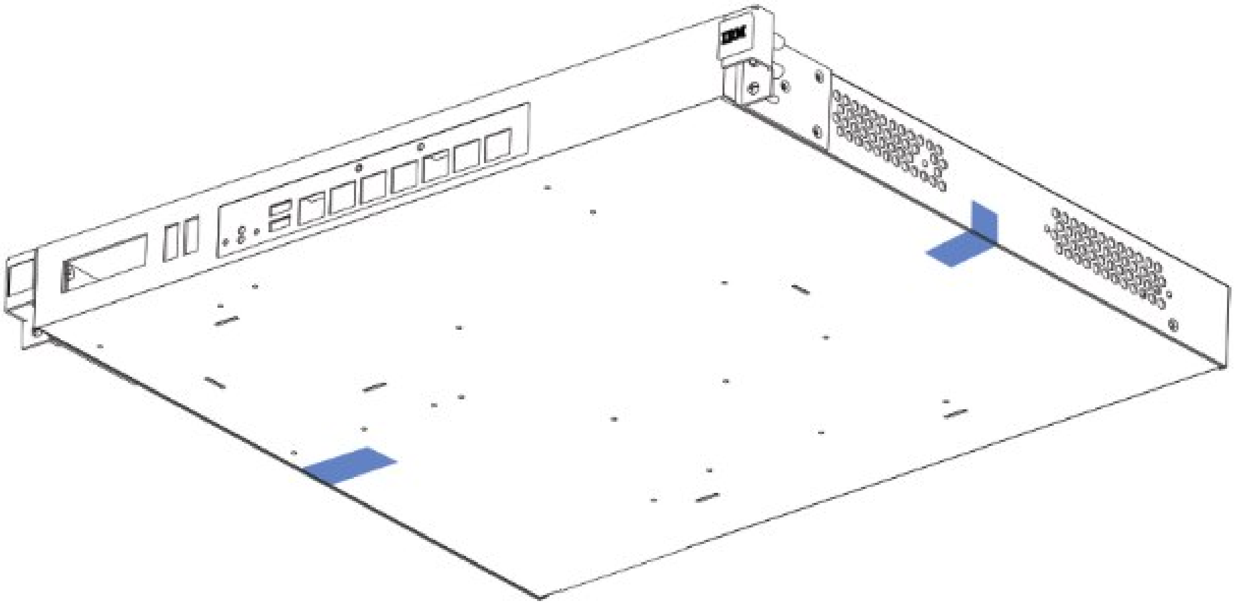


Figure 5 - GX4004 Tamper Evidence Label Placement (Bottom)

3.1.4.2 GX5000 Series

A total of eight tamper evidence labels are required and are included with the appliance. Application of the tamper evidence labels is as follows:

1. Turn off and unplug the system.
2. Clean the enclosure before applying the tamper evidence labels.
3. Place Label #1 over the top/right side of the enclosure as shown in Figure 6 - GX5000 Series Tamper Evidence Label Placement (Front)
4. Place Label #2 over the top/left side of the enclosure as shown in Figure 6 - GX5000 Series Tamper Evidence Label Placement (Front)
5. Place Label #3 over the top of the enclosure and the two fan baffles as shown in Figure 6 - GX5000 Series Tamper Evidence Label Placement (Front)
6. Place each of the #4 labels over the top hard drive bay as shown in Figure 6 - GX5000 Series Tamper Evidence Label Placement (Front)
7. Place each of the #5 labels over the bottom hard drive bay as shown in Figure 6 - GX5000 Series Tamper Evidence Label Placement (Front)
8. Place Label #6 over the front-right/bottom as shown in Figure 6 - GX5000 Series Tamper Evidence Label Placement (Front)
9. Place Label #7 on the back of the module as shown in Figure 7 – GX5000 Tamper Evidence Label Placement (Rear/RIght)
10. Place Label #8 over top/back as shown in Figure 7 – GX5000 Tamper Evidence Label Placement (Rear/RIght)

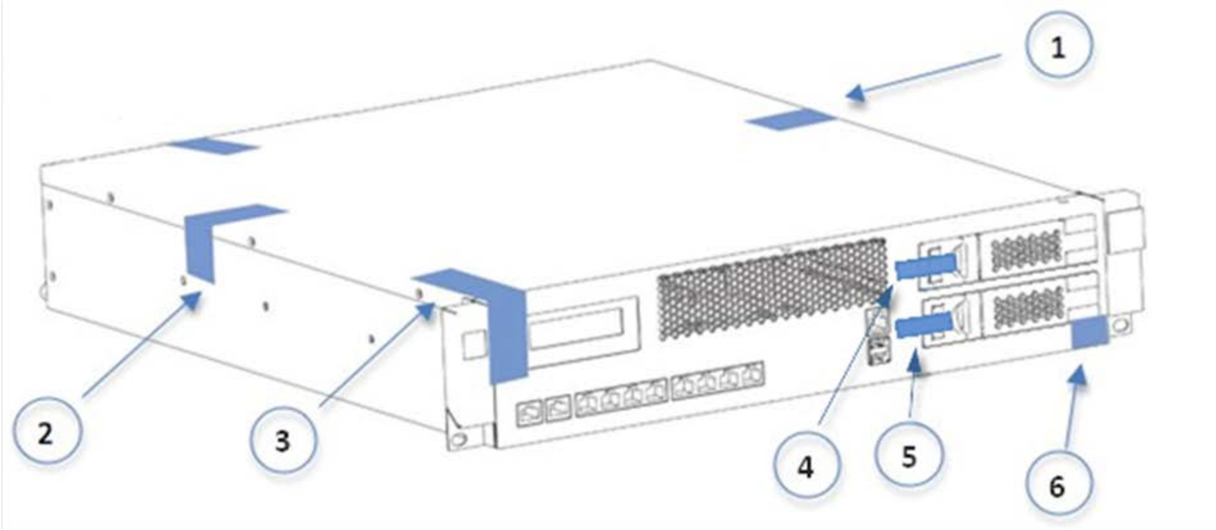


Figure 6 - GX5000 Series Tamper Evidence Label Placement (Front)

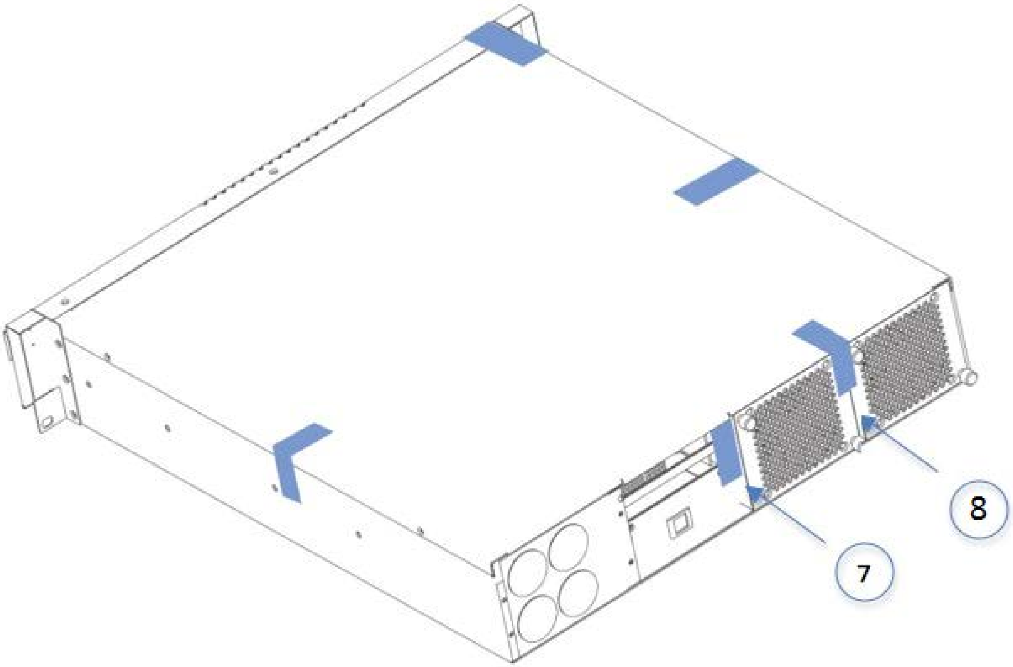


Figure 7 – GX5000 Tamper Evidence Label Placement (Rear/RIght)

3.1.4.3 GX7412 and GX7800 Series

A total of eight tamper evidence labels are required and are included with the appliance. Application of the tamper evidence labels is as follows:

1. Turn off and unplug the system.
2. Clean the enclosure before applying the tamper evidence labels.
3. Place Label #1 over the top/left side of the enclosure as shown in Figure 8 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)
4. Place Label #2 over the top/right side of the enclosure as shown in Figure 8 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)
5. Place Labels #3 and #4 over the removable hard drives as shown in Figure 8 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)
6. Place Label #5 over the top of the enclosure and the outer left fan baffle as shown in Figure 8 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)
7. Place Label #6 over the top of the enclosure and the outer right fan baffle as shown in Figure 8 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)

8. Place Labels #7 and #8 over the power supplies and edge of chassis as shown in Figure 9 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Rear and Top)

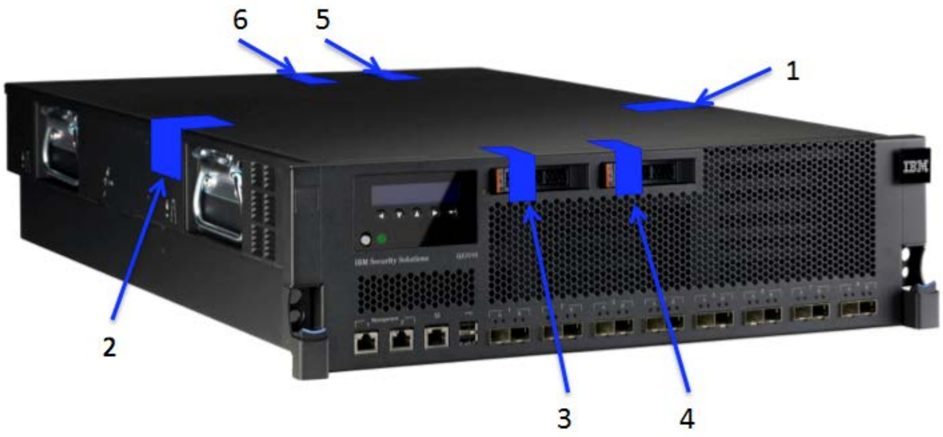


Figure 8 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)

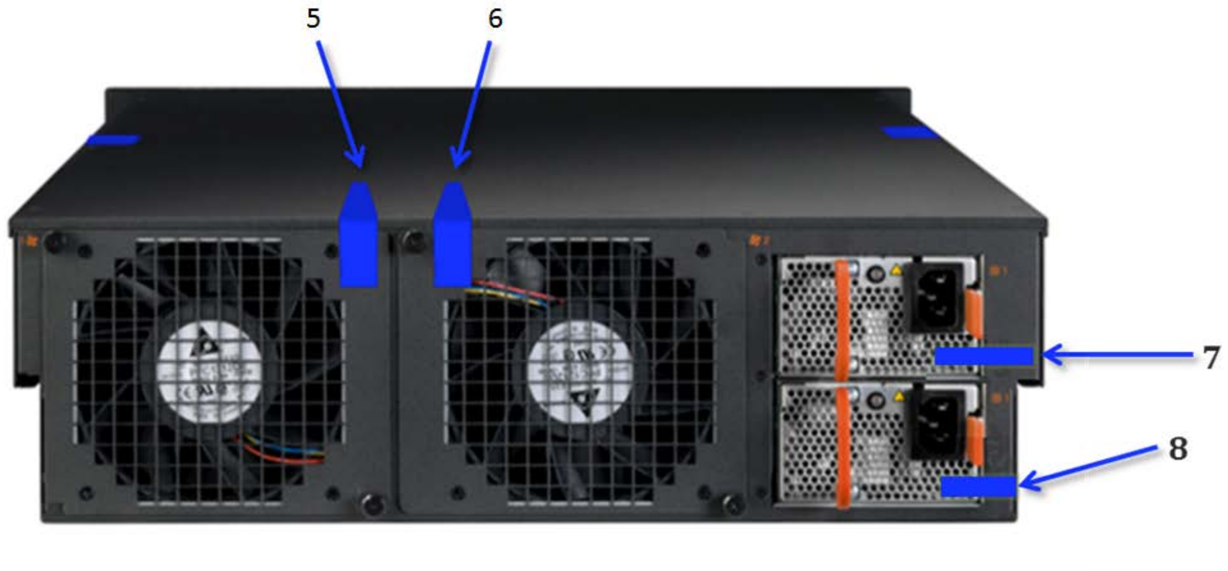


Figure 9 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Rear and Top)

3.2 User Guidance

3.2.1 General Guidance

The User role is defined by a management session over a TLS tunnel. As such, this role is authenticated, and no additional guidance is required to maintain FIPS mode of operation.

End of Document