FIPS 140-2 Non-Proprietary Security Policy

IBM Internet Security Systems Proventia GX Series Security Appliances Version 4.3

Document Version 1.2

January 31, 2013

Prepared For:

IBM Internet Security Systems, Inc.

6303 Barfield Road

Atlanta, GA 30328

www.iss.net

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 Proventia GX Series Security Appliances Version 4.3.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

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 Canada (CSEC) Cryptographic Module Validation Program (CMVP) runs the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for products meeting FIPS 140 validation. *Validated* is the term given to a product that is documented and tested against the FIPS 140 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 Proventia GX Series Security Appliances Version 4.3 from IBM Internet Security Systems 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 Internet Security Systems Proventia GX Series Security Appliances Version 4.3 may also be referred to as the "modules" in this document.

1.3 External Resources

The IBM Internet Security Systems website (http://www.iss.net) contains information on the full line of products from IBM Internet Security Systems, including a detailed overview of the Proventia GX Series Security Appliances Version 4.3 solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/) contains links to the FIPS 140-2 certificate and IBM Internet Security Systems contact information.

1.4 Notices

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
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
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
SHA	Secure Hashing Algorithm

Table 1 – Acronyms and Terms

2 IBM Internet Security Systems Proventia GX Series Security Appliances Version 4.3

2.1 Product Overview

The Proventia Network Intrusion Prevention System (IPS) automatically blocks malicious attacks while preserving network bandwidth and availability. The Proventia 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 Proventia GX Series Security Appliances Version 4.3 can be securely managed via the following interfaces:

- Proventia 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

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	Standard	CAVP Certificate	Use
Asymmetric Key	RSA with 1536-bit modulus	RFC2246 (TLS v1.0, PKCS1.5)	7412 and 7800: 1035	Sign / verify operations Key transport
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 180-3	7412 and 7800: 1756	Message digest in TLS sessions Module integrity via SHA-1
Keyed Hash	HMAC-SHA1	FIPS 198	7412 and 7800: 1211	Message verification
Symmetric Key	AES 256 in CBC mode	FIPS 197	7412 and 7800: 2006	Data encryption / decryption
Random Number Generation	ANSI X9.31	ANSI X9.31 (TDES)	7412 and 7800: 1049	Random Number Generation

Table 3 – Algorithm Certificates

2.3.2 Non-Approved Algorithms

The module implements the following non-FIPS approved algorithms:

- Firmware-based random number generator (dev/urandom)
    - This RNG is used only as a seeding mechanism to the FIPS-approved PRNG.

2.4 Cryptographic Module Specification

The modules are the IBM Internet Security Systems GX7412 and GX7800 running firmware version 4.3. Each module is classified as a multi-chip standalone cryptographic module and contains a cryptographic module to manage secure communications with Proventia Manager and SiteProtector Management System. The physical cryptographic boundary is defined as the module case.

2.4.1 Excluded Components

Excluded components include the following:

- Monitoring Ports
    - 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
    - This port is not security relevant and does not interact with the cryptographic processing of the appliance.
- Network Card
    - The network card provides input/output functionality from the motherboard to the exterior network; it does not provide any FIPS security relevant processing.

Although the actual data over these interfaces is excluded, the appliances do provide analysis of data. These scan results are encrypted by the cryptographic module and sent to the management interfaces (i.e., Proventia Manager and/or SiteProtector) for review.

The following keys are excluded because SSH is non-functional in FIPS mode of operation due to disabled root privileges (see Section 3 – Guidance and Secure Operation):

- RSA Private 1024-bit for sign / verify operations and key establishment for SSHv1
- RSA Private 1024-bit for sign / verify operations and key establishment for SSHv2
- DSA Private 1024-bit for sign / verify operations and key establishment for SSHv2

These excluded keys cannot be used in FIPS mode of operation; they can only be used in non-FIPS mode. Additionally, the Command Line Interface is “non functional” in FIPS mode of operation due to disabled root privileges.

The module illustrations are provided in the table below:

MODULE	MODULE ILLUSTRATION
7412	

MODULE	MODULE ILLUSTRATION
7800	

Table 4 – Module Illustrations

2.4.2 FIPS Mode / Non-FIPS Mode

The module contains a FIPS mode and a non-FIPS mode. The module can only be enabled for FIPS mode at the time of initial configuration. Once the module is configured for FIPS mode, the only way to return the module to a non-FIPS approved mode of operation is to reimage the module. 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.

Since FIPS mode and non-FIPS mode cannot exist simultaneously, there is no overlap in generation/sharing/zeroization of CSPs between modes of operation because the module must be reimaged to transition between the two modes. The non-FIPS mode security functions & services (including service inputs, service outputs, & roles performing those services) are consistent between the two modes with the exception of the Self Test service, which does not exist in non-FIPS mode. Self tests are only run when the module is in FIPS mode.

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 and obtaining IPS version information
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 Network traffic bypass (i.e., traffic not subjected to analysis engines)
Management Port 1	Communication with Proventia Manager and SiteProtector Management System

Physical Interface	Description / Use
Management Port 2 (excluded)	Exclusively for sending TCP Reset responses. This interface is excluded from the validation.

Table 5 – 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
Data Output	Management 1
Control Input	Management 1 Serial Console Port USB Ports LCD Panel
Status Output	Management 1 LCD Panel LEDs
Power	Power Plug On/Off Switch

Table 6 – Logical Interface / Physical Interface Mapping

2.6 Roles, Services, and Authentication

The module is accessed via Command Line Interface (CLI), Proventia 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 IP address, subnet mask, etc.), allowing an operator to initialize the module for FIPS mode of operation. The LCD Management only allows basic diagnostic services.

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 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.

More details can be found on page 29 of *Proventia Network IPS G and GX Appliance User Guide*.

2.6.1.2 Proventia Manager

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

- Monitor appliance status
- View log files
- Register SiteProtector
- Configure password
- IDS/IPS configuration (excluded from FIPS mode)

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 Proventia Manager. If managing a group of appliances along with other sensors, the centralized

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

management capabilities of SiteProtector may be preferred. SiteProtector controls the following management functions of the appliance:

- Monitor appliance status
- View log files
- Configure password
- IDS/IPS configuration (excluded from FIPS mode)

After the appliance is registered with SiteProtector, the functions above can be viewed in Proventia Manager and changed only from SiteProtector.

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 1 Power switch	None	Crypto Officer User
Decrypt	Decrypts a block of data using AES	Initiate AES decryption / data decrypted	Management 1	Session Key	Crypto Officer User
Encrypt	Encrypts a block of data using AES	Initiate AES encryption/ data encrypted	Management 1	Session Key	Crypto Officer User

Service	Description	Service Input / Output (API)	Interface	Key/CSP Access	Roles
Establish Session	Provides a protected session for establishment of AES keys with peers	Initiate session establishment / session established	Management 1	Private Key Public Key HMAC Key Premaster Secret (48 Bytes) Master Secret (48 Bytes)	Crypto Officer User
Zeroize CSPs	Clear CSPs from memory	Terminate Session / CSPs cleared	Management 1	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 1 Serial Console Port USB Ports LCD Panel LEDs	None	Crypto Officer User

Table 7 – Operator Services and Descriptions

2.6.3 Operator Authentication

The CO role authentication via CLI (when initially configuring the module for FIPS mode) or Proventia Manager over HTTPS/TLS in FIPS mode. Other than status functions available by viewing LEDs, the services described in Table 7 – Operator Services and Descriptions are available only to authenticated operators. When using Proventia Manager, the CO enters the password over a TLS session using the module's PKI to establish the secure channel.

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. Assuming 10 attempts per second

via a scripted or automatic attack, the probability of a success with multiple attempts in a one minute period is $600/62^6$, which is less than 1/100,000.

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 1536 bit keys via RSA. A 1536-bit RSA key has 96-bits of equivalent strength. The probability of a successful random attempt is 1/2^96, 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 60/2^96 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 Internet Security Systems 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.

2.9 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	Services	Privileges
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
PRNG Seed	160-bit system Entropy seed the X9.31 PRNG	Use dev / urandom to gather bytes from several areas of system data (including time/date), concatenate them together and hash via SHA-1	**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
PRNG Seed Key	256-bit value to seed the FIPS-approved	Gather bytes from several areas of system data (including	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer None

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Services	Privileges
	ANSI X9.31 PRNG	time/date)	**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 1536-bit for sign / verify operations and key establishment[2] for SiteProtector to GX appliances over TLS	Internal generation at installation by X9.31 PRNG	**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 1536-bit for sign / verify	Internal generation at installation by X9.31 PRNG	**Storage**: On disk in plaintext **Type:** Static	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer R W D

[2] Key establishment methodology provides at least 96-bits of encryption strength

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Services	Privileges
	operations and key establishment[3] for external entities (such as SiteProtector) to GX appliances over TLS. Encryption/Decryption of the Premaster Secret for entry/output		**Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Output**: plaintext during TLS negotiation		User R
External Entity Public Key	RSA Public 1536-bit key associated with remote entities (such as the browser or SiteProtector)	External generation by FIPS-approved technique	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Agreement**: NA **Entry**: Plaintext **Output**: NA	Establish Session	Crypto Officer R W D User R W D
HMAC key	160-bit HMAC-SHA1 for message	Partitioned from Master Secret	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer R W D

[3] Key establishment methodology provides at least 96-bits of encryption strength

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Services	Privileges
	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 appliance.	Not generated by the module; defined by the human user	**Storage**: On disk hashed with SHA-512 **Type:** Static **Association**: controlled by the operating system	**Agreement**: NA **Entry**: Manual entry **Output**: NA	Configure	Crypto Officer R W D User R W D
Premaster Secret (48 Bytes)	RSA-Encrypted Premaster Secret Message	Internal generation by X9.31 PRNG	**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 X9.31 PRNG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer None

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Services	Privileges
			Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: NA		User None
SNMP AES Key	AES CBC 256-bit key for encryption / decryption of SNMP traffic	Internal Generation via the Allowed SNMPv3 Key Derivation Function (KDF) (SP-800-135)	**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	Decrypt Encrypt	Crypto Officer R W D User R W D
Crypto Officer SNMPv3 Password	Alphanumeric passwords externally generated by a human user. Input to the SNMPv3 KDF	Not generated by the module; defined by the human user	**Storage**: On disk hashed with SHA-512 **Type:** Static **Association**: controlled by the operating system	**Agreement**: NA **Entry**: Manual entry **Output**: NA	Configure	Crypto Officer R W D User None
Crypto Officer SNMPv3 Authentication Password CSP	Used to generate SNMPv3 message authentication	Not generated by the module; defined by the human user	**Storage**: On disk hashed with SHA-512 **Type:** Static **Association**: controlled by the operating system	**Agreement**: NA **Entry**: Manual entry **Output**: NA	Configure	Crypto Officer R W D User None

R = Read W = Write D = Delete

Table 8 - Key/CSP Management Details

Public keys are protected from unauthorized 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 SHA-1
- RSA pairwise consistency (signing and signature verification)
- AES KAT (encryption and decryption)
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- HMAC-SHA1 KAT
- KAT for Approved PRNG

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:

- Pairwise consistency test for RSA implementation
- Continuous RNG test run on output of ANSI X9.31 PRNG

- Continuous test on output of ANSI X9.31 PRNG seed mechanism
- Continuous RNG test for non-approved firmware RNG
- Continuous test to ensure seed and seed key are not the same values

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 or in non-FIPS mode. Please see Section 3 for guidance on configuring and maintaining FIPS mode. Once in non-FIPS mode, the only way to resume FIPS mode is to reimage the module and perform a clean install for FIPS mode. In this case, all persistent CSPs are zeroized.

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://webapp.iss.net/myiss/login.jsp
2. Select **Downloads** from the menu
3. Choose **FIPS enabled systems** from the **Select a Product** dropdown menu and then select **Go**
4. Select the appropriate firmware from the **Version** dropdown menu then select **Go**
5. Select **Other Updates** and select **Continue** next to the bundle listing for the appropriate firmware
6. Accept the End User License and select **Submit**
7. Download the ***.iso** image and follow the upgrade instructions in the *Reinstalling Appliance Firmware* section of *IBM Proventia Network Intrusion Prevention System G/GX Appliance User Guide*.

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. Once the module is configured for FIPS mode, the only way to return the module to a non-FIPS approved mode of operation is to reimage the module. 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 4.3. 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.
- Root privilege to the module must be disabled; therefore, SSH cannot be used in FIPS mode of operation.

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 Internet Security Systems 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 Internet Security Systems support and request part number *FIPS-LABELS: FIPS 140 tamper evidence labels*.

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 GX7412 and GX7800 Series

A total of seven 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 1 – 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 1 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)
5. Place Label #3 over the top of the enclosure and the outer right fan baffle as shown in Figure 1 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)
6. Place Label #4 over the top of the enclosure and the outer left fan baffle as shown in Figure 1 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)
7. Place Label #5 over the power supplies and edge of chassis as shown in Figure 2 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Rear and Top)
8. Place Labels #6 and #7 over removable hard drives as shown in Figure 1 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)

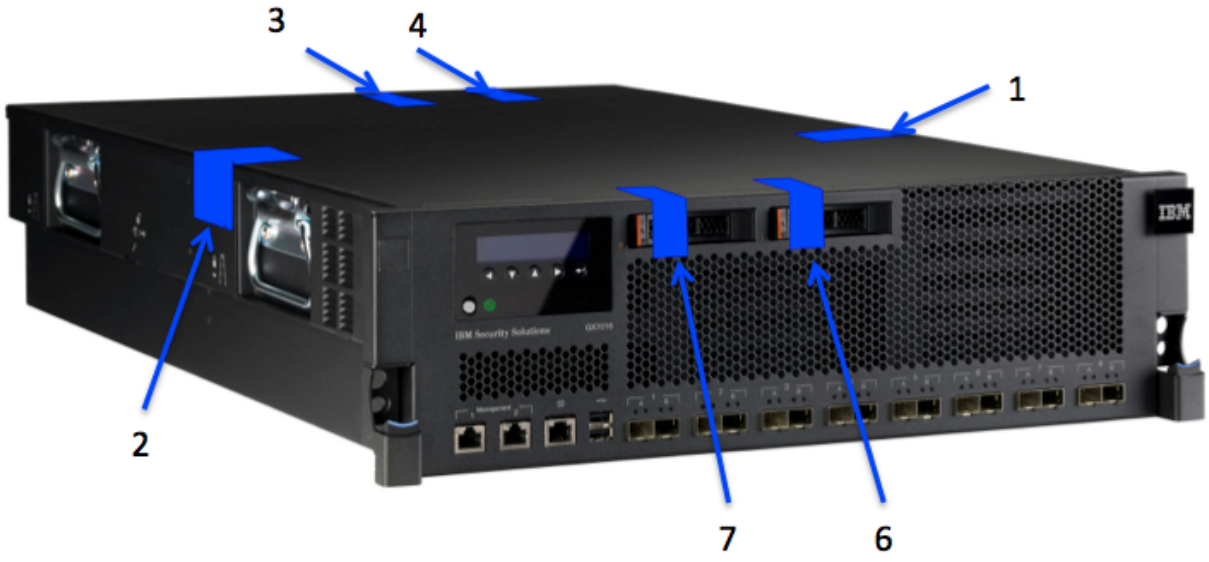

Figure 1 – GX7412 and GX7800 Series Tamper Evidence Label Placement (Front and Sides)

Figure 2 – 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
