IBM Corporation

IBM Security QRadar FIPS Appliance

Hardware Part Number: QR24; Firmware Version: v7.1 MR1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.6

Prepared for:

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722
United Stated of America

Phone: +1 914-499-1900
http://www.ibm.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States America

Phone: +1 703-267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section introduces the non-proprietary Security Policy for the IBM Security QRadar FIPS Appliance.

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the IBM Security QRadar FIPS Appliance. This Security Policy describes how the IBM Security QRadar FIPS Appliance meets the security requirements of FIPS Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The IBM Security QRadar FIPS Appliance is referred to in this document as QRadar, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The IBM website (www.ibm.com) contains information on the full line of solutions from IBM.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to IBM Corporation. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to IBM and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact IBM.

2 IBM Security QRadar FIPS Appliance

This section describes the IBM Security QRadar FIPS Appliance by IBM Corporation.

2.1 Overview

IBM's QRadar Release v7.1 MR1 is a distributed network security management platform that provides situational awareness and compliance support through the combination of flow-based network knowledge, security event correlation, log management, and asset-based vulnerability assessment.

QRadar integrates previously disparate functions (including risk management, log management, network behavior analytics, and security event management) into a total security intelligence solution, making it the most intelligent, integrated, and automated SIEM product available. Built on an IBM platform, the QRadar solution provides users with crucial visibility into what is occurring with their networks, data centers, and applications to better protect Information Technology (IT) assets and meet regulatory requirements.

QRadar collects and processes data including log data (from security devices, network devices, applications, and databases); network activity data, or "flows" (from network taps, mirror ports, or third-party flow sources such as NetFlow), and vulnerability assessment data. The product produces security events by real-time event and flow matching and by comparing the collected data to historical flow-based behavior patterns. The security events are then correlated by the product to produce weighted alerts (i.e. offenses) which can be viewed in the web-based QRadar Graphical User Interface (GUI) as well as sent to users or other solutions via email, syslog, or SNMP[1] trap.

QRadar:

- Provides a customizable interface through which users can view summaries and detailed information about offenses, log and event activity, and network activity (flows) occurring on a given network.
- Analyzes overall network security, vulnerability states, and network traffic behavior.
- Automatically discovers servers and hosts operating on a given network in order to build an asset profile. User identity, vulnerability data and passively learned services information are correlated back to the asset profile.
- Allows users to create, distribute, and manage reports for any data.

QRadar tracks significant incidents and threats, and builds a history of supporting and relevant information. Information such as point-in-time, offending users or targets, attacker profiles, vulnerability state, asset value, active threats and records of previous offenses all help provide security teams with the intelligence they need to act regardless of where they are.

QRadar employs cryptographic functions to secure the GUI and the QConsole interface. The QConsole is used either locally or over Secure Shell (SSH) to manage the cryptographic module. Administration of the appliance and viewing network events takes place on the GUI over Transport Layer Security (TLS) sessions.

The IBM Security QRadar FIPS Appliance (seen in Figure 1 below) is an enterprise-class network security management appliance that combines security information, event management, and log management, and is well-suited for organizations ranging from medium-sized to large, globally-deployed entities. QRadar

[1] SNMP – Simple Network Management Protocol

serves as the base platform for geographically-dispersed organizations or any organization that requires an integrated solution to monitor their global network with the efficiency of a single web-based QRadar user interface.

Figure 1 – IBM Security QRadar FIPS Appliance

To provide security for all QRadar flow and event traffic between appliances, SSH encryption can be enabled via the QConsole interface. The appliance employs a cryptographic library to provide its security services needed for the SSH tunnels and the HTTPS[2]-secured GUI sessions.

The IBM Security QRadar FIPS Appliance is validated at the following FIPS 140-2 Section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A[3]
7	Cryptographic Key Management	2
8	EMI/EMC[4]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	2

[2] HTTPS – Hypertext Transfer Protocol - Secure
[3] N/A – Not Applicable
[4] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.2 Module Specification

The IBM Security QRadar FIPS Appliance is a multi-chip standalone hardware module that meets overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the QRadar is defined by the hard metal appliance chassis, which surrounds all the hardware and software components.

2.3 Module Interfaces

Interfaces on the module can be categorized as the following FIPS 140-2 logical interfaces:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

These logical ports map to the module's physical ports and interfaces. Physical ports and interfaces for the module are as follows (quantities appear in parentheses):

Front:

- Up to 12 hot-swappable Hard Disk Drives
- (13) Hard Drive Activity Indicators
- (12) Hard Drive Status Indicators
- Power Button
- Power Supply Status Indicators
- Universal Serial Bus (USB) Ports
- System error Indicator
- Locator
- System Identification (ID) label

Rear:

- Systems-management Ethernet Interface (optional)
- Gb[5] Ethernet RJ-45 Connectors
- Ethernet activity light-emitting diodes (LED)s
- Ethernet link LEDs
- NMI[6] Button
- Power Supply Interfaces
- Power Supply Status Indicators
- (1) 9-Pin Serial Port Connector
- (2) USB Ports
- (2) 15-pin Video Connectors
- (2) PCIe[7] slots
- (4) Hot swappable Hard Disk Drives

Figure 2 and Figure 3 illustrate the front and back panel features and indicators of the module.

[5] Gb – Gigabit
[6] NMI – Non-Maskable Interrupt
[7] PCIe – Peripheral Component Interconnect Express

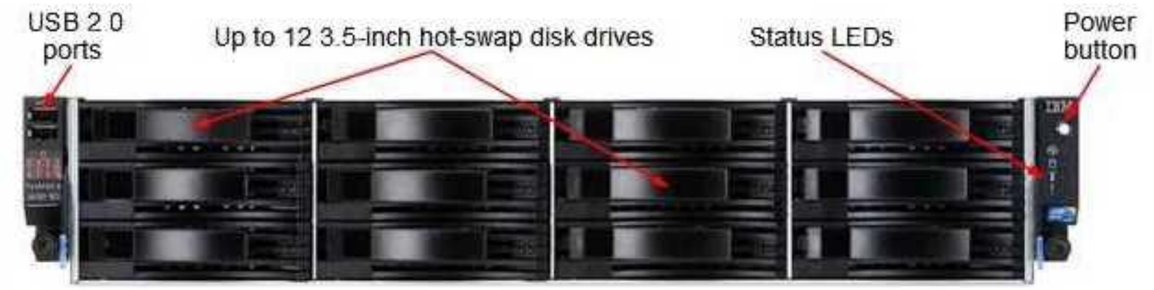

Figure 2 – QRadar FIPS Appliance Front Panel Features and Indicators

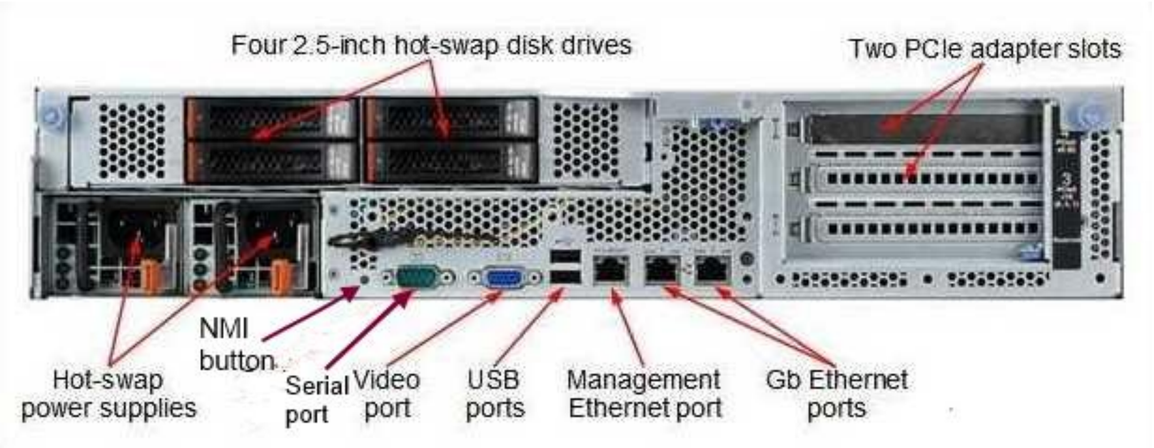

Figure 3 – QRadar FIPS Appliance Back Panel Features and Indicators

All of these physical interfaces map to logical interfaces defined by FIPS 140-2, as described in Table 2.

Table 2 – FIPS 140-2 Logical and Physical Interface Mappings

FIPS 140-2 Logical Interface	Module Interface
Data Input	• Ethernet interfaces • Serial connector • USB ports
Data Output	• Ethernet interfaces • Serial connector • USB ports
Control Input	• System management interface • Ethernet interfaces • NMI button • Power button • Serial connector

FIPS 140-2 Logical Interface	Module Interface
Status Output	• System management interface • Hard drive status and activity indicators • Ethernet interfaces • Ethernet interface activity and link indicators • Power supply status indicators • Serial connector • System error indicator • Video connector
Power	• Power supply interface

2.4 Roles, Services, and Authentication

The following sections described the authorized roles supported by the module, the services provided for those roles, and the authentication mechanisms employed.

2.4.1 Authorized Roles

The module supports role-based authentication. There are three authorized roles in the module that an operator may assume: a Crypto-Officer (CO) role, a FIPS Admin role, and a User role.

- Crypto-Officer – The Crypto-Officer role performs administrative services on the module, such as initialization, configuration, and monitoring of the module. Before accessing the module for any administrative service, the operator must authenticate to the module. The module offers 2 management interfaces:
  - Web GUI – Accessible only by User roles
  - QConsole – Accessible only by CO and FIPS Admin roles

- FIPS Admin – The FIPS Admin role has the ability to modify system files, view logs, and reboot the appliance.

- User – The User role has the ability to perform basic cryptographic operations.

2.4.2 Services

All services require that operators assume an authorized role. The services associated with each role are listed in Table 3, Table 4, and Table 5 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 3 use the following indicators to show the type of access required:

- **R (Read)**: The CSP is read
- **W (Write)**: The CSP is established, generated, modified, or zeroized
- **X (Execute)**: The CSP is used within an Approved or Allowed security function or authentication mechanism

Table 3 – Crypto-Officer Role's Services

Service	Description	Input	Output	CSP and Type of Access
Commit	Apply changes to system files	Command	Command Response	None
Deploy	Start a full deploy on the appliance. Restarts all services	Command	Command Response and Status Output	None
Disable FIPS	Takes the module out of FIPS mode; reboots appliance; restarts services	Command	Command Response and Status Output	Advanced Encryption Standard (AES) – W Triple Data Encryption Standard (Triple-DES) – W RSA public/private keys – W Diffie-Hellman (DH) – W (keyed) Hash Message Authentication Code (HMAC) – W
Display status	Displays status of the operating system (OS), required RPM[8] files, log settings, and FIPS mode	Command	Command Response and Status Output	None
Get logs	Collects system log data	Command	Command Response	None
Modify log source	Modifies the sources for the system log data	Command	Command Response	None
Reboot	Reboots the module	Command	Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
Start, stop, or restart a service	Starts, stops, or restarts any service the CO has access to on the appliance	Command	Command Response	AES – W Triple-DES – W
Shutdown	Shuts down the appliance	Command	Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W

Table 4 – FIPS Admin Role's Services

Service	Description	Input	Output	CSP and Type of Access
Commit	Apply changes to system files	Command	Command Response	None
Deploy	Start a full deploy on the appliance. Restarts all services	Command	Command Response and Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W

[8] RPM – Red Hat Package Manager

Service	Description	Input	Output	CSP and Type of Access
Get logs	Collects system log data	Command	Command Response	None
Modify log source	Modifies the sources for the system log data	Command	Command Response	None
Reboot	Reboots the module	Command	Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
Shutdown	Shuts down the appliance	Command	Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W

Table 5 – User Role's Services

Service	Description	Input	Output	CSP and Type of Access
Admin GUI User only				
Manage Roles	View, create, edit, and delete operator roles for GUI only.	Command	Command Response	None
Manage Accounts	Create, edit, and disable operator accounts	Command	Command Response	None
Set Authentication Type	Set the module to perform authentication via system, RADIUS[9], TACACS[10], or LDAP[11]/Active Directory	Command	Command Response	RADIUS key – W TACACS key – W LDAP credential – W
Manage License Keys	View, update, and export license keys	Command	Command Response	None
Restart System	Restart the module	Command	Command Response	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W
Shut Down System	Shut down the module	Command	Command Response	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W

[9] RADIUS – Remote Authentication Dial-In User Service

[10] TACACS – Terminal Access Control Access Control System

[11] LDAP – Lightweight Directory Access Protocol

Service	Description	Input	Output	CSP and Type of Access
Admin GUI User only				
Configure Access Settings	Configure firewall access, update host set-up, configure interface roles, change passwords, and update system time	Command	Command Response	User passwords – W, X
Configure System	Set up network hierarchy, system settings, system notifications schedules, and Console settings	Command	Command Response	None
Manage Authorized Services	View, add, and revoke authorized services; configure customer support service	Command	Command Response	None
Manage Backup and Recovery	Manage backup archives and backup/restore data	Command	Command Response	None
Edit Deployment	Create a deployment, assign connections, and configure individual module component	Command	Command Response	AES – R, W, X Triple-DES – R, W, X
Manage Flow Sources	Manage flow sources and flow source aliases	Command	Command Response	None
Configure Remote Networks and Services	Manage QRadar remote networks and services	Command	Command Response	None
Configure Rules	Configure rules to perform tests on events, flows, and offenses	Command	Command Response	None
Discover Servers	Discover servers for creating server-type building blocks	Command	Command Response	None
Forward Syslog Data	Forward raw or normalized syslog data to specified destinations	Command	Command Response	None
Select Data Sources	Provides access to vulnerability scanners, log source management, custom event and flow properties, and flow sources	Command	Command Response	None
Configure Plug-Ins	Provides access to plug-in components, such as the plug-in for the QRadar Risk Manager	Command	Command Response	None
View Audit Logs	Allow User to view audit log files	Command	Command Response	None
Perform self-tests	Run self-tests on demand via reboot	Command	Status Output	None

Service	Description	Input	Output	CSP and Type of Access
Admin GUI User only				
Zeroize	Zeroizes the module to the factory default state	Command	Status Output	AES – W Triple-DES – W RSA public/private keys – W DH – W HMAC – W RADIUS key –W TACACS key – W
All Users				
Manage Dashboard	View, create, edit, and delete a dashboard	Command	Command Response	None
Analyze Events	Analyze records from a network activity log	Command	Command Response	None
Analyze Flows	Monitor network flow data in real-time	Command	Command Response	None
Manage Assets	View and manage asset profiles	Command	Command Response	None
Manage Reports	Create, generate, customize, and view reports	Command	Command Response	None

2.4.3 Authentication Mechanisms

The module supports role-based authentication to control access to services that require access to sensitive keys and CSPs. The CO and FIPS Admin roles are the only roles authorized to access the QConsole. Users can only connect to the Web GUI.

To access module services, the CO and FIPS Admin role must authenticate using a user ID and password. This can be done locally or using SSH to establishing a secure tunnel to the QConsole. Secure sessions that authenticate the CO and FIPS Admin only provide the services associated with those roles (i.e., they have no interface available to access other services). Each CO or FIPS Admin SSH session remains active and secured using the tunneling protocol until the operator logs out or an inactivity time is reached.

Users connecting to the module through the Web GUI must first establish a TLS session. These Users then enter a username and password which may be authenticated locally or through the use of external RADIUS, TACACS, or LDAP servers.

The module employs the authentication methods described in Table 6 below**Error! Reference source not found.** to authenticate a Crypto-Officer, FIPS Admin, and User.

Table 6 – Authentication Mechanisms Employed by the Module

Role	Type of Authentication	Authentication Strength
Crypto-Officer and FIPS Admin	Password	Passwords are required to be at least 6 characters long. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and special characters can be used with repetition, which gives a total of 69 characters to choose from. The chance of a random attempt falsely succeeding is 1:69^6, or 1: 107,918,163,081. This would require about 1,079,181 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps[12]. Hence, at most 60,000,000,000 bits of data (1000 × 10^6 × 60 seconds, or 6 x 10^{10}) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 812,759 attempts can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding.
User	Password or Certificate	Passwords are required to be at least 6 characters long. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and special characters can be used with repetition, which gives a total of 94 characters to choose from. The chance of a random attempt falsely succeeding is 1:94^6, or 1: 689,869,781,056. This would require about 6,898,697 attempts in one minute to raise the random attempt success rate to more than 1:100,000. Since the user is locked out for 30 minutes after every 5 unsuccessful attempts, the most attempts that could be done in one minute would be 5. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding. Certificates used as part of TLS and SSH are at a minimum 1024 bits. The chance of an attack falsely succeeding is 1:2^{80}, or 1:120,893 x 10^{24}. The fastest network connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data (1000 × 10^6 × 60 seconds, or 6 × 10^{10}) can be transmitted in one minute. The passwords are sent to the module via security protocols TLS and SSH. These protocols provide strong encryption (AES 128-bit key at minimum, providing 128 bits of security) and require large computational and transmission capability. The probability that a brute force attack will succeed or a false acceptance will occur is less than 1:2^{128} x 84^4.

2.4.3.1 Authentication Data Protection

The module does not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. Authentication data can only be modified by the operator who has assumed the

[12] Gbps – Gigabits per second

User role with administrator privileges. The module hashes User's passwords with an SHA-1[13] hash function and stores the hashed password in a password database. CO and FIPS Admin roles passwords are encrypted using Triple-DES and stored in a password database. If a User attempts to access the system multiple times (5 by default) using invalid information, the User must wait the configured amount of time (30 minutes by default) before attempting to access the system again.

2.5 Physical Security

The IBM Security QRadar FIPS Appliance is a multi-chip standalone cryptographic module. The module is contained in a hard metal chassis which is defined as the cryptographic boundary of the module. The module's chassis is opaque within the visible spectrum. The enclosure of the module has been designed to satisfy Level 2 physical security requirements. There are a limited set of ventilation holes provided in the case that, when coupled with factory-installed internal opacity baffles, prevent visual inspection the internal components of the module. Tamper-evident seals are applied to the case to provide physical evidence of attempts to remove the chassis cover or front bezel.

The QRadar system has been tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.6 Operational Environment

The module employs a non-modifiable operating environment. The module runs Red Hat Enterprise Linux (RHEL) v6.3, and operators are provided with no mechanisms with which to modify the operating system. Also, the module does not provide a mechanism to add additional software/firmware onto the appliance. The module's firmware is executed by the module's Intel Xeon processor.

2.7 Cryptographic Key Management

Security functions offered by the libraries in the module's Approved mode of operation (and their associated algorithm implementation certificate numbers) are listed in Table 7 below.

Table 7 – Approved Algorithm Implementations

Algorithm	Certificate Number
AES in ECB[14]/CBC[15]/CFB[16]/OFB[17] modes: 128/192/256-bit	#2562
Triple-DES in ECB/CBC/CFB8/CFB64/OFB modes: 168/192-bit	#1550
RSA ANSI X9.31 signature generation (2048/3072-bit); signature verification (1024/2048/3072-bit)	#1313
RSA PKCS[18] #1.5 signature generation (2048/3072-bit); signature verification (1024/2048/3072-bit)	#1313
RSA PSS[19] signature generation (2048/3072-bit); signature verification (1024/2048/3072-bit)	#1313

[13] SHA – Secure Hash Algorithm
[14] ECB – Electronic Code Book
[15] CBC – Cipher Block Chaining
[16] CFB – Cipher Feedback
[17] OFB – Output Feedback
[18] PKCS – Public-Key Cryptography Standards

Algorithm	Certificate Number
SHA-1, SHA-256, SHA-512	#2160
HMAC using SHA-1, SHA-256, SHA-512	#1581
ANSI X9.31 Pseudo-Random Number Generator (PRNG) using AES	#1216

***NOTE**: The following security functions have been deemed "deprecated" or "legacy-use" by NIST. Please refer to NIST Special Publication 800-131A for specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms.*

- *Two-key Triple-DES*
- *RSA 1024-bit signature verification*
- *ANSI X9.31 PRNG*

Key derivation functions implemented by the module (and their associated CVL[20] certificate numbers) are listed in Table 8 below.

Table 8 – Approved Key Derivation Function Implementations

Algorithm	Certificate Number
TLS 1.0 KDF using SHA-1	#194
SSH KDF using SHA-1, SHA-256, and SHA-512	#194

***NOTE**: The TLS and SSH protocols have not been reviewed or tested by the CAVP and CMVP*

The module implements the following non-Approved security functions which are allowed for use in a FIPS-Approved mode of operation:

- non-Approved random number generator for seed generation
- Message Digest 5 (MD5) for password hashing

The module utilizes the following key establishment methodologies which are allowed for use in a FIPS-Approved mode of operation:

- Diffie-Hellman (key agreement; key establishment methodology provides at least 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

The module also includes the following non-compliant algorithms:

- 1024-bit RSA ANSI X9.31 signature generation
- 1024-bit RSA PKCS #1 signature generation
- 1024-bit RSA PSS signature generation

[19] PSS – Probabilistic Signature Scheme

[20] CVL – Component Validation List

The module supports the CSPs listed below in Table 9.

Table 9 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP/Key Type	Generation / Input	Output	Storage	Zeroization	Use
AES Keys ECB, CBC, OFB, CFB 128	AES 128, 192, 256-bit keys	Internally generated	Never	Plaintext in volatile memory	On session termination or by command, power cycle, reboot	TLS or SSH session key Encryption/decryption
Triple-DES Keys ECB, CBC, CFB 8, CFB 64, OFB	Triple-DES 168, 192-bit key	Internally generated	Never	Plaintext in volatile memory	On session termination or by command, power cycle, reboot	TLS or SSH session key Encryption/decryption
RSA Private Key	RSA 1024, 2048 and 3072-bit key	Imported via TLS	Never	Plaintext in volatile memory	By command, power cycle, reboot	Signature generation, decryption Negotiating TLS or SSH sessions
RSA Public Key	RSA 1024, 2048 and 3072-bit key	Imported via TLS	Never Output during TLS/SSH negotiation in plaintext	Plaintext in volatile memory	By command, power cycle, reboot	Signature verification, encryption Negotiating TLS or SSH sessions
DH Public Key	Public components of DH protocol	Module's public key is internally generated via Approved FIPS PRNG. Other entities' public keys are sent to the module in plaintext.	Output during TLS/SSH negotiation in plaintext	Plaintext in volatile memory	By command, power cycle, reboot	Negotiating SSH or TLS sessions
DH Private Key	Private components of DH protocol	Internally generated	Never	Plaintext in volatile memory	By command, power cycle, reboot	Negotiating SSH or TLS sessions

.

CSP	CSP/Key Type	Generation / Input	Output	Storage	Zeroization	Use
ANSI X9.31PRNG Seed	128-bit random value	Taken from dev/urandom	Never	Plaintext in volatile memory	By command, power cycle, reboot	Generate random number
PRNG Seed Key	AES 128-, 192-, or 256-bit key	Generated internally	Never	Plaintext in volatile memory	By command, power cycle, reboot	Generate random number
Crypto-Officer Password FIPS Admin Password	Passphrase of at least six characters	Entered by a CO or FIPS Admin locally	Never	Stored on disk in encrypted form	Zeroized when the password is updated with a new password	Used for authenticating all COs and FIPS Admin over CLI[21]
User Password	Passphrase of at least five characters	Entered by User over secure TLS channel	Never	Stored on disk in hashed form	Zeroized when the password is updated with a new password	Used for authenticating all Users over GUI
RADUIS credential	Alpha-numeric string	Entered by User over secure TLS channel	Never	Stored on disk in hashed form	Zeroized when the password is updated with a new password	This password is used by the module to authenticate itself to the RADIUS server. This password is required for the module to validate the credential supplied by the user with the RADIUS server
LDAP credential	Alpha-numeric string	Entered by User over secure TLS channel	Never	Stored on disk in hashed form	Zeroized when the password is updated with a new password	This password is used by the module to authenticate itself to the LDAP server. This password is required for the module to validate the credential supplied by the user with the LDAP server
TACACS Server Encryption Key	Alpha-numeric string	Entered by User over secure TLS channel	Never	Stored on disk in hashed form	Zeroized when the password is updated with a new password	A shared secret to remote TACACS server

[21] CLI – Command Line Interface

.

CSP	CSP/Key Type	Generation / Input	Output	Storage	Zeroization	Use
HMAC Key	HMAC key SHA-1, 256, or 512	Internally generated	Never	Plaintext in volatile memory	By command, power cycle, reboot	Message Authentication
Software Integrity Keys	HMAC SHA-256 key	Externally generated and hard-coded in the image	Never	Hard-coded in plaintext	By uninstalling the module	Used to perform the software integrity test at power-on.
SMNP Privacy Key	AES CFB 128-bit key	Externally generated, imported in encrypted form via a secure TLS or SSH session	Never	Stored on disk in hashed form	By command, power cycle, reboot	Encrypting SNMPv3 packets

2.7.1 Key Generation

The module uses an ANSI X9.31 Appendix A.2.4 PRNG implementation to generate cryptographic keys. This PRNG is FIPS-Approved as shown in Annex C to FIPS PUB 140-2.

2.7.2 Key Entry and Output

The cryptographic module itself does not support key entry or key output from its physical boundary. However, keys are passed to the module as parameters from the applications resident on the host platform via the exposed APIs. Similarly, keys and CSPs exit the module in plaintext via the well-defined exported APIs.

2.7.3 Key/CSP Storage and Zeroization

Symmetric, asymmetric, and HMAC keys are either provided by or delivered to the calling process, and are subsequently destroyed by the module at the completion of the API call. Keys and CSPs stored in random access memory (RAM) can be zeroized by a power cycle or a host system reboot. The X9.31 PRNG seed and seed key are initialized by the module at power-up and remain stored in RAM until the module is uninitialized by a host system reboot or power cycle. The HMAC keys that are used to verify the integrity of the module during power-on self tests are stored in files residing on the host IBM FIPS Appliance.

2.8 EMI/EMC

QRadar was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

This section describes the power-up and conditional self-tests performed by the module.

2.9.1 Power-Up Self-Tests

The IBM Security QRadar FIPS Appliance performs the following self-tests automatically at power-up:

- Software integrity check (HMAC-SHA-512) over kernel and critical components of the module
- Software integrity check (HMAC SHA-256) over core cryptographic provider
- Known Answer Tests (KATs)
  - AES (Encrypt)
  - AES (Decrypt)
  - Triple-DES (Encrypt)
  - Triple-DES (Decrypt)
  - RSA (Signature Generation)
  - RSA (Signature Verification)
  - HMAC SHA-1
  - HMAC SHA-256
  - HMAC SHA-512
  - ANSI X9.31 PRNG

If any of the tests listed above fails to complete successfully, the module enters into a critical error state where all cryptographic operations and output of any data is prohibited. An error message is logged for the CO to review and requires action on the CO’s part to clear the error state.

2.9.2 Conditional Self-Tests

The IBM Security QRadar FIPS Appliance performs the following conditional self-tests:

.

- Continuous PRNG Test
- RSA Pairwise Consistency Check for sign/verify

Failure of any conditional test listed above leads the module to a soft error state and logs an error message.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3 Secure Operation

The IBM Security QRadar FIPS Appliance meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation. The use of any interfaces and services not documented herein are prohibited and considered in violation of this Security Policy, and shall result in the non-compliant operation of the module.

3.1 Crypto-Officer Guidance

The Crypto-Officer shall be responsible for setup, initialization, and management of the module. This Security Policy (as well as the *IBM Security QRadar Version 7.1.0 (MR1) FIPS Installation Guide*) provides instructions for applying physical security seals on the appliance. This guidance should be used in conjunction with the *IBM Security QRadar Hardware Installation Guide* to install the module and place it into its Approved mode of operation. Setting the module into its Approved mode will automatically create the crypto and admin accounts which are the only authorized QConsole accounts in FIPS mode.

3.1.1 Appliance Setup

Before the module can be placed into its Approved mode of operation, the Crypto-Officer shall install all required physical security mechanisms. Twenty (20) tamper-evident seals are included with the appliance. Sixteen (16) seals are required for FIPS physical security and must be installed before the appliance is placed in the server rack.

The internal opacity baffles will be installed prior to delivery; it is the responsibility of the CO to ensure that these baffles are in place. Additionally, the CO must place the tamper-evident seals on the module as described in the information provided below. This information can also be found in the *IBM Security QRadar Version 7.1.0 (MR1) FIPS Installation Guide.* After the seals are placed as instructed below, the module can be powered up and the Crypto-Officer may proceed with initialization.

3.1.1.1 Prepare Module for Tamper-Evident Seal Application

To apply the seals, the appliance surfaces must first be cleaned with rubbing alcohol or an alcohol swab in the area where the tamper-evident seals will be placed. Also, the location must be free of dust or debris before installing the seals.

3.1.1.2 Tamper-Evident Seal Application

Place the tamper-evident seals on the appliance as indicated in the steps below. Note that seals for installation steps marked as "**OPTIONAL**" can alternatively be saved and used as spares, if desired.

1. (**OPTIONAL**) Apply two (2) seals on top of the appliance across the horizontal seam as shown in Figure 4.

.

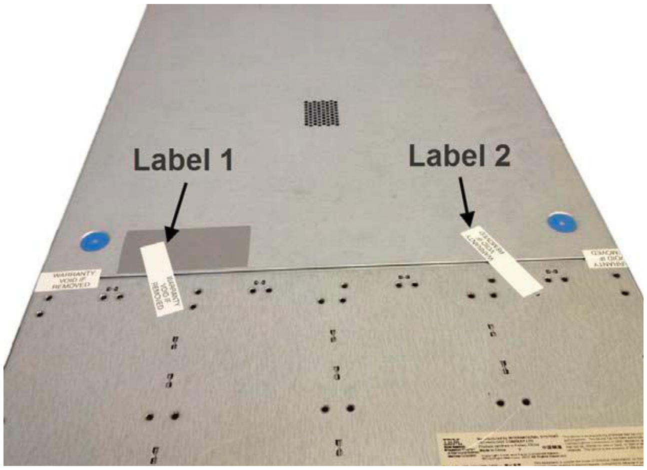

Figure 4 – Tamper-Evident Seal Application Positions (Top)

2. Apply two (2) seals to cover the left and right side panel seam of the appliance as shown in Figure 5. The seals should cover the front and rear panel seam edges and then wrap around to each side of the appliance.

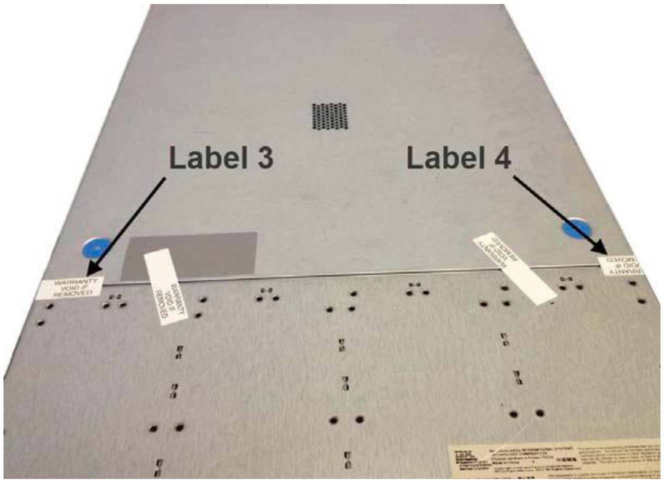

Figure 5 – Tamper-Evident Seal Application Positions (Top/Side)

3. Apply two (2) seals on the side, near the back of the appliance as shown in Figure 6.

.

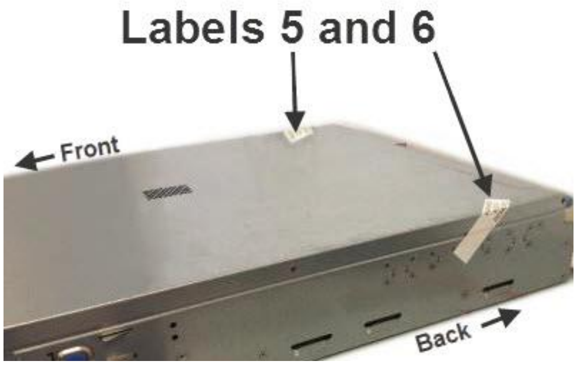

Figure 6 – Tamper-Evident Seal Application Positions (Top/Rear)

4. (**OPTIONAL**) Apply two (2) seals at the rear of the appliance as shown in Figure 7.

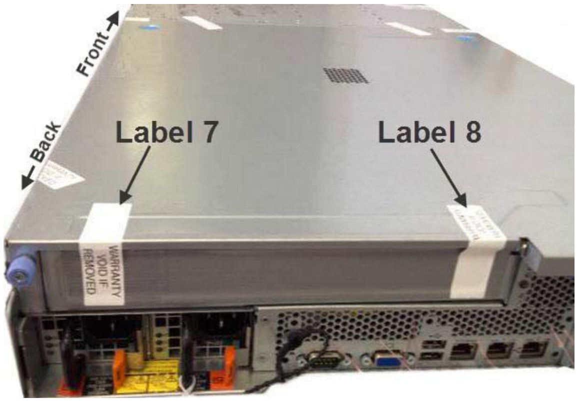

Figure 7 – Tamper-Evident Seal Application Positions (Rear)

5. Apply twelve (12) seals to cover the hard drive bays as shown in Figure 8. Ensure that the seals wrap tightly to the top and bottom of the drive bays.

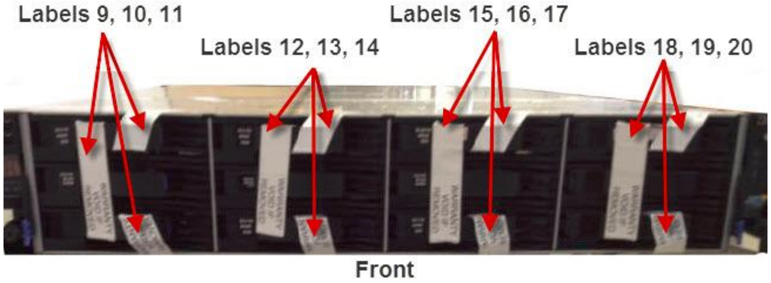

Figure 8 – Tamper-Evident Seal Application Positions (Front)

3.1.2 Initialization

The *IBM Security QRadar Version 7.1.0 (MR1) FIPS Installation Guide* includes instructions on placing the module in FIPS mode. Since the underlying cryptographic libraries always operate in FIPS mode, setting the appliance in FIPS mode creates a jailed shell that only allows access to the QConsole to the crypto and admin accounts.

3.1.3 Management

The Crypto-Officer shall monitor the module's status regularly and is responsible for ensuring that only the services listed in Section 2.4.2 of this document are used. If any irregular activity is noticed or the module is consistently reporting errors, then IBM customer support should be contacted.

3.1.4 Physical Inspection

For the module to operate in its Approved mode, the internal opacity baffles must be in place, and the tamper-evident seals must be placed by the CO role as specified in Section 3.1.1 above. Per FIPS 140-2 Implementation Guidance (IG) 14.4, the CO 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 where the tamper-evident seals are removed or installed to ensure that the security of the module is maintained during such changes and that the module is returned to its Approved state

The CO is also required to periodically inspect the module for evidence of tampering at intervals specified per end-user policy. The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of malice.

To replace a seal, the CO must first remove any remnants of the previous seal. Then, the new seal shall be applied according to the guidance in Section 3.1.1.1 above. To request additional seals, the Crypto-Officer can call the IBM Support Line and order the FRU[22] part number 00AN000.

3.1.5 Zeroization

The Crypto-Officer or FIPS Admin may zeroize all keys, CSPs, and certificates by rebooting the appliance via power-cycle or GUI command. The Crypto-Officer should then follow the steps outlined in the *IBM Security QRadar Version 7.1.0 (MR1) FIPS Installation Guide* to return the module to FIPS-Approved mode.

3.2 User Guidance

Only the module's cryptographic functionalities are available to the User. Users shall only the services that are listed in Table 5. Although the User does not have any ability to modify the configuration of the module, they should report to the Crypto-Officer if any irregular activity is noticed.

3.3 Non-Approved Mode of Operation

When initialized and configured according to the Crypto-Officer guidance in this Security Policy, the module does not support a non-Approved mode of operation.

[22] FRU – Field Replaceable Unit

4 Acronyms

This section describes the acronyms used in this document.

Table 10 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DH	Diffie-Hellman
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
Gb	Gigabit
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol - Secure
ID	Identification
IT	Information Technology
KAT	Known Answer Test
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
MD5	Message Digest 5
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NMI	Non-Maskable Interrupt

.

Acronym	Definition
NVLAP	National Voluntary Laboratory Accreditation Program
OFB	Output Feedback
OS	Operating System
PCIe	Peripheral Component Interconnect Express
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
PSS	Probabilistic Signature Scheme
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
RNG	Random Number Generator
RPM	Red Hat Package Manager
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS	Terminal Access Control Access Control System
TLS	Transport Layer Security
USB	Universal Serial Bus

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United Stated of America

Phone: +1 703-267-6050
Email: info@corsec.com
http://www.corsec.com