iboss, Inc.

FireSphere 7960

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 0.6

Date: 9/20/16

iboss, Inc.
4110 Campus Point Court
San Diego, CA 92121

Table of Contents

List of Tables

List of Figures

Appendix

1 Introduction

This document defines the Security Policy for the iboss FireSphere 7960 module, hereafter denoted the Module. The Module is an IPS (Intrusion Protection System). The Module meets FIPS 140-2 overall Level 1 requirements.

Table 1 – Cryptographic Module Configurations

	Module/HW Version	FW Version	Limited OE
1	FireSphere 7960_FIPS	8.2.0.10	CentOS 6.4 x64 with 2x Intel Xeon E5-2650

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated Intrusion Protection System. The cryptographic module is a rack mountable chassis. The module embodiment is defined as a multi-chip standalone cryptographic module per FIPS 140-2. The cryptographic boundary is defined as the entire chassis, including all hardware, software, and firmware components.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. The module is built using a General Purpose PC and the physical boundary and cryptographic boundary is the entire PC chassis.

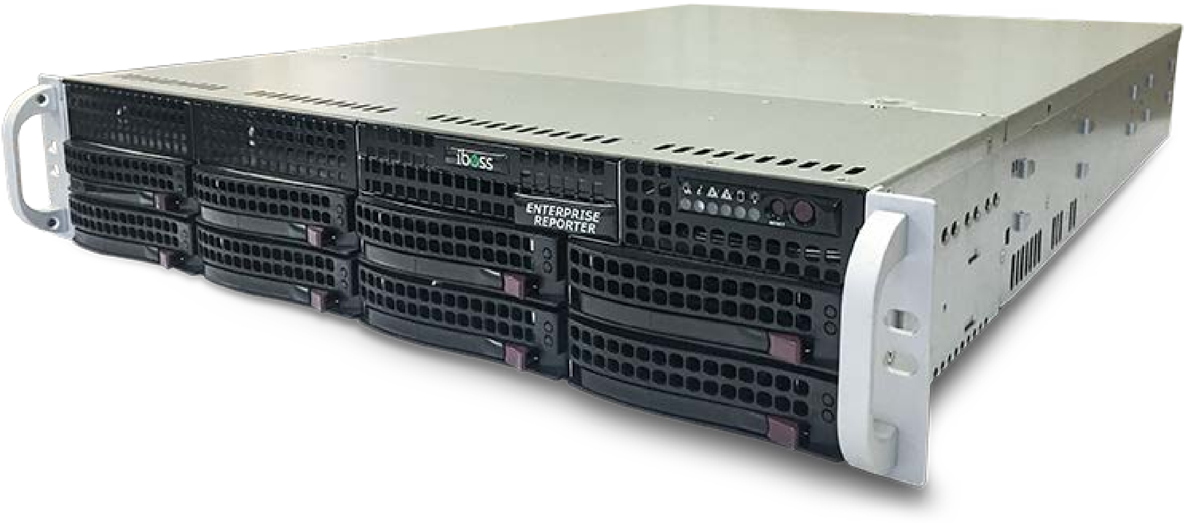


Figure 1 – iboss Firesphere 7960_fips

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Serial Port: RS-232	Provides a limited management console	Control in | Status out
WAN Port: RJ45 - 1G copper	Data monitoring	Control in | Status out | Data in | Data out
LAN Port: RJ45 - 1G copper	Data monitoring	Control in | Status out | Data in | Data out
2x AC 110	Redundant power supplies	Power
Push Buttons	Power button	Control in
LEDs	HDD and Power	Status out
VGA	Used for diagnostic purposes	Status out

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

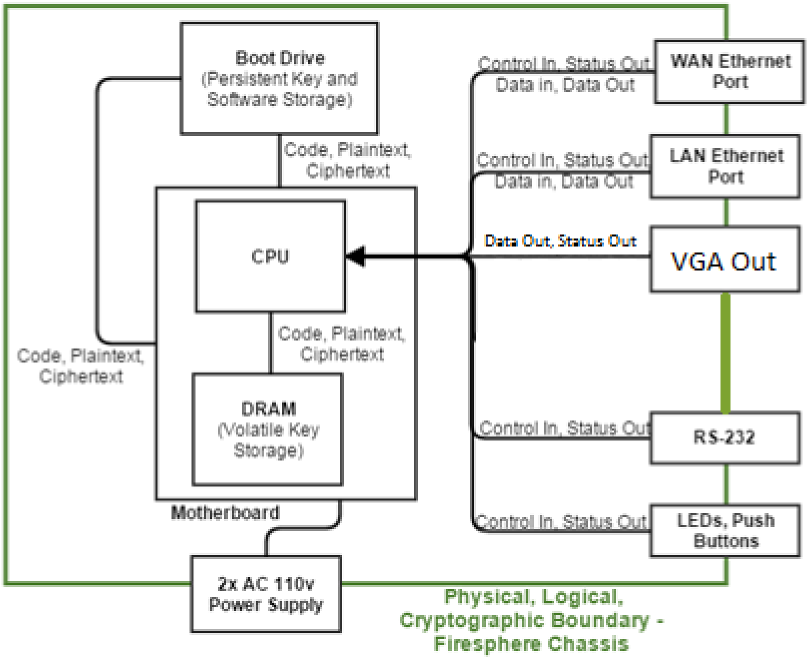


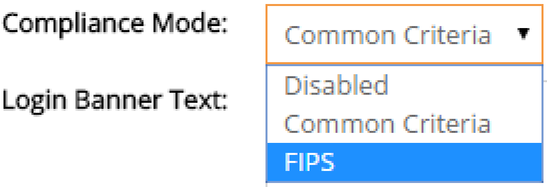
Figure 2 – Module Block Diagram

The module contains a limited operational environment, which is stored and executed on the Boot Drive at power-up.

1.3 Mode of Operation

The module will contain both a FIPS-approved and non-FIPS-approved mode of operation. The non-FIPS-approved mode of operation allows additional services and unencrypted network protocols, but does not allow any additional (unapproved) cryptographic algorithms. Please see the Appendix for a listing of non-Approved functions. To verify that a module is in the Approved mode of operation, the administration interface (HTTPS/TLS) provides an indicator. In addition, the device supports a login banner, which is only enabled in FIPS-approved mode.

The module is shipped in FIPS-approved mode by default. In order to switch modes, the user can navigate to the Settings->Additional Settings panel in the HTTPS GUI and toggle the "Compliance Mode" option. The three supported features are Disabled, Common Criteria, and FIPS and are shown below.


Compliance Mode: Common Criteria ▼

Login Banner Text:

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the table(s) below.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Implementation	Description	Cert #
AES	OpenSSL	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: CBC Key sizes: 128, 256 bits	3902
AES	Java	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: CBC Key sizes: 128, 256 bits	3562
AES Key Wrap	OpenSSL	[SP800-38F Section 3.1] Function: Key Unwrap Modes: AES-128-CBC + HMAC, AES-256-CBC + HMAC	3902
AES Key Wrap	Java	[SP800-38F Section 3.1] Function: Key Unwrap Modes: AES-128-CBC + HMAC, AES-256-CBC + HMAC	3562
DRBG	OpenSSL	[SP 800-90A] Functions: CTR DRBG with AES-256 Security Strengths: 256 bits (CTR DRBG with AES-128 was tested but not used by the module.)	1118

Algorithm	Implementation	Description	Cert #
RSA	OpenSSL	[FIPS 186-2, 186-4, PKCS1.5, X9.31, and PSS)] FIPS 186-2 X9.31 Signature Verification:2048, 3072 bits with SHA-256, SHA-384, and SHA-512 FIPS 186-4 X9.31 Signature Verification:2048, 3072 bits with SHA-256, SHA-384, and SHA-512 FIPS 186-2 PKCS1.5 Signature Verification: 2048, 3072 bits with SHA-256, SHA-384, and SHA-512 FIPS 186-4 PKCS1.5 Signature Verification: 2048, 3072 bits with SHA-256, SHA-384, and SHA-512 FIPS 186-4 PSS Signature Verification: 2048, 3072 bits with SHA-256, SHA-384, and SHA-512 FIPS 186-4 Key Generation X9.31: Appendix B.3.3: Mod 2048, 3072, Table C.3, Random Public Key Exponent FIPS 186-4 Signature Generation X9.31: Mod 2048, 3072, with SHA-256, SHA-384, and SHA-512 FIPS 186-4 Signature Generation PKCS1.5: Mod 2048, 3072, with SHA-256, SHA-384, and SHA-512 FIPS 186-4 Signature Generation PSS: Mod 2048, 3072, with SHA-256, SHA-384, and SHA-512 (RSA-1024 Signature Verification, and Signature Generation/Verification with SHA-224, were tested but not used by the module.)	1987
RSA	Java	[FIPS 186-2, 186-4, PKCS1.5)] FIPS 186-2 PKCS1.5 Signature Verification: 2048, 3072 bits with SHA-256, SHA-384, and SHA-512 FIPS 186-4 PKCS1.5 Signature Verification: 2048, 3072 bits with SHA-256, SHA-384, and SHA-512 (RSA-1024 Signature Verification, and Signature Generation/Verification with SHA-224, were tested but not used by the module.)	1831
SHA	Java	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2931
SHA	OpenSSL	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512 (SHA-224 was tested but not used by the module.)	3215

Algorithm	Implementation	Description	Cert #
HMAC	OpenSSL	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-256 (HMAC with SHA-224, SHA-384, and SHA-512 were tested but not used by the module.)	2532
HMAC	Java	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-256 (HMAC with SHA-224, SHA-384, and SHA-512 were tested but not used by the module.)	2269
TLS KDF (CVL)	OpenSSL	[SP800-135] Function: Key Derivation for TLS Variants: TLSv1.1 and TLSv1.2 SHA sizes: SHA-1 for TLSv1.1; SHA-256 and SHA-384 for TLSv1.2 (Note that TLSv1.0 is not implemented; the KDF is the same for TLSv1.0 and TLSv1.1.)	757
TLS KDF (CVL)	Java	[SP800-135] Function: Key Derivation for TLS Variants: TLSv1.0/1.1 and TLSv1.2 SHA sizes: SHA-1 for TLSv1.0/v1.1; SHA-256 and SHA-384 for TLSv1.2 (Note that TLSv1.0 is not implemented; the KDF is the same for TLSv1.0 and TLSv1.1.)	607

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Non-SP 800-56B Compliant RSA Key Transport (Encapsulation)	[IG D.9] RSA (key encapsulation; key establishment methodology provides 112 (RSA-2048) or 128 (RSA-3072) bits of encryption strength)
MD5 within TLS v1.1	[IG G.13]
NDRNG	[Annex C] Hardware Non-Deterministic RNG; minimum of 256 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG.

Table 6 – Protocols Allowed in FIPS Mode

Protocol	Description
TLS v1.1/v1.2[1]	Cipher Suites: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256

This protocol has not been reviewed or tested by the CAVP and CMVP.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 7 – Critical Security Parameters (CSPs)

CSP	Description / Usage
Authentication Server (LDAP/AD) Pre-Shared Secret	Description: ASCII Pre-shared key of variable length used to authenticate LDAP authentication server. Stored as encrypted by Sensitive Settings Data Encryption Key. Generation: N/A Storage: Persistently on file system Entry: By user through TLS interface Output: N/A Zeroization: Overwritten with zeroes
SSL TLS Private Key	Description: RSA 2048 with SHA-256 certificate and private key for SSL UI functionality. Generation: Generated upon first-boot after factory initialization or reset to factory default. Storage: Persistently on file system Entry: By user through TLS interface Output: N/A Zeroization: Overwritten with zeroes
User Password	Description: Password for the User role Generation: Generated externally Storage: Persistently on file system Entry: By user over TLS interface Output: N/A

[1] All TLS cipher-suites supported are based on RSA-2048 or RSA-3072 with SHA-256, which provides 112 or 128 bits of security strength, respectively.

CSP	Description / Usage
	Zeroization: Overwritten with new password
CO Password	Description: Password for the Crypto Officer role Generation: Generated externally Storage: Persistently on file system Entry: By user over TLS interface Output: N/A Zeroization: Overwritten with new password
TLS_pre_master_secret	Description: When RSA is used for server authentication and key exchange, a 48-byte TLS_pre_master_secret is generated by the client, encrypted under the server's public key, and sent to the server. The server uses its private key to decrypt the TLS_pre_master_secret. Both parties then convert the TLS_pre_master_secret into the TLS_master_secret. Generation: TLS Client: Generated via SP800-90A DRBG upon session initialization TLS Server: N/A Storage: In RAM Entry: TLS Client: N/A TLS Server: Input into the module after being encrypted (non-compliant SP800-56B) with the server's TLS RSA public key Output: TLS Client: Sent to the server as part of TLS KDF, encrypted using non-compliant SP800-56B RSA encryption. TLS Server: N/A Zeroization: Upon device reset
TLS_master_secret	Description: Derived from the TLS_pre_master_secret (and other data) as part of the TLS KDF. This is always 48 bytes in length. Generation: Based on TLS KDF Storage: In RAM Entry: N/A Output: N/A Zeroization: Upon device reset
TLS_key_block[2]	Description: Derived from the TLS_master_secret using the TLS KDF and provides key material for the encryption (AES-128 or AES-256)

[2] All TLS cipher-suites supported are based on RSA-2048 or RSA-3072 with SHA-256, which provides 112 or 128 bits of security strength, respectively.

CSP	Description / Usage
	and message authentication (HMAC-SHA1 or HMAC-SHA256). Generation: Based on TLS KDF Storage: In RAM Entry: N/A Output: N/A Zeroization: Upon device reset
TLS session encryption key	Description: Extracted from the TLS key block to provide TLS session encryption (AES-128-CBC or ASE-256-CBC). Generation: Based on TLS KDF Storage: In RAM Entry: N/A Output: N/A Zeroization: Upon device reset
TLS session authentication key	Description: Extracted from the TLS key block to provide TLS session authentication (HMAC-SHA1 or HMAC-SHA256). Generation: Based on TLS KDF Storage: In RAM Entry: N/A Output: N/A Zeroization: Upon device reset
Sensitive Settings Data Encryption Key	Description: AES-256-CBC key used for encrypting specific settings within a global configuration settings file. It is stored in plaintext on the file system. Generation: Generated upon first-boot after factory initialization or reset to factory default via SP800-90A DRBG. Storage: Persistently on file system Entry: N/A Output: N/A Zeroization: Overwritten with zeroes
Backup-file AES-256 encryption key	Description: AES-256-CBC key used for encrypting configuration backup files. Stored as encrypted by Sensitive Settings Data Encryption Key. Generation: N/A Storage: Persistently on file system Entry: By user through TLS interface as hexadecimal value Output: N/A Zeroization: Overwritten with zeroes

CSP	Description / Usage
DRBG Seed	Description: Seed from NDRNG, used to feed DRBG. Generation: Output from NDRNG Storage: In RAM Entry: N/A Output: N/A Zeroization: Upon device reset
DRBG State	Description: Internal state (V and Key) of the CTR DRBG. Generation: State is updated by various DRBG functions Storage: In RAM Entry: N/A Output: N/A Zeroization: Upon device reset

2.2 Public Keys

Table 8 – Public Keys

Key	Description / Usage
Firmware FW Load Public Key	RSA 2048 with SHA-256 Public Key used for signature verification of firmware updates. Storage: Persistently on file system Entry: Included with firmware update Output: N/A Zeroization: Overwritten with zeroes
SSL TLS Public Key	Description: RSA 2048 with SHA-256 certificate and private key for SSL UI functionality. Generation: Generated upon first-boot after factory initialization or reset to factory default. Storage: Persistently on file system Entry: By user through TLS interface Output: Plaintext in the TLS handshake Zeroization: Overwritten with zeroes
SSL MITM TLS Public Key	Description: RSA 2048 with SHA-256 certificate for SSL MITM functionality. Generation: Generated upon first-boot after factory initialization or reset to factory default. Storage: Persistently on file system Entry: By user through TLS interface Output: Plaintext in the TLS handshake Zeroization: Overwritten with zeroes

Key	Description / Usage
LDAP/AD Public TLS Public Key	Description: RSA 2048 with SHA-256 certificate used to authenticate TLS connections to an LDAP/AD server. Generation: N/A Storage: Persistently on file system Entry: By user through TLS interface Output: N/A Zeroization: Overwritten with zeroes
SMTP Public TLS Public Key	Description: RSA 2048 with SHA-256 certificate used to authenticate TLS connections to a SMTP server. Generation: N/A Storage: Persistently on file system Entry: By user through TLS interface Output: N/A Zeroization: Overwritten with zeroes
Syslog Public TLS Public Key	Description: RSA 2048 with SHA-256 certificate used to authenticate TLS connections to a syslog server. Generation: N/A Storage: Persistently on file system Entry: By user through TLS interface Output: N/A Zeroization: Overwritten with zeroes
Update Server Public TLS Server Certificate	Description: RSA 2048 with SHA-256 certificate used to authenticate TLS connections to the Update server. Generation: N/A Storage: N/A Entry: Presented by remote server during establishment of TLS connections Output: N/A Zeroization: Overwritten with zeroes
CA certificate bundle	Description: Set of RSA 2048 with SHA-256 public certificates used to validate TLS connections to TLS servers. Generation: N/A Storage: Persistently on file system Entry: Provided with TOE installation Output: N/A Zeroization: Overwritten with zeroes

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles using session management with HTTPs. The Module does not support a maintenance role and/or bypass capability. The Module supports concurrent operators. Concurrent operators are managed by the HTTPs server and will support as many operators as system resources allow for. The module only contains a restricted GUI that disallows access to any authentication CSPs.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer (IPS Administrator) – Has read/write access to all IPS related functionality and device management. A Delegated Admin with the “Can Access Settings” permission enabled	Identity-based	Username and password
User	User (IPS Analyst / Delegated Admin) – Admin configured permissions to access, at most, all options except module key management.	Identity-based	Username and password

3.2 Authentication Methods

Username and password

The module allows for passwords that contains alphanumeric characters and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")". The module supports an administrator-configurable minimum password length, which can be set to a minimum of 15 characters. Therefore, the probability that an attacker can guess a password randomly is 1/72^15, which is less than 1/1,000,000. The module only allows three failed authentication attempts per 15 minutes, therefore the probability that an attacker can guess the password in a one minute period is 3/72^15, which is less than 1/100,000. No feedback is given to the user through the CLI interface. On the GUI interface, the password is obscured by the browser using a password field.

Table 10 – Authentication Description

Authentication Method	Probability	Justification
Username and password	1/72^15 for a single attempt, 3/72^15 for repeated attempts.	The character key space is uppercase letters, lowercase letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")". Therefore, the key space allows for a total of 72 different characters. In addition, the module enforces at least a 15 character minimum password length.

3.3 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Table 11 – Authenticated Services

Service	Description	CO	U
Configure and perform inbound and outbound network baselining and anomaly detection.	Analyze data movement across the Ethernet interfaces and compare it to the network baseline.	X	X
Configure and perform malware sandboxing	Allows the administrator to upload and analyze potential malware.	X	X
Configure alerts and reactions for network filtering, baselining, and IPS functionality.	When the device detects abnormal traffic, the administrator can configure one of several reactions: alert via email and/or syslog, block the connection, or send a TCP reset.	X	X
Configure and perform IPS functionality.	Snort-based network filtering and alerts.	X	X
Configure and enable remote authentication servers and settings (LDAP over TLS)	Allows the module to rely on an external authentication server for local administration.	X	
Configure and enable network logging communications (postgres, or UDP)	Allows the module to connect to a FireSphere 14600 via TLS and report network activity information.	X	
Configure and enable logging (syslog over TLS)	Allows the module to connect to a remote Syslog server for auditing purposes.	X	

Service	Description	CO	U
Configure and enable email alerts (SMTP over TLS)	Allows the module to connect to a remote email server for notification purposes.	X	
Configure user and administrator accounts, groups, passwords, and permissions.	Allows the administrator to add, delete, and modify permissions and user accounts on the system.	X	
Backup and restore settings	Allow the user to initiate or configure periodic backup of some persistent settings and CSPs to an AES-256 encrypted file, and restore the settings and CSPs from an AES-256 encrypted file.	X	
Reset to Default Settings - Zeroize	Destroys all CSPs, accessible only through CLI.	X	
Manage device subscription data	Allows the administrator to configure FireSphere licensing configuration.	X	
Fetch update	Initiate the update process, which will download and install an update from the iboss servers. This will force a device reboot.	X	
Toggle FIPS-approved mode	Switches from FIPS-approved to non-FIPS-approved mode, forces a reset to factory default settings.	X	
Display threat dashboard	Analyze and generate reports based on collected network data through the TLS administrative interface. Includes realtime log displays, global threat displays, network health (bandwidth), QoS reports and settings, data exfiltration events, threat controls,	X	X
Report generation	Display and export reports based on historical network analysis data. Allows scheduled report generation.	X	X
Display, filter, and sort log events	Includes local audit events, URL events, data exfiltration, blocked from callbacks, malware, APT events, and IPS events.	X	X
Configure outgoing SMTP over TLS	Allow the device to send email alerts, and configure optional outgoing authentication to SMTP server using username and password.	X	
Configure additional administrative settings, including network settings, time	Modify non security relevant administrative features such as time.	X	
Manage log data	Allows the administrator to modify the local IPS log data configuration.	X	

Service	Description	CO	U
Configure TLS certificates and keys	Allows the administrator to modify the TLS UI private keys and certificates.	X	
Poweroff, reboot	Shutdown or reboot the system.	X	
Import backup encryption key	Allow the user to provide an AES-256 CBC key for backup and restore purposes.	X	

Table 12 – Unauthenticated Services

Service	Description
Module Reset (Self-test)	Reset the Module by unplugging the module, or pressing the front reset button.
Initiate GUI - HTTPS/TLS	Initialize a TLS session with the module, presenting the user with a login page.
Show Status	LEDs display power on and HDD status, display a login banner on the TLS login page, and UDP bandwidth tracking.

Each service is documented thoroughly in user guidance.

Table 13 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 13 – CSP Access Rights within Services

Service	CSPs								
	Auth PSS	SSL TLS UI Private Key	SSL TLS PMS	SSL TLS MS	SSL TLS KB and Session Keys	Settings Encryption Key	Backup Encryption Key	User and CO Passwords	DRBG Seed and State
Configure and perform inbound and outbound network baselining and anomaly detection.									
Display threat dashboard									
Report generation									
Display, filter, and sort log events									
Configure and perform malware sandboxing									
Configure alerts and reactions for network filtering, baselining, and IPS functionality.									
Configure outgoing SMTP over TLS		R	RW	RW	RW				
Configure and enable network logging communications (postgres, or UDP)									
Configure and enable remote authentication servers and settings (LDAP over TLS)	W		RW	RW	RW				
Configure additional administrative settings, including network settings, time									
Configure and enable logging (syslog over TLS)			RW	RW	RW				
Manage device subscription data									
Manage log data									
Reset to Default Settings - Zeroize	Z	GZ	Z	Z	Z	Z	Z	Z	Z
Toggle FIPS-approved mode	Z	GZ	Z	Z	Z	Z	Z	Z	Z
Configure user and administrator accounts, groups, passwords, and permissions.	W							W	
Configure TLS certificates and keys		WZ							
Poweroff, reboot			Z	Z	Z				ZG
Fetch update			Z	Z	Z				ZG
Backup and restore settings	RW	RW				RW	RW		

Import backup encryption key							WZ		
Module Reset (Self-test)				Z	Z	Z			ZG
Initiate GUI - HTTPS/TLS			R	RW	RW	RW			
Show Status									
Configure and perform IPS functionality.									
Configure and enable email alerts (SMTP over TLS)									

4 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 14 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the FIPS error state.

If self-tests are completed successfully, the module reports "FIPS KAT self-tests complete" of the HTTPS GUI.

Table 14 – Power Up Self-tests

Test Target	Description
Firmware Integrity	CRC32 of all binary and executable files on the system
AES (Java)	KATs: Encryption, Decryption Modes: CBC Key sizes: 128 bits, 256 bits
AES (OpenSSL)	KATs: Encryption, Decryption Modes: CBC Key sizes: 128 bits, 256 bits
DRBG (OpenSSL)	KATs: CTR DRBG Security Strengths: 256 bits
RSA (OpenSSL)	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits, 3072 bits
RSA (Java)	KATs: Signature Verification Key sizes: 2048 bits, 3072 bits
SHA (Java)	KATs: SHA-1, SHA-256, SHA-384, SHA-512
SHA (OpenSSL)	KATs: SHA-1, SHA-256, SHA-384, SHA-512
HMAC-SHA (Java)	KATs: HMAC with SHA-1, SHA-256, SHA-384, SHA-512
HMAC-SHA (OpenSSL)	KATs: HMAC with SHA-1, SHA-256, SHA-384, SHA-512

Table 15 – Conditional Self-tests

Test Target	Description
NDRNG (OpenSSL)	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
DRBG (OpenSSL)	DRBG Continuous Test performed when a random value is requested from the DRBG.
RSA (OpenSSL)	RSA Pairwise Consistency Test performed on every RSA key pair generation.
DRBG Health Checks (OpenSSL)	Performed conditionally per SP 800-90A r1 Section 11.3. Required per IG C.1.

Test Target	Description
Firmware Load	RSA 2048 signature verification performed when firmware is loaded.

5 Physical Security Policy

The module is compliant with FIPS 140-2 Level 1 Physical Security requirements: The module uses commercial grade components and standard passivation.

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The module does not support mitigation of other attacks.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The module provides identity-based authentication.
3. The module clears previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. The operator is capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does support concurrent operators.
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.
13. The module does not have any external input/output devices used for entry/output of data.
14. The module does not enter or output plaintext CSPs.
15. The module does not output intermediate key values.

16. If the module remains inactive in any valid role for an administrator-configurable maximum period of minutes, the module automatically logs out the operator.
17. The module enforces a timed access protection mechanism that supports at most three (3) authentication attempts per 15 minutes. After three (3) consecutive unsuccessful Password validation attempts have occurred, the module shall enforce a wait period of at least 15 minutes before any more login attempts can be attempted. This wait period is not enforced if the module power is momentarily removed. The wait period is enforced across concurrent connections.
18. The module does not allow an authenticated user to change roles without re-authentication.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 16 – References

Abbreviation	Full Specification Name
[FIPS140-2]	Security Requirements for Cryptographic Modules, May 25, 2001
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011
[FIPS 197, SP 800-38A]	Federal Information Processing Standards Publication 197 November 26, 2001 Announcing the ADVANCED ENCRYPTION STANDARD (AES)
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[FIPS 186-4]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS)
[FIPS 180-4]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Secure Hash Standard (SHS)
[FIPS 198-1]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION The Keyed-Hash Message Authentication Code (HMAC)

Table 17 – Acronyms and Definitions

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
CAVP	Cryptographic Algorithm Validation Program (CAVP)
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
CTR	Counter
DRBG	Deterministic Random Bit Generator
GUI	Graphical User Interface
HMAC-SHA	Hashed Message Authentication Code - Secure Hash Algorithm
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MITM	Man In The Middle

Acronym	Definition
RS-232	Recommended Standard 232 (computer serial interface, IEEE)
RSA	Rivest, Shamir, & Adleman (public key encryption technology)
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAN	Wide Area Network

Appendix: Non-Approved Services

The module implements the following functions in the non-Approved mode:

Report Manager

- Settings – General Settings – SNMP Monitoring
- Settings – OAuth2 Integration
- Settings – SDN Controller Integration
- Settings – iboss MobileEther MDM Integration
- Settings – Remote Management

Secure Web Gateway

- Remote Management
- LDAP Authentication
- TLS Protected communication between Secure Web Gateway and Report Manager

Plaintext Communications for:

- Settings – LDAP Settings
- Settings – Syslog Logging
- Settings – Email Server Settings

Display of Private Data for:

- SMB – Backup of reports and logs
- Settings – Certificates