Non-Proprietary Security Policy for the FIPS 140-2 Level 2 Validated Fortress Secure Wireless Access Bridge (SWAB) ES520

Hardware Models: ES520V1 and ES520V2

Firmware Version: 2.6.11

(Document Version: 1.04.1)

February 2008

Revised: June 2008

Revised: July 2008

Revised: September 2008

Revised: October 2008

This Security Policy for Fortress Technologies, Inc., of the FIPS 140-2 validated Fortress Secure Wireless Access Bridge (SWAB) ES520, defines general rules, regulations, and practices under which the module was designed and developed and for its correct operation. These rules and regulations have been and must be followed in all phases of security projects, including the design, development, manufacture service, delivery and distribution, and operation of products.

Contents

List of Figures and Tables

1.0 Introduction

1.1 The Purpose of this Document

From this point on, the Security Policy will refer to the Secure Wireless Access Bridge (SWAB) ES520 module as, "SWAB" or "the module".

This Security Policy defines all security rules under which the SWAB must operate and which it must enforce. The SWAB must comply with all FIPS 140-2 level 2 requirements.

1.2 Products

The SWAB products that this Security Policy is relevant are identified as:

Hardware Module Numbers: ES520V1 and ES520V2

Firmware Version: 2.6.11

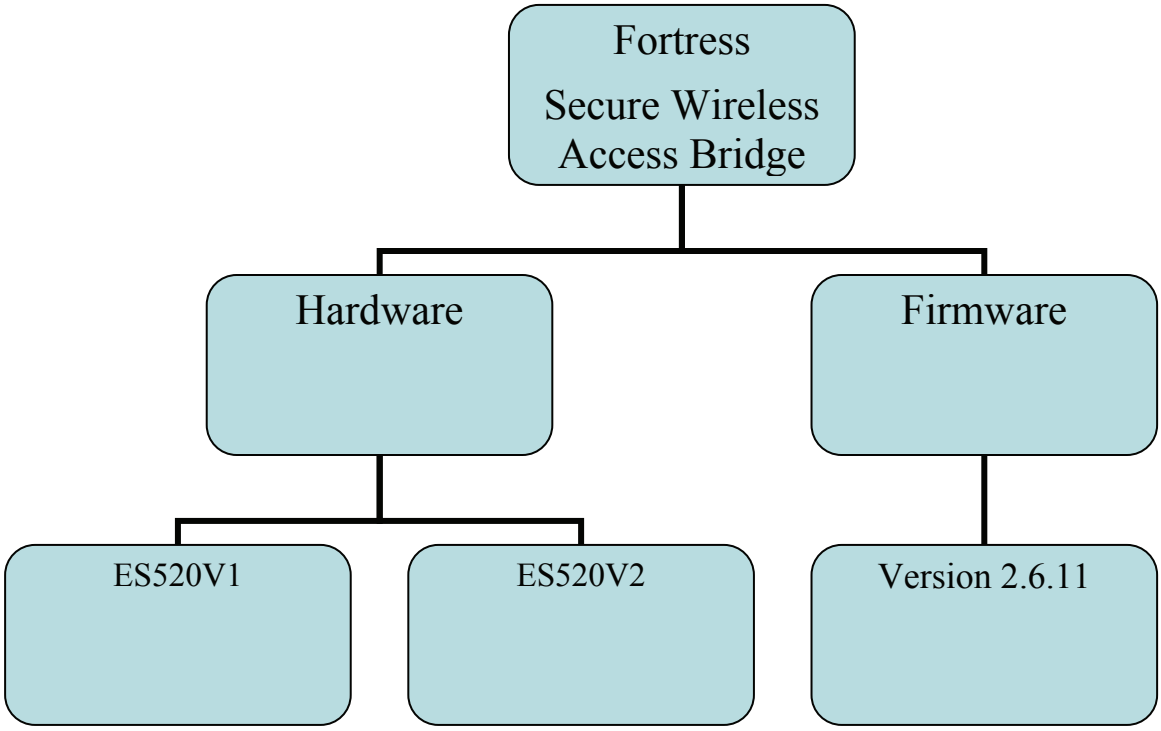

Figure 1: The Fortress Secure Access Bridge Top Level Configuration

1.3 Functional Description

The SWAB is an all-in-one network access family with the most stringent security available today built in. The SWAB top level configurable hierarchy is shown in Figure 1. They serve as wireless bridges, WLAN access points, have an eight-port LAN switch, and perform the functions necessary to secure a wireless connection.

The SWAB uses the **Mobile Security Protocol** (MSP) to secure data. **MSP** uses the Diffie-Hellman (DH) for peer-to-peer key generation and agreement and uses AES-CBC for strong encryption. Once it's installed and configured, operation is automatic, requiring no or little administrator intervention as it protects data transmitted on WLANs and between WLAN devices and the wired LAN.

A sample application for the SWAB is shown in Figure 2. The rugged, compact chassis of the SWAB are uniquely designed, acting as an external heat sink to eliminate the need for fans and filters. The SWAB can be used indoors or outdoors with the Mast-Mounting and Weatherizing kits shipped with every device. The SWAB can be quickly and transparently integrated into an existing network. It can be powered with standard AC current or as an Ethernet powered device (PD) through its WAN port, which supports power over Ethernet (PoE).

Features of the SWAB include:

- Command Line Management
- Graphic User Interface Management
- Tamper Resistance Hardware
- Automatic Configuration

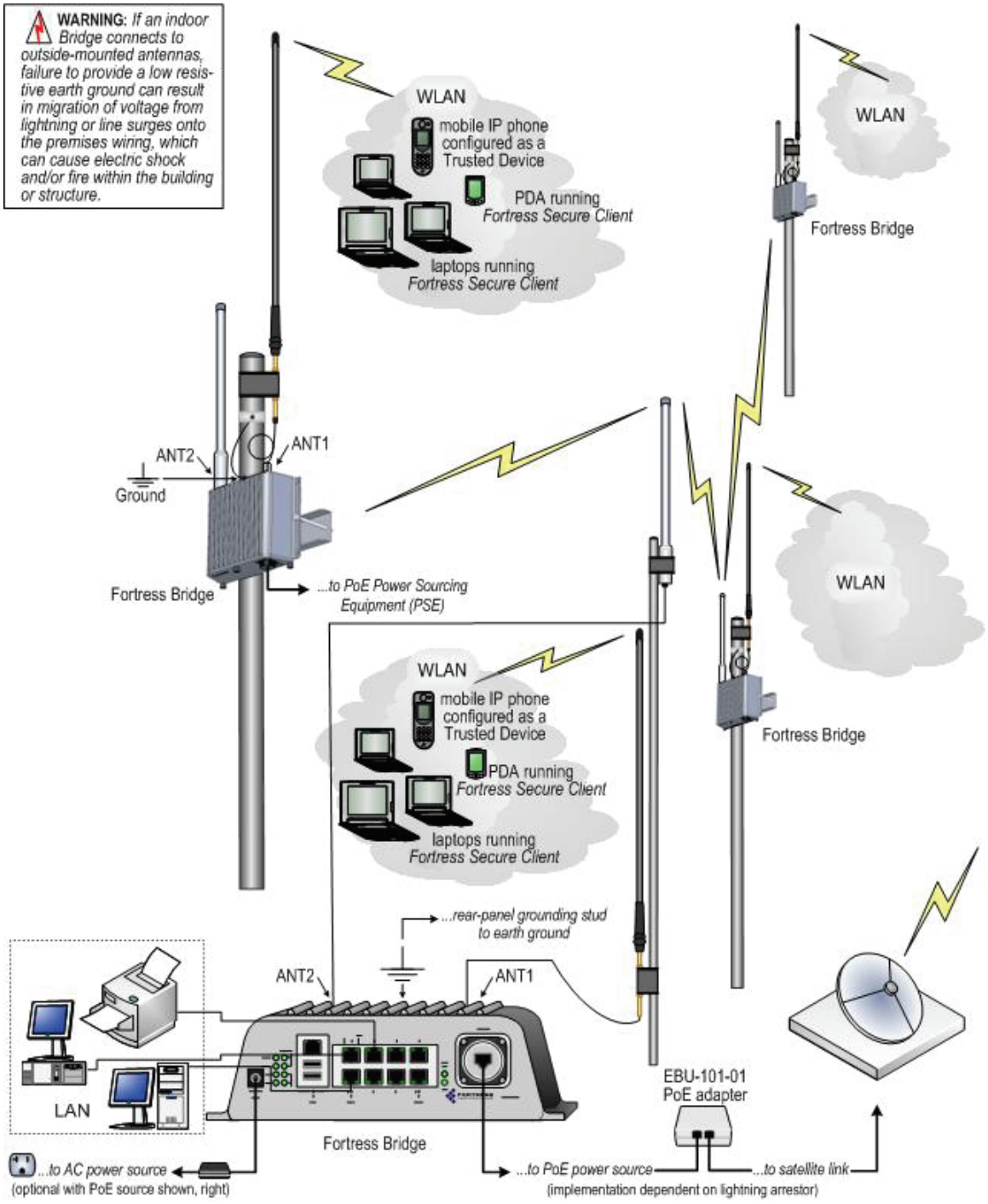

Figure 2: Example Configuration of the SWAB

2.0 Identification and Authentication Policy

2.1 Roles

The SWAB supports two roles: a Crypto Officer role and an End User role. There are three variants of the Crypto Officer role, as specified in the table below. The End User can only use cryptographic services. Table 1 shows more detail on the roles.

Role	Definition
Administrator	Can access the SWAB by using the web graphical user interface. This user can configure, monitor and use the diagnostic services of the SWAB.
Operator	Can access the SWAB by using the web graphical user interface. This user can monitor and use the diagnostic services of the SWAB.
System Administrator	Can access the SWAB by using the command line interface either by a direct connect serial cable or by using a Secure Shell (SSH) connections. This user can configure, monitor and use the diagnostic services of the SWAB and set or perform certain critical functions.
End User	An end user can use cryptographic services of the SWAB.

Table 1: Roles

2.2 Authentication Data

All roles for the SWAB must be authenticated. Authentication for the Crypto Officer is by means of a password. Authentication for an End User is by means of the Access ID. Table 2 shows the types and data needed for the passwords and Access ID. Table 3 calculates the strength of the mechanism for each authentication method. Authentication data is stored as plaintext in the configuration database.

Role	Type of Authentication	Authentication Data
Administrator	Administrator Password	The Crypto Officer roles by the System Administrator, Administrator or Operator require a password for authentication. The SWAB requires that the password must be a minimum of 15 characters long, which are selectable and each of the characters is allowed to be any of the symbols a-z, A-Z, 0-9, or any of the 30 punctuation characters found on a typical English language keyboard (!@#$%^&*()_+{}|:"<>?-=[]\;',./), then the number of possible combinations becomes 1/(26+26+10+30)^15 = 1(92^15). This meets the 1/ 1,000,000 requirement..
Operator	Operator Password	Same as Administrator
System Administrator	System Administrator Password	Same as Administrator
End User	Access ID	16 Bytes

Table 2: Role and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Administrator-Password	A operator can make 8 (2^3) attempts at authentication in a given one-minute interval. This leaves a probability of: (1/92^8)/8 = 1/641,523,591,421,952 for a false acceptance in a one minute interval; which is much less than the 1 in 10^5 requirement.
Operator - Password	A operator can make 8 (2^3) attempts at authentication in a given one-minute interval. This leaves a probability of: (1/92^8)/8 = 1/641,523,591,421,952 for a false acceptance in a one minute interval; which is much less than the 1 in 10^5 requirement.
System Administrator - Password	A operator can make 8 (2^3) attempts at authentication in a given one-minute interval. This leaves a probability of: (1/92^8)/8 = 1/641,523,591,421,952 for a false acceptance in a one minute interval; which is much less than the 1 in 10^5 requirement.
End User - Access ID	Access ID is 32 hex characters. The worst case probability of guessing the AccessID is 1 in 16^32.

Table 3: Strengths of Authentication Mechanisms

3.0 Access Control Policy

3.1 Services Provided

An End User can establish a secure connection from itself over a wireless network to the SWAB encrypted interface and then have the ability to bridge through the SWAB. This will work only if the End User has the appropriate Access ID.

The main service of the SWAB is to encrypt/decrypt the connection over the wireless network. The other services include configuring, monitoring, and diagnosing the SWAB itself. Table 4 details the SWABs services.

Service	Description
Encryption/Decryption	The End User can use the cryptographic services of the SWAB.
Show Status	A Crypto Officer who is allowed access to the GUI or CLI can observe status parameters of the SWAB.
Configuration Write (Including Bypass Configuration)	A Crypto Officer (System Administrator or Administrator) who is allowed access to the GUI or CLI can change configuration parameters in the SWAB. This includes configuring the module bypass capabilities..
Configuration Read	A Crypto Officer who is allowed access to the GUI or CLI can read configuration parameters in the SWAB.
Set FIPS Mode	A Crypto Officer (System Administrator) who is allowed access to the CLI can set FIPS Mode
Diagnostic Services	A Crypto Officer who is allowed access to the GUI or CLI can use SWAB network diagnostic services.
Zeroization	A Crypto Officer (System Administrator) who is allowed access to the CLI can zeroize module (reset to defaults command).

Table 4: SWAB Services

3.2 Services each Role is Authorized to Perform

Each role is only authorized to perform certain services. Table 5 shows what services each role can perform.

Role/Authorized Service	Encryption/ Decryption	Show Status	Configuration Read	Configuration Write	Diagnostic Services	Key Zeroization	Set FIPS
Administrator		X	X	X	X		
Operator		X	X		X		
System Administrator		X	X	X	X	X	X
End User	X						

Table 5: Services each Role is authorized to perform

3.3 Cryptographic keys and CSP

All the cryptographic keys and critical security parameters used in the SWAB are detailed in Table 6. The SWAB uses a dual Diffie Hellman key procedure. This approach protects someone from doing a “man-in-the-middle” attack on a secure connection.

The SWAB mandates the use of passwords for administration and it uses an approved pseudo random number generated for its supple of random numbers.

Type	Name	Use for
Key	Module Secret Key	AES
	Static Private Key	Diffie Hellman
	Static Public Key	Diffie Hellman
	Static Secret Encryption Key	AES
	Dynamic Private Key	Diffie Hellman
	Dynamic Public Key	Diffie Hellman
	Dynamic Session Key	AES
	Static Group Key	AES
	Public Dynamic Group Key	Diffie Hellman
	Private Dynamic Group Key	Diffie Hellman
	Dynamic Group Key	AES
	RNG Key	ANSI X9.31 RNG
	Configuration DB Key (Not a CSP)	AES
Seed	RNG Seed	ANSI X9.31 RNG
End User - Authentication Data	Access ID 16 or 32 Hexadecimal Digits	Authentication
Passwords	Operator Password	Authentication
	Administrator Password	Authentication
	System Administrator Password	Authentication

Table 6: Cryptographic keys and CSPs

Zeroization: Zeroization is accomplished by executing a reset to defaults command from the command line interface by the System Administrator. All keys and CSPs that are used for the security of data packets are stored in RAM that is zeroed during a Command Line Interface (CLI) command "**reset**”. This sets the ACCESSID and all passwords stored in the configuration data base to the factory defaults.

3.4 Roles, Services and Access to CSPs

The End User can only use cryptographic services of the SWAB. The End User has no access to the SWAB itself. The SWAB does not allow access to any of its cryptographic keys. The Crypto Officer can access some critical security parameters as shown in Table 7.

Role	Service/CSP	Access ID	Administrator Password	System Administrator Password	Operator Password
Administrator	Configuration Write	X	X	X	X
System Administrator	Configuration Write	X	X	X	X
Operator	No Access				
End User	No Access				

Table 7: Roles, Services, and Access to Keys or CSPs

3.5 Self-Tests

The SWAB conducts the following self-tests at power-up and conditionally as needed, when a module performs a particular function or operation:

A. Power-Up Tests

- Cryptographic Algorithm Test: AES KAT, HMAC KAT, SHS KAT, and RNG KAT
- Firmware Integrity Test: HMAC
- Critical Functions Tests: MAC Address Test, Bypass Test

B. Conditional Test

- Continuous Random Number Generator Test (Approved and non-Approved RNGs)
- Bypass Test

Failure of any self-test listed above puts the module in its error state.

3.6 Cryptographic Algorithms

The SWAB applies the following cryptographic algorithms:

FIPS Algorithms	NIST-FIPS Certificate Number
AES (CBC, encrypt/decrypt; 128, 192, 256)	#686 and #694
SHS (SHA-1 (Byte), SHA-256 (Byte))	#714 and #721
HMAC	#365 and #371
ANSI X9.31 RNG	#400 and #406
Non-FIPS Algorithms	
Diffie-Hellman (key agreement; key establishment methodology provides either 80 bits of encryption strength using D-H key size of 1024 bits or 112 bits of encryption strength using D-H key size of 2048 bits), MD5, RSA (non-compliant), Hardware RNG	N/A

Table 8: Cryptographic Algorithms Applied by SWAB

3.7 Protocol Support

The SWAB F/W v2.6.11 supports the Diffie-Hellman key exchange protocol. F/W v2.6.11 only allows 1024 or 2048 bit D-H key sizes in FIPS mode. In addition these are the only D-H key sizes allowed by the F/W in any mode. The key derivation function follows SP800-56A guidance.

4.0 Physical Security Policy

The SWAB Firmware is installed by Fortress Technologies on a production-quality, FCC certified hardware device, the SWAB, which also define the module's physical boundary. Both hardware platforms are manufactured to meet FIPS 140-2, L2 requirements. Table 9 details the recommended physical security activities that should be carried out the Crypto Officer.

The host hardware platform server must be located in a controlled access area. Tamper evidence is provided by the use of an epoxy potting material covering the chassis access screws. The Crypto Officer is responsible for applying the coating with the vendor provided epoxy adhesive. A pair of screws on the front and back panel must be covered with the material, as well as two screws, diagonally opposed, on the WAN cover plate on the front. Figures 3, 4, 5, and 6 show the front and back of each of the module hardware model (ES520V1 and ES520V2).

4.1 Tamper Evidence Application

Locate the container of Loctite 425 adhesive provided by the vendor. Prop the module in a front panel upright position. Lightly moisten each of the screws in the upper right and left corner of the module, and then apply two drops of adhesive each of the two screw heads. In addition repeat the process for two screws, diagonally opposed, on the WAN cover plate on the front. Insure that the adhesive flows over and completely covers the screw head. Allow the adhesive to cure for 5 minutes. Turn the module over and repeat the process for the upper right and left screw on the rear panel.

Table 9 lists recommended physical security related activities at the user's site.

Physical Security Object	Recommended Inspection frequency	Inspection Guidance
Appropriate chassis screws covered with epoxy coating.	Daily	Inspect screw heads for chipped epoxy material. If found, remove module from service.
Overall physical condition of the module	Daily	Inspect all cable connections and the module's overall condition. If any discrepancy found, correct and test the system for correct operation or remove module from service.

Table 9: Recommended Physical Security Activities

Figure 3: Front View of the SWAB Hardware (ES520V1) Showing the Blue Thread Locker

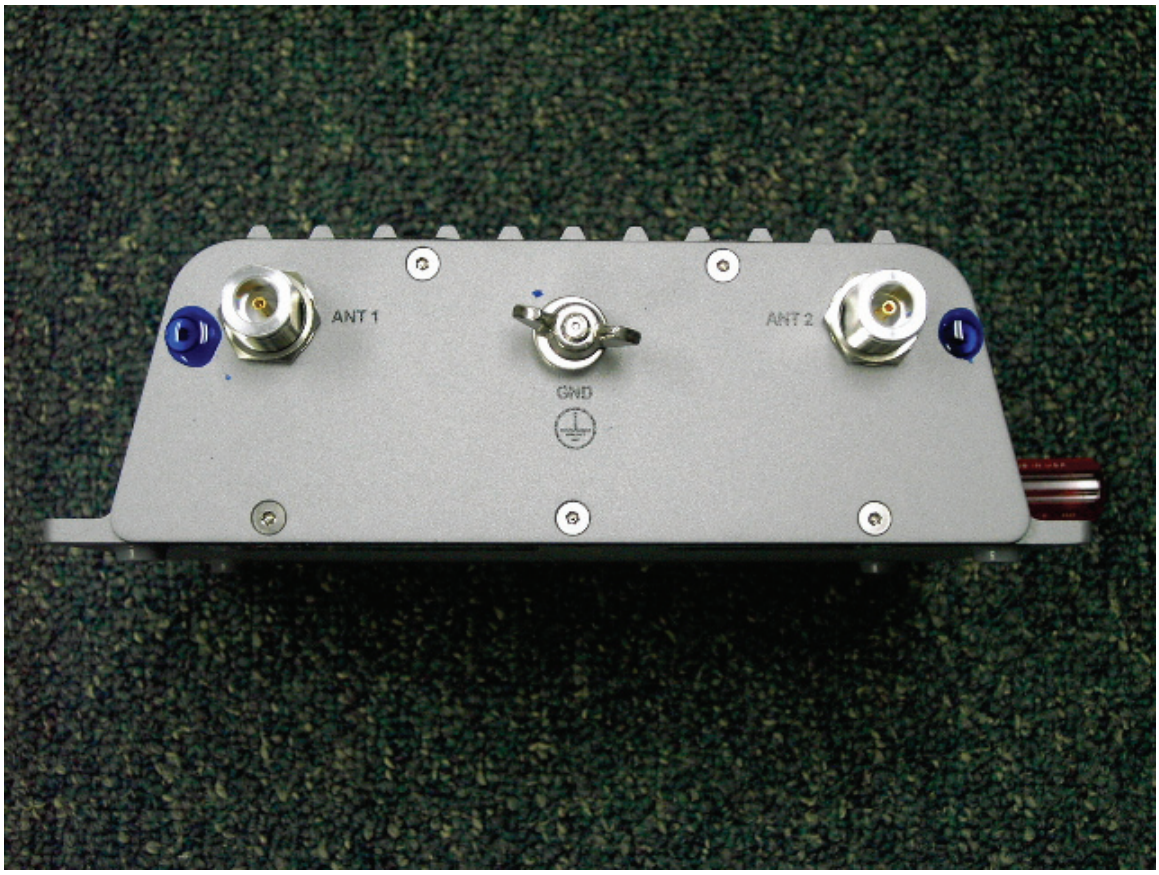

Figure 4: Rear View of the SWAB Hardware (ES520V1) Showing the Blue Thread Locker

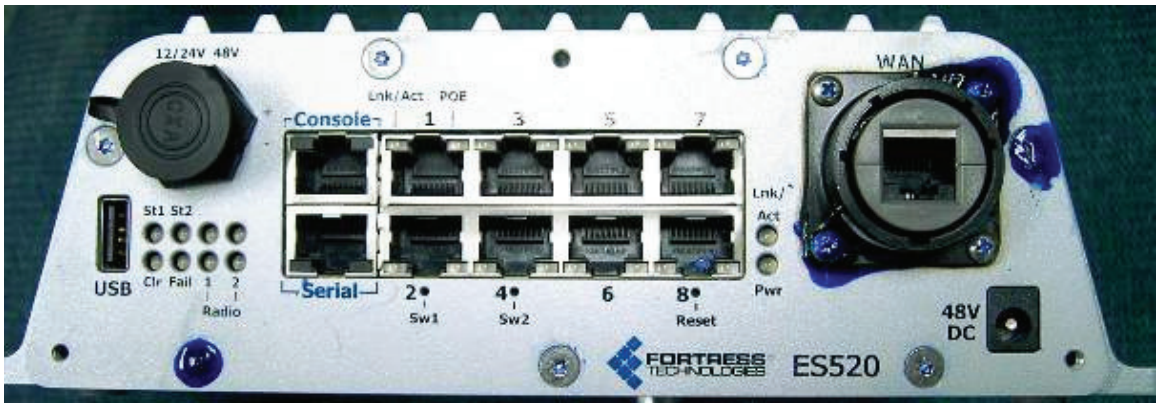

Figure 5: Front View of the SWAB Hardware (ES520V2) Showing the Blue Thread Locker

Figure 6: Rear View of the SWAB Hardware (ES520V2) Showing the Blue Thread Locker

5.0 Firmware Security

Firmware upgrade is not permitted in FIPS mode. Executing a non-validated firmware version invalidates the module's FIPS Approved status. Contact Fortress Technologies for information on firmware upgrades. Self-tests validate the operational status of each product, including critical functions and files. If the firmware is compromised, the module enters an error state in which no cryptographic processing occurs, preventing a security breach through a malfunctioning device.

6.0 Operating System Security

The SWAB operates automatically after power-up. The SWAB operates on Fortress Technologies proprietary version of hardened Linux that is installed along with the module's software, with user access to standard OS functions eliminated. The module provides no means whereby an operator could load and execute software or firmware that was not included as part of the module's validation.

7.0 Security Policy for Mitigation of Other Attacks

No special mechanisms are built in the SWAB; however, the cryptographic module is designed to mitigate several specific attacks above the FIPS defined functions. Additional features that mitigate attacks are listed here:

1. The dynamic session key is changed at least once every 24 hours, with 4 hours being the factory default duration: *Mitigates key discovery.*
2. A second Diffie-Hellman key exchange produces a dynamic common secret key in each of the modules by combining the other module's dynamic public key with the module's own dynamic private key: *Mitigates "man-in-the-middle" attacks*.
3. All key exchanges are encrypted: *Mitigates encryption key sniffing by hackers.*
4. Compression and encryption of header information inside of the frame, making it impossible to guess. Use of strong encryption further protects the information. Any bit flipping would be useless in this frame to try to change the IP address of the frame: *Mitigates active attacks from both ends*.
5. Encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*

6. Multi-factor Authentication: The Fortress Secure Wireless Access Bridge guards the network against illicit access with "multi-factor authentication", checking three levels of access credentials before allowing a connection. These are:
    a) *Network authentication* requires a connecting device to use the correct shared identifier for the network
    b) *Device authentication* requires a connecting device to be individually recognized on the network, through its unique device identifier.
    c) *User authentication* requires the user of a connecting device to enter a recognized user name and password.

8.0 EMI/EMC

The SWAB are FCC compliant and certified (Part 15, Subpart B, Class A) devices.

9.0 Customer Security Policy Issues

Fortress Technologies, Inc. expects that after the module's installation, any potential *customer* (government organization or commercial entity or division) *employs its own internal security policy* covering all the rules under which the module(s) and the customer's network(s) must operate. In addition, the customer systems are expected to be upgraded as needed to contain appropriate security tools to enforce the internal security policy.

9.1 FIPS Mode

The SWAB must be configured in FIPS mode during module initialization. FIPS can be enabled or disabled only by System Administrator using the CLI. To set FIPS mode use the **set fips on** command. AES encryption must be used in FIPS mode. Firmware uploads are not permitted in FIPS mode.

All operators are able to determine FIPS mode via:

1. System Administrator: Using the "show fips" command.
2. Administrator: Observing the FIPS Enabled GUI banner
3. Operator: Observing the FIPS Enabled GUI banner.

9.2 Alternating BYPASS Mode

The SWAB may be configured to allow the passing of cleartext traffic in either **Normal** (non-FIPS) or **FIPS** mode. If Cleartext Traffic is **Enabled** (default**)** the Bridge's front-panel **Cleartext** LED flashes a signal whenever the Bridge passes unencrypted traffic. The Cleartext setting status (on/off) may be determined from the GUI under the "Security Settings" menu by either the Operator or Administrator. Cleartext may be disabled by a System Administrator using the **set cleartext off** CLI command or an Administrator by setting Security Settings Cleartext to **Off,** then executing **Apply** on the Security Settings GUI.

10.0 Maintenance Issues

The SWAB has no operator maintainable components. Unserviceable modules must be returned to the factory for repair.