Non-Proprietary Security Policy
for the FIPS 140-2 Level 2 Validated
Fortress Secure Bridge

Firmware Version 5.1

(Document Version 1.14.4)

March 31, 2009

This security policy of Fortress Technologies, Inc., for the FIPS 140-2 validated Fortress Secure Bridge (FSB), defines general rules, regulations, and practices under which the FSB 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

This security policy defines all FIPS 140-2 level 2 security rules under which the Fortress Secure Bridge (FSB) complies with and enforces. The FSB is a multi-chip standalone module.

1.2 Products

The current FSB products this Security Policy is relevant to are identified as:

Hardware FSB Numbers: ES520V1 and ES520V2

Firmware Version: 5.1

The FSB top level configurable hierarchy is shown in Figure 1.

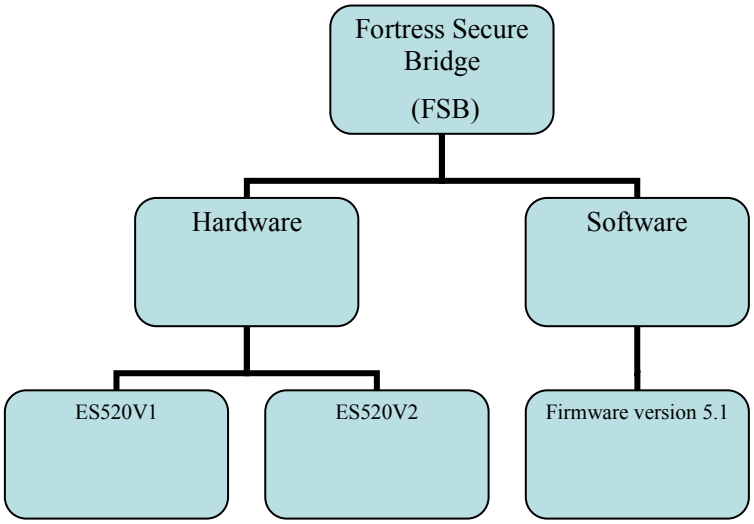

Figure 1: The Fortress Secure Bridge Top Level Configuration

1.3 Glossary of Terms

- **AES (Advanced Encryption Standard):** also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government.
- **ANSI (American National Standards Institute):** a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States
- **CBC (cipher-block chaining):** A mode of operation where each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks processed up to that point. Also, to make each message unique, an initialization vector must be used in the first block.
- **Crypto Officer (Crypto Officer):** an operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions.

- **CTR (Counter):** generates the next keystream block by encrypting successive values of a "counter". The counter can be any simple function which produces a sequence which is guaranteed not to repeat for a long time. It allows a random access property during decryption. The IV/nonce and the counter can be concatenated, added, or XORed together to produce the actual unique counter block for encryption.
- **Diffie-Hellman:** is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
- **ECB (Electronic codebook**): This is the simplest of the encryption modes. The message is divided into blocks and each block is encrypted separately. The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks; thus, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all.
- **EAP (Extensible Authentication Protocol**): is a universal authentication framework frequently used in wireless networks and Point-to-Point connections.
- **EAP-TLS:** is an IETF open standard that is the original standard wireless LAN EAP authentication protocol, and is well-supported among wireless vendors.
- **Hard Key:** A key that is generated using information that is static.
- **HMAC (Hash Message Authentication Code**): a keyed Hash Message Authentication Code is a type of message authentication code (MAC) calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key.
- **HTTPS:** Hypertext Transfer Protocol over Secure Socket Layer
- **IEEE 802.11:** is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands.
- **IEEE 802.11i:** Is an amendment to the IEEE 802.11 standard specifying security mechanisms for wireless networks.
- **IV (initialization vector):** is a block of bits that is required to allow a stream cipher or a block cipher to be executed in any of several streaming modes of operation to produce a unique stream independent from other streams produced by the same encryption key, without having to go through a (usually lengthy) re-keying process.
- **MAC (Message Authentication Code):** a short piece of information used to authenticate a message.
- **MIC (Message Integrity code):** is a short piece of information used to check the integrity of a message. This is the same as a MAC. Normally in communications this would be called a MAC (Message Authentication Code) however since the term MAC is used in IEEE 802 products to mean the physical address of a Network Interface Card the term MIC was created.
- **Mode:** In cryptography, a block cipher operates on blocks of fixed length, often 64 or 128 bits. Because messages may be of any length, and because encrypting the same plaintext under the same key always produces the same output (as described in the ECB), several modes of operation have been invented which allow block ciphers to provide confidentiality for messages of arbitrary length.

- **Multi-factor Authentication™:** The FSB guards the network against illicit access by checking three levels of access credentials before allowing a connection.
    - Network authentication mandates that connecting devices use the correct shared identifier for the network. The Fortress Security System requires all members of a secure network to authenticate with the correct Access ID.
    - Device authentication mandates that a connecting device is individually recognized on the network through its unique device identifier. The Fortress Security System requires each device to authenticate on the secure network with the unique Device ID generated for that device.
    - User authentication requires the user of a connecting device to enter a recognized user name and valid credentials, a password, for example, or a digital certificate. The Fortress Security System can authenticate users locally
- **Nonce:** stands for number used once. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.
- **PMK (Pairwise Master Key):** an EAP exchange will provide the shared secret key called a PMK (Pairwise Master Key) in IEEE 802.11 security. This key is designed to last the entire session and should be exposed as little as possible.
- **PRNG (pseudorandom number generator**): is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRNG's state.
- **RNG (Random Number Generator):** is a computational or physical device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. appear random.
- **PSK (Pre Shared Key):** is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used.
- **PTK (Pairwise Transient Key):** A Key generated by concatenating the following attributes in IEEE 802.11 security: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address and STA MAC address.. The product is then put through a cryptographic hash function.
- **SHA (Secure Hash Algorithm):** these are a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.
- **TRNG (True Random Number Generator):** This is the Fortress implementation of a non-deterministic Random Number Generator. The design of the TRNG contains two free-running oscillators, a fast and slow one. Neither is intentionally related in any way, and indeed the relationship changes with physical affects. The basic principle of operation is that the slow oscillator samples the fast one, and it is the thermal jitter effects present on the slow oscillator which are “measured” as the sources of random entropy. The TRNG is used to generate real cryptographically strong random numbers to use as seeds into the PRNG. The PRNG are started from this arbitrary starting state, using the TRNG ‘random’ seed state.
- **TLS (Transport Layer Security):** Along with its predecessor the Secure Sockets Layer (SSL) are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant

messaging and other data transfers. TLS in this module is implemented by using SSL 3.1.

- **WPA2 (Wireless Protected Access 2):** The advanced protocol, certified through Wi-Fi Alliance's WPA2 program, implements the mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm, CCMP, which is considered fully secure.
- **ANSI X9.31 PRNG:** This is a cryptographically secure pseudo-random number generator with properties that make it suitable for use in cryptography.

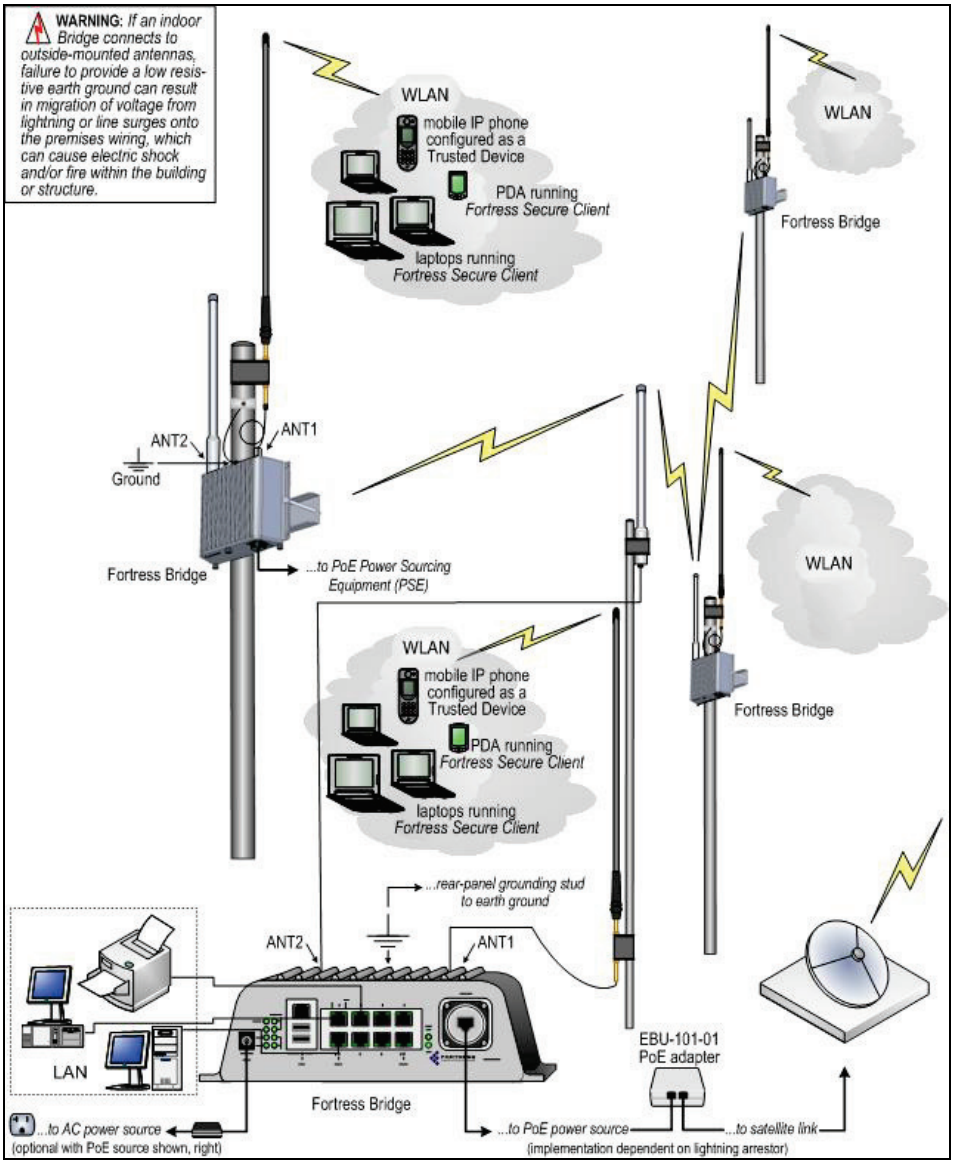

Figure 2: Example Configuration of the FSB

1.4 Functional Description

The FSB is an all-in-one network access device that implements the strongest security commercially available today. It can serve simultaneously as a wireless bridge (or a

node in a wireless mesh network), a WLAN access point, and an eight-port LAN switch, while it encrypts traffic and provides Multi-factor Authentication™ for devices on the network it secures.

The hardware is a rugged, compact chassis as shown in a sample network drawing in Figure 2. The FSB can be used indoors or outdoors with the Mast-Mounting and Weatherizing kits shipped with every device. The FSB can be quickly and transparently integrated into an existing network to provide enhanced FIPS 140-2 security. The FSB can have up to eleven data input or output interfaces:

Any of the interfaces can be used within a Clear Text Zone[1] or Encrypted Zones[2]. The unit can be powered with standard AC current or as an Ethernet powered device (PD) through its WAN port, which supports power over Ethernet (PoE). The FSB can accept secure or unsecured connections from the wireless device (i.e. laptops or handheld) by means of its low powered WAN interface or from wired devices (i.e. workstation or printers) by means of one of their Ethernet interfaces. The FSB can be wirelessly networked together by using its high power Ethernet interface or it WAN Ethernet interface.

The FSB uses two methods to protect and secure End Users data. They are the Fortress' proprietary Mobile Security Protocol (MSP) or the Robust Security Network (RSN) which is the IEEE 802.11i security recommendation. Both of these methods can protect IEEE802.11 wireless network communication while MSP can also protect Ethernet communication. It also uses the SSL protocol to protect HTTPS connections into the GUI or SSH connections (SSH use the same cryptographic algorithms as SSL) into the CLI.

1.5 Mobile Security Protocol (MSP)

MSP is used to secure connections between an End User and the FSB. MSP uses the Diffie-Hellman (D-H) or Elliptical Curve Cryptography Diffie-Hellman (ECDH) for key generation and agreement, AES-CBC for strong encryption and Multi-factor Authentication for added protection for clients. It protects both users Peer-to-Peer packets and Multicast/Broadcast packets.

FSB supports the National Security Agency Suite B recommendations using the 384 bit prime-modulus curve.

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.

For peer-to-peer packets MSP uses a unique dual Diffie-Hellman or ECDH key generation method that will not only protect user packets but will also protect against "Man in the Middle" attacks. The first key exchanged is masked using AES (i.e. 128, 192 or 256 bits depending on the configuration) encryption using the Module Secret Key (Hardkey) and is considered plaintext for the FIPS validation. This creates a Diffie-

[1] Clear Test Zone refers to the portions of the network that are trusted and that the FSB will normally only send and receive packets that have not been FIPS encrypted. These could be packets that have come from a encrypted zone that have been decrypted or packet that have originated from the FSB like from the GUI, CLI or SNMP.

[2] Encrypted Zone refers to the portions of the network that are untrusted and that the FSB will normally only send or receive encrypted packets.

Hellman (1024 or 2048 depending on configuration) or 384 bit ECDH intermediate key that is hashed with other information to create the AES Static Secret Encryption Key. The second key exchanged is AES encrypted using the Static Secret Encryption Key This creates an intermediate Diffie-Hellman key or ECDH Key that is Hashed with other information to create an AES Dynamic Secret Encryption Key. User's Peer-to Peer packets are AES encrypted using this Dynamic Secret Encryption Key.

For multicast and broadcast packets MSP also has a unique protocol. When the module is first powered-up a Multicast/Broadcast packets are masked using AES with a Static Group Key and is considered plaintext for the FIPS validation. At this time a Public Dynamic Group Key is passed around the network as a token by a Master FSB. A Private Dynamic Group Key is calculated by each module on the network. From this a Dynamic Group Key is calculated by each module (replacing the Static Group Key) for AES encryption.

The encryption keys used for AES are equal to or greater than 80 bit strength as defined by NIST Special Publication 800-57 and the key establishment method as defined in NIST Special Publication 800-56A.

1.6 Robust Security Network (RSN)

RSN is used to secure connections between an End User and the FSB. RSN is a component of WPA2 that implements only the FIPS capable portions of the IEEE 802.11i security recommendations. It uses the AES-CCM (CCMP) IEEE 802.11i security which utilizes two methods to acquire a master key: one method uses a pre-shared Master Key that is configured by the Crypto Officer (Crypto Officer) and the other gets the Master Key from an EAP-TLS session. If the latter is used a Pair-wise Master Key is generated between the Client and Authentication Server (AS). The AS sends this to the FSB. A Pairwise Transient Key will be generated between the client and the FSB. A four way handshake is used to guarantee that both the Client and the FSB will have the appropriate information and will generate the same Pairwise Transient Key.

1.7 Secure Sockets Layer (SSL)

The SSL protocol is used to secure HTTPS connections into the FSB GUI that a Crypto Officer can use for administration. The FSB uses the SSL version 3.1 as a library. SSL provides confidentiality, integrity, and message digest services. OpenSSL toolkit version 1.1.1 with patch was used in the creation of the SSL library.

1.8 Secure Shell

The SSH protocol is used to secure remote terminal connections into the FSB that a Crypto Officer can use for administration. The SSH protocol uses the same cryptographic algorithms as SSL.

1.9 Secure Configuration Propagation (SCP)

In a mesh network of FSBs, a user can designate one of them as the network's Secure Configuration Propagation (SCP) master Bridge and then use the SCP master to automatically propagate configuration changes to the rest of the network Bridges.

SCP runs only over AES encrypted MSP interfaces[3], so the Crypto Officer must pre-configure and deploy a network connected only through interfaces in the Bridge's

[3] It will use the active configuration, default if nothing was configured or the current configuration.

encrypted zone.

The FSB to be included in an SCP network or must be at their factory-default settings.

The SCP slave Bridges receive and adopt the settings propagated from the master Bridge.

1.10 Management

The FSB can be managing by the following:

- Internet browser through the Graphical User Interface (GUI);
- A directly connected terminal plugged into the Console Port through the Command Line Interface (CLI);
- A remote workstation using SSH through the CLI;
- using SNMP Version 3 Network Station or Utility.

1.11 Algorithms

This software contains four different security methods MSP, RSN, SSL and SSH. MSP and RSN will secure End User data while SSL and SSH will secure Crypto Officer connections to the FSB. They all use the algorithms as detailed in Table 1. The non-FIPS algorithms are detailed in Table 2.

The AMD Alchemy will execute the code containing the algorithms that are mainly written in the C or C++ programming language. The FPGA will have loaded a binary package that will set up the chip for the algorithm processing. This will define the makeup of the FPGA and was designed using a binary language called VHDL.

Table 1: FIPS **Approved** Algorithms

Algorithm	Cert #	Implementation	Operational Environment	Val Date	Modes/States/Key sizes/ Description/Notes
AES	698	**Fortress SWAB FW Algorithms**	AMD Alchemy MIPS Processor	1/30/2008	**ECB(e/d; 128,192,256); CBC(e/d; 128,192,256)**
AES	694	**Fortress SWAB FPGA Algorithms**	Xilinx Spartan FPGA	1/17/2008	**CBC(e/d; 128,192,256)** **CCM (KS: 128)** **(Assoc. Data Len Range: 22 - 30)** **(Payload Length Range: 1 - 32)** **(Nonce Length(s): 13)** **(Tag Length(s): 8**
AES	688	**Fortress SWAB 5.0 SSL**	AMD Alchemy MIPS Processor	12/31/2007	**ECB(e/d; 128,192,256); CBC(e/d; 128,192,256); CFB8(e/d; 128,192,256); CFB128(e/d; 128,192,256); OFB(e/d; 128,192,256)**
RSA	439	**Fortress Secure Bridge 5.1 SSL**	AMD Alchemy MIPS Processor	11/4/2008	**ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-1Cert#717**
SHS	726	**Fortress SWAB FW Algorithms**	AMD Alchemy MIPS Processor	1/30/2008	**SHA-1** (BYTE-only) **SHA-384** (BYTE-only)
SHS	722	**Fortress SWAB SHS and HMAC**	Xilinx Spartan FPGA	1/17/2008	**SHA-256** (BYTE-only) **SHA-512** (BYTE-only)
SHS	721	**Fortress SWAB FPGA Algorithms**	Xilinx Spartan FPGA	1/17/2008	**SHA-1** (BYTE-only)
SHS	717	**Fortress SWAB 5.0 SSL**	AMD Alchemy MIPS Processor	12/31/2007	**SHA-1** (BYTE-only) **SHA-224** (BYTE-only) **SHA-256** (BYTE-only) **SHA-384** (BYTE-only) **SHA-512** (BYTE-only)

Algorithm	Cert #	Implementation	Operational Environment	Val Date	Modes/States/Key sizes/ Description/Notes
SHS	715	**Fortress SWAB SHS-384 Algorithm**	AMD Alchemy MIPS Processor	12/31/2007	**SHA-384** (BYTE-only)
HMAC	376	**Fortress SWAB FW Algorithms**	AMD Alchemy MIPS Processor	1/30/2008	**HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS) SHS** Cert#726 **HMAC-SHA384 (Key Size Ranges Tested: KS=BS) SHS** Cert#726
HMAC	372	**Fortress SWAB SHS and HMAC**	Xilinx Spartan FPGA	1/17/2008	**HMAC-SHA256 (Key Size Ranges Tested: KS=BS) SHS** Cert#722 **HMAC-SHA512 (Key Size Ranges Tested: KS=BS) SHS**Cert#722
HMAC	371	**Fortress SWAB FPGA Algorithms**	Xilinx Spartan FPGA	1/17/2008	**HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) SHS** Cert#721 **HMAC-SHA384 (Key Size Ranges Tested: KS<BS) SHS** Cert#715
HMAC	367	**Fortress SWAB 5.0 SSL**	AMD Alchemy MIPS Processor	12/31/2007	**HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS) SHS** **HMAC-SHA224 (Key Size Ranges Tested: KS=BS) SHS** **HMAC-SHA256 (Key Size Ranges Tested: KS=BS) SHS** **HMAC-SHA384 (Key Size Ranges Tested: KS=BS) SHS** **HMAC-SHA512 (Key Size Ranges Tested: KS=BS) SHS**
ANSI X9.31 PRNG	409	**Fortress SWAB FW Algorithms**	AMD Alchemy MIPS Processor	1/30/2008	**ANSI X9.31 PRNG [TDES-2Key];**
ANSI X9.31 PRNG	406	**Fortress SWAB FPGA Algorithms**	Xilinx Spartan FPGA	1/17/2008	**ANSI X9.31 PRNG [TDES-2Key];**
ANSI X9.31 PRNG	402	**Fortress SWAB 5.0 SSL**	AMD Alchemy MIPS Processor	12/31/2007	**ANSI X9.31 PRNG [TDES-2Key];**

Table 2: Non-FIPS Approved Algorithms

Algorithm	Notes
Diffie-Hellman	Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength; non-compliant less than 80-bits of encryption strength); EC Diffie-Hellman (key agreement; key establishment methodology provides 192 bits of encryption strength)
MD5	Used within SSL to create the “Key Block”, The key block is the repository for information that will be used for encryption key generation part of TLS Key Derivation Function.
Hardware RNG	True Random Number Generator used to generate seeds for the ANSI X9.31 PRNG

2.0 Identification and Authentication Policy

2.1 Roles

- Crypto Office Roles
  - Log Viewer: account users can view only high-level system health indicators and only those log messages unrelated to configuration changes.
  - Maintenance[4]: account users can view complete system and configuration information and perform a few administrative functions but cannot make configuration changes.
  - Administrator: This is the main manager/administrator of the FSB.
- User Roles
  - MSP End User: This role will utilize either a MSP secure client loaded on a workstation or a MSP secure controller like the FSB to establish a secure connection over an untrusted network.
  - RSN End User: This role will utilize either a RSN (802.11i) secure client loaded on a workstation or a RSN (802.11i) secure controller like a VPN to establish a secure connection over an untrusted network.

2.2 Services

The following list summarizes the services that are provided by the FSB:

- Encryption: use the encryption services of the FSB;
- Show Status: observe status parameters of the FSB;
- View Log: view log messages;
- Write Configuration: change parameters in the FSB including changing the FIPS Mode and Bypass Setting plus doing a zeroization;
- Read Configuration: read parameters in the FSB;
- Diagnostic Services: execute some network diagnostic services and self tests of the FSB;
- Write Password: change passwords;
- Upgrade: Upgrade the unit with a new release of firmware.

2.3 Authentication and Authentication Data

All roles must be authenticated before they can use module services. The module uses role based authentication. This can be processed either internally by the module or externally using an EAP authentication server.

2.3.1 Authentication Methods

All roles must be authenticated if they use FSB services. For Crypto Officer

[4] The Maintenance User is a CO and is not the same as a maintenance user as defined in FIPS 140-2.

authentication, a User Name and Password must be presented. The module forces the Crypto-Officer to change the default password at first login. The FSB will not accept new passwords that do not meet specified requirements. A Crypto Officer can utilize four secure communication methods to access the FSB, They are:

- Secure SSL connection;
- Directly connected terminal;
- Secure SSH connection;
- SNMP.

SNMP is authenticated since it's enabled and configured within an already authenticated Secure SSL, Direct Connect or Secure SSH connection.

A Crypto Officer can apply up to nine rules for administrative passwords that allow stronger passwords. This can be reviewed in the User Guide. Both modules having the same Access ID authenticate the MSP user. The RSN End User will use either a Shared Secret or will be authenticated by the use of an external EAP Server (i.e. Radius). The Authentication Data for each of these roles are shown in Table 3.

Table 3: Authentication Data

Role	Type of Authentication	Connect Using	Authentication Data
Log Viewer	Password	Secure SSL	The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters.
Maintenance	Password	Secure SSL	The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters.
Administrator	Password	Secure SSL Direct Connect Secure SSH SNMP	The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters.
MSP End User	Access ID	MSP	16-byte Access ID. (FIPS Mode) Non-FIPS users may select 8-byte s
RSN End User	Master Key or Secret	RSN	16 bytes

2.3.2 Authentication Server Methods

The Crypto Officer can also be authenticated by using an Authentication Server. The Authentication Server can be the one built into the FSB, one on another FSB or it can be an external Authentication Server like FreeRadius or Juniper's Steel Belted Radius Server that is running on a hardware Server platform

The service(s) available are determined by the FSB's configuration for authentication services as determined by the settings in Authentication Servers and/or Local Authentication.

To use an external server (RADIUS) for administrator authentication, it must be configured to use Fortress's Vendor-Specific Attributes (see User Guide for more information).

Authentication Strength

The probability of guessing the authentication data is shown in Table 4.

Table 4: Probability of guessing the authentication data

Role	Probability of guessing the authentication data	Probability of guessing the authentication data with multiple attempts
Log Viewer	Between 1/(1+91)^8 and 1/(1+91)^32.	The FSB requires that all variants of the Crypto Officer manually enter the password. Manual entry limits the number of attempts to eight per minute, therefore, the probability would be between one in (2^3)/(2^62)^8 and one in (2^3)/(2^92)^32 which is less than 1 in 10^5. The maximum number of login attempts can be set between 1 and 9 and lockout duration between 0 and 60 minutes.
Maintenance		
Administrator		
MSP End User	Either 1/(1+1)^64 or 1/(1+1)^128 for a 8 or 16- byte Access ID respectively. 16-byte used in FIPS Mode	User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Access ID this represents 120x10^6 password attempts per minute. The 2^64/120x10^6 ~ = 2^64/2^7x2^20 or a probability one in 2^37 which is better than 1 in 10^5 .
RSN End User	1/(1+1)^128.	Shared Secret: User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Shared Secret this represents 120x10^6 attempts per minute. The 2^64/120x10^6 ~ = 2^64/2^7x2^20 or a probability one in 2^37 which is less than 1 in 10^5 .
		Using EAP: User authentication attempts are limited by accessing a EAP based authentication. The best this could be is no better than the shared secret thus the same rational applies.

3.0 Cryptographic keys and CSP

3.1 For MSP

The FSB contains a number of cryptographic keys and Critical Security Parameters (CSP) for MSP as shown in Table 5. All keys are generated using FIPS approved algorithms and methods as defined in SP800-56.

Table 5: MSP Keys

Key	Key Type	Generation	Storage	Use
Module Secret Key (Hardkey) Uses Manually entered AccessID as material. Not a valid FIPS key.	AES – 128, 192, or 256 bit.	Seeded with the 16-bytes of AccessID Seed is SHA256 hashed and 32 byte result is sent to encryption engine to form the key. The Key will be truncated to the size of the key that is configured	Kept in RAM never stored on disk.	Used to mask static Diffie-Hellman public key requests and responses over the wire.
Static Private Key	Diffie-Hellman: 1024 or 2048 bits ECDH: 384 bits	Automatically Generated A loop is started where the ANSI X9.31 PRNG is seeded with 32 bytes from the TRNG each time through the loop. The Dynamic Diffie-Hellman Private key is build by appending 32 bytes of ANSI X9.31 PRNG output each time through the loop until the required Diffie-Hellman Key Size is met.	Kept in RAM never stored on disk.	Along with received Diffie-Hellman Static Public Key from partner is used to generate the Static Secret Encryption Key
Static Public Key	Diffie-Hellman:1024 or 2048 bits ECDH: 384 bits	Automatically Generated Above Diffie-Hellman Static Private Key is fed to the CRT[5] function to generate this key The base prime of 2 and the Oakley Moduli of the corresponding Diffie-Hellman Key Sizes are used in the computations.	Kept in RAM never stored on disk.	Sent to communicating Module in a packet masked with the MSK (Hardkey)
Static Secret Encryption Key	AES – 128,192, or 256 bit.	Automatically Generated Received Diffie-Hellman Static Public Key from communicating partner and the Diffie-Hellman Static Private Key is fed to the CRT function. The actual key that is used for AES encryption is formed to the appropriates size (128,192, or 256 bit.) by using the SP800-56A key derivation function recommendations.	Kept in RAM never stored on disk.	Used to encrypt dynamic public key requests and responses over the wire.
Dynamic Private Key	Diffie-Hellman: 1024 or 2048 bits ECDH: 384 bits	Automatically Generated A loop is started where the ANSI X9.31 PRNG is seeded with 32 bytes from the TRNG each time through the loop. The Dynamic Private key is built by appending 32 bytes of ANSI X9.31 PRNG output each time through the loop until the required Key Size is met.	Kept in RAM never stored on disk.	Along with received Dynamic Public Key from partner is used to generate the Dynamic Secret Encryption Key
Dynamic Public Key	Diffie-Hellman: 1024 or 2048 bits	Automatically Generated Above Diffie-Hellman Dynamic Private Key is fed to the CRT function to generate this key. The	Kept in RAM never	Sent to communicating Module in a packet encrypted with the Static

[5] CRT – Chinese Remainder Theorem {z = (g^x % p)^x' % p = (g^x' % p)^x % p}

Key	Key Type	Generation	Storage	Use
	ECDH: 384 bits	new Enhanced Security's base prime of 2 and the Oakley Moduli of the corresponding Diffie-Hellman Key Sizes are used in the computations.	stored on disk.	Secret Encryption Key
Dynamic Secret Encryption Key	AES – 128, 192, or 256 bit.	Automatically Generated Received Diffie-Hellman Dynamic Public Key from communicating partner and the Diffie-Hellman Dynamic Private Key is fed to the CRT function. Results are then sent to encryption engine to form the key. The actual key that is used for AES encryption is formed to the appropriates size (128,192, or 256 bit.) by using the SP800-56A key derivation function recommendations.	Kept in RAM never stored on disk.	Used to encrypt all packets between two communicating Modules over the wire
Static Group Key (SGK) Uses Manually entered AccessID as key component. Not a valid FIPS key	AES – 128, 192, or 256 bit.	Generated using the AccessID and a SALT constant to seed the Approved RNG.	In RAM never saved in non-volatile memory.	Used to mask user-data frames until a DGK becomes active or the unicast DKey is computed.
Public Dynamic Group Key (PubDGK)	Diffie-Hellman 1024 or 2048 bits	Automatically Generated The Public Group Key is passed around the network as a token by each Module. This key is computed by one MPS Module ('originator') and relayed by all other Modules.	In RAM never saved in non volatile memory.	This key is used to generate the Dynamic Group Key.
Private Dynamic Group Key (PrvDGK).	Diffie-Hellman 1024 or 2048 bits	Automatically Generated from AccessID The Private Group key is computed by each Module using Diffie-Hellman, and results in the same binary value for each member of the group.	In RAM never saved in non	This key is used to generate the Dynamic Group Key.
Dynamic Group Key (DGK)	AES – 128, 192, or 256 bit.	Automatically Generated Resulting Common Dynamic Group Key from the Diffie-Hellman function.	In RAM never saved in non	Used for user-data broadcast/multicast traffic. Generate with same DH functions that generate the Static and Dynamic Secret encryption key.

3.2 For RSN

An RSN or 802.11i wireless secure LAN can use either a PreShared Secret Key (PSK) or a EAP generated master key. If a PSK is used each peer must configure the correct hex value. This PSK becomes the Master Key. If the EAP method is use the Master Key is generate through the EAP process and it's correctly given to both the Client and FSB.

For the EAP process the RSN or 802.11i architecture contains the following components: 802.1X for authentication (entailing the use of EAP and an authentication server), RSN keeps track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication. Another important element of the authentication process is the four-way handshake. The Master Key for RSN can be either manually configured through the GUI, CLI or SNMP or can be automatically generated by using the approved EAP authentication method. This product conforms to the current 802.11 specification that defines these security components.

RSN is the IEEE 802.11i security recommendations which are now part of the IEEE 802.11 Specification for wireless LAN networks. The keys for RSN are shown in Table 6.

Table 6: RSN Keys

Key	Key Type	Generation	Storage	Use
Pairwise Master Key (PMK)	256 bit key.	Using the key generation procedure as defined in the IEEE 802.11 specification. Pre-shared key Manual entry of PMK (64-hex digits). EAP Method PMK is created using key material generated during authentication, which is then transferred to FSB using RADIUS protocol.	Kept in RAM never stored on disk.	Used to derive pairwise transient key (PTK).
Pairwise Transient Key (PTK)	For AES-CCMP, 384 bit key comprised of three 128 bit keys: Data Encryption/Integrity key, EAPOL-Key Encryption key, and EAPOL-Key Integrity key.	Using the key generation procedure as defined in the IEEE 802.11[6] specification. The Pairwise Transient Automatically recomputed every time a mobile device associates with FSB using PMK, a nonce from end user station and STP, and the MAC address of the end user station and STP.	Kept in RAM never stored on disk.	Used to protect link between end user station and FSB.
Group Master Key (GMK)	256 bit key.	Using the key generation procedure as defined in the IEEE 802.11 specification. Random number automatically generated by FSB FIPS ANSI X9.31 PRNG, Programmable rekey period, default of 86400 seconds.	Kept in RAM never stored on disk.	Used to derive group transient key (GTK).
Group Transient Key (GTK)	For RSN/TKIP and WPA, 256 bit key comprised of two 128 bit keys: Group Encryption key and Group Integrity key. For AES-CCMP, 128 bit key comprised of Group	A Using the key generation procedure as defined in the IEEE 802.11 specification. Automatically Computed using GMK, a nonce, and MAC address of FSB. Programmable rekey period, default of 600 seconds. Programmable rekey option when end user stations possessing current GTK leaves BSS, default is enabled.	Kept in RAM never stored on disk.	Used to protect multicast and broadcast (group) messages sent from FSB to associated end user station. .

[6] Using the Pseudo Random Function defined in IEEE 802.11i (8.5.1.1), HMAC-SHA1

Key	Key Type	Generation	Storage	Use
	Encryption/Integrity key.			
PRF	HMAC 80-bit	ANSI X9.31 RNG	RAM Never strored on disk	IEEE802.11i HMAC SHA-1 PRF function

RSN Key Chart Descriptions and Abbreviations

- AES: Advance Encryption Standard
- AP: Access Point CCMP: Counter Mode with Cipher Block Chaining
- BSS: Basic Service Set
- EAPOL: Extensible Authentication Protocol over LAN
- Message Authentication Code Protocol
- Nonce: One time random number
- PRF: Pseudo Random Function
- Radius: Remote Authentication Dial In User Service
- RSN: Robust Security Network
- RSNA: Robust Security Network Architecture
- STA: Workstation or Wireless PC
- TKIP: Temporal Key Integrity Protocol
- WPA: Wi-Fi Protected Access

3.3 For SSL and SSH

The SSL protocol is used to establish a FIPS secured connection from a management workstation running a standard Internet Browser to either the FSB GUI or the CLI. The SSH protocol uses the cryptographic algorithms of the SSL protocol. The cryptographic keys for SSL and SSH are shown in Table 7.

Table 7: SSL and SSH Crypto Keys

Key	Key Type	Generation	Storage	Use
RSA Private Key SSL	RSA Key 2048 bit	Automatically Generated PR=(e,n) See below	Kept in RAM never stored on disk.	Used to encrypted data. Used to decrypt data for signature purposes.
RSA Public Key SSL	RSA Key	Automatically Generated PU=(d,n) See below	Kept in RAM never stored on disk.	Used to decrypt data Used to encrypt data for signature purposes
DH Private Key SSL & SSH	Diffie-Hellman Key (1024 bits)	Seed is automatically pulled from ANSI X9.31 PRNG.The private key is computed as follows: key = (base prime) ^ (hash of seed) mod (module prime).	Kept in RAM never stored on disk.	Used along to calculate the Pre-Master Secret from DH
DH Public Key SSL & SSH	Diffie-Hellman Key	The DH Private Key is fed to the Diffie-Hellman function to automatically generate this key	Kept in RAM never stored on disk.	Used along to calculate the Pre-Master Secret from DH
Key Block SSL & SSH	Generic Key Information	Automatically Generated by SSL Protocol	Kept in RAM never stored on disk.	The Key Block is the keying material that is generated for the AES encryption key or the RSA public/private key pair will taken from.
Secret Encryption Key (SSH and SSL Session Key)	AES Key 128, 192, 256 bit	Automatically taken from the Key Block depending on Key Size	Kept in RAM never stored on disk.	Encrypt Data Packets

SSL Key Chart Descriptions and Abbreviations

p, q p and q are both prime where p does not equal q

$n = p \times q$

$\varphi(n) = (p-1)(q-1)$

$\gcd(\varphi(n), e) = 1;\ 1 < e < \varphi(n)$

$d = e^{-1} \pmod{\varphi(n)}$ in)

ClientHello.random: This is a random number that is received from the Client.

ServerHello.random: This is a random number that is generated by the FCB.

3.4 Critical Security Parameters

There are other critical security parameters that present in the FSB as shown in Table 8.

Table 8: Other Keys and Critical Security Parameters

CSP	Type	Generation	Storage	Use
Access ID 32 Hex Digits	Seed	Generated by the Approved RNG when in FIPS Mode.	Non Volatile Storage	MSK, SGK & privD-H Group key component and used for authentication
Pre-Master Secret (S) from RSA	Secret	A 48 byte secret is generated by the client.	Kept in RAM never stored on disk.	The client will send this data encrypted with the RSA Public Key to the FSB and it will be used to generate the Master Secret,
Pre-Master Secret (S) from DH	Diffie-Hellman Key	Diffie-Hellman: Both Client and Server Generates a Public Key. The Public Keys are exchanged using a Diffie-Hellman transfer and using Diffie-Hellman key calculation common secret key is generated that will become the Pre-Master Secret	Kept in RAM never stored on disk.	Used to develop the Master Secret
Master Secret	Secret	By TLS Protocol	Kept in RAM never stored on disk.	This is the key that is used to encrypt the Data
Administrator Password	Password	8 to 16 Characters, entered by the Administrator Crypto Officer	Non Volatile Storage	To authenticate the Log View
Log Viewer Password	Password	8 to 16 Characters, entered by the Administrator or Log Viewer Crypto Officer	Non Volatile Storage	To authenticate the operator
Maintenance Password	Password	8 to 16 Characters, entered by the Administrator or Maintenance Crypto Officer	Non Volatile Storage	To authenticate the Maintenance
SNMPV3 Authentication Pass phrase	Pass phrase	8 to 64 Characters	Non Volatile Storage	To authenticate the use of SNMPV3
D-H Prime Number	Intermediate Crypto Value	Hard Code Value	Non Volatile Storage	The D-H Algorithm
Upgrade Key	RSA Public Key	The upgrade key is the public RSA key used to decrypt the SHA hash value that is attached to the firmware image that has been loaded from an external workstation via the GUI. The FSB will decrypt this hash and compare it to another SHA hash that it calculates on the loaded image, If both hashes are the same it prove the integrity of the image and it will be powered up. If the hash is not equal it proves the image has been corrupted and it will not be powered up.	Non Volatile Storage	Used to decrypt the Hash value that is attached to the upgrade package
Load Key	RSA Public Key	The load key is the public RSA key used to decrypt the SHA hash value that is	Non Volatile	Used to decrypt the Hash value that is

CSP	Type	Generation	Storage	Use
		attached to the executable firmware image that has been loaded from the internal flash drive. The FSB will decrypt this hash value and compare it to a SHA hash that it has calculated on the loaded image, If both hashes are the same it proves the integrity of the image and it will be powered up. If the hashes are not the same it proves the image has been corrupted and it will not be powered up.	Storage	attached to the load package
PRNG ANSI X9.31 Seed	Random Seeding information received from the TRNG	Automatically Generated per seeding A loop is started where the ANSI X9.31 PRNG is seeded with 64 bits from the TRNG each time through the loop.	Non Volatile Storage	The TRNG contains two free-running oscillators, a fast and slow one. Neither is intentionally related in any way, and indeed the relationship changes with physical affects. The basic principle of operation is that the slow oscillator samples the fast one, and it is the thermal jitter effects present on the slow oscillator, which are “measured” as the sources of random entropy.
PRNG ANSI X9.31 Key K1, K2	Internal 3DES Key 192 bits	Automatically Generated per seeding Internal Key generate from the seed and seed key	Non Volatile Storage	This is an internal key used for ANSI X9.31 PRNG.
HMAC Key	SSL	Generated within the SSL package	Non Volatile Storage	SSL module integrity SSL code integrity SSL message integrity
Configuration Data Base Key (Not a CSP)	AES	Hardcoded	Non Volatile Storage	Used to obfuscate the Data Base however not a CSP.
Pre-Shared Key	Component	Manual Entry	Non Volatile Storage	Used to create the PSK

4.0 Access Control Policy

The same Crypto Officer may not be simultaneously logged in. However, the module supports concurrent login of different crypto-officer variants. An administrator and maintenance or other combination of crypto-officers may be logged in at the same time.

4.1 Roles each Service is authorized to Perform

In general a Crypto Officer is allowed to login and manage the FSB and end users can use cryptographic services as shown in Table 9.

Table 9: Roles each Service is authorized to Perform

Roles/Service	Encryption Services	Show Status	View Log	Read Configuration	Write Configuration (including Bypass, Setting FIPS Mode)	Diagnostic Services including self tests	Write Password	Upgrade Services	Zeroization
Log Viewer			X				X		
Maintenance		X	X	X		X	X		
Administrator		X	X	X	X	X	X[7]	X	X
MSP End User	X								
RSN End User	X								

The following CSPs are entered into the module:

Key Component	Key	Role
AccessID	Module Secret Key	Administrator Crypto-Officer
AccessID	Static Group Key	Administrator Crypto-Officer
Pre-shared key	Pairwise Master Key	Administrator Crypto-Officer

The AccessID must be changed, at first installation, to the value used by the other networked modules.

4.2 Roles, Services and Access to Keys or CSPs

The FSB doesn't allow the access of encryption keys and most critical security parameters. These are protected within the operating environment. The FSB does allow the configuration of some important parameters and passwords as detailed in Table 10.

[7] Can change all CO passwords. The Administrator can lock the Log Viewer and Maintenance passwords so they can't be changed.

Table 10: Roles who has Access to Keys or CSPs

Service	Role	Access to Cryptographic Keys and CSPs
Write Passwords (Login)	Administrator C-O Maintenance C-O LogViewer	All C-O variant Roles: W(E) Maintenance Role: W(E) Logviewer Role: W(E)
Encryption	MSP and RSN User	All keys: E
Show Status View Log	Administrator C-O Maintenance C-O Logviewer C-O	N/A
Write Configuration Set-FIPS mode Set Bypass mode Set AccessID	Administrator C-O	Password (All C-O Variants): W 802.11 Preshared Key: W AccessID: W SNMP Passphrase: W
Read Configuration	Administrator C-O Maintenance C-O	N/A
Diagnostic Self-Tests	Administrator C-O Maintenance C-O	N/A
Upgrade	Administrator C-O	Upgrade Key: E
Zeroization	Administrator C-O	All Keys & CSP: W (Configuratin Data Base Key not Zeroized)

W = Write access, R = Read access, E = Execute access

4.3 Zeroization

All keys and Critical Security Parameters (CSP)s are stored in a database and zeroed when restoring the defaults. Other configuration values are returned to their factory default. The following table shows the FIPS relevant default settings.

To restore the Defaults from the Front Panel

1. Press and hold SW1.
2. Still holding SW1, press and hold SW2 for 10 seconds. All LEDs will flash fast

(green) to indicate that factory default[8] settings will be restored.

3. Hold both switches down for another 10 seconds, until all LEDs light solid green.

If you release the switches before the LEDs light solid green, the operation is cancelled and settings will remain unchanged.

4. Release both switches.

After you have successfully initiated the restore operation, the FSB will reboot automatically.

After booting, the FSB LEDs will resume normal operation and all configuration settings, including the IP address of the FSB's management interface will be at their factory-default values.

To restore default settings via the GUI:

1. Log on to the FSB GUI through an Administrator-level account and select Tools -> System Tools from the menu on the left.
2. In the Reset to Factory Defaults frame click EXECUTE.
3. Click OK at the confirmation query. At the top of the screen the GUI displays: Reset to Factory Defaults - please be patient.
4. Close your browser.

In order to re-access a FSB reset to factory defaults you must use a new browser instance on a computer with a nonrouted connection to the FSB's clear zone and an IP address in the same subnet (192.168.254.0) as the FSB's default address.

After restoring default settings, the FSB will have to be reconfigured for use. The common network AccessID must be re-entered. The crypto-officer is forced to enter a new password prior to gaining access. To do so you can re-install it as you would a new FSB. Alternatively, you can back the configuration up before you reset the FSB to its defaults and then restore the backup configuration, after you have manually configured network properties and passwords.

Table 11: Defaults and Zeroization

CSP	Reset value (Default)
AccessID	All Zeros
Log Viewer Password	maintenance
Maintenance Password	logviewer
SNMPV3 Authentication Pass phrase	FSGSnmpAdminPwd.
Preshared Key	All Zeros

[8] This will reset the box back to what it was set to out of the factory. Any changes in the configuration will be lost and all key and CSP will be zeroed.

4.4 Upgrades

4.4.1 Introduction

The FSB can be upgraded in FIPS mode. The Upgrade packaged is downloaded from a workstation via using the GUI. The upgrade is integrity checked and stored on the internal flash and booted. The previous image is kept stored on flash and can be selected as the boot image in case of problems with the upgrade image.

4.4.2 Selecting Software Image

The FSB stores two, user-selectable copies (or images) of the FSB software on separate partitions of the internal flash memory.

When the FSB's software is upgraded the new software is first written to the non-running boot partition, overwriting any version stored there. When the FSB is rebooted to complete the upgrade process, it boots from the partition to which the upgrade was downloaded, with the same configuration settings that were in effect before the upgrade procedure.

The FSB then defaults to the boot partition with the latest software image—the last image booted—whenever it restarts.

New configuration changes are not written to the non-running boot partition. If you boot from the non-running boot partition, configuration settings will return to those in effect at the time the FSB's software was last upgraded.

To select the next boot image:

1. Log on to the FSB GUI through an Administrator-level account and select Tools -> System Tools from the menu on the left.
2. In the System Tools screen's Version frame, in Image for Next Boot, select the next image to boot from the dropdown.
3. Click EXECUTE.

4.4.3 Getting the Upgrade FSB Software

Fortress Technologies regularly releases updated versions of the FSB software to add new features, improve functionality and/or fix known bugs. Upgrade files may be shipped to the customer on CD-ROM or, more often, made available for downloading from a customers account on www.fortresstech.com.

4.4.4 Integrity of the Upgrade Bridge Image

The upgrade package for the FSB uses a RSA Signature Algorithm for integrity checking of the image. This algorithm uses a Public/Private Key Pair. A SHA-1 digest is taken of the Upgrade Image and encrypted using RSA using a Private Key. This encrypted hash is appended to the image. After the image is downloaded, the FSB uses the corresponding Public Key to decrypt this Hash and will compare that Hash to another it will do on the image. If they match the integrity is verified.

5.0 Physical Security Policy

5.1 Hardware

The FCB includes two ES hardware model; the ES520V1 and the ES520V2 as shown in Figure 3.

5.2 Tamper Evidence Application

The FSB hardware uses Loctite 425 blue adhesive to cover screws for tamper evidences as shown in Figure 3 and Figure 4. This adhesive is usually applied during manufacturing however the adhesive can be applied by the vendor or the user at the site.

5.3 Tamper Evidence Inspections

The FSB Firmware is installed by Fortress Technologies on a production-quality, FCC certified hardware device, one of the FSB hardware enclosures, which also define the FSB's physical boundary. All hardware platforms are or will be manufactured to meet FIPS 140-2, L2 requirements. Table 12 details the recommended physical security activities that should be carried out by 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. Some screws on the front and back panel are covered with the material for tamper evidence as detailed in the above section. A sample screw with the adhesive coving for the ES products is shown in Figure 3 and Figure 4.

Table 12: Recommended Physical Security Activities

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

Figure 3: Front View of the ES520V2 (Left) and ES520V1 (Right) with Blue Blocker

Figure 4: Back View of the ES520V2 (Left) and ES520V1 (Right) with Blue Blocker

6.0 Firmware Security

Self-tests validate the operational status of each product, including critical functions and files. If the firmware is compromised, the FSB enters an error state in which no cryptographic processing occurs, preventing a security breach through a malfunctioning device.

7.0 Operating System Security

The FSB operates automatically after power-up. The FSB operates on Fortress Technologies proprietary version of hardened Linux operating system that is installed along with the FSB's software, with user access to standard OS functions eliminated. The FSB provides no means whereby an operator could load and execute software or firmware that was not included as part of the FSB's validation. Updates to the firmware are supported, but can only be made using the Vendor provided services.

8.0 Self Tests

The following tables will summaries the FCM self tests. A self-test status indication is provided in the event log (passed or failed) for both the CLI and GUI interfaces.

Table 13: Self Tests

Test	Description
	MIPS Power Up Test
AES Known Answer Test (KAT) Note: For all lengths, CBC and ECB modes	A known answer test is performed
RSA KAT	A known answer test is performed
ANSI X9.31 PRNG	A known answer test is performed
SHA (1, 256, 384, 512). KAT	A known answer test is performed
HMAC (SHA 1,256,384, 512)	A known answer test is performed
Software/ Firmware Integrity Check	Uses a RSA Signature Algorithm for integrity checking of the image. This algorithm uses a Public/Private Key Pair. A SHA-1 (SSL) digest is taken of the Upgrade Image and encrypted using RSA (SSL) with a Private Key. This encrypted hash is appended to the image. After the image is loaded, the FSB uses the corresponding Public Key to decrypt this Hash and will compare that Hash to another it will do on the image. If they match the integrity is verified.
Elliptical Curve Test	A known answer test is performed
Bypass Test	See Below
	FPGA Power up Test
AES KAT Note: For all lengths, CBC and ECB modes	A known answer test is performed
ANSI X9.31 PRNG Random Number Test	A known answer test is performed
SHA (1,384) KAT Test	A known answer test is performed
HMAC (SHA (1,384)) KAT Test	A known answer test is performed
	MIPS Conditional Tests
Software/ Firmware Load Check This is used when upgrading the FSB.	The upgrade package for the FSB uses a RSA Signature Algorithm for integrity checking of the image. This algorithm uses a Public/Private Key Pair. A SHA-1 (SSL) digest is taken of the Upgrade Image and encrypted using RSA (SSL) using a Private Key. This encrypted hash is appended to the image. After the image is downloaded, the FSB uses the corresponding Public Key to decrypt this Hash and will compare that Hash to another it will do on the image. If they match the integrity is verified.
Duplicate Key Entry Test	When a value is configured it's required to be entered the value a second time. Both values are compared. If the don't equal a message will force the values to be entered again. Even through the AccessID is not a key its material used to generate a key so the test is preformed. This test is also used when inputting the PSK for RSN.
ANSI X9.31 PRNG Test	This test will compare the current random number and a previous random number output to ensure that they are not the same. If they are the same the test failed.
MSP Bypass Test	When a MAC lookup table entry changes, the bypass test tests whether clear packets can be sent into the encrypted zone. or not, and they cover combinations of hosts, guests, and clients as SAs or DAs, plus they cover broadcast vs unicast packets. An error occurs if the Packets don't match the known answers.

RSN Bypass Test	When a MAC lookup table entry changes, or is added or deleted. The CCMP bypass tests are intended to test whether packets are receiving the proper type of encryption as configured. An error occurs if the Packets don't match the known answers.
Bypass Mechanism Test	There are a set of special values (the FIPS mode for example) that have an additional CRC protecting them while they are in memory and they are protected by the SHA1 hash used when the information is stored on the compact flash.
FPGA Conditional Tests	
ANSI X9.31 PRNG	This test will compares the current random number and a previous random number output to ensure that they are not the same. If they are the same the test failed.

9.0 Security Policy for Mitigation of Other Attacks Policy

No special mechanisms are built in the FSB; 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 MSP Dynamic Secret Encryption Key is changed at least once every 24 hours, with 4 hours being the factory default duration: Mitigates key discovery.
2. In the MSP, the 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. In MSP and RSN key exchanges after the first Diffie-Hellman exchange are encrypted: *Mitigates encryption key sniffing by hackers.*
4. In MSP compression and encryption of header information inside of the frame, making it impossible to guess. MSP, RSN or SSL uses 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. In both MSP and RSN encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
6. In MSP Multi-factor Authentication: The FSB 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.

10.0 EMI/EMC

All models of the FSB hardware are FCC compliant and certified (Part 15, Subpart J, Class A) devices.

11.0 Customer Security Policy Issues

Fortress Technologies, Inc. expects that after the FSB'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 FSB(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.

11.1 FIPS Mode

FIPS Mode Requirements:

a. At module start-up the module shall be set to FIPS Mode.

b. The AccessID shall be generated using the Approved RNG option or to the network AccessID value if joining an established network. A valid FIPS network shall use an Approved RNG generated AccessID.

c. The Pre-Shared Key shall be entered using 64-hex values. The passphrase method shall not be used in the FIPS mode of operation

The FSB comes up in the FIPS operating mode during module initialization. FIPS can be disabled or enabled through the GUI or through the Command Line Interface (CLI) by the Administrator. When FIPS is disabled FIPS tests are not executed.

- On the GUI the Mode Indicator (Left Top of the GUI Screen) will show whether the unit is in Normal or FIPS module. To change operating mode on the GUI:
  - Log on to the Bridge GUI through an Administrator-level account and select Configuration -> Security from the menu on the left. On the Security screen click EDIT.
  - In the Edit Security screen's Security Settings frame change the Operating Mode to Normal or FIPS.
- To change operating mode on the CLI
  - The operating mode can be determined by whether the command prompt displays FIPS; Normal operating mode displays only the hostname and single-character command prompt (> or #).
  - FIPS operating mode is the default Bridge mode of FSB: Bridge CLI operation. The FSB Normal operating mode does not comply with FIPS.
  - Change between operating modes with the set fips command. To turn FIPS operating mode on:
    - # set fips on
- To place the Bridge in Normal operating mode, turn FIPS operating mode off:
  - FIPS# set fips off
- You must be logged on to an administrator-level account to change the operation mode.

11.2 Alternating BYPASS Mode

The FSB may be configured to allow cleartext traffic in the encrypted zone in **FIPS** mode. The FSB will support alternating Bypass since it allows both clear text and encrypted data on the same interface. Cleartext Traffic is enabled by configuring a Trusted Device rule or using a protocol that needs clear text authentication service. This protocol (IEEE802.1x) is used for port-based Network Access Control and is used within the IEEE 802.11i security recommendations. The module performs alternating Bypass by allowing cleartext traffic and encrypted traffic together.

IF Cleartext Traffic is **Enabled** the hardware's front-panel **Cleartext** LED flashes a signal whenever the Bridge passes unencrypted traffic in an encrypted zone.

12.0 Maintenance Issues

The FSB have no operator maintainable components. Unserviceable FSB must be returned to the factory for repair.