

FORTRESSTM

TECHNOLOGIES

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

Models

**Hardware: ES210, ES300, ES520
Firmware: V5.1, V5.1.1, V5.2.1, V5.2.1.1162 and V5.3.0**

(Document Version 6.00)

July 2010

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.

REVISION HISTORY

<u>Rev</u>	<u>Date</u>	<u>Author</u>	<u>Description</u>
1.0	Sept, 2009	Bill McIntosh	Initial Release
2.0	Oct, 2009	Bill McIntosh	Incorporated lab comments
3.0	Nov, 2009	Bill McIntosh	Incorporated lab comments
4.0	Mar, 2010	Tony Margalis	Incorporated NIST comments
5.0	April, 2010	Tony Margalis	Incorporated V5.3.0
6.0	July, 2010	Tony Margalis	Incorporated V5.2.1.1162

Contents

CONTENTS 3

LIST OF FIGURES AND TABLES 5

1.0 INTRODUCTION 6

 1.1 THE PURPOSE OF THIS DOCUMENT 6

 1.2 PRODUCTS 6

 1.3 RELATED DOCUMENTS 6

 1.4 GLOSSARY OF TERMS..... 7

 1.5 FUNCTIONAL DESCRIPTION..... 10

 1.6 OVERALL AND INDIVIDUAL FIPS 140-2 LEVELS..... 12

 1.7 MOBILE SECURITY PROTOCOL (MSP) 12

 1.8 ROBUST SECURITY NETWORK (RSN) (AVAILABLE IN THE ES210, ES520)..... 12

 1.9 SECURE SOCKETS LAYER (SSL) 13

 1.10 SECURE SHELL 13

 1.11 SECURE CONFIGURATION PROPAGATION (SCP) - V5.1.1 ONLY 13

 1.12 MANAGEMENT 13

 1.13 ALGORITHMS..... 13

 1.14 GUI VIEWS 15

2.0 IDENTIFICATION AND AUTHENTICATION POLICY..... 16

 2.1 ROLES..... 16

 2.2 SERVICES..... 16

 2.3 AUTHENTICATION AND AUTHENTICATION DATA..... 17

 2.3.1 *Authentication Methods*..... 17

 2.3.2 *Authentication Server Methods*..... 18

 2.3.3 *Authentication Strength* 18

 2.3.4 *Administrative Accounts* 19

3.0 CRYPTOGRAPHIC KEYS AND CSP 20

 3.1 FOR MSP..... 20

 3.2 FOR RSN (AVAILABLE IN THE ES210, ES520V1 AND ES520V2)..... 21

 3.3 FOR SSL AND SSH..... 23

 3.4 CRITICAL SECURITY PARAMETERS 24

4.0 ACCESS CONTROL POLICY..... 26

 4.1 ROLES EACH SERVICE IS AUTHORIZED TO PERFORM 26

 4.2 ROLES, SERVICES AND ACCESS TO KEYS OR CSPS 26

 4.3 ZEROIZATION 27

 4.4 UPGRADES..... 28

4.4.1	<i>Introduction</i>	28
4.4.2	<i>Selecting the Firmware Image</i>	28
5.0	PHYSICAL SECURITY POLICY	29
5.1	HARDWARE	29
5.2	DISTRIBUTION AND DELIVERY.....	29
5.3	TAMPER EVIDENCE APPLICATION	29
5.4	TAMPER EVIDENCE INSPECTIONS	29
6.0	FIRMWARE SECURITY	31
7.0	OPERATING SYSTEM SECURITY	31
8.0	SELF TESTS	32
9.0	SECURITY POLICY FOR MITIGATION OF OTHER ATTACKS POLICY	33
10.0	EMI/EMC	33
11.0	CUSTOMER SECURITY POLICY ISSUES	33
12.0	FIPS MODE	33
12.1	FIPS MODE REQUIREMENTS.....	34
12.2	ALTERNATING BYPASS MODE.....	34
13.0	MAINTENANCE ISSUES	35

List of Figures and Tables

Figure 1: ES210 Network 9

Figure 2: ES300 Network 9

Figure 3: Example Configuration of the ES520..... 10

Figure 4: ES210 with Tamper Evidence Tape 30

Figure 5: ES300 with Blue Blocker 30

Figure 6: ES520V1 with Blue Blocker..... 31

Figure 7: ES520V2 with Blue Blocker..... 31

Table 1: Firmware to Hardware hierarchy 6

Table 2: Physical Port Difference Listing 11

Table 3: Individual FIPS Level..... 12

Table 4: Protocols and Features Usage..... 13

Table 5: FIPS Approved Algorithms 14

Table 6: Non-FIPS Approved Algorithms..... 14

Table 7: Authentication Data..... 17

Table 8: Probability of guessing the authentication data 18

Table 9: MSP Keys..... 20

Table 10: RSN Keys (Available in the ES210, ES520V1 and V2)..... 21

Table 11: SSL and SSH Crypto Keys..... 23

Table 12: Other Keys and Critical Security Parameters 24

Table 13: Roles each Service is authorized to Perform 26

Table 14: Roles who have Access to Keys or CSPs..... 26

Table 15: Defaults and Zeroization 28

Table 16: Recommended Physical Security Activities 30

Table 17: Self Tests 32

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 Modules: ES210, ES300, ES520V1 and ES520V2

Firmware Version: 5.1, 5.1.1, 5.2.1, 5.2.1.1162 and 5.3.0

Table 1 shows the FSB Firmware to Hardware hierarchy.

Table 1: Firmware to Hardware hierarchy

Hardware Module	Firmware V5.1	Firmware V5.1.1	Firmware V5.2.1	Firmware V5.2.1.1162	Firmware V5.3.0
ES210			✓	✓	✓
ES300	✓	✓			
ES520V1	✓	✓	✓	✓	✓
ES520V2	✓	✓	✓	✓	✓

1.3 Related Documents

#	Document Name	Date
1	IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	12 June 2007

1.4 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.
- **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.
- **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.

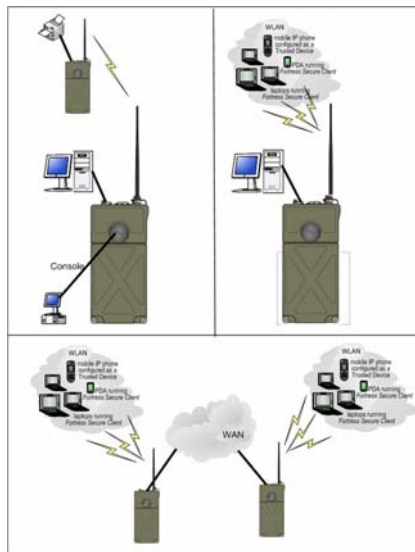


Figure 1: ES210 Network

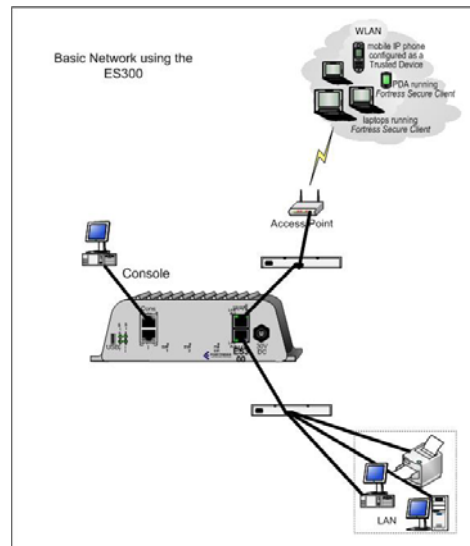


Figure 2: ES300 Network

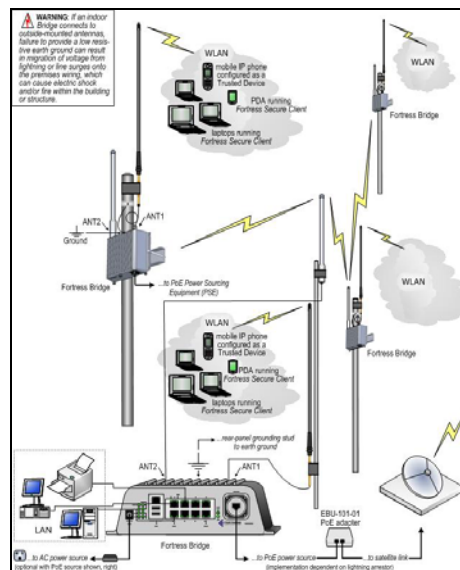


Figure 3: Example Configuration of the ES520

1.5 Functional Description

The FSB is an all-in-one network access device that implements the strongest security commercially available today. Depending on the model it can serve simultaneously as a wireless bridge (ES210, ES520), a wired bridge (all models) a node in a wireless mesh network (ES210, ES520), a WLAN access point (ES210, ES520), and an eight-port LAN switch (ES520), while it encrypts traffic and provides Multi-factor Authentication™ for devices on the network it secures.

The ES520 V1 (i.e. legacy unit) has one 48V power input along with 2 unused USB ports. The newer ES520 V2 has one 48V power input along with a variable 12/24 power input connector and 1 unused USB port. USB ports are for future development and are not functional at this time.

The hardware enclosures are all rugged, compact chassis as shown in a sample network drawings above. The FSB can be used indoors or outdoors. The FSB can be quickly and transparently integrated into an existing network to provide enhanced FIPS 140-2 security.

The LED's indicate the FSB is booting or operating normally and when clear text is in the encrypted zone. For the ES210 and ES520 V1&V2 there is are LEDs to indicate when radio(s) are on/off or passing traffic or when a firmware error occurs. For the ES210 only there is an LED indicating the battery condition.

Any of the interfaces can be used within a Clear Text Zone¹ or Encrypted Zones². The unit can be powered with standard AC current (using a AC/DC Converter), as an Ethernet powered device (PD) through its WAN port which supports power over Ethernet

¹ Clear Text 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.

(PoE) or with a battery (ES210). The FSB can accept secure or unsecured connections from a device (i.e. laptops or handheld) by means of an Ethernet interface (all models) or by its low powered WAN interface (ES210, ES520). The FSB can be wirelessly networked together by using its high power Ethernet interface or its WAN Ethernet interface (ES520).

The FSB in v5.3.0 can create its own wireless mesh network. This allows the coverage area to be extended with each additional node that is meshed together. This also allows the network to be more robust with each additional node added to the network.

The FSB uses two methods to protect and secure End Users data. They are the Fortress' proprietary Mobile Security Protocol (MSP) available on all models or IEEE 802.11 security recommendations referred to as Robust Security Network (RSN) available on the ES210 and the ES520. 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.

Table 2: Physical Port Difference Listing

<i>Port/Product</i>	<i>ES210</i>	<i>ES300</i>	<i>ES520 V1</i>	<i>ES520 V2</i>
Switch Ethernet Ports	None	None	8	8
LAN Ethernet Port (Switch)	None	None	1	1
WAN Ethernet Port	1	1	1	1
Aux Ethernet Port (LAN)	1	1	None	None
WLAN IEEE 802.11a/b/g Port	1	None	1	1
WAN 1 High Power IEEE 802.11 b/g Port	None	None	None	1
WAN 2 High Power IEEE 802.11a Port	None	None	1	None
GPS Antenna Port	1	None	None	None
USB Ports (Not Used)	None	1	2	1
Console Port	1-3 pin	1-RJ48	1-RJ48	1-RJ48
Serial Port	None	1-RJ48	None	1-RJ48
LED	4	4	8	8
Pushbuttons	3	3	3	3
Static DC Power Port	None	None	48 V DC	48 V DC
Selectable DC Power Port	None	None	None	12v/24v/48v
Variable DC Power Port Input	7-30 Volt	7-30 Volt	None	None
AC Power Input	None	None	None	None
Internal Battery	1	None	None	None

1.6 Overall and Individual FIPS 140-2 Levels

This product has an overall FIPS 140-2 certification of level 2.

Table 3: Individual FIPS Level

FIPS Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	2
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

1.7 Mobile Security Protocol (MSP)

MSP is used by all FSBs to secure connections between an End User and the FSB. MSP uses the Diffie-Hellman (D-H) or Elliptic 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.

1.8 Robust Security Network (RSN) (Available in the ES210, ES520)

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 802.11 security recommendations. It uses the AES-CCM (CCMP) IEEE 802.11 security recommendations which utilize 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.

1.9 Secure Sockets Layer (SSL)

The SSL protocol is used by all FSBs 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.

1.10 Secure Shell

The SSH protocol is used by all FSBs 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.

1.11 Secure Configuration Propagation (SCP) - V5.1.1 only

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.

1.12 Management

The FSB can be managed 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.

Table 4: Protocols and Features Usage

<i>Port/Product</i>	<i>ES210</i>	<i>ES300</i>	<i>ES520 V1</i>	<i>ES520 V2</i>
Mobile Secure Protocol	√	√	√	√
Robust Secure Network	√	No	√	√
Secure Socket Layer	√	√	√	√
Secure SHell	√	√	√	√
Secure Configuration Propagation	√	√	√	√
Graphic User Interface	√	√	√	√
Command Line Interface	√	√	√	√
SNMP	√	√	√	√

1.13 Algorithms

This firmware contains four different security methods MSP, SSL and SSH for all FSB and the RSN for the ES210, ES520V1 and ES520V2. All hardware versions use all algorithms listed below. 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 5. The non-FIPS algorithms are detailed in Table 6.

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 5: FIPS Approved Algorithms

Algorithm	Cert #	Implementation	Operational Environment
AES	698	Fortress SWAB FW Algorithms	AMD Alchemy MIPS Processor
AES	694	Fortress SWAB FPGA Algorithms	Xilinx Spartan FPGA
AES	688	Fortress SWAB 5.0 SSL	AMD Alchemy MIPS Processor
RSA	439	Fortress Secure Bridge 5.1 SSL	AMD Alchemy MIPS Processor
SHS	726	Fortress SWAB FW Algorithms	AMD Alchemy MIPS Processor
SHS	722	Fortress SWAB SHS and HMAC	Xilinx Spartan FPGA
SHS	721	Fortress SWAB FPGA Algorithms	Xilinx Spartan FPGA
SHS	717	Fortress SWAB 5.0 SSL	AMD Alchemy MIPS Processor
SHS	715	Fortress SWAB SHS-384 Algorithm	AMD Alchemy MIPS Processor
HMAC	376	Fortress SWAB FW Algorithms	AMD Alchemy MIPS Processor
HMAC	372	Fortress SWAB SHS and HMAC	Xilinx Spartan FPGA
HMAC	371	Fortress SWAB FPGA Algorithms	Xilinx Spartan FPGA
HMAC	367	Fortress SWAB 5.0 SSL	AMD Alchemy MIPS Processor
ANSI X9.31 PRNG	409	Fortress SWAB FW Algorithms	AMD Alchemy MIPS Processor
ANSI X9.31 PRNG	406	Fortress SWAB FPGA Algorithms	Xilinx Spartan FPGA
ANSI X9.31 PRNG	402	Fortress SWAB 5.0 SSL	AMD Alchemy MIPS Processor

Table 6: 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

1.14 GUI Views

This firmware contains three GUI Views: Advanced View, Simple View or Legacy View.

When firmware is installed on a ES210, ES300 or ES520V2 platform it will be able to use either the Advanced View and Simple View. If the firmware is installed on an ES520V1 platform it will automatically use the Legacy View.

The Advanced View or Simple View can be toggled through the GUI. The Advance View contains configuring, monitoring and maintaining parameters. The Simple View only contains a subset of these parameters.

The Legacy View contains configuring, monitoring and maintaining parameters that closely resemble Fortress' legacy products.

The code is exactly the same and all security functions are the same in all versions.

2.0 Identification and Authentication Policy

2.1 Roles

There are five Crypto Officer Roles.

- Crypto Officer Roles
 - Advanced and Simple Views:
 - Log Viewer: account users can view only high-level system health indicators and only those log messages unrelated to configuration changes.
 - Maintenance³: account users can view complete system and configuration information and perform a few administrative functions but cannot make configuration changes.
 - Administrator: the main manager/administrator of the FSB.
 - Legacy View (ES520 v1 only)
 - Operator: account users can view complete system and configuration information and perform a few administrative functions but cannot make configuration changes.
 - csscaisi: 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: (ES210 and ES520 V1 & V2 only) 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 both in FIPS mode and Non-FIPS mode:

- 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, Bypass Setting, Zeroization and setting passwords;
- Read Configuration: read parameters in the FSB;
- Diagnostic: execute some network diagnostic and self tests services of the FSB;
- Upgrade: Upgrade the unit with a new release of firmware.

³ The Maintenance User is a CO and is not the same as a maintenance user as defined in FIPS 140-2.

2.3 Authentication and Authentication Data

All roles must be authenticated before they can use module services. The module uses identity 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 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 7.

Table 7: Authentication Data

<i>Operator</i>	<i>Type of Authentication</i>	<i>Connect Using</i>	<i>Authentication Data</i>
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.
operator	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.
csscaisi	Password	Secure SSL	The possible character space is 91

<i>Operator</i>	<i>Type of Authentication</i>	<i>Connect Using</i>	<i>Authentication Data</i>
			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.

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).

2.3.3 Authentication Strength

The probability of guessing the authentication data is shown in Table 8.

Table 8: 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		
operator		
cssCAISI		
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 120×10^6 password attempts per minute. The $2^64/120 \times 10^6 \sim = 2^64/2^7 \times 2^{20}$ 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 120×10^6 attempts per minute. The $2^64/120 \times 10^6 \sim = 2^64/2^7 \times 2^{20}$ 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.
--	--	---

2.3.4 Administrative Accounts

The FSB uses identity based authentication. The identities are configured by adding administrative accounts to a Role. These are configured through the GUI. For instance the product can have multiple administrative accounts each having a unique Username and Password and each being assigned to a particular role (i.e., Log Viewer, Maintenance or Administrator). When a user is logged into the FSB he will have all the rights of the Role he has been assigned.

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 9. All keys are generated using FIPS approved algorithms and methods as defined in SP800-56. All the keys are kept in RAM and never stored to disk

Table 9: MSP Keys

Key	Key Type	Generation	Use
Module Secret Key (Hardkey)	AES – 128, 192, or 256 bit.	Uses Manually entered AccessID as material. Not a valid FIPS key.	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 using the ANSI X9.31 PRNG.	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 using Diffie Hellman or ECDH.	Sent to communicating Module in a packet masked with the MSK (Hardkey)
Static Secret Encryption Key	AES – 128,192, or 256 bit.	Automatically Generated using Diffie Hellman or ECDH.	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 using Diffie Hellman or ECDH.	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 ECDH: 384 bits	Automatically Generated using Diffie Hellman or ECDH.	Sent to communicating Module in a packet encrypted with the Static Secret Encryption Key
Dynamic Secret Encryption Key	AES – 128, 192, or 256 bit.	Automatically Generated using Diffie Hellman or ECDH.	Used to encrypt all packets between two communicating Modules over the wire
Static Group Key (SGK) Uses Manually entered AccessID as a seed.	AES – 128, 192, or 256 bit.	Generated using the AccessID and a SALT constant to seed the Approved RNG.	Used to mask user-data frames until a DGK becomes active or the unicast DKey is computed.

3.2 For RSN (Available in the ES210, ES520V1 and ES520V2)

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 used the Master Key is generate through the EAP process and it's correctly given to both the Client and FSB.

RSN are FIPS capable portions of the the IEEE 802.11 Specification for wireless LAN networks. The keys for RSN are shown in Table 10.

All keys are keep in RAM and never stored on disk.

Table 10: RSN Keys (Available in the ES210, ES520V1 and V2)

Key	Key Type	Generation	Use
Pairwise Master Key (PMK)	256 bit key.	Using the key generation procedure as defined in the IEEE 802.11 specification. <u>Pre-shared key:</u> a) Electronically entered as plaintext over a direct connection to the console port b) Electronically entered encrypted over a network connection via SSH or SSL <u>EAP Method:</u> PMK is created using key material generated during authentication, which is then transferred to FSB using RADIUS protocol.	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 ⁴ specification.	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.	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 Encryption/Integrity key.	Using the key generation procedure as defined in the IEEE 802.11 specification.	Used to protect multicast and broadcast (group) messages sent from FSB to associated end user station. .
PRF	HMAC 80-bit	ANSI X9.31 RNG	IEEE802.11i HMAC SHA-1

⁴ Using the Pseudo Random Function defined in IEEE 802.11i (8.5.1.1), HMAC-SHA1

			PRF function
--	--	--	--------------

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 11. All keys are kept in RAM and never stored on disk.

Table 11: SSL and SSH Crypto Keys

Key	Key Type	Generation	Use
RSA Private Key SSL	RSA Key 2048 bit	Automatically Generated	Used to encrypted data. Used to decrypt data for signature purposes.
RSA Public Key SSL	RSA Key 1024 bits	Automatically Generated	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.	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	Used along to calculate the Pre-Master Secret from DH
Key Block SSL & SSH	Generic Key Information	Automatically Generated by SSL Protocol	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	Encrypt Data Packets

3.4 Critical Security Parameters

There are other critical security parameters that present in the FSB as shown in Table 12. The Pre-Master Secret from RSA and DH and the Master Secret for DH are kept in RAM everything is in Non-Volatile Storage.

Table 12: Other Keys and Critical Security Parameters

CSP	Type	Generation	Use
Access ID 32 Hex Digits	Seed	Generated by the Approved RNG when in FIPS Mode.	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.	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	Used to develop the Master Secret
Master Secret	Secret	By TLS Protocol	This is the key that is used to encrypt the Data
Log Viewer Password	Password	8 to 16 Characters, entered by the Crypto Officer	To authenticate the Log View
Maintenance or operator Password	Password	8 to 16 Characters, entered by the Crypto Officer	To authenticate the operator
Administrator or csscaisi Password	Password	8 to 16 Characters, entered by the Crypto Officer	To authenticate the Maintenance
SNMPV3 Authentication Pass phrase	Pass phrase	8 to 64 Characters	To authenticate the use of SNMPV3
D-H Prime Number	Intermediate Crypto Value	Hard Code Value	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.	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 attached to the executable firmware image that has been loaded from the internal flash drive	Used to decrypt the Hash value that is 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.	Seed the ANSI X9.31
PRNG ANSI X9.31 Key K1, K2	Internal 3DES Key	Automatically Generated per seeding	This is an internal key used for ANSI X9.31

CSP	Type	Generation	Use
	192 bits	Internal Key generate from the seed and seed key	PRNG.
HMAC Key	SSL	Generated within the SSL package	SSL module integrity SSL code integrity SSL message integrity
Configuration Data Base Key (Not a CSP)	AES	Hardcoded	Used to obfuscate the Data Base however not a CSP.
Pre-Shared Key	Component	Manual Entry	Used to create the PTK and the PMK

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 13.

Table 13: Roles each Service is authorized to Perform

Role/Services	Encryption	Show Status	View Log	Write Configuration (including Bypass, Setting FIPS Mode, Setting Passwords, and Zeroization)	Read Configuration	Diagnostic (including self tests)	Upgrade
Administrator		√	√	√	√	√	√
Maintenance		√	√		√	√	
Log Viewer			√				
csscaisi		√	√	√	√	√	√
operator		√	√		√	√	
MSP End User	√						
RSN End User	√						

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 14.

Table 14: Roles who have Access to Keys or CSPs

Service	Role	Access to Cryptographic Keys and CSPs	R	W	E
Encryption	MSP	Access ID			√
	RSN	PreShared Secret (IEEE)			
		All Keys			
Show Status	Administrator	None	√		
	Maintenance				
	Logviewer				
	csscaisi				
	operator				

Service	Role	Access to Cryptographic Keys and CSPs	R	W	E
View Log	Administrator	None	√		
	Maintenance				
	Logviewer				
	csscaisi operator				
Write Configuration	Administrator	Change own, Maintenance, and Logviewer password		√	
	csscaisi	Change own and operator password		√	
	Administrator csscaisi	Set Access ID Set Bypass Set FIPS Mode zeroization Set SNMP Passphrase Set IEEE 802.11 Preshared Key		√	
Read Configuration	Administrator	None	√		
	Maintenance				
	Csscaisi				
	operator				
Diagnostic (including self tests)	Administrator	None			√
	Maintenance				
	csscaisi				
	operator				
Upgrade	Administrator	Upgrade Key			√
	csscaisi				

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

4.3 Zeroization

Only the CSP's listed in Table 15 are stored in a database, which are zeroed when restoring the defaults. Other configuration values are returned to their factory default. All other keys and keying material are stored in RAM and are zeroized when the unit is either rebooted or powered off. Please refer to the appropriate User Guide to determine the actual zeroization process.

Table 15: Defaults and Zeroization

CSP	Reset value
AccessID	All Zeros
Administrator Password	Default Password
Log Viewer Password	Default Password
Maintenance Password	Default Password
CAISI Password	Default Password
operator Password	Default Password
SNMPV3 Authentication Pass phrase	FSGSnmpAdminPwd.
Preshared Key	All Zeros

4.4 Upgrades

4.4.1 Introduction

The FSB firmware can be upgraded in FIPS mode and in Non-FIPS mode. Any firmware version that can be loaded on the FSB has been FIPS validated. The upgrade image is downloaded from a workstation via using the GUI. The upgrade image 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 the Firmware Image

The FSB stores two, user-selectable copies (or images) of the FSB software on separate partitions of the internal flash memory. Please refer to the User Guide to determine how to select the image for execution.

5.0 Physical Security Policy

5.1 Hardware

The FCB executes the following hardware platforms:

- ES210
- ES300
- ES520 Version 1
- ES520 Version 2

Refer to the figures below.

5.2 Distribution and Delivery

The purchaser will receive an invoice that indicates which product(s) were purchased along with the serial number(s) of the product being shipped.

The FSB is then packed and sealed and also has a packing slip placed on the outside of the box so the customer can verify the contents. The packing slip indicates the product in the package along with the serial number of the TOE.

FSB's are shipped via UPS directly from Fortress Technologies to the customer site.

5.3 Tamper Evidence Application

ES210

The hardware uses 2 tamper evidence destructible 3/8 X 3/4 inch vinyl tape as shown in Figure 4. The tape is applied during manufacturing. If the tape is removed or becomes damaged it's recommended that the unit be returned to Fortress to reapply.

ES300, ES520V1 and ES520V2

These hardware platforms use Loctite 425 blue adhesive to cover screws for tamper evidences. The ES300 as shown in Figure 5 has 4 screws total with loctite, 2 screws on the left and right of the front cover and 2 screws on the left and right of the back cover. The ES520's as shown in Figure 6 and Figure 7 have 6 screws total with loctite, 2 screws on the left and right of the front cover and 2 screws on the left and right of the back cover, in addition two diagonally opposing screws on the WAN port are covered with loctite. The adhesive is applied during manufacturing. If the glue is removed or becomes damaged it's recommended that the unit be returned to Fortress to reapply.

5.4 Tamper Evidence Inspections

The FSB Firmware is installed by Fortress Technologies on a production-quality, FCC certified hardware device, which also define the FSB's physical boundary. All hardware platforms are or will be manufactured to meet FIPS 140-2, L2 requirements. Table 16 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 epoxy potting material covering the chassis access screws or by vinyl tape.

If using epoxy potting material then some screws on the front and back panel are covered with the material for tamper evidence as shown in Figure 6, Figure 7 and Figure 8.

Table 16: Recommended Physical Security Activities

<i>Physical Security Object</i>	<i>Recommended Frequency of Inspection</i>	<i>Inspection Guidance</i>
Appropriate chassis screws covered with epoxy coating.	Daily	Inspect screw heads for chipped epoxy material. If found, remove FSB from service.
Tape appropriately Applied	Daily	Inspect the tape to make sure it securely in place.
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.

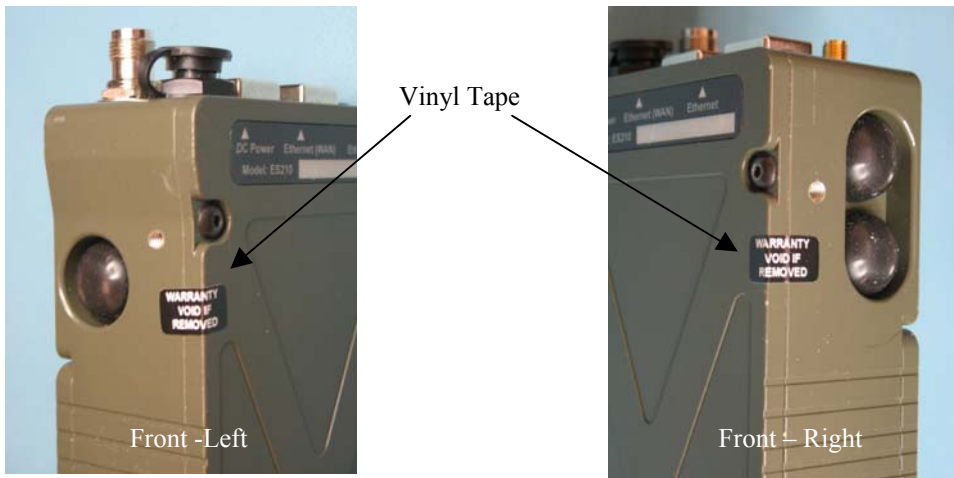


Figure 4: ES210 with Tamper Evidence Tape



Figure 5: ES300 with Blue Blocker

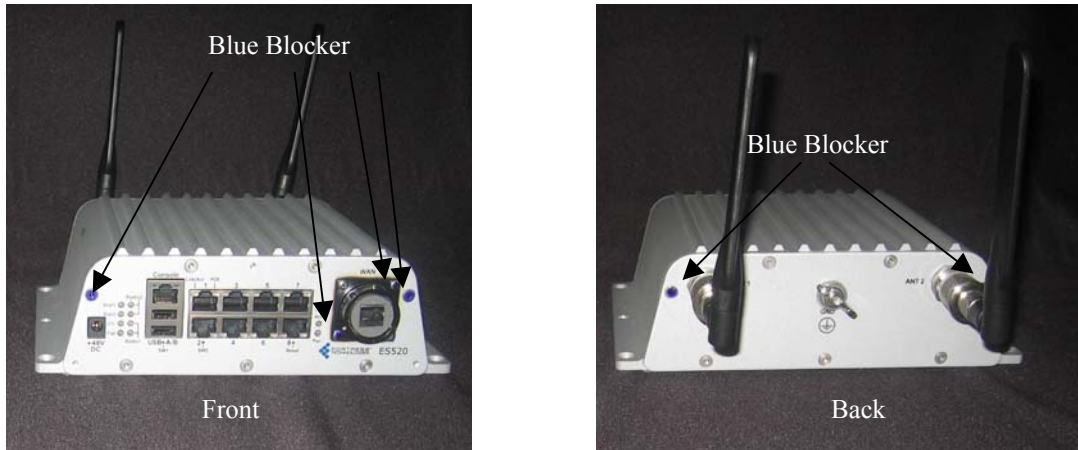


Figure 6: ES520V1 with Blue Blocker

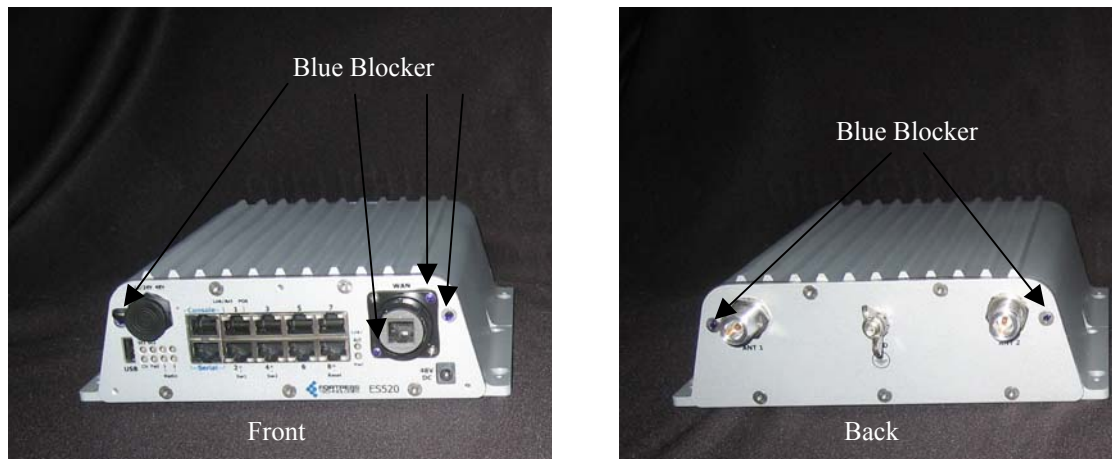


Figure 7: ES520V2 with Blue Blocker

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 FSB self tests. A self-test status indication is provided in the event log (passed or failed) for both the CLI and GUI interfaces, including the firmware load test.

Table 17: Self Tests

Test	Description	MSP	MSP	SSL	RSN	RSN
		Alchemy MIPS Processor	Xilinx Spartan FPGA	Alchemy MIPS Processor	Alchemy MIPS Processor	Xilinx Spartan FPGA
<i>Power Up Test</i>						
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			√		
RNG (All Implementations)	A known answer test is performed.	√	√	√	√	
SHA (1, 384). KAT	A known answer test is performed	√	√	√	√	
SHA (256, 512). KAT	A known answer test is performed	√		√		
HMAC (SHA 1,384)	A known answer test is performed	√	√	√	√	
HMAC (SHA 256, 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.	√	√	√	√	√
Elliptic Curve Test	A known answer test is performed	√				
<i>Conditional Tests</i>						
Software/ Firmware Load Check This is used when upgrading the BRIDGE.	The upgrade package for the Bridge uses a RSA Signature Algorithm for integrity checking of the image.	√	√	√	√	√
RNG Test (All Implementations)	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.	√	√	√		
Bypass Test	Bypass test run happens when a MAC lookup table entry changes or when an interface is added/changed/deleted.	√	√	√	√	√
Bypass Mechanism Test	This will do an integrity check on the parameters that are used to turn on and off allowing clear text traffic to bypass cryptographic processing. This guarantees these parameters were not compromised.	√		√		

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.

12.0 FIPS Mode

12.1 FIPS Mode Requirements

The following are the requirements for FIPS mode:

- a. At module start-up the module shall be set to FIPS Mode.
- b. A valid FIPS network shall use an Approved RNG generated AccessID from one FSB. All other FSB in the network will need to be setup using this 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.
- d. Enable the SSH protocol for remote CLI management.

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 mode. 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.

12.2 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 when using IEEE802.1x.

A Trusted Device is activated by configuring the Trusted Device/AP Settings then clicking APPLY to apply the setting.

The IEEE-802.1x authentication is enabled by setting the parameter in the Ethernet Setting to On then clicking APPLY to apply the setting.

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 on the ES300, ES520V1 and V2 or the Crypto LED on the ES210 flashes a signal whenever the Bridge passes unencrypted traffic in an encrypted zone.

13.0 Maintenance Issues

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