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

Fortress Mesh Points

Hardware:

ES210: Tactical Mesh Point

ES300: Inline Network Encryptor

ES440: Infrastructure Mesh Point

ES520 (V1 & V2): Deployable Mesh Point

ES820: Vehicle Mesh Point

Firmware: 5.3.1

August 2011

This security policy of Fortress Technologies, Inc., for the FIPS 140-2 validated Fortress Mesh Points (FMP), defines general rules, regulations, and practices under which the FMP 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 3
1.0 IDENTIFICATION AND AUTHENTICATION POLICY 4
1.1 ROLES 4
1.2 SERVICES 4
1.3 AUTHENTICATION AND AUTHENTICATION DATA 5
1.3.1 Authentication Methods 5
1.3.2 Authentication Server Methods 6
1.3.3 Authentication Strength 6
1.3.4 Administrative Accounts 7
2.0 CRYPTOGRAPHIC KEYS AND CSP 8
2.1 FOR MSP 8
2.2 FOR RSN 9
2.3 FOR SSL AND SSH 10
2.4 CRITICAL SECURITY PARAMETERS 11
3.0 ACCESS CONTROL POLICY 13
3.1 ROLES EACH SERVICE IS AUTHORIZED TO PERFORM 13
3.2 ROLES, SERVICES AND ACCESS TO KEYS OR CSPS 13
3.3 ZEROIZATION 15
3.4 UPGRADES 15
3.4.1 Introduction 15
3.4.2 Selecting Software Image 15
4.0 PHYSICAL SECURITY POLICY 16
4.1 HARDWARE 16
4.2 TAMPER EVIDENCE APPLICATION 16
4.3 TAMPER EVIDENCE INSPECTIONS 16
5.0 SECURITY POLICY FOR MITIGATION OF OTHER ATTACKS POLICY 21
6.0 FIPS MODE 21
7.0 CUSTOMER SECURITY POLICY ISSUES 22

List of Figures and Tables

Figure 1: ES210 Tamper Evidence 17
Figure 2: ES300 Tamper Evidence 18
Figure 3: ES440 Tamper Evidence 18
Figure 4: ES520 Version 1 Tamper Evidence 19
Figure 5: ES520 Version 2 Tamper Evidence 19
Figure 6: ES820 Tamper Evidence 20

Table 1: Authentication Data 5
Table 2: Probability of guessing the authentication data 6
Table 3: MSP Keys 8
Table 4: RSN Keys 9
Table 5: SSL and SSH Crypto Keys 10
Table 6: Other Keys and Critical Security Parameters 11
Table 7: Roles each Service is authorized to perform 13
Table 8: Roles who has Access to Keys or CSPs 14
Table 9: Defaults and Zeroization 15
Table 10: Recommended Physical Security Activities 17

1.0 Identification and Authentication Policy

1.1 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.
  - Maintenance[1]: 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 FMP.

  Legacy Views:

  - 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 FMP.

There are two User Roles.

- 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 FMP 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.

1.2 Services

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

- Encryption: use the encryption services of the FMP;
- Show Status: observe status parameters of the FMP;
- View Log: view log messages;
- Write Configuration: change parameters in the FMP including changing the FIPS Mode, Bypass Setting, Zeroization and setting passwords;
- Read Configuration: read parameters in the FMP;

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

- Diagnostic: execute some network diagnostic and self tests services of the FMP;
- Upgrade: Upgrade the unit with a new release of firmware.

1.3 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.

1.3.1 Authentication Methods

All roles must be authenticated if they use FMP 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 FMP will not accept new passwords that do not meet specified requirements. A Crypto Officer can utilize four secure communication methods to access the FMP, 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 following table.

Table 1: Authentication Data

Operator	*Type of Authentication*	*Connect Using*	*Authentication Data*
Log Viewer	Password	HTTP over TLS (HTTPS)	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	HTTP over TLS (HTTPS)	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	HTTP over TLS (HTTPS) 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	HTTP over TLS (HTTPS)	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	HTTP over TLS (HTTPS)	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

1.3.2 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 FMP, one on another FMP or it can be an external Authentication Server.

The service(s) available are determined by the FMP'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).

1.3.3 Authentication Strength

The probability of guessing the authentication data is shown in following table.

Table 2: Probability of guessing the authentication data

Role	Probability of guessing the authentication data	Probability of guessing the authentication data with multiple attempts
Log Viewer **Maintenance** **Administrator** **operator** **csscaisi**	Between 1/(1+91)^8 and 1/(1+91)^32.	The FMP 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.
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.

1.3.4 Administrative Accounts

The FMP 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 FMP he will have all the rights of the Role he has been assigned.

2.0 Cryptographic Keys and CSP

2.1 For MSP

The FMP contains a number of cryptographic keys and Critical Security Parameters (CSP) for MSP as shown in the following table. 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 3: 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 DRBG 800-90 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.

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

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

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

Table 4: RSN Keys

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. 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 FMP 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[2] specification.	Used to protect link between end user station and FMP.
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 FMP to associated end user station. .
PRF	HMAC 128 bit	DRBG 800-90 PRNG	IEEE802.11i HMAC SHA-1 PRF function

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

2.3 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 FMP 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 the following table. All keys are kept in RAM and never stored on disk.

Table 5: 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 DRBG 800-90 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

2.4 Critical Security Parameters

There are other critical security parameters that present in the FMP as shown in the following table. The Pre-Master Secret from RSA and DH and the Master Secret for DH are kept in RAM, and all other critical security parameters are in Non-Volatile Storage.

Table 6: 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.	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 Maintenance or operator
Administrator or csscaisi Password	Password	8 to 16 Characters, entered by the Crypto Officer	To authenticate the Administrator or csscaisi
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	Public RSA key (256 byte) used to decrypt the SHA hash value that is attached to the firmware image that has been loaded from an external workstation.	Used to decrypt the Hash value that is attached to the upgrade package
Load Key	RSA Public Key	Public RSA key (256 byte) used to decrypt the SHA hash value that is attached to the 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 (OpenSSL)	TRNG Random Seeding information	Automatically Generated by TRNG for seeding X9.31 PRNG	Seed the OpenSSL X9.31 PRNG
PRNG ANSI X9.31 Key K1, K2 (OpenSSL)	Triple-DES	Automatically Generated by TRNG	Seed key for OpenSSL X9.31 PRNG
PRNG ANSI X9.31 Seed (FPGA)	TRNG Random Seeding information	Automatically Generated by TRNG for seeding X9.31 PRNG	Seed the FPGA X9.31 PRNG
PRNG ANSI X9.31 Key K1, K2 (FPGA)	Triple-DES	Automatically Generated by TRNG	Seed key for FPGA X9.31 PRNG
Configuration Data	AES	Hardcoded	Used to obfuscate the Data Base

Base Key (Not a CSP)			however not a CSP.
Pre-Shared Key	Component	Manual Entry	Used to create the PTK and the PMK
HMAC DRBG entropy	Seed	Automatically Generated by TRNG	Entropy used as input to SP 800-90 HMAC DRBG
HMAC DRBG V Value	Counter	Automatically generated by DRBG	Internal V value used as part of SP 800-90 HMAC DRBG
HMAC DRBG Key	Seed	Automatically generated by DRBG	Key value used for the HMAC of the SP 800-90 HMAC DRBG
HMAC DRBG init_seed	Seed	Automatically generated by TRNG	Initial seed value used in SP 800-90 HMAC DRBG

3.0 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.

3.1 Roles each Service is authorized to Perform

In general a Crypto Officer is allowed to login and manage the FMP and end users can use cryptographic services as shown in the following table.

Table 7: 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	√						

3.2 Roles, Services and Access to Keys or CSPs

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

Table 8: Roles who has Access to Keys or CSPs

Service	Role	Access to Cryptographic Keys and CSPs	R	W	E
Encryption	MSP RSN	Access ID PreShared Secret (IEEE) All Keys			√
Show Status	Administrator Maintenance Logviewer csscaisi operator	None	√		
View Log	Administrator Maintenance Logviewer csscaisi operator	None	√		
Write Configuration	Administrator	Change own, Maintenance, and Logveiwer password		√	
	csscaisi	Change own and operator password		√	
	Administrator csscaisi	Set Access ID Set Bypass Set FIPS Mode zeroization Set SNMP Passphase Set IEEE 802.11 Preshared Key		√	
Read Configuration	Administrator Maintenance Csscaisi operator	None	√		
Diagnostic **(including self tests)**	Administrator Maintenance csscaisi operator	None			√
Upgrade	Administrator csscaisi	Upgrade Key			√

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

3.3 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. Please refer to the appropriate User Guide to determine the actual zeroization process.

Table 9: 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

3.4 Upgrades

3.4.1 Introduction

The FMP firmware can be upgraded in FIPS mode. The validated 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.

3.4.2 Selecting Software Image

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

4.0 Physical Security Policy

4.1 Hardware

The FCB executes the following hardware platforms:

- ES210
- ES300
- ES440
- ES520 Version 1
- ES520 Version 2
- ES820

Refer to the figures below.

4.2 Tamper Evidence Application

ES210, ES440, ES820

The hardware uses 3/8 X 3/4 inch tamper evidence destructible vinyl tape as shown in the following figures. 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 as shown in the following figures. 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.

4.3 Tamper Evidence Inspections

The FMP Firmware is installed by Fortress Technologies on a production-quality, FCC certified hardware device, which also define the FMP's physical boundary. All hardware platforms are or will be manufactured to meet FIPS 140-2, L2 requirements. The following table 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 vinyl tape, the tape is applied to the edge of the panel. If using epoxy potting material then some screws on the front and back panel are covered with the material for tamper evidence, see the following figures.

Table 10: 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 FMP from service.
Tape appropriately Applied	Daily	Inspect the tape to make sure it is securely in place and inspect for evidence of tamper. Some examples of tamper evidence include, but are not limited to, peeling, lack of tape, looseness, no tape at seam of unit.
Overall physical condition of the FMP	Daily	Inspect all cable connections and the FMP's overall condition. If any discrepancy found, correct and test the system for correct operation or remove FMP from service.

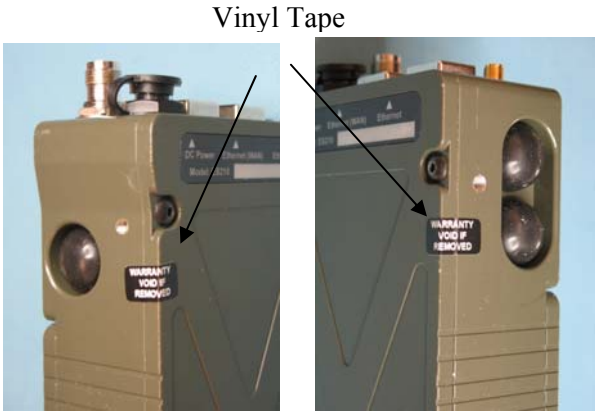

Figure 1: ES210 Tamper Evidence

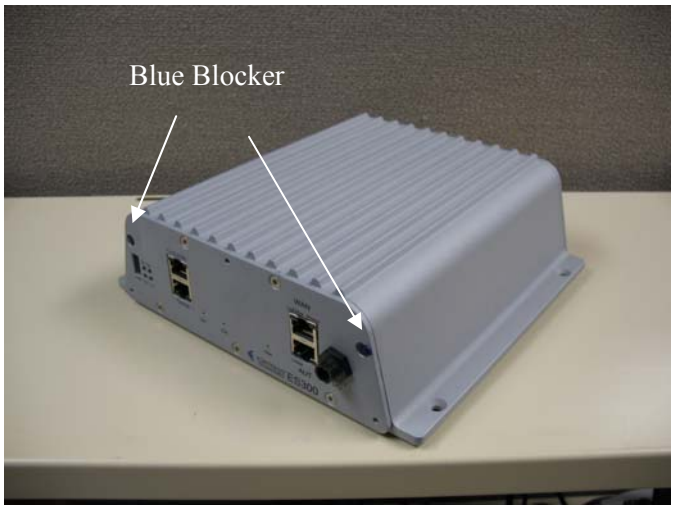

Figure 2: ES300 Tamper Evidence

Figure 3: ES440 Tamper Evidence

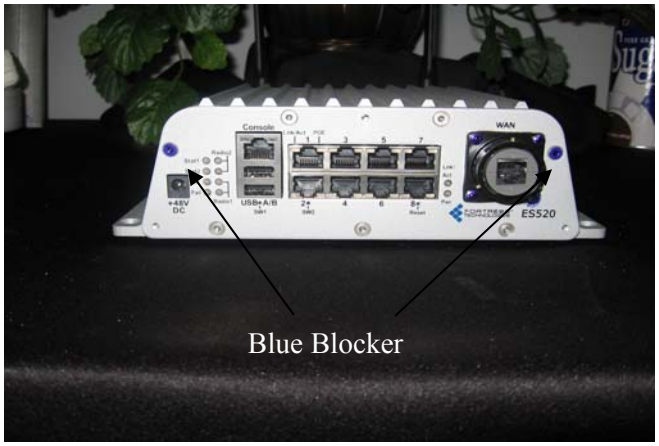

Figure 4: ES520 Version 1 Tamper Evidence

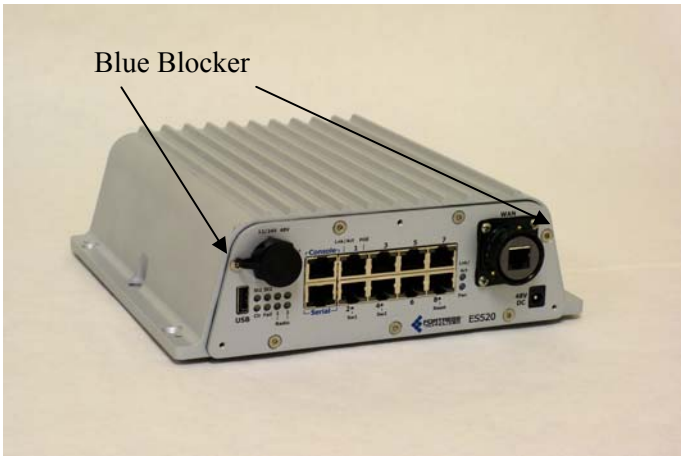

Figure 5: ES520 Version 2 Tamper Evidence

Figure 6: ES820 Tamper Evidence

5.0 Security Policy for Mitigation of Other Attacks Policy

No special mechanisms are built in the FMP; 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 FMP 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.

6.0 FIPS Mode

The following are the requirements for FIPS mode:

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.
d. Enable the SSH protocol for remote CLI management.

The FMP 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 FMP: Bridge CLI operation. The FMP 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.

7.0 Customer Security Policy Issues

Fortress Technologies, Inc. ships the module in sealed packaging and is delivered by a recognized package delivery company (UPS or FedEx) or a carrier of your choice. The recipient should check for any signs of tamper upon receipt.

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