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

ES520

Firmware Version 2.6.1

(Document Version 1.1)

February, 2007

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

Contents

List of Figures and Tables

1.0 Introduction

This security policy defines all security rules under which the Fortress Secure Wireless Access Bridge ES520 must operate and which it must enforce, including rules from relevant standards such as FIPS. The Fortress Secure Wireless Access Bridge ES520 must comply with all FIPS 140-2 level 2 requirements.

1.1 Identification

Hardware Module Numbers: ES520

Firmware Version: 2.6.1

The Fortress Secure Wireless Access Bridge ES520, also referred to as the ES520, is a *a multi-chip standalone electronic cryptographic encryption module*. The cryptographic boundary of the module is the ES520 hardware enclosure. This module operates as an *electronic encryption device* designed to prevent unauthorized access to data transferred across a wireless network. The ES520 is designed to prevent unauthorized access to data transferred across a wireless network. It provides strong encryption (AES 128, 192 and 256 bit keys) and advanced security protocols.

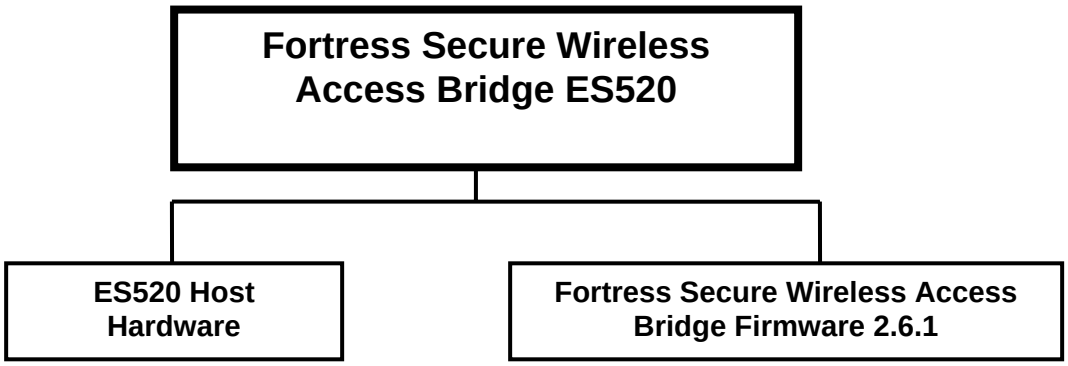

Figure 1: The ES520 Fortress Secure Access Bridge Top Level Configuration

The ES520 encrypts and decrypts traffic transmitted on a network, protecting all clients "behind" it on a protected network. Only the cryptographic officers can log into the module. The flavors of Cryptographic Officer are defined as:

- When accessing through the Bridge GUI
  - Administrator
  - Operator
- When accessing through the Command Line Interface (CLI)
  - System Administrator,

The ES520 operates at the datalink, layer of the OSI model. Most of the security protocols are implemented without human intervention to prevent any chance of human error.

The ES520 requires no special configuration for different network applications. Its security protocols are implemented without human intervention to prevent any chance of human error; therefore, the products operate with minimal intervention from the user. It secures communication within LANs, WANs, and WLANs.

The ES520 offers point-to-point-encrypted communication for the computer and Local Area Network (LAN) or Wireless LAN (WLAN) it protects. The products encrypt outgoing data from a client device and decrypts incoming data from networked computers located at different sites. Two or more ES520 can also communicate with each other directly. A typical application of the ES520 is shown in Figure 2.

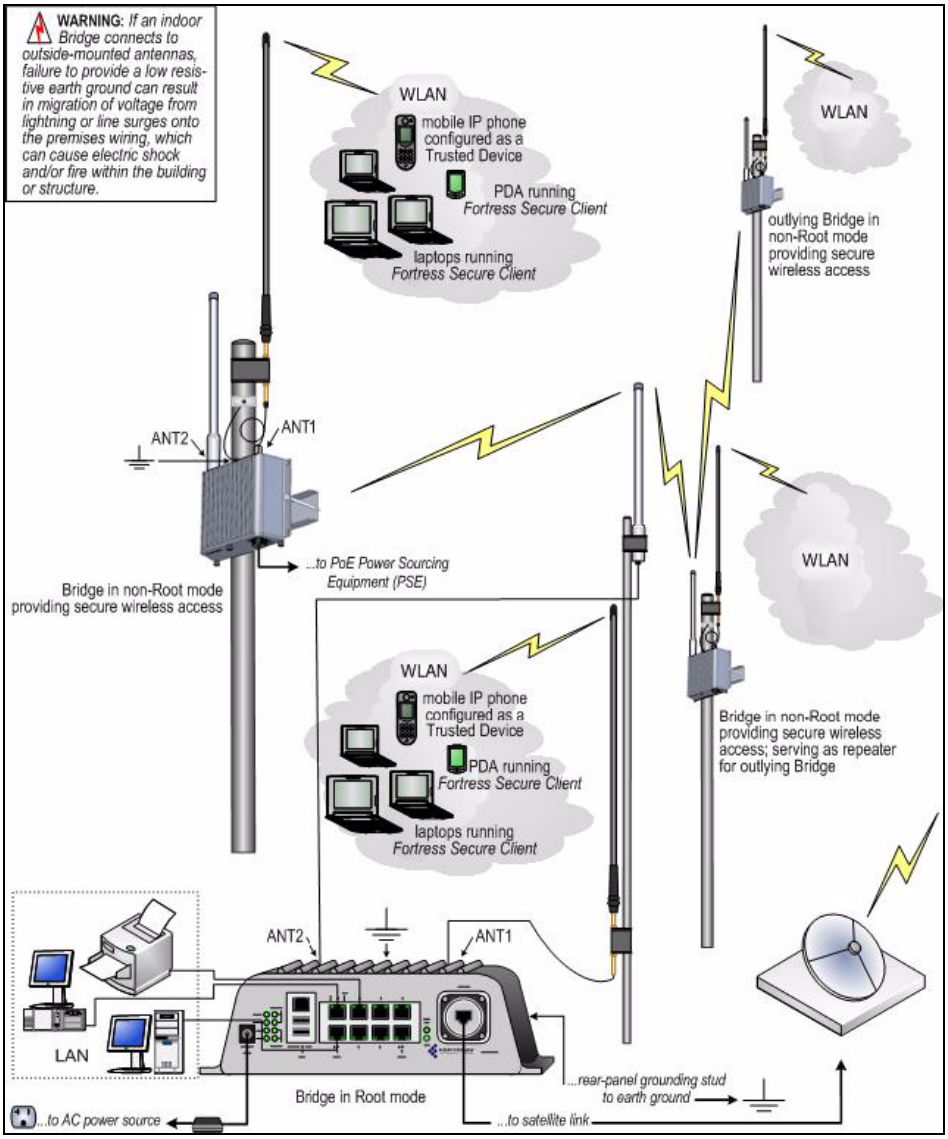

Figure 2: Example Configuration of the ES520

2.0 ES520 Security Features

The ES520 provides true datalink layer security. To accomplish this, it was designed with the security features described in the following sections.

2.1 Fortress Secure Wireless Access Bridge Design Concepts

The following security design concepts were applied to the ES520:

1. Use strong, proven encryption solutions, such as AES with 128, 192 and 256 bit keys.
2. Minimize the human intervention to the module operation with a high degree of automation to prevent human error and to ease the use and management of a security solution.
3. Secure all points where a LAN, WLAN, or WAN can be accessed by using a unique access ID, defined by the customer, to identify authorized devices and authenticate them when also using an AirFortress™ Access Control Server.
4. For FIPS 140-2, Level 2 validation the ES520 firmware can be installed only in the production grade, ES520, FCC-compliant computer hardware at the customer's site or at Fortress Technologies' production facilities. This hardware meets all FIPS 140-2, Level 2 requirements.

The underlying Wireless Link Layer Security™ (wLLS) technology ensures that cryptographic processing is secure on a wireless network, automating most of the security operations to prevent any chance of human error. wLLS builds upon the proven security architecture of Fortress Technologies Secure Packet Shield™ protocol, with several enhancements to support wireless security needs. Because wLLS operates at the datalink layer, header information is less likely to be intercepted. In addition to applying standard strong encryption algorithms, wLLS also compresses data; disguising the length of the data to prevent analytical attacks and yielding a significant performance gain on network throughput.

The ES520 require no special configuration for different network applications, although customers are encouraged to change certain security settings, such as the system administrator password and the access ID for the device, to ensure that each customer has unique parameters that must be met for access. The ES520 allow role-based access to user interfaces that access the appropriate set of management and status monitoring tools. Direct console access supports the majority of System Administrator tasks and a browser-based interface supports Administrator access.

2.2 Module Interfaces

The ES520 include the following physical ports:

1. Eight port Ethernet switch;
2. One WAN Power over Ethernet (POE) Port;
3. One serial port RJ-45;
4. Two USB ports (not used);
5. One WLAN1: ANT1 radio configured as 802.11a/b/g tri-speed port;
6. One WLAN2: ANT2 radio configured as high gain 802.11a port (5.7–5.8 GHz);
7. Three Recessed Switches (SW1, SW2, Reset)
8. One 48V DC power input port;

The ES520 includes the following Fortress logical interfaces:

1. UData I/O: Unencrypted Data Input and Output.
2. EData I/O: Encrypted Date Input and Output.
3. C/M Bridge GUI: A Cryptographic Officer can configure and monitor the ES520 via the Bridge Graphical User Interface (GUI) by using an SSL WEB Browser over an IP network. Note: SSL is only used for administrative traffic and may be considered cleartext for FIPS 140-2.
4. C/M CLI Direct: A Cryptographic Officer can configure and monitor the ES520 via the Command Line Interface (CLI) using a directly connected terminal.
5. C/M CLI SSH: A Cryptographic Officer can configure and monitor the ES520 via Command Line Interface (CLI) using SSH over an IP network. Note: SSH is only used for administrative traffic and may be considered cleartext for FIPS 140-2.
6. Mode/BO Selection: This will configure a Bridge to serve as the root node in a bridged network. Also used to set the front panel LEDs to blackout mode. Note: These can be configured also through the Bridge GUI or CLI.
7. Reset: Resets the ES520.
8. Power: Power input.

The mapping of the Physical Ports to the Logical Interface is shown Table 1.

Table 1: Physical Port to Logical Interface Mappings

	Logical Interfaces							
Physical Ports	**UData I/O**	**EData I/O**	**C/M Bridge GUI SSL**	**C/M CLI Direct**	**C/M CLI SSH**	**Mode Selection**	**Reset**	**Power**
Eight Port Ethernet Switch	X		X		X	X	X	
WAN POE Port	X	X	X		X	X	X	X
WLAN1	X	X	X			X	X	
WLAN2	X	X	X			X	X	
Serial Port				X		X	X	
Two USB Ports (not used)								
SW1						X		
SW2						X		
Reset							X	
48v power input port								X

The physical interfaces are categorized into five FIPS 140-2 defined types of logical interfaces (“Data In”, “Data Out”, “Control”, “Status”, “Power”), as follows.

Table 2: Physical Port to FIPS 140-2 Logical Interface Mappings

Physical Ports	Data In	Data Out	Control	Status	Power
Eight Port Ethernet Switch	X	X	X	X	
WAN POE Port	X	X			X
WLAN1	X	X			
WLAN2	X	X			
Serial Port			X	X	
Two USB Ports (not used)					
Recessed Switch (SW1)			X		
Recessed Switch (SW2)			X		
Recessed Switch (Reset)			X		
48v power input port					X

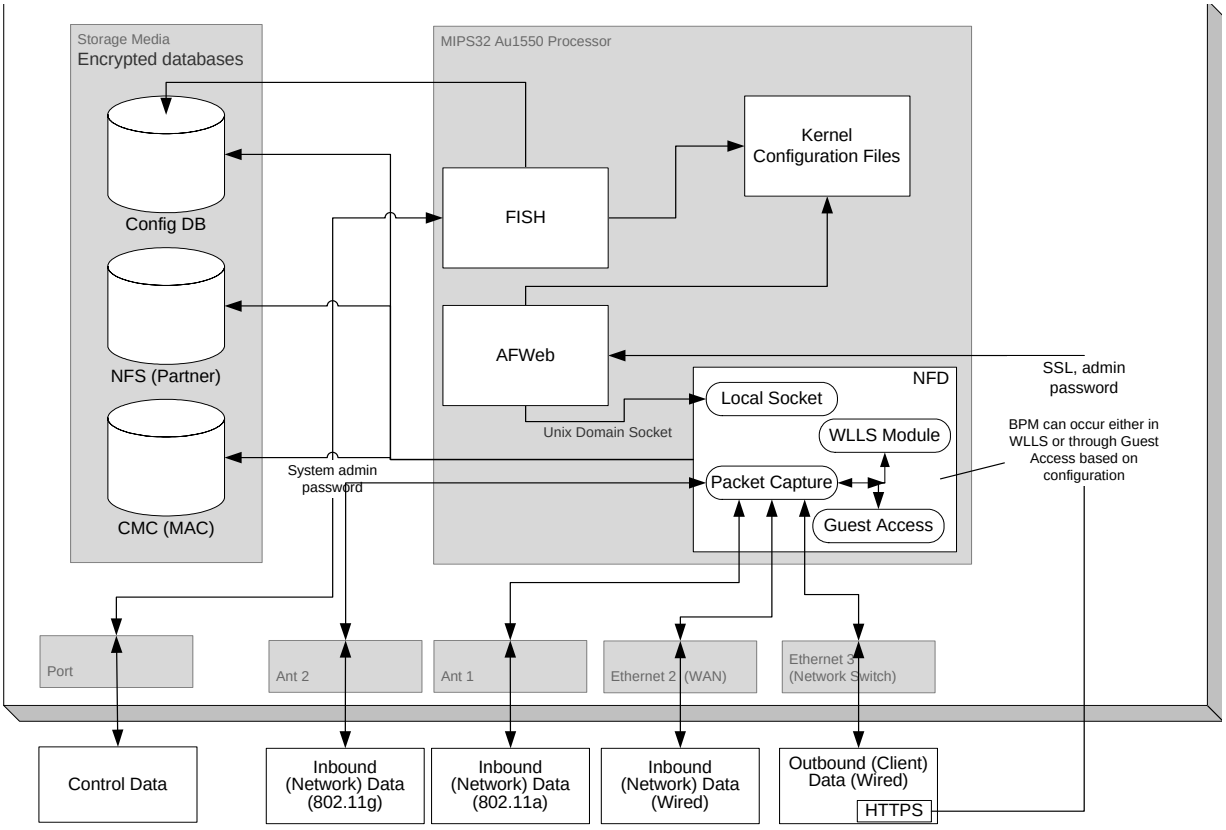

Figure 3. Information Flow through ES520

3.0 Identification and Authentication Policy

3.1 Roles

The ES520 employs role-based authentication.

The ES520 supports the following flavors of Cryptographic Officer and User roles:

- When accessing through Bridge GUI
    - Administrator: Has the ability to configure and monitor all parameters.
    - Operator: Has the ability to monitor most parameters.
- When accessing through Command Line Interface (CLI)
    - System Administrator: Has the ability to configure and monitor most parameters

The module supports one flavor of User role:

- End User: Benefits from the ES520 cryptographic processing without manual intervention, thus eliminating any direct interaction with the module; the ES520 secures data transparently to users.

3.2 Authentication

User authentication is by a 16 hexadecimal digit Access ID (64-bit). Crypto-Officer authentication is by 8-character password selectable from 72 keyboard characters. Therefore, the User strength of authentication is one in 2^64 and the Crypto-Officer one in 72^8. The module supports both internal authentication and authentication via a RADIUS server for Crypto-Officers.

3.3 Services

The following services are provided in the module:

- Creating and maintaining tables (including Encryption Bypass tables)
- Establishing the module's keys
- Key agreement using encrypted Diffie-Hellman exchanges to prevent man-in-the-middle attacks
- Reinitiating key exchange at user-specified intervals
- Zeroizing keys if power to the module is turned off
- Performing self-tests automatically at every power-on and/or by the cryptographic officer's demand.
- Display status
- Upgrade the entire module's firmware.
- Authenticating devices attempting to communicate with the ES520
- Filtering packets to prevent any unencrypted (and, therefore, unauthorized) packets from entering the network
- Encrypting and decrypting packets at the datalink layer (OSI level 2)
- Authenticating the origin of packets

3.4 Self-Tests

The ES520 conducts the following self-tests at power-up and conditionally as needed, when a module performs a particular function or operation:

A. Power-Up Tests

- Cryptographic Algorithm Test: AES KAT, HMAC KAT, SHS KAT, and RNG KAT
- Software/Firmware Integrity Test: HMAC (SHA-1)
- Critical Functions Test: Mac Address Test, Bypass Test

B. Conditional Test

- Continuous Random Number Generator test
- Bypass Test
- Firmware Load Test

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

3.5 Cryptographic Key Management

The ES520 automatically performs all cryptographic processing and key management functions.

3.5.1 Cryptographic Keys

The ES520 uses seven cryptographic keys:

- Module's Secret Key (Symmetric, AES): 128-bit, 192-bit, or 256-bit
- Static Private Key: 512-bit
- Static Public Key: 512-bit
- Static Secret Encryption Key (Symmetric, AES)): 128-bit, 192-bit, or 256-bit
- Dynamic Private Key: 512-bit
- Dynamic Public Key: 512-bit
- Dynamic Session Key (Symmetric, AES): 128-bit, 192-bit, or 256-bit

The module uses the following additional CSPs:

- Access ID 64-bits
- Crypto-Officer Password 8-characters with a cardinality of 72

Notes:

- The public and private keys above refer to those used in the Diffie-Hellman key agreement protocol.
- An ANSI X9.31 A.2.4 pseudo-random number generator is used with Diffie-Hellman key agreement (D-H Dynamic Key Pair).

3.5.2 Key Storage

No encryption keys are stored permanently in the module's hardware. Public, private and session keys are stored in RAM.

3.5.3 Zeroization of Keys

Module session keys are automatically zeroized when the system is turned off and re-established at every boot-up of the host hardware. All session keys can be zeroized manually as needed.

3.5.4 Cryptographic Algorithms

The ES520 apply the following cryptographic algorithms:

Table 3: Cryptographic Algorithms Applied by ES520

FIPS Algorithms	NIST-FIPS Certificate number
AES (ECB, CBC, encrypt/decrypt; 128, 192, 256)	423
SHS (SHA-1 (Byte))	494
HMAC	198
ANSI X9.31 RNG	218
Non-FIPS Algorithms	
Diffie-Hellman (key agreement; key establishment methodology provides 56 bits of encryption strength), MD5, RSA (non-compliant), Triple-DES (non-compliant), DSS (non-compliant), Blowfish, DES, RC2, RC4, RC5, Safer, Skipjack, MD2, MD4, MD5, GUAVA, IDEA, Hardware RNG (True RNG)	N/A

4.0 Access Control Policy

The ES520 allows role-based access to the Cryptographic Officers. The ES520 can be accessed by:

- The Bridge GUI with a standard browser over an IP network.
- The CLI with a directly connected terminal.
- The CLI using a SSH based terminal emulator over an IP network or directly connected.

The following tables, defined by Fortress Technologies' Access Control Policy, show the authorized access and services supported and allowed to each role within each product.

4.1 Roles Defined

- **Crypto-Officer (Administrator, accessed through Bridge GUI interface)**
  - **Show:** Retrieves a specified set of data for review but not modification.
  - **Select** Pick or change a parameter from a pulled down menu.
  - **Enable/Disable:** Activates a service like turning on the radio.
  - **Enter/Clear Value:** Enter a value into an entry window.
  - **Add/Delete Entry:** Add an instance of a rule.
- **Crypto-Officer (Operator, accessed through Bridge GUI interface)**
  - **Show:** Retrieves a specified set of data for review but not modification.
  - **Enter/Clear Value:** Enter a value into an entry window.
- **Crypto-Officer (System Administrator, accessed through CLI interface)**
  - **Show:** Displays system information, configuration.
  - **Set:** Sets the configuration
  - **Add:** Add an instance of a rule or device
  - **Disable:** Disable an instance of a rule or device
- **End User**
  - **Show:** Displays information, profile
  - **Select:** Pick or change a parameter
  - **Enter/Clear:** Enter a value
  - **Add/Delete:** Add an instance of a profile
  - **Request:** Request a transmission type

4.2 Available Administrator Services

The Administrator is a Crypto-Officer that can log into the ES520 by using a standard Web Browser (from a workstation on an IP network) over a SSL connection. Once logged into the ES520 the Administrator will be allowed the services shown in table 4. In general the Administrator is allowed to configure and monitor anything on ES520 that is available by the Bridge GUI.

Table 4: Services Available to the Crypto-Officer (Administrator)

Security Relevant Data Item	Description	Show	Select	Enable/Disable	Enter/Clear	Add/Delete Entry
LAN Settings	Set Host Name, IP parameters,	X	X		X	
WLAN Settings	AP Mode, Radio Parameters	X	X	X	X	
VAP Settings	SSID, Security Suite, WPA parameters, Virtual Access Points	X			X	
Password	Set Administrative Password	X	X		X	
Security Settings	Select Crypto Algorithm, Authentication, Re-Keying Interval, Access ID	X	X	**X**	X	
TD Management (Bypass Mode)	Add a trusted device	X			X	X
SNMP Settings (non-FIPS Mode)	Enable/Disable SNMP and configure parameters	X		X	X	
System Options	Set system time, upgrade firmware, backup and restore settings, set Blackout mode, System Boot, configure external RADIUS server client	X	X		X	
Statistics	Check system statistics	X				
Tracking	Track Sessions	X				
Associations	Monitor Associations	X				
System Log	Monitor system log	X				
Diagnostics	Check interface and wireless statistics, Ping and Traceroute	X			X	

4.3 Available Operator Services

The Operator is a Crypto-Officer that can log into the ES520 by using a standard Web Browser (from a workstation on an IP network) over a SSL connection. Once logged into the ES520 the Operator will be allowed the services as shown in table 5. The Operator is only allowed to monitor parameters on the ES520 that are available from the Bridge GUI.

Table 5: Services Available to the Crypto-Officer (Operator)

Security Relevant Data Item	Description	Show	Select	Enable/Disable	Enter/Clear	Add/Delete Entry
LAN Settings	Set Host Name, IP parameters,	X				
WLAN Settings	AP Mode, Radio Parameters	X				
VAP Settings	SSID, Security Suite, WPA parameters, Virtual Access Points	X				
Password	Set Administrative Password	X				
Security Settings	Select Crypto Algorithm, Authentication, Re-Keying Interval, Access ID	X				
TD Management (Bypass Mode)	Add a trusted device	X				
SNMP Settings (non-FIPS Mode)	Enable/Disable SNMP and configure parameters	X				
System Options	Set system time, upgrade firmware, backup and restore settings, set Blackout mode, System Boot	X				
Statistics	Check system statistics	X				
Tracking	Track Sessions	X				
Associations	Monitor Associations	X				
System Log	Monitor system log	X				
Diagnostics	Check interface and wireless statistics, Ping and Traceroute	X			X	

4.4 Available System Administrator Services

The System Administrator is a Crypto-Officer that can log into the ES520 by using a directly connected terminal. Once logged into the Command Line Interface (CLI) the ES520 the System Administrator will be allowed the services as shown in table 6. In general the System Administrator is allowed to configure and monitor anything on ES520 that is available by the CLI. This includes the automatic running of Self Test anytime a configurable parameter is changed.

Table 6: Services Available to the Crypto-Officer (System Administrator)

Security Relevant Data Item	Description	Show	Set	Add	Disable
802.1x	Enable IEEE 802.1x and configure parameters	X	X		
Authentication	Set whether to use internal or external authentication server	X	X		
Access ID	Set Access ID		X		
Blackout	Set the LED to blackout mode	X	X		
Cleartext	Enable Cleartext mode	X	X		
Clients	Show Clients	X			
Clock	Set the clock	X	X		
Compression	Enable compression on data	X	X		
Crypto	Select Crypto Parameters	X	X		
Device	Show Device ID	X			
FIPS	Enable FIPS Mode	X	X		
GUI	Enable GUI	X	X		
Multicast	Enable Multicast	X	X		
Network	Set Network parameters including hostname, IP Address	X	X		
Partners	Set trusted partners	X			
Password	Set Web or CLI Password		X		
Radius	Set radius server	X			
SAC	Enable and configure Secure Automatic Configuration	X	X		
SNMP (not enabled in FIPS mode)	Set SNMP parameters	X	X		
SSH	Enable Secure Shell	X	X		
STP	Enable Spanning Tree	X	X		
Wanport	Set the WAN Port as an Encrypted Interface	X	X		
Trusted Device	Configure a Trusted Device			X	X
AP	Configure a Access Point			X	X
Ping	Performs a ping on an IP address		X		
Reboot	Reboots the module		X		
Traceroute	Perform a traceroute		X		

4.5 Available End User Services

The End User will use the cryptographic services of the ES520. The End User does not have the ability to connect to the ES520 therefore it cannot configure or monitor the device.

The End User can do one of the following:

- Utilize a Fortress Secure Client on a workstation to establish a secure connection to the ES520;
- Be established as a trusted device by the Crypto-Officer. This will allow it to access the trusted network by using a cleartext connection without using the Fortress Secure Client.
- Be physically connected behind another Fortress security gateway product and allow that product to establish a secure connection

The End User does have some important roles (if the End User is using a Fortress Secure Client in FIPS mode then only the Crypto-Officer can perform these roles) that must be performed in order to establish encrypted communication with a ES520. These are shown in Table 7.

Note: Some earlier clients will allow the direct configuration of the encryption protocol and the turning encryption on and off.

Table 7: End User Services

Service		Show	Select	Enable/Disable	Enter/Clear Value	Add/Delete Entry	Request
Use Profile	**The end user will pick the profile to use for the wireless connection.**	X	X				
Create Profile	**The Crypto-Officer (System Administrator) can create a profile that has the cryptographic parameters**					X	
Enable Encryption	**Enable encryption within the profile**		X				
Type of Encryption	**Pick type of encryption**		X				
Access ID	**Configuration either a default Access ID or a custom.**				X		
Trusted Device	**An End User has the options to request a cleartext connection.**						X

5.0 Physical Security Policy

The module's firmware is installed by Fortress Technologies on a production-quality, FCC certified hardware device, the ES520, which also defines the module's physical boundary. The hardware platform is manufactured to meet FIPS 140-2, Level 2 physical security requirements. Table 8 details the recommended physical security activities that should be carried out by the Crypto-Officer.

The module 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. All screws on the front and back panel are covered with the material as shown in Figures 5 and 6. Table 8 lists recommended physical security related activities at the user's site.

Table 8: 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 module from service.
Overall physical condition of the module	Daily	Inspect all cable connections and the module's overall condition. If any discrepancy found, correct and test the system for correct operation or remove module from service.

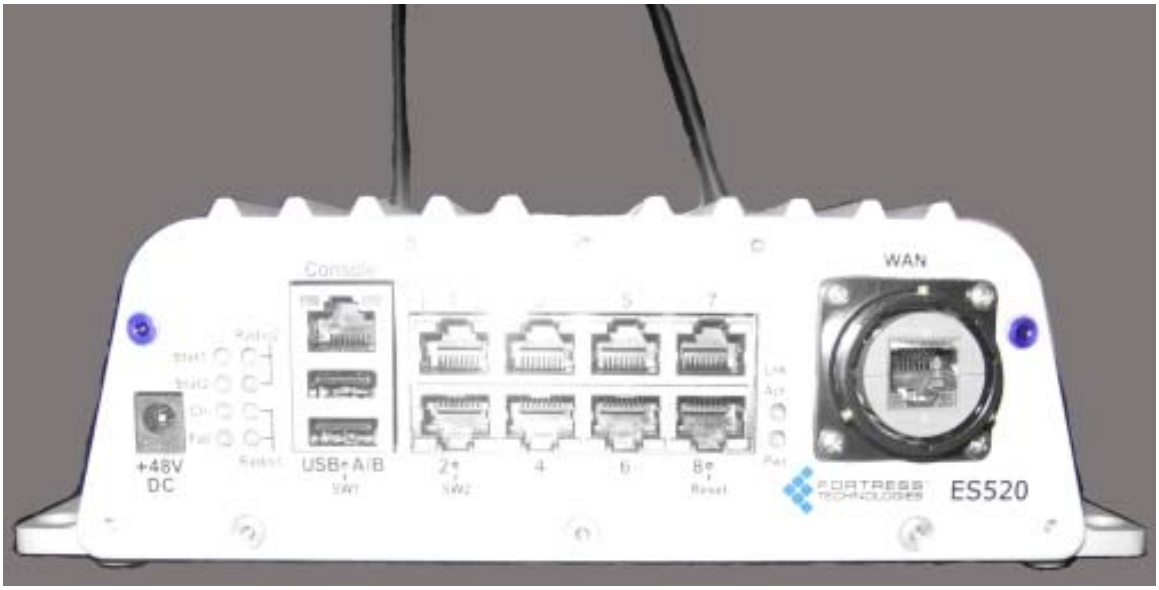

Figure 5. Front View of the ES520 Hardware Showing the Blue Thread Locker

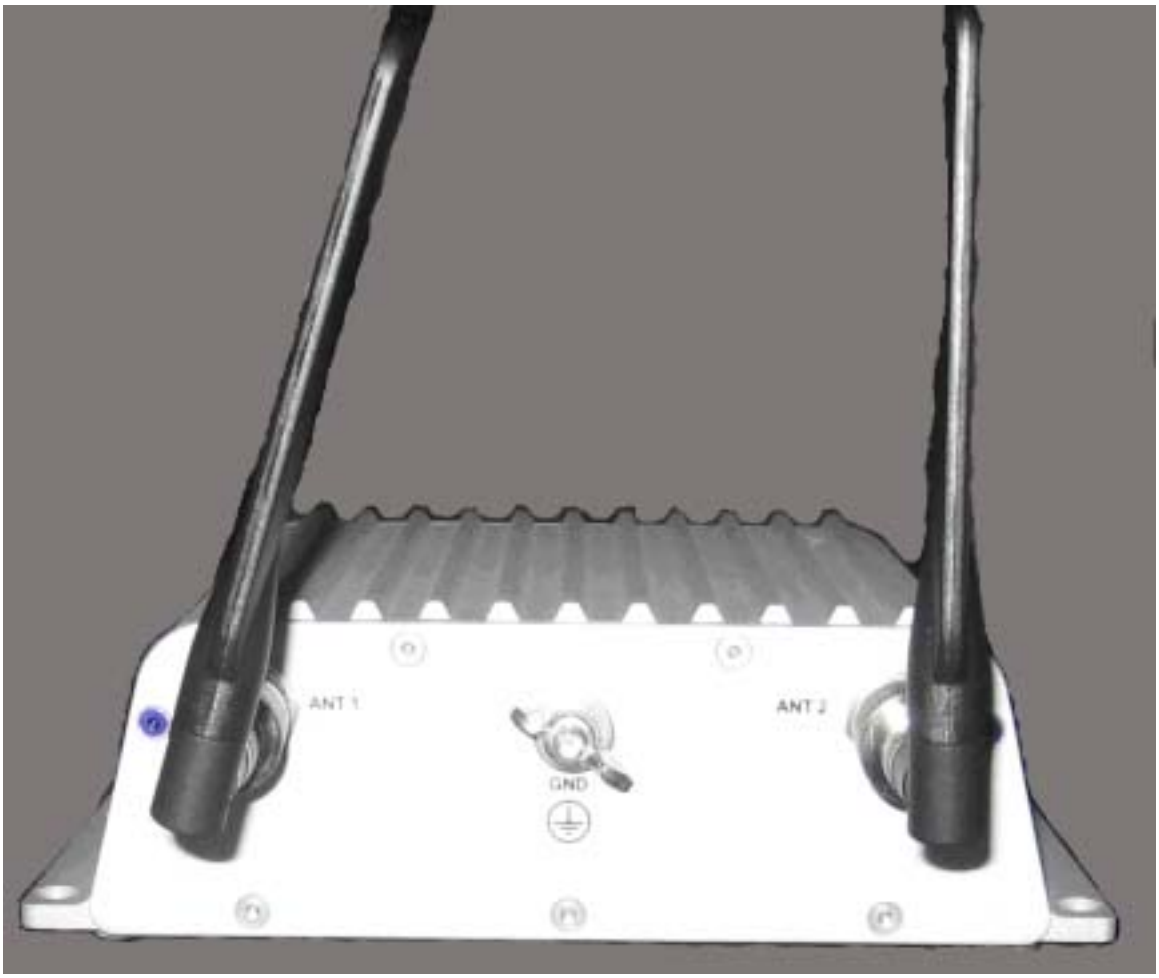

Figure 6. Rear View of the ES520 Hardware Showing the Blue Thread Locker

6.0 Firmware Security

Firmware components are not available to either the Crypto-Officer or User. The operator has only limited access to module via the Bridge GUI or CLI tools. Firmware can only be upgraded by the Administrator (Crypto-Officer). Self-tests validate the operational status of each product, including critical functions and files. If the firmware is compromised, the module enters an error state in which no cryptographic processing occurs, preventing a security breach through a malfunctioning device. Any non-validated firmware subsequently loaded and executed within the FIPS 140-2 validated cryptographic module invalidates the original validation.

7.0 Operating System Security

The ES520 operates automatically after power-up. The ES520 operates on Fortress Technologies proprietary version of hardened Linux 2.4.16 that is installed along with the module's firmware, with user access to standard OS functions eliminated. The module provides no means whereby an operator could load and execute software or firmware that was not included as part of the module's validation. Updates to the firmware are supported, but can only be made using the Vendor provided services.

8.0 Mitigation of Other Attacks Policy

No special mechanisms are built in the ES520 module; however, the cryptographic module is designed to mitigate several specific attacks above the FIPS defined functions. Additional features that mitigate attacks are listed here:

1. The dynamic session key is changed at least once every 24 hours, with 4 hours being the factory default duration: *Mitigates key discovery.*
2. A second Diffie-Hellman key exchange produces a dynamic common secret key in each of the modules by combining the other module's dynamic public key with the module's own dynamic private key: *Mitigates "man-in-the-middle" attacks.*
3. All key exchanges are encrypted: *Mitigates encryption key sniffing by hackers.*
4. Compression and encryption of header information inside of the frame, making it impossible to guess. Use of strong encryption further protects the information. Any bit flipping would be useless in this frame to try to change the IP address of the frame: *Mitigates active attacks from both ends.*
5. Encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
6. Multi-factor Authentication: The Fortress Secure Wireless Access Bridge guards the network against illicit access with "multi-factor authentication", checking three levels of access credentials before allowing a connection. These are:
    a) *Network authentication* requires a connecting device to use the correct shared identifier for the network
    b) *Device authentication* requires a connecting device to be individually recognized on the network, through its unique device identifier.
    c) *User authentication* requires the user of a connecting device to enter a recognized user name and password.

9.0 EMI/EMC

The ES520 are FCC compliant and certified (Part 15, Subpart J, Class B) devices.

10.0 Customer Security Policy Issues

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

10.1 FIPS Mode

The ES520 enters into FIPS mode during module initialization. FIPS can be disabled by using Command Line Interface to access the console port and then deselecting FIPS modes. FIPS can be verified by using the show FIPS command.

11.0 Maintenance Issues

The ES520 have no operator maintainable components. Unserviceable modules must be returned to the factory for repair.