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

Firmware Version 5.1.2

(Document Version 2.5)

December 2009

This security policy of Fortress Technologies, Inc., for the FIPS 140-2 Fortress Controller – X (FC-X), defines general rules, regulations, and practices under which the FC-X (or referred to as BRIDGE in the document) was designed and developed and for its correct operation. These rules and regulations have been and must be followed in all phases of security projects, including the design, development, manufacture service, delivery and distribution, and operation of products.

Contents

List of Figures and Tables

1.0 Introduction

1.1 The Purpose of this Document

This security policy defines all FIPS 140-2 overall level 2 security rules under which the FC-X (also referred to as Bridge) complies with and enforces. The Bridge is a multi-chip standalone module.

1.2 Products

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

Hardware: FC-X Where X = 250, 250SB(Suite B), 500, 500SB, 1500, 1500SB

Firmware Version: 5.1.2

The top level configurable hierarchy is shown in Figure 1.

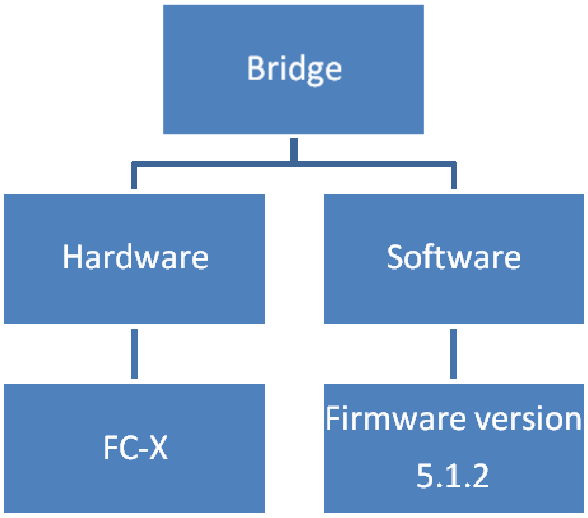

Figure 1: BRIDGE Top Level Configuration

1.3 Glossary of Terms

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

- **CTR (Counter):** generates the next keystream block by encrypting successive values of a "counter". The counter can be any simple function which produces a sequence which is guaranteed not to repeat for a long time. It allows a random access property during decryption. The IV/nonce and the counter can be concatenated, added, or XORed together to produce the actual unique counter block for encryption.
- **Diffie-Hellman:** is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
- **ECB (Electronic codebook**): This is the simplest of the encryption modes. The message is divided into blocks and each block is encrypted separately. The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks; thus, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all.
- **EAP (Extensible Authentication Protocol**): is a universal authentication framework frequently used in wireless networks and Point-to-Point connections.
- **EAP-TLS:** is an IETF open standard that is the original standard wireless LAN EAP authentication protocol, and is well-supported among wireless vendors.
- **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
- **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 BRIDGE 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.
- **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.
- **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.
- **ANSI X9.31 PRNG:** This is a cryptographically secure pseudo-random number generator with properties that make it suitable for use in cryptography.

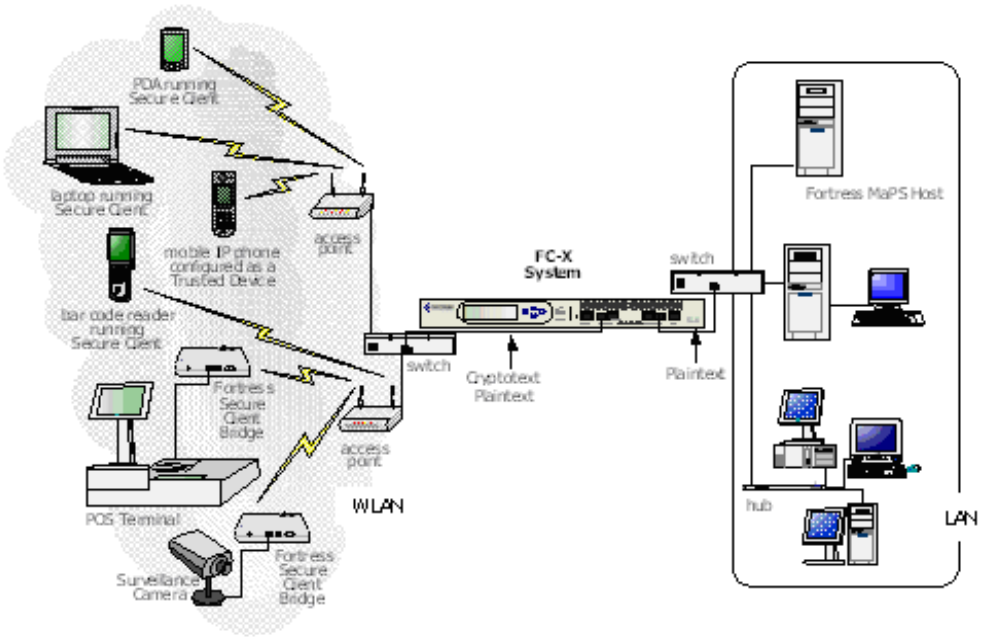

Figure 2: Example Configuration

1.4 Functional Description

The Bridge is a standalone hardware and firmware cryptographic module and security gateway designed to prevent a hacker from “sniffing” and reading data transferred across a wired or wireless network. Here -X in FC-X suffix indicates the number of active devices served by the module as shown in Table 1. This is determined by the License Key that is entered into the GUI. The License key will dictate the performance (therefore Maximum Active Devices) or whether Suite B is enabled in the product. The initial License Key is configured at manufacturing however a customer can upgrade by purchasing the appropriate License Key. When Suite B is installed the module configuration is becomes an “SB” as shown in the table below (for instance FC-250SB).

Table 1: Active Devices

Module Configuration	Maximum Active Devices	With Suite B
FC-250	500	
FC-250SB	500	√
FC-500	1000	
FC-500SB	1000	√
FC-1500	3300	
FC-1500SB	3300	√

This is a security appliance that provides a secure edge to the corporate network by protecting communications between other wireless devices and the rest of the network as shown in Figure 2. Because the Bridge implements encryption at the Media Access Control (MAC) layer, not only does it protect important network information, it functions as a transparent LAN BRIDGE so it can be quickly and transparently integrated into an existing network. Operation is almost automatic, requiring no or little administrator intervention as it protects data transmitted on WLANs (wireless LANs) and between WLAN devices and the wired local area network and over an IP network.

The Bridge's hardware is a 1U rack mount unit. The Bridge can be quickly and transparently integrated into an existing network to provide enhanced FIPS 140-2 security. The Bridge has two data Input or output interfaces, one Console interface and one Aux interface (not used).

Either of the interfaces can be used within a Clear Text Zone[1] or Encrypted Zones[2]. The unit is powered with standard AC current. The Bridge can accept secure or unsecured connections from the wireless or wired devices.

1.5 Ports and Interfaces

Only data entering and leaving the physical ports through logical interfaces is processed by the cryptographic module.

[1] Clear Text Zone refers to the portions of the network that are trusted and that the FC-X 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 FC-X like from the GUI, CLI or SNMP.

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

Physical Ports

Table 2: Physical Ports

Physical Ports	Description
LAN – Ethernet- Encrypted	A Ethernet Interface that is used to connect to the encrypted zone.
Optical – Encrypted	A high speed optical interface that is used to connect to the encrypted zone.
LAN – Ethernet- Unencrypted	A Ethernet Interface that is used to connect to the unencrypted zone.
Optical – Unencrypted	A high speed optical interface that is used to connect to the unencrypted zone.
Aux – Ethernet (Not Used)	Not Used
Console	Serial port used to connect to a terminal
Power	AC Power Input
Front Panel LCD	LCD Display used for limited system monitoring
Front Panel Push Button	Push Buttons used to scroll through line menu viewed on the LCD
LED	LEDs used for limited alerts

Logical Interfaces

Table 3: Logical Interface

Type	Logical Interface	Description
Data In and Data Out	Plaintext User Data	**Plaintext data can come in or be sent out through this logical interface.**
	Ciphertext User Data (AES, 3DES, RSA)	**Ciphertext or encrypted user data can come in or sent out. this logical interface.**
Control Input	GUI	**A crypto officer can connect to the MODULE using a Browser for control and configuration.**
	CLI	**A crypto officer can connect to the MODULE using a terminal, terminal emulator or a SSH connection for control and configuration.**
	Front Panel Interface	**Can be used to reset the BRIDGE to a default configuration.**
Status Out	GUI	**A crypto officer can connect to the MODULE using a Browser to view configuration and status information.**
	CLI	**A crypto officer can connect to the MODULE using a terminal, terminal emulator or a SSH connection to view configuration and status information.**
	LED	**Four LEDs are shown:** • **Power: Power On** • **Status: FIPS Error** • **Cleartext: Bypass Mode** • **Failover: Not used**
	Front Panel Interface	**Used to view limited information about the BRIDGE.**

Notes

- The MODULE GUI uses a standard “off the shelf” workstation and browser and CLI uses a standard terminal or a workstation using SSH.
- The operation of the buttons or switches are explained in the respective User Guide.
- Direct connect CLI (uses a terminal or terminal emulator).
- SSL (TLS) GUI, SSH CLI and SNMP operate using the IP protocol over a FIPS secure connection from a workstation. These packets enter over the Ethernet

ports along with data packets. Once the packets are decoded and queued they are processed separately. Data packets are encrypted or unencrypted and passed through to the other Ethernet interface. Control and status packets are either absorbed by the device or sent out as an IP packet.

1.6 Mobile Security Protocol (MSP)

MSP is used to secure connections between an End User and the BRIDGE. MSP uses the Diffie-Hellman (D-H) or Elliptical Curve Cryptography Diffie-Hellman (ECDH) for key generation and agreement, AES-CBC for encryption and Multi-factor Authentication for added protection for clients

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

Once it's installed and configured, operation is automatic, requiring no or little administrator intervention as it protects data transmitted on WLANs and between WLAN devices and the wired LAN.

For peer-to-peer packets MSP uses a dual Diffie-Hellman or ECDH key generation method that will not only protect user packets but will also protect against "Man in the Middle" attacks. The Dynamic Secret Encryption Key results from the Diffie-Hellman key agreement process.

User's Peer-to Peer packets are AES encrypted using this Dynamic Secret Encryption Key.

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

1.7 Secure Sockets Layer (SSL)

The SSL or TLS protocols are used to secure HTTPS connections into the BRIDGE GUI that a Crypto Officer can use for administration. SSL and TLS provides confidentiality, integrity, and message digest services. OpenSSL toolkit version 1.1.1 with patch was used in the creation of the SSL and TLS library.

1.8 Secure Shell

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

1.9 Secure Configuration Propagation (SCP)

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

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

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

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

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

1.10 Management

The BRIDGE is 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.

1.11 Algorithms

This software contains three different security methods MSP, SSL (TLS) and SSH. MSP secures End User data while SSL (TLS) and SSH will secure Crypto Officer connections to the BRIDGE. The non-FIPS algorithms are detailed in Table 5.

Table 4: FIPS Approved Algorithms

Algorithm	Cert #	Implementation	Operational Environment	Val Date	Modes/States/Key sizes/ Description/Notes
AES	852	Fortress Secure Bridge Algorithms	Broadcom MIPS Processor	8/28/2008	ECB(e/d; 128,192,256); CBC(e/d; 128,192,256)
AES	389	FC-X Algorithms	Xilinx Spartan FPGA	5/12/2006	CBC(e/d; 128,192,256)
AES	853	Fortress Secure Bridge Algorithms (SSL)	Broadcom MIPS Processor	8/28/2008	ECB(e/d; 128,192,256); CBC(e/d; 128,192,256); CFB8(e/d; 128,192,256); CFB128(e/d; 128,192,256); OFB(e/d; 128,192,256)
TDES	703	Fortress Secure Bridge Algorithms (SSL)	Broadcom MIPS Processor	8/28/2008	TECB(e/d; KO 1,2); TCBC(e/d; KO 1,2); TCFB8(e/d; KO 1,2); TCFB64(e/d; KO 1,2); TOFB(e/d; KO 1,2)
RSA	488	Fortress Secure Bridge Algorithms (SSL)	Broadcom MIPS Processor	3/12/2009	ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-1
SHA	845	Fortress Secure Bridge Algorithms	Broadcom MIPS Processor	8/28/2008	SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)
SHA-1	721	Fortress SWAB FPGA Algorithms	Xilinx Spartan FPGA	1/17/2008	SHA-1 (BYTE-only)
SHA-256 **SHA-512**	722	Fortress SWAB SHS and HMAC	Xilinx Spartan FPGA	1/17/2008	SHA-256 (BYTE-only) SHA-512 (BYTE-only)
SHA-384	715	Fortress SWAB SHS-384 Algorithm	Xilinx Spartan FPGA	12/31/2007	SHA-384 (BYTE-only)
SHS	846	Fortress Secure Bridge Algorithms (SSL)	Broadcom MIPS Processor	8/28/2008	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)
HMAC	469	Fortress Secure Bridge Algorithms	Broadcom MIPS Processor	8/28/2008	HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS) SHS Cert#845 HMAC-SHA256 (Key Size Ranges Tested: KS=BS) SHS Cert#845 HMAC-SHA384 (Key Size Ranges Tested: KS=BS) SHS Cert#845 HMAC-SHA512 (Key Size Ranges Tested: KS=BS) SHSCert#845
HMAC	371	Fortress SWAB FPGA Algorithms	Xilinx Spartan FPGA	1/17/2008	HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) SHS HMAC-SHA384 (Key Size Ranges Tested: KS<BS) SHS
HMAC	569	Fortress Secure Bridge Algorithms (SSL)	Broadcom MIPS Processor	3/12/2009	HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS) SHS HMAC-SHA224 (Key Size Ranges Tested: KS=BS) SHS HMAC-SHA256 (Key Size Ranges Tested: KS=BS) SHS HMAC-SHA384 (Key Size Ranges Tested:

Algorithm	Cert #	Implementation	Operational Environment	Val Date	Modes/States/Key sizes/ Description/Notes
					KS=BS) SHS HMAC-SHA512 (Key Size Ranges Tested: KS=BS) SHS
ANSI X9.31 PRNG	487	Fortress Secure Bridge Algorithms	Broadcom MIPS Processor	8/28/2008	ANSI X9.31 PRNG [TDES-2Key];
ANSI X9.31 PRNG	189	FC-X Algorithms	Xilinx Spartan FPGA	1/17/2008	ANSI X9.31 PRNG [TDES-2Key];
ANSI X9.31 PRNG	488	Fortress Secure Bridge Algorithms (SSL)	Broadcom MIPS Processor	8/28/2008	ANSI X9.31 PRNG [TDES-2Key];

Table 5: 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 all ANSI X9.31 PRNGs**

1.12 Overall and Individual FIPS 140-2 Levels

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

Table 6: 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**

2.0 Identification and Authentication Policy

2.1 Roles

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

2.2 Services

The FC-X can be run in FIPS or non-FIPS mode. All services are available in both modes. The only service difference is that upon self-test failure the data output via the data output interface is not inhibited in non-FIPS mode. The following list summarizes the services:

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

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 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 crypto module will not accept new passwords that do not meet specified requirements. A Crypto Officer can utilize four

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

secure communication methods to access the crypto module, 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 Authentication Data for each of these roles are shown in Table 7.

Table 7: Authentication Data

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

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 BRIDGE, one on another BRIDGE or it can be an external Authentication Server like FreeRadius or Juniper's Steel Belted Radius Server that is running on a hardware Server platform

The service(s) available are determined by the BRIDGEs 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 BRIDGE requires that all variants of the Crypto Officer manually enter the password. Manual entry limits the number of attempts to eight per minute, therefore, the probability would be between one in (2^3)/(2^62)^8 and one in (2^3)/(2^92)^32 which is less than 1 in 10^5. The maximum number of login attempts can be set between 1 and 9 and lockout duration between 0 and 60 minutes.**
Maintenance		
Administrator		
MSP End User	Either 1/(1+1)^64 or 1/(1+1)^128 for a 8 or 16- byte Access ID respectively. 16-byte used in FIPS Mode	**User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Access ID this represents 120x10^6 password attempts per minute.** **The 2^64/120x10^6 ~ = 2^64/2^7x2^20 or a probability one in 2^37 which is better than 1 in 10^5 .**

3.0 Cryptographic keys and CSP

3.1 For MSP

The BRIDGE contains a number of cryptographic keys and Critical Security Parameters (CSP) for MSP as shown in Table 9.

Table 9: MSP Keys and CSPs

Key/CSP	Type	Generation	Storage	Use
Access ID **16 bytes (CSP)**	Seed	Generated by the Crypto Officer	Non Volatile Storage	**Authentication**
Static Private Key	Diffie-Hellman: 1024 or 2048 bits ECDH: 384 bits	Automatically Generated using the ANSI X9.31 PRNG.	Kept in RAM never stored on disk.	**Used with 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 the Diffie-Hellman or ECDH algorithms.	Kept in RAM never stored on disk.	**Sent to communicating Module in a packet.**
Static Secret Encryption Key	AES – 128,192, or 256 bit.	Automatically Generated using the Diffie-Hellman or ECDH algorithms.	Kept in RAM never stored on disk.	**Used to encrypt dynamic public key requests and responses over the wire.**
Dynamic Private Key	Diffie-Hellman: 1024 or 2048 bits ECDH: 384 bits	Automatically Generated using the ANSI X9.31 PRNG.	Kept in RAM never stored on disk.	**Used with 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 the Diffie-Hellman or ECDH algorithms.	Kept in RAM never stored on disk.	**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 the Diffie-Hellman or ECDH algorithms.	Kept in RAM never stored on disk.	**Used to encrypt all packets between two communicating Modules over the wire**
PRNG ANSI X9.31 Seed	Random Seeding information from the TRNG	Automatically Generated per seeding using the TRNG. A loop is started where the ANSI X9.31 PRNG is seeded with 64 bits from the TRNG each time through the loop.	Non Volatile Storage	**ANSI X9.31 PRNG output is used for MIPS cryptographic operations.**
PRNG ANSI X9.31 2-key 3DES	Internal 3DES Key (112 bits)	Automatically Generated per seeding Internal Key generate from the seed and seed key	Non Volatile Storage	**This is an internal key used for MIPS ANSI X9.31 PRNG.**
PRNG ANSI X9.31 Seed	Random Seeding information from the TRNG	Automatically Generated per seeding using the TRNG. A loop is started where the ANSI X9.31 PRNG is seeded with 64 bits from the TRNG each time through the loop.	Non Volatile Storage	**ANSI X9.31 PRNG output is used for FPGA cryptographic operations.**
PRNG ANSI X9.31 2-key 3DES	Internal 3DES Key (112 bits)	Automatically Generated per seeding Internal Key generate from the seed and seed key	Non Volatile Storage	**This is an internal key used for FPGA ANSI X9.31 PRNG.**

3.2 For SSL (TLS) and SSH

The SSL (TLS) protocol is used to establish a FIPS secured connection from a management workstation running a standard Internet Browser to either the BRIDGE's GUI or the CLI. The SSH protocol uses the cryptographic algorithms of the SSL protocol. The cryptographic keys for SSL (TLS) and SSH are shown in Table 10.

Table 10: SSL (TLS) and SSH Crypto Keys

Key	Key Type	Generation	Storage	Use
RSA Private Key **SSL**	RSA Key 2048 bit	Automatically Generated Seeded by Approved RNG	Kept in RAM never stored on disk.	**Used to encrypt data. for signature purposes.**
RSA Public Key **SSL**	RSA Key	Automatically Generated	Kept in RAM never stored on disk.	**Used to decrypt data for signature purposes**
DH Private Key **SSL & SSH**	Diffie-Hellman Key (1024 bits)	Pulled from ANSI X9.31 PRNG.	Kept in RAM never stored on disk.	**Used along to calculate the Pre-Master Secret from DH**
DH Public Key **SSL & SSH**	Diffie-Hellman Key (1024-bits)	Generated from the DH algorithm.	Kept in RAM never stored on disk.	**Used along to calculate the Pre-Master Secret from DH**
Key Block **SSL & SSH**	Generic Key Information	Automatically Generated by SSL Protocol	Kept in RAM never stored on disk.	**Generated for the AES encryption key or the RSA public/private.**
Secret Encryption Key (SSH and SSL Session Key)	AES Key 128, 192, 256 bit	Automatically taken from the Key Block depending on Key Size	Kept in RAM never stored on disk.	**Encrypt Data Packets**
PRNG ANSI X9.31 Seed	Random Seeding information received from the TRNG	Automatically Generated per seeding using the TRNG. A loop is started where the ANSI X9.31 PRNG is seeded with 64 bits from the TRNG each time through the loop.	Non Volatile Storage	**ANSI X9.31 PRNG output is used for SSL cryptographic operations.**
PRNG ANSI X9.31 2-key 3DES	Internal 3DES Key (112 bits)	Automatically Generated per seeding Internal Key generate from the seed and seed key	Non Volatile Storage	**This is an internal key used for SSL ANSI X9.31 PRNG.**

3.3 Critical Security Parameters

There are other critical security parameters that are present in the BRIDGE as shown in Table 11.

Table 11: Other Keys and Critical Security Parameters

CSP	Type	Generation	Storage	Use
Administrator Password	Password	8 to 16 Characters, entered by the Administrator Crypto Officer	Non Volatile Storage	**To authenticate this Crypto Officer**
Log Viewer Password	Password	8 to 16 Characters, entered by the Administrator or Log Viewer Crypto Officer	Non Volatile Storage	**To authenticate this Crypto Officer**
Maintenance Password	Password	8 to 16 Characters, entered by the Administrator or Maintenance Crypto Officer	Non Volatile Storage	**To authenticate this Crypto Officer**
SNMPV3 Authentication Pass phrase	Pass phrase	8 to 64 Characters Entered by Administrative Crypto-Officer	Non Volatile Storage	**To authenticate the use of SNMPV3**
Upgrade Key	RSA Public Key	Public RSA key generated external to the module using approved FIPS key generation methods. Hardcoded.	Non Volatile Storage	**Used to decrypt the Hash value that is attached to the upgrade package**
Load Key	RSA Public Key	Public RSA key generated external to the module using approved FIPS key generation methods. Hardcoded.	Non Volatile Storage	**Used to decrypt the Hash value that is attached to the load package**
HMAC Key	SSL	Generated within the SSL package	Non Volatile Storage	**SSL module integrity** **SSL code integrity** **SSL message integrity**

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 BRIDGE and end users can use cryptographic services in both FIPS and non-FIPS mode of operation as shown in Table 12.

Table 12: Roles each Service is authorized to Perform

Roles/Service	Encryption Services	Show Status	View Log	Write Configuration (including Bypass, Setting FIPS Mode)	Read Configuration	Diagnostic Services including self tests	Write Password	Upgrade Services	Zeroization
Log Viewer			X				X		
Maintenance		X	X		X	X	X		
Administrator		X	X	X	X	X	X[5]	X	**X**
MSP End User	X								

4.2 Access to Keys or CSPs

The BRIDGE doesn't allow the access of encryption keys and most critical security parameters. These are protected within the operating environment. The BRIDGE does allow the configuration of some important parameters and passwords as detailed in Table 13.

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

Table 13: Access to Keys or CSPs

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

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

4.3 Zeroization

All keys and Critical Security Parameters (CSP)s are stored in a database and zeroed on system reset.

Table 14: Defaults and Zeroization

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

4.4 Upgrades

4.4.1 Introduction

The BRIDGE must be upgraded in FIPS mode to maintain FIPS 140-2 validation. The loaded firmware must also be validated. The Upgrade packaged is downloaded from a workstation via using the GUI or CLI. The upgrade is integrity checked and stored on the internal flash and booted. The previous image is kept stored on flash and can be selected as the boot image in case of problems with the upgrade image.

4.4.2 Upgrade Firmware

Fortress Technologies regularly releases updated versions of the software to add new features, improve functionality and/or fix known bugs. The distribution of this firmware is discussed in section 5.3.

4.4.3 Integrity of the Upgrade BRIDGE Image

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

5.0 Physical Securty Policy

5.1 Tamper Evidence Application

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

5.2 Tamper Evidence Inspections

The Firmware is installed by Fortress Technologies on a production-quality, FCC certified hardware device, which also define the physical boundary. All hardware platforms are or will be manufactured to meet FIPS 140-2, L2 requirements. Table 15 details the recommended physical security activities that should be carried out by the Crypto Officer.

Table 15: 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 BRIDGE from service.**
Overall physical condition of the BRIDGE	Daily	**Inspect all cable connections and the BRIDGE's overall condition. If any discrepancy found, correct and test the system for correct operation or remove BRIDGE from service.**

Figure 3: Position of Intrusion Detection Screws

5.3 Hardware and Firmware Distribution

Fortress Technologies, Inc. is careful when distributing and delivering new hardware and updated firmware to customers. All firmware is shipped from the Fortress facility in Oldsmar, Florida or Westford, Massachusetts to either a Fortress employee or an approved customer contact via a commercial package service. The firmware is never put

on a company server or Web site for downloading. The firmware is integrity protected so no altering of the code can occur if the media was highjack during shipment. The integrity of the firmware is checked when the new update is being loaded on the FC-X. The only user that is allowed to install an update is a valid Crypto Officer Administrator that is successfully logged on the FC-X. The company believes that these steps will help keep the firmware secure.

6.0 Firmware Security

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

7.0 Operating System Security

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

8.0 FIPS Self Tests

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

Table 16: Self Tests

Test	Description	MSP Broadcom MIPS Processor	MSP Xilinx Spartan FPGA	SSL Broadcom MIPS Processor
Power Up Test				
AES Known Answer Test (KAT) Note: For all lengths, CBC and ECB modes	A known answer test is performed	√	√	√
RSA KAT	A known answer test is performed	√		√
RNG (all RNGs)	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. A SHA-1 (SSL) digest is taken of the Upgrade Image and encrypted using RSA (SSL) with a Private Key. This encrypted hash is appended to the image. After the image is loaded, the BRIDGE uses the corresponding Public Key to decrypt this Hash and will compare that Hash to another it will do on the image. If they match the integrity is verified.	√		√
Elliptical Curve Test	A known answer test is performed	√		
Conditional Tests				
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. This algorithm uses a Public/Private Key Pair. A SHA-1 (SSL) digest is taken of the Upgrade Image and encrypted using RSA (SSL) using a Private Key. This encrypted hash is appended to the image. After the image is downloaded, the BRIDGE uses the corresponding Public Key to decrypt this Hash and will compare that Hash to another it will do on the image. If they match the integrity is verified.	√		
Duplicate Entry Test	The value is entered twice and compared for accuracy.	√		

Test	Description	MSP Broadcom MIPS Processor	MSP Xilinx Spartan FPGA	SSL Broadcom MIPS Processor
RNG Test **(All RNGs)**	**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	**When a MAC lookup table entry changes, the bypass test tests whether clear packets can be sent into the encrypted zone o r not.**	√		√
Bypass Mechanism Test	**This will do a integrity test on the configurable values that are used to trigger the FC-X to allow or not allow clear text packets to pass through the FC-X.**	√		√

9.0 Security Policy for Mitigation of Other Attacks Policy

No special mechanisms are built in the BRIDGE; 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. Dynamic Secret Encryption Key is changed at least once every 24 hours, with 4 hours being the factory default duration: Mitigates key discovery.
2. 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. Key exchanges after the first Diffie-Hellman exchange are encrypted: *Mitigates encryption key sniffing by hackers.*
4. Compression and encryption of header information inside of the frame, making it impossible to guess. MSP, SSL (TLS) or SSH 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. 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 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.

10.0 EMI/EMC

All models of the 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 BRIDGE'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 BRIDGE's and the customer's network(s) must operate. In addition, the customer systems are expected to be upgraded as needed to contain appropriate security tools to enforce the internal security policy.

11.1 FIPS Mode

FIPS Mode Requirements:

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

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

The BRIDGE's 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.

11.2 Alternating BYPASS Mode

The BRIDGE may be configured to allow cleartext traffic in the encrypted zone in FIPS mode. The BRIDGE will support alternating Bypass since it allows both clear text and encrypted data on the same interface.

The two actions needed to invoke alternating Bypass are:

- Configure a Trusted Device/AP and Save the settings, or;
- Enable 802.1X Authentication and Save the settings;

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

12.0 Maintenance Issues

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