Non-Proprietary Security Policy for the FIPS 140-2 Level 2 Validated Fortress Security Controller (FC-*X*)

November 2006

Prepared by the Fortress Technologies, Inc.
Government Technology Group
4023 Tampa Rd. Suite 2000. Oldsmar, FL 34677

Document Version 1.10

Contents

List of Figures and Tables

1.0 SUMMARY

This security policy of Fortress Technologies, Inc., for the FIPS 140-2 security level 2 validated Fortress Security Controller (FC-*X)*, defines general rules, regulations, and practices under which the Fortress Security Controller (FC-*X)* was designed and developed and for its correct and safe 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.

The product name: Fortress Security Controller (FC-*X)* hereafter referred to as FC-*X*. Here the -*X* suffix indicates the number of active devices served by the module as listed in Table 1.

Table 1: Summary of the FC-*X* Configurations

Module Configuration	Maximum Active Devices (*)
FC-250	500
FC-500	1000
FC-1500	3300

(*): Concurrently connected Secure Clients, Trusted Devices, access points and Guests

The number of clients i.e. the value of "*X*" can be changed with the licensed "key" provided by the Fortress Technologies, Inc. The module's selected configuration is displayed by the LCD on the front of the FC-*X* hardware.

Firmware: FC-*X* 4.0.3

Hardware: FC-*X*

The cryptographic boundary of the FC-*X* is the self-contained compiled code that is installed at the point of manufacture into production-quality compliant FC-*X* computer hardware. The physical boundary is the FC-*X* hardware platform on which the module firmware component is installed. This firmware and computer hardware system operates as an *electronic encryption device* designed to prevent unauthorized access to data transferred across a wireless network. It provides strong encryption (AES) and advanced security protocols.

The FC-*X* encrypts and decrypts traffic transmitted on the network in FIPS mode, protecting all clients "behind" it on a protected network. Only authorized personnel, the Crypto Officer, can log into the module and set up the mode of operation: FIPS or normal. The default mode of operation is FIPS.

The FC-*X* operates at the datalink, (also known as MAC) layer of the OSI model. The security functionalities are implemented without human intervention to prevent any chance of human error.

The FC-*X* requires no special configuration for individual network applications. The product operates with minimal intervention from the user. It secures communication within LANs, WANs, and WLANs.

The FC-*X* offers point-to-point-encrypted communication for the computer and Local Area Network (LAN) or Wireless LAN (WLAN) it protects. The FC-*X* encrypts outgoing data from a

client device and decrypts incoming data from networked computers located at different sites. Two or more FC-*X* s can also communicate with each other directly. Typical applications of the FC-*X*s are shown in Figures 1 and 2.

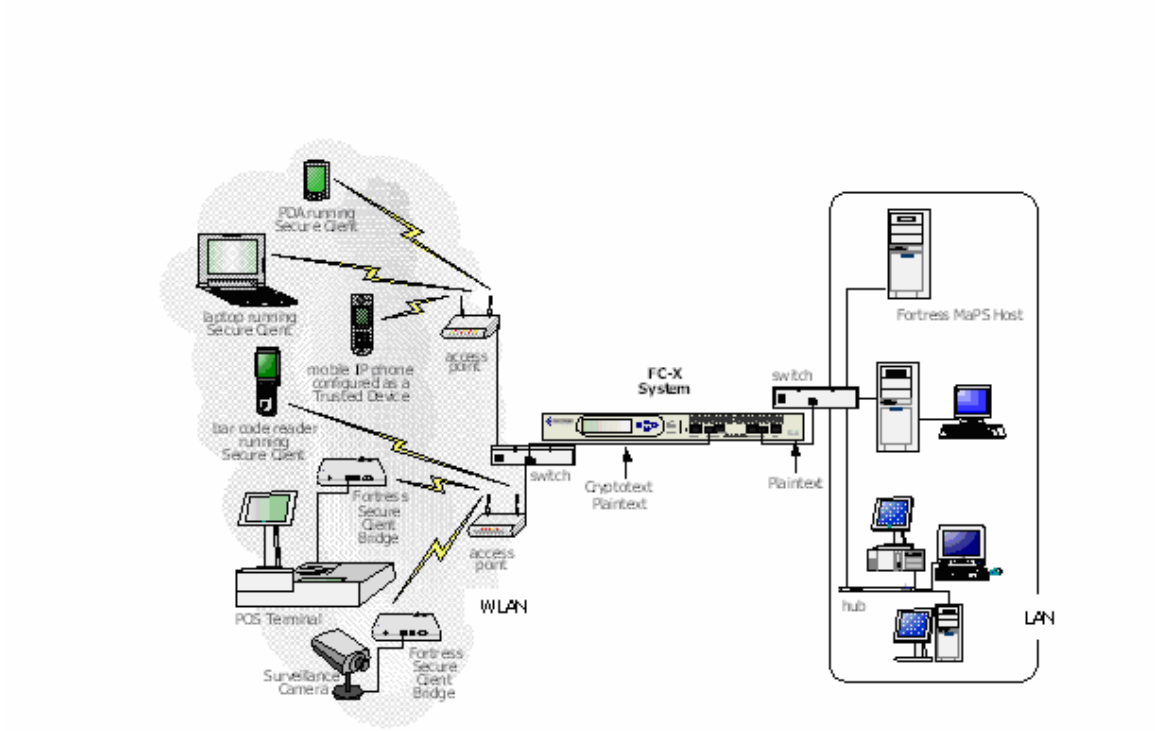

Figure 1: Example Configuration of FC-*X* in a WAN

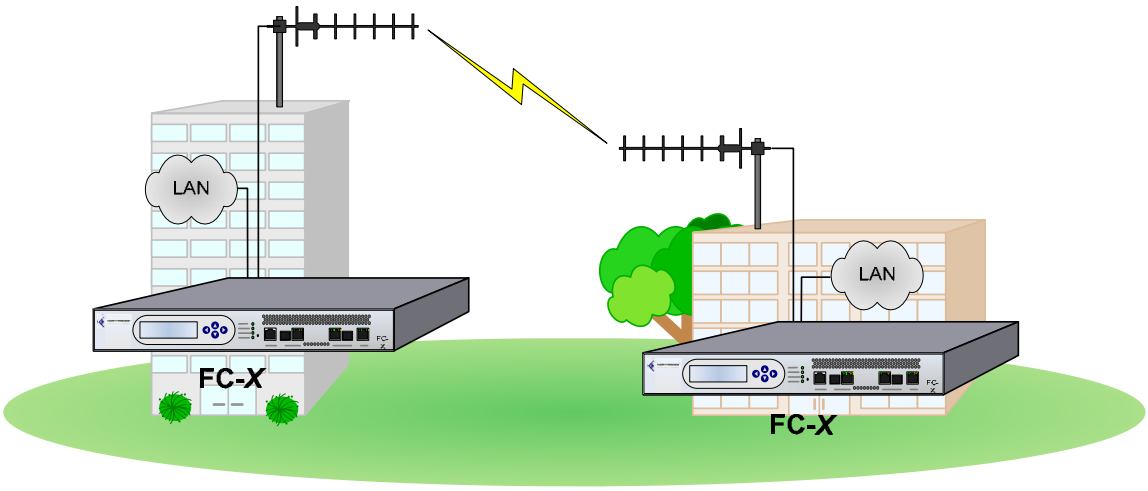

Figure 2: Example Communication Layout of two FC-*X* s

2.0 The FC-*X* Security Features

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

2.1 The FC-*X* Cryptographic Firmware

The following security design concepts were applied to the FC-*X*:

1. Use of a network-specific access ID assures that only FC-*X* units using this same unique value can become a configured partner.
2. The FC-*X* uses FIPS-approved and non-approved security functions as listed in Table 2 (FIPS-approved security Functions) and Table 3 (non-approved security functions).
3. The device automatically performs all applicable self-tests at power-up, conditionally, or as initiated by the cryptographic officer.
4. The FC-*X* enforces strong authentication of communicating parties.
5. The FC-*X* applies strong authentication of the origin of the packets.
6. The dynamic session key is changed at least once every 24 hours, with 4 hours being the factory default duration.
7. All key exchanges are encrypted with 256–key AES.
8. Data in transit is integrity checked.
9. Header information is compressed and encrypted inside of the frame, making it impossible to guess. Use of strong encryption further protects the information. Any bit flipping to try to change the IP address of the frame would be useless in this frame.
10. Encryption happens at the datalink layer so that all network layer information is hidden.
11. No encryption keys are stored permanently in the module.
12. All firmware is stored in executable format in the module.
13. Tamper evident hardware.
14. Plaintext data transfer is selectable by the System Administrator, (Crypto-Officer) only with trusted clients.

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. The wLLS builds upon the proven security architecture of Fortress Technologies Secure Packet Shield™ (SPS) 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 AES 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 FC-*X* requires no special configuration for individual network applications, other than to change certain security settings, such as the password and the access ID for the device, to ensure that each customer has unique parameters that must be met for access. The FC-*X* performs role-

based authentication.

3.0 Module Interfaces

The FC-*X* cryptographic module's physical interfaces are listed here and shown in Figure 3.

The FC-*X* hardware module physical/external I/O ports are:

- Copper Ethernet Ports (10/100/1000BT) - 3 Ports
- SFP Pluggable Ethernet Ports (1000BX) - 2 optional Ports (these ports replace the corresponding copper port when the optional optical SFP module is installed).
- Console RS232 Port (per Cisco RJ45 DTE standard).

The FC-*X* includes two logical interfaces for information flow: "Encrypted" for encrypted and plaintext data across a LAN or WLAN and "Unencrypted" for data sent as plaintext to clients on the protected wired network the host hardware is deployed on. The "Encrypted" interface connects the module to an access point or just removes AP, and to an unprotected LAN or WLAN; the "Unencrypted" interface connects the module to a protected network node. The FC-*X* does not allow plaintext transmission of cryptographic keys, or critical security parameters across a LAN or WLAN. The FC-*X* includes a console interface for use by the Crypto Officer in setting FIPS mode and entering other control data.

A 110 VAC power interface is provided at the back panel of the chassis.

A status output interface is provided using front panel LEDs and LCD display.

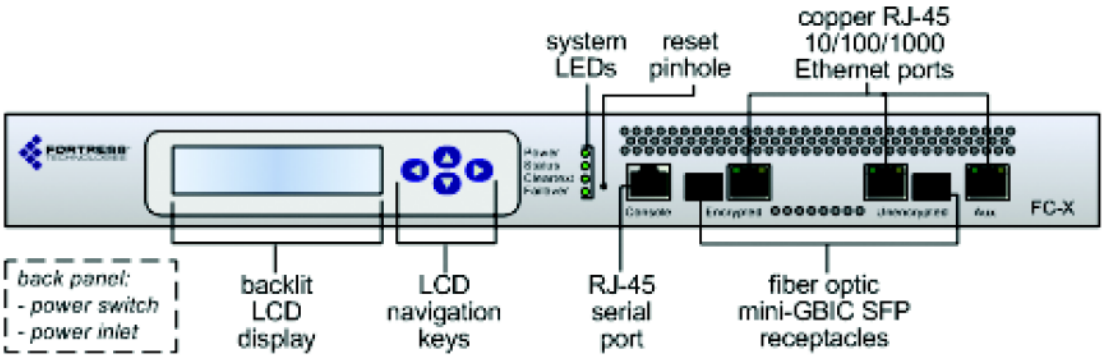

Figure 3: Front View of the FC-*X*

4.0 Identification and Authentication Policy

4.1 Roles

The FC-*X* employs role-based authentication, and supports the following roles:

- Crypto Officer
  - System Administrator; access through the FISH
  - Administrator; access through the WEB only
- Crypto Officer; Operator, access through the WEB only

- User; Client/end user, partner

The *Crypto-Officer* logs into the module and uses the Fortress Interface shell (FISH, physically connected to the module serial port) or AFWeb (GUI, HTTPS), performing the following tasks:

- Set the operational mode (FIPS or non-FIPS) of the module
- Configure the unique access ID
- Zeroize all cryptographic keys as needed
- Configure security settings
- Configure use of an authentication server
- Delete client database as needed
- Delete partner database as needed
- Reset configuration database
- Reset the FC-*X* to factory default settings, which also zeroizes cryptographic keys
- Perform diagnostics as explained in Section 11.0 and configuring the number of users.
- Enter the system date and time
- Enter the device serial number
- Ping a device on the network
- Trace a packet
- Clear the client MAC database
- Change the Operator role password
- Reboot the FC-*X*

The *Operator* cannot change any system or cryptographic settings and accesses the system only through the browser-based interface.

Users/Client, partner benefit from the FC-*X* cryptographic processing without manual intervention, thus eliminating any direct interaction with the module; the FC-*X* secures data transparently to users.

4.2 Authentication

User authentication is by a 16 hexadecimal digit Access ID (64-bit). Crypto-Officer authentication is by 8-character password (72^8). The probability of guessing a password is 1/72^8 which is less than the standard 1/10^6 success rate; the probability of guessing an Access ID is 2^64 which exceeds the standard 1/10^6 requirement. Cycle time for login is approximately 7.5 seconds; at this rate the possibility of guessing a password over a one minute interval exceeds the standards 1/10^5 attempts

5.0 Services

The following services are provided in the module:

- Show Status
- Self-tests
- Approved Security Functions
- Automatic Key Management
- Cryptographic Operations
- Plaintext transfer with trusted clients.

6.0 Self Tests

The FC-*X* conducts the following self-tests at power-up and conditionally as needed, when a module performs a particular function or operation. Self-tests can also be initiated periodically by the Crypto Officer during the normal operation of the module.

Power-Up Tests (BCM1250 Dual MIPS Integrated Processor)

- Cryptographic Algorithm Test: AES KAT, HMACKAT, SHS KAT, and RNG KAT
- Software/Firmware Integrity Test: HMAC
- Critical Functions Test. (Twenty crucial files are tested).

Power-Up Tests (FPGA)

- Cryptographic Algorithm Test: AES KAT, HMAC KAT, SHS KAT, and RNG KAT
- Software/Firmware Integrity Test: EDC (32-bit)

Conditional Test (BCM1250 Dual MIPS Integrated Processor)

- Continuous Random Number Generator test
- Per-Packet Bypass Test
- Bypass Test

Conditional Test (FPGA)

- Continuous Random Number Generator test

Failure of any self-test listed above puts the module in its error state, indicated by the Status LED and updates the log file.

7.0 Cryptographic Key Management

The FC-*X* itself automatically performs all cryptographic processing and key management functions.

7.1 Key Management

The FC-*X* uses seven cryptographic keys:

Key	**Key Type**	**Creation**
Module Secret Key (MSK)	AES - 256 bits.	Seeded with 8 bytes of Access ID and 8 bytes of Fortress pre-defined constant. Seed is SHA1 hashed and result sent to encryption engine to form the key.
Static Private Key (Diffie-Hellman)	512-bit Key	Seeded with 16 bytes of predefined constant. Seed is SHA-1 hashed and used per the Diffie-Hellman protocol.
Static Public Key (Diffie-Hellman)	512-bit Key	Above Diffie-Hellman Static Private Key is used to create this key per the Diffie-Hellman protocol.
Static Secret Encryption Key (AES)	AES - 256 bits.	Established through Diffie-Hellman Key Establishment
Dynamic Private Key (Diffie-Hellman)	512-bit Key	512 bits are generated by the ANSI X.9.31 RNG and used as this key.
Dynamic Public Key (Diffie-Hellman)	512-bit Key	Above Diffie-Hellman Dynamic Private Key is used to create this key per the Diffie-Hellman protocol.
Dynamic Session Key	AES - 128, 192,	Established through Diffie-Hellman Key Establishment

(Dynamic Common Secret Key) (AES)	or 256 bits.	

7.2 Key Storage

No encryption keys are stored permanently in the module's hardware. Public, private and session keys are stored in RAM. The Access ID is stored encrypted.

7.3 Zeroization of Keys

The keys of the FC-*X* are automatically zeroized when the system is turned off and created at every boot-up of the host hardware. All keys are all zeroized together and cannot be zeroized individually by either rebooting the module or by the reset command.

7.4 Protocol Support

The FC-*X* supports the Diffie-Hellman, SHS, and automatic creation methods.

7.5 Cryptographic Algorithms

The FC-*X* applies the following cryptographic algorithms:

Table 2: FIPS Algorithms Applied by the FC-*X*

FIPS Algorithms	NIST-FIPS Certificate number
AES (CBC, encrypt/decrypt; with key lengths of 128, 192, 256)	390, 389
SHS (SHA-1 (Byte))	465
HMAC	174
RNG: ANSI X9.31	190, 189

Table 3: Non-FIPS Algorithms Applied by the FC-*X*

Non-FIPS Algorithms
Diffie-Hellman (Key Agreement), MD5, Hardware RNG, RSA (non-compliant), SHS (non-compliant), HMAC (non-compliant)

NOTE: The module contains an implementation of SHS and HMAC on the resident MIPS processor and FPGA processor. Fortress Technologies did not perform algorithm testing for the HMAC and SHS on the FPGA processor. This is why the algorithms are listed as compliant and non-complaint. Only the SHS and HMAC associated with the referenced algorithm certificates (on the MIPS processor) are used for FIPS 140-2 relevant functionality.

8.0 Access Control Policy

The FC-*X* allows role-based access to user interfaces that access to the appropriate set of

management and status monitoring tools.

The Cryptographic Officer manages the cryptographic configuration of the FC-*X*. Operators can review module status. Because of the FC-*X* automates cryptographic processing, end users do not have to actively initiate cryptographic processing; the FC-*X* encrypts and decrypts data sent or received by users operating authenticated devices connected to the FC-*X*.

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.

Table 4: Role of the Crypto Officer (System Administrator (FISH) and Administrator (AFWEB))

Security Relevant Data Item	Show	Set	Enable	Disable	Add	Delete	Reboot	Password	Zeroize	Reset	Default Reset
MaPS/Access Control Server (non-FIPS only)	X	X	X	X						X	X
Access ID		X							X	X	X
Access point	X				X	X				X	X
GUI manager/agent (FISH Only)			X	X						X	X
Client (FISH only)						X			X	X	X
Config database										X	X
Crypto keys									X[2]	X	X
Cryptography algorithm/key length	X	X									
Device ID	X										
Device MAC	X										
FIPS mode	X	X	X	X			X			X	X
Hostname	X	X								X	X
IP Address	X	X								X	X
Netmask	X	X								X	X
Network gateway	X	X								X	X
Partner/Client (FISH only)						X			X	X	X
Rekey interval	X	X								X	X
Passwords: sysadm, admin & operator								X			X
Self Tests							X				
Serial number of Client	X	X									
SNMP			X	X							X
SSH (FISH only)			X	X							X

Table 5: Role of Operator at the AFWEB

Security Relevant Data Item	Show	Set	Delete	Reboot	Password
MaPS/Access Control Server (non-FIPS only)	X				
Access point	X				
Partners/Clients DB (Browser only)			X		
Cryptography algorithm	X				
Device ID	X				
Device MAC	X				
FIPS mode	X				
Hostname	X				
IP Address	X				
Netmask	X				
Network gateway	X				
Rekey interval	X				
Self Tests				X	
SNMP	X				

Table 6: Role of User/Client

Service	Execute	Read
Encryption	X	
Decryption	X	
Module Authentication	X	
Key Generation	X	
Tables		X
Packet Filter	X	
Packet Authentication	X	
Packet Integrity	X	

9.0 Physical Security Policy

The FC-*firmware* installed by Fortress Technologies on a production-quality, FCC-certified hardware device, the FC-*X*, which also defines the module's physical boundary. The FC-*X* is manufactured to meet FIPS 140-2, L2 requirements.

The FC-*X* 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. Table 7 lists recommended physical security related activities at the user's site.

Table 7: Recommended Physical Security Activities.

Physical Security Mechanism	Recommended Frequency of Inspection	Inspection Guidance
All chassis screws covered with epoxy coating.	Daily	Inspect screw heads for chipped epoxy material. If found, remove module from service.
Login the FC-*X*	Daily	Perform power-up test, check out the module's log file.
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.

10.0 Firmware Security Policy

Firmware components are not available to either the Crypto-officer or User. The operator has only limited access to module via the AFWEB. Firmware cannot be changed, nor can the firmware be partially upgraded. 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.

11.0 Operating System Security

The FC-*X* operates automatically after power-up and operates on limited non-modifiable 32 bit MIPS version of Linux 2.4.16. Therefore the operational environment of the FC-*X* is *non-modifiable*; it 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.

12.0 Mitigation of Other Attacks Policy

The cryptographic module is designed to mitigate several specific attacks above the FIPS defined functions, although no special mechanisms are built in the FC-*X* module. 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. The Crypto Officer can define this time interval: *Mitigates key discovery efforts.*
2. All key exchanges are encrypted: *Mitigates a hacker who might use a network analyzer device or a personnal computer utility called a sniffer to read the public keys that are being sent between two communicating peers.*
3. Normal or unauthenticated Diffie-Hellman Key Agreement Protocol can be vulnerable to "man in the middle" attack. A "man-in-the-middle" attack is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. In order to protect for this a dual Diffie Hellman key agreement scheme is used. This scheme totally hides the public keying information passed within the Diffie Hellman key exchanges messages from attackers by encrypting the key exchange messages, making it impossible an attacker to perform a "man in the middle" attack: *Mitigates "man-in-the-middle" attacks.*
4. Header information is compressed and encrypted inside of the frame, making it impossible to guess. Use of strong encryption further protects the information. Any bit flipping in this frame to try to change the IP address of the frame would be useless: *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 FC-*X* 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.

13.0 EMI/EMC

Fortress Technologies, Inc. installs the FC-*X* firmware only on the FC-*X* computer hardware, which is FCC-compliant and certified (Part 15, Subpart J, Class B).

14.0 Customer Security Policy Issues

Fortress Technologies, Inc. expects that, after the module's installation, any potential *customer* (government organization or commercial entity or division) *employ 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.

14.1 FIPS Mode

The Crypto Officer must select the module's operation mode with each client. He/she can select FIPS mode or Normal mode during module initialization. FIPS mode is the default mode of operation.

15.0 Maintenance Issues

The FC-*X* has no operator maintainable components. Inoperable modules must be returned to Fortress Technology, Inc. for repair.