FORTRESS™
TECHNOLOGIES

Non-Proprietary Security Policy for the FIPS 140-2 Level 2 Validated Fortress Security Controller, FC-*X* 4.1.1

June 2007

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

Document Version 1.3

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*) firmware version 4.1.1, defines general rules, regulations, and practices under which the 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, firmware version 4.1.1, hereafter referred to as FC-*X*. Here -*X* suffix indicates the number of active devices served by the module.

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 Vendor (operator configurable). The module's selected configuration is displayed by the LED on the front of the FC-*X* hardware.

NOTE: The module was tested in each of the three configurations.

Firmware: 4.1.1

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* using Mobile Security Protocol (MSP) operates at the datalink layer of the OSI model. The security functionalities are implemented without human intervention to prevent any chance of human error. It also supports routable Mobile Secure Protocol (rMSP) which allows the Crypto Officer the ability to configure Internet Protocol (IP) tunnels to a supported Fortress Gateway or Client thus allowing a secure datalink layer connection over an IP network.

The FC-*X* requires no special configuration for individual network applications unless rMSP is configured. 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 2 and 3.

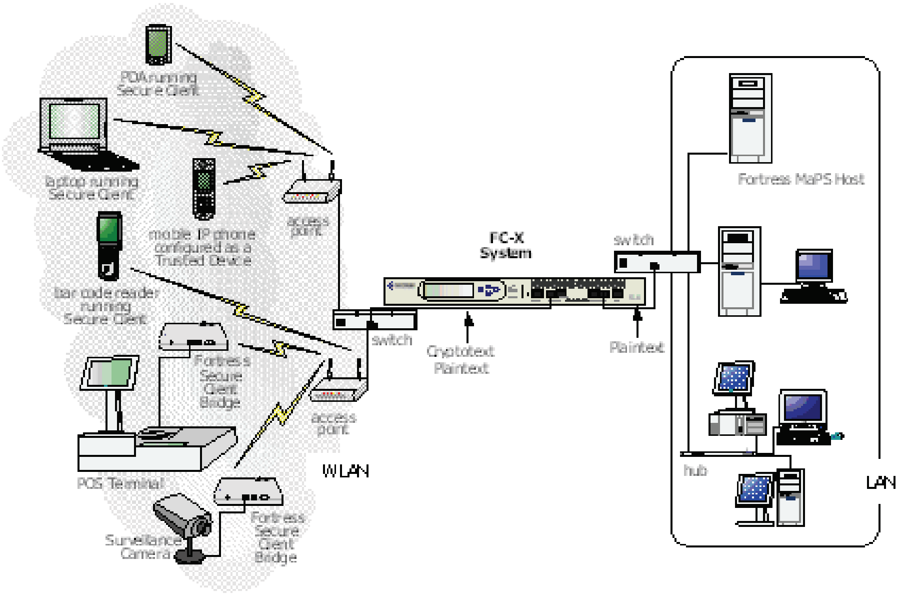

Figure 1: Example Configuration of FC-X Wireless Modules in a WAN

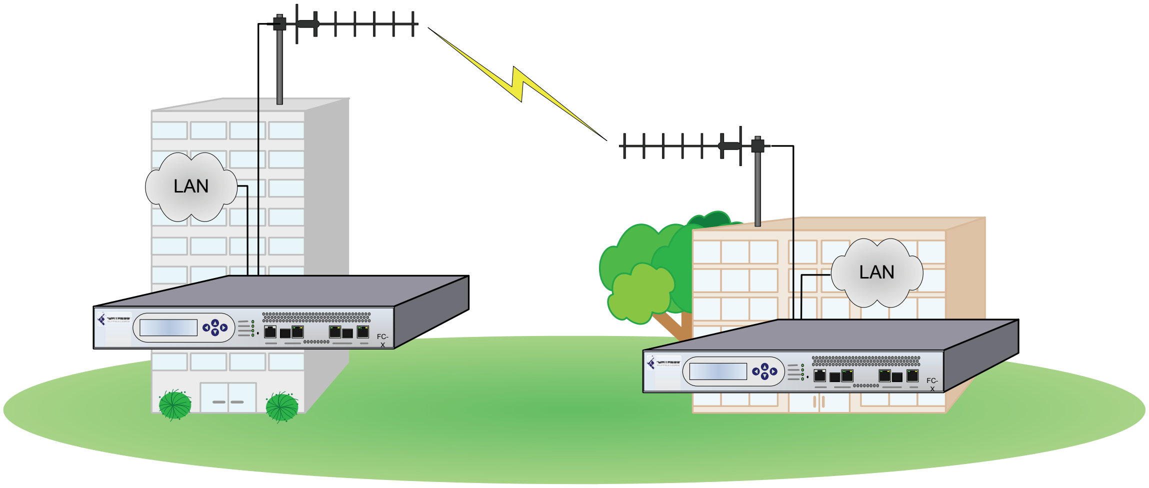

Figure 2: Example Communication Layout of two FC-Xs

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,* firmware version 4.1.1:

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 3 and Table 4.
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 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. 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. 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 4.

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.

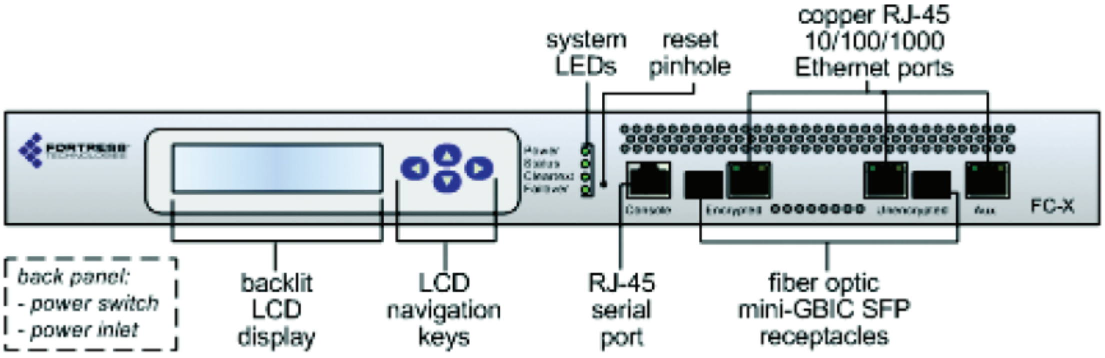

Figure 3: Front View of the FC-X

4.0 Identification and Authentication Policy

4.1 Roles

The FC-*X* employs role-based authentication, and, as shown in Table 1, supports two Roles: the Crypto Officer and User.

Table 1: Roles

Role	Sub-Role	Type Authentication	Logical Interface	Authentication Data
Crypto Officer	Administrator	Password of 10-16 Characters	*GUI*	*10-16 characters long, which are selectable from upper and lowercase letters and numbers, special characters and space are total 72 characters.*
	Operator	Same	*GUI*	*Same*
	System Administrator	Same	*CLI*	*Same*
User	End User	64-bits	*Data Input/Output*	*Access ID*

4.2 Services

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 has also been designed for ease of configuration and management for the Crypto Officer. Only a few services require configuration. Table 2 is the services that are supported on the FC-X.

Table 2: Services

Category	Service	Monitor	Change	Execute	Automatic
Communication	Bridging				X
	Tunneling (rMSP)				X
	Failover				X
Security Functions	Encrypt/Decrypt (MSP)				X
	Bypass				X
Self Tests	Crypto Algorithm Tests				X
	Firmware Integrity Check				X
	SHA1 and SHA256 HMAC Test				X
	Access ID Entry Test				X
	Continuous Rand Number Generator Test				X
	Bypass Test				X
Show Status	General Status, Statistics, Tracking and Logging	X			
Configuration	System Properties	X	X		
	Security and Authentication	X	X		
	Failover	X	X		
	Filters Rules and Policies	X	X		
	Routable MSP	X	X		
	Timeouts	X	X		
	SNMP	X	X		
	AP/Trusted Device Management (Bypass)	X	X		
	VLAN	X	X		
	Archive, Upgrade (non FIPS) and Boot	X	X		
	Select Normal or FIPS	X	X		
Diagnostics	Restart Gateway			X	
	Reset Connection or Factory Configuration			X	
	Generate diagnostics file			X	

4.3 Authentication Mechanisms

User authentication is by a 16 to 32 hexadecimal digit Access ID (64-bit – 128 bit). The probability of guessing an Access ID is 2^64 which exceeds the standard 1/10^6 requirement.

Crypto Officer authentication is by a minimum 10-character password with a ASCII library of 72 characters (72^10). The probability of guessing a password is 1/72^10 which is less than the standard 1/10^6 success rate. The 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 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).
- Bypass Test

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

Conditional Test (FPGA)

- Continuous Random Number Generator test

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

6.0 Cryptographic Key Management

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

6.1 Key Management

The FC-*X* uses eleven cryptographic keys:

Key	Key Type	Notes
Module Secret Key (MSK)	AES - 256 bits.	N/A
Static Private Key (Diffie-Hellman)	512-bit Diffie-Hellman Intermediate value	Not for use in FIPS mode
	1024-bit, 1538-bit, or 2048-bit Diffie-Hellman Intermediate value	N/A
Static Public Key (Diffie-Hellman)	512-bit Diffie-Hellman Intermediate value	Not for use in FIPS mode
	1024-bit, 1538-bit, or 2048-bit Diffie-Hellman Intermediate value	N/A
Static Secret Encryption Key (AES)	AES - 256 bits.	N/A
Dynamic Private Key (Diffie-Hellman)	512-bit Diffie-Hellman Intermediate value	Not for use in FIPS mode
	1024-bit, 1538-bit, or 2048-bit Diffie-Hellman Intermediate value	N/A
Dynamic Public Key (Diffie-Hellman)	512-bit Diffie-Hellman Intermediate value	Not for use in FIPS mode
	1024-bit, 1538-bit, or 2048-bit Diffie-Hellman Intermediate value	N/A
Dynamic Session Key (Dynamic Common Secret Key) (AES)	AES - 128, 192, or 256 bits.	N/A
Static Group Key	AES - 128, 192, or 256 bits.	N/A
Private Dynamic Group Key (Diffie-Hellman Intermediate value)	1024-bit Diffie-Hellman Intermediate value	N/A
Public Dynamic Group Key (Diffie-Hellman Intermediate value)	1024-bit Diffie-Hellman Intermediate value	N/A
Dynamic Group Key	AES - 128, 192, or 256 bits.	N/A

Note: 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 generates random numbers used for Diffie-Hellman. The Diffie-Hellman keys are configurable from 512 bits to 2048 bits providing a high degree of encryption strength (512 bit Diffie-Hellman not for use in FIPS-Mode). The AES key length is configurable to be 128, 192 or 256 bits.

6.2 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 AES encrypted.

6.3 Zeroization of Keys

The session keys of the FC-*X*, which are encrypted, are automatically zeroized when the system is turned off and created at every boot-up of the host hardware.

6.4 Cryptographic Algorithms

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

Table 3: FIPS Algorithms Applied by the FC-X

FIPS Algorithms	NIST-FIPS Certificate number
AES (CBC, encrypt/decrypt; with key lengths of 128, 192, 256)	389, 390
SHS (SHA-1 (Byte))	465
SHS (SHA-256 (Byte))	538
HMAC SHA-1	174
RNG: ANSI X9.31	189, 190

Table 4: Non-FIPS Algorithms Applied by the FC-X

Non-FIPS Algorithms
Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 112 bits of encryption strength; non-compliant less than 80-bits of encryption strength), MD5, RSA

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.

7.0 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 and operation of the FC-*X*. The FC-*X* automates cryptographic processing, therefore 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 Crypto Officer roles by the System Administrator require a password for authentication. The FC-X requires that the password must be 10-16 characters long, which are selectable from upper and lowercase letters and numbers, special characters and space. Table 5 shows the access controls rules for each of the roles.

Table 5: Access Control Rules

Role	Sub role	Logical Interface	Rules
Crypto Officer	Administrator	GUI	Show Status
			Monitor Configuration
			Change Configuration
			Execute Diagnostics
Crypto Officer	Operator	GUI	Show Status
			Monitor Configuration
			Execute Diagnostics
Crypto Officer	Systems Administrator	CLI	Show Status
			Monitor Configuration
			Change Configuration
			Execute Diagnostics
User		Data Input/Output	Encrypt/Decrypt
			Bypass

8.0 Physical Security Policy

The FC-*X* firmware (version 4.1.1) is 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, Level 2 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 6 lists recommended physical security related activities at the user's site.

Table 6: 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.
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.

9.0 Software Security Policy

Software and firmware components are not available to either the Crypto Officer or User. The operator has only limited access to module via the Web GUI, CLI or SNMP. Firmware cannot be changed. 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.

10.0 Operating System Security

The FC-*X* operates automatically after power-up. The FC-*X* operates on a limited non-modifiable 32 bit MIPS version of Linux. Therefore the operational environment is *non-modifiable*, 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. Firmware cannot be loaded when operating in FIPS mode.

11.0 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. 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. 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.

12.0 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).

13.0 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.

13.1 FIPS Mode

The Crypto Officer can select the module's operation mode. He/she can select FIPS mode or Normal Mode using the Web GUI or command line interface (CLI). FIPS mode is the default mode of operation. The Crypto Officer must disable Diffie-Hellman using 512-bit keys.

Diffie-Hellman using 512-bit intermediate values may not be used in FIPS-mode.

14.0 Maintenance Issues

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