Non-Proprietary Security Policy for the FIPS 140-2 Level 2 Validated AirFortress® Wireless Security Gateway Hardware Model AF2100 Firmware Version 2.5.6

(Document Version 2.2)

June 2007

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

Contents

List of Figures

List of Tables

SUMMARY

This Security Policy of Fortress Technologies, Inc., for the FIPS 140-2 validated AirFortress® Wireless Security Gateway, 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.

1.0 Introduction

This Security Policy defines all security rules under which the AirFortress® Wireless Security Gateway Cryptographic Module must operate and which it must enforce, including rules from relevant standards, such as FIPS 140-2. The module complies with all FIPS 140-2 level 2 requirements.

1.1 Identification

Hardware Model Number: AF2100

Firmware Version: V2.5.6

The AF2100 hardware models are referred to as the AirFortress® Wireless Security Gateway, or module, in this document. The module is a *multi-chip standalone electronic cryptographic encryption module*. The cryptographic boundary of the module is the hardware enclosure, which contains the self-contained compiled code installed at the point of manufacturing. This module operates as an *electronic encryption device* designed to prevent unauthorized access to data transferred across a wireless network. It provides strong encryption (Triple-DES and AES) and advanced security protocols.

The module encrypts and decrypts traffic transmitted on that network in FIPS mode, protecting all clients "behind" it on a protected network. Only authorized personnel can log into the module.

The module operates at the datalink layer of the OSI mode. The module 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 module 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 modules can also communicate with each other directly. A typical application of the module is shown in "Figure 1" and "Figure 2" below.

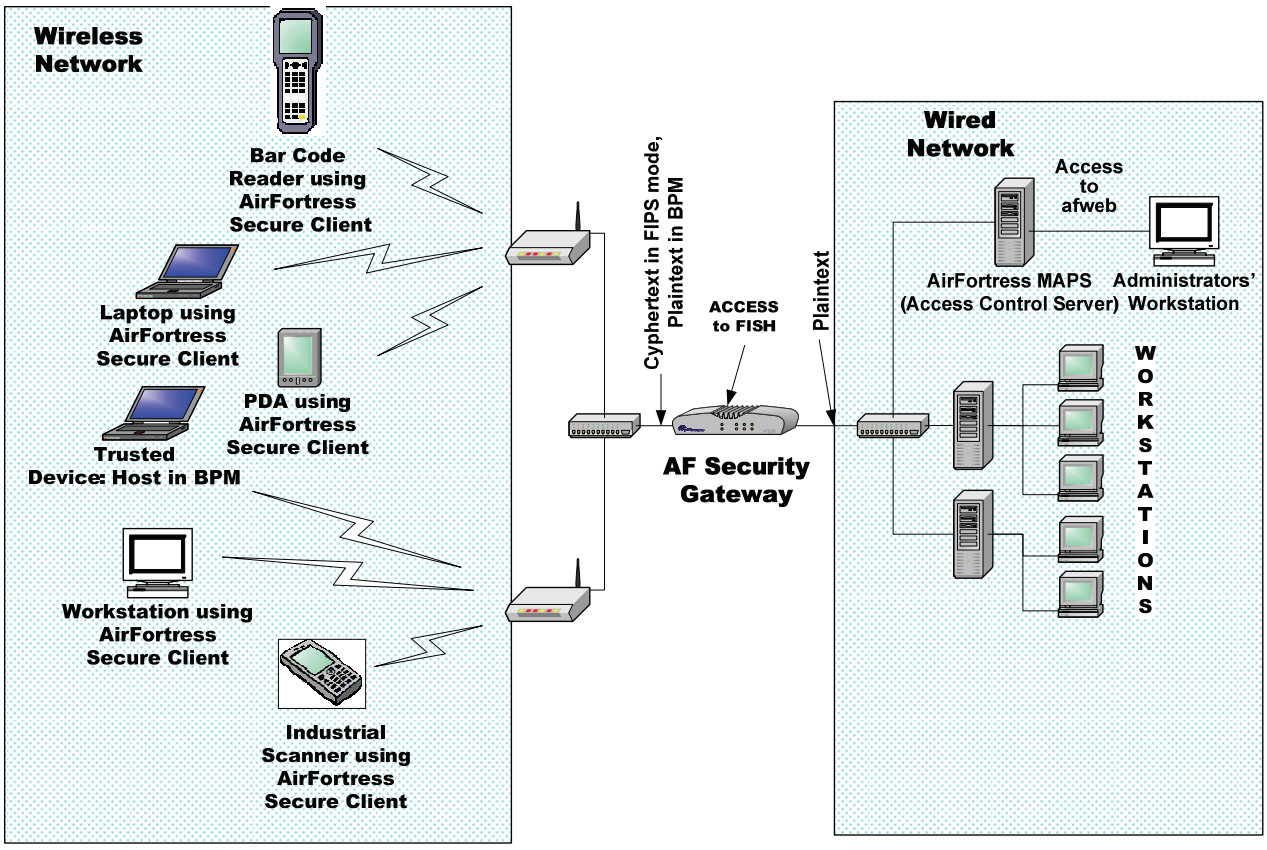

Figure 1: Example Configuration of AirFortress® Wireless Security Gateway in a WAN

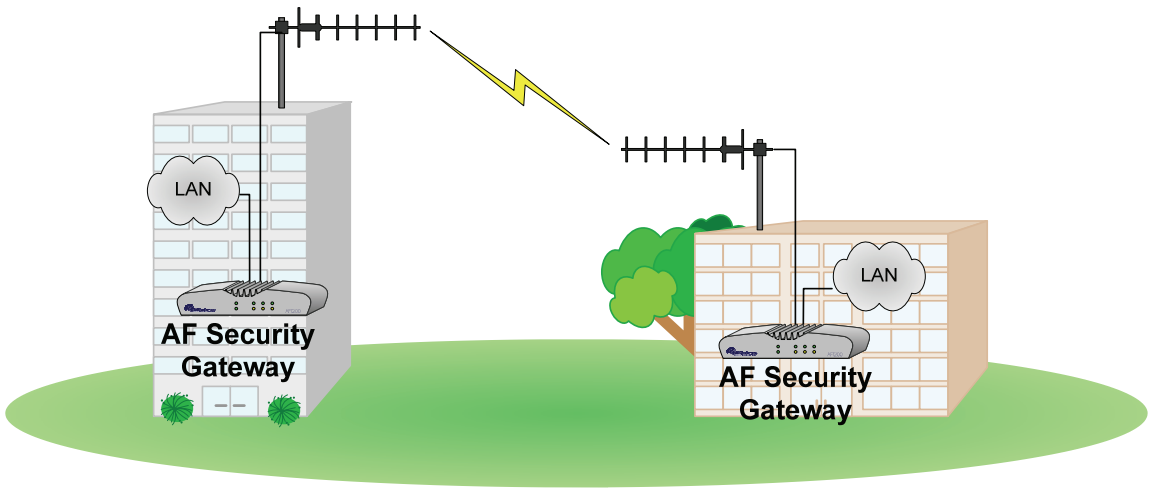

Figure 2: AirFortress® Wireless Security Gateway Communication Layout

2.0 Security Features

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

2.1 Cryptographic Module Design Concepts

The following security design concepts were applied to the AirFortress® Wireless Security Gateway:

1. Use FIPS-approved and NIST recommended cryptographic algorithms, such as Triple-DES and AES.
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. The module firmware is installed only in production grade, AF2100, FCC-compliant computer hardware at the customer's site or at Fortress Technologies' production facilities. This hardware meets all FIPS 140-2, Level 2 physical security 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 using FIPS-approved and NIST recommended cryptographic 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 module requires no special configuration for different network applications, although customers are encouraged to change certain security settings, such as, Crypto-Officer password and the access ID for the device, to ensure that each customer has unique parameters that must be met for access. The module allows role-based access to user interfaces that access the appropriate set of management and status monitoring tools. Direct console and browser access support Crypto-Officer tasks.

2.2 Module Interfaces

The module includes two logical interfaces for information flow, "Encrypted" for encrypted data in FIPS mode across a LAN or WLAN and "Unencrypted" for data sent as plaintext to clients on the protected wired network. These logical interfaces correspond with two separate network interface cards (NICs) provided by the hardware (hardware shown in "Figure 3" and "Figure 4"). The Network interface connects the module to an access point to an unprotected LAN or WLAN; the Client interface connects the module to a protected node for a network. Data sent and received through the Network interface to a connected access point are always encrypted; the module does not allow plaintext transmission of data, cryptographic keys, or critical security parameters across a LAN or WLAN

The AirFortress® Wireless Security Gateway includes a console interface for use by the Crypto-Officer in setting FIPS mode and the entering other control data and serves a status output interface along with the front panel LEDs on the host hardware.

Power Input: AF2100, 5 VDC

3.0 Identification and Authentication Policy

3.1 Roles

The module employs role-based authentication.

The module supports the following operator roles: Crypto-Officer (System Administrator and Administrator) and User. Users benefit from the cryptographic processing without manual intervention, thus eliminating any direct interaction with the module; the module secures data transparently to users.

The module supports two types of Crypto-Officer; System Administrator and Administrator.

3.1.1 Authentication

Authentication is described in the "Table 1" and "Table 2" below.

Table 1: Roles and Required Identification and Authentication

Role	Authentication Type	Authentication Data
User	Role Based	16h-digit Access ID
Crypto-Officer (System Administrator)	Role Based	8-Character Password
Crypto-Officer (Administrator)	Role Based	8-Character Password

3.1.2 Strength of Authentication

The crypto-Officer must assign each networked module a network specific Access ID at installation. This is used to authenticate the user. Crypto-Officer authentication for the first time by using a vendor provided password which is changed at installation.

Table 2: Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
16h-digit Access ID	One in 2^64
8-Character Password	One in 72^8

The probability of a random false acceptance for user authentication is one in 2^64 and for a Crypto-Officer is one in 72^8. Both exceed the required 1 in 10^6 requirements.

The module is designed to attempt eight User authentication attempts after power-on. If it fails to authenticate with the User, it enters a non-functioning idle state until a reset occurs, then another authentication attempt is made. Since the reset initialization is outside of the User's control, a User can make 8 attempts at authentication in a given one-minute interval. This leaves a probability of 8*(1/2)^64 = (2^3)/(2^64) = (1/2)^61 for a false acceptance in a one minute interval; greatly exceeding the 1 in 10^5 requirements.

For Crypto-Officer authentication, the cycle time for the module to deny access and present a fresh login interface is eight seconds. The number of login attempts available in a minute is seven and a half (7.5) login attempts per minute. At this rate, the possibility of guessing the password in a one-minute interval exceeds the 1 in 10^5 requirements of the standard.

4.0 Cryptographic Key Management

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

4.1 Cryptographic Keys

The module uses seven cryptographic keys:

- Module's Secret Key (DES, Triple-DES 192-bits, and AES 128-, 192-, 256-bits)
- Diffie-Hellman Static Private Key (512-bits)
- Diffie-Hellman Static Public Key (512-bits)
- Static Secret Encryption Key (DES, Triple-DES 192-bits, and AES 128-, 192-, 256-bits)
- Diffie-Hellman Dynamic Private Key (512-bits)
- Diffie-Hellman Dynamic Public Key (512 bits)
- Dynamic Session Key (DES, Triple-DES 192-bits, and AES 128-, 192-, 256-bits)

Notes:

- The public and private keys above refer to those used in the Diffie-Hellman key agreement protocol. The Diffie-Hellman key agreement methodology provides 56-bits of encryption strength.
- DES and 512-Bit Diffie-Hellman not for use in FIPS-mode.

An ANSI X9.31 A.2.4 Pseudo-Random Number Generator creates random numbers used with the key establishment algorithm (Diffie-Hellman). The ANSI X9.31 A.2.4 Pseudo-Random Number Generator (PRNG) is seeded using the non-Approved RNG (internal entropy pool).

4.2 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 and Device ID are permanently written in the program.

4.3 Zeroization of Keys

The encrypted session keys are automatically zeroized when the system is turned off and regenerated at every boot-up of the host hardware. All session keys can be zeroized manually if required.

4.4 Protocol Support

The module supports the Diffie-Hellman key agreement, and automatic rekeying.

4.5 Cryptographic Algorithms

The AirFortress® Wireless Security Gateway applies the following cryptographic algorithms:

Table 3: Algorithms Applied by the AirFortress® Wireless Security Gateway

FIPS Algorithms	NIST-FIPS Validation Number
AES (ECB, CBC, encrypt/decrypt; 128, 192, 256)	14
Triple-DES (CBC, encrypt/decrypt)	107
HMAC (SHA-1)	62
SHS	316
Non-FIPS Algorithms	
Diffie-Hellman (key agreement; Non-Compliant less than 80-bits of encryption strength), MD5, RSA (Non-Compliant), ANSI X9.31 RNG (Non-Compliant), non-Approved RNG, DES	

4.6 Self-Tests

The module 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, Triple-DES KAT, DES KAT, HMAC-SHA-1 KAT, SHS KAT, and RNG KAT
- Software/Firmware Integrity Test: HMAC (SHA-1)
- Critical Functions Test: HMAC of four critical binaries (nfd, nfwatcher, AFWEB, AFFISH)

B. Conditional Test

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

Notes:

- Failure of any self-test listed above puts the module in its error state.
- The "Firmware Load Test" is associated with the "Firmware Upgrade (firmware load)" service identified in "Table 4" below. Any non-validated firmware subsequently loaded and executed within the FIPS 140-2 validated cryptographic module invalidates the original validation.

5.0 Access Control Policy

The module allows role-based access to user interfaces that access to the appropriate set of management and status monitoring tools. Direct console access (via a non-networked device or GPC) supports System Administrator access, and a non-encrypted browser-based interface supports Administrator access.

The System Administrator manages the cryptographic configuration of the module. Administrators can review module status and manage system settings where appropriate but not cryptographic settings when the modules are operating in FIPS mode. Because the module automates cryptographic processing, end users do not have to actively initiate cryptographic processing; the module encrypts and decrypts data sent or received by users operating authenticated devices connected to the module. The module also supports a bypass capability that may be configured by the System Administrator.

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

Function/Service	Show	Set	Enable	Disable	Add	Delete	Reboot	Password	Zeroize	Reset	Default Reset
Access Control Server	X	X	X	X						X	X
Access ID		X							X	X	X
Access point	X				X	X				X	X
AFWEB			X	X						X	X
ARP	X										
Client DB (NF.cmc)						X			X	X	X
Config database										X[1]	X
Crypto keys									X[2]	X	X
Cryptography algorithm	X	X									
Device ID	X										
Device MAC	X										
FIPS mode			X	X						X	X
Hostname	X	X								X	X
Interface	X										
IP Address	X	X								X	X
Memory	X										
Netmask	X	X								X	X
Network gateway	X	X								X	X
Partner DB (nfdsdb.nfs)						X			X	X	X
Rekey interval	X	X								X	X
Role passwords								X			X
Self Tests							X				
Serial number	X	X									
SNMP (non-FIPS only)			X	X							X
Trusted database (bypass)	X				X	X				X	X
Firmware Upgrade (firmware load)					X	X					

[1]The `reset` command resets the configuration database except for the serial number, device ID, MAC address, cryptographic algorithm selected, and user passwords. The `default reset` command resets everything except for the serial number. All cryptographic keys are automatically recreated at the system reboot, and reset except the Module's Secret Key.

[2]When the system administrator logs in, cryptographic processing halts, which effectively zeroizes the keys.

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

Function/Service	Show	Set	Delete	Reboot	Password
Access Control Server	X				
Access point	X				
Client DB (NF.cmc)			X		
Cryptography algorithm	X				
Device ID	X				
Device MAC	X				
FIPS mode	X				
Hostname	X				
Interface	X				
IP Address	X				
Netmask	X				
Network gateway	X				
Rekey interval	X				
Role passwords					X[1]
Self Tests				X	
Serial number	X	X			
SNMP (non-FIPS only)	X				

[1]The administrator can only change the administrator password and not the system administrator password.

Table 6: Services Available to the User

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

6.0 Physical Security Policy

The AirFortress® Wireless Security Gateway firmware is installed by Fortress Technologies on a production-quality, FCC-certified AF2100 hardware devices, which are also define the module's physical boundary. The hardware is manufactured to meet FIPS 140-2, Level 2 requirements.

The host hardware 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 are covered with the material as shown in "Figure 3" and "Figure 4" below. "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 tampered, 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.

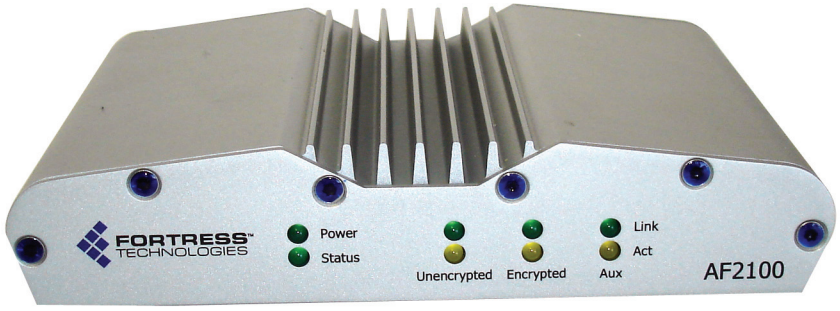

Figure 3: Front View of the AF2100 Hardware Showing the Blue Thread Locker

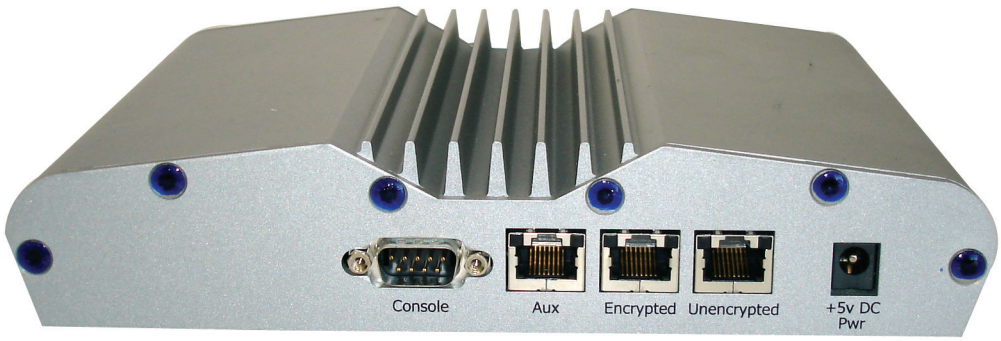

Figure 4: Back View of the AF2100 Hardware Showing the Blue Thread Locker

7.0 Firmware Security Policy

Firmware components are not available to either the Crypto-Officer. They have only limited access to module via the AFWEB or/and AFFISH tools. Firmware upgrades are permitted in FIPS mode and are subject to the Firmware Load Conditional Test. 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.

8.0 Operating System Security

The module operates automatically after power-up. The operating system is a limited non-modifiable version of Linux 2.4.16 that is installed with the module's firmware. User access to standard OS functions is 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.

9.0 Mitigation of Other Attacks Policy

The cryptographic module is designed to mitigate several specific attacks. Features, which 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.*

10.0 EMI/EMC

Fortress Technologies, Inc. installs the AirFortress™ Wireless Security Gateway Firmware only on computer hardware, which is FCC-compliant and certified: Part 15, Subpart J.

11.0 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.

11.1 FIPS Mode

The Crypto-Officer must select FIPS mode during module initialization. Set FIPS by using AFFISH to access the console port and then selecting FIPS enable. Once FIPS is enabled the prompt changes to "<FIPS>" and the AFWEB Interface reports "FIPS MODE ENABLED" as indicators.

12.0 Maintenance Issues

The AirFortress® Wireless Security Gateway has no operator maintainable components. Inoperable modules must be returned to the factory for repair.