Non-Proprietary Security Policy for the FIPS 140-2 Level 2 Validated AirFortress® Wireless Security Gateways

Hardware Models AF7500 and AF2100

(Document Version 2.3)

February 2008

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 Gateways, 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 Gateways cryptographic module must operate and which it must enforce, including rules from relevant standards such as FIPS. The module complies with all FIPS 140-2 level 2 requirements.

1.1 Identification

Hardware Model Number: AF2100, AF7500

Firmware Version: V3.1

The AirFortress® Wireless Security Gateways (AF7500 and AF2100 hardware models) are referred to as the AF Wireless Security Gateways or gateways or module, in this document. The module is a *hardware cryptographic module*, comprising *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 that is 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. The AF Wireless cryptographic module is designed to prevent unauthorized access to data transferred across a wireless network. It provides strong encryption (Triple-DES and AES) and advanced security protocols. DES encryption can no longer be used in FIPS mode.

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, the administrator, system administrator and operator (cryptographic officers) can log into the module.

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

The 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 cryptographic modules 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 cryptographic modules 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.

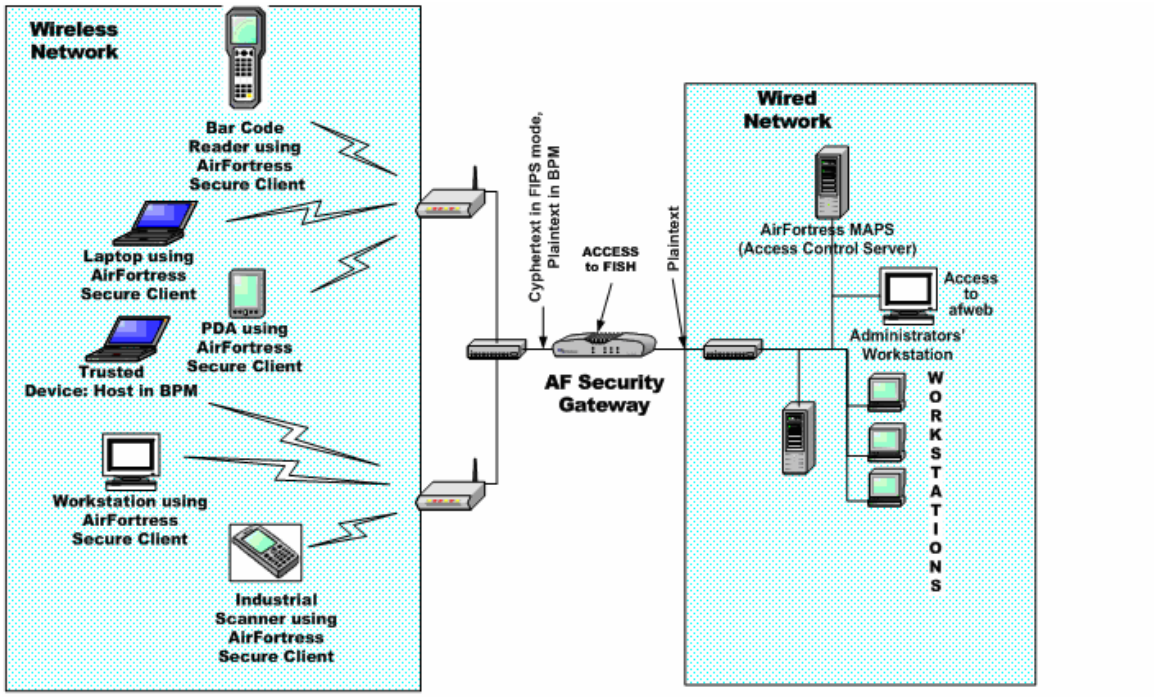

Figure 1: Example Configuration of AirFortress® Security Gateways in a WAN

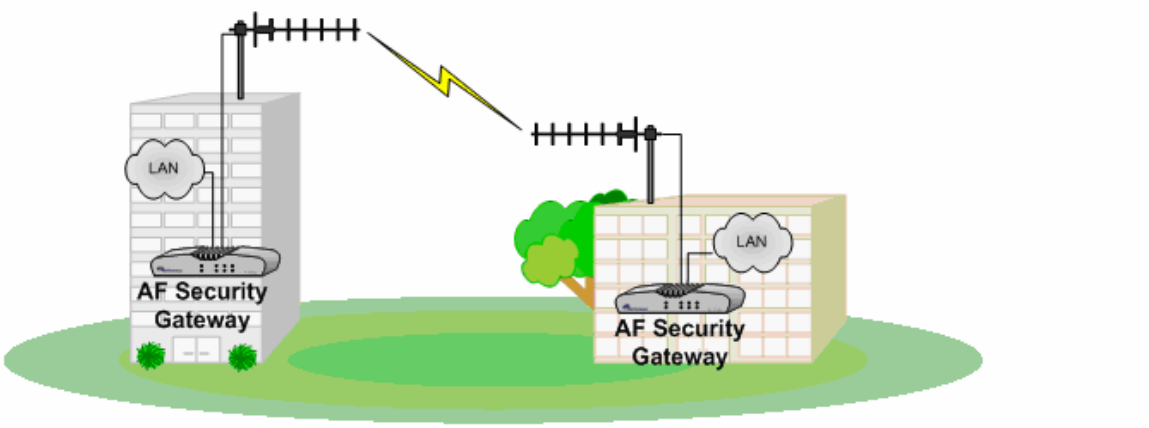

Figure 2: AirFortress® Security Gateways Communication Layout

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 The AF Wireless Security Gateways Cryptographic Module

The following security design concepts were applied to the AF Wireless Security Gateways:

1. Use strong, proven encryption solutions, Triple DES (TDES) 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® Management and Policy Server (MaPS).
4. The module firmware is installed only in production grade, AF7500 or AF2100, FCC-compliant computer hardware at the at Fortress Technologies' production facilities or as an upgrade at the customer's site. This hardware meets all FIPS 140-2 Level 2 requirements.

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

The module requires no special configuration for different network applications, although customers are encouraged to change certain security settings, such as the system administrator

password and the access ID for the device, to ensure that each customer has unique parameters that must be met for access. The module allows role-based access to user interfaces that access the appropriate set of management and status monitoring tools. Direct console access supports the majority of system administrator (cryptographic officer) tasks and a browser-based interface supports administrator access.

2.2 Module Interfaces

Physical Interfaces AF2100

1. 2 RJ-45 10/100 Mbps Ethernet ports
    a. Encrypted
    b. Unencrypted
2. 1 RJ-45 10/100 Aux Ethernet Port
3. 1 DB-9 Console Port
4. +V 5 DC Power Port
5. eight front-panel system LEDs
    a. Power - G
    b. Status Failover (Fail) - G
    c. Unencrypted Link - G
    d. Unencrypted Act - Y
    e. Encrypted Link - G
    f. Encrypted Act -Y
    g. Aux Link- G
    h. Aux Act – Y

Physical Interfaces AF7500

1. 2 RJ-45 10/100 Mbps Ethernet ports
    a. Encrypted
    b. Unencrypted
2. 1 RJ-45 10/100 Aux Ethernet Port
3. 1 DB-9 Console Port
4. 110/220 AC Power Port
5. eight front-panel system LEDs
    c. Power - G
    d. Status Failover (Fail) - G
    e. Unencrypted Link - G
    f. Unencrypted Act - Y
    g. Encrypted Link - G
    h. Encrypted Act -Y
    i. Aux Link- G
    j. Aux Act – Y

Logical Interfaces

1. Control Input
    a. WFWeb using SSL WEB Browser over an IP network through the Ethernet Port Encrypted or Unencrypted[1]

[1] Communications over WFWeb are not considered encrypted from a FIPS perspective.

   b. FISH using a directly connected terminal through the DB-9 serial port
   c. Fortress Interface Shell (FISH) using SSH over an IP network through the Ethernet Port Encrypted or Unencrypted[2]
2. Data Input/Output
   a. Encrypted
   b. Unencrypted
3. Status Output
   a. LED indicators as listed.
   b. Internal Audio buzzer (w/ software controllable volume possible),
   c. WFWeb with the attached browser.
   d. FISH in the attached monitor

Bypass mode is indicated as follows (over the status output):

AF2100: momentary off from the Status LED every few seconds.
AF7500: momentary off from the Status LED every few second accompanied by a double chirp from the module speaker every 20 seconds.

3.0 Identification and Authentication Policy

3.1 Roles

The module employs role-based authentication.

The module supports the following cryptographic officer roles:

- Administrator: Uses the wfWeb or MAPS to configure, monitor and perform diagnostics on the module.
- Operator: Uses the wfWeb to monitor and perform diagnostics on the module.
- System Administrator: Uses the FISH command line interface to configure, monitor and perform diagnostics on the module

The module support one user:

- End Users: This user benefits from the cryptographic processing without manual intervention, thus eliminating any direct interaction with the module; the module secures data transparently to users.

All tasks for the roles are summarized in table 4 through table 8.

3.1.1 Authentication

User authentication is by a 32 hexadecimal digit Access ID (128-bit). All Crypto-Officer role authentication is by 8-character password selectable from 72 keyboard characters.

3.1.2 Strength Of Authentication

The probability of a random false acceptance is:

[2] Communications through SSH are not considered encrypted from a FIPS perspective.

1. Crypto-Officer Role: The minimum character length for passwords is 8. Password characters can be either upper or lower-case letters, numbers, or some special characters (totaling 72 possible characters). Thus, the probability of random false acceptance is one in 72^8.
2. User Role: The AccessID is a 128-bit binary value. Thus, the probability of random false acceptance is one in 2^128.

Both of these probabilities exceed the one in 1,000,000 requirement.

For Crypto Officer authentication, the cycle time between authentication attempts is 8 seconds, allowing only 7.5 authentication attempts per minute. Given this cycle time and number of possible combinations (72^8), the requirement of one in 100,000 is met.

Similarly, for user authentication, an operator is allowed 8 attempts to establish a connection with Access ID. Given this and the number of possible combinations (128^8), the requirement of one in 100,000 is met

3.2 Services

The following services[3] are provided in the module:

- Show Status
  - Show status by LED located on the front of the AF2100 and AF7500
  - wfWeb
    - Allows the Monitoring of Partners
    - Show Log messages
  - FISH
    - Display Access Points connected
    - Display Clients
    - Display Partners
    - Display Roam
  - MAPS
    - Access the Fortress Only MIB (communications are plaintext)
- Perform Self Test
  - Power-Up Tests
    - Cryptographic Algorithm Test: AES KAT, Triple-DES KAT, HMAC-SHA-1 KAT, HMAC-SHA-256 KAT, and RNG KAT
    - Software/Firmware Integrity Test: HMAC-SHA-256
    - Critical Functions Test: None
  - Conditional Test
    - Continuous Random Number Generator test
    - Bypass Test
    - Firmware Load Test
- Perform Approved Security Functions
  - Encrypts and Decryptes packets:
    - Triple-DES (192 bit key)
    - AES (128 bit, 192 bit and 256 bit keys)
  - Create the module's keys

[3] This list just gives an overview of some of the services. Please refer to tables 4 through 8 for a complete list of services.

  - PRNG X9.31
  - HMAC-SHA1
  - HMAC-SHA256
  - Creating and maintaining tables
  - Reinitiating key exchange at user-specified intervals
  - Zeroizing keys if power to the module is turned off
- Other
  - Packet Compression

4.0 Cryptographic Key Management

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

4.1 Key Generation

The following values are generated using the module's ANSI X9.31 RNG:

- D-H Static Private Key 512-bits, 1024-bits and 2048-bits
- D-H Dynamic Private Key 512-bits, 1024-bits and 2048-bits

Notes:

- The public and private keys above refer to those used in the Diffie-Hellman key agreement protocol.

An ANSI X9.31 A.2.4 pseudo-random number generator generates random numbers used for keying the key establishment algorithm.

4.2 Key Storage

Only the module's HardKey is stored across power cycles. It is stored in the module's FLASH. Public, private and session keys are stored in RAM.

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 other information can be zeroized manually by entering 'reset default' in FISH. Zeroization of the HardKey is performed by upgrading the firmware of the module.

4.4 Protocol Support

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

4.5 Cryptographic Algorithms

The AF Wireless Security Gateways applies the following cryptographic algorithms:

Table 1: FIPS Approved Security Functions

Algorithms	NIST-FIPS Validation Number
AES (CBC, encrypt/decrypt; 128, 192, 256)	550
Triple-DES (CBC, encrypt/decrypt)	546
SHA-1 (Byte)	615
SHA-256	615
HMAC-SHA-1	291
HMAC-SHA-256	291
RNG (X9.31)	318

Table 2: Algorithms Allowed in FIPS Mode

Algorithm	Comments
Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength; non-compliant less than 80 bits of encryption strength)	Only 1024 or 2048 Diffie-Hellman can be used in FIPS mode.

Table 3: Excluded Security Functions

Algorithms	Comments
MD5, RSA	Not allowed in FIPS mode
DES	No longer accepted by FIPS as an approved security function

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. Browser-based interface and Direct console access supports the system tasks.

The administrator and system administrator (cryptographic officer roles) manages the cryptographic configuration of the module. The Operator (limited role cryptographic officer role) can review module status and manage system settings where appropriate but not cryptographic settings when the modules are operating in FIPS mode. Because of 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 following tables, defined by Fortress Technologies' Access Control Policy, show the authorized access and services tasks supported and allowed to each role within each product.

Table 4: Role of Administrator (WFWeb Cryptographic Officer)

Function/Service	Show	Select	Enable/ Disable	Enter/ Clear	Add/ Edit/ Delete Entry
System properties					
Network Properties	X			X	
Manage Gateways using MaPS	X			X	
System date and time	X			X	
Security Settings					
Security	X	X	X	X	
Change Access ID	X			X	
GUI access	X	X		X	
CLU access	X	X			
Authentication	X		X	X	
Failover					
Failover Setup	X	X			
Manual override	X			X	
SNMP					
Enable SNMP	X	X		X	
Configure SNMP traps	X			X	
AP/TD Management					
Access Management Rules	X			X	X
Access Point	X		X		
VLAN Settings					
VLAN mode	X	X		X	
VLAN map record	X				X
Archive Settings					
Archive System Settings				X	
Restore System Settings	X			X	
Upgrade					
Upgrade System	X			X	
View Log	X				
Ping		X			
Trace Route		X			
Restart Gateways		X			
Reset Connections		X			
Reset to Default Settings		X			

Generate File	X

Table 5: Role of Operator (WFWeb Cryptographic Officer)

Function/Service	Show	Select	Enable/ Disable	Enter/ Clear	Add/ Edit/ Delete Entry
System properties					
Network Properties	X				
Manage Gateways using MaPS	X				
System date and time	X				
Security Settings					
Security	X				
Change Access ID	X				
GUI access	X				
CLU access	X				
Authentication	X				
Failover					
Failover Setup	X				
Manual override	X				
SNMP					
Enable SNMP	X				
Configure SNMP traps	X				
AP/TD Management					
Access Management Rules	X				
Access Point	X				
VLAN Settings					
VLAN mode	X				
VLAN map record	X				
Archive Settings					
Archive System Settings					
Restore System Settings	X				
Upgrade					
Upgrade System	X				
View Log	X				
Ping		X			
Trace Route		X			
Restart Gateways		X			
Reset Connections		X			

Reset to Default Settings	X			

Table 6: Role of the System Administrator (FISH Cryptographic Officer)

Function/Service	Show	Set	Add/Del/Edit	Enable/Disable
Clock	X	X		
Devices	X	X		
Engine	X	X		
Maps	X	X		
Password		X		
Radius		X		
SNMP	X	X		
VLAN	X	X		
Uptime	X			
Add AP			X	
Add Trusted Device			X	
SNMP Trap			X	
Static Host Mac		X		
Traceroute		X		
Zero		X		
save		X		
AP	X			
Clients	X			
Mobile	X			
Netstat	X			
Partners	X			
Roam	X			
AFWeb				X
FIPS mode				X
MAPS				X
Radius				X
Silent Device				X
SNMP				X
SSH				X
Encrypted management				X
Clear text access				X

Guest Access	X

Table 7: Role of the Administrator (Crypto Officer using SNMP-V3)

MIB	Function	MIB	Function
afEnableLogMessages	Whether to enable the centralized logging or not.	afDisableAlarm	Setting this value to true will disable the audible alarm.
afResetClientMACDb	Setting this value to true will reset the database tracking all connected devices.Trying to read this object will return false or the value 2.	afRebootGateway	Setting this value to true will reboot the Gateways. Trying to read this object will return zero."
afMapsTunnelEncryption	The encryption type for the Maps Tunnel.	afRemoteLoggingLevel	The Remote Logging Level.
afDisconnectSessions	This object has the Mac addresses of the sessions to be disconnected. The value ff:ff:ff:ff:ff:ff indicates All sessions. Up to 10 Mac addresses can be specified separated by comma. The Mac address must be specified in the format 01:02:03:ab:cd:ef.	afTimeZoneOffset	The time difference between the Gateways' time zone and GMT in minutes.
afGuestAccessEnabled	Setting this value to true enables Guest devices to pass cleartext traffic after they have been authenticated by a MaPS server.	afClearTextAcccessEnabled	Setting this value to true enables all cleartext policy allowed, traffic to go through the gateways. Disabling this flag, or setting it to false, disables all cleartext traffic i.e. AP management traffic, Trusted device traffic including that traffic required by Guests to Authenticate.
afMODPsize	`The MODP size(s) allowed to be used.` Bit location * 256 = Modp size	afNewAccess	The string contains the New Access ID to be used by the gateways. This object is write only; Attempt to read this object will return Nothing.
afOldAccessID	The string contains the Old Access ID that is used by the gateways. This object is write only; Attempt to read this object will return Nothing.	`afPushAccessTimeWindow`	The time window value in seconds.
afPushAccessCmd	Setting this object to start(1) will push the new Access ID. The other 3 objects afNewAccessID, afOldAccessID and afPushAccessTimeWindow must be set before setting this. Once this object is set to start(1), it may be stopped by setting this object to	afPushAccessElapsedTime	This object indicates the elapsed time since the push access started.

	stop(2).		
rsNumber	This object indicates the number of rules present in the Gateways.	rsTable	This table contains the rules sent by Maps.
rsEntry	A row describing a given entry in the rules table.	rsIndex	Unique value for each rule.
resident	Unique global id in the Maps.	rsDescr	Textual description of the rule.
rsSrcPhysAddress	MAC address of the source host.	rsSrcNetAddress	IP address of the source host in string format. The net mask may be optionally specified. For example, 12.13.14.15/24. Up to 10 IP addresses can be specified separated by comma.
rsSrcPortNumbers	This can be a range or individual ports of upto 10 entries separated by commas. Range is separated by:. Examples: '30:40,45', 'Any','10,20'	rsDstPhysAddress	MAC address of the destination host in string format. Up to 10 MAC addresses can be specified separated by comma. The address must be specified in the format 01:02:03:ab:cd:ef.
rsDstNetAddress	IP address of the destination host in string format. The net mask may be optionally specified. For example, 12.13.14.15/24. Up to 10 IP addresses can be specified separated by comma.	rsDstPortNumbers	This can be a range or individual ports of upto 10 entries separated by commas. Range is separated by:. Examples: '30:40,45', 'Any','10,20'
rsTimeBasedIndex	A integer value that indicates which Time based rules are to be applied for this rule set.	rsCOSValue	A integer value range between 1-5 indicating the class of service for the rule set.
rsApplyInetRule	This object indicates whether the internet rule has to be applied for this rule set or not.	rsProtocol	This object indicates whether the ICMP packets are allowed for this device or not.
rsConnType	This object indicates the protocol.	rsAllowICMP	This object indicates whether this rule set is for an Encrypted connection (Secured devices and Users) OR for a Clear connection(Trusted devices, Guest Users and Static).
rsFlags	This is a flags field.	rsStatus	The status of this conceptual row. Only createAndGo(4), notInService(2), destroy(6) and acive(1) are supported.
tbNumber	This object indicates the number of time based templates present in the Gateways.	tbTable	This table contains the time based templates sent by Maps.
tbEntry	A row describing a given entry in the time based template table.	tbIndex	Unique value for each time based template.
tbIdent	Entry index for this template.	tbDayofWeek	The day(s) of the week.
tbStartTime	The time in minutes to specify when the rule will begin to act	tbEndTime	The time in minutes to specify when the rule will finish.
tbStatus	The status of this conceptual row. Only createAndGo(4),	tbType	The type of the time based template.

	notInService(2), destroy(6) and acive(1) are supported.		
irNumber	This object indicates the number of internet rules present in the Gateways.	irTable	This table contains the internet rules sent by Maps.
irEntry	A row describing a given entry in the internet rules table.	irIndex	Unique value for each internet rule.
irNetAddress	Network address to be denied	irNetMask	Network mask.
irStatus	The status of this conceptual row. Only createAndGo(4), notInService(2), destroy(6) and acive(1) are supported.		

Table 8: Role of User/Client

Function/Service	Show	Select	Enable/ Disable	Enter/Clear Value	Add/Delete Entry	Request
Use Profile	X	X				
Create Profile					X	
Enable Encryption		X				
Type of Encryption		X				
Access ID				X		
Trusted Device						X

The module contains the following security relevant data items (SRDI):

Table 9: Module Security Relevant Data Items

Security Relevant Data Item	SRDI Description	Storage Location
AccessID	A 128bit value used for authentication between the module and a peer module or a computer connecting with the Fortress Client software.	FLASH
Dynamic Secret Encryption Key	A Triple-DES or AES key used to encrypt End User data communications.	RAM
Common Static Encryption Key	A Triple-DES or AES key used to encrypt the key establishment process of the Dynamic Secret Encryption Key	RAM
Diffie-Hellman Dynamic Private Key	The Diffie-Hellman private value used to establish the Common Dynamic Encryption Key	RAM
Diffie-Hellman Static Private Key	Diffie-Hellman private value used to establish the Static Secret Encryption Key.	RAM
Static Group Key	This key is used to encrypt multicast transmissions until	RAM

	the Dynamic Group Key becomes active	
Dynamic Group Key	This key is used to encrypt user data broadcast/multicast transmissions.	RAM
Private Dynamic Group Key	The Diffie-Hellman value used to establish the Dynamic Group Key	RAM
HardKey	Used to encrypt failover communications transmitted over the "Aux" port. Also used as the HMAC key during the firmware load test.	FLASH
Administrator Password	The password that protects the “admin” user while logging on to the web interface.	FLASH
FISH Password	This is authentication data used to authenticate to the command line interface.	FLASH
Operator Password	This is authentication data used to authenticate to the "operator" user of the web interface.	FLASH
MaPS Password	A shared secret used for communication with a MAPS server.	FLASH
SNMP Password	The SNMP password is used for authentication to the SNMP server.	FLASH
RADIUS Password	A shared secret used for communication with a RADIUS server.	FLASH

The module allows controlled access to the SRDIs contained within it. The following table defines the access that an operator has to each SRDI while operating the module in a given role performing a specific service. The permissions are categorized as a set of four separate permissions: read, write, execute, delete. If no permission is listed, then an operator outside the module has no access to the SRDI.

Table 10: SRDI/Role/Service Policy

AF Wireless Security Gateways SRDI/Role/Service Access Policy	Security Relevant Data Item	AccessID	Dynamic Secret Encryption Key	Common Static Encryption Key	Diffie-Hellman Dynamic Private Key	Diffie-Hellman Static Private Key	Static Group Key	Dynamic Group Key	Private Dynamic Group Key	HardKey	Administrator Password	FISH Password	Operator Password	MaPS Password	SNMP Password	RADIUS Password
Role/Service																
User role																
Send Data Through the Module		x	x	x	x	x	x	x	x	x						
Crypto Officer Role																
GUI module configuration		w									w		w	w	w	w
GUI Diagnostics		x	x	x	x	x	x	x	x	x						
FISH module configuration		w										w	w	w	w	w
FISH Diagnostics		x	x	x	x	x	x	x	x	x						
SNMP module configuration		w											w	w		w
UpgradeFirmware		w	w	w	w	w	w	w	w	w / d	w	w	w	w	w	w
Zeroize command		d									d	d	d	d	d	d
Power cycle			d	d	d	d	d	d	d	4						

w = write

x = execute

d = delete

6.0 Physical Security Policy

The AF Wireless Security Gateways firmware is installed by Fortress Technologies on a production-quality, FCC-certified AF7500 and 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. The epoxy is applied during the manufacturing of the product by Fortress manufacturing personnel. All screws on the top panel are covered with the material as shown in Figures 3, 4, 5 and 6. Table 11 lists recommended physical security related activities at the user's site.

Table 11: 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 tempered, 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 AF7500 Hardware

Figure 4: Top and Front View of the AF7500 Hardware Showing the Blue Thread Locker

Figure 5: Front View of the AF2100 Hardware Showing the Blue Thread Locker

Figure 6: Back View of the AF2100 Hardware Showing the Blue Thread Locker

7.0 Software Security Policy

The firmware can be upgraded: replaceable with newer versions. A self-test validates the authenticity of the upgraded firmware by checking the firmware's keyed hash. If the firmware is compromised as determined by the test, the module enters an error state in which no cryptographic processing occurs, preventing a security breach through a malfunctioning device.

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. The firmware of the Gateways can be upgraded by using the included Fortress upgrade utility that is accessed by the Graphic User Interface (GUI).

9.0 Mitigation of Other Attacks Policy

No special mechanisms are built in the AirFortress® Wireless Security Gateways, however, besides the FIPS requirements 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) 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.*

4) Encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*

5) Multi-factor Authentication: The AirFortress® Wireless Security Gateways 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

Fortress Technologies, Inc. installs the AirFortress® Wireless Security Gateways 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

Select or deselects FIPS mode by using FISH to access the console port and then selecting FIPS enable. Once FIPS is enabled the prompt changes to "<FIPS>" and the AF Web Interface reports "FIPS MODE ENABLED" as indicators. Additionally, the module is only in its FIPS mode of operation when DES and 512-bit Diffie-Hellman are not used.

12.0 Maintenance Issues

The AF Wireless Security Gateways has no operator maintainable components. Inoperable modules must be returned to the factory for repair.