Non-Proprietary Security Policy for AirFortress™ Wireless Security Gateway Cryptographic Module

March 15, 2002

This security policy of Fortress Technologies, Inc. for the AirFortress™ Wireless Security Gateway Cryptographic Module (AF Gateway) defines general rules, regulations, and practices under which the AF Gateway 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.

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Contents

Figures and Tables

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1.0 Introduction

This security policy defines all security rules under which all products the AirFortress™ Wireless Security Gateway (AF Gateway) must operate and enforce, including rules from relevant standards such as FIPS.

The AF Gateway is a *cryptographic software system* that operates as a multi-chip standalone cryptographic module. The cryptographic boundary of the AF Gateway is the self-contained compiled code that is installed at the point of manufacturing into production-quality compliant computer hardware. The physical boundary is the hardware platform, such as a typical PC, on which the AF Gateway is installed.

The AF Gateway software and computer hardware combination operates as an *electronic encryption device* designed to prevent unauthorized access to data transferred across a wireless network. The AF Gateway encrypts and decrypts traffic transmitted on that network, protecting all clients "behind" it on a protected network. Only authorized personnel, such as the system administrator (cryptographic officer), can log into the module.

The AF Gateway operates at the datalink, (also known as MAC) layer of the OSI model as shown in Figure 1. Most of the security protocols are implemented without human intervention to prevent any chance of human error.

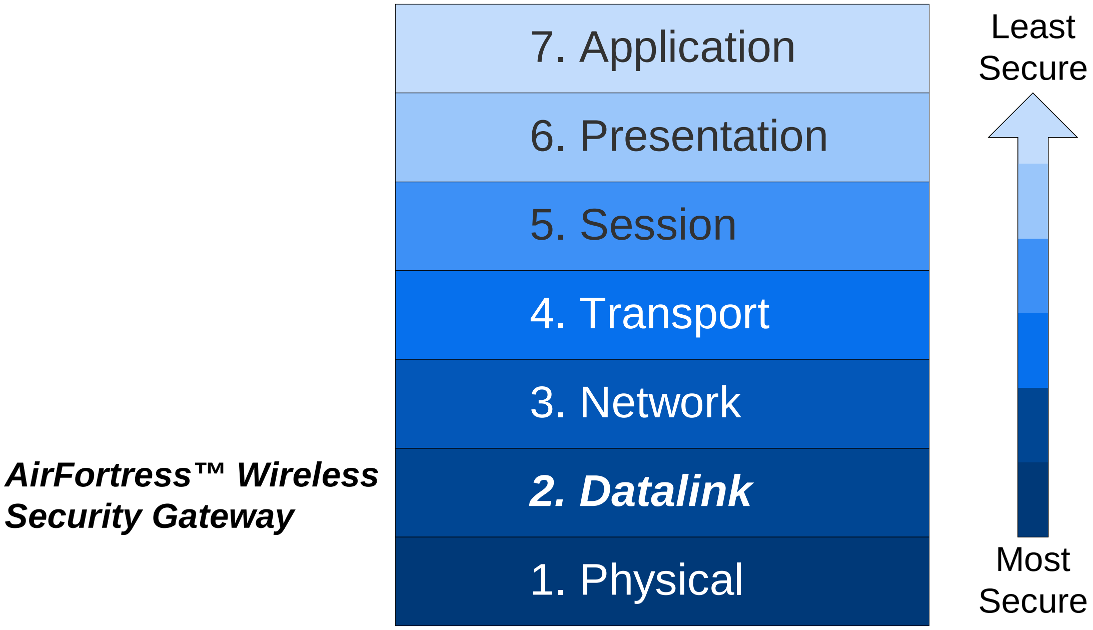

Figure 1. The Seven Layers of the OSI Reference Module

The AF Gateway 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 system administrator (cryptographic officer role) manages the cryptographic configuration of the AF Gateway. Administrators 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 AF Gateway automates cryptographic processing, end users do not have to actively initiate cryptographic processing; the AF Gateway encrypts and decrypts data sent or received by users operating authenticated devices connected to the AF Gateway.

The AF Gateway 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 AF Gateways can also communicate with each other directly.

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.0 AF Gateway Security Features

The AF Gateway provides true datalink layer (Layer 2 in Figure 1) security. To accomplish this, it was designed with the minimum security features described in the following sections.

2.1 Cryptographic Module

The following security design concepts guide the development of the AF Gateway:

1. Use strong, proven encryption solutions such as 3DES and AES.
2. Protect data at or below the level of vulnerability
3. 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.
4. Secure all points where a LAN, WLAN, or WAN can be accessed by using a unique Company Access ID, defined by the customer, to identify and authenticate authorized devices.
5. The AF Gateway can be installed only in production grade, FCC-compliant level computer hardware at the customer's site or at Fortress Technologies, Inc. laboratory.

The AF Gateway is an *electronic encryption module* designed to prevent unauthorized access to data transferred across a wireless network. It provides strong encryption (TDES, DES, and AES, or IDEA for commercial application) and advanced security protocols.

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 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 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 AF Gateway 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 AF Gateway allows role-based access to user interfaces that access to 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.

The AF Gateway can be configured only in Standard mode of operation, which provides encrypted communication in a network with other sites protected by the AF Gateway.

2.2 Module Interfaces

The AF Gateway includes two logical interfaces for information flow, Network (eth1) for encrypted data across a LAN or WLAN and Client (eth0) for data sent as plaintext to clients on the protected wired network that the AF Gateway is deployed on. These logical interfaces correspond with two separate network interface cards (NICs) provided by the hardware platform. 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 AF Gateway

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

does not allow plaintext transmission of data, cryptographic keys, or critical security parameters across a LAN or WLAN. Figure 2 shows this information flow in relation to a standard set of computer components that will be present on any platform on which the AF Gateway is installed.

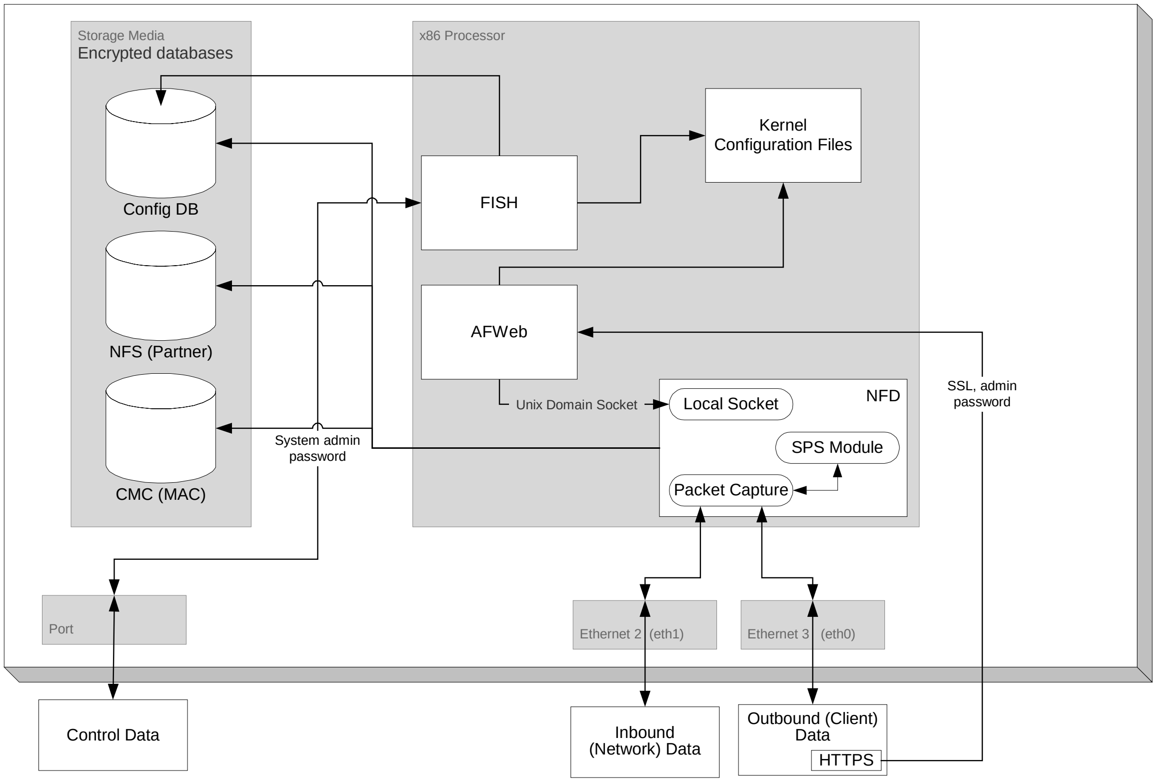

Figure 2. Information Flow Through the AF Gateway

2.3 Roles and Services

2.3.1 Roles

The AF Gateway supports the following operator roles: System Administrator (cryptographic officer), Administrator, and User.

The system administrator role is the module’s cryptographic officer. The system administrator performs the following tasks in particular:

- Set the operational mode (FIPS or non-FIPS) of the Gateway
- Configure the unique access ID
- Zeroize all cryptographic keys as needed
- Configure security settings
- Deletes client database (NF.cmc) as needed
- Deletes partner database (nfdsdb.nfs) as needed
- Resets configuration database
- Resets the AF Gateway to factory default settings, which also zeroizes cryptographic keys

The administrator role can monitor system status and perform the following tasks:

- Enter the system date and time
- Enter the device serial number
- Ping a device on the network (an AF Gateway cannot ping the clients that it protects)
- Trace a packet
- Clear the client MAC database
- Change the administrator role password
- Reboot the AF Gateway

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

The system administrator and the administrator must enter the correct role password to access the system. When operators change the password upon installing the AF Gateway, passwords must be of a minimum specified length.

User devices communicate through the AF Gateway and use the AirFortress Secure Client application; these devices are referred to as *secure clients*. Users send packets to and receive packets from the AF Gateway. They benefit from the AF Gateway cryptographic processing without manual intervention, thus eliminating any direct interaction with the module; the AF Gateway secures data transparent to users. Secure clients establish access to the AF Gateway using their device ID as their user ID and their SKeys as the password.

2.3.2 Services

The following *key management* services are provided in the module without requiring operator intervention:

- Generating the module's keys
- Generating cryptographic keys using encrypted Diffe-Hellman exchanges to prevent man-in-the-middle attacks
- Creating and maintaining tables (users can manually clear tables)
- Authenticating devices attempting to communicate with the AF Gateway
- Reinitiating key exchange at user-specified intervals
- Zeroizing keys if power to the module is turned off

The following *cryptographic operations* services are provided in the module without requiring operator intervention:

- Filtering packets to prevent any unencrypted (and, therefore, unauthorized) packets from entering the network
- Encrypting and decrypting packets at the datalink layer (OSI level 2)
- Authenticating the origin of packets
- Testing packet integrity using a SHA-1 hash

Other services performed by the module include monitoring and displaying device status and performing all self-tests.

The following tables show the services supported and allowed to each role within each product. As a user does not have any interaction with the module or its security relevant data items, a separate usage table is not included for this role.

Table 1. AF Gateway System Administrator (Cryptographic Officer)

Security Relevant Data Item	Show	Set	Enable	Disable	Add	Delete	Reboot	Password	Zeroize	Reset	Default Reset
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
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

[1] The `reset` command resets the configuration database except for the serial number, device ID, MAC address, cryptographic algorithm, and user passwords.

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

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table 2. AF Gateway Administrator

Security Relevant Data Item	Show	Set	Delete	Reboot	Password
Access Control Server (non-FIPS only)	X				
Access ID					
Access point	X				
afweb					
ARP					
Client DB (NF.cmc)			X		
Config database					
Crypto keys					
Cryptography algorithm	X				
Device ID	X				
Device MAC	X				
FIPS mode	X				
Hostname	X				
Interface	X				
IP Address	X				
Memory					
Netmask	X				
Network gateway	X				
Partner DB (nfdsdb.nfs)					
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.

2.4 Physical Security

The AF Gateway software is installed by Fortress Technologies on a production-quality, FCC-certified hardware device (such as a PC), which also defines the module’s physical boundary. The minimum requirements for the computer hardware are as follows:

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

- x86 processor system board, 150MHz - 2000MHz
- one available serial port
- 64 MB DRAM
- two rtl8139 or eepro100 based Network Interface Cards
- 20 MB storage media (IDE)
- Overall system must be, at minimum, FCC-compliant (Part 15, Subpart J, Class A)

These hardware requirements ensure that any hardware platform on which the AF Gateway is installed complies with the requirements for FIPS Security Level 1 at a minimum. The physical security of a deployed AF Gateway is determined by the customer's security policy.

2.5 Software Security

The AF Gateway software is written in C and C++ and operates on the Linux operating system. The software is installed in the host hardware storage medium in as a complied executable. If maintenance requires opening the hardware, the Fortress Technologies-authorized technician performing the maintenance zeroizes the critical security parameters.

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

2.6 Operating System Security

The AF Gateway operates automatically after power-up. The AF Gateway operates on Linux, 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. Updates to the software are supported, but can only be made using the provided services or following specific procedures.

2.7 Cryptographic Key Management

The AF Gateway itself automatically performs all cryptographic processing and key management functions.

2.7.1 Key Generation

The AF Gateway uses five cryptographic keys, generated by FIPS-validated protocols:

- Module's Secret Key
- Static Private Key
- Static Public Key
- Dynamic Private Key
- Dynamic Public Key

2.7.2 Protocol Support

The AF Gateway supports the Diffie-Hellman, SHA-1 and automatic key re-generation protocols.

2.7.3 Key Storage

No encryption keys are stored permanently in the modules hardware.

2.7.4 Zeroization of Keys

The session keys, which are encrypted, of the AF Gateway 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 as needed.

2.8 Cryptographic Algorithms

The AF Gateway applies FIPS-validated DES, Triple DES, Diffie-Hellman, HMAC-SHA-1, and SHA-1 for FIPS validated operation. AES and IDEA algorithms are also available for non-FIPS operation.

2.9 EMI/EMC

Fortress Technologies installs the AF Gateway only on FCC-compliant (Part 15, Subpart J, Class A) computer hardware.

2.10 Self-Tests

The AF Gateway conducts self-tests at power-up and conditionally as needed, when a module performs a particular function or operation. The following list of all self-tests includes both power-up tests and conditional tests that apply to the AF Gateway.

A. *Power-Up Tests*
   - Cryptographic Algorithm Test
   - Software/Firmware Test
   - Critical Functions Test

B. *Conditional Tests*
   - Continuous Random Number Generator test

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

3.0 Customer Security Policy Issues

FTI expects that after the module's installation, any potential *customer* (government organization or commercial entity or division) *employs its own internal security policy* covering all the rules under which the 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.

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.0 Maintenance Issues

Only the Fortress Technologies security officer can perform physical maintenance of the hardware devices on which the AF Gateway is installed. All software installation and reinstallation for modules operating in FIPS mode are performed by Fortress Technologies. Software troubleshooting to resolve an error state may require the product to be returned to Fortress Technologies or for a Fortress-authorized technician to perform maintenance at the customer's site.

- * - * -

End of the "Non-Proprietary Security Policy for the AirFortress™ Wireless Security Gateway (AF Gateway) Cryptographic Module

© Copyright Fortress Technology, Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.