Non-Proprietary Security Policy for the FIPS 140-2 Validated AirFortress™ Wireless Security Gateway Cryptographic Module Version 2.4

February 12, 2004

This security policy of Fortress Technologies, Inc., for the FIPS 140-2 validated AirFortress™ Wireless Security Gateway Cryptographic Module (AF Gateway), Version 2.4, 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 © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Contents

Figures and Tables

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
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 the AirFortress™ Wireless Security Gateway (AF Gateway) must operate and which it must enforce, including rules from relevant standards such as FIPS. The AF Gateway complies with all FIPS level 1 requirements.

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, the system administrator (cryptographic officer) and administrators, 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.

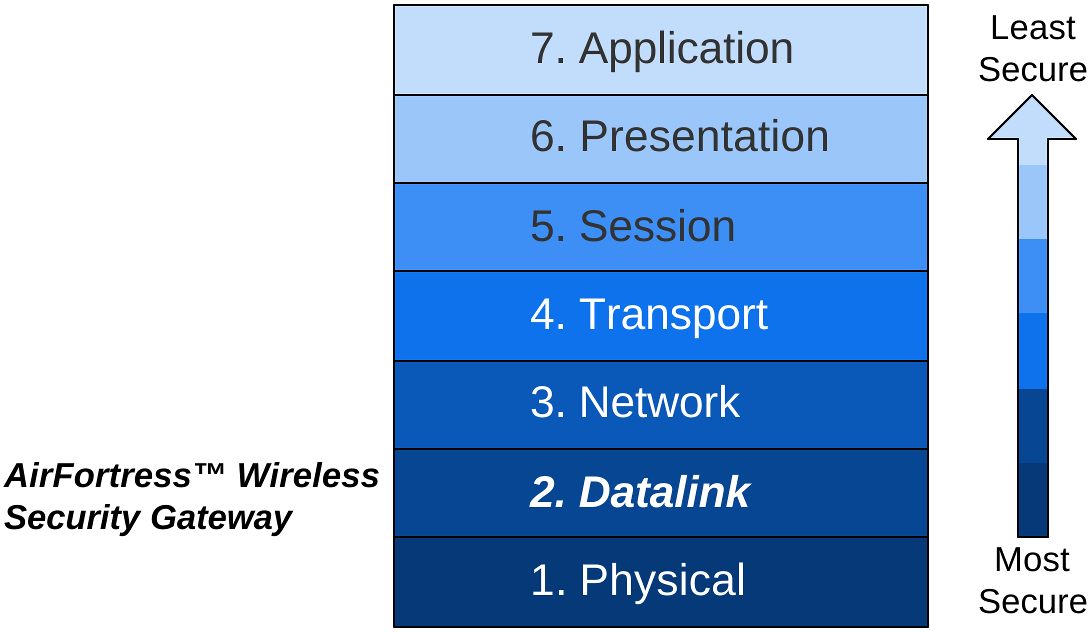

Figure 1. The Seven Layers of the OSI Reference Module

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 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. A typical application of the AF Gateway is shown in Figure 2.

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

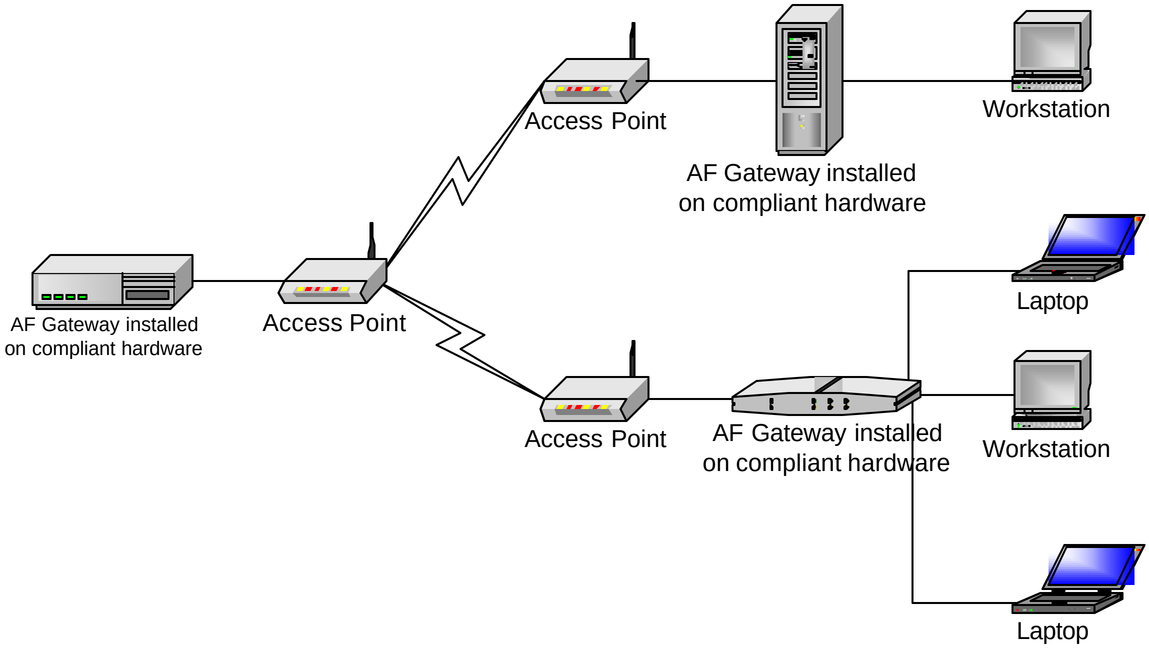
Access Point
AF Gateway installed on compliant hardware
Workstation
AF Gateway installed on compliant hardware
Access Point
Laptop
Access Point
AF Gateway installed on compliant hardware
Workstation
Laptop

Figure 2. Example Configuration of AirFortress™ Wireless Security Gateway Modules in a WAN

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
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 were applied to the AF Gateway:

1. Use strong, proven encryption solutions, such as 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™ Access Control Server.
4. The AF Gateway can be installed only in production grade, FCC-compliant level computer hardware at the customer's site or at Fortress Technologies' productio n facilities.

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 and AES) and advanced security protocols. DES encryption is available for use with legacy systems.

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 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 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

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 does not allow plaintext transmission of data, cryptographic keys, or critical security parameters across a LAN or WLAN. Figure 3 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.

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

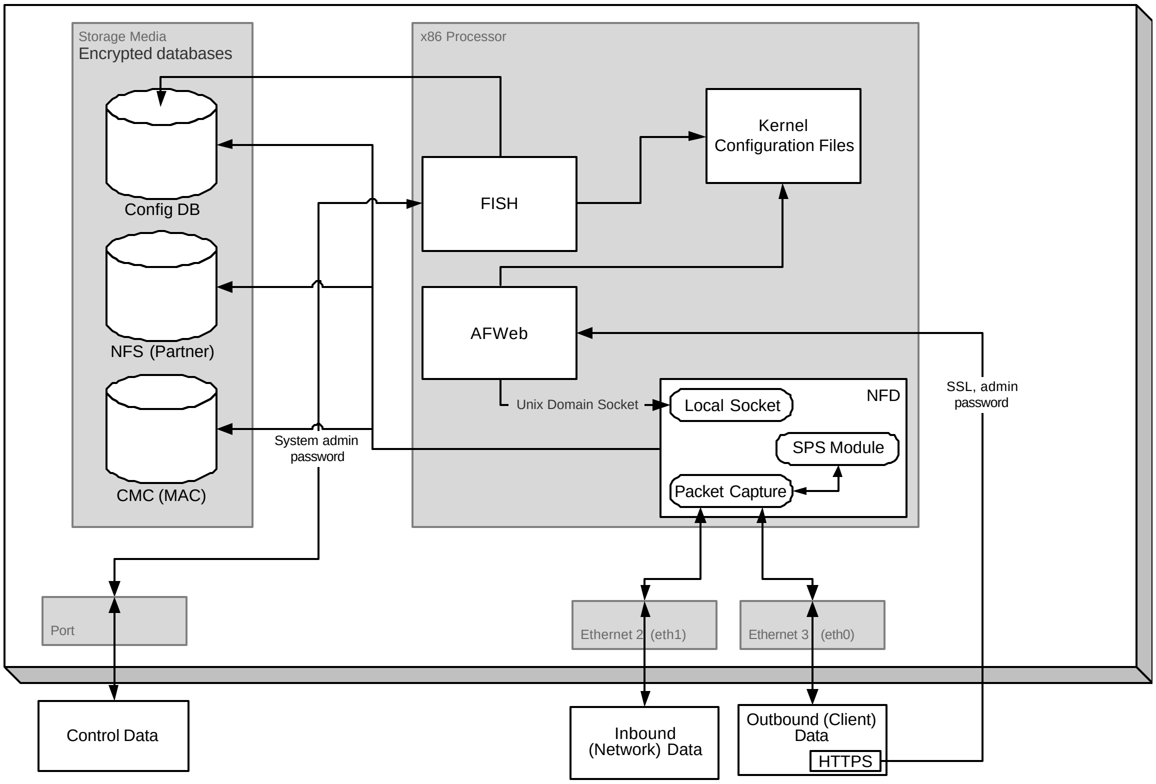

Figure 3. Information Flow Through the AF Gateway

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

3.0 Identification and Authentication Policy

3.1 Roles

The AF Gateway employs role-based authentication.

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

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
- Define use and configuration of an authentication server
- 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 zeroizes current cryptographic keys and requires creation of a new session key for further communication
- Enter the system date and time
- Enter the device serial number
- Ping a device on the unencrypted network (devices on the encrypted network are tracked directly)
- Trace a packet
- Change the system passwords
- Upgrade the AF Gateway software with Fortress 140-2 validated software upgrades
- Reboot the AF Gateway

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

3.1.1 Authentication

User authentication is by a 16 hexadecimal digit Access ID (64-bit). Crypto-Officer authentication is by 8-character password (72^8).

3.2 Services

The following services are provided in the module:

Crypto-Officer

- Configuration as described above
- Creating and maintaining tables (crypto-officer can manually clear tables)
- Generating the module's keys
- Reinitiating key exchange at user-specified intervals

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

- Zeroizing keys if power to the module is turned off
- Performing self-tests automatically at every power-on and/or by the cryptographic officer's demand.
- Display status
- Upgrade the entire module's software

User

- Generating cryptographic keys using encrypted Diffe-Hellman exchanges to prevent man-in-the-middle attacks
- Authenticating devices attempting to communicate with the AF Gateway
- 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 HMAC-SHA-1 hash

3.3 Self-Tests

The AF Gateway 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, TDES KAT, DES KAT, HMAC-SHA-1 KAT, SHA-1 KAT, and RNG KAT
  - Software/Firmware Integrity Test: HMAC-SHA-1
  - Critical Functions Test: None

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

Failure of any self-test listed above puts the module in its error state. Once in the error state, the module cannot be restored to a usable condition without returning the module to the manufacturer for recovery.

3.4 Cryptographic Key Management

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

3.4.1 Key Generation

The AF Gateway uses seven cryptographic keys, generated by FIPS-approved processes:

- Module's Secret Key (Symmetric, TDES, and AES)
- Static Private Key
- Static Public Key
- Static Secret Encryption Key (Symmetric, TDES, and AES)
- Dynamic Private Key
- Dynamic Public Key
- Dynamic Session Key (Symmetric, TDES, and AES)

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Notes:

- Symmetric DES keys are used for backward compatibility with legacy units.
- 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 key generation.

3.4.2 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 stored encrypted.

3.4.3 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.

3.4.4 Protocol Support

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

3.4.5 Cryptographic Algorithms

The AF Gateway applies the following cryptographic algorithms:

FIPS Algorithms	Certificate number
AES (ECB, CBC, encrypt/decrypt; 128, 192, 256)	14
TDES (CBC, encrypt/decrypt)	19
DES (ECB, CBC, encrypt/decrypt)	23
SHA-1 (Byte)	34
HMAC-SHA-1	34 (Vendor affirmed)

Non-FIPS Algorithms
Diffie-Hellman (Key Agreement)

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.0 Access Control Policy

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 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 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 1. AF Gateway System Administrator (Cryptographic Officer)

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

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Function/Service	Show	Set	Enable	Disable	Add	Delete	Reboot	Password	Zeroize	Reset	Default Reset
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 selected, and user passwords. The `default reset` command resets everything except for the serial number. All cryptographic keys are automatically regenerated 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 2. AF Gateway Administrator

Function/Service	Show	Set	Delete	Reboot	Password
Access Control Server	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				

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Function/Service	Show	Set	Delete	Reboot	Password
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.

Table 3. AF Gateway User

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

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

5.0 Physical Security Policy

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:

- 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 B)

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.

The host hardware platform server must be located in a controlled access area.

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

6.0 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.

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

7.0 Operating System Security

The AF Gateway operates automatically after power-up. The AF Gateway operates on a Fortress edited version of Linux 2.4.16 that is installed along with the module's software, with user access to standard OS functions eliminated. This non-modifiable operating system is known as the Fortress Interface and Shell (FISH) version 2.4. 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. The FISH provides a limited Command Line Interface for a Crypto-Officer to configure the module.

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

8.0 Mitigation of Other Attacks Policy

No special mechanisms are built in the AF Gateway, however, the cryptographic module is designed to mitigate several specific attacks. 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: *Mitigates key discovery*.
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. Compression and encryption of header information inside of the frame, making it impossible to guess. Use of strong encryption further protects the information. Any bit flipping would be useless in this frame to try to change the IP address of the frame: *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.*

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9.0 EMI/EMC

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

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10.0 Customer Security Policy Issues

Fortress Technologies 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.

10.1 FIPS Mode

The Crypto-Officer must select FIPS mode during module initialization. Set FIPS by using AF 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.

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11.0 Maintenance Issues

Only a Fortress Technologies security engineer can perform physical maintenance of the hardware devices on which the AF Gateway is installed. Software upgrades are provided to the customer by Fortress Technologies and can be applied using the provided mechanisms. 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.

Copyright © 2004 Fortress Technology, Inc., 4025 Tampa Rd., Suite 1111, Oldsmar, FL 34677
This document can be reproduced and distributed only whole and intact, including this copyright notice.