National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Fortress Wireless Secure Gateway

Report Number: CCEVS-VR-VID10174-2007

Dated: 23 October 2007

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jerome F. Myers
Dianne Hale

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Fortress Wireless Gateway at EAL3. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 28 June 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.3, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 3 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the Fortress Wireless Gateway AF2100, AF7500, and FC-X. The TOE Security Function (TSF) includes Audit, Packet Encryption/Decryption, Information Flow Control, Identification and Authentication, Security Management, and Protection of the TOE itself.

- Audit - Audit services allow authorized administrators to detect and analyze potential security violations.
- Packet Encryption/Decryption - Packet encryption and decryption services provide mechanisms to encrypt and decrypt data as it is exchanged with wireless endpoints on the WLAN for the purpose of preserving confidentiality and integrity.
- Information Flow Control - The TOE receives plaintext from the LAN, and then encrypts it, retransmitting it out encrypted on the WLAN side. Only wireless endpoints that are configured for the same Access ID as the FSG, except for systems specified for bypass operation, may transmit information through the FSG.
- Identification and Authentication – The TOE requires that authorized administrative users are uniquely identified and authenticated before accessing audit/configuration information stored on the system.
- Security Management - Security Management provides administrators with the capabilities to configure, monitor and manage the FSG
- Protection of the TOE - The TOE protects itself through Identity and Access Control and also by ensuring that attempts to modify, deactivate, or circumvent the TOE security functions are prevented. Self-tests execute when the system starts, periodically during system execution, and on command of an admin. Failure of any self-test puts the module in an error state requiring vendor repair.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifier

Evaluation Identifiers for Fortress Wireless Gateway	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Fortress Wireless Gateway – FCX, AF2100, and AF7500
Protection Profile	N/A
Security Target	Fortress Wireless Secure Gateway® Security Target, September 26, 2007,
Evaluation Technical Report	Evaluation Technical Report for the Fortress Wireless Secure Gateway Document No. F3-0807-007, Dated September 27, 2007.
Conformance Result	Part 2 conformant and EAL3 Part 3 conformant
Version of CC	CC Version 2.3 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on July 5, 2006.
Version of CEM	CEM Version 2.3 and all applicable NIAP and International Interpretations effective on July 5, 2006.
Sponsor	Fortress Technologies 4023 Tampa Road Suite 2000 Oldsmar, FL 34677
Developer	Fortress Technologies 4023 Tampa Road Suite 2000 Oldsmar, FL 34677
Evaluator(s)	**COACT Incorporated**

Evaluation Identifiers for Fortress Wireless Gateway	
	Ching Lee, *Lead Evaluator* Pascal Patin, *Evaluator* Brooks Leitch, *Evaluator* Ryan Kane, *Evaluator* Anthony Busciglio, *Evaluator*
Validator(s)	**NIAP CCEVS** Jerome F. Myers Dianne Hale

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0427 – Identification of Standards
I-0347 - Including Sensitive Information In Audit Records
I-0407 - Empty Selections Or Assignments
I-0410 - Auditing Of Subject Identity For Unsuccessful Logins
I-0429 - Selecting One Or More

International Interpretations

None

3 TOE Description

The Fortress Secure Gateway® (FSG) is a security appliance that provides a secure perimeter to an enterprise network by protecting communications between wireless devices on a Wireless Local Area Network (WLAN) and the rest of the network (Local Area Network (LAN)) and restricting the wireless systems that may access the LAN. The FSG does not have a radio and will function with any standard AP for radio communications. The objective of the TOE is to safeguard confidential and sensitive information. The FSG implements encryption at the Media Access Control (MAC) layer, and by doing so, enables the FSG to prevent vulnerabilities to confidentiality and integrity from being exploited. Once implemented, the operation of the FSG is automatic, requiring no administrator intervention.

The FSG is designed to prevent a hacker from “sniffing” and reading data transferred across a wireless network. The TOE firmware performs key computations, and encrypts and decrypts data packets, receiving plaintext data from systems on the LAN, and then encrypting the plaintext to produce ciphertext. Similarly, the FSG receives ciphertext traffic from the wireless endpoints, then decrypts and forwards it to systems on the LAN. The administrator selects which encryption algorithms to use for communicating to all devices on the network. The algorithms that the administrator may select include 3DES or AES in various key sizes.
The administrator may configure bypass operations on the FSG that permit specified traffic (based on MAC address, IP address and TCP/UDP port) to pass through the FSG without

encryption or decryption. Some examples of systems that may require this functionality are: management of access points (whose packets exchanged with the LAN systems are not forwarded over wireless media), “guest” wireless users (whose traffic is not considered sensitive), or devices such as digital scales that do not support cryptographic operations. All traffic received from these devices may be mapped to a single “Hotspot VLAN ID” when it is forwarded to the LAN.

The FSG is designed to securely communicate in a point to point configuration between two FSG’s, with the Fortress SecureBridge, and with the Fortress Secure Client on a PC or laptop. The Fortress Secure Client enables PC’s, laptops, PDA’s and Tablets to securely communicate with a network protected by a FSG. The Fortress SecureBridge is a self-contained unit with its own wireless network interface card (NIC) that secures a device that cannot install a Fortress Secure Client (like a cash register, gas pump etc…).
The following FSG models are included in this product line:

A) AF2100
B) AF7500
C) FC-X

The TOE consists of any FSG model that makes up the product line. Each model consists of a single configuration. The firmware for each model provides identical security functionality and is known as AirFortress Gateway 3.1 (AFG3) and AirFortress Gateway 4.1 (AFG4). Differences between the models are limited to performance, enclosure (desktop versus rack mount), and the types of Ethernet interfaces.

The physical boundary of the TOE includes the entire appliance. All hardware peripherals for the network that the TOE communicates with, such as printers, routers, client systems and other hardware devices, are all outside the boundary of the TOE.

The FSG has logically distinct physical interfaces that define all entry and exit points to and from the appliance. The physical interfaces are:

- LAN network interface (designated as "eth0" or Unencrypted Port) - a port for plaintext data input/output streams with LAN systems
- WLAN network interface (designated as "eth1" or Encrypted Port) - a port for ciphertext data input/output streams with WLAN systems
- Console interface (designated as Console Port) – serial interface used for management
- Aux interface – not used in the evaluated configuration

The administrator accesses the FSG through a Console Port using a Command Line Interface (CLI) known as FISh (Fortress Interface Shell). A Web interface (AFWeb) allows the administrator to remotely manage the network settings and security functions through a GUI as well. Remote management is performed over an encrypted channel using both AES or Triple-DES (FIPS 140-2 certified) encryption at the link layer and HTTPS on the WLAN side of the TOE and HTTPS on the LAN side of the TOE. AFWeb provides two levels of access (admin and operator) to support multiple levels of administrator access.

The administrator logs into the FSG by supplying an account and the correct password. The length of the password is selectable, and can consist of 8-16 characters including at least one each upper case, lower case, and numeric characters. At least 4 characters must be changed when a new password is created.

The logical boundaries of the TOE include the security functions that the TOE provides. The TOE Security Function (TSF) includes Audit, Packet Encryption/Decryption, Information Flow Control, Identification and Authentication, Security Management, and Protection of the TOE itself.

Audit

Audit services that allow authorized administrators to detect and analyze potential security violations. When an FSG state changes (its starts or stops), an audit record is generated.

Additionally, when a potential violation of security policy has been detected, an audit record is generated. In all cases, timestamps are applied to audit records and the FSG supplies its own timestamps.

Packet Encryption/Decryption

Packet encryption and decryption services provide mechanisms to encrypt and decrypt data as it is exchanged with wireless endpoints on the WLAN for the purpose of preserving confidentiality and integrity. Cryptographic key agreement between wireless endpoints and the FSG occurs using the Diffie-Hellman protocol.

Information Flow Control

The TOE receives plaintext from the LAN, and then encrypts it, retransmitting it out encrypted on the WLAN side.

The FSG receives ciphertext from the WLAN side, decrypts it, and then retransmits it out in plaintext on the LAN side. Plaintext received from the wireless network side will be discarded unless a bypass feature is specified for that traffic. A common Access ID must be configured on the FSG and all wireless endpoints that desire to communicate through the FSG. Only wireless endpoints that are configured for the same Access ID as the FSG, except for systems specified for bypass operation, may transmit information through the FSG.

Identification and Authentication

The FSG requires that authorized administrative users are uniquely identified and authenticated before accessing audit/configuration information stored on the system.

Security Management

Security Management provides administrators with the capabilities to configure monitor and manage the FSG. The FSG supports multiple administrative roles to provide a “least privilege” model for TOE administrative access:

Admin – The privileged account has full permissions to manage the FSG. This account is accessible via both FISh and AFWeb.

Operator – The operator account has view-only permission to monitor the current settings and status of the AFSG via AFWeb.

Protection of the TOE

The TOE protects itself through Identity and Access Control and also by ensuring that attempts to modify, deactivate, or circumvent the TOE security functions are prevented.
Self-tests execute when the system starts, periodically during system execution, and on command of an admin. During self-tests, cryptographic keys are not calculated and traffic is not passed. Failure of any self-test puts the module in an error state (indicated by the Status LED) and updates the log file. Once in the error state, the system must be returned to the vendor for repair.

4 Assumptions

The assumptions listed below are assumed to be met by the environment and operating conditions of the system.

A.AREA It is assumed that the IT environment, including the area of installation, provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.DELIVERY The administrator correctly installs the TOE according to the installation and guidance documentation.

A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrative guidance.

5 Threats

The following threats are addressed by the TOE.

Threats Addressed by the TOE

T.AUDIT_ COMPROMISE An unsophisticated user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user’s action.

T.CORRUPTION An unsophisticated unauthorized wireless user may attack information exchanged between the TOE and wireless endpoints by modifying unprotected wireless traffic.

T.DISCLOSURE An unsophisticated unauthorized wireless user may gain unauthorized access to information exchanged between the TOE and wireless endpoints by capturing unprotected wireless traffic.

T.FAILURE An unsophisticated malicious user may take advantage of a failure of the operation of the TOE to gain unauthorized access to information.

T.MASQUERADE An unsophisticated user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

6 Organisational Security Policies

The following Organisational Security Policies are required by the TOE.

P.ACCESS All wireless endpoints that attempt to communicate via the TOE must have knowledge of the Access ID configured in

	the TOE or be explicitly authorized to communicate in plaintext.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.AUTO	The TOE processes all cryptographic operations, including key exchanges, to eliminate the possibility of human error.
P.CRYPTOGRAPHY	For all cryptographic functions addressed by FIPS 140-2, only NIST FIPS validated cryptography is used by the TOE on a physical or logical port being used over a unprotected network.
P.MANAGE	The administrator is the only person who manages the TOE, the TSF data, and the security functions.
P.RECORD	All security relevant events in the TOE are recorded and archived in log files.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

7 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. This evaluation does not verify all claims made in the product’s end-user documentation. The verification of the security claims is limited to those claims made in the TOE SFRs and TOE Summary Specification (see ST sections 5 and 6 respectively). Section 8.1 of this report and Section 2.2.1 of the ST provides a list of functionality excluded from the evaluation.

2. All hardware peripherals for the network that the TOE communicates with, such as printers, routers, client systems and other hardware devices, are all outside the boundary of the TOE and therefore outside the scope of this evaluation. In addition, although the TOE requires appropriately configured clients to communicate with the FSG, client software was not part of the evaluated product. The evaluated configuration only consists of a single FSG appliance (Model AF2100, AF7500, or FC-X) operating in stand-alone mode, not any other model released or in process.

3. Although the TOE requires authorized administrative users are identified and authenticated before accessing audit/configuration information stored on the system, it only provides accountability to the granularity of the administrator role. The TOE provides a single “admin” login and all administrators login in as that role. There are no individual accounts for each administrator.

4. The majority of the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. Unless a FIPS certificate number is listed in Table 10 of the ST, the cryptography has only been asserted as tested by the vendor.

8 Architecture Information

The physical boundary of the TOE includes the entire appliance. All hardware peripherals for the network that the TOE communicates with, such as printers, routers, client systems and other hardware devices, are all outside the boundary of the TOE. The hardware chassis and interfaces of the AF2100 model are depicted below.

Figure 1 - AF2100

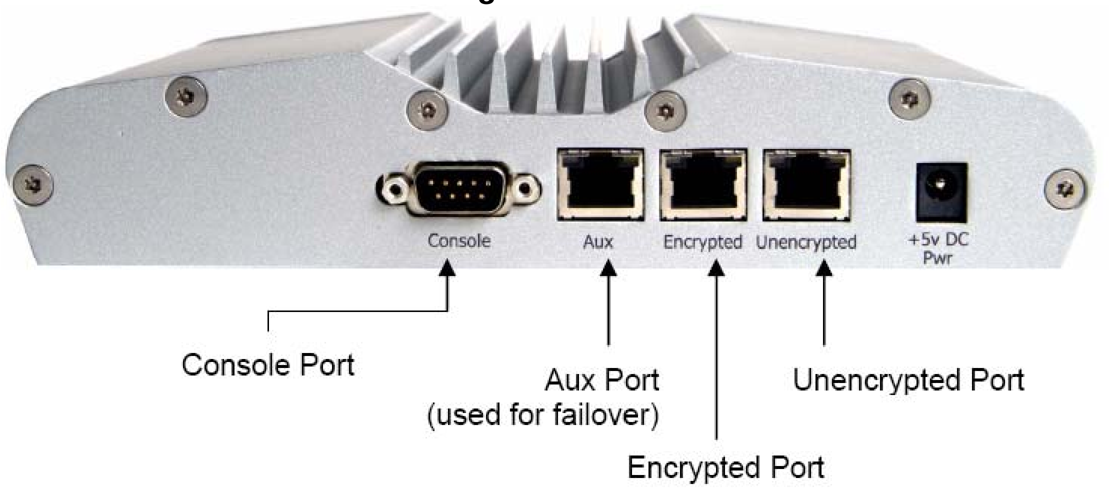


Figure 2 - AF7500

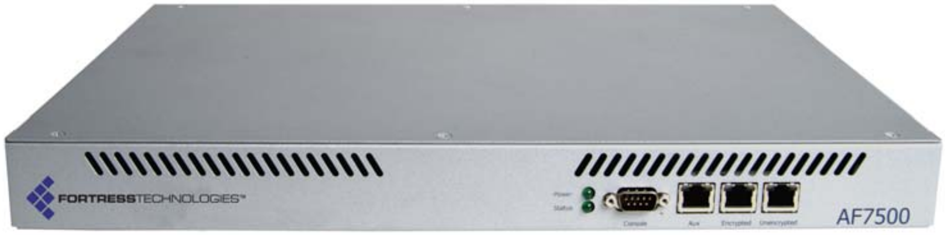
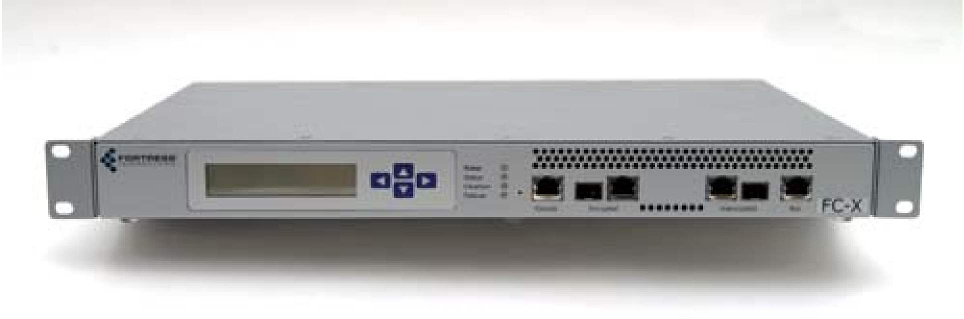


Figure 3 - FC-X Model



The FSG has logically distinct physical interfaces that define all entry and exit points to and from the appliance. The physical interfaces are:

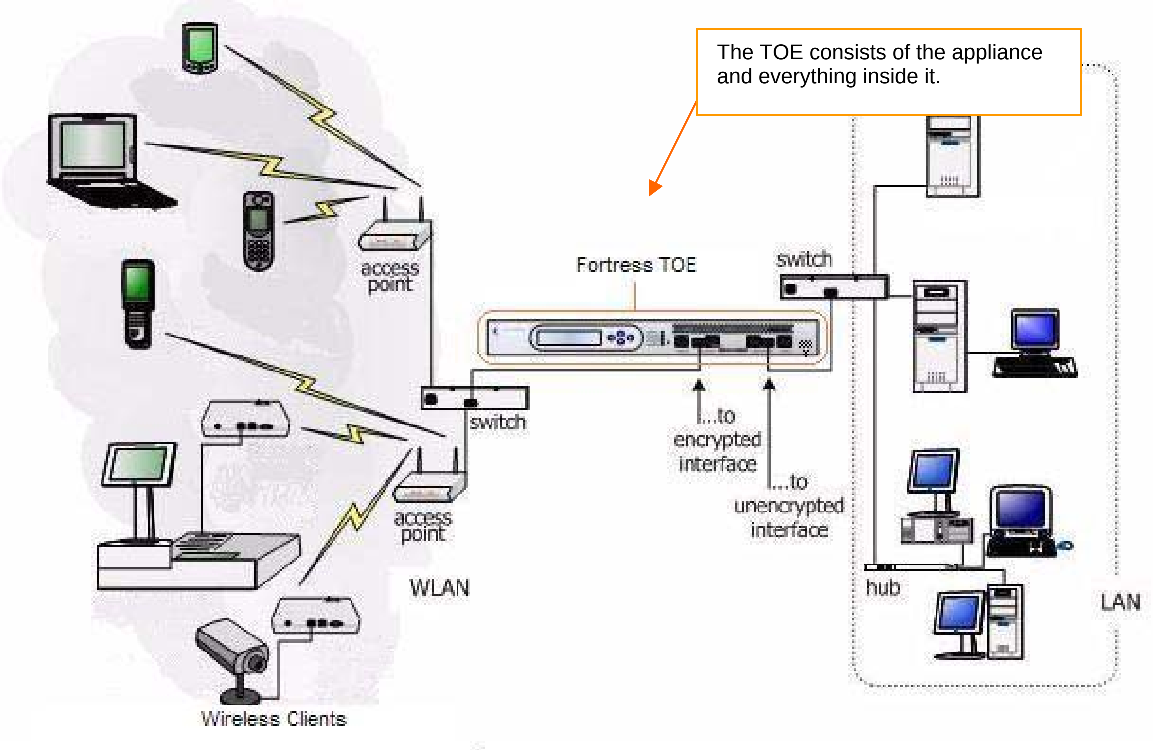
- LAN network interface (designated as "eth0" or Unencrypted Port) - a port for plaintext data input/output streams with LAN systems
- WLAN network interface (designated as "eth1" or Encrypted Port) - a port for ciphertext data input/output streams with WLAN systems
- Console interface (designated as Console Port) – serial interface used for management
- Aux interface – not used in the evaluated configuration

The administrator accesses the FSG through a Console Port using a Command Line Interface (CLI) known as FISh (Fortress Interface Shell). A Web interface (AFWeb) allows the administrator to remotely manage the network settings and security functions through a GUI as well. Remote management is performed over an encrypted channel using both AES or Triple-DES (FIPS 140-2 certified) encryption at the link layer and HTTPS on the WLAN side of the TOE and HTTPS on the LAN side of the TOE. AFWeb provides two levels of access (admin and operator) to support multiple levels of administrator access.

The administrator logs into the FSG by supplying an account and the correct password. The length of the password is selectable, and can consist of 8-16 characters including at least one each upper case, lower case, and numeric characters. At least 4 characters must be changed when a new password is created.

An example of the TOE in a network configuration is depicted in the figure below.

Figure 4 - Physical Boundary



The TOE consists of the appliance and everything inside it.

8.1 Evaluated Configuration

The evaluated configuration consists of a single FSG (of any referenced model) operating in stand-alone mode. A terminal is connected to the FSG serial port for management access (FISh). One or more IT systems are present on the LAN side, and one or more IT systems are present on the WLAN side. An IT system on the LAN side is used for AFWeb access to the FSG.

Evaluated Configuration Options

- The FSG operates in FIPS-enabled operational mode at all times after initial configuration. In this mode, the following functionality is not supported:
  - SNMP
  - Remote logging of audit information
- SSH for remote FISh interactions with an administrator is not enabled. While a FISH session is active, traffic forwarding between the WLAN and LAN sides is disabled per the FIPS 140-2 validation of the cryptographic module. Remote administration should be performed via the AFWeb rather than FISh.
- Failover (to a second FSG appliance) functionality is not evaluated. This functionality requires additional security claims not common to stand-alone mode.
- The FSG operates as a stand-alone device. Interactions with the optional Fortress Management and Policy Server (MaPS) are not evaluated. The following functionality is normally used in conjunction with the MaPS and multiple FSGs and is therefore excluded from the evaluation:
  1) Subnet Roaming
  2) VLANs (other than the Hotspot VLAN)
  3) Blocking wireless endpoints that appear to be involved in spoofing attacks
  4) Remote authorization using a Radius Server
  5) The upgrade functionality to upgrade the firmware.

9 Product Delivery

The Fortress FSG Gateways are packed and shipped from Fortress Technologies, Inc, typically shipped via UPS directly to the customer site.
The customer will receive 3 automated emails from Fortress Technologies:

- Sales Order Placed – this email shows the customer the order has been placed.
- Order Shipped email – this email provides the carriers tracking number(s).
- Invoice email – this email is a copy of the invoice for the order.

This ensures that the customer can determine the identification of the TOE when the package is delivered. To verify the contents, a packing slip is attached to the outside of the box that shows the exact invoice ordered.

The Fortress AF2100 are each delivered with:

A) AF2100 quick start guide
B) CD containing:
  1) GatewayGuide3.1.pdf Admin Guide
  2) Release Notes GW3.1.3050Q.pdf
  3) UGupdateGW3.1.3050M.pdf AF2100 firmware
  4) update_complete.ver.2900AQ.pkg
  5) update_complete.ver.3050Q.pkg
  6) update_part_1.ver.2300FH.pkg
  7) update_part_2.ver.2300FH.pkg

The Fortress AF7500 are each delivered with:

A) AF7500 quick start guide
B) CD containing:
  1) GatewayGuide3.1.pdf Admin Guide
  2) Release Notes GW3.1.3050Q.pdf
  3) UGupdateGW3.1.3050M.pdf AF7500 firmware

4) update_complete.ver.2900AQ.pkg
5) update_complete.ver.3050Q.pkg
6) update_part_1.ver.2300FH.pkg
7) update_part_2.ver.2300FH.pkg

The Fortress FC-X are each delivered with:

A). FC-X quick start guide
B). CD containing:
1) FCxGuide4.1.pdf Admin Guide
2) Release Notes FCX4.1.3450AC.pdf
3) gw.4.1.3450AC.pkg FC-X firmware
4) AF-ACCESSPOINT-MIB Used for SNMP Viewer

All of documents and guides were evaluated.

10 IT Product Testing

Testing was performed between May 21 through May 25 2007 at the COACT facilities in Columbia, Maryland. COACT employees performed the tests.

10.1 Evaluator Functional Test Environment

The test configuration will include each version of the TOE to be evaluated: Fortress Technologies AF2100, AF7500, and FC-X. The hardware used to setup the network is three PCs (two for console configuration of the TOE, and one used as a sniffer) and a hub to attach all the components.

10.1.1 System Hardware

A) 4 Personal Computers
1) PC 1 – MS Windows XP Professional
2) PC 2 – MS Windows 2000
3) PC 3 – MS Windows XP Professional
B) Two Ethernet Hubs
C) AF2100
D) AF7500
E) FC-X

10.1.2 Installed System Software

A) Wireshark version 0.99.4 (PC 1 and PC 2)
B) Tiger Suite version 4.0 (PC 3)
C) SnagIt 8 (PC 1 and PC 2)
D) SnagIt 7 (PC 3)
E) NMapGUI version 0.2 BETA (PC 3)
F) Tenable Nessus Security Scanner version 3.0 (PC 2)
G) Opera Browser version 9.2.1 (PC2)
H) Putty release 0.59 (PC 1 and PC 2)
I) Ethereal version 0.9.16 (PC 3)
J) Fortress Technologies Secure Client 3.1 (PC 2)

10.1.3 Test Equipment /Tools

A) Two Ethernet Hubs

10.1.4 Test Configuration

The following figure graphically displays the test configuration used for functional testing.

1. Test Configuration/Setup

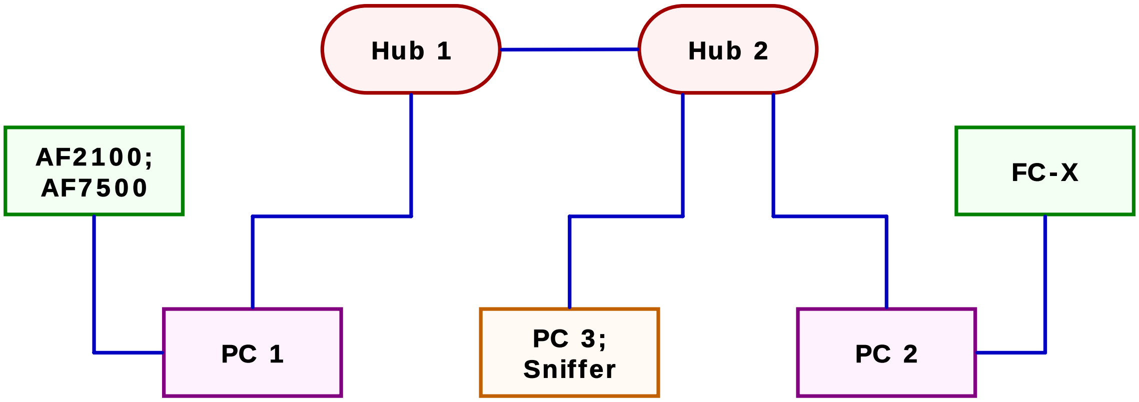


Table 2 - Test Components

Component	Description
PC 1 (Secure Gateway Management Console)	MS Windows XP Professional Version 2002, SP 2 Intel Pentium 367 MHz 256 MB RAM
PC 2 (Secure Gateway Management Console)	MS Windows 2000 Version 5.00.2195 SP4 Intel Pentium 1.6 GHz 256 MB RAM
PC 3 (Sniffer)	MS Windows XP Professional Version 2002, SP 2 Intel Pentium 367 MHz 256 MB RAM

10.1.5 Test Assumptions

The functional test environment/configuration requires these assumptions:

A) It is assumed that the IT environment, including the area of installation, provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

B) The administrator correctly installs the TOE according to the installation and guidance documentation.

C) Administrative users are trusted to be non-hostile within the scope of their role.

10.2 Functional Test Results

The evaluation team selected all of the vendor tests that are relevant to the Security Functions in the ST and omitted the tests for the IT Environment for the Gateway (AF2100 and AF7500) and a selection of the tests from the FCX. The Gateway referenced in the rest of this document refers to both the AF2100 and AF7500. Since all of the FCX tests were based on all of the Gateway tests, the evaluator selected a sampling of 9 out of the 21 tests to ensure that the results were the same.

10.3 Evaluator Independent Testing

The evaluation team selected a sample of the vendor tests to be reproduced. The tests selected validated the security functions and the TOE operational status. The purpose of this testing was to provide evidence which indicates that the TSF behaves as expected. Furthermore, this testing provides evidence that indicates that the Wireless Gateway functionalities related to the TSF behave as expected. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests. The results of the testing activities were that all tests gave expected (correct) results. The results of the functional testing are documented in the vendor and CCTL proprietary report, COACT document F3-0807-008, Fortress Wireless Gateway Functional Test Report, dated September 27, 2007.

10.4 Evaluator Penetration Tests

The evaluator examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources included:

A) www.osvdb.org/Irongeek.com
B) www.sans.org
C) www.cert.org
D) www.isc2.org

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicting that the vulnerability is non-exploitable in the intended environment of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

10.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

11 RESULTS OF THE EVALUATION

The evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the identified vulnerabilities by testing the Wireless Gateways for selected developer identified vulnerabilities.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, COACT document F3-0807-009, Fortress Wireless Gateway Penetration Test Report, dated September 27, 2007.

The evaluation determined that the product meets the requirements for EAL 3. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

12. VALIDATOR COMMENTS

Prospective users of these devices will find a helpful collection of useful information in the Executive Summary and Clarification of Scope portions of this report.

The Validators found that the evidence reviewed prior and during the Final Validation Oversight Review (VOR) supported the determination that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validators agree that the CCTL presented appropriate rationales to support the evaluation results presented in the Evaluation Technical Report for the Fortress Wireless Gateway. The Validators conclude that the evaluation and Pass result for the ST and TOE are complete and correct.

13. Security Target

Fortress Wireless Secure Gateway Security Target, September 26, 2007, is incorporated here by reference.

14. List of Acronyms

CC	Common Criteria
BPM	Bypass Mode
EAL3	Evaluation Assurance Level 3
ISO	International Standards Organisation
IT	Information Technology
CAID	Company Access ID
CAVP	Cryptographic Algorithm Validation Program
NIAP	National Information Assurance Partnership
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
FIPS	Federal Information Processing Standards
FISh	Fortress Interface Shell
FSG	Fortress Secure Gateway
GIG	Global Information Grid
HARA	High-Assurance Remote Access

ISSE	Information System Security Engineers
MAC	Media Access Control
RFC	Request For Comments
SNMP	Simple Network Management Protocol

15. Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.3, dated August 2005
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.3, dated August 2005
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.3, dated August 2005
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.3, dated August 2005
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.3, dated August 2005
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000