FORTRESS™
TECHNOLOGIES

EAL 3
Security Target

Fortress Secure Gateway

Date: September, 2007

Fortress Technologies, Inc. **4023 Tampa Road** **Suite 2000** **Oldsmar, FL 34677**	**Tel: +1.813.288.7388** **Toll Free: +1.888.4PRIVACY** **Fax: 813.288.7389**

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Fortress Secure Gateway®. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
1	September 26, 2007 Initial Release

[This page left intentionally blank.]

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

BPM	Bypass Mode
CAID	Company Access ID
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
EAL3	Evaluation Assurance Level 3
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
IT	Information Technology
MAC	Media Access Control
NIAP	National Information Assurance Partnership
PP	Protection Profile
RFC	Request For Comments
SF	Security Function
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for Fortress Secure Gateway. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) and international interpretations through July 5, 2006. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Fortress Secure Gateway® Security Target, document number SV-0306-001(6), dated August 21, 2007

1.2 TOE Reference

Fortress Secure Gateway® product family, consisting of the following models:

A) AF2100, version 1.0, AFSG firmware version 3.1

B) AF7500, version 1.0, AFSG firmware version 3.1

C) FC-X, version 1.0, AFSG firmware version 4.1

1.3 Evaluation Assurance Level

Assurance claims conform to EAL3 (Evaluation Assurance Level 3) augmented by ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.4 Keywords

Wireless, gateway, confidentiality, integrity, computer, security, security target, Fortress, Common Criteria.

1.5 TOE Overview

This Security Target defines the Common Criteria requirements for the Fortress Secure Gateway. The TOE consists of the appliance models AF2100, AF7500 and FC-X. Differences between the models are limited to performance, enclosure (desktop versus rack mount), and the types of Ethernet interfaces. The TOE sits between wired and wireless portions of an enterprise network and provides integrity and confidentiality of wireless traffic and restricts access of wireless endpoints to wired network systems.

1.6 Security Target Organisation

- Chapter 1 of this ST provides introductory and identifying information for the TOE.
- Chapter 2 describes the TOE and provides some guidance on its use.
- Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

- Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.
- Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.
- Chapter 6 is the TOE Summary Specification, a description of the functions provided by the Fortress Secure Gateway to satisfy the security functional and assurance requirements.
- Chapter 7 identifies any claims of conformance to a registered Protection Profile (PP).
- Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.7 Common Criteria Conformance

The TOE, Fortress Secure Gateway, is compliant with the Common Criteria (CC) Version 2.3, functional requirements (Part 2) extended (by NIAP interpretations only) and assurance requirements (Part 3) EAL3 augmented by ALC_FLR.2.

1.8 Protection Profile Conformance

The TOE does not claim conformance to any Protection Profile.

1.9 Conventions

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with Times New Roman bold text

Descriptions of Graphical User Interface (GUI) menu titles are indicated in **Arial Narrow bold text.**

References to product features are indicated in Arial Narrow standard.

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Fortress Secure Gateway 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 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

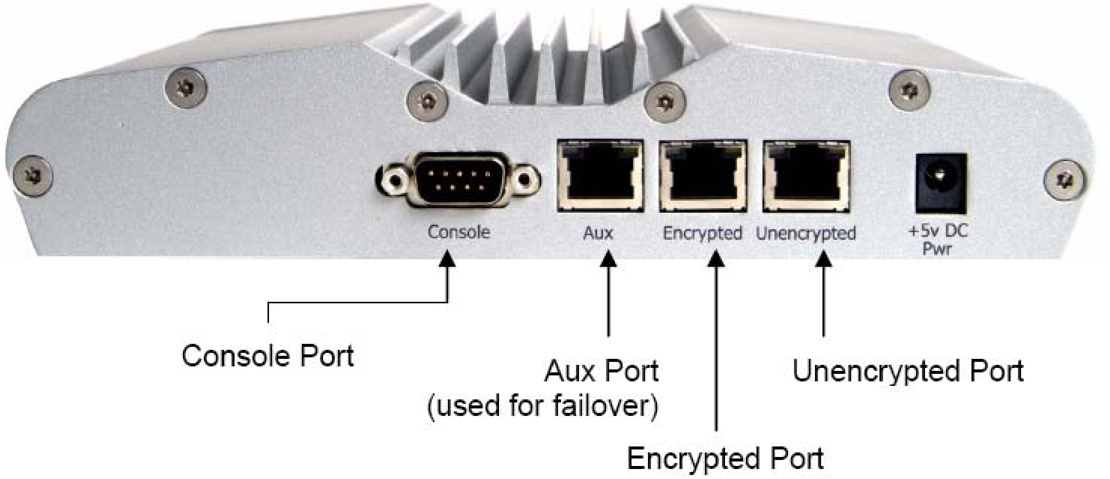
C) FC-X

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.

2.1.1 Physical Boundary

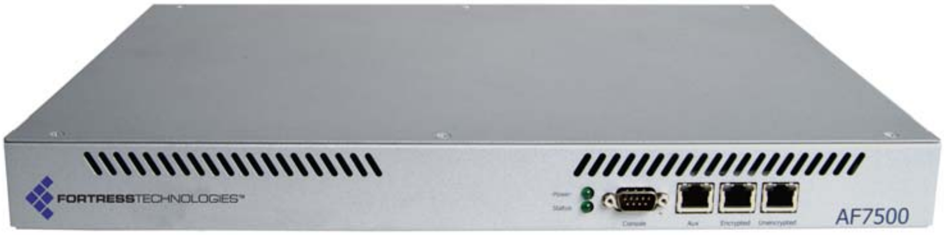
The physical boundary of the TOE includes the entire appliance. All hardware peripherals for the network that the TOE communicates with, such as printers, routers, client systems and other hardware devices, are all outside the boundary of the TOE. The hardware chassis and interfaces of the AF2100 model are depicted in Figure 1.

Figure 1 - AF2100 Model



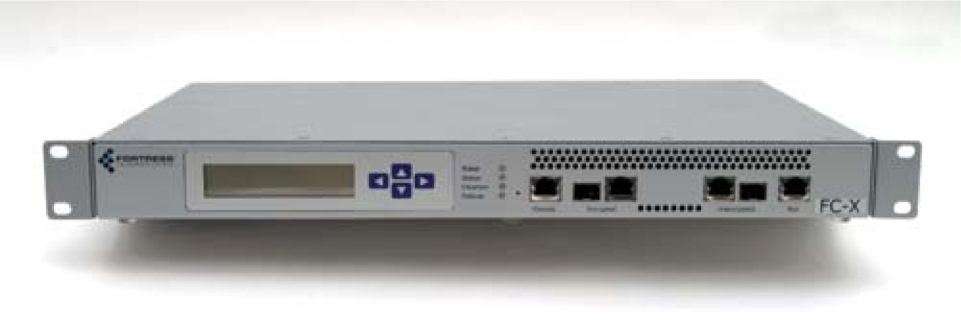
The hardware chassis and interfaces of the AF7500 model are depicted in Figure 2.

Figure 2 - AF7500 Model



The hardware chassis and interfaces of the FC-X model are depicted in Figure 3.

Figure 3 - FC-X Model



The FC-X allows you to connect your encrypted and unencrypted networks with either SFP Transceivers or RJ-45 10/100/1000 Mbps Auto-MDIX Ports

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

A) LAN network interface (designated as "eth0" or Unencrypted Port) - a port for plaintext data input/output streams with LAN systems

B) WLAN network interface (designated as "eth1" or Encrypted Port) - a port for ciphertext data input/output streams with WLAN systems

C) Console interface (designated as Console Port) – serial interface used for management

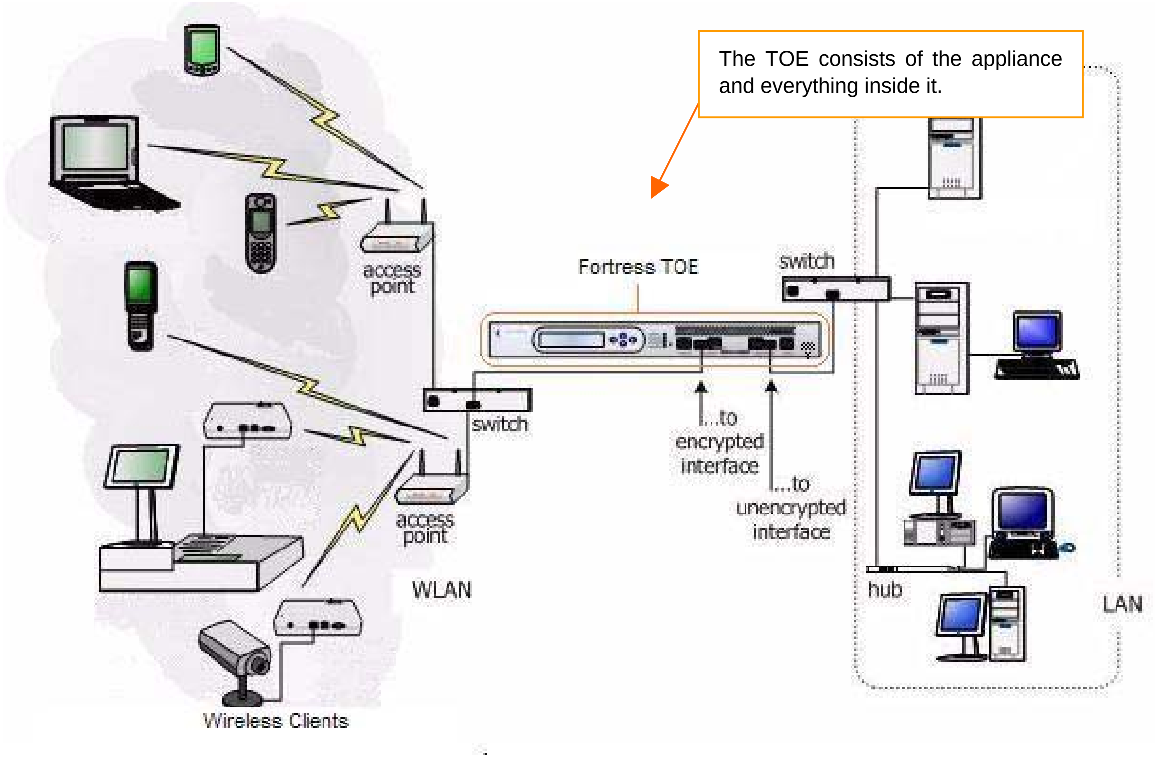
D) Aux interface – not used in the evaluated configuration

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.
Fortress TOE
switch
access point
switch
...to encrypted interface
...to unencrypted interface
access point
WLAN
hub
LAN
Wireless Clients

2.1.2 Logical Boundary

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.

2.1.2.1 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. When a security policy has been violated, an audit record is generated. Additionally, when an administrator logins in or changes configuration, an audit record is generated. In all cases, timestamps are applied to audit records and the FSG supplies its own timestamps.

2.1.2.2 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.

2.1.2.3 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.

2.1.2.4 Identification and Authentication

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

2.1.2.5 Security Management

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

A) Admin* – The privileged account has full permissions to manage the FSG. This account is accessible via AFWeb.

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

C) Sysadm* – This account once in Privileged mode (superset of functions) has full permissions to manage the FSG. This account is accessible via FISh.

The TOE 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.

* = Admin and sysadm are synonymous and will be referred to as Admin throughout this document.

2.1.2.6 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.

2.1.3 TOE Data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information.

Security attributes enable the TOE to enforce the security policy. Authentication data enables the TOE to identify and authenticate users.

Users are administrators that manage the TOE. Subjects are IT systems on the LAN or WLAN sides that transmit network packets to the TOE to be forwarded to the other network. The network packets represent information that the TOE controls the flow of. There are no objects.

Table 1 - TOE Data

Name	Description	AD	UA	SA	IA	GE
System date/time settings	The system date and time settings enable the TOE to make decisions about timeout and re-keying applications. Without time settings, the TOE cannot determine how to perform connection timeouts and re-keying intervals.					✓
Encryption algorithm	The encryption algorithm instructs the TOE on how to encrypt the data.					✓
Access ID	A 14-digit hexadecimal string configured in the TOE. All endpoints that attempt to communicate with the TOE must be configured with the same Access ID.					✓
Re-keying interval	The re-keying interval instructs the TOE on how often to change its encryption keys					✓
Role	The TOE user ‘admin’ via AFWeb and ‘sysadm’ via FISh are used to login as an administrator.		✓			
Password	The password enables the TOE to either authenticate, or fail to authenticate, an administrator.	✓				
Bypass list	A list of WLAN tuples (MAC address, IP address and TCP/UDP ports) that are permitted to send and receive plaintext traffic. The bypass list also specifies if each system is permitted to initiate communication with a LAN system or if it can only respond to communication initiated by a LAN system.					✓
Hotspot VLAN ID	Plaintext traffic received from the WLAN that is authorized to be forwarded (via the bypass list) may be mapped to a specified Hotspot VLAN ID when forwarded to the LAN side.					✓
Hard Key	The key is generated using the common Access ID and is used to protect information being exchanged during the Diffie-Hellman Static Key exchange and as a broadcast key.			✓		
Endpoint Static Private Key	The key generated for each endpoint at initial connection startup that is kept secret.			✓		
Endpoint Static Public Key	The key generated from the Endpoint Static Private Key and shared with the specific endpoint using the Diffie-Hellman key agreement protocol.			✓		

Name	Description	AD	UA	SA	IA	GE
Endpoint Static Common Secret Key (SKey)	The key generated for each endpoint using the FSG's Endpoint Static Private Key for that endpoint and the static public key communicated by the endpoint during the Diffie-Hellman key exchange. The Endpoint Static Common Secret Key is used to protect the Diffie-Hellman dynamic key exchange.			✓		
Endpoint Dynamic Private Key	The key is generated for each endpoint periodically during the lifetime of the session with each endpoint and is kept secret.			✓		
Endpoint Dynamic Public Key	The key generated from the Endpoint Dynamic Private Key and shared with the specific endpoint using the Diffie-Hellman key agreement protocol.			✓		
Endpoint Common Secret Key (DKey)	The key generated for each endpoint using the FSG's Endpoint Dynamic Private Key for that endpoint and the dynamic public key communicated by the endpoint during the Diffie-Hellman key exchange. The Endpoint Common Secret Key is used to protect the Diffie-Hellman dynamic key exchange.			✓		
Endpoint identifier	MAC address that uniquely identifies an IT system on the wireless network			✓		
Presumed source endpoint identifier	When a network packet is received from the wireless network, the source MAC address is the presumed source endpoint identifier				✓	
Presumed source IP address	When a plaintext network packet is received from the WLAN side, the source IP address is the presumed source IP address				✓	
Presumed source TCP/UDP port	When a plaintext network packet is received from the WLAN side, the source TCP or UDP port is the presumed source TCP/UDP port				✓	
Destination endpoint identifier	When a network packet is received from either network, the destination MAC address included in the network packet is the destination endpoint identifier.				✓	
Destination IP address	When a network packet is received from either network, the destination IP address included in the network packet is the destination identifier.				✓	
Destination TCP/UDP port	When a network packet is received from either network, the destination IP address included in the network packet is the destination identifier.				✓	

Legend: AD=Authentication data; UA=User attribute; SA=Subject attribute; IA=Information attribute; GE=Generic Config. Information

2.1.4 Rationale for Non-Bypassability and Separation

The FSG is a device that includes firmware that executes on top of an underlying hardware system. Together, the firmware application and underlying hardware make up the TOE.

The TOE is protected from interference. The firmware is not a general purpose operating system and does not allow generic users to introduce new processes or executable code to the system. The audit trail is entirely contained within the TOE and cannot be access unless you login into the TOE with a valid administrator account. Arbitrary entry into the TOE is not possible and therefore the TSF is protected against external interference by untrusted objects.

The TOE provides strictly controlled functionality to the users within the TSC. By limiting access through role based access control, the TSF is protected from corruption or compromise.

2.2 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.

2.2.1 Evaluated Configuration Options

A) The FSG operates in FIPS-enabled operational mode at all times after initial configuration. In this mode, the following functionality is not supported:

  1) SNMP

  2) Remote logging of audit information

B) 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.

C) Failover (to a second FSG appliance) functionality is not evaluated. This functionality requires additional security claims not common to stand-alone mode.

D) 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.

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2 - Assumptions

A.Type	Description
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	Administrative users are trusted to be non-hostile within the scope of their role.

3.3 Threats

The threats to security that are addressed are found in the following table:

Table 3 - Threats

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

3.4 Organisational Security Policies

The TOE requires the enforcement of Organisational Security Policies as listed in the following table:

Table 4 - Organisational Security Policies

Policy	Policy Description
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 TOE provides accountability to the granularity of the administrator role. If there are multiple authorized administrators, they share the same login and do not have individual accounts.
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.

CHAPTER 4

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's environment. The security objectives identify the responsibilities of the TOE, the TOE's environment. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the objectives listed in the following table:

Table 5 - Security Objectives for the TOE

O.Type	Security Objective
O.ACCESS	All administrators are required to authenticate with passwords that cannot be easily guessed before performing any management functions.
O.AUDIT	The TOE detects security relevant events and creates audit event records.
O.AUDIT_PROTECTION	The TOE provides the capability to protect audit information from unauthorized access.
O.CRYPTOGRAPHY	For all cryptographic functions addressed by FIPS 140-2, the TOE cryptographic functions are validated via CAVP or CMVP.
O.ENCRYPT	The confidentiality and integrity of information exchanged with wireless endpoints are protected using FIPS validated encryption algorithms automatically performed by the TOE, unless explicitly authorized for plaintext operation.
O.KEY_EXCHANGE	The TOE is able to securely and transparently exchange encrypted secret keys without any human action, and regenerate them at every power-up and periodically during operation.
O.MANAGE	The TOE provides mechanisms for secure management of the TOE.
O.SELF_PROTECTION	The TSF maintains a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.RBAC	The TOE prevents users from gaining access to and performing operations on its resources for which their role is not explicitly authorized by establishing the Role Based Access Control (RBAC) principle.
O.TEST	The TSF is tested to ensure the correct operation occurs at a customer's site.

4.2 Security Objectives for the Environment

The TOE's environment must satisfy the objectives listed in the following table:

Table 6 - Security Objectives for the Environment

OE.Type	IT Environment Security Objective
OE.INSTALL	The administrator installs the TOE in accordance with the installation and guidance documentation supplied with the TOE.

OE.Type	IT Environment Security Objective
OE.KEY	The administrator configures all wireless endpoints that will communicate via the TOE with the same Access ID configured in the TOE.
OE.SECURE	The customer provides a physically secure facility to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators are able to access such functionality.
OE.TRAINING	All personnel given administrator privileges, or who perform crypto-custodian duties, are given training. The training shall include giving the class attendants appropriate documentation, sufficient to enable them to fulfill their duties in a secure fashion.
OE.TRUST	Only trusted personnel are given privileges to operate the TOE.

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

5.1 TOE Security Functional Requirements

The functional requirements for the TOE consist of the following components derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* - with the exception of NIAP interpretations and completed operations. The TOE Security Functional Requirements are listed in the following table:

Table 7 - TOE Security Functional Requirements

Component	Name
FAU_GEN.1-NIAP-0347	Audit Data Generation
FAU_GEN.2-NIAP-0410	User Identity Association
FAU_SAR.1	Audit Review
FAU_STG.1-NIAP-0429	Protected Audit Trail Storage
FAU_STG.4-NIAP-0407	Prevention of Audit Data Loss
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1-NIAP-0407	Simple Security Attributes
FIA_SOS.1	Verification of Secrets
FIA_UAU.2	User Authentication Before Action
FIA_UID.2	User Identification Before Management
FMT_MOF.1	Management of Security Functions Behavior
FMT_MSA.1	Management of Security Attributes
FMT_MSA.2	Secure Security Attributes
FMT_MSA.3	Static Attribute Initialization
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	Partial TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FPT_TST.1	TSF Testing
FTP_TRP.1	Trusted Path

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1-NIAP-0347 Audit Data Generation

FAU_GEN.1.1-NIAP-0347 The TSF generates audit records of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *All auditable events identified in the table below.*

Auditable events and details with applicable SFRs are listed in the following table:

Table 8 - Auditable Events and Details

Component	Auditable Event	Details
FAU_GEN.1-NIAP-0347	None	Not applicable
FAU_GEN.2-NIAP-0410	None	Not applicable
FAU_SAR.1	None	Not applicable
FAU_STG.1-NIAP-0429	None	Not applicable
FAU_STG.4-NIAP-0407	None	Not applicable
FCS_CKM.1	Cryptographic key generation	Success or Failure, type of key, associated endpoint
FCS_CKM.4	Cryptographic key destruction	
FCS_COP.1	Crypto Engine Errors Hashing Errors Compression Errors Key Engine Errors Bootstrap Errors Self Test Failure Code Failure Key agreement	Failure in cryptographic processing Hashing Engine fails Packet can't be compressed Cannot generate key Startup process did not operate correctly Self Test failure during device operation Fatal Trap occurred in code Result, type of key, associated endpoint
FDP_IFC.1	System and communication errors detected.	Not applicable
FDP_IFF.1-NIAP-0407	Discarding network packets, bypass forwarding	Not applicable
FIA_SOS.1	System configurations changes made by the administrator	Passwords
FIA_UAU.2	All use of the authentication mechanism	User id, Success or Failure
FIA_UID.2	None	Not applicable
FMT_MOF.1	All modifications in the behavior of the functions in the TSF	In FIPS mode only by the administer (cryptographic officer)
FMT_MSA.1	System configurations changes made by the administrator	Access ID
FMT_MSA.2	None	Not applicable
FMT_MSA.3	None	Not applicable
FMT_MTD.1	System configurations changes made by the administrator	Access ID, Admin password, Bypass list, Cryptographic keys, Encryption algorithm, Hotspot VLAN ID, Operator password, Re-keying interval, System time and date
FMT_SMF.1	None	Not applicable
FMT_SMR.1	None	Not applicable
FPT_RVM.1	None	Not applicable

Component	Auditable Event	Details
FPT_SEP.1	None	Not applicable
FPT_STM.1	None	Not applicable
FPT_TST.1	Execution of the TSF self tests	Result
FTP_TRP.1	None	Not applicable

FAU_GEN.1.2-NIAP-0347 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components, *the additional information identified in the table above, column 3*.

5.1.1.2 FAU_GEN.2-NIAP-0410 User Identity Association

FAU_GEN.2.1-NIAP-0410 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *the admin and operator roles* with the capability to read *all audit information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.4 FAU_STG.1-NIAP-0429 Protected Audit Trail Storage

FAU_STG.1.1-NIAP-0429 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2-NIAP-0429 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

5.1.1.5 FAU_STG.4-NIAP-0407 Prevention of Audit Data Loss

FAU_STG.4.1-NIAP-0407 The TSF shall overwrite the oldest stored audit records and take no other actions if the audit trail is full.

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *as described below* and specified cryptographic key sizes *as described below* that meet the following *standards described below*:

Table 9 - Cryptographic Key Generation

Algorithm	Key Size in Bits	Standards
SHS (SHA-1) Cert #615	160, 384	FIPS 180-2

5.1.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *FIPS 140-2*

5.1.2.3 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform *the operations described below* in accordance with a specified cryptographic algorithm *multiple algorithms in the modes of operation described below* and cryptographic key sizes *multiple key sizes described below* that meet the following *multiple standards described below*:

Table 10 - Cryptographic Operations

Operation	Algorithm (mode)	Key Size in Bits	Standards
Encryption and decryption	Triple-DES (CBC) Cert #546	192	FIPS 46-3
	AES (CBC, ECB) Cert #550	128, 192, 256	FIPS 197
	DES (vendor affirmed)	56	FIPS 46-3
	IDEA (vendor affirmed)	128	U.S. Patent # 5,214,703
	RC2 (vendor affirmed)	40	RFC 2268
	RC4 (vendor affirmed)	40	RSA Security
	RC5 (vendor affirmed)	128	RSA Security
Key agreement	Diffie-Hellman (vendor affirmed)	512	RFC 2631
Message authentication coding	HMAC (SHA-1) Cert #291	128, 160	FIPS 198
	HMAC (MD5) (vendor affirmed)	128, 160	FIPS 198
Hashing	SHS Cert #615	128, 160	FIPS 180-2
	MD2 (vendor affirmed)	128	RFC 1319
	MD5 (vendor affirmed)	128, 160	RFC 1321
Random Number Generation	PRNG Cert #318	Not Applicable	ANSI X9.17

5.1.3 User Data Protection (FDP)

5.1.3.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *Packet Flow Control SFP* on *subjects: IT systems connected to the WLAN or LAN that send network packets to the TOE; information: network packets received by the TOE; operations: packet forwarding.*

5.1.3.2 FDP_IFF.1-NIAP-0407 Simple Security Attributes

FDP_IFF.1.1-NIAP-0407 The TSF shall enforce the *Packet Flow Control SFP* based on the following types of subject and information security attributes:

A) *Subject: IT system on the LAN*

1) *None*

B) *Subject: IT system on the WLAN*

1) *Endpoint identifier (MAC Address)*

2) *Endpoint Common Secret Key*

C) *Information: network packet received by the TOE from the LAN*

1) *Destination MAC address*

2) *Destination IP address*

3) *Destination TCP/UDP port*

D) *Information: network packet received by the TOE from the WLAN*

1) *Presumed source endpoint identifier*

2) *Presumed source IP address*

3) *Presumed source TCP/UDP port*

FDP_IFF.1.2-NIAP-0407 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

A) *A unicast network packet received by the TOE from the LAN is encrypted using the Endpoint Common Secret Key for that endpoint and forwarded to the WLAN.*

B) *A multicast or broadcast network packet received by the TOE from the LAN is encrypted using the Hard Key and forwarded to the WLAN. If bypass operations are configured, the network packet is also forwarded in plaintext.*

C) *A unicast network packet received by the TOE from the WLAN is decrypted using the Endpoint Common Secret Key for that endpoint and forwarded to the LAN side.*

D) *A multicast or broadcast network packet received by the TOE from the WLAN is decrypted using the Hard Key and forwarded to the LAN.*

FDP_IFF.1.3-NIAP-0407 The TSF shall enforce the following information flow control rules: no additional information flow control SFP rules.

FDP_IFF.1.4-NIAP-0407 The TSF shall provide the following *additional SFP capabilities for plaintext traffic exchanges:*

A) *If the destination MAC address, IP adresss, and the TCP/UDP port is matched in the bypass list (Trusted Devices' List), then the network packet is forwarded to the WLAN endpoint without being encrypted. .*

B) *If the presumed source endpoint identifier, presumed source IP address, and presumed source TCP/UDP port of a plaintext network packet received from a WLAN system match a bypass list entry, the following rules apply:*

1) *If the session is already established, the network packet is forwarded.*

2) *If the session is not already established but the bypass list entry authorizes the WLAN endpoint to initiate sessions, the network packet is forwarded.*

3) *If the session is not already established and the bypass list entry does not authorize the WLAN endpoint to initiate sessions, the network packet is discarded.*

4) *If a Hotspot VLAN ID is enabled (default setting is off), all received plaintext network packets are forwarded to that single isolated Hotspot VLAN when transmitted.*

C) *If the presumed source endpoint identifier, presumed source IP address, and presumed source TCP/UDP port of a plaintext network packet received from a WLAN system do not match a bypass list entry, the network packet is discarded.*

FDP_IFF.1.5-NIAP-0407 The TSF shall explicitly authorise an information flow based upon the following rules: no explicit authorisation rules.

FDP_IFF.1.6-NIAP-0407 The TSF shall explicitly deny an information flow based upon the following rules:

A) *If a network packet is received from a wireless endpoint on the WLAN but the decryption is not valid (i.e., the integrity vector is not correct), the network packet is discarded.*

5.1.4 Identification and Authentication (FIA)

5.1.4.1 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet 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*.

5.1.4.2 FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

Application Note: If the user is not authenticated the network packets are dropped and no passing of traffic is allowed.

5.1.4.3 FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each user to identify itself before any other TSF-mediated actions on behalf of that user. Security Management (FMT)

5.1.4.4 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of the functions *the functions listed in the table below* to *the admin and operator roles, as shown in the table below*.

Table 11 - Management of Security Functions

Security Function	Admin				Oper.
	Determine	**Disable**	**Enable**	**Modify**	**Determine**
Bypass operations	✓	✓	✓	✓	✓
Cryptographic Operations	✓	✓	✓	✓	✓
Hotspot VLAN ID insertion	✓	✓	✓	✓	✓

5.1.4.5 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the *Packet Flow Control SFP* to restrict the ability to modify the security attributes *Access ID* to *the admin role*.

Application Note: Although the Access ID is not directly referenced as a security attribute in the Packet Flow Control SFP, the Endpoint Common Secret Key can't be established until the Access ID is supplied by the admin.

5.1.4.6 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the *Packet Flow Control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *no roles* to specify alternative initial values to override the default values when an object or information is created.

5.1.4.7 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete the *data described in the table below* to *the authorised administrator roles as described in the following table.*

Table 12 - Management of TSF Data

TSF Data Description	Admin			Operator		
	Query	**Delete**	**Modify**	**Query**	**Delete**	**Modify**
Access ID	✓		✓	✓		
Admin password	✓		✓			
Bypass list	✓		✓	✓		
Cryptographic keys		✓				
Encryption algorithm	✓		✓	✓		
Hotspot VLAN ID	✓	✓	✓	✓		
Operator password	✓		✓			
Re-keying interval	✓		✓	✓		
System time and date	✓		✓	✓		

5.1.4.8 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

A) Manage cryptographic operations

B) Manage TSF data

C) Manage bypass operations

D) Manage support for the Hotspot VLAN

5.1.4.9 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *admin and operator*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.2 FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.3 FPT_STM.1 Reliable Time Stamps

FTP_STM.1.1 The TSF shall be able to provide reliable time-stamps for its own use.

5.1.5.4 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests during initial start-up to demonstrate the correct operation of *the cryptographic module portion of the TSF*.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *the TSF configuration data*.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.6 Trusted Path/Channels (FTP)

5.1.6.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *remote administrator sessions*.

5.2 Security Requirements for the IT Environment

No security requirements are levied on the IT Environment.

5.3 TOE Security Assurance Requirements

The TOE meets the assurance requirements for basic robustness: EAL3 augmented. These requirements are summarised in the following table:

Table 13 - TOE Security Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
	ADV_HLD.1	Descriptive High-Level Design
	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Life Cycle Support	ALC_FLR.2	Flaw Reporting Procedures
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.1	Examination of Guidance
	AVA_SOF.1	Strength of TOE Security Function Evaluation
	AVA_VLA.1	Developer Vulnerability Analysis

5.4 Strength of Function for the TOE

The only probabilistic or permutational mechanism in the product is the password mechanism used to authenticate users (FIA_SOS.1). The SOF for this mechanism is SOF-Basic.

5.5 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale:

Table 14 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1-NIAP-0347	No other components.	FPT_STM.1	Satisfied
FAU_GEN.2-NIAP-0410	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied by FAU_GEN.1-NIAP-0347 Satisfied by FIA_UID.2
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied by FAU_GEN.1-NIAP-0347
FAU_STG.1-NIAP-0429	No other components.	FAU_GEN.1	Satisfied by FAU_GEN.1-NIAP-0347
FAU_STG.4-NIAP-0407	FAU_STG.3	FAU_STG.1	Satisfied by FAU_STG.1-NIAP-0429
FCS_CKM.1	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Satisfied Satisfied Not satisfied. This SFR is not required because there is no user input for security attributes for key generation; key generation is performed automatically by the TOE.
FCS_CKM.4	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Satisfied Not satisfied. This SFR is not required because there is no user input for security attributes for key destruction.
FCS_COP.1	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Satisfied Satisfied Not satisfied. This SFR is not required because there is no user input for security attributes for cryptographic operations; cryptographic operations are performed automatically by the TOE.
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied by FDP_IFF.1-NIAP-0407
FDP_IFF.1-NIAP-0407	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied Satisfied
FIA_SOS.1	No other components.	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	FIA_UID.1	None	n/a
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied

SFR	Hierarchical To	Dependency	Rationale
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2
FPT_RVM.1	No other components.	None	n/a
FPT_SEP.1	No other components.	None	n/a
FPT_STM.1	No other components.	None	n/a
FPT_TST.1	No other components.	None	Satisfied
FTP_TRP.1	No other components.	None	n/a

CHAPTER 6

6. TOE Summary Specification

6.1 Security Functions

6.1.1 Audit

Starting and stopping of the audit function is recorded by the FSG in the log file. The FSG also logs other significant event information including:

A) Key generation – result, type of key, and associated wireless endpoint

B) Key distribution - result, type of key, and associated wireless endpoint

C) Key destruction - result, type of key, and associated wireless endpoint

D) Administrative login attempts – account, result

E) Changes to the cryptographic operations – change

F) Self-test information - result

G) System configuration changes – changed parameter and value

H) Bypass operations – Enabled or Disabled

Every event recorded in the log file includes a date and time stamp and the type of event. When applicable, the event also includes the subject identity associated with the event and the outcome. The identity of the system that causes specific auditable events is marked in the event log by either its IP address or MAC address.

Authorized administrators (admin and operator) have the ability to access and read all auditable events using the View Log information on the Monitor interface of AFWeb. The auditable events are categorized into columns making it user friendly and easy for the authorized administrator to interpret the information. When View Log is selected, the log file that is actually read is `dns.log` stored in the `/LOGS` directory. The log file is kept in a partition separate from the rest of the TOE firmware to prevent it from overflowing into the / directory.

The log can contain a maximum of approximately 7000 log messages (approximate because record sizes vary somewhat). When the log is full, the oldest records are deleted to make space for new records. The FSG does not provide any administrator mechanism to modify or delete audit records.

6.1.2 Packet Encryption / Decryption

This security function is focused on the packet encryption and decryption that occurs specifically for packets exchanged with wireless endpoints. On the FSG, encryption happens at the MAC layer so that all network layer information is concealed (other than bypass operations). Each FSG uses the following key types:

A) A Hard Key common to the FSG and all wireless endpoints that communicate through it (based on the Access ID). The Hard Key is used to protect the SKey negotiation and to protect multicast and broadcast packets.

B) An Endpoint Static Common Secret Key (SKey) per wireless endpoint used to protect the dynamic key exchange

C) An Endpoint Common Secret Key (DKey) per wireless endpoint used to protect network packets.

The Access ID is a 16 digit hexadecimal number that is configured by the administrator. The unit's secret key is a SHA-1 hash-function of the Access ID. The Access ID must be common to the FSG and all wireless endpoints that intend to communicate with encrypted packets through an FSG. The Hard Key is used for broadcast traffic sent to all wireless endpoints. This key is used to protect the key exchange to generate an SKey with a specific wireless endpoint via a Diffie-Hellman exchange, which utilizes the PseudoRandom Number Generator of the FSG.

Once established, the SKey for a specific wireless endpoint is used to distribute the information used to establish the dynamic session key (DKey) for the same wireless endpoint. This process again utilizes a Diffie-Hellman exchange and the PseudoRandom Number Generator of the FSG. The DKey is maintained until it is refreshed or the FSG is restarted or all keys are zeroized. The DKey is used to encrypt and decrypt network packets exchanged with the wireless endpoints.

Network packet encryption and decryption for WLAN endpoints occurs with a single algorithm configured for all operations. The administrator may specify either Triple-DES (192 bit keys) or AES (128, 192, or 256 bit keys).

6.1.3 Information Flow

The FSG controls network packets flowing between the wireless WLAN and the LAN. Network packets flowing from the LAN to a wireless endpoint on the WLAN are normally encrypted to prevent disclosure or modification. Devices that do not support cryptographic services may be configured to work in bypass mode, which permits specific traffic flows (specified by MAC address, IP address, and TCP/UDP port) to be forwarded without encryption. The following rules are used to determine the key used to encrypt network packets:

A) The DKey established for the unicast destination endpoint identifier specified in the network packet. If the DKey has not yet been established, outgoing packets are queued.

B) The Hard Key is used for multicast and broadcast network packets. Note that when bypass operations are configured, these packets are also sent in plaintext.

Network packets received from the WLAN to be forwarded to the LAN must be encrypted with an appropriate key (unless authorized for bypass operations), assuring the integrity of the received data. An appropriate key could be:

A) The HKey for multicast and broadcast traffic.

B) The DKey associated with the source MAC address of the network packet for unicast traffic.

If a network packet is received encrypted and its integrity cannot be verified when decrypted (i.e., the correct key was not used to encrypt the network packet), the FSG discards that network packet.

Bypass operations may be configured for WLAN endpoints to enable their traffic to flow through the FSG without encryption and decryption. Permitted traffic flows are configured with the WLAN system's MAC and IP addresses as well as a list of TCP/UDP ports. Each WLAN system may be permitted to initiate traffic to LAN systems or only to respond to sessions initiated by a LAN system. Network packets that match one of the configured traffic flows are forwarded. Network packets that do not match a configured traffic flow are discarded. If a Hotspot VLAN ID is configured in the system, then all bypass traffic forwarded to the LAN side includes the Hotspot VLAN ID in the transmitted network packet.

6.1.4 Identification and Authentication

Identification and Authentication is performed on the administrator interfaces - Fortress Interface Shell (FISh) and AFWeb. No functions can be performed unless an administrator logs into the FSG with a valid account and password. The only valid account for FISh is "sysadm" while AFWeb supports the "admin" and "operator" accounts. Both sysadm and admin are associated with the admin role, while the operator account is associated with the operator role.

Each password is selectable by an admin according to the following rules: consisting of 8-16 mixed case characters including at least one each upper case, one lower case, one numeric, and one special character. (An example of an approved password is `emPagd2!.)`

6.1.5 Security Management

There are two levels of administrator access to AFWeb: *Admin* and *Operator,* corresponding to the admin and operator roles respectively. The Fortress Interface Shell (FISh) supports *Admin* mode only. *Operator* mode is view-only, and permits only a subset of functionality to be executed. With AFWeb, different screens are presented to the different access levels.

Only the admin role has the ability to modify configuration settings. The configuration settings available to the accounts are shown in the following table. "R" indicates the parameter may be read, "C" indicates the parameter may be read and changed, while "D" indicates the value may be deleted.

Table 15 - Security Management Access

Name	admin	operator
Access id	C	R
Admin password	C	
Bypass list	C	R
Cryptographic keys	D	
Encryption algorithm	C	R
Hotspot VLAN ID	C,D	R
Operator password	C	
Re-keying interval	C	R
System date/time settings	C	R

Interfaces exist for both sysadm and admin to disable and enable the cryptographic operations. However, the evaluated configuration calls for cryptographic operations to be enabled at all times (after initial configuration); therefore, these interfaces are not invoked during normal operation.

Configuration of the Access ID is restricted to a 16 digit hexadecimal value. By default wireless endpoints without the required Access ID are blocked from communicating through the FSG.

AFWeb sessions are initiated by the remote user. Communication between the FSG and the remote user utilizes OpenSSL in the FSG to provide integrity and privacy. OpenSSL supports the Secure Sockets Layer (SSL v2/v3) or Transport Layer Security (TLS v1) protocols. The end user specifies the selection of SSL or TLS as well as the specific mode of operation when communication is initiated. The FSG supports the defined cipher suites in SSL v2, SSL v3 and TLS v1.

6.1.6 Protection of the TOE

The TOE is implemented as a stand-alone appliance that does not permit users to introduce general-purpose executable code onto the appliance. Administrators are required to authenticate before performing any management functions. Interfaces made available to administrators are well defined and have controlled functionality. The FSG performs all cryptographic operations automatically without human input.

Self-tests execute when the system starts, periodically during system execution, and on command of an admin. The self-tests exercise the cryptographic module to verify its correct operation, and if any failure is detected the FSG enters a failed mode. Failure of any self-test listed above 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. Successful results of the self-tests are stored in the audit log for review. The Configuration Database on the TOE is integrity checked. Any errors will make the Configuration Database unusable. The audit log file is currently a flat text file that is not checked.

6.2 Assurance Measures

Assurance Class	Component ID	Document satisfying Assurance Component
Configuration Management	ACM_CAP.2	The following Configuration Management procedures are described in this documentation: • Use of the CVS tool for revision control • Use of documented procedures for product builds • Use of documented procedures for product test • Use of documented procedures for release to manufacturing • Use of documented procedures for distribution to customers • List of configuration items and evidence that they are maintained by the CVS tool

Assurance Class	Component ID	Document satisfying Assurance Component
Delivery and Operation	ADO_DEL.1	This document includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.
	ADO_IGS.1	These documents describe the procedures necessary for secure installation, generation, and start-up of the TOE.
Development	ADV_FSP.1	These documents provide the purpose and method of use of all external TSF interfaces and completely represent the TSF.
	ADV_HLD.1	These documents describe the high-level design and the security functionality provided by each subsystem of the TSF. These documents also identify the interfaces, and the interfaces to the subsystems.
	ADV_RCR.1	The correspondence between the TOE security functions and the high-level design subsystems is described in these documents.
Guidance Documents	AGD_ADM.1	Guidance to administrators is effectively supported by the listed documentation for this requirement.
	AGD_USR.1	Guidance to non-administrative users is effectively supported by the listed documentation for this requirement.
Life Cycle Support	ALC_FLR.2	These documents describe flaw remediation guidance and enables users to submit reports back to the developers
Tests	ATE_COV.1	These documents map tests to the functional specification, and to the testing data.
	ATE_FUN.1	These documents describe the functional and penetration tests performed including their results.
	ATE_IND.2	These documents describe the functional and penetration tests performed and their results
Vulnerability Assessment	AVA_MSU.1	An analysis of the user provided documentation describing the installation and configuration, the administrator interfaces and commands is performed by the evaluation team to ensure the documentation is consistent and provide all the required guidance for an administrator to install, configure and administer the TOE in a secure manner.
	AVA_SOF.1	These documents include a strength of function analysis to support the SOF-basic claim. The analysis includes identifying the TOE password space and probability of a password being compressed.
	AVA_VLA.1	These documents describe the vulnerability analysis performed and the results of the analysis.

6.3 Strength of Function Claim

The only probabilistic or permutational mechanism in the product is the password mechanism used to authenticate users (Identification and Authentication). The SOF for this mechanism is SOF-Basic.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This security target makes no conformance claims to any Protection Profile.

7.2 Protection Profile Refinements

Not applicable. See 7.1

7.3 Protection Profile Additions

Not applicable. See 7.1

7.4 Protection Profile Rationale

Not applicable. See 7.1

CHAPTER 8

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

8.1 Rationale for IT Security Objectives

This section demonstrates that the identified security objectives cover all aspects of the security needs - showing that each threat and assumption is addressed by one or more security objectives. The following table identifies for each threat, policy and assumption, the security objective(s) that address it:

Table 16 - Threats, Policies and Policies Mapped to Security Objectives

	O.ACCES	O.AUDIT	O.AUDIT_PROTECTION	O.CRYPTOGRAPHY	O.ENCRYPT	O.KEY_EXCHANGE	O.MANAGE	O.SELF_PROTECTION	O.RBAC	O.TEST	OE.INSTALL	OE.KEY	OE.SECURE	OE.TRAINING	OE.TRUST
T.AUDIT_ COMPROMISE			X					X							
T.CORRUPTION				X	X	X						X			
T.DISCLOSURE				X	X	X						X			
T.FAILURE										X					
T.MASQERADE	X														
P.ACCESS						X						X			
P.ACCOUNTABILITY	X	X	X												
P.AUTO					X	X									
P.CRYPTOGRAPHY				X											
P.MANAGE	X						X								
P.RECORD		X	X												
P.ROLES	X								X						
A.AREA													X		
A.DELIVERY											X			X	
A.NO_EVIL															X

8.1.1 Rationale Showing Threats, Policies and Assumptions to Security Objectives

The following table describes the rationale for the threat to security objectives mapping:

Table 17 - Threats, Policies, Assumptions Mapped to Security Obj. Rationale

Threat, Policy, or Assumption	Rationale
T.AUDIT_ COMPROMISE	O.AUDIT_PROTECTION and O.SELF_PROTECTION address this threat by restricting access to audit records.
T.CORRUPTION	O.CRYPTOGRAPHY, O.ENCRYPT, O.KEY_EXCHANGE and OE.KEY address this threat by ensuring that all cooperating systems have a common Access ID and that validated encryption is used to protect the integrity of all data exchanges between the TOE and wireless endpoints. Systems that are not concerned with corruption may be explicitly authorized for plaintext operation.
T.DISCLOSURE	O.CRYPTOGRAPHY, O.ENCRYPT, O.KEY_EXCHANGE and OE.KEY address this threat by ensuring that all cooperating systems have a common Access ID and that validated encryption is used to protect the confidentiality of all data exchanges between the TOE and wireless endpoints. Systems that are not concerned with disclosure may be explicitly authorized for plaintext operation.
T.FAILURE	O.TEST addresses this threat by ensuring the deployed system is tested for correct operation.
T.MASQERADE	O.ACCES addresses this threat by ensuring that administrators successfully perform the I&A process before gaining access to any TOE functionality.
P.ACCESS	O.KEY_EXCHANGE and OE.KEY address this policy by ensuring the Access ID is available to the TOE and all wireless endpoints that will communicate via the TOE and that key exchanges utilize the Access ID.
P.ACCOUNTABILITY	O.ACCES, O.AUDIT and O.AUDIT_PROTECTION address this policy by providing for audit generation of security relevant events performed by administrators and protecting the audit trail for subsequent analysis.
P.AUTO	O.ENCRYPT and O.KEY_EXCHANGE address this policy by ensuring that cryptographic operations are performed automatically by the TOE.
P.CRYPTOGRAPHY	O.CRYPTOGRAPHY addresses this policy by ensuring that all relevant cryptographic functions are validated by the appropriate program according to FIPS 140-2.
P.MANAGE	O.ACCES and O.MANAGE address this policy by providing secure management functions for properly authenticated administrators.
P.RECORD	O.AUDIT and O.AUDIT_PROTECTION address this policy by providing for audit generation of security relevant events and protecting the audit trail for subsequent analysis.
P.ROLES	O.ACCES and O.RBAC address this policy by providing multiple administrator roles with distinct privileges and requiring administrators to perform I&A to gain access to the functions of any role.
A.AREA	OE.SECURE addresses this assumption by providing a physically secure facility for the TOE.
A.DELIVERY	OE.INSTALL and OE.TRAINING address this assumption by ensuring trained personnel properly install the TOE.
A.NO_EVIL	OE.TRUST addresses this assumption by restricting operation of the TOE to trusted personnel.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives. The following table identifies for each TOE security objective, the SFR(s) that address it:

Table 18 - SFRs to Security Objectives Mapping

	O.ACCES	O.AUDIT	O.AUDIT_PROTECTION	O.CRYPTOGRAPHY	O.ENCRYPT	O.KEY_EXCHANGE	O.MANAGE	O.SELF_PROTECTION	O.RBAC	O.TEST
FAU_GEN.1-NIAP-0347		X								
FAU_GEN.2-NIAP-0410		X								
FAU_SAR.1			X							
FAU_STG.1-NIAP-0429			X							
FAU_STG.4-NIAP-0407			X							
FCS_CKM.1				X		X				
FCS_CKM.4				X						
FCS_COP.1				X	X	X				
FDP_IFC.1					X					
FDP_IFF.1-NIAP-0407					X					
FIA_SOS.1	X									
FIA_UAU.2	X									
FIA_UID.2	X									
FMT_MOF.1							X		X	
FMT_MSA.1							X		X	
FMT_MSA.3							X		X	
FMT_MTD.1						X	X		X	
FMT_SMF.1							X		X	
FMT_SMR.1							X			
FPT_RVM.1								X		
FPT_SEP.1								X		
FPT_STM.1		X								
FPT_TST.1										X
FTP_TRP.1							X			

The following table provides the details of TOE security objective(s):

Table 19 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	FIA_SOS.1, FIA_UAU.2 and FIA_UID.2 address this objective by

Security Objective	SFR and Rationale
	requiring administrators to perform I&A with defined accounts and passwords that are not easily guessed before they are able to perform any management function.
O.AUDIT	FAU_GEN.1-NIAP-0347, FAU_GEN.2-NIAP-0410 and FPT_STM.1 address this objective by providing for the generation of audit event records for security relevant events. The audit event records include a timestamp.
O.AUDIT_PROTECTION	FAU_SAR.1, FAU_STG.1-NIAP-0429 and FAU_STG.4-NIAP-0407 address this objective by permitting all administrators to review the audit log. Audit event records may not be modified or deleted by administrators. When the audit log is full, the oldest records are deleted to make room for new records.
O.CRYPTOGRAPHY	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 address this objective by requiring algorithms to have CAVP certificates and to be implemented in a CMVP validated cryptographic module. Diffie-Hellman is not addressed by FIPS 140-2 and is vendor affirmed to conform to the relevant RFC.
O.ENCRYPT	FCS_COP.1, FDP_IFC.1 and FDP_IFF.1-NIAP-0407 address this objective by stating the rules for traffic exchange with wireless endpoints. All traffic must be encrypted with either Triple-DES or AES unless explicitly authorized for plaintext operation. Any endpoints that do not have the common Access ID are prevented from passing encrypted traffic through the TOE.
O.KEY_EXCHANGE	FCS_CKM.1, FCS_COP.1 and FMT_MTD.1 address this objective by requiring Diffie-Hellman key agreement with wireless endpoints. This process uses SHS and PRNG. The lifetime of the session key is configured by the sysadm or admin.
O.MANAGE	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 and FTP_TRP.1 address this objective by defining the administrator roles and operations that may be performed by each. AFWeb interactions are protected from disclosure and modification.
O.SELF_PROTECTION	FPT_RVM.1 and FPT_SEP.1 address this objective by requiring that the TOE protect itself from bypass, interference and tampering.
O.RBAC	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 and FTP_TRP.1 address this objective by defining multiple roles and restricting the capabilities of the operator role.
O.TEST	FPT_TST.1 address this objective by requiring testing of the cryptographic module, verification of the integrity of TSF code and data, and testing of the abstract machine on which the TSF depends.

8.2.2 Rationale for Security Functional Requirements of the Environment Objectives

No security requirements are levied on the IT Environment.

8.2.3 Security Assurance Requirements Rationale

8.2.3.1 TOE Security Assurance Requirements Rationale

The TOE meets the assurance requirements for EAL3 augmented.

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market for targeted use in low risk environments.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3 from part 3 of the Common Criteria.

8.3 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs. The following tables provide a mapping between the TOE's Security Functions and the SFRs:

Table 20 - SFRs to TOE Security Functions Mapping

	Audit	Packet Encryption / Decryption	Information Flow	Identification & Authentication	Security Management	Protection of the TOE
FAU_GEN.1-NIAP-0347	X					
FAU_GEN.2-NIAP-0410	X					
FAU_SAR.1	X					
FAU_STG.1-NIAP-0429	X					
FAU_STG.4-NIAP-0407	X					
FCS_CKM.1		X				
FCS_CKM.4		X				
FCS_COP.1		X			X	
FDP_IFC.1			X			
FDP_IFF.1-NIAP-0407			X			
FIA_SOS.1				X		
FIA_UAU.2				X		
FIA_UID.2				X		
FMT_MOF.1					X	
FMT_MSA.1					X	
FMT_MSA.3					X	
FMT_MTD.1					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_RVM.1						X
FPT_SEP.1						X

	Audit	Packet Encryption / Decryption	Information Flow	Identification & Authentication	Security Management	Protection of the TOE
FPT_STM.1	X					
FPT_TST.1						X
FTP_TRP.1					X	

The following table describes the rationale for why security functions are mapped to specific SFRs.

Table 21 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1-NIAP-0347	**Audit** – The Audit SF addresses this SFR via generation of audits, including all the specific events called for by the SFR and the specific audit event record details.
FAU_GEN.2-NIAP-0410	**Audit** – The Audit SF addresses this SFR because user identity is included in the audit records. Depending on the type of audit, user identity might be the administrator role or the endpoint identifier for one of the wireless endpoints.
FAU_SAR.1	**Audit** – The Audit SF addresses this SFR because both administrator roles are able to view the audit records vie AFWeb and the information is presented in a human readable form.
FAU_STG.1-NIAP-0429	**Audit** – The Audit SF addresses this SFR because no mechanism ir provided for any user to delete or modify audit information.
FAU_STG.4-NIAP-0407	**Audit** – The Audit SF addresses this SFR because the oldest records are overwritten when the fixed-size audit file exceeds its space.
FCS_CKM.1	**Packet Encryption/Decryption** – The Packet Encryption/Decryption SF addresses this SFR because SHS is used to form the secret key from the Access ID.
FCS_CKM.4	**Packet Encryption/Decryption** – The Packet Encryption/Decryption SF addresses this SFR because the keys are destroyed when the FSG is restarted or when the admin role issues a zeroize command.
FCS_COP.1	**Packet Encryption/Decryption and Security Management** – The Packet Encryption/Decryption SF addresses this SFR because both AES and TDES are available as cryptographic algorithms to be specified by the admin role for use in protecting traffic exchanged with the wireless endpoints and the PRNG is used in the Diffie-Hellman process. All of the specified cryptographic operations are utilized in the support of SSL v2, SSL v3, or TLS v1, and of one those is required to establish an HTTPS connection to the AFWeb interface described in the Security Management SF.

SFR	SF and Rationale
FDP_IFC.1	**Information Flow –** The Information Flow SF addresses this SFR because the information flow control policy is defined in terms of IT systems on the LAN and wireless endpoints (subjects), network packets (information), and packet forwarding between the WLAN and LAN (operations).
FDP_IFF.1-NIAP-0407	**Information Flow –** The Information Flow SF addresses this SFR because the information flow control rules are specified according to attributes of the subjects and information specified in FDP_IFC.1.
FIA_SOS.1	**Identification and Authentication –** The Identification and Authentication SF addresses this SFR because passwords consist of 8-16 mixed case characters including at least one each upper case, one lower case, one numeric, and one special character.
FIA_UAU.2	**Identification and Authentication –** The Identification and Authentication SF addresses this SFR because all administrators must provide the correct password for the account they have specified before any other action is permitted.
FIA_UID.2	**Identification and Authentication –** The Identification and Authentication SF addresses this SFR because all administrators must identify themselves as one of the predefined accounts (sysadm for FISh, admin and operator for AFWeb) before any other action is permitted.
FMT_MOF.1	**Security Management –** The Security Management SF addresses this SFR because the admin and sysadm accounts have the ability to view and modify the cryptographic operation settings.
FMT_MSA.1	**Security Management –** The Security Management SF addresses this SFR because the Access ID may only be changed by the admin role.
FMT_MSA.3	**Security Management –** The Security Management SF addresses this SFR because wireless endpoints configured with the wrong Access ID are not permitted to exchange traffic with LAN systems.
FMT_MTD.1	**Security Management –** The Security Management SF addresses this SFR by providing the capability to manage the TSF data in the ways specified in the SFR.
FMT_SMF.1	**Security Management –** The Security Management SF addresses this SFR because the SF provides the ability to manage cryptographic operations and TSF data.
FMT_SMR.1	**Security Management –** The Security Management SF addresses this SFR because the admin and operator roles provide different access levels.
FPT_RVM.1	**Protection of the TOE –** The Protection of the TOE SF addresses this SFR because the controlled interfaces presented to users insures that the TSP is enforced.
FPT_SEP.1	**Protection of the TOE –** The Protection of the TOE SF addresses this SFR because the TOE executes in its own domain and users are not permitted to introduce new programs or processes to the TOE.
FPT_STM.1	**Audit –** The Audit SF addresses this SFR because the TOE provides timestamps that are saved in the audit records.
FPT_TST.1	**Protection of the TOE –** The Protection of the TOE SF addresses this SFR because the cryptographic module is exercised by the self tests. The self tests include verification of the integrity of the TSF code and configuration data.
FTP_TRP.1	**Security Management –** The Security Management SF addresses this SFR because SSL or TLS is used to protect the HTTPS traffic of the AFWeb users.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.

8.5 Strength of Function Rationale

SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." Because this ST identifies unsophisticated threat agents, SOF-basic was chosen.