MOTOROLA SOLUTIONS

Motorola
RFS7000 Wireless LAN Switch
and
AP-7131N Wireless Access Point
Security Target

Document Version
Version: 1.51
March 25, 2014

Prepared For:

InfoGard Laboratories, Inc.
709 Fiero Lane, Suite 25
San Luis Obispo, Ca 93401

Prepared By:
Gordon McIntosh
.

Notices:

TABLE OF CONTENTS

List of Tables

List of Figures

1 Security Target (ST) Introduction

The structure of this document is defined by CC v3.1r3 Part 1 Annex A.2, "Mandatory contents of an ST":

- Section 1 contains the ST Introduction, including the ST reference, Target of Evaluation (TOE) reference, TOE overview, and TOE description.
- Section 2 contains conformance claims to the Common Criteria (CC) version, package claims, as well as rationale for these conformance claims.
- Section 3 contains the security problem definition, which includes threats, Organizational Security Policies (OSP), and assumptions that must be countered, enforced, and upheld by the TOE and its operational environment.
- Section 4 contains statements of security objectives for the TOE, and the TOE operational environment as well as rationale for these security objectives.
- Section 5 contains definitions of any extended security requirements claimed in the ST.
- Section 6 contains the security function requirements (SFR), the security assurance requirements (SAR), as well as the rationale for the claimed SFR and SAR.
- Section 7 contains the TOE summary specification, which includes the detailed specification of the IT security functions

1.1 Security Target Reference

The Security Target reference shall uniquely identify the Security Target.

ST Title:	Motorola RFS7000 Wireless LAN Switch and AP-7131N Wireless Access Point Security Target
ST Version Number:	Version 1.51
ST Author(s):	Gordon D McIntosh and Robert Day
ST Publication Date:	March 25, 2014
Keywords:	Wireless

This Security Target describes the security aspects of the RFS7000-GR Wireless LAN Switch operating together with one or more AP-7131N Wireless Access Point(s) operating in adaptive mode, connected together via LAN. The AP-7131N is fully described as a standalone device in a separate Security Target [15], which is included by reference and therefore is considered a part of this Security Target, all information contained remains valid in this evaluation. This is done to clarify those aspects of operation of the devices operating together that may be obscured by combining both devices into a single, excessively complex security target.

Unless otherwise indicated, this Security Target describes the RFS7000 switch security features and the adaptive features of the AP-7131N not otherwise described in, or the differences to those described in [15]; these areas will be clearly indicated with "**AP-7131N Adaptive Mode:**".

1.2 Target of Evaluation Reference

The Target of Evaluation reference shall identify the Target of Evaluation.

TOE Developer	Motorola Solutions, Inc. 6480 Via Del Oro San Jose, CA, 95119
TOE Name:	Motorola RFS7000 RF Switch and AP-7131N Wireless Access Point
TOE Version[1]	Motorola RFS7000-GR RF Switch Hardware Version: RFS-7010-1000-WR, Rev. G

[1] The TOE is currently undergoing a FIPS re-certification; until completed, the version numbers will not match the FIPS documentation

Software Version: 4.1.4.0-029GR
Orderable SKUs:
RFS-7010-10010-GR Rev. B (licensed for 128 ports)
RFS-7010-10020-GR Rev. B (licensed for 256 ports)
RFS-7010-10030-GR Rev. B (licensed for 16 ports)
RFS-7010-100R0-GR Rev. B (licensed for zero ports)

Motorola AP-7131N Wireless Access Point
Software Version: 4.0.4.0-045GRN
Hardware Version AP-7131N-66040-FGR Rev. D (US Only)
AP-7131N-66040-FWW Rev. F (Worldwide use, except US)

1.3 Target of Evaluation Overview

1.3.1 TOE Product Type

The TOE is a distributed system, comprised of a RFS7000-GR RF Switch and one or more AP-7131N Wireless Access Point devices. A wireless switch is a hardware device used to control the operation of multiple wireless access points and to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices. A wireless Access Point (AP) is a hardware appliance used to provide secure Wireless Local Area Network (WLAN) connectivity between a set of wireless client devices and a wired network. The term wireless client is used interchangeably with mobile unit (MU) throughout this document.

1.3.2 TOE Usage

The intended usage of the TOE is to manage inbound and outbound traffic between a set of wireless client devices and a wired network.

1.3.3 TOE Major Security Features Summary

- Security Audit
  - Reports security relevant events to allow system administrators to detect, review, and analyze potential security violations.
- Cryptographic Support
  - Provides the underlying mechanisms to protect TSF code, TSF data, and user data as it is transmitted within the TOE
- User data protection
  - Provides secure user data transmission, and residual data protection mechanisms
- Identification and Authentication for administrators
  - Mandates authorized administrators to be uniquely identified and authenticated before accessing information stored on the system
- Security Management
  - Provides system administrators tools to manage the security features provided by the TOE
- Protection of the TSF
  - Provides accurate time reference, and self-test functions.
- TOE Access
  - Provides session control and access banner display.
- Trusted Path/Channels
  - Provides secure transmission of data to/from trusted entities in the IT environment
- Intrusion Detection
  - Rogue Access Point (AP) Detection
    - Provides detection of rogue access points that constitute threats to the TOE

1.3.4 TOE IT environment hardware/software/firmware requirement summary

The TOE IT operational environment is required to provide support for TOE security functions as follows:

- Audit (Syslog) Server
  - Provides the capability to store and protect audit information
  - Provides the capability to selectively view audit information
- RADIUS (AAA) Server
  - Provides external source for administrative and wireless user authentication
- NTP Server
  - Provides reliable time stamps
- LDAP Server
  - Provides external source for user database information and user authentication
- SFTP Server
  - Provides repository for backing up configuration files
- SNMP Server (Manager)
  - Provides a source for SNMP management and destination for SNMP Traps
    Requires the use of a MIB browser or equivalent SNMP Management software
  - Shown as Remote Administration in Figure 1 - Typical TOE deployment diagram

1.4 Target of Evaluation Description

This section describes the TOE physical and logical boundaries; the physical boundaries describe the TOE hardware, software and the related guidance documentation; the logical boundary describes what logical security features are included in the TOE.

The TOE, the Motorola RFS7000 RF Switch and AP-7131N Wireless Access Point, are LAN connected devices that manage inbound and outbound traffic on the wireless network; they are used to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices.

The evaluation covers model RFS7000 RF Switch with software version 4.1.4.0-029GR, and two models of the AP-7131N, the AP-7131N-66040-FGR Rev. D and the AP-7131N-66040-FWW Rev. F; both are shipped with identical software, version 4.0.4.0-045GRN.

The AP-7131N appliances protect data exchanged with wireless client devices using IEEE 802.11i wireless security protocol; the RFS7000 provides additional capabilities for management and user data protection. In the evaluated configuration, one RFS7000 appliance manages multiple AP-7131N appliances; supporting up to 1024 AP-7131N wireless access points.

The RFS7000 portion of the TOE is a rack-mounted hardware appliance in a 1U chassis; it includes four (4) Gigabit Ethernet ports, which provide network connectivity, and one (1) 100Mbit Ethernet port (unused). An RS-232 serial interface (using RJ-45 connector) is used for local administration; this is also referred to as the console.

The AP-7131N portion of the TOE includes two (2) Ethernet ports (one (1) for LAN, one (1) for WAN), one (1) serial port, six (6) LEDs, one (1) reset button and six (6) antennas. Refer to [15] for additional information.

As shown in Figure 1 - Typical TOE deployment diagram, the TOE supports local and remote management options through the RFS7000 switch; however, remote management of the AP-7131N portion of the TOE operating in the adaptive mode is also supported. In the adaptive mode, the AP-7131N interacts with a RFS7000 switch; receiving configuration data from the RFS7000, allowing the RFS7000 to manage the AP-7131N remotely. The RFS7000 does not have its own radio interfaces; it uses the radio interfaces of the adopted APs to support 802.11a/b/g/n standards.

As mentioned in Section 1.1, the AP-7131N is fully described as a standalone device in a separate Security Target, The Motorola AP-7131N Wireless Access Point Security Target. [15] This Security Target

describes the RSF-7000 security features and the additional security features of the AP-7131N operating in the adaptive mode, or differences between the standalone mode and adaptive mode. Unless otherwise indicated, the security features of the AP-7131N are as described in [15] and are included by reference.

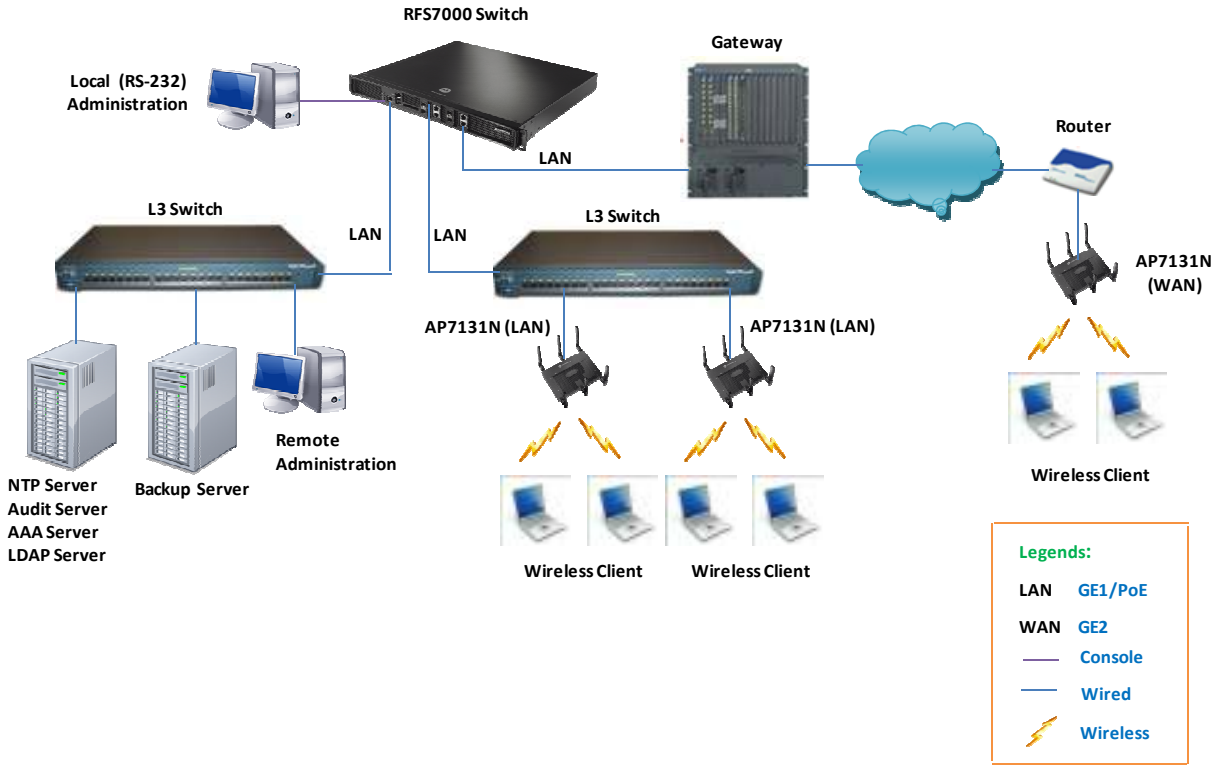


Figure 1 - Typical TOE deployment diagram

1.4.1.1 Target of Evaluation Physical Boundaries

The TOE consists of two types of appliances, a single RFS7000 switch and one or more AP-7131N Wireless Access Point(s) connected via LAN; both include a set of general-purpose and network processors that execute the internal TOE software, as well as volatile and non-volatile storage components.

The physical boundary of the RFS7000 portion of the TOE is composed of a metal and hard plastic case with tamper-evident seals. The device includes four (4) Gigabit Ethernet ports, which provide network connectivity, and one (1) 100Mbit Ethernet port (unused). An RS-232 Serial Port is used for local administration. One CompactFlash card slot, two USB ports, and the 100Mbit Ethernet port are not used and are covered by a tamper evident label at the factory.

The physical boundary of the AP-7131N portion of the TOE is described in [15].

1.4.1.2 TOE Guidance Documentation

The TOE guidance documentation delivered is listed in Section 9, “References,” within Table 25 - TOE Guidance Documentation.

1.4.2 Target of Evaluation Logical Boundaries

The logical boundaries of the TOE include those security functions implemented exclusively by the TOE. These security functions were summarized in Section 1.3.3 above and further described in the following subsections. A more detailed description of the implementation of these security functions is provided in Section 7, "TOE Summary Specification."

1.4.2.1 Audit services

The TOE has the ability to selectively generate audit records from potentially security relevant events and transmit these records to the audit server in the environment. The TOE is dependent on the audit server for the storage, the tools to review audit logs, the protection of audit logs from overflow, and the restriction of access to audit logs. The network connection between the TOE and the external audit server is secured using IPSec security protocol. Audit information generated by the TOE includes date and time of the event, user who caused the event to be generated (if known), and other event specific data.

1.4.2.2 Cryptographic services

The TOE provides cryptographic mechanisms to protect TSF code and data, including mechanisms to encrypt, decrypt, hash, digitally sign data, and perform cryptographic key agreement. The evaluated configuration uses NIST CAVP compliant cryptographic algorithms.

1.4.2.3 User data protection

The TOE protects user data, i.e., only that data exchanged with wireless client devices, using the IEEE 801.11i wireless security protocol, mediates the flow of information passing to and from the LAN port, and ensures that resources used to pass network packets through the TOE do not contain any residual information.

1.4.2.3.1 Firewall

The TOE implements a firewall that filters traffic addressed to the TOE as well as traffic passing through the TOE; e.g., all packets flowing to/from the LAN ports on the RFS7000. An administrative user can develop a set of policies that are composed of rules that dictate requirements to be satisfied to pass network packets. For each rule, if the requirement is met, it is considered to have passed otherwise it is failed. The combination of the rules allows for a branching of processing based on passes and failures. At the conclusion of the evaluation of all rules that make up a policy, the policy is considered to have passed if there was a branch through the processing of the policy that passed. If, and only if, the policy passes, the packet is allowed to pass through the TOE.

The rules can be based on the packet protocol validity, and/or specific elements in the packet contents such as presumed address, user identity, presumed address of source subject, presumed address of destination subject, transport layer protocol, and the TOE interface on which traffic arrives and departs.

1.4.2.4 Identification and Authentication

The TOE keeps a local database of administrator usernames and passwords and utilizes password-based authentication to authenticate administrators connecting remotely using SSH protocol, or locally using a serial console connection. The TOE also provides a capability to authenticate administrator against an external RADIUS authentication server. When a pre-defined number of unsuccessful authentication attempts for a remote administrator has been reached, the administrator user is disabled until re-enabled using a local console connection.

The TOE can authenticate wireless users utilizing the RFS7000 internal RADIUS server, or an external RADIUS authentication server; both implement EAP-TLS, EAP-TTLS and EAP-PEAP authentication protocols. The trusted channel between the TOE and the external authentication server is protected using IPSec/IKE security protocol with pre-shared keys. EAP-TLS uses a client certificate for user authentication; the username is embedded in the certificate. EAP-TTLS and EAP-PEAP use a password for user authentication.

No services are provided by the TOE until the user is successfully identified and authenticated.

1.4.2.5 Security Management

The management of the security relevant parameters of the TOE is performed by the authorized administrator; the TOE provides the following management interfaces:

- Command Line Interface (CLI) via
  - Local RS-232 console connection (RJ-45 connector),
  - Remote SSH interface via the LAN ports
- Remote HTTPS JAVA based Web UI via the LAN ports, and
- Remote SNMP interface via the LAN ports

AP-7131N Adaptive Mode:
In the evaluated configuration, the TOE supports an "Adaptive" mode in which the AP-7131N is adopted by a RFS7000 switch, where the switch provides configuration data, thus providing an additional management interface. When operating in adaptive mode, all other AP-7131N management interfaces are unchanged.

1.4.2.6 TOE Access

There are two sets of advisory/warning messages displayed before establishing a user session; both are displayed before the login/password prompt. The first message displayed before the login prompt is: "This Device is running in Common Criteria Mode," and cannot be changed by the administrator.

The second message displayed before the login prompt can be changed by the administrator and can have a length between 10 and 1024 characters.

The TOE terminates administrative sessions after an administrator configurable time interval of inactivity is reached for SSH, Local CLI, and Web UI sessions.

1.4.2.7 Trusted Path / Channels

The TOE provides trusted paths for authentication functions, communications to remote audit server, NTP functions, and the import/export of configuration files for management.

1.4.2.8 Intrusion Detection

1.4.2.8.1 Rogue Access Point Detection

The TOE provides rogue AP detection, i.e., any unauthorized active AP operating within the radio coverage of an authorized AP. When a rogue-AP is detected, the administrative user is notified with a SNMP trap and a syslog message.

1.4.2.9 Protection of the TSF

The TOE identification and authentication security functions allow only authenticated administrative users direct access to the TOE; wireless users can only authenticate to the TOE and then pass traffic though the TOE, i.e., wireless users are not allowed to execute instructions on the TOE.

Authenticated administrative users are allowed to login via the CLI and Web UI to access all management functions; additionally, authenticated SNMP administrators are allowed access to limited administrative functions. These management interfaces do not allow administrative users access to the underlying operating system and there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

All remote interfaces to the TOE are protected by secure channels; however, the TOE and its underlying hardware and firmware are required to be physically protected from unauthorized access.

The TOE has the capability to obtain reliable time from a remote Network Time Protocol (NTP) Server to provide reliable time stamps for audit services. Additionally, the system administrator can manually set

the time (maintained locally in the hardware Real Time Clock (RTC)) on the TOE using the Web UI or CLI management interfaces.

The TOE provides the capability to run a set of self-tests on power-on, on demand, and periodically to verify the correct operation of the TOE's underlying hardware, TOE software and cryptographic modules. Additional cryptographic tests are performed during normal operation. The security of network data is maintained by zeroizing the memory location corresponding to a network packet, after the packet has been processed by the TOE.

The combination of physical protection by the environment, restriction of direct access to the TOE to authenticated administrative users, having no general-purpose computing resources on the TOE, and securing all remote interfaces with secure communications channels, provide sufficient protections such that the TSF cannot be bypassed, corrupted, or otherwise compromised.

1.5 Roles, User Data, and TSF Data

The TOE supports the following roles:

1. Crypto-officer
    a. Cryptographic functions and network management
2. Monitor
    a. Read-only access
3. System Administrator
    a. General system configuration administrative access
4. Web Administrator
    a. Web authorization for hotspot user access
5. Superuser
    a. Administrative root access
6. SNMP administrator
    a. Remote administrative access
7. Wireless user
    a. Wireless users can pass data through the TOE but do not have direct access

User data is any data that passes through the TOE; it does not affect the operation of the TSF.

TSF data includes the following:

- System configuration information
- Security attributes belonging to the administrator
    - authentication credentials (password)
- User identification credentials (username, password)
- Cryptographic Certificates and keys
- Audit data

1.6 Notation, formatting, and conventions

The notation, formatting, and conventions used in this security target are defined below; these styles and clarifying information conventions were developed to aid the reader.

Where necessary, the ST author has added application notes to provide the reader with additional details to aid understanding; they are italicized and usually appear following the element needing clarification. Those notes specific to the TOE are marked "TOE Application Note;" those taken from the WLAN AS Protection Profile are marked "Application Note."

The notation conventions that refer to iterations, assignments, selections, and refinements made in this security target are in reference to SARs and SFRs taken directly from CC Part 2 and Part 3.

The CC permits four component operations: assignment, iteration, refinement, and selection to be performed on requirement components. These operations are defined in Common Criteria, Part 1; paragraph 6.4.1.3.2, “Permitted operations on components” as:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

Iterations made by the ST author are indicated by a number in parenthesis following the requirement number, e.g., FIA_UAU.1.1 (1); the iterated requirement titles are similarly indicated, e.g., FIA_UAU.1 (1).

Assignments made by the ST author are identified with ***bold italics;*** selections are identified with **bold text.**

Refinements made by the ST author are identified with "**Refinement:**" right after the short name; the refined text indicated by underlined text; any refinement that performs a deletion in text is noted in the endnotes sections indicated.

2 Conformance Claims

2.1 Common Criteria Conformance Claims

This Security Target is conformant to the Common Criteria Version 3.1r3, CC Part 2 extended [8], and CC Part 3 [9].

2.2 Conformance to Security Packages

This Security Target does not claim conformance to any security function requirements package, neither as package-conformant or package-augmented.

This Security Target is Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2.

3 Security Problem Definition

3.1 Threats

The following subsections define the security threats for the TOE, characterized by a threat agent, an asset, and an adverse action of that threat agent on that asset.

3.1.1 Threats countered by the TOE and TOE IT Environment

Table 1 - Threats countered by the TOE and TOE IT Environment		
#	Threat	Description
1	T.ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
2	T.ACCIDENTAL_CRYPTO_COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
3	T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
4	T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
5	T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
6	T.POOR_TEST	The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
7	T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
8	T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
9	T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.
10	T.UNAUTHORIZED_ ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
11	T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.
12	T.UNAUTH_AP	An attacker may place an unauthorized AP in the radio coverage area of a 802.11 wireless network allowing the attacker to remotely access or attack the network, or configure the unauthorized AP to appear like an authorized unit, giving the attacker access to the Wireless Client's data.

3.2 Organizational Security Policies

3.2.1 Organizational Security Policies for the TOE

Table 2 - Organizational Security Policies for the TOE and TOE IT Environment		
#	OSP	Description
1	P.ACCESS_BANNER	The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other

Table 2 - Organizational Security Policies for the TOE and TOE IT Environment		
#	OSP	Description
		appropriate information to which users consent by accessing the system.
2	P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
3	P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
4	P.CRYPTOGRAPHY_VALIDATED	Only NIST CAVP validated cryptographic algorithms are acceptable for key generation and key agreement, and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
5	P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
6	P.NO_AD_HOC_NETWORKS	In accordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.

3.3 Assumptions on the TOE Operational Environment

This section describes the assumptions that are made on the operational environment in which the TOE is intended to be used in order to be able to provide security functionality. It includes information about the physical, personnel, and connectivity aspects of the environment. The operational environment must be managed in accordance with the provided guidance documentation. The following subsections define specific conditions that are assumed to exist in an environment where the TOE is deployed.

3.3.1 Assumptions on Physical Aspects of the Operational Environment:

The TOE is intended for application in areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

Table 3 - Assumptions on Physical Aspects of the Operational Environment	
Assumption	Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment

3.3.2 Assumptions on Personnel Aspects of the Operational Environment

Table 4 - Assumptions on Personnel Aspects of the Operational Environment	
Assumption	Description
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.

3.3.3 Assumptions on Connectivity aspects of the Operational Environment:

Table 5 - Assumptions on Connectivity Aspects of the Operational Environment	
Assumption	Description
A.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 6 - Security Objectives for the TOE		
#	TOE Objective	Description
1	O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
2	O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
3	O.CONFIGURATION_ IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.
4	O.CORRECT_TSF_OPERATION	The TOE will provide the capability to verify the correct operation of the TSF.
5	O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE.
6	O.CRYPTOGRAPHY_VALIDATED	The TOE will use NIST CAVP validated crypto algorithms for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.
7	O.DISPLAY_BANNER	The TOE will display an advisory warning prior to establishing an administrator session regarding use of the TOE prior to permitting the use of any TOE services that requires authentication.
8	O.DOCUMENTED_ DESIGN	The design of the TOE is adequately and accurately documented.
9	O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
10	O.MEDIATE	The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.
11	O.PARTIAL_FUNCTIONAL_TESTING	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
12	O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
13	O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
14	O.TIME_STAMPS	The TOE shall obtain reliable time stamps.
15	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
16	O.VULNERABILITY_ ANALYSIS	The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.
17	O.ROGUE_AP_DETECTION	The TOE shall provide security functions to detect an unauthorized AP operating in the radio coverage area of the 802.11 wireless network as well as generate notifications to the administrator when detected.

4.1.1 Rationale for the Security Objectives for the TOE

4.1.1.1 Mappings of TOE Security Objectives to Threats and OSP

The following table shows the mapping of security objectives for the TOE to threats countered by that objective and/or the OSP enforced by that objective.

Table 7 - Mapping of TOE Security Objectives to Threats and OSP

		Threats												OSP					
#	TOE Objective	T.ACCIDENTAL_ADMIN_ ERROR	T.ACCIDENTAL_ CRYPTO_ COMPROMISE	T.MASQUERADE	T.POOR_DESIGN	T.POOR_IMPLEMENTATION	T.POOR_TEST	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_ SESSION	T.UNAUTHORIZED_ ACCESS	T.UNAUTH_ADMIN_ACCESS	T.UNAUTH_AP	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.CRYPTOGRAPHIC	P.CRYPTOGRAPHY_VALIDATED	P.ENCRYPTED_CHANNEL	P.NO_AD_HOC_NETWORKS
1	O.ADMIN_GUIDANCE	X										X							
2	O.AUDIT_GENERATION														X				
3	O.CONFIGURATION_IDENTIFICATION				X	X													
4	O.CORRECT_TSF_OPERATION						X												
5	O.CRYPTOGRAPHY															X	X	X	
6	O.CRYPTOGRAPHY_VALIDATED																X	X	
7	O.DISPLAY_BANNER													X					
8	O.DOCUMENTED_ DESIGN				X		X												
9	O.MANAGE	X							X		X	X			X				
10	O.MEDIATE										X							X	X
11	O.PARTIAL_FUNCTIONAL_TESTING					X	X												
12	O.RESIDUAL_INFORMATION		X					X	X							X			
13	O.SELF_PROTECTION		X						X		X								
14	O.TIME_STAMPS														X				
15	O.TOE_ACCESS			X						X	X	X			X				
16	O.VULNERABILITY_ ANALYSIS				X	X	X												
17	O.ROGUE_AP_DETECTION												X						

4.1.1.2 Security Objectives Rationale for Threats and OSP

This section presents the rationale that justifies the security objectives for the TOE is suitable to counter those threats to be countered by the TOE and justifies the security objectives are suitable to enforce the OSP.

O.ADMIN_GUIDANCE

O.ADMIN_GUIDANCE helps to mitigate the threats, T.ACCIDENTAL_ADMIN_ ERROR and T.UNAUTH_ADMIN_ACCESS, by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure.

O.AUDIT_GENERATION

O.AUDIT_GENERATION addresses the policy, P.ACCOUNTABILITY, by providing the Administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.).

O.CONFIGURATION_ IDENTIFICATION

O.CONFIGURATION_IDENTIFICATION plays a role in countering the threat, T.POOR_DESIGN, by requiring the developer to provide control of the changes made to the TOE's design documentation and the ability to report and resolve security flaws. It plays a role in countering the threat, T.POOR_IMPLEMENTATION, by requiring the developer to provide control of the changes made to the TOE's design. This ensures that changes to the TOE are performed in structure manner and tracked.

O.CORRECT_TSF_OPERATION

O.CORRECT_ TSF_OPERATION plays a role in countering the threat, T.POOR_TEST, by providing assurance that the TSF continues to operate as expected in the field.

O.CRYPTOGRAPHY

O.CRYPTOGRAPHY satisfies the policies, P. CRYPTOGRAPHY and P.CRYPTOGRAPHY_VALIDATED, by requiring the TOE to implement NIST CAVP validated cryptographic algorithms. These algorithms will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. It satisfy the policy, P.ENCRYPTED_CHANNEL, by requiring the TOE to implement NIST CAVP validated cryptographic algorithms. These algorithms will provide confidentiality and integrity protection of TSF data while in transit to wireless clients that are authorized to join the network.

O.CRYPTOGRAPHY_VALIDATED

O.CRYPTOGRAPHY_VALIDATED satisfies the policy, P.CRYPTOGRAPHY_VALIDATED, by requiring that all cryptographic algorithms for cryptographic services be NIST CAVP validated. This will provide assurance that the NIST-approved security functions and random number generation will be in accordance with NIST and validated according the CAVP. It satisfy the policy, P.ENCRYPTED_CHANNEL, by requiring the TOE to implement NIST CAVP validated cryptographic algorithms. These algorithms will provide confidentiality and integrity protection of TSF data while in transit to wireless clients that are authorized to join the network.

O.DISPLAY_BANNER

O.DISPLAY_BANNER satisfies the policy, P.ACCESS_BANNER, by ensuring that the TOE displays an administrator configurable banner that provides all users with a warning about unauthorized use of the TOE. A banner will be presented for all TOE services that allow direct access to the TOE. In other words, it will be required for all administrative actions.

O.DOCUMENTED_ DESIGN

O.DOCUMENTED_DESIGN counters the threat, T_POOR_DESIGN, to a degree by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered.

O.DOCUMENTED_DESIGN helps to counters the threat, T_POOR_TEST, by ensuring that the TOE's documented design satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE.

O.MANAGE

O.MANAGE contributes to mitigating the threat, T.ACCIDENTAL_ADMIN_ ERROR, by providing administrators the capability to view and manage configuration settings. For example, if the administrator made a mistake when configuring the set of permitted users' authentication credentials, providing the capability to view the lists of authentication credentials affords them the ability to review the list and discover any mistakes that might have been made.

O.MANAGE mitigates the threat, T.TSF_COMPROMISE, by restricting access to administrative functions and management of TSF data to the administrator.

O.MANAGE mitigates the threat, T_UNAUTHORIZED_ACCESS, by restricting the ability to modify the security attributes associated with the TOE to the administrator. This objective ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

O.MANAGE mitigates the threat, T_UNAUTH_ADMIN_ACCESS, by restricting access to administrative functions and management of TSF data to the administrator

O.MEDIATE

O.MEDIATE mitigates the threat, T_UNAUTHORIZED_ACCESS, by ensuring that all network packets that flow through the TOE are subject to the information flow policies.

O.MEDIATE satisfies the policy, P. ENCRYPTED_CHANNEL, by allowing the TOE administrator to set a policy to encrypt all wireless traffic.

O.MEDIATE works to support the policy, P.NO_AD_HOC_NETWORKS, by ensuring that all network packets that flow through the TOE are subject to the information flow policies.

O.PARTIAL_FUNCTIONAL_TESTING

O.PARTIAL_FUNCTIONAL_TESTING helps mitigate the threat, T_POOR_DESIGN, by increasing the likelihood that any errors that do exist in the implementation will be discovered through testing.

O.PARTIAL_FUNCTIONAL_TESTING helps mitigate the threat, T_POOR_IMPLEMENTATION, by ensuring that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing.

O.RESIDUAL_INFORMATION

O.RESIDUAL_INFORMATION contribute to the mitigation of the threats, T.RESIDUAL_DATA, T.ACCIDENTAL_CRYPTO_COMPROMISE, and T.TSF_COMPROMISE, by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.

O.RESIDUAL_INFORMATION satisfies the policy, P. CRYPTOGRAPHY, by ensuring that cryptographic data are securely cleared.

O.SELF_PROTECTION

O.SELF_PROTECTION contributes to the mitigation of the threat, T.ACCIDENTAL_CRYPTO_COMPROMISE by ensuring the TOE will have adequate protection from external sources and that all TSP functions are invoked.

O.SELF_PROTECTION contributes to the mitigation of the threat, T.TSF_COMPROMISE, by requiring the TOE be able to protect itself from tampering and that the security mechanisms in the TOE cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF data or TSF executables.

O.SELF_PROTECTION contributes to the mitigation of the threat, T.UNAUTHORIZED_ACCESS, by requiring the TOE require all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services.

O.TIME_STAMPS

O.TIME_STAMPS plays a role in supporting the policy, P.ACCOUNTABILITY, by requiring the TOE to provide a reliable time stamp (via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred.

O.TOE_ACCESS

O.TOE_ACCESS supports the policy P.ACCOUNTABILITY and helps mitigate the threats T.MASQUERADE, T.UNATTENDED_ SESSION, T_UNAUTHORIZED_ACCESS, and T.UNAUTH_ADMIN_ACCESS by controlling logical access to the TOE and its resources. This objective ensures that users are identified and authenticated so that their actions may be tracked by the administrator.

O.VULNERABILITY_ANALYSIS

O.VULNERABILITY_ANALYSIS contributes to the mitigation of the threat, T.POOR_DESIGN, by ensuring that the TOE has been analyzed for obvious vulnerabilities and that any vulnerability found have been removed or otherwise mitigated, this includes analysis of any probabilistic or permutational mechanisms incorporated into a TOE claiming conformance to this ST.

O.ROGUE_AP_DETECTION

O.ROGUE_AP_DETECTION mitigates the threat, T.UNAUTH_AP, by ensuring the TOE provide security functions to detect unauthorized APs operating in the radio coverage area of the 802.11 wireless network as well as generate notifications to the administrator when detected.

4.2 Security Objectives for the TOE Operational Environmental

Table 8 - Security Objectives for the TOE Operational Environmental		
#	Objective	Description
1	OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information and the authentication credentials.
2	OE.AUDIT_REVIEW	The IT Environment will provide the capability to selectively view audit information.
3	OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
4	OE.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
5	OE.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
6	OE.PHYSICAL	The environment provides physical security commensurate with the value of the TOE and the data it contains.
7	OE.PROTECT_MGMT_COMMS	The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE and time service in a manner that is commensurate with the risks posed to the network.
8	OE.RESIDUAL_INFORMATION	The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
9	OE.SELF_PROTECTION	The environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
10	OE.TIME_STAMPS	The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
11	OE.TOE_ACCESS	The environment will provide mechanisms that support the TOE in providing a user's logical access to the TOE.
12	OE.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

4.2.1 Rationale for the Security Objectives for the TOE Operational Environment

4.2.1.1 Mappings of Security Objectives to Threats, OSP, and Assumptions

Table 9 - Mapping of TOE Security Objectives to Threats, OSP, and Assumptions, shows the mapping of security objectives for the TOE operational environment to threats countered by that objective, the OSP enforced by that objective, and/or the assumption upheld by that objective.

Table 9 - Mapping of TOE Security Objectives to Threats, OSP, and Assumptions															
		Threats							OSP			Assumptions			
#	TOE Objective	T.ACCIDENTAL_ADMIN_ERROR	T.ACCIDENTAL_CRYPTO_COMPROMISE	T.MASQUERADE	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNAUTHORIZED_ACCESS	T.UNAUTH_ADMIN_ACCESS	P.ACCOUNTABILITY	P.ENCRYPTED_CHANNEL	P.NO_AD_HOC_NETWORKS	A.NO_EVIL	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TOE_NO_BYPASS
1	OE.AUDIT_PROTECTION								X						
2	OE.AUDIT_REVIEW								X						
3	OE.MANAGE					X	X	X							
4	OE.NO_EVIL	X						X				X			
5	OE.NO_GENERAL_PURPOSE	X											X		
6	OE.PHYSICAL													X	
7	OE.PROTECT_MGMT_COMMS									X					
8	OE.RESIDUAL_INFORMATION		X		X										
9	OE.SELF_PROTECTION		X			X	X								
10	OE.TIME_STAMPS								X						
11	OE.TOE_ACCESS			X			X		X						
12	OE.TOE_NO_BYPASS			X							X				X

4.2.1.2 IT Security Objectives Rationale for Threats and OSP, and Assumptions

This section presents the rationale that justifies the security objectives for the TOE operational environment is suitable to counter those threats to be countered by the TOE operational environment, justifies the security objectives are suitable to enforce the OSP and the assumptions are upheld by that objective.

OE.AUDIT_PROTECTION

OE.AUDIT_PROTECTION satisfies the policy, P.ACCOUNTABILITY, by providing protected storage of TOE and IT environment audit data in the environment.

OE.AUDIT_REVIEW

OE.AUDIT_REVIEW helps satisfy the policy, P.ACCOUNTABILITY, by supporting accountability mechanisms for viewing and sorting the audit logs

OE.MANAGE

OE.MANAGE helps mitigate the threat, T.TSF_COMPROMISE, by ensuring that the administrator can view security relevant audit events.

OE.MANAGE. helps mitigate the threat, T.UNAUTHORIZED_ACCESS, by restricting the ability to modify the security attributes associated with the TOE to the administrator. These objectives ensure that no other user can modify the information flow policy to bypass the intended TOE security policy.

OE.MANAGE helps mitigate the threat, T.UNAUTH_ADMIN_ACCESS, by restricting access to administrative functions and management of TSF data to the administrator.

OE.NO_EVIL

OE.NO_EVIL contributes to mitigating the threat, T.ACCIDENTAL_ADMIN_ ERROR, by ensuring that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.

OE.NO_EVIL helps mitigate the threat, T.UNAUTH_ADMIN_ACCESS, by ensuring that the TOE administrators have guidance that instructs them in how to administer the TOE in a secure manner.

By ensuring sites using the TOE administrators are non-hostile, appropriately trained and follow all administrator guidance, the assumption A.NO_EVIL is addressed.

OE.NO_GENERAL_PURPOSE

OE.NO_GENERAL_PURPOSE mitigate the threat, T.ACCIDENTAL_ADMIN_ ERROR, by ensuring that there can be no accidental errors due to the introduction of unauthorized software or data, by ensuring that there are no general-purpose or storage repository applications available on the TOE.

By ensuring the operational environment require there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE, the assumption A. NO_GENERAL_PURPOSE is addressed.

OE.PHYSICAL

By ensuring the operational environment provides physical security commensurate with the value of the TOE and the data it contains, the assumption A. PHYSICAL is addressed.

OE.PROTECT_MGMT_COMMS

OE.PROTECT_MGMT_COMMS helps to satisfy the policy, P.ENCRYPTED_CHANNEL, by providing that the audit records, remote network management information and authentication data will be protected by means of a protected channel in the environment.

OE.RESIDUAL_INFORMATION

OE.RESIDUAL_INFORMATION contributes to the mitigation of the threats, T.RESIDUAL_DATA and T.ACCIDENTAL_CRYPTO_COMPROMISE, by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.

OE.SELF_PROTECTION

OE.SELF_PROTECTION help mitigate the threats, T.ACCIDENTAL_CRYPTO_COMPROMISE and T.TSF_COMPROMISE by ensuring that the TOE IT environment will have protection similar to that of the TOE.

.

OE.SELF_PROTECTION contributes to the mitigation of the threat, T.UNAUTHORIZED_ACCESS, by requiring the TOE IT environment require all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services.

OE.TIME_STAMPS

OE.TIME_STAMPS supports the policy, P.ACCOUNTABILITY, by ensuring that the TOE IT environment provides time services.

OE.TOE_ACCESS

OE.TOE_ACCESS help mitigate the threats, T.MASQUERADE and T.UNAUTHORIZED_ACCESS by controlling logical access to the TOE and its resources.

OE.TOE_ACCESS supports the policy, P.ACCOUNTABILITY, by controlling logical access to the TOE and its resources. This objective ensures that users are identified and authenticated so that their actions may be tracked by the administrator.

OE.TOE_NO_BYPASS

OE.TOE_NO_BYPASS helps mitigate the threat T.MASQUERADE, and supports the policy, P.NO_AD_HOC_NETWORKS, by ensuring that wireless clients must be configured to use the wireless access system for all information flowing between a wireless client and any other host on the network. If the clients are properly configured, any information passing through the TOE will be inspected to ensure it is authorized by TOE polices.

By ensuring the operational environment require wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE, the assumption A. TOE_NO_BYPASS is addressed.

5 Extended Components Definition

This section defines the extended security functional requirements for the TOE. The security functional requirement components defined in this security target are CC Part 2 extended.

Table 10 - TOE Security Functional Requirements CC Part 2 Extended				
#	SFR	Description	Dependencies	Hierarchical to
1	FCS_BCM_(EXT).1	Baseline Cryptographic Module	None	None
2	FCS_CKM_(EXT).2	Cryptographic Key Handling and Storage	None	None
3	FCS_COMM_PROT_EXT.1	Communications Protection	None	None
4	FCS_COP_(EXT).1	Extended: Random Number Generation	None	None
5	FCS_HTTPS_EXT.1	HTTPS	None	None
6	FCS_SFTP_EXT.1	SSH File Transfer Protocol	FCS_SSH_EXT.1	None
7	FCS_SSH_EXT.1	SSH Protocol	None	None
8	FCS_TLS_EXT.1	TLS Protocol	None	None
9	FCS_IPSEC_EXT.1	Internet Protocol Security (IPSec)	None	None
10	FCS_EAP-TLS_EXT.1	EAP-TLS Authentication Protocol	FCS_TLS_EXT.1	None
11	FCS_EAP-TTLS_EXT.1	EAP-TTLS Authentication Protocol	FCS_TLS_EXT.1	None
12	FCS_PEAP_EXT.1	PEAP Authentication Protocol	FCS_TLS_EXT.1	None
13	FCS_RAD_EXT.1	RADIUS Authentication Protocol	FCS_IPSEC_EXT.1	None
14	FCS_SNMPv3_EXT.1	SNMPv3	None	None
15	FIA_UAU_(EXT).1	Multiple authentication methods	None	None
16	FID_APD_EXT.1	Rogue Access Point Detection	None	None
17	FPT_STM_(EXT).1	Reliable Time Stamps	None	None
18	FPT_TST_EXT.1	TSF Testing	None	None
19	FPT_ITC_EXT.1	Inter-TSF Trusted Channel	None	None

5.1.1 Class FCS:

This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software. The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include, but are not limited to, identification and authentication, non-repudiation, trusted path, trusted channel and data separation.

5.1.1.1 FCS_BCM_(EXT) Baseline Cryptographic Module

Family Behavior

This family addresses requirements to use only certified cryptography to protect communications between the TSF, to separate parts of the TSF, and/or external IT entities.

Component leveling

FCS_BCM_(EXT): Baseline Cryptographic Module	1

FCS_BCM_(EXT).1 Baseline Cryptographic Module requires the TSF to use only cryptographic algorithms that have been validated by the NIST Cryptographic Algorithm Validation Program.

Management: FCS FCS_BCM_(EXT).1

There are no management activities foreseen.

Audit: FCS_BCM_(EXT).1

There are no auditable events foreseen.

5.1.1.1.1 FCS_BCM_(EXT).1 Baseline Cryptographic Module

Hierarchical to: None

Dependencies: None

FCS_BCM_(EXT).1.1 All cryptographic functions implemented by the TOE shall be validated by NIST CAVP and include an algorithm validation certificate.

5.1.1.2 FCS_CKM_(EXT).2 Extended: Cryptographic Key Handling and Storage

Family Behavior

This family addresses requirements to use securely store and handle cryptographic keys.

Component leveling

FCS_CKM_(EXT).2: Extended: Cryptographic Key Handling and Storage	1

FCS_CKM_(EXT).2: Extended: Cryptographic Key Handling and Storage requires the TSF to ensure keys are transferred properly, that they are stored securely, destroyed when no longer needed, and not archived when expired.

Management: FCS_CKM_(EXT).2

The following actions could be considered for the management functions in FMT:

Configuration of the inactivity timer.

Audit: FCS_CKM_(EXT).2

Basic: Error(s) detected during cryptographic key transfer.

5.1.1.2.1 FCS_CKM_(EXT).2 Extended: Cryptographic Key Handling and Storage

Hierarchical to: None

Dependencies: None

FCS_CKM_(EXT).2.1	The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).
Application Note:	*A parity check is an example of a key error detection check.*
FCS_CKM_(EXT).2.2	The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.
Application Note:	*A persistent key, such as a file encryption key, is one that must be available in the system over long periods of time. A non-persistent key, such as a key used to encrypt or decrypt a single message or a session, is one that is ephemeral in the system.*
Application Note:	*"When not in use" is interpreted in the strictest sense so that persistent keys only exist in plaintext form during intervals of operational necessity. For example, a file encryption key exists in plaintext form only during actual encryption and/or decryption processing of a file. Once the file is decrypted or encrypted, the file encryption key should immediately be covered for protection.*
Application Note:	*A "split knowledge procedure" is a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.*
FCS_CKM_(EXT).2.3	The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.
Application Note:	*The cryptographic administrator must have the ability to set a threshold of inactivity after which non-persistent keys must be destroyed in accordance with FCS_CKM.4.*
FCS_CKM_(EXT).2.4	The TSF shall prevent archiving of expired (private) signature keys.
Application Note:	*This requirement is orthogonal to typical system back-up procedures. Therefore, it does not address the problem of archiving an active (private) signature key during a system back-up and saving the key beyond its intended life span.*

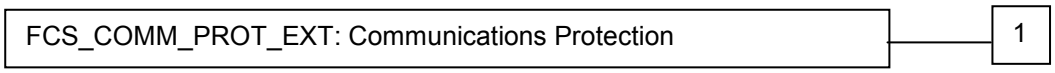
5.1.1.3 FCS_COMM_PROT_EXT Communications Protection

FCS_COMM_PROT_EXT Communications Protection addresses requirements to use a cryptographic protocol to protect communications between the TSF and external IT entities.

Family Behavior

This family provides requirements that address communications security on a network.

Component leveling



FCS_COMM_PROT_EXT.1 Communications Protection requires the TSF provide either IPsec or SSH to provide communications security to separate parts of the TSF, and/or external IT entities; optionally, TLS/HTTPS may also be selected if implemented in the TSF.

Management: FCS_COMM_PROT_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FCS_COMM_PROT_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.3.1 FCS_COMM_PROT_EXT.1 Communications Protection

Hierarchical to: None

Dependencies: None

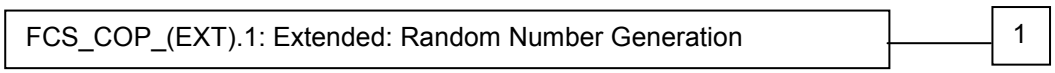
FCS_COMM_PROT_EXT.1.1 The TSF shall protect communications using [selection: *IPsec, SSH*] and [selection: *TLS/HTTPS, no other protocol*].

5.1.1.4 FCS_COP_(EXT).1 Extended: Random Number Generation

Family Behavior

This family addresses requirements for suitable random number generators for the TOE.

Component leveling



FCS_COP_(EXT).1: Extended: Random Number Generation requires the TSF to use a NIST approved random number generator, and to ensure the RNG/PRNG sources are not tampered with.

Management: FCS_COP_(EXT).1

There are no management activities foreseen.

Audit: FCS_COP_(EXT).1

There are no auditable events foreseen.

5.1.1.4.1 FCS_COP_(EXT).1 Extended: Random Number Generation

Hierarchical to: None

Dependencies: None

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG [*assignment: one of the RNGs specified in FIPS 140-2 Annex C*] seeded by [*selection:*

(1) one or more independent hardware-based entropy sources, and/or
(2) one or more independent software-based entropy sources, and/or
(3) a combination of hardware-based and software-based entropy sources.]

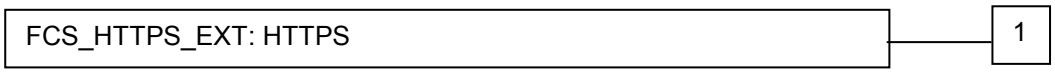
FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/pseudorandom number generation (PRNG) sources.

5.1.1.5 FCS_HTTPS_EXT HTTPS

Family Behavior

This family addresses the requirements for the use of HTTPS as a secure communications protocol.

Component leveling



FCS_HTTPS_EXT.1 HTTPS specifies conformance to the appropriate RFC and to the underlying transport protocol.

Management: FCS_HTTPS_EXT.1

There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

Basic: Failure to establish a HTTPS Session
Establishment and/or termination of a HTTPS session

5.1.1.5.1 FCS_HTTPS_EXT.1 HTTPS

Hierarchical to: None

Dependencies: None

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

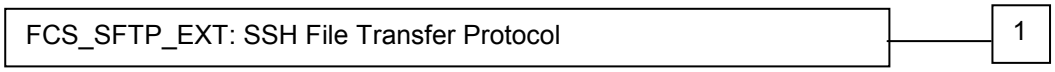
FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.1.1.6 FCS_SFTP_EXT SSH File Transfer Protocol

Family Behavior

This family addresses the requirements for the use of SFTP as a secure communications protocol.

Component leveling



FCS_SFTP_EXT.1 SSH File Transfer Protocol specifies conformance to the appropriate RFC and to the underlying transport protocol.

Management: FCS_SFTP_EXT.1

There are no management activities foreseen.

Audit: FCS_SFTP_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

Basic: Failure of the file transfer

5.1.1.6.1 FCS_SFTP_EXT.1 SSH File Transfer Protocol

Hierarchical to: None

Dependencies: FCS_SSH_EXT.1

FCS_SFTP_EXT.1.1	The TSF shall implement the SSH File Transfer Protocol as specified in draft-ietf-secsh-filexfer-13.txt, July 10, 2006.
FCS_SFTP_EXT.1.2	The TSF shall ensure the SFTP connection has privacy and integrity features provided by the underlying SSH transport protocol as specified in FCS_SSH_EXT.1.

5.1.1.7 FCS_SNMPV3_EXT.1 SNMP V3

SNMP v3, Simple Network Management Protocol version 3, is a networking protocol that provides the ability to monitor and configure network devices.

Family Behavior

This family provides requirements that address use of the SNMPv3 protocol.

Component leveling

FCS_SNMPV3_EXT: SNMPV3	1

FCS_SNMPV3_EXT SNMPV3 requires conformance to the appropriate RFCs and critical security parameters.

Management: FCS_SNMPV3_EXT.1
The following actions could be considered for the management functions in FMT:

- The modification of SNMP configuration parameters

Audit: FCS_SNMPV3_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication failures

5.1.1.7.1 FCS_SNMPV3_EXT.1 SNMPV3

Hierarchical to: None

Dependencies: None

FCS_SNMPV3_EXT.1.1 The TSF shall implement the SNMPV3 protocol that complies with RFCs:

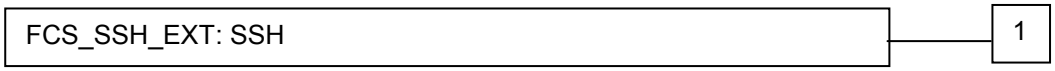
- 3411 (Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks),
- 3414 (User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)),
- 3415 (View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- 3417 (Transport Mappings for the Simple Network Management Protocol (SNMP)), and
- [**selection:**
  - **3826 (The Advanced Encryption Standard (AES_ Cipher Algorithm in the SNMP User-based Security Model),**
  - **5608 (Remote Authentication Dial-In User Service (RADIUS) Usage for Simple Network Management Protocol (SNMP) Transport Models),**
  - **6353 (Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)),**
  - **no other RFC].**

5.1.1.8 FCS_SSH_EXT SSH

Family Behavior

This family addresses the requirements for the use of SSH as a secure communications protocol.

Component leveling



FCS_SSH_EXT.1 SSH requires conformance to the appropriate RFCs and critical security parameters.

Management: FCS_SSH_EXT.1

The following actions could be considered for the management functions in FMT:
Setup of configurable security values

Audit: FCS_SSH_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

Basic: Failure to establish an SSH session
Establishment and/or termination of an SSH session

5.1.1.8.1 FCS_SSH_EXT.1 SSH Protocol

Hierarchical to: None

Dependencies: None

FCS_SSH_EXT.1.1	The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.
Application Note:	*The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.*
FCS_SSH_EXT.1.2	The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.
FCS_SSH_EXT.1.3	The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [*assignment: timeout period*], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [*assignment: maximum number of attempts*] attempts.
FCS_SSH_EXT.1.4	The TSF shall ensure that the SSH protocol implementation supports the password-based authentication method as described in RFC 4252.
FCS_SSH_EXT.1.5	The TSF shall ensure that, as described in RFC 4253, packets greater than [*assignment: number of bytes*] bytes in an SSH transport connection are dropped.
Application Note:	*RFC 4253 provides for the acceptance of "large packets" with the caveat that the packets should be of "reasonable length" or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining "reasonable length" for the TOE.*
FCS_SSH_EXT.1.6	The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-192, AES-CBC-256, no other algorithms.

FCS_SSH_EXT.1.7	The TSF shall ensure that the SSH transport implementation uses SSH_RSA and no other public key algorithms, as its public key algorithm(s).
Application Note:	*RFC 4253 specifies required and allowable public key algorithms. This requirement makes SSH-RSA "required" and allows two others to be claimed in the ST. The ST author should make the appropriate selection, selecting "no other public key algorithms" if only SSH_RSA is implemented.*
FCS_SSH_EXT.1.8	The TSF shall ensure that data integrity algorithms used in SSH transport connection is hmac-sha1, and [*selection: hmac-sha1-96*, hmac-md5, hmac-md5-96, no other].

.

FCS_SSH_EXT.1.9	The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.1.1.9 FCS_IPSEC_EXT Internet Protocol Security (IPSec)

Family Behavior

This family addresses the requirements for the use of IPsec as a secure communications protocol.

Component leveling

FCS_IPSEC_EXT: Internet Protocol Security (IPsec)	1

FCS_IPSEC_EXT.1 IPsec requires conformance to the appropriate RFCs and critical security parameters.

Management: FCS_IPSEC_EXT.1

The following actions could be considered for the management functions in FMT:

- Setup of configurable security values

Audit: FCS_IPSEC_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

Basic: Failure to establish an IPsec SA
Establishment and/or termination of an IPsec SA

5.1.1.9.1 FCS_IPSEC_EXT.1 Internet Protocol Security (IPSec)

Hierarchical to: None

Dependencies: None

FCS_IPSEC_EXT.1.1 The TSF shall implement IPsec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-192, AES-CBC-256 (as specified by RFC 3602), [selection: *no other algorithms, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*] and using IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109; [selection: *no other method, IKEv2 as defined in RFCs 4306, 4307*] to establish the security association.

Application Note: *Support for AES-CBC-128 and AES-CBC-256 is required above; if AES-GCM-128 or AES-GCM-256 are supported then the appropriate selection should be made, otherwise select "no other algorithm".*

It is acceptable to refine this requirement for IKEv1 and/or IKEv2 to include RFC 4868 as optional claimed hash algorithms. If this is done, the ST author should adjust the appropriate FCS_COP.1 iteration accordingly.

Support for IKEv1 is required above; if IKEv2 is supported then that selection should be made, otherwise select "no other method."

The ST author must make the appropriate selections and assignments to reflect the IPsec implementation. The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.

HMAC-SHA 1 is required by the RFCs as the hash algorithm used by the IKE implementation for CBC mode. If other hash algorithms are to be claimed, then either the requirement or the TSS section must identify those algorithms and the appropriate selections need to be made in the appropriate FCS_COP.1 iteration.

For IKEv1, the above requirement is to be interpreted as requiring the IKE implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109.

Suite B algorithms (RFC 4869) are the preferred algorithms for implementation.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

Application Note: *The above requirement can be accomplished either by providing an authorized administrator-configurable lifetimes (with appropriate FMT requirements and instructions in documents mandated by AGD_OPE, as necessary), or by "hard coding" the limits in the implementation.*

FCS_IPSEC_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to [assignment: *number between 100 - 200*] MB of traffic for Phase 2 SAs.

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP)*, [*assignment: other DH groups that are implemented by the TOE], no other DH groups*].

FCS_IPSEC_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the [*selection: PSK, DSA, rDSA, ECDSA*] algorithm.

Application Note: *The selected algorithm should correspond to an appropriate selection for the appropriate FCS_COP.1 iteration.*

FCS_IPSEC_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) and [selection: username/password, no other method] for use in authenticating its IPsec connections.

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

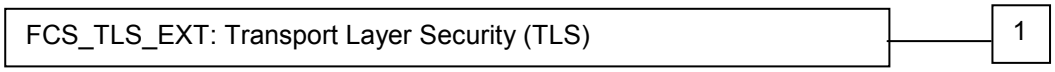
1. Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")");
2. Pre-shared keys [assignment: *supported lengths*].

5.1.1.10 FCS_TLS_EXT Transport Layer Security (TLS)

Family Behavior

This family addresses the requirements for the use of TLS as a secure communications protocol.

Component leveling



FCS_TLS_EXT.1 TLS requires conformance to the appropriate RFCs and critical security parameters.

Management: FCS_TLS_EXT.1

The following actions could be considered for the management functions in FMT:

- Setup of configurable security values

Audit: FCS_TLS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Basic: Failure to establish a TLS session
  Establishment and/or termination of a TLS session

5.1.1.10.1 FCS_TLS_EXT.1 TLS

Hierarchical to: None

Dependencies: None

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2346), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

- Mandatory ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA

- Optional ciphersuites:
  - [selection:
  - *None*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *TLS_RSA_WITH_AES_128_CBC_SHA256*
  - *TLS_RSA_WITH_AES_256_CBC_ SHA256*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256*
  - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
  - *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  -].

5.1.1.11 FCS_EAP-TLS_EXT EAP_TLS Authentication Protocol

EAP-TLS, Extensible Authentication Protocol-Transport Layer Security, uses the TLS protocol authentication hand shaking implementation for 802.1x authentication. TLS provides certificates for client and server authentication, dynamic session key generation, and protection of the authentication session.

Family Behavior

This family provides requirements that address authentication on a 802.1x wireless network.

Component leveling

FCS_EAP-TLS_EXT: EAP-TLS Authentication Protocol	1

FCS_EAP-TLS_EXT.1 EAP-TLS Authentication Protocol requires the TSF provide the facilities to authenticate to the wireless network.

Management: FCS_EAP-TLS_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FCS_EAP-TLS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.11.1 FCS_EAP-TLS_EXT.1 EAP-TLS Authentication Protocol

Hierarchical to: None

Dependencies: FCS_TLS_EXT.1

FCS_EAP-TLS_EXT.1.1 The TSF shall implement the EAP-TLS authentication protocol that complies with RFC 5216.

FCS_EAP-TLS_EXT.1.2 The TSF shall implement TLS 1.0[2], and [selection: *TLS v1.1, TLS v1.2, no other*] protocol as specified in FCS_TLS_EXT.1.

FCS_EAP-TLS_EXT.1.3 The TSF shall ensure that the EAP-TLS authentication protocol support the following ciphersuites[3]:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA per RFC4346
- Optional Ciphersuites:
  - [selection:
  - *None*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *TLS_RSA_WITH_AES_128_CBC_SHA*
  - *TLS_RSA_WITH_AES_256_CBC_SHA*].

Application note: *Since TLS supports ciphersuite negotiation, peers completing the TLS negotiation will also have selected a ciphersuite, which includes encryption and hashing methods. Since the ciphersuite negotiated within EAP-TLS*

[2] RFC5216: Section 2.4 Ciphersuite and Compression Negotiation
[3] RFC5216: Section 2.4 Ciphersuite and Compression Negotiation

	applies only to the EAP conversation, TLS ciphersuite negotiation MUST NOT be used to negotiate the ciphersuites used to secure data. *TLS also supports compression as well as ciphersuite negotiation. However, during the EAP-TLS conversation the EAP peer and server MUST NOT request or negotiate compression.*
FCS_EAP-TLS_EXT.1.4	The TSF EAP-TLS implementation[4] [selection: supports validating the peer certificate using RFC 3280 compliant path validation, is pre-configured with the necessary intermediate certificates to complete path validation, relies on the EAP-TLS peer to provide this information as part of the TLS handshake, does not support certificate path validation].
FCS_EAP-TLS_EXT.1.5	EAP-TLS implementation[5] provides [selection: *its entire certificate chain minus the root, only the server certificate*] to facilitate certificate validation by the peer
FCS_EAP-TLS_EXT.1.6	The TSF shall ensure that once a TLS session is established, the EAP-TLS implementation validate that the identity represented in the peer certificate is appropriate and authorized for use with EAP-TLS[6].
Application note:	*The authorization process makes use of the contents of the certificate as well as other contextual information. It is recommended that the EAP-TLS implementation be able to authorize based on the EAP-TLS Peer-Id. In EAP-TLS, the Peer-Id is determined from the subject or subjectAltName fields in the peer certificates. For details, see Section 4.1.2.6 of RFC3280.*
FCS_EAP-TLS_EXT.1.7	The TSF shall ensure that the EAP-TLS implementation supports the use of Certificate Revocation Lists (CRLs), and [selection: *Online Certificate Status Protocol (OCSP), no other*] methods to check certification revocation status[7].

.

[4] RFC5216: Section 5.3 Certificate Validation
[5] RFC5216: Section 5.3 Certificate Validation
[6] RFC5216: Section 5.3 Certificate Validation
[7] RFC5216: Section 5.4 Certificate Revocation

5.1.1.12 FCS_EAP-TTLS_EXT EAP_TTLS Authentication Protocol

EAP-TTLS, Extensible Authentication Protocol - Tunneled Transport Layer Security, is an extension of the EAP-TLS authentication protocol for 802.1x authentication. EAP-TTLS supports password and (optionally) certificate for client and server authentication.

Family Behavior

This family provides requirements that address authentication on a 802.1x wireless network.

Component leveling

FCS_EAP-TTLS_EXT: EAP-TTLS Authentication Protocol	1

FCS_EAP-TTLS_EXT.1 EAP-TTLS Authentication Protocol requires the TSF provide the facilities to authenticate to the wireless network.

Management: FCS_EAP-TTLS_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FCS_EAP-TTLS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.12.1 FCS_EAP-TTLS_EXT.1 EAP-TLS Authentication Protocol

Hierarchical to: None

Dependencies: FCS_TLS_EXT.1

FCS_EAP-TTLS_EXT.1.1	The TSF shall implement the EAP-TTLSv0 authentication protocol that complies with RFC 5281.
FCS_EAP-TTLS_EXT.1.2	The TSF shall implement[8] [selection: *TLS 1.0, TLS v1.1, TLS v1.2*] as specified in FCS_TLS_EXT.1.
FCS_EAP-TTLS_EXT.1.3	The TSF shall ensure that the EAP-TTLS implementation supports EAP[9], [selection: *PAP, CHAP, MS-CHAP-V2, EAP-MS-CHAP-V2, EAP-GTC, no other*] tunneled authentication methods.
. FCS_EAP-TTLS_EXT.1.4	The TSF shall ensure that the EAP-TTLS implementation supports MD5-Challenge[10],[selection: [assignment: *list of supported EAP types*], *No other*] EAP type.

.

[8] RFC5281: Section 7.7 TLS Version
[9] RFC5281: Section 11.4 Mandatory Tunneled Authentication Support
[10] RFC5281: Section 11.4 Mandatory Tunneled Authentication Support

5.1.1.13 FCS_PEAP_EXT PEAP Authentication Protocol

PEAP, Protected Extensible Authentication Protocol, is is a protocol that encapsulates the EAP within an encrypted and authenticated TLS tunnel to correct a deficiencies in EAP because EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided.

Family Behavior

This family provides requirements that address authentication on a 802.1x wireless network.

Component leveling

FCS_PEAP_EXT: PEAP Authentication Protocol	1

FCS_PEAP_EXT.1 PEAP Authentication Protocol requires the TSF provide the facilities to authenticate to the wireless network.

Management: FCS_PEAP_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FCS_PEAP_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.13.1 FCS_PEAP_EXT.1 PEAP Authentication Protocol

Hierarchical to: None

Dependencies: FCS_TLS_EXT.1

FCS_PEAP_EXT.1.1 The TSF shall implement the PEAPv0 and PEAPv1 authentication protocol that complies with RFC draft-kamath-pppext-peapv0-00.

FCS_PEAP_EXT.1.2 The TSF shall implement TLS 1.0, [selection: TLS v1.1, TLS v1.2] as specified in FCS_TLS_EXT.1.

FCS_PEAP_EXT.1.3 The TSF shall ensure that the EAP-TLS authentication protocol support the following ciphersuites:

- Mandatory Ciphersuites:
  - TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- Optional Ciphersuites:
  - [selection:
  - *None*
  - *TLS_RSA_WITH_AES_128_CBC_SHA*
  -].

FCS_PEAP_EXT.1.4 The TSF shall ensure that the PEAP implementation supports [selection: EAP-MS-CHAP-V2, EAP-GTC] authentication methods.

5.1.1.14 FCS_RAD_EXT RADIUS Authentication Protocol

RADIUS, Remote Authentication Dial In User Service, is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

Family Behavior

This family provides requirements that address authentication on a 802.1x wireless network.

Component leveling

FCS_RAD_EXT: RADIUS Authentication Protocol	1

FCS_RAD_EXT.1 RADIUS Authentication Protocol requires the TSF provide the facilities to authenticate to the wireless network.

Management: FCS_RAD_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FCS_RAD_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.14.1 FCS_RAD_EXT.1 RADIUS Authentication Protocol

Hierarchical to: None

Dependencies: FCS_IPSEC_EXT.1

FCS_RAD_EXT.1.1	The TSF shall implement the RADIUS authentication protocol that complies with RFCs 2138, 3579, and 3580.
FCS_RAD_EXT.1.2	The TSF shall protect RADIUS communications using IPsec as specified in FCS_IPSEC_EXT.1.
FCS_RAD_EXT.1.3	The TSF shall ensure that the RADIUS implementation supports [selection: PAP, CHAP, EAP-TLS, EAP-TTLS, EAP-MS-CHAP-V2, EAP-GTC, PEAP] authentication methods.

5.1.2 Class FIA: Identification and Authentication

Families in this class address the requirements for functions to establish and verify a claimed user identity.

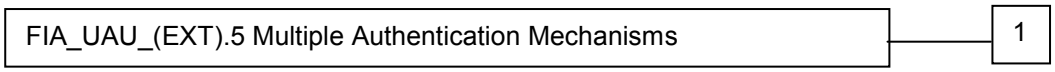
Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g. identity, groups, roles, security or integrity levels)

5.1.2.1 FIA_UAU_(EXT).5 Multiple Authentication Mechanisms

Family Behavior

This family provides requirements that providing multiple methods to authenticate users to the TOE.

Component leveling



FIA_UAU_(EXT).5 Multiple Authentication Mechanisms requires the TSF to provide both local and remote mechanisms to authenticate administrative and wireless users to the TOE.

Management: FIA_UAU_(EXT).5
The following actions could be considered for the management functions in FMT:

- Whether the TOE should use local or remote authentication
- Whether to use remote authentication for administrative users, wireless users, or both

Audit: FIA_UAU_(EXT).5
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Failure to receive a response from the remote authentication server

5.1.2.1.1 FIA_UAU_(EXT).5 Multiple Authentication Methods

Hierarchical to:	None
Dependencies:	None
FIA_UAU_(EXT).5.1	The TSF shall provide local authentication, and a remote authentication mechanism to perform user authentication.
FIA_UAU_(EXT).5.2	The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

5.1.3 Class FID: Intrusion Detection

This class contains families of functional requirements that relate to intrusion detection of IT entities that constitute threats to the TOE.

5.1.3.1 FID_APD_EXT Rogue Access Point Detection

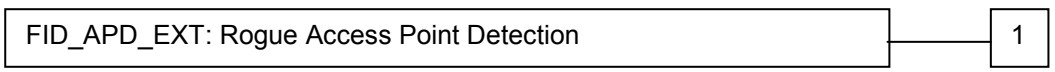
A Rogue Access Point (AP) is an unauthorized active AP operating within the radio coverage area of a 802.11 wireless network; it may possess properties rendering its operation as unauthorized and/or threatening to the authorized access point(s) and/or wireless client communications to/from the LAN.

Any unauthorized active AP operating within the radio coverage of an authorized AP could be identified as a Rogue AP; even if it is not connected to the wired LAN. One threat for a facility is that an attacker places an AP onto a wired network, then leaves the property; allowing the attacker to remotely access or attack the network. Alternatively, an attacker may place an unauthorized AP within the radio coverage area of a commercial wireless network; configure to appear like an authorized AP, allowing the attacker access to the wireless client's data.

Family Behavior

This family provides requirements that address detection of Rogue Access Points in a wireless network.

Component leveling



FID_APD_EXT.1 Rogue Access Point Detection requires the TSF provide the facilities to detect the presence of Rogue Access Points that lie within the range of and constitute a threat to the wireless network.

Management: FID_APD_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FID_APD_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Triggering of the Rogue AP detection routine described in FID_APD_EXT.1.1

5.1.3.1.1 FID_APD_EXT.1 Rogue Access Point Detection

Hierarchical to:	None
Dependencies:	None
FID_APD_EXT.1.1	The TSF shall be able to detect a Rogue Access Point operating within the radio coverage area of an 802.11 wireless network using the following detection method: [assignment: *specify the detection methods used*].
FID_APD_EXT.1.2	Upon detection of a Rogue Access Point, the TSF shall take the following actions: [assignment: *specify the action to be taken*].

5.1.4 Class FPT: Protection of the TSF

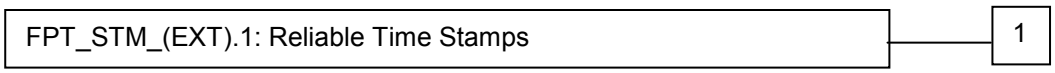
This class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data.

5.1.4.1 FPT_STM_(EXT) Reliable Time Stamps

Family Behavior

This family provides requirements that address providing reliable, accurate time to the TOE.

Component leveling



FPT_STM_(EXT).1: Reliable Time Stamps requires the TSF to synchronize its time with an external time source.

Management: FPT_STM_(EXT).1
The following actions could be considered for the management functions in FMT:

- Configuration of the external time server

Audit: FPT_STM_(EXT).1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Changes to the time

5.1.4.1.1 FPT_STM_(EXT).1 Reliable Time Stamps

Hierarchical to:	None
Dependencies:	None
FPT_STM_EXT.1.1	The TSF shall be able to provide reliable time stamps, synchronized via an external time source, for its own use.

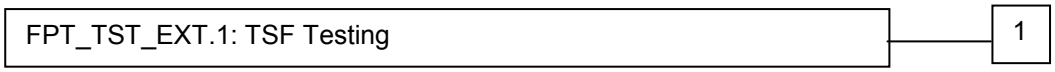
Application Note: *The TOE must be capable of obtaining a time stamp via an NTP server.*

5.1.4.2 FPT_TST_EXT TSF Testing

Family Behavior

This family provides requirements that address self tests run by the TOE

Component leveling



FPT_TST_EXT.1: TSF Testing requires the TSF run self tests at various times to ensure its proper operation.

Management: FPT_TST_EXT.1
The following actions could be considered for the management functions in FMT:

- none

Audit: FPT_TST_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Execution of the self test, including success and failure of each test

5.1.4.2.1 FPT_TST_EXT.1 TSF Testing

Hierarchical to:	None
Dependencies:	None
FPT_TST_EXT.1.1	The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.
FPT_TST_EXT.1.2	The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

5.1.5 Class FTP: Trusted path/channels

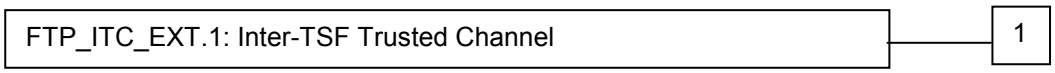
Families in this class provide requirements for a trusted communication path between users and the TSF, and for a trusted communication channel between the TSF and other trusted IT products.

5.1.5.1 FTP_ITC_EXT.1 Inter-TSF Trusted Channel

Family Behavior

This family provides requirements that address the use of secure communications with entities in the IT environment.

Component leveling



FTP_ITC_EXT.1: Inter-TSF Trusted Channel requires the TSF to use secure communication methods and mutual authentication between itself and the IT environment.

Management: FTP_ITC_EXT.1
The following actions could be considered for the management functions in FMT:

- Configuration of attributes of the secure channel

Audit: FTP_ITC_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Initiation/Closure of a trusted channel;

5.1.5.1.1 FTP_ITC_EXT.1 Inter-TSF Trusted Channel

Hierarchical to:	None
Dependencies:	None
FPT_ITC_EXT.1.1	The TOE shall provide an encrypted communication channel between itself and entities in the TOE IT Environment that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FPT_ITC_EXT.1.2	The TSF shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.
FPT_ITC_EXT.1.3	The TSF shall initiate communication via the trusted channel for [all authentication functions, remote logging, time, [*selection: [assignment: communications with authorized IT entities determined by the ST author], none*]].

Application Note: If a certificate authority server plays a role in the authentication of users, then the CA is considered an authorized IT entity and the TSF is expected to initiate secure communications with this entity. It is assumed that the IT environment includes an NTP server, an audit server and/or an authentication server.

5.2 Extended Security Assurance Requirement Definitions

There are no extended Security Assurance Requirements defined in this Security Target.

5.3 Rationale for Extended Security Requirements

This section presents the rationale for the inclusion of the extended requirements found in this Security Target.

5.3.1 Rationale for Extended Security Function Requirements

The following cryptographic support SFRs are extended, as Part II of the Common Criteria does not include an SFR that describes the requirements for the use of cryptographic communications protocols used to protect networked communications. These security functions are considered critical in environments having threats that may compromise the communication channel between administrators, other portions of the (distributed) TOE, or external IT entities.

FCS_COMM_PROT_EXT.1	Communications Protection
FCS_HTTPS_EXT.1	HTTPS
FCS_SFTP_EXT.1	SSH File Transfer Protocol
FCS_SNMPv3_EXT	SNMPv3 Protocol
FCS_SSH_EXT.1	SSH Protocol
FCS_TLS_EXT.1	TLS Protocol
FCS_IPSEC_EXT.1	Internet Protocol Security (IPSec)

The following cryptographic support SFRs are extended, as Part II of the Common Criteria does not include an SFR that describes the requirements for the use of cryptographic authentication protocols used to protect networked communications. These security functions are considered critical in environments having threats that may compromise the communication channel between administrators, other portions of the (distributed) TOE, or external IT entities.

FCS_EAP-TLS_EXT.1	EAP-TLS Authentication Protocol
FCS_EAP-TTLS_EXT.1	EAP-TTLS Authentication Protocol
FCS_PEAP_EXT.1	PEAP Authentication Protocol
FCS_RAD_EXT.1	RADIUS Authentication Protocol

The following Intrusion Detection SFR is extended, as Part II of the Common Criteria does not include an SFR that describes the detection of Rogue Access Points. These security functions are considered critical in environments where these rogue units represent a threat to the TSF.

FID_APD_EXT.1	Rogue Access Point Detection

The following SFRs are extended, with the rationale provided in the table below:

FCS_BCM_(EXT).1	Baseline cryptographic module	This extended requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.
FCS_CKM_(EXT).2	Cryptographic key handling and storage	This extended requirement is necessary since the CC does not specifically provide components for key handling and storage.
FCS_COP_(EXT).1	Random number generation	This extended requirement is necessary since the CC cryptographic operation components address only specific algorithm types and operations requiring specific key sizes.
FDP_PUD_(EXT).1	Protection of User Data	This extended requirement is necessary because the Common Criteria IFC/AFC requirements do not accommodate access control policies that are not object/attribute based. The FDP_PUP_(EXT).1

		requirement allows the administrator allow or disallow access based upon an administrator setting indicating whether or not unencrypted data may transit the wireless LAN.
FIA_UAU_(EXT).5	Multiple authentication mechanisms	This extended requirement is needed for local administrators because there is concern over whether or not existing CC requirements specifically require that the TSF provide authentication. Authentication provided by the TOE is implied by other FIA_UAU requirements and is generally assumed to be a requirement when other FIA_UAU requirements are included in a TOE. In order to remove any potential confusion about this ST, an extended requirement for authentication has been included. This ST also requires the IT environment to provide an authentication server to be used for authentication of remote users. It is important to specify that the TSF must provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server. In addition, the TOE must provide the portions of the authentication mechanism necessary to obtain and enforce an authentication decision from the IT environment.
FPT_TST_(EXT).1	TSF Testing	This extended requirement is necessary to divide the TOE testing requirements between those necessary for the TOE itself and those specific to cryptographic modules.
FTP_ITC_(EXT).1	Inter-TSF trusted channel	This extended requirement is necessary because the existing trusted channel requirement is written with the intent of protecting communication between distributed portions of the TOE rather than between the TOE and its trusted IT environment.

5.3.2 Rationale for Extended Security Assurance Requirements

There are no extended Security Assurance Requirements defined in this ST; therefore, no rationale is presented.

6 Security requirements

This section describes the security functional and assurance requirements for the TOE; those that are CC Part 2 conformant, CC Part 2 extended, and CC Part 3 conformant.

6.1 Security Function Requirements

This section describes the functional requirements for the TOE. The security functional requirement components in this security target are CC Part 2 conformant or CC Part 2 extended as defined in Section 2, Conformance Claims. Table 11 - TOE Security Functional RequirementsTable 11 - TOE Security Functional Requirements, lists the SFRs included in this Security Target.

Table 11 - TOE Security Functional Requirements

#	SFR	Description	Operations
1	FAU_GEN.1	Audit data generation	A - S
2	FAU_GEN.2	User identity association	---
3	FAU_SEL.1	Selective audit	A - S
4	FCS_BCM_(EXT).1	Extended: baseline cryptographic module	S
5	FCS_CKM.1 (1)	Cryptographic symmetric key generation	I
6	FCS_CKM.1 (2)	Cryptographic asymmetric key generation	A – S - I
7	FCS_CKM.2	Cryptographic key distribution	S
8	FCS_CKM_(EXT).2	Cryptographic key handling and storage	---
9	FCS_CKM.4	Cryptographic key destruction	---
10	FCS_COP.1 (1)	Cryptographic operation (Data encryption/decryption)	A – S - I
11	FCS_COP.1 (2)	Cryptographic operation (Digital Signature)	A – S - I
12	FCS_COP.1 (3)	Cryptographic operation (Hashing)	S - I
13	FCS_COP.1 (4)	Cryptographic operation (Key agreement)	A - S - I
14	FCS_COP_(EXT).1	Extended: random number generation	A – S
15	FCS_COMM_PROT_EXT.1	Communications Protection	S
16	FCS_EAP-TLS_EXT.1	EAP-TLS Authentication Protocol	S
17	FCS_EAP-TTLS_EXT.1	EAP-TLS Authentication Protocol	S
18	FCS_HTTPS_EXT.1	HTPS	---
19	FCS_IPSEC_EXT.1	Internet Protocol Security (IPsec)	A - S
20	FCS_PEAP_EXT.1	PEAP Authentication Protocol	S
21	FCS_RAD_EXT.1	RADIUS Authentication Protocol	S
22	FCS_SFTP_EXT.1	SSH File Transfer Protocol	---
23	FCS_SNMPv3_EXT.1	SNMPv3	S
24	FCS_SSH_EXT.1	SSH	A - S
25	FCS_TLS_EXT.1	TLS	S
26	FDP_ACC.1	Subset access control	A
27	FDP_ACF.1	Security attribute based access control	A
28	FDP_IFC.1 (1)	Subset information flow control (Traffic Filter SFP)	A - I

Table 11 - TOE Security Functional Requirements			
#	SFR	Description	Operations
29	FDP_IFC.1 (2)	Subset information flow control (Unauthenticated TOE Services SFP)	A - I
30	FDP_IFC.1 (3)	Subset information flow control (Authenticated Information Flow SFP)	A - I
31	FDP_IFF.1-NIAP-0417 (1)	Simple security attributes (Traffic Filter SFP)	A – R - I
32	FDP_IFF.1-NIAP-0417 (2)	Simple security attributes (Unauthenticated TOE Services SFP)	A – R - I
33	FDP_IFF.1-NIAP-0417 (3)	Simple security attributes (Authenticated Information Flow SFP)	A – R - I
34	FDP_RIP.1	Subset residual information protection	S
35	FIA_AFL.1	Administrator authentication failure handling	A
36	FIA_ATD.1 (1)	Administrator attribute definition	A - I
37	FIA_ATD.1 (2)	User attribute definition	A – I - R
38	FIA_UAU.1 (1)	Timing of authentication (Administrative user)	A – I - R
39	FIA_UAU.1 (2)	Timing of authentication (Wireless user)	A – I - R
40	FIA_UAU_(EXT).5	Multiple authentication mechanisms	R
41	FIA_UID.2	User identification before any action	---
42	FIA_USB.1	User-subject binding	R - A
43	FID_APD_EXT.1	Rogue Access Point Detection	A
44	FMT_MOF.1 (1)	Management of security functions behavior (Cryptographic Function)	I
45	FMT_MOF.1 (2)	Management of security functions behavior (Audit Record Generation)	I – R
46	FMT_MOF.1 (3)	Management of security functions behavior (Authentication)	I - R
47	FMT_MOF.1 (4)	Management of security functions behavior (Firewall)	I - A - S
48	FMT_MOF.1 (5)	Management of security functions behavior (Intrusion Detection)	I - A - S
49	FMT_MSA.1	Management of security attributes	A - S
50	FMT_MSA.2[11]	Secure security attributes	---
51	FMT_MSA.3 (1)	Static attribute initialization (Role-Based Access Control SFP)	A - S - R - I
52	FMT_MSA.3 (2)	Static attribute initialization (Traffic Filter SFP)	A - S - R - I
53	FMT_MSA.3 (3)	Static attribute initialization (Unauthenticated TOE Services SFP)	A - S - R - I
54	FMT_MSA.3 (4)	Static attribute initialization (Authenticated Information Flow SFP)	A - S - R - I
55	FMT_MTD.1 (1)	Management of Audit pre-selection data	A - S - I
56	FMT_MTD.1 (2)	Management of TSF data (Administrative user authentication)	A - S - I
57	FMT_MTD.1 (3)	Management of TST data (Wireless user authentication)	A - S - I
58	FMT_SMF.1 (1)	Specification of management functions (Cryptographic Functions)	I

[11] The dependency on ADV_SPM.1 was removed, the ST author believes it was an error; ADV_SPM.1 is a requirement at EAL6.

Table 11 - TOE Security Functional Requirements			
#	SFR	Description	Operations
59	FMT_SMF.1 (2)	Specification of Management Functions (TOE Audit Record Generation)	I
60	FMT_SMF.1 (3)	Specification of management functions (Cryptographic Key Data)	I
61	FMT_SMF.1 (4)	Specification of management functions (Firewall)	I
62	FMT_SMF.1 (5)	Specification of management functions (Intrusion Detection)	I
63	FMT_SMR.1	Security roles	A
64	FPT_ITT.1	Basic internal TSF data transfer protection	---
65	FPT_STM_(EXT).1	Reliable time stamps	---
66	FPT_TST_EXT.1	TSF Testing	---
67	FPT_TST.1 (1)	TSF Testing (for cryptography)	R - I
68	FPT_TST.1 (2)	TSF Testing (for key generation components)	R - I
69	FTA_SSL.3	TSF-initiated termination	---
70	FTA_TAB.1	Default TOE access banners	---
71	FTP_ITC_EXT.1 (1)	Inter-TSF trusted channel	S

6.1.1 Security Audit

6.1.1.1 FAU_GEN Audit data generation

6.1.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events listed in column “Auditable Events” *Table 12 - TOE Auditable Events*; and[12]

c) ***None***.

Table 12 - TOE Auditable Events			
#	Requirement	Auditable Events	Additional Audit Record contents
1	FAU_GEN.1	None	None
2	FAU_GEN.2	None	None
3	FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the Administrator performing the function
4	FCS_CKM.1 (1)	Generation of a key	The identity of the Administrator performing the function
5	FCS_CKM.1 (2)	Generation of a key	The identity of the Administrator performing the function
6	FCS_CKM_EXT.2	Error(s) detected during	If available - the authentication credentials of

[12] The WLAN AS PP is inconsistent as it specifies the minimum level of audit, but adds a table that is not referenced in FAU_GEN.1.1. The ST author believes the required events are listed in the table.

Table 12 - TOE Auditable Events			
#	Requirement	Auditable Events	Additional Audit Record contents
		cryptographic key transfer	subjects with which the invalid key is shared
7	FCS_CKM.4	Destruction of a cryptographic key	The identity of the Administrator performing the function
8	FCS_COP.1 (1), (2),(3),(4)	None	None
9	FCS_COP_(EXT).1	None	None
10	FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
11	FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Establishment/Termination of an IPsec SA.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
12	FCS_SFTP_EXT.1	Failure of the file transfer	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
13	FCS_SNMPV3_EXT.1	Failure to authenticate SNMP message	None
14	FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
15	FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
16	FCS_EAP-TLS_EXT.1	Authentication success and failures	None
17	FCS_EAP-TTLS_EXT.1	Authentication success and failures	None
18	FCS_PEAP_EXT.1	Authentication success and failures	None
19	FCS_RAD_EXT.1	Authentication success and failures	None
20	FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP.	None
21	FDP_IFF.1-NIAP-0417 (1)	Decisions to permit requested information flows Failure to reassemble fragmented packets	Presumed IP address of source subject IP address of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface associated on which the TOE received the packet Identity of the rule that allowed or disallowed the packet flow Reason why fragmented packets could not be reassembled (i.e., invalid fragment identifier, invalid offset, invalid fragment data length)
22	FDP_IFF.1-NIAP-0417 (2)	Decisions to permit/deny information flows between a subject and the TOE	Presumed IP address of source subject IP address of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface associated on which the TOE received the packet Identity of the rule that allowed or disallowed the packet flow, if applicable

Table 12 - TOE Auditable Events			
#	Requirement	Auditable Events	Additional Audit Record contents
23	FDP_IFF.1-NIAP-0417 (3)	Decisions to permit/deny information flows between a subject and the TOE Failure to reassemble fragmented packets	Presumed IP address of source subject IP adddress of destination subject ESSID Authentication, Encryption Type AP Location Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Port ACL, if applicable Stateful packet inspection attributes
24	FDP_RIP.1	None	None
25	FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)	None
26	FIA_ATD.1 (1), (2)	None	None
28	FIA_UAU.1 (1), (2)	Use of the authentication mechanism (success or failure)	User identity - the TOE SHALL NOT record invalid passwords the audit log.
29	FIA_UAU_(EXT).5	Authentication success or failure Failure to receive a response from the remote authentication server	For admin users, the user name, mode of authentication For wireless users, the information flow to authenticate the user, user name Identification of the Authentication server that did not reply
30	FIA_UID.2	None	None
31	FIA_USB.1	Unsuccessful binding of user security attributes to a subject	None
32	FID_APD_EXT.1	Detection of Rogue AP	BSSID/MAC address of the Rogue AP ESSID of the Rogue AP Count
33	FMT_MOF.1 (2)	Start or Stop of audit record generation	None
34	FMT_MOF.1 (3)	Changes to the TOE remote authentication settings; Changes to the threshold of failed authentication attempts; Changes to the session lock timeframe	The identity of the Administrator performing the function.
35	FMT_MSA.2	All offered and rejected values for security attributes	None
36	FMT_MTD.1 (1)	Changes to the set of rules used to pre-select audit events.	None
37	FMT_MTD.1 (2)	Changing the TOE authentication credentials	None – the TOE SHALL NOT record authentication credentials in the audit log.
38	FMT_SMR.1	Modifications to the group of users that are part of a role	None
39	FPT_STM_(EXT).1	Changes to the time	None
40	FPT_TST_(EXT).1	Execution of the self test	Success or Failure of test

Table 12 - TOE Auditable Events			
#	Requirement	Auditable Events	Additional Audit Record contents
41	FPT_TST.1	Execution of the self test	Success or Failure of test
42	FPT_TST.2	Execution of the self test	Success or Failure of test
43	FTA_SSL.3	TSF Initiated Termination	Termination of an interactive session by the session locking mechanism
44	FTP_ITC_(EXT).1	Initiation/Closure of a trusted channel;	Identification of the remote entity with which the channel was attempted/created; Success of failure of the event

FAU_GEN.1.2 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 (if applicable), 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 included in the PP/ST, ***information specified in column three of Table 12.***

Application Note: *Event type is defined to be the severity level indicator as it is defined in IETF RFC 3164 The BSD syslog Protocol.*

6.1.1.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 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.

6.1.1.1.3 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) user identity, event type,

b) device interface, wireless client identity

Application Note: *Event type is defined to be the severity level indicator as it is defined in IETF RFC 3164 The BSD syslog Protocol.*

Application Note: *The device interface is the physical interface upon which user (or administrative) data is received/sent (e.g. WLAN interface, wired LAN interface, serial port, administrative LAN interface, etc.).*

6.1.2 Class FCS: Cryptographic support

6.1.2.1 FCS_CKM Cryptographic Key Management

6.1.2.1.1 FCS_BCM_(EXT).1 Extended: baseline cryptographic module

FCS_BCM_(EXT).1.1 All cryptographic functions implemented by the TOE shall be validated by NIST CAVP and include an algorithm validation certificate.

6.1.2.1.2 FCS_CKM.1 (1) Cryptographic key generation (for symmetric keys)

FCS_CKM.1.1(1) **Refinement**[13]:The TSF shall generate symmetric cryptographic keys using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity protection to generated symmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.

Application Note: *NIST SP 800-57 "Recommendation for Key Management" Section 6.1 states: "Integrity protection can be provided by cryptographic integrity mechanisms (e.g. cryptographic checksums, cryptographic hashes, MACs, and signatures), non-cryptographic integrity mechanisms (e.g. CRCs, parity, etc.) […], or physical protection mechanisms". Guidance for the selection of appropriate integrity mechanisms is given in Sections 6.2.1.2 and 6.2.2.2 of NIST SP 800-57 "Recommendation for Key Management".*

6.1.2.1.3 FCS_CKM.1 (2) Cryptographic key generation (for asymmetric keys)

FCS_CKM.1.1 (2) **Refinement**[14]: The TSF shall generate asymmetric cryptographic keys in accordance with the mathematical specifications of the FIPS-approved or NIST-recommended standard ***FIPS 186-2***, using a domain parameter generator and **FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1** in a cryptographic key generation scheme that meets the following:

- The TSF shall provide integrity protection and assurance of domain parameter and public key validity to generated asymmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.
- Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 112 bits using conservative estimates.

Application Note: *NIST SP 800-57 "Recommendation for Key Management" Section 6.1 states: "Integrity protection can be provided by cryptographic integrity mechanisms (e.g. cryptographic checksums, cryptographic hashes, MACs, and signatures), non-cryptographic integrity mechanisms (e.g. CRCs, parity, etc.) […], or physical protection mechanisms." Guidance for the selection of appropriate integrity mechanisms is given in Sections 6.2.1.2 and 6.2.2.2 of NIST SP 800-57 "Recommendation for Key Management".*

Application Note: *Assurance of domain parameter and public key validity provides confidence that the parameters and keys are arithmetically correct. Guidance for the selection of appropriate validation mechanisms is given in NIST SP 800-57 "Recommendation for Key Management," NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," and FIPS PUB 186-2, "Digital Signature Standard."*

Application Note: *See NIST Special Publication 800-57, "Recommendation for Key Management" for information about equivalent key strengths.*

[13] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

[14] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

6.1.2.1.4 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **manual (physical method), and automated (electronic) method** that meets the following:

- NIST Special Publication 800-57, "Recommendation for Key Management" Section 8.1.5
- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

Application Note: *NIST Special Publication 800-56A "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" is only applicable when public key schemes are used in key transport methods.*

Application Note: *DoD applications may have additional key distribution requirements related to the DoD PKI and certificate formats.*

6.1.2.1.5 FCS_CKM_(EXT).2 Extended: Cryptographic Key Handling and Storage

FCS_CKM_(EXT).2.1 The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

Application Note: *A parity check is an example of a key error detection check.*

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

Application Note: *Note that this requirement is stronger than the FIPS 140-2 key storage requirements, which state: "Cryptographic keys stored within a cryptographic module shall be stored in plaintext form or encrypted form."*

Application Note: *A persistent key, such as a file encryption key, is one that must be available in the system over long periods of time. A non-persistent key, such as a key used to encrypt or decrypt a single message or a session, is one that is ephemeral in the system.*

Application Note: *"When not in use" is interpreted in the strictest sense so that persistent keys only exist in plaintext form during intervals of operational necessity. For example, a file encryption key exists in plaintext form only during actual encryption and/or decryption processing of a file. Once the file is decrypted or encrypted, the file encryption key should immediately be covered for protection.*

Application Note: *A "split knowledge procedure" is a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.*

FCS_CKM_(EXT).2.3 The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

Application Note: *The cryptographic administrator must have the ability to set a threshold of inactivity after which non-persistent keys must be destroyed in accordance with FCS_CKM.4.*

FCS_CKM_(EXT).2.4 The TSF shall prevent archiving of expired (private) signature keys.

Application Note: *This requirement is orthogonal to typical system back-up procedures. Therefore, it does not address the problem of archiving an active (private)*

signature key during a system back-up and saving the key beyond its intended life span.

6.1.2.1.6 FCS_CKM.4 Cryptographic key destruction

Application Note: *Note that this requirement is stronger than the FIPS 140-2 key zeroization requirements, which state: "A cryptographic module shall provide methods to zeroize all plaintext secret and private cryptographic keys and CSPs within the module."*

FCS_CKM.4.1 **Refinement**[15]**:** The TSF shall destroy cryptographic keys in accordance with a cryptographic key zeroization method that meets the following:

a) Key Zeroization Requirements in FIPS PUB 140-2 "Security Requirements for Cryptographic Modules

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete.

Application Note: *The term "immediate" here is meant to impart some urgency to the destruction: it should happen as soon as practical after the key is no longer required to be in plaintext. It is certainly permissible to complete a critical section of code before destroying the key. However, the destruction shouldn't wait for idle time, and there shouldn't be any non-determined event (such as waiting for user input) which occurs before it is destroyed.*

c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical cryptographic security parameter to another location.

Application Note: *Item c) pertains to the elimination of internal, temporary copies of keys/parameters during processing, and not to the locations that are used for the storage of the keys, which are specified in item b). The temporary locations could include memory registers, physical memory locations, and even page files and memory dumps.*

d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

Application Note: *Although verification of the zeroization of each intermediate location consisting of non-volatile memories is desired here (by checking for the final known alternating data pattern), it is not required at this time.*

e) For volatile memory and non-volatile EEPROM and Flash memories, the zeroization shall be executed by a single direct overwrite consisting of a pseudo random pattern, followed by a read-verify.

6.1.2.2 Cryptographic operation (FCS_COP)

6.1.2.2.1 FCS_COP.1 (1) Cryptographic operation (for data encryption/decryption)

FCS_COP.1.1 (1) **Refinement**: The TSF shall perform ***symmetric encryption and decryption*** in accordance with ~~a specified~~ the FIPS-approved security cryptographic algorithms

a) TDEA with three independent keys operating in CBC mode,

[15] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

b) AES operating in CBC and CFB mode

and cryptographic key sizes

a) 168-bits

b) 128-bits, 192-bits, and 256-bits

that meet the following:

a) conformant to FIPS 46-3 (TDEA), conformant to FIPS 81 (CBC mode),

b) conformant to FIPS 197 (AES, CBC mode).

6.1.2.2.2 FCS_COP.1 (2) Cryptographic operation (for cryptographic signature)

FCS_COP.1.1 (2) The TSF shall perform cryptographic signature services[16] using the FIPS-approved security function **RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of *2048 bits*** that meets NIST Special Publication 800-57, "Recommendation for Key Management."

6.1.2.2.3 FCS_COP.1 (3) Cryptographic operation (for cryptographic hashing)

FCS_COP.1.1 (3) **Refinement:**[17] The TSF shall perform cryptographic hashing services using the FIPS-approved security function Secure Hash Algorithm and message digest size of **160, 256 bits**.

Application Note: *The message digest size should correspond to double the system symmetric encryption key strength.*

6.1.2.2.4 FCS_COP.1 (4) Cryptographic Operation (for cryptographic key agreement)

Application Note: *"Cryptographic key agreement" is a procedure where the resultant secret keying material is a function of information contributed by two participants, so that no party can predetermine the value of the secret keying material independently from the contributions of the other parties.*

FCS_COP.1.1 (4) **Refinement**[18]**:** The TSF shall perform cryptographic key agreement services using the FIPS-approved security function as specified in NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

***1) Diffie-Hellman Key Agreement Algorithm* and cryptographic key sizes (modulus) of *2048 bits*,**

that meets NIST Special Publication 800-57, "Recommendation for Key Management."

Application Note: *Some authentication mechanism on the keying material is recommended. In addition, repeated generation of the same shared secrets should be avoided.*

Application Note: *FIPS 140-2 Annex D specifies references for FIPS-approved Key Establishment Techniques, one of which is NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography."*

[16] Cryptographic signature services includes digital signature generation and verification

[17] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007[17] NIAP approved addition of 160-bits to the selections permitted in the WLAN AS PP

[18] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

6.1.2.2.5 FCS_COP_(EXT).1 Extended: random number generation

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG ***ANSI X9.31*** seeded by **one or more independent software-based entropy sources**.

FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

6.1.2.3 Communications Protocols

6.1.2.3.1 FCS_COMM_PROT_EXT.1 Communications Protection

FCS_COMM_PROT_EXT.1.1 The TSF shall protect communications using **SSH, IPsec, and TLS/HTTPS.**

6.1.2.3.2 FCS_HTTPS_EXT.1 HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

6.1.2.3.3 FCS_IPSEC_EXT.1 Internet Protocol Security (IPsec)

FCS_IPSEC_EXT.1.1 The TSF shall implement IPsec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-192, AES-CBC-256 (as specified by RFC 3602), **no other algorithms** and using IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109; **no other method** to establish the security association.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

FCS_IPSEC_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to ***200*** MB of traffic for Phase 2 SAs.

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and **no other DH groups**.

FCS_IPSEC_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the **PSK** algorithm

FCS_IPSEC_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) and **no other method** for use in authenticating its IPsec connections.

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

1) Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”);
2) Pre-shared keys ***with lengths from 8 to 256 characters.***

6.1.2.3.4 FCS_SFTP_EXT.1 SSH File Transfer Protocol

FCS_SFTP_EXT.1.1 The TSF shall implement the SSH File Transfer Protocol as specified in draft-ietf-secsh-filexfer-13.txt, July 10, 2006.

FCS_SFTP_EXT.1.2 The TSF shall ensure the SFTP connection has privacy and integrity features provided by the underlying SSH transport protocol as specified in FCS_SSH_EXT.1.

6.1.2.3.5 FCS_SNMPV3_EXT.1 SNMPV3

FCS_SNMPV3_EXT.1.1 The TSF shall implement the SNMPV3 protocol that complies with RFCs:

- 3411 (Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks),
- 3414 (User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)),
- 3415 (View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- 3417 (Transport Mappings for the Simple Network Management Protocol (SNMP)), and
  - **3826 (The Advanced Encryption Standard (AES_ Cipher Algorithm in the SNMP User-based Security Model).**

FCS_SNMPV3_EXT.1.2 The TSF shall ensure that SNMPv3 uses AES128-CFB for privacy and HMAC_SHA-96 for authentication.

6.1.2.3.6 FCS_SSH_EXT.1 SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of ***600 seconds***, and provide a limit to the number of failed authentication attempts a client may perform in a single session to ***an administrator configurable number between 1 and 1024, with a default of 3*** attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the password-based authentication method as described in RFC 4252.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFC 4253, packets greater than ***32768*** bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-192, AES-CBC-256, **no other algorithms**.

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and **no other public key algorithms,** as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that data integrity algorithms used in SSH transport connection is hmac-sha1 **and hmac-sha1-96**.

FCS_SSH_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

6.1.2.3.7 FCS_TLS_EXT.1 TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols **TLS 1.0 (RFC 2346)** supporting the following ciphersuites:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
- Optional Ciphersuites:
  - **None**

6.1.2.4 Authentication Protocols

6.1.2.4.1 FCS_EAP-TLS_EXT.1 EAP-TLS Authentication Protocol

FCS_EAP-TLS_EXT.1.1 The TSF shall implement the EAP-TLS authentication protocol that complies with RFC 5216.

FCS_EAP-TLS_EXT.1.2 The TSF shall implement TLS 1.0[19], and **no other** protocol as specified in FCS_TLS_EXT.1.

FCS_EAP-TLS_EXT.1.3 The TSF shall ensure that the EAP-TLS authentication protocol support the following ciphersuites[20]:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA per RFC4346
- Optional Ciphersuites:
  - **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**
  - **TLS_DHE_RSA_WITH_AES_256_CBC_SHA**
  - **TLS_RSA_WITH_AES_128_CBC_SHA**
  - **TLS_RSA_WITH_AES_256_CBC_SHA**

Application note: *Since TLS supports ciphersuite negotiation, peers completing the TLS negotiation will also have selected a ciphersuite, which includes encryption and hashing methods. Since the ciphersuite negotiated within EAP-TLS applies only to the EAP conversation, TLS ciphersuite negotiation must not be used to negotiate the ciphersuites used to secure data.*

TLS also supports compression as well as ciphersuite negotiation. However, during the EAP-TLS conversation the EAP peer and server must not request or negotiate compression.

FCS_EAP-TLS_EXT.1.4 The TSF EAP-TLS implementation[21] **relies on the EAP-TLS peer to provide this information as part of the TLS handshake**.

FCS_EAP-TLS_EXT.1.5 EAP-TLS implementation[22] provides **only the server certificate** to facilitate certificate validation by the peer

FCS_EAP-TLS_EXT.1.6 The TSF shall ensure that once a TLS session is established, the EAP-TLS implementation validate that the identity represented in the peer certificate is appropriate and authorized for use with EAP-TLS[23].

Application note: *The authorization process makes use of the contents of the certificate as well as other contextual information. It is recommended that the EAP-TLS implementation be able to authorize based on the EAP-TLS Peer-Id. In EAP-TLS, the Peer-Id is determined from the subject or subjectAltName fields in the peer certificates. For details, see Section 4.1.2.6 of RFC3280.*

FCS_EAP-TLS_EXT.1.7 The TSF shall ensure that the EAP-TLS implementation supports the use of Certificate Revocation Lists (CRLs), and **no other** methods to check certification revocation status[24].

[19] RFC5216: Section 2.4 Ciphersuite and Compression Negotiation
[20] RFC5216: Section 2.4 Ciphersuite and Compression Negotiation
[21] RFC5216: Section 5.3 Certificate Validation
[22] RFC5216: Section 5.3 Certificate Validation
[23] RFC5216: Section 5.3 Certificate Validation
[24] RFC5216: Section 5.4 Certificate Revocation

6.1.2.4.2 FCS_EAP-TTLS_EXT.1 EAP-TTLS Authentication Protocol

FCS_EAP-TTLS_EXT.1.1 The TSF shall implement the EAP-TTLSv0 authentication protocol that complies with RFC 5281.

FCS_EAP-TTLS_EXT.1.2 The TSF shall implement[25] **TLS 1.0** as specified in FCS_TLS_EXT.1

FCS_EAP-TTLS_EXT.1.3 The TSF shall ensure that the EAP-TTLS implementation supports EAP[26], **MD5, MSCHAP-V2, PAP** tunneled authentication methods.

FCS_EAP-TTLS_EXT.1.4 The TSF shall ensure that the EAP-TTLS implementation supports MD5-Challenge[27], **No other** EAP type.

6.1.2.5 FCS_PEAP_EXT.1 PEAP Authentication Protocol

FCS_PEAP_EXT.1.1 The TSF shall implement the PEAPv0 and PEAPv1 authentication protocol that complies with RFC draft-kamath-pppext-peapv0-00.

FCS_PEAP_EXT.1.2 The TSF shall implement TLS 1.0, as specified in FCS_TLS_EXT.1.

FCS_PEAP_EXT.1.3 The TSF shall ensure that the EAP-TLS authentication protocol support the following ciphersuites:

- Mandatory Ciphersuites:
  - TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- Optional Ciphersuites:
  - **None**

FCS_PEAP_EXT.1.4 The TSF shall ensure that the PEAP implementation supports **EAP-MS-CHAP-V2, EAP-GTC** authentication methods.

6.1.2.5.1 FCS_RAD_EXT.1 RADIUS Authentication Protocol

FCS_RAD_EXT.1.1 The TSF shall implement the RADIUS authentication protocol that complies with RFCs 2138, 3579, and 3580.

FCS_RAD_EXT.1.2 The TSF shall protect RADIUS communications using IPsec as specified in FCS_IPSEC_EXT.1.

FCS_RAD_EXT.1.3 The TSF shall ensure that the RADIUS implementation supports **PAP, EAP-TLS, EAP-TTLS, EAP-MS-CHAP-V2, EAP-GTC, PEAP** authentication methods.

6.1.3 Class FDP: User data protection

6.1.3.1 FDP_ACC Access control policy

6.1.3.1.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the ***Role-Based Access Control SFP*** on

- ***Subjects: All authenticated users assigned roles as defined in FMT_SMR.1,***
- ***Objects: All management commands accessible via CLI, Web UI, and SNMP***
- ***Operations: Execution of commands***

[25] RFC5281: Section 7.7 TLS Version
[26] RFC5281: Section 11.4 Mandatory Tunneled Authentication Support
[27] RFC5281: Section 11.4 Mandatory Tunneled Authentication Support

6.1.3.2 FDP_ACF Access control functions

6.1.3.2.1 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***Role-Based Access Control SFP*** to objects based on the following: ***Subject: Role, Object: Role***

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- ***the user must be authenticated and assigned to a role;***
- ***all management commands must be assigned a security attribute indicating which role or roles can execute that command;***
- ***the users' access to management commands is restricted based upon the users' assigned role; and***
- ***users can only be associated with one role at any given session***.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***none***.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the ***none***.

6.1.3.3 FDP_IFC Information flow control policy

6.1.3.3.1 FDP_IFC.1 (1) Subset information flow control (*Traffic Filter SFP*)

FDP_IFC.1.1 (1) The TSF shall enforce the ***Traffic Filter SFP*** on

- ***source subject: TOE interface on which information is received;***
- ***destination subject: TOE interface to which information is destined;***
- ***information: network packets; and***
- ***operations: pass information.***

Application Note: *The Traffic Filter SFP allows authenticated and unauthenticated users to pass information through the TOE, with TSF mediation according to the rules defined by the authorized administrator.*

Application Note: *In a firewall, the central issue is that there are two "subjects" (the sender of the packet (information) and the receiver of the packet) neither of which are under the control of the TOE. In order to use the FDP_IF* requirements, we associate the potential set of subjects with a firewall interface. This makes sense because an administrator is able to determine what sets of IP addresses (for example) are associated with each of the physical firewall interfaces (assuming no other "backdoor" connectivity). Associating this potential set of subjects with an interface also allows the specification of subject attributes to be associated with something that is actually part of the TOE (the physical interface), as well as allow FDP_IFF.1.2-NIAP-0417 to be written so that it actually makes sense.*

Note that "operations" also is different from an operating-system-centric world because there is only one operation that the subjects really want: that the information is passed through the firewall.

6.1.3.3.2 FDP_IFC.1 (2) Subset information flow control (*Unauthenticated TOE Services SFP*)

FDP_IFC.1.1 (2) The TSF shall enforce the ***Unauthenticated TOE Services SFP*** on:

- ***source subject: TOE interface on which information is received;***
- ***destination subject: the TOE;***

- ***information: network packets; and***
- ***operations: accept or reject network packet.***

Application Note: *This policy is used to express how the TOE enforces rules concerning network traffic that is destined for the TOE, and the protocols that are allowed as specified in FIA_UAU.1 (1). The intent of this iteration of the requirement is control how the TOE responds to network traffic destined for the TOE, this policy does not have to be enforced in the firewall ruleset (e.g., could be an authorized administrator configurable and TOE controlled via another mechanism).*

In a firewall, the central issue is that there are two "subjects" (the sender of the packet (information) and the receiver of the packet) neither of which are under the control of the TOE. In order to use the FDP_IF requirements, we associate the potential set of subjects with a firewall interface. This makes sense because an administrator is able to determine what sets of IP addresses (for example) are associated with each of the physical firewall interfaces (assuming no other "backdoor" connectivity). Associating this potential set of subjects with an interface also allows the specification of subject attributes to be associated with something that is actually part of the TOE (the physical interface), as well as allow FDP_IFF.1.2-NIAP-0417 to be written so that it actually makes sense.*

Note that "operations" refers to the TOE accepting or rejecting the network packet, since the TOE is not technically always providing the "service". In the case of ARP, another machine (e.g., router on the same subnet) is providing an ARP "service" by providing updates to the TOE's routing tables.

6.1.3.3.3 FDP_IFC.1 (3) Subset information flow control (Authenticated Information Flow SFP)

FDP_IFC.1.1 (3) The TSF shall enforce the ***Authenticated Information Flow SFP*** on

- ***subjects: a wireless user that sends and receives information through the TOE, only after authenticated at the TOE per FIA_UAU.5;***
- ***information: network packets; and***
- ***operations: pass information***

6.1.3.4 FDP_IFF Information flow control functions

6.1.3.4.1 FDP_IFF.1-NIAP-0417 (1) Simple security attributes (Traffic Filter SFP)

FDP_IFF.1.1-NIAP-0417 (1) The TSF shall enforce the ***Traffic Filter SFP*** based on the following types of subject and information security attributes**:**

a) Source subject security attributes:
  a. set of source subject identifiers;
b) Destination subject security attributes:
  a. Set of destination subject identifiers;

Application Note: *For the subjects, the administrator knows the set of identifiers that can be associated with the physical firewall interfaces; therefore, they are not "presumed" identifiers.*

c) Information security attributes:
  a. presumed IP address of source subject;
  b. identity of destination subject;
  c. transport layer protocol;
  d. source subject service identifier;

e. destination subject service identifier (e.g., TCP or UDP destination port number);

d) Stateful packet attributes:

a. Connection-oriented protocols:

i. sequence number;

ii. acknowledgement number;

iii. Flags:

- ***SYN;***
- ***ACK;***
- ***RST;***
- ***FIN;***

b. Connectionless protocols:

i. source and destination network identifiers;

***ii.* source and destination service identifiers;**

Application Note: *The stateful packet attributes are not specified in the ruleset as are the other security attributes. These attributes are intended to be used in FDP_IFF.1.3-NIAP-0417(1) as part of the stateful packet inspection. The TOE keeps state about a connection (e.g., a TCP connection) or pseudo-connection (e.g., UDP stream) and uses that information in determining whether to permit information to flow.*

FDP_IFF.1.2-NIAP-0417 (1) **Refinement**: The TSF shall permit an information flow between a source subject and a destination subject via a controlled operation if the following rules hold:

- ***the presumed identity of the source subject is in the set of source subject identifiers;***
- ***the identity of the destination subject is in the set of source destination identifiers;***
- ***the selected information flow policy rule specifies that the information flow is to be permitted****.*

Application Note: *The TSF does not support information flow policy rules that contain information security attribute values, or wildcards that "stand" for multiple values of the same type.*

FDP_IFF.1.3-NIAP-0417 (1) The TSF shall enforce the following:

- ***fragmentation rule:***
  - ***prior to applying the information policy ruleset, the TOE completely reassembles fragmented packets;***
- ***stateful packet inspection rules:***
  - ***whenever a packet is received that is not associated with an allowed established session (e.g., the SYN flag is set without the ACK flag being set), the information flow policy ruleset, as defined in FDP_IFF.1.2-NIAP-0417(1), is applied to the packet;***
  - ***otherwise, the TSF associates a packet with an allowed established session using the stateful packet attributes***.

Application Note: *This requirement has two distinctive rules that are applied. The first rule ensures that the TOE reassembles packets before applying the policy rules. The TOE ensures that fragments are handled properly and the TOE will drop any malformed packets (e.g., duplicate fragments, invalid offsets) and eliminates the security concern of fragments being received out of order at the target host.*

The second rule requires that the TOE maintains state for connection-oriented sessions and connectionless "pseudo" sessions. The TOE uses the stateful packet attributes to determine if a packet already belongs to a "session" that has been allowed by the TOE's ruleset. If a packet cannot be associated with a session, then the ruleset is applied. Connectionless sessions are subject to these rules and allow an IT entity to respond to a connectionless packet without having to specify a rule in the ruleset to explicitly allow the flow.

FDP_IFF.1.4-NIAP-0417 (1) The TSF shall provide the following ***the authorized administrator shall have the capability to view all information flows allowed by the information flow policy ruleset before the ruleset is applied***.

FDP_IFF.1.5-NIAP-0417 (1) The TSF shall explicitly authorize an information flow based on the following rules: **no explicit authorization rules**.

FDP_IFF.1.6-NIAP-0417 (1) The TSF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;

Application Note: *The intent of this requirement is to ensure that a user cannot send packets originating on one TOE interface claiming to originate on another TOE interface.*

b) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;

Application Note: *A broadcast identity is one that specifies more than one host address on a network. It is understood that the TOE can only know the sub-netting configuration of networks directly connected to the TOE's interfaces and therefore can only be aware of broadcast addresses on those networks.*

c) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier;

d) The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject

6.1.3.4.2 FDP_IFF.1-NIAP-0417 (2) Simple security attributes (Unauthenticated TOE Services SFP)

FDP_IFF.1.1-NIAP-0417 (2) **Refinement:** The TSF shall enforce the ***Unauthenticated TOE Services SFP*** based on the following types of subject and information security attributes**:**

a) Source subject security attributes:
a. set of source subject identifiers;

b) Destination subject security attributes;
a. TOE's network identifier;

Application Note: *For the subjects, the administrator knows the set of identifiers that can be associated with the physical firewall interfaces; therefore, they are not "presumed" identifiers. The term "identifiers" was used instead of "addresses"*

to allow for technologies that are not address-based (e.g., circuit identifiers instead of source and destination addresses).

c) Information security attributes:

- ***presumed identity of source subject;***
- ***identity of destination subject;***
- ***transport layer protocol;***
- ***source subject service identifier;***
- ***destination subject service identifier (e.g., TCP or UDP destination port number); and***

Application Note: *Not all of the above security attributes will exist in all network packets. The intent is that if a network packet includes any of the above security attributes, those attributes will be used in the policy decision. The data link frame type identifies the type of data the data link header encapsulates (e.g., in the case of ARP, the frame type value is 0x0806). The transport layer protocol is what is specified in the 8-bit protocol field in the IP header (e.g., this would include ICMP (value of 1) and is not limited to TCP (value of 6) or UDP (value of 17)). The concept of a "service identifier" may differ depending on the networking stack used; the intent is to specify a service that may exist above the network and transport layers in the protocol stack. A "service" in the IP stack would be NTP, TFTP, etc.*

- ***ICMP message type and code as specified in RFC 792, other information security attributes associated with services identified in FAU_UAU.1.***

FDP_IFF.1.2-NIAP-0417 (2) **Refinement:** The TSF shall permit an information flow between a source subject and the TOE via a controlled operation if the following rules hold:

- ***the presumed identity of the source subject is in the set of source subject identifiers;***
- ***the identity of the destination subject is the TOE;***
-

FDP_IFF.1.3-NIAP-0417 (2) The TSF shall enforce the following information flow control rules:

- ***The TOE shall allow source subjects to access TOE services ICMP, list of other network services provided by the TOE consistent with FIA_UAU.1 (1) without authenticating those source subjects; and***

Application Note: *The intent of this requirement is to allow users to access services such as ICMP Echo (ping) without authentication. However, since some sites may not want to allow this capability, the second bullet was added so that an administrator (see FMT_MOF.1 (6)) can restrict the services available.*

- ***The TOE shall allow the list of services specified immediately above to be enabled (become available to unauthenticated users) or disabled (become unavailable to unauthenticated users).***

FDP_IFF.1.4-NIAP-0417 (2) The TSF shall provide the following ***the authorized administrator shall have the capability to view all information flows allowed by this information flow control policy before the policy is applied***.

Application Note: *The intent here is to provide the authorized administrator the capability to see what information flow controls will be applied to the TOE before those controls are activated. This gives the administrator the opportunity to address*

any errors or unintended TOE interactions with users. In the case of this policy, information flow is between a network device and the TOE.

FDP_IFF.1.5-NIAP-0417 (2) The TSF shall explicitly authorize an information flow based on the following rules: ***none***

FDP_IFF.1.6-NIAP-0417 (2) The TSF shall explicitly deny an information flow based on the following rules:

- ***The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;***
- ***The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;***

Application Note: *A broadcast identity is one that specifies more than one host on a network. It is understood that the TOE can only know the sub-netting configuration of networks directly connected to the TOE's interfaces and therefore can only be aware of broadcast addresses on those networks.*

- ***The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier; and***
- ***The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the TOE.***

6.1.3.4.3 FDP_IFF.1-NIAP-0417 (3) Simple security attributes (Authenticated Information Flow SFP)

FDP_IFF.1.1-NIAP-0417 (3) - The TSF shall enforce the ***Authenticated Information Flow SFP*** based on the following types of subject and information security attributes:

a) Source subject security attributes:
a. source network identifier;
b) Destination subject security attributes:
b. Set of destination subject identifiers;

Application Note: *The authorized administrator knows the set of identifiers that can be associated with the physical firewall interfaces; therefore, they are not "presumed" identifiers.*

.

c) Information security attributes:
c. ESSID,
d. Authentication type,
e. Encryption type,
f. AP Location,
g. identity of destination subject;
h. transport layer protocol;
i. destination subject service identifier (e.g., TCP destination port number);
d) Role-based attributes

j. MAC Address[28]
k. Physical location of AP/Radio[29]
l. Radius Group Name

Application Note: *The TOE also implements Role-based filtering, where a role is a group of authenticated wireless clients (AKA MU); role-based filtering refers to applying firewall policies to the wireless clients grouped in a role. Any traffic coming from the wireless client is subject to the firewall policies (access-lists) applied to its associated role.*

e) Stateful packet attributes:
a. Connection-oriented protocols:
i. sequence number;
ii. acknowledgement number;
iii. Flags:
- ***SYN;***
- ***ACK;***
- ***RST;***
- ***FIN;***

b. Connectionless protocols:
i. source and destination network identifiers;
***ii.* source and destination service identifiers;**

Application Note: *The stateful packet attributes are not specified in the ruleset as are the other security attributes. These attributes are intended to be used in FDP_IFF.1.3-NIAP-0417 (3) as part of the stateful packet inspection.*

FDP_IFF.1.2-NIAP-0417 (3) **Refinement:** The TSF shall permit an information flow between a source subject and a destination subject via a controlled operation if the following rules hold:

- ***the source subject has successfully authenticated to the TOE;***
- ***the identity of the destination subject is in the set of destination identifiers, and***
- ***the selected information flow policy rule specifies that the information flow is to be permitted via the authenticated proxy selected by the rule.***

FDP_IFF.1.3-NIAP-0417 (3) The TSF shall enforce the following:

- ***fragmentation rule:***
  - ***prior to applying the information policy ruleset, the TOE completely reassembles fragmented packets;***
- ***stateful packet inspection rules:***
  - ***whenever a packet is received that is not associated with an allowed established session (e.g., the SYN flag is set without the ACK flag being set), the information flow policy ruleset, as defined in FDP_IFF.1.2-NIAP-0417 (1), is applied to the packet;***
  - ***otherwise, the TSF associates a packet with an allowed established session using the stateful packet attributes***.

[28] A MAC address can be specified as a specific MAC or a mask. All clients having MAC matching the mask will be grouped into a role.
[29] Location refers to the physical location of the AP/radio that the wireless client is connected. This must be pre-configured on the AP

FDP_IFF.1.4-NIAP-0417 (3) The TSF shall provide the following ***the authorized administrator shall have the capability to view all information flows allowed by the information flow policy ruleset before the ruleset is applied***.

FDP_IFF.1.5-NIAP-0417 (3) The TSF shall explicitly authorize an information flow based on the following rules: ***none***.

FDP_IFF.1.6-NIAP-0417 (3) The TSF shall explicitly deny an information flow based on the following rules: ***none***.

6.1.3.5 FDP_RIP Residual information protection

6.1.3.5.1 FDP_RIP.1 (1) Subset residual information protection

FDP_RIP.1.1 (1) The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: network packet objects.

Application Note: *This requirement ensures that the TOE does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet.*

6.1.4 Class FIA: Identification and authentication

6.1.4.1 FIA_AFL Authentication failures

6.1.4.1.1 FIA_AFL.1 (1) Administrator authentication failure handling

FIA_AFL.1.1 (1) The TSF shall detect when an administrator configurable positive integer within the range of ***1 to 1024*** of unsuccessful authentication attempts occur related to remote administrators logging on to the WLAN access system.

FIA_AFL.1.2 (1) R**efinement:** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall prevent remote login on that logical interface by administrators until an action is taken by a local Administrator.

Application Note: *This requirement applies to remote administrator login and does not apply to SNMP users or the local login of the TOE, since it does not make sense to lock a local administrator's account in this fashion. For the purpose of this ST, remote administrator refers to administrators that do not have either Serial cable or local console access to the TOE.*

Application Note: *This requirement does NOT require that the TOE allow remote administration. However, if the TOE does allow administrators to login to the TOE remotely (e.g. from the wired interface or a management network) then it must provide a mechanism to prevent brute force attacks on the administrative account.*

ST Application Note: *Lockouts are applied per interface (GUI, SSH) and not per user. For example, if one user locks out the SSH interface after exceeding the allowed number of login attempts, the SSH interface is locked out for all users, until the interface lockout is removed.*

6.1.4.2 FIA_ATD User attribute definition

6.1.4.2.1 FIA_ATD.1 (1) Administrator attribute definition

FIA_ATD.1.1 (1) The TSF shall maintain the following minimum list of security attributes belonging to individual administrators: password, ***username, and role***.

6.1.4.2.2 FIA_ATD.1 (2) User attribute definition

FIA_ATD.1.1 (2) **Refinement:** The TSF shall maintain the following minimum list of security attributes belonging to individual remotely authenticated wireless users: ***username and password***.

6.1.4.3 FIA_UAU User authentication

6.1.4.3.1 FIA_UAU.1 (1) Timing of authentication (Administrative user)

FIA_UAU.1.1 (1) **Refinement:** The TSF shall allow ***ICMP, DHCP, ARP, the passing of authentication data to and from the remote authentication server, wired network traffic, TSF mediation in accordance with the Unauthenticated TOE Services SFP*** on behalf of the administrative user to be performed before the administrative user is authenticated.

Application Note: *Unauthenticated ICMP traffic to the TOE is allowed to support a commonly used service. An authorized administrator may disable this service*

When an ARP (Address Resolution Protocol) request packet is received from a user, the access point forwards it over all enabled interfaces except over the interface the ARP request packet was received .On receiving the ARP response packet, the access point database keeps a record of the destination address along with the receiving interface. With this information, the access point forwards any directed packet to the correct destination.

The TOE may also be used as a wired network switch, passing and filtering traffic between its LAN ports.

FIA_UAU.1.2 (1) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3.2 FIA_UAU.1 (2) Timing of authentication (Wireless user)

FIA_UAU.1.1 (2) **Refinement:** The TSF shall allow ***the passing of authentication data to and from the remote authentication server, TSF mediation in accordance with the Traffic Filter SFP*** on behalf of the wireless user to be performed before the wireless user is authenticated.

FIA_UAU.1.2 (2) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3.3 FIA_UAU_(EXT).5 Extended: multiple authentication mechanisms

FIA_UAU_(EXT).5.1 **Refinement** The TSF shall provide local authentication, and a remote authentication mechanism to perform user authentication. The TSF shall provide the following local authentication mechanisms

1. local password-based authentication of local administrators connected via RS-232,
2. local password-based authentication of remote administrators connected via SSH,
3. local password-based authentication of remote administrators connected via HTTPS,
4. local username and password-based authentication of remote administrators using SNMPv3.
5. local 802.1x EAP authentication using
    a. EAP-TLS,
    b. EAP-TTLS (MD5, PAP and MSCHAP-V2), or

c. EAP-PEAP (GTC and MSCHAP-V2)

to perform wireless user authentication using local user database,

6. local 802.1x EAP authentication using
   a. EAP-TTLS (PAP), or
   b. EAP-PEAP (GTC)

to perform wireless user authentication using a remote LDAP user database.

The TSF shall provide the client to facilitate remote authentication via the following authentication protocols:

1. RADIUS that complies with RFCs 2138, 3579, and 3580

FIA_UAU_(EXT).5.2 The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

.

Application Note: *This extended requirement is needed for local administrators because there is disagreement over whether existing CC requirements specifically require the TSF provide authentication. That the TOE provide authentication is implied by other FIA_UAU requirements, and generally assumed to be a requirement when other FIA_UAU requirements are included in a TOE. In order to remove any potential confusion about this ST, an extended requirement for authentication has been included. This ST mandates that the TOE provide the client to facilitate remote authentication via an authentication server. The IT environment will provide the authentication server, and it is important to specify that the TSF must provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server.*

Since FIA_UAU.5.1 and 5.2 require that the TSF provide authentication mechanisms, this extended requirement is needed with respect to the remote users to specify that the TSF invoke a remote authentication mechanism rather than provide it.

6.1.4.4 FIA_UID User identification

6.1.4.4.1 FIA_UID.2 User identification before any action

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

6.1.4.5 FIA_USB User-subject binding

6.1.4.5.1 FIA_USB.1 User-subject binding

FIA_USB.1.1 **Refinement:** The TSF shall associate the following administrative user security attributes with subjects acting on the behalf of that user: ***username, role***.

FIA_USB.1.2 **Refinement:** The TSF shall enforce the following rules on the initial association of an administrative user security attributes with subjects acting on the behalf of users: ***upon successful identification and authentication, the username shall be that of the user that has authenticated successfully***.

FIA_USB.1.3 **Refinement:** The TSF shall enforce the following rules governing changes to the administrative user security attributes associated with subjects acting on the behalf of users: ***no changes shall be allowed.***

6.1.5 Class FID: Intrusion detection

6.1.5.1 FID_APD_EXT.1 Rogue Access Point Detection

FID_APD_EXT.1.1 The TSF shall be able to detect a Rogue Access Point operating within the radio coverage area of an 802.11 wireless network using the following detection methods:

- ***detection of AP broadcasting a vendor default SSID***
- ***detection of AP broadcasting SSID in beacon***
- ***excessive traffic from AP***
- ***AP transmitting at suspiciously high power level***
- ***an unauthorized AP (not in whitelist) broadcasting on authorized SSID***

FID_APD_EXT.1.2 Upon detection of a Rogue Access Point, the TSF shall take the following actions:

- ***Notify the administrative user with a SNMP trap***
- ***Generate a syslog message***
- ***Add to the list of detected Rogue APs accessible by the administrative user via the CLI and/or Web UI***

6.1.6 Class FMT: Security management

6.1.6.1 FMT_MOF Management of functions in TSF

6.1.6.1.1 FMT_MOF.1 (1) Management of cryptographic security functions behavior

FMT_MOF.1.1 (1) **Refinement:** The TSF shall restrict the ability to ***modify the behavior of*** the cryptographic functions

- ***Crypto: load a key***
- ***Crypto: delete/zeroize a key***
- ***Crypto: set a key lifetime***
- ***Crypto: set the cryptographic algorithm mode and key size***
- ***Crypto: execute self tests of TOE hardware and the cryptographic functions***

to ***Superuser and Crypto-Officer. The sysadmin role can also load a key***.

6.1.6.1.2 FMT_MOF.1 (2) Management of audit security functions behavior

FMT_MOF.1.1 (2) **Refinement:** The TSF shall restrict the ability to enable, disable, and modify the behavior of the functions

- Audit: pre-selection of the events which trigger an audit record,
- Audit: start and stop of the audit function

to Superuser, System Administrator, and Read/Write SNMP administrator

6.1.6.1.3 FMT_MOF.1 (3) Management of authentication security functions behavior

FMT_MOF.1.1 (3) **Refinement:** The TSF shall restrict the ability to modify the behavior of the Authentication functions

- Auth: allow or disallow the use of an authentication server to Superuser, sysadmin, and Read/Write SNMP administrator.

- Auth: set the number of authentication failures that must occur before the TOE takes action to disallow future logins to Superuser and Read/Write SNMP administrator
- Auth: set the length of time a session may remain inactive before it is terminated to Superuser, sysadmin, and Read/Write SNMP administrator.

6.1.6.1.4 FMT_MOF.1 (4) Management of Firewall security functions behavior

FMT_MOF.1.1 (4) The TSF shall restrict the ability **to enable, disable, and modify the behavior** of the functions

- ***Enable and disable individual firewall features***
  - ***Denial of Service Filters***
  - ***Layer 2 Filters***
  - ***Layer 3 Filters***
  - ***WLAN Filters***
  - ***Role-Based Filters***
- ***Enable and disable pre-configured filters***
- ***Create, change, and delete firewall rules***

to ***Superuser, Crypto-officer (cannot delete any filters, and cannot affect Role-based filters), and Read/Write SNMP administrator.***

6.1.6.1.5 FMT_MOF.1 (5) Management of Intrusion Detection security functions behavior

FMT_MOF.1.1 (5) The TSF shall restrict the ability **to enable, disable, and modify the behavior** of the functions

- ***Rogue AP Detection Method***
- ***Rogue AP white listing***
- ***Display Rogue AP Details***

to ***Superuser, Crypto-officer, and Read/Write SNMP administrator.***

6.1.6.2 FMT_MSA Management of security attributes

6.1.6.2.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***Role-Based Access Control SFP*** to restrict the ability to **query, modify, delete** the security attributes ***username, password, allowed interfaces, and role*** to ***Superuser***.

6.1.6.2.2 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

6.1.6.2.3 FMT_MSA.3 (1) Static attribute initialization (*Role-Based Access Control SFP*)

FMT_MSA.3.1 (1) The TSF shall enforce the ***Role-Based Access Control SFP*** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (1) The TSF shall allow the ***no user*** to specify alternative initial values to override the default values when an object or information is created.

6.1.6.2.4 FMT_MSA.3 (2) Static attribute initialization (*Traffic Filter SFP)*

FMT_MSA.3.1 (2) **Refinement:** The TSF shall enforce the ***Traffic Filter SFP*** to provide **permissive** default values for traffic filter information flow security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (2) The TSF shall allow ***no user*** to specify alternative initial values to override the default values when an object or information is created.

6.1.6.2.5 FMT_MSA.3 (3) Static attribute initialization (*Unauthenticated TOE Services SFP*)

FMT_MSA.3.1 (3) **Refinement:** The TSF shall enforce the ***Unauthenticated TOE Services SFP*** to provide **permissive** default values for the unauthenticated TOE services information flow policy ruleset that is used to enforce the SFP.

Application Note: *"restrictive" in this case means that by default information is not allowed to flow (according to the referenced policies) unless an explicit rule in the information flow policy ruleset allows an information flow. By default, information is not allowed to flow.*

FMT_MSA.3.2 (3) The TSF shall allow ***no user*** to specify alternative initial values to override the default values when an object or information is created.

6.1.6.2.6 FMT_MSA.3 (4) Static attribute initialization (Authenticated Information Flow SFP)

FMT_MSA.3.1 (4) **Refinement:** The TSF shall enforce the ***Authenticated Information Flow SFP*** to provide **permissive** default values for the authenticated information flow policy ruleset that is used to enforce the SFP.

FMT_MSA.3.2 (4) The TSF shall allow ***no user*** to specify alternative initial values to override the default values when an object or information is created.

6.1.6.3 FMT_MTD Management of TSF data

6.1.6.3.1 FMT_MTD.1 (1) Management of Audit pre-selection data

FMT_MTD.1.1 (1) The TSF shall restrict the ability to **query, modify, clear, create** the ***set of rules used to pre-select audit events*** to ***monitor (query only), superuser, sysadmin, Read/Write SNMP administrator, and Read Only SNMP administrator (query only).***

6.1.6.3.2 FMT_MTD.1 (2) Management of TSF Data (Administrative user authentication)

FMT_MTD.1.1 (2) The TSF shall restrict the ability to **query, modify, delete, clear, *create*** the ***Administrative user authentication credentials*** to ***superuser***.

6.1.6.3.3 FMT_MTD.1 (3) Management of TSF data (Wireless user authentication)

FMT_MTD.1.1 (3) The TSF shall restrict the ability to **modify, delete** the ***wireless user authentication credentials*** to ***superuser***.

6.1.6.4 FMT_SMF Specification of Management Functions

6.1.6.4.1 FMT_SMF.1 (1) Specification of management functions (cryptographic function)

FMT_SMF.1.1 (1) **Refinement:** The TSF shall be capable of performing the following security management functions: configure administrator authentication, query and set the encryption/decryption of network packets (via FCS_COP.1(1)) in conformance with the administrators configuration of the TOE.

6.1.6.4.2 FMT_SMF.1 (2) Specification of management functions (TOE audit record generation)

FMT_SMF.1.1 (2) The TSF shall be capable of performing the following security management functions: query, enable or disable Security Audit.

Application Note: *This requirement ensures that those responsible for TOE administration are able to start or stop the TOE generation of audit records*

6.1.6.4.3 FMT_SMF.1 (3) Specification of management functions (cryptographic key data)

FMT_SMF.1.1 (3) [30] **Refinement**[31]**:** The TSF shall be capable of performing the following security management functions: query, set, modify, and delete the cryptographic keys and key data ~~in support of FDP_PUD_(EXT).~~

Application Note: *The intent of this requirement is to provide the ability to configure the TOE's cryptographic key(s). Configuring the key data may include: setting key lifetimes, setting key length, etc.*

6.1.6.4.4 FMT_SMF.1 (4) Specification of management functions (Firewall)

FMT_SMF.1.1 (4) The TSF shall be capable of performing the following security management functions: ***enable and disable individual firewall features, and configure firewall rules and settings***.

Application Note: *This requirement ensures that those responsible for TOE administration are able to manage firewall configuration*

6.1.6.4.5 FMT_SMF.1 (5) Specification of management functions (Intrusion Detection)

FMT_SMF.1.1 (5) The TSF shall be capable of performing the following security management functions: ***enable, disable, and configure intrusion detection settings***.

6.1.6.5 FMT_SMR Security management roles

6.1.6.5.1 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- ***Crypto-Officer (aka Nwadmin),***
- ***Monitor,***
- ***System Administrator,***
- ***Web Administrator,***
- ***Superuser,***
- ***Read-only SNMP administrator***
- ***Read/Write SNMP administrator, and***
- ***Wireless user.***

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

Application Note: *The only user allowed direct access to the TOE are those users assigned the roles Crypto-Officer, Monitor, System Administrator, Web Administrator, Superuser, SNMP administrator. Wireless users can pass data through the TOE but do not have direct access. A role of wireless user is included in the TOE, but the scope of that role should be defined only to the extent necessary to support the activities of wireless users passing data through the TOE.*

This ST also assumes that the TOE will contain a local authentication mechanism and the capability to use a remote authentication server. Although users are sometimes referred to as local or remote, these references do not imply a role.

[30] Modified to delete the phrase "and enable/disable verification of cryptographic key testing", per NIAP PD-0145: Enabling/Disabling of Verification of Cryptographic Key Testing in WLAN PP

[31] FDP_PUD_(EXT) is not included in this ST as it relates to actually performing encryption/decryption of wireless user traffic, which is completely handled in the 7131 portion of the TOE and is addressed in that ST. FMT_SMF.1(3) in the context of the RFS7000 addresses management of keys used within the RFS7000 itself.

6.1.7 Class FPT: Protection of the TSF

6.1.7.1 FPT_ITT Internal TOE TSF data transfer

6.1.7.1.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from **disclosure and modification** when it is transmitted between separate parts of the TOE.

6.1.7.2 FPT_STM Time stamps

6.1.7.2.1 FPT_STM_EXT.1 Reliable time stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps, synchronized via an external time source, for its own use.

Application Note: *The TOE must be capable of obtaining a time stamp via an NTP server.*

6.1.7.3 FPT_TST TSF self test

6.1.7.3.1 FPT_TST_EXT.1 Extended: TSF testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

6.1.7.3.2 FPT_TST.1(1) TSF testing(for cryptography)

FPT_TST.1.1 (1) **Refinement:** The TSF shall run a suite of self-tests in accordance with FIPS PUB 140-2 during initial start-up (on power on), at the request of the cryptographic administrator (on demand), under various conditions defined in section 4.9.1 of FIPS 140-2, and periodically (at least once a day) to demonstrate the correct operation of the following cryptographic functions

- key error detection;
- cryptographic algorithms;
- RNG/PRNG

Application Note: These tests apply regardless of whether the cryptographic functionality is implemented in hardware, software, or firmware.

FPT_TST.1.2 (1) **Refinement:** The TSF shall provide authorized ~~users~~ cryptographic administrators with the capability to verify the integrity of **TSF data** related to the cryptography by using TSF-provided cryptographic functions.

Application Note: *Refer to FCS_COP.1.1 (2) and FCS_COP.1.1 (3) for TSF-provided cryptographic services*

FPT_TST.1.3(1) **Refinement:** The TSF shall provide authorized ~~users~~ cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the cryptography by using TSF-provided cryptographic functions.

Application Note: *Refer to FCS_COP.1.1 (2) and FCS_COP.1.1 (3) for TSF-provided cryptographic services.*

6.1.7.3.3 FPT_TST.1(2) TSF testing (for key generation components)

FPT_TST.1.1(2) **Refinement:** The TSF shall perform self tests immediately after generation of a key to demonstrate the correct operation of each key generation component. If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited.

Application Note: *Key generation components are those critical elements that compose the entire key generation process (e.g., any algorithms, any RNG/PRNGs, any key generation seeding processes, etc.).*

Application Note: *These self-tests on the key generation components can be executed here as a subset of the full suite of self-tests run on the cryptography in FPT_TST.1 (1) as long as all elements of the key generation process are tested.*

FPT_TST.1.2(2) **Refinement:** The TSF shall provide authorized ~~users~~ cryptographic administrators with the capability to verify the integrity of **TSF data** related to the key generation by using TSF-provided cryptographic functions.

Application Note: *Refer to FCS_COP.1.1 (2) and FCS_COP.1.1 (3) for TSF-provided cryptographic services*

FPT_TST.1.3(2) **Refinement:** The TSF shall provide authorized ~~users~~ cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the key generation by using TSF-provided cryptographic functions.

Application Note: *Refer to FCS_COP.1.1 (2) and FCS_COP.1.1 (3) for TSF-provided cryptographic services.*

6.1.8 Class FTA: TOE access

6.1.8.1 FTA_SSL Session locking and termination

6.1.8.1.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate a local interactive or wireless session after an administrator configurable time interval of user inactivity.

Application Note: *This requirement applies to both local administrative sessions and wireless users that pass data through the TOE.*

6.1.8.2 FTA_TAB TOE access banners

6.1.8.2.1 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.1.9 Class FTP: Trusted path/channels

6.1.9.1 FTP_ITC Inter-TSF trusted channel

6.1.9.1.1 FTP_ITC_EXT.1 Inter-TSF trusted channel

FTP_ITC_EXT.1.1 The TOE shall provide an encrypted communication channel between itself and entities in the TOE IT Environment that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_EXT.1.2 The TSF shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.

FTP_ITC_EXT.1.3	The TSF shall initiate communication via the trusted channel for all authentication functions, remote logging, time, ***configuration file import and export***.
Application Note:	*If a certificate authority server plays a role in the authentication of users, then the CA is considered an authorized IT entity and the TSF is expected to initiate secure communications with this entity. It is assumed that the IT environment includes an NTP server, an audit server and/or an authentication server.*

6.2 Security Assurance Requirements for the TOE

This Security Target is Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 as shown in Table 13 – Assurance Requirements below. The security assurance requirements for the TOE consist of the following components that are CC Part 3 conformant as summarized in Table 13 below and detailed in the following subsections. These requirements are included by reference.

Table 13 – Assurance Requirements		
Assurance Class	Assurance Component	Assurance Components Description
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life-cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2[32]	Flaw Reporting Procedures
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Analysis of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

[32] ALC_FLR.2 is an augmentation over EAL-2

6.3 Security Requirements Rationale

6.3.1 Security Function Requirements Rationale

Table 14 - TOE SFR/SAR to Objective Mapping satisfies the requirement to trace each SFR back to the security objectives for the TOE.

Table 14 - TOE SFR/SAR to Objective Mapping																			
	TOE Objective																		
	SFR/SAR	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_DENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_ DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ ANALYSIS	O.ROGUE_AP_DETECTION
1	FAU_GEN.1(1)		X															
2	FAU_GEN.2		X															
3	FAU_SEL.1		X															
4	FCS_BCM_(EXT).1					X	X											
5	FCS_CKM.1(1)					X	X											
6	FCS_CKM.1(2)					X	X											
7	FCS_CKM.2					X	X											
8	FCS_CKM_(EXT).2					X	X						X					
9	FCS_CKM.4					X	X						X					
10	FCS_COP.1(1)					X	X											
11	FCS_COP.1(2)					X	X											
12	FCS_COP.1(3)					X	X											
13	FCS_COP.1(4)					X	X											
14	FCS_COP_(EXT).1					X	X											
15	FCS_COMM_PROT_EXT.1					X												
16	FCS_EAP-TLS_EXT.1					X												
17	FCS_EAP-TTLS_EXT.1					X												
18	FCS_HTTPS_EXT.1					X												
19	FCS_IPSEC_EXT.1					X												
20	FCS_PEAP_EXT.1					X												
21	FCS_RAD_EXT.1					X												
22	FCS_SFTP_EXT.1					X												
23	FCS_SNMPv3_EXT.1					X												
24	FCS_SSH_EXT.1					X												
25	FCS_TLS_EXT.1					X												
26	FDP_ACC.1									X								
27	FDP_ACF.1									X								
28	FDP_IFC.1(1)										X							
29	FDP_IFC.1(2)										X							
30	FDP_IFC.1(3)										X							
31	FDP_IFF.1-NIAP-0407 (1)										X							

Table 14 - TOE SFR/SAR to Objective Mapping																			
	TOE Objective																		
	SFR/SAR	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_DENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_ DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ ANALYSIS	O.ROGUE_AP_DETECTION
32	FDP_IFF.1-NIAP-0407 (2)										X							
33	FDP_IFF.1-NIAP-0407 (3)										X							
34	FDP_RIP.1												X					
35	FIA_AFL.1															X		
36	FIA_ATD.1(1)															X		
37	FIA_ATD.1(2)															X		
38	FIA_UAU.1 (1)										X					X		
39	FIA_UAU.1 (2)										X					X		
40	FIA_UAU_(EXT).5										X					X		
41	FIA_UID.2										X					X		
42	FIA_USB.1		X															
43	FID_APD_EXT.1																	X
44	FMT_MOF.1(1)									X								
45	FMT_MOF.1(2)									X								
46	FMT_MOF.1(3)									X								
47	FMT_MOF.1(4)									X								
48	FMT_MOF.1(5)									X								
49	FMT_MSA.1									X								
50	FMT_MSA.2									X								
51	FMT_MSA.3 (1)									X								
52	FMT_MSA.3 (2)									X								
53	FMT_MSA.3 (3)									X								
54	FMT_MSA.3 (4)									X								
55	FMT_MTD.1 (1)									X								
56	FMT_MTD.1 (2)									X								
57	FMT_MTD.1 (3)									X								
58	FMT_SMF.1 (1)									X								
59	FMT_SMF.1 (2)									X								
60	FMT_SMF.1 (3)									X								
61	FMT_SMF.1 (4)									X								
62	FMT_SMF.1 (5)									X								
63	FMT_SMR.1 (1)									X								
64	FPT_ITT.1															X		
65	FPT_STM_(EXT).1		X												X			
66	FPT_TST_EXT.1				X													
67	FPT_TST.1 (1)				X													
68	FPT_TST.1 (2)				X													
69	FTA_SSL.3															X		
70	FTA_TAB.1							X										
71	FTP_ITC_EXT.1		X													X		

Table 14 - TOE SFR/SAR to Objective Mapping																		
	TOE Objective																	
	SFR/SAR	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_DENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_ DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ ANALYSIS	O.ROGUE_AP_DETECTION
	ADV_ARC.1													X				
	ADV_FSP.2								X									
	ADV_TDS.1								X									
	AGD_OPE.1	X																
	AGD_PRE.1	X																
	ALC_CMC.2			X														
	ALC_CMS.2			X														
	ALC_DEL.1	X																
	ALC_FLR.2			X														
	ATE_COV.1											X						
	ATE_FUN.1											X						
	ATE_IND.2											X						
	AVA_VAN.2																X	

6.3.1.1 Security Function Requirements Rationale

The following paragraphs present the rationale that demonstrates that the SFRs meet all security objectives for the TOE.

O.ADMIN_GUIDANCE

ALC_DEL.1 ensures that the administrator has the ability to begin their TOE installation with a *clean* (e.g., malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE

The AGD_PRE.1 requirement ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The Installation, Generation and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration.

The AGD_OPE.1 requirement mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a description of how to set up and use the auditing features of the TOE.

AGD_OPE.1 AND AGD_PRE.1 analysis during evaluation will ensure that the guidance documentation can be followed unambiguously to ensure the TOE is not misconfigured in an insecure state due to confusing guidance.

O.AUDIT_GENERATION

FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this ST.

FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.

FAU_SEL.1 allows for the selection of events to be audited. This requires that the criteria used for the selection of auditable events to be defined. For example, the user identity can be used as selection criterion for the events to be audited.

FIA_USB.1 plays a role in satisfying this objective by requiring a binding of security attributes associated with users that are authenticated with the subjects that represent them in the TOE. This only applies to authorized users, since the identity of unauthenticated users cannot be confirmed. Therefore, the audit trail may not always have the proper identity of the subject that causes an audit record to be generated (e.g., presumed network address of an unauthenticated user may be a spoofed address).

FPT_STM_(EXT).1 supports the audit functionality by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events.
FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE IT environment (the audit server and the time server).

O.CONFIGURATION_ IDENTIFICATION

ALC_CMC.2 contributes to this objective by requiring the developer have a configuration management plan that describes how changes to the TOE and its evaluation deliverables are managed.

ALC_CMS.2 is necessary to define the items that must be under the control of the CM system. This requirement ensures that the TOE implementation representation, design documentation, test documentation (including the executable test suite), user and administrator guidance, and CM documentation are tracked by the CM system.

ALC_FLR.2 plays a role in satisfying this objective by requiring the developer to have procedures that address flaws that have been discovered in the product, either through developer actions (e.g., developer testing) or discovery by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis to ensure new flaws are not created while fixing the discovered flaws.

O.CORRECT_ TSF_OPERATION

FPT_TST_(EXT).1 is necessary to ensure the correctness of the TSF software and TSF data. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce

its security policies. The FPT_TST.1(1) for crypto and FPT_TST.1(2) for key generation functional requirement has been included to address the critical nature and specific handling of the cryptographic related TSF data. Since the cryptographic TSF data has specific FIPS PUB requirements associated with them it is important to ensure that any fielded testing on the integrity of these data maintains the same level of scrutiny as specified in the FCS functional requirements.

O.CRYPTOGRAPHY

Baseline cryptographic services are provided in the TOE by NIST CAVP compliant algoritms implemented in hardware, in software, or in hardware/software combinations [FCS_BCM_(EXT).1].

Contributing to this objective, the requirements for each of the cryptographic communications protocols are more exactly specified with the following:

- FCS_COMM_PROT_EXT.1 , Communications Protection
- FCS_EAP-TLS_EXT.1 , EAP-TLS Authentication Protocol
- FCS_EAP-TTLS_EXT.1 , EAP-TLS Authentication Protocol
- FCS_HTTPS_EXT.1 , HTTPS
- FCS_IPSEC_EXT.1 , Internet Protocol Security (IPsec)
- FCS_PEAP_EXT.1 , PEAP Authentication Protocol
- FCS_RAD_EXT.1 , RADIUS Authentication Protocol
- FCS_SFTP_EXT.1 , SSH File Transfer Protocol
- FCS_SNMPv3_EXT.1, SNMPv3
- FCS_SSH_EXT.1 , SSH
- FCS_TLS_EXT.1 , TLS

The cryptographic services offered by this baseline capability are augmented and customized in the TOE to support medium robustness environments. These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys [FCS_CKM.1 (1)], and the generation of asymmetric keys [FCS_CKM.1 (2)]; methods of manual and automated cryptographic key distribution [FCS_CKM.2]; cryptographic key destruction [FCS_CKM.4]; techniques for cryptographic key validation and packaging [FCS_CKM.1]; and cryptographic key handling and storage [FCS_CKM_(EXT).2]. Specific functional requirements in the area of cryptographic operations address data encryption and decryption [FCS_COP.1 (1)]; cryptographic signatures [FCS_COP.1 (2)]; cryptographic hashing [FCS_COP.1 (3)]; cryptographic key agreement [FCS_COP.1 (4)]; and improved random number generation [FCS_COP_(EXT).1].

O.CRYPTOGRAPHY_VALIDATED

Baseline cryptographic services are provided in the TOE by NIST CAVP compliant algorithms implemented in hardware, in software, or in hardware/software combinations [FCS_BCM_(EXT).1]. The cryptographic services offered by this baseline capability are augmented and customized in the TOE to support medium robustness environments. These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys [FCS_CKM.1 (1)], and the generation of asymmetric keys [FCS_CKM.1 (2)]; methods of manual and automated cryptographic key distribution [FCS_CKM.2]; cryptographic key destruction [FCS_CKM.4]; techniques for cryptographic key validation and packaging [FCS_CKM.1]; and cryptographic key handling and storage [FCS_CKM_(EXT).2]. Specific functional requirements in the area of cryptographic operations address data encryption and decryption [FCS_COP.1 (1)]; cryptographic signatures [FCS_COP.1 (2)]; cryptographic hashing [FCS_COP.1 (3)]; cryptographic key agreement [FCS_COP.1 (4)]; and improved random number generation [FCS_COP_(EXT).1].

O.DISPLAY_BANNER

FTA_TAB.1 meets this objective by requiring that the TOE display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the administrator, who can specify any warnings regarding unauthorized use of the TOE and remove any

product or version information if they desire. The only time that it is envisioned that an authenticated session would need to be established is for the performance of TOE administration. Bannering is not necessary prior to use of services that pass network traffic through the TOE.

O.DOCUMENTED_DESIGN

ADV_FSP.2 and ADV_TDS.1 support this objective by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered.

ADV_TDS.1 and ADV_FSP.2 are also used to ensure that the TOE design is consistent across the Design and the Functional Specification.

O.MANAGE

The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirements' rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions.

FMT_MOF.1 (1), (2), (3), (4) and (5) ensure that the administrator has the ability manage the cryptographic, audit, authentication, firewall, and Intrusion detection functions.

FMT_MSA.1 provides that only the Crypto-officer and Superuser have the ability to modify security attributes for the firewall.

FMT_MSA.2 provides the administrator the ability to accept only secure values and modify security attributes.

FMT_MSA.3 (1), (2), (3) and (4) ensures the TSF enforce the SFP to provide restrictive initial default values, and provides the administrator the ability to override the default values.

FMT_MTD.1 (1), (2), and (3) ensure that the administrator can manage TSF data.

FMT_SMR.1 defines the specific security roles to be supported.

FMT_SMF.1 (1), (2), (3), (4) and (5) support this objective by identifying the management functions for cryptographic data, audit records, cryptographic key data, firewall settings, and Intrusion detection settings.

FDP_ACC.1 and FDP_ACF.1 support this objective by providing role-based access controls that allows clear differentiation of management duties.

O.MEDIATE

FIA_UAU.1 (1), (2), (3), FIA_UAU_(EXT).5 and FIA_UID.2 support the TOE's ability to mediate packet flow based upon the authentication credentials of the wireless user. Additionally, FDP_IFC.1 (1) and FDP_IFF.1-NIAP-0407 (1) ensure the TOE has the ability to mediate the flow of data subject to the Traffic Filter SFP; FDP_IFC.1 (2) and FDP_IFF.1-NIAP-0407 (2) ensure the TOE has the ability to mediate the flow of data from unauthenticated users accessing TOE services; FDP_IFC.1 (3) and FDP_IFF.1-NIAP-0407 (3) ensure the TOE has the ability to mediate the flow of data subject to the Authenticated Information Flow SFP.

O.PARTIAL_FUNCTIONAL_TESTING

ATE_FUN.1 requires the developer to provide the necessary test documentation to allow for an independent analysis of the developer's security functional test coverage. In addition, the developer must provide the test suite executables and source code, which the evaluator uses to independently verify the vendor test results and to support of the test coverage analysis activities.

ATE_COV.1 requires the developer to provide a test coverage analysis that demonstrates the extent to which the TSFI are tested by the developer's test suite. This component also requires an independent confirmation of the extent of the test suite, which aids in ensuring that correct security relevant functionality of a TSFI is demonstrated through the testing effort.

ATE_IND.2 requires an independent confirmation of the developer's test results by mandating that a subset of the test suite be run by an independent party. This component also requires an independent party to craft additional functional tests that address functional behavior that is not demonstrated in the developer's test suite. Upon successful completion of these requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.

O.RESIDUAL_ INFORMATION

FDP_RIP.1 is used to ensure the contents of resources are not available once the resource is reallocated. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data).

FCS_CKM_(EXT).2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.1, in that when a cryptographic key is moved from one location to another (e.g., calculated in some scratch memory and moved to a permanent location) that the memory area is immediately cleared as opposed to waiting until the memory is reallocated to another subject.

FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to a user.

O.SELF_PROTECTION

ADV_ARC.1 provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs. Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation.

O.TIME_STAMPS

FPT_STM_(EXT).1 requires that the TOE be able to obtain reliable time stamps for its own use and therefore, partially satisfies this objective. Time stamps include date and time, and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.

O.TOE_ACCESS

FIA_UID.2 plays a role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions. In most cases, the identification cannot be authenticated (e.g., a user attempting to send a data packet through the TOE that does not require authentication. It is impractical to require authentication of all users that attempt to send data through the TOE, therefore, the requirements specified in the TOE require authentication where it is deemed necessary. This

does impose some risk that a data packet was sent from an identity other than that specified in the data packet.

FIA_UAU.1 (1), and FIA_UAU_(EXT).5 contribute to this objective by ensuring that administrators and users are authenticated before they are provided access to the TOE or its services except for those specifically specified.

In order to control logical access to the TOE an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable).

FIA_AFL.1 ensures that the TOE can protect itself and its users from brute force attacks on their authentication credentials.

FIA_ATD.1 (1) and (2) Management requirements provide additional control to supplement the authentication requirements.

FTA_SSL.3 ensures that inactive user and administrative sessions are dropped.
FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE IT environment (the remote authentication server)
FPT_ITT.1 protects data being transferred between different parts of the TOE from modification and disclosure; this is necessary to protect access to the TOE.

O.VULNERABILITY_ ANALYSIS

The AVA_VAN.2 component provides the necessary level of confidence that vulnerabilities do not exist in the TOE that could cause the security policies to be violated. AVA_VAN.2 requires the evaluator to perform a search for potential vulnerabilities in all the TOE deliverables. For those vulnerabilities that are not eliminated by the developer, a rationale must be provided that describes why these vulnerabilities cannot be exploited by a threat agent with a basic attack potential, which is in keeping with the desired assurance level of this TOE. This component provides the confidence that security flaws do not exist in the TOE that could be exploited by a threat agent of basic attack potential to violate the TOE's security policies. For this TOE, the vulnerability analysis is specified for an attack potential of basic.

This requirement ensures the evaluator has performed an analysis of the authentication mechanism to ensure the probability of guessing a user's authentication data would require a medium-attack potential, as defined in Annex B of the CEM.

O.ROGUE_AP_DETECTION

FID_APD_EXT.1 ensures the TSF can detect Rogue APs operating within the radio coverage area of an 802.11 wireless network, and generate the appropriate messages to notify the administrator.

6.3.1.2 Security requirement dependency analysis

Table 15 - SFR Component Dependency Mapping maps the dependencies that exist for each SFR. If the column labeled “satisfied” shows a dependency that has not been resolved, the rationale is provided in the text following the table, why this dependency does not apply for the TOE.

Table 15 - SFR Component Dependency Mapping			
#	Component	Dependencies	Satisfied [Component #]
1	FAU_GEN.1	FPT_STM.1	FPT_STM_(EXT).1
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
3	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	FAU_GEN.1 FMT_MTD.1 (1)
4	FCS_BCM_(EXT).1	None	None
5	FCS_CKM.1 (1)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP_(EXT).1 FCS_CKM.4 FMT_MSA.2
6	FCS_CKM.1 (2)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP_(EXT).1 FCS_CKM.4 FMT_MSA.2
7	FCS_CKM.2	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2	FCS_CKM.1 (1), (2) FMT_MSA.2
8	FCS_CKM_(EXT).2	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2	FCS_CKM.1 (1), (2) FMT_MSA.2
9	FCS_CKM.4	[FTP_ITC.1 or FCS_CKM.1] FMT_MSA.2	FCS_CKM.1 (1), (2) FMT_MSA.2
10	FCS_COP.1 (1)	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 (1) FCS_CKM.4 FMT_MSA.2
11	FCS_COP.1 (2)	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 (2) FCS_CKM.4 FMT_MSA.2
12	FCS_COP.1 (3)	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	No FCS_CKM.4 FMT_MSA.2
13	FCS_COP.1 (4)	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 (2) FCS_CKM.4 FMT_MSA.2
14	FCS_COP_(EXT).1	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	No FCS_CKM.4 FMT_MSA.2
15	FCS_COMM_PROT_EXT.1	None	None
16	FCS_HTTPS_EXT.1	None	None
17	FCS_SFTP_EXT.1	FCS_SSH_EXT.1	FCS_SSH_EXT.1
18	FCS_SNMPv3_EXT.1	None	None
19	FCS_SSH_EXT.1	None	None
20	FCS_TLS_EXT.1	None	None
21	FCS_IPSEC_EXT.1	None	None
22	FCS_EAP-TLS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1
23	FCS_EAP-TTLS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1
24	FCS_PEAP_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1
25	FCS_RAD_EXT.1	FCS_IPSEC_EXT.1	FCS_IPSEC_EXT.1
26	FDP_ACC.1	None	FDP_ACF.1
27	FDP_ACF.1	None	FDP_ACC.1 FMT_MSA.3 (1)
28	FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1-NIAP-0407 (1)
29	FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.1-NIAP-0407 (2)

Table 15 - SFR Component Dependency Mapping			
#	Component	Dependencies	Satisfied [Component #]
30	FDP_IFC.1(3)	FDP_IFF.1	FDP_IFF.1-NIAP-0407 (3)
31	FDP_IFF.1-NIAP-0407 (1)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 (1) FMT_MSA.3 (2)
32	FDP_IFF.1-NIAP-0407 (2)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 (2) FMT_MSA.3 (3)
33	FDP_IFF.1-NIAP-0407 (3)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 (3) FMT_MSA.3 (4)
34	FDP_RIP.1	None	None
35	FIA_AFL.1	FIA_UAU.1	FIA_UAU.1 (1)
36	FIA_ATD.1 (1)	None	None
37	FIA_ATD.1 (2)	None	None
38	FIA_UAU.1 (1)	FIA_UID.1	FIA_UID.2
39	FIA_UAU.1 (2)	FIA_UID.1	FIA_UID.2
40	FIA_UAU_(EXT).5	None	None
41	FIA_UID.2	None	None
42	FIA_USB.1	FIA_ATD.1	FIA_ATD.1 (1), (2)
43	FID_APD_EXT.1	None	None
44	FMT_MOF.1 (1)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 (1) FMT_SMR.1
45	FMT_MOF.1 (2)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 (2) FMT_SMR.1
46	FMT_MOF.1 (3)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 (3) FMT_SMR.1
47	FMT_MOF.1 (4)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 (4) FMT_SMR.1
48	FMT_MOF.1 (5)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 (5) FMT_SMR.1
49	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1 (4)
50	FMT_MSA.2[33]	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_IFC.1 FMT_MSA.1 FMT_SMR.1
51	FMT_MSA.3 (1)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 (1) FMT_SMR.1
52	FMT_MSA.3 (2)	FMT_MSA.1 FMT_SMR.1	No FMT_SMR.1
53	FMT_MSA.3 (3)	FMT_MSA.1 FMT_SMR.1	No FMT_SMR.1
54	FMT_MSA.3 (4)	FMT_MSA.1 FMT_SMR.1	No FMT_SMR.1
55	FMT_MTD.1(1)	FMT_SMR.1	FMT_SMR.1
56	FMT_MTD.1 (2)	FMT_SMR.1	FMT_SMR.1
57	FMT_MTD.1 (3)	FMT_SMR.1	FMT_SMR.1
58	FMT_SMF.1 (1)	None	None
59	FMT_SMF.1 (2)	None	None
60	FMT_SMF.1 (3)	None	None
61	FMT_SMF.1 (4)	None	None
62	FMT_SMF.1 (5)	None	None
63	FMT_SMR.1	FIA_UID.1	FIA_UID.2
64	FPT_ITT.1	None	None
65	FPT_STM_(EXT).1	None	None
66	FPT_TST_EXT.1	None	None
67	FPT_TST.1 (1)	None	None

[33] The dependency on ADV_SPM.1was removed by the ST author, it is assumed this was an error.

Table 15 - SFR Component Dependency Mapping			
#	Component	Dependencies	Satisfied [Component #]
68	FPT_TST.1 (2)	None	None
69	FTA_SSL.3	None	None
70	FTA_TAB.1	None	None
71	FTP_ITC_EXT.1 (1)	None	None

Rationale for unsatisfied dependencies:

Each functional requirement, including extended requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. With the exception of dependencies related to FCS_COP.1(3), FCS_COP_(EXT).1, FDP_IFF.1-NIAP-0407 (1), and FMT_MSA.2 (2), all dependencies in this ST have been satisfied.

FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing) is an algorithm and does not require FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation; therefore these dependencies are not required to be satisfied.

The TOE's implementation of FCS_COP_(EXT).1Random Number Generation is an algorithm that does not require FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation; therefore these dependencies are not required to be satisfied.

The dependency of FMT_MSA.3 (2), (3) and (4) on FMT_MSA.1 is not required as this Security Target uses FMT_MOF.1 (4) instead. FMT_MOF.1 (4) more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this security Target.

6.3.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the Common Criteria EAL2 assurance package augmented with ALC_FLR.2. The Common Criteria allows assurance packages to be augmented, which allows the addition of assurance components from the Common Criteria not already included in the EAL.

Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures and correcting security flaws (ALC_FLR.2). The EAL chosen is based on the statement of the security environment (threats, organizational policies, assumptions) and the security objectives defined in this ST. The sufficiency of the EAL chosen (EAL2 augmented) is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE

Given the amount of assurance deemed necessary to meet the security environment and objectives of the TOE and the intent of EAL 2, EAL 2 is an appropriate level of assurance for the TOE described in this ST. Therefore, EAL2 augmented is an appropriate level of assurance for the TOE.

Table 16 shows the matrix of Security Assurance requirements; the ST assurance levels are shown in **BOLD** text, which clearly demonstrates that this Security Target meets EAL2+.

Table 16 - Evaluation assurance level summary								
Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	1	**2**	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1

Table 16 - Evaluation assurance level summary								
Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
	ADV_TDS		**1**	2	3	4	5	6
Guidance Documents	AGD_OPE	1	**1**	1	1	1	1	1
	AGD_PRE	1	**1**	1	1	1	1	1
Life-cycle Support	ALC_CMC	1	**2**	3	4	4	5	5
	ALC_CMS	1	**2**	3	4	5	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	**1**	1	1	1	1	1
	ASE_ECD	1	**1**	1	1	1	1	1
	ASE_INT	1	**1**	1	1	1	1	1
	ASE_OBJ	1	**2**	2	2	2	2	2
	ASE_REQ	1	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	1	**1**	1	1	1	1	1
Tests	ATE_COV		**1**	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		**1**	1	1	1	2	2
	ATE_IND	1	**2**	2	2	2	2	3
Vulnerability Assessment	AVA_VAN	1	**2**	2	3	4	5	5

Table 17 - SAR Component Dependency Mapping, maps the dependencies that exist for each SAR to demonstrate all SAR dependencies are satisfied.

Table 17 - SAR Component Dependency Mapping		
Component	Dependencies	Satisfied
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	Yes – ADV_FSP.2 Yes – ADV_TDS.1
ADV_FSP.2	ADV_TDS.1	Yes – ADV_TDS.1
ADV_TDS.1	ADV_FSP.2	Yes - ADV_FSP.2
AGD_OPE.1	ADV_FSP.1	Yes - ADV_FSP.2
AGD_PRE.1	None	--
ALC_CMC.2	ALC_CMS.1	Yes – ALC_CMS.2
ALC_CMS.2	None	--
ALC_DEL.1	None	--
ALC_FLR.2	None	--
ATE_COV.2	ADV_FSP.2 ATE_FUN.1	Yes – ADV_FSP.2 Yes - ATE_FUN.1
ATE_FUN.1	ATE_COV.1	Yes - ATE_COV.1
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	Yes – ADV_FSP.2 Yes – AGD_OPE.1 Yes – AGD_PRE.1 Yes – ATE_COV.1 Yes - ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1	Yes - ADV_ARC.1 Yes - ADV_FSP.2 Yes - ADV_TDS.1 Yes – AGD_OPE.1

Table 17 - SAR Component Dependency Mapping		
	AGD_PRE.1	Yes - AGD_PRE.1

7 TOE Summary Specification

7.1 Implementation description of TOE SFRs

This section provides evaluators and potential consumers of the RFS7000 portion of the TOE with a high-level description of each SFR, thereby enabling them to gain a general understanding of how the TOE is implemented. These descriptions are intentionally not overly detailed, thereby disclosing no proprietary information. This sections refers to SFRs defined in Section 6, Security requirements. The implementation of the AP7131 portion of the TOE is described in Reference [15].

7.1.1 Adopting 7131 Access Points - Overview

When an RFS7000 wireless controller is deployed in a system with multiple AP7131 access points, the RFS7000 performs one or more of the following functions:

1. Centralized management and provisioning of the access points (required)
2. Authentication for wireless clients (optional)
3. Routing of wireless traffic (optional)

The process of connecting an AP7131s to the RFS7000 is called “adoption” of the access point. The access point is then said to be running in adaptive mode.

7.1.1.1 Centralized management and provisioning

Once it adopts an access point, the RFS7000 pushes the appropriate configuration parameters to the access point. In this way large wireless networks with multiple access points can be centrally managed to ensure consistent application of security policies and network settings.
The most important configuration parameter for Common Criteria purposes is whether each WLAN is configured to be an “independent” or an “extended” WLAN. If a WLAN is configured to be “independent” then it will operate the same as a standalone AP7131, except for the centralized management piece. The differences in functionality when configured as an extended WLAN are described below.

7.1.1.2 Wireless Client Authentication

The RFS7000 can perform wireless client authentication on behalf of the AP7131 for extended WLANs if the “AAP_Proxy” setting is enabled. If AAP_Proxy is disabled, or the WLAN is set to independent, then the AP7131 performs authentication as a standalone access point, as described Reference [15].

7.1.1.3 Wireless traffic routing

When a WLAN is configured as extended, then the AP7131 does none of the switching, routing, or traffic flow enforcement for the received wireless traffic. The AP7131 receives the wireless traffic, decrypts the wireless PDU, and sends it to the RFS7000 through an IPSec tunnel for further processing.

7.2 TOE Security Functions

The TFS supports the following security functions:

- Security Audit
- Cryptographic Support
- User data protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels
- Intrusion Detection

7.2.1 Security Audit

7.2.1.1 Audit Generation

The TOE has the ability to selectively generate audit records from potentially security relevant events and transmit these records to the audit server in the environment.

Syslog messages at level 5 - LOG_NOTICE are used to satisfy the requirements for the content of audit records. Audit events include the date and time of the event, type of event, subject identify (if applicable), outcome (success or failure) of the event; some events require additional information as specified in FAU_GEN.1. The TOE supports user subject binding, associating each user to all program execution on behalf of that user, therefore, the user identity can always be associated to an audit event.

Table 18 – Syslog Support, shows the syslog levels supported; audit records are those tagged with Syslog level 5.

Table 18 – Syslog Support

Syslog level	Description
0 - LOG_EMERG	An emergency condition. The system is unusable
1 - LOG_ALERT	This message warrants an immediate action
2 - LOG_CRIT	Critical Condition
3 - LOG_ERR	Error
4 - LOG_WARNING	Warning
5 - LOG_NOTICE	Normal but a significant condition
6 - LOG_INFO	Information only
7 - LOG_DEBUG	This message appears only during debug mode

The TOE is dependent on an audit server in the IT Environment (a Syslog server) for the storage; the tools to review audit logs, the protection of audit logs from overflow, and the restriction of access to audit logs. All levels of Syslog messages are transmitted to the audit server in the IT environment immediately after generation, the audit server must filter the syslog messages (for level 5) to obtain just audit records.

The TOE can configure one Syslog server and two (2) backup Syslog servers. If the connection to the Syslog server(s) goes down, or the Syslog server(s) is unable to receive Syslog messages for any reason, the logs continue to be logged locally. The log messages generated when the Syslog server is unavailable will not be sent to the server when it is restored, but will be stored in the local file system in the file /var/log/messages.log; the maximum size of this file is 2MB. Once this file is full, it is moved to the file /var/log/messages.1.log and new logs continue to get written to /var/log/messages.log. If the file /var/log/messages.log fill again, it is again moved to /var/log/messages.1.log, overwriting the file, and the previous log messages are permanently lost. This effectively gives the administrator 4MB of effective storage before log messages are lost.

The file system used for audit record storage is temporary (/dev/ram mounted on /var/log), therefore, the locally archived logs are available only until the next reboot.

The network connection between the TOE and the external audit server is required to be secured using the IPSec security protocol. If the IPsec tunnel has not been established, no Syslog messages will be sent to the Audit Server. If the IPsec connection fails between the TOE and the Audit Server, a SNMP trap is generated and set to the SNMP server in the IT Environment to notify the administrator. If the Audit Server fails but the IPsec tunnel remains intact, no notification is sent.

FAU_GEN.1, FAU_GEN.2

The time stamp used for audit records is covered in Section 7.2.6, Protection of the TSF

Reliable Time Stamps.

7.2.1.2 Selective Audit generation

The TOE provides the ability to include/exclude events using filters based on the following parameters. A maximum of 10 filters can be created.

1. Filter precedence number (index ranging from 1 to 10)
2. IP Address
3. Permit/Deny
4. User who initiated operation
5. How this user is logged into the system (device interface)
    a. Device interface is defined as management interface or login source
        i. console (CLI),
        ii. Network – SSH (CLI via wired or wireless), Web UI (via wired or wireless)
            1. IP address (available for wired or wireless)
            2. MU MAC address (wireless only)
        iii. any, any of the above
6. The MAC address of Mobile unit used to do the operation

Parameter 3, 4, 5, and 6 can take wildcard value as 'any'. The IP address and username can be used as user identities. They can be used independently or can be used together (using an OR operation) to filter audit records.

The event type is not included in the filtering criteria listed above, however, the administrator has the option to set the log-levels (event type) separately. By default, the log-level is 5 (LOG_NOTICE). This covers all the audit logs originating from configuration change or management commands. Event types for the logs are given in Table 18 – Syslog Support. Level 5 (LOG_NOTICE) satisfies the requirements for the content of the audit records.

If filter rule matches for some operation, the outcome will depend on the 'log' or 'not-log' parameter of that filter.

Filter precedence is a rule index between 1 to 10 where 1 indicates high precedence, 10 indicates low precedence. The precedence number can be used to permit, deny or see details of a filter. The rule that has the highest filter precedence number will be followed if all the other parameters are same.

Audit log filters can be created, deleted and displayed from the CLI (both console and ssh), GUI and SNMP.
The System Administrator and Superuser roles can perform these operations using the Web UI and CLI; the SNMP administrator must have snmpmanager permissions to perform.

FAU_SEL.1

7.2.2 Cryptographic Support

The TOE utilizes cryptographic functions for the purposes of data protection using SSHv2, SFTP, SNMPv3, TLS1.0-based trusted paths used for the TOE administration, as well as for the IPSec-based trusted channel established between the TOE and external authentication, audit and time servers.
FCS_COMM_PROT_EXT.1

The TOE implements all cryptographic operations in software using OpenSSL copnfigured in FIPS mode, QuickSec, net-snmp, and OpenSSH. QuickSec is used only for IPSec, net-snmp and OpenSSH are used for their respective key generation capabilities, and OpenSSL is used for all other cryptographic operations.

The TOE cryptographic algorithms are NIST CAVP validated, as indicated by the certificate numbers listed below. **FCS_BCM_(EXT).1**

The following algorithms (Certificate #) were validated:

- AES (Certificates #2752, and #2765) **FCS_COP.1.1 (1)**
- TDES (Certificate #1656) **FCS_COP.1.1 (1)**
- RSA (Certificate #1443) **FCS_COP.1.1 (2)**
- SHS (Certificates #2321 and #2326) **FCS_COP.1.1 (3)**
- HMAC (Certificates #1726 and #1731)
- RNG (Certificate #1268 and #1270) **FCS_COP_(EXT).1.1**
- KDF (Certificates #190, #191, #192, #193) **FCS_CKM.1.1(1), (2)**

The TOE supports distributing cryptographic keys manually through the local serial port connection, and automatically through a remote SSH connection, as well as through the remote Web UI.

The TOE encrypts all persistently stored secret and private keys while not in use using 256-bit AES Master Encryption Key in CBC mode. The master encryption key used to encrypt and decrypt the persistent secrets and private keys is generated using a proprietary split knowledge procedure.

The TOE will destroy all session keys after administrator-defined period of inactivity; this applies to all security protocols supported by the TOE.

The TOE will check the public key validity time on export, and will not allow export or backup of expired certificates or public keys. **FCS_CKM_(EXT).2**

The TOE implements an ANSI X9.31 NIST CAVP approved random number generator in both the OpenSSL and QuickSec modules. ANSI X9.31 requires the initialization vector to never repeat, so the TOE uses the system time to seed the PRNG. The TOE implements this requirement using the Gettimeofday() function to generate a 64 bit seed; this function uses the underlying hardware real time clock. The TOE protects the integrity of the generated keys using physical security mechanisms and by performing a key integrity check on start up and periodically once a day. **FCS_BCM_(EXT).1**

A key zeroisation function implemented by the module zeroizes all cryptographic keys and critical security parameters by overwriting the storage area three times with an alternating pattern for all memory except RAM. For RAM memory, zeroisation is performed by a single direct overwrite consisting of a pseudo random pattern.
All intermediate storage areas for cryptographic keys and critical security parameters are zeroized upon the transfer of the key or CSP to another location. **FCS_CKM.4**

The module implements an administrator command to manually input/output cryptographic keys, including the IPSec pre-shared keys and RADIUS authentication key.

7.2.2.1 Cryptographic support for SSH, SFTP

The TOE uses the Secure Shell Protocol (SSH) version 2.0 to provide secure remote management of the TOE; it is implemented using openSSH operating in FIPS mode. It implements key exchange using the Diffie-Hellman algorithm with a 2048-bit key (DH Group 14). Note that 2 other DH groups appears to be offered by the TOE's SSH server, but these are merely protocols to negotiate a fixed DH group. The only group that is functional is DH Group 14. **FCS_COP.1.1 (4), FCS_CKM.2.1, FCS_SSH_EXT.1**

SFTP (SSH File Transfer Protocol), is an extension of the SSH v 2.0 and provides secure file transfer capability for the following management functions:

- Configuration file import/export
- Certificate import/export

The SFTP server in the IT environment must support:

- RSA host key size 2048 or greater
- AES128-CBC, AES192-CBC, AES256-CBC encryption
- HMAC-SHA1 or HMAC-SHA1-96 for authentication

FCS_SFTP_EXT.1

7.2.2.2 Cryptographic support for TLS

The TOE uses the TLSv1.0 protocol to support the HTTPS protocol used for secure management of the TOE using the Web UI and for Hotspot features; it is implemented using openssl-fips. It implements key exchange using the Diffie-Hellman algorithm with a 2048-bit key. **FCS_COP.1.1 (4), FCS_CKM.2.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1**

The TOE implements the following ciphers when using TLS:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

7.2.2.3 Cryptographic support for IPSec

The TOE uses IPSec to protect TSF data transfers between the TOE and the Audit Server, RADIUS Server, and the NTP Server. The TOE supports two modes of operation - Transport and Tunnel. Transport Mode provides a secure connection between two endpoints as it encapsulates the IP payload. Tunnel Mode encapsulates the entire IP packet to provide a virtual "secure hop" between two gateways.

IPsec may be configured to use the manual key mode or IKEv1, which uses PSK and DH group14 for key exchange to setup a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.
FCS_CKM.2.1, FCS_COP.1 (4), FCS_IPSEC_EXT.1

- For Manual key exchange
  - ESP Type: ESP with Authentication
  - ESP encryption algorithm: AES-128, AES-192, AES-256
  - ESP authentication algorithm: SHA-1
- For Auto key exchange (IKEv1)
  - ESP Type: ESP with Authentication
  - ESP encryption algorithm: AES-128, AES-192, AES-256
  - ESP authentication algorithm: SHA-1
  - IKEv1 authentication algorithm: SHA-1
  - IKEv1 authentication mode: Pre-shared key
  - IKEv1 encryption algorithm: AES-128, AES-192, AES-256
  - Diffie-Hellman Group: Group14 - 2048bit

7.2.2.4 Cryptographic support for Simple Network Management Protocol (SNMP)

The TOE administrator may also use the Simple Network Management Protocol version 3 (SNMPv3) for limited management of the TOE. SNMP versions 1 and 2 are disabled. Only AES/SHA-1 is supported for the implemented SNMPv3; the DES/MD5 option has been disabled. Security level “authPriv” only is supported, SHA-1 for authentication (auth) and AES for privacy (Priv). Security Level with ‘noAuthNoPriv’ and ‘authNoPriv’ is not supported. **FCS_SNMPv3_EXT.1**

7.2.3 User Data Protection

The TOE implements the Role-Based Access Control SFP, assigning each management command a fixed attribute, which indicates which role or roles can execute that command. When a user is created, the Superuser assigns a username, password, available interface(s) and the role(s) for the user; the role is used to limit the commands that user can execute. The superuser can assign the user a single role or multiple roles; however, a user can only assume one role at a time.

Table 19 – Role vs Feature

Features	Roles

Table 19 – Role vs Feature	
Cryptographic parameters	superuser, crypto-officer
Audit functions	superuser, sysadmin, Read/Write SNMP Administrator
Authentication data for administrative users	Superuser
Authentication data for wireless users	superuser
ACLs - roles and interfaces assigned to users	superuser, crypto-officer
Creating guest users for hotspot	webadmin

The assigned interface(s) limit the interface a user may log into the TOE to perform management functions. The following rules apply:
For users with Superuser, Crypto-officer, System Administrator, and Monitor roles:

1. When only console access is configured, then only console access is available.
2. When only SSH access is configured, then only SSH access is available.
3. When console and SSH access are configured, then both console and SSH access are available.
4. When no access restrictions are configured, then access to console, SSH and Web UI are available.

Users with the Web administrator role can only access the TOE through the Web UI.

FDP_ACC.1, FDP_ACF.1, FMT_MSA.3 (1)

The memory locations corresponding to network packets processed by the TOE are zeroized after the packet is processed. **FDP_RIP.1**

7.2.3.1 Firewall

The TOE implements a firewall that filters traffic addressed to the TOE as well as traffic passing through the TOE; e.g., all packets flowing to/from the LAN ports on the RFS7000. The firewall supports protection against Denial of Service attacks, Layer 2 and Layer 3 stateful inspection filtering, WLAN traffic, and role-based filtering. (A Role in this context refers to a group of authenticated wireless clients) The Layer 3 firewall is implemented using Safenet, Inc.'s quicksec; the Layer 2 firewall is implemented by Motorola Solutions.

Filters are applied to network packets in the following order:

1. Denial of Service Filters
2. Layer 2 Filters
3. Layer 3 Filters
4. WLAN Filters
5. Role-Based Filters

The Superuser and Crypto-officer roles can enable and disable each set of the above filters individually using the CLI or Web UI, and the Read/Write SNMP role can change them via SNMP. Additionally, the DoS Filters included some pre-configured filters that can be enabled and disabled individually.

For administrative (wired) users, the flow mediation is in accordance with the Traffic Filter SFP.
Filters are applied in the following order, prior to authentication:

1. Denial of Service (DoS) Filters
2. Layer 2 Filters (Port ACLs) for wired users - applied on physical Ethernet interface & Inbound traffic only.

3. Layer 3 Filters (Router ACLs) - applied on VLAN interface & Inbound traffic only. Here VLAN mapped to the physical Ethernet interface.

For wireless users, flow mediation is in accordance with the Authenticated Information Flow SFP. Filters are applied in the following order, after WLAN authentication:

1. WLAN Filters - filter/mark packets based on WLAN (MAC address / groups of MAC addresses) from which they arrived; these filters are applied to inbound & outbound traffic.
2. Role-Based Filters - applied to group of authenticated wireless clients on inbound & outbound traffic.

For flows destined for the TOE, flow mediation is in accordance with the Unauthenticated TOE Services SFP; this policy does not have to be enforced in the firewall ruleset, Note that "operations" refers to the TOE accepting or rejecting the network packet, since the TOE is not technically always providing a "service". **FMT_MOF.1 (4), FMT_SMF.1 (4)**

7.2.3.1.1 DoS Filters

The firewall uses a collection of filters to screen information packets for known types of Denial of Service (DoS) attacks. These filters can be disabled or enabled collectively, or in some cases, individually. Table 20 - Denial of service Attacks, describes the DoS attacks detected, if they can be disabled or enabled individually, and if a syslog message is generated.

Table 20 - Denial of service Attacks

Attack	Description	Disabled Individually	Syslog
LAND	Source IP is equal to Destination IP and Source Port is equal to Destination Port	NO	YES
TCP XMAS Scan	Sequence Number zero and FIN, URG and PUSH bits are set.	NO	YES
TCP NULL Scan	Sequence Number zero and all control bits are set to zero.	NO	YES
TCP FIN Scan	FIN Bit set and Sequence Number not valid.	NO	YES
Very Small IP TTL	TTL in the IP packet is less than the minimum value (1) defined on the wireless switch.	NO	YES
Smurf	Uses Source IP spoofing and ICMP echo to an IP broadcast address.	YES	YES
Winnuke	Uses TCP URG bit in header and sets URG pointer to point beyond the end of the frame. The program is specifically meant to crash Windows systems as windows TCP/IP stack does not handle OOB (Out of Band) data correctly. WinNuke program specifically uses port 139, but other ports are also vulnerable.	NO	YES
Invalid IP Protocol	An IP datagram with an invalid IP protocol	YES	YES
IP Fragmentation related attacks.	Attacks are based on one of the following parameters: - Very small IP fragment - Empty IP fragment - Overlapping IP fragment - Large no of fragments with the total length of all fragments going beyond 65536 which is the max IP datagram length - Duplicate fragments Some common known attacks based on the above anomalies are: - TearDrop, TearDrop2, Ping of Death, Syndrop, Opentear, Overdrop, Nestea, Targa 3, Newtear, Bonk, Boink, SSPing, Flushot, Jolt	NO	YES (log message will be general specifying one of the mentioned anomalies in the fragment chain)
Source IP Spoofing	Sending IP packets with source IP as some other hosts IP address.	YES	YES

ICMP Router Advertisement	The ICMP router discovery messages are called "Router Advertisements" and "Router Solicitations". Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. The attacker can spoof these messages and re-direct all traffic to its own system by modifying the routes on the target host.	YES	YES
UDP Short Header	IP datagram with total packet length < 28	NO	YES
Twinge	Sending a flood of non-echo ICMP packets to the target. The aim is to flood the network so that legitimate clients cannot access services on the target.	YES.	YES
IP Source Route Option	The "source routing" feature of TCP/IP allows the sender of network traffic to force the traffic to be routed through a certain point on the network. This is useful because it allows intruders to force packets to travel in unexpected directions.	YES	YES
Fraggle, Ascend, Echo/chargen	Broadcast UDP packets are sent to the target machine on echo (7), chargen (19), daytime (13) and qotd (17) ports.These services are outdated now, but were used in earlier days to provide information such as date and time (daytime,13), test connectivity (echo,7) and to generate a stream of characters (chargen,19). An attacker can send a flood of traffic to port 19 causing the server to process the data and then discard it.	YES	YES
Snork	UDP packet with destination port set to 135 and source port set to either of 7, 19 or 135. This attack is targeted against Windows NT RPC service. A single packet sent to a Windows NT system can cause the CPU usage to go upto 100% for a period of 5-120 sec.	YES	YES
TCP header fragmentation	IP Fragments containing in-complete TCP header. TCP header spans across fragments	YES. In some scenarios, TCP header can include TCP options and can span across fragments.	YES
TCP Short Header	IP datagram containing incomplete TCP header. TCP header length field in TCP header should be at least 20 bytes.	NO	YES
TCP bad sequence number	TCP sequence number checks for a resent-SYN, SYN+ACK or ACK, FIN, FIN+ACK. These type of attacks are usually man-in-the-middle attacks where the attacker injects a packet with invalid sequence number to terminate the connection.	NO	YES
TCP Postconnection SYN	Sending TCP packet with SYN flag set after the connection is established.	NO	YES
TCP Invalid Urgent Offset	Urgent pointer in TCP packet is pointing beyond the end of frame. Generic case of WinNuke attack	NO	YES
TCP SYN Flood	Sending large no of TCP SYN packets to the target to leave half-open TCP connections.	YES. User can configure SYN flood rate and max-incomplete connection threshold	YES
RFProwl	Related to TCP header fragmentation especially with TCP header size more than 20 bytes.	NO	NO. It will be detected as

			TCP header fragmented attack.
FTP Bounce	IP address in the FTP PORT command is not same as the IP address of the client (active) and server(passive)	YES	YES

FDP_IFC.1 (1), (2), (3), FDP_IFF.1-NIAP-0417 (1), (2), (3)

7.2.3.1.2 Layer 2, Layer 3, and WLAN Filters

The Superuser or Crypto-officer can configure firewall filter rules using available CLI commands interface, or the Web UI, and the Read/Write SNMP role can change them via SNMP. The TOE uses Access Control Lists (ACLs) to implement the rules filters. The ACL consists of series of entries called an Access Control Entry (ACE); each ACE defines a rule which defines whether a packet needs to be switched/routed or dropped. The firewall filters are initialized to provide permissive default values.

The switch supports the following ACLs to implement Layer 2 and Layer 3 stateful inspection filtering:

- *Router ACLs*
  - Applied to VLAN (Layer 3) interfaces; on inbound traffic packets routed through the switch
  - Traffic filtering is based on
    - *Source IP address*
    - *Destination IP address*
    - *Source Port*
    - *Destination Port*
    - *ICMP identifier*
    - *Incoming interface index*
    - *IP Protocol*
- *Port ACLs*
  - Applied to Layer 2 interface, switched packets only
  - Traffic filtering is based on:
    - Source IP address
    - Destination IP address
    - Source Port
    - Destination Port
    - ICMP identifier
    - Incoming interface index
    - IP Protocol
    - Source MAC
    - Destination MAC
    - Ethertype
    - VLAN-ID
    - 802.1p bits
- *Wireless LAN ACLs*
  - A Wireless LAN ACL is designed to filter/mark packets based on the wireless LAN from which they arrived rather than filtering the packets arrived on Layer 2 ports.

Every ACE within an ACL is made up of an action and matching criteria. The action defines what to do with the packet if it matches the specified criteria.
The following actions are supported:

- *Deny*
  - Instructs the ACL not to allow a packet to proceed to its destination.
- *Permit*
  - Instructs the ACL to allows a packet to proceed to its destination.
- *Mark*
  - Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit.
  - The fields that can be modified are,

        - 8021p <0-7> - Used only with action type mark to specify 8021p VLAN user priority between 0 - 7.
        - dscp <0-63> - Modifies DSCP TOS bits in the IP header. Specify the DSCP codepoint value between 0 - 63.
        - os <0-255> - Used to specify Type of Service (tos) bits in the IP header between 0 - 255.
    - The action type "mark" is functional only over a Port ACL.
    - The "mark" decision is made when the ACL entry is matched.

The rules within an ACL are applied to packets based on their precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules with the same precedence value. ACEs with lower precedence are always applied first to packets

FDP_IFC.1 (1), (2), FDP_IFF.1-NIAP-0417 (1), (2), FMT_MSA.3 (2), (3), FMT_MOF.1 (4), FMT_SMF.1 (4)

7.2.3.1.3 Role-Based Filtering

The TOE also implements Role-Based filtering in accordance with the Authenticated Information Flow SFP, where a role is a group of authenticated wireless clients (AKA MU); role-based filtering refers to applying firewall policies to the wireless clients grouped in a role. Any traffic coming from the wireless client is subject to the firewall policies (access-lists) applied to its associated role.

The role assignment to clients is based on match criteria of:

- User or device identify (MAC Address)
- Physical location of AP/Radio
- Associated ESSID
- Encryption scheme for the Wlan
- Authentication scheme for the Wlan
- Radius Group Name

Physical Location: Location refers to the physical location of the AP/radio that the wireless client connected to. This must be pre-configured on the AP
RFS7000(config-wireless)#ap 1 location Basement

MAC Address: A MAC address can be specified as a specific MAC or a mask. All clients having MAC matching the mask will be grouped into a role.

FDP_IFC.1 (3), FDP_IFF.1-NIAP-0417 (3), FMT_MSA.3 (4)

7.2.4 Identification and Authentication

The TOE keeps a local database of administrator passwords and utilizes password-based authentication to authenticate administrators connecting remotely using SSH protocol, over HTTPS (TLSv1.0) Web UI or locally using a serial console connection. The TOE also provides a capability to authenticate administrator against an external RADIUS authentication server. Administrative users are required to authenticate prior using any TOE functions except those necessary for remote authentication and basic protocols necessary for TOE operation. **FIA_ATD.1 (1), FIA_UAU.1 (1)**

The TOE monitors the number of failed authentication attempts; when the administrator-defined threshold of unsuccessful authentication attempts for a remote administrator has been reached, that remote administrator interface is disabled until re-enabled using a local console connection. Note that the lockout is applied per interface (GUI, SSH) and not per user. If a user reaches the limit of failed login attempts via SSH, for example, then the SSH interface is locked for all users. The same user can attempt to authenticate via the GUI. The local console CLI is the primary management interface for the TOE and is used to remove the interface lock; therefore, the local console interface is never locked.

The CLI supports commands to set the threshold value for SSH and Web UI login failure; and to remove the lock so the SSH administrative interface and/or the Web UI may again be used. The default value is 3 authentication attempts, the maximum is 1024. The SNMP interface does not have a limit on authentication attempts. **FIA_AFL.1 (1)**

The TOE supports wireless user authentication using the internal Radius server or an external Radius server. When the AP-7131N is configured to use the RFS7000 as its external RADIUS Server, the RFS7000 portion of the TOE provides the IEEE 802.1X authentication services using its internal RADIUS server. When the internal RADIUS Server is used, the user credentials can be obtained from a local database or an external LDAP server. When the local database is used, users and groups can be added using the CLI or Web UI management interfaces, and are stored locally on the TOE. When using either local database or external LDAP database the identification and authentication is based on the username and password attributes.

The TOE's internal radius server is implemented using FreeRADIUS modified to support only FIPS 140-2 approved ciphers; all non-FIPS approved ciphers are disabled. For IEEE 802.1X EAP, authentication may use a local RADIUS server using a local user database, a local RADIUS server using a remote LDAP user database, or utilize services of an external RADIUS authentication server.

1. Local RADIUS Server for 802.1x EAP authentication using local user database supports
   a. EAP-TLS,
   b. EAP-TTLS (MD5, PAP and MSCHAP-V2), or
   c. EAP-PEAP (GTC and MSCHAP-V2)
2. Local RADIUS Server for 802.1x EAP authentication using remote LDAP user database supports
   a. EAP-TTLS (PAP), or
   b. EAP-PEAP (GTC).

For the external Radius server configurations, the TOE supports a primary radius server and optionally, a secondary radius server.

The authentication is based on IEEE 802.1X EAP-TLS, EAP-TTLS and EAP-PEAP authentication protocols. The TOE acts as the 802.1X authenticator and utilizes services of an external RADIUS authentication server to provide wireless user authentication. During the authentication phase, the TOE serves as an intermediary passing authentication messages between the wireless client device and the external authentication server. If the authentication is successful, the authentication server passes the TOE 802.11i session keys used to establish a 802.11i secure connection between the TOE and the wireless client device. Once the connection is established, the wireless client device may access the protected wired network utilizing the TOE as a gateway. The network connection between the TOE and the external authentication server is protected using the IPSec security protocol. EAP-TLS authentication protocol uses a client certificate for wireless user authentication, EAP-TTLS and EAP-PEAP protocols use password-based authentication. **FCS_RAD_EXT.1, FCS_EAP-TLS_EXT.1, FCS_EAP-TTLS_EXT.1, FCS_PEAP_EXT.1**

No services, other than those necessary to provide remote authentication support and the necessary basic protocol support, are provided by the TOE until the user is successfully identified and authenticated. **FIA_ATD.1 (2), FIA_UID.2, FIA_UAU.1 (2), FIA_UAU_(EXT).5**

SFTP is interactive by nature, which is supported by the CLI where the administrator can enter the authentication credentials, however, if the Web UI is to be used, the TOE also implements a non-interactive support initiated by the administrator from the RFS7000 as described below:

To establish non-interactive communication with the SFTP server, the SFTP server will need the public key of the RFS7000. This is accomplished using the 'keytransfer' command from the CLI which generates public and private RSA keys. The public key is transferred to the SFTP server and is appended to the .ssh/authorized_keys file that is present in the home directory of that user. This ensures that the device can transfer files between itself and the SFTP server in a non-interactive manner.

After a user has authenticated, the TOE maintains an association between that user and any program execution done on behalf of that user. This association is maintained as long as any program execution associated with a user continues. **FIA_USB.1**

7.2.4.1 EAP-TLS X.509 Client Certificate Authentication

The following is a summary of the processing performed to authenticate a X.509 Client Certificate.

1. The TOE sends a peer certificate request to the peer(MobileUnit)
2. The peer(MU) sends its certificate to the AP
3. The verification process will begin at the TOE
    a. The certificate chain is checked by beginning with the 'subject certificate'[34] and then proceeds through the intermediate certificates up to a trusted 'root certificate', typically issued by a trusted certification authority.
4. At each level (in the path tree)
    a. Incoming certificate's signature/fingerprint is checked and verified with the CA cert by the TOE.
    b. If the above check succeeds, TOE verifies the certificate has been issued by a trusted Certificate Authority.
    c. If (b) succeeds, TOE verifies that the certificate is valid for the present date(ie it is being present within its validity dates)
    d. If (c) succeeds, TOE verifies that the certificate has not been revoked by its issuing certificate authority, by checking with respect to a certificate revocation list.
    e. If the above steps succeed, TOE verifies the credentials presented by the certificate fulfill the following additional requirements:
        i. Certificate Common Name (CN) Validation
            1. Certificate Common Name should be present in Radius user database.
        ii. Access Control List (ACL) Verification,
            1. Wireless user must be member of the radius group ACL configured in TOE
        iii. Policy Verification
            1. TOE verifies that wireless user can access TOE at this instant based on policy configured (all days / weekdays / any particular days).
5. If the verification fails, the TLS handshake is immediately terminated with an alert message containing the reason for the verification failure.
6. On success, a peer-id will be created for the user and the session will be established between TOE and its user.

7.2.5 Security Management

The management of the security relevant parameters of the TOE is performed by the authorized administrator roles defined below. These are the only roles that have direct access to the TOE functions; however, the TOE supports the SNMP administrator role providing remote management and a SNMP trap interface via the SNMPv3 protocol. The SMNPv3 interface supports all commands supported on the Web UI interface.

The TOE supports the following administrative roles:

1. Crypto-officer
    a. Cryptographic functions and network management
2. Monitor
    a. Read-only access
3. System Administrator
    a. General system configuration administrative access
4. Web Administrator

[34] Subject certificate: leaf level peer certificate which has the fingerprint of CA
Note: The TOE does path validation only when the peer provides 'path information' of the peer's certificate, which the peer has to provide at the time of TLS handshake. However, the TOE will not validate the certificate's path by connecting to the internet, or pre-configure the necessary intermediate certificates to complete path validation.

    a. Web authorization for hotspot user access
5. Superuser
    a. Administrative root access
6. Read only SNMP administrator (snmpoperator)
    a. Read-only remote administrative access
7. Read/Write SNMP administrator (snmpmanager, snmptrap)
    a. Read/Write remote administrative access
    b. By convention, the built-in snmpmanager account is used for getting/setting OIDs, and the snmptrap account is used for receiving traps.

The TOE also supports the wireless user role; however, this user has no access to TOE functions and can only pass data through the TOE.

FMT_SMR.1

The TOE provides the following management interfaces:

- Command Line Interface (CLI) via
    - Local RS-232 console connection,
    - Remote SSH interface via the LAN
- Remote HTTPS & SNMPv3 JAVA based Web UI via the LAN
- Remote SNMP interface via the LAN
    - Remote management and trap support
- Configuration file downloaded by SFTP

The CLI, SNMP and Web UI provide interfaces to provide the following:

- Manage cryptographic functions **FMT_MOF.1(1)** as follows:
    - Load the cryptographic key (CLI only)
    - Zeroize a key (CLI only)
    - Set a key lifetime
    - Set the cryptographic algorithm (CLI only)
    - Start self tests of the TOE cryptographic functions (CLI only)
- Manage audit functions **FMT_MOF.1(2)**
    - Selection of the events types which trigger an audit record,
    - Start and stop of the audit function.
- Manage authentication functions **FMT_MOF.1(3)**
    - Allow or disallow the use of an authentication server
    - Set the number of authentication failures that must occur before the TOE takes action to disallow future logins (for remote administration only)
    - Set the length of time a session may remain inactive before it is terminated
- Manage Firewall Functions **FMT_MOF.1(4)**
    - Enable and disable individual firewall features
        - Denial of Service Filters
        - Layer 2 Filters
        - Layer 3 Filters
        - WLAN Filters
        - Role-Based Filters
    - Enable and disable pre-configured filters
    - Create, change, and delete firewall rules
- Manage Intrusion Detection functions **FMT_MOF.1(5)**
    - Change the Rogue AP Detection Method
    - Change Rogue AP approved listing
    - Display Rogue AP Details
- Enforce the Role-Based Access Control SFP to restrict the change the security attributes, user role(s), username, password, and available interface(s) **FMT_MSA.1**
- Enforce the Role-Based Access Control SFP **FMT_MSA.3 (1)**
- Enforce the Traffic Filter SFP**. FMT_MSA.3 (2)**

- Enforce the Unauthenticated TOE Services SFP**. FMT_MSA.3 (3)**
- Enforce the Authenticated Information Flow SFP**. FMT_MSA.3 (4)**
- Manage audit functions **FMT_MTD.1(1)**
    - Support to create, delete rules are provided.
    - Support to "query" and "modify" the rules have not been provided. User has to clear the rule and create a new rule instead of modifying.
- Manage administrative authentication data **FMT_MTD.1(2)**
- Manage wireless user authentication data **FMT_MTD.1(3)**
- Configure administrative authentication and the cryptographic functions of the wired network interface. **FMT_SMF.1(1)**
- Configure audit functions **FMT_SMF.1(2)**
- Configure wireless cryptographic keys **FMT_SMF.1(3)**
- Configure Firewall rules and settings **FMT_SMF.1 (4)**
- Configure Intrusion Detection Settings **FMT_SMF.1 (5)**

The CLI, Web UI, and SNMP interfaces test the input of all security attributes to ensure that the values input result in a secure configuration prior to acceptance of the input. **FMT_MSA.2**

All management functions require the administrator to be successfully authenticated prior to access.

7.2.5.1 Local RS-232 Command Line Interface (CLI)

The primary management interface to the TOE is the local RS-232 interface; this provides the administrator local access to all available commands; the CLI commands are documented in user guidance. [1]

7.2.5.2 SSH

The TOE uses the Secure Shell Protocol (SSH) to allow the administrator access to the CLI for secure remote management of the TOE. The SSH protocol is accessible via either the LAN ports. This interface supports all commands accessible via the local CLI connected via RS-232 except the following:

- clear remote-login-lock

7.2.5.3 Simple Network Management Protocol (SNMP)

The TOE can also use the Simple Network Management Protocol version 3 (SNMPv3) for management of the TOE; the implementation is based on NET-SNMP.

SNMPv3 uses Management Information Bases (MIBs) to manage the device configuration and monitor network devices in remote locations using a MIB Browser or equivalent SNMP Management software. MIB information accessed via SNMP is defined by a set of managed objects called Object Identifiers (OIDs). An OID is used to uniquely identify each object variable of a MIB.

In the evaluated configuration, the supported SNMP capability is the same as the Web UI interface; SNMP versions 1 and 2 are disabled.
SNMP v3 with a security level of ‘authPriv’ is supported. Authentication via SHA-1 is supported, for privacy only AES encryption is supported, DES has been disabled.

There is no support for the security level of noAuthNoPriv and authNoPriv.

There are three (3) SNMP administrative users pre-configured on the TOE; no other SNMP users can be configured. The pre-configured SNMP users and access are as follows:

1. snmptrap (read/write access to OIDs)
2. snmpmanager (read/write access to OIDs)
3. snmpoperator (read only access to OIDs)

SNMP users' can access all OIDs except cryptographic related OIDs as defined above, but can only read cryptographic related OIDs. This read or read/write access is provided using the MAX-ACCESS option in the MIB.

To access the MIB objects on the device, the MIB Browser(or any SNMP management tool) must use the pre-configured users. The configuration options on the MIB Browser are vendor specific; guidance is provided in [1] to configure common MIB browsers.

7.2.5.4 Configuration file downloaded by SFTP

Configuration settings for the TOE can be imported from or exported to the SFTP Server in the IT Environment. This allows the administrator to save the current configuration before making significant changes or restoring a default configuration. The TOE uses the CLI and Web UI interfaces to initiate a SSH File Transfer Protocol for Configuration file export/import. Administrators with Superuser, crypto-officer and/or sysadmin roles can import/export a configuration file.

There are two ways to import a configuration file:

- Importing a new config file onto the **startup config** file replaces the existing startup config file. A single audit record is generated upon performing this import operation.
- Importing a new config file onto the **running config** file merges it with the current running configuration. "merge" means same config items are overwritten, existing distinct config items are retained and new distinct config items are appended. Separate audit record is generated for each line of the configuration file for this import operation.

7.2.5.5 JAVA based Web UI Applet

The TOE uses a JAVA based Web UI accessible via the HTTPS protocol for secure management of the TOE. This applet is supported using the ACME Laboratories, tiny/turbo/throttling HTTP server (thttpd). The Web UI is only accessible using browsers that support the TLSv1.0 protocol. Additionally, the administrator must ensure Oracle's (formerly SUN) JRE (version 1.6 or above) is installed on the computer accessing the Web UI applet; Microsoft's Java Virtual Machine must be disabled if installed.

This interface supports all commands accessible via the SNMP interface.

7.2.5.6 AP-7131N Adaptive Mode:

An adaptive AP (AAP) is an AP-7131N Wireless Access Point that can be adopted by an RFS7000 switch; which provides management capability of the AP-7131N. The RFS7000 does not have its own radio interfaces; it uses the radio interfaces of the adopted APs to support 802.11a/b/g/n standards. An AAP receives its configuration from the switch initially as part of its adoption sequence. Subsequent configuration changes on the switch are reflected on the AAP. An AAP applies the configuration changes it receives from the switch after 30 seconds from the last received switch configuration message. When the configuration is applied on the AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds) forcing associated MUs to disassociate. MUs will immediately re-associate.
Table 21 – AAP Configuration Items, contains the configuration items that can be modified on the switch, which gets pushed to the AP.
While in adaptive mode, the AP mode will still have all its configuration items enabled. Any changes done on the AP will take effect. Any changes done on the switch will be pushed to the AP and it overrides that specific configuration item done from the AP.

Table 21 – AAP Configuration Items

Configuration Item	Expanded form	Pointers to documentation	From
ACS	Automatic Channel Selection	4.7.1 - Configuring Access Port Radios (4-72)	Switch SRG
WIPS	Wireless Intrusion Protection System (RFS7000 supports	4.7.1.2 Configuring an AP's Global Settings (4-76)	Switch SRG

Table 21 – AAP Configuration Items			
	WIPS)		
Static Ip	static IP address for AP.	**20.1.8 ap-ip (20-15**	**Switch CRG**
Voice admission control	Voice Call Admission Control	point 18 (4-82)	Switch SRG
Channel	Channel related configurations	4.8.1 Configuring AP Adoption Defaults	Switch SRG
Power	Power configurations	4.8.1 Configuring AP Adoption Defaults	Switch SRG
Wlan Inactivity Timeout	Inactivity timeout in seconds. If a frame is not received from a mobile unit for this interval, the mobile unit is disassociated.	**20.1.50 wlan (20-87)**	**Switch CRG**
Portal_Rates	Portal rates configuration	Configuring Rate Settings (4-83)	Switch SRG
Per_AP_Country_ Code	country-code can be configured for a particular ap	no reference	
Tx_Power	Transmit power	point 6. The Calibration Configuration section (4-103)	Switch SRG
OFDM	Orthogonal frequency-division multiplexing	6.2.5 AP Containment (6-9)	Switch SRG
Antenna_Control	antenna control configs	point 17. Advanced Properties (4-80)	Switch SRG
WTP_QoS	Wireless Transaction Protocol - Quality of Service	QOS Weight (4-23)	Switch SRG
Load_Balancing	load balancing	Dynamic AP Load Balancing (5-37)	Switch SRG
802.11 Capabilities	Short Preambles	4.7.1.3 Editing AP Settings (4-78)	Switch SRG
Wlan_Bandwidth	wlan bandwidth settings	4.5.1 Configuring WLANs (4-22)	Switch SRG
Rogue AP	point 7 & 8	4.7.1.3 Editing AP Settings (4-78)	Switch SRG
STP	Spanning Tree Protocol	4.10.1 Configuring a Bridge (4-127)	Switch SRG
SNMP	Simple Network Management Protocol	7.3.1 Configuring SNMP v3 Access, 7.4 Configuring SNMP Traps	Switch SRG
ABG_Scan_Config	Configure ABG-scan mode on the AP	**20.1.5 ap (20-9)**	**Switch CRG**
RTLS	Real Time Locationing System	5.8.4 Configuring SOLE Parameters (5-64)	Switch SRG
MU_ACL	Mobile Unit - Access Control List	6.4.9 Adding a new Wireless Filter	Switch SRG
Wlan_Config	Radius related Config	Configuring 802.1x EAP (4-31)	Switch SRG
	WPA2	Configuring WPA2 using CCMP (4-39)	Switch SRG
	Mu Timeout	4.5.1.3 Configuring Authentication Types (4-30)	Switch SRG
	ACL	6.4.2 Attaching an ACL on a WLAN Interface/Port	Switch SRG
	Mu Rate Limiting	4.5.1 Configuring WLANs (4-21, 4-22)	Switch SRG
	Dynamic Vlan	4.5.1.1 Editing the WLAN Configuration - Dynamic Assignment (4-27)	Switch SRG
	Vlan ID	4.5.1 Configuring WLANs (4-21)	Switch SRG
	Mode - Independent or Extended	4.5.1 Configuring WLANs (4-22)	Switch SRG
	L3 Mobility	5.5.1 Configuring Layer 3 Mobility	Switch SRG
	Client Bridge Back Haul	4.7.1.1 Configuring an AP Mesh Network (4-75)	Switch SRG
	Authentication Type	4.5.1 Configuring WLANs (4-22)	Switch SRG
	Encryption type	4.5.1 Configuring WLANs (4-22)	Switch SRG
	Mesh ESSID	B.1.12.1 Configuring Adaptive AP Mesh	Switch SRG
	WMM - Wireless MultiMedia	4.8.4 Configuring WMM	Switch SRG
Radio Config	radio_id	4.7.1.4 Adding Aps	Switch SRG

Table 21 – AAP Configuration Items			
	bssid	4.8.3 Configuring WLAN Assignment (pt 4)	Switch SRG
	beacon interval	4-95: Editing AP Settings	Switch SRG
	dtim interval	4-96: DTIM Periods	Switch SRG

7.2.6 Protection of the TSF

7.2.6.1 Reliable Time Stamps

The TOE has the capability to obtain reliable time from a remote Network Time Protocol (NTP) Server to provide reliable time stamps for audit services. Additionally, the system administrator can manually set the time (maintained locally in the hardware Real Time Clock (RTC)) on the TOE using the CLI management interface.

The RFS7000 can act as a NTP client, NTP server (relay) or NTP peer. When an administrator performs any NTP-related configuration, the NTP daemon is started and NTP becomes available. By default, NTP is not available. NTP stores its configuration in /var/etc/ntpd.conf. Every time user enters/modifies a configuration, the *ntpd.conf* file is re-generated and ntpd restarted for it to read the new conf file.

To establish a connection to an external NTP server or a NTP client, the TOE requires an IPsec tunnel to have been previously established between the TOE and the NTP Server/NTP clients; if no IPsec tunnel can be established, the NTP service cannot be used.

The RFS7000 can also act as a NTP relay, it gets timestamp information from a configured NTP server and it relays it to its NTP clients. If the RFS7000 is unable to get the requested timestamp information from NTP server, it will not relay updated timestamp & in turn clients will not be updated.

The RFS7000 can be configured as NTP client; once configured, it will synchronize its internal clock to an external NTP timeserver. The RFS7000 can be configured to use multiple NTP Servers. The guidance documentation [4] provides full configuration details.

The RFS7000 can also be configured as a NTP peer; when so configured, each device shares its time information with the other peer devices, and each device can provide time synchronization to the other. The guidance documentation [4] provides full configuration details.

If the system administrator updates the system time, the NTP client continues running and will update the system time on the next NTP update. **FPT_STM_(EXT).1**

7.2.6.2 TOE Self-Tests

The TOE implements the following set of FIPS 140-2 self-tests, which are executed during initial start-up, periodically once a day, upon administrator request via the CLI, and whenever a crypto key is generated

- Integrity check using SHA-256 of the image and persistent keys
- Power-up tests for openSSL library
  - AES encryption/decryption - 128 bit
  - 3DES-ECB encryption/decryption
  - RSA keypair generation and signature generation/verification - 2048 bit
  - SHA-1 hash
  - SHA-256 hash
  - HMAC-SHA-1 hash
  - HMAC-SHA-256 hash
  - RNG
- Power-up tests for QuickSec library

- RNG test
- SHA test
- HMAC-SHA-1 test
- AES test

These FIPS 140-2 self-tests may be invoked by the system administrator via the CLI:

- CLI:
  - RFS7000#run self-test

Success results are logged to `fipscheck.log` and they can be viewed by using the following CLI command:

- RFS7000# show crypto-log <cr>

Failure results are logged to `fipserror.log` file & they can be viewed by using the following CLI command:

- RFS7000# show crypto-error-log <cr>

The TOE also implements a set of hardware self tests that are executed by the boot loader when the device boots up that verify the correct operation of the underlying hardware.
These test cover:

1. RAM
2. NOR Flash
3. NAND Flash
4. Ethernet
5. PCI

Integrity check on persistent keys:
On initial startup, the default persistent keys are concatenated into a combined key and the SHA-256 hash of this combined key is calculated. This hash value is stored in a file. As authorized users create custom keys to use instead of the defaults, this process is repeated to generate a new hash over the modified keyset. During startup, the combined SHA-256 Hash of the persistent keys are calculated (as above) and compared against the stored hash value. This integrity check is also performed as part of the run self-test run-time self-test.

FPT_TST.1 (1), FPT_TST.1 (2), FPT_TST_EXT.1

If the self-tests fail, an error message is displayed on console, logged and the TOE is rebooted.

7.2.6.3 TOE Access

There are two sets of advisory/warning messages displayed before establishing a user session; both are displayed before the login/password prompt. The first message displayed before the login prompt is: “This Device is running in Common Criteria Mode,” and cannot be changed by the administrator.

The second message displayed before the login prompt can be changed by the administrator and can have a length between 10 and 250 characters. The Superuser and system administrator roles can change the message by executing a CLI command as given below:

- RFS7000(config)# access-banner <msg-txt>

This message is stored in a file called /etc2/accbanner.txt. This file is not directly accessible to any user including the administrator. The only way to change the contents of this file is using the CLI command given above.

An example of these warning messages before the login/password prompt is displayed below:

Please press Enter to activate this console.

RFS7000 login: cli

This Device Is Running In Common Criteria Mode.

Attention:
This is a protected and private wireless system. No un-authorized access allowed.
You must have proper rights to access and manage this system from the authorized personnel.
Do you want to proceed? (y/n): y

User Access Verification

Username: admin
Password:

FTA_TAB.1

The TOE terminates user sessions after a time interval of user inactivity is reached as follows:

- **SSH session**: Administrator can configure user interactivity timeout for SSH Login
  - Default timeout value is 120 seconds.
- **CLI console session**: An administrator-configurable timeout value is used for Local interactive session (CLI console).
  - Default time is 180 seconds.
- **HTTPS session** administrator configurable session inactivity timeout
  - Default time is 60 minutes

FTA_SSL.3.1

7.2.7 Trusted Path/Channels

The TOE provides trusted paths for connection to authentication functions, communications to remote audit server, NTP functions, SNMPv3 authentication, and the import/export of configuration files for management via SFTP. **FTP_ITC_EXT.1**

Additionally, the TOE protects internal data transfers between the RFS7000 and the AP7131 portions of the ToE via the IPSec protocol. **FPT_ITT.1**

7.2.7.1 SSH

The TOE supports SSHv2 for remote administration of the TOE; this SSH interface gives the administrator access to the CLI. This interface authenticates the SSH server using the SSH Server's public certificate, the client is authenticated using a username and password. Section 7.2.2.1 describes the cryptographic support provided to protect the channel data from modification or disclosure.

7.2.7.2 TLS

The TOE supports TLS1.0 for remote administration of the TOE; this interface gives the administrator access to the Web UI. This interface authenticates the server using the server's public certificate; the client is authenticated using a username and password. Section 7.2.2.2 describes the cryptographic support provided to protect the channel data from modification or disclosure.

7.2.7.3 SNMPv3

The TOE supports SNMPv3 for remote administration of the TOE; this interface gives the SNMP administrator access to the management commands. This interface uses a shared secret that is used to provide assured identification of the end-points. The shared secret must be entered at both the client and

server by an authorized administrator prior to establishing a SNMP session. Section 7.2.2.4 describes the cryptographic support provided to protect the channel data from modification or disclosure.

7.2.7.4 SFTP

The TOE supports SFTP for importing and exporting configuration files to/from the TOE; SFTP is an extension of the SSH v 2.0 and depends on the SSH transport layer to provides assured identification of its end-points and protection of the channel data from modification or disclosure.

7.2.7.5 IPsec

The TOE maintains a trusted channel for communication with the adopted AP7131 access points, and the audit, RADIUS, and Network Time Protocol servers in the IT Environment. The TOE also allows users to create a VPN to the TOE for secure remote connections. The channel is protected by the IPSec protocol with manual keys and can be initiated by the TOE or the other party. The Administrator has to configure an explicit IPsec tunnel between RFS7000 and the connected endpoint. The trusted channel is based on the IPsec/IKE protocol with pre-shared keys. Section 7.2.2.3 describes the cryptographic support provided to protect the channel data from modification or disclosure.

In addition to the pre-shared IKE keys, remote user VPNs can be configured to require a username and password to authenticate to the TOE. The username and password can be stored locally on the TOE, or on a remote RADIUS server.

7.2.8 Rogue Access Point Detection

The TOE provides rogue AP detection, i.e., any unauthorized active AP operating within the radio coverage of an authorized AP. When a rogue-AP is detected, the administrative user is notified with a SNMP trap and a syslog message is generated. In addition, the admin can look for detected rogue APs using the CLI and Web UI interfaces. An audit event is generated when a rogue-AP is detected.

The TOE detection mechanism uses the Access Point to assist in Rogue AP detection using one the following administrator selectable methods:

- RF On-Channel Detection
  - Enables the access point to detect rogue APs on its current (legal) channel setting
- RF Scan by Detector Radio
  - A dedicated Detector AP scans for Rogue APs on all channels.
- RF 'ABG' Scan
  - Scan for rouges over all channels on both of the access point's 11a and 11bg radio bands.

After performing the scan to detect all AP MAC addresses in the wireless coverage range, the scan results are compared with the list of allowed AP MAC addresses maintained on the TOE. If the MAC address of a detected AP matches an entry on the administrator configured approved list, it is ignored; otherwise, it is reported as a Rogue AP and added to the Rogue AP list, a syslog message generated and a Trap message sent to the SNMPv3 manager.

The Superuser or Crypto-officer roles have the ability to review the Approved AP list as well as the Rogue AP list, move APs from the Rogue AP list to the Approved AP list, and the adopted AP sends the following information to the Switch, which maintains a table with the following information:

- MAC address of the detected rogue AP
- AP MAC address
- ESSID of the detected rogue AP
- Signal strength of the detected rogue AP
- Channel on which the AP was detected
- Time when the AP was detected

FID_APD_EXT.1, FMT_MOF.1 (5), FMT_SMF.1 (5).

7.2.8.1 Supported Wireless Intrusion detection System (WIDS) Events

In adaptive mode, an AP7131 can be configured to collect all the beacons it hears and forward them to the switch for analysis. The RFS7000 portion of the TOE will perform the types of analysis listed in Table 22.

Table 22 – Supported WIDS Events			
No	Attack type	EventType	Counter-measures
1	ap-default-configuration	anomaly-detection	Send SNMP trap, generate syslog
2	ap-ssid-broadcast-in-beacon	anomaly-detection	Send SNMP trap, generate syslog
3	fake-ap-flood	excessive-operations	Send SNMP trap, generate syslog
4	suspicious-ap-high-rssi	anomaly-detection	Send SNMP trap, generate syslog
5	unauthorized-ap-using-authorized-ssid	anomaly-detection	Send SNMP trap, generate syslog

7.2.8.1.1 AP Default Configuration

Configuration problems are a significant source of security vulnerabilities on wireless networks. Typically, the vendor's default configuration is a well known SSID operating on a well known channel, and not utilizing any encryption or authentication mechanism. APs may revert to factory default settings in certain cases when a firmware upgrade fails or a corrupted configuration is encountered. This is also a problem mainly associated with "thick APs". An authorized AP that is not using the correct configuration will allow unchallenged access to the wireless network and poses similar security risks to that of a rogue AP. Additionally, while the authorized AP is in a default configuration state, the authorized client stations will be unlikely to successfully authenticate to the basic service set (BSS), effectively causing a denial of Service (DoS) on the wireless network.

7.2.8.1.2 AP SSID Broadcast in Beacon

The Service Set Identifier (SSID) identifies a wireless network and allows distinction between different wireless networks operating in the same airspace. If the SSID is broadcast in every beacon frame, most wireless stations will show it as an available network to connect to. Broadcast of the SSID in the beacon is not required by the 802.11 specification; it is recommended to disable broadcast of SSID in the beacon.

The TSF monitors for the SSID being broadcast in the beacon and compares this behavior to the defined value in the AP's Configuration Policy.

7.2.8.1.3 Suspicious AP - High RSSI

An unauthorized AP is an access point that has been seen operating in your airspace but has not been added to the list of authorized or ignored access points. By default, all APs are considered unauthorized unless explicitly identified in the switch as either authorized or ignored. The unauthorized AP may be a neighboring device, internal to the network, or an AP created by a malicious user. The unauthorized AP may potentially be inside the enterprise and may or may not be attached to the wired network. The unauthorized AP could also be an AP setup by a malicious user that is intended to be used to perform Phishing, or evil twin attacks.

Because wireless networking is not constrained by traditional physical boundaries such as the walls of the physical location, an unauthorized AP may be physically outside the enterprise perimeter but transmitting into your airspace. In this case, the AP is simply a neighboring device and presents no immediate security risk to your enterprise.

Unauthorized APs may exist as

- AP physically located inside the building
- AP outside the building

For this event, switch raises an alarm whenever beacons with signal strength exceeding threshold are received. In densely populated areas such as cities or multi-tenant offices, this alarm should be considered low priority since the frequent occurrences of seen devices may not present a security threat. For environments with strict no-wireless policies, responding to this alarm is critical in ensuring that a wireless-free environment is maintained.

7.2.8.1.4 Fake AP Flood

Fake-AP is an open source perl script utilizing the Host AP Driver for Intersil Prism2/2.5/3 hardware. It was developed as a proof of concept to emulate thousands of counterfeit APs. The tool injects beacon frames with spoofed (fake) source/BSSID addresses and SSIDs into the air, resulting in clients and reconnaissance tools detecting numerous APs which physically do not exist. The address and SSID of the fake APs can come from predefined text files included with the tool or user defined files. The tool cycles through these files creating random combinations of SSID and BSSID.

Purpose of the Fake-AP tool :
The purpose of this tool is to hide real APs amongst the thousands of fake APs, making wireless reconnaissance tools ineffective. This attack could also be used against a wireless intrusion detection system (WIDS). Another popular use of Fake-AP is to cause a denial of service to wireless clients by flooding the AP table of the clients and thus preventing the client from finding valid APs to connect to. Most recent wireless supplicants are now immune to Fake-AP attacks.

Security Impact :
The overall security impact of a Fake-AP flood attack is minimal but warrants heightened security awareness of the affected areas. The Fake-AP tool has minimal impact on recent clients.

7.2.8.1.5 Unauthorized AP Using Authorized SSID

The service set identifier (SSID) is used to identify a wireless network, which is comprised of multiple APs using the same SSID. Non-sanctioned APs that are observed using the unauthorized SSID may indicate malicious attack; a malicious attack could be an attempt to phish valid clients from the sanctioned network and should be investigated promptly or as a result of a configuration error; a sanctioned AP could that hasn't been authorized in the WIDS platform.

FMT_MOF.1 (5), FMT_SMF.1 (5)

8 Acronyms

Table 23 - TOE Related Abbreviations and Acronyms	
Abbreviations / Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security Protocol
EAP-TTLS	EAP-Tunneled Transport Layer Security Protocol
FIPS 140-2	Federal Information Processing Standard Publication 140-2
IKE	Internet Key Exchange Protocol
IP	Internet Protocol
IPSec	IP Security Protocol
IT	Information Technology
LAN	Local Area Network
NTP	Network Time Protocol
MAC	Media Access Control
MU	Mobile Unit, used interchangeably with wireless client
PEAP	Protected Extensible Authentication Protocol
SSH	Secure Shell Protocol
TLS	Transport Layer Security Protocol
Triple DES	Triple Data Encryption Standard
WLAN	Wireless Local Area Network
WLAN AS PP	US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.1, July 2007.

Table 24 - CC Related Acronyms	
Acronym	Acronym Description
CAP	Composed Assurance Package
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
DAC	Discretionary Access Control
DOD	Department of Defense
DOD	See DOD
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

9 References

Table 25 - TOE Guidance Documentation		
Reference	Description	Control Number
[1]	AP-7131N-FGR Access Point Product Reference Guide	72E-161311-01 Rev B
[2]	AP-7131N-FGR Access Point Installation Guide	72E-161312-01 Rev B
[3]	Motorola RFS7000GR Series RF Switch WiNG System Reference Guide	72E-161314-01 Rev B
[4]	Motorola RFS7000GR Series RF Switch CLI Reference Guide	72E-161313-01 Rev B
[5]	Motorola RFS7000GR Series RF Switch Installation Guide	72E-161315-01 Rev B

Table 26 - Common Criteria v3.1 References			
Reference	Description	Version	Date
[7]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2009-07-001	V3.1 R3	July 2009
[8]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components CCMB-2009-07-002	V3.1 R3	July 2009
[9]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components CCMB-2009-07-003	V3.1 R3	July 2009
[10]	Common Criteria for Information Technology Security Evaluation Evaluation Methodology CCMB-2009-07-004	V3.1 R3	July 2009

Table 27 – Supporting Documents			
Reference	Description	Version	Date
[12]	NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revised)	---	March, 2007
[13]	NIST Special Publication 800-56 Recommendation On Key Establishment Schemes, [http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf].	Draft 2.0	January 2003
[14]	NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography		March, 2007
[15]	Motorola AP-7131N Wireless Access Point Security Target	1.68	March 2014

MOTOROLA SOLUTIONS

Motorola AP-7131N Wireless Access Point Security Target

Document Version
Version: 1.68
2014-03-11

Prepared For:

InfoGard Laboratories, Inc.
709 Fiero Lane, Suite 25
San Luis Obispo, Ca 93401

Prepared By:
Gordon McIntosh and Rob Day
.

Notices:

Table of Contents

Tables

Figures

1 Security Target (ST) Introduction

The structure of this document is defined by CC v3.1r3 Part 1 Annex A.2, “Mandatory contents of an ST”:

- Section 1 contains the ST Introduction, including the ST reference, Target of Evaluation (TOE) reference, TOE overview, and TOE description.
- Section 2 contains conformance claims to the Common Criteria (CC) version, and package claims.
- Section 3 contains the security problem definition, which includes threats, Organizational Security Policies (OSP), and assumptions that must be countered, enforced, and upheld by the TOE and its operational environment.
- Section 4 contains statements of security objectives for the TOE, and the TOE operational environment as well as rationale for these security objectives.
- Section 5 contains definitions of any extended security requirements claimed in the ST.
- Section 6 contains the security function requirements (SFR), the security assurance requirements (SAR), as well as the rationale for the claimed SFR and SAR.
- Section 7 contains the TOE summary specification, which includes the detailed specification of the IT security functions

1.1 Security Target Reference

The Security Target reference shall uniquely identify the Security Target.

ST Title: Motorola AP-7131N Wireless Access Point Security Target
ST Version Number: Version 1.68
ST Author(s): Gordon D McIntosh and Rob Day
ST Publication Date: 2014-03-11

Keywords: Wireless

1.2 Target of Evaluation Reference

The Target of Evaluation reference shall identify the Target of Evaluation.

TOE Developer	Motorola Solutions, Inc. 6480 Via Del Oro San Jose, CA, 95119
TOE Name:	Motorola AP-7131N Wireless Access Point
TOE Software Version:	4.0.4.0-045GRN
TOE Hardware Version	AP-7131N-66040-FGR Rev. D (US Only) AP-7131N-66040-FWW Rev. F (Worldwide use, except US)

1.3 Target of Evaluation Overview

1.3.1 TOE Product Type

The TOE is classified as a Wireless Access Point device; a hardware device used to provide secure Wireless Local Area Network (WLAN) connectivity between a set of wireless client devices and a wired network.

1.3.2 TOE Usage

The intended usage of the TOE is to manage inbound and outbound traffic between a set of wireless client devices and a wired network.

1.3.3 TOE Major Security Features Summary

- Security Audit
  - Reports security relevant events to allow system administrators to detect, review, and analyze potential security violations.
- Cryptographic Support
  - Provides the underlying mechanisms to protect TSF code, TSF data, and user data as it is transmitted within the TOE
- User data protection
  - Provides secure user data transmission, and residual data protection mechanisms
- Identification and Authentication for administrators
  - Mandates authorized administrators to be uniquely identified and authenticate before accessing information stored on the system
- Security Management
  - Provides system administrators tools to manage the security features provided by the TOE
- Protection of the TSF
  - Provides accurate time reference, and self-test functions.
- TOE Access
  - Provides session control and access banner display.
- Trusted Path/Channels
  - Provides secure transmission of data to/from trusted entities in the IT environment
- Intrusion Detection
    - Rogue Access Point (AP) Detection
      - Provides detection of rogue access points that constitute threats to the TOE

1.3.4 TOE IT environment hardware/software/firmware requirement summary

The TOE IT operational environment is required to provide support for TOE security functions as follows:

- Audit (Syslog) Server
    - Provides the capability to store and protect audit information
    - Provides the capability to selectively view audit information
- RADIUS (AAA) Server
    - Provides external source for administrative and wireless user authentication
- NTP Server
    - Provides reliable time stamps
- LDAP Server
    - Provides external source for user database information and user authentication
- SFTP Server
    - Provides repository for backing up configuration files
- SNMP Server (Manager)
    - Provides a source for SNMP management and destination for SNMP Traps
    - Requires the use of a MIB browser or equivalent SNMP Management software

1.4 Target of Evaluation Description

This section describes the TOE physical and logical boundaries; the physical boundaries describe the TOE hardware, software and the related guidance documentation; the logical boundary describes what logical security features are included in the TOE.

The TOE, the Motorola AP-7131N Access Point, is a device that manages inbound and outbound traffic on a 802.11a/b/g/n wireless network; it is used to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices. The module protects data exchanged with wireless client devices using IEEE 802.11i wireless security protocol. The TOE has one (1) physical LAN port supporting two (2) unique LAN interfaces, one (1) physical WAN port, one (1) serial port, six (6) LEDs, one (1) reset button and six (6) antennas.

The evaluation covers two models of the AP-7131N, the AP-7131N-66040-FGR Rev. D and the AP-7131N-66040-FWW Rev. F; both are shipped with identical software, version 4.0.4.0-045GRN. The two models are identical except that the radio frequency bands of the FGR are preconfigured for use in the USA only; the radio frequency bands of the FWW are configurable for all supported countries except the USA. The differences between the two models are limited to the frequency bands supported and the menu used to select the country of use; all security functions are identical. The software detects the model on startup.

The TOE supports two deployment options, a standalone deployment and a Mesh deployment. In the standalone deployment, all AP-7131Ns are connected directly to the LAN and/or WAN wired networks. Wireless users connect to the AP via the 802.11a/b/g/n wireless communication link.

In a Mesh deployment, only one AP-7131N must be connected directly to the LAN and/or WAN wired network; this AP is configured as a base bridge. Another AP-7131, configured as a client bridge, can connect to the wired network through the base bridge via 802.11a/b/g/n wireless communication link. An AP-7131N can be configured as both base bridge and client bridge, allowing the AP to act as a repeater; the Mesh configuration supports as many as three repeaters connected in series. All client and base bridges are capable to serve as fully functional APs, connecting to wireless users via 802.11a/b/g/n. Each client bridge must authenticate itself to the corresponding base bridge using Pre-Shared Keys (PSK).

In Figure 1 - Typical TOE Standalone deployment diagram, the following features are shown:

- Wireless clients connected via 802.11a/b/g/n
- Local administration connected via RS-232
    - Access to management functions via Command Line Interface (CLI)
- Remote administration connected by LAN
    - May also connect via the WAN port (not shown)
    - Supports
        - SSHv2 access to management functions via Command Line Interface (CLI)
        - HTTPS access to Java based Web UI management functions via web browser
            - Requires TLSv1.0 support
        - SNMPv3 access to limited management functions
- Requires the following support from the IT Environment
    - SFTP server connected via SSHv2
    - NTP Server connected via IPsec tunnel
    - Audit (Syslog) Server tunnel connected via IPsec tunnel
    - RADIUS (AAA) Server connected via IPsec tunnel
    - LDAP Server connected via IPsec tunnel
    - SNMP Server (Manager) using SNMPv3
        - Shown as Remote Administration

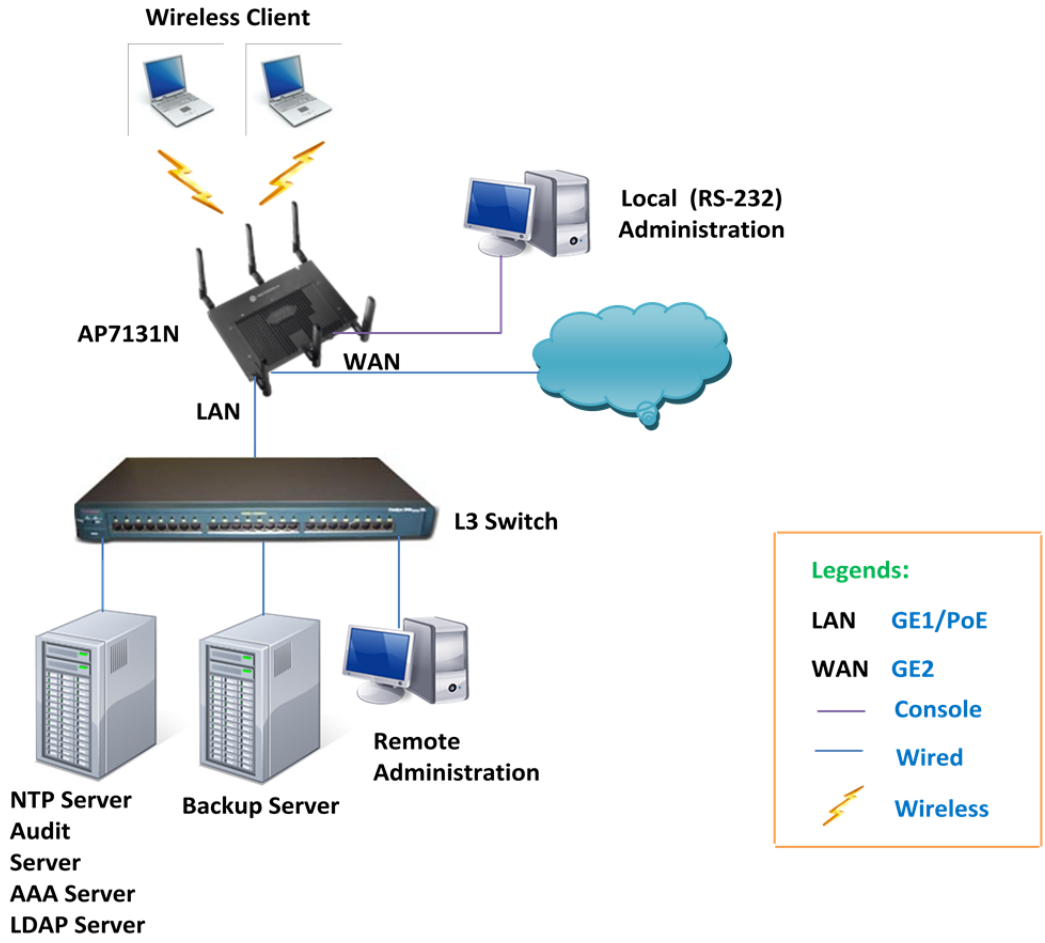


Figure 1 - Typical TOE Standalone deployment diagram

In Figure 2 - Typical TOE Mesh deployment diagram, the following features are shown:

- Mesh base bridge showing RS-232, LAN, and WAN wired connections, with
  - Wireless clients and client bridge connected via 802.11a/b/g/n (three levels)
- Local administration connected via RS-232
  - Access to management functions via Command Line Interface (CLI)
- Remote administration connected by LAN
  - May also connect via the WAN port (not shown)
  - Supports
    - SSHv2 access to management functions via Command Line Interface (CLI)
    - HTTPS access to Java based Web UI management functions via web browser
      - Requires TLSv1.0 support
    - SNMPv3 access to limited management functions
- Requires the following support from the IT Environment
  - SFTP server connected via SSHv2
  - NTP Server connected via IPsec tunnel
  - Audit (Syslog) Server tunnel connected via IPsec tunnel
  - RADIUS (AAA) Server connected via IPsec tunnel
  - LDAP Server connected via IPsec tunnel
  - SNMP Server (Manager) using SNMPv3

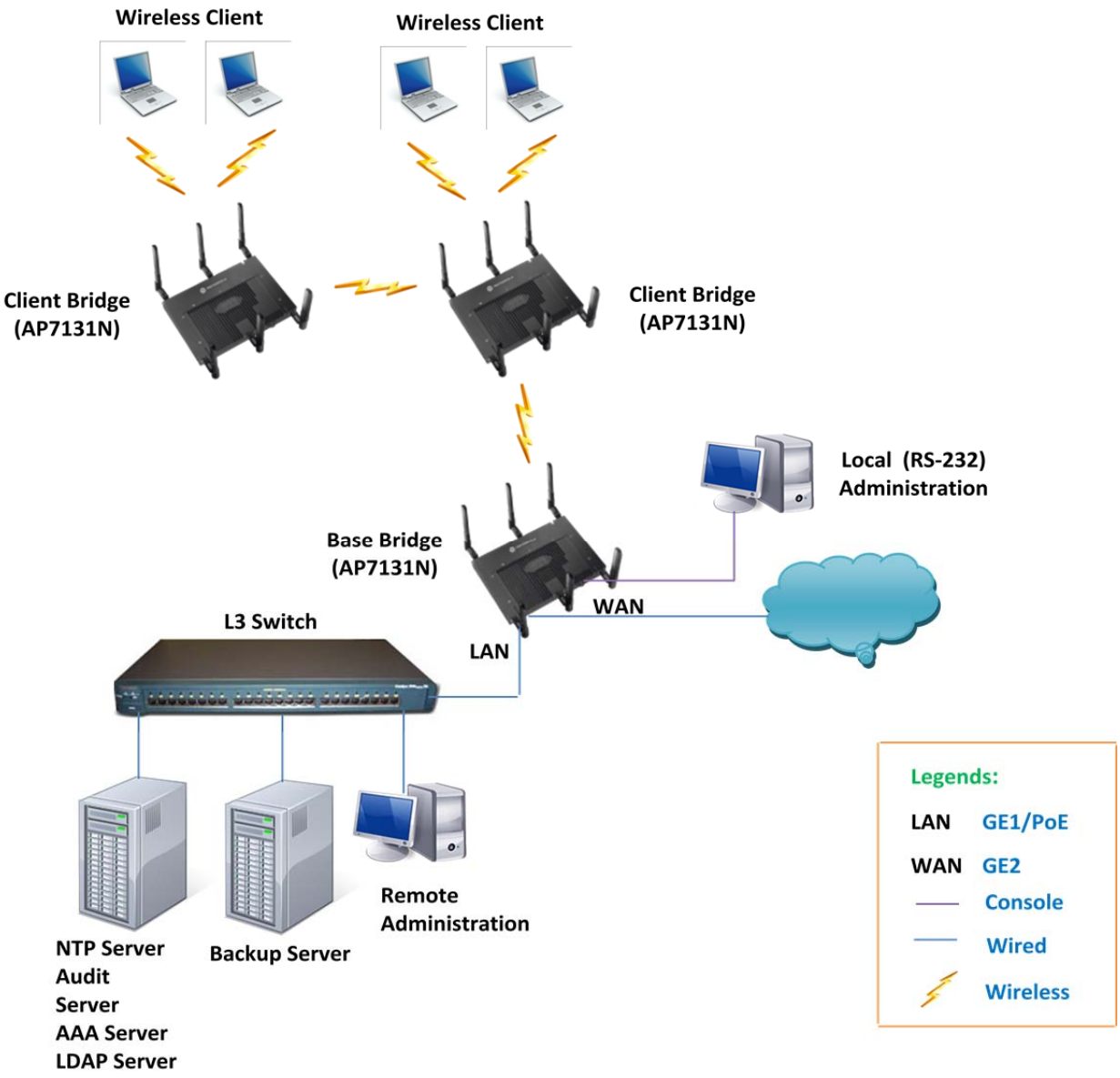


Figure 2 - Typical TOE Mesh deployment diagram

As shown in Figure 1 and Figure 2, the TOE supports local and remote management options. Not shown in these figures is remote management in the “Adaptive” mode from a Motorola RFS-7000 switch. This is specifically not shown as it is not part of the evaluated configuration; however, it is mentioned here for completeness, allowing this Security Target be referenced from other security targets supporting the feature.

In the adaptive mode, the AP-7131N interacts with a RFS-7000 switch; receiving configuration data from the RFS-7000, allowing the RFS-7000 manage the AP-7131N remotely.

1.4.1 TOE LAN/WAN/WLAN Interfaces

The TOE supports the following LAN, WAN, and WLAN interfaces:

- LAN port - The physical interface provided to connect a physical wire to the AP LAN. The access point has one LAN (GE1/POE) port with a single MAC address.

- WAN port - The physical interface provided to connect a physical wire to the AP WAN. The access point has one WAN (GE2) port with a single MAC address.
- WLAN port - There is not a physical connector associated with the WLAN port; this represents the physical radio antenna(s) for the WLAN.

The TOE physical LAN port supports two (2) logical LAN interfaces, LAN1 and LAN2. Each can be configured separately as outlined in [1], Section 5.1.2 Configuring LAN1 and LAN2 Settings. References to the LAN interface are a generic reference to either LAN1 or LAN2

The TOE physical WAN port supports the WAN interface. For detailed information on configuring the WAN interface see [1], Section 5.2 Configuring WAN Settings.

The TOE supports sixteen (16) logical WLAN interfaces on each access point, each identified with a unique ESSID. For detailed information on configuring the WLAN interfaces see [1], Section 5.3, Enabling Wireless LANs (WLANs).

1.4.1.1 Target of Evaluation Physical Boundaries

The TOE is delivered as an appliance, which includes a set of general-purpose and network processors that execute the internal TOE software, as well as volatile and non-volatile storage components. The physical boundary of the TOE is composed of a metal and hard plastic case with tamper-evident seals.

The TOE physical boundary includes a set of network Ethernet ports used to provide network connectivity, a serial console port used for local administration, a set of status LEDs as well as a power port used to provide a source of external electric power.

1.4.1.2 TOE Guidance Documentation

The TOE guidance documentation delivered is listed in Section 9, “References,” within Table 25 - TOE Guidance Documentation.

1.4.2 Target of Evaluation Logical Boundaries

The logical boundaries of the TOE include those security functions implemented exclusively by the TOE. These security functions were summarized in Section 1.3.3 above and further described in the following subsections. A more detailed description of the implementation of these security functions is provided in Section 7, “TOE Summary Specification.”

1.4.2.1 Audit services

The TOE has the ability to selectively generate audit records from potentially security relevant events and transmit these records to the audit server in the environment. The TOE is dependent on the audit server for the storage, the tools to review audit logs, the protection of audit logs from overflow, and the restriction of access to audit logs. The network connection between the TOE and the external audit server must be secured using IPSec security protocol. Audit information generated by the TOE includes date and time of the event, user who caused the event to be generated (if known), and other event specific data.

1.4.2.2 Cryptographic services

The TOE provides cryptographic mechanisms to protect TSF code and data, including mechanisms to encrypt, decrypt, hash, digitally sign data, and perform cryptographic key agreement. The evaluated configuration uses NIST CAVP compliant cryptographic algorithms.

1.4.2.3 User data protection

The TOE protects user data, i.e., only that data exchanged with wireless client devices, using the IEEE 801.11i standard wireless security protocol, mediates the flow of information passing to and from the WAN port, and ensures that resources used to pass network packets through the TOE do not contain any residual information.

1.4.2.3.1 Firewall Function

The TOE Security Function Policies (SFPs) allow an administrator to specify rules that are used to mediate the flow of information (network packets) to implement firewall functions comprised of pre-configured filters, subnet access filters, content filters, and IP filters. Additionally, network address translation and stateful packet inspection are provided.

The firewall pre-configured filters are able to screen information packets for known types of system attacks. Some of the access point's filters are pre-configured for well-known attacks; others are configurable by the administrator to allow custom rules for each deployment.

The firewall subnet access allows an authorized administrator to control access between LAN1, LAN2 and WAN interfaces based on an administrator-defined rule set. Additionally, the firewall implements advanced subnet access that allows the authorized administrator to define complex access rules and filtering.

Content filtering allows authorized administrators to block specific commands and URL extensions from going out through the access point's WAN port; capabilities include block outbound specific HTTP[1] commands, disable or restrict specific kinds of SMTP traffic, and disable or restrict specific kinds of FTP traffic.

The TOE enforces IP filtering rules on packets flowing on the access point's LAN1 or LAN2 interfaces and within any of the 16 access point WLANs based on an administrator-defined rule set.

These firewall functions are implemented using the TOE defined policies, the Traffic Filter SFP and the Unauthenticated TOE Services SFP.

For administrative users, TSF mediation is in accordance with the Unauthenticated TOE Services SFP. For wireless users, TSF mediation is in accordance with the Traffic Filter SFP.

The Traffic Filter SFP allows authenticated wireless users to pass information through the TOE. The TSF mediation occurs before & after the WLAN authentication action:

- The flow mediation that occurs before the WLAN authentication for the wireless users is to drop (implicit deny) any packets from unauthenticated wireless users. This rule is default, i.e. all unauthenticated traffic is dropped.
- The flow mediation that occurs after the WLAN authentication is to filter traffic according to the rules defined by the authorized administrator.

The Unauthenticated TOE Services SFP is used to express how the TOE enforces rules concerning network traffic that is destined for the TOE, and the protocols that are allowed.

These policies are composed of rules that dictate requirements to be satisfied to pass network packets; for each rule, if the requirement is met, it is considered to have passed otherwise it is failed. The combination of the rules allows for a branching of processing based on passes and failures. At the conclusion of the evaluation of all rules that make up a policy, the policy is considered to have passed if there was a branch through the processing of the policy that passed. If, and only if, the policy passes, the packet is allowed to pass through the TOE.

The rules can be based on the packet protocol validity, and/or specific elements in the packet contents such as presumed address of source subject, presumed address of destination subject, transport layer protocol, and the TOE interface on which traffic arrives and departs.

[1] HTTP port 80 only

1.4.2.4 Identification and Authentication

The TOE requires the system administrators be authenticated before access to the TOE is granted; administrators may login to the TOE via a local RS-232 connection, and remotely via SSH, or HTTPS. Additionally the TOE supports limited administration via SNMP. Administrators may connect to the TOE remotely via the LAN, WAN, or 802.11a/b/g/n interfaces.

Administrators may be authenticated locally using a local database, or may be authenticated using a remote RADIUS server. Twenty-five (25) local administrative accounts are supported with one (1) default account that has a fixed username and an initial password; the initial password is required to be changed at first use. The other twenty-four (24) local accounts may be added to the local database using the default account. An unlimited number of remote administrative accounts are supported using a remote RADIUS server.

The TOE requires the SNMP administrator be authenticated using a username and password before access to the TOE is granted; all SNMP administrator authentication is done locally. Prior to any SNMP access being allowed, the SNMP administrators' access must be configured by the administrator via the CLI or Web UI; SNMP administrators can be added or deleted as required by the administrator.

The TOE requires wireless users and Mesh connected APs to authenticate before access to the wired network is granted by the TOE; authentication of wireless users may be performed locally using manual Pre-Shared Key (PSK), or using IEEE 802.1X EAP-TLS, EAP-TTLS and EAP-PEAP authentication protocols. Authentication of Mesh connected APs must use manual PSKs.

For manual PSK, a 256-bit key is used for authentication as well as generating the encryption key to encrypt the data stream; therefore, only wireless users and mesh connected APs possessing the key may access the network. This key is entered manually as a string of 64 hexadecimal digits.

For IEEE 802.1X EAP, authentication may use a local RADIUS server using a local user database, a local RADIUS server using a remote LDAP user database, or utilize services of an external RADIUS authentication server.

1. Local RADIUS Server for 802.1x EAP authentication using local user database supports
   a. EAP-TLS,
   b. EAP-TTLS (MD5, PAP and MSCHAP-V2), or
   c. EAP-PEAP (GTC and MSCHAP-V2)
2. Local RADIUS Server for 802.1x EAP authentication using remote LDAP user database supports
   a. EAP-TTLS (PAP), or
   b. EAP-PEAP (GTC)

The TOE limits the number of failed authentication attempts by an administrative user via a remote interface to three (3); then the interface is disabled. If the SSH interface or Web UI interface is disabled, the local RS-232 CLI must be used to re-enable the interface.

1.4.2.5 Security Management

The management of the security relevant parameters of the TOE is performed by the authorized administrator; the TOE provides the following management interfaces:

- Command Line Interface (CLI) via
  - Local RS-232 console connection,
  - Remote SSH interface via the LAN, WAN ports, and 802.11 wireless interface
- Remote HTTPS JAVA based Web UI via the LAN, WAN ports, and 802.11 wireless
- Remote SNMPv3 interface via the LAN, WAN ports, and 802.11 wireless

Additionally, configuration files may be imported to or exported from the TOE via a SFTP client interface that requires the support of the SFTP Server in the IT Environment; this is not considered a direct management interface.

Finally, as mentioned in Section 1.4, “Target of Evaluation Description”, the TOE supports an “Adaptive” mode that is not a part of the evaluated configuration; but will be evaluated in a separate evaluation. In the adaptive mode, the AP-7131N adopts to a RFS-7000 switch to obtain configuration data, thus providing an additional management interface. When operating in adaptive mode, all other management interfaces are unchanged.

The locally connected CLI provides an interface for all management functions; the remote SSH CLI supports all management functions except remove remote session (Web UI and SSH) locks; the Web UI supports all commands accessible via Console CLI except the following:

- Rmlock command,
- Export/import of certificates
- Transfer_keys command

The SNMPv3 interface supports a limited set of administrative functions; these allow an administrator to manage network performance, find and solve network problems, plan for network growth, and gather information from its network components.

1.4.2.6 TOE Access

There are two sets of advisory/warning messages displayed before establishing a user session; both are displayed before the login/password prompt. The first message displayed before the login prompt is: “This Device is running in Common Criteria Mode,” and cannot be changed by the administrator.

The second message displayed before the login prompt can be changed by the administrator and can have a length between 10 and 1024 characters.

The TOE terminates administrative sessions after an administrator configurable time interval of inactivity is reached for SSH, Local CLI, and Web UI sessions; additionally, wireless user sessions will also be terminated after an administrator configurable time interval of wireless user inactivity.

1.4.2.7 Trusted Path / Channels

The TOE provides trusted paths for authentication functions, communications to remote audit server, NTP functions, and the import/export of configuration files for management

1.4.2.8 Intrusion Detection (Rogue Access Point)

The TOE provides rogue AP detection, i.e., any unauthorized active AP operating within the radio coverage of an authorized AP. When a rogue-AP is detected, the administrative user is notified with a SNMP trap and a syslog message.

1.4.2.9 Protection of the TSF

The TOE identification and authentication security functions allow only authenticated administrative users direct access to the TOE; wireless users can only authenticate to the TOE and then pass traffic though the TOE, i.e., wireless users are not allowed to execute instructions on the TOE.

Authenticated administrative users are allowed to login via the CLI and Web UI to access all management functions; additionally, authenticated SNMP administrators are allowed access to limited administrative functions. These management interfaces do not allow administrative users access to the underlying operating system and there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

All remote interfaces to the TOE are protected by secure channels; however, the TOE and its underlying hardware and firmware are required to be physically protected from unauthorized access.

The TOE has the capability to obtain reliable time from a remote Network Time Protocol (NTP) Server to provide reliable time stamps for audit services. Additionally, the system administrator can manually set

the time (maintained locally in the hardware Real Time Clock (RTC)) on the TOE using the Web UI or CLI management interfaces.

The TOE provides the capability to run a set of self-tests on power-on and on demand to verify the correct operation of the TOE's underlying hardware, TOE software and cryptographic modules. Additional cryptographic tests are performed during normal operation. The security of network data is maintained by zeroizing the memory location corresponding to a network packet, after the packet has been processed by the TOE.

The combination of physical protection by the environment, restriction of direct access to the TOE to authenticated administrative users, having no general-purpose computing resources on the TOE, and securing all remote interfaces with secure communications channels, provide sufficient protections such that the TSF cannot be bypassed, corrupted, or otherwise compromised.

1.5 Roles, User Data, and TSF Data

The TOE supports the following roles:

1. Administrators[2]
    a. Regular Administrators
        a) Privileged local or remote system administration
        b) The only user (along with 'admin' superuser) allowed direct access to the TOE security relevant interfaces
    b. 'admin' superuser
        a) In addition to regular administrator functions, can also manage other regular administrators' accounts
2. SNMP administrator
    a. Limited, remote administrative access
3. Wireless user
    a. Wireless users can pass data through the TOE but do not have direct access

User data is any data that passes through the TOE; it does not affect the operation of the TSF.

TSF data includes the following:

- System configuration information
- Security attributes belonging to the administrator
    - authentication credentials (password)
- Security attributes belonging to the SNMP administrator
    - authentication credentials (username, password)
- Wireless user identification credentials (username, password)
- Cryptographic certificates and keys
- Audit data

1.6 Notation, formatting, and conventions

The notation, formatting, and conventions used in this security target are defined below; these styles and clarifying information conventions were developed to aid the reader.

Where necessary, the ST author has added application notes to provide the reader with additional details to aid understanding; they are italicized and usually appear following the element needing clarification.

The notation conventions that refer to iterations, assignments, selections, and refinements made in this security target are in reference to SARs and SFRs taken directly from CC Part 2 and Part 3 as well as any SFRs and SARs taken from a protection profile.

[2] Throughout the Security Target, the term "administrators" includes both Regular Administrators and the 'admin' superuser, unless otherwise noted.

The CC permits four component operations: assignment, iteration, refinement, and selection to be performed on requirement components. These operations are defined in Common Criteria, Part 1; paragraph 6.4.1.3.2, “Permitted operations on components” as:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

Iterations made by the ST author are indicated by a number in parenthesis following the requirement number, e.g., FIA_UAU.1.1 (1); the iterated requirement titles are similarly indicated, e.g., FIA_UAU.1 (1).

Assignments made by the ST author are identified with ***bold italics;*** selections are identified with **bold text.**

Refinements made by the ST author are identified with "**Refinement:**" right after the short name; the refined text indicated by underlined text; any refinement that performs a deletion in text is noted in the endnotes sections indicated.

2 Conformance Claims

2.1 Common Criteria Conformance Claims

This Security Target is conformant to the Common Criteria Version 3.1r3, CC Part 2 extended [8], and CC Part 3 [9].

2.2 Conformance to Security Packages

This Security Target does not claim conformance to any security function requirements package, neither as package-conformant or package-augmented.

This Security Target is Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2.

3 Security Problem Definition

3.1 Threats

The following subsections define the security threats for the TOE, characterized by a threat agent, an asset, and an adverse action of that threat agent on that asset

3.1.1 Threats countered by the TOE and TOE IT Environment

Table 1 - Threats countered by the TOE and TOE IT Environment

#	Threat	Description
1	T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
2	T.ACCIDENTAL_CRYPTO_COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
3	T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
4	T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
5	T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
6	T.POOR_TEST	The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
7	T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
8	T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
9	T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
10	T.UNAUTHORIZED_ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
11	T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.
12	T.UNAUTH_ACCESS_POINT	An attacker may place an unauthorized AP in the radio coverage area of a 802.11 wireless network allowing the attacker to remotely access or attack the network, or configure the unauthorized AP to appear like an authorized AP, giving the attacker access to the Wireless Client's data.

3.2 Organizational Security Policies

3.2.1 Organizational Security Policies for the TOE

Table 2 - Organizational Security Policies for the TOE and TOE IT Environment		
#	OSP	Description
1	P.ACCESS_BANNER	The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
2	P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
3	P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
4	P.CRYPTOGRAPHY_VALIDATED	Only NIST CAVP validated cryptographic algorithms are acceptable for key generation and key agreement, and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
5	P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
6	P.NO_AD_HOC_NETWORKS	In accordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.

3.3 Assumptions on the TOE Operational Environment

This section describes the assumptions that are made on the operational environment in which the TOE is intended to be used in order to be able to provide security functionality. It includes information about the physical, personnel, and connectivity aspects of the environment. The operational environment must be managed in accordance with the provided guidance documentation. The following subsections define specific conditions that are assumed to exist in an environment where the TOE is deployed.

3.3.1 Assumptions on Physical Aspects of the Operational Environment:

The TOE is intended for application in areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

Table 3 - Assumptions on Physical Aspects of the Operational Environment	
Assumption	Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment

3.3.2 Assumptions on Personnel Aspects of the Operational Environment

Table 4 - Assumptions on Personnel Aspects of the Operational Environment	
Assumption	Description
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.

3.3.3 Assumptions on Connectivity aspects of the Operational Environment:

Table 5 - Assumptions on Connectivity Aspects of the Operational Environment	
Assumption	Description
A.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 6 - Security Objectives for the TOE		
#	TOE Objective	Description
1	O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
2	O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
3	O.CONFIGURATION_IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.
4	O.CORRECT_TSF_OPERATION	The TOE will provide the capability to verify the correct operation of the TSF.
5	O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE.
6	O.CRYPTOGRAPHY_VALIDATED	The TOE will use NIST CAVP validated crypto algorithms for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.
7	O.DISPLAY_BANNER	The TOE will display an advisory warning prior to establishing an administrator session regarding use of the TOE prior to permitting the use of any TOE services that requires authentication.
8	O.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.
9	O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
10	O.MEDIATE	The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.
11	O.PARTIAL_FUNCTIONAL_TESTING	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
12	O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
13	O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
14	O.TIME_STAMPS	The TOE shall obtain reliable time stamps.
15	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
16	O.VULNERABILITY_ANALYSIS	The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.
17	O.ROGUE_AP_DETECTION	The TOE shall provide security functions to detect an unauthorized AP operating in the radio coverage area of the 802.11 wireless network as well as generate notifications to the administrator when detected.

4.1.1 Rationale for the Security Objectives for the TOE

4.1.1.1 Mappings of TOE Security Objectives to Threats and OSP

The following table shows the mapping of security objectives for the TOE to threats countered by that objective and/or the OSP enforced by that objective.

Table 7 - Mapping of TOE Security Objectives to Threats and OSP

		Threats												OSP					
#	TOE Objective	T.ACCIDENTAL_ADMIN_ERROR	T.ACCIDENTAL_CRYPTO_COMPROMISE	T.MASQUERADE	T.POOR_DESIGN	T.POOR_IMPLEMENTATION	T.POOR_TEST	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.UNAUTH_ADMIN_ACCESS	T.UNAUTH_ACCESS_POINT	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.CRYPTOGRAPHIC	P.CRYPTOGRAPHY_VALIDATED	P.ENCRYPTED_CHANNEL	P.NO_AD_HOC_NETWORKS
1	O.ADMIN_GUIDANCE	X										X							
2	O.AUDIT_GENERATION														X				
3	O.CONFIGURATION_IDENTIFICATION				X	X													
4	O.CORRECT_TSF_OPERATION						X												
5	O.CRYPTOGRAPHY															X	X	X	
6	O.CRYPTOGRAPHY_VALIDATED																X	X	
7	O.DISPLAY_BANNER													X					
8	O.DOCUMENTED_DESIGN				X		X												
9	O.MANAGE	X							X		X	X			X				
10	O.MEDIATE										X							X	X
11	O.PARTIAL_FUNCTIONAL_TESTING					X	X												
12	O.RESIDUAL_INFORMATION		X					X	X							X			
13	O.SELF_PROTECTION		X						X		X								
14	O.TIME_STAMPS														X				
15	O.TOE_ACCESS			X						X	X	X			X				
16	O.VULNERABILITY_ANALYSIS				X	X	X												
17	O.ROGUE_AP_DETECTION												X						

4.1.1.2 Security Objectives Rationale for Threats and OSP

This section presents the rationale that justifies the security objectives for the TOE is suitable to counter those threats to be countered by the TOE and justifies the security objectives are suitable to enforce the OSP.

O.ADMIN_GUIDANCE

O.ADMIN_GUIDANCE helps to mitigate the threats, T.ACCIDENTAL_ADMIN_ERROR and T.UNAUTH_ADMIN_ACCESS, by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the

mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure.

O.AUDIT_GENERATION

O.AUDIT_GENERATION addresses the policy, P.ACCOUNTABILITY, by providing the Administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.).

O.CONFIGURATION_IDENTIFICATION

O.CONFIGURATION_IDENTIFICATION plays a role in countering the threat, T.POOR_DESIGN, by requiring the developer to provide control of the changes made to the TOE's design documentation and the ability to report and resolve security flaws. It plays a role in countering the threat, T.POOR_IMPLEMENTATION, by requiring the developer to provide control of the changes made to the TOE's design. This ensures that changes to the TOE are performed in structure manner and tracked.

O.CORRECT_TSF_OPERATION

O.CORRECT_TSF_OPERATION plays a role in countering the threat, T.POOR_TEST, by providing assurance that the TSF continues to operate as expected in the field.

O.CRYPTOGRAPHY

O.CRYPTOGRAPHY satisfies the policies, P. CRYPTOGRAPHY and P.CRYPTOGRAPHY_VALIDATED, by requiring the TOE to implement NIST CAVP validated cryptographic algorithms. These algorithms will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. It satisfy the policy, P.ENCRYPTED_CHANNEL, by requiring the TOE to implement NIST CAVP validated cryptographic algorithms. These algorithms will provide confidentiality and integrity protection of TSF data while in transit to wireless clients that are authorized to join the network.

O.CRYPTOGRAPHY_VALIDATED

O.CRYPTOGRAPHY_VALIDATED satisfies the policy, P.CRYPTOGRAPHY_VALIDATED, by requiring that all cryptographic algorithms for cryptographic services be NIST CAVP validated. This will provide assurance that the NIST-approved security functions and random number generation will be in accordance with NIST and validated according the CAVP. It satisfy the policy, P.ENCRYPTED_CHANNEL, by requiring the TOE to implement NIST CAVP validated cryptographic algorithms. These algorithms will provide confidentiality and integrity protection of TSF data while in transit to wireless clients that are authorized to join the network.

O.DISPLAY_BANNER

O.DISPLAY_BANNER satisfies the policy, P.ACCESS_BANNER, by ensuring that the TOE displays an administrator configurable banner that provides all users with a warning about unauthorized use of the TOE. A banner will be presented for all TOE services that allow direct access to the TOE. In other words, it will be required for all administrative actions.

O.DOCUMENTED_DESIGN

O.DOCUMENTED_DESIGN counters the threat, T_POOR_DESIGN, to a degree by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development

understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered.

O.DOCUMENTED_DESIGN helps to counters the threat, T_POOR_TEST, by ensuring that the TOE's documented design satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE.

O.MANAGE

O.MANAGE contributes to mitigating the threat, T.ACCIDENTAL_ADMIN_ERROR, by providing administrators the capability to view and manage configuration settings. For example, if the administrator made a mistake when configuring the set of permitted users' authentication credentials, providing the capability to view the lists of authentication credentials affords them the ability to review the list and discover any mistakes that might have been made.

O.MANAGE mitigates the threat, T.TSF_COMPROMISE, by restricting access to administrative functions and management of TSF data to the administrator.

O.MANAGE mitigates the threat, T_UNAUTHORIZED_ACCESS, by restricting the ability to modify the security attributes associated with the TOE to the administrator. This objective ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

O.MANAGE mitigates the threat, T_UNAUTH_ADMIN_ACCESS, by restricting access to administrative functions and management of TSF data to the administrator

O.MEDIATE

O.MEDIATE mitigates the threat, T_UNAUTHORIZED_ACCESS, by ensuring that all network packets that flow through the TOE are subject to the information flow policies.

O.MEDIATE satisfies the policy, P. ENCRYPTED_CHANNEL, by allowing the TOE administrator to set a policy to encrypt all wireless traffic.

O.MEDIATE works to support the policy, P.NO_AD_HOC_NETWORKS, by ensuring that all network packets that flow through the TOE are subject to the information flow policies.

O.PARTIAL_FUNCTIONAL_TESTING

O.PARTIAL_FUNCTIONAL_TESTING helps mitigate the threat, T_POOR_DESIGN, by increasing the likelihood that any errors that do exist in the implementation will be discovered through testing.

O.PARTIAL_FUNCTIONAL_TESTING helps mitigate the threat, T_POOR_IMPLEMENTATION, by ensuring that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing.

O.RESIDUAL_INFORMATION

O.RESIDUAL_INFORMATION contribute to the mitigation of the threats, T.RESIDUAL_DATA T.ACCIDENTAL_CRYPTO_COMPROMISE, and T.TSF_COMPROMISE, by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.

O.RESIDUAL_INFORMATION satisfies the policy, P. CRYPTOGRAPHY, by ensuring that cryptographic data are securely cleared.

O.SELF_PROTECTION

O.SELF_PROTECTION contributes to the mitigation of the threat, T.ACCIDENTAL_CRYPTO_COMPROMISE by ensuring the TOE will have adequate protection from external sources and that all TSP functions are invoked.

O.SELF_PROTECTION contributes to the mitigation of the threat, T.TSF_COMPROMISE, by requiring the TOE be able to protect itself from tampering and that the security mechanisms in the TOE cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF data or TSF executables.

O.SELF_PROTECTION contributes to the mitigation of the threat, T.UNAUTHORIZED_ACCESS, by requiring the TOE require all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services.

O.TIME_STAMPS

O.TIME_STAMPS plays a role in supporting the policy, P.ACCOUNTABILITY, by requiring the TOE to provide a reliable time stamp (via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred.

O.TOE_ACCESS

O.TOE_ACCESS supports the policy P.ACCOUNTABILITY and helps mitigate the threats T.MASQUERADE, T.UNATTENDED_SESSION, T_UNAUTHORIZED_ACCESS, and T.UNAUTH_ADMIN_ACCESS by controlling logical access to the TOE and its resources. This objective ensures that users are identified and authenticated so that their actions may be tracked by the administrator.

O.VULNERABILITY_ANALYSIS

O.VULNERABILITY_ANALYSIS contributes to the mitigation of the threat, T.POOR_DESIGN, by ensuring that the TOE has been analyzed for obvious vulnerabilities and that any vulnerability found have been removed or otherwise mitigated, this includes analysis of any probabilistic or permutational mechanisms incorporated into a TOE claiming conformance to this ST.

O.ROGUE_AP_DETECTION

O.ROGUE_AP_DETECTION mitigates the threat, T.UNAUTH_ACCESS_POINT, by ensuring the TOE provide security functions to detect unauthorized APs operating in the radio coverage area of the 802.11 wireless network as well as generate notifications to the administrator when detected.

4.2 Security Objectives for the TOE Operational Environmental

Table 8 - Security Objectives for the TOE Operational Environmental		
#	Objective	Description
1	OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information and the authentication credentials.
2	OE.AUDIT_REVIEW	The IT Environment will provide the capability to selectively view audit information.
3	OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
4	OE.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
5	OE.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
6	OE.PHYSICAL	The environment provides physical security commensurate with the value of the TOE and the data it contains.
7	OE.PROTECT_MGMT_COMMS	The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE and time service in a manner that is commensurate with the risks posed to the network.
8	OE.RESIDUAL_INFORMATION	The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
9	OE.SELF_PROTECTION	The environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
10	OE.TIME_STAMPS	The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
11	OE.TOE_ACCESS	The environment will provide mechanisms that support the TOE in providing a user's logical access to the TOE.
12	OE.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

4.2.1 Rationale for the Security Objectives for the TOE Operational Environment

4.2.1.1 Mappings of Security Objectives to Threats, OSP, and Assumptions

Table 9 - Mapping of TOE Security Objectives to Threats, OSP, and Assumptions, shows the mapping of security objectives for the TOE operational environment to threats countered by that objective, the OSP enforced by that objective, and/or the assumption upheld by that objective.

Table 9 - Mapping of TOE Security Objectives to Threats, OSP, and Assumptions															
		Threats							OSP			Assumptions			
#	TOE Objective	T.ACCIDENTAL_ADMIN_ERROR	T.ACCIDENTAL_CRYPTO_COMPROMISE	T.MASQUERADE	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNAUTHORIZED_ACCESS	T.UNAUTH_ADMIN_ACCESS	P.ACCOUNTABILITY	P.ENCRYPTED_CHANNEL	P.NO_AD_HOC_NETWORKS	A.NO_EVIL	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TOE_NO_BYPASS
1	OE.AUDIT_PROTECTION								X						
2	OE.AUDIT_REVIEW								X						
3	OE.MANAGE					X	X	X							
4	OE.NO_EVIL	X						X				X			
5	OE.NO_GENERAL_PURPOSE	X											X		
6	OE.PHYSICAL													X	
7	OE.PROTECT_MGMT_COMMS									X					
8	OE.RESIDUAL_INFORMATION		X		X										
9	OE.SELF_PROTECTION		X			X	X								
10	OE.TIME_STAMPS								X						
11	OE.TOE_ACCESS			X			X		X						
12	OE.TOE_NO_BYPASS			X							X				X

4.2.1.2 IT Security Objectives Rationale for Threats and OSP, and Assumptions

This section presents the rationale that justifies the security objectives for the TOE operational environment is suitable to counter those threats to be countered by the TOE operational environment, justifies the security objectives are suitable to enforce the OSP and the assumptions are upheld by that objective.

OE.AUDIT_PROTECTION

OE.AUDIT_PROTECTION satisfies the policy, P.ACCOUNTABILITY, by providing protected storage of TOE and IT environment audit data in the environment.

OE.AUDIT_REVIEW

OE.AUDIT_REVIEW helps satisfy the policy, P.ACCOUNTABILITY, by supporting accountability mechanisms for viewing and sorting the audit logs

OE.MANAGE

OE.MANAGE helps mitigate the threat, T.TSF_COMPROMISE, by ensuring that the administrator can view security relevant audit events.

OE.MANAGE. helps mitigate the threat, T.UNAUTHORIZED_ACCESS, by restricting the ability to modify the security attributes associated with the TOE to the administrator. These objectives ensure that no other user can modify the information flow policy to bypass the intended TOE security policy.

OE.MANAGE helps mitigate the threat, T.UNAUTH_ADMIN_ACCESS, by restricting access to administrative functions and management of TSF data to the administrator.

OE.NO_EVIL

OE.NO_EVIL contributes to mitigating the threat, T.ACCIDENTAL_ADMIN_ERROR, by ensuring that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.

OE.NO_EVIL helps mitigate the threat, T.UNAUTH_ADMIN_ACCESS, by ensuring that the TOE administrators have guidance that instructs them in how to administer the TOE in a secure manner.

By ensuring sites using the TOE administrators are non-hostile, appropriately trained and follow all administrator guidance, the assumption A.NO_EVIL is addressed.

OE.NO_GENERAL_PURPOSE

OE.NO_GENERAL_PURPOSE mitigate the threat, T.ACCIDENTAL_ADMIN_ERROR, by ensuring that there can be no accidental errors due to the introduction of unauthorized software or data, by ensuring that there are no general-purpose or storage repository applications available on the TOE.

By ensuring the operational environment require there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE, the assumption A. NO_GENERAL_PURPOSE is addressed.

OE.PHYSICAL

By ensuring the operational environment provides physical security commensurate with the value of the TOE and the data it contains, the assumption A. PHYSICAL is addressed.

OE.PROTECT_MGMT_COMMS

OE.PROTECT_MGMT_COMMS helps to satisfy the policy, P.ENCRYPTED_CHANNEL, by providing that the audit records, remote network management information and authentication data will be protected by means of a protected channel in the environment.

OE.RESIDUAL_INFORMATION

OE.RESIDUAL_INFORMATION contributes to the mitigation of the threats, T.RESIDUAL_DATA and T.ACCIDENTAL_CRYPTO_COMPROMISE, by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.

OE.SELF_PROTECTION

OE.SELF_PROTECTION help mitigate the threats, T.ACCIDENTAL_CRYPTO_COMPROMISE and T.TSF_COMPROMISE by ensuring that the TOE IT environment will have protection similar to that of the TOE.

OE.SELF_PROTECTION contributes to the mitigation of the threat, T.UNAUTHORIZED_ACCESS, by requiring the TOE IT environment require all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services.

OE.TIME_STAMPS

OE.TIME_STAMPS supports the policy, P.ACCOUNTABILITY, by ensuring that the TOE IT environment provides time services.

OE.TOE_ACCESS

OE.TOE_ACCESS help mitigate the threats, T.MASQUERADE and T.UNAUTHORIZED_ACCESS by controlling logical access to the TOE and its resources.

OE.TOE_ACCESS supports the policy, P.ACCOUNTABILITY, by controlling logical access to the TOE and its resources.

This objective ensures that users are identified and authenticated so that their actions may be tracked by the administrator.

OE.TOE_NO_BYPASS

OE.TOE_NO_BYPASS helps mitigate the threat T.MASQUERADE, and supports the policy, P.NO_AD_HOC_NETWORKS, by ensuring that wireless clients must be configured to use the wireless access system for all information flowing between a wireless client and any other host on the network. If the clients are properly configured, any information passing through the TOE will be inspected to ensure it is authorized by TOE polices.

By ensuring the operational environment require wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE, the assumption A.TOE_NO_BYPASS is addressed.

5 Extended Components Definition

This section provides definition of the extended security functional and assurance requirements; the components that are CC Part 2 extended, and CC Part 3 extended, i.e., NIAP interpreted requirements, and extended requirements.

5.1 Extended Security Function Requirements Definitions

This section defines the extended security functional requirements for the TOE. The security functional requirement components defined in this security target are CC Part 2 extended.

Table 10 - TOE Security Functional Requirements CC Part 2 Extended

#	SFR	Description	Dependencies	Hierarchical to
1	FCS_BCM_(EXT).1	Baseline Cryptographic Module	None	None
2	FCS_CKM_(EXT).2	Cryptographic Key Handling and Storage	None	None
3	FCS_COMM_PROT_EXT.1	Communications Protection	None	None
4	FCS_COP_(EXT).1	Extended: Random Number Generation	None	None
5	FCS_HTTPS_EXT.1	HTTPS	None	None
6	FCS_SFTP_EXT.1	SSH File Transfer Protocol	FCS_SSH_EXT.1	None
7	FCS_SSH_EXT.1	SSH Protocol	None	None
8	FCS_TLS_EXT.1	TLS Protocol	None	None
9	FCS_IPSEC_EXT.1	Internet Protocol Security (IPSec)	None	None
10	FCS_EAP-TLS_EXT.1	EAP-TLS Authentication Protocol	FCS_TLS_EXT.1	None
11	FCS_EAP-TTLS_EXT.1	EAP-TTLS Authentication Protocol	FCS_TLS_EXT.1	None
12	FCS_PEAP_EXT.1	PEAP Authentication Protocol	FCS_TLS_EXT.1	None
13	FCS_RAD_EXT.1	RADIUS Authentication Protocol	FCS_IPSEC_EXT.1	None
14	FCS_SNMPv3_EXT.1	SNMPv3	None	None
15	FDP_PUD_(EXT).1	Protection of User Data	None	None
16	FIA_UAU_(EXT).1	Multiple authentication methods	None	None
17	FID_APD_EXT.1	Rogue Access Point Detection	None	None
18	FPT_STM_(EXT).1	Reliable Time Stamps	None	None
19	FPT_TST_EXT.1	TSF Testing	None	None
20	FPT_ITC_EXT.1	Inter-TSF Trusted Channel	None	None

5.1.1 Class FCS:

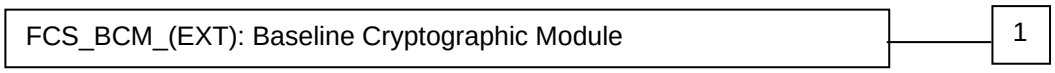
This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software. The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include, but are not limited to, identification and authentication, non-repudiation, trusted path, trusted channel and data separation.

5.1.1.1 FCS_BCM_(EXT) Baseline Cryptographic Module

Family Behavior

This family addresses requirements to use only certified cryptography to protect communications between the TSF, to separate parts of the TSF, and/or external IT entities.

Component leveling



FCS_BCM_(EXT).1 Baseline Cryptographic Module requires the TSF to use only cryptographic algorithms that have been validated by the NIST Cryptographic Algorithm Validation Program.

Management: FCS FCS_BCM_(EXT).1

There are no management activities foreseen.

Audit: FCS_BCM_(EXT).1

There are no auditable events foreseen.

5.1.1.1.1 FCS_BCM_(EXT).1 Baseline Cryptographic Module

Hierarchical to: None

Dependencies: None

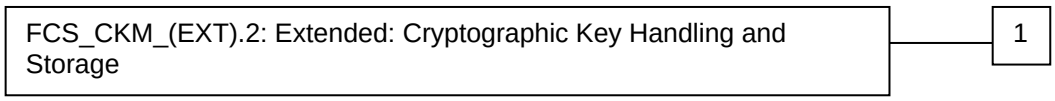
FCS_BCM_(EXT).1.1 All cryptographic functions implemented by the TOE shall be validated by NIST CAVP and include an algorithm validation certificate.

5.1.1.2 FCS_CKM_(EXT).2 Extended: Cryptographic Key Handling and Storage

Family Behavior

This family addresses requirements to use securely store and handle cryptographic keys.

Component leveling



FCS_CKM_(EXT).2: Extended: Cryptographic Key Handling and Storage requires the TSF to ensure keys are transferred properly, that they are stored securely, destroyed when no longer needed, and not archived when expired.

Management: FCS_CKM_(EXT).2

The following actions could be considered for the management functions in FMT:

Configuration of the inactivity timer.

Audit: FCS_CKM_(EXT).2

Basic: Error(s) detected during cryptographic key transfer.

5.1.1.2.1 FCS_CKM_(EXT).2 Extended: Cryptographic Key Handling and Storage

Hierarchical to: None

Dependencies: None

FCS_CKM_(EXT).2.1	The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).
Application Note:	*A parity check is an example of a key error detection check.*
FCS_CKM_(EXT).2.2	The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.
Application Note:	*A persistent key, such as a file encryption key, is one that must be available in the system over long periods of time. A non-persistent key, such as a key used to encrypt or decrypt a single message or a session, is one that is ephemeral in the system.*
Application Note:	*"When not in use" is interpreted in the strictest sense so that persistent keys only exist in plaintext form during intervals of operational necessity. For example, a file encryption key exists in plaintext form only during actual encryption and/or decryption processing of a file. Once the file is decrypted or encrypted, the file encryption key should immediately be covered for protection.*
Application Note:	*A "split knowledge procedure" is a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.*
FCS_CKM_(EXT).2.3	The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.
Application Note:	*The cryptographic administrator must have the ability to set a threshold of inactivity after which non-persistent keys must be destroyed in accordance with FCS_CKM.4.*
FCS_CKM_(EXT).2.4	The TSF shall prevent archiving of expired (private) signature keys.
Application Note:	*This requirement is orthogonal to typical system back-up procedures. Therefore, it does not address the problem of archiving an active (private) signature key during a system back-up and saving the key beyond its intended life span.*

5.1.1.3 FCS_COMM_PROT_EXT Communications Protection

Family Behavior

This family addresses requirements to use a cryptographic protocol to protect communications between the TSF, to separate parts of the TSF, and/or external IT entities.

Component leveling

FCS_COMM_PROT_EXT.1 Communications Protection requires the TSF provide either IPsec or SSH to provide communications security to separate parts of the TSF, and/or external IT entities; optionally, TLS/HTTPS may also be selected if implemented in the TSF.

Management: FCS_COMM_PROT_EXT.1

There are no management activities foreseen.

Audit: FCS_COMM_PROT_EXT.1

There are no auditable events foreseen.

5.1.1.3.1 FCS_COMM_PROT_EXT.1 Communications Protection

Hierarchical to: None

Dependencies: None

FCS_COMM_PROT_EXT.1.1 The TSF shall protect communications using [selection: *IPsec, SSH*] and [selection: *TLS/HTTPS, no other protocol*].

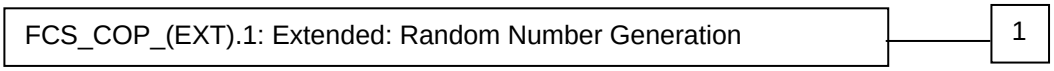
Application Note: *The intent of the above requirement is to use a cryptographic protocol to protect communications. Either IPsec or SSH is required; however, both may be selected if implemented by a conformant TOE. Additionally, TLS/HTTPS may be selected if that is implemented.*

5.1.1.4 FCS_COP_(EXT).1 Extended: Random Number Generation

Family Behavior

This family addresses requirements for suitable random number generators for the TOE.

Component leveling



FCS_COP_(EXT).1: Extended: Random Number Generation requires the TSF to use a NIST approved random number generator, and to ensure the RNG/PRNG sources are not tampered with.

Management: FCS_COP_(EXT).1

There are no management activities foreseen.

Audit: FCS_COP_(EXT).1

There are no auditable events foreseen.

5.1.1.4.1 FCS_COP_(EXT).1 Extended: Random Number Generation

Hierarchical to: None

Dependencies: None

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG [*assignment: one of the RNGs specified in FIPS 140-2 Annex C*] seeded by [*selection:*

(1) one or more independent hardware-based entropy sources, and/or
(2) one or more independent software-based entropy sources, and/or
(3) a combination of hardware-based and software-based entropy sources.]

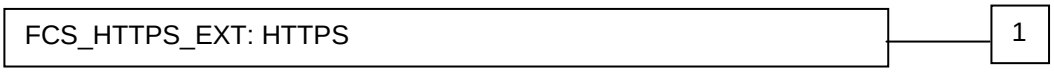
FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/pseudorandom number generation (PRNG) sources.

5.1.1.5 FCS_HTTPS_EXT HTTPS

Family Behavior

This family addresses the requirements for the use of HTTPS as a secure communications protocol.

Component leveling



FCS_HTTPS_EXT.1 HTTPS specifies conformance to the appropriate RFC and to the underlying transport protocol.

Management: FCS_HTTPS_EXT.1

There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

Basic: Failure to establish a HTTPS Session
Establishment and/or termination of a HTTPS session

5.1.1.5.1 FCS_HTTPS_EXT.1 HTTPS

Hierarchical to: None

Dependencies: None

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.1.1.6 FCS_SFTP_EXT SSH File Transfer Protocol

Family Behavior

This family addresses the requirements for the use of SFTP as a secure communications protocol.

Component leveling

FCS_SFTP_EXT: SSH File Transfer Protocol	1

FCS_SFTP_EXT.1 SSH File Transfer Protocol specifies conformance to the appropriate RFC and to the underlying transport protocol.

Management: FCS_SFTP_EXT.1

There are no management activities foreseen.

Audit: FCS_SFTP_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

Basic: Failure of the file transfer

5.1.1.6.1 FCS_SFTP_EXT.1 SSH File Transfer Protocol

Hierarchical to: None

Dependencies: FCS_SSH_EXT.1

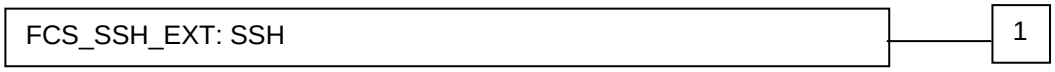
FCS_SFTP_EXT.1.1	The TSF shall implement the SSH File Transfer Protocol as specified in draft-ietf-secsh-filexfer-13.txt, July 10, 2006.
FCS_SFTP_EXT.1.2	The TSF shall ensure the SFTP connection has privacy and integrity features provided by the underlying SSH transport protocol as specified in FCS_SSH_EXT.1.

5.1.1.7 FCS_SSH_EXT SSH

Family Behavior

This family addresses the requirements for the use of SSH as a secure communications protocol.

Component leveling



FCS_SSH_EXT.1 SSH requires conformance to the appropriate RFCs and critical security parameters.

Management: FCS_SSH_EXT.1

The following actions could be considered for the management functions in FMT:
Setup of configurable security values

Audit: FCS_SSH_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

Basic: Failure to establish an SSH session
Establishment and/or termination of an SSH session

5.1.1.7.1 FCS_SSH_EXT.1 SSH Protocol

Hierarchical to: None

Dependencies: None

FCS_SSH_EXT.1.1	The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.
Application Note:	*The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.*
FCS_SSH_EXT.1.2	The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.
FCS_SSH_EXT.1.3	The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [*assignment: timeout period*], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [*assignment: maximum number of attempts*] attempts.
FCS_SSH_EXT.1.4	The TSF shall ensure that the SSH protocol implementation supports the password-based authentication method as described in RFC 4252.
FCS_SSH_EXT.1.5	The TSF shall ensure that, as described in RFC 4253, packets greater than [*assignment: number of bytes*] bytes in an SSH transport connection are dropped.
Application Note:	*RFC 4253 provides for the acceptance of "large packets" with the caveat that the packets should be of "reasonable length" or dropped. The assignment*

	should be filled in by the ST author with the maximum packet size accepted, thus defining "reasonable length" for the TOE.
FCS_SSH_EXT.1.6	The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [selection: AES-CBC-192, no other algorithms].
FCS_SSH_EXT.1.7	The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [*selection: SSH_DSS, PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms*], as its public key algorithm(s).
Application Note:	*RFC 4253 specifies required and allowable public key algorithms. This requirement makes SSH-RSA "required" and allows two others to be claimed in the ST. The ST author should make the appropriate selection, selecting "no other public key algorithms" if only SSH_RSA is implemented.*
FCS_SSH_EXT.1.8	The TSF shall ensure that data integrity algorithms used in SSH transport connection is hmac-sha1, and [*selection: hmac-sha1-96*, hmac-md5, hmac-md5-96, no other].
FCS_SSH_EXT.1.9	The TSF shall ensure that SSH supports diffie-hellman-group14-sha1 and [*selection*: *diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256, no other groups*] for key exchange.

5.1.1.8 FCS_IPSEC_EXT Internet Protocol Security (IPSec)

Family Behavior

This family addresses the requirements for the use of IPsec as a secure communications protocol.

Component leveling

FCS_IPSEC_EXT: Internet Protocol Security (IPsec)	1

FCS_IPSEC_EXT.1 IPsec requires conformance to the appropriate RFCs and critical security parameters.

Management: FCS_IPSEC_EXT.1

The following actions could be considered for the management functions in FMT:
Setup of configurable security values

Audit: FCS_IPSEC_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

Basic: Failure to establish an IPsec SA
Establishment and/or termination of an IPsec SA

5.1.1.8.1 FCS_IPSEC_EXT.1 Internet Protocol Security (IPSec)

Hierarchical to: None

Dependencies: None

FCS_IPSEC_EXT.1.1	The TSF shall implement IPsec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-192, AES-CBC-256, [selection: *no other algorithms, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*] and using IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109; [selection: *no other method, IKEv2 as defined in RFCs 4306, 4307*] to establish the security association.
Application Note:	*Support for AES-CBC-128 and AES-CBC-256 is required above; if AES-GCM-128 or AES-GCM-256 are supported then the appropriate selection should be made, otherwise select "no other algorithm".* *It is acceptable to refine this requirement for IKEv1 and/or IKEv2 to include RFC 4868 as optional claimed hash algorithms. If this is done, the ST author should adjust the appropriate FCS_COP.1 iteration accordingly.* *Support for IKEv1 is required above; if IKEv2 is supported then that selection should be made, otherwise select "no other method."* *The ST author must make the appropriate selections and assignments to reflect the IPsec implementation. The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.*

HMAC-SHA 1 is required by the RFCs as the hash algorithm used by the IKE implementation for CBC mode. If other hash algorithms are to be claimed, then either the requirement or the TSS section must identify those algorithms and the appropriate selections need to be made in the appropriate FCS_COP.1 iteration.

For IKEv1, the above requirement is to be interpreted as requiring the IKE implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109.

Suite B algorithms (RFC 4869) are the preferred algorithms for implementation.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

Application Note: *The above requirement can be accomplished either by providing Security Administrator-configurable lifetimes (with appropriate FMT requirements and instructions in documents mandated by AGD_OPE, as necessary), or by "hard coding" the limits in the implementation.*

FCS_IPSEC_EXT.1.4 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP)*, [*assignment: other DH groups that are implemented by the TOE], no other DH groups*].

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement Peer Authentication using the [selection: PSK, DSA, rDSA, ECDSA] algorithm.

Application Note: *The selected algorithm should correspond to an appropriate selection for the appropriate FCS_COP.1 iteration.*

FCS_IPSEC_EXT.1.6 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.

FCS_IPSEC_EXT.1.7 The TSF shall support the following:

1. Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "*", "(", and ")");
2. Pre-shared keys of [assignment: *supported lengths*].

5.1.1.9 FCS_TLS_EXT Transport Layer Security (TLS) protocol

Family Behavior

This family addresses the requirements for the use of TLS as a secure communications protocol.

Component leveling

FCS_TLS_EXT: Transport Layer Security (TLS)	1

FCS_TLS_EXT.1 TLS requires conformance to the appropriate RFCs and critical security parameters.

Management: FCS_TLS_EXT.1

The following actions could be considered for the management functions in FMT:
Setup of configurable security values

Audit: FCS_TLS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Basic: Failure to establish a TLS session
  Establishment and/or termination of a TLS session

5.1.1.9.1 FCS_TLS_EXT.1 TLS Protocol

Hierarchical to: None

Dependencies: None

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2346), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

- Mandatory ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- Optional ciphersuites:
  - [selection:
  - *None*
  - *TLS_RSA_WITH_AES_128_CBC_SHA256*
  - *TLS_RSA_WITH_AES_256_CBC_ SHA256*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256*
  - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
  - *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  -].

5.1.1.10 FCS_EAP-TLS_EXT EAP_TLS Authentication Protocol

EAP-TLS, Extensible Authentication Protocol-Transport Layer Security, uses the TLS protocol authentication hand shaking implementation for 802.1x authentication. TLS provides certificates for client and server authentication, dynamic session key generation, and protection of the authentication session.

Family Behavior

This family provides requirements that address authentication on a 802.1x wireless network.

Component leveling

FCS_EAP-TLS_EXT: EAP-TLS Authentication Protocol	1

FCS_EAP-TLS_EXT.1 EAP-TLS Authentication Protocol requires the TSF provide the facilities to authenticate to the wireless network.

Management: FCS_EAP-TLS_EXT.1
The following actions could be considered for the management functions in FMT:
The management (addition, removal, or modification) of actions

Audit: FCS_EAP-TLS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.10.1 FCS_EAP-TLS_EXT.1 EAP-TLS Authentication Protocol

Hierarchical to: None

Dependencies: FCS_TLS_EXT.1

FCS_EAP-TLS_EXT.1.1 The TSF shall implement the EAP-TLS authentication protocol that complies with RFC 5216 Section 1, 2.1 to 2.3, 3, 4, and 5.1 to 5.3.

FCS_EAP-TLS_EXT.1.2 The TSF shall implement TLS 1.0[3] and [selection: *TLS v1.1, TLS v1.2, no other*] protocol as specified in FCS_TLS_EXT.1.

FCS_EAP-TLS_EXT.1.3 The TSF shall ensure that the EAP-TLS authentication protocol support the following ciphersuites:

- [selection:
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA*
- *TLS_RSA_WITH_AES_256_CBC_SHA*].

Application note: *Since TLS supports ciphersuite negotiation, peers completing the TLS negotiation will also have selected a ciphersuite, which includes encryption and hashing methods. Since the ciphersuite negotiated within EAP-TLS applies only to the EAP conversation, TLS ciphersuite negotiation MUST NOT be used to negotiate the ciphersuites used to secure data.*

TLS also supports compression as well as ciphersuite negotiation. However, during the EAP-TLS conversation the EAP peer and server MUST NOT request or negotiate compression.

[3] RFC5216: Section 2.4 Ciphersuite and Compression Negotiation

FCS_EAP-TLS_EXT.1.4	The TSF EAP-TLS implementation[4] [selection: supports validating the peer certificate using RFC 3280 compliant path validation, is pre-configured with the necessary intermediate certificates to complete path validation, relies on the EAP-TLS peer to provide this information as part of the TLS handshake, does not support certificate path validation].
FCS_EAP-TLS_EXT.1.5	EAP-TLS implementation[5] provides [selection: *its entire certificate chain minus the root, only the server certificate*] to facilitate certificate validation by the peer
FCS_EAP-TLS_EXT.1.6	The TSF shall ensure that once a TLS session is established, the EAP-TLS implementation validate that the identity represented in the peer certificate is appropriate and authorized for use with EAP-TLS[6].
Application note:	*The authorization process makes use of the contents of the certificate as well as other contextual information. It is recommended that the EAP-TLS implementation be able to authorize based on the EAP-TLS Peer-Id. In EAP-TLS, the Peer-Id is determined from the subject or subjectAltName fields in the peer certificates. For details, see Section 4.1.2.6 of RFC3280.*

[4] RFC5216: Section 5.3 Certificate Validation
[5] RFC5216: Section 5.3 Certificate Validation
[6] RFC5216: Section 5.3 Certificate Validation

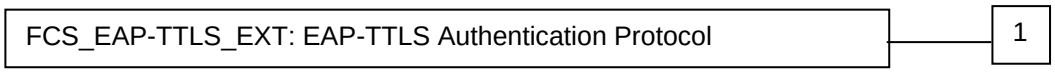
5.1.1.11 FCS_EAP-TTLS_EXT EAP_TTLS Authentication Protocol

EAP-TTLS, Extensible Authentication Protocol - Tunneled Transport Layer Security, is an extension of the EAP-TLS authentication protocol for 802.1x authentication. EAP-TTLS supports password and (optionally) certificate for client and server authentication.

Family Behavior

This family provides requirements that address authentication on a 802.1x wireless network.

Component leveling



FCS_EAP-TTLS_EXT EAP-TTLS Authentication Protocol requires the TSF provide the facilities to authenticate to the wireless network.

Management: FCS_EAP-TTLS_EXT.1
The following actions could be considered for the management functions in FMT:
The management (addition, removal, or modification) of actions

Audit: FCS_EAP-TTLS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.11.1 FCS_EAP-TTLS_EXT.1 EAP-TTLS Authentication Protocol

Hierarchical to: None

Dependencies: FCS_TLS_EXT.1

FCS_EAP-TTLS_EXT.1.1	The TSF shall implement the EAP-TTLSv0 authentication protocol that complies with RFC 5281.
FCS_EAP-TTLS_EXT.1.2	The TSF shall implement[7] [selection: *TLS 1.0, TLS v1.1, TLS v1.2*] as specified in FCS_TLS_EXT.1.
FCS_EAP-TTLS_EXT.1.3	The TSF shall ensure that the EAP-TLS implementation supports EAP[8], [selection: *PAP, CHAP, MS-CHAP-V2, EAP-MS-CHAP-V2, EAP-GTC, and no other*] tunneled authentication methods.
. FCS_EAP-TTLS_EXT.1.4	The TSF shall ensure that the EAP-TLS implementation supports MD5-Challenge[9], [selection: [assignment: *list of supported EAP types*], *and no other*] EAP type.

[7] RFC5281: Section 7.7 TLS Version
[8] RFC5281: Section 11.4 Mandatory Tunneled Authentication Support
[9] RFC5281: Section 11.4 Mandatory Tunneled Authentication Support

5.1.1.12 FCS_PEAP_EXT PEAP Authentication Protocol

PEAP, Protected Extensible Authentication Protocol, is a protocol that encapsulates the EAP within an encrypted and authenticated TLS tunnel to correct deficiencies in EAP because EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided.

Family Behavior

This family provides requirements that address authentication on an 802.1x wireless network.

Component leveling

FCS_PEAP_EXT: PEAP Authentication Protocol	1

FCS_PEAP_EXT PEAP Authentication Protocol requires the TSF provide the facilities to authenticate to the wireless network.

Management: FCS_PEAP_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FCS_PEAP_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.12.1 FCS_PEAP_EXT.1 PEAP Authentication Protocol

Hierarchical to: None

Dependencies: FCS_TLS_EXT.1

FCS_PEAP_EXT.1.1 The TSF shall implement the PEAPv0 and PEAPv1 authentication protocol that complies with RFC draft-kamath-pppext-peapv0-00 and RFC draft-josefsson-pppext-eap-tls-eap-05 respectively.

FCS_PEAP_EXT.1.2 The TSF shall implement TLS 1.0, [**selection: TLS v1.1, TLS v1.2, and no other version**] as specified in FCS_TLS_EXT.1.

FCS_PEAP_EXT.1.3 The TSF shall ensure that the EAP-TLS authentication protocol support the following ciphersuites[10]:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
- Optional Ciphersuites:
  - [selection:
  - *None*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *TLS_RSA_WITH_AES_128_CBC_SHA*
  - *TLS_RSA_WITH_AES_256_CBC_SHA*
  -].

[10] RFC draft-josefsson-pppext-eap-tls-eap-05: Section 2.1 PEAP Part 1

FCS_PEAP_EXT.1.4 The TSF shall ensure that the PEAP implementation supports [selection: *EAP-MS-CHAP-V2, EAP-GTC*] authentication methods.

5.1.1.13 FCS_RAD_EXT RADIUS Authentication Protocol

RADIUS, Remote Authentication Dial In User Service, is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

Family Behavior

This family provides requirements that address authentication on a 802.1x wireless network.

Component leveling

FCS_RAD_EXT RADIUS Authentication Protocol requires the TSF provide the facilities to authenticate to the wireless network.

Management: FCS_RAD_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FCS_RAD_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication success and failures

5.1.1.13.1 FCS_RAD_EXT.1 RADIUS Authentication Protocol

Hierarchical to: None

Dependencies: FCS_IPSEC_EXT.1

FCS_RAD_EXT.1.1 The TSF shall implement the RADIUS authentication protocol that complies with RFCs 2865, 3579, and 3580.

FCS_RAD_EXT.1.2 The TSF shall protect RADIUS communications using IPsec as specified in FCS_IPSEC_EXT.1.

FCS_RAD_EXT.1.3 The TSF shall ensure that the RADIUS implementation supports [**selection: PAP, CHAP, EAP-TLS, EAP-TTLS, EAP-MS-CHAP-V2, EAP-GTC, PEAP**] authentication methods.

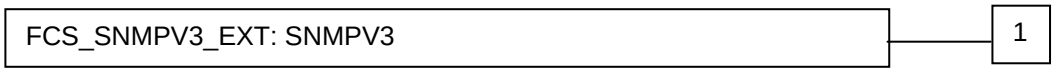
5.1.1.14 FCS_SNMPV3_EXT.1 SNMP V3

SNMP v3, Simple Network Management Protocol version 3, is a networking protocol that provides the ability to monitor and configure network devices.

Family Behavior

This family provides requirements that address use of the SNMPv3 protocol.

Component leveling



FCS_SNMPV3_EXT SNMPV3 requires conformance to the appropriate RFCs and critical security parameters.

Management: FCS_SNMPV3_EXT.1
The following actions could be considered for the management functions in FMT:

- The modification of SNMP configuration parameters

Audit: FCS_SNMPV3_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Authentication failures

5.1.1.14.1 FCS_SNMPV3_EXT.1 SNMPV3

Hierarchical to: None

Dependencies: None

FCS_SNMPV3_EXT.1.1 The TSF shall implement the SNMPV3 protocol that complies with RFCs:

- 3411 (Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks),
- 3414 (User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)),
- 3415 (View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- 3417 (Transport Mappings for the Simple Network Management Protocol (SNMP)), and
- [**selection:**
  - **3826 (The Advanced Encryption Standard (AES_ Cipher Algorithm in the SNMP User-based Security Model),**
  - **5608 (Remote Authentication Dial-In User Service (RADIUS) Usage for Simple Network Management Protocol (SNMP) Transport Models),**
  - **6353 (Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)),**
  - **no other RFC].**

FCS_SNMPV3_EXT.1.2 The TSF shall ensure that SNMPv3 uses AES128-CBC for privacy and HMAC_SHA-96 for authentication.

5.1.2 Class FDP: User Data Protection

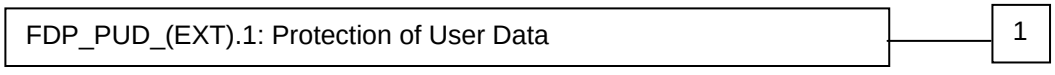
This class contains families specifying requirements related to protecting user data.

5.1.2.1 FDP_PUD_(EXT).1: Protection of User Data

Family Behavior

This family provides requirements that ensure wireless data is appropriately encrypted.

Component leveling



Management: FDP_PUD_(EXT).1
The following actions could be considered for the management functions in FMT:

- Enabling or disabling encryption for wireless data

Audit: FDP_PUD_(EXT).1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Enabling or disabling TOE encryption of wireless traffic

5.1.2.1.1 FDP_PUD_(EXT).1 Protection of User Data

Hierarchical to: None

Dependencies: None

FDP_PUD_(EXT).1.1 When the administrator has enabled encryption, the TSF shall:

- encrypt authenticated user data transmitted to a wireless client from the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP.1(1)
- decrypt authenticated user data received from a wireless client by the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP.1(1).

Application Note: *This requirement allows the TOE administrator to require that all user data transmitted on the WLAN be encrypted using the cryptographic algorithms specified by FCS_COP.*

5.1.3 Class FIA: Identification and Authentication

Families in this class address the requirements for functions to establish and verify a claimed user identity.

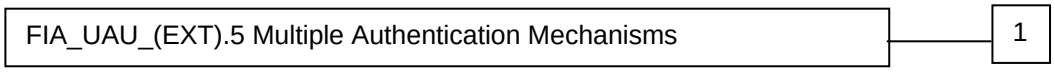
Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g. identity, groups, roles, security or integrity levels)

5.1.3.1 FIA_UAU_(EXT).5 Multiple Authentication Mechanisms

Family Behavior

This family provides requirements that providing multiple methods to authenticate users to the TOE.

Component leveling



FIA_UAU_(EXT).5 Multiple Authentication Mechanisms requires the TSF to provide both local and remote mechanisms to authenticate administrative and wireless users to the TOE.

Management: FIA_UAU_(EXT).5
The following actions could be considered for the management functions in FMT:

- Whether the TOE should use local or remote authentication

- Whether to use remote authentication for administrative users, wireless users, or both

Audit: FIA_UAU_(EXT).5
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Failure to receive a response from the remote authentication server

5.1.3.1.1 FIA_UAU_(EXT).5 Multiple Authentication Methods

Hierarchical to:	None
Dependencies:	None
FIA_UAU_(EXT).5.1	The TSF shall provide local authentication, and a remote authentication mechanism to perform user authentication.
FIA_UAU_(EXT).5.2	The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

5.1.4 Class FID: Intrusion Detection

This class contains families of functional requirements that relate to intrusion detection of IT entities that constitute threats to the TOE.

5.1.4.1 FID_APD_EXT Rogue Access Point Detection

A Rogue Access Point (AP) is an unauthorized active AP operating within the radio coverage area of a 802.11 wireless network; it may possess properties rendering its operation as unauthorized and/or threatening to the authorized access point(s) and/or wireless client communications to/from the LAN/WAN.

Any unauthorized active AP operating within the radio coverage of an authorized AP could be identified as a Rogue AP; even if it is not connected to the wired LAN. One threat for a facility is that an attacker places an AP onto a wired network, then leaves the property; allowing the attacker to remotely access or attack the network. Alternatively, an attacker may place an unauthorized AP within the radio coverage area of a commercial wireless network; configure to appear like an authorized AP, allowing the attacker access to the wireless client's data.

Family Behavior

This family provides requirements that address detection of Rogue Access Point in a wireless network.

Component leveling

FID_APD_EXT: Rogue Access Point Detection	1

FID_APD_EXT.1 Rogue Access Point Detection requires the TSF provide the facilities to detect the presence of Rogue Access Points that lie within the range of and constitute a threat to the wireless network.

Management: FID_APD_EXT.1
The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions

Audit: FID_APD_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Triggering of the Rogue AP detection routine described in FID_APD_EXT.1.1

5.1.4.1.1 FID_APD_EXT.1 Rogue Access Point Detection

Hierarchical to:	None
Dependencies:	None
FID_APD_EXT.1.1	The TSF shall be able to detect a Rogue Access Point operating within the radio coverage area of a 802.11 wireless network using the following detection method: [assignment: *specify the detection method to be used*].
FID_APD_EXT.1.2	Upon detection of a Rogue Access Point, the TSF shall take the following actions: [assignment: *specify the action to be taken*].

5.1.5 Class FPT: Protection of the TSF

This class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data.

5.1.5.1 FPT_STM_(EXT) Reliable Time Stamps

Family Behavior

This family provides requirements that address providing reliable, accurate time to the TOE.

Component leveling

FPT_STM_(EXT).1: Reliable Time Stamps	1

FPT_STM_(EXT).1: Reliable Time Stamps requires the TSF to synchronize its time with an external time source.

Management: FPT_STM_(EXT).1
The following actions could be considered for the management functions in FMT:

- Configuration of the external time server

Audit: FPT_STM_(EXT).1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Changes to the time

5.1.5.1.1 FPT_STM_(EXT).1 Reliable Time Stamps

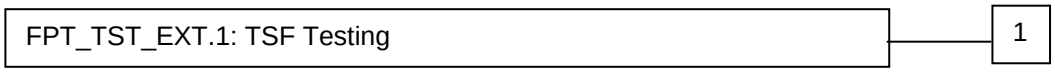
Hierarchical to:	None
Dependencies:	None
FPT_STM_EXT.1.1	The TSF shall be able to provide reliable time stamps, synchronized via an external time source, for its own use.
Application Note:	*The TOE must be capable of obtaining a time stamp via an NTP server.*

5.1.5.2 FPT_TST_EXT TSF Testing

Family Behavior

This family provides requirements that address self tests run by the TOE

Component leveling



FPT_TST_EXT.1: TSF Testing requires the TSF run self tests at various times to ensure its proper operation.

Management: FPT_TST_EXT.1
The following actions could be considered for the management functions in FMT:

- none

Audit: FPT_TST_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Execution of the self test, including success and failure of each test

5.1.5.2.1 FPT_TST_EXT.1 TSF Testing

Hierarchical to:	None
Dependencies:	None
FPT_TST_EXT.1.1	The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.
FPT_TST_EXT.1.2	The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

5.1.6 Class FTP: Trusted path/channels

Families in this class provide requirements for a trusted communication path between users and the TSF, and for a trusted communication channel between the TSF and other trusted IT products.

5.1.6.1 FTP_ITC_EXT.1 Inter-TSF Trusted Channel

Family Behavior

This family provides requirements that address the use of secure communications with entities in the IT environment.

Component leveling

FTP_ITC_EXT.1: Inter-TSF Trusted Channel requires the TSF to use secure communication methods and mutual authentication between itself and the IT environment.

Management: FTP_ITC_EXT.1
The following actions could be considered for the management functions in FMT:

- Configuration of attributes of the secure channel

Audit: FTP_ITC_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- Minimal: Initiation/Closure of a trusted channel;

5.1.6.1.1 FTP_ITC_EXT.1 Inter-TSF Trusted Channel

Hierarchical to:	None
Dependencies:	None
FPT_ITC_EXT.1.1	The TOE shall provide an encrypted communication channel between itself and entities in the TOE IT Environment that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FPT_ITC_EXT.1.2	The TSF shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.
FPT_ITC_EXT.1.3	The TSF shall initiate communication via the trusted channel for [all authentication functions, remote logging, time, [*selection: [assignment: communications with authorized IT entities determined by the ST author], none*]].
Application Note:	*If a certificate authority server plays a role in the authentication of users, then the CA is considered an authorized IT entity and the TSF is expected to initiate secure communications with this entity. It is assumed that the IT environment includes an NTP server, an audit server and/or an authentication server.*

5.2 Extended Security Assurance Requirement Definitions

There are no extended Security Assurance Requirements defined in this Security Target.

5.3 Rationale for Extended Security Requirements

This section presents the rationale for the inclusion of the extended requirements found in this Security Target.

5.3.1 Rationale for Extended Security Function Requirements

The following cryptographic support SFRs are extended, as Part II of the Common Criteria does not include an SFR that describes the requirements for the use of cryptographic communications protocols used to protect networked communications. These security functions are considered critical in environments having threats that may compromise the communication channel between administrators, other portions of the (distributed) TOE, or external IT entities.

FCS_COMM_PROT_EXT.1	Communications Protection
FCS_HTTPS_EXT.1	HTTPS
FCS_SFTP_EXT.1	SSH File Transfer Protocol
FCS_SNMPV3_EXT.1	SNMPv3
FCS_SSH_EXT.1	SSH Protocol
FCS_TLS_EXT.1	TLS Protocol
FCS_IPSEC_EXT.1	Internet Protocol Security (IPSec)

The following cryptographic support SFRs are extended, as Part II of the Common Criteria does not include an SFR that describes the requirements for the use of cryptographic authentication protocols used to protect networked communications. These security functions are considered critical in environments having threats that may compromise the communication channel between administrators, other portions of the (distributed) TOE, or external IT entities.

FCS_EAP-TLS_EXT.1	EAP-TLS Authentication Protocol
FCS_EAP-TTLS_EXT.1	EAP-TTLS Authentication Protocol
FCS_PEAP_EXT.1	PEAP Authentication Protocol
FCS_RAD_EXT.1	RADIUS Authentication Protocol

The following Intrusion Detection SFR is extended, as Part II of the Common Criteria does not include an SFR that describes the detection of Rogue Access Points. This security function is considered critical in environments where a Rogue Access Point represent a threat to the TSF.

FID_APD_EXT.1 Rogue Access Point Detection

The following SFRs are extended, with the rationale provided in the table below:

FCS_BCM_(EXT).1	Baseline cryptographic module	This extended requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.
FCS_CKM_(EXT).2	Cryptographic key handling and storage	This extended requirement is necessary since the CC does not specifically provide components for key handling and storage.
FCS_COP_(EXT).1	Random number generation	This extended requirement is necessary since the CC cryptographic operation components address only specific algorithm types and operations requiring specific key sizes.
FDP_PUD_(EXT).1	Protection of User Data	This extended requirement is necessary because the Common Criteria IFC/AFC requirements do not accommodate access control policies that are not object/attribute based. The FDP_PUP_(EXT).1 requirement allows the administrator allow or disallow access based upon an administrator setting indicating whether or not unencrypted data may transit the wireless LAN.
FIA_UAU_(EXT).5	Multiple authentication mechanisms	This extended requirement is needed for local administrators because there is concern over whether or not existing CC requirements specifically require that the TSF provide authentication. Authentication provided by the TOE is implied by other FIA_UAU requirements and is generally assumed to be a requirement when other FIA_UAU requirements are included in a TOE. In order to remove any potential confusion about this ST, an extended requirement for authentication has been included. This ST also requires the IT environment to provide an authentication server to be used for authentication of remote users. It is important to specify that the TSF must provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server. In addition, the TOE must provide the portions of the authentication mechanism necessary to obtain and enforce an authentication decision from the IT environment.
FPT_TST_(EXT).1	TSF Testing	This extended requirement is necessary to divide the TOE testing requirements between those necessary for the TOE itself and those specific to cryptographic modules.
FTP_ITC_(EXT).1	Inter-TSF trusted channel	This extended requirement is necessary because the existing trusted channel requirement is written with the intent of protecting communication between distributed portions of the TOE rather than between the TOE and its trusted IT environment.

5.3.2 Rationale for Extended Security Assurance Requirements

There are no extended Security Assurance Requirements defined in this ST; therefore, no rationale is presented.

6 Security requirements

This section describes the security functional and assurance requirements for the TOE; those that are CC Part 2 conformant, CC Part 2 extended, and CC Part 3 conformant.

6.1 Security Function Requirements

This section describes the functional requirements for the TOE. The security functional requirement components in this security target are CC Part 2 conformant or CC Part 2 extended as defined in Section 2, Conformance Claims. Table 11 - TOE Security Functional Requirements, lists the SFRs included in this Security Target.

Table 11 - TOE Security Functional Requirements

#	SFR	Description	Operations
1	FAU_GEN.1	Audit data generation	A - R - S
2	FAU_GEN.2	User identity association	---
3	FAU_SEL.1	Selective audit	A - S
4	FCS_BCM_(EXT).1	Baseline cryptographic module	S
5	FCS_CKM.1(1)	Cryptographic symmetric key generation	I
6	FCS_CKM.1(2)	Cryptographic asymmetric key generation	A – S - I
7	FCS_CKM.2	Cryptographic key distribution	S
8	FCS_CKM_(EXT).2	Cryptographic key handling and storage	---
9	FCS_CKM.4	Cryptographic key destruction	---
10	FCS_COP.1(1)	Cryptographic operation (Data encryption/decryption)	A - R - S - I
11	FCS_COP.1(2)	Cryptographic operation (Digital Signature)	A – S - I
12	FCS_COP.1(3)	Cryptographic operation (Hashing)	S - I
13	FCS_COP.1(4)	Cryptographic operation (Key agreement)	A - S - I
14	FCS_COP_(EXT).1	Extended: random number generation	A – S
15	FCS_COMM_PROT_EXT.1	Communications Protection	S
16	FCS_EAP-TLS_EXT.1	EAP-TLS Authentication Protocol	S
17	FCS_EAP-TTLS_EXT.1	EAP-TLS Authentication Protocol	S
18	FCS_HTTPS_EXT.1	HTTPS	---
19	FCS_IPSEC_EXT.1	Internet Protocol Security (IPsec)	A - S
20	FCS_PEAP_EXT.1	PEAP Authentication Protocol	S
21	FCS_RAD_EXT.1	RADIUS Authentication Protocol	S
22	FCS_SFTP_EXT.1	SSH File Transfer Protocol	---
23	FCS_SNMPV3_EXT.1	SNMPv3	S
24	FCS_SSH_EXT.1	SSH	A - S
25	FCS_TLS_EXT.1	TLS	S
26	FDP_IFC.1 (1)[11]	Subset information flow control (Traffic Filter SFP)	A – I

[11] Based on U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments Version 1.1 January 09, 2006.

Table 11 - TOE Security Functional Requirements			
#	SFR	Description	Operations
27	FDP_IFC.1 (2)[12]	Subset information flow control (Unauthenticated TOE Services SFP)	A - I
28	FDP_IFF.1-NIAP-0417 (1)[13]	Simple security attributes (Traffic Filter SFP)	A – R - I
29	FDP_IFF.1-NIAP-0417 (2)[14]	Simple security attributes (Unauthenticated TOE Services SFP)	A - R - I
30	FDP_PUD_(EXT).1	Protection of User Data	---
31	FDP_RIP.1	Subset residual information protection	S
32	FIA_AFL.1	Administrator authentication failure handling	A
33	FIA_ATD.1(1)	Administrator attribute definition	A - I
34	FIA_ATD.1(2)	User attribute definition	A - I
35	FIA_UAU.1(1)	Timing of Authentication (Administrative user)	A – I - R
36	FIA_UAU.1(2)	Timing of Authentication (Wireless user)	A – I - R
37	FIA_UAU.4	Single-use authentication mechanisms	A
38	FIA_UAU_(EXT).5.1	Multiple authentication mechanisms	---
39	FIA_UID.2	User identification before any action	---
40	FIA_USB.1	User-subject binding	R
41	FID_APD_EXP.1	Rogue Access Point Detection	A
42	FMT_MOF.1(1)	Management of security functions behavior (Cryptographic Function)	A – I - R
43	FMT_MOF.1(2)	Management of security functions behavior (Audit Record Generation)	A - S - I
44	FMT_MOF.1(3)	Management of security functions behavior (Authentication)	A - S - I
45	FMT_MOF.1(4)	Management of security functions behavior (Firewall)	A - S - I
46	FMT_MOF.1(5)	Management of security functions behavior (Intrusion Detection)	A - S - I
47	FMT_MOF.1(6)	Management of security functions behavior (Communication and authentication protocol)	A - S - I
48	FMT_MOF.1(7)	Management of security functions behavior (Configuration File Import and Export)	A - S - I
49	FMT_MSA.2[15]	Secure security attributes	---
50	FMT_MSA.3	Static attribute initialization	A – S - R
51	FMT_MTD.1(1)	Management of Audit pre-selection data	I
52	FMT_MTD.1(2)	Management of authentication data (Administrator)	I
53	FMT_SMF.1(1)	Specification of management functions (Cryptographic Functions)	I - R

[12] Based on U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments Version 1.1 January 09, 2006.
[13] Based on U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments Version 1.1 January 09, 2006.
[14] Based on U.S. Government Traffic-Filter Firewall Protection Profile For Medium Robustness Environments Version 1.1 January 09, 2006.
[15] The dependency on ADV_SPM.1 was removed, the ST author believes it was an error; ADV_SPM.1 is a requirement at EAL6.

Table 11 - TOE Security Functional Requirements			
#	SFR	Description	Operations
54	FMT_SMF.1(2)	Specification of Management Functions (TOE Audit Record Generation)	I
55	FMT_SMF.1(3)	Specification of management functions (Cryptographic Key Data)	I
56	FMT_SMF.1(4)	Specification of Management Functions (Firewall)	A - S - I
57	FMT_SMF.1(5)	Specification of management functions (Intrusion Detection)	A - S - I
58	FMT_SMF.1(6)	Specification of management functions (Communication Protocol)	A - S - I
59	FMT_SMF.1(7)	Specification of management functions (Configuration File Import and Export)	A - S - I
60	FMT_SMR.1	Security roles	R
61	FPT_STM_(EXT).1	Reliable time stamps	---
62	FPT_TST_EXT.1	TSF Testing	---
63	FPT_TST.1(1)	TSF Testing (for cryptography)	R - I
64	FPT_TST.1(2)	TSF Testing (for key generation components)	R - I
65	FTA_SSL.3	TSF-initiated termination	---
66	FTA_TAB.1	Default TOE access banners	---
67	FTA_TSE.1	TOE Session Establishment	A
68	FTP_ITC_EXT.1	Inter-TSF trusted channel	S
69	FTP_TRP.1	Trusted path	A

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN Audit data generation

6.1.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 **Refinement:** The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events listed in column “Auditable Events” of *Table 12 - TOE Auditable Events*; and

c) ***None***.

Table 12 - TOE Auditable Events[16]			
#	Requirement	Auditable Events	Additional Audit Record contents
1	FAU_GEN.1	None	None
2	FAU_GEN.2	None	None
3	FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the Administrator performing the function Logging source (Interface) Success or Failure of the function.

[16] FMT_REV.1 removed from this table, as this is the only reference in the ST.

Table 12 - TOE Auditable Events[16]			
#	Requirement	Auditable Events	Additional Audit Record contents
			Note: The identity of the Administrator means username (admin), MAC address of MU - when the operation is performed from a session opened from the MU, IP address – IP address of the host from where the session is opened.
4	FCS_CKM.1 (1)	Generation of a key	The identity of the Administrator performing the function
5	FCS_CKM.1 (2)[17]	Generation of a key	The identity of the Administrator performing the function
6	FCS_CKM_EXT.2	Error(s) detected during cryptographic key transfer	If available - the authentication credentials of subjects with which the invalid key is shared
7	FCS_CKM.4	Destruction of a cryptographic key	The identity of the Administrator performing the function
8	FCS_COP.1 (1), (2),(3),(4)	None	None
9	FCS_COP_(EXT).1	None	None
10	FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
11	FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Establishment/Termination of an IPsec SA.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
12	FCS_SFTP_EXT.1	Failure of the file transfer	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
13	FCS_SNMPV3_EXT.1	Failure to authenticate SNMP message	None
14	FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
15	FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
16	FCS_EAP-TLS_EXT.1	Authentication success and failures	None
17	FCS_EAP-TTLS_EXT.1	Authentication success and failures	None
18	FCS_PEAP_EXT.1	Authentication success and failures	None
19	FCS_RAD_EXT.1	Authentication success and failures	None
20	FDP_IFF.1-NIAP-0417 (1)	Decisions to deny requested information flows	Presumed IP address and MAC address of source subject

[17] Correction to iteration made by ST author

Table 12 - TOE Auditable Events[16]			
#	Requirement	Auditable Events	Additional Audit Record contents
		Failure to reassemble fragmented packets	Identity of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface associated on which the TOE received the packet Identity of the rule that allowed or disallowed the packet flow Reason why fragmented packets could not be reassembled (i.e., invalid fragment identifier, invalid offset, invalid fragment data length)
21	FDP_IFF.1-NIAP-0417 (2)	Decisions to deny information flows between a subject and the TOE	Presumed IP address and MAC address of source subject Identity of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface associated on which the TOE received the packet Identity of the rule that allowed or disallowed the packet flow, if applicable
22	FDP_PUD_(EXT).1[18]	Enabling or disabling TOE encryption of wireless traffic	The identity of the Administrator performing the function.
23	FDP_RIP.1	None	None
24	FID_APD_EXT.1	Detection of Rogue AP	None
25	FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)	None
26	FIA_ATD.1 (1), (2)[19]	None	None
27	FIA_UAU.1 (1), (2)	Use of the authentication mechanism (success or failure)	User identity - the TOE SHALL NOT record invalid passwords the audit log.

[18] Correction to SFR reference made by ST author
[19] Correction: Selection operators noted

Table 12 - TOE Auditable Events[16]			
#	Requirement	Auditable Events	Additional Audit Record contents
28	FIA_UAU_(EXT).5	Failure to receive a response from the remote authentication server	Identification of the Authentication server that did not reply
29	FIA_UID.2	None	None
30	FIA_USB.1	Unsuccessful binding of user security attributes to a subject	None
31	FID_APD_EXT.1	Triggering of the Rogue AP detection routine described in FID_APD_EXT.1.1	None
32	~~FMT_MOF.1 (1)~~ [20]	~~Changing the TOE encryption algorithm including the selection not to encrypt communications~~	~~Encryption algorithm selected (or none)~~
33	FMT_MOF.1 (2)	Start or Stop of audit record generation	None
34	FMT_MOF.1 (3)	Changes to the TOE remote authentication settings; Changes to the threshold of failed authentication attempts; Changes to the session lock timeframe	The identity of the Administrator performing the function.
35	FMT_MOF.1 (4)	Enable or disable of firewall	None
36	FMT_MOF.1 (5)	Change of detection method	None
37	FMT_MOF.1 (6)	Change of detection method	None
38	FMT_MOF.1 (7)	Configuration file import or export	User identity, operation, status of operation, login source, IP addres and MAC address
39	FMT_MSA.2	All offered and rejected values for security attributes	None
40	FMT_MTD.1 (1)	Changes to the set of rules used to pre-select audit events.	None
41	FMT_MTD.1 (2)	Changing the TOE authentication credentials	None – the TOE SHALL NOT record authentication credentials in the audit log.
43	FMT_SMR.1	Modifications to the group of users that are part of a role	None
44	FPT_STM_(EXT).1	Changes to the time	None
45	FPT_TST_(EXT).1	Execution of the self test	Success or Failure of test The identity of the Administrator performing the test Logging source (Interface) through test is initiated
46	FPT_TST.1	Execution of the self test	Success or Failure of test The identity of the Administrator performing the test Logging source (Interface) through test is initiated
47	FPT_TST.2	Execution of the self test	Success or Failure of test The identity of the Administrator performing the test Logging source (Interface) through test is initiated
48	FTA_SSL.3	TSF Initiated Termination	Termination of an interactive session by the session locking mechanism
49	FTA_TSE.1	Rejection of user login	Identification of the user attempting login

[20] The TOE has no option to change the encryption algorithm; therefore, there will be no audit log required.

Table 12 - TOE Auditable Events[16]			
#	Requirement	Auditable Events	Additional Audit Record contents
50	FTP_ITC_(EXT).1	Initiation/Closure of a trusted channel;	Identification of the remote entity with which the channel was attempted/created; Success of failure of the event
51	FTP_TRP.1	Initiation of a trusted path[21]	Identification of the remote entity with which the path was attempted/created; Success of failure of the event

FAU_GEN.1.2 **Refinement:** 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 (if applicable), 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 included in the PP/ST, information specified in column three of Table 12.

Application Note: *Event type is defined to be the severity level indicator as it is defined in IETF RFC 3146 The BSD syslog Protocol.*

6.1.1.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 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.

6.1.1.1.3 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) user identity, event type;

b) device interface, wireless client identity.

Application Note: *Event type is defined to be the severity level indicator as it is defined in IETF RFC3164 The BSD syslog Protocol.*

Application Note: *The device interface is the physical interface upon which user (or administrative) data is received/sent (e.g. WLAN interface, wired LAN interface, serial port, administrative LAN interface, etc.).*

6.1.2 Class FCS: Cryptographic support

6.1.2.1 FCS_CKM Cryptographic Key Management

6.1.2.1.1 FCS_BCM_(EXT).1 Baseline Cryptographic Module

FCS_BCM_(EXT).1.1 All cryptographic functions implemented by the TOE shall be validated by NIST CAVP and include an algorithm validation certificate.

[21] Correction of terminology made

6.1.2.1.2 FCS_CKM.1 (1) Cryptographic key generation (for symmetric keys)

FCS_CKM.1.1 (1) **Refinement**[22]**:** The TSF shall generate symmetric cryptographic keys using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity protection to generated symmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.

Application Note: *NIST SP 800-57 "Recommendation for Key Management" Section 6.1 states: "Integrity protection can be provided by cryptographic integrity mechanisms (e.g. cryptographic checksums, cryptographic hashes, MACs, and signatures), non-cryptographic integrity mechanisms (e.g. CRCs, parity, etc.) […], or physical protection mechanisms". Guidance for the selection of appropriate integrity mechanisms is given in Sections 6.2.1.2 and 6.2.2.2 of NIST SP 800-57 "Recommendation for Key Management".*

6.1.2.1.3 FCS_CKM.1 (2) Cryptographic key generation (for asymmetric keys)

FCS_CKM.1.1 (2) **Refinement**[23]The TSF shall generate asymmetric cryptographic keys in accordance with the mathematical specifications of the FIPS-approved or NIST-recommended standard ***FIPS 186-2***, using a domain parameter generator and **FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1** in a cryptographic key generation scheme that meets the following:

- The TSF shall provide integrity protection and assurance of domain parameter and public key validity to generated asymmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.
- Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 112 bits using conservative estimates.

Application Note: *NIST SP 800-57 "Recommendation for Key Management" Section 6.1 states: "Integrity protection can be provided by cryptographic integrity mechanisms (e.g. cryptographic checksums, cryptographic hashes, MACs, and signatures), non-cryptographic integrity mechanisms (e.g. CRCs, parity, etc.) […], or physical protection mechanisms." Guidance for the selection of appropriate integrity mechanisms is given in Sections 6.2.1.2 and 6.2.2.2 of NIST SP 800-57 "Recommendation for Key Management".*

Application Note: *Assurance of domain parameter and public key validity provides confidence that the parameters and keys are arithmetically correct. Guidance for the selection of appropriate validation mechanisms is given in NIST SP 800-57 "Recommendation for Key Management," NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," and FIPS PUB 186-2, "Digital Signature Standard."*

Application Note: *See NIST Special Publication 800-57, "Recommendation for Key Management" for information about equivalent key strengths.*

[22] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

[23] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

6.1.2.1.4 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **manual (physical method), and automated (electronic) method** that meets the following:

- NIST Special Publication 800-57, "Recommendation for Key Management" Section 8.1.5
- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

Application Note: *NIST Special Publication 800-56A "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" is only applicable when public key schemes are used in key transport methods.*

Application Note: *DoD applications may have additional key distribution requirements related to the DoD PKI and certificate formats.*

6.1.2.1.5 FCS_CKM_(EXT).2 Extended: Cryptographic Key Handling and Storage

FCS_CKM_(EXT).2.1 The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

Application Note: *A parity check is an example of a key error detection check.*

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

Application Note: *Note that this requirement is stronger than the FIPS 140-2 key storage requirements, which state: "Cryptographic keys stored within a cryptographic module shall be stored in plaintext form or encrypted form."*

Application Note: *A persistent key, such as a file encryption key, is one that must be available in the system over long periods of time. A non-persistent key, such as a key used to encrypt or decrypt a single message or a session, is one that is ephemeral in the system.*

Application Note: *"When not in use" is interpreted in the strictest sense so that persistent keys only exist in plaintext form during intervals of operational necessity. For example, a file encryption key exists in plaintext form only during actual encryption and/or decryption processing of a file. Once the file is decrypted or encrypted, the file encryption key should immediately be covered for protection.*

Application Note: *A "split knowledge procedure" is a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.*

FCS_CKM_(EXT).2.3 The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

Application Note: *The cryptographic administrator must have the ability to set a threshold of inactivity after which non-persistent keys must be destroyed in accordance with FCS_CKM.4.*

FCS_CKM_(EXT).2.4 The TSF shall prevent archiving of expired (private) signature keys.

Application Note: *This requirement is orthogonal to typical system back-up procedures. Therefore, it does not address the problem of archiving an active (private)*

signature key during a system back-up and saving the key beyond its intended life span.

6.1.2.1.6 FCS_CKM.4 Cryptographic key destruction

Application Note: *Note that this requirement is stronger than the FIPS 140-2 key zeroization requirements, which state: "A cryptographic module shall provide methods to zeroize all plaintext secret and private cryptographic keys and CSPs within the module."*

FCS_CKM.4.1 **Refinement**[24]: The TSF shall destroy cryptographic keys in accordance with a cryptographic key zeroization method that meets the following:

a) Key Zeroization Requirements in FIPS PUB 140-2 "Security Requirements for Cryptographic Modules"

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete.

Application Note: *The term "immediate" here is meant to impart some urgency to the destruction: it should happen as soon as practical after the key is no longer required to be in plaintext. It is certainly permissible to complete a critical section of code before destroying the key. However, the destruction shouldn't wait for idle time, and there shouldn't be any non-determined event (such as waiting for user input) which occurs before it is destroyed.*

c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical cryptographic security parameter to another location.

Application Note: *Item c) pertains to the elimination of internal, temporary copies of keys/parameters during processing, and not to the locations that are used for the storage of the keys, which are specified in item b). The temporary locations could include memory registers, physical memory locations, and even page files and memory dumps.*

d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

Application Note: *Although verification of the zeroization of each intermediate location consisting of non-volatile memories is desired here (by checking for the final known alternating data pattern), it is not required at this time.*

e) For volatile memory and non-volatile EEPROM and Flash memories, the zeroization shall be executed by a single direct overwrite consisting of a pseudo random pattern, followed by a read-verify.

6.1.2.2 FCS_COP Cryptographic operation

6.1.2.2.1 FCS_COP.1 (1) Cryptographic operation (for data encryption/decryption)

FCS_COP.1.1 (1) **Refinement**: The TSF shall perform ***symmetric encryption and decryption*** in accordance with ~~a specified~~ the FIPS-approved security cryptographic algorithms

[24] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

a) TDEA with three independent keys operating in CBC mode,

b) AES operating in CCM, CFB, and CBC mode

and cryptographic key sizes

a) 168-bits

b) 128-bits, 192-bits, and 256-bits

that meet the following:

a) conformant to FIPS 46-3 (TDEA), conformant to FIPS 81 (CBC mode),

b) conformant to FIPS 197 (AES, CBC mode).

6.1.2.2.2 FCS_COP.1 (2) Cryptographic operation (for cryptographic signature)

FCS_COP.1.1 (2) The TSF shall perform **cryptographic signature services**[25] in accordance with a specified cryptographic algorithm **RSA Digital Signature Algorithm (rDSA)** and cryptographic key size **(modulus) of *2048 bits*** that meets the following: **NIST Special Publication 800-57, "Recommendation for Key Management."**

6.1.2.2.3 FCS_COP.1 (3) Cryptographic operation (for cryptographic hashing)

FCS_COP.1.1 (3) **Refinement**[26]: The TSF shall perform **cryptographic hashing services** using the FIPS-approved security function Secure Hash Algorithm and message digest size of **160, 256 bits**.

Application Note: *The message digest size should correspond to double the system symmetric encryption key strength.*

6.1.2.2.4 FCS_COP.1 (4) Cryptographic Operation (for cryptographic key agreement)

Application Note: *"Cryptographic key agreement" is a procedure where the resultant secret keying material is a function of information contributed by two participants, so that no party can predetermine the value of the secret keying material independently from the contributions of the other parties.*

FCS_COP.1.1 (4) **Refinement**[27]: The TSF shall perform cryptographic key agreement services using the FIPS-approved security function as specified in NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

***1) Diffie-Hellman Key Agreement Algorithm* and cryptographic key sizes (modulus) of *2048 bits*,**

that meets NIST Special Publication 800-57, "Recommendation for Key Management."

Application Note: *Some authentication mechanism on the keying material is recommended. In addition, repeated generation of the same shared secrets should be avoided.*

Application Note: *FIPS 140-2 Annex D specifies references for FIPS-approved Key Establishment Techniques, one of which is NIST Special Publication 800-*

[25] Cryptographic signature services includes digital signature generation and verification

[26] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

[27] Refinement is consistent with the corresponding SFR refinement in the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments (WLAN AS PP), version 1.1, dated July 25, 2007

56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography."

6.1.2.2.5 FCS_COP_(EXT).1 Extended: random number generation

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG ***ANSI X9.31***[28] seeded by **one or more independent software-based entropy sources**.

FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

6.1.2.3 Communications Protocols

6.1.2.3.1 FCS_COMM_PROT_EXT.1 Communications Protection

FCS_COMM_PROT_EXT.1.1 The TSF shall protect communications using **SSH, IPsec, and TLS/HTTPS.**

6.1.2.3.2 FCS_HTTPS_EXT.1 HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

6.1.2.3.3 FCS_IPSEC_EXT.1 Internet Protocol Security (IPsec)

FCS_IPSEC_EXT.1.1 The TSF shall implement IPsec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-192, AES-CBC-256, **no other algorithms** and using IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109; **no other method** to establish the security association.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

FCS_IPSEC_EXT.1.4 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and **no other DH groups**.

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement Peer Authentication using the **PSK** algorithm.

FCS_IPSEC_EXT.1.6 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.

FCS_IPSEC_EXT.1.7 The TSF shall support the following:

> Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "*", "(", and ")");
>
> Pre-shared keys ***from 8 to 49 characters***.

6.1.2.3.4 FCS_SFTP_EXT.1 SSH File Transfer Protocol

FCS_SFTP_EXT.1.1 The TSF shall implement the SSH File Transfer Protocol as specified in draft-ietf-secsh-filexfer-13.txt, July 10, 2006.

FCS_SFTP_EXT.1.2 The TSF shall ensure the SFTP connection has privacy and integrity features provided by the underlying SSH transport protocol as specified in FCS_SSH_EXT.1.

[28] ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, January 31, 2005

6.1.2.3.5 FCS_SNMPV3_EXT.1 SNMPV3

FCS_SNMPV3_EXT.1.1 The TSF shall implement the SNMPV3 protocol that complies with RFCs:

- 3411 (Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks),
- 3414 (User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)),
- 3415 (View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- 3417 (Transport Mappings for the Simple Network Management Protocol (SNMP)), and
  - **3826 (The Advanced Encryption Standard (AES_ Cipher Algorithm in the SNMP User-based Security Model).**

FCS_SNMPV3_EXT.1.2 The TSF shall ensure that SNMPv3 uses AES128-CBC for privacy and HMAC_SHA-96 for authentication.

6.1.2.3.6 FCS_SSH_EXT.1 SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of ***600 seconds*** and provide a limit to the number of failed authentication attempts a client may perform in a single session to ***3*** attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the password-based authentication method as described in RFC 4252.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFC 4253, packets greater than ***32768*** bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, **AES-CBC-192**.

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH_RSA **and no other public key algorithms,** as its public key algorithm(s).

Application Note: *RFC 4253 specifies required and allowable public key algorithms. This requirement makes SSH-RSA "required" and allows others to be claimed in the ST. The ST author should make the appropriate selection, selecting "no other public key algorithms" if only SSH_RSA is implemented.*

FCS_SSH_EXT.1.8 The TSF shall ensure that data integrity algorithms used in SSH transport connection is hmac-sha1, and **hmac-sha1-96**.

FCS_SSH_EXT.1.9 The TSF shall ensure that SSH supports diffie-hellman-group14-sha1 and **diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256** for key exchange.

6.1.2.3.7 FCS_TLS_EXT.1 TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols **TLS 1.0 (RFC 2346)** supporting the following ciphersuites:

- Mandatory ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- Optional ciphersuites:
  - **None**

6.1.2.4 Authentication Protocols

6.1.2.4.1 FCS_EAP-TLS_EXT.1 EAP-TLS Authentication Protocol

FCS_EAP-TLS_EXT.1.1 The TSF shall implement the EAP-TLS authentication protocol that complies with RFC 5216 Section 1, 2.1 to 2.3, 3, 4, and 5.1 to 5.3.

FCS_EAP-TLS_EXT.1.2 The TSF shall implement TLS 1.0[29] and **no other** protocol as specified in FCS_TLS_EXT.1.

FCS_EAP-TLS_EXT.1.3 The TSF shall ensure that the EAP-TLS authentication protocol support the following ciphersuites:

- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**
- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA**
- **TLS_RSA_WITH_AES_128_CBC_SHA**
- **TLS_RSA_WITH_AES_256_CBC_SHA**

Application note: *Since TLS supports ciphersuite negotiation, peers completing the TLS negotiation will also have selected a ciphersuite, which includes encryption and hashing methods. Since the ciphersuite negotiated within EAP-TLS applies only to the EAP conversation, TLS ciphersuite negotiation must not be used to negotiate the ciphersuites used to secure data.*
TLS also supports compression as well as ciphersuite negotiation. However, during the EAP-TLS conversation the EAP peer and server must not request or negotiate compression.

FCS_EAP-TLS_EXT.1.4 The TSF EAP-TLS implementation[30] **relies on the EAP-TLS peer to provide this information as part of the TLS handshake**.

FCS_EAP-TLS_EXT.1.5 EAP-TLS implementation[31] provides **only the server certificate** to facilitate certificate validation by the peer

FCS_EAP-TLS_EXT.1.6 The TSF shall ensure that once a TLS session is established, the EAP-TLS implementation validate that the identity represented in the peer certificate is appropriate and authorized for use with EAP-TLS[32].

Application note: *The authorization process makes use of the contents of the certificate as well as other contextual information. It is recommended that the EAP-TLS implementation be able to authorize based on the EAP-TLS Peer-Id. In EAP-TLS, the Peer-Id is determined from the subject or subjectAltName fields in the peer certificates. For details, see Section 4.1.2.6 of RFC3280.*

6.1.2.4.2 FCS_EAP-TTLS_EXT.1 EAP-TTLS Authentication Protocol

FCS_EAP-TTLS_EXT.1.1 The TSF shall implement the EAP-TTLSv0 authentication protocol that complies with RFC 5281.

[29] RFC5216: Section 2.4 Ciphersuite and Compression Negotiation
[30] RFC5216: Section 5.3 Certificate Validation
[31] RFC5216: Section 5.3 Certificate Validation
[32] RFC5216: Section 5.3 Certificate Validation

FCS_EAP-TTLS_EXT.1.2 The TSF shall implement[33] **TLS 1.0** as specified in FCS_TTLS_EXT.1

FCS_EAP-TTLS_EXT.1.3 The TSF shall ensure that the EAP-TTLS implementation supports EAP[34], **MD5, PAP, MS-CHAP-V2** tunneled authentication methods.

FCS_EAP-TTLS_EXT.1.4 The TSF shall ensure that the EAP-TTLS implementation supports MD5-Challenge[35], **No other** EAP type.

6.1.2.5 FCS_PEAP_EXT.1 PEAP Authentication Protocol

FCS_PEAP_EXT.1.1 The TSF shall implement the PEAPv0 and PEAPv1 authentication protocol that complies with RFC draft-kamath-pppext-peapv0-00 and RFC draft-josefsson-pppext-eap-tls-eap-05 respectively.

FCS_PEAP_EXT.1.2 The TSF shall implement TLS 1.0 **and no other version** as specified in FCS_TLS_EXT.1.

FCS_PEAP_EXT.1.3 The TSF shall ensure that the EAP-TLS authentication protocol support the following ciphersuites[36]:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
- Optional Ciphersuites:
  - **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**
  - **TLS_DHE_RSA_WITH_AES_256_CBC_SHA**
  - **TLS_RSA_WITH_AES_128_CBC_SHA**
  - **TLS_RSA_WITH_AES_256_CBC_SHA**

FCS_PEAP_EXT.1.4 The TSF shall ensure that the PEAP implementation supports **EAP-MS-CHAP-V2, EAP-GTC** authentication methods.

6.1.2.5.1 FCS_RAD_EXT.1 RADIUS Authentication Protocol

FCS_RAD_EXT.1.1 The TSF shall implement the RADIUS authentication protocol that complies with RFCs 2138, 3579, and 3580.

FCS_RAD_EXT.1.2 The TSF shall protect RADIUS communications using IPsec as specified in FCS_IPSEC_EXT.1.

FCS_RAD_EXT.1.3 The TSF shall ensure that the RADIUS implementation supports **PAP, EAP-TLS, EAP-TTLS, EAP-MS-CHAP-V2, EAP-GTC, PEAP** authentication methods.

6.1.3 Class FDP: User data protection

6.1.3.1 FDP_IFC Information flow control policy

6.1.3.1.1 FDP_IFC.1 (1) Subset information flow control (*Traffic Filter SFP*)

FDP_IFC.1.1 (1) The TSF shall enforce the ***Traffic Filter SFP*** on

- ***source subject: TOE interface on which information is received;***
- ***destination subject: TOE interface to which information is destined;***
- ***information: network packets; and***
- ***operations: pass information.***

[33] RFC5281: Section 7.7 TLS Version
[34] RFC5281: Section 11.4 Mandatory Tunneled Authentication Support
[35] RFC5281: Section 11.4 Mandatory Tunneled Authentication Support
[36] RFC draft-josefsson-pppext-eap-tls-eap-05: Section 2.1 PEAP Part 1

Application Note: *The Traffic Filter SFP allows authenticated and unauthenticated users to pass information through the TOE, with TSF mediation according to the rules defined by the administrator and SNMP administrator.*

Application Note: *In a firewall, the central issue is that there are two "subjects" (the sender of the packet (information) and the receiver of the packet) neither of which are under the control of the TOE. In order to use the FDP_IF* requirements, we associate the potential set of subjects with a firewall interface. This makes sense because an administrator is able to determine what sets of IP addresses (for example) are associated with each of the physical firewall interfaces (assuming no other "backdoor" connectivity). Associating this potential set of subjects with an interface also allows the specification of subject attributes to be associated with something that is actually part of the TOE (the physical interface), as well as allow FDP_IFF.1.2-NIAP-0417 to be written so that it actually makes sense.*

Note that "operations" also is different from an operating-system-centric world because there is only one operation that the subjects really want: that the information is passed through the firewall.

6.1.3.1.2 FDP_IFC.1 (2) Subset information flow control (*Unauthenticated TOE Services SFP*)

FDP_IFC.1.1 (2) The TSF shall enforce the ***Unauthenticated TOE Services SFP]*** on:

- ***source subject: TOE interface on which information is received;***
- ***destination subject: the TOE;***
- ***information: network packets; and***
- ***operations: accept or reject network packet.***

Application Note: *This policy is used to express how the TOE enforces rules concerning network traffic that is destined for the TOE, and the protocols that are allowed as specified in FIA_UAU.1 (1). The intent of this iteration of the requirement is control how the TOE responds to network traffic destined for the TOE, this policy does not have to be enforced in the firewall ruleset (e.g., could be Security Administrator configurable and TOE controlled via another mechanism).*

Note that "operations" refers to the TOE accepting or rejecting the network packet, since the TOE is not technically always providing the "service". In the case of ARP, another machine (e.g., router on the same subnet) is providing an ARP "service" by providing updates to the TOE's routing tables.

6.1.3.2 FDP_IFF Information flow control functions

6.1.3.2.1 FDP_IFF.1-NIAP-0417 (1) Simple security attributes (*Traffic Filter SFP*)

FDP_IFF.1.1-NIAP-0417 (1) The TSF shall enforce the ***Traffic Filter SFP*** based on the following types of subject and information security attributes**:**

- ***a) Source subject security attributes:***
  - ***a. set of source subject identifiers;***
- ***b) Destination subject security attributes:***
  - ***a. Set of destination subject identifiers;***
- ***c) Information security attributes:***
  - ***a. presumed identity of source subject;***
  - ***b. identity of destination subject;***
  - ***c. transport layer protocol;***
  - ***d. source subject service identifier;***
  - ***e. destination subject service identifier (e.g., TCP or UDP destination port number);***
- ***d) Stateful packet attributes:***

a. Connection-oriented protocols:
i. sequence number;
ii. acknowledgement number;
iii. Flags:
- ***SYN;***
- ***ACK;***
- ***RST;***
- ***FIN;***

b. Connectionless protocols:
i. source and destination network identifiers;
ii. source and destination service identifiers;

Application Note: *The stateful packet attributes are not specified in the ruleset as are the other security attributes. These attributes are intended to be used in FDP_IFF.1.3-NIAP-0417(1) as part of the stateful packet inspection. The TOE keeps state about a connection (e.g., a TCP connection) or pseudo-connection (e.g., UDP stream) and uses that information in determining whether to permit information to flow.*

e) Content filtering specific attributes:
a. Outbound HTTP[37] requests
i. Web proxy
ii. ActiveX
b. Outbound URL extensions
i. Specified URL or filename extensions
c. SMTP commands
i. HELO
ii. MAIL
iii. RCPT
iv. DATA
v. QUIT
vi. SEND
vii. SAML
viii. RESET
ix. VFRY
x. EXPN
d. FTP functions
i. Store files
ii. Retrieve files
iii. Directory list
iv. Create directory
v. Change directory
vi. Passive operations

f) Subnet access specific attributes
a. Full access (no protocol rules)
b. Limited access with protocols allowed or denied
i. HTTP
ii. TELNET
iii. FTP
iv. SMPT
v. POP
vi. DNS
vii. Transport protocols
1. ALL

[37] Port 80 only

2. ***TCP***
3. ***UDP***
4. ***ICMP - Internet Control Message Protocol***
5. ***AH - Authentication Header***
6. ***ESP - Encapsulating Security Protocol***
7. ***GRE - General Routing Encapsulation***

g) IP filtering specific attributes

a. Protocol

i. ALL,
ii. TCP,
iii. UDP,
iv. ICMP,
v. PIM,
vi. GRE,
vii. RSVP,
viii. IDP,
ix. PUP,
x. EGP,
xi. IPIP,
xii. ESP,
xiii. AH,
xiv. IGMP,
xv. IPVG,
xvi. COMPR_H and
xvii. RAW_IP.

FDP_IFF.1.2-NIAP-0417 (1) **Refinement**: The TSF shall permit an information flow between a source subject and a destination subject via a controlled operation if the following rules hold:

- ***the presumed identity of the source subject is in the set of source subject identifiers;***
- ***the identity of the destination subject is in the set of source destination identifiers;***
- ***the selected information flow policy rule specifies that the information flow is to be permitted***.

Application Note: *The TSF does not support information flow policy rules that contain information security attribute values, or wildcards that "stand" for multiple values of the same type.*

FDP_IFF.1.3-NIAP-0417 (1) The TSF shall enforce the following:

- ***fragmentation rule:***
  - ***prior to applying the information policy ruleset, the TOE completely reassembles fragmented packets;***
- ***stateful packet inspection rules:***
  - ***whenever a packet is received that is not associated with an allowed established session (e.g., the SYN flag is set without the ACK flag being set), the information flow policy ruleset, as defined in FDP_IFF.1.2-NIAP-0417(1), is applied to the packet;***
  - ***otherwise, the TSF associates a packet with an allowed established session using the stateful packet attributes***.

Application Note: *This requirement has two distinctive rules that are applied. The first rule ensures that the TOE reassembles packets before applying the policy rules.*

The TOE ensures that fragments are handled properly and the TOE will drop any malformed packets (e.g., duplicate fragments, invalid offsets) and eliminates the security concern of fragments being received out of order at the target host.
The second rule, requires that the TOE maintains state for connection-oriented sessions and connectionless "pseudo" sessions. The TOE uses the stateful packet attributes to determine if a packet already belongs to a "session" that has been allowed by the TOE's ruleset. If a packet cannot be associated with a session, then the ruleset is applied. Connectionless sessions are subject to these rules and allow an IT entity to respond to a connectionless packet without having to specify a rule in the ruleset to explicitly allow the flow.

When a packet is received, usually "sanity" checks are made first (e.g., format and frame checks to make sure that the packet is well formed). If an address is all zeros (e.g., MAC address, Source IP address), the packet is discarded. If the packet passes the sanity checks, the TOE searches to see if the packet is associated with an existing session. If it is connectionless, the TOE may create a "pseudo session" to associate connectionless packets with a connection and therefore represent the connectionless data stream.

In an IP-based network stack, if a session already exists, the TCP packet's sequence number, acknowledgment number and flags (e.g., SYN, FIN) are checked to make sure that the packet really belongs to the session (e.g., an invalid sequence number can indicate a hijacked session). If the packet cannot be associated with an established session, the TOE's ruleset is applied to the packet.

FDP_IFF.1.4-NIAP-0417 (1) The TSF shall provide the following ***the authorized administrator shall have the capability to view all information flows allowed by the information flow policy ruleset before the ruleset is applied***.

Application Note: *Some firewalls create additional rules as a side-effect of creating a rule; for example, a firewall may create a rule allowing an FTP data channel when a rule allowing FTP (control connections) is created. This requirement allows an administrator to view the entire ruleset so that they can identify such rules and confirm that the ruleset reflects the desired policy. "before the rule set is applied" means that the administrator is able to view the entire rule set before it is put into use on the TOE. This gives the administrator the opportunity to address any errors or unintended flows.*

FDP_IFF.1.5-NIAP-0417 (1) The TSF shall explicitly authorize an information flow based on the following rules: **no explicit authorization rules**.

FDP_IFF.1.6-NIAP-0417 (1) The TSF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;

Application Note: *The intent of this requirement is to ensure that a user cannot send packets originating on one TOE interface claiming to originate on another TOE interface.*

b) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;

Application Note: *A broadcast identity is one that specifies more than one host address on a network. It is understood that the TOE can only know the sub-netting configuration of networks directly connected to the TOE's interfaces and therefore can only be aware of broadcast addresses on those networks.*

c) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier;

d) The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject

6.1.3.2.2 FDP_IFF.1-NIAP-0417 (2) Simple security attributes (*Unauthenticated TOE Services SFP)*

FDP_IFF.1.1-NIAP-0417 (2) **Refinement:** The TSF shall enforce the ***Unauthenticated TOE Services SFP*** based on the following types of subject and information security attributes**:**

a) Source subject security attributes:
- ***set of source subject identifiers;***

b) Destination subject security attributes;
- ***TOE's network identifier;***

Application Note: *For the subjects, the administrator knows the set of identifiers that can be associated with the physical firewall interfaces; therefore, they are not "presumed" identifiers. The term "identifiers" was used instead of "addresses" to allow for technologies that are not address-based (e.g., circuit identifiers instead of source and destination addresses).*

c) Information security attributes:
- ***presumed identity of source subject;***
- ***identity of destination subject;***
- ***transport layer protocol;***
- ***source subject service identifier;***
- ***destination subject service identifier (e.g., TCP or UDP destination port number); and***

Application Note: *Not all of the above security attributes will exist in all network packets. The intent is that if a network packet includes any of the above security attributes, those attributes will be used in the policy decision. The data link frame type identifies the type of data the data link header encapsulates (e.g., in the case of ARP, the frame type value is 0x0806). The transport layer protocol is what is specified in the 8-bit protocol field in the IP header (e.g., this would include ICMP (value of 1) and is not limited to TCP (value of 6) or UDP (value of 17)). The concept of a "service identifier" may differ depending on the networking stack used; the intent is to specify a service that may exist above the network and transport layers in the protocol stack. A "service" in the IP stack would be NTP, TFTP, etc.*

- ***ICMP message type and code as specified in RFC 792, other information security attributes associated with services identified in FAU_UAU.1.***

FDP_IFF.1.2-NIAP-0417 (2) **Refinement:** The TSF shall permit an information flow between a source subject and the TOE via a controlled operation if the following rules hold:

- ***the presumed identity of the source subject is in the set of source subject identifiers;***
- ***the identity of the destination subject is the TOE;***

FDP_IFF.1.3-NIAP-0417 (2) The TSF shall enforce the following information flow control rules:

- ***The TOE shall allow source subjects to access TOE services ICMP, list of other network services provided by the TOE consistent with FIA_UAU.1 (1) without authenticating those source subjects; and***

Application Note: *The intent of this requirement is to allow users to access services such as ICMP Echo (ping) without authentication. However, since some sites may not want to allow this capability, the second bullet was added so that an administrator (see FMT_MOF.1 (6)) can restrict the services available.*

- ***The TOE shall allow the list of services specified immediately above to be enabled (become available to unauthenticated users) or disabled (become unavailable to unauthenticated users).***

FDP_IFF.1.4-NIAP-0417 (2) The TSF shall provide the following ***the authorized administrator shall have the capability to view all information flows allowed by this information flow control policy before the policy is applied***.

Application Note: *The intent here is to provide the authorized administrator the capability to see what information flow controls will be applied to the TOE before those controls are activated. This gives the administrator the opportunity to address any errors or unintended TOE interactions with users. In the case of this policy, information flow is between a network device and the TOE.*

FDP_IFF.1.5-NIAP-0417 (2) The TSF shall explicitly authorize an information flow based on the following rules: ***none***

FDP_IFF.1.6-NIAP-0417 (2) The TSF shall explicitly deny an information flow based on the following rules:

- ***The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;***
- ***The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;***

Application Note: *A broadcast identity is one that specifies more than one host on a network. It is understood that the TOE can only know the sub-netting configuration of networks directly connected to the TOE's interfaces and therefore can only be aware of broadcast addresses on those networks.*

- ***The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier; and***

- ***The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the TOE.***

6.1.3.3 FDP_PUD Protection of user data

6.1.3.3.1 FDP_PUD_(EXT).1 Protection of user data

FDP_PUD_(EXT).1.1 When the administrator has enabled encryption, the TSF shall:

- encrypt authenticated user data transmitted to a wireless client from the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP.1(1)
- decrypt authenticated user data received from a wireless client by the radio interface of the wireless access system using the cryptographic algorithm(s) specified in FCS_COP.1(1).

Application Note: *This requirement allows the TOE administrator to require that all user data transmitted on the WLAN be encrypted using the cryptographic algorithms specified by FCS_COP.*

6.1.3.4 FDP_RIP Residual information protection

6.1.3.4.1 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: network packet objects.

Application Note: *This requirement ensures that the TOE does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet.*

6.1.4 Class FIA: Identification and authentication

6.1.4.1 FIA_AFL Authentication failures

6.1.4.1.1 FIA_AFL.1 Administrator authentication failure handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within the range of ***1 to 3*** of unsuccessful authentication attempts occur related to remote administrators logging on to the WLAN access system.

FIA_AFL.1.2 **Refinement:** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall prevent remote login on that logical interface by administrators until an action is taken by a local Administrator.

Application Note: *This requirement applies to remote administrator login and does not apply to the local login of the TOE, since it does not make sense to lock a local administrator's account in this fashion. For the purpose of the ST, remote administrator refers to administrators that do not have either Serial cable or local console access to the TOE.*

Application Note: *This requirement does NOT require that the TOE allow remote administration. However, if the TOE does allow administrators to login to the TOE remotely (e.g. from the wired interface or a management network) then*

it must provide a mechanism to prevent brute force attacks on the administrative account.

ST Application Note: *Lockouts are applied per interface (GUI, SSH) and not per user. For example, if one user locks out the SSH interface after exceeding the allowed number of login attempts, the SSH interface is locked out for all users, until the interface lockout is removed.*

6.1.4.2 FIA_ATD User attribute definition

6.1.4.2.1 FIA_ATD.1 (1) Administrator attribute definition

FIA_ATD.1.1 (1) The TSF shall maintain the following minimum list of security attributes belonging to individual administrators: ***username, password.***

6.1.4.2.2 FIA_ATD.1 (2) User attribute definition

FIA_ATD.1.1 (2) **Refinement:** The TSF shall maintain the following minimum list of security attributes belonging to individual remotely authenticated wireless users: ***username and shared secret***[38].

6.1.4.3 FIA_UAU User authentication

6.1.4.3.1 FIA_UAU.1 (1) Timing of authentication (Administrative user)

FIA_UAU.1.1 (1) **Refinement:** The TSF shall allow ***ICMP, ARP, DHCP, the passing of authentication data to and from the remote authentication server, TSF mediation in accordance with the Unauthenticated TOE Services SFP*** on behalf of the administrative user to be performed before the administrative user is authenticated.

Application Note: *Unauthenticated ICMP traffic to the TOE is allowed to support a commonly used service. An authorized administrator may disable this service*

When an ARP (Address Resolution Protocol) request packet is received from a user, the access point forwards it over all enabled interfaces except over the interface the ARP request packet was received .On receiving the ARP response packet, the access point database keeps a record of the destination address along with the receiving interface. With this information, the access point forwards any directed packet to the correct destination.

FIA_UAU.1.2 (1) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3.2 FIA_UAU.1 (2) Timing of authentication (Wireless user)

FIA_UAU.1.1 (2) **Refinement:** The TSF shall allow ***the passing of authentication data to and from the remote authentication server, TSF mediation in accordance with the Traffic Filter SFP*** on behalf of the wireless user to be performed before the wireless user is authenticated.

FIA_UAU.1.2 (2) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3.3 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to ***the default local administrative account using the fixed username "admin".***

[38] A shared secret may refer to a password for username/password based authentication or to a Pre-Shared Key (PSK) in the case of 802.11i authentication.

6.1.4.3.4 FIA_UAU_(EXT).5 Extended: multiple authentication mechanisms

FIA_UAU_(EXT).5.1 **Refinement** The TSF shall provide local authentication, and a remote authentication mechanism to perform user authentication. The TSF shall provide the following local authentication mechanisms:

1. local username and password-based authentication of local administrators connected via RS-232,
2. local username and password-based authentication of remote administrators connected via SSH,
3. local username and password-based authentication of remote administrators connected via HTTPS,
4. local manual PSK to perform wireless user and Mesh AP authentication,
5. local 802.1x EAP authentication using
    a. EAP-TLS that complies with RFC 5216,
    b. EAP-TTLSv0 (MD5, PAP and MS-CHAP-V2) that complies with RFC 5281, or
    c. PEAPv2 (EAP-GTC and EAP-MS-CHAP-V2) that complies with RFC draft-josefsson-pppext-eap-tls-eap-10

    to perform wireless user authentication using local user database,
6. local 802.1x EAP authentication using
    a. EAP-TTLS (PAP) that complies with RFC 5281, or
    b. PEAP (EAP-GTC)) that complies with draft-josefsson-pppext-eap-tls-eap-10

    to perform wireless user authentication using a remote LDAP user database.

The TSF shall provide the client to facilitate remote authentication via the following authentication protocols:

1. RADIUS that complies with RFCs 2138, 3579, and 3580

FIA_UAU_(EXT).5.2 The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

Application Note: *This extended requirement is needed for local administrators because there is disagreement over whether existing CC requirements specifically require the TSF provide authentication. That the TOE provide authentication is implied by other FIA_UAU requirements, and generally assumed to be a requirement when other FIA_UAU requirements are included in a TOE. In order to remove any potential confusion about this ST, an extended requirement for authentication has been included. This ST mandates that the TOE provide the client to facilitate remote authentication via an authentication server. The IT environment will provide the authentication server, and it is important to specify that the TSF must provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server.*

Since FIA_UAU_(EXT).5.1 and 5.2 require that the TSF provide authentication mechanisms, this extended requirement is needed with respect to the remote users to specify that the TSF invoke a remote authentication mechanism rather than provide it.

6.1.4.4 FIA_UID User identification

6.1.4.4.1 FIA_UID.2 User identification before any action

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

Application Note: *This requirement does not refer to management and control packets that must be allowed to pass between the WLAN client and the access system before authentication. It is assumed that this information is not user specific and therefore not covered by this requirement.*

Application Note: *It is also important to note that the identification credential presented to the authentication server (e.g. a user name) will be related to but not necessarily the same as the identification credential (e.g. MAC address of a remote system) that is used to enforce FDP_PUD_(EXT).*

6.1.4.5 FIA_USB User-subject binding

6.1.4.5.1 FIA_USB.1 User-subject binding.

FIA_USB.1.1 **Refinement:** The TSF shall associate the following administrative user security attributes with subjects acting on the behalf of that user: ***username***.

FIA_USB.1.2 **Refinement:** The TSF shall enforce the following rules on the initial association of an administrative user security attributes with subjects acting on the behalf of users: ***upon successful identification and authentication, the username shall be that of the user that has authenticated successfully***.

FIA_USB.1.3 **Refinement:** The TSF shall enforce the following rules governing changes to the administrative user security attributes associated with subjects acting on the behalf of users: ***no changes shall be allowed.***

6.1.5 Class FID: Intrusion Detection

6.1.5.1 FID_APD_EXT.1 Rogue Access Point Detection

FID_APD_EXT.1.1 The TSF shall be able to detect a Rogue Access Point operating within the radio coverage area of a 802.11 wireless network using the following detection method: ***Comparison of an AP MAC address detected during a scan of the wireless coverage area to a list of allowed AP MAC addresses; if the detected AP MAC address is not is not in the allowed list, it is a Rogue AP*** .

FID_APD_EXT.1.2 Upon detection of a Rogue Access Point, the TSF shall take the following actions:

- ***Notify the administrative user with a SNMP trap***
- ***Generate a syslog message***
- ***Add to the list of detected Rogue APs accessible by the administrative user via the CLI and/or Web UI***

6.1.6 Class FMT: Security management

6.1.6.1 FMT_MOF Management of functions in TSF

6.1.6.1.1 FMT_MOF.1 (1) Management of security functions behavior (Cryptographic Function)

FMT_MOF.1.1 (1) **Refinement:** The TSF shall restrict the ability to **modify the behavior of** the cryptographic functions

- ***Crypto: load a key***
- ***Crypto: delete/zeroize a key***
- ***Crypto: set a key lifetime***
- ***Crypto: set the cryptographic algorithm mode and key size***
- ***Crypto: execute self tests of TOE hardware and the cryptographic functions***

to ***administrator***.

6.1.6.1.2 FMT_MOF.1 (2) Management of security functions behavior (Audit Record Generation)

FMT_MOF.1.1 (2) The TSF shall restrict the ability to **enable, disable, and modify** the behavior of the functions

- ***Audit: pre-selection of the events which trigger an audit record,***
- ***Audit: start and stop of the audit function***

to ***administrator and SNMP administrator***.

6.1.6.1.3 FMT_MOF.1 (3) Management of security functions behavior (Authentication)

FMT_MOF.1.1 (3) The TSF shall restrict the ability to **modify** the behavior of the functions

- ***Auth: allow or disallow the use of an authentication server***
- ***Auth: set the number of authentication failures that must occur before the TOE takes action to disallow future logins***
- ***Auth: set the length of time a session may remain inactive before it is terminated***

to ***administrator and SNMP administrator***.

6.1.6.1.4 FMT_MOF.1 (4) Management of security functions behavior (Firewall)

FMT_MOF.1.1 (4) The TSF shall restrict the ability **to enable, disable, and modify the behavior** of the functions

- ***Enable and disable pre-configured filters***
- ***Create, change, and delete firewall rules***

to ***administrator and SNMP administrator***.

6.1.6.1.5 FMT_MOF.1 (5) Management of security functions behavior (Intrusion Detection)

FMT_MOF.1.1 (5) The TSF shall restrict the ability **to enable, disable, and modify the behavior** of the functions

- ***Rogue AP Detection Method***
- ***Rogue AP white listing***
- ***Display Rogue AP Details***

to ***administrator and SNMP administrator***.

6.1.6.1.6 FMT_MOF.1 (6) Management of security functions behavior (Communication and authentication protocol)

FMT_MOF.1.1 (6) The TSF shall restrict the ability **to modify the behavior** of the functions

- ***IPsec Phase 1 SA lifetime configuration***
- ***IPsec Phase 2 SA lifetime configuration***
- ***SSH timeout period configuration***
- ***SSH authentication failure limit configuration***
- ***Local authentication vs remote RADIUS authentication***

- ***Local database vs remote LDAP database***
- ***802.1x authentication method and EAP type configuration***
- ***SNMPv3 traps***

to ***administrator and SNMP administrator***, and

- ***SNMPv3 users and access***

to ***administrator.***

6.1.6.1.7 FMT_MOF.1 (7) Management of security functions behavior (Configuration File Import and Export)

FMT_MOF.1.1 (7) The TSF shall restrict the ability **to modify the behavior** of the functions

- ***Configuration file import and export***

to ***administrator and SNMP administrator***.

6.1.6.2 FMT_MSA Management of security attributes

6.1.6.2.1 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

6.1.6.2.2 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 **Refinement:** The TSF shall enforce the ***Traffic Filter SFP, Unauthenticated TOE Services SFP*** to provide **permissive** default values for information flow security attributes that are used to enforce the SFP.

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

6.1.6.3 FMT_MTD Management of TSF data

6.1.6.3.1 FMT_MTD.1 (1) Management of Audit pre-selection data

FMT_MTD.1.1 (1) **Refinement:** The TSF shall restrict the ability to query, ~~modify~~, clear, create the set of rules used to pre-select audit events to the administrator.

Application Note: Directly modifying audit pre-selection data is not supported. The administrator must clear the old rule and create a new rule instead.

6.1.6.3.2 FMT_MTD.1 (2) Management of authentication data (administrator)

FMT_MTD.1.1 (2) **Refinement:** The TSF shall restrict the ability to query, modify, delete, clear, create the authentication credentials, user identification credentials ~~to administrators~~ according to Table 13

Table 13 – Management of Authentication data

User	Authentication Credentials (passwords)	User Identification Credentials (usernames)
Admin superuser	• Query – none • Modify – SNMP, self, and regular administrators • Delete – SNMP and regular administrators (as part of removing account) • Clear – SNMP and regular administrators (as part of removing account) • Create – SNMP and regular administrators	• Query – SNMP, self, and regular administrators • Modify – SNMP, self, and regular administrators • Delete – SNMP and regular administrators (as part of removing account) • Clear – SNMP and regular administrators (as part of removing account) • Create – SNMP and regular administrators

Table 13 – Management of Authentication data		
User	Authentication Credentials (passwords)	User Identification Credentials (usernames)
Regular administrator	• Query- none • Modify – self and SNMP adminstrators • Delete – SNMP administrators • Clear – SNMP administrators • Create – self and SNMP administrators	• Query – self and SNMP adminstrators • Modify - self and SNMP adminstrators • Delete – SNMP administrators • Clear – SNMP administrators • Create – SNMP administrators
SNMP Adminstrators	• None	• None

6.1.6.4 FMT_SMF Specification of Management Functions

6.1.6.4.1 FMT_SMF.1 (1) Specification of management functions (Cryptographic Function)

FMT_SMF.1.1 (1) **Refinement:** The TSF shall be capable of performing the following security management functions: configure administrator authentication, query and set the encryption/decryption of network packets (via FCS_COP.1(1)) in conformance with the administrators configuration of the TOE.

Application Note: *This requirement ensures that those responsible for TOE administration are able to select an encryption algorithm identified in FCS_COP.1(1).*

6.1.6.4.2 FMT_SMF.1 (2) Specification of management functions (TOE Audit Record Generation)

FMT_SMF.1.1 (2) The TSF shall be capable of performing the following security management functions: query, enable or disable Security Audit.

Application Note: *This requirement ensures that those responsible for TOE administration are able to start or stop the TOE generation of audit records*

Application Note: *Auditing is an inherent function of the ToE; the only way to start or stop the audit function is to power up/down the ToE. The functions to perform shutdown/restart are restricted to administrator access.*

6.1.6.4.3 FMT_SMF.1 (3) Specification of management functions (Cryptographic Key Data)

FMT_SMF.1.1 (3) The TSF shall be capable of performing the following security management functions: query, set, modify, and delete the cryptographic keys and key data in support of FDP_PUD_(EXT).

Application Note: *The intent of this requirement is to provide the ability to configure the TOE's cryptographic key(s). Configuring the key data may include: setting key lifetimes, setting key length, etc.*

6.1.6.4.4 FMT_SMF.1 (4) Specification of management functions (Firewall)

FMT_SMF.1.1 (4) The TSF shall be capable of performing the following security management functions: ***enable, disable, and configure firewall rules and settings***.

Application Note: *This requirement ensures that those responsible for TOE administration are able to manage firewall configuration*

6.1.6.4.5 FMT_SMF.1 (5) Specification of management functions (Intrusion Detection)

FMT_SMF.1.1 (5) The TSF shall be capable of performing the following security management functions: ***enable, disable, and configure intrusion detection settings***.

Application Note: *This requirement ensures that those responsible for TOE administration are able to manage intrusion detection configuration*

6.1.6.4.6 FMT_SMF.1 (6) Specification of management functions (Communication Protocol)

FMT_SMF.1.1 (6) The TSF shall be capable of performing the following security management functions: ***configure communication protocol settings***.

Application Note: *This requirement ensures that those responsible for TOE administration are able to manage communication protocol configuration*

6.1.6.4.7 FMT_SMF.1 (7) Specification of management functions (Configuration File Import and Export)

FMT_SMF.1.1 (7) The TSF shall be capable of performing the following security management functions: ***configuration file import and export***.

6.1.6.5 FMT_SMR Security management roles

6.1.6.5.1 FMT_SMR.1 Security roles

FMT_SMR.1.1 **Refinement:** The TSF shall maintain the roles administrator, SNMP administrator, wireless user.

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

Application Note: *The only user allowed direct access to the TOE is the administrator. Wireless users can pass data through the TOE but do not have direct access. A role of wireless user is included in the TOE, but the scope of that role should be defined only to the extent necessary to support the activities of wireless users passing data through the TOE.*

This ST also assumes that the TOE will contain a local authentication mechanism and the capability to use a remote authentication server. Although users are sometimes referred to as local or remote, these references do not imply a role.

6.1.7 Class FPT: Protection of the TSF

6.1.7.1 FPT_STM Time stamps

6.1.7.1.1 FPT_STM_EXT.1 Reliable time stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps, synchronized via an external time source, for its own use.

Application Note: *The TOE must be capable of obtaining a time stamp via an NTP server.*

6.1.7.2 FPT_TST TSF self test

6.1.7.2.1 FPT_TST_EXT.1 Extended: TSF testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

6.1.7.2.2 FPT_TST.1 (1) TSF testing(for cryptography)

FPT_TST.1.1 (1) **Refinement:** The TSF shall run a suite of self-tests in accordance with FIPS PUB 140-2 during initial start-up (on power on), at the request of the cryptographic administrator (on demand), under various conditions defined in section 4.9.1

of FIPS 140-2, and periodically (at least once a day) to demonstrate the correct operation of the following cryptographic functions

- key error detection;
- cryptographic algorithms;
- RNG/PRNG

Application Note: *These tests apply regardless of whether the cryptographic functionality is implemented in hardware, software, or firmware.*

FPT_TST.1.2 (1) **Refinement:** The TSF shall provide authorized ~~users~~ cryptographic administrators with the capability to verify the integrity of **TSF data** related to the cryptography by using TSF-provided cryptographic functions

Application Note: *Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services*

FPT_TST.1.3 (1) **Refinement:** The TSF shall provide authorized ~~users~~ cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the cryptography by using TSF-provided cryptographic functions

Application Note: *Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services .*

6.1.7.2.3 FPT_TST.1 (2) TSF testing (for key generation components)

FPT_TST.1.1 (2) **Refinement:** The TSF shall perform self tests immediately after generation of a key to demonstrate the correct operation of each key generation component. If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited.

Application Note: *Key generation components are those critical elements that compose the entire key generation process (e.g., any algorithms, any RNG/PRNGs, any key generation seeding processes, etc.).*

Application Note: *These self-tests on the key generation components can be executed here as a subset of the full suite of self-tests run on the cryptography in FPT_TST.1(1) as long as all elements of the key generation process are tested.*

FPT_TST.1.2 (2) **Refinement:** The TSF shall provide authorized ~~users~~ cryptographic administrators with the capability to verify the integrity of **TSF data** related to the key generation by using TSF-provided cryptographic functions.

Application Note: *Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services*

FPT_TST.1.3 (2) **Refinement:** The TSF shall provide authorized ~~users~~ cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the key generation by using TSF-provided cryptographic functions.

Application Note: *Refer to FCS_COP.1.1(2) and FCS_COP.1.1(3) for TSF-provided cryptographic services .*

6.1.8 Class FTA: TOE access

6.1.8.1 FTA_SSL Session locking and termination

6.1.8.1.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1	The TSF shall terminate a local interactive or wireless session after an administrator configurable time interval of user inactivity.
Application Note:	*This requirement applies to both local administrative sessions and wireless users that pass data through the TOE.*

6.1.8.2 FTA_TAB TOE access banners

6.1.8.2.1 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1	Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.1.8.3 FTA_TSE TOE Session Establishment

6.1.8.3.1 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1	The TSF shall be able to deny session establishment based on ***the users authentication group, the WLAN being accessed, the time of day, and the day of week.***

6.1.9 Class FTP: Trusted path/channels

6.1.9.1 FTP_ITC Inter-TSF trusted channel

6.1.9.1.1 FTP_ITC_EXT.1 Inter-TSF trusted channel

FTP_ITC_EXT.1.1	The TOE shall provide an encrypted communication channel between itself and entities in the TOE IT Environment that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC_EXT.1.2	The TSF shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.
FTP_ITC_EXT.1.3	The TSF shall initiate communication via the trusted channel for all authentication functions, remote logging, time, ***configuration file import and export***.
Application Note:	*If a certificate authority server plays a role in the authentication of users, then the CA is considered an authorized IT entity and the TSF is expected to initiate secure communications with this entity. It is assumed that the IT environment includes an NTP server, an audit server and/or an authentication server.*

6.1.9.1.2 FTP_TRP Trusted path

6.1.9.1.3 FTP_TRP.1 Trusted path

FTP_TRP.1.1	The TSF shall provide a communication path between itself and wireless 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, replay or disclosure.
FTP_TRP.1.2	The TSF shall permit wireless client devices to initiate communication via the trusted path.

FTP_TRP.1.3	The TSF shall require the use of the trusted path for wireless user authentication, ***remote TOE administration.***
Application Note:	*This requirement ensures that the initial exchange of authentication information between the wireless client and the access system is protected.*

6.2 Security Assurance Requirements for the TOE

This Security Target is Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 as shown in Table 14 – Assurance Requirements below. The security assurance requirements for the TOE consist of the following components that are CC Part 3 conformant as summarized in Table 14 below and detailed in the following subsections. These requirements are included by reference.

Table 14 – Assurance Requirements

Assurance Class	Assurance Component	Assurance Components Description
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life-cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2[39]	Flaw Reporting Procedures
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Analysis of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

[39] ALC_FLR.2 is an augmentation over EAL-2

6.3 Security Requirements Rationale

6.3.1 Security Function Requirements Rationale

Table 15 - TOE SFR/SAR to Objective Mapping satisfies the requirement to trace each SFR back to the security objectives for the TOE.

Table 15 - TOE SFR/SAR to Objective Mapping																		
		TOE Objective																
#	SFR/SAR	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_DENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	O.ROGUE_AP_DETECTION
1	FAU_GEN.1		X															
2	FAU_GEN.2		X															
3	FAU_SEL.1		X															
4	FCS_BCM_(EXT).1					X	X											
5	FCS_CKM.1(1)					X	X											
6	FCS_CKM.1(2)					X	X											
7	FCS_CKM.2					X	X											
8	FCS_CKM_(EXT).2					X	X						X					
9	FCS_CKM.4					X	X						X					
10	FCS_COP.1 (1)					X	X											
11	FCS_COP.1 (2)					X	X											
12	FCS_COP.1 (3)					X	X											
13	FCS_COP.1 (4)					X	X											
14	FCS_COP_(EXT).1					X	X											
15	FCS_COMM_PROT_EXT.1					X	X											
16	FCS_EAP-TLS_EXT.1					X	X											
17	FCS_EAP-TTLS_EXT.1					X	X											
18	FCS_HTTPS_EXT.1					X	X											
19	FCS_IPSEC_EXT.1					X	X											
20	FCS_PEAP_EXT.1					X	X											
21	FCS_RAD_EXT.1					X	X											
22	FCS_SFTP_EXT.1					X	X											
23	FCS_SNMPV3_EXT.1					X	X											
24	FCS_SSH_EXT.1					X	X											
25	FCS_TLS_EXT.1					X	X											
26	FDP_IFC.1 (1)										X							
27	FDP_IFC.1 (2)										X							
28	FDP_IFF.1-NIAP-0417 (1)										X							
29	FDP_IFF.1-NIAP-0417 (2)										X							
30	FDP_PUD_(EXT).1										X							
31	FDP_RIP.1												X					

Table 15 - TOE SFR/SAR to Objective Mapping																		
		TOE Objective																
#	SFR/SAR	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_DENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	O.ROGUE_AP_DETECTION
32	FIA_AFL.1															X		
33	FIA_ATD.1 (1)															X		
34	FIA_ATD.1 (2)															X		
35	FIA_UAU.1 (1)										X							
36	FIA_UAU.1 (2)															X		
37	FIA_UAU.4										X					X		
38	FIA_UAU_(EXT).5										X					X		
39	FIA_UID.2										X					X		
40	FIA_USB.1		X															
41	FID_APD_EXT.1																	X
42	FMT_MOF.1 (1)									X								
43	FMT_MOF.1 (2)									X								
44	FMT_MOF.1 (3)									X								
45	FMT_MOF.1 (4)									X								
46	FMT_MOF.1 (5)									X								
47	FMT_MOF.1 (6)									X								
48	FMT_MOF.1 (7)									X								
49	FMT_MSA.2									X								
50	FMT_MSA.3									X								
51	FMT_MTD.1 (1)									X								
52	FMT_MTD.1 (2)									X								
53	FMT_SMF.1 (1)									X								
54	FMT_SMF.1 (2)									X								
55	FMT_SMF.1 (3)									X								
56	FMT_SMF.1 (4)									X								
57	FMT_SMF.1 (5)									X								
58	FMT_SMF.1 (6)									X								
59	FMT_SMF.1 (7)									X								
60	FMT_SMR.1									X								
61	FPT_STM_(EXT).1		X												X			
62	FPT_TST_EXT.1				X													
63	FPT_TST.1 (1)				X													
64	FPT_TST.1 (2)				X													
65	FTA_SSL.3															X		
66	FTA_TAB.1							X										
67	FTA_TSE.1															X		
68	FTP_ITC_EXT.1		X													X		
69	FTP_TRP.1															X		
	ADV_ARC.1													X				
	ADV_FSP.2								X									

Table 15 - TOE SFR/SAR to Objective Mapping																		
		TOE Objective																
#	SFR/SAR	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_DENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	O.ROGUE_AP_DETECTION
	ADV_TDS.1								X									
	AGD_OPE.1	X																
	AGD_PRE.1	X																
	ALC_CMC.2			X														
	ALC_CMS.2			X														
	ALC_DEL.1	X																
	ALC_FLR.2			X														
	ATE_COV.1											X						
	ATE_FUN.1											X						
	ATE_IND.2											X						
	AVA_VAN.2																X	

6.3.1.1 Security Function Requirements Rationale

The following paragraphs present the rationale that demonstrates that the SFRs meet all security objectives for the TOE.

O.ADMIN_GUIDANCE

ALC_DEL.1 ensures that the administrator has the ability to begin their TOE installation with a *clean* (e.g., malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE

The AGD_PRE.1 requirement ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The Installation, Generation and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration.

The AGD_OPE.1 requirement mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a description of how to set up and use the auditing features of the TOE.

AGD_OPE.1 AND AGD_PRE.1 analysis during evaluation will ensure that the guidance documentation can be followed unambiguously to ensure the TOE is not misconfigured in an insecure state due to confusing guidance.

O.AUDIT_GENERATION

FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this ST.

FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.

FAU_SEL.1 allows for the selection of events to be audited. This requires that the criteria used for the selection of auditable events to be defined. For example, the user identity can be used as selection criterion for the events to be audited.

FIA_USB.1 plays a role is satisfying this objective by requiring a binding of security attributes associated with users that are authenticated with the subjects that represent them in the TOE. This only applies to authorized users, since the identity of unauthenticated users cannot be confirmed. Therefore, the audit trail may not always have the proper identity of the subject that causes an audit record to be generated (e.g., presumed network address of an unauthenticated user may be a spoofed address).

FPT_STM_(EXT).1 supports the audit functionality by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events.
FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE IT environment (the audit server and the time server).

O.CONFIGURATION_IDENTIFICATION

ALC_CMC.2 contributes to this objective by requiring the developer have a configuration management plan that describes how changes to the TOE and its evaluation deliverables are managed.

ALC_CMS.2 is necessary to define the items that must be under the control of the CM system. This requirement ensures that the TOE implementation representation, design documentation, test documentation (including the executable test suite), user and administrator guidance, and CM documentation are tracked by the CM system.

ALC_FLR.2 plays a role in satisfying this objective by requiring the developer to have procedures that address flaws that have been discovered in the product, either through developer actions (e.g., developer testing) or discovery by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis to ensure new flaws are not created while fixing the discovered flaws.

O.CORRECT_TSF_OPERATION

FPT_TST_(EXT).1 is necessary to ensure the correctness of the TSF software and TSF data. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce its security policies. The FPT_TST.1(1) for crypto and FPT_TST.1(2) for key generation functional requirement has been included to address the critical nature and specific handling of the cryptographic related TSF data. Since the cryptographic TSF data has specific FIPS PUB

requirements associated with them it is important to ensure that any fielded testing on the integrity of these data maintains the same level of scrutiny as specified in the FCS functional requirements.

O.CRYPTOGRAPHY

Baseline cryptographic services are provided in the TOE by NIST CAVP compliant algorithms implemented in hardware, in software, or in hardware/software combinations [FCS_BCM_(EXT).1].

Contributing to this objective, the requirements for each of the cryptographic communications protocols and authentication protocols are more exactly specified with the following:

- FCS_COMM_PROT_EXT.1 , Communications Protection
- FCS_EAP-TLS_EXT.1 , EAP-TLS Authentication Protocol
- FCS_EAP-TTLS_EXT.1 , EAP-TLS Authentication Protocol
- FCS_HTTPS_EXT.1 , HTTPS
- FCS_IPSEC_EXT.1 , Internet Protocol Security (IPsec)
- FCS_PEAP_EXT.1 , PEAP Authentication Protocol
- FCS_RAD_EXT.1 , RADIUS Authentication Protocol
- FCS_SFTP_EXT.1 , SSH File Transfer Protocol
- FCS_SMMPV3_EXT.1,SNMPv3
- FCS_SSH_EXT.1 , SSH
- FCS_TLS_EXT.1 , TLS

The cryptographic services offered by this baseline capability are augmented and customized in the TOE to support medium robustness environments. These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys [FCS_CKM.1 (1)], and the generation of asymmetric keys [FCS_CKM.1 (2)]; methods of manual and automated cryptographic key distribution [FCS_CKM.2]; cryptographic key destruction [FCS_CKM.4]; techniques for cryptographic key validation and packaging [FCS_CKM.1]; and cryptographic key handling and storage [FCS_CKM_(EXT).2]. Specific functional requirements in the area of cryptographic operations address data encryption and decryption [FCS_COP.1 (1)]; cryptographic signatures [FCS_COP.1 (2)]; cryptographic hashing [FCS_COP.1 (3)]; cryptographic key agreement [FCS_COP.1 (4)]; and improved random number generation [FCS_COP_(EXT).1].

O.CRYPTOGRAPHY_VALIDATED

Baseline cryptographic services are provided in the TOE by NIST CAVP compliant algoithms implemented in hardware, in software, or in hardware/software combinations [FCS_BCM_(EXT).1]. These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys [FCS_CKM.1 (1)], and the generation of asymmetric keys [FCS_CKM.1 (2)]; methods of manual and automated cryptographic key distribution [FCS_CKM.2]; cryptographic key destruction [FCS_CKM.4]; techniques for cryptographic key validation and packaging [FCS_CKM.1]; and cryptographic key handling and storage [FCS_CKM_(EXT).2]. Specific functional requirements in the area of cryptographic operations address data encryption and decryption [FCS_COP.1 (1)]; cryptographic signatures [FCS_COP.1 (2)]; cryptographic hashing [FCS_COP.1 (3)]; cryptographic key agreement [FCS_COP.1 (4)]; and improved random number generation [FCS_COP_(EXT).1].

O.DISPLAY_BANNER

FTA_TAB.1 meets this objective by requiring that the TOE display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the administrator, who can specify any warnings regarding unauthorized use of the TOE and remove any product or version information if they desire. The only time that it is envisioned that an authenticated session would need to be established is for the performance of TOE administration. Bannering is not necessary prior to use of services that pass network traffic through the TOE.

O.DOCUMENTED_DESIGN

ADV_FSP.2 and ADV_TDS.1 support this objective by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered.

ADV_TDS.1 and ADV_FSP.2 are also used to ensure that the TOE design is consistent across the Design and the Functional Specification.

O.MANAGE

The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirements' rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions.

FMT_MOF.1 (1), (2), (3), (4), (5), (6) and (7) ensure that the administrator has the ability manage the cryptographic, audit, authentication, Firewall, Intrusion Detection functions, communication and authentication, and configuration file import and export functions.

FMT_MSA.2 provides the administrator the ability to accept only secure values and modify security attributes.

FMT_MSA.3 provides no mechanism to supply alternative initial values to override the default restrictive values for information flow security attributes.

FMT_MTD.1(1), (2), and (3) ensure that the administrator can manage TSF data.

FMT_SMR.1 defines the specific security roles to be supported.

FMT_SMF.1 (1), (2), (3), (4), (5), (6) and (7) support this objective by identifying the management functions for cryptographic data, audit records, cryptographic key data, Firewall, Intrusion Detection, and communication and authentication protocols, and configuration file import and export functions.

O.MEDIATE

FIA_UAU.1 (2), FIA_UAU_(EXT).5 and FIA_UID.2 ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the wireless user.

FDP_IFC.1 (1), (2) and FDP_IFF.1-NIAP-0417 (1) and (2) ensure that the TOE has the ability to mediate packet flow of the wireless user based upon rules established by the administrator.

FDP_PUD_(EXT).1 allows the administrator to control whether or not unencrypted data will be allowed to pass through the TOE.

O.PARTIAL_FUNCTIONAL_TESTING

ATE_FUN.1 requires the developer to provide the necessary test documentation to allow for an independent analysis of the developer's security functional test coverage. In addition, the developer must provide the test suite executables and source code, which the evaluator uses to independently verify the vendor test results and to support of the test coverage analysis activities.

ATE_COV.1 requires the developer to provide a test coverage analysis that demonstrates the extent to which the TSFI are tested by the developer's test suite. This component also requires an

independent confirmation of the extent of the test suite, which aids in ensuring that correct security relevant functionality of a TSFI is demonstrated through the testing effort.

ATE_IND.2 requires an independent confirmation of the developer's test results by mandating that a subset of the test suite be run by an independent party. This component also requires an independent party to craft additional functional tests that address functional behavior that is not demonstrated in the developer's test suite. Upon successful completion of these requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.

O.RESIDUAL_INFORMATION

FDP_RIP.1 is used to ensure the contents of resources are not available once the resource is reallocated. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data).

FCS_CKM_(EXT).2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.1, in that when a cryptographic key is moved from one location to another (e.g., calculated in some scratch memory and moved to a permanent location) that the memory area is immediately cleared as opposed to waiting until the memory is reallocated to another subject.

FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to a user.

O.SELF_PROTECTION

ADV_ARC.1 provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs. Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation.

O.TIME_STAMPS

FPT_STM_(EXT).1 requires that the TOE be able to obtain reliable time stamps for its own use and therefore, partially satisfies this objective. Time stamps include date and time, and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.

O.TOE_ACCESS

FIA_UID.2 plays a role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions. In most cases, the identification cannot be authenticated (e.g., a user attempting to send a data packet through the TOE that does not require authentication. It is impractical to require authentication of all users that attempt to send data through the TOE, therefore, the requirements specified in the TOE require authentication where it is deemed necessary. This does impose some risk that a data packet was sent from an identity other than that specified in the data packet.

FIA_UAU.1 (1), FIA_UAU.4, and FIA_UAU_(EXT).5 contribute to this objective by ensuring that administrators and users are authenticated before they are provided access to the TOE or its services, with the exception of specified functions, and that the default password shipped with the TOE is changed at first use.

In order to control logical access to the TOE an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to

login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable).

FIA_AFL.1 ensures that the TOE can protect itself and its users from brute force attacks on their authentication credentials.

FIA_ATD.1 (1) and (2) Management requirements provide additional control to supplement the authentication requirements.

FTA_SSL.3 ensures that inactive user and administrative sessions are dropped.

FTA_TSE.1 ensures that wireless users can only access the TOE during authorized time periods

FTP_TRP.1 ensures that remote users have a trusted path in order to authenticate. FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE IT environment (the remote authentication server)

O.VULNERABILITY_ANALYSIS

The AVA_VAN.2 component provides the necessary level of confidence that vulnerabilities do not exist in the TOE that could cause the security policies to be violated. AVA_VAN.2 requires the evaluator to perform a search for potential vulnerabilities in all the TOE deliverables. For those vulnerabilities that are not eliminated by the developer, a rationale must be provided that describes why these vulnerabilities cannot be exploited by a threat agent with a basic attack potential, which is in keeping with the desired assurance level of this TOE. This component provides the confidence that security flaws do not exist in the TOE that could be exploited by a threat agent of basic attack potential to violate the TOE's security policies. For this TOE, the vulnerability analysis is specified for an attack potential of basic.

This requirement ensures the evaluator has performed an analysis of the authentication mechanism to ensure the probability of guessing a user's authentication data would require a medium-attack potential, as defined in Annex B of the CEM.

O.ROGUE_AP_DETECTION

FID_APD_EXT.1 ensures the TOE is able to detect a Rogue Access Point operating within the radio coverage area of a 802.11 wireless network, and specifies the actions taken when detected.

6.3.1.2 Security requirement dependency analysis

Table 16 - SFR Component Dependency Mapping maps the dependencies that exist for each SFR. If the column labeled “satisfied” shows a dependency that has not been resolved, the rationale is provided in the text following the table, why this dependency does not apply for the TOE.

Table 16 - SFR Component Dependency Mapping

#	Component	Dependencies	Satisfied
1	FAU_GEN.1	FPT_STM.1	FPT_STM_(EXT).1
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
3	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	FAU_GEN.1 FMT_MTD.1(1)
4	FCS_BCM_(EXT).1	None	None
5	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP_(EXT).1 FCS_CKM.4 FMT_MSA.2
6	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP_(EXT).1 FCS_CKM.4 FMT_MSA.2
7	FCS_CKM.2	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2	FCS_CKM.1(1), (2) FMT_MSA.2
8	FCS_CKM_(EXT).2	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2	FCS_CKM.1(1), (2) FMT_MSA.2
9	FCS_CKM.4	FTP_ITC.1 or FCS_CKM.1] FMT_MSA.2	FCS_CKM.1(1), (2) FMT_MSA.2
10	FCS_COP.1(1)	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1(1), FCS_CKM.4 FMT_MSA.2
11	FCS_COP.1(2)	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1(2), FCS_CKM.4 FMT_MSA.2
12	FCS_COP.1(3)	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	No FCS_CKM.4 FMT_MSA.2
13	FCS_COP.1(4)	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1(2), FCS_CKM.4 FMT_MSA.2
14	FCS_COP_(EXT).1	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	No FCS_CKM.4 FMT_MSA.2
15	FCS_COMM_PROT_EXT.1	None	None
16	FCS_EAP-TLS_EXT.1	FCS_TLS_EXT.1	None
17	FCS_EAP-TTLS_EXT.1	FCS_TLS_EXT.1	None
18	FCS_HTTPS_EXT.1	None	None
19	FCS_IPSEC_EXT.1	None	None
20	FCS_PEAP_EXT.1	FCS_TLS_EXT.1	None
21	FCS_RAD_EXT.1	FCS_IPSEC_EXT.1	None
22	FCS_SFTP_EXT.1	FCS_SSH_EXT.1	None
23	FCS_SNMPV3_EXT.1	None	None
24	FCS_SSH_EXT.1	None	None
25	FCS_TLS_EXT.1	None	None

Table 16 - SFR Component Dependency Mapping			
#	Component	Dependencies	Satisfied
26	FDP_IFC.1 (1)	FDP_IFF.1	FDP_IFF.1-NIAP-0417 (1)
27	FDP_IFC.1 (2)	FDP_IFF.1	FDP_IFF.1-NIAP-0417 (2)
28	FDP_IFF.1-NIAP-0417 (1)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 (1) FMT_MSA.3
29	FDP_IFF.1-NIAP-0417 (2)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 (2) FMT_MSA.3
30	FDP_PUD_(EXT).1	None	None
31	FDP_RIP.1	None	None
32	FID_APD_EXT.1	None	None
33	FIA_AFL.1 (1)	FIA_UAU.1	FIA_UAU.1 (1), (2)
34	FIA_ATD.1 (1)	None	None
35	FIA_ATD.1 (2)	None	None
36	FIA_UAU.1 (1)	FIA_UID.1	FIA_UID.2
37	FIA_UAU.1 (2)	FIA_UID.1	FIA_UID.2
38	FIA_UAU.4	None	None
39	FIA_UAU_(EXT).5	None	None
40	FIA_UID.2	None	None
41	FIA_USB.1	FIA_ATD.1	FIA_ATD.1(1), (2)
42	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1(1) FMT_SMR.1
43	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1(2) FMT_SMR.1(1)
44	FMT_MOF.1(3)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1(3) FMT_SMR.1
45	FMT_MOF.1(4)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1(4) FMT_SMR.1
46	FMT_MOF.1(5)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1(5) FMT_SMR.1
47	FMT_MOF.1(6)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1(6) FMT_SMR.1
48	FMT_MOF.1(7)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1(7) FMT_SMR.1
49	FMT_MSA.2[40]	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_IFC.1 No FMT_SMR.1
50	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	No FMT_SMR.1
51	FMT_MTD.1(1)	FMT_SMR.1	FMT_SMR.1
52	FMT_MTD.1(2)	FMT_SMR.1	FMT_SMR.1
53	FMT_SMF.1(1)	None	None
54	FMT_SMF.1(2)	None	None
55	FMT_SMF.1(3)	None	None
56	FMT_SMF.1(4)	None	None
57	FMT_SMF.1(5)	None	None
58	FMT_SMF.1(6)	None	None
59	FMT_SMF.1(7)	None	None
60	FMT_SMR.1(1)	FIA_UID.1	FIA_UID.2
61	FPT_STM_(EXT).1	None	None
62	FPT_TST_EXT.1	None	None
63	FPT_TST.1(1)	None	None
64	FPT_TST.1(2)	None	None
65	FTA_SSL.3	None	None
66	FTA_TAB.1	None	None

[40] The dependency on ADV_SPM.1was removed by the ST author, it is assumed this was an error.

Table 16 - SFR Component Dependency Mapping			
#	Component	Dependencies	Satisfied
67	FTA_TSE.1	None	None
68	FTP_ITC_EXT.1	None	None
69	FTP_TRP.1	None	None

Rationale for unsatisfied dependencies:

Each functional requirement, including extended requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. With the exception of dependencies related to FCS_COP.1(3), FCS_COP_(EXT).1, FMT_MSA.1, and FMT_MSA.2, all dependencies in this ST have been satisfied.

FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing) is an algorithm and does not require FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation; therefore these dependencies are not required to be satisfied.

The TOE's implementation of FCS_COP_(EXT).1, Random Number Generation, is an algorithm that does not require FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation; therefore these dependencies are not required to be satisfied.

The dependency that FMT_MSA.2 and FMT_MSA.3 have on FMT_MSA.1 is not required because the administrator is the only role allowed direct access to the TOE management functions. This is implemented using identification and authentication, no access control SFP is implemented; therefore, this dependency is not required.

6.3.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the Common Criteria EAL2 assurance package augmented with ALC_FLR.2. The Common Criteria allows assurance packages to be augmented, which allows the addition of assurance components from the Common Criteria not already included in the EAL.

Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures and correcting security flaws (ALC_FLR.2). The EAL chosen is based on the statement of the security environment (threats, organizational policies, assumptions) and the security objectives defined in this ST. The sufficiency of the EAL chosen (EAL2 augmented) is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE

Given the amount of assurance deemed necessary to meet the security environment and objectives of the TOE and the intent of EAL 2, EAL 2 is an appropriate level of assurance for the TOE described in this ST. Therefore, EAL2 augmented is an appropriate level of assurance for the TOE.

Table 17 shows the matrix of Security Assurance requirements; the ST assurance levels are shown in **BOLD** text, which clearly demonstrates that this Security Target meets EAL2+.

Table 17 - Evaluation assurance level summary								
Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	1	**2**	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1

Table 17 - Evaluation assurance level summary								
Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
	ADV_TDS		**1**	2	3	4	5	6
Guidance Documents	AGD_OPE	1	**1**	1	1	1	1	1
	AGD_PRE	1	**1**	1	1	1	1	1
Life-cycle Support	ALC_CMC	1	**2**	3	4	4	5	5
	ALC_CMS	1	**2**	3	4	5	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	**1**	1	1	1	1	1
	ASE_ECD	1	**1**	1	1	1	1	1
	ASE_INT	1	**1**	1	1	1	1	1
	ASE_OBJ	1	**2**	2	2	2	2	2
	ASE_REQ	1	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	1	**1**	1	1	1	1	1
Tests	ATE_COV		**1**	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		**1**	1	1	1	2	2
	ATE_IND	1	**2**	2	2	2	2	3
Vulnerability Assessment	AVA_VAN	1	**2**	2	3	4	5	5

Table 18 - SAR Component Dependency Mapping, maps the dependencies that exist for each SAR to demonstrate all SAR dependencies are satisfied.

Table 18 - SAR Component Dependency Mapping		
Component	Dependencies	Satisfied
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	Yes – ADV_FSP.2 Yes – ADV_TDS.1
ADV_FSP.2	ADV_TDS.1	Yes – ADV_TDS.1
ADV_TDS.1	ADV_FSP.2	Yes - ADV_FSP.2
AGD_OPE.1	ADV_FSP.1	Yes - ADV_FSP.2
AGD_PRE.1	None	--
ALC_CMC.2	ALC_CMS.1	Yes – ALC_CMS.2
ALC_CMS.2	None	--
ALC_DEL.1	None	--
ALC_FLR.2	None	--
ATE_COV.2	ADV_FSP.2 ATE_FUN.1	Yes – ADV_FSP.2 Yes - ATE_FUN.1
ATE_FUN.1	ATE_COV.1	Yes - ATE_COV.1
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	Yes – ADV_FSP.2 Yes – AGD_OPE.1 Yes – AGD_PRE.1 Yes – ATE_COV.1 Yes - ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1	Yes - ADV_ARC.1 Yes - ADV_FSP.2 Yes - ADV_TDS.1 Yes – AGD_OPE.1

Table 18 - SAR Component Dependency Mapping		
	AGD_PRE.1	Yes - AGD_PRE.1

7 TOE Summary Specification

7.1 Implementation description of TOE SFRs

This section provides evaluators and potential consumers of the TOE with a high-level description of each SFR, thereby enabling them to gain a general understanding of how the TOE is implemented. These descriptions are intentionally not overly detailed, thereby disclosing no proprietary information. This sections refers to SFRs defined in Section 6.1, Security Function Requirements.

7.2 TOE Security Functions

The TFS supports the following security functions:

- Security Audit
- Cryptographic Support
- User data protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels
- Rogue AP Detection

7.2.1 Security Audit

7.2.1.1 Audit Generation

The TOE has the ability to selectively generate audit records from potentially security relevant events and transmit these records to the audit server in the environment. The TOE uses Syslog format messages implemented using the busybox tool set.

Busybox combines versions of many common UNIX utilities into a single small executable; however, they have fewer options than their full-featured equivalents.

Syslog messages at level 5 - LOG_NOTICE are used to satisfy the requirements for the content of audit records. Audit events include the date and time of the event, type of event, subject identify (if applicable), outcome (success or failure) of the event; some events require additional information as specified in FAU_GEN.1. The TOE supports user subject binding, associating each user to all program execution on behalf of that user, therefore, the user identity can always be associated to an audit event.

Table 19 – Syslog Support, shows the syslog levels supported; audit records are those tagged with Syslog level 5.

Table 19 – Syslog Support

Syslog level	Description
0 - LOG_EMERG	An emergency condition. The system is unusable
1 - LOG_ALERT	This message warrants an immediate action
2 - LOG_CRIT	Critical Condition
3 - LOG_ERR	Error
4 - LOG_WARNING	Warning
5 - LOG_NOTICE	Normal but a significant condition
6 - LOG_INFO	Information only
7 - LOG_DEBUG	This message appears only during debug mode

The TOE is dependent on an audit server in the IT Environment (a Syslog server) for the storage; the tools to review audit logs, the protection of audit logs from overflow, and the restriction of access to audit logs. All levels of Syslog messages are transmitted to the audit server in the IT environment immediately after generation, the audit server must filter the syslog messages (for level 5) to obtain just audit records.

The TOE can configure only one Syslog server; no backup servers can be configured. If the connection to the Syslog server goes down, or the Syslog server is unable to receive Syslog messages for any reason, the logs continue to be logged locally. The log messages generated during the time the Syslog server is unavailable will not be sent to the server when it is restored, but will be stored in the local file system (tmpfs(rw)) in the file /var/log/messages; the maximum size of this file is 100KB. Once this file is full, it is moved to the file /var/log/messages.0 and new logs continue to get written to /var/log/messages. If the file /var/log/messages fill again, it is again moved to /var/log/messages.0, overwriting the file, and the previous log messages are permanently lost. This effectively gives the administrator 200KB of effective storage before log messages are lost.

The file system used for audit record storage is temporary (tmpfs), therefore, the locally archived logs are available only until the next reboot.

The network connection between the TOE and the external audit server is required to be secured using the IPSec security protocol. If the IPsec tunnel has not been established, no Syslog messages will be sent to the Audit Server. If the IPsec connection fails between the TOE and the Audit Server, a SNMP trap is generated and set to the SNMP server in the IT Environment to notify the administrator. If the Audit Server fails but the IPsec tunnel remains intact, no notification is sent.

FAU_GEN.1, FAU_GEN.2

The time stamp used for audit records is covered in Section 7.2.6.1, Reliable Time Stamps.

7.2.1.2 Selective Audit generation

The TOE provides the ability to include/exclude events using filters based on the following parameters. A maximum of 10 filters can be created.

1. Filter precedence number (index ranging from 1 to 10)
2. Log/not-log to an external syslog server
3. User who initiated operation (username)
4. How this user is logged into the system (device interface). Device interface is defined as management interface or login source
    a. console (CLI),
    b. Network – SSH (CLI via wired or wireless), Web UI (via wired or wireless)
        i. IP address (available for wired or wireless)
        ii. MU MAC address (wireless only)
    c. any, any of the above
5. The IP address (IPaddr) of the remote client used for management
6. The MAC address of Mobile unit used to do the operation

Parameter 3, 4, 5 & 6 can take wildcard value as 'any'. The IP address and username can be used as user identities. They can be used independently or can be used together (using an OR operation) to filter audit records.

The event type is not included in the filtering criteria listed above, however, the administrator has the option to set the log-levels (event type) separately. By default, the log-level is 5 (LOG_NOTICE). This covers all the audit logs originating from configuration change or management commands. Event types for the logs are given in Table 19 – Syslog Support. Level 5 (LOG_NOTICE) satisfies the requirements for the content of the audit records.

If filter rule matches for some operation, the outcome will depend on the 'log' or 'not-log' parameter of that filter.

Filter precedence is a rule index between 1 to 10 where 1 indicates high precedence, 10 indicates low precedence. The precedence number can be used to permit, deny or see details of a filter. The rule that has the highest filter precedence number will be followed if all the other parameters are same.

Example:

A rule is configured to not to log for <MAC ADDRESS> with lesser precedence number.
#set audit-filter 5 no-log <username> network any

Another rule is configured to log messages with this MAC address & it has higher precedence.
#set audit-filter 1 log <username> network 00:11:22:33:44:55:66
Because the second rule has higher precedence number, the audit log will be generated for that particular <MAC ADDRESS>

CLI commands are available to create, delete and display filters. **FAU_SEL.1**

7.2.2 Cryptographic Support

The TOE utilizes cryptographic functions for the purposes of data protection using the 802.11i standard, SSHv2, SFTP, SNMPv3, TLS1.0-based trusted paths used for the TOE administration, as well as for the IPSec-based trusted channel established between the TOE and external authentication, audit and time servers. **FCS_COMM_PROT_EXT.1**

The TOE implements most cryptographic operations using openSSL. AES-CCMP and SHA for 802.11 are implemented by the hardware microprocessor, Cavium Octeon CN5010.

The TOE cryptographic algorithms are NIST CAVP validated as indicated by the certificate numbers listed below. **FCS_BCM_(EXT).1**

The following algorithms (Certificate #) were validated:

- AES (Certificates #2752, #861, and #1114) **FCS_COP.1.1 (1)**
- Triple-DES (Certificates #1655) **FCS_COP.1.1 (1)**
- SHS (Certificate #2320) **FCS_COP.1.1 (3)**
- HMAC (Certificates #1725)
- RSA (Certificate #1442) **FCS_CKM.1.1(2)**, **FCS_COP.1.1 (2)**
- RNG (Certificates #1267) **FCS_COP_(EXT).1.1 , FCS_CKM.1.1(1), (2)**
- KDF (Certificates #20, #186, #187, #188, #189)

The TOE supports distributing cryptographic keys manually through the local serial port connection, and automatically through a remote SSH connection, as well as through the remote Web UI.

When not in use, the TOE stores the following persistent secrets, and private keys in encrypted form using the AES128 algorithm using a master encryption key:

- Admin password
- Switch Discovery Passphrase (AAP)
- LDAP server password
- pam (authentication) radius shared secret
- Radius Server - HotSpot Primary/Secondary Secret
- Accounting Radius Server HS Secret
- IKE Preshare Key (authentication passphrase)
- WAN PPPoE password
- WAN DynDNS Password
- RIP MD5 key
- RIP password

- LAN 802.1x EAP authentication Password
- Proxy realm
- Radius client secret
- Radius user id
- EAP External Accounting Secret
- EAP Primary/Secondary Secret

The master encryption key used to encrypt and decrypt the persistent secrets and private keys listed above is generated using a proprietary algorithm.

The following persistent secret and private keys are stored using split knowledge procedures when not in use:

- CCMP Key
- VPN SPD Outbound ESP Encryption Key
- VPN SPD Outbound ESP Authentication Key
- VPN SPD Outbound AH Authentication Key
- VPN SPD Inbound ESP Encryption Key
- VPN SPD Inbound ESP Authentication Key
- VPN SPD Inbound AH Authentication Key

The TOE will check the public key validity time on export, and will not allow export or backup of expired certificates or public keys. **FCS_CKM_(EXT).2**

The TOE uses openSSL to implement the ANSI X9.31 NIST CAVP approved random number generator; ANSI X9.31 uses a PRNG seed be based on the system time to ensure the Initialization Vector never repeats. The TOE implements this requirement using the Gettimeofday() function to generate a 64 bit seed; this function uses the underlying hardware real time clock. The TOE protects the integrity of the generated keys using physical security mechanisms and by performing a key integrity check on start up and periodically once a day. **FCS_BCM_(EXT).1**

A key zeroisation function implemented by the module zeroizes all cryptographic keys and critical security parameters by overwriting the storage area three times with an alternating pattern for all memory except RAM. For RAM memory, zeroisation is performed by a single direct overwrite consisting of a pseudo random pattern.
All intermediate storage areas for cryptographic keys and critical security parameters are zeroized upon the transfer of the key or CSP to another location. **FCS_CKM.4**
The module implements an administrator command to manually input/output cryptographic keys, including the IPSec pre-shared keys and RADIUS authentication key.

7.2.2.1 Cryptographic support for 802.11i

The TOE implements the 802.11i standard to protect user data being transmitted between wireless mobile devices and the TOE; it supports manual PSK and the following Extensible Authentication Protocol (EAP) methods:

- EAP-Transport Layer Security (EAP-TLS)
- EAP-Tunneled Transport Layer Security (EAP-TTLS) , and
- EAP-Protected Extensible Authentication Protocol, EAP-PEAP

EAP_TLS, EAP_TTLS, and EAP-PEAP implement key exchange using the Diffie-Hellman algorithm with a 2048-bit key. **FCS_COP.1.1 (4), FCS_CKM.2.1, FCS_EAP-TLS_EXT.1, FCS_EAP-TTLS_EXT.1, FCS_PEAP_EXT.1**

Users using manual PSK enter the key as 64 hexadecimal characters; the PSK key as entered is used for authentication, however, it is also used to derive the encryption key.

7.2.2.2 Cryptographic support for SSH, SFTP

The TOE uses the Secure Shell Protocol (SSH) version 2.0 to provide secure remote management of the TOE; it is implemented using openSSH, operating in FIPS mode. It implements key exchange using the Diffie-Hellman algorithm with a 2048-bit key (DH Group 14). **FCS_COP.1.1 (4), FCS_CKM.2.1, FCS_SSH_EXT.1**

SFTP (SSH File Transfer Protocol), is an extension of the SSH v 2.0 and provides secure file transfer capability for the following management functions:

- Configuration file import/export
- Certificate import/export

The SFTP server in the IT environment must support:

- RSA host key size 2048 or greater
- AES128-CBC, AES192-CBC, or AES256-CBC encryption
- HMAC-SHA1 or HMAC-SHA1-96 for authentication

FCS_SFTP_EXT.1

7.2.2.3 Cryptographic support for TLS

The TOE uses the TLSv1.0 protocol to support the HTTPS protocol used for secure management of the TOE using the Web UI and for Hotspot features; it is implemented using openSSL. It implements key exchange using the Diffie-Hellman algorithm with a 2048-bit key. **FCS_COP.1.1 (4), FCS_CKM.2.1**, **FCS_TLS_EXT.1, FCS_HTTPS_EXT.1**

The TOE implements the following ciphers when using TLS:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

7.2.2.4 Cryptographic support for IPSec

The TOE uses IPSec to protect TSF data transfers between the TOE and the Audit Server, RADIUS Server, and the NTP Server; IPsec may be configured to use the manual key mode or IKEv1, which uses PSK and DH group14 for key exchange to setup a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained. **FCS_CKM.2.1, FCS_COP.1 (4), FCS_IPSEC_EXT.1**

- For Manual key exchange
  - AH Authentication: SHA-1
  - ESP Type: ESP (or) ESP with Authentication
  - ESP encryption algorithm: AES-128, AES-192, AES-256
  - ESP authentication algorithm: SHA-1
- For Auto key exchange (IKEv1)
  - AH Authentication: SHA-1
  - ESP Type: ESP (or) ESP with Authentication
  - ESP encryption algorithm: AES-128, AES-192, AES-256
  - ESP authentication algorithm: SHA-1
  - IKEv1 authentication algorithm: SHA-1
  - IKEv1 authentication mode: Pre-shared key
  - IKEv1 encryption algorithm: AES-128, AES-192, AES-256
  - Diffie-Hellman Group: Group14-2048bit

7.2.2.5 Cryptographic support for Simple Network Management Protocol (SNMP)

The TOE administrator may also use the Simple Network Management Protocol version 3 (SNMPv3) for limited management of the TOE. SNMP versions 1 and 2 are disabled. Only AES/SHA-1 is supported for the implemented SNMPv3; the DES/MD5 option has been disabled.
FCS_SNMPV3_EXT.1

7.2.3 User Data Protection

The TOE implements the 802.11i wireless security standard to protect authenticated user data exchanged with a wireless client, which utilizes AES-CCM encryption with 128-bit keys.
FDP_PUD_(EXT).1.1

The memory locations corresponding to network packets processed by the TOE are zeroized when the packet is processed. **FDP_RIP.1**

7.2.3.1 Information flow control

The information flow control Security Function Policies (SFPs) provide policies for the TOE functions that control the information flow through the TOE interfaces; specifically the WLAN, WAN, LAN1 and LAN2 interfaces. The SFPs implemented are the Traffic Filter SFP, and the Unauthenticated TOE Services Policy SFP.

The Traffic Filter SFP mediates information flows from users through the TOE, according to rules defined by an authorized administrator. This policy controls information flows between the LAN1, LAN2, and WLAN interfaces.

The Unauthenticated TOE Services Policy SFP allows unauthenticated users to use TOE services by sending packets to the TOE and receiving responses back from it. This policy is used to express how the TOE enforces rules concerning network traffic that is destined for the TOE. This policy controls information flows from/to the LAN1, LAN2, and/or WAN interfaces to/from the internal TOE services; it can allow or deny management access to the access point from the LAN1, LAN2 or WAN interfaces using different protocols such as HTTPS, SSH2 or SNMP.

The access options can enable or disable LAN1, LAN2 and/or WAN access; if access to an interface is disabled, it prevents an administrator from configuring the access point using that interface. The function mediates information flows by users prior to authentication to control the interfaces that authentication of administrative users is allowed.

The TOE Security Function Policies (SFPs) allow an administrator specify rules that are used to mediate the flow of information (network packets) to implement firewall functions comprised of pre-configured filters, subnet access filters, content filters, and IP filtering. Each of these filters act independently; there is no interaction between the filters. The order of filtering is given below:

Packets entering or leaving the AP's WLAN port:

1. IP filtering

Packets entering or leaving the AP's LAN port:

1. IP filtering
2. Advanced Subnet Access filters
3. Subnet Access filters

Packets entering into AP's WAN port:

1. Pre-configured filters

Packets leaving through the AP's WAN port:

1. Content Filtering

Additional firewall functions provided are network address translation and stateful packet inspection.

7.2.3.1.1 Pre-configured filters

The firewall pre-configured filters are able to screen information packets for known types of system attacks; these are located on the WAN side of the AP. Some of the access point's filters are pre-configured for well-known attacks; others are configurable by the administrator to allow custom rules for each deployment. The TOE implements the following pre-configured filters:

- SYN Flood Attack Check
  - A SYN flood attack requests a connection and then fails to promptly acknowledge a destination host's response, leaving the destination host vulnerable to a flood of connection requests.
- Source Routing Check
  - A source routing attack specifies an exact route for a packet's travel through a network, while exploiting the use of an intermediate host to gain access to a private host.
- Winnuke Attack Check
  - A "Win-nuking" attack uses the IP address of a destination host to send junk packets to its receiving port.
- FTP Bounce Attack Check
  - An FTP bounce attack uses the PORT command in FTP mode to gain access to arbitrary ports on machines other than the originating client.
- IP Unaligned Timestamp Check
  - An IP unaligned timestamp attack uses a frame with the IP timestamp option, where the timestamp is not aligned on a 32-bit boundary.
- Sequence Number Prediction Check
  - A sequence number prediction attack establishes a three-way TCP connection with a forged source address. The attacker guesses the sequence number of the destination host response.
- Mime Flood Attack Check
  - A MIME flood attack uses an improperly formatted MIME header in "sendmail" to cause a buffer overflow on the destination host.
- Max Header Length (>=256)
  - Use the Max Header Length field to set the maximum allowable header length (at least 256 bytes).
- Max Headers (>=12)
  - Use the Max Headers field to set the maximum number of headers allowed (at least 12 headers).

7.2.3.1.2 Subnet access and advance subnet access

The firewall subnet access allows an authorized administrator to control access between LAN1, LAN2 and WAN interfaces. Access between LAN1, LAN2, and WAN are separately controllable and can be characterized as having full, limited, or no access. (Access can be controlled between LAN1 and LAN2, LAN1 and WAN, and LAN2 and WAN)

- Full access allows all traffic may pass between two interfaces; no protocol rules are specified.
- Limited access allows one or more protocols to be specified within a set of administrator-defined rules.
  - The set of preconfigured protocols that can be controlled are:
    - HTTP (TCP, port 80)
    - TELNET (TCP, port 23)
    - FTP (TCP, port 21)
    - SMTP TCP, port 25)
    - POP (TCP, port 109, 110)
    - DNS (TCP + UDP, port 53)

    - Additional (non-preconfigured) protocols that can be added and controlled are:
        - TCP – Transport Control Protocol
        - UDP – User Datagram Protocol
        - ICMP - Internet Control Message Protocol
        - AH - Authentication Header
        - ESP - Encapsulating Security Protocol
        - GRE **-** General Routing Encapsulation

- No access denies all network traffic between the two interfaces. All protocols are denied, without exception.

Additionally, the firewall advanced subnet access may override subnet access; allowing an authorized administrator to define complex access rules and filtering based on parameters such as source port, destination port, and transport protocol between LAN1, LAN2 and WAN interfaces. To enable advanced subnet access, the subnet access rules must be overridden. The administrator can configure firewall filter rules using available CLI commands or using the Web UI with following parameters:

- Inbound or Outbound
    - Select Inbound or Outbound to specify if a firewall rule is intended for inbound or outbound traffic.
    - Traffic entering the access point's LAN1, LAN2 or WLAN from a client is classified as Inbound traffic; traffic leaving the access point's LAN1, LAN2 or WLAN in route to a client is classified as Outbound traffic.
- Source IP
    - The Source IP range defines the origin address or address range for the firewall rule. To configure the Source IP range, click on the field. A new window displays for entering the IP address and range.
- Destination IP
    - The Destination IP range determines the target address or address range for the firewall rule. To configure the Destination IP range, click on the field. A new window displays for entering the IP address and range.
- Transport Protocols may be selected from the following.
    - ALL Enables all of the protocol options described below
    - TCP Transmission Control Protocol
    - UDP User Datagram
    - ICMP Internet Control Message Protocol
    - AH Authentication Header component of IP Security Protocol
    - ESP Encapsulating Security Protocol component of IP Security Protocol
    - GRE General Routing Encapsulation
- Src. Ports (Source Ports)
    - The source port range determines which ports the firewall rule applies to on the source IP address.
- Dst. Ports (Destination Ports)
    - The destination port range determines which ports the firewall rule applies to on the destination IP address.

7.2.3.1.3 Content filtering

Content filtering allows authorized administrators to block specific commands and URL extensions from going out through the access point's WAN port; capabilities include block outbound specific HTTP[41] commands, disable or restrict specific kinds of SMTP traffic, and disable or restrict specific kinds of FTP traffic. The administrator can configure firewall filter rules using available CLI commands or using the Web UI with following parameters:

[41] HTTP port 80 only

- Block Outbound HTTP
  - HyperText Transport Protocol (HTTP) is the protocol used to transfer information to and from Web sites. HTTP Blocking allows for blocking of specific HTTP commands going outbound on the access point WAN port. HTTP blocks commands on port 80 only.The Block Outbound HTTP option allows blocking of the following (user selectable) outgoing HTTP requests:
    - Web Proxy - Blocks the use of Web proxies by clients
    - ActiveX - Blocks all outgoing ActiveX requests by clients. Selecting ActiveX only blocks traffic (scripting language) with an .ocx extension.
- Block Outbound URL Extensions
  - Enter a URL extension or file name per line in the format of filename.ext. An asterisk (*) can be used as a wildcard in place of the filename to block all files with a specific extension.
- Block Outbound SMTP Commands
  - Simple Mail Transport Protocol (SMTP*)* is the Internet standard for host-to-host mail transport. SMTP generally operates over TCP on port 25. SMTP filtering allows the blocking of any or all outgoing SMTP commands. Check the box next to the command to disable that command when using SMTP across the access point's WAN port.
    - *HELO* - (Hello) Identifies the SMTP sender to the SMTP receiver.
    - *MAIL*- Initiates a mail transaction where data is delivered to one or more mailboxes on the local server.
    - *RCPT* - (Recipient) Identifies a recipient of mail data.
    - *DATA* - Tells the SMTP receiver to treat the following information as mail data from the sender.
    - *QUIT* - Tells the receiver to respond with an **OK** reply and terminate communication with the sender.
    - *SEND* - Initiates a mail transaction where mail is sent to one or more remote terminals.
    - *SAML* - (Send and Mail) Initiates a transaction where mail data is sent to one or more local mailboxes and remote terminals.
    - *RESET* - Cancels mail transaction and informs the recipient to discard data sent during transaction.
    - *VRFY* - Asks receiver to confirm the specified argument identifies a user. If argument does identify a user, the full name and qualified mailbox is returned.
    - *EXPN* - (Expand) Asks receiver to confirm a specified argument identifies a mailing list. If the argument identifies a list, the membership list of the mailing list is returned.

- Block Outbound FTP Actions
  - File Transfer Protocol (FTP) is the Internet standard for host-to-host mail transport. FTP generally operates over TCP port 20 and 21. FTP filtering allows the blocking of any or all outgoing FTP functions. Check the box next to the command to disable the command when using FTP across the access point's WAN port.
    - Storing Files - Blocks the request to transfer files sent from the client across the AP's WAN port to the FTP server.
    - Retrieving Files - Blocks the request to retrieve files sent from the FTP server across the AP's WAN port to the client.
    - Directory List - Blocks requests to retrieve a directory listing sent from the client across the AP's WAN port to the FTP server.
    - Create Directory - Blocks requests to create directories sent from the client across the AP's WAN port to the FTP server.
    - Change Directory - Blocks requests to change directories sent from the client across the AP's WAN port to the FTP server.
    - Passive Operation - Blocks passive mode FTP requests sent from the client across the AP's WAN port to the FTP server.

7.2.3.1.4 IP filtering

IP filtering allows an administrator-defined rule set be used to mediate packets flowing on the access point's LAN1 or LAN2 interfaces and within any of the 16 access point WLAN; these rules determine which IP packets are processed normally by the access point and which are discarded. If discarded, a packet is deleted and ignored (as if never received). The allow/deny mechanism used by IP filtering makes it similar to an access control list (ACL).
IP filtering supports the creation of up to 20 filter rules enforced at layer 3. Once defined, using the access point's SNMP, GUI or CLI), filtering rules can be enforced on the access point's LAN1 or LAN2 interfaces and within any of the 16 access point WLANs. An additional default action is also available denying traffic when filter rules fail. IP filtering is a network layer facility and does not know anything about the application using the network connections, only the connections themselves.

There are important rules a packet adheres to when it is compared with the filter policy list:

1. Packets are always filtered in sequential order (filtering always begins with the first filter policy displayed in the IP Filtering screen, then the second, third, and so on).
2. Packets are compared with lines of the filter policy list until a match is made. Once a packet matches a line of the list, it's acted upon, and no further comparisons take place. If inspected packets are determined to not be IP packets, it permitted by the access point for its inbound or outbound destination.

Once a filter policy is created, apply it to an interface in either an incoming or outgoing direction.

- Traffic entering the access point's LAN1, LAN2 or WLAN (1-16) from a client is classified as Incoming traffic.
- Traffic leaving the access point's LAN1, LAN2 or WLAN (1-16) in route to a client is classified as Outgoing traffic.

To define the attributes of a new IP Filtering policy, the following policy (or filtering rule) attributes require definition.

- Filter name
  - Name for the filter policy unique to its function in order to differentiate it from others that may have somewhat similar configurations
- Protocol
  - Specify the protocol used for the filter policy. The options are:[42]
    - ALL,
    - TCP,
    - UDP,
    - ICMP,
    - PIM,
    - GRE,
    - RSVP,
    - IDP,
    - PUP,
    - EGP,
    - IPIP,
    - ESP,
    - AH,
    - IGMP,
    - IPVG,
    - COMPR_H and
    - RAW_IP.
- Port Start

[42] The protocol number can also be used as the protocol name. This allows the use or protocols that are not within the drop-down menu.

  - Defines the socket number (or port) number representing the beginning protocol port range either allowed or denied permission to the target LAN1, LAN2 or WLAN.
- Port End
  - Defines the socket number (or port) number representing the ending protocol port range either allowed or denied permission to the target LAN1, LAN2 or WLAN.
- Src Start
  - Creates a range beginning source IP address to be either allowed or denied IP packet forwarding. The source address is where the packet originated. Setting the Src End value the same as the Src Start allows or denies just this address without defining a range.
- Src End
  - Providing this address completes a range of source (data origination) addresses than can either be allowed or denied access to the LAN1, LAN2 or WLAN.
- Dst Start
  - Creates a range beginning destination IP address to be either allowed or denied IP packet forwarding. Setting the Dst End value the same as the Dst Start allows or denies just this address without defining a range.
- Dst End
  - Providing this address completes a range of destination addresses than can either be allowed or denied access to the LAN1, LAN2 or WLAN.
- In Use
  - Displays YES if the listed filter policy is currently being utilized by LAN1, LAN2 or a WLAN. NO is displayed if the listed policy is currently not be utilized by either of the LAN ports or any of the access point's 16 WLANs.

FDP_IFC.1 (1), (2), FDP_IFF.1-NIAP-0417 (1), (2), FMT_MSA.3, FMT_MOF.1 (4), FMT_SMF.1 (4)

7.2.4 Identification and Authentication (I&A)

The TOE requires administrative users that manage the TOE to be successfully identified prior to using any TOE functions; however, the following TSF mediated functions are permitted prior to authentication:

- ICMP,
- ARP,
- DHCP,
- The passing of authentication data to and from the remote authentication server,
- TSF mediation in accordance with the Unauthenticated TOE Services SFP

FIA_UID.2, FIA_UAU.1 (1)

Wireless users must also be properly identified prior to being allowed to pass data through the TOE; however, the following TSF mediated functions are permitted prior to authentication:

- The passing of authentication data to and from the remote authentication server,
- TSF mediation in accordance with the Traffic Filter SFP

Application Note: *All users, whether authenticated or not, will always be identified at least by a source network identifier. In the case of authenticated users (administrators and authorized IT entities) there will probably be a "userid".*

FIA_UID.2, FIA_UAU.1 (2)

7.2.4.1 Administrative user I&A

The TOE utilizes username password-based authentication to authenticate administrators connecting locally using the serial console connection, remotely using the SSH protocol or over HTTPS (TLSv1.0) using the Web UI, or via SNMP. Administrators may connect remotely via the LAN, WAN, or 802.11a/b/g/n interfaces.

The source of authentication credentials is an administrator configurable option; authentication may be set to use a local database, or may be set to us a remote RADIUS server. If using the local database, twenty-five (25) administrative accounts are supported with one (1) default account that has a fixed username and an initial password, which must be changed at first use. **FIA_UAU.4** The other twenty-four (24) local accounts may be added to the local database using the default “admin” account. An unlimited number of remote administrative accounts are supported using the remote RADIUS server.

If using the remote RADIUS server option and the remote RADIUS server cannot be reached, the TOE will failover to the local database. Administrative usernames and passwords must be synchronized manually between the local and remote RADIUS server. **FIA_ATD.1 (1)**

The TOE monitors the number of failed authentication attempts; when the administrator-defined threshold of unsuccessful authentication attempts for a remote administrator has been reached, that remote administrator interface is disabled until re-enabled using a local console connection. Note that the lockout is applied per interface (GUI, SSH) and not per user. If a user reaches the limit of failed login attempts via SSH, for example, then the SSH interface is locked for all users. The same user can attempt to authenticate via the GUI. The local console CLI is the primary management interface for the TOE and is used to remove the interface lock; therefore, the local console interface is never locked.

The CLI supports commands to set the threshold value for SSH and Web UI login failure; and to remove the lock so the SSH administrative interface and/or the Web UI may again be used. The default and maximum threshold value is three (3) authentication attempts. **FIA_AFL.1 (1)**

The TOE authenticates SNMP administrators prior to allowing access to the TOE; each SNMPv3 request contains the username/password along with the message. If the authentication fails, then this request is dropped by the netsnmp agent.

SFTP is interactive by nature, which is supported by the CLI where the administrator can enter the authentication credentials, however, if the Web UI is to be used, the TOE also implements a non-interactive support initiated by the admin from the AP-7131N device as described below:

- To establish non-interactive communication with the SFTP server, the SFTP server will need the public key of the AP-7131N. This is accomplished by the following method:
    - The admin will configure the SFTP server's IP address and a user name using the CLI
    - For configuration files, the admin will then execute a CLI command "transfer_keys_cfg" on the AP-7131N, and when prompted, will enter a password for the user on the SFTP server.
    - The command "transfer_keys_cfg" generates public and private RSA keys. The public key is transferred to the SFTP server and is appended to the .ssh/authorized_keys file that is present in the home directory of that user. This ensures that the device can transfer files between itself and the SFTP server in a non-interactive manner.
- After these steps are completed, the Web UI can be used from this screen.
    - System Configuration - > Config Import/Export from the access point menu tree

After a user has authenticated, the TOE maintains an association between that user and any program execution done on behalf of that user. This association is maintained as long as any program execution associated with a user continues. **FIA_USB.1**

7.2.4.2 Wireless user I&A

The TOE requires wireless users and Mesh connected APs to authenticate before access to the wired network is granted by the TOE; authentication of wireless users may be performed locally using manual Pre-Shared Key (PSK), or using IEEE 802.1X EAP-TLS, EAP-TTLS and EAP-PEAP authentication protocols. Authentication of Mesh connected APs must use manual PSKs.

When the TOE is configured for manual PSK authentication, a 256-bit key is used for authentication as well as generating the encryption key to encrypt the data stream; therefore, only wireless users and mesh connected APs possessing the key may access the network. This key is entered manually as a string of 64 hexadecimal digits.

Authentication may be performed locally using a local database or an internal RADIUS server and remotely using an external RADIUS server. If the internal RADIUS Server is selected, the user authentication credentials can be obtained from the local database or an external LDAP server. When the local database is used, users and groups can be added using the CLI or Web UI management interfaces, and are stored locally on the TOE. When using LDAP, only PEAP-GTC and TTLS/PAP are supported. **FIA_ATD.1.1 (2)**

The TOE's internal radius server is implemented using FreeRADIUS-server modified to support only FIPS 140-2 approved ciphers; all non-FIPS approved ciphers are disabled. The TOE supports EAP-TLS, EAP-TTLS and EAP-PEAP authentication types. **FCS_RAD_EXT.1, FCS_EAP-TLS_EXT.1, FCS_EAP-TTLS_EXT.1, FCS_PEAP_EXT.1**

When using the external RADIUS server, the TOE acts as the 802.1X authenticator and utilizes services of the external RADIUS authentication server to provide wireless user authentication based on IEEE 802.1X EAP-TLS, EAP-TTLS and EAP-PEAP authentication protocols During the authentication phase, the TOE serves as an intermediary passing authentication messages between the wireless client device and the external authentication server. If the authentication is successful, the authentication server passes the TOE 802.11i session keys used to establish a 802.11i secure connection between the TOE and the wireless client device. Once the connection is established, the wireless client device may access the protected wired network utilizing the TOE as a gateway. The network connection between the TOE and the external authentication server is protected using the IPSec security protocol. EAP-TLS authentication protocol uses a X.509 client certificate for wireless user authentication, EAP-TTLS and EAP-PEAP protocols use password-based authentication. The X.509 Client Certificate authentication is described in Section 7.2.4.3, EAP-TLS X.509 Client Certificate Authentication.

For the external Radius server configurations, the TOE supports a primary radius server and optionally, a secondary radius server

Wireless user authentication is summarized in Table 20 – Wireless user authentication.

Table 20 – Wireless user authentication

Local / Remote	Authentication Method	Authentication credentials
Local	PSK	PSK (64 hexadecimal digits)
Local	802.1x EAP-TLS	X.509 Client Certificate
Local	802.1x EAP-TTLSv0	Username/Password from local database
Local	802.1x PEAP EAP-GTC	The Generic Token Card Type is defined for use with various Token Card implementations, which require user input. The Request contains an ASCII text message and the Reply contains the Token Card information necessary for authentication. Typically, this would be information read by a user from the Token card device and entered as ASCII text
Local	802.1x PEAP EAP-MS-CHAP-V2	Username/Password from local database
Remote	802.1x EAP-TLS	X.509 Client Certificate
Remote	802.1x EAP-TTLSv0	Username/Password
Remote	802.1x PEAP EAP-GTC	The Generic Token Card Type is defined for use with various Token Card implementations, which require user input. The Request contains an ASCII text message and the Reply contains the Token Card information

Table 20 – Wireless user authentication		
		necessary for authentication. Typically, this would be information read by a user from the Token card device and entered as ASCII text
Remote	802.1x PEAP EAP-MS-CHAP-V2	Username/Password

FIA_UAU_(EXT).5

7.2.4.3 EAP-TLS X.509 Client Certificate Authentication

The following is a summary of the processing performed to authenticate a X.509 Client Certificate.

1. The TOE sends a peer certificate request to the peer(MobileUnit)
2. The peer(MU) sends its certificate to the AP
3. The verification process will begin at the TOE
   a. The certificate chain is checked by beginning with the 'subject certificate'[43] and then proceeds through the intermediate certificates up to a trusted 'root certificate', typically issued by a trusted certification authority.
4. At each level (in the path tree)
   a. Incoming certificate's signature/fingerprint is checked and verified with the CA cert by the TOE.
   b. If the above check succeeds, TOE verifies the certificate has been issued by a trusted Certificate Authority.
   c. If (b) succeeds, TOE verifies that the certificate is valid for the present date
   d. If the above steps succeed, TOE verifies the credentials presented by the certificate fulfill the following additional requirements:
      i. Certificate Common Name (CN) Validation
         1. Certificate Common Name should be present in Radius user database.
      ii. Access Control List (ACL) Verification,
         1. Wireless user must be member of the radius group ACL configured in TOE
      iii. Policy Verification
         1. TOE verifies that wireless user can access TOE at this instant based on policy configured (all days / weekdays / any particular days).
5. If the verification fails, the TLS handshake is immediately terminated with an alert message containing the reason for the verification failure.
6. On success, a peer-id will be created for the user and the session will be established between TOE and its user.

7.2.5 Security Management

The management of the security relevant parameters of the TOE is performed by the authorized administrator. There are two types of administrators, "regular" administrators, and a "superuser" account with the pre-defined name 'admin.' The 'admin' account name is hardcoded and cannot be changed. In addition to all functions available to regular administrators, the 'admin' account can manage all other locally stored regular administrator accounts.

The administrator is the only role that has direct access to the TOE functions; however, the TOE also supports the SNMP administrator role providing limited management and a SNMP trap Interface via the SNMPv3 protocol. A complete listing of the available SNMP management features is listed in Table 21 – SNMPv3 Feature Support, and a complete listing of the traps supported is listed in Table 22 – SNMPv3 Trap Support.

The TOE also supports the wireless user role; however, this user has no access to TOE functions and can only pass data through the TOE. **FMT_SMR.1**

[43] Subject certificate: leaf level peer certificate which has the fingerprint of CA
Note: The TOE does path validation only when the peer provides 'path information' of the peer's certificate which the peer has to provide at the time of TLS handshake. However, the TOE will not validate the certificate's path by connecting to the internet, or pre-configure the necessary intermediate certificates to complete path validation.

The TOE provides the following management interfaces:

- Command Line Interface (CLI) via
  - Local RS-232 console connection,
  - Remote SSH interface via the LAN, WAN, and 802.11 wireless interface
- Remote HTTPS JAVA based Web UI via the LAN, WAN and 802.11 wireless interface
- Remote SNMP interface via the LAN, WAN and 802.11 wireless interface
  - Limited management and trap support only
- Configuration file downloaded by SFTP

The CLI and Web UI provide interfaces to provide the following:

- Manage cryptographic functions **FMT_MOF.1(1)** as follows:
  - Load the cryptographic key
  - Zeroize a key
  - Set a key lifetime
  - Set the cryptographic algorithm
  - Start self tests of the TOE cryptographic functions
- Manage audit functions **FMT_MOF.1(2)**
  - Selection of the events which trigger an audit record,
  - Start and stop of the audit function. Auditing is an inherent function of the ToE, so the only way to start or stop the audit function is to power up/down the ToE. The functions to perform shutdown/restart are restricted to administrator access.
- Manage authentication functions **FMT_MOF.1(3)**
  - Allow or disallow the use of an authentication server
  - Set the number of authentication failures that must occur before the TOE takes action to disallow future logins (for remote administration only)
  - Set the length of time a session may remain inactive before it is terminated
- Manage Firewall Functions **FMT_MOF.1(4)**
  - Enable and disable pre-configured filters
  - Create, change, and delete firewall rules
- Manage Intrusion Detection functions **FMT_MOF.1(5)**
  - Change the Rogue AP Detection Method
  - Change Rogue AP approved listing
  - Display Rogue AP Details
- Manage communication and authentication protocol behavior **FMT_MOF.1(6)**
  - Modify IPsec SA lifetimes
  - Modify SSH timeout period and authentication failure limits
  - Select local vs remote authentication
  - Select local database vs. remote LDAP database
  - Select 802.1x authentication method and EAP type
  - Configure SNMP traps and access
- Manage configuration file import and export behavior **FMT_MOF.1(7)**
  - Set the Filename, the SFTP Server IP Address, Filepath, and the username.
    - Reference Section 4.9 Importing/Exporting Configurations, page 4-50 [1]
- Manage audit functions **FMT_MTD.1(1)**
  - Support to create, delete rules are provided.
  - Support to "query" and "modify" the rules have not been provided. User has to clear the rule and create a new rule instead of modifying.
  - These function are restricted to administrator only.
- Manage authentication data. Regular administrators can only manage their own authentication data, and view the list of other regular administrator accounts. The ‘admin’ account can manage its own password and add/delete/edit authentication data for regular administrators. **FMT_MTD.1(2)**
- Configure administrative authentication and the cryptographic functions of the wired network interface. **FMT_SMF.1(1)**

- Configure audit functions **FMT_SMF.1(2)**
- Configure wireless cryptographic keys **FMT_SMF.1(3)**
- Configure Firewall rules and settings **FMT_SMF.1 (4)**
- Configure intrusion detection settings **FMT_SMF.1 (5)**
- Configure communication and authentication protocol settings **FMT_SMF.1 (6)**
- Configure configuration file import and export settings **FMT_SMF.1 (7)**

The CLI, Web UI, and SNMP interfaces test the input of all security attributes to ensure that the values input result in a secure configuration prior to acceptance of the input. **FMT_MSA.2**

The TSF provides permissive default values for all Firewall settings (information flow security attributes) – all firewalls and filters are disabled by default. **FMT_MSA.3**

All management functions require the administrator to be successfully authenticated prior to access.

7.2.5.1 Local RS-232 Command Line Interface (CLI)

The primary management interface to the TOE is the local RS-232 interface; this provides the administrator local access to all available commands; the CLI commands are documented in user guidance. [1]

7.2.5.2 SSH

The TOE uses the Secure Shell Protocol (SSH) to allow the administrator access to the CLI for secure remote management of the TOE. The SSH protocol is accessible via either the LAN or WAN ports. This interface supports all commands accessible via the local CLI connected via RS-232 except the following:

- rmlock command

7.2.5.3 Simple Network Management Protocol (SNMP)

The TOE can also use the Simple Network Management Protocol version 3 (SNMPv3) to provide limited management of the TOE; the implementation is based on NET-SNMP.

SNMPv3 uses Management Information Bases (MIBs) to manage the device configuration and monitor network devices in remote locations using a MIB Browser or equivalent SNMP Management software. MIB information accessed via SNMP is defined by a set of managed objects called Object Identifiers (OIDs). An OID is used to uniquely identify each object variable of a MIB.

In the evaluated configuration, the supported SNMP features are listed in Table 21 – SNMPv3 Feature Support and the supported SNMPv3 traps are listed in Table 22 – SNMPv3 Trap Support; SNMP versions 1 and 2 are disabled.

Table 21 – SNMPv3 Feature Support

Feature	Sub-feature	Description	Equivalent CLI commands
dot1x	Auth configuration	This table provides the option to read the configuration details of Authenticator PAE (Port Access Entity) associated with each port.	
	Auth statistics	This table provides the option to read the statistics details of Authenticator PAE associated with each port.	
	auth diagnostics	This table provides the option to read the diagnostics details of Authenticator PAE associated with each port.	
	auth session statistics	This table provides the option to read the session statistics details of Authenticator PAE associated with each port.	
apRf	apRadio	This table lists the properties of the radios • AP radio Setting, • Radio Configuration, • BSS (Basic Service Set), • WLAN BSS, • ESS (Extended Service Set) to BSS mapping status, • Radio Mesh, • Radio WLAN bandwidth, • 802.11n radio configuration, • Setting and Modulation.	admin(network.wireless.radio.802-11n[2.4 GHz])>show radio ? <cr> : perform the function admin(network.wireless.radio.802-11n[2.4 GHz])>set ? or admin(network.wireless.radio.802-11n[5.0 GHz])>set ? placement : set Radio location ch-mode : set Channel Selection channel : set Channel (for User Selection only) power : set Power Level rf-mode : set default data rates of the 802.11 mode selected rates : set Radio Data Rates beacon : set Beacon Interval dtim : set DTIM Period Interval aggr : set Aggregation shortgi : en/dis Short Guard Interval (40MHz only) preamble : enable/disable Support Short Preamble rts : set RTS Threshold range : set Extended Range

Table 21 – SNMPv3 Feature Support			
Feature	Sub-feature	Description	Equivalent CLI commands
			qos : set RF QoS qbss-beacon : set QBSS Load Eval Beacon Interval qbss-mode : enable/disable QBSS Load Element single-antenna : Enable/Disable Single Antenna
	apWlan	This table lists the WLAN feature: • WLAN configuration, • Security Policy, • WLAN Authentication, • WLAN Crypto, • WLAN MU ACL and ACL policy, • QOS policy, • bandwidth shared among the WLAN	admin(network.wireless.wlan.create)>set ? ess : set ESS ID wlan-name : set WLAN name 5.0GHz : enable/disable on 5.0 GHz radio 2.4GHz : enable/disable on 2.4 GHz radio mesh : enable/disable Client Bridge Mesh Backhaul hotspot : enable/disable Hotspot Mode max-mu : set maximum number of MUs idle-timeout : set MU idle timeout security : set Security Policy name acl : set MU Access Control Policy name no-mu-mu : enable/disable Disallow MU-MU Communication sbeacon : enable/disable Use Secure Beacon bcast : enable/disable WLAN Accept Broadcast ESSID qos : set Quality of Service Policy name rate-limiting : enable/disable Per-MU Rate Limiting limit-w2wl : set per-MU rate limit (wired-to-wireless) limit-wl2w : set per-MU rate limit (wireless-to-wired)
	apHotSpot	This table lists the Hotspot configuration White List entries for HotSpot for the WLANs	admin(network.wireless.wlan.hotspot)>show hotspot ? all <cr> : all wlans <idx><cr> : idx - wlan index (1-16) admin(network.wireless.wlan.hotspot.radius)>set ? server : set hotspot radius server ip-address secret : set hotspot radius secret acct-mode : set hotspot radius accounting mode acct-server : set hotspot radius accounting server ip-address acct-secret : set hotspot radius accounting server secret acct-timeout : set hotspot radius accounting timeout acct-retry : set hotspot radius accting retry sess-mode : set hotspot user session timeout mode sess-timeout : set hotspot user session timeout
	apMus	This table lists MU-Locationing functionality supported.	admin(network.wireless.mu-locationing)>? show : show MU Locationing configuration set : set MU Locationing parameters .. : go to parent menu / : go to root menu save : save cfg to system flash quit : quit cli admin(network.wireless.mu-locationing)>set ?

Table 21 – SNMPv3 Feature Support			
Feature	Sub-feature	Description	Equivalent CLI commands
			mode : enable/disable MU Locationing size : set number of MU's in the MU Locationing Table
	apIpFilter	Following is list of IP Filtering functionality supported: WLAN/LAN configuration and policy	admin(network.ipfilter)>show? <cr> : perform the function admin(network.ipfilter)>set ? name : set name of ip filter protocol : set protocol of ip filter port-start : set starting port of ip filter port-end : set ending port of ip filter saddr-start : set starting source address of ip filter saddr-end : set ending source address of ip filter daddr-start : set starting dest address of ip filter daddr-end : set ending dest address of ip filter
apSwitch	apWan	This table list the wan feature supported: • VPN tunnel configuration, • Point to Point Protocol over Ethernet client information, • Wan Port, • Dynamic DNS configuration	admin(network.wan)>show ? <cr> : perform the function admin(network.wan.dyndns)>show ? <cr> : perform the function admin(network.wan.dyndns)>set ? mode : enable/disable dyndns username : set dyndns username password : set dyndns password hostname : set dyndns hostname admin(network.wan)>set speed ? <speed><cr> : speed - (10M/100M/1000M) admin(network.wan)>set duplex ? <duplex><cr> : duplex - (half/full) admin(network.wan)>set auto-negotiation ? <auto-negotiation><cr> : auto-negotiation - (enable/disable)
	apLan	This table lists the LAN feature supported: • LAN Configuration • apLan802dt1xAuth, • VLAN configuration, • Subnetting, • LAN Filter configuration, • LAN bridge, • LAN port configuration	

Table 21 – SNMPv3 Feature Support			
Feature	Sub-feature	Description	Equivalent CLI commands
	apWnmpPing	This table list the Wireless network management protocol Ping settings	
	apFlashLed	This table lists the configuration of Flash Led destination Mac Address.	
	apKnown list	This table lists the configuration of AP known list i.e., IP, MAC Address.	admin(stats)>show known-ap? known-ap : show Known APs Summary/Details
	apAap	This table lists the AP Switch Auto Discovery and AP adoption functionalities.	admin(system.aap-setup)>? show : show Adaptive AP information set : set Adaptive AP parameters delete : delete static switch address assignments .. : go to parent menu / : go to root menu save : save cfg to system flash quit : quit cli admin(system.aap-setup)>set ? auto-discovery: set switch auto-discovery mode ipadr : set switch ip addresses name : set switch domain name port : set control port passphrase : set switch passphrase ac-keepalive : set the AC KeepAlive period load-balancing: enable/disable AAP Load Balancing
apNotifications	AP notification and Trap	This table has a list of SNMP notification and traps	admin(system.snmp.traps)>show trap ? <cr> : perform the function
apRap	Remote AP Band config	This table list the Detector Mode and Band for RF scan and also to scan both A and BG Bands for remote AP	admin(network.wireless.rogue-ap)>set detector-scan ? <op-mode><cr> : op-mode - (disable, scan11a, scan11bg)
apStats	AP wireless Statistics	This table lists the statistics information of Mesh network, Mesh bridge, STP (Spanning Tree Protocol) State and STP port interface.	admin(stats)>show mesh ? <cr :perform the function admin(stats)>show stp ? <LAN-idx><cr> : LAN Index (1, 2) : 1-LAN1, 2-LAN2
	apnStats	This table list the statistics info of Radio stats, Portal Tx/Rx, MU Tx/Rx, WLAN Tx/Rx	admin(stats)>show radio ? <cr> : perform the function admin(stats)>show wlan ? <cr> : perform the function

Table 21 – SNMPv3 Feature Support			
Feature	Sub-feature	Description	Equivalent CLI commands
	apDiagStats	This Table list the CPU and RAM diagnostic statistics	
	apLanStats	This table list the statistics of LAN, packet Tx/Rx by the LAN	admin(stats)>show lan ? <LAN-idx><cr> : LAN Index (1, 2) : 1-LAN1, 2-LAN2
apMgmtAccess	None	This table lists the network management access to the switch. Also list the trusted host information	
apRouter	None	This list information of Interface whose Default Gateway is used when both LAN and WAN are DHCP clients	admin(network.router)>set ? auth : set rip authentication type dir : set rip direction id : set MD5 authentication ID key : set MD5 authentication key passwd : set password for simple authentication type : set RIP type dgw-iface : Set the Default gateway Interface to be used
apManualTime	None	This object provide the options for Current system time configuration of AP manually	admin(system.ntp)>set ? mode : set NTP mode server : set NTP server intrvl : set NTP sync interval in minutes time : set system time zone : set time zone admin(system.ntp)>? show : show Network Time Protocol (NTP) parameters date-zone : show date, time and time zone zone-list : show the list of time zones set : set Network Time Protocol (NTP) parameters .. : go to parent menu / : go to root menu save : save cfg to system flash quit : quit cli admin(system.ntp)>zone-list ? <cr> : perform the function
apAdmin	FIPS/CC specific items	This table provide the options to configure the login message, auth failures, console timeout, audit log settings	admin(system.access)>set ? applet : set Applet HTTPS Access parameters app-timeout : set applet timeout ssh : set CLI SSH Access parameters auth-timeout : set max time allowed for SSH auth procedure inactive-timeout: set max inactivity allowed in SSH session console-timeout: set max inactivity allowed for Console session rlogin : set remote login failure threshold (SSH/GUI) snmp : set SNMP Access parameters

Table 21 – SNMPv3 Feature Support			
Feature	Sub-feature	Description	Equivalent CLI commands
			admin-auth : set Admin Authentication mode server : set Radius Server IP for Admin Authen secret : set Radius Shared Secret for Admin Authen msg : set AP-713x Login message
apRadiusServer	None	This table list the radius server user group details and access details	admin(system.userdb)>? user : go to User sub menu group : go to Group sub menu save : save cfg to system flash .. : go to parent menu / : go to root menu
WIPS settings	None	wireless intrusion prevention system primary and secondary server settings	admin(network.wireless.wips)>set server ? <idx> <a.b.c.d><cr> : idx - WIPS server index (1 or 2) : WIPS server IP address admin(network.wireless.wips)>show ? <cr> : perform the function
apPower	None	This object list the AP power configuration feature e.g., Power Mode, Power options, power Status	admin(system.power-setup)>show Power Mode : Auto Power Status : Full Power 3af Power Option : default 3at Power Option : default Default Radio : Radio1 admin(system.power-setup)>set ? mode : set power mode power-option : set power option def-radio : set default radio
ccWanVpnKeyAutoTable	ccWanVpnKeyAutoEntry: ccWanVpnKeyAutoIkeKeyLifetime	This table provides the option to configure (read and write) the number of seconds that the IPsec Phase 1 SA is valid.	admin(network.wan.vpn)>set ike lifetime ? <name> <lifetime> : name of tunnel - 1 to 13 characters : IKE key life time in seconds (300 -86400)
apWanVpnKeyAutoTable	apWanVpnKeyAutoEntry: apWanVpnKeyAutoSALifeTime	This table provides the option to configure (read and write) the number of seconds that the IPsec Phase 2 SA is valid.	admin(network.wan.vpn)>set salife ? <name> <lifetime> : Name of tunnel - 1 to 13 characters : SA Life time in seconds (300 - 28800)
apLoadCfg	apLoadCfgServerFilename, apLoadCfgServerPath, apLoadCfgServerIpAddr, apLoadCfgSftpUsername	This table provides the option to set the Configuration Filename, File path, SFTP server IP Address, and the username.	admin(system.config)> set ? file <filename> Sets the configuration file name (1 to 39 characters in length). path <path> Defines the path used for the configuration file upload. server <ipaddress> Sets the SFTP server IP address. user <username> Sets the SFTP user name (1 to 39 characters in length).
	apLoadCfgOperation	This table provides the option to import/export configuration file from/to the SFTP server.	admin(system.config)> export Exports access point configuration to a designated system. import Imports configuration to the access point.

Table 22 – SNMPv3 Trap Support	
Trap/Notification	Description
apMuVlan	A MU has been associated with a Radio Address.
apLanMonitor	Radios are either been SHUTTING DOWN or RESTORING because of a certain activity at LAN Port.
apWpaCounterMeasure	When a subsequent MIC failure occurs within 60 seconds of the preceding failure, the AP will disassociate all associated STAs. The AP will not deliver any class 3 TKIP (Temporal Key Integrity Protocol) encrypted data frames to or from any peer as well as disallow new associations for a period of 60 seconds
apMuHotspotState	An MU is either authenticated or de-authenticated on a Hotspot enabled WLAN. Upon authenticating with a RADIUS Server the state of the MU is changed from HOTSPOT to DATA_READY and the vice versa upon Time out or Logging out of that particular MU.
apDynDNSUpdate	A DynDNS Update has been sent to DynDns.org
ccPortalAdopted	A Portal has been adopted by the switch.
ccPortalUnAdopted	A Portal has been un-adopted by the switch.
ccPortalDenied	A Portal has been denied adoption by the switch.
ccMuAssociated	An MU has been associated to a Portal adopted by this switch. Example: MU MAC1 has associated to Portal MAC2.
ccMuUnAssociated	An MU has been un-associated to a Portal adopted by this switch.
ccMuDenied	An MU has been denied association to a Portal adopted by this switch.
ccSnmpAclViolation	An attempt to communicate via SNMP to the switch has been denied based on configured ACLs
ccConfigChange	The configuration of this switch has changed.
ccPortStatusChange	A [physical] port's state has changed from up-->down or down-->up.
ccCfAlmostFull	The compact flash is almost full; For a Used=x, Capacity=y, Threshold=z.
ccFirewallUnderAttack	The firewall has detected an attack in progress.
ccSumStatsMu	A summary statistic has crossed the prescribed threshold by an MU. Example: Threshold of value 'x' has been crossed y MU MAC with IP-addr.
ccSumStatsPortal	A summary statistic has crossed the prescribed threshold by a Portal. Example: Threshold of value 'x' has been crossed by a Portal index with MAC
ccRadarDetected	Radar has been detected on a Portal channel. Example: Radar has been detected on Portal MAC1, on channel 2
ccSumStatsWlan	A summary statistic has crossed the prescribed threshold by a WLAN.
ccSumStatsSwitch	A summary statistic has crossed the prescribed threshold by the entire Switch.
ccLanVlanActivated	A VLAN is activated. Whenever a MU is associated with the switch, and it receives a VLAN attribute from the radius server, the specified VLAN is activated.
ccDhcpOptionsFileTransferStatus	Trap to say that the device received DHCP options instructing it to load new configuration file, and that it has completed the transfer. The varbinds tell if the transfer was successful.
ccRedundancyStateChange	The state of this switch's ccRedundancyOperState has changed
ccRapNewApprovedAp	A new AP has been heard that was in some manner authorized
ccRapNewRogueAp	A new AP has been heard that was NOT authorized.

SNMPv3 with a security level of ‘authPriv’ is supported. Authentication via SHA-1 is supported, for privacy only AES encryption is supported, DES has been disabled.

There is no support for the security level of noAuthNoPriv and authNoPriv.

The SNMP administrator must be configured via the CLI or Web UI prior to availability.

User can be configured with access permission of read-only and read-write The SNMP Access Control screen's Access Control List (ACL) uses Internet Protocol (IP) addresses to restrict access to the AP’s SNMP interface.

User can read and write non-security sensitive OIDs, but can only read security sensitive OIDs. This read or read/write access is provided using the MAX-ACCESS option in the MIB.

To access the MIB objects on the device, the MIB Browser(or any SNMP management tool) also needs to add the users and auth/priv options exactly as created using the CLI or Web UI. The configuration options on the MIB Browser are vendor specific; guidance is provided in [1] to configure common MIB browsers.

7.2.5.4 Configuration file downloaded by SFTP

Configuration settings for the TOE can be imported from or exported to the SFTP Server in the IT Environment. This allows the administrator to save the current configuration before making significant changes or restoring a default configuration; additionally, multiple APs can be configured quickly to a common configuration. The TOE uses the CLI interface to initiate a SSH File Transfer Protocol for Configuration file export/import. When a configuration file is imported, all configuration items on the importing AP are deleted and then updated by the imported file and a single audit record is generated by both the importing and exporting APs.

Imported configuration files can overwrite all settings that are available via the CLI with the exception of the admin password; the admin password will only be overwritten if the device is in the factory default configuration, otherwise it is skipped.

If the imported configuration file changes the syslog server settings, logs will be sent to the new syslog server after the IPsec tunnel is established.

7.2.5.5 JAVA based Web UI Applet

The TOE uses a JAVA based Web UI accessible via the HTTPS protocol for secure management of the TOE. This applet is supported using the Apache Web Server, apache-httpd 1.3.41. The Web UI is only accessible using browsers that support the TLSv1.0 protocol. Additionally, the administrator must ensure Oracle's (formerly SUN) JRE (version 1.6 or above) is installed on the computer accessing the Web UI applet; Microsoft's Java Virtual Machine must be disabled if installed.

The Web UI is available to all users having the administrator role. This interface supports all commands accessible via the local CLI connected via RS-232 except the following:

- rmlock command
- Export/import of certificates
- Transfer keys command

7.2.6 Protection of the TSF

7.2.6.1 Reliable Time Stamps

The TOE has the capability to obtain reliable time from a remote Network Time Protocol (NTP) Server to provide reliable time stamps for audit services. Additionally, the system administrator can manually set the time (maintained locally in the hardware Real Time Clock (RTC)) on the TOE using the Web UI or CLI management interfaces.

The TOE supports configuration of up to three NTP Servers (via the Web UI or CLI management interfaces) referred to as the preferred timeserver, the first alternate timeserver, and the second alternate timeserver. The NTP configuration includes mode (enabled or disabled), synchronization interval, and time zone; each timeserver is configured with independent IPv4 address and port number.

The administrator must start the NTP client manually; when started, the NTP client will attempt to synchronize with the preferred timeserver by sending a request to the server; once the NTP client receives the response, it will update the system time. If the preferred timeserver cannot be used, the NTP client will automatically try the first alternate timeserver, then the second alternate timeserver. Similarly, if an established connection fails, the NTP client will attempt to use the alternate timeservers in sequence.

To establish a connection to a timeserver, the TOE requires an IPsec tunnel have been previously established between the TOE and the NTP Server; if no IPsec tunnel can be established, the NTP service cannot be used.

If the system administrator updates the system time, the NTP client stops running until it is manually enabled again. **FPT_STM_(EXT).1**

7.2.6.2 TOE Self-Tests

The TOE implements the following set of self-tests, which are executed during initial start-up, periodically once a day, or upon administrator request via the CLI or Web UI.

- Integrity check of the image – SHA-256 of the image is used.
- Power-up tests for openSSL library
  - RNG Test
  - AES encryption/decryption - 128 bit
  - RSA key generation and encryption/decryption - 2048 bit
  - 3DES-ECB encryption/decryption
  - RSA key generation and signature validation - 2048 bit
  - SHA-256 hash
  - HMAC-SHA-1 hash
  - HMAC-SHA-256 hash
- Power-up tests for wireless crypto library
  - AES-CCM encryption/decryption for CCMP - 128 bit
- Power-up tests for IPsec cryptographic functions
  - RNG Test
  - AES encryption/decryption - 128 bit
  - 3DES-ECB encryption/decryption
  - SHA-1 hash
  - HMAC-SHA-1 hash

The integrity of TSF data is verified using sha256 message digest as follows:

- The original message digest of the data is calculated and stored in file /etc/fips/data_files.sha256 on the first time the image boots up
- During Self-Test, the message digest of the data is calculated at run time and stored in /tmp/data_files.sha256.
- These two digests are then compared to verify the integrity of TSF data.

"openssl dgst -sha256" command is used to calculate the message digest.

These self-tests may be invoked by the system administrator via CLI, and Web UI as follows:

- CLI:
  - admin(system.fips-test)>run-self-test <cr>
- Web UI:
  - Path: System Settings > "Run Self Test"
    - Click on "Run Self Test" button under "System Settings" tab.

Success results are logged to `fipscheck.log` and they can be viewed by using following CLI command:

- admin(system.fips-test)>showlog success <cr>

Failure results are logged to `fipserror.log` file & they can be viewed by using following CLI command:

- admin(system.fips-test)>showlog error <cr>

The TOE also implements a set of hardware self tests that are executed by the bootloader when the device boots up that verify the correct operation of the underlying hardware.

These test cover:

1. RAM
2. NOR Flash
3. NAND Flash
4. Ethernet
5. PCI

If the self-tests fail, an error message is displayed on console, logged and the TOE is rebooted.
FPT_TST.1 (1), FPT_TST.1 (2), FPT_TST_EXT.1

7.2.7 TOE Access

There are two sets of advisory/warning messages displayed before establishing a user session. The first message displayed before the login prompt is: “This Device is running in Common Criteria Mode,” and cannot be changed by the administrator.

The second message displayed after the login prompt can be changed by the administrator and can have a length between 10 and 1024 characters. This can be changed by executing a CLI command as given below:
admin(system.access)> set msg <login-msg-text>

This message is stored in the file /etc/motd. This file is not directly accessible to any user including the administrator. The only way to change the contents of this file is using the CLI command given above.

An example of these warning messages before the login/password prompt is displayed below:

> This Device is running in Common Criteria Mode
>
> **********
> Attention:
> This is a protected and private wireless system. No un-authorized access is allowed.
> You must have proper rights to access & manage system from authorized personnel.
> **********
>
> login: admin
> Password:

FTA_TAB.1

The TOE terminates user sessions after a time interval of user inactivity is reached as follows:

- **SSH session**: Administrator can configure user interactivity timeout for SSH Login
  - Default timeout value is 120 seconds.
- **CLI console session**: An administrator-configurable timeout value is used for Local interactive session (CLI console).
  - Default time is 600 seconds.
- **Wireless session**: Administrator can configure user interactivity timeout for WLAN MU (wireless session).
  - Default timeout is 30 minutes
- HTTPS session:
  - administrator configurable session inactivity timeout – default is 180 seconds

FTA_SSL.3.1

The TOE can restrict access of groups of wireless users based in time of day and day of the week. Users can be excluded from all wireless networks defined on the TOE, or only a subset of the defined wireless networks. **FTA_TSE.1**

7.2.8 Trusted Path/Channels

The TOE provides trusted paths for authentication functions, communications to remote audit server, NTP functions, SNMPv3 authentication, and the import/export of configuration files for management. **FTP_ITC_(EXT).1, FTP_TRP.1**

7.2.8.1 802.11i

The TOE maintains a trusted path with wireless users during the wireless user authentication phase. The trusted path is based on EAP-TLS, EAP-TTLS and EAP-PEAP protocols and can be established by wireless client devices with the help of the external authentication server, which performs authentication and cryptographic key derivation operations required by the EAP-TLS, EAP-TTLS and EAP-PEAP protocols

7.2.8.2 SSH

The TOE supports SSHv2 for remote administration of the TOE; this SSH interface gives the administrator access to the CLI. This interface authenticates the SSH server using the SSH Server's public certificate, the client is authenticated using a username and password. Section 7.2.2.2 describes the cryptographic support provided to protect the channel data from modification or disclosure.

7.2.8.3 TLS

The TOE supports TLS1.0 for remote administration of the TOE; this interface gives the administrator access to the Web UI. This interface authenticates the server using the server's public certificate; the client is authenticated using a username and password. Section 7.2.2.3 describes the cryptographic support provided to protect the channel data from modification or disclosure.

7.2.8.4 SNMPv3

The TOE supports SNMPv3 for remote administration of the TOE; this interface gives the SNMP administrator access to the management commands. This interface uses the username and password that is used to provide assured identification of the end-points. The password (shared secret) must be entered at both the client and server by an authorized administrator prior to establishing a SNMP session. Section 7.2.2.5 describes the cryptographic support provided to protect the channel data from modification or disclosure.

7.2.8.5 SFTP

The TOE supports SFTP for importing and exporting configuration files to/from the TOE; SFTP is an extension of the SSH v 2.0 and depends on the SSH transport layer to provides assured identification of its end-points and protection of the channel data from modification or disclosure.

7.2.8.6 IPsec

The TOE maintains a trusted channel for communication with the audit, RAIDUS, and Network Time Protocol servers in the IT Environment. The channel is protected by the IPSec protocol with manual keys and can be initiated by the TOE or the other party. The Administrator has to configure an explicit IPsec tunnel between AP-7131NAccess Point and the RADIUS server, Audit (syslog) server, NTP server. The trusted channel is based on the IPsec/IKE protocol with pre-shared keys. Section 7.2.2.4 describes the cryptographic support provided to protect the channel data from modification or disclosure.

7.2.9 Intrusion Detection (Rogue Access Point)

The TOE provides rogue AP detection, i.e., any unauthorized active AP operating within the radio coverage of an authorized AP. When a rogue-AP is detected, the administrative user is notified with a SNMP trap and a syslog message is generated. In addition, the admin can look for detected rogue APs using the CLI and Web UI interfaces. An audit event is generated when a rogue-AP is detected.

The TOE Rogue AP detection mechanism uses one the following administrator selectable methods:

- RF On-Channel Detection
  - Enables the access point to detect rogue APs on its current (legal) channel setting
- RF Scan by Detector Radio
  - A dedicated Detector AP scans for Rogue APs on all channels.
- RF 'ABG' Scan
  - Scan for rouges over all channels on both of the access point's 11a and 11bg radio bands.

After performing the scan to detect all AP MAC addresses in the wireless coverage range, then comparing the scan results with the list of allowed AP MAC addresses maintained on the TOE. If the MAC address of a detected AP matches an entry on the administrator configured approved list, it is ignored; otherwise, it is reported as a Rogue AP and added to the Rogue AP list, a syslog message generated and a Trap message sent to the SNMPv3 manager. Additionally, the administrator can enable the automatic addition of all detected Motorola/Symbol APs to allowed list.

The administrator has the ability to review the Approved AP list as well as the Rogue AP list, move APs from the Rogue AP list to the Approved AP list, and display specific details for any AP on the Rogue AP list. The available details are as follows:

- *BSSID/MAC*
  - Displays the MAC address of the rogue AP.
- *ESSID*
  - Displays the ESSID of the rogue AP.
- *RSSI*
  - Shows the *Relative Signal Strength* (RSSI) of the rogue AP.

FID_APD_EXT.1, FMT_MOF.1 (5), FMT_SMF.1 (5)

8 Acronyms

Table 23 - TOE Related Abbreviations and Acronyms	
Abbreviation /Acronym	Description
AES	Advanced Encryption Standard
ANonce	Authenticator nonce
BSS	Basic Service Set
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security Protocol
EAP-TTLS	EAP-Tunneled Transport Layer Security Protocol
ESS	Extended Service Set
FIPS 140-2	Federal Information Processing Standard Publication 140-2
IKE	Internet Key Exchange Protocol
IP	Internet Protocol
IPSec	IP Security Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
NTP	Network Time Protocol
PEAP	Protected Extensible Authentication Protocol
PMK	Pair-wise Master Key
PRF	Pseudo Random Function
PSK	Pre-Shared Key
PTK	Pair-wise Transient Key
RTC	Real Time Clock
SF	Security Function
SFP	Security Function Policy
SNonce	Supplicant nonce
SPA	Supplicant MAC address
SSH	Secure Shell Protocol
TLS	Transport Layer Security Protocol
Triple DES	Triple Data Encryption Standard
WLAN	Wireless Local Area Network
WLANAS PP	US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.1, July 2007.

Table 24 - CC Abbreviations and Acronyms	
Abbreviation/Acronym	Description
CAP	Composed Assurance Package
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
DAC	Discretionary Access Control

Table 24 - CC Abbreviations and Acronyms	
Abbreviation/Acronym	Description
DOD	Department of Defense
DoD	See DOD
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

9 References

Table 25 - TOE Guidance Documentation		
Reference	Description	Control Number
[1]	AP-7131N-FGR Access Point Product Reference Guide	72E-161311-01 Rev B
[2]	AP-7131N-FGR Access Point Installation Guide	72-161312-01 Rev B
[3]	Motorola Solutions AP7131N-GR Common Criteria Supplement	72E-170133-01 Rev A

Table 26 - Common Criteria v3.1 References			
Reference	Description	Version	Date
[7]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2009-07-001	V3.1 R3	July 2009
[8]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components CCMB-2009-07-002	V3.1 R3	July 2009
[9]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components CCMB-2009-07-003	V3.1 R3	July 2009
[10]	Common Criteria for Information Technology Security Evaluation Evaluation Methodology CCMB-2009-07-004	V3.1 R3	July 2009

Table 27 – Supporting Documents			
Reference	Description	Version	Date
[12]	NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revised)	---	March, 2007
[13]	NIST Special Publication 800-56 Recommendation On Key Establishment Schemes, [http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf].	Draft 2.0	January 2003
[14]	NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography		March, 2007