AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0]

Security Target Version [1.1]

May 10, 2007

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

CygnaCom Solutions Proprietary

Revision History:

Date	Version	Author	Description
September 20, 2006	0.0.01	Swapna Katikaneni	First Draft
September 29,2006	0.1		Eap Submission
10/31/2006	0.1a	D. Zenelaj	Minor corrections based on the comments of "ST Review per CCEVS Policies 10 and 13" , October 20, 2006
1/17/2007	0.2	Swapna Katikaneni	- Minor changes in T.Bypass, T.MisconfiguredAP, T.RogueAP, T.UnAuthorizedAssociation, T.UnidentifiedActions, and O.Admin - Add FPT_ITT.1 to the IT Environment - Iterate FIA_ATD (attributes for SAFE are stored in the IT Environment) - Add additional details to sections 2.4.1 and 6.1.4 SA-1 as needed.
1/25/2007	0.2a	Swapna Katikaneni	Update to FAU_GEN.1
3/27/2007	1.0	D. Zenelaj	Minor updates for consistency with ADV documentation
5/10/2007	1.1	D. Zenelaj	Changes to address issues for VOR date 26 April 2007.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

1.1 Security Target Identification

Table 1-1 below provides ST Identification Information.

Table 1-1 Security Target Identification

TOE Identification:	AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition Enterprise Edition [v 2.0]
ST Title:	AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0] Security Target
ST Version:	1.1
ST Author(s):	Swapna Katikaneni; Dragua Zenelaj
ST Date:	May 10, 2007
Assurance Level:	EAL2
Common Criteria Version	2.3
Strength of Function:	SOF-Basic
Registration:	<To be filled in upon registration>
Keywords:	Wi-Fi Firewall, Access Point(AP), Wireless Local Area Network(WLAN)

1.2 Security Target Overview

AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0] is a wireless intrusion detection and prevention system. It protects a target network from over-the-air wireless attacks from unauthorized Wi-Fi activities. These can come in the form of Rogue APs or unauthorized wireless devices attempting to connect to the target network.

- SpectraGuard Enterprise is a wireless intrusion detection and prevention solution consisting of a Server and wireless Sensor devices, which continuously scan the airwaves and provide automatic protection against any unauthorized Wi-Fi activities.
- SpectraGuard SAFE Enterprise Edition (Security Agent For Endpoints) provides wireless security for mobile users. It monitors and prevents wireless threats and misconfigurations that may pose a security threat to the data on the mobile computer. SpectraGuard SAFE Enterprise Edition Server Edition integrates with SpectraGuard Enterprise. It allows all the SpectraGuard SAFE Enterprise Edition users to be managed centrally on the SpectraGuard Enterprise Server

These solutions provide comprehensive prevention for all types of threats, across all bands and (allowed) channels. The products can be configured to block threats automatically and a single sensor is capable of blocking multiple threats

1.3 Conformance Claims

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.3. There are no PP claims.

1.4 Document Organization

- Section 1, Introduction, identifies the Security Target, includes an Overview, CC Claims, Acronyms, References, Terminology, and Document Conventions.
- Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.
- Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment, any applicable organizational security policies, and threats relevant to secure TOE operation.
- Section 4, Security Objectives, defines the security objectives for the TOE and its environment.
- Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.
- Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.
- Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.
- Section 8, Rationale presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

1.5 Conventions, Terminology, Acronyms

This section specifies the formatting information used in this ST.

1.5.1 Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. All of the components in this ST are taken directly from Part 2 of the CC except the ones noted with "_EXP" in the component name. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1 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.

This ST indicates which text is affected by each of these operations in the following manner:

- Iterations are identified with a dash and a number "-#". These follow the short family name and allow components to be used more than once with varying operations. “*” refers to all iterations of a component.
- Assignments and Selections specified by the ST author are in [***italicized bold text***].
- Refinements are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in italicized bold and underlined text.
- Explicitly Stated Requirements are specified with a “_EXP” added to the component name.
- Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *Application Note: italicized text*.
- NIAP and CCIMB Interpretations have been reviewed. The original CC text modified by the interpretation is not denoted nor explained.

1.5.2 Terminology

- **Authorized Administrator** - An administrator who has been identified and authenticated by the TOE and has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given to them.
- **802.11**-An IEEE wireless LAN specification for over-the-air interface between a wireless Client and a base station or between two wireless Clients
- **Access Point**-Access Point also referred to, as an AP is a station(component that connects to the wireless medium) that provides distribution services. It is the hub used by wireless Clients for communicating with each other and connecting to the WLAN.
- **Ad hoc Network**-A network formed by peer-to-peer connections between wireless Clients. It is difficult to enforce tight security policy controls on ad hoc connections. Therefore, ad hoc connections create a security vulnerability
- **Authorized Client**-An Authorized Client is one that has successfully connected to an Authorized AP at least once. Once identified as Authorized, a Client remains Authorized until it is deleted by the administrator and is re-classified as Unauthorized
- **Classification Policy**-Classification Policy allows the administrator to define AP and Client classification policies to control automatic movement of APs and Clients to the appropriate folders
- **Client**-A laptop, a handheld device, or any other system that uses the wireless medium (802.11 standard) for communication
- **Event Audit Data**-The event data collected about the wireless network.
- **Folder** - A folder holds a specific category of access points or clients.
- **Hostname**-A unique name by which a computer is identified on the network
- **Indeterminate AP**-An AP for which the TOE cannot determine whether it is plugged into the wired network. This AP should be inspected and classified by the administrator
- **IP Address**-Internet Protocol Address, a 32-bit numeric identifier for a computer or a device on the network
- **Network Status**-Network status specifies if the network is locked or unlocked. Once a protected network segment is locked, all new APs connected to it are pre-classified as Rogue and have to be approved manually. If a protected network segment is unlocked, any new APs connected to this network will be automatically classified based on the Security, Protocol, SSID, and Vendor Settings

- **Potentially Authorized AP**-A new AP plugged into your wired network and conforming to the Network Policy settings (SSID, Vendor, Encryption, and Protocol) for its network segment; this AP must be inspected before manually classifying it as Authorized AP.
- **Potentially External AP**-A new AP not plugged into the wired network. This is an AP usually belonging to a neighbor. It does not pose a threat to the protected wired network
- **Potentially Rogue AP**-A new AP plugged into the protected wired network but not conforming to the Network Policy settings (SSID, Vendor, Encryption, and Protocol) for its network segment. This AP is never authorized and can be automatically classified as Rogue AP based on the Classification Policy
- **Security Settings**-An IEEE 802.11 defined MAC–level privacy mechanism that protects the contents of data frames from eavesdropping using encryption
- **SSID**-A unique token identifying an 802.11 WLAN; all wireless devices on a WLAN must employ the same SSID to communicate with each other.
- **System Audit Data** - The logs generated based on the actions of the TOE itself. This includes the authentication of users accessing the TOE, actions taken directly on the TOE, and actions of the TOE itself.
- **System Data -**Non security relevant data required for the operation of the TOE. Examples of system data for this TOE are Operating region, channels to defend, channels to monitor, RF Signal computation constants, etc.
- **Target Network** - The domain of devices that the TOE protects.
- **Threat** - Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
- **Threat Agent** - Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.
- **TOE Security Function (TSF) Data** - Information used by the TSF in making TOE security policy (TSP) decisions. TSF data may be influenced by users if allowed by the TSP. Security attributes, authentication data, and information flow control policy's subject and object security attributes are examples of TSF data.
- **Unauthorized Client**-A Client that is not authorized; an Unauthorized Client has never connected successfully to an Authorized AP
- **Unauthorized User** - Any person who is not authorized, under the TSP, to access the TOE. This definition also applies to authorized users who seek to exceed their authority.
- **User** - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
- **User Data** - Data created by and for the authorized user that does not affect the operation of the TSP. User data is separate from the TSF data, which has security attributes associated with it and the system data, which is required for the system to operate but is not security relevant.
- **VPN**-Virtual Private Network, a network constructed using public wires to connect nodes. For example, there are a number of systems that enable the administrator to create networks using the Internet as the medium for transporting data; these systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted
- **Vulnerability -** A weakness that can be exploited to violate the TOE security policy.
- **WEP**-Wired Equivalent Privacy, an IEEE 802.11 defined MAC–level privacy mechanism that protects the contents of data frames from eavesdropping using encryption
- **WLAN**-Wireless Local Area Network that uses high frequency radio waves, rather than wires to communicate between nodes

1.5.3 Acronyms

The acronyms used within this Security Target:

Table 1-2 Acronyms

Acronym	Definition
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
AP	Access Point
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
FAU	Security Audit
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTP	Trusted Channels/Path
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
ID	Identifier
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
OS	Operating System
SAFE	Security Agent For Endpoints
SF	Security Function
SFP	Security Function Policy
SGE	SpectraGuard Enterprise
SSID	Service Set Identifier
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol

Acronym	Definition
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

1.5.4 References

This section contains descriptions of documents pertaining to this ST and or subject TOE.

Table 1-3 References

ID	Document Title	Version
[CC]	*Common Criteria for Information Technology Security Evaluation*, CCMB-2005-08-002, Version 2.3, August 2005.	2.3
[CC Supp]	AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0] Common Criteria Supplement to the Guidance Documentation	1.6
[CM]	AirTight Networks SpectraGuard Enterprise and SpectraGuard SAFE Enterprise Edition Configuration Management	1.0
[DEL]	AirTight Networks SpectraGuard Enterprise and SpectraGuard SAFE Enterprise Edition	0.2
[FSP]	AirTight Networks SpectraGuard Enterprise and SpectraGuard SAFE Enterprise Edition Development Specification (FSP/HLD/RCR) Common Criteria Evaluation	1.0
[E Install]	SpectraGuard Enterprise Installation Guide	5.0
[E Quick Setup]	SpectraGuard Enterprise Quick Setup Guide	5.0
[E User Guide]	SpectraGuard Enterprise User Guide	5.0
[PP Guide]	Text for ISO/IEC WD 15446, Information technology – Security techniques – Guide for production of Protection Profiles and Security Targets 1999-07-07	1.27.22
[SAFE User Guide]	SAFE User Guide - located on SAFE client	2.0
[SOF]	AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0], Strength of Function Analysis	1.0
[TP CYG]	Evaluation Test Report AirTight Networks SpectraGuard Enterprise v5.0 and SpectraGuard SAFE Enterprise Edition v2.0	1.0
[TP Dev]	Developer Test Report AirTight Networks SpectraGuard Enterprise v5.0 and SpectraGuard SAFE Enterprise Edition v2.0	1.0
[VA]	AirTight Networks SpectraGuard Enterprise and SpectraGuard SAFE Enterprise Edition Vulnerability Analysis	1.0
[Web Help]	SAFE Web Help document	2.0

2 TOE Description

2.1 Product Type

AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0] is a wireless intrusion detection and prevention system. It protects a target network from over-the-air wireless attacks from unauthorized Wi-Fi activities. These can come in the form of Rogue APs or unauthorized wireless devices attempting to connect to the target network.

2.2 TOE Components

SpectraGuard Enterprise is a wireless intrusion detection and prevention solution comprising of a Server and wireless Sensor devices, which continuously scan the airwaves and provide automatic protection against any unauthorized Wi-Fi activities. The sensors communicate with the centralized SpectraGuard Server. All management of the entire solution is done through a web-based GUI. The system architecture of SpectraGuard Enterprise is illustrated below.

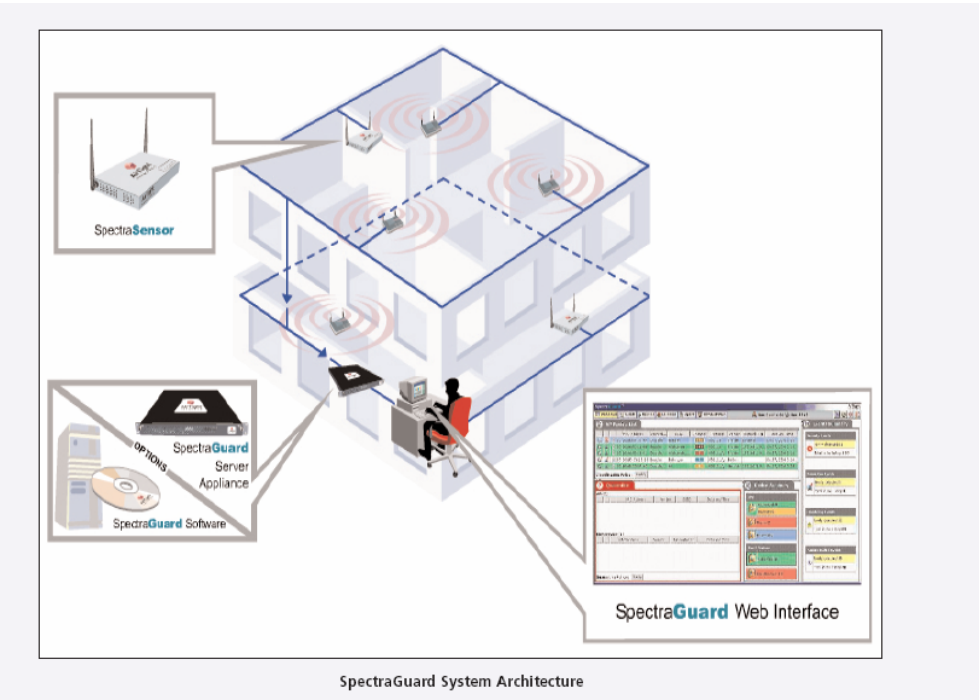

Figure 2-1 Spectraguard System Architecture

SpectraGuard SAFE Enterprise Edition (Security Agent For Endpoints) provides wireless security for mobile users. It monitors and prevents wireless threats and misconfigurations that may pose a security threat to the data on the mobile computer. SpectraGuard SAFE Enterprise Edition Enterprise Edition integrates with SpectraGuard Enterprise. It allows all the SpectraGuard SAFE Enterprise Edition users to be managed centrally on the SpectraGuard Enterprise Server

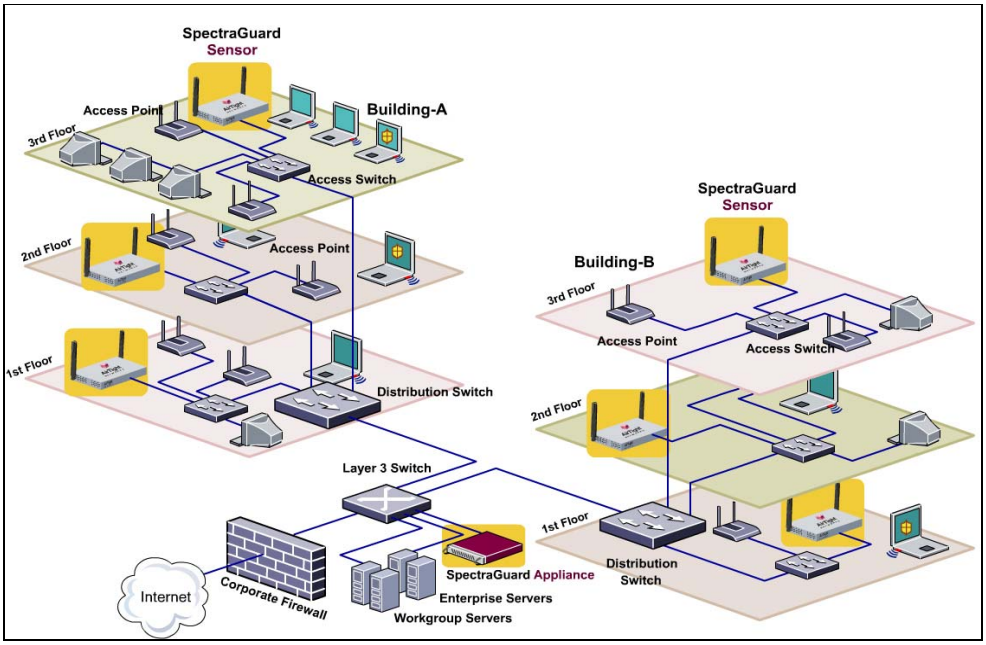

Figure 2-2 Typical Deployment

2.3 TSF Physical Boundary and Scope of the Evaluation

The TOE includes the following:

- SpectraGuard Enterprise Server v5.0 comprised of all AirTight Networks developed software, firmware, and hardware on the SpectraGuard Enterprise appliance (Labeled as SpectraGuard Appliance in the figure below) with Management Console v5.0
- SpectraGuard Sensors v5.0 comprised of all AirTight Networks developed software, firmware, and hardware on the SpectraGuard Enterprise appliance
- SAFE Enterprise Edition v2.0 client is a software-only component

The Enterprise Server including Sensors can be used independent of SAFE. This means that installing and using the Enterprise Server and Sensors will protect the target network. SAFE is an additional component that can be installed on mobile devices to provide an additional level of protection for wireless laptops.

Note: The SAFE Enterprise Edition client is configured in the Management Console with all security, event, and preference settings set by the Authorized Administrator. The SAFE Enterprise Edition client is configured so the end user cannot change these settings for all security profiles. [1]

[1] Section 9.12.1 [User Guide], “Do not allow the user to override the above settings”option is turned on.

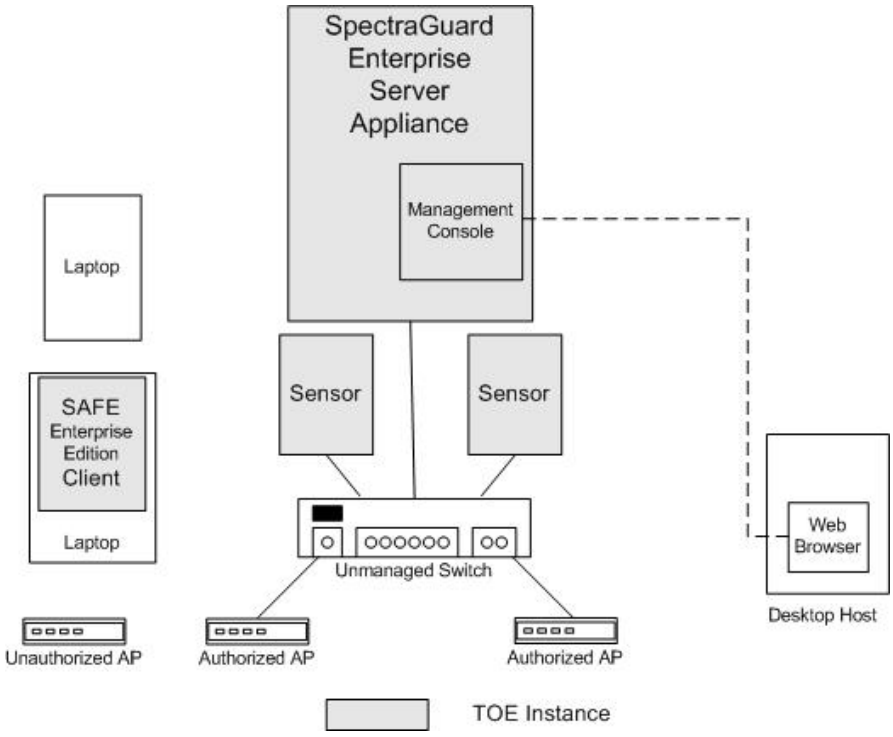

Figure 2-3 TOE Boundary

The following items are external to the TOE:

- Third Party Software that the TOE relies upon
- Underlying operating system (OS) software and hardware for the machine on which SAFE is installed.
- Desktop Host used to access Management Console via web browser
- Transport standards HTTPS implementations
- SSH implementation
- Web server and browser software
- Wireless Access Points

2.4 Logical Boundaries

The logical boundaries of the TOE can be described in the terms of the security functionalities that the TOE provides to the target network that utilizes at least one of the TOE components for detection and protection against any unauthorized Wi-Fi activities.

The logical boundary of the TOE will be broken down into the following security class features which are further described in sections 5 and 6 of the ST.

2.4.1 Security Audit

The Enterprise Server component generates audit records for the actions on the Enterprise Server (system audit data) as well as for the events monitored by the Enterprise Server and SAFE respectively (event audit data).

From the Enterprise Server component's Management Console, an authorized administrator[2] can read the event audit data generated by the Enterprise Server and SAFE components. The system audit and event audit data records are provided in tabularized text suitable for the user to interpret the information.

The Enterprise Server provides protection of the audit records. SAFE stores the events in a database (MDB) file. The file is password protected and the password is internally known only to the SAFE application and is not revealed to users. This password prevents users from directly reading or altering the event data.

2.4.2 Information Flow Control

The TOE enforces information flow control policy by granting or denying access to the protected network based upon the information flow policy defined by an authorized administrator.

2.4.3 Identification and Authentication

The SpectraGuard Server requires that administrators be properly identified and authenticated prior to performing any administrative tasks on the system.

2.4.4 Security Management

The SpectraGuard Server provides a web-based interface (Management Console) to manage the configuration of the server. SpectraGuard SAFE Enterprise Edition users are managed centrally on the SpectraGuard Enterprise Server through the web-based interface. Authorized Administrators are able to create, modify, and view the Information flow security policy rules and manage the TOE.

2.4.5 Partial Protection of TSF

The SpectraGuard Server protects its programs and data from unauthorized access through its own interfaces. The TSF ensures that all information that flows through it must flow through the policy enforcement mechanisms.

[2] The Authorized Administrator role includes all of the administrative roles defined in the product - from a security perspective.

2.5 TOE Operational Environment

It is assumed that there will be no untrusted users or software on the SpectraGuard host used for managing the TOE components. SpectraGuard Enterprise and SAFE rely upon the IT environment to provide protection of data transfer between TOE components.

The TOE security environment can be categorized as follows:

2.5.1 Security Audit

The Enterprise server system audit data is viewable by being downloaded through the Management Console to a text file. Once the file is saved to the local disk drive the OS identification and authentication allows access to the file.

On the SAFE client, once a user has logged into the OS, they have access to view the local SAFE event audit data via the SAFE GUI.

SAFE relies on the underlying operating system of the client on which it is installed for partial protection of audit trail data.

2.5.2 Identification and Authentication

SpectraGuard SAFE Enterprise Edition relies on the underlying OS for identification and authentication. The user security attributes for SpectraGuard SAFE Enterprise Edition are maintained by the underlying OS.

2.5.3 Partial Protection of TSF

SpectraGuard SAFE Enterprise Edition relies on the IT environment to provide security capabilities for the TOE's protection. For the TOE's own protection the IT environment includes requirements that relate to the integrity of the TSF. These include SFP domain separation, non-bypassability, and a reliable time-stamp. The IT environment supports the TSF by ensuring that that all information flows through the policy enforcement mechanisms. The IT environment's security functional policy must be invoked and succeed before allowing another IT environment function to proceed.

3 TOE Security Environment

This section identifies secure usage assumptions, organizational security policies, and threats to security.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 Assumptions

Item	Assumption ID	Assumption Description
1	A.Access	An authorized administrator can access the TOE locally via a serial cable, remotely via HTTPS, or remotely via SSH.
2	A.AuditBackup	Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.
3	A.Admin	The administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
4	A.Manage	It is assumed that one or more administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
5	A.NoUntrusted	It is assumed that there will be no untrusted users of the TOE and no untrusted software on the TOE.
6	A.Physical	It is assumed that the hardware and software critical to the security policy enforcement will be protected from unauthorized physical modification.
7	A.ProtectComm	Those responsible for the TOE will ensure the communications between the TOE components are secure.
8	A.Users	It is assumed that users will protect their authentication data.

Application Note: A Access and A.ProtectComm provides for secure communications between the Server and Sensors. In addition they provide for secure communications between the GUI/CLI Console and TOE components. This can be accomplished by the following:

1. *Secure HTTPS channel via SSL for the GUI Console*
2. *Secure SSH channel between the CLI User Console and Server using any standard SSH client utility.*
3. *There is a direct connection between the CLI User Console and Server via a serial cable.*

3.2 Threats

There are threats to the assets against which protection will be required. A ‘threat’ is simply an undesirable event, possibly caused by an identified threat agent, which places, or may place, the assets at risk.[3] The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product. The threats are identical to both the server and SAFE. The server can mitigate all the threats, but SAFE adds an additional level of security.

[3] [PP Guide], p.19

Table 3-2 Threats

Item	Threat ID	Threat Description
1	T.Adhoc	An Authorized Client may connect to another client, whether Authorized , Unauthorized or Banned which might result in compromise of TSF data on the client.
2	T.AuditCompromise	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.
3	T.AuthClient	An Authorized Client of the TOE may connect to Rogue or External(neighboring) APs which might result in compromise of TSF data on the client
4	T.Bypass	An unauthorised user may attempt to bypass the information flow control policy. If the attacker is successful, TSF data may be lost or altered.
5	T.MaliciousTSFCompromise	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
6	T.Masquerade	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.
7	T.MisconfiguredAP	An attacker may gain access to the protected network through misconfigured APs. If the attacker is successful, TSF data may be lost or altered.
8	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
9	T.RogueAP	An attacker may gain access to the protected network through Unauthorized Access Points connected to the protected network. If the attacker is successful, TSF data may be lost or altered.
10	T.UnAuthorizedAssociation	An attacker may gain access to the protected network through a connection between the Authorized AP and an Unauthorized Client. If the attacker is successful, TSF data may be lost or altered.
11	T.UnidentifiedActions	Failure of the authorized administrator to identify and act upon unauthorized actions may occur. If the attacker is successful, TSF data may be lost or altered.

4 Security Objectives

The following sections describe the security objectives for the TOE and for the TOE environment.

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 TOE Security Objectives

Item	TOE Objective	TOE Objective Description
1	O.Admin	The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
2	O.Audit	The TOE will provide the capability to detect and create records of security-relevant events.
3	O.AuditProtection	The TOE will provide the capability to protect audit information.
4	O.AuditReview	The TOE will provide the capability to selectively view audit information
5	O.IFlow-Enterprise	The SpectraGuard Enterprise will detect and take action against attempts by unauthorized users, unauthorized access points or unauthorized clients to bypass, deactivate, or tamper with the security policy defined for the TOE by an authorized administrator
6	O.IFlow-SAFE	The SpectraGuard SAFE Enterprise Edition will detect and take actions against attempts by unauthorized access points to bypass, deactivate, or tamper with the security policy defined for the TOE by an authorized administrator
7	O.IDAuth	The TOE will maintain user security attributes and will identify and authenticate the users prior to allowing access to TOE functionality.
8	O.NonBypass	The TOE must ensure the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed.
9	O.PartialSelfProtection	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.

4.2 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for the IT Environment

Item	Objective for IT Environment	Description
1E	OE.AuditProtection	The IT environment will provide the capability to protect audit information.
2E	OE.IDAuth	The IT environment will be able to identify and authenticate users prior to allowing access to IT environment functions and data.
3E	OE.NonBypass	The IT environment will ensure that the IT environment's security functional policy is invoked and succeeds before allowing another IT environment function to proceed.
4E	OE.PartialSelfProtection	The IT 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.
5E	OE.ProtectData	The IT environment will protect TSF data when transferred between TOE Components.
6E	OE.Time	The IT Environment will provide reliable time stamps.

4.2.1 Security Objectives for the Non-IT Environment

The Non-IT security objectives are as follows:

Table 4-3 Security Objectives for Non-IT Security Environment

Item	Non-IT Environment Objective	Non-IT Environment Objective Description
1E	ON.Access	The administrator must ensure that the communications between the User Console and the TOE is secure
2E	ON.AuditBackup	Those responsible for the TOE must ensure that the audit files will be backed up and will monitor disk usage to ensure audit information is not lost.
3E	ON.Install	Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner that maintains IT security.
4E	ON.NoUntrusted	The administrator must ensure that there is no untrusted users and no untrusted software on the TOE
5E	ON.Operations	The TOE will be managed and operated in a secure manner as outlined in the supplied guidance.
6E	ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
7E	ON.Physical	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
8E	ON.ProtectAuth	Users must ensure that their authentication data is held securely and not disclosed to unauthorized persons.
9E	ON.ProtectComm	The administrator must ensure that the communications between the TOE components are secure.

5 Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, assurance components from Part 3 of the CC, NIAP and International interpretations, and explicit functional components derived from the CC components.

5.1 Security Functional Requirements for the TOE

Table 5-1 below summarizes the security functional requirements for the TOE. They consist of the components derived from Part 2 of the CC (and if applicable, explicitly stated requirements).

Table 5-1 Security Functional Requirements for the TOE

Item	SFR ID	SFR Title
1	FAU_GEN.1*	Audit data generation
2	FAU_SAR.1	Audit review
3	FAU_SAR_EXP.2	Restricted audit review
4	FAU_SAR_EXP.3	Selectable audit review
5	FAU_SEL_EXP.1	Selective audit
6	FAU_STG_EXP.1-1	Protected audit trail storage
7	FDP_NPT_EXP.1	Network Protection Policy
8	FDP_CPT_EXP.1	Client Protection Policy
9	FIA_ATD_EXP.1-1	User attribute definition
10	FIA_UAU_EXP.2-1	User authentication before any action
11	FIA_UID_EXP.2-1	User identification before any action
12	FMT_MOF.1 *	Management of security functions behaviour
13	FMT_MTD.1*	Management of TSF data
14	FMT_SMF.1	Specification of management functions
15	FMT_SMR_EXP.1	Security roles
16	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
17	FPT_SEP_EXP.1-1	TSF domain separation

Note: The component of the TOE to which the SFR corresponds has been indicated in the title of the SFR in parentheses. Additional details can be found included in the TSS section. Also note, * denotes iterated component.

5.1.1 Class FAU: Security audit

5.1.1.1 FAU_GEN.1-1 Audit data generation (Enterprise)

FAU_GEN.1.1-1 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 for the [***not specified***] level of audit; and

c) **[*the audit events specified in Table 5-2*]**.

FAU_GEN.1.2-1 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***the additional information identified in Table 5-2***].

Table 5-2 Enterprise Audit Events

Item	SFR	Auditable Events	Additional Information
1	FAU_GEN.1-1	None	Not Applicable
2	FAU_SAR.1	None	Not Applicable
3	FAU_SAR_EXP.2	None	Not Applicable
4	FAU_SAR_EXP.3-1	None	Not Applicable
5	FAU_SEL_EXP.1	All modifications to the audit configuration that occur while the audit collection functions are operating	Identity of authorized user
6	FAU_STG_EXP.1-1	None	Not Applicable
7	FDP_CPT_EXP.1	All decisions on requests for information flow.	Security attributes of the subject
8	FDP_NPT_EXP.1	All decisions on requests for information flow.	Security attributes of the subjects
9	FIA_ATD_EXP.1-1	None	Not Applicable
10	FIA_UAU_EXP.2-1	Successful and unsuccessful use of the authentication mechanism	User Identity
11	FIA_UID_EXP.2-1	Successful and unsuccessful use of the identification mechanism	User Identity
12	FMT_MOF.1*	None	Not Applicable
13	FMT_MTD.1-1	Use of Administration Function	Identity of authorized user
14	FMT_SMF.1	None	Not Applicable
15	FMT_SMR_EXP.1	None	Not Applicable
16	FPT_RVM_EXP.1-1	None	Not Applicable
17	FPT_SEP_EXP.1-1	None	Not Applicable

5.1.1.2 FAU_GEN.1-2 Audit data generation (SAFE)

FAU_GEN.1.1-2 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 for the [***not specified***] level of audit; and

c) [***the audit events specified in Table 5-3***].

FAU_GEN.1.2-2 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, 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, [***the additional information identified in Table 5-3***].

Table 5-3 SAFE Audit Events

Item	SFR	Auditable Events	Additional Information
1b	FAU_GEN.1-2	None	Not Applicable
2	FAU_SAR.1	None	Not Applicable
4	FAU_SAR_EXP.3-2	None	Not Applicable
8	FDP_CPT_EXP.1	All decisions on requests for information flow.	Security attributes of the subject
12b	FMT_MOF.1-2	None	Not Applicable
13b	FMT_MTD.1-2	None	Not Applicable
14	FMT_SMF.1	None	Not Applicable

5.1.1.3 FAU_SAR.1 Audit Review (Enterprise and SAFE)

FAU_SAR.1.1 The TSF shall provide [***an authorized administrator***] with the capability to read [***all audit trail data***] from the audit records.

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

5.1.1.4 FAU_SAR_EXP.2 Restricted audit review (Enterprise)

FAU_SAR_EXP.2.1 The TSF shall prohibit all users read access to the event audit records, except those users that have been granted explicit read-access.

5.1.1.5 FAU_SAR_EXP.3-1 Selectable Audit Review (Enterprise)

Formatted: French (France)

FAU_SAR_EXP.3.1-1 The TSF shall provide the ability to perform searches and sorting of event audit data based on:

a) Severity of an event;

b) Event status;

c) Event location;

d) Event description;

e) Event Category;

f) Event type within a category;

g) Range of dates and times ;

5.1.1.6 FAU_SAR_EXP.3-2 Selectable audit review (SAFE)

FAU_SAR_EXP.3.1-2 The TSF shall provide the ability to perform searches and sorting of event audit data based on

1. Event Type
2. Security Profile
3. Event Summary
4. Event Duration.

5.1.1.7 FAU_SEL_EXP.1 Selective audit (Enterprise)

Formatted: French (France)

FAU_SEL_EXP.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) event type.

b) none.

5.1.1.8 FAU_STG_EXP.1-1 Protected Audit Trail Storage (Enterprise)

FAU_STG_EXP.1.1-1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG_EXP.1.2-1 The TSF shall be able to [***prevent***] unauthorized modifications to the audit records in the audit trail.

5.1.2 Class FDP: User Data Protection

5.1.2.1 FDP_NPT_EXP.1 Network Protection Policy (Enterprise)

FDP_NPT_EXP.1.1 The Enterprise Server shall protect the Wired Network from unauthorized Access points or Unauthorized Clients based in the following rules:

A. Information flow through a newly discovered Access Point connected to a network segment and the enterprise network is allowed provided:

   1. The Access Point satisfies the following set of rules,

   a) The network segment being accessed by the Access point is protected by the Enterprise Server, and

   b) The status of the network segment being accessed by the Access Point is unlocked, and

   c) The Access Point conforms to the default 802.11 policy or the custom 802.11 policy(security settings, protocol) defined for the network segment by the Enterprise Server administrator, and

   d) Presumed SSID of the Access point is in the set of SSIDs allowed to access the network, and

   e) Presumed vendor of the Access Point is in the set of AP vendors recognized by the network

   and

   2. Presumed MAC address of the Access Point is in the set of MAC addresses recognized by the Server as an authorized Access Point.

B. Information flow between a newly discovered client and the enterprise network through an authorized access point is allowed provided:

   - Presumed MAC address of the client is in the set of MAC addresses recognized by the Enterprise Server as an authorized client

C. Information flow between an unauthorized client or an uncategorized client and the enterprise network through an access point is allowed provided:

- The unauthorized or uncategorized Client has been reclassified as an authorized client based upon its association with the Access Point as defined by the administrator or automatic client classification policy

D. The Server along with the Sensor will disrupt and block the information flow between the Client and the Access point by broadcasting DEAUTHENTICATE packets if the information flow between an unauthorized client and the Enterprise network does not match any of the above A, B, C rules**.**

5.1.2.2 FDP_CPT_EXP.1 Client Protection Policy (SAFE)

FDP_CPT_EXP.1.1 (SAFE) - The SAFE shall protect an Authorized Client by allowing it to connect to Authorized Access Points only based on the following rules:

A. Information flow between an authorized client and an access point is allowed ***provided:***

1. ***The presumed MAC address and SSID of the access point are specified in the wireless security policy of the SAFE as an allowed access point***

   - **If the AP MAC address and SSID is not configured within the SAFE client as being authorized, a warning is displayed on the SAFE Console.**

5.1.3 Class FIA: Identification and authentication

5.1.3.1 FIA_ATD_EXP.1-1 User attribute definition (Enterprise)

FIA_ATD_EXP.1.1-1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) **[*User identity;***

b) ***Password*****].**

5.1.3.2 FIA_UAU_EXP.2-1 User authentication before any action (Enterprise)

FIA_UAU_EXP.2.1-1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.3 FIA_UID_EXP.2-1 User identification before any action (Enterprise)

FIA_UID_EXP.2.1-1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Class FMT: Security Management (FMT)

5.1.4.1 FMT_MOF.1-1 Management of security functions behaviour (Enterprise)

FMT_MOF.1.1-1 The TSF shall restrict the ability to [***determine the behaviour of, modify the behaviour of***] the functions [

- Auditing
- Information flow security policy rules
- Identification and authentication

] to [***authorized administrator***].

5.1.4.2 FMT_MOF.1-2 Management of security functions behaviour (SAFE)

FMT_MOF.1.1-2 The TSF shall restrict the ability to [***determine the behaviour of, modify the behaviour of***] the functions [

- Auditing
- Information flow security policy rules

] to [***authorized administrator***].

5.1.4.3 FMT_MTD.1-1 Management of TSF data (Enterprise)

FMT_MTD.1.1-1 The TSF shall restrict the ability to **[*see operations specified in Table 5-4*]** the **[*TSF Data as specified in Table 5-4*]** to **[*the authorized administrator*].**

Table 5-4 Management of TSF Data

Item	Security Function	Operation	TSF data
Enterprise Settings through Management Console			
1	Security Audit	View	Audit Logs
2	Security Audit	View, create, schedule, modify and delete	Customized Audit Reports
3	Identification and Authentication	Query, modify, delete and assign	user attributes defined in FIA_ATD_EXP.1.1
4	Security Management	View properties and status of	Access points, clients and sensors
5	Security Management	Reclassify	Access points and clients
6	Security Management	Locate distance from a sensor	Access points and clients
7	Security Management	Merge, split	Authorized Access points
8	Security Management	Add, delete, import a planner file of	Location node
9	Security Management	Activate	Event generation and Intrusion Prevention
10	Security Management	Set	parameters for Access points, clients and sensors
11	Security Management	Set record constants per	sensor
12	Security Management	Set	Parameters for sensor server communication
13	Security Management	Add, Import	Banned(Unauthorized) AP list
14	Security Management	Add, Import	Banned(Unauthorized) client list
15	Security Management	Add to vendor list	Vendor name
16	Security Management	View, add, modify	Operating region, channels to defend, channels to monitor
17	Security Management	View details and status	Enterprise server
18	Security Management	Start and stop	Enterprise server
19	Security Management	Create, query, modify and delete	Login ID of an authorized administrator
20	Security Management	Create and modify	own password
21	Security Management	create, modify, and view	Information flow security policy rules

5.1.4.4 FMT_MTD.1-2 Management of TSF data (SAFE)

FMT_MTD.1.1-2 The TSF shall restrict the ability to [***see operations specified in Table 5-5***] the [***TSF Data as specified in Table 5-5***] to [***the authorized administrator***].

Table 5-5 Management of TSF Data

Item	Security Function	Operation	TSF data
SAFE Settings through the Management Console			
22	Security Audit	View and set number of days until deletion of old logs	Audit Logs
23	Security Management	Add, Delete	AP to/from Allowed list
24	Security Management	View status	SAFE
25	Security Management	View and change settings of the current security profile and change to a different security profile	Security profile
26	Security Management	View, modify	Event notification settings
27	Security Management	create, modify, and view	Information flow security policy rules

5.1.4.5 FMT_SMF.1 Specification of Management Functions (Enterprise and SAFE)

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

- ***determine the behaviour of and modify the behaviour of the functions specified in sections 5.1.4.1 (see FMT_MOF.1*),***
- ***query, modify, delete, and other operations as specified in Table 5-3 on the TSF Data as specified in Tables 5-4 and 5-5 (See FMT_MTD.1*)***
- ***End users are able to view the settings of SAFE via the SAFE Console on the client laptop (See Table 5-6)***

Table 5-6 View TSF Data (SAFE)

Item	Security Function	Operation	TSF data
30	Security Audit	View	Audit Logs
31	Security Management	View details and status	Network Interface
32	Security Management	View status	SAFE
33	Security Management	View settings of the current security profile and switch between authorized security profiles	Security profile

Item	Security Function	Operation	TSF data
34	Security Management	View	Event notification settings
35	Security Management	View	Information flow security policy rules

]

5.1.4.6 FMT_SMR_EXP.1 Security roles (Enterprise)

FMT_SMR_EXP.1.1 The TSF shall maintain the roles **[*Authorized Administrator*[4]].**

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

5.1.5 Class FPT: Protection of the TOE Security Functions

5.1.5.1 FPT_RVM_EXP.1-1 Non-bypassability of the TSP (Enterprise and SAFE)

FPT_RVM_EXP.1.1-1 The TSF, when invoked by the underlying IT environment, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.2 FPT_SEP_ EXP.1-1 TSF domain separation (Enterprise and SAFE)

FPT_SEP_ EXP.1.1-1 The TSF, when invoked by the underlying host IT environment, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_ EXP.1.2-1 The TSF, when invoked by the underlying host IT environment, shall enforce separation between the security domains of subjects in the TSC.

5.1.6 Strength of Function

The overall strength of function requirement is SOF-basic. The strength of function requirement applies to FIA_UAU_EXP.2. The SOF claim for FIA_UAU_EXP.2 is SOF-basic. The strength of the "secrets" mechanism is consistent with the objectives of authenticating users (O.IDAuth). Strength of Function shall be demonstrated for the non-certificate based authentication mechanisms to be SOF-basic, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a low-level attack potential.

5.2 Security Requirements for the IT Environment

Table 5-7 below summarizes the security functional requirements for the IT environment. They consist of the components derived from Part 2 of the CC (and if applicable, explicitly stated requirements).

[4] *The various Administrative roles described in the ITSF, SM-4, are treated as a single security role* "authorized administrator",

Table 5-7 Security Functional Requirements for the IT Environment

Item	SFR ID	SFR Title
1E	FAU_STG_EXP.1-2	Protected audit trail storage
2E	FIA_ATD_EXP.1-2	User attribute definition
3E	FIA_UAU_EXP.2-2	User authentication before any action
4E	FIA_UID_EXP.2-2	User identification before any action
5E	FPT_ITT.1	Basic internal TSF data transfer protection
6E	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
7E	FPT_SEP_EXP.1-2	TSF domain separation
8E	FPT_STM.1	Reliable time stamps

5.2.1 Class FAU: Security audit

5.2.1.1 FAU_STG_EXP.1-2 Protected Audit Trail Storage (SAFE)

FAU_STG_EXP.1.1-2 Refinement: The ***IT Environment*** shall protect the stored audit records from unauthorized deletion.

FAU_STG_EXP.1.2-2 Refinement: The ***IT Environment*** shall be able to prevent unauthorized modifications to the audit records in the audit trail.

5.2.2 Class FIA: Identification and authentication

5.2.2.1 FIA_ATD_EXP.1-2 User attribute definition (SAFE)

FIA_ATD_EXP.1.1-2 Refinement: The ***IT Environment*** shall maintain the following list of security attributes belonging to individual users:

a) **[*User identity;***

b) ***Password*****].**

5.2.2.2 FIA_UAU_EXP.2-2 User authentication before any action (SAFE)

FIA_UAU_EXP.2.1-2 Refinement: The ***IT Environment*** shall require each user to be successfully authenticated before allowing any other ***IT Environment***-mediated actions ***and SAFE mediated*** actions on behalf of that user.

5.2.2.3 FIA_UID_EXP.2-2 User identification before any action (SAFE)

FIA_UID_EXP.2.1-2 Refinement: The ***IT Environment*** shall require each user to identify itself before allowing any other ***IT Environment***-mediated actions ***and SAFE mediated*** actions on behalf of that user.

5.2.3 Class FPT: Protection of the TOE Security Functions

5.2.3.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 Refinement: The ***IT Environment*** shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE.

Application Note: FPT_ITT.1 ensures the connection between TOE Components is secure:

1. *connection between the Management Console and*
2. *Server and the Server and Sensors .*

5.2.3.2 FPT_RVM_EXP.1-2 Non-bypassability of the TSP (Enterprise and SAFE)

FPT_RVM_EXP.1.1-2 The security functions of the IT environment shall ensure that IT environment security policy enforcement functions are invoked and succeed before each function within the scope of control of the IT environment is allowed to proceed.

5.2.3.3 FPT_SEP_EXP.1-2 TSF domain separation (Enterprise and SAFE)

FPT_SEP_EXP.1.1-2 The security functions of the IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope and control of the IT environment.

FPT_SEP_EXP.1.2-2 The security functions of the IT environment shall enforce separation between the security domains of subjects in the scope of control of the IT environment.

5.2.3.4 FPT_STM.1 Reliable time stamps (Enterprise and SAFE)

FPT_STM.1.1 Refinement: The ***IT Environment*** shall be able to provide reliable time stamps for its own use.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-7.

Table 5-8 EAL2 Assurance Components

Item	Component	Component Title
1.	ACM_CAP.2	Configuration items
2.	ADO_DEL.1	Delivery procedures
3.	ADO_IGS.1	Installation, generation, and start-up procedures
4.	ADV_FSP.1	Informal functional specification
5.	ADV_HLD.1	Descriptive high-level design
6.	ADV_RCR.1	Informal correspondence demonstration
7.	AGD_ADM.1	Administrator guidance
8.	AGD_USR.1	User guidance
9.	ATE_COV.1	Evidence of coverage
10.	ATE_FUN.1	Functional testing
11.	ATE_IND.2	Independent testing – sample
12.	AVA_SOF.1	Strength of TOE security function evaluation
13.	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

Section 6 describes the specific security functions that meet the criteria of the security class features that are described in section 2.5. The following sections describe the IT Security Functions of SpectraGuard Enterprise server and SAFE. These interfaces provide the security functions which satisfy the TOE security functional requirements. This section includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met.

Table 6-1 Security Functional Requirements mapped to Security Functions

Security Class	SFR Item	SFRs	Security Functions
Security audit	1	FAU_GEN.1*	SA-1
	2	FAU_SAR.1	SA-2
	3	FAU_SAR_EXP.2	SA-3
	4	FAU_SAR_EXP.3*	SA-4
	5	FAU_SEL_EXP.1	SA-5
	6	FAU_STG_EXP.1-1	SA-6
Information Flow Control	7	FDP_NPT_EXP.1	IF-1
	8	FDP_CPT_EXP.1	
Identification and authentication	9	FIA_ATD_EXP.1-1	IA-1
	10	FIA_UAU_EXP.2-1	IA-2
	11	FIA_UID_EXP.2-1	IA-3
Security management	12	FMT_MOF.1*	SM-1
	13	FMT_MTD.1*	SM-2
	14	FMT_SMF.1	SM-3
	15	FMT_SMR_EXP.1	SM-4
Protection of the TSF	16	FPT_RVM_EXP.1-1	TP-1
	17	FPT_SEP_EXP.1-1	TP-2

6.1.2 Security Audit

SA-1 Audit events (FAU_GEN.1*)

FAU_GEN.1* describes the auditing capabilities of SpectraGuard Enterprise and SAFE . Both the TOE components collect audit data and provide an interface for authorized administrators to review generated audit records.

Enterprise server and SAFE generate records for two separate classes of events:

- Authentication/access to the TOE, actions taken directly on the TOE and
- The events monitored by the TOE.

All audit records include the date/time of the event, the identity associated with the event (such as the attributes of the access point/client or user), the success/failure of the event and a description of the event.

For audit events resulting from actions of identified users, the TOE shall be able to associate each auditable event with the identity of the user that caused the event. For each audit event type, additional information on audit record contents is specified in Tables 5-2 and 5-3 (Audit Events).

Authentication/access to the TOE, actions taken directly on the TOE and the start and stop of the audit service are noted in the audit log. The audit logs are stored on the TOE for the Enterprise server. All Enterprise Server log information is stored in a file format that is accessible only by the TOE components. SAFE relies on the underlying OS for storage of audit logs.

SA-2 Audit review (FAU_SAR.1)

From the SpectraGuard Enterprise and SAFE Administrative Interfaces, an authorized administrator[5] can read the audit data generated by the collection of events monitored by the TOE components. "All audit data" encompasses the system audit and event audit data. System audit data includes events associated with monitoring the TOE itself. Event audit data is the event audit data that is gathered from monitoring the wireless network. The audit records are provided in tabularized text suitable for the user to interpret the information.

Additionally, SpectraGuard Enterprise provides a capability for authorized administrators to review the event audit data of SpectraGuard SAFE Clients registered with the SpectraGuard Enterprise Server through the SGE Server's Management Console.

SA-3 Restricted audit review (FAU_SAR_EXP.2)

The TSF prohibits all users read access to the audit records, except those users that have been granted explicit read-access. Unauthorized users are not able to read the audit records in the audit trail.

From the Enterprise Server component's Management Console, an authorized administrator can read the event audit data generated by the Enterprise Server and SAFE components. The system audit and event audit data records are provided in tabularized text suitable for the user to interpret the information.

SA-4 Selectable audit review (FAU_SAR_EXP.3*)

SpectraGuard Enterprise provides a capability for authorized administrators to sort and search event audit data by Severity of an event, Event status, Event location, Event description, Event Category, Event type within a category, and Range of date and time. SpectraGuard Enterprise also enables

[5] The Authorized Administrator role includes all of the administrative roles defined in the product - from a security perspective.

authorized administrators to search events for specific text, helping to locate the target text within large amount of data. [FAU_SAR_EXP.3-1]

SpectraGuard SAFE Enterprise Edition enables an authorized user to sort and search for any string in the columns provided in the drop-down menu of the Administrative Interface namely—Event Type, Security Profile, Event Summary and Event Duration. [FAU_SAR_EXP.3-2] In this case the authorized user is identified and authenticated by the Operating System.

Enterprise Server allows for searching and sorting of the event audit data within the Management Console. Enterprise Server relies on the Operating System for viewing the system audit data which is downloaded and saved as a text file on the machine that is accessing the Enterprise Appliance via a Management Console. An authorized administrator can view the audit log files with a text editor.

SA-5 Selective audit (FAU_SEL_EXP.1)

SpectraGuard Enterprise provides a capability for authorized administrators to include or exclude generation of auditable events related to event audit data of a selected type from the events screen of the administrative Interface.

SA-6 Protected Audit Trail Storage (FAU_STG_EXP.1-1)

SpectraGuard Enterprise protects the stored audit records on the TOE from unauthorised deletion and modifications via the TSFI.

SpectraGuard Enterprise retains log files of system activities (system audit data). Log files are restricted by size. When the maximum allowed size of a log file is reached, the log file is rotated and the next log file is selected.

SAFE partially relies on the underlying operating system of the client on which it is installed for protection of audit trail data. SAFE stores the events in a database (MDB) in a file. The file is password protected and the password is internally known only to the SAFE application and is not revealed to users. This password prevents users from directly reading or altering the event data.

6.1.3 Information Flow Control

IF-1 Network Protection Policy for SpectraGuard Enterprise and Client Protection Policy for SAFE (FDP_NPT_EXP.1, FDP_CPT_EXP.1)

Formatted: English (U.S.)

Network Protection Policy for SpectraGuard Enterprise :

Access Point Classification:

SpectraGuard Enterprise automatically assigns the default 802.11 policy to all the newly detected wired network segments (subnets). Default security policy is overriden by setting a specific 802.11 security policy for each subnet.

SpectraGuard Enterprise compares all newly discovered APs that are connected to a subnet against the 802.11 security policy (Status, SSID, Vendor, Encryption, and Protocol—for that network segment). Based on this comparison, SpectraGuard Enterprise automatically assigns a suggested classification to each AP and places it in the **Uncategorized AP** list.

New access points appear in four categories in the **Uncategorized AP list**:

- **Potentially Authorized APs**: New APs that are connected to the network and conform to the **Network Policy** settings.
- **Potentially Rogue APs**: New APs that are connected to the network but do ***not*** conform to the Network Policy.
- **Potentially External APs**: New APs that are ***not*** connected to the network i.e APs that belong to a neighbor and do not pose a threat to the protected wired network.

- **Indeterminate APs**: APs for which SpectraGuard Enterprise cannot determine whether they are connected to the network.

Uncategorized AP's are classified into Authorized APs, Rogue APs and External APs either manually or automatically based on the AP classification policy. Automatic movement is enabled only for movement of:

- Potentially External APs to the External AP folder
- Potentially Rogue APs to the Rogue AP folder

Client Classification:

SpectraGuard Enterprise categorizes Clients as follows:

- Authorized: If the Client is permitted to connect to an Authorized AP
- Unauthorized: If the Client is not permitted to connect to an Authorized AP

The Client Classification Policy determines how Clients are classified upon initial discovery and subsequent AP associations.

Newly discovered clients can be classified as authorized/unauthorized if the MAC address of the clients exists in the list of authorized clients/banned client respectively.

Under Initial Client Classification, an authorized administrator can specify if newly discovered Clients, which are Uncategorized by default should be classified as Authorized or Unauthorized.

Under Automatic Client Classification, an authorized administrator can select one or more options to enable SpectraGuard Enterprise to automatically re-classify uncategorized or unauthorized Clients based on their associations with APs.

Intrusion Prevention:

The Intrusion Prevention Policy determines the wireless threats against which SpectraGuard Enterprise protects the network automatically. SpectraGuard Enterprise automatically moves such threat-posing APs and Clients to quarantine. SpectraGuard Enterprise can protect against multiple threats simultaneously. The connection to the WLAN for unauthorized AP's and Clients is denied by broadcasting DEAUTHENTICATE packets.

Client Protection Policy for SAFE :

Formatted: English (U.S.)

A Wireless Security Profile defines the blocking policy to prohibit unwanted wireless activities. Three security policies are provided—Work, Away, and Home. An authorized administrator can set the profile based on the environment in which the computer is operating. The active security policy determines the blocking policy.

Information flow between an authorized client and an access point is allowed provided, the presumed MAC address and SSID of the access point are specified in the wireless security policy of the SAFE as an allowed access point.

6.1.4 Identification and Authentication

IA-1 User Attribute Definition (FIA_ATD_EXP.1-1)

The SpectraGuard Enterprise maintains the following user security attributes for administrators:

- Login ID
- Password

SpectraGuard Enterprise server maintains the user role in addition to the above described attributes.

The user security attributes for SpectraGuard SAFE Enterprise Edition are maintained by the IT environment.

IA-2 User authentication before any action (FIA_UAU_EXP.2-1)

The SpectraGuard Enterprise requires each user to successfully authenticate with a password before being allowed any other actions. SpectraGuard SAFE Enterprise Edition relies on the underlying OS for authentication.

IA-3 User identification before any action (FIA_UID_EXP.2-1)

The SpectraGuard Enterprise Server requires each user to self identify before being allowed to perform any other actions. SpectraGuard SAFE Enterprise Edition relies on the underlying OS for identification.

6.1.5 Security management

SM-1 Management of security functions behaviour (FMT_MOF.1*)

Each of the TOE components provides an administrator with the ability to manage the security functions through a web interface.

The SpectraGuard server enables the authorized administrator to determine and modify the behavior of audit, information flow security rules, and identification and authentication functions. The Management Console is used to enable the authorized administrator to determine and modify the behavior of audit and information flow security rules functions of the SAFE Enterprise Edition client.

SM-2 Management of TSF Data (FMT_MTD.1*)

The SpectraGuard Enterprise restricts the ability to perform operations as specified in Table 5-4 by restricting the ability to manage all TSF data to the Authorized Administrator. [FMT_MTD.1-1]

SpectraGuard SAFE Enterprise Edition is managed via the Management Console. The end user is able to view the specified events and TSF data as specified in Table 5-5. [FMT_MTD.1-2]

SM-3 Specification of Management Functions (FMT_SMF.1)

The TOE is capable of performing the following security management functions:

- determine the behaviour of and modify the behaviour of the functions specified in sections 5.1.4.1 (see FMT_MOF.1*),
- query, modify, delete, and other operations as specified in Table 5-3 on the TSF Data as specified in Tables 5-4 and 5-5 (See FMT_MTD.1*)
- ***End users are able to view the settings of SAFE via the SAFE Console on the client laptop (See Table 5-5)***].

SM-4 Security Roles (FMT_SMR_EXP.1)

According to the ST, the TOE supports one security role: Authorized Administrator

The Authorized Administrator role has the ability to enable, disable, or modify the behavior of all security functions. The TOE maintains this role and supports associating users to this role

SpectraGuard Enterprise within the Console maintains the following roles that are all considered authorized administrators for the purpose of this security target:

- Superuser

- Administrator
- Operator
- Viewer

The user roles and their respective rights on the SGE server are as follows:[6]

User Roles				User Rights
Superuser	Administrator	Operator	Viewer	
✔	✘	✘	✘	Add, delete, modify and manage SpectraGuard Enterprise users
✔	✔	✘	✘	Modify all screens on the Administration tab (excluding User Management screens)
✔	✔	✔	✘	Modify and delete events
✔	✔	✔	✘	Add, delete and modify devices(APs and Clients)
✔	✔	✔	✘	Add, delete and modify locations
✔	✔	✔	✘	Calibrate location tracking
✔	✔	✔	✘	Add, delete, modify and schedule reports
✔	✔	✔	✘	Move devices in and out of quarantine
✔	✔	✔	✘	Troubleshoot devices
✔	✔	✔	✔	View all product screens (excluding User Management screens)

6.1.6 TSF Self-Protection

TP-1 Non-bypassability (FPT_RVM_EXP.1-1)

Formatted: French (France)

The TOE prevents bypassing of the TSF by requiring that all actions be bound to a set of authentication credentials. This ensures that a user must first authenticate successfully to the TOE before access to the management interface is granted.

SpectraGuard Enterprise provides this funtionality by itself but SpectraGuard SAFE Enterprise Edition relies on the underlying OS also to provide non-bypassability.

In addition, the TOE provides non-bypassability by the enforcement of the network protection policy.

TP-2 TSF domain separation (FPT_SEP_EXP.1-1)

SpectraGuard Enterprise maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

SpectraGuard SAFE Enterprise Edition relies on the IT environment to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

6.2 SOF Claims

The threat level for the TOE authentication function is assumed to be SOF-basic. This defines a level of authentication strength of function where analysis shows that the function provides basic protection against straightforward or intentional breach of TOE security by attackers possessing a minimum attack potential.

[6] [User Guide] Section 9.9

IA-2 User authentication before any action, is realized by probabilistic or permutational mechanisms. The methods used to provide difficult-to-guess passwords are probabilistic. The specific password policy is specified in the [CC Supp] as the following:

- Minimum length of 8 characters,
- At least 1 lower case letter,
- At least 1 upper case letter,
- At least 1 number,
- Password must not contain the login ID,
- Password must not contain any spaces,

These password quality metrics are configured by the Administrator of the TOE.

The SOF claim for IA-2 is SOF-basic.

6.3 Assurance Measures

The TOE satisfies CC EAL2 assurance requirements. Table 6-2 identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by AirTight Networks to satisfy the CC EAL2 assurance requirements.

Table 6-2 - Security Assurance Measures

Assurance Component	How requirement will be met	Document Version
ACM_CAP.2 Configuration items	The vendor provided configuration management documents and a Configuration Item list.	[CM]
ADO_DEL.1 Delivery procedures	The vendor provided delivery procedures.	[DEL]
ADO_IGS.1 Installation, generation and startup procedures	The vendor provided secure installation, generation and start up procedures.	[E Install] [E Quick Setup]
ADV_FSP.1 Informal functional specification	The vendor provided informal function specification.	[FSP]
ADV_HLD.1 Descriptive high-level design	The vendor provided descriptive high-level design document.	[FSP]
ADV_RCR.1 Informal correspondence demonstration	The informal correspondence demonstration provided in the design documentation. ST to FSP in the FSP, FSP to HLD in the HLD.	[FSP]
AGD_ADM.1 Administrator Guidance	The vendor submitted system administration manual.	[CC Admin] [CC Supp]

Assurance Component	How requirement will be met	Document Version
AGD_USR.1 User Guidance	The vendor submitted user guide.	[E User Guide] [CC Supp] [Web Help] [SAFE User Guide]
ATE_COV.1 Evidence of coverage	The analysis of test coverage submitted in the evaluation evidence.	[TP Dev]
ATE_FUN.1 Functional testing	The test evidence submitted to the CCTL.	[TP Dev]
ATE_IND.2 Independent testing - sample	The laboratory used development evidence submitted by the vendor along with functional testing evidence as a baseline for an independent test plan.	[TP CYG]
AVA_SOF.1 Strength of TOE security function evaluation	The vendor submitted analysis of the SOF for the password.	[SOF]
AVA_VLA.1 Developer vulnerability analysis	The vendor submitted vulnerability analysis. The laboratory conducted an independent vulnerability assessment by building on the vendor's. The laboratory conducted penetration testing.	[VA]

7 PP Claims

This ST was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Assumptions

Table 8-1 shows that all of the assumptions are addressed by Non-IT security objectives. Rationale is provided for each Assumption in the table.

Table 8-1 All Assumptions Addressed

Assumption ID	Non-IT Objective Addressing Assumption	Rationale
A.Access	ON.Access	This objective provides for secure communication between the User Consoles (GUI and CLI) and the TOE
A.AuditBackup	ON.AuditBackup	This objective provides for the backing up of audit files and makes sure that disk usage is monitored.
A.Admin	ON.Install	This objective provides for secure installation and configuration of the TOE.
	ON.Operations	This objective provides for operation procedures to be in place.
A.Manage	ON.Person	This objective provides for competent personnel to administer the TOE.
A.NoUntrusted	ON.NoUntrusted	This objective provides for the protection of the TOE from untrusted software and users.
A.Physical	ON.Physical	This objective provides for the physical protection of the TOE
A.ProtectComm	ON.ProtectComm	This objective provides for secure communication between the TOE components
A.Users	ON.ProtectAuth	This objective provides for users protecting their authentication data.

8.1.2 Threats to Security

Table 8-2 shows that all the identified threats to security are countered by Security Objectives for the TOE and IT Environment. Rationale is provided for each threat in the table.

Table 8-2 All Threats to Security Countered

Item	Threat ID	Security Objective Addressing the Threat	Rationale
1	T.Adhoc	O.IFlow-Enterprise	This objective counters this threat by detecting and taking action against attempts by unauthorized users, unauthorized access points or unauthorized clients to bypass, deactivate, or tamper with the information flow policy ,defined for the TOE by an authorized administrator, to gain access to the protected network
2	T.AuditCompromise	O.AuditProtection	O.AuditProtection contributes to mitigating this threat by controlling access to the individual audit log records. No one is allowed to modify audit records, the Administrator is the only one allowed to delete audit records.
		OE.AuditProtection	OE.AuditProtection counters this threat by restricting the ability of users in the IT Environment to access the audit log file.
3	T.AuthClient	O.IFlow-Enterprise	This objective counters this threat by detecting and taking action against attempts by authorized clients to bypass, deactivate, or tamper with the information flow policy ,defined for the TOE by an authorized administrator, to gain access to external or rogue APs
4	T.Bypass	O.NonBypass	This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable. This is supported by OE.NonBypass
		OE.NonBypass	This objective supports countering this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that IT environment security functions not be bypassable

Item	Threat ID	Security Objective Addressing the Threat	Rationale
5	T.MaliciousTSFCompromise	O.PartialSelfProtection	O.PartialSelfProtection is necessary so that the TSF protects itself and its resources from inappropriate access through its own interfaces.
		OE.PartialSelfProtection	OE.PartialSelfProtection is necessary so that the TSF is protected from other processes executing on the workstation used to access the TOE or the clients.
		O.Admin	This objective also contributes to mitigating this threat by providing management tools to make it easier for administrators to manage the TOE security functions. More specifically, providing administrators the capability to view and edit configuration settings through a GUI.
		OE.ProtectData	OE.ProtectData contributes to mitigating this threat by the IT Environment providing an SSH protected connection between the Management Console and Server. In addition, this objective ensures a protected connection between the Server and Sensors.
6	T.Masquerade	O.IDAuth	This objective mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how authorized administrators and workstation users can access the TOE, and by mandating the type and strength of the authentication mechanisms, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective allows the TOE to correctly interpret information used during the authentication process so that it can make the correct decisions when identifying and authenticating users.
		OE.IDAuth	This objective provides for authentication of users prior to any TOE data access on the client machines.

Item	Threat ID	Security Objective Addressing the Threat	Rationale
7	T.MisconfiguredAP	O.IFlow-Enterprise	This objective counters this threat by detectingproviding that the SpectraGuard Enterprise will detect and takingtake action against attempts by unauthorized users, unauthorized access points or unauthorized clients to bypass, deactivate, or tamper with the information flow policy ,, defined for the TOE by an authorized administrator, to gain access to the protected network.
		IFlow-SAFE	This objective counter this treat by providing that the SpectraGuard SAFE Enterprise Edition will detect and take actions against attempts by unauthorized access points to bypass, deactivate, or tamper with the security policy defined for the TOE by an authorized administrator, to gain access to the protected network.
		O.Admin	This objective also contributes to mitigating this threat by providing management tools to make it easier for administrators to manage the TOE security functions. More specifically, providing administrators the capability to view and edit configuration settings through a GUI.
8	T.Mismanage	O.Admin	This objective also contributes to mitigating this threat by providing management tools to make it easier for administrators to manage the TOE security functions. More specifically, providing administrators the capability to view and edit configuration settings through a GUI.
9	T.RogueAP	O.IFlow-Enterprise	This objective counters this threat by providing that the SpectraGuard Enterprise will detect and take action against attempts by unauthorized users, unauthorized access points or unauthorized clients to bypass, deactivate, or tamper with the information flow policy, defined for the TOE by an authorized administrator, to gain access to the protected network.
		O.IFlow-SAFE	This objective counter this treat by providing that the SpectraGuard SAFE Enterprise Edition will detect and take actions against attempts by unauthorized access points to bypass, deactivate, or tamper with the security policy defined for the TOE by an authorized administrator, to gain access to the protected network.
10	T.UnAuthorizedAssociation	O.IFlow-Enterprise	This objective counters this threat by detecting and taking action against attempts by unauthorized users, unauthorized access points or unauthorized clients to bypass, deactivate, or tamper with the information flow policy ,defined for the TOE by an authorized administrator, to gain access to the protected network
11	T.UnidentifiedActions	O.Audit	This objective helps to mitigate this threat by recording actions for later review

Item	Threat ID	Security Objective Addressing the Threat	Rationale
		O.AuditReview	This objective helps to mitigate this threat by providing the Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events (e.g. failed logins, self-test failures, etc.).
		OE.Time	OE.Time helps to mitigate this threat by ensuring that audit records have correct timestamps.

Table 8-3 Reverse Mapping of Security Objectives for the TOE to Threats

Note: This table is provided to show completeness by demonstrating all security objectives for the TOE map to at least one threat

Item	TOE Objective	Threat/Policy
1	O.Admin	T.Mismanage, T.MaliciousTSFCompromise T.MisconfiguredAP
2	O.Audit	T.UnidentifiedActions
3	O.AuditProtection	T.AuditCompromise
4	O.AuditReview	T.UnidentifiedActions
5	O.IFlow-Enterprise	T.Adhoc, T.AuthClient, T.MisconfiguredAP, T.RogueAP, T.UnAuthorizedAssociation
6	O.IFlow-SAFE	T.RogueAP T.MisconfiguredAP
7	O.IDAuth	T.Bypass
8	O.NonBypass	T.Bypass
9	O.PartialSelfProtection	T.MaliciousTSFCompromise

Table 8-4 Reverse Mapping of Security Objectives for the Environment to Assumptions/Threats

Note: This table is provided to show completeness by demonstrating all security objectives for the environment map to at least one assumption, threat, or policy.

Item	Security Objective for Environment	Assumption/Threat/Policy
9	OE.AuditProtection	T.AuditCompromise
10	OE.IDAuth	T.Masquerade
11	OE.NonBypass	T.Bypass
12	OE.PartialSelfProtection	T.MaliciousTSFCompromise
13	OE.ProtectData	T.MaliciousTSFCompromise
14	OE.Time	T.UnidentifiedActions

Item	Security Objective for Environment	Assumption/Threat/Policy
1E	ON. Access	A.Access
2E	ON.AuditBackup	A.AuditBackup
3E	ON.Install	A.Admin
4E	ON.NoUntrusted	A.NoUntrusted
5E	ON.Operations	A.Admin
		A.NoUntrusted
6E	ON.Person	A.Manage
7E	ON.Physical	A.Physical
8E	ON.ProtectAuth	A.Users
9E	ON.ProtectComm	A.ProtectComm

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements for the TOE

Table 8-6 shows that all of the security objectives of the TOE are satisfied. Rationale for each objective is included in the below table.

Table 8-5 All Objectives Met by Functional Requirements

Objective	SFR ID	SFR Title	Rationale
O.Audit	FAU_GEN.1*	Audit data generation	FAU_GEN.1* define the set of events that the TOE must be capable of recording. This requirement ensures that an 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.
	FAU_SEL_EXP.1	Selective audit	Selective audit, requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events
O.Admin	FAU_SAR.1	Audit review	Audit review (TOE), ensures that an authorized administrator will be able to read all audit records within the administrator's scope of control.
	FAU_SAR_EXP.2	Restricted audit review	Restricted audit review (TOE), requires that access to audit data be restricted to authorized users.
	FAU_SEL_EXP.1	Selective audit	Selective audit, requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events
	FMT_MOF.1*	Management of security functions behaviour	The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirement's rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions
	FMT_MTD.1*	Management of TSF data	FMT_MTD.1 specifies the management of TSF Data according to assigned roles.
	FMT_SMF.1	Specification of management functions	FMT_SMF.1 requires the TSF be capable of performing the specified security management functions.

Objective	SFR ID	SFR Title	Rationale
	FMT_SMR_EXP.1	Security roles	FMT_SMR_EXP.1 requires that the TSF maintain user roles. The TSF is able to associate a human user with one or more roles and these roles isolate administrative functions in that the functions of these roles do not overlap. If a security administrator were to perform a malicious action, the auditing requirements afford some measure of detectability of the rogue administrator's actions.
O.AuditReview	FAU_SAR.1	Audit review	Audit review (TOE), ensures that an authorized administrator will be able to read all audit records within the administrator's scope of control.
	FAU_SAR_EXP.2	Restricted audit review	Restricted audit review (TOE), requires that access to audit data be restricted to authorized users.
	FAU_SAR_EXP.3	Selectable audit review	Selectable audit review (TOE), defines that the administrator can perform searches and sorting of the audit data based on various criteria as listed in the SFR.
O.AuditProtection	FAU_SAR_EXP.2	Restricted audit review	Restricted audit review (TOE), requires that access to audit data be restricted to authorized users.
	FAU_STG_EXP.1-1	Protected audit trail storage	The FAU_STG family dictates how the audit trail is protected. The TOE restricts the ability to delete audit records to the authorized Administrator. FAU_STG_EXP.1-1 defines the actions that must be available to the administrator. This helps to ensure that audit records are kept until the Administrator deems they are no longer necessary. This requirement also ensures that no one has the ability to modify audit records (e.g., edit any of the information contained in an audit record). This ensures the integrity of the audit trail is maintained.
O.IFlow-Enterprise	FDP_NPT_EXP.1*	Network Protection Policy	This requirement ensures that the SpectraGuard Enterprise has the ability to monitor the protected network and take action against attempts by unauthorized users, unauthorized access points or unauthorized clients to bypass, deactivate, or tamper with the network protection policy defined for SpectraGuard Enterprise by an authorized administrator.

Objective	SFR ID	SFR Title	Rationale
O.IFlow-SAFE	FDP_CPT_EXP.1	Client Protection Policy	This requirement ensures that the SAFE has the capability to detect and take action against attempts by authorized clients to bypass, deactivate, or tamper with the client protection policy ,defined for the TOE by an authorized administrator, to gain access to external or rogue APs
O.IDAuth	FIA_ATD_EXP.1-1	User attribute definition	User attribute definition, which requires that the TSF maintain security attributes of user.
	FIA_UAU_EXP.2-1	User authentication before any action	User authentication before any action; requires each user to be successfully authenticated before allowing access to the TOE.
	FIA_UID_EXP.2-1	User identification before any action	User identification before any action; requires that users be successfully identified before allowing access to the TOE
O.NonBypass	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	Non-bypassability of the TSP, which requires that the TSF ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
O.PartialSelfProtection	FPT_SEP_EXP.1-1	TSF domain separation	TSF domain separation; requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by untrusted users. The TSF must enforce separation between security domains of subjects in the TSC.

Table 8-6 Reverse mapping of TOE SFRs to TOE Security Objectives

Note: This table has been provided for completeness to show that all security functional requirements map to at least one TOE Security Objective.

Item	SFR ID	TOE Security Objective
1	FAU_GEN.1*	O.Audit
2	FAU_SAR.1	O.Admin, O.AuditReview
3	FAU_SAR_EXP.2	O.Admin, O.AuditProtection, O.AuditReview
4	FAU_SAR_EXP.3	O.AuditReview
5	FAU_SEL_EXP.1	O.Admin,O.Audit
6	FAU_STG_EXP.1-1	O.AuditProtection
8	FDP_NPT_EXP.1	O.IFlow-Enterprise
9	FDP_CPT_EXP.1	O.IFlow-SAFE
10	FIA_ATD_EXP.1-1	O.IDAuth
11	FIA_UAU_EXP.2-1	O.IDAuth

Item	SFR ID	TOE Security Objective
12	FIA_UID_EXP.2-1	O.IDAuth
13	FMT_MOF.1*	O.Admin
14	FMT_MTD.1*	O.Admin
15	FMT_SMF.1	O.Admin
16	FMT_SMR_EXP.1	O.Admin
17	FPT_RVM_EXP.1-1	O.NonBypass
18	FPT_SEP_EXP.1-1	O.PartialSelfProtection

8.2.2 Dependencies

The table below shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical components are denoted by an (H) following the dependency reference. (E) designates that the SFR is for the IT Environment.

Table 8-7 TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1*	Audit data generation	FPT_STM.1	6(E)
2	FAU_SAR.1	Audit review	FAU_GEN.1*	1
3	FAU_SAR_EXP.2	Restricted audit review	FAU_SAR.1	2
4	FAU_SAR_EXP.3	Selectable audit review	FAU_SAR.1	2
5	FAU_SEL_EXP.1	Selective Audit	FAU_GEN.1*, FMT_MTD.1	1 13
6	FAU_STG_EXP.1-1	Protected audit trail storage	FAU_GEN.1	1
8	FDP_NPT_EXP.1	Network Protection Policy	No dependencies	N/A
9	FDP_CPT_EXP.1	Client Protection Policy	No dependencies	N/A
10	FIA_ATD_EXP.1-1	User attribute definition	No dependencies	N/A
11	FIA_UAU_EXP.2-1	User authentication before any action	FIA_UID.1	11(H)
12	FIA_UID_EXP.2-1	User identification before any action	No dependencies	N/A
13	FMT_MOF.1*	Management of security functions behaviour	FMT_SMF.1 FMT_SMR_EXP.1	14 15
14	FMT_MTD.1*	Management of TSF data	FMT_SMF.1 FMT_SMR_EXP.1	14 15
15	FMT_SMF.1	Specification of management functions	No dependencies	N/A
16	FMT_SMR_EXP.1	Security roles	FIA_UID.1	11(H)
17	FPT_RVM_EXP.1-1	Nonbypassability of the TSP	No dependencies	N/A
18	FPT_SEP_EXP.1-1	TSF domain separation	No dependencies	N/A

Table 8-8 IT Environment Dependencies are Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1E	FAU_STG_EXP.1	Protected audit trail storage	FAU_GEN.1	1
2E	FIA_ATD_EXP.1-2	User attribute definition	No dependencies	N/A
3E	FIA_UAU_EXP.2-2	User authentication before any action	FIA_UID.1	3E(H)
4E	FIA_UID_EXP.2-2	User identification before any action	No dependencies	N/A
5E	FPT_ITT.1	Basic internal TSF data transfer protection	No dependencies	N/A
6E	FPT_RVM_EXP.1-2	Nonbypassability of the TSP	No dependencies	N/A
7E	FPT_SEP_EXP.1-2	TSF domain separation	No dependencies	N/A
8E	FPT_STM.1	Reliable time stamps	No dependencies	N/A

8.2.3 Strength of Function Rationale

A strength of function level of SOF-basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product. As stated in section 6.1.7, there is one security function based on probabilistic methods, IA-2. See section 5.3.4 for the objective that SOF supports. The specific "strength" required of the methods used to provide difficult-to-guess passwords are defined administratively in the CC Supplement document

8.2.4 Evaluation Assurance Level Rationale

Evaluation Assurance Level EAL2 was chosen to provide a moderate level of assurance due to the low level threat of malicious attacks.

8.2.5 Explicitly Stated Requirements Rationale

FPT_RVM_EXP.1 and FPT_SEP_EXP.1 had to be explicitly stated because they provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. According to CCIMB RI#19, which states the following: "Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. Since the iterations of FPT_RVM_EXP.1 and FPT_SEP_EXP.1 span both the TOE requirements and IT Environment, they must be explicitly stated. FAU_STG_EXP.1-1 had to be explicitly stated as SAFE does not satisfy the requirement without the support from the IT environment. FIA_ATD_EXP.1 had to be explicitly stated since SAFE relies on the IT Environment to maintain the user security attributes. FAU_SAR_EXP.2 and FAU_SAR_EXP.3.1 had to be explicitly stated because the Enterprise Server allows for the system audit data log file to be downloaded as a text file to the Administrator's local machine. Once the file is downloaded it is protected by the Operating System's identification and authentication and file access rights. As a result, the system audit data log files can be viewed with a text editor. Searching and sorting of the event audit data is allowed only within the Management Console. FAU_SEL_EXP.1 had to be explicitly stated because including and excluding auditable events from the set of audited events is only provided for event audit data within the Management Console. FDP_NPT_EXP.1 and FDP_CPT_EXP.1 have been explicitly stated to specify

information flow control policies for wireless networks and to describe the TOE's actual behavior as verifiable assertions. FMT_SMR_EXP.1 had to be explicitly stated because SAFE does not maintain user roles. FIA_UAU_EXP.2 and FIA_UID_EXP.2 had to be explicitly stated because SAFE relies on the OS for identification and authentication.

8.2.6 Security Functional Requirements for the IT Environment

Table 8-10 shows that all of the security objectives for the IT environment are satisfied. Rationale for each objective is included in the below table.

Table 8-9 All Objectives for the IT Environment map to Requirements in the IT environment

Objective	SFR ID	SFR Title	Rationale
OE.AuditProtection	FAU_STG_EXP.1	Protected audit trail storage	FAU_STG_EXP.1 requires the Operating System to protect the audit log file from unauthorized deletion
OE.IDAuth	FIA_ATD_EXP.1-2	User attribute definition	FIA_ATD_EXP.1-2 requires the Operating System to store user attribute definitions.
	FIA_UAU_EXP.2-2	User authentication before any action	FIA_UAU_EXP.2 requires that a user be authenticated by the TOE before accessing the TOE.
	FIA_UID_EXP.2-2	User identification before any action	FIA_UID_EXP.2 requires that a user be identified to the TOE in order to access to the TOE.
OE.NonBypass	FPT_RVM_EXP.1-2	Non-bypassability of the TSP	FPT_RVM_EXP.1-2 defined that the IT environment will support the TOE's non-bypassability functions
OE.PartialSelfProtection	FPT_SEP_EXP.1-2	TSF domain separation	FPT_SEP_EXP.1-2 requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment must enforce separation between security domains of subjects in the Operating System's Scope of Control.
OE.ProtectData	FPT_ITT.1	Basic internal TSF data transfer protection	FPT_ITT.1 requires the IT Environment to protect TSF data when it is being transferred between separate TOE Components.
OE.Time	FPT_STM.1	Reliable time stamps	FPT_STM.1 requires that time stamps be provided by the IT environment.

Table 8-10 Reverse Mapping of Environment SFRs to Environment Security Objectives

Note: This table has been provided for completeness to show that all security functional requirements for the IT Environment map to at least one Security Objective for the IT Environment.

Environment SFR ID	Environment Security Objectives
FAU_STG_EXP.1-2	OE.AuditProtection
FIA_ATD_EXP.1-2	OE.IDAuth
FIA_UAU_EXP.2-2	OE.IDAuth
FIA_UID_EXP.2-2	OE.IDAuth
FPT_ITT.1	OE.ProtectData
FPT_RVM_EXP.1-2	OE.NonBypass
FPT_SEP_EXP.1-2	OE.PartialSelfProtection
FPT_STM.1	OE.Time

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions Rationale

Table 8-12 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-11 Mapping of Functional Requirements to TOE Summary Specification

#	SFR ID	SFR Title	ITSF Ref No.	Rationale
1	FAU_GEN.1*	Audit data generation	SA-1	Specifies the types of events to be audited, and the information to be recorded in an audit record.
2	FAU_SAR.1	Audit review	SA-2	Specifies who has the capability to read information from the audit records.
3	FAU_SAR_EXP.2	Restricted audit review	SA-3	Specifies that only specific users have read access to the audit records.
4	FAU_SAR_EXP.3*	Selectable audit review	SA-4	Specifies audit selection features for SpectraGuard Enterprise, and SpectraGuard SAFE Enterprise Edition .
5	FAU_SEL_EXP.1	Selective audit	SA-5	Specifies audit events that can be included or excluded from the audit logs for SpectraGuard Enterprise
6	FAU_STG_EXP.1-1	Protected audit trail storage	SA-6	Specifies that the TOE protects the stored audit records from unauthorized deletion and modification via the management console for SpectraGuard Enterprise.
8	FDP_NPT_EXP.1	Network Protection Policy	IF-1	Specifies the Network protection policy for Enterprise Server
9	FDP_CPT_EXP.1	Client Protection Policy		Specifies the Client Protection Policy for SAFE

#	SFR ID	SFR Title	ITSF Ref No.	Rationale
10	FIA_ATD_EXP.1-1	User attribute definition	IA-1	Specifies the security attributes maintained for each user.
11	FIA_UAU_EXP.2-1	User authentication before any action	IA-2	Specifies that each user must be successfully authenticated with a password before being allowed any other actions.
12	FIA_UID_EXP.2-1	User identification before any action	IA-3	Specifies that each user must identify himself/herself before being allowed to perform any other actions.
13	FMT_MOF.1*	Management of security functions behaviour	SM-1	Specifies the functions which an authorized administrator for the TOE can determine the behavior and modify the behavior
14	FMT_MTD.1*	Management of TSF data	SM-2	Specifies that the TOE components restrict the ability to access TSF data to the Authorized Administrator.
15	FMT_SMF.1	Specification of management functions	SM-3	Specifies the security management functions to determine the behaviour of security functions, security attributes, and TSF data.
16	FMT_SMR_EXP.1	Security roles	SM-4	Specifies the roles maintained in SpectraGuard Enterprise and SpectraGuard SAFE Enterprise Edition.
17	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	TP-1	Specifies the TOE ensures that the SpectraGuard Information Flow Control SFP is invoked and succeeds before each function is allowed to proceed.
18	FPT_SEP_EXP.1-1	TSF domain separation	TP-2	Specifies that the TOE maintains a security domain for its own execution and enforces separation between security domains of users.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.