Security Target for Common Criteria Evaluation:

AirDefense Enterprise 7.2

February 8, 2008

Version 1.9

Document Reference: ST

Prepared For:

AirDefense, Inc.
4800 North Point Parkway
Suite 100
Alpharetta, GA 30022
www.airdefense.net

Prepared By:

Apex Assurance Group, LLC
5448 Apex Peakway Drive
Suite 101
Apex, NC 27502
www.apexassurance.com

Document Revision History

Revision	Date	Description
1.0	June 27, 2007	Rework 7.0 ST to reflect 7.2 and include SFRs from IDS PP
1.1	August 7, 2007	Address lab verdicts
1.2	August 29, 2007	Address additional comments
1.3	September 19, 2007	Address remaining ST-ETR comments
1.4	October 22, 2007	Address several issues with FSP-ETR and HLD-ETR
1.5	November 13, 2007	Address FIPS references per fVOR
1.6	December 27, 2007	Update description for IDS_ANL1.1
1.7	January 30, 2008	Minor Updates per fVOR
1.8	January 31, 2008	Minor modifications per SAIC's review
1.9	February 8, 2008	Add FMT_MTD.1c requirement

Table of Contents

1. SECURITY TARGET INTRODUCTION..6
1.1 Security Target Reference.. 6
1.2 TOE Reference.. 6
1.3 Evaluation Assurance Level.. 6
1.4 Keywords.. 6
1.5 TOE Overview.. 7
1.6 Security Target Organization.. 7
1.7 Common Criteria Conformance.. 7
1.8 Protection Profile Conformance.. 7
1.9 Conventions.. 8
1.10 Acronym List.. 8
2. TOE DESCRIPTION..10
2.1 AirDefense Enterprise 7.2.. 10
2.2 Physical Boundary.. 12
2.2.1 Hardware/Software Components.. 12
2.3 Logical Boundary.. 14
2.3.1 Security Audit.. 14
2.3.2 Identification and Authentication.. 14
2.3.3 Traffic Analysis.. 15
2.3.4 Security Management.. 15
2.3.5 Protection of Security Functions.. 15
2.4 Evaluated Configuration.. 16
3. SECURITY ENVIRONMENT..17
3.1 Introduction.. 17
3.2 Assumptions.. 17
3.3 Threats.. 17
3.4 Organizational Security Policies.. 18
4. SECURITY OBJECTIVES..19
4.1 Security Objectives for the TOE.. 19
4.2 Security Objectives for the IT Environment.. 19
4.3 Security Objectives for the Non-IT Environment.. 20
5. IT SECURITY REQUIREMENTS..21
5.1 TOE Security Functional Requirements.. 21
5.1.1 Security Audit (FAU).. 22
5.1.1.1 FAU_GEN.1 (EXP).. 22
5.1.1.2 FAU_SAR.1 Audit Review.. 22
5.1.1.3 FAU_SAR.2 Restricted Audit Review.. 22
5.1.1.4 FAU_SAR.3 Selectable Audit Review.. 22
5.1.1.5 FAU_STG.1 Protected Audit Trail Storage.. 23
5.1.1.6 FAU_STG.2 Guarantees of Audit Data Availability.. 23
5.1.2 Cryptographic Support (FCS).. 23

5.1.2.1 FCS_CKM.1 Cryptographic Key Generation 23
5.1.2.2 FCS_CKM.2 Cryptographic Key Distribution 23
5.1.2.3 FCS_CKM.4 Cryptographic Key Destruction 23
5.1.2.4 FCS_COP.1 Cryptographic Operation 23
5.1.3 Identification and Authentication (FIA) 24
5.1.3.1 FIA_ATD.1 User Attribute Definition 24
5.1.3.2 FIA_UAU.2 User Authentication before Any Action 24
5.1.3.3 FIA_UID.2 User Identification before Any Action 24
5.1.4 Security Management (FMT) 24
5.1.4.1 FMT_MOF.1 Management of Security Functions Behavior 24
5.1.4.2 FMT_MTD.1 Management of TSF Data 25
5.1.4.3 FMT_SMF.1 Specification of Management Functions 25
5.1.4.4 FMT_SMR.1 Security Roles 25
5.1.5 Protection of the TSF (FPT) 25
5.1.5.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection 25
5.1.5.2 FPT_RVM.1 Non-Bypassability of the TSP 26
5.1.5.3 FPT_SEP.1 TSF Domain Separation 26
5.1.5.4 FPT_STM.1 Reliable Time Stamps 26
5.1.6 IDS Component 26
5.1.6.1 IDS_ANL.1 Analysis (EXP) 26
5.1.6.2 IDS_RCT.1 React (EXP) 26
5.1.6.3 IDS_RDR.1 Restricted Data Review (EXP) 26
5.1.6.4 IDS_SDC.1 TOE Data Collection (EXP) 27
5.2 Strength of Function for the TOE 27
5.3 CC Component Hierarchies and Dependencies 28

6. TOE SUMMARY SPECIFICATION 30
6.1 Security Functions 30
6.1.1 Security Audit 30
6.1.2 Security Management 31
6.1.3 Identification and Authentication 32
6.1.4 Traffic Analysis 33
6.1.5 Protection of Security Functions 35
6.1.5.1 Cryptographic Support 36
6.2 TOE Security Assurance Requirements 37

7. PROTECTION PROFILE CLAIMS 38

8. RATIONALE 39
8.1 Rationale for IT Security Objectives 39
8.1.1 Rationale Showing Threats to Security Objectives 40
8.2 Security Requirements Rationale 42
8.2.1 Rationale for Security Functional Requirements of the TOE Objectives 42
8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives 45
8.2.3 Security Assurance Requirements Rationale 45
8.2.3.1 TOE Security Assurance Requirements Rationale 45
8.2.3.2 Rationale for TOE Assurance Requirements Selection 47

8.3 TOE Summary Specification Rationale.. 47
8.4 PP Claims Rationale 51
8.5 Rationale for Explicitly Stated Requirements... 51
8.6 Strength of Function Rationale.. 51

List of Tables

Figure 1 – AirDefense Enterprise Deployment..11

Figure 2 – TOE Physical Boundary...13

List of Figures

Figure 1 – AirDefense Enterprise Deployment..11

Figure 2 – TOE Physical Boundary...13

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Target of Evaluation, which is the AirDefense Enterprise 7.2 solution. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.1 Security Target Reference

Document Title:	Security Target for Common Criteria Evaluation: AirDefense Enterprise 7.2
Document Version:	1.9
Date of Release:	February 8, 2008

1.2 TOE Reference

The Target of Evaluation is the AirDefense Enterprise 7.2 wireless security solution for enterprise networks. The TOE is a combined hardware/software TOE and includes the following components:

- AirDefense 2270 Appliance
- AirDefense M510 and M520 Sensors
- AirDefense Enterprise 7.2

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.4 Keywords

The following keywords are applicable to the TOE: Wireless, Security.

1.5 TOE Overview

The AirDefense Enterprise 7.2 is a wireless IDS solution, designed to monitor the traffic received from any 802.11a/b/g source. By monitoring this traffic, the AirDefense Enterprise 7.2 system can detect identity theft attacks and violations of site-specific wireless security policies.

1.6 Security Target Organization

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organizational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the TOE to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.7 Common Criteria Conformance

The TOE is compliant with the Common Criteria (CC) Version 2.3, functional requirements (Part 2) extended and assurance requirements (Part 3) conformant for EAL2.

1.8 Protection Profile Conformance

The TOE does not claim conformance to any registered Protection Profile.

1.9 Conventions

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

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

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

1.10 Acronym List

ADE	AirDefense Enterprise
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CA	Certificate Authority
CAVP	Crytpographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
DEK	Data Encryption Key
DH	Diffie-Hellman
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
IT	Information Technology
KEK	Key Encryption Key
LAN	Local Area Network
NIAP	National Information Assurance Partnership
PP	Protection Profile
RFC	Request for Comment
SHA	Secure Hashing Algorithm
SHS	Secure Hashing Standard
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target

TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface
TSP	TOE Security Policy

2. TOE Description

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

2.1 AirDefense Enterprise 7.2

The AirDefense Enterprise 7.2 (ADE 7.2) is a wireless network solution designed to remotely monitor the traffic received from any 802.11 source. By monitoring this traffic, the AirDefense Enterprise 7.2 system can detect identity theft attacks and violations of site-specific wireless security policies defined within the ADE 7.2 user interface.

The AirDefense Enterprise 7.2 system runs on single, purpose-built, dedicated server appliance which is termed the 2270 appliance, and also includes separate, purpose built remote sensors that can range from 1 to 300 on one single server appliance. The 2270 Server runs a pre-configured version of the Red Hat Linux Operating System that has been tuned to only run a few key services, with all other ports and functions closed and/or turned off. The services that are present in the operation of the server include SNMP functions, SSL functions, internal syslog functions, and HTTPS Web services. The Red Hat kernel has been compiled with version 2.4.32. Running on top of this Red Hat kernel is the core ADE 7.2 server software. The Server appliance software processes all network traffic received by the hardware network interface that is received from the remote sensors. A user with access privileges can access the correlated data through AirDefense Management GUI that is accessible via a secure, remote, web-based administration Java application.

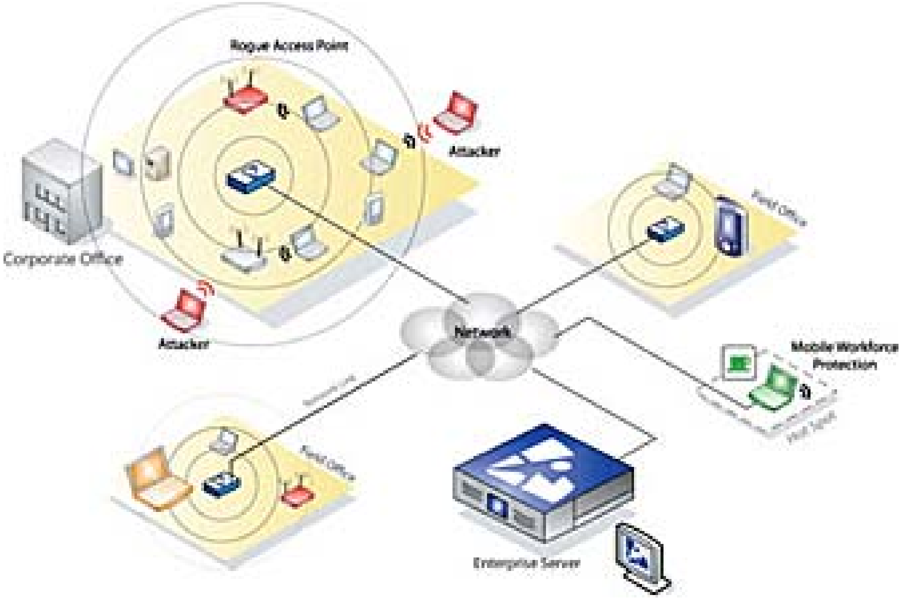
The M510 and M520 remote sensors are also dedicated stand alone devices that are tuned for listening to all wireless 802.11a/b/g traffic that is present within its field of reception. These dedicated sensors run an embedded, real time operating system of the Red Hat. This OS has also been modified to only have specific services functioning that are needed to perform the required functions that the AirDefense sensor software requires for processing and transmitting back to the server appliance. It is the AirDefense Sensor software version 4.5.0.13 that is running on top of the embedded Red Hat Operating System that provides the interfaces and functionality for the Remote Sensor portion of the TOE. These dedicated sensors communicate over a wired network utilizing a dedicated AES encrypted TCP/IP socket connection to the remote Server appliance.

Each Remote Sensor covers approximately 40,000 square feet. Remote Sensors should be installed within an area of desired coverage in an attempt to provide the sensor(s) with the best reception of all potential 802.11 traffic. This will help ensure that any wireless traffic received by the sensor from any 802.11 source on the network is sent to the central server appliance for processing and correlation. The sensor sends 802.11 headers of that traffic to the central Server for processing and does not normally include any data that might have been received by the remote sensors from Access Points and client stations.

The Remote Sensors must be in proximity to the entire footprint of the monitored network to ensure detection of a rogue 802.11 device. Remote Sensors must also be able to connect to the Server via a wired network.

The following figure illustrates a network protected by the TOE:

Figure 1 – AirDefense Enterprise Deployment



The 2270 Server appliance processes all of the collected wireless network traffic messages from each of the Remote Sensors connected to it. The Server appliance portion of the TOE can detect wireless identity thefts, and violations of site-specific wireless security policies (Allowable Use Policies) that can be crafted by a site administrator or manager.

All users must authenticate into the AirDefense server via the Management GUI from a remote host to view all relevant information, including traffic analysis summaries that are presented on the main dashboard, review the system audit events, and review all alarm data generated by events reflecting suspected security violations, and any alarms or policy violations. When a user with a admin or manager role authenticates to the AirDefense Management GUI, he or she can craft the allowable use policies; configure unauthorized Access Points and Stations as either authorized or ignored, create the site specific allowable use policies that includes the authentication and encryption methods used on their wireless network, set the allowed vendor policy, and any network allowed time usage restrictions. The TOE subsequently detects any wireless network traffic that does not match a configured policy. If the TOE detects illegal traffic, it will create an alarm record for administrators or managers to review and subsequently act upon for remediation.

An authenticated user with the role of Admin or Manager can create the Allowable Use Policies based upon several attributes of the monitored traffic. These include wireless authentication mode, channel (wireless broadcast frequency), connection rate, Service Set Identifier (SSID) broadcast status, wireless encryption protocol (e.g. WEP, WPA), vendor specific ID, date, and time of day.

The audit events portion of the TOE records all user login and logout events, and any system wide configuration changes that have been made and by which user account.

2.2 Physical Boundary

This section lists the hardware and software components of the product and denotes which are in the TOE and which are in the environment. The TOE cannot function without the Server and Sensor hardware.

2.2.1 Hardware/Software Components

This table identifies software and hardware components and indicates whether each component is in the TOE or the Environment:

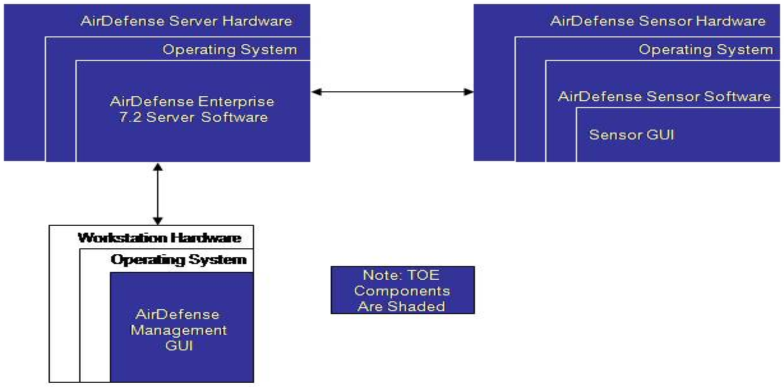
Table 1 - Enterprise 7.2 Components

Component	Description	TOE	Environment
Server Software	Processes all network traffic received by the hardware network interface, and provides a secure, web-based administration interface	✓	
Server Hardware	Dedicated, purpose-built hardware devices for running AirDefense Server Software	✓	
AirDefense Management GUI	Web-based application for managing Server Software	✓	
Management Workstation	Runs Web-based AirDefense Management GUI via browser connection Server software		✓
Sensor Software	Receives wireless traffic and sends the encrypted headers to the Server for processing. These communications are encrypted to protect their integrity.	✓	
Sensor Management GUI	Web-based application for managing Sensor Software	✓	

Component	Description	TOE	Environment
Sensor Hardware	Dedicated, purpose-built hardware devices for running AirDefense Sensor Software	✓	

A diagram of the TOE boundary is provided in the following figure:

Figure 2 – TOE Physical Boundary


AirDefense Server Hardware
Operating System
AirDefense Enterprise 7.2 Server Software
AirDefense Sensor Hardware
Operating System
AirDefense Sensor Software
Sensor GUI
Workstation Hardware
Operating System
AirDefense Management GUI
Note: TOE Components Are Shaded

The TOE configuration contains one Server and one or more Sensors.

An authenticated user can access the Server by two methods; via the Web-based AirDefense Management GUI, and via the CLI that is accessed either by a directly attached terminal or through an SSH client session.

Additionally, the Server software communicates directly with the Network Interface Card (NIC), through the operating system, for receiving communications from the Sensors.

The Sensor software receives wireless traffic from the Wireless NIC (via the operating system) and forwards that traffic to the Server through the wired Ethernet NIC (again via the operating system). The Sensors provide interfaces for local administration and configuration.

To configure the Dedicated Server portion of TOE, a directly attached terminal is required. An administrator must connect a monitor with an RGB connection, and a PS/2 keyboard to the appropriate port on the rear of the server appliance. Once this is done the administrator can login to the server management CLI interface[1]. with the *smxmgr user* account. Once the administrator has successfully logged in, all of the basic server parameters can be configured. This includes whether the server should use DHCP of a statically assign IP address, the DNS server address, the Host Name, Mail relay address, add addresses to the host allow and disallow table, setting the time zone, and setting the NTP server name.

2.3 Logical Boundary

At a high level, the logical boundaries of the TOE are the security functions implemented at TOE interfaces, including security audit, identification and authentication for the administrative functions, the management of the security management, information flow control, and the self-protection of the TOE itself.

Please refer to Section 6 of this document for more detail on the each logical boundary.

2.3.1 Security Audit

The TOE generates audit records of security relevant events including user authentication as well as configuration changes by an administrator, such creating, modifying, or deleting a policy.

Authenticated users with the Admin role are able to review audit events through the AirDefense Management GUI interface.

2.3.2 Identification and Authentication

The TOE performs the I&A function for the AirDefense Management GUI interface. There are 4 user roles, which are Admin, Manager, Network Operator, and Guest. The TOE requires the users to be authenticated before any access to the management interfaces is granted. Authentication requires a valid username and password combination.

[1] The CLI is used during installation and initial configuration of the TOE. As specified in the Administrative Guidance, only the AirDefense Management GUI should be used once the TOE is running in the evaluated configuration.

2.3.3 Traffic Analysis

The TOE controls the flow of information in a wireless network by comparing various parameters of attached devices against allowable use policies defined by the administrator. If the device is not allowed for use on the wireless network, the TOE will create an alarm and drop the device from the network (if configured to do so).

Additionally, alarms are generated when traffic analysis suggests that an identity theft attack is detected or when traffic that doesn’t match Allowable Use Policies is detected.

2.3.4 Security Management

The TOE provides the ability for the Administrator to create and manage Allowable Use Policies. These policies are created and managed through the web-based administrative interface. The attributes that these policies can be based on are: wireless authentication mode, channel (wireless broadcast frequency), connection rate, Service Set Identifier (SSID) broadcast status, wireless protocol (e.g. WEP), access point ID, host ID, date, and time of day.

A graphical interface supports creating policies. The Administrator uses HTTPS pull-down menus to specify the attributes they wish to include in a policy, then an input field or pull-down menu to specify the value that the attribute must meet.

The TOE associates users with one of four roles (Admin, Manager, Network Operator, and Guest), and each role has a specific set of available services. The user in the admin role is responsible for the overall configuration and administration of the TOE. The other roles are more restricted.

2.3.5 Protection of Security Functions

The TOE protects security functions via the Server and Sensor Operating Systems, which maintains a security domain for their own execution, protects the TSF from interference and tampering by untrusted subjects in the scope of control of the respective OS. The TOE also provides secure communication between components. Secure communications are required and achieved via SSL communications (HTTPS) between the Server and the AirDefense Management GUI and a SSL/TLS tunnel between the Server and Sensor(s). The cryptographic functions implemented to achieve these secure communications are not FIPS certified but are vendor asserted to be FIPS compliant. More details of cryptographic functions can be found in Section 5 and Section 6 of this document.

2.4 Evaluated Configuration

In order to comply with the evaluated configuration, the following hardware and software components should be used:

Table 2 - TOE Components and Version Numbers for Evaluated Configuration

TOE Component	Version/Model Number
AirDefense Server Software	Version: Enterprise 7.2 Hardware Requirements: • AirDefense 2270 Appliance
AirDefense Sensor Software	Version: 4.5.0.13 Hardware Requirements: • AirDefense M510 and M520 Sensors
AirDefense Management GUI	Version: Enterprise 7.2 Hardware Requirements: • Workstation running Microsoft Windows NT version 4 or later, Windows 2000, or Windows XP • Web browser

3. Security Environment

3.1 Introduction

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

A) assumptions about the environment,

B) threats to the assets and

C) organizational security policies.

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

3.2 Assumptions

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

Table 3 - Assumptions

Assumption	Description
A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware.
A.NETWORK	There will be a wired network that supports TCP communications connecting the Server to the Remote Sensors. This network functions properly.
A.NOEVIL	The administrator is competent and will install and configure the TOE according to the administrator guidance.
A.PASSWORD	Administrators will use passwords that conform to the administrator guidance.
A.SINGLE_POINT	All wireless communications received by the sensors flow through the server.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and the IT environment.

Table 4 - Threats

Threat	TOE Threats
T.ADMIN_NOAUTH	An attacker gains administrative privileges to the TOE by accessing the TOE through its administrative interface, and this access occurs without notice.
T.ATTACK	An attacker denies the service of a wireless Access Point by flooding it with traffic, without being detected.
T.COMP_MANAGE	Data may be compromised while traversing the connection between the TOE components.
T.NO_ACCOUNT	An administrator might perform actions for which they are not accountable.
T.POLICY_VIOLATE	An attacker gains unauthorized use of the network by broadcasting wireless network traffic in violation of the Allowable Use Policies, without being detected.
T.SEC_BYPASS	The TOE might be subject to malicious tampering or bypass of its security mechanisms.

3.4 Organizational Security Policies

There are no Organizational Security Policies identified for this TOE.

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's IT environment and the TOE's non-IT environment. The security objectives identify the responsibilities of the TOE, the TOE's IT environment, and the TOE's non-IT environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the IT environment are designated as *OE.objective*. Objectives that apply to the non-IT environment are designated with an *ON.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives:

Table 5 - Security Objectives for the TOE

Objective	Security Objective
O.AUDIT	The TOE must record and provide review of events of security relevance to the system.
O.AUTHENTICATE	The TOE must require users of the AirDefense Management GUI to authenticate in order to access the management interface.
O.DETECT	The TOE must detect traffic that is in violation of the Allowable Use Policies.
O.MANAGE	The TOE must provide the Administrator with ongoing configuration of the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability.
O.SECURE_COMM	The TOE shall securely transfer data between components.
O.SELF_PROTECT	The TOE will maintain a domain for its own execution and domains for separate application processes that protect itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.TIMESTAMP	The TOE must provide a reliable timestamp.

4.2 Security Objectives for the IT Environment

Objective	Security Objective
OE.SECURE_COMM	The IT environment will provide secure communications between the TOE components.

4.3 Security Objectives for the Non-IT Environment

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures. The TOE's Non-IT environment must satisfy the following objectives:

Table 6 - Security Objectives for the Non-IT Environment

Objective	Security Objectives for the Non-IT Environment
ON.COMPLETE	All wireless traffic that enters the monitored network is received by the TOE sensors.
ON.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware.
ON.NETWORK	There will be a network that supports TCP communication connecting the Server to the Remote Sensors. This network functions properly.
ON.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when installing and using the TOE. Administration is competent and on-going.
ON.PASSWORD	Users will use passwords that conform to the guidance.

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. The SFRs defined in this section are derived from Part 2 of the CC.

5.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* with the exception of italicized items listed in brackets. These bracketed items include either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces.

Security Functional Requirements are summarized in the table below:

Table 7 - Security Functional Requirements Summary

Class Heading	Class_Family	Description
Security Audit	FAU_GEN.1 (EXP)	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.2	Guarantees of Audit Data Availability
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User Authentication before any action
	FIA_UID.2	User Identification before any action
Security Management	FMT_MOF.1a&b	Management of Security Functions Behavior
	FMT_MTD.1a&b	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_RVM.1	Non-bypassability of the TSP

	FPT_SEP.1	TSF Domain Separation
	FPT_STM.1	Reliable Time Stamps
IDS Component	IDS_ANL.1 (EXP)	Analysis (EXP)
	IDS_RCT.1 (EXP)	React (EXP)
	IDS_RDR.1 (EXP)	Restricted Data Review (EXP)
	IDS_SDC.1 (EXP)	TOE Data Collection (EXP)

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 (EXP)

FAU_GEN.1(EXP) The TSF shall be able to generate an audit record of the following auditable events: *successful use of authentication mechanism, and configuration and management of the following: Allowable Use Policy, Sensor Manager, and User Management.*

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

a) Date and time of the event, type of event, and subject identity that caused the event.

5.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*Administrator*] with the capability to read [*all 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.

5.1.1.3 FAU_SAR.2 Restricted Audit Review

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

5.1.1.4 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to perform [sorting] of audit data based on [*Time, Username, Section, Description*].

5.1.1.5 FAU_STG.1 Protected Audit Trail Storage

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

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

5.1.1.6 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [*all stored*] audit records will be maintained when the following conditions occur: [TOE failure].

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Pseudorandom Number Generator*] and specified cryptographic key sizes [*256*] that meets the following: [*ANSI X9.31*].

5.1.2.2 FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [*TLS v1.0*] that meets the following: [*RFC 2246*].

5.1.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

5.1.2.4 FCS_COP.1 Cryptographic Operation

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

Table 8 - Cryptographic Operations

Operation	Algorithm (mode)	Key Size in Bits	Standards
Encryption and Decryption	AES (CBC mode)	256	FIPS 197

Key distribution / agreement	TLSv1.0	p = 1024
		g = 2
			RFC 2246

Hashing	SHS (SHA-1)	160 (size of digest)	FIPS 180-2
Random Number Generation	ANSI X9.31	256	ANSI X9.31

Application Note: The cryptographic algorithms in the Server and sensor components of the TOE have not been validated by the CAVP, nor have they been analyzed or tested to conform to cryptographic standards during this evaluation. These implementations have only been asserted as tested by the vendor.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*username, password, role*].

5.1.3.2 FIA_UAU.2 User Authentication before Any Action

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

5.1.3.3 FIA_UID.2 User Identification before Any Action

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

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1a The TSF shall restrict the ability to [modify the behavior of] the functions [*management function view* audit log] to [*Administrator*].

FMT_MOF.1.1b The TSF shall restrict the ability to [modify the behavior of] the functions [*management functions: allowable use policy creation and modification, alarm notification, alarm enablement, and sensor operation*] to [*Administrator and manager*].

5.1.4.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1a The TSF shall restrict the ability to [query] the [*system date and time*] to [A*dministrator*].

FMT_MTD.1.1b The TSF shall restrict the ability to [delete, and [*create*]] [*user accounts*, including *username, password,* and *role]* to [A*dministrator*].

FMT_MTD.1.1c The TSF shall restrict the ability to [clear] the [alarms] to [administrator, manager, and network operator roles].

5.1.4.3 FMT_SMF.1 Specification of Management Functions

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

1) *Allowable Use Policy creation and configuration*
2) *Alarm Notification*
3) *Alarm Enablement*
4) *Sensor Operation*
5) *view of the audit log*
6) *Management of user account info*
7) *Clear Alarms*

5.1.4.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [A*dministrator, Manager, and Network Operator*].

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_ITT.1a Basic Internal TSF Data Transfer Protection

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

5.1.5.2 FPT_RVM.1 Non-Bypassability of the TSP

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

5.1.5.3 FPT_SEP.1 TSF Domain Separation

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

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

5.1.5.4 FPT_STM.1 Reliable Time Stamps

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

5.1.6 IDS Component

5.1.6.1 IDS_ANL.1 Analysis (EXP)

IDS_ANL.1.1 The TOE shall perform the following analysis function(s) on all IDS data received: [*correlation of data and comparison against Allowable Use Policies*]

IDS_ANL.1.2 The TOE shall record within each analytical result at least the following information:

a. Date and time of the result, type of result, and identification of data source.

5.1.6.2 IDS_RCT.1 React (EXP)

IDS_RCT.1.1 The TOE shall generate an alarm, send notification and take *action* to not allow the end point to access the internal network when an intrusion is detected.

5.1.6.3 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The TOE shall provide [*an Authorized* User] with the capability to read the IDS data as defined in IDS_ANL.1 and IDS_SDC.1.

IDS_RDR.1.2 The TOE shall provide the IDS data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The TOE shall prohibit all users read access to the IDS data, except those users that have been granted explicit read-access.

5.1.6.4 IDS_SDC.1 TOE Data Collection (EXP)

IDS_SDC.1.1 The TOE shall be able to collect the following information from the targeted wireless IT System resource(s):

1) *Endpoint identifier (MAC Address)*
2) *Service Set Identifier (SSID)*
3) *Parameters for comparison to Allowable Use Policies to include the following:*
    - *wireless authentication mode*
    - *channel (wireless broadcast frequency)*
    - *connection rate*
    - *SSID*
    - Wireless encryption mode
    - *vendor specific ID*
    - *time of day*

5.2 **FPT_ITT.1b Basic Internal TSF Data Transfer Protection**

FPT_ITT.1.1b The ~~TSF~~ IT environment shall protect TSF data from [disclosure and modification] when it is transmitted between separate parts of the TOE.

5.3 Strength of Function for the TOE

This security target includes one probabilistic or permutational function:

- Identification and Authentication
    - FIA_UAU.2 – Authentication of Administrators

The SOF for these mechanisms is SOF-Basic.

The following functions are cryptographic and thus are out of scope for Strength of Function in this Security Target:

- Cryptographic support
  - FCS_COP.1 – Cryptographic Operation
  - FCS_CKM.1 – Cryptographic Key Generation
  - FCS_CKM.2 – Cryptographic Key Distribution
  - FCS_CKM.4 – Cryptographic Key Destruction

5.4 CC Component Hierarchies and Dependencies

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

Table 9 - TOE SFR Dependency Detail

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1(EXP)	No other components.	FPT_STM.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied by FAU_GEN.1(EXP)
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components.	FAU_SAR.1	Satisfied
FAU_STG.1	No other components.	FAU_GEN.1	Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FCS_CKM.1	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Satisfied by FCS_CKM.2, FCS_COP.1, FCS_CKM.4 See note following this table regarding FMT_MSA.2
FCS_CKM.2	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Satisfied by FCS_CKM.1, FCS_CKM.4 See note following this table regarding FMT_MSA.2
FCS_CKM.4	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Satisfied by FCS_CKM.1 See note following this table regarding FMT_MSA.2
FCS_COP.1	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Satisfied by FCS_CKM.1, FCS_CKM.4 See note following this table regarding FMT_MSA.2
FIA_ATD.1	No other components.	None	N/A
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2, which is

SFR	Hierarchical To	Dependency	Rationale
			hierarchical to FIA_UID.1
FIA_UID.2	FIA_UID.1	None	Not applicable
FMT_MOF.1a&b	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied by FMT_SMF.1, FMT_SMR.1
FMT_MTD.1a&b	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied by FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	No other components.	None	N/A
FMT_SMR.1	No other components.	FIA_UID.2	Satisfied
FPT_ITT.1	No other components.	None	N/A
FPT_RVM.1	No other components.	None	N/A
FPT_SEP.1	No other components.	None	N/A
FPT_STM.1	No other components.	None	N/A
IDS_ANL.1 (EXP)	No other components.	None	N/A
IDS_RCT.1 (EXP)	No other components.	None	N/A
IDS_RDR.1 (EXP)	No other components.	None	N/A
IDS_SDC.1 (EXP)	No other components.	None	N/A

Note that the dependencies for FMT_MSA.2 are not met because the cryptographic module is currently undergoing FIPS validation. The TOE initializes this module in “FIPS mode” and uses this module exactly as specified by the FIPS 140-2 validation testing; therefore, the dependencies of secure key values are satisfied by this module's validation as FIPS 140-2 compliant.

6. TOE Summary Specification

This section presents the Security Functions implemented by the TOE. The Assurance Measures applied to ensure the correct implementation of the TOE Security Functions are listed in Section 6.2 – TOE Security Assurance Requirements and detailed in Section 8.2.3 – Security Assurance Requirements Rationale.

6.1 Security Functions

6.1.1 Security Audit

The server portion of the TOE generates audit records for system security events, changes to the Allowable Use Policies, changes within the Sensor Manager, User Management, i.e. User creation, modification or deletion, and successful user authentication.

No user can access the audit trail in any way if they are not first authenticated. The audit records are reviewed from the appliance manager module within the AirDefense GUI interface. Only the user role of Admin can access the Appliance Management module. The role of admin is able to clear the audit trail but the TOE does not provide an interface for users to modify the audit trail no matter what their defined role is set to. Through the administrative interface a user with a role of Admin can review the audit trail in an easy-to-read table, and this table can be sorted by *Time, Username, Section*[2]*,* and *Description*[3]*.*

If there is a total system failure, the audit records can be preserved if the server portion of the TOE was configured for automatic database backups and those backups where then stored off of the server.

The Security Audit function of the TOE meets the following SFRs:

- FAU_GEN.1 (EXP)
- FAU_SAR.1
- FAU_SAR.2
- FAU_SAR.3
- FAU_STG.1
- FAU_STG.2

[2] Details the type of change, such as Policy, Configuration, etc.

[3] Provides the details of log events, such as policy modification, or deletion

6.1.2 Security Management

Four user roles exist in the TOE: Admin, Manager, Network Operator, and Guest; only the Admin and Manager roles are considered administrative roles and can perform administrative functions. Admin/administrators are used interchangeably throughout the ST. All authenticated users are considered authorized users. All user accounts must be configured with one of following roles:

- Admin Users: Have both read and write privileges throughout the UI, in every module within the server GUI application. These privileges includes deleting users, adding new users to the TOE, configuring policies, sensor configurations, configuring alarm priorities, clearing alarms, enabling notifications performing system backups and restores and reviewing the audit log.
- Manager Users: have the same privileges as the Admin role, with the exception that a Manager cannot view or modify user accounts or access to the audit logs.
- Network Operator Users: have read-only access to the Alarm Manager but can clear alarms and has read-only access to the policy manager, but has no access to Alarm Configurations or to the Appliance Manager module which includes user account management, notifications, database backups and restores and access to the audit logs.
- Guest Users: only have read-only access to the following AirDefense Enterprise GUI program areas: Dashboard, Alarm Manager, Sensor Manager and Policy Manager, no other system areas can be viewed or accessed.

An authenticated user can access the Server by two methods; via the Web-based AirDefense Management GUI, and via the CLI that is accessed either by a directly attached terminal or through an SSH client session.

A login account with the role of Admin or manager uses the administrative interfaces to manage the TSF. Once authenticated, this user can manage allowable use policies including creating, deleting, and modifying. This user account can also specify the attributes to include in a policy and specific parameters for the attribute. These policies can be based on many important site-specific attributes of wireless 802.11 traffic, such as wireless authentication mode, channel (wireless broadcast frequency), connection rate, Service Set Identifier (SSID) broadcast status, and wireless encryption (e.g. WEP or AES). Additionally, the following environmental and site-specific attributes can be specified: access point ID (registered MAC), host ID (registered MAC), and time of day.

Violations of the Allowable Use Policies by monitored WLAN devices will trigger alarms. A login account with the role of Admin or Manager is capable of managing these alarms by enabling/disabling them, changing their priorities, configuring rules/mechanisms for remote alarm notification, and creating custom filters with which to better view the alarms.

Further, a login account with role of Admin is capable of managing the configuration of the Remote Sensors which send to the Server the observed 802.11 wireless network traffic headers for processing, correlation, and display. Specifically, the authenticated admin user to the sensor's management interface is able to configure the sensor's primary and secondary server addresses, whether to use DHCP or Static IP addressing, turn on or off the external syslog service and set the IP address of the external syslog server, turn on or off the location function of the sensor LEDs, upgrading the sensor firmware, and change the admin or manager account passwords.

The Security Management function of the TOE meets the following SFRs:

- FIA_ATD.1
- FMT_MOF.1a
- FMT_MOF.1b
- FMT_MTD.1a
- FMT_MTD.1b
- FMT_MTD.1c
- FMT_SMF.1
- FMT_SMR.1

6.1.3 Identification and Authentication

The only way that users can access the TOE is by logging into the management interface (e.g., the AirDefense Management GUI, CLI, or the Sensor GUI). I&A is performed by the TOE for all of these interfaces. The login page asks the user to enter a username and password. The username must be a valid user, and the password must be correct for the given username. Once successfully logged into the particular management interface, the user is both identified and authenticated.

When a user authenticates to the TOE, they have access to only the services available for the role defined for that user account. The password for any user role needs to meet the following criteria:

- Contain no spaces or tabs
- Contain at least one uppercase alphabetical characters
- Contain at least one lowercase alphabetical characters
- Contain at least one digit

- Contain 1 or more symbols from this list: `~!@#$%^&*()_+=?<>{};:”./
- Be longer than 5 characters
- Be shorter than 34 characters

The strength of function is referenced for The Authentication and Identification security function as an SOF-Basic.

The Identification and Authentication function of the TOE meets the following SFRs:

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2

6.1.4 Traffic Analysis

All wireless traffic that has been intercepted by the TOE is displayed in the Alarm Manager section of the Enterprise Management GUI. All decisions to permit or deny the traffic based on conformance or nonconformance to an Allowable Use Policy are also displayed here. These events show details that includes sufficient information to detect identity theft attacks, rogue detection and activity that is not allowed according to the set policies that have been configured. These events that are recorded in the Alarm Manager include: the date, time, host MAC address, and the identity of the capturing Remote Sensor.

Identity theft attacks are identified when the behavior of a wireless card does not match its vendor as determined by the broadcast MAC address. There are two types of identity theft attacks that will results in endpoint denial of service:

1. De-authentication: Occurs when an attacker is spoofing the MAC address of an Access Point and is either telling a specific host or all hosts to de-authenticate. Upon detection, the TOE will deny service/connectivity to the respective endpoint.
2. Disassociation: Occurs when an attacker is spoofing the MAC address of an Access Point and is either telling a specific host or all hosts to disassociate. Upon detection, the TOE will deny service/connectivity to the respective endpoint.

The server will display all triggered alarms in the alarm manager window. In addition, the server will also send an e-mail to the administrator, and if configured, the server will also send out syslog info, and SNMP trap information to an external receiver (third-party security notification device).

The TOE evaluates traffic in real-time and determines if an alarm record should be made of the suspicious traffic. These records would then include the data that is within the Management Frame Headers of the intercepted packets. The TOE works from a set of Allowable Use Policies that are defined by the Administrator and by the built-in traffic analysis algorithms. These built-in algorithms are used to check for any detected Denial of Service frames (DoS) and Disassociate frames that are originating from either an AP or a station that is within the coverage area of the deployed sensors. Detection of Denial of Service (DoS) events that involve Deauthentication and Disassociation activities require three conditions to be met: 1) signature matching (built-in algorithms), 2) invalid use of the protocol (802.11a/b/g), and 3) policy checking. These DoS events rely exclusively on analysis of 802.11 Management Frame Headers. The headers must match a signature (signature matching), must be voluminous enough to be out of character with the normal network (protocol abuse), and must happen on an authorized access point or station.

The Allowable Use Policies define the allowable wireless traffic for the network protected by the TOE. The allowable use policies are created during the initial server setup process. The attributes of an allowable use policy that can be used to define these policies are: wireless authentication mode (open or shared), channel (wireless broadcast frequency), connection rate, Service Set Identifier (SSID), broadcast status, wireless encryption protocol (WEP, WPA or WPA2), access point ID, host ID, and time of day.

These parameters are initially set during the initial server setup procedures and then can be later re-configured or additional policies can be created via the Policy Manager in the AirDefense Management GUI. The TOE reviews the endpoint identifier, and if these parameters are identified as being allowed on the network, the TOE will subject the wireless device to the Allowable Use Policies. Otherwise, the session from the wireless device is terminated.

For example, utilizing pull-down menus and text fields, the Administrator defines a rule that traffic from a particular host is only allowed to be received by a specific access point using WEP. Then, if the TOE receives traffic that does not match those three attributes, an alarm is generated. Allowable Use Policies provide a means for the administrator to specify the conditions by which a wireless device can operate within the sensor’s operational coverage area.

Allowable use policy violations are detected by analyzing management frames headers of the wireless traffic and comparing the observed behavior to the defined policy generating events on any activity that is not allowed in the policy as configured by the administrator as shown in the above example.

The TOE analyzes traffic in a wireless network by comparing various parameters of attached devices against allowable use policies defined by the user role of Admin. If the device is not allowed for use on the wireless network (i.e., there is a violation of allowable use policies), the TOE will create an alarm and drop the device from the network.

All data collected from the remote sensors and analyzed by the server against the Allowable Use Policies or the built-in traffic analysis algorithms can be reviewed by an authenticated user to determine what type of violations/alarms are being reported by the server. The server will disconnect or drop an unauthorized device from the WLAN but it will still be necessary to determine this device's location to either authorize it if it belongs in the monitored airspace or remove from service if it is found not to be an authorized device within the monitored airspace.

The IDS data is defined as the information collected by the sensor(s) and analyzed by the server including:

1. Unauthorized devices (Access Points and Stations)
2. Identity Theft Attacks
3. Acceptable use Policy violations
4. Violations against the built-in 802.11a/b/g protocol analysis algorithms

The Traffic Analysis function is designed to satisfy the following security functional requirements:

- IDS_ANL.1 (EXP)
- IDS_RCT.1 (EXP)
- IDS_RDR.1 (EXP)
- IDS_SDC.1 (EXP)

6.1.5 Protection of Security Functions

The TOE maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the TOE.

All TOE operations are self-contained, and all administration and configuration operations are performed within the physical boundary of the TOE. Neither the Sensor nor the Server support or perform non-product specific functionality because the TOE does not implement a general purpose operating system.

All users (including authorized administrators) have to be authenticated prior to performing any actions on the TOE. All user and allowable use policy data is controlled via the management GUI, which requires authenticated access and connects to the Server component via required SSL connections. These SSL connections utilize the HTTPS protocol to support the required secure communications between the AirDefense Management GUI and the server and the required secure communications between each sensor and the server. The TOE initializes these secure communications as described in section 6.1.5.1.

6.1.5.1 Cryptographic Support

The cryptographic functions implemented within this TOE are not FIPS certified but are vendor asserted to be FIPS compliant.

Communications between each TOE component are protected via a SSL/TLS encrypted tunnel utilizing the HTTPS protocol. In AirDefense Management GUI to server connections, the TOE supports form-based authentication[4] to authenticate the client. The TOE then uses a Diffie-Hellman operation for key agreement, using P length of 1024-bits and G length of 2-bits. The TOE uses the output of ANSI X9.31 to create a 256-bit AES key (key generation), and this key is used to encrypt data over the SSL/TLS tunnel. As specified in the SSL/TLS protocol, SHA-1 hashing is used for message/data integrity.

For Server to Sensor communications, the TOE uses certificate-based authentication for each peer. The TOE uses the output of ANSI X9.31 to create a 256-bit AES key (key generation), and this key is used to encrypt data over the SSL/TLS tunnel. As specified in the SSL/TLS protocol, SHA-1 hashing is used for message/data integrity.

Once the 256-bit AES keys are generated, they are stored in RAM and used for SSL/TLS session encryption and decryption. When the session is terminated, keys are overwritten with 0’s (e.g. key destruction via zeroization) as specified in the FIPS 140-2 requirements. Keys are stored in plaintext and are protected from unauthorized disclosure via peer authentication. The AES keys are not visible to any human operator of the TOE, including authenticated administrators.

The Protection of Security Functions function is designed to satisfy the following security functional requirements:

- FCS_CKM.1
- FCS_CKM.2
- FCS_CKM.4
- FCS_COP.1
- FPT_ITT.1
- FPT_RVM.1
- FPT_SEP.1
- FPT_STM.1

[4] The username and password are entered in a text box / dialog within the AirDefense Management GUI. The username and password are sent to the Server in encrypted form over an SSL/TLS tunnel.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are the components of the EAL2 package defined in the CC Part 3 and are summarized in the following table:

Table 10 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration items
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

7. Protection Profile Claims

This Security Target does not claim conformance to any registered Protection Profile though it does leverage explicitly stated SFRs in the *Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006.* See the “Rationale for Explicitly Stated Requirements” section of this document for more information.

8. Rationale

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

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 11 - Threats and Assumptions to Security Objectives Mapping

Objective Threat / Assumption	O.AUDIT	O.AUTHENTICATE	O.DETECT	O.MANAGE	O.SECURE_COMM	O.SELF_PROTECT	O.TIMESTAMP	ON.COMPLETE	ON.ENVIRON	ON.NETWORK	ON.NOEVILADMIN	ON.PASSWORD	OE.NETWORK
T.ADMIN_NOAUTH	✓	✓					✓						
T.ATTACK			✓	✓			✓						
T.COMP_MANAGE					✓								
T.NO_ACCOUNT	✓			✓			✓						
T.POLICY_VIOLATE	✓		✓	✓			✓	✓					
T.SEC_BYPASS						✓							
A.ENVIRON									✓				
A.NETWORK										✓			✓
A.NOEVIL											✓		
A.PASSWORD												✓	
A.SINGLE_POINT								✓					

8.1.1 Rationale Showing Threats to Security Objectives

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

Table 12 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.ADMIN_NOAUTH An attacker gains administrative privileges to the TOE by accessing the TOE through its administrative interface, and this access occurs without notice.	O.AUDIT mitigates this threat which ensures the TOE record security-relevant events and provide the Administrator with review capabilities. The TOE enables the Administrator to detect malicious activity and verify proper system behavior. O.AUDIT is supported by O.TIMESTAMP which ensures that the record contains the time and date that the event occurs. O.AUTHENTICATE mitigates this threat by requiring administrators to identify and authenticate at the management interface.
T.ATTACK An attacker denies the service of a wireless Access Point by flooding it with traffic, without being detected.	O.DETECT mitigates this threat by requiring the TOE to detect this type of attack traffic. O.MANAGE mitigates this threat by providing configuration of the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit function, O.MANAGE directly supports O.AUDIT which addresses threats countered by the TOE. O.TIMESTAMP mitigates this threat by providing the TOE with a reliable timestamp. O.TIMESTAMP supports the TOE's auditing capabilities, and auditing is used by the TOE to counter all of its threats.
T.COMP_MANAGE Data may be compromised while traversing the connection between the TOE components.	O.SECURE_COMM mitigates this threat by providing a secure session between TOE components.
T.NO_ACCOUNT An administrator might perform actions for which they are not accountable.	O.AUDIT mitigates this threat by requiring the TOE to record security-relevant events and provide the Administrator with review capabilities. The TOE enables the Administrator to detect malicious activity and verify proper system behavior. O.MANAGE mitigates this threat by providing configuration of the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit function, O.MANAGE directly supports O.AUDIT which addresses threats countered by the TOE. O.TIMESTAMP mitigates this threat by providing the TOE with a reliable timestamp. OE.TIMESTAMP supports the TOE's auditing capabilities, and auditing is used by the TOE to counter all of its threats.

T.TYPE	Security Objectives Rationale
T.POLICY_VIOLATE An attacker gains unauthorized use of the network by broadcasting wireless network traffic in violation of the Allowable Use Policies, without being detected.	O.AUDIT mitigates this threat by requiring the TOE to record security-relevant events and provide the Administrator with review capabilities. The TOE enables the Administrator to detect malicious activity and verify proper system behavior. O.DETECT mitigates this threat by requiring the TOE to detect this type of attack traffic. O.MANAGE mitigates this threat by providing configuration of the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit function, O.MANAGE directly supports O.AUDIT which addresses threats countered by the TOE. O.TIMESTAMP mitigates this threat by providing the TOE with a reliable timestamp. OE.TIMESTAMP supports the TOE's auditing capabilities, and auditing is used by the TOE to counter all of its threats. ON.COMPLETE addresses this threat by requiring the Non-IT Environment to ensure that all wireless traffic that enters the monitored network is processed by the TOE server component.
T.SEC_BYPASS The TOE might be subject to malicious tampering or bypass of its security mechanisms.	O.SELF_PROTECT mitigates this threat by ensuring that the TSF can protect itself from users within the TSC. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the audit trail. Ensuring that the TSF is always invoked is also critical to the mitigation of this threat.
A.ENVIRON The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware.	ON.ENVIRON addresses this assumption by requiring the Non-IT Environment to ensure that the environment in which the TOE is located provides physical security, uninterruptible power, and temperature control.
A.NETWORK There will be a network that supports TCP communication connecting the Server to the Remote Sensors. This network functions properly.	ON.NETWORK addresses this assumption by requiring the Non-IT Environment to ensure that the network on which the server communicates with the sensors functions properly. OE.NETWORK IT Environment provides secure communications between the TOE components
A.NOEVIL The administrator is competent and will install and configure the TOE according to the administrator guidance.	ON.NOEVILADMIN addresses this assumption by requiring the Non-IT Environment to ensure that Administrators are non-hostile, competent, and follow the administrator guidance when installing and using the TOE.
A.PASSWORD Administrators will use passwords that conform to the administrator guidance.	ON.PASSWORD addresses this assumption by requiring the Non-IT Environment to ensure that the Administrators will use passwords that conform to the administrator guidance.

T.TYPE	Security Objectives Rationale
A.SINGLE_POINT All wireless communications received by the sensors flow through the server.	ON.COMPLETE addresses this assumption by requiring the Non-IT Environment to ensure that all wireless traffic that enters the monitored network is processed by the TOE server component.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 13 - SFRs to Security Objectives Mapping

Objective SFR	O.AUDIT	O.AUTHENTICATE	O.DETECT	O.MANAGE	O.SECURE_COMM	O.SELF_PROTECT	O.TIMESTAMP
FAU_GEN.1(EXP)	✓						
FAU_SAR.1	✓						
FAU_SAR.2				✓			
FAU_SAR.3	✓			✓			
FAU_STG.1	✓						
FAU_STG.2	✓						
FCS_CKM.1					✓		
FCS_CKM.2					✓		
FCS_CKM.4					✓		
FCS_COP.1					✓		
FIA_ATD.1		✓					
FIA_UID.2		✓					

Objective SFR	O.AUDIT	O.AUTHENTICATE	O.DETECT	O.MANAGE	O.SECURE_COMM	O.SELF_PROTECT	O.TIMESTAMP
FIA_UAU.2		✓					
FMT_MOF.1a				✓			
FMT_MOF.1b				✓			
FMT_MTD.1a				✓			
FMT_MTD.1b				✓			
FMT_MTD.1c				✓			
FMT_SMF.1				✓			
FMT_SMR.1				✓			
FPT_ITT.1a					✓	✓	
FPT_ITT.1b					✓	✓	
FPT_RVM.1		✓				✓	
FPT_SEP.1						✓	
FPT_STM.1	✓						✓
IDS_ANL.1 (EXP)			✓				
IDS_RCT.1 (EXP)			✓				
IDS_RDR.1 (EXP)			✓				
IDS_SDC.1 (EXP)			✓				

The following table provides the detail of TOE security objective(s).

Table 14 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDIT The TOE must record and provide review of events of security relevance to the system.	FAU_SAR.1 supports this objective by requiring the TOE to provide audit trail review capabilities to the Administrator; a mechanism is provided for the Administrator to gain information about system functionality and threats. FAU_SAR.3 supports this objective by requiring the TOE to provide a mechanism to sort audit data to allow the Administrator to view information by a specific category. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1(EXP)].

Security Objective	SFR and Rationale
	The TOE prevents unauthorized modification and deletion of audit records [FAU_STG.1]. The TOE ensures audit records are maintained if there is a operational failure in the TOE [FAU_STG.2]. Time stamps associated with an audit record must be reliable [FPT_STM.1].
O.AUTHENTICATE The TOE must require users of the AirDefense Management GUI to authenticate in order to access the management interface.	Users authorized to access the TOE are defined using an identification and authentication process and associated with a specific role [FIA_ATD.1, FIA_UID.2, FIA_UAU.2]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1].
O.DETECT The TOE must detect traffic that is in violation of the Allowable Use Policies.	IDS_ANL.1 (EXP) supports this objective by specifying comparative analysis on the traffic against Allowable Use Policies. IDS_SDC.1 (EXP) supports this objective by specifying the set of events occurring on monitored IT systems whose occurrence indicates a potential violation of the TSP. IDS_RCT.1 (EXP) supports this objective by specifying the creation of an alarm upon detection of a security violation. IDS_RDR.1 (EXP) supports this objective by allowing all data collected and analyzed against Allowable Use Policies to be reviewed by an Authorized Administrator via the AirDefense Management GUI.
O.MANAGE The TOE must provide the Administrator with ongoing configuration of the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability.	FAU_SAR.2 supports this objective by allowing only authorized users to review audit data. FAU_SAR.3 supports this objective by allowing authorized users to sort audit data FMT_MOF.1a&b supports this objective by specifying that the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability can be managed by the Administrator. FMT_MTD.1a,b,&c supports this objective by specifying that the Alarms, Monitored WLAN Devices, Users, Audit Trail Records, and Database can be managed by the Administrator. FMT_SMF.1 supports this objective by specifying that the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability can be managed. FMT_SMR.1 supports this objective by specifying that the TSF shall maintain the Administrator role.
O.SECURE_COMM The TOE shall securely transfer data between components.	FCS_CKM.1 ensures robust key generation. FCS_CKM.2 ensures standards-based key distribution FCS_CKM.4 ensures keys are overwritten securely

Security Objective	SFR and Rationale
	FCS_COP.1 provides cryptographic support for protection of data transfer between components. FPT_ITT.1a requires that the TOE protects TSF data from one component to another via a secure tunnel. FPT_ITT.1b requires that the IT environment protects TSF data between the TOE components.
O.SELF_PROTECT The TOE will maintain a domain for its own execution and domains for separate application processes that protect itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.	The TOE is required to protect the audit data from deletion The TOE is self contained and offers limited interfaces to reduce tampering from external sources. All users (including authorized administrators) have to be authenticated prior to performing any actions on the TOE. Additionally, all information flow control rules are invoked before traffic is allowed. [FPT_RVM.1, FPT_SEP.1]. FPT.ITT.1 requires that the TOE protects TSF data from one component to another via a secure tunnel.
O.TIMESTAMP	FPT_STM.1 supports this objective by providing a reliable timestamp.

8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives

Security Objective	SFR and Rationale
OE.SECURE_COMM	FPT_ITT.1b The IT environment in conjunction with the TOE ensures the protection of communication between separate components of the TOE

8.2.3 Security Assurance Requirements Rationale

8.2.3.1 TOE Security Assurance Requirements Rationale

The TOE meets the assurance requirements for EAL2. The following table provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 15 - Assurance Measures

Component ID	Rationale
ACM_CAP.2	Configuration items: The implementation and documentation of procedures for the development of the TOE, including a configuration list of uniquely identified items.

Component ID	Rationale
	Evidence Title: *AirDefense Configuration Items*
ADO_DEL.1	Delivery procedures: The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner. Evidence Title: *AirDefense Delivery Procedures*
ADO_IGS.1	Installation, generation, and start-up procedures: Documentation provided to the end users instructing the end users how to install and configure the TOE in a secure manner. Evidence Title: *AirDefense Installation and Start-up Procedures*
ADV_FSP.1	Informal functional specification: Functional Specification for the TOE describing the TSF and the TOE's external interfaces. Evidence Title: *AirDefense Functional Specification*
ADV_HLD.1	Descriptive high-level design: System Design for the TOE providing descriptions of the TSF structure in the form of subsystems and the functionality of each subsystem. Evidence Title: *AirDefense High Level Design*
ADV_RCR.1	Informal correspondence demonstration: The documentation of the correspondence between the TSS, FSP and HLD in specifically provided deliverables. Evidence Title: *AirDefense Correspondence*
AGD_ADM.1	Administrator guidance: Documentation provided to the customers instructing the customer how to configure the TOE in a secure manner. Evidence Title: *AirDefense Administrator Guidance*
AGD_USR.1	User guidance: Documentation provided to the customers instructing the users how to use the TOE. Evidence Title: *AirDefense User Guidance*
ATE_COV.1	Evidence of coverage: Documented correspondence between the security functions and tests. Evidence Title: *AirDefense Test Coverage Evidence*
ATE_FUN.1	Functional testing: The implementation and documentation of the test procedures including expected and actual results. Evidence Title: *AirDefense Test Plan*
ATE_IND.2	Functional testing: The implementation and documentation of the test procedures including expected and actual results. Evidence Title: *AirDefense*
AVA_SOF.1	Strength of TOE security function evaluation: The documentation for the Strength of Function Assessment. Evidence Title: *AirDefense Strength of Function*
AVA_VLA.1	Developer vulnerability analysis: Vulnerability Assessment of the TOE and its deliverables is performed and documented to ensure that identified security flaws are countered. Evidence Title: *AirDefense Vulnerability Analysis*

8.2.3.2 Rationale for TOE Assurance Requirements Selection

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

The general level of assurance for the TOE is:

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

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

8.3 TOE Summary Specification Rationale

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

Table 16 - SFRs to TOE Security Functions Mapping

TSF SFR	IDENTIFICATION & AUTHENTICATION	SECURITY AUDIT	TRAFFIC ANALYSIS	SECURITY MANAGEMENT	PROTECTION OF SECURITY FUNCTIONS
FAU_GEN.1(EXP)		✓			
FAU_SAR.1		✓			
FAU_SAR.2		✓			
FAU_SAR.3		✓			
FAU_STG.1		✓			
FAU_STG.2		✓			
FCS_CKM.1					✓

TSF SFR	IDENTIFICATION & AUTHENTICATION	SECURITY AUDIT	TRAFFIC ANALYSIS	SECURITY MANAGEMENT	PROTECTION OF SECURITY FUNCTIONS
FCS_CKM.2					✓
FCS_CKM.4					✓
FCS_COP.1					✓
FIA_ATD.1	✓				
FIA_UID.2	✓				
FIA_UAU.2	✓				
FMT_MOF.1a				✓	
FMT_MOF.1b				✓	
FMT_MTD.1a				✓	
FMT_MTD.1b				✓	
FMT_MTD.1c				✓	
FMT_SMF.1				✓	
FMT_SMR.1				✓	
FPT_ITT.1					✓
FPT_RVM.1					✓
FPT_SEP.1					✓
FPT_STM.1		✓			
IDS_ANL.1 (EXP)			✓		
IDS_RCT.1 (EXP)			✓		
IDS_RDR.1 (EXP)			✓		
IDS_SDC.1 (EXP)			✓		

Table 17 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1(EXP)	Supported by the Security Audit function. The Security Audit function provides for the creation of records of different types of events. This directly fulfils this SFR.
FAU_SAR.1	Supported by the Security Audit function. The Security Audit function provides the Administrator the ability to review audit records in tabular form through the administrative interface.
FAU_SAR.2	Supported by the Security Audit function. The TOE is required to restrict the review of audit data to those granted with explicit read-access
FAU_SAR.3	Supported by the Security Audit function. The TOE is required to provide the administrator with the capability to sort of audit data
FAU_STG.1	Supported by the Security Audit function by preventing unauthorized modifications to audit records.
FAU_STG.2	Supported by the Security Audit function by protecting the audit data from deletion as well as guaranteeing the availability of the audit data in the event of storage exhaustion, failure or attack
FCS_CKM.1	Supported by Protection of Security Functions function. The TOE supports strong, standards-based methods for cryptographic key generation
FCS_CKM.2	Supported by Protection of Security Functions function. The TOE supports strong, standards-based methods for cryptographic key distribution.
FCS_CKM.4	Supported by Protection of Security Functions function. The TOE supports strong, standards-based methods for cryptographic key destruction.
FCS_COP.1	Supported by Protection of Security Functions function. The TOE supports strong, standards-based cryptographic methods for the following cryptographic operations: data encryption and decryption, digital signature generation and verification, random number generation, and cryptographic key agreement.
FIA_ATD.1	The Identification and Authentication and Security Management functions support this SFR by providing the capability to associate users with roles, which is configured by the administrator and is determined by the username of the user.
FIA_UID.2	Supported by the Identification and Authentication function. The Identification and Authentication function provides a secure login page to the AirDefense Management GUI and requires users to successfully authenticate before allowing them any access to the TOE. An authenticated user is also an identified user.
FIA_UAU.2	Supported by the Identification and Authentication function. The Identification and Authentication function provides a secure login page to the AirDefense Management GUI and requires users to successfully authenticate before allowing them any access to the TOE.

SFR	SF and Rationale
FMT_MOF.1a&b	Supported by the Security Management function. The Security Management function provides the ability for the Administrator to configure the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability. These features and capabilities provide control of the security functions enforced by the TOE.
FMT_MTD.1a,b,&c	The Security Management function restricts the ability to manage Audit storage threshold, Policy Definition for System data collection, analysis and reaction, and System Date and Time to the authorized Administrator. The TOE provides the ability for only the Admin, Manager and Network Operator roles to clear alarms.
FMT_SMF.1	Supported by the Security Management function. The Security Management function provides the ability for the Administrator to configure the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability. These features and capabilities provide control of the security functions enforced by the TOE.
FMT_SMR.1	Supported by the Security Management function. The Security Management function provides the Administrator role. This directly fulfils the FMT_SMF.1 requirement which specifies that the Administrator be able to configure the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability. Network Operator and Guest roles are also provided. Network Operator provides read-only management role privileges. No modification privileges are granted to the Network Operator role with the exception of the following: acknowledge, clear, and purge of alarms; create and save alarm filters. The Guest role is read-only with no application level modification privileges with the exception of create and save alarm filters. This directly fulfils the FMT_MTD.1 requirement which specifies the capabilities of the Administrator, Network Operator, and Guest roles.
FPT_ITT.1	The Protection of Security Functions function supports this SFR by protecting TSF data from modification when it is transmitted between separate parts of the TOE .
FPT_RVM.1	The Protection of Security Functions function supports this SFR by ensuring that all information traffic is subjected to the information process flow policy.
FPT_SEP.1	The Protection of Security Functions function supports this SFR by providing limited interfaces to reduce tampering from external sources. Additionally, all users (including authorized administrators) have to be authenticated prior to performing any actions on the TOE.
FPT_STM.1	The Security Audit function supports this SFR by using reliable timestamps for each audit and alarm generated within the TOE.

SFR	SF and Rationale
IDS_ANL.1 (EXP)	The Traffic Analysis function supports this SFR by utilizing the information process flow policy to monitor the data entering the TOE and analyze against Allowable Use Policies to determine a potential violation of the TSP.
IDS_RCT.1 (EXP)	The Traffic Analysis function supports this SFR by creating an alarm in the alarm manager on detection of a security violation.
IDS_RDR.1 (EXP)	The Traffic Analysis function supports this SFR by providing an Authorized Administrator with the capability to review all data collected and analyzed against Allowable Use Policies.
IDS_SDC.1 (EXP)	The Traffic Analysis function supports this SFR by utilizing the information process flow policy to monitor and process the data entering the TOE.

8.4 PP Claims Rationale

This Security Target does not claim conformance to any registered Protection Profile.

8.5 Rationale for Explicitly Stated Requirements

A family of IDS requirements was created to specifically address the data collected and analyzed by the TOE. The *Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006* was used as a basic model for creating these requirements, and these requirements may not follow the exact wording of what is stated in the Protection Profile.

The purpose of this family of requirements is to address the unique nature of the TOE data and provide requirements for collecting the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

Modeled after FAU_GEN.1 because the TOE does not audit on startup and shutdown functions.

8.6 Strength of Function Rationale

This security target includes one probabilistic or permutational function of a non-cryptographic nature. Relevant security functions and security functional requirements include:

- Identification and Authentication
    - FIA_UAU.2 – Authentication of Administrators

Part 1 of the CC defines “Strength of Function (SOF)” in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three Strength of Function levels defined in Part 1:

- SOF-basic
- SOF-medium
- SOF-high.

The claimed minimum strength of function for this Security Target is SOF-basic, which is defined in CC Part 1 section 2.3 as:

> A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST. The attributes chosen for inclusion in this ST were determined to be acceptable for SOF-basic and would adequately protect information in a Basic Robustness Environment.