AirDefense Guard Version 3.5 Security Target
July 29, 2005

AirDefense, Inc.
4800 North Point Parkway
Suite 100
Alpharetta, GA 30022
Phone: 770-663-8115
Fax: 770-453-9601

DOCUMENT INTRODUCTION

Prepared By:	Prepared For:
COACT, Inc.	AirDefense
9140 Guilford Road, Suite G	4800 North Point Parkway
Columbia, Maryland 21046-2587	Suite 100
	Alpharetta, GA 30022

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the AirDefense Guard Version 3.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
	July 31, 2003 Initial release.
1	September 22, 2003 Addressing initial ETR.
2	January 12, 2004 Addressing validator comments.
3	February 10, 2004 Addressing validator comments.
4	March 22, 2005 Addressing validator comments.
5	April 21, 2005 Addressing validator comments.
6	April 26, 2005 Addressing validator comments.
7	April 29, 2005 Addressing validator comments.
8	May 5, 2005 Addressing Validator comments.
9	May 13, 2005 Updating I&A and DoS info
10	May 16, 2005 Updating I&A for Sensor serial interface
11	May 26, 2005 Updated version of TOE
12	June 20, 2005 Final updates
13	July 13, 2005 SOF updates
14	July 29, 2005 Updated Figure 2

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC	Common Criteria
EAL2	Evaluation Assurance Level 2
IT	Information Technology
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the AirDefense Guard Version 3.5. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) and international interpretations through August 15, 2003. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the AirDefense Guard Version 3.5 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

AirDefense Guard Version 3.5 Security Target
Revision 14
July 29, 2005

1.1.2 TOE Reference

AirDefense Guard Version 3.5

Composed of the following components and their versions:

A) AirDefense Server 3.5.0.20 SM1

B) AirDefense Sensor 4.0.1.10

1.1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.1*.

1.1.4 Keywords

Wireless, Network, Security, Intrusion, Detection, IDS, WLAN, 802.11

1.2 TOE Overview

This Security Target defines the requirements for the AirDefense Guard Version 3.5. The TOE is an intrusion detection system for wireless networks. The TOE is designed to monitor the traffic received by wireless access points of a network. By monitoring this traffic, the TOE can detect denial of service attacks, identity theft, as well as violations of site-specific security policies.

1.2.1 Security Target Organisation

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

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

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

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

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

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the AirDefense Guard Version 3.5 to satisfy the security functional and assurance requirements.

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

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

1.3 Common Criteria Conformance

This Security Target is compliant with the functional requirements (Part 2) of the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9,* extended by FAU_GEN_EXP.1, and all National Information Assurance Partnership (NIAP) and international interpretations through August 15, 2003. This Security Target is compliant with assurance requirements (Part 3 of CC) for EAL2.

1.4 Protection Profile Conformance

The AirDefense Guard Version 3.5 does not claim conformance to any registered Protection Profile.

1.5 Document Conventions

The CC defines four operations on security functional requirements. The font conventions below identify the conventions for the operations defined by the CC.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***indicated with bold text and italics***

Iteration: indicated with typical CC requirement naming followed by a number in parenthesis for each iteration (e.g., FMT_MOF.1 (1))

CHAPTER 2

2. TOE Description

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

2.1 AirDefense Guard Version 3.5 TOE Description

The AirDefense Guard is an intrusion detection system for wireless networks. It is designed to monitor the traffic received by wireless access points of a network. By monitoring this traffic, the AirDefense Guard can detect denial of service attacks, identity thefts, as well as violations of site-specific security policies.

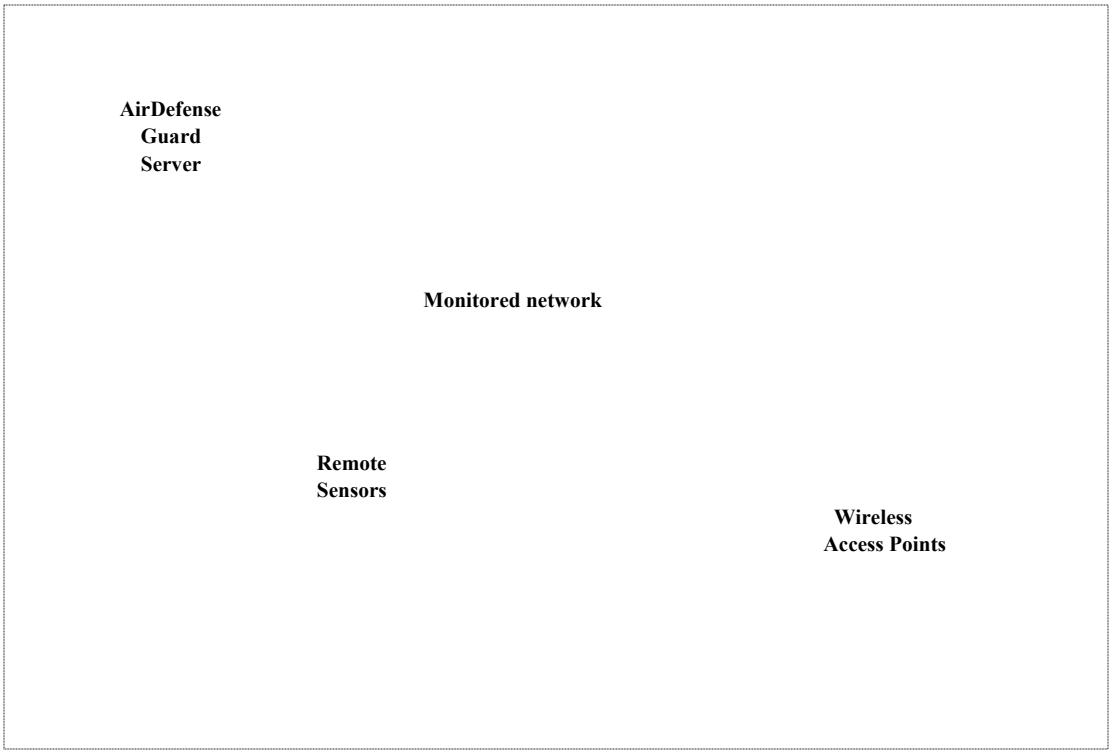
The AirDefense Guard is delivered as ready-to-use appliances. It consists of a Server and some number of Remote Sensors. The Server can support up to 500 Remote Sensors. The Server appliance is a dedicated computer running hardened Linux. The hardened Linux has all services disabled except those that are required to support the TOE, i.e. FTP and Telnet are disabled. The appliance is also running custom software that provides the interfaces and functionality for the Server portion of the TOE, this includes Open SSL for secure communications. The Server software receives all network traffic that is received by the hardware network interface, and provides a secure, web-based administration interface.

The Remote Sensors are also dedicated appliances running hardened Linux. Custom software is running on these appliances to provide the interfaces and functionality for the Remote Sensor portion of the TOE. The dedicated hardware device also has a wireless network adapter operating on the 802.11B standard.

Each Remote Sensor covers approximately 40,000 square feet. Remote Sensors should be installed on the monitored network in an attempt to cover the entire footprint of the network. This will help ensure that any wireless traffic received by access points on the network is also received by the TOE. When a Remote Sensor receives wireless traffic, the headers for the traffic are sent to the Server for processing. These communications are encrypted to protect their integrity. This encryption capability is built into the Remote Sensor and the Server appliances.

The following figure illustrates a network protected by the TOE. The Remote Sensors must be in proximity to the entire footprint of the monitored network, not just near wireless access points. This is due to the fact that a rogue access point can be added to the network anywhere along the footprint. Remote Sensors must also be able to connect to the Server via a network. They may use the monitored network for this purpose.

Figure 1 - Deployment Scenario of TOE



The Server processes the wireless traffic headers that each of its Remote Sensors sends to it to detect security threats. The TOE can detect denial of service (DoS) attacks, wireless identity thefts, and violations of site-specific security policies (Allowable Use Policies) that can be crafted by the site administrator.

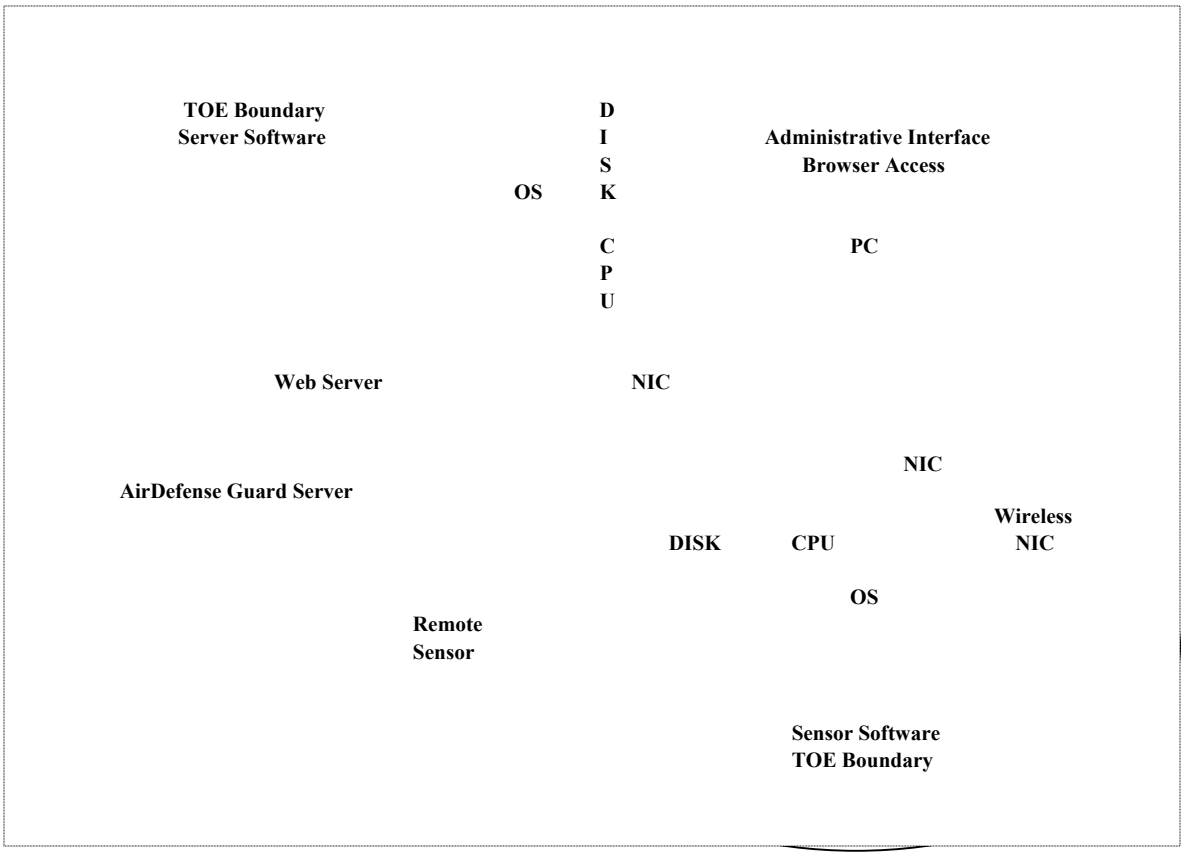
Users must log onto the Server to view security relevant information. The Server's interface traffic analysis, review of system audit events, and review of traffic audit events reflecting suspected security violations. This interface also allows the Administrator to craft the Allowable Use Policies. The TOE subsequently detects any wireless network use that does not match a policy. If the TOE detects illegal traffic, it will create an audit record for users to review.

The Administrator can create the Allowable Use Policies upon several attributes of the monitored traffic. These are wireless authentication mode, channel (wireless broadcast frequency), connection rate, Service Set Identifier (SSID) broadcast status, wireless protocol (e.g. WEP), authorized access points ID, host ID, date, and time of day.

2.1.1 Physical Boundary

The physical boundary of the TOE includes the Server software and the Remote Sensor software. Hardware is not included. A diagram of the TOE boundaries is provided in the following figure.

Figure 2 - Physical Boundary of TOE



The Server software provides the web-based administrative interface through a web server that is not part of the TOE. The server also provides a Command Line Interface (CLI) through a directly-attached keyboard and display. Additionally, the Server software communicates directly with the Network Interface Card (NIC), through the operating system, while receiving communications from the Remote Sensors.

The Sensor software provides a web-based administrative interface through an integrated web server. The Sensor software also provides a serial interface for management. 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).

2.1.2 Logical Boundary

The logical boundaries of the TOE are defined by the protection mechanisms provided by the TOE. These are summarized in the categories below.

2.1.2.1 Security Audit

The TOE generates audit records on standard system security events like start-up and shutdown. Additionally, events are generated when traffic analysis suggests that a denial of service attack, identity theft attack, or when traffic that doesn't match Allowable Use Policies is detected.

Users are also able to peruse audit events through the Server GUI and CLI interfaces.

2.1.2.2 Identification and Authentication

The user roles are Administrator, Network Operator, and Guest. The TOE requires the users to be authenticated before any access to the management interfaces is granted. Authentication requires a proper username and password combination.

The TOE performs the I&A function for the Server and Sensor GUI interfaces as well as the Sensor serial interface. The IT Environment (operating system) performs the I&A role for the Server CLI.

2.1.2.3 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 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 can use HTTP 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.

2.2 Evaluated Configuration

2.2.1 Remote Administration

Remote Administration, which permits SSH access to a Sensor over its Ethernet interface, is not enabled.

2.2.2 Encryption Mode

The Encryption Mode is set to On, which enables SSL for communication between sensors and the server.

2.2.3 Secondary Server

A Secondary Server is not included in the evaluated configuration.

CHAPTER 3

3. Security Environment

This chapter identifies the following:

A) IT related threats countered by the TOE and the environment.

B) Significant assumptions about the TOE's operational environment.

C) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies assumptions (A), threats countered by the TOE (T), threats countered by the operational environment (TE), and organisational security policies (P).

3.1 Threats

The threats identified in the following subsections are addressed by the TOE and IT environment, respectively. For the threats below, attackers are assumed to be of low attack potential.

3.1.1 Threats Addressed by the TOE

T.POLICY_VIO	An attacker gains unauthorized use of the network by broadcasting wireless network traffic in violation of the Allowable Use Policies, without being detected.
T.ID_THEFT	An attacker gains the privileges of a valid user by assuming the hardware identity of that user, without being detected.
T.DOS_ATTACK	An attacker denies the service of a wireless Access Point by flooding it with traffic, without being detected.
T.UNAUTH_ADMIN	An attacker gains administrative privileges to the TOE by accessing the TOE through its administrative interface.

3.1.2 Threats Addressed by the IT Environment

TE.TAMPER	Other processes on the hosting platforms interfere with the integrity of the TSF or TSF data.
TE.SENSR_DATA	An attacker compromises communications between a Remote Sensor and the Server.

3.2 Assumptions

Assumptions are ordered into three groups. They are personnel assumptions, physical environment assumptions, and IT environment assumptions. Personnel assumptions describe characteristics of personnel who are relevant to the TOE. Physical environment assumptions describe characteristics of the non-IT environment that the TOE is deployed in. IT environment assumptions describe the technology environment that the TOE is operating within.

3.2.1 Personnel Assumptions

A.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.
A.PLATFORM	The Administrator will ensure that the platforms used to host the TOE conform to the hardware and software outlined in the administrator guidance.
A.INSTALL	The Administrator will install and configure the AirDefense Guard Server and Remote Sensors according to the administrator guidance.
A.PASSWORD	Administrators will use passwords that conform to the administrator guidance, being at least five characters in length.
A.NETWORK	There will be a network that supports TCP communication connecting the Server to the Remote Sensors. This network functions properly.

3.2.2 Physical Environment Assumptions

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.COMPLETE	All wireless traffic that enters the monitored network is received by the TOE sensors.

3.2.3 IT Environment Assumptions

None

3.3 Organisational Security Policies

None

CHAPTER 4

4. Security Objectives

The objectives identified in the following subsections ensure that all the threats listed in Chapter three are addressed by the TOE and the operating environment, respectively.

4.1 Security Objectives of the TOE

O.DETECT	The TOE must detect traffic that is part of an identity theft, part of a DoS attack, or in violation of the Allowable Use Policies.
O.AUTHENTICATE	The TOE must require users of the Server and Sensor GUIs to authenticate in order to access the management interface.
O.AUDIT	The TOE must record and provide review of events of security relevance to the system and wireless traffic monitored by the system.
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.

4.2 Security Objectives of the Environment

The security objectives for the IT environment are listed below.

OE.NOTAMPER	The IT Environment will provide dedicated platforms to host the TOE and will forward network traffic to proper destinations.
OE.SENSR_DATA	The IT Environment must protect the communications between the Server and the Remote Sensors from disclosure and modification.
OE.TIMESTAMP	The IT Environment must provide a reliable timestamp for use by the TOE.
OE.PROTECT_AUDIT	The IT Environment must protect the record of events of security relevance to the system and wireless traffic monitored by the system from unauthorized deletion or modification.
OE.AUTHENTICATE	The IT Environment must require users of the Server CLI to authenticate in order to access the management interface.

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.

OE.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

OE.PLATFORM	The Administrator will ensure that the platforms used to host the TOE conform to the hardware and software outlined in the administrator guidance.
OE.INSTALL	The Administrator will install and configure the AirDefense Guard Server and Remote Sensors according to the administrator guidance.
OE.PASSWORD	Users will use passwords that conform to the guidance, being at least five characters in length.
OE.NETWORK	There will be a network that supports TCP communication connecting the Server to the Remote Sensors. This network functions properly.
OE.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.
OE.COMPLETE	All wireless traffic that enters the monitored network is received by the TOE sensors.

4.3 Rationale for IT Security Objectives

This section provides the rationale that all IT security objectives address threats against the TOE or the Environment.

O.DETECT	Addresses T.POLICY_VIO, T.ID_THEFT, and T.DOS_ATTACK. By requiring the TOE to detect traffic of each of these three attacks, the threat of these attacks occurring without detection is eliminated.
O.AUTHENTICATE	Addresses T.UNAUTH_ADMIN for users accessing the TOE via the Server and Sensor GUIs. By requiring users to authenticate before accessing the TOE, attackers without accounts cannot access the management interfaces of the TOE.
O.AUDIT	Addresses all threats countered by the TOE. 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 behaviour.
O.MANAGE	Addresses all threats countered by the TOE. 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.

The objectives below are levied on the environment.

OE.NOTAMPER	Addresses TE.TAMPER. By requiring the IT Environment to provide dedicated host platforms to support the TOE, the

	threat of other processes tampering with the TSF or TSF data is eliminated, as the only other processes are part of the OS.
OE.SENSR_DATA	Addresses TE.SENSR_DATA. By requiring the IT Environment to protect the communications between the Remote Sensors and the Server from disclosure and modification, the communications are protected from tampering.
OE.TIMESTAMP	This objective addresses all threats countered by the TOE. By providing the TOE with a reliable timestamp, OE.TIMESTAMP supports the TOE's auditing capabilities. Auditing is used by the TOE to counter all of its threats.
OE.PROTECT_AUDIT	Addresses all threats countered by the TOE. By requiring the IT Environment to protect the records of events of security relevance to the system and wireless traffic monitored by the system from unauthorized deletion or modification, the Administrator is able to detect malicious activity and verify proper system behavior.
OE.AUTHENTICATE	Addresses T.UNAUTH_ADMIN for users accessing the TOE via the Server CLI. By requiring users to authenticate before accessing the TOE, attackers without accounts cannot access the management interfaces of the TOE.

Table 1 - Mappings for IT Security Objectives to Threats and Assumptions

	T.POLICY_VIO	T.ID_THEFT	T.DOS_ATTACK	T.UNAUTH_ADMIN	TE.TAMPER	TE.SENSR_DATA
O.DETECT	X	X	X			
O.AUTHENTICATE				X		
O.AUDIT	X	X	X	X		
O.MANAGE	X	X	X	X		
OE.NOTAMPER					X	
OE.SENSR_DATA						X
OE.TIMESTAMP	X	X	X	X		
OE.PROTECT_AUDIT	X	X	X	X		
OE.AUTHENTICATE				X		

4.4 Rationale for Non-IT Security Objectives of the Environment

This section provides the rationale that all security objectives for the operating environment are traced back to aspects of the addressed threats, policies, or assumptions.

OE.NOEVILADMIN By requiring the Non-IT Environment to ensure that Administrators are non-hostile, competent, and follow the administrator guidance when using the TOE, the assumption A.NOEVILADMIN is addressed.

OE.PLATFORM By requiring the Non-IT Environment to ensure that the platform used to host the TOE conforms to the hardware and software outlined in the administrator guidance, the assumption A.PLATFORM is addressed.

OE.INSTALL By requiring the Non-IT Environment to ensure that the TOE is installed and configured in accordance with the administrator guidance, the assumption A.INSTALL is addressed.

OE.PASSWORD By requiring the Non-IT Environment to ensure that the Administrators will use passwords that conform to the administrator guidance, the assumption A.PASSWORD is addressed.

OE.NETWORK By requiring the Non-IT Environment to ensure that the network on which the server communicates with the sensors functions properly, the assumption A.NETWORK is addressed.

OE.ENVIRON 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, the assumption A.ENVIRON is addressed.

OE.COMPLETE By requiring the Non-IT Environment to ensure that all wireless traffic that enters the monitored network is received by the TOE sensors, the assumption A.COMPLETE is addressed.

Table 2 - Mappings for Assumptions to Security Objectives for the Environment

	A.NOEVILADMIN	A.PLATFORM	A.INSTALL	A.PASSWORD	A.NETWORK	A.ENVIRON	A.COMPLETE
OE.NOEVILADMIN	X						
OE.PLATFORM		X					
OE.INSTALL			X				
OE.PASSWORD				X			
OE.NETWORK					X		
OE.ENVIRON						X	
OE.COMPLETE							X

CHAPTER 5

5. IT Security Requirements

This section contains the security requirements that are relevant to the TOE. These requirements consist of functional components from Part 2 of the CC and assurance components from Part 3 of the CC.

This section also contains the TOE Strength of Function claim and rationale for all of components provided in this section.

Table 3 - Security Functional Requirements

Security Functional Requirements of the TOE	
FAU_GEN_EXP.1	Audit Data Generation
FAU_SAA.3	Simple Attack Heuristics
FAU_SAR.1	Audit Review
FAU_SEL.1	Selective Audit
FIA_UAU.2	User Authentication Before any Action
FIA_UID.2	User Identification Before any Action
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
Security Functional Requirements of the IT Environment	
FAU_STG.1	Protected Audit Trail Storage
FIA_UAU.2	User Authentication Before any Action
FIA_UID.2	User Identification Before any Action
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

5.1 Security Functional Requirements of the TOE

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN_EXP.1 Audit Data Generation (Explicitly Stated)

Hierarchical to: No other components.

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

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

b) **Wireless traffic packets received by the TOE**

FAU_GEN_EXP.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for the traffic events: host IP**

address, host MAC address, and the identity of the capturing Remote Sensor for wireless traffic received by the TOE.

Dependencies: FPT_STM.1 Reliable Time Stamps.

Rationale for explicitly stated SFR: The TOE is a set of applications that cannot ensure audit records for the start-up and shutdown of the audit functions. FAU_GEN_EXP.1 is derived from FAU_GEN.1 with the requirment for audit of start-up and shutdown deleted.

5.1.1.2 FAU_SAA.3 Simple Attack Heuristics

Hierarchical to: FAU_SAA.1 Potential Violation Analysis.

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events **denial of service attack, identity theft attack** that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of **date, time, host IP address, host MAC address, and the identity of the capturing Remote Sensor for wireless traffic received by the TOE.**

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Dependencies: No dependencies.

5.1.1.3 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **the 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.

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.4 FAU_SEL.1 Selective Audit

Hierarchical to: No other components.

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

a) host identity,

b) **Allowable Use Policies, which can be crafted by specifying appropriate values for the following attributes: 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, and time of day.**

Dependencies: FAU_GEN.1 Audit Data Generation,

FMT_MTD.1 Management of TSF Data.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 FIA_UAU.2(1) User Authentication Before any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication.

FIA_UAU.2.1(1) The TSF shall require each user ***of the Server and Sensor GUIs and the Sensor Serial Interface*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of Identification.

5.1.2.2 FIA_UID.2(1) User Identification Before any Action

Hierarchical to: FIA_UID.1 Timing of Identification.

FIA_UID.2.1(1) The TSF shall require each user ***of the Server and Sensor GUIs and the Sensor Serial Interface*** to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.1.3 Security Management (FMT)

5.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other components.

FMT_MOF.1.1(1) The TSF shall restrict the ability to determine the behaviour of the functions **Allowable Use Policies, Alarm Notification, Alarm Enablement, Alarm Priority, Sensor Operation, and Selective Audit** to **the Administrator, Network Operator, and Guest**.

FMT_MOF.1.1(2) The TSF shall restrict the ability to disable, enable, and modify the behaviour of the functions **Allowable Use Policies, Alarm Notification, Alarm Enablement, Alarm Priority, Sensor Operation, and Selective Audit** to **the Administrator**.

FMT_MOF.1.1(3) The TSF shall restrict the ability to determine the behaviour of, disable, enable, and modify the behaviour of the functions **Alarm Filtering** to **the Administrator, Network Operator, and Guest**.

Dependencies: FMT_SMR.1 Security Roles.

5.1.3.2 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1(1) The TSF shall restrict the ability to query the **Alarms** to **the Administrator, Network Operator, and Guest.**

FMT_MTD.1.1(2) The TSF shall restrict the ability to clear, **acknowledge**, and **purge** the **Alarms** to **the Administrator and Network Operator.**

FMT_MTD.1.1(3) The TSF shall restrict the ability to query the **Monitored WLAN Devices** to **the Administrator, Network Operator, and Guest.**

FMT_MTD.1.1(4) The TSF shall restrict the ability to modify, delete and **create** the **Monitored WLAN Devices** to **the Administrator.**

FMT_MTD.1.1(5) The TSF shall restrict the ability to query, modify, delete and **create** the **Users** to **the Administrator.**

FMT_MTD.1.1(6) The TSF shall restrict the ability to query the **authentication failure and alarm notification failure Audit Trail Records** to **the Administrator.**

FMT_MTD.1.1(7) The TSF shall restrict the ability to **backup** and **recover** the **Database** to **the Administrator.**

Dependencies: FMT_SMR.1 Security Roles.

5.1.3.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

a) **Allowable Use Policies**

b) **Alarm Notification**

c) **Alarm Enablement**

d) **Alarm Priority**

e) **Alarm Filtering**

f) **Sensor Operation**

g) **Selective Audit**

Dependencies: No dependencies.

5.1.3.4 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles: **Administrator, Network Operator, and Guest**.

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

Dependencies: FIA_UID.1 Timing of Identification.

5.2 Security Functional Requirements of the IT Environment

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

FAU_STG.1.1 The ***IT Environment*** shall protect the stored audit records in the audit trail from unauthorised deletion.

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

Dependencies: FAU_GEN.1 Audit Data Generation.

5.2.2 Identification and Authentication (FIA)

5.2.2.1 FIA_UAU.2(2) User Authentication Before any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication.

FIA_UAU.2.1(2) The ***IT Environment*** shall require each user ***of the Server CLI*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of Identification.

5.2.2.2 FIA_UID.2(2) User Identification Before any Action

Hierarchical to: FIA_UID.1 Timing of Identification.

FIA_UID.2.1(2) The ***IT Environment*** shall require each user ***of the Server CLI*** to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.2.3 Protection of the TSF (FPT)

5.2.3.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

Hierarchical to: No other components.

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

Dependencies: No dependencies.

5.2.3.2 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

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

Dependencies: No dependencies.

5.2.3.3 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

FPT_SEP.1.1 The ***IT Environment*** shall maintain a security domain for ***the TOE's*** own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ***IT Environment*** shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2.3.4 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

FPT_STM.1.1 The ***IT Environment*** shall be able to provide reliable time-stamps for ***the TOE's*** use.

Dependencies: No dependencies.

5.3 Security Assurance Requirements of the TOE

The TOE meets the assurance requirements for EAL2. These requirements are summarised in Table 1.

Table 4 - Assurance Requirements

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

5.4 Strength of Function Claim of the TOE

The claimed minimum strength of function for the TOE is SOF-basic.

The only probabilistic or permutational mechanism in the TOE is the password mechanism used to authenticate the users. The SFR that specifies this mechanism is FIA_UAU.2(1).

5.5 Rationale for Security Functional Requirements of the TOE

This section provides the rationale for mapping functional requirements to the security objectives of the TOE.

FAU_GEN_EXP.1	Supports O.AUDIT and O.DETECT. By requiring the TOE to produce audit records for basic level events O.AUDIT is supported. By requiring the TOE to record events of wireless traffic received by the TOE, the objective O.DETECT is supported, because event data is generated which can be analyzed to detect the stated attacks.
FAU_SAA.3	Supports O.DETECT. By requiring the TOE to analyze audit data to detect signatures of possible violations of the Allowable Use Policies, O.DETECT is met, because the attacks covered by O.DETECT will be discovered.
FAU_SAR.1	Supports O.AUDIT and O.DETECT. By requiring the TOE to provide audit trail review capabilities to the Administrator, the objectives O.AUDIT and O.DETECT are met, because a mechanism is provided for the Administrator to gain information about system functionality and threats.
FAU_SEL.1	Supports O.DETECT. By requiring the TOE to provide a configurable auditing mechanism, O.DETECT is met, because it requires the TOE to provide a mechanism that detects traffic that is not within specified Allowable Use Policies.
FIA_UAU.2(1)	Supports O.AUTHENTICATE. By preventing GUI and Sensor Serial Interface users from accessing any function of the TOE without being authenticated, the objective is met, because the objective requires authentication before access to the administrative interface is granted.
FIA_UID.2(1)	Supports O.AUTHENTICATE. By preventing GUI and Sensor Serial Interface users from accessing any function of the TOE without being identified, the objective is met, because the objective requires authentication (which implies identification as a valid username is required) before access to the administrative interface is granted.
FMT_MOF.1	Supports O.MANAGE. 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, this SFR supports the objective, because the objective requires the TOE to provide 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.
FMT_MTD.1	Supports O.MANAGE. By specifying that the Alarms, Monitored WLAN Devices, Users, Audit Trail Records, and Database can be managed by the Administrator, this SFR supports the objective, because these TSF Data support the allowable use policies, alarm

notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability.

FMT_SMF.1 Supports O.MANAGE. By specifying that the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability can be managed, the objective is met, because O.MANAGE requires the TOE to provide the ability for the administrator user to configure the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability.

FMT_SMR.1 Supports O.MANAGE. By specifying that the TSF shall maintain the Administrator role, the objective is supported, because O.MANAGE requires the Administrator be given the functionality to configure the allowable use policies, alarm notification, alarm enablement, alarm priority, alarm filtering, sensor operation, and selective audit capability.

Table 5 - Mappings Between Functional Requirements of the TOE and Objectives

	O.DETECT	O.AUTHENTICATE	O. AUDIT	O.MANAGE
FAU_GEN_EXP.1	X		X	
FAU_SAA.3	X			
FAU_SAR.1	X		X	
FAU_SEL.1	X			
FIA_UAU.2(1)		X		
FIA_UID.2(1)		X		
FMT_MOF.1				X
FMT_MTD.1				X
FMT_SMF.1				X
FMT_SMR.1				X

5.6 Rationale for Security Functional Requirements of the IT Environment

This section provides the rationale for mapping functional requirements to the security objectives of the IT environment.

FAU_STG.1 Supports OE.PROTECT_AUDIT. By requiring the IT Environment to protect and prevent unauthorized deletion or modification of the audit records, the objective is met, because it requires a complete audit trail to ensure comprehensive system coverage for there respective capabilities.

FIA_UAU.2(2) Supports OE.AUTHENTICATE. By preventing Server CLI users from accessing any function of the TOE without being

authenticated, the objective is met, because the objective requires authentication before access to the administrative interface is granted.

FIA_UID.2(2) — Supports OE.AUTHENTICATE. By preventing Server CLI users from accessing any function of the TOE without being identified, the objective is met, because the objective requires authentication (which implies identification as a valid username is required) before access to the administrative interface is granted.

FPT_ITT.1 — Supports OE.SENSR_DATA. By requiring the IT environment to prevent modifications to and disclosure of the communications between the Server and Remote Sensors, the objective to protect those communications is met.

FPT_RVM.1 — Supports OE.NOTAMPER. By requiring the IT Environment to ensure execution of the TSP enforcement functions before any functions of the TOE are instantiated, the IT environment provides conditions under which the TOE may invoke its own protections against bypass.

FPT_SEP.1 — Supports OE.NOTAMPER. By requiring the IT Environment to provide a separate domain of execution, it is assured that other processes will not interfere with the execution of the TSP, as required by the objective.

FPT_STM.1 — Supports OE.TIMESTAMP. By requiring the IT Environment to provide a reliable timestamp for the TOE's use the objective is met.

Table 6 - Mappings Between Functional Requirements of the IT Environment and Objectives

	OE.PROTECT_AUDIT	OE.NOTAMPER	OE.SENSR_DATA	OE.TIMESTAMP	OE.AUTHENTICE
FAU_STG.1	X				
FIA_UAU.2(2)					X
FIA_UID.2(2)					X
FPT_ITT.1			X		
FPT_RVM.1		X			
FPT_SEP.1		X			
FPT_STM.1				X	

5.7 Rationale for TOE Objectives Coverage

This section offers rationale that the objectives of the TOE are fully covered by SFRs that are mapped to them.

O.DETECT	Is satisfied by FAU_GEN_EXP.1, FAU_SAA.3, FAU_SAR.1, FAU_SEL.1, and FAU_STG.1. These satisfy this objective of detection, as FAU_GEN_EXP.1 requires the creation of audit records, FAU_STG.1 protects them, FAU_SEL.1 allows the Administrator to focus their collection, FAU_SAA.3 analyses them to detect attack patterns, and FAU_SAR.1 allows the Administrator to peruse them. Having a history of audit events is required to detect prolonged attacks, this history is provided by the FAU_GEN_EXP.1. Automatic detection is provided by FAU_SAA.3, and manual detection is provided by FAU_SAR.1. Finally, focusing audit collection with FAU_SEL.1 allows the Administrator to fine tune the above mechanisms of detection.
O.AUTHENTICATE	Is satisfied by FIA_UAU.2(1) and FIA_UID.2(1). These satisfy this objective of authentication, as FIA_UAU.2(1) requires the GUI and Sensor Serial Interface users to authenticate before allowing access to the TSF and FIA_UID.2(1), timing of identification, must be done before or at the time of authentication.
O.AUDIT	Is supported by FAU_GEN_EXP.1, FAU_SAR.1. These satisfy this objective of auditing, as FAU_GEN_EXP.1 requires the creation of audit records and FAU_SAR.1 allows the Administrator to peruse them.
O.MANAGE	Is supported by FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. These satisfy this objective of management, as FMT_MOF.1, FMT_MTD.1, and FMT_SMF.1 require the TOE to allow the administrator user to manage the selective audit capability as required by the objective. FMT_SMR.1 specifies the roles which are allowed to perform the management.

5.8 Rationale for IT Environment Objectives Coverage

This section offers rationale that the objectives of the IT Environment are fully covered by SFRs that are mapped to them.

OE.NOTAMPER	Is satisfied by FPT_RVM.1 and FPT_SEP.1. Being assured that the IT Environment will invoke the TSP enforcement functions before any functions of the TOE are instantiated and that the TOE has its own domain of execution fulfills the objective of having traffic forwarded to the proper destinations.
OE.SENSR_DATA	Is satisfied by FPT_ITT.1, because this SFR specifies the communications between parts of the TOE are protected from disclosure and modification, which is exactly what the objective requires.

OE.TIMESTAMP	Is satisfied by FPT_STM.1, because this SFR specifies a reliable timestamp is provided, which is exactly what the objective requires.
OE.PROTECT_AUDIT	Is satisfied by FAU_STG.1, because this SFR specifies that unauthorized deletion or modification to the audit records be prevented, which is exactly what the objective requires.
OE.AUTHENTICATE	Is satisfied by FIA_UAU.2(2) and FIA_UID.2(2). These satisfy this objective of authentication, as FIA_UAU.2(2) requires the Server CLI users to authenticate before allowing access to the TSF and FIA_UID.2(2), timing of identification, must be done before or at the time of authentication.

5.9 Rationale for Security Assurance Requirements of the TOE

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks (being considered of low potential) is not greater than moderate and the product will have undergone a search for obvious flaws.

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.

5.10 Rationale for Strength of Function Claim

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

5.11 Rationale for IT Security Requirement Dependencies

The following table lists the claimed TOE and IT Environment security requirements and their dependencies. This section also contains rationale for any dependencies that are not satisfied.

Table 7 - Functional Requirements Dependencies

SFR	Dependencies	Hierarchical To
FAU_GEN_EXP.1	FPT_STM.1	None
FAU_SAA.3	None	FAU_SAA.1
FAU_SAR.1	FAU_GEN.1	None

SFR	Dependencies	Hierarchical To
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	None
FAU_STG.1	FAU_GEN.1	None
FIA_UAU.2	FIA_UID.1	FIA_UAU.1
FIA_UID.2	None	FIA_UID.1
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	None
FMT_MTD.1	FMT_SMR.1	None
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	None
FPT_ITT.1	None	None
FPT_RVM.1	None	None
FPT_SEP.1	None	None
FPT_STM.1	None	None

FIA_UAU.2 and FMT_SMR.1 are dependent upon FIA_UID.1. FIA_UID.2 is hierarchical to FIA_UID.1; therefore this dependency is satisfied.

FAU_SAR.1, FAU_SEL.1, and FAU_STG.1 are dependent on FAU_GEN.1. This dependency is satisfied by FAU_GEN_EXP.1, which is derived from FAU_GEN.1 but excludes the requirement to audit start-up and shutdown of thr audit function.

5.12 Rationale for the Set of IT Security Requirements Providing a Mutually Supportive Whole

The security requirements of the IT Environment support the security requirements of the TOE to provide a mutually supportive whole by providing; protection of the audit trail (FAU_STG.1), protection of the transfer of internal TSF data (FPT_ITT.1), non-bypassability of the TSP (FPT_RVM.1), domain separation of the TSF (FPT_SEP.1), and reliable time stamps (FPT_STM.1), all of which provide the necessary support to the Security Audit, and Security Management requirements of the TOE.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Security Audit

The TOE generates two different categories of audit records. The first type is for system security events. Standard system security events include start-up, shutdown, changes in system IP configuration, and changes to the Allowable Use Policies.

The other category of audit events is traffic based. These event records describe wireless traffic that has been intercepted by the TOE. Record details include sufficient information to detect denial of service attacks and identity theft attacks. This includes the date, time, host IP address, host MAC address, and the identity of the capturing Remote Sensor.

The traffic records are analyzed for identity theft attacks and denial of service attacks. 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 denial of service attacks:

A) Denial of Service 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.

B) Denial of Service 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.

The TOE also provides a filtering mechanism to generate audit records. This mechanism evaluates traffic in real-time and determines if an audit record should be made of the suspicious traffic. These records would then include all of the data in the intercepted packets. The mechanism works from a set of Allowable Use Policies that are defined by the Administrator. These define acceptable wireless traffic for the network protected by the TOE. The attributes that can be used to define these policies 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.

For example, utilizing pull-down menus and text fields, the Administrator can define 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 audit record is generated.

No user can access the audit trail in any way if they are not authenticated with the administrative interface. Through the administrative interface the Administrator can review the audit trail in easy-to-read tables.

The Security Audit function of the AirDefense Guard meets the following SFRs:

A) FAU_GEN_EXP.1

B) FAU_SAA.3

C) FAU_SAR.1

D) FAU_SEL.1

6.1.2 Security Management

Three roles exist in the TOE: Administrator, Network Operator, and Guest. All three roles have the ability to view (query) all data via the Server and Sensor GUIs. Network Operators also have the ability to clear and purge alarms via the Server GUI.

The Administrator uses the administrative interfaces to manage the TSF. The administrative interfaces consist of both web-based applications that are served securely from a web-server, and CLI based applications that are served via secure shell (ssh) on the Server and via physical connection to the serial port on the Sensors.

Once authenticated, in addition to the auditing capabilities, the Administrator can manage the Allowable Use Policies that define the selective audit capability. This is supported by the administrative interface that supports creating, deleting, and modifying these policies. The Administrator can use HTTP 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.

These policies can be based on many important attributes of wireless 802.11B traffic. These include wireless authentication mode, channel (wireless broadcast frequency), connection rate, Service Set Identifier (SSID) broadcast status, and wireless protocol (e.g. WEP). Additionally, the following environmental and site-specific attributes can be specified: access point ID, host ID, date, and time of day.

Violation of the Allowable Use Policies by monitored WLAN devices will trigger alarms. The Administrator 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, the Administrator is capable of managing the operation of the Sensors which feed to the Server the observed network traffic. Specifically, this includes the ability to configure the wireless channel scanning pattern used by the Sensors and the address of the Server.

The Security Management function of the AirDefense Guard meets the following SFRs:

A) FMT_MOF.1

B) FMT_MTD.1

C) FMT_SMF.1

D) FMT_SMR.1

6.1.3 Identification and Authentication

The only way to access the TOE is by logging into the management interfaces. I&A is performed by the TOE for the following management interfaces: the Server web interface the Sensor web interface, and the Sensor Serial Interface.

The Server and Sensor web interfaces are provided from the Server and the Sensors through a web server over secure HTTP. The only page that is served without authentication and identification is the login page. The login page asks the user to enter a username and password. The username must be a valid administrator, and the password must be correct for the given username. Once successfully logged into the web administrative interface, the Administrator is both identified and authenticated.

The Sensor Serial Interface is provided only via physical connection to a sensor's serial port. The login prompt asks the user to enter a username and password. The username must be the dedicated userid for this interface, and the password must be correct for the dedicated userid. In accordance with A.ENVIRON, physical access to the serial interface is restricted to authorized personnel. Once successfully logged into the serial interface, the Administrator is able to change the network configuration of the Sensor.

The Identification and Authentication function of the AirDefense Guard meets the following SFRs:

A) FIA_UAU.2(1)

B) FIA_UID.2(1)

6.2 Assurance Measures

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.

The following table demonstrates the correspondence between the security assurance requirements listed in Chapter 5 to the developer evidence.

Table 8 - Assurance Correspondence

Component ID	Developer Evidence
ACM_CAP.2	AirDefense NIAP Configuration Management.doc
ADO_DEL.1	Operations Process.vsd
ADO_IGS.1	QuickStart_r3.5_i2.0.pdf AD_UserGuide_r3.5_7.0.pdf
ADV_FSP.1	AirDefense NIAP Functional Spec v12.doc AD_UserGuide_r3.5_7.0.pdf
ADV_HLD.1	AD_HL_DESIGN_v7.doc

Component ID	Developer Evidence
ADV_RCR.1	AirDefense NIAP Informal Correspondence Demonstration v32.doc
AGD_ADM.1	AD_UserGuide_r3.5_7.0.pdf
AGD_USR.1	AD_UserGuide_r3.5_7.0.pdf
ATE_COV.1	AirDefense NIAP Test Coverage.doc
ATE_FUN.1	User Role Test Plan 3.5.doc Sensor Manager Test Plan 3.5.doc Reports Test Plan 3.5.doc Policy Manager Test Plan 3.5.doc Notification Manager Test Plan 3.5.doc Dashboard Test Plan 3.5.doc Command Line Test Plan 3.5.doc Alarm Manager Test Plan 3.5.doc Alarm Detection Test Plan 3.5.doc Admin Manager Test Plan 3.5.doc Lab Configuration V3.5.doc
ATE_IND.2	NA
AVA_SOF.1	E2-0703-042 RTF AirDefense Guard Security Target v13.doc
AVA_VLA.1	AVA-VLA.1 AirDefense Vulnerability Assessment Document v2.1.doc

6.2.1 Rationale for Assurance Correspondence Mapping

The following section provides a rationale for each Assurance Correspondence mapping presented in Table 8.

ACM_CAP.2 — Component ACM_CAP.2 maps to Developer Evidence AirDefense NIAP Configuration Management.doc. This Developer Evidence clearly identifies the TOE and its associated configuration items, which satisfies component ACM_CAP.2.

ADO_DEL.1 — Component ADO_DEL.1 maps to Developer Evidence AirDefense Operations Process.vsd. This Developer Evidence describes the procedures used to maintain security of the TOE when distributing the TOE to the user's site, which satisfies component ADO_DEL.1.

ADO_IGS.1 — Component ADO_IGS.1 maps to Developer Evidence AirDefense QuickStart_r3.5_i1.2.pdf and AD_UserGuide_r3.5_7.0.pdf. This Developer Evidence describes the procedures and steps for the secure installation, generation, and start-up of the TOE, resulting in it's secure configuration, which satisfies component ADO_IGS.1.

ADV_FSP.1	Component ADV_FSP.1 maps to Developer Evidence AirDefense AirDefense NIAP Functional Spec v12.doc and AD_UserGuide_r3.5_7.0.pdf. This Developer Evidence provides an adequate description of the security functions of the TOE to determine whether the security functions provided by the TOE are sufficient to satisfy the security functional requirements of the ST, which satisfies component ADV_FSP.1.
ADV_HLD.1	Component ADV_HLD.1 maps to Developer Evidence AD_HL_DESIGN_v7.doc. This Developer Evidence provides a description of the TSF in terms of major structural units and is a correct realization of the functional specification, which satisfies component ADV_HLD.1.
ADV_RCR.1	Component ADV_RCR.1 maps to Developer Evidence AirDefense AirDefense NIAP Informal Correspondence Demonstration v32.doc. This Developer Evidence clearly identifies that the TOE has correctly and completely implemented the requirements of the ST and functional specification in the high-level design, which satisfies component ADV_RCR.1.
AGD_ADM.1	Component AGD_ADM.1 maps to Developer Evidence AD_UserGuide_r3.5_7.0.pdf. This Developer Evidence describes how to administer the TOE in a secure manner, which satisfies component AGD_ADM.1.
AGD_USR.1	Component AGD_USR.1 maps to Developer Evidence AirDefense AD_UserGuide_r3.5_7.0.pdf. This Developer Evidence provides instructions and guidelines for the secure use of the TOE, which satisfies component AGD_USR.1.
ATE_COV.1	Component ATE_COV.1 maps to Developer Evidence AirDefense AirDefense NIAP Test Coverage.doc. This Developer Evidence shows correspondence between the tests identified in the test documentation and the functional specification, which satisfies component ATE_COV.1.
ATE_FUN.1	Component ATE_FUN.1 maps to the Developer Evidence shown in Table 8. This Developer Evidence provides functional test documentation that is sufficient to demonstrate that security functions perform as specified, which satisfies component ATE_FUN.1.
ATE_IND.2	Component ATE_IND.2 maps to work performed by the CCTL. No additional developer evidence is required.
AVA_SOF.1	Component AVA_SOF.1 maps to Developer Evidence E2-0703-042 RTF AirDefense Guard Security Target v13.doc. Section 5.10 of this Developer Evidence clearly identifies the SOF claims and the analysis that supports them, which satisfies component AVA_SOF.1.

AVA_VLA.1	Component AVA_VLA.1 maps to Developer Evidence AVA-VLA.1 AirDefense Vulnerability Assessment Document v2.1.doc. This Developer Evidence describes exploitable obvious vulnerabilities of the TOE when deployed in its intended environment, which satisfies component AVA_VLA.1.

6.3 Rationale for TOE Security Functions

The following section provides a rationale showing how each Security Functional Requirement is supported by the security functions enforced by the TOE.

FAU_GEN_EXP.1	Is supported by the Security Audit function. The Security Audit function provides for the creation of records of different types of events. This directly fulfils FAU_GEN_EXP.1.
FAU_SAA.3	Is supported by the Security Audit function. The Security Audit function provides automatic analysis of the traffic audit records to detect denial of service attacks and identity theft attacks. This directly fulfils FAU_SAA.3.
FAU_SAR.1	Is 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. This directly fulfils FAU_SAR.1.
FAU_SEL.1	Is supported by the Security Audit function. The Security Audit function detects when wireless traffic does not meet one of the defined Allowable Use Policies. When this occurs, a full audit record is made with the traffic. This directly fulfils FAU_SEL.1.
FIA_UAU.2(1)	Is supported by the Identification and Authentication function. The Identification and Authentication function provides a secure login page to the management GUIs and Sensor Serial Interface, and requires users to successfully authenticate before allowing them any access to the TOE. This directly fulfils the FIA_UAU.2(1) requirement.
FIA_UID.2(1)	Is supported by the Identification and Authentication function. The Identification and Authentication function provides a secure login page to the management GUIs and Sensor Serial Interface , and requires users to successfully authenticate before allowing them any access to the TOE. An authenticated user is also an identified user. Therefore, this fulfils the FIA_UAU.2(1) requirement.
FMT_MOF.1	Is 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.1 Is supported by the Security Management function. The Security Management function provides the ability for the Administrator to manage the Alarms, Monitored WLAN Devices, Users, Audit Trail Records, and Database. This data directly supports the security functions enforced by the TOE.

FMT_SMF.1 Is 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 Is 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.

Table 9 - Mappings Between Functional Requirements and TOE Security Functions

	Security Audit	Security Management	Identification and Authentication
FAU_GEN_EXP.1	X		
FAU_SAA.3	X		
FAU_SAR.1	X		
FAU_SEL.1	X		
FIA_UAU.2(1)			X
FIA_UID.2(1)			X
FMT_MOF.1		X	
FMT_MTD.1		X	
FMT_SMF.1		X	

	Security Audit	Security Management	Identification and Authentication
FMT_SMR.1		X	

6.4 Rationale for Satisfaction of Strength of Function Claim

The claimed minimum strength of function is SOF-basic. The User's logon requirement, FIA_UAU.2(1), contains a permutational function requiring an SOF analysis. Therefore, an analysis is presented:

Password space for the Server and Sensor Graphical User Interfaces:

Only administrators can set passwords through the management interfaces. The password can contain upper and lower case letters and digits. This provides at least 62 distinct characters. Guidance directs the administrators to set the password to a minimum of 5 characters. Guidance also directs not using anything you would find in a dictionary, in any language or jargon, or any names or numbers that may be associated with the individual. Based on a typical high-speed Ethernet and experience with the brute-force attack engines, a conservative estimated transfer of 5,000 guesses can be made each second (0.0002 seconds/attempt). Therefore, the password space is calculated as follows (divided by two for average):

Password length: p = 5

Unique characters: c = 62

Seconds per attempt: s = 0.0002

Dictionary and other words and numbers: d = 20,000

Average length of successful attack in days =

= (s * c^p – d seconds) / (60 * 60 * 24 seconds per day) / 2

= (0.0002 * 62^5 – 20,000) / (60 * 60 * 24) / 2

= 1 day

Using the approach detailed in the CEM Part 2 Annex B, the values for "Identifying Value" and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (5) and Access to TOE (6) for a total of 11. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of 'Basic', resistant to an attack potential of 'low'.

Strength of Function for the Sensor Serial Interface:

The userid and password used for I&A on the Serial Interface are fixed and can't be changed by any users. However, access to the serial interface is restricted to authorized

users in accordance with A.ENVIRON. Therefore, even if the dedicated userid/password becomes known, the exploiting value for access to the TOE is not practical, and SOF-Basic is satisfied.

CHAPTER 7

7. Protection Profile Claims

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

7.1 Protection Profile Reference

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

7.2 Protection Profile Refinements

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

7.3 Protection Profile Additions

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

7.4 Protection Profile Rationale

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

CHAPTER 8

8. Rationale

This chapter provides rationale or references to rationale required for this Security Target.

8.1 Security Objectives Rationale

Sections 4.3 - 4.4 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.5 - 5.11 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 – 6.4 provide the TSS rationale.

8.4 Protection Profile Claims Rationale

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