National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme Validation Report

AirDefense Guard Version 3.5

Report Number: CCEVS-VR-05-0109

Dated: 29 July 2005

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Royal Purvis
Mitretek Systems
Falls Church, Virginia

Elizabeth Foreman
Mitretek Systems
Falls Church, Virginia

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

Table of Figures

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the AirDefense Guard, Version 3.5 at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 13 July 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

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, e.g. 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.

As with any other wireless device the coverage range of each Remote Sensor depends upon the physical environment in which it is placed. In a location without physical interference, each Remote Sensor covers approximately 40,000 square feet. Remote Sensors should be installed on the monitored network in a configuration that covers 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 needed to address the threat of an 802.11B rogue access point being 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.

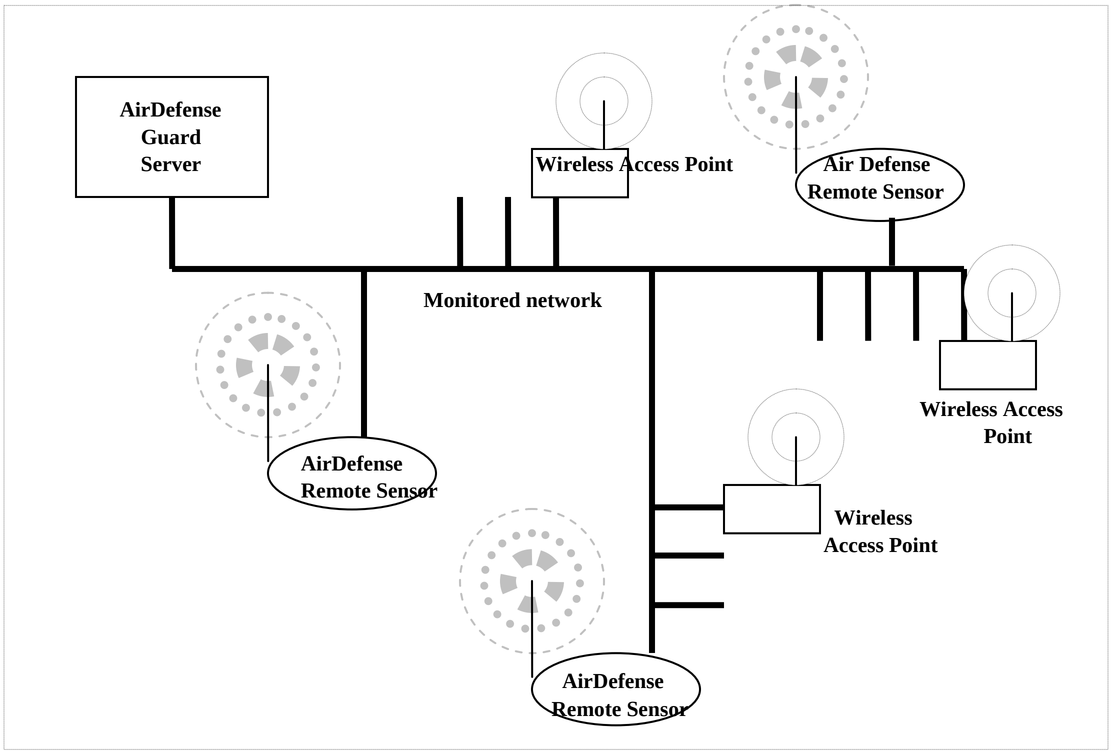

Figure 1: Typical Deployment Scenario

The Server processes the wireless traffic headers that each of its remote AirDefense 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 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- the organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Evaluation Identifiers for AirDefense Guard, Version 3.5	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	AirDefense Guard Version 3.5
Protection Profile	N/A
Security Target	AirDefense Guard Version 3.5 Security Target, Revision 14 dated July 29, 2005
Evaluation Technical Report	AirDefense Guard Version 3.5 Evaluation Technical Report, Document No. E2-0605-005(2), Dated July 29, 2005
Conformance Result	Part 2 conformant and EAL2 Part 3 conformant
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on August 15, 2003.
Version of CEM	CEM Version 1.0 [5], [6], and all applicable NIAP and International Interpretations effective on August 15, 2003
Sponsor	AirDefense 4800 Northpoint Parkway Suite 100 Alpharetta, GA 30022

Evaluation Identifiers for AirDefense Guard, Version 3.5	
Developer	AirDefense 4800 Northpoint Parkway Suite 100 Alpharetta, GA 30022
Evaluator(s)	**COACT Incorporated** Bob West Anthony Busciglio Brian Pleffner Tom Benkart
Validator(s)	**NIAP CCEVS** Dr. Jerome Myers Royal Purvis Elizabeth Foreman

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation began on August 15, 2003.

NIAP Interpretations

I-0405 – American English Is An Acceptable Refinement

I-0422 – Clarification Of ``Audit Records"

I-0423 – Some Modifications To The Audit Trail Are Authorized

I-0427 – Identification Of Standards

International Interpretations

RI#003 – Unique identification of configuration items in the configuration list (11 February 2002)

RI#008 – Augmented and Conformant overlap (31 July 2001)

RI#016 – Objective for ADO_DEL (11 February 2002)

RI#019 – Assurance Iterations (11 February 2002)

RI#031 – Obvious vulnerabilities (25 October 2002)

RI#049 – Threats met by environment (16 February 2001)

RI#064 – Apparent higher standard for explicitly stated requirements (16 February 2001)

RI#065 – No component to call out security function management (31 July 2001)

RI#075 – Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1 (15 October 2000)

RI#084 – Aspects of objectives in TOE and environment (31 July 2001)

RI#085 – SOF Claims additional to the overall claim (11 February 2002)

RI#116 – Indistinguishable work units for ADO_DEL (31 July 2001)

RI#127 – Work unit not at the right place (25 October 2002)

3 Security Policy

The TOE does not implement any security policies in the traditional sense of access control policies. However, the TOE implements several security policies associated with its use as an Intrusion Detection System for wireless networks. Those policies deal with restrictions on the persons that may administer the TOE and access the information collected by the TOE. More specifically, the TOE implements an Identification and Authentication Policy and an Audit Policy.

3.1 Identification and Authentication Policy

The user roles are Administrator, Network Operator, and Guest. The TOE requires users be authenticated before any access to the management interfaces is granted. Authentication requires a proper username and password combination. The TOE implements the I&A policy for the Server and Sensor GUI interfaces and for the Sensor serial interface. The IT Environment (underlying Linux operating system) performs the I&A role for the Server CLI.

3.2 Security Audit Policy

The TOE implements a policy for the generation of audit records. The TOE generates audit records on standard system security events including start-up and shutdown. Additional audit events are generated when traffic analysis suggests a denial of service attack, an identity theft attack, or when traffic is detected that doesn’t match an administratively configured “Allowable Use Policy”.

The configurable “Allowable Use Policies” are specified in terms of the communications attributes of the wireless authentication mode, the wireless channel, the connection rate, the Service Set Identifier (SSID) broadcast status, the wireless protocol (e.g. WEP), the access point ID, the host (client) ID, date, and time of day.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The evaluation made the following assumption concerning product usage:

- Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.
- The Administrator will ensure that the platforms used to host the TOE conform to the hardware and software outlined in the administrator guidance.
- The Administrator will install and configure the AirDefense Guard Server and Remote Sensors according to the administrator guidance.
- Administrators will use passwords that conform to the administrator guidance, being at least five characters in length.
- There will be a network that supports TCP communication connecting the Server to the Remote Sensors. This network functions properly.
- The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware.
- All wireless traffic that enters the monitored network is received by the TOE sensors.

4.2 Clarification of Scope

The AirDefense Sensor appliance has a capability that permits SSH access over its Ethernet interface for some administrative access. This interface is disabled in the evaluated configuration.

The AirDefense product supports the installation of a “Secondary Server”. This use of this capability is not included in the evaluated configuration.

The TOE is an Intrusion Detection System for specific types of wireless networks. The TOE was only evaluated for wireless networks that exclusively use the 802.11b protocol. The TOE does not claim to detect nor analyze traffic that uses any of the other commonly available wireless protocols, in particular, 802.11g and 802.11a. The vendor has asserted that the TOE has some capabilities for the detection of other protocols. However, those capabilities were not included within the scope of this evaluation. Although this limits any statements that can be made in this report about the effectiveness of the TOE at detecting an unauthorized installation of an 802.11g or 802.11a access point on the network, it does not alter the effectiveness of the TOE at detecting rogue access points that implement 802.11b.

The TOE boundary does not include the underlying hardware, operating systems, firewall applications, web services, and the SQL DBMS that are needed by the TOE.

These items are components of the IT Environment that are delivered and installed with the TOE. The TOE vulnerability analysis included some analysis of obvious vulnerabilities of these IT Environment components by non-administrators on the wired side of the network. However, that vulnerability analysis does not constitute a full vulnerability analysis of those IT Environment components.

5 Architectural Information

The TOE is comprised of one AirDefense Server and one or more AirDefense Sensors. The TOE component that resides on the Server is a software application that is further subdivided into thirteen subsystems that present external interfaces to the IT Environment. The TOE component that resides on the sensor consists of a single software subsystem. The overall architecture of the TOE is illustrated in Figure 3: TOE Boundary on page 15. AirDefense Sensors communicate with the AirDefense Server using SSL. The specifics of the architectural decomposition are proprietary to the vendor and will not be further described in this report. However, Figure 1 illustrates the relationship with the key components of the IT Environment that are not considered to be part of the evaluated TOE. In particular, it shows that the underlying hardened Linux Operating Systems are relied upon to protect the TOE from inappropriate access. Although not explicitly shown in the diagram, this dependence utilizes standard Linux firewall capabilities. In addition, the Web Server that is shown for providing administrative access to some of the TOE data is shown as residing in the IT Environment. One additional component of the IT Environment is the SQL DBMS that also resides on the server. Audit records and other records of network activity are maintained as SQL records.

6 Delivery and Documentation

There are two AirDefense products that are associated with the TOE: The AirDefense Guard Version 3.5.0.20SM1 and the AirDefense Sensor Version 4.0.1.10. The evaluated version of the AirDefense server software application is preinstalled on a hardware server platform that is shipped with the AirDefense Guard Version 3.5.0.20 SM1. The AirDefense Guard is always delivered with at least one AirDefense Server and one AirDefense Sensor. The evaluated version of the AirDefense sensor software application is preinstalled on the hardware platform that is shipped with each AirDefense Sensor Version 4.0.1.10. The evaluated configuration only requires one Server and enough (up to 500, but possibly only one) Sensors to cover all potential locations for the placement of access points. Additional AirDefense Sensors may be separately purchased.

Both components of the TOE are software products that come preinstalled as network appliances that include most of the necessary hardware and software to install and use the TOE in its evaluated configuration. The TOE delivery does not include the backbone network, the terminals for serial port communications with the AirDefense Sensor or Server, and network workstations from which administrators might communicate with the TOE over the backbone network.

In addition to the TOE components on their respective IT Environment platforms, the delivery includes the following two hard copy documents:

- AirDefense User Guide Release 3.5 Issue 7.0
- AirDefense Quick Start Release 3.5 Issue 2.0

If additional AirDefense Sensors are purchased separately from the initial acquisition of an AirDefense Server, then the version of the sensor that must be used to meet the constraints of this evaluation is Version 4.0.1.10. This product is delivered in a similar manner to the original AirDefense Guard components. Namely, it is a network appliance that includes the sensor component of the TOE preinstalled on a hardware and software platform. However, no additional documentation is shipped with the AirDefense Sensor.

7 IT Product Testing

7.1 Developer Testing

The developer maintains a suite of tests for confirming that the product meets its advertised functional requirements. Testing was performed by the developer at facilities in Atlanta, GA.

The basic test configuration for the evaluated configuration is illustrated in Figure 2: Test Configuration. The test configuration included several major components, a network (represented by PCs and switches) monitored by the TOE, the AirDefense TOE (Server and Sensor) installed on their respective devices, and a keyboard and monitor attached to the AirDefense Server to act as a management console. A wired workstation was configured on the network for TOE administration and another workstation was configured on the network with port scanning software, network sniffing software, and an HTTP flooder. The network was configured with multiple wireless access points and wireless workstations. Testing was performed in a mixed environment with several brands and models of 802.11b access points and several 802.11b enabled client workstations.

The following figure graphically displays the test configuration used for functional and penetration testing. This setup was also used for the evaluation team independent and penetration testing.

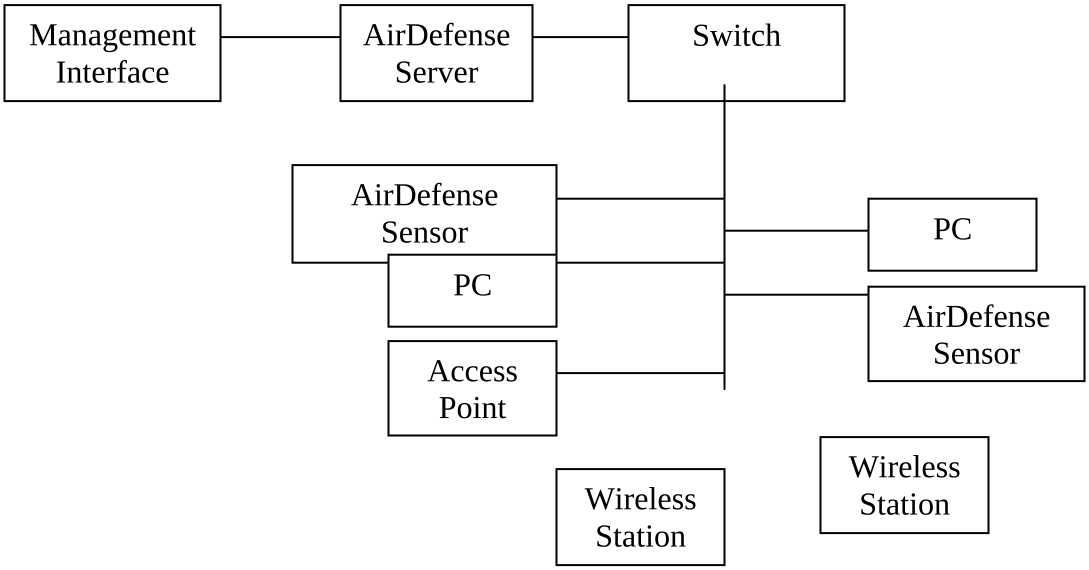

Figure 2: Test Configuration

Test documentation including test plans, test procedures, a description of the test configuration, test coverage documentation, expected test results, and actual test results were provided to the CCTL for review. The developers test documentation was provided in a suite of.eleven documents with the following titles:

AirDefense User Role Test Plan v.3.5;
AirDefense Sensor Manager Test Plan v.3.5;
AirDefense Reports Test Plan v.3.5;
AirDefense Policy Manager Test Plan v.3.5;
AirDefense Notification Manager Test Plan v.3.5;
AirDefense Dashboard Test Plan v.3.5;
AirDefense Command Line Test Plan v.3.5;
AirDefense Alarm Manager Test Plan v.3.5;
AirDefense Alarm Detection Test Plan v.3.5;
AirDefense Admin Manager Test Plan v.3.5;
Lab Configuration V3.5

The first ten documents detail the testing of the system and the “Lab Configuration” provided a detailed listing with software versions and platform identifiers for all test equipment and instructions for proper configuration of the test network.

The evaluators reviewed the developers tests and test results to ensure that the developers testing and test results were appropriate for the evaluated configuration. An evaluation team review of all of the security functions and the mapping between security functions and tests confirmed that security functions were appropriately tested by the developer tests. The combined suite of test documentation provided direct test coverage for all but one of the SFRs. The only SFR that was not explicitly covered by the vendor test suite was the explicitly stated requirement, FAU_GEN_EXP.1 which modified FAU_GEN.1 to incorporate wireless packet auditing. The evaluators included additional testing of that SFR in their independent testing.

7.2 Evaluator Testing

Evaluation team testing was conducted on June 13, 2005 at the AirDefense facility in Atlanta, Georgia. The evaluation team performed the following activities during testing:

1. Installation of the TOE
2. Execution of a subset of the developer's functional tests
3. Independent Testing
4. Vulnerability Testing (AVA_VLA.1)

The evaluation team selected a subset of the developer test to repeat and the evaluators also developed some additional tests to separately test some of the functionality. The evaluation team testing was performed on a similar configuration to that used by the system developers, (see Figure 2: Test Configuration on page 5.) There were three simplified versions of the configuration that were used for penetration testing.

A vendor representative was available to facilitate some of the testing. The role of the vendor representative was to facilitate the resolution of any apparent discrepancies between the evaluator's test results and the expected test results. There were no discrepancies noted

The evaluation team's independent testing included some variants of the original vendor tests with modified parameters and also some tests specifically constructed to further test FAU_GEN_EXP.1. The results of the evaluation teams functional and independent testing is documented in the AirDefense and COACT proprietary document, E2-0505-0019(1) AirDefense Functional Testing Report. The subset of the developer tests that the evaluators repeated constituted approximately 20% of the developer tests. Those tests were selected in a manner that included tests for each of the SFRs and from 8 of the 9 separate vendor test plan documents

Finally, the evaluators performed an analysis of the vendor hypothesized vulnerabilities and associated tests. The evaluators determined that the vendor had done an appropriate vulnerability analysis and associated testing. As a result, there were only a few potential vulnerabilities tested by the evaluators.

One aspect of the vulnerability testing that the evaluators gave special attention was the IT Environment. Since the TOE is delivered with hardware platforms, operating systems, and some applications (in particular the firewall features of Linux and the Web server) that protect the TOE from the wired network, standard network attack and vulnerability analysis tools were used to confirm that the TOE was not subject to any obvious attacks from the wired network side by non-administrative users of the wired network. Similar analysis and testing were separately performed by the developers and by the evaluators. The results of the evaluation teams vulnerability testing is documented in the AirDefense and COACT proprietary document, E2-0505-0018(3) AirDefense Penetration Testing Report.

The end result of the testing activities was that all tests gave expected (correct) results. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities.

The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

8 Evaluated Configuration

8.1 TOE

This section documents the configuration of the IT product during the evaluation. The TOE covers configurations with one AirDefense Guard Server and one or more (up to 500) AirDefense Sensors.

8.1.1 Physical Boundary of TOE

The TOE consists of two software components - one of which resides in each AirDefense Remote Sensor and the other resides in the AirDefense Server. The physical boundary of the TOE is illustrated in Figure 3: TOE Boundary. The figure illustrates key aspects of the hardware and software that are outside of the scope of the TOE boundary as well as showing that the TOE is confined within the hardware that is acquired with the TOE.

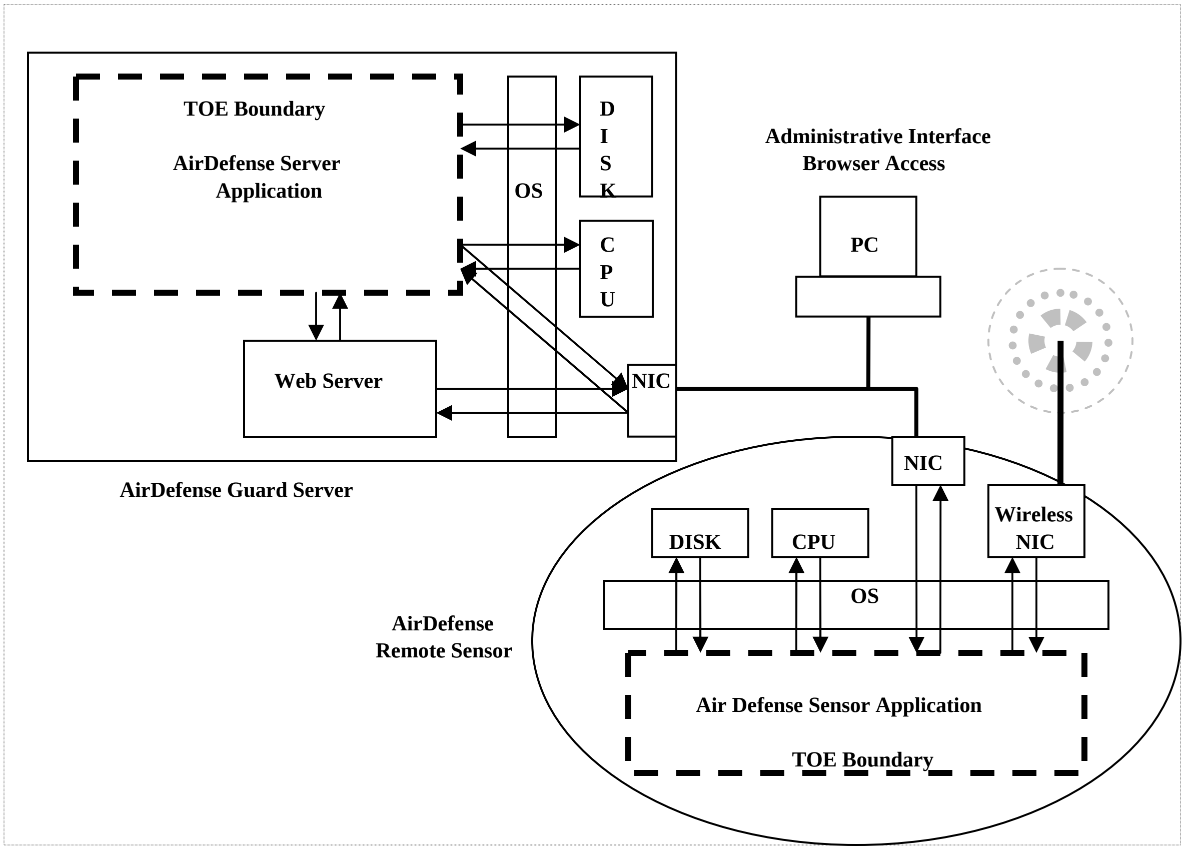

Figure 3: TOE Boundary

8.1.2 Logical Boundary of TOE

The logical boundary of the TOE is the defined by the security mechanisms that the TOE provides. The ST defines those mechanisms as:

> **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.
>
> **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.

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.

8.1.3 Platform for TOE

The underlying hardware and software platforms for the TOE are part of the IT Environment, but they are included in the appliance products that one must purchase to obtain the TOE. Hence there is no other special equipment that one must separately acquire to install the TOE in its evaluated configuration on an existing network that uses 802.11B devices for wireless access. The underlying platform for the AirDefense server includes the following:

Hardware box with network interface
Hardened Linux based OS
Firewall Application
Web Server
SQL DBMS

The underlying platform for the AirDefense Sensor includes the following:

Hardware box with network interface and radio for monitoring 802.11B
Hardened Linux based OS
Firewall Application

8.1.4 IT Environment of TOE

The IT Environment for the TOE is illustrated in Figure 1: Typical Deployment Scenario on page 5 and in Figure 3: TOE Boundary on page 15. There are two components to the IT Environment – the basic network that the TOE is designed to operate within and the base hardware and software platforms upon which the TOE operates. As was noted in the previous section of this report, the base network is assumed to have a wired Ethernet backbone and access points that comply with the 802.11B standard. The hardware and software platforms that host the TOE are part of the appliances that are delivered with the TOE and are further described in the previous section.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.1 and CEM, Version 1.0.,

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document *AirDefense Guard Version 3.5 Evaluation Technical Report, Document No. E2-0605-005(2), Dated July 29, 2005 [9]* contain the verdicts of "PASS" for all the work units.

The evaluation determined the product to be Part 2 compliant, as well, meeting the requirements for Part 3, and EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10 Validator Comments

The "Clarification of Scope" section (page 4) of this report noted that the evaluated configuration for the TOE requires the use of hardware and software in the IT environment that is included in the product distribution but is not included within the scope of this evaluation. Although this is the case, it should also be noted that some vulnerability analysis was performed on those components of the IT environment. In particular, the network interfaces to the base platforms that host the server and sensor were scanned for obvious vulnerabilities from the general user side of the network. Since only authorized administrators are permitted to access the server and sensor hosts, the network interface vulnerability analysis is sufficient to significantly limit the risk of vulnerabilities within the IT environment impacting the security functionality of the TOE or otherwise introducing vulnerabilities into the overall network.

Another limitation in the scope was the restriction to 802.11b networks. The product developer claims that the product has some capabilities to sense 802.11g network activity as well. However, the 802.11g functionality was not explicitly described in the Security Target and hence not tested. The primary differences between the AirDefense Guard capabilities for 802.11b and 802.11g or 802.11a are in the radios that reside in the AirDefense sensors. There are also some minor differences in the channel allocation that would impact the interface for an 802.11a radio. When 802.11g or 802.11a capabilities are enabled on the sensor radios it should be fairly simple to update the evaluation evidence to incorporate those capabilities.

11 Security Target

The Security Target, "AirDefense Guard Version 3.5 Security Target, Revision 14 dated July 29,2005" [9] is included here by reference.

12 Glossary

12.1 Definition of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DBMS	Database Management System
DLL	Dynamically Linked Library
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HTTP	Hypertext Transport Protocol
I&A	Identification and Authentication
IT	Information Technology
NIAP	National Information Assurance Program
NIC	Network Interface Card
NIST	National Institute of Science & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
WEP	Wired Equivalent Privacy

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[8] Common Criteria Evaluation and Validation Scheme for Information Technology Security Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, February 2002

[9] AirDefense Guard Version 3.5 Evaluation Technical Report , Document No. E2-0605-005(2), Dated July 29, 2005

[10] AirDefense Guard Version 3.5 Security Target, Revision 14 dated July 29, 2005

[11] AirDefense User Guide Release 3.5 Issue 7.0

[12] AirDefense Quick Start Release 3.5 Issue 2.0