National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

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

Report Number: CCEVS-VR-07-0033
Dated: June 8, 2007
Version: Version 1.0

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

Table of Contents

Table of figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the. product SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0], a product of AirTight Networks, Inc, Mountain View, CA.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

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

The Enterprise Server (including Sensors) and SpectraGuard SAFE Enterprise Edition (Security Agent For Endpoints) can be used independently. SAFE is an additional component that can be installed on mobile devices to provide further protection. It monitors and mitigates wireless threats and mis-configurations that may pose a security threat to the data on the mobile computer. SAFE Enterprise Edition integrates with SpectraGuard Enterprise and allows all the SpectraGuard SAFE Enterprise Edition users to be managed centrally on the SpectraGuard Enterprise Server.

The SpectraGuard Enterprise solution includes:

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

Aspects of the following security functions are controlled / provided by the TOE in conjunction with its information technology (IT) environment:

- Identification and Authentication
- Security Audits;
- Information Flow Control;
- Scan managed devices
- Security management

The following are explicitly excluded from the TOE configuration, but are included in its IT environment:

- Third Party Software that the TOE relies upon
- Hardware platforms and Operating Systems;
- Third party core and rollup relational databases;
- Transport standards HTTPS (using SSL/TLS) implementation
- SSH implementation and any other data encryption mechanism
- Web servers and browsers including the hardware hosts;
- Wireless Access Points

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during March 2006. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.3 [CC] Part 2 and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.3, [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap.ccevs.org. The Security Target (ST) is contained within the document Security Target for SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0] [ST]. The ST has been shown to be compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of CC.

2. Identification

Target of Evaluation:	SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE Enterprise Edition [v 2.0]
Evaluated Software:	SpectraGuard Enterprise [v 5.0] and SpectraGuard Sensors Build 5.0.56 SpectraGuard SAFE Enterprise Edition [v 2.0] Build 2.0.27
Developer:	AirTight Networks, Inc 339 N. Bernardo Avenue, Suite #200 Mountain View, CA 94043
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive

	McLean, VA 22102-3305
Evaluator	Debra Baker, Cygnacom Solutions
Validation Scheme:	National Information Assurance Partnership CCEVS
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

- **Information Flow Control**

The TOE enforces the information flow control policy by granting or denying access to the protected network based upon the information flow policy defined by an authorized administrator. The Sensor component will attempt to disrupt and block unauthorized information flows between the clients and access points by broadcasting DEAUTHENTICATE packets. When the SAFE component is installed on a client, the client is only allowed to connect to authorized access points.

- **Identification and authentication**

The Server component requires that administrators be properly identified and authenticated prior to performing any administrative tasks on the system. The SAFE component relies on the underlying OS for identification and authentication.

- **Security Audit**

The Server and SAFE components generate audit records for administrative actions and relevant events. An authorized administrator can review the audit data in a tabularized text format. Additionally, authorized administrators can review the reports of the SAFE clients through the Server's management console.

- **Security Management**

The Server component provides a web-based interface to manage the configuration of the server. The SAFE component users are managed centrally on the Server through its web-based interface. Authorized administrators are able to create, modify, and view the information flow security policy rules and manage the TOE.

- **Partial Protection of the TSF**

The Server, Sensor, and SAFE components work together with their IT environments to protect their programs and data from unauthorized access.

A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

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

Note: * denotes iterated component.

IT Environment Security Functional Requirements

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

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- It is assumed that TOE components are stored in a secure physical location to prevent unauthorized physical modification.
- Only trusted, knowledgeable, and authorized administrators will be able to manage, configure, operate, and access TOE, database and the underlying operating system according to the TOE documentation.
- No untrusted users will access the TOE or no untrusted software or data will reside on the TOE.
- TOE depends on the underlying operating system for a reliable time stamps.
- It is assumed that users will protect their authentication data.
- It is assumed that there is the capability to hash and store user passwords.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL2 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. TOE depends on IT environment for the following:
    a. to provide the capability to protect audit information.

b. to provide assured client identification and authentication of users prior to allowing access to IT environment functions and data.
c. to ensure that the IT environment's security functional policy is invoked and succeeds before allowing another IT environment function to proceed.
d. to maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
e. to protect TSF data when transferred between TOE Components.
f. to provide reliable time stamps.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The TOE consists of the following components:

- SpectraGuard Enterprise(comprised of Server, Sensors and the Management Console) v5.0
- SpectraGuard SAFE Enterprise Edition v2.0

All data and control information that is exchanged between the TOE's Server, Sensor, and SAFE components is done using a proprietary protocol. The protocol uses UDP and TCP for the transport layer (port 3851 on both sides) and encrypts information using the AES (128 bit) algorithm.

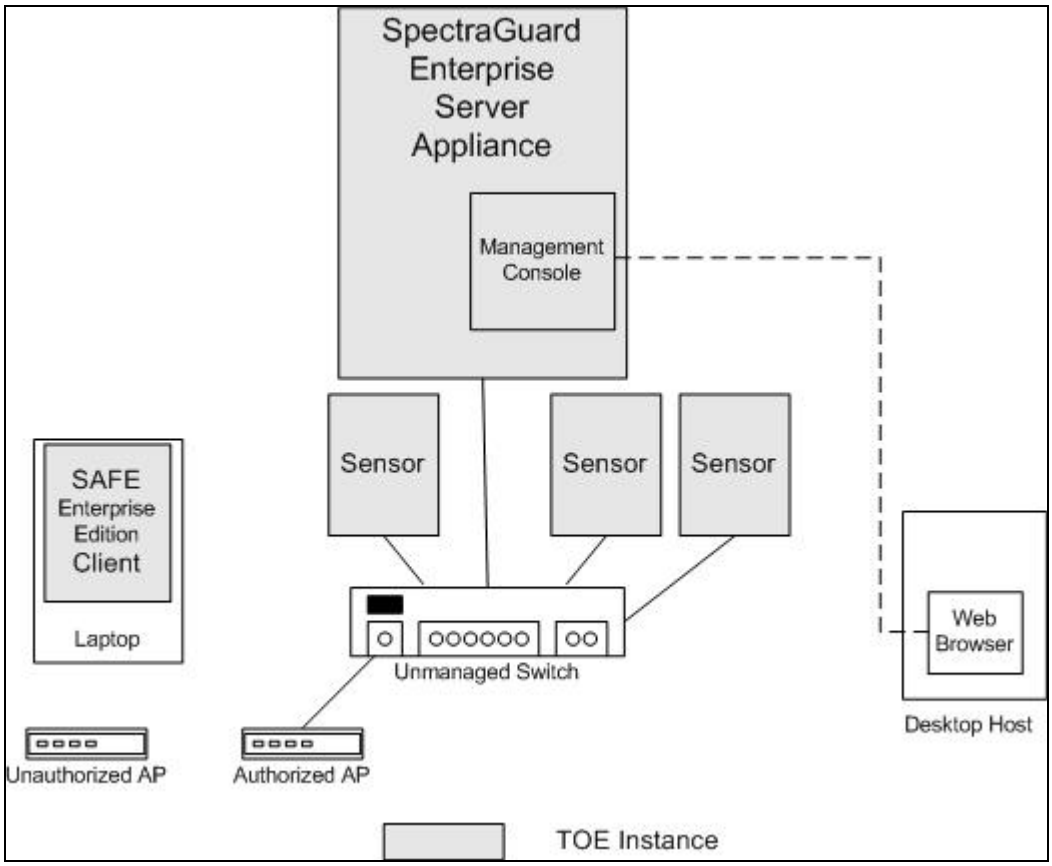

Figure 1 TOE Physical Boundary

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- AirTight Networks SpectraGuard Enterprise [v5.0] and SpectraGuard SAFE Enterprise Edition [v2.0] Security Target (ST) V1.1; May 10, 2007
- AirTight Networks SpectraGuard Enterprise [v5.0] and SpectraGuard SAFE Enterprise Edition [v2.0] Configuration Management Common Criteria Supplement to the Guidance Documentation V1.6 March 27, 2007
- AirTight Networks SpectraGuard Enterprise and SpectraGuard SAFE Enterprise Edition Configuration Management V1.0 March 27, 2007
- SpectraGuard Enterprise Deployment Guide V5.0 (undated)
- SpectraGuard Enterprise Installation Guide V5.0 (undated)
- SpectraGuard Enterprise Quick Setup Guide V5.0 (undated)
- SpectraGuard Enterprise User Guide V5.0 (undated)
- SAFE User Guide V2.0

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Developer Testing

The vendor testing was conducted at one of the vendor locations in Pune, India and covered the security functions identified in Section 6.1 of the ST. These security functions were: Security audit, Information Flow Control, Identification and Authentication, Security Management, and partial Protection of the TSF.

The testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures consisted primarily of manually invoking functions described in the product's user and administrative guides and verifying the function's behavior. The evaluator sampled developer's tests.

The evaluator determined that the vendor tested (at a high level) most of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined

that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluator determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

7.2 Evaluator Independent Testing

Because the Server and Sensor components come pre-installed on appliances, there is no installation of software is necessary. The evaluator configured the appliance up for the target network. The test configuration included:

- 1 SpectraGuard Enterprise Server Appliance v5.0; Build 5.0.56 (pre-installed)
- 2 Spectraguard Sensor Appliance v5.0; Build 5.0.56 (pre-installed)
- 1 SpectraGuard SAFE client v2.0; Build 2.0.27
  - 1 Dell Laptop Hardware: Intel Pentium III processor 751 MHz, 256 MB of RAM, D-Link AirPlus DWL-G650_revB Utility Version 2.5.4 Driver version 2.2.4.71
  - Software: Microsoft Windows XP Pro Version 2002 Service Pack 2

- 1 Desktop Machine used with Java based Management Console
  - 1 Dell Desktop machine Hardware: Intel Pentium 4 CPU 3.40GHz 3.39 GHz, 1.99 GB of RAM Software: Microsoft Windows XP Pro Version 2002 Service Pack 2 with latest updates
- 1 Laptop (No AirTight Software Installed- just used for blocking tests)
  - IBM Thinkpad Pentium M processor 1.6 GHZ 1.5 Gig of RAM
  - Atheros communications A/B/G Wireless LAN Mini PCI adapter
  - Software: Microsoft Windows XP Pro Version 2002 Service Pack 2 with latest updates

- Networks: TCP/IP installed and configured
- Wireless Protocols: 802.11 wireless
- Server Interface Auto-sensing 10/100/1000 Mbps Ethernet

The evaluation team sampled developer tests and verified the results. The evaluation team then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality. The evaluator tests successfully demonstrated blocking of both a mis-configured AP and Rogue AP that was connected to the target network. The evaluation team conducted a port scan using the Nmap Vulnerability Scanner. No vulnerabilities were found using Nmap.

7.3 Strength of Function

The TOE depends on the strength of the passwords used to authenticate access by administrative users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The overall strength of function (SOF) requirements claim for the TOE is SOF-Basic, which effectively requires resistance to password guessing attacks of greater than one day.

The TOE's SOF analysis assumes passwords length to be a minimum of 8 with at least one each of a lower case, an upper case, a special character, and a numeric character. It further assumes that the administrator has specified the allowed number of login failures as 10 in 30 minutes as well as a lockout time of 5 minutes.

8. Evaluated Configuration

The AirTight Networks evaluated configuration consists of the following:

- 1 SpectraGuard Enterprise Server Appliance v5.0; Build 5.0.56 (pre-installed)
- Spectraguard Sensor Appliance v5.0; Build 5.0.56 (pre-installed)
- SpectraGuard SAFE client v2.0; Build 2.0.27

9. Results of 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 version 2.3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 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.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name

ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

10. Validator Comments/Recommendations

Be sure to note the assumptions and clarifications of scope in section 4 of this report. Additionally:

1. The effectiveness of the information flow control mechanism depends on the client's and access point's response to the DEAUTHENTICATE packets that are transmitted by the Sensor component. This mechanism is more effective with wireless adapter cards that conform to standard protocols. Cards with turbo mode and certain non-standard devices may be less effectively disrupted. Please refer to section 3 to the CC Supplement for a list of the supported wireless adapters and access points.
2. The Server and Sensors components by themselves are sufficient to protect the target network from the threats identified in section 3.2 of the ST. The SAFE component is an optional component that can be installed on wireless clients to provide further protection. When the SAFE component is installed on a client, the client is only allowed to connect to authorized access points.
3. Known vulnerabilities in the IT environment could be exploited to bypass the TOE's security policies. While these vulnerabilities are outside the scope of the evaluation, it is expected that the customer should install the latest security critical patches to components of the IT environment. Please refer to CC Supplement document for the list of the open source products that are bundled with the Server and Sensor components and the vendor's policy of updating the IT environment software when a vulnerability is found. Under unusual circumstances, the SAFE component might not be compatible with a specific operating system patch. The customer is advised to check the AirTight Networks web site for any restrictions on specific patches to the operating system.

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and recommended to CCEVS Management that an EAL2 certificate rating be issued for the AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE [v 2.0].

11. Security Target

The Security Target for AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE [v 2.0] is contained within the document Security Target for AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE [v 2.0], Version 1.1 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria Evaluation Methodology
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OS	Operating System
PP	Protection Profile
SFR	Security Functional Requirement
SGE	SpectraGuard Enterprise Server
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://niap.nist.gov/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- AirTight Networks (http://www.airtightnetworks.net/).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CCEVS3] Guidance to Validators of IT Security Evaluations, Version 1.0, February 2000.
- [CCEVS4] Guidance to Common Criteria Testing Laboratories, Draft, Version 1.0, March 2001.

Other Documents

- [ST] Security Target for AirTight Networks SpectraGuard Enterprise [v 5.0] and SpectraGuard SAFE [v 2.0] Version 1.1, May 10, 2007.