National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

AirTight Networks SpectraGuard® Enterprise, Version 6.5

Report Number: **CCEVS-VR-10441-2012**

Dated: **11 June 2012**

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 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

List of Figures

1 Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product SpectraGuard Enterprise, Version 6.5

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.

The Target of Evaluation (TOE) is wireless intrusion prevention system (WIPS). It consists of SpectraGuard Enterprise Server component (also referred as "Server"), SpectraGuard Enterprise Management Console component (also referred as "Console"), and SpectraGuard Enterprise Sensor component (also referred as "Sensor").

The Sensors scan WiFi radio channels and wired network segments, and report scan data to the Server. The Server performs analysis of the data reported by Sensors to identify and respond to unauthorized wireless activity. The Console facilitates user interaction with the TOE. The TOE ensures conformance of wireless activity to security policy, and addresses security violations such as rogue WiFi networks, unauthorized WiFi connections, WiFi network mis-configurations and wireless denial of service attacks.

The TOE operates in "overlay" fashion, i.e., Sensors are not inline the wireless connections or the wired connections. Rather, they rely on broadcast nature of the wireless medium to collect wireless scan data. They also rely on broadcast subset of traffic in the wired network to collect wire-side scan data.

The TOE performs following security functionality: auditing of security relevant events; TOE user account administration; cryptographic support of secure communications; TOE user identification and authentication; role based access to management of security functions; TOE user session security functions; trusted communication between components; and system data collection, analysis, review, availability and loss prevention.

The TOE is intended for use in computing environments where there is a low-level threat of malicious attacks. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in May 2012 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 3.1 R3 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2 from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, [CEM]. This Security Target claims demonstrable compliance to *U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments*, Version 1.7, July 25, 2007 (IDS System PP).

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 “AirTight Networks SpectraGuard® Enterprise, Version 6.5, Security Target, Version 1.6, April 25, 2012”

2 Identification

Target of Evaluation: SpectraGuard Enterprise, Version 6.5:

- SpectraGuard Enterprise Server appliance SA-350 including software version 6.5
- SpectraGuard Enterprise Server VMware software SE-SW-VM version 6.5
- SpectraGuard Enterprise Sensor appliance SS-300-AT-C-10 including Sensor software version 6.5

Evaluated Software and Hardware:

- SpectraGuard Enterprise Server appliance model SA-350 including the Server software version 6.5 along with the appliance hardware, and the Linux OS and the third party applications included in the appliance.
- SpectraGuard Enterprise Server software SE-SW-VM version 6.5 running on VMware ESX, ESXi or vSphere virtual machine version 4.0 or above along with the hardware of the virtual machine, and the Linux operating system emulated on the virtual machine and the included third party applications.
- SpectraGuard Enterprise Management Console version 6.5 running as Java applet in Internet Explorer (IE) web browser on Windows 2000, Windows XP, or Windows 7 computer.
- SpectraGuard Enterprise Sensor appliance SS-300-AT-C-10 including Sensor software version 6.5 along with the appliance hardware, and the Linux OS and the third party applications included in the appliance.

Developer:	AirTight Networks, Inc
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr., Suite 5400 McLean, VA 22102-3321
Evaluators:	Dragua Zenelaj, Nicholas Goble and Swapna Katikaneni
Validation Scheme:	National Information Assurance Partnership CCEVS
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, July 2009
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, July 2009

3 Security Policy

The TOE's security policy is expressed in the security functional requirements identified in Section 6.1 of the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

The TOE provides the following security features:

3.1 Summary

3.1.1 SECURITY AUDIT

The TOE is able to audit the use of the administration/management functions. This function records attempts to access the system itself, such as successful and failed authentication, as well as the actions taken by TOE users once they are authenticated.

The audit data is protected by the access control mechanisms of the database and OS of the TOE components and by the TOE management Console interface. Only Superuser has access to the audit records. The Superuser can download the audit records for viewing. At the time of downloading, sorting and filtering criteria can be specified for the audit records.

The audit records are stored in the TOE for configurable number of days. Once any record becomes older than the configured lifetime, it is automatically deleted. The TOE does not place any limit on the size of the audit trail, the only limit comes from the size of the disk. When the occupied disk size approaches the capacity, the TOE generates early warning.

Security Audit relies on the Operational Environment with a properly configured text editor (such as Microsoft Excel, WordPad etc.) application to support viewing of the downloaded audit logs. It also depends on the Operational Environment to provide secure communication path between the TOE Server and management Console.

3.1.2 CRYPTOGRAPHIC SUPPORT

The TOE performs cryptographic functions for: a) Sensor-Server communication, b) Console-Server communication, c) SSH utility in Sensor and Server. The Sensor-Server communication protocol is proprietary and uses FIPS 140-2 approved algorithms for key generation, encryption and message integrity. The Console-Server communication follows TLS version 1.0 standard and the SSH utility follows SSH version 2 standard. The TOE supports FIPS and non-FIPS operation modes.

3.1.3 IDENTIFICATION AND AUTHENTICATION

The TOE requires all users to provide unique identification and authentication data before any access to the system is granted. User identification and authentication is done by the TOE though username/password authentication, optionally using an external authentication server. The TOE also supports client certificate-based authentication option, such as CAC authentication. For certificate-based authentication, TOE supports optional two-factor authentication with password in addition to client certificate.

All authorized TOE users must have a user account with security attributes that control the user's access to TSF data and management functions. These security attributes include user name, password, role and location node identity for TOE users.

The TOE enforces a password policy for users who authenticate via the TOE. The TOE will also prevent a user from accessing the system after a configurable number of failed login attempts.

Identification and Authentication depends on the Operational Environment to provide an external authentication server if that feature is configured. It also depends on the Operational Environment to provide a secure communications path between the TOE and the external authentication server.

3.1.4 SECURITY MANAGEMENT

The TOE provides a web-based (using HTTPS) management interface for all run-time TOE administration. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role.

Security Management relies on a management console in the Operational Environment with a properly configured Web Browser to support the web-based management interfaces.

3.1.5 TOE ACCESS

The TOE will terminate a user's interactive session after a configurable inactivity time. Before establishing a user session, the will display an advisory warning message regarding unauthorized use of the TOE.

3.1.6 PROTECTION OF SECURITY FUNCTIONS

The TOE ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured through strong encryption during both setup and the transition of data. The TOE Server is FIPS 140-2 Level 1 certified and the TOE Sensor is FIPS 140-2 Level 2 certified.

3.1.7 SYSTEM DATA COLLECTION

The TOE detects WiFi threats and vulnerabilities. For this, it collects information from IEEE 802.11 protocol transmission frames detected on WiFi radio channels and IEEE 802.3 protocol traffic detected in the wired part (Ethernet) of the monitored network subnets. Sensors collect the above-mentioned data and send it to the Server.

3.1.8 SYSTEM DATA ANALYSIS

The TOE performs various types of analyses such as signatures, anomaly, wired/wireless traffic correlation and devices configuration check, on the collected data to detect wireless threats and vulnerabilities. When threats/vulnerabilities are detected, the TOE generates alarms and (if optionally configured to do so) sends alarms by email, SNMP, syslog etc. to external servers in the operational environment.

3.1.9 SYSTEM DATA REVIEW, AVAILABILITY AND LOSS

TOE stores user action logs and events data in the database that is included in the TOE. User action logs can be downloaded by authorized administrator from Console as TSV (tab separated values) format file. Events are displayed in tabular form on Console. The user action logs and events are automatically deleted after administrator configured lifetime expires for them. Events are also automatically deleted when total number of events exceeds the administrator configured thresholds. When auto deletion happens, the most recent logs and events are always maintained. The TOE also proactively notifies the administrator via event if the disc occupancy reaches unsafe limits so that administrator can take appropriate action (e.g., backup) to free up the disc space. TOE also facilitates automatic periodic backup of database.

3.2 Operational Environment Objectives

The TOE's operating environment must satisfy the following objectives.

- The IT Environment will provide reliable timestamps to the TOE.
- Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
- Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
- Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
- Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
- The TOE is interoperable with the IT System it monitors.

- The Operational Environment must provide email service to receive and store email notifications from the TOE.
- The Operational Environment must provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.

  Note: This *is only applicable when the TOE is configured to use an external LDAP and/or RADIUS authentication service.*
- The Operational Environment must provide secure communications between the TOE and the servers in the environment that support the security functionality of the TOE.

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 EAL 2 assurance requirements:

- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.2 Use of a CM system
- ALC_CMS.2 Parts of the TOE CM coverage
- ALC_DEL.1 Delivery procedures

4.2 Assumptions

TOE Intended Usage Assumptions:

- The TOE has access to all the IT System data it needs to perform its functions. (A.ACCESS)

  The administrators must make sure that the TOE components have full access to the networks and external servers in the Operational Environment.

- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. (A.DYNMIC)

  Administrators must make sure that they use the administrative functions of the GUI/CLI to modify the TOE configuration in response to any Operational Environment changes.

- The TOE is appropriately scalable to the IT System the TOE monitors. (A.ASCOPE)

  Administrators must make sure that they deploy sufficient number of Sensors to provide adequate radio coverage of wireless environment to be protected. They must also ensure that Sensors are configured to attach to the wired subnetworks (virtual LANs (VLANs)) to be protected from wireless intrusions such as Rogue APs.

TOE Physical Assumptions:

- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. (A.PROTCT)

  The Sensors and the Server must be protected from physical tampering. For example, Sensors could be deployed in the ceiling should be considered. This not only makes them difficult to access for tampering, but also helps achieve better radio coverage. Server must also be protected from physical tampering. For example, Server could be installed in the secure server room.

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.LOCATE)

  Access to the TOE components must be physically restricted.

TOE Personnel Assumptions:

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. (A.MANAGE)

  Administrators must be assigned to perform configuration, receive notifications, and perform actions on the events that TOE generates.

- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. (A.NOEVIL)

  Administrators of the TOE must be carefully selected and be properly trained.

- The TOE can only be accessed by authorized users. (A.NOTRST)

  Only required personnel should have user accounts on the system and they must protect their authentication information (username and password).

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 (EAL 2 in this case).
2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 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. The following are not included in the Evaluation Scope:
    - SpectraGuard Secure Agent For Endpoints (SAFE), as this feature is optional and requires separate license. *Note: The basic license for the TOE includes experimental license for SAFE. This experimental SAFE feature is not be used in the evaluated configuration of the TOE.*
    - High Availability (HA) feature, as it is nothing but redundant Server component.
    - OPSEC integration feature, as it requires specialized OPSEC operational environment.
    - Performance Monitoring feature which is concerned with performance monitoring rather than wireless intrusion prevention. It also requires a separate license.
    - Integration with WLAN controllers (Aerohive, Aruba, Cisco, HP Procurve), as this feature is optional, requires third party product, and may not operate with every WLAN controller found in the operational environment. This feature is included in the base license. The integration feature is used to read the list of wireless devices managed by the WLAN controllers and automatically populate them as Authorized APs and clients in the TOE. This is done to ease the initial setup, rather than a necessity. That is, TOE is capable to perform this operation even without the WLAN controller integration (e.g., input a file with the list of MAC addresses of such devices, manually categorize devices using GUI menu, etc.). The integration may also be used to read into the TOE a list of unmanaged APs and clients detected by WLAN APs and the signal strengths of such devices. Again, this is not a necessity, since the TOE itself is capable of detecting all wireless devices and their signal strengths by itself using the channel scanning Sensors. Importantly, the TOE does not write any information to the WLAN controllers. The read only operations are performed either over SNMP or over a JAVA API implemented by the TOE.

5. The Operational Environment needs to provide the following capabilities:
    a. A trusted DHCP server for automatic IP address assignment.
    b. A trusted DNS server for zero configuration installation.
    c. An NTP server for automatic time setting.
    d. An email server for the administrator to receive notifications and reports via email.
    e. A syslog server for administrator alert notifications.
    f. An SNMP server for administrator alert notifications.
    g. An external authentication LDAP server that supports LDAPv3 (compliant with RFCs 2251-2256, 2829-2830).
    h. An external authentication RADIUS server compliant with RFCs 2865 and 2866.
    i. A managed Wireless Local Area Network (WLAN) to be monitored. (Note: The TOE is also used to enforce no-WiFi policy in those networks that do not have managed WLAN of their own. Hence, existence of a managed WLAN is only optional for operation of the TOE). The TOE works with all WLAN environments, which are compliant with IEEE 802.11 family of standards.
    j. In monitored WLAN environments, optional integration with Wireless Local Area Network (WLAN) controller is supported for Aerohive HiveManager version 3.4 or above, Aruba controller OS version 3.3 or above, Cisco Wireless LAN Controller (WLC) version 5.2 or above, and HP ProCurve controller version 5.4 or above.
    k. Unmanaged (neighborhood) Wireless Local Area Networks (WLANs) to be monitored.
    l. A card reader attached to the computer from where the Console is accessed to facilitate client certificate based authentication using smart cards.

5 Architectural Information

The evaluated configuration of the TOE includes the following TOE components:

- **Server Component**

a) SpectaGuard Enterprise Server appliance SA-350:

The TOE Server application software version 6.5 is embedded in the SpectraGuard Enterprise Server appliance model SA-350. The appliance hardware and the Linux (Centos 5.2 kernel version 2.6.18-92) operating system installed on the appliance provide support for the intrusion detection and associated security management functions of the TOE, and are included in the TOE.

b) SpectraGuard Enterprise Server application software SE-SW-VM:

The TOE Server application software version 6.5 is also available for VMware ESX, ESXi and vSphere virtual machines versions 4.0 or above. The VMware virtual machine environment provides support for the intrusion detection and associated security management functions of the TOE, and is included in the TOE. SE-SW-VM software is provided as a OVF (Open Virtualization Format) version 1.0 file that is suitable for hosting on VMware ESX, ESXi, and vSphere virtual machines.

- **Sensor Component**

SpectraGuard Enterprise Sensor appliance model SS-300-AT-C-10:

The TOE Sensor application software version 6.5 is embedded in the Sensor appliance model SS-300-AT-C-10. The Sensor appliance hardware and the Linux version 2.6.15) operating system installed on it provides support for the intrusion detection and associated security management functions of the TOE, and are included in the TOE.

- **Console Component**

The TOE Console version 6.5 runs as Java applet in Internet Explorer web browser (IE 5.5 or above) on Microsoft Windows XP/Vista/7 machine. There is no need to install any software to run the Console. The Console applet is received from the Server when the Server is accessed from within web browser.

The TOE boundary is depicted in Figure 1 (shown with yellow background). The SpectraGuard Enterprise Server depicted in the figure represents either a) SA-350

appliance including its hardware and software, or b) SE-SW-VM server software including the virtual machine that hosts it.

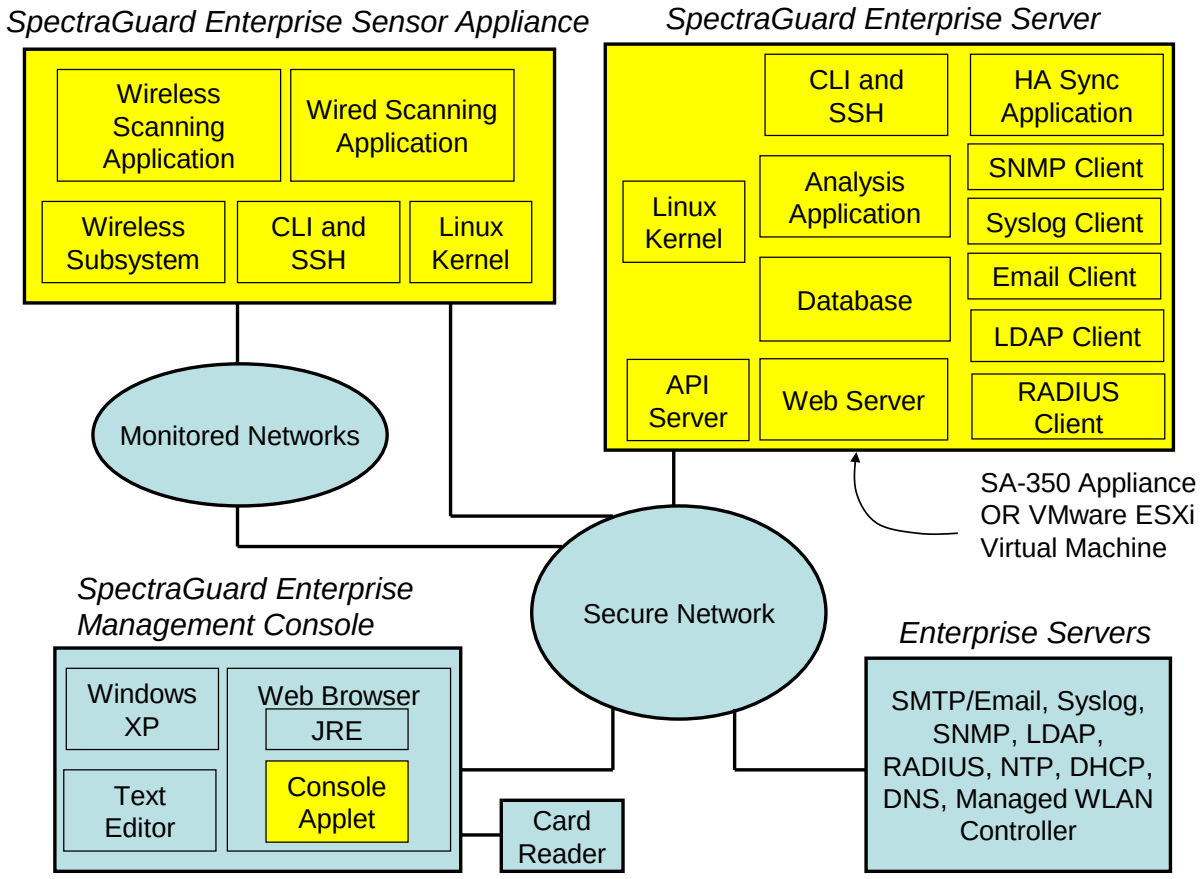

Figure 1: TOE Boundary

6 Documentation

The TOE is physically delivered to the End-User. The following guidance documentation is part of the TOE and is delivered in printed form and as PDFs on the installation media:

- User Guide for AirTight Networks SpectraGuard® Enterprise, Version 6.5, October 22, 2010
- Installation Guide for AirTight Networks SpectraGuard® Enterprise, Version 6.5, December 12, 2011
- Quick Setup Guide for AirTight Networks SpectraGuard Enterprise Version 6.5
- Release Notes for AirTight Networks SpectraGuard Enterprise Version 6.5
- Common Criteria Supplement, SpectraGuard Enterprise, Version 6.5, April 25, 2012

7 IT Product Testing

At EAL 2, the overall purpose of the testing activity is “independently testing a subset of the TSF, whether the TOE behaves as specified in the design documentation, and to gain confidence in the developer's test results by performing a sample of the developer's tests” (ATE_IND.2, 14.6.2.1 [CEM])

At EAL 2, the developer’s test evidence must “show the correspondence between the tests provided as evaluation evidence and the functional specification. However, the coverage analysis need not demonstrate that all TSFI have been tested, or that all externally visible interfaces to the TOE have been tested. Such shortcomings are considered by the evaluator during the independent testing.” (ATE_COV.1, 14.3.1.3 [CEM])

This section describes the testing efforts of the vendor and the evaluation team.

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]).

7.1 Developer Testing

The developer testing effort that is described in detail in the Developer Test Plan involved executing the test sets in the test configurations described in Section 8: Evaluated Configuration.

7.1.1 OVERALL TEST APPROACH AND RESULTS:

The Developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. These test cases were mapped to SFRs, TSFIs, Subsystems and Internal Interfaces listed in the ST, Functional Specification [FSP], TOE Design Document [TDS] and Test Coverage Document [COV]. After the test cases were defined, test procedures were written by the Vendor’s development team to exercise each test case.

The tests provided by the developer are manual tests performed via the Console GUI and commands via CLI.

7.1.2 DEPTH AND COVERAGE

All developer test cases test the TOE security functions by stimulating an external interface.

All the developer tests are performed using the Console interface or by entering commands through the CLI. The evaluator determined that the test cases as described in the test documentation adequately exercise the internal interfaces.

TOE testing directly tests external TSF interfaces and indirectly tests (exercised implicitly) internal subsystem interfaces. The behavior of the TSF is realized at its interfaces.

Given the Evaluation Assurance level (EAL 2) TOE testing is adequate. All the external TSF interfaces are tested. TOE testing exercises all security functions identified in the Functional Specification [FSP]. It indirectly tests the security functions and subsystem interfaces as presented in the TOE Design [TDS].

The evaluator ensured that the vendor tests provided included the tests such that:

- All Security Functions are tested
- All External interfaces are exercised
- All Security Functional Requirements are tested.
- All relevant security relevant features mentioned in the Administration/User Guides are covered in testing.

7.1.3 RESULTS

The evaluator checked the test procedures and the Test Evidence and found that the expected test results are consistent with the actual test results provided. For each test case examined, the evaluator checked the expected results in the test procedures with the actual results provided in the Test Evidence and found that the actual results were consistent with the expected results. The evaluator checked all of the test procedures.

Given the Evaluation Assurance level (EAL 2), the evaluator determined that AirTight's TOE testing is adequate. All the external TSF interfaces are tested. TOE testing exercises all security functions identified in the Functional Specification.

7.2 Evaluator Independent Testing

The evaluator performed the following activities during independent testing:

- Execution the Developer's Functional Tests (ATE_IND.2)
- Team-Defined Functional Testing (ATE_IND.2)
- Vulnerability/Penetration Testing (AVA_VAN.2)

7.2.1 EXECUTION THE DEVELOPER'S FUNCTIONAL TESTS

The evaluator selected to about 60% of the developer's tests:

- As a means of ensuring the coverage of the security features.
- As a means to gain confidence in the developer's test results.
- A quick means of ensuring TOE is in a properly configured state.

The developer's test cases were executed only after the TOE was installed in the evaluated configuration that is consistent with the Security Target (Section 1) and the Common Criteria Supplement Document. The evaluator confirmed that the test

configuration was consistent with the evaluated configuration in the Security Target and the Airtight CC Supplement.

The test configurations used by the evaluator were the same as that used by the developer.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the retests being consistent with expected results.

All of the Developer's Functional Tests rerun by the Evaluator received a 'Pass' verdict.

7.2.2 TEAM-DEFINED FUNCTIONAL TESTING

The Evaluator selected individual test procedures from the set of Developer Functional Tests, and modified the input parameters to ensure fuller coverage of security functions and correctness of developer reported results (ensuring that the results were not canned).

Additional tests were developed for the purpose of verifying that the product operates in accordance with Vendor claims, i.e. that a bug is fixed or a capability operates as described in the product documentation.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the tests being consistent with expected results. Anomalies found were addressed by updating the required documents.

All of the Team-Defined Tests received a 'Pass' verdict.

7.2.3 VULNERABILITY/PENETRATION TESTING

The Penetration tests for TOE were developed according to the following strategy:

- The Evaluator looked for possible security vulnerabilities by examining the Vulnerability Analysis, Functional Specification, TOE Design Document and TOE Security Target.
- The Evaluator analyzed the different components that comprise the TOE for existing vulnerabilities.
- The Evaluator searched public vulnerability databases for vulnerabilities that corresponded to these components.
- The Evaluator has hypothesized vulnerabilities requiring low attack potential that apply to the TOE.
- The Penetration tests will cover hypothesized vulnerabilities and potential misuse of guidance.
- The tests for potential misuse of guidance will cover installing the TOE from the guidance documentation and sampling the documented administrator procedures.
- The Evaluator will perform a systematic vulnerability analysis of the TOE.

The TOE Penetration testing was performed with the following assumptions and guidelines:

- Penetration testing will be limited to attacks by a malicious entity with limited technical skills and unsophisticated exploits.
- TOE Administrators are trusted personnel; any vulnerabilities resulting from Administrator use constitute a case of misuse, rather than purposeful activity with malicious intent.
- The platforms running all the TOE Components/applications have been configured securely as described in the Guidance documents to include:
    - Minimal OS features installed or enabled
    - Minimal system privileges configured
    - Only user accounts for authorized system administrators
- The organization operating the TOE has defined and is following good backup and recovery procedures that allow the TOE to be recovered to a secure configuration in the event of a loss of the TOE.

The test results and screenshots for the test cases were recorded during the evaluator testing. Overall success of this testing was measured by 100% of the tests being consistent with expected results. Anomalies were documented along with suggested / required solutions.

There was one anomaly found, which was addressed by the developer by updating the user guidance documentation

8 Evaluated Configuration

The evaluated configuration includes the following:

- SpectraGuard Enterprise Server version 6.5
- SpectraGuard Enterprise Management Console version 6.5
- SpectraGuard Enterprise Sensor version 6.5

The Test Configuration consisted of SpectraGuard Enterprise Server appliance SA-350 including Server software version 6.5 and SpectraGuard Enterprise Sensor appliance SS-300-AT-C-10 including Sensor software version 6.5. The SpectraGuard Enterprise Management Console will be accessed using Internet Explorer (IE) version 9.0 using JRE version 1.6u30 or higher on Windows 7 computer.

Another Test Configuration consisted of SpectraGuard Enterprise Server software SE-SW-VM version 6.5 running on VMware ESXi version 4.0 and SpectraGuard Enterprise Sensor appliance SS-300-AT-C-10 including Sensor software version 6.5. It suffices to test one virtual machine environment, as others are equivalent and interoperable with it. The SpectraGuard Enterprise Management Console will be accessed using Internet Explorer (IE) version 9.0 using JRE version 1.6u30 or higher on Windows 7 computer.

The Sensor appliance SS-300-AT-C-10 includes two WiFi radio modules. Any of these radio modules can be tuned via software to monitor any WiFi channel. In the SS-300-AT-C-10 Sensor appliance, the first radio module is tuned to rotate on one subset of WiFi channels (in 2.4 GHz band) and the second radio module is tuned to rotate on the other subset of WiFi channels (in 5 GHz band).

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 3.1 R3 of the CC and the CEM.

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.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 2 augmented with ALC_FLR.2. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted.

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.1 Basic design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.2 Use of a CM system
- ALC_CMS.2 Parts of the TOE CM coverage
- ALC_DEL.1 Delivery procedures
- ALC_FLR.2 Flaw reporting procedures
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.2 Security objectives
- ASE_REQ.2 Derived security requirements
- ASE_SPD.1 Security problem definition
- ASE_TSS.1 TOE summary specification
- ATE_COV.1 Evidence of coverage
- ATE_FUN.1 Functional testing

- ATE_IND.2 Independent testing – sample
- AVA_VAN.2 Vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached Pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.
- The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

10 Validators Comments/Recommendations

The validators have no comments or specific recommendations.

11 Security Target

AirTight Networks SpectraGuard® Enterprise, Version 6.5, Security Target, Version 1.6, April 25, 2012

12 Glossary

12.1 Acronyms

The following are product specific and CC specific acronyms.

AES-CBC	Advanced Encryption Standard – Cipher Block Chaining
AP	Access Point
CA	Certificate Authority
CAC	Common Access Card
CC	Common Criteria [for IT Security Evaluation]
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
HMAC-SHA-1	Hash Message Authentication Code-Systematic Hashing-Algorithm-1
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IDS	Intrusion Detection System
IE	Internet Explorer
IP	Internet Protocol
IT	Information Technology
JRE	Java Runtime Environment
LDAP	Lightweight Directory Assistance Protocol
MAC	Medium Access Control
ND	Network Detector

NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
OVF	Open Virtualization Format
PP	Protection Profile
RADIUS	Remote Authentication Dial-in User Service
RFC	Request for Comments
SFR	Security Functional Requirements
SSH	Secure Shell
SNDC	Sensor Network Detector Combo
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol/Internet Protocol
TLS	Transport Security Layer
TOE	Target of Evaluation
TSF	TOE Security Functions
TSV	Tab Separated Values
UDP	User Datagram Protocol
GUI	Graphical User Interface
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller

12.2 Terminology

This section defines the product-specific and CC-specific terms. Not all of these terms are used in this document.

Terminology	**Definition**

Terminology	Definition
Assets	Information or resources to be protected by the countermeasures of a TOE.
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Audit Log (Audit Trail)	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	To establish the validity of a claimed user or object.
Authentication Object	An object which contains the settings for connecting to and retrieving user data from an external authentication server.
Authorized Administrator (TOE Administrator)	The authorized users that manage the TOE or a subset of its TSF data and management functions.
Availability	Assuring information and communications services will be ready for use when expected.
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.
Evaluation	Assessment of a PP, a ST or a TOE, against defined criteria.
Frame	A block of data sent over the link transmitting the identities of the sending and receiving stations, error-control information, and message.
Information Technology (IT) System	May range from a computer system to a computer network.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.

Terminology	Definition
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection	The process of analyzing network traffic for potential intrusions and storing attack data for security analysis.
Intrusion Detection System (IDS)	A combination of sensors, scanners, and analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
Intrusion Event	A record of the network traffic that violated an intrusion policy.
Intrusion Prevention	The concept of intrusion detection with the added ability to block or alter traffic that is undesirable from security perspective.
IT Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Network	Two or more machines interconnected for communications.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs
Scanner data	Data collected by the scanner functions.
Scanner functions	The active part of the scanner responsible for collecting traffic information that may be representative of vulnerabilities in and misuse of IT resources (i.e., scanner data).
Security	A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Signatures	Patterns of network traffic that can be used to detect attacks or exploits.

Terminology	Definition
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Threat	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.
WiFi	Wireless network based on IEEE 802.11 protocol family

13 Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com/labs/common-criteria/index.htm).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-004.