National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134

Cisco Unified Wireless Network & Wireless Intrusion Detection System

Report Number:	**CCEVS-VR-VID10324-2009**
Dated:	**25 March 2009**
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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Dr. Patrick Mallett
The MITRE Corporation
McLean, VA

Franklin Haskell
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
Eve Pierre
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Unified Wireless Network & Wireless Intrusion Detection System (henceforth referred to as WLAN). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in March 2009. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 2 augmented with ACM_SCP.1, ALC_FLR.2, and AVA_MSU.1.

The Target of Evaluation (TOE) is a Wireless LAN access system with an integrated Wireless Intrusion Detection System (WIDS). The Wireless LAN access system defined in this ST are multiple products operating together to provide secure wireless access to a wired and wireless network. The Wireless Intrusion Detection System defined in this ST are the WIDS capabilities defined in this ST including intrusion detection signatures, rogue AP and rogue device detection with location tracking, and 802.11 management frame protection (MFP). This TOE as identified above is the Cisco Wireless LAN Access System TOE which provides end-to-end wireless encryption, centralized WLAN management, authentication, authorization, and accounting (AAA) policy enforcement, and wireless intrusion detection (WIDS) with location tracking.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level 2 (EAL 2 augmented with ACM_SCP.1, ALC_FLR.2, and AVA_MSU.1) have been met.

The technical information included in this report was obtained from the Cisco Unified Wireless Network & Wireless Intrusion Detection System Security Target.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 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 desiring 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's 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 Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Cisco Unified Wireless Network & Wireless Intrusion Detection System composed of the following components: Cisco Aironet 1130, 1230, and 1240 AG Series Access Points; Cisco 4400 Series Wireless LAN Controllers; Cisco Catalyst 6500 Series Wireless Integrated Services Module (WiSM) with the Supervisory 720 module; Cisco Wireless Control System (WCS); Cisco Secure Access Control Server (ACS), Cisco 2710 Wireless Location Appliance; Kiwi Syslog Daemon; Syslog-ng
Protection Profile	US Government Wireless Local Area Network (WLAN), Access System, Protection Profile for Basic Robustness Environments, April 2006, Version 1.0.
ST:	Cisco Unified Wireless Network & Wireless Intrusion Detection System Security Target, Version 1.0, March 23, 2009
Evaluation Technical Report	Evaluation Technical Report For the Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) (Proprietary), Version 1.1, March 24, 2009
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3 Part 2: Evaluation Methodology, Supplement: ALC_FLR- Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc
Developer	Cisco Systems, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Dr. Patrick Mallett, The MITRE Corporation, McLean, VA Franklin Haskell, The MITRE Corporation, Bedford, MA

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Overview

The TOE is a system of products that are administratively configured to interoperate together to provide a WLAN. The TOE is meant to allow mobile, wireless clients to be roaming hosts on the wireless network, and to connect to the wired network using access points (APs). The TOE has Access Point TOE components (Cisco Aironet 1130, 1230, and 1240 AG Series Access Points), Controller TOE components (Cisco 4400 Series Wireless Controllers and the Cisco Catalyst 6500 Series WiSM (Cisco Wireless Services Module) with the Supervisory 720 module), ACS TOE component (Cisco Secure Access Control Server), WCS TOE components (Cisco Wireless Control System), a Location Appliance TOE component (Cisco 2710 Location Appliance), and Syslog TOE component (Kiwi Syslog Daemon and Syslog-ng).

Note that although there are several TOE components, there are only two administrative interfaces: the ACS and the WCS. Because of this, there are two main administrator roles on the TOE. Throughout the ST, these are individually identified as the WCS Administrator or the ACS Administrator where appropriate. Portions of the ST that identify only 'administrator,' should be understood to mean both the ACS Administrator and the WCS administrator.

3.2 TOE Physical Boundary

The TOE physical boundary defines all hardware and software that is required to support the TOE's logical boundary and the TOE's security functions. The TOE's support of the logical boundary and security functions is divided into functional components (TOE components) which are described in this section.

The following table identifies the required components in the evaluated configuration and identifies whether or not they are within the TOE boundary. This is followed by a sample network arrangement of the TOE and detailed subsections on each TOE component.

TOE Component Name	Required Number and Versions	Within the TOE Boundary?
AP	At least one of the following: • Cisco Aironet 1130 AG Series Access Point, • Cisco Aironet 1230AG Series Access Point, or • Cisco Aironet 1240 AG Series Access Point each running software Version 4.1.185.10 FIPS and including the Cisco FIPS kit part number AIRLAP-FIPSKIT	Yes

4400 Controller[1] or 6500 WiSM/Supe720	At least one of the following: • Cisco 4400 Series Wireless LAN Controller running software Version 4.1.185.10 FIPS; and the Cisco FIPS kit part number AIRWLC4400-FIPSKIT, or • Catalyst 6500 Wireless Integrated Service Module (WiSM) w/software Version 4.1.185.10 FIPS; 720 Supervisor w/software IOS version 12.2(18)SXF15A; a 6503, 6504, 6506, 6509 or 6513 Catalyst chassis; and the Cisco FIPS kit part number CVPN6500FIPS/KIT	Yes
WCS Software	Cisco Wireless Control System (WCS) Version 4.2.97.0	Yes
WCS host OS	One of the following as a host OS for WCS: • Windows 2003 SP1 or greater Server, or • Red Hat Linux AS/ES Version 4 OS	No
ACS Software	One or more Cisco Secure Access Control Server (ACS) Version 4.2	Yes
ACS host OS	Windows 2000/2003 Server to host the ACS Software	No
Location Appliance	One or more Cisco 2710 Wireless Location Appliances running version 3.1.38.0	Yes
Kiwi Syslog Daemon or Syslog-ng	One or more of the following: • Kiwi Syslog Daemon Version 8.3.30, or • Syslog-ng Version 2.0.9	Yes
Syslog host OS	For Kiwi: • Windows 2000 or 2003 Server For Syslog-ng: • Red Hat Enterprise Linux Version 4 or 5	No

Figure 1 depicts a sample TOE configuration, highlighting the physical boundary. The shaded portions define the components in the physical boundary. The un-shaded portions define the components supplied by the IT Environment.

.

[1] Note that Figure 1 shows the 4400 Controller or the 6500 WiSM among the entities connected to the wired network. This is representative of the fact that these two controllers have identical interfaces and functionality.

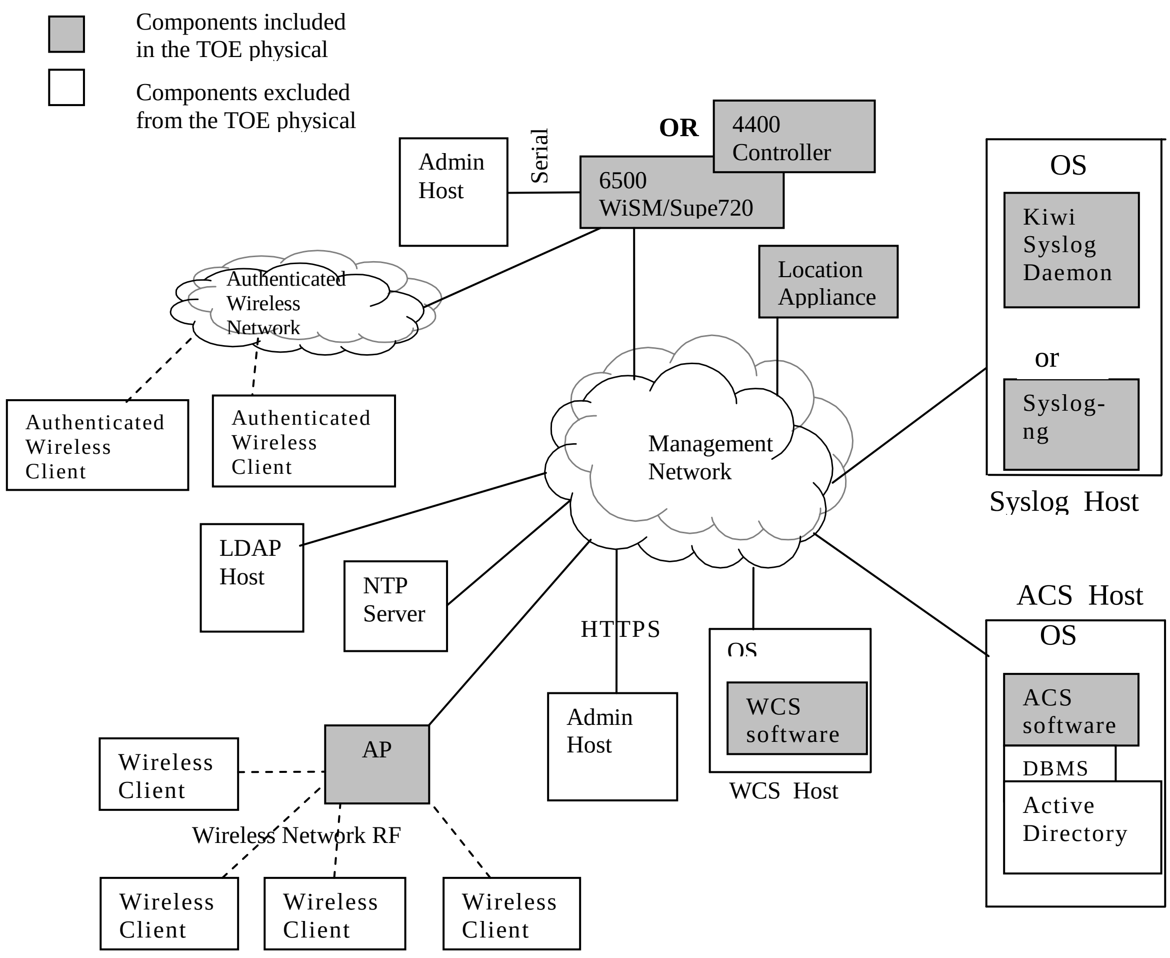

Figure 1: TOE Physical Boundary – Remote Access Configuration

.

3.3 TOE Logical Boundary

This section identifies the security functions that the TSF provides.

- Administration (FMT)
- Audit (FAU)
- Encryption (FCS)
- Identification and Authentication (FIA)
- Information Flow Control (FDP)
- Self Protection (FPT)

3.3.1 Administration (FMT)

The TOE's Administrator security functions provides security capabilities that guarantees all administrators are required to identify and authenticate to the TOE before any administrative or monitoring actions can be performed. The TOE only allows administration of the TOE to occur from the wired network. The TOE's Management Security Capability provides administrator support functionality that enables a human user to configure and manage TOE components.

3.3.2 Audit (FAU)

The TOE's Audit security function supports audit record generation and selective audit record generation functionality. The TOE's audit data viewing capability provides administrator support functionality that enables administrators to view audit records and selective view audit records along with allowing them to selectively choose what events they want audited.

- The TOE will generate a WIDS audit record that contains events about an IT system.
- The TOE monitors the wireless network traffic and performs analysis based on the information it has collected and generates events/alerts for potential intrusions that it has identified. The TOE has 17 standard Wireless Intrusion Detection Signatures (WIDS) which it uses to detect unauthorized or threatening WLAN activity including the following:
  - Denial of service/interference events, including
    - Association Request Flood
    - Reassociation Request Flood
    - Broadcast Request Flood
    - Disassociation Flood
    - Deauthentication Flood
    - EAPOL Flood
  - Events matching attack signatures, including
    - NULL Probe Response – Zero length SSID element
    - NULL Probe Response – No SSID element
    - Broadcast Deauthentication Frame
    - Reserved Management sub-types 6 and 7
    - Reserved Management sub-type D
    - Reserved Management sub-types E and F
    - NetStumbler 0.3.20
    - NetStumbler 0.3.23
    - NetStumbler 0.3.30
    - NetStumbler Generic
    - Wellenreiter
- Additionally, all administrator actions related to the management of TSF data and configuration data are logged by the TOE's audit generation functionality.

These audit records are viewable through the TOE's audit data viewing capability.

3.3.3 Encryption (FCS)

The TOE's wireless network Encryption security function ensure that when an administrator has configured encryption that all network packet data payloads are encrypted with the scheme defined by the administrator for those flows of information occurring in the RF domain. This allows for the TOE to provide end-to-end encryption capabilities between wireless clients, trusted APs and trusted nodes that reside within the TOE.

3.3.4 Identification and Authentication (FIA)

The TOE's Identification and Authentication security function provides I&A support of all wireless client hosts connecting to the trusted wired network from the wireless network along with providing I&A support to make sure all administrators are properly identified and authenticated before accessing TOE functionality.

3.3.5 Information Flow Control (FDP)

The TOE's Information Flow Control security function provides control of information by enforcing the encryption scheme that has been administratively configured.

3.3.6 Self Protection (FPT)

The TOE provides for non-bypassability and domain separation of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by a user by controlling a user session and the actions carried out during a user session. By maintaining and controlling a user session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered or tampered with for those users that are within the TSC.

4 Assumptions

The following assumptions were made during the evaluation of WLAN:

Administrators are non-hostile, appropriately trained and follow all administrator guidance.

There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

There will be only one human user performing WCS administrator configuration and review functions.

The syslog communications between the TOE components must happen over a separate protected network from the wireless client network.

On the syslog host, all users are considered to be Syslog administrators

5 Documentation

The following documentation was used as evidence for the evaluation of the WLAN:

5.1 Configuration Management

1. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Configuration Management and Flaw Remediation Documentation, Version 13, February 23, 2009

5.2 Delivery and Operation

1. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Installation, Generation and Startup Documentation, Version 17.0, February 19, 2009
2. Delivery Documentation for Cisco Unified Wireless, Version 4.0, February 18, 2009

5.3 Design Documentation

1. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Functional Specification, Version 13.0, February 5, 2009
2. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) High Level Design, Version 13.0, February 5, 2009
3. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Platform Representation Correspondence, Version 5.0, February 23, 2009

5.4 Guidance Documentation

1. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Administrator Guide, Version 13.0, February 23, 2009

2. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) User Guide, Version 10.0, February 6, 2009
3. Cisco Location Appliance Configuration Guide Version 3.1 October 2007 (Text Part Number: OL-14430-01)
4. User Guide for Cisco Secure Access Control Server for Windows Release 4.2 (Text Part Number: OL-14386-02)
5. Cisco Wireless Control System Configuration Guide Software Release 4.2, October 2007 (Text Part Number: OL-14610-01)

5.5 Life Cycle

1. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Configuration Management and Flaw Remediation Documentation, Version 13, February 23, 2009

5.6 Testing

1. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Test Coverage, Version 13, February 23, 2009

5.7 Vulnerability Assessment

1. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Strength of Function, Version 9.0, February 23, 2009
2. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Vulnerability Analysis, Version 8.0, February 23, 2009

6 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Cisco WLAN, Version 1.0, March 2, 2009.

6.1 Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces in the design. These security functions include:

- Administration
- Audit
- Encryption
- Identification and Authentication

- Information Flow Control
- Self Protection

6.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Evaluated Configuration Guide, reran most (94%) developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team ran its tests on the configuration depicted in Figure 2. The configuration presented is representative of the possible combinations of the TOE components because it includes a model of each TOE component and provides clients to use/attack to the TOE for common usage. The evaluation team verified the hardware models and software versions of each component during testing. The VLAN Admin Network represents the Management Network depicted in Figure 1.

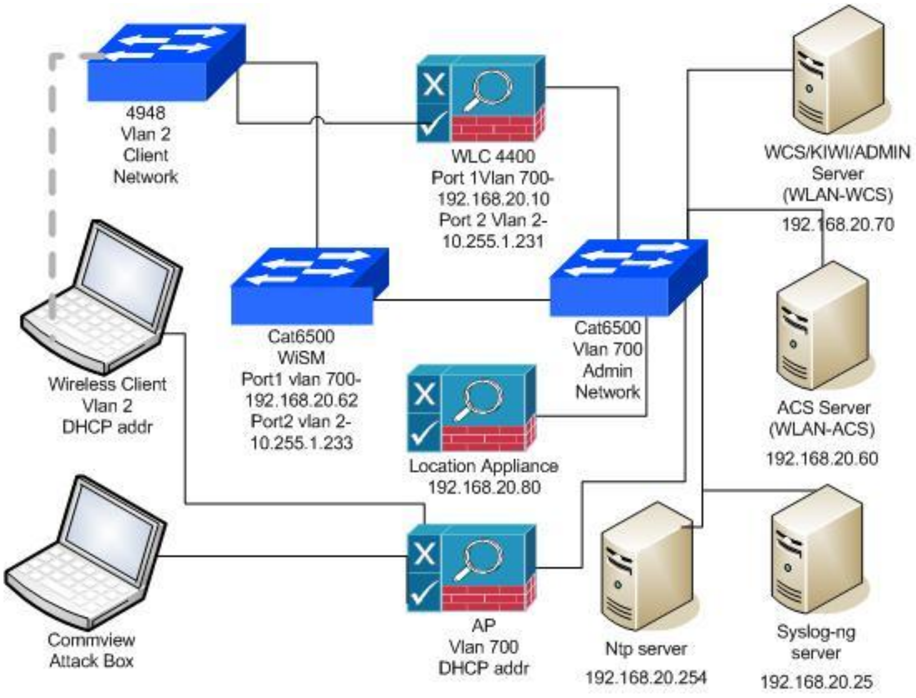

Figure 2 Test Configuration

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is:

1. Cisco Aironet 1130 AG Series Access Point hardware and WLAN software image version 4.1.185.10 FIPS, Cisco Aironet 1230 AG Series Access Point hardware and WLAN software image version 4.1.185.10 FIPS, and Cisco Aironet 1240

AG Series Access Point hardware and WLAN software image version 4.1.185.10 FIPS;

2. Cisco 4400 Series Wireless LAN Controllers hardware and WLAN software image version 4.1.185.10 FIPS;
3. Cisco Catalyst 6500 Series Wireless Integrated Services Module (WiSM) (Version 4.1.185.10 FIPS), 720 Supervisor blade (version 12.2(18)SXF15A) and all software running on both cards;
4. Wireless Control System (WCS) Version 4.2.97.0 software distribution
5. Secure Access Control Server (ACS) Version 4.2.0.124.8 software distribution
6. Cisco Wireless Location Appliance series 2710 (Software version 3.1.38.0)
7. Syslog, the Kiwi Syslog Daemon Version 8.3.30 software distribution or the Syslog-ng version 2.0.9 software distribution

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco Wireless Local Area Network Access System with Integrated Wireless Intrusion Detection System (WIDS) Installation, Generation and Startup Documentation, Version 17.0, February 19, 2009** document.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL2 augmented with ACM_SCP.1, ALC_FLR.2, and AVA_MSU.1 work units received a passing verdict.

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 2.3] and CEM version 1.0 [5], [6]. The evaluation determined the Cisco WLAN TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) augmented with ACM_SCP.1, ALC_FLR.2, and AVA_MSU.1 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

8.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the WLAN product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 augmented with ACM_SCP.1 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified

8.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team verified the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, and a high-level design document,. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 augmented with AVA_MSU.1 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.9 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of a sample of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

The validators would like to call the attention of potential customers to the fact that this evaluation is for a collection of interrelated products rather than just one (perhaps monolithic) product as is the usual CCEVS practice. Customers should make sure they are buying all the parts they need for their situation.

10 Annexes

Not applicable.

11 Security Target

The Security Target is identified as Cisco Unified Wireless Network & Wireless Intrusion Detection System Security Target, Version 1.0, March 23, 2009

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.3, August 2005.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.3, August 2005.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.3, August 2005.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

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

[7] Science Applications International Corporation. *Evaluation Technical Report for the* Cisco Unified Wireless Network & Wireless Intrusion Detection System *Part 2 (Proprietary),* Version 1.1, March 24, 2009.

[8] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco WLAN, ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 1.0, March 2, 2009.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Cisco Unified Wireless Network & Wireless Intrusion Detection System Security Target, Version 1.0, March 23, 2009