

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

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

Cisco Wide Area Application Services

Report Number: CCEVS-VR-10314-2010
Dated: 31 August 2010
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

Franklin Haskell

Mitre Corporation

McLean, VA

John Nilles

Aerospace Corporation

Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton

Eve Pierre

Quang Trinh

Science Applications International Corporation

Columbia, Maryland

Table of Contents

1	Executive Summary	1
2	Identification	1
3	Architectural Information	3
3.1	TOE Overview	3
3.1.1	TOE Product Type	3
3.1.2	Required non-TOE Hardware/ Software/ Firmware	3
3.2	TOE Description	4
3.3	Physical Scope of the TOE	4
3.3.1	Cisco WAVE 274, 474, 574, Cisco WAE 674, 7341 and 7371	4
3.3.2	Cisco NME-WAE 502 and 522	6
3.3.3	Cisco WAE Inline Network Adapter	6
3.3.4	Cisco WAAS 4.2.1 Software	7
4	Security Policy	7
4.1.1	Security Management	8
4.1.2	Access Control	8
4.1.3	Audit	8
4.1.4	CIFS File Cache	9
4.1.5	Identification and Authentication	9
4.1.6	Self Protection	10
5	Assumptions	10
6	Documentation	11
6.1	Design Documentation	11
6.2	Guidance Documentation	11
6.3	Life Cycle	11
6.4	Testing	12
7	IT Product Testing	12
7.1	Developer Testing	12
7.2	Evaluation Team Independent Testing	12
8	Evaluated Configuration	12
9	Results of the Evaluation	13
9.1	Evaluation of the Security Target (ASE)	13
9.2	Evaluation of the Development (ADV)	13
9.3	Evaluation of the Guidance Documents (AGD)	14
9.4	Evaluation of the Life Cycle Support Activities (ALC)	14
9.5	Evaluation of the Test Documentation and the Test Activity (ATE)	14
9.6	Vulnerability Assessment Activity (AVA)	15
9.7	Summary of Evaluation Results	15
10	Validator Comments/Recommendations	15
11	Annexes	15
12	Security Target	15
13	Glossary	16

14 Bibliography 16

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Wide Area Application Services solution (henceforth referred to as WAAS). 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 July 2010. 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 4 augmented with ALC_FLR.1.

The TOE is Wide Area Application Services provided by Cisco Systems, Inc. The Wide Area Application Services [WAAS] is an application acceleration and WAN optimization solution allowing IT organization to consolidate costly branch office servers and storage into centrally-managed data centers and to deploy new applications directly from a data center, while still offering LAN-like application performance regardless of location. The solution helps to optimize the performance of any TCP-based application operating over a Wide Area Network (WAN) environment.

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 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). 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 reviewed evaluation evidence, work units and successive versions of the ETR. The validation team concurs with the CCTL conclusion the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST).

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.1) have been met.

The technical information included in this report was obtained from the Cisco Wide Area Application Services Security Target and analysis performed by the Validation Team.

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 Wide Area Application Services solution including: Wide Area Virtualization Engine (WAVE) 274, 474, 574; Wide Area Application Engine (WAE) 674, 7341 and 7371; WAE Network Module (NME-WAE) NME-WAE 502, NME-WAE 522 and WAE Inline Network Adapter. The software version is Cisco WAAS version 4.2.1
Protection Profile	None
ST:	Cisco Wide Area Application Services Security Target, Version 20, May 2010
Evaluation Technical Report	Evaluation Technical Report For the Cisco Wide Area Application Services (WAAS) (Proprietary,)Version 0.2, May 28, 2010
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 2 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

Item	Identifier
CCEVS Validators	Franklin Haskell, Mitre Corporation, McLean, VA
	John Nilles, Aerospace Corporation, McLean, VA

3 Architectural Information

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

3.1 TOE Overview

3.1.1 TOE Product Type

The Cisco WAAS (TOE) is a network application delivery solution for Wide Area Networks (WANs) – geared for branch and mobile employee deployments. By deploying WAAS, IT organizations can consolidate costly branch-office servers and storage in centrally managed data centers, and to deploy new applications directly from the data center, while offering LAN-like application performance for remote users. The WAAS defined in this ST covers multiple hardware appliance products loaded with the WAAS 4.2.1 software package, which comprises the solution.

The TOE consists of hardware and software used to provide application services acceleration between client machines (workstation) and the application servers (e.g., Web servers, file servers). The TOE is the WAAS solution running software v4.2.1.

3.1.2 Required non-TOE Hardware/ Software/ Firmware

The TOE requires (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 1: IT Environment Components

IT Environment Component	Required	Usage/Purpose Description for TOE performance
Cisco 2811, 2821, 2851, 3825 and 3845 routers; running Cisco IOS software 12.4(9)T or 12.4(9)T1	Yes, for NME-WAE 502 TOE component only	The NME-WAE which is a pluggable module for routers is dependent on its IT Environment, the router, to supply the power it needs to run.
Cisco 3825 and 3845 routers; running Cisco IOS software 12.4(15)T	Yes, for NME-WAE 522 TOE component only	The NME-WAE which is a pluggable module for routers is dependent on its IT Environment, the router, to supply the power it needs to run.
Web browser	YES	Administrators will use to communicate with the TOE; GUI administrative web interface. The recommended web browser is Internet Explorer version 5.5 or higher.
SSH Client	YES	Administrators will use to communicate with the TOE via CLI administrative interfaces. Any SSH

IT Environment Component	Required	Usage/Purpose Description for TOE performance
		client may be used. Examples include, PuTTY
NAS or File Servers for which CIFS file-caching is optimized by WAAS	YES	These servers will contain the files for which the TOE optimizes access.
Other application servers for which TCP traffic is optimized by WAAS	YES	These servers provide applications that are optimized by the TOE.
Authentication, Authorization, and Accounting (AAA) server (RADIUS, TACACS+ and Windows Authentication servers)	OPTIONAL	The TOE may optionally be configured to use IT Environment supplied services. If configured to use these services, communication is over trusted channels.
Time Server	OPTIONAL	Optionally provide time stamps in deployment scenarios in which an external time source is desirable.

3.2 TOE Description

This section provides an overview of the Cisco WAAS Target of Evaluation (TOE). This section also defines the physical and logical boundaries, summarizes the security functions, and describes the evaluated configuration.

3.3 Physical Scope of the TOE

The following lists the products included in the TOE physical scope of the TOE and described in the following sections.

1. Cisco WAE 674, 7341 and 7371;
2. Cisco WAVE 274, 474, 574;
2. Cisco NME-WAE 502 and 522;
3. Cisco WAAS 4.2.1 Software;
4. Cisco Wide Area Application Services Configuration Guide software release 4.2.1;
5. Cisco Wide Area Application Services Command Reference Software release 4.2.1

3.3.1 Cisco WAVE 274, 474, 574, Cisco WAE 674, 7341 and 7371

The TOE includes the complete hardware and software solution provided in the Cisco appliances WAVE 274, 474, 574 and WAE 674, 7341 and 7371. All these appliances execute the same software load WAAS 4.2.1. The difference between the WAVE appliances and the WAE appliances is that the WAVE appliances include the ability to provide virtualization services for locally hosted IT services. Virtualization is excluded from the evaluated configuration. In the evaluated configuration all TOE appliance operate identically. The following tables identify the physical configurations of the WAE and WAVE appliances.

Table 2: TOE WAE Devices Physical Specification

	WAE 674	WAE 7341	WAE 7371
SW Version	4.2.1	4.2.1	4.2.1
DRAM	4 or 8 GB	12 GB	24 GB
Hard Drive	600 GB Hard Drive	900 GB	1.5 TB
Inline Card	4-port inline card	4-port inline card	4-port inline card
Interfaces	(2) 10/100/1000BASE-T	(2) 10/100/1000BASE-T	(2) 10/100/1000BASE-T
Power	(1) 835W hot-swap AC Redundant power available	(2) 835W hot-swap AC	(2) 835W hot-swap AC

Table 3: TOE WAVE Devices Physical Specification

	WAVE 274	WAVE 474	WAVE 574
SW Version	4.2.1	4.2.1	4.2.1
DRAM	3 GB	3 GB	3 GB or 6 GB
Hard Drive	250 GB Hard Drive	250 GB Hard Drive	500 GB Hard Drive
Inline Card	4-port inline card	4-port inline card	4-port inline card
Interfaces	(1) 10/100/1000BASE-T	(1) 10/100/1000BASE-T	(2) 10/100/1000BASE-T
Power	One 240W AC	One 240W AC	One 400W AC

These WAE and WAVE appliances can be logically configured as either a Central Manager (CM) or as an application accelerator. The table that follows describes the configurations of the WAE and WAVE appliances.

Table 4: TOE Device Role Description

Device Role	Description
Application Accelerator: Branch (WAE/WAVE//NME- WAE)	The branch device is a client-side, optionally file-caching device that serves client requests at remote sites and branch offices. As a general optimization device, the device acts as a client-side optimization entity of the two-device solution, optimizing the TCP connections going through the device. As a file-caching device, the device is deployed at each branch office or remote campus providing near-LAN access to a cached view of data center server files/folders. For non-cached files the branch device forwards the request to the data center WAE. On getting a response, the branch device can choose to cache the file that the client requested and is getting served.
Application Accelerator: Data Center (WAE/WAVE only)	The data center device is a server-side component that resides at the data center and connects directly to one or more application servers, file servers, or network-attached storage (NAS). As a general optimization device, the device acts as a server-side optimization entity of the two-device solution, optimizing the TCP connections going through the device. As a head-end of a file-caching solution, requests received from branch devices over the WAN are translated by the data center device into its original file server protocol and forwarded to the appropriate file server. When the data center file server responds, the device forwards the response back to the branch device.

Central Manager (CM) (WAE/WAVE only)	For every WAAS solution, the TOE must have one primary WAAS Central Manager (CM) device that is responsible for managing the other devices in the solution. The CM device hosts the WAAS Central Manager GUI which is a Web-based interface that allows administrators to configure, manage, and monitor the WAAS devices that make up the TOE solution. The CM resides on a dedicated WAE/WAVE appliance.
---	--

3.3.2 Cisco NME-WAE 502 and 522

The TOE includes the router pluggable module, NME-WAE. This module executes the WAAS 4.2.1 software load. The NME-WAE can only be configured to be an application accelerator device in the evaluated Redirection Configuration. The only differences between the NME-WAE (502 and 522) and the Cisco appliances WAVE 274, 474, 574 and WAE 674, 7341 and 7371 are that (a) the NME-WAE is loadable/pluggable into a Cisco router and (b) NME-WAE cannot be used in inline configuration. The TOE boundary for the NME-WAE encompasses the complete hardware and software product of the NME-WAE. The router is considered part of the IT environment and considered a remote trusted IT product. The following table identifies the physical configurations of the NME-WAE module.

Table 5: TOE NME-WAE Physical Specification

	NME-WAE 502	NME-WAE 522
SW Version	4.2.1	4.2.1
DRAM	1 GB	2 GB
Hard Drive	120 GB	160 GB
Inline Card	Not supported	Not supported
Interfaces	10/100/1000 Gigabit Ethernet connectivity to router backplane	10/100/1000 Gigabit Ethernet connectivity to router backplane
Power	Provided by router	Provided by router
Supported Routers	Cisco 2811, 2821, 2851, 3825, or 3845	Cisco 3825 or 3845
Supported Router SW	12.4(9)T or 12.4(9)T1	12.4(15)T




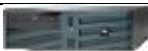



3.3.3 Cisco WAE Inline Network Adapter

The TOE includes the Cisco WAE inline network adapter which provides an inline traffic interception capability - attributes may be set by the administrator to control which interfaces are to be used over which VLANs. By default, the inline adapter operates on all inline-capable interfaces and VLANs. The administrator may configure the inline redirection feature using the CLI or Central Manager GUI. The inline network adapter is a PCI-X or PCIe network interface card that contains two pairs of Gigabit Ethernet ports (LAN and WAN).

The table that follows shows each TOE component and identifies the roles that each can assume.

Table 6: TOE NME-WAE Physical Specification

TOE Component	Possible Roles
----------------------	-----------------------

WAE 674		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAE 7341		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAE 7371		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAVE 274		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAVE 474		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAVE 574		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
NME-WAE 502		Application Accelerator: Branch Application Accelerator: Data Center
NME-WAE 522		Application Accelerator: Branch Application Accelerator: Data Center

3.3.4 Cisco WAAS 4.2.1 Software

The TOE includes the software load WAAS 4.2.1. The physical boundary is the complete image binary of the WAAS 4.2.1 release. This software includes a version of Linux kernel version 2.6 customized for use as part of the WAAS solution.

4 Security Policy

This section summarizes the security functionality of the TOE:

- Security Management
- Access Control
- Audit
- CIFS File Cache
- Identification and Authentication
- Self Protection.

4.1.1 Security Management

The TOE's Security Management functionality provides management support functionality that enables a human user to manage and configure the TOE securely. The Security Management functionality guarantees that management actions can only be performed after an authorized user has been authenticated. An authorized user is one who has been successfully identified and authenticated. The TOE manages user roles to ensure restricted access to the security functions, acceleration services, and data of the TOE to only those users that are authorized for a specific service. The TOE can be managed locally or remotely by the administrator.

The TOE's Security Management functionality ensures that users are only allowed access to resources that they have been explicitly authorized to use. Authorized users are only allowed to carry out operations associated with their assigned role as follows:

- The TOE controls which users can modify and configure the security settings of the TOE.
- This security function controls which users can change and configure the file services acceleration policies and file caching policies of the TOE as defined by FDP_ACC.1(2) and FDP_ACF.1(2).

4.1.2 Access Control

The TOE provides the ability to control traffic flow through the TOE.

An IP ACL (permit/deny) policy is an administratively configured access control list that is applied to traffic destined for the TOE management interfaces. IP ACLs can filter traffic (permit or deny traffic flow) based on the following: Source IP address, Destination IP address, Protocol, Source Port, and Destination Port.

Note: These access controls are designed as protection for access to the TOE itself and not meant to filter traffic passed through the TOE.

4.1.3 Audit

The TOE's Audit functionality supports audit record generation, storage, and audit review by authorized users. Audit records are stored in a combination of syslog and errlog files on the hard drive of the TOE devices. The appliance (WAE/WAVE) and module (NME-WAE) TOE devices maintain time to generate a reliable timestamp which is applied to each audit event record. The TOE solution can optionally be configured to receive initial time from the IT environment (i.e., NTP Server).

Both the application accelerator and Central Manager TOE components generate and store audit records. The application accelerator TOE component provides that ability to view

locally stored audit record relevant to the device. The Central Manager provides the ability to view all audit records relevant to all TOE devices. The application accelerator TOE components forward local audit records to the Central Manager at regular intervals.

4.1.4 CIFS File Cache

The TOE's File Cache Security Function relies on the IT Environment file server(s) to enforce file permission access controls for cached files.

The TOE's File Cache Security Function also protects user data by using encrypted storage (encrypted file system) for the cached files.

The TOE's File Cache function includes user data pre-positioning capability – a feature to fill the cache periodically in order to provide cache-hit performance even for a first user. This feature includes: (1) initiating CIFS connection to the server, (2) passing server authentication, and (3) reading file data and meta-data and storing the in the cache. File meta-data that is stored in cache include various file attributes, file access control lists (ACLs) and permissions. The File Cache function uses a “pre-position user” credential that has been configured in the IT environment. This is similar to other users that access the file server except that the TOE itself initiates the connection with the user credentials for the purposes of pre-positioning files. Branch WAE devices use user name and password to retrieve preposition from the file server via Data Center WAE device. The credentials associated with the “pre-position user” are input by the TOE administrator into the IT environment file server as an authorized user. The Credentials are also input into the TOE during configuration by the TOE administrator. The credentials are stored internal to the TOE and are never output to unauthorized users. No direct user access is provided to any cached file using the preposition credentials. These credentials are input into the TOE and stored within the TOE as other TOE configuration information. Only the default TOE administrator and administrators whose associated role is defined with the necessary permission can access the credentials. Access is only granted after the authorized administrator is successfully authenticated by the TOE.

4.1.5 Identification and Authentication

This functionality requires administrators that manage and configure the TOE to successfully authenticate before they are allowed to carry out any other actions that are mediated by the TOE. Proper and successful authentication is required for all user interfaces of the TOE. Successful identification and authentication of administrators is required whether the administrator is security relevant or non-security relevant. A non-security relevant is an administrator for which the associated role has no access to security relevant functionality. The TOE supports local and remote administration. Remote administration is only allowed using SSH or HTTPS protected communications. By default, the TOE uses the local authentication database to verify user credentials. The TOE can optionally be configured to use an external authentication server instead of the TOE's local authentication database. To support external authentication, the administrator must

explicitly configure the TOE to support additional authentication methods. The TOE administrator can configure the types of authentication supported and order in which the authentication method is applied.

When an application accelerator device is activated, a unique hash tag is associated with the device and exchanged with the device. This tag is used by the device to identify itself in all future communication with the CM.

4.1.6 Self Protection

The TOE solution includes multiple hardware components containing non-modifiable software, in which, all operations in the TSF scope of control are protected from interference and tampering by untrusted subjects. All administration and configuration operations are performed within the physical boundary of the TOE. The TOE has been designed so that TSF data, User data, and Security Attributes within the TSF Scope of Control can only be manipulated via the TOE CLI and GUI interfaces which mediate all actions through these interfaces.

Communications between TOE components (branch, data center, and CM) are protected by Transport Layer Security (TLS) with the exception of the Print Services UI which is not used in the evaluated configuration. The TOE protects remote management and configuration sessions with SSH version 2 and HTTPS.

The TOE can control the termination of a CLI or GUI session based on a settable inactive session parameter. After the set amount of time of inactivity has been reached, the TOE will terminate the interactive session. The TOE will also terminate a Secure Shell (SSH) session that is being negotiated after a configurable inactivity period while the negotiation occurs.

All sensitive data on the TOE in persistent storage, such as files and database, are encrypted using strong encryption (AES 256). Strong encryption is enforced when Secure Store feature is enabled on both CM and WAE.

The cryptography within the TOE has not been FIPS validated. The strength of the cryptographic operations performed by the TOE is vendor asserted.

The TOE cannot be bypassed, corrupted, or otherwise compromised.

5 Assumptions

The following assumptions were made during the evaluation of WAAS:

- The Management LAN is trusted. All services such as optional external AAA servers, or NTP servers are provided by the management LAN, and all devices attached to the management LAN are trusted to perform in a secure manner.

- Administrators of the TOE are assumed to be non-hostile, trusted to perform their duties in a secure manner, and expected to follow all security policies and procedures applicable to their deployment.
- All TOE components are assumed to be in a physically secure environment.
- Clock sources external to the TOE are configured accurately so as to provide a trusted clock source to the TOE's internal clock.
- Interconnected switches and routers, which are part of the IT Environment, that communicate with the TOE components that make up the WAAS solution are assumed to have protection against unauthorized access.

6 Documentation

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

6.1 Design Documentation

1. Cisco Wide Area Application Services (WAAS) Functional Specification, Version 12, April 2010
2. Cisco Wide Area Application Services (WAAS) High Level Design, Version 10, March 2010

6.2 Guidance Documentation

1. Cisco Wide Area Application Services (WAAS) Common Criteria EAL4+ Administrator Guide, Version 5.0, May 2010
2. Cisco Wide Area Application Services Configuration Guide, Software Release 4.2.1, June 22, 2010
3. Cisco WAAS Quick Configuration Guide, Software Release 4.2.1, June 22, 2010
4. Configuring Cisco WAAS Network Modules for Cisco Access Routers, January 7, 2009
5. Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide, October 2008
6. Cisco Wide Area Application Services Command Reference, Software Release 4.2.1, June 22, 2010

6.3 Life Cycle

1. Cisco Wide Area Application Services (WAAS) Configuration Management Plan and Delivery Procedures, Version 3.0, March 2010

6.4 Testing

1. Cisco Wide Area Application Services (WAAS) Common Criteria Test Plan and Coverage Analysis, Version 14, April 2010
2. Actual test Results, WAAS Test Evidence.doc

7 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 Wide Area Application Services, Version 1.0, May 2010.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification and high level design. 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:

- Security Management
- Access Control
- Audit
- CIFS File Cache
- Identification and Authentication
- Self Protection

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Evaluated Configuration Guide, reran a sample of the 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.

While all TOE hardware models are functionally tested, only the 502, 674 (2), and 7371 were included in the Common Criteria test configuration with test results/output recorded by Cisco. Additionally, the test bed includes a 274; 474; and 522 (housed in an ISR 3825 router) that the team used for its testing. Since the code and hence security functionality is the same among the platforms, the evaluation team is going to sample to platforms.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Cisco Wide Area Application Services solution including:

- Wide Area Virtualization Engine (WAVE) 274, 474, 574;
- Wide Area Application Engine (WAE) 674, 7341 and 7371;
- WAE Network Module (NME-WAE) NME-WAE 502, NME-WAE 522

- WAE Inline Network Adapter
- Software release 4.2.1

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco Wide Area Application Services (WAAS) Common Criteria EAL4+ Administrator Guide, Version 7, August 2010** document.

9 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 EAL4 augmented with ALC_FLR.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 1.1] and CEM version 3.1. The evaluation determined the Cisco WAAS TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.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.

9.1 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 WAAS 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.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 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 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.

9.3 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.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE. The ALC evaluation also 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 evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Cisco.

In addition to the EAL 4 ALC CEM work units, 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.

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

The evaluation team applied each EAL 4 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 and high level design 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.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's 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.

9.7 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 the entire 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.

10 Validator Comments/Recommendations

The validators noted the following.

No audit record is generated when the audit system is shutdown. If the customer is depending upon a steady stream of audit records then the customer should ensure that some sort of record should appear in some log indicating that audit has been disabled.

Customers should be sure to understand the implications of setting ACLs on each WAAS device.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Cisco Wide Area Application Services Security Target, Version 20, May 2010*.

13 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.

14 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 3.1, Revision 2, dated: September 2007.
- [2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.
- [3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

- [4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security: Evaluation Methodology*, Version 3.1, Revision 2, dated: September 2007.
- [5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 2.0, September 2008.
- [6] Science Applications International Corporation. *Evaluation Technical Report for the Cisco Wide Area Application Services Part 2 (Proprietary)*, Version 0.2, May 28, 2010.
- [7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco Wide Area Application Services, ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 3.0, August 2010.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.
- [10] Cisco Wide Area Application Services Security Target, Version 20, May 2010.