National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco Systems ACE XML Gateway and Manager Version 5.0.3

Report Number:	CCEVS-VR-VID10076-2008
Dated:	12 August 2008
Version:	1.5

**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

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Systems ACE XML Gateway and Manager Version 5.03. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of Cisco Systems ACE XML Gateway and Manager Version 5.0.3 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 26 March 2008.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and meets the assurance requirements of EAL 3 augmented with ALC_FLR.2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is ACE XML Gateway and Manager Version 5.03 provided by Cisco Systems, Inc. The TOE is an application and supporting operating system that is run on an x86 architecture computer system. The TOE is a self-contained IT appliance that can be configured to run as a Cisco ACE XML Gateway, as a Cisco ACE XML Manager, or as both Gateway and Manager simultaneously. The evaluated configuration excludes the configuration that runs both the Manager and the Gateway simultaneously on a single ACE XML appliance. The ACE XML Gateway stands between an untrusted network (the Internet) and a trusted network (such as a restricted-access corporate intranet). All traffic between the two networks must pass through the Gateway. The Gateway allows only authorized traffic to pass from the untrusted network to the trusted network. Authorized administrators specify the criteria that traffic must meet in order to pass through the Gateway. The Gateway blocks traffic that does not meet these criteria. The Gateway generates an audit trail that documents the performance of the Gateway, the disposition of every message it processes, and other security-relevant events. The ACE XML Manager provides a graphical user interface (GUI) that authorized administrators use to specify the message-processing behavior of the Gateway, monitor the performance of the Gateway, and manage the Gateway remotely. The Manager GUI provides a means of viewing the audit trail generated by all Gateways in the scope of the Manager's control and the activities of the users of the Manager.

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 adduced. This Validation Report is not an endorsement of the Cisco Systems ACE XML Gateway and Manager Version 5.0.3 product by any agency of the US Government and no warranty of the product is either expressed or implied.

During this validation, the Validators reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The Validator determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

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

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; and
- 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 Systems ACE XML Gateway and Manager Version 5.0.3
Protection Profile	Not applicable.
ST:	Cisco Systems, Inc. ACE XML Gateway and Manager Version 5.0.3 Security Target, Version 1.0, 25 July 2008
Evaluation Technical Report	Evaluation Technical Report for Cisco Systems ACE XML Gateway and Manager Version 5.0.3, Part 1 (Non-Proprietary), Version 2.5, 5 June 2008, Part 2 (Proprietary), Version 2.0, 25 July 2008

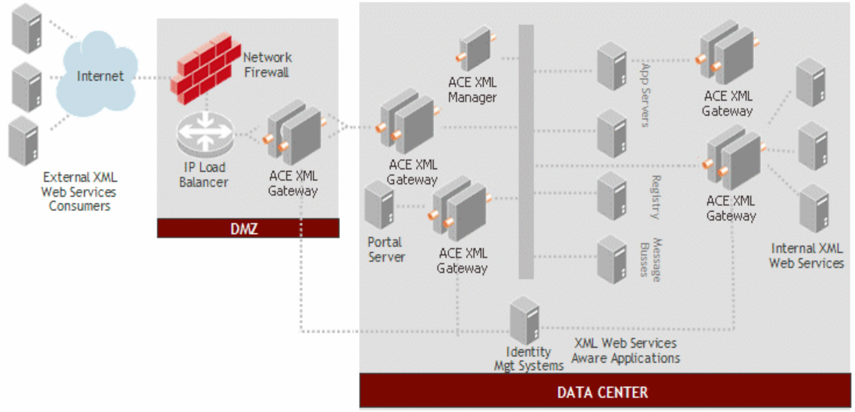
Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Conformance Result	CC Part 2 conformant and Part 3 conformant, EAL 3 augmented with ALC_FLR.2
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation (SAIC), Columbia, MD
CCEVS Validator	Kenneth Eggers, Orion Security Solutions, Inc. and John Nilles, Aerospace Corporation

3 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

3.1 Architectural Overview

The TOE is an application-level proxy that processes XML and SOAP messages sent across TCP/IP networks using HTTP(S) protocols. XML is a flexible formal text format derived from SGML and commonly used to define more specialized markup languages for representing computer data. SGML is an ISO-standard language for describing data formats, based on IBM's Generalized Markup Language. SOAP is an XML-based protocol for making remote procedure calls by means of text messages, using HTTP(S) as the transport mechanism. The TOE is depicted in the figure below in the context of its location in the IT environment.



The TOE cannot be bypassed; in order to reach the trusted network, traffic from the untrusted network must pass through the Gateway, subject to the rules the Web Services SFP defines.

3.2 Physical Boundaries

The components that make up the TOE are:

Gateway – The Gateway executable. Subject to the rules of the Web Services SFP, the Gateway proxies XML and SOAP messages sent across TCP/IP networks using HTTP(S) protocols. The Gateway application runs in the context of a custom version of Linux installed on a 1U chassis, which is a Hewlett-Packard DL360 G5 server hardware appliance with nCipher nForce 1600 cryptographic module.

Manager – The Manager application. The Manager application provides a GUI that authorized administrators use to administer the Gateway application; in particular, to define the Web Services SFP that the Gateway enforces. The Manager application runs in the context of an Apache Tomcat application, which runs in the context of a custom version of Linux installed on a 1U chassis (a Hewlett-Packard DL360 G5 server hardware appliance with nCipher nForce 1600 cryptographic module).

Tomcat – Each ACE XML appliance embeds an Apache Tomcat v. 5.0.16 application server that the Manager uses to publish its Web-based GUI.

Shell - A terminal-based program that runs automatically when an authorized administrator logs in to the console of an ACE XML Manager or Gateway machine. The Shell provides tools for low-level administration of ACE XML systems, such as changing network configuration.

Operating system files – A number of operating system files are used by both the Gateway and the Manager for configuration and logging.

Operating System – Each ACE XML appliance embeds a custom, package-reduced installation of the Linux operating system. This operating system runs on the server hardware chassis, hosting the TOE software and the Web server that publishes the Manager GUI.

Server Hardware chassis – The ACE XML appliance is built on a Hewlett-Packard DL360 G5 server hardware chassis. This chassis hosts the Operating System, Application Server, TOE software/firmware and nCipher 1600 cryptomodule. Note that although the cryptomodule resides physically on the server chassis, the ST considers this module to be provided by the IT environment because it is used "off-the-shelf" with no modifications. For local storage, the server chassis provides two 72 GB hard drives configured as a RAID 1 array by the manufacturer of the chassis. The server chassis also has four physical Ethernet ports, and connections for a serial keyboard and VGA monitor.

4 Assumptions

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- The TOE is appropriately scalable to the IT System the TOE monitors and has access to all the IT System data it needs to perform its functions.
- Information cannot flow among the internal and external networks unless it passes through the TOE.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access and modifications.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- Those responsible to manage the TOE are competent individuals, that only authorized users can gain access to the TOE, and that they are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

5 Security Policy

5.1 Threats and Organizational Security Policies

The security objectives to be met by the TOE are generally designed to implement organizational security policies. However, self-protection and non-bypassability can only be described as a threat.

5.1.1 Threats

The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

5.1.2 Organizational Security Policies

The following organizational security policies must be implemented by the TOE and its environment as identified in the Security Target. With the exception of the threat identified in the preceding section, all of the security objectives are derived from these organizational security policies.

- The TOE must provide user accountability for information flows through the TOE and for all use of security functions. The events are audited and presented in a readable format.
- The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
- The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
- The TOE must provide functionality that enables an authorized administrator or user with appropriate security roles to use the TOE security functions, and must ensure that only authorized administrators or users with appropriate security roles are able to access such functionality.
- The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
- The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

The TOE provides a secure environment for the exchange and use of XML, providing protection against malicious content and denial-of-service attacks, and providing confidentiality and integrity of valuable and private messages, and appropriate access control for those services. In addition, the TOE may optionally be configured to provide persistent logging of messages, to interact with external authorization services, and to transform messages during processing.

5.2 Security Functional Policies

The Security Functional Policies (SFPs) implemented by the TOE are based on the set of security policies that support security audit, user data protection, identification and authentication, security management, and protection of the TSF.

Note: Much of the description of the TOE security policy has been extracted from the Security Target.

5.2.1 Security Audit

The TOE generates audit events for the minimum level of audit. The TOE provides Manager GUI interfaces that can be used to read the audit trail. The TOE restricts access to the audit trail, requiring authentication using its local account authentication mechanism.

5.2.2 User Data Protection

The TOE enforces the WEB SERVICES SFP on SOAP or HTTP(S) destination service traffic sent through the TOE from one consumer (subject) to another. The TOE enforces the WEB SERVICES SFP, using "authenticators" to verify the user and group identity of a consumer of a service, using "handlers" to validate incoming messages, using "routes" to pass accepted message to "service descriptors," and using "service descriptors" to manage traffic with SOAP or HTTP(S) destination services according to the WEB SERVICES SFP configuration for a given Web service. The TOE supports multiple message-filtering mechanisms for use by the WEB SERVICES SFP depending on configuration for a given Web service. The TOE includes pluggable authentication modules that can call external authentication servers to verify the user and group identity of a consumer of a service for message-filtering purposes.

5.2.3 Identification and Authentication

The TOE disables user or administrator accounts after three failed login attempts to the Manager. The TOE maintains user identities, authentication data for supported authentication mechanisms, and role information. The TOE offers no TSF-mediated functions until the user is authenticated. The TOE requires username/password for all user accesses to the Manager. The TOE offers no TSF-mediated functions until the user is identified.

5.2.4 Security Management

The TOE restricts the ability to specify the Web Services SFP to authorized administrators. The TOE provides restrictive default values for security attributes used to enforce the WEB SERVICE SFP. The TOE also allows authorized administrators to specify alternative initial values. The TOE restricts the ability to initialize and set user authentication data to authorized administrators. The TOE restricts the ability to modify and reset an account's own password to authorized administrators and users. The TOE restricts the ability to view or query audit records to authorized administrators or users that have been assigned appropriate security roles. The TOE provides authorized administrators with the ability to manage Web services, to manage users, and to manage the audit trail using the Manager. The TOE supports two types of users, authorized administrators and users. The single factory-configured administrator account always has all security roles (in particular, the ConsoleAdmin role), cannot be modified or deleted, and is considered an “authorized administrator”. The second category of administrative user is a user that has been assigned zero or more system-defined roles. The system-defined roles are “Operations”, “Access Control”, MTL (message traffic log), or “Routing” is considered an “authorized administrator” and any other user accounts are considered simply “users.” The non-administrative or user category comprises view-only accounts (External Developer and Policy View) on the Manager.

5.2.5 Protection of the TSF

The TOE can generate reliable time stamps for its own use. The TOE can send handler test messages in order to demonstrate the correct operation of a configured handler, route, service descriptor, Web service, and the underlying network. The TOE can also test its network configuration in order to demonstrate its correct configuration. The TOE uses SSL when managing the Gateway using the Manager to protect TSF data from disclosure. The TOE protects against denial-of-service attacks by blocking traffic after administratively-configurable thresholds are met. The TOE protects against content-based attacks by rejecting messages that contain content marked as blocked. The WEB SERVICES SFP cannot be bypassed by consumers. Similarly, both Gateway and Manager interfaces are restricted to authorized administrators and user account-holders.

Upon startup, the TOE enters a restrictive default state in which no users are logged in, and then resumes normal operation. Because the TOE cannot be bypassed, this default state is secure: the Gateway enforces the current Web Services SFP independently of the Manager, the Gateway accepts changes to the current Web Services SFP only from its Manager, and the user interface to the Manager provides no access to TSFs until the user identifies and authenticates successfully.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation

Document	Version	Date
Cisco Systems, Inc. ACE XML Gateway and Manager Version 5.0.3 Functional Specification Document	0.14	June 4, 2008
Cisco Systems, Inc. ACE XML Gateway and Manager Version 5.0.3 High Level Design Document	0.11	May 23, 2008

Guidance documentation

Document	Version	Date
Using the Cisco Systems ACE XML Gateway and Manager Version 5.0.3, Technical Documentation, Version 5.0.3	5.0.3.200807090224	

Configuration Management documentation

Document	Version	Date
Cisco Systems, Inc. Cisco ACE XML Configuration Management Procedures	Version 1.0	

Delivery and Operation documentation

Document	Version	Date
Cisco Systems ACE XML Gateway and Manager Version 5.0.3 Cisco ACE XML Delivery Procedures	Version 2.0	July 30, 2007
Using the Cisco Systems ACE XML Gateway and Manager Version 5.0.3, Technical Documentation, Version 5.0.3	200807090224	

Life Cycle Support documentation

Document	Version	Date
Cisco Systems ACE XML Development Security and Flaw Remediation Procedures	0.81	08/22/07

Test documentation

Document	Version	Date
Cisco System, Inc. ACE XML Gateway and Manger Version 5.0.3 Common Criteria Specific Functional Tests: Coverage Analysis	Version 0.6	March 23, 2008
Cisco System, Inc. ACE XML Gateway and Manger Version 5.0.3 Common Criteria Specific Functional Tests: Test Plan	Version 0.7	March 25, 2008
Cisco System, Inc. ACE XML Gateway and Manger Version 5.0.3 Common Criteria Specific Functional Tests: Test Plan Part 1 of 3	Version 0.7	March 24, 2008
Cisco System, Inc. ACE XML Gateway and Manger Version 5.0.3 Common Criteria Specific Functional Tests: Test Plan Part 2 of 3	Version 0.7	March 24, 2008
Cisco System, Inc. ACE XML Gateway and Manger Version 5.0.3 Common Criteria Specific Functional Tests: Test Plan Part 3 of 3	Version 0.7	March 24, 2008
Appendix: Test Code Reference,		March 18, 2008

The actual test results have been submitted to the evaluation team in various text files, PDFs, screenshots, and .d, .i, and .s file types. Section 11 of the Test Plan describes how to correlate the log files to the test cases.

Vulnerability Assessment documentation

Document	Version	Date
Cisco Systems ACE XML Gateway and Manager Version 5.0.3 Cisco ACE XML Vulnerability Assessment Procedures	Version 1.8	July 15, 2007

Security Target

Document	Version	Date
Cisco Systems, Inc. ACE XML Gateway and Manager Version 5.0.3 Security Target	1.0	25 July 2008

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, User data protection, Identification and authentication, Security management, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire automated test suite and a subset of the vendor's manual tests. In addition to rerunning the vendor's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

The vendor provided the ACE XML Gateway, ACE XML Manager, and the necessary computers for the test environment.

The following hardware is necessary to create the test configuration:

- Two ACE XML Gateway and Manager (AXG) appliances consisting of a Hewlett-Packard DL360 G5 chassis configured at the Cisco Systems factory with the operating system, hardware cryptomodule, TOE software, firmware, and local storage required to function as instances of:
    - Cisco Systems ACE XML Gateway Version 5.0.3 and
    - Cisco Systems ACE XML Manager Version 5.0.3,

- External serial console – for installation, generation, and startup of TOE and for specified administrative maintenance activities,
- Computer/Workstation on which the authorized administrator's Web browser runs to present the Manager GUI,
- Build machine that is a Linux-based computer configured to provide HTTPUnit, CVS, test scripts, and ACE XML source code,

Backend machine that is a Linux-based computer that utilizes an instance of Apache Tomcat to provide HTTP(S) and SOAP services that SOATest can access only through the Gateway,

- Windows machine that runs the SOATest tool, and Ethernet router,
- CAT 5e cabling, and
- Additional items required to create a functional gigabyte Ethernet network environment.

The following software is required to be installed on the machines used for the test:

- ACE XML Gateway and Manager (AXG) version 5.0.3 (TOE software),
- Test programs,
- Test utility programs,
- SOATest v. 5.1.1—Automated test harness by Parasoft, and
- HTTPUnit v. 1.5.4—automated test harness by Meterware, Inc.

7.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, requires one ACE XML appliance that runs as a dedicated ACE XML Manager only (the "Manager appliance"), and at least one additional ACE XML appliance that runs as a dedicated Gateway only (the "Gateway appliance"). To use the product in the evaluated configuration, the Manager appliance and Gateway appliances must be configured as specified in the section “Creating the Common Criteria Evaluated Configuration,” starting at page 627 of “Using the Cisco Systems ACE XML Gateway and Manager Version 5.0.3, Technical Documentation, Version 5.0.3,” Version 5.0.3.200807090224,

The following features are not included in the evaluated configuration:

- Cryptography: Cryptographic functionalities are provided by the environment in the evaluated configuration.

- LDAP Support for Message Authentication and Authorization: In the Common Criteria evaluated configuration LDAP Support is not allowed for authentication and authorization of messages.
- Java SDK: In the Common Criteria evaluated configuration Java SDK customization or authorization logic is not allowed.
- Message Transformation: In the Common Criteria evaluated configuration transformations specified in the XSL language to messages are not allowed.
- Message Caching: In the Common Criteria evaluated configuration end-user specified message caching is not allowed.
- SNMP Monitoring: In the Common Criteria evaluated configuration SNMP monitoring is excluded.
- System Snapshot diagnostic tool: The use of the system snapshot functionality is not allowed in the Common Criteria evaluated configuration.
- Access Control: Sub-policies: The Common Criteria evaluated configuration does not allow the creation of and excludes the use of sub-policies other than the factory-configured "Shared" sub-policy.
- Access Control: Approval-Based Deployment: The Common Criteria evaluated configuration does not allow the approval-based deployment feature to be enabled.
- Access Control: Alternate Authentication Mechanisms: LDAP: LDAP authentication of Manager user accounts is not allowed in the Common Criteria evaluated configuration.
- Message Routing: Fast path Engine: The Common Criteria evaluated configuration excludes use of the “Reactor” (also known as the Fast Path) message-processing engine.
- Protocols: The Common Criteria evaluated configuration excludes the use of the SMTP, JMS, MQ or TIBCO message protocols for use with handlers and service descriptors.

All communications between Manager and Gateway instances must take place exclusively on the trusted network over a secure, encrypted connection.

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on March 2005. The evaluation confirmed that the Cisco Systems ACE XML Gateway and Manager Version 5.0.3 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 conformant, and assurance requirements (Part 3) for EAL3 augmented with ALC_FLR.2. The details of the evaluation are recorded in the CCTL’s evaluation technical report; Final Evaluation Technical Report for the Cisco Systems ACE XML Gateway and

Manager Version 5.0.3, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Cisco Systems, Inc. ACE XML Gateway and Manager Version 5.0.3 Security Target, Version 1.0, 25 July 2008.

The Validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

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 threats, policies, and assumptions, a statement of security requirements claimed to be met by the Cisco Systems ACE XML Gateway and Manager Version 5.0.3 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 3 augmented with ALC_FLR.2 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, delivery and installation documentation 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.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 3 augmented with ALC_FLR.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 followed the Cisco Systems, Inc. ACE XML Gateway and Manager Version 5.0.3 Common Criteria Specific Functional Tests Test Plan, Version 0.7, 24 March 2008 and the Using the Cisco Systems ACE XML Gateway and Manager Version 5.0.3, Technical Documentation, Version 5.0.3.200807090224 to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 augmented with ALC_FLR.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 high-level design documents. 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.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 3 augmented with ALC_FLR.2 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The Using the Cisco Systems ACE XML Gateway and Manager Version 5.0.3, Technical Documentation, Version 5.0.3.200807090224 was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation Team applied each EAL 3 augmented with ALC_FLR.2 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. To support the ALC evaluation, the Evaluation Team performed a Life Cycle (LC) audit. During the audit, the Evaluation Team witnessed the use of the security measures as described in the LC documentation and sampled records created by using the security procedures.

In addition to the EAL 3 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 systematic procedures exist for managing flaws discovered in the TOE.

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

The Evaluation Team applied each EAL 3 augmented with ALC_FLR.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 and high level design specification. The Evaluation Team exercised the entire set of the vendor automated test suite and performed a sampling (30%) of the vendor's manual test suite. In addition, the Evaluation Team 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.

9.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 3 augmented with ALC_FLR.2 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.

9.9 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 the entire set of the vendor's automated test suite, a sampling (30%) of the vendor's manual test cases, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

11 Security Target

The Security Target is identified as Systems, Inc. ACE XML Gateway and Manager Version 5.0.3 Security Target, Version 1.0, dated 25 July 2008. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 3 augmented with ALC_FLR.2.

12 Glossary

The following definitions are used throughout this document:

Authenticator A security policy component that specifies a collection of subject security attributes and values that positively identifies a message sender to the Web Services SFP. An incoming message must satisfy all of the requirements of a defined authenticator as a prerequisite to further processing by a handler in the same authorization group as the authenticator. An authenticator filters messages (FDP) on values in the headers of a message incoming to the Gateway. Authenticators are not user accounts and a consumer who sends a message to a service the ACE XML Gateway protects has not logged on to the TOE.

Authorization Group A representation of a group composed of authenticators and handlers. Authenticators in an authorization group can access a common set of handlers that route messages to protected services. Satisfying the requirements of an authenticator in the group makes an incoming message eligible for further processing by one of the handlers in the group. The message is not available to handlers outside of the authorization group. The TOE provides authorization groups to ease management of access permissions and to organize authenticators for convenience.

CC Common Criteria

Client Certificate The X.509 certificate that authenticates a client to a server; for example, the certificate that authenticates the sender of a message to the Gateway. Administrators of the Web services SFP can specify that the Gateway use the Distinguished Name value to authenticate the sender of a message for purposes of establishing an SSL connection to the Gateway for processing the message.

CM Control Management

Consumer A client that connects to the ACE XML Gateway in an attempt to gain access to its protected services. Clients do not log into the TOE.

CPU Central Processing Unit

Cryptomodule A hardware module that includes a processor specialized for generating, storing and using keys for cryptographic operations.

Denial-of-service attack An attack in which a service is flooded with so many requests that it becomes unavailable to legitimate users. To prevent Denial-of-Service attacks, the TOE monitors the frequency of incoming requests; when the rate of requests from a particular IP address exceeds a policy-specified threshold, the TOE blocks requests from that address for a policy-specified amount of time.

DO Delivery Operation

EAL Evaluation Assurance Level

GUI Graphical User Interface; a human interface that maps computer functions to graphical objects that the user can manipulate by means of a pointing device to perform tasks. Contrast with command-line interface, which requires the user to type text-based commands to perform tasks.

Handler The component of the Web Services SFP that manages communication with consumers. When an incoming message meets all requirements imposed by an authenticator, the message is eligible for further processing by a handler that is a member of the authenticator's authorization group. The message is not available to handlers outside of the authorization group. A handler specifies the message protocol and network endpoint/port on which the Gateway accepts message traffic, as well as various criteria the incoming message must meet in order to be eligible for further processing by the Web Services SFP. A handler also passes a response from a protected service back to the consumer that made the original request, again subject to all requirements of the Web Services SFP. The ACE XML Manager GUI provides a graphical representation of each handler in the Web Services SFP. Authorized administrators interact with the Manager GUI to create, delete, or modify handlers or other policy objects that define the Web Services SFP.

HTTP header
A text record sent at the beginning of an HTTP or HTTPS message. Request message headers provide information about the client to the server receiving the request, such as the type of browser being used. In addition to information the header is required to provide, it may also include optional values such as the HTTP Basic username and password of the sender. Response message headers provide information from the sever to the client that made the original request; for example, a response message may contain an error code that attempts to explain the reason a request did not succeed.

HTTP(S)
A typographical convention the TOE user interface and documentation uses to indicate use of either of the HTTP or HTTPS protocols. The HTTPS (HyperText Transfer Protocol Secure) protocol is the HTTP protocol conducted in a session managed by a security protocol, such as SSL or TLS.

I/O
Input/Output

PP
Protection Profile

SF
Security Functions

SFR
Security Functional Requirement(s)

SSL
Secure Sockets Layer, a secure protocol used to validate the identities of participants in a transaction and create an encrypted connection over which the transaction can take place.

SOAP
Simple Object Access Protocol, an XML-based standard for making remote procedure calls by means of text messages, using HTTP(S) as the transport mechanism.

ST
Security Target

TOE
Target of Evaluation

TSF
TOE Security Functions

TSP
TOE Security Policy

TSC TSF Scope of Control

XML Extensible Markup Language, a flexible formal text format derived from SGML that is commonly used to define more specialized markup languages for representing structured data.

XML Schema Validation The use of an XML schema document to test the validity of the structure or content of an XML document of the type the schema describes. See also Schema.

XML Signature Verification A method of establishing the authenticity of a document or its sender by using a shared secret (key) to recompute a cryptographic digest computed from the contents of the document or the certificate the sender presents. If the two signatures match, the document or sender is authentic..

13 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

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

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

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R.

[6] Cisco Systems ACE XML Gateway and Manager Version 5.0.3 FINAL Non-Proprietary ETR – Part 1.

[7] Cisco Systems ACE XML Gateway and Manager Version 5.0.3 FINAL Proprietary ETR – Part 2 and Supplemental Team Test Plan.

[8] Cisco Systems, Inc. ACE XML Gateway and Manager Version 5.0.3 Security Target, Version 1.0, 25 July 2008.

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