National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Actional Corporation
XML Web Services Management and
XML Firewall Security Solution
Actional Security Gateway

Report Number: CCEVS-VR-05-0089
Dated: 11 January 2005
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Robin Medlock
The MITRE Corporation
Bedford, Massachusetts

Julie Evans
National Security Agency
Ft. George G. Meade, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of Actional XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway, Version 3.1.2.5 was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 20 December 2004. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

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 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). 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 adduced.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, 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 cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The SAIC evaluation team concluded that the Common Criteria requirements have been met for Evaluation Assurance Level EAL2, augmented with ADV_SPM.1 (Informal TOE security policy model), ALC_FLR.2 (Flaw reporting process), and AVA_MSU.1 (Examination of guidance).

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

Disclaimer: The information contained in this Validation Report is not an endorsement of the Actional Security Gateway product by any agency of the US Government and no warranty of the product is either expressed or implied.

1.1 Evaluation Details

Evaluated Product: Actional Security Gateway Version 3.1.2.5

CCTL: Science Applications International Corporation

Evaluation Completion: 20 December 2004

CC: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

CEM: Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6, January 1997; Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 1.0, August 1999.

Evaluation Assurance Class: EAL 2 Augmented with ADV_SPM.1, ALC_FLR.2, AVA_MSU.1

1.2 Interpretations

The Evaluation Team determined that the following CCIMB Interpretations were applicable to this evaluation:

Work Unit	International Interpretation	International Interpretation Description
FAU_GEN.1	RI-202	Selecting One or More items in a selection operation and using "None" in an assignment
FAU_STG.1	RI-141	Some Modifications to the Audit Trail Are Authorized
FDP_ACF.1	RI-103	Association of Access Control Attributes with Subjects and Objects
FDP_IFF.1	RI-104	Association of Information Flow Attributes with Subjects and Objects
FIA_AFL.1	RI-111	Settable Failure Limits are Permitted
FIA_USB.1	RI-137	Rules governing binding should be specifiable
FMT_MOF.1 FMT_MSA.1 FMT_SMF.1	RI-065	No component to call out security function management
FMT_MSA.3	RI-201	"Other properties" specified by assignment
FMT_MSA.3	RI-202	Selecting One or More items in a selection operation and using "None" in an assignment
ACM_CAP.2	RI-003	Unique identification of configuration items in the configuration list

Work Unit	International Interpretation	International Interpretation Description
ADO_IGS.1 ADO_VLA.1	RI-051	Use of documentation without C & P elements

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

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) 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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1 Evaluation Identifiers

Evaluation Completion:	20 December 2004
TOE:	Actional Security Gateway Version 3.1.2.5
Developer:	Actional Corporation, Inc. 800 W. El Camino Real, Suite 120 Mountain View, CA., 94040
ST:	Actional Corporation XML Web Services Management and XML Firewall Security Solution Actional Security Gateway Security Target
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

CEM:	Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6, January 1997; Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 1.0, August 1999.
Evaluation Assurance Class:	EAL 2 Augmented with ADV_SPM.1, ALC_FLR.2, AVA_MSU.1
PP:	The TOE does not claim conformance to a PP.
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Evaluation Team:	Shukrat Abbas (Lead Evaluator) Terrie Diaz
Validation Team:	Robin Medlock The MITRE Corporation 7515 Colshire Drive McLean, VA 22102-7508 Julie Evans National Security Agency (NSA) 9800 Savage Rd Ft. Meade, MD 20755-6740

3 Security Policy

The Security Policy of the TOE is enforced by the security functions of the TOE. These security functions are described below. The Security Policy is described and informally modeled in the Security Policy Model document.

3.1 Identification and Authentication

The TOE requires ASG administrators to provide unique identification and authentication data before any administrative access to the system is granted. The TOE also supports the capability to authenticate external service consumers.

3.2 User Data Protection

The TOE enforces a role-based access control (RBAC) policy that controls ASG administrator access and what operations can be performed on TOE objects. This policy is shown in Table 2 below.

Table 2 RBAC Security Functional Policy

Objects	**Subjects**					
	Root Admin.	**Publisher**	**Sec. Admin.**	**Gateway Admin.**	**Console Admin.**	**Console User Admin**
Admin Roles	Create Edit Delete Assign					Create Edit Delete Assign
Admin Users	Create Edit Delete					Create Edit Delete
Auth. Directories.	Create Edit Delete Enable Disable		Create Edit Delete Enable Disable			
Base Operations	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Base Services	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Data Stores	Create Edit Delete	Create Edit Delete				

Objects	Subjects					
	Root Admin.	**Publisher**	**Sec. Admin.**	**Gateway Admin.**	**Console Admin.**	**Console User Admin**
Data Store Entries	Create Edit Delete	Create Edit Delete				
Gateways	Create Edit Delete Push Pull Monitor Clear Start Stop			Create Edit Delete Push Pull Monitor Clear Start Stop		
Published Operations	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Published Ports	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Published Service Views	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Reports	Create Edit Delete View		Create Edit Delete View	View		
Shared Rule Groups	Create Edit Delete Use	Use	Create Edit Delete Use			
Op-specific Rule Groups	Create Edit Delete Use	Create Edit Delete Use				
Rules	Create Edit Delete Change State	Create Edit Delete Change State	Create Edit Delete Change state			
System-defined Rule Groups	Use	Use	Use			
Scheduled Jobs/Task	Create Edit Delete Execute			Create Edit Delete Execute		

Objects	Subjects					
	Root Admin.	**Publisher**	**Sec. Admin.**	**Gateway Admin.**	**Console Admin.**	**Console User Admin**
Tasks	Create Edit Delete			Create Edit Delete		
Scheduled Job	Start Stop			Start Stop		
Service Requestor Roles	Create Edit Delete		Create Edit Delete			

The TOE also enforces an information flow control policy that controls service requestor access to web-based services that it protects. Enforcement is based on the address of the source/destination subject, the requested service operation, and other security attributes.

3.3 Audit

The TOE generates audit records of login attempts, user lockouts, configuration changes, and start-up and shutdown of the audit functions. It also provides the capability to read and sort audit records to authorized ASG administrators.

3.4 Security Management

The TOE provides the ability for ASG administrators to manage the security functions of the TOE as described in Table 3 below.

Table 3 Management of Security Functions

FUNCTIONS	AUTHORIZED IDENTIFIED ROLES					
	Root Administrator	**Publisher**	**Security Administrator**	**Gateway Administrator**	**Console Administrator**	**Console User Administrator**
Modify the behavior of administrative role	X					X
Enable assignment of user to administrative role	X					X
Modify behavior of/Enable/Disable authentication directory	X		X			
Modify behavior of data store	X	X				
Modify behavior of data store entry	X	X				
Modify behavior of gateway administration functionality	X			X		
Enable release of locked account	X					X
Enable/Disable published operation	X	X	X			
Enable/Disable published port	X	X	X			

FUNCTIONS	AUTHORIZED IDENTIFIED ROLES					
	Root Administrator	Publisher	Security Administrator	Gateway Administrator	Console Administrator	Console User Administrator
Create/Edit/Delete published service view	X	X				
Enable/Disable published service view	X	X	X			
Modify behavior of shared rule group	X		X			
Modify behavior of operation-specific rule group	X	X				
Modify behavior of/Enable/Disable rules	X	X	X			
Modify behavior of service requestor role	X		X			
Enable a push configuration from manager to gateway	X	X[1]		X		
Enable a pull log retrieval from gateway	X			X		
Enable a configuration pull from gateway to manager	X			X		

3.5 Cryptographic Support

The TOE provides cryptographic support for encryption, decryption, signing, hashing, checksum computation, and verification. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

3.6 Protection of the Security Functions

The TOE ensures that enforcement functions are invoked and succeed before the function is allowed to proceed.

3.7 XML Message Server Requirements

The TOE enables an authorized user to hide backed resources, URLs, and Web Services operations from the Service Requestor. It also supports multiple XML message formats, protocols and PKI technology formats, and it enables the mapping of credentials of a service requestor into a username and password combination for the base service.

[1] Publisher can only push configurations to non-production Gateways. Root Admin and Gateway Admin can push configuration to non-production and production Gateways.

4 Threats and Assumptions

4.1 Threats Addressed by the TOE

The Security Target identified the following threats that the evaluated product addresses:

T.NOAUTH An unauthorized user may attempt to bypass the security (identification and authentication) of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.ATKPOT An unauthorized user may attempt to circumvent TOE security functions using obvious vulnerabilities.

T.BRUTEF An unauthorized user may attempt a brute force attack in which authentication data may be repeatedly guessed in order to gain access to the TOE and/or its data.

T.MASQUE An unauthorized user may attempt to capture identification and authentication data to use for the purpose of masquerading as an authorized administrator of the TOE.

T.REMATK An unauthorized user may attempt to view, modify, and/or delete sensitive and/or security-related information that is sent between a remotely located authorized administrator and the TOE.

T.FACCNT An unauthorized user may attempt to access TSFs invoking security functions that may go undetected.

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove, destroy, or corrupt data stored by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the TOE's functions by halting execution of the TOE.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.GOTHRU An unauthorized user may attempt to distribute malicious information or messages to pass through the TOE.

T.NOVALD An unauthorized user may cause the XML messages passing through the TOE to not be checked for well-formed structure validation.

4.2 Threats Addressed by the Environment

The Security Target identified the following threats that the environment addresses:

T.AUDFUL An unauthorized user may attempt to exhaust storage capacity in effort to lose audit records and prevent future audit records from being recorded.

4.3 Usage Assumptions

The Security Target identified the following assumptions for usage of the evaluated product:

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or application) on the machine on which the TOE resides.

A.PUBLIC The machine on which the TOE resides does not host public data.

4.4 Personnel Assumptions

The Security Target identified the following assumptions for personnel who use the evaluated product:

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

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

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

4.5 Environmental Assumptions

The Security Target identified the following assumptions for IT environment in which the evaluated product operates:

A.DBPROT The database used by the TOE for ASG Manager audit storage will be located on a trusted network to prevent unauthorized tampering and modification of audit records.

A.SECSTR The key store used by the TOE for x.509 certificate and key storage will be placed within the trusted network to protect certificates and keys from tampering.

A.TIME The operating environment of the TOE will provide a reliable timestamp.

4.6 Physical Assumptions

The Security Target identified the following assumptions for physical environment in which the evaluated product operates:

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

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

5 Architectural Information

The TOE is the Actional Security Gateway version 3.1.2.5 (i.e. "ASG"). ASG is a subset of the product that secures and manages Web Services networks. ASG is a communications infrastructure that uses XML-based messages for communication. ASG provides a support environment for multiple XML standards (i.e., SOAP (simple object access protocol), WSDL and UDDI). ASG is functionally a combination of an XML firewall, a Service Tracker, an XML Broker, and a Service Manager.

The ASG product architecture consists of two major components: the Actional Security Gateway and the ASG Manager.

The ASG Manager utilizes an ASG web-based User Interface (UI) that facilitates all the management functions of the Actional Security Gateway. The ASG Manager manages one or more Actional Security Gateways. Moreover, the ASG Manager is both logically and physically separate from the Actional Security Gateway. The ASG Manager performs all policy rule-sets for the Actional Security Gateway to enforce.

The Actional Security Gateway, which serves as the web services environment policy enforcer, includes security capabilities that secure and monitor a network operating at the application level. The ASG deployments are the policy enforcement points that intercept and process messages. The XML firewall functionality consists of XML message filtering mechanisms.

The ASG can be located within the DMZ, behind the network firewall, or at each Web Service depending upon the configuration desired. The ASG may be deployed in a variety of ways:

- As a single ASG;
- As load-balanced ASGs for scalability and failover; and
- Separate ASGs – for example, in a corporation where policies differ by department.

The boundary of the TOE encompasses all of the components that are encompassed by the red line in Figure 1 below. The two logical components of distinction that lie within the TOE boundary are the ASG Manager and the Actional Security Gateway (both are software components).

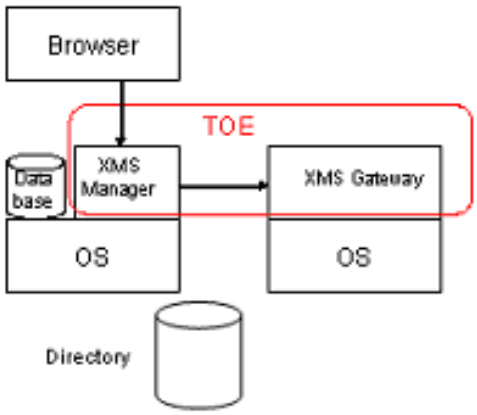

Figure 1 TOE Boundary and Logical Interaction between the ASG and External Components

6 Documentation

During the course of the evaluation, the CCTL had access to an extensive amount of documentation and evidence. Note that Actional Security Gateway document names reflect the Westbridge Technology product name and branding (prior to the merger of Actional Corporation with Westbridge Technology)

The following was utilized as evidence for the Configuration Management assurance:

- Westbridge Technology, Inc. XML Web Services Management and Security Solution XML Message Server Version 3.0 Configuration Management, v1.4 10/25/2004

The following were utilized as evidence for the Delivery and Operation assurance:

- Westbridge Technology, Inc. XML Web Services Management and Security Solution XML Message Server Version 3.1 Secure Delivery and Installation, v1.5 11/02/2004
- Westbridge XML Message Server Installation Guide, Version 3.1 May 2004
- Westbridge XMS Appliance Installation Guide, Version 3.1 August 2004
- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Version 3.1, Administrative Guidance Supplement

The following was utilized as evidence for the Development assurance:

Design Documentation:

- Westbridge Technology, Inc. XML Web Services Management and XML Firewall Security Solution XML Message Server Version 3.1 Functional Specification v2.4
- Westbridge Technology, Inc. XML Web Services Management and XML Firewall Security Solution, XML Message Server (XMS) Version 3.1 High Level Design, Version 2.4
- Westbridge Technology, Inc. XML Web Services Management and XML Firewall Security Solution, XML Message Server (XMS) Version 3.1 Representation Correspondence, Version 2.4
- Westbridge The XML Message Server Reference Guide Version 3.1.1
- Westbridge Technology, Inc. XML Web Services Management and XML Firewall Security Solution XML Message Server Version 3.0 Security Policy Model v0.3

Supporting Documentation:

- Westbridge The XML Message Server Release Notes Version 3.1

- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Version 3.1, Administrative Guidance Supplement
- Westbridge Technology, Inc. Getting Started with XMS: Basic Administration, Version 3.1.1, July 2004
- Westbridge Technology, Inc. Getting Started with XMS: Advance Topics, Version 3.1.1, July 2004
- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Version 3.1 Security Target, Version 0.28
- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Version 3.1, Administrative Guidance Supplement

The following were utilized as evidence for the Guidance Documentation assurance:

- Westbridge Technology Inc XML Web Services management and Security Solution XML Message Server v3.1 Vulnerability Assessment v. 2.2 November 16, 2004
- Westbridge Technology, Inc. Getting Started with XMS: Basic Administration, Version 3.1.1, July 2004
- Westbridge Technology, Inc. Getting Started with XMS: Advance Topics, Version 3.1.1, July 2004
- The XML Message Server Reference Guide v3.1.1
- The XML Message Server Release Notes v3.1
- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Version 3.1, Administrative Guidance Supplement
- The XML Message Server Installation Guide, Version 3.1, May 2004
- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Version 3.1 Security Target, Version 0.28

The following was used as evidence for the Lifecycle Support assurance:

- XML Message Server Version 3.1 Flaw Remediation Procedures, Version 3.0, 29 September 2004

The following were utilized as evidence for the Security Target:

- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Security Target, Version 1.0

The following were utilized as evidence for the Test Activity assurance:

- Westbridge Technology, Inc. XML Web Services Management and Security Solution XML Message Server Version 3.1 Test Plan, Version 1.4, 19, November 2004
- Westbridge XML Message Server Version 3.1 Test Cases documents (GEN11.doc, SAR3.doc, COP1.doc, IFC1.doc, IFF1.doc, AFL1.doc, ATD1.doc, UAU2.doc, UID2.doc, MOF1.doc, MSA1.doc, MSA3.doc, MTD1.doc, SMR1.doc, RVM1.doc, MAP1.doc, SUP1.doc, and VEW1.doc)
- Westbridge Technology, Inc. XML Web Services Management and XMS Firewall Security Solution, XML Message Server (XMS) Version 3.1 Functional Specification, Version 2.4
- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Version 3.1, Administrative Guidance Supplement

The following were utilized as evidence for the Vulnerability Assessment assurance:

- Westbridge Technology Inc XML Web Services management and Security Solution XML Message Server v3.1 Vulnerability Assessment v. 2.2 November 16, 2004
- Westbridge Technology, Inc. Getting Started with XMS: Basic Administration, Version 3.1.1, July 2004
- Westbridge Technology, Inc. Getting Started with XMS: Advance Topics, Version 3.1.1, July 2004
- The XML Message Server Reference Guide v3.1.1
- The XML Message Server Release Notes v3.1
- Westbridge Technology, Inc. XML Web Services Management and XML Firewall Security Solution, XML Message Server version 3.1 Administrative Guidance Supplement, version 1.4
- The XML Message Server Installation Guide, Version 3.1, May 2004
- Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Version 3.1 Security Target, Version 0.28

7 IT Product Testing

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

7.1 Developer Testing

Evaluator analysis of the developer's test coverage and functional testing indicates that the developer's testing is adequate to satisfy the requirements of EAL2. Each security functional requirement test is described in a separate test case document. Each test case document includes the test overview, which describes the goal of the test being performed as well as different scenarios to fully exercise the security function.

Each test case document also outlines the test configuration requirements, such as the test roles, test prerequisites, and initialization. The security functions exercised are Security Audit, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, and XML Message Server Requirements.

The vendor's testing methodology enforces the exercise of the TOE graphical user interfaces (GUIs) that are used to manage the security functions and demonstrates the enforcement of the security functions. The testing effectively demonstrates the functions of the gateway via the creation of published services views associated with rules and operations, and the use of the product test tool, which demonstrates the accuracy of the published services views.

7.2 Evaluator Testing

The evaluation team chose a subset of vendor tests to rerun, which represented over 20% of the total vendor tests. The subset of the vendor tests exercised the Security Audit, user Data Protection, Identification and Authentication, Security Management, Protection of the TSF, and XMS Requirements. Each test was run successfully, with the actual results matching the expected results.

The evaluation team expanded on the vendor tests to devise a set of independent tests which exercised specific security-related behavior of all the security functions identified in the security target. Each test of the sets ran successfully, demonstrating the expected behavior.

7.3 Penetration Testing

Based on the evaluation team's review of the evaluation evidence for possible vulnerabilities, the team's penetration activity consisted of manual testing to exercise procedures consistent with the administrator guidance. The penetration testing did not uncover any vulnerabilities.

8 Evaluated Configuration

The evaluation testing was performed on a vendor-provided TOE-embedded appliance with a Linux-based environment, consistent with the environment identified in the ST. The appliance included both the ASG Manager and the ASG Gateway. The testing environment consisted of two PCs connected via a hub to the TOE appliance and a remote connection via the Internet to an MQ Server on the vendor site for MQ Server tests.

Before testing began on each product within the TOE, the evaluation team applied the configuration steps given in the configuration guide, utilizing the network settings applicable to the CCTL test environment.

9 Results of the Evaluation

The evaluation was conducted based on the Common Criteria (CC), Version 2.1, dated August 1999; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999; and all applicable National and International Interpretations in effect on 8 December 2003. The evaluation confirmed that the Actional Security Gateway Version 3.1.2.5 product is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) and assurance requirements (Part 3) for EAL2 augmented with Examination of Guidance (AVA_MSU.1), Flaw Reporting Procedures (ALC_FLR.2), and an Informal TOE Security Policy Model (ADV_SPM.1). The details of the evaluation are recorded in the CCTL's evaluation technical report, *Evaluation Technical Report for Actional Security Gateway*, January 7, 2005. The product was evaluated and tested against the claims presented in the *Actional Corporation, Inc. XML Web Services Management and XML Firewall Security Solution Actional Security Gateway Security Target*, Version 1.0.

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

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the Actional TOE 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 2 ACM CEM work unit. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the Actional CM process to ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation. The evaluation team ensured that the following items were

considered configuration items: TOE implementation, design documentation, test documentation, and user guidance.

9.3 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 securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during that process.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit, and augmented this with the EAL3 ADV_SPM.1 (Informal TOE Security Policy Model) work units. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF implements/employs the security functions. The design documentation consists of a functional specification and a high-level design document. The documentation was augmented with an informal TOE security Policy Model for this evaluation. 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 2 AGD CEM work unit. The evaluation team verified the adequacy of the administrator guidance in describing how to securely administer the ASG TOE.

9.6 Evaluation of the Life Cycle Support (ALC)

The evaluation team applied each EAL2 ALC CEM work unit, and augmented this with ALC_FLR.2 (Flaw Reporting Procedures) work units. The evaluation team assessed the Actional life-cycle support processes to determine that discipline and control is established in the processes of refinement of the TOE during its development and maintenance.

9.7 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 functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the Actional test suite, and devised an independent set of team tests and penetration tests. The

Actional 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 2 AVA CEM work unit, and augmented this with the EAL3 AVA_MSU.1 (Examination of Guidance) work units. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the Actional strength of function analysis and the Actional vulnerability analysis as well as 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 vendor test suite, several independent tests, and the penetration test further demonstrated the claims in the ST.

10 Validator Comments and Recommendations

The validator observations support the evaluation team's conclusion that the Actional Security Gateway, version 3.1.2.5, meets the claims stated in the Security Target.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

11 Security Target

The Security Target, *Actional Corporation XML Web Services Management and XML Firewall Security Solution, Actional Security Gateway Security Target, Document Version 1.0* is included here by reference.

12 Glossary

3DES	Triple data encryption standard
AES	Advanced encryption standard
ASG	Actional Security Gateway, Version 3.1.2.5
CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration management
CRL	Certificate revocation list
CRM	Customer relationship management
DES	Data encryption standard
DMZ	Demilitarized zone
EAL	Evaluation assurance level
ERP	Enterprise resource planning
HSQLDB	Hypersonic SQL database
HTTP	Hypertext transfer protocol
HTTPS	Secure hypertext transfer protocol
JMS	Java message service
LDAP	Lightweight directory access protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NVLAP	National Voluntary Laboratory Assessment Program
OCSP	Online certificate status protocol
OS	Operating system
PKCS #7	Public key cryptography standard - Cryptographic message syntax standard
PKCS #10	Public key cryptography standard - Certification request syntax standard
PKCS #11	Public key cryptography standard - Cryptographic token interface standard
PKCS #12	Public key cryptography standard - Personal information exchange syntax standard
PKI	Public key infrastructure
SAML	Security assertion markup language
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SLA	Service level agreement
SMTP	Simple mail transfer protocol
SNMP	Simple network management protocol
SOAP	Simple object access protocol
SSL	Secure sockets layer
ST	Security Target
TCP	Transmission control protocol
TOE	Target of Evaluation
TSF	Target of Evaluation (TOE) security function
TSP	Target of Evaluation (TOE) security policy
UDDI	Universal Description, Discovery and Integration protocol

UI	User Interface
WS-Security	Web Services Security
WSDL	Web service definition language
XKMS	XML key management specification
XML	Extensible markup language
ASG	Actional Security Gateway v3.1.2.5
XPath	XML Path Language
XSLT	Extensible stylesheet language transformations

13 Bibliography

The evaluation and validation methodology was drawn from the following:

[1] Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and General Model, dated August 1999, Version 2.1, CCIMB-99-031.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, dated August 1999, Version 2.1, CCIMB-99-032.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, dated August 1999, Version 2.1, CCIMB-99-033.

[4] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, Version 0.6, CEM-99/017.

[5] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, Version 1.0, CEM-99/045.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, Supplement: ALC_FLR – Flaw Remediation, dated February 2002, Version 1.1, CEM-2001/0015R.

[7] Evaluation Technical Report for Actional Security Gateway Version 3.1.2.5 dated 7 January 2005.

[8] Actional Security Gateway Security Target, Version 1.0.

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

14 International Interpretations

Interpretations used in this product evaluation are as follows:

Work Unit	International Interpretation	International Interpretation Description
FAU_GEN.1	RI-202	Selecting One or More items in a selection operation and using "None" in an assignment
FAU_STG.1	RI-141	Some Modifications to the Audit Trail Are Authorized
FDP_ACF.1	RI-103	Association of Access Control Attributes with Subjects and Objects
FDP_IFF.1	RI-104	Association of Information Flow Attributes with Subjects and Objects
FIA_AFL.1	RI-111	Settable Failure Limits are Permitted
FIA_USB.1	RI-137	Rules governing binding should be specifiable
FMT_MOF.1	RI-065	No component to call out security function management
FMT_MSA.1	RI-065	No component to call out security function management
FMT_MSA.3	RI-201	"Other properties" specified by assignment
FMT_MSA.3	RI-202	Selecting One or More items in a selection operation and using "None" in an assignment
FMT_SMF.1	RI-065	No component to call out security function management
ACM_CAP.2	RI-003	Unique identification of configuration items in the configuration list
ADO_IGS.1	RI-051	Use of documentation without C & P elements
ADO_VLA.1	RI-051	Use of documentation without C & P elements