National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Layer 7 SecureSpan Product Suite 4.1

Report Number: CCEVS-VR-VID10207-2010
Dated: 13 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

Jandria Alexander

Aerospace Corporation
Columbia, MD

Jean Hung

MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Layer 7 SecureSpan Product Suite 4.1 product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in June 2010. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 2.3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

The SAIC evaluation team determined that the product satisfies conformance claims of Common Criteria Part 2 Conformant and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 4, augmented with ALC_FLR.2. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. 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 Layer 7 SecureSpan Product Suite 4.1 comprises two components: the SecureSpan Gateway; and the SecureSpan Manager. The SecureSpan Gateway is a hardware-based XML firewall and service gateway designed to protect Web services and mediate communications between client and services residing in different identity, security or middleware domains. The SecureSpan Manager application is a GUI application that provides the user with an administrative interface to manage the SecureSpan Gateway.

Layer 7 SecureSpan Product Suite 4.1, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the Layer 7 SecureSpan Product Suite 4.1 Security Target.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Layer 7 SecureSpan Product Suite 4.1
Sponsor:	Layer 7 Inc. 1100 Melville Street, Suite 405 Vancouver, BC V6E 4A6 Canada
Developer:	Layer 7 Inc. 1100 Melville Street, Suite 405 Vancouver, BC V6E 4A6 Canada
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	November 14, 2006
Completion Date:	13 August 2010

CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.
Evaluation Class:	EAL 4, augmented with ALC_FLR.2
Description:	The Layer 7 SecureSpan Product Suite 4.1 provides a hardware-based XML and SOAP web service firewall and associated GUI-based management application.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Layer 7 SecureSpan Product Suite 4.1 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	None
Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Dawn Campbell Katie Sykes
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE is intended to counter.

T.MEDIAT	An unauthorized user may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.TRANSMIT	An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing them to intercept and modify transmitted information.
T.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized users.

2 Identification

The evaluated product is the SecureSpan Product Suite v4.1, comprising SecureSpan Gateway 4.1-6 and SecureSpan Manager Version 4.1 Build 3826

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the Layer 7 SecureSpan Product Suite 4.1 security policy has been extracted and reworked from the Layer 7 SecureSpan Product Suite 4.1 ST and Final ETR.*

3.1 Security Audit

The TOE has the capability to generate audit records of management activities performed by an authorized administrator and of information flow control decisions taken by the SecureSpan Gateway component. Generated audit records contain information that includes date and time of event, type of event, the identity of the subject that caused the event, and the outcome (success or failure) of the event. It should be noted that the SecureSpan Gateway provides the timestamp for all audit records.

3.2 Cryptographic Support

The TOE implements cryptographic functionality to support SSL that is used to protect communication between the TOE components from disclosure and modification. The TOE also ensures that cryptographic operations are validated in the policy context and the routing decisions are made in that context. The TOE incorporates the Sun Crypto Accelerator 6000 PCI-E Adaptor, which is FIPS 140-2 Level 3 validated (certificate #778).

3.3 User Data Protection

The TOE enforces an information flow control policy on service requests sent by consumers to services (SOAP web services and XML applications) published via the TOE, and on service responses sent by published services to consumers. The information flow does not involve consumers sending messages to other consumers, or web services sending responses to other web services. The TOE enforces the information flow control policy using consumer identities to authenticate the user and policy assertions to validate the content/structure of incoming messages. Accepted messages are routed to the destination service.

3.4 Identification and Authentication

The TOE maintains user IDs, authentication data, and role information for TOE users and user ID, authentication data, and groups for web service consumers. The Internal Identity Provider (IIP) users and groups are controlled by the TSF. The IIP is populated during installation and configuration of the TOE. There are two types of users defined in the IIP; those that logon to the TOE (TOE users) and those that only appear in the message traffic (web service consumers). The TOE allows unauthenticated access to Web services on behalf of the user to be performed before the user is successfully identified and authenticated. The TOE also supports multiple authentication methods, credentials such as passwords and X.509 client certificates.

3.5 Security Management

The TOE supports a number of security management roles that provide for fine-grained control of the security management functions. The users that are assigned to security management roles are

considered to be authorized administrators. The TOE provides the authorized administrators with the ability, based on role assignments, to manage the policy assertions, user accounts, and audit function.

3.6 Protection of the TSF

The TOE uses SSL to create a secure channel to protect the communication between the SecureSpan Manager and the SecureSpan Gateway. In addition, the TOE ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The SecureSpan Gateway provides the timestamp for the audit records while the IT environment is relied upon to provide a reliable timestamp for the SecureSpan Manager component, to support its inactivity timeout.

3.7 TOE Access

The TOE provides the capability for the TSF to determinate when there is user inactivity and terminates the session. A user will have to re-authenticate and start a new session.

4 Assumptions

The following assumptions are identified in the ST:

A.LOCATE The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

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 administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

4.1 Clarification of Scope

The Target of Evaluation (TOE) is the Layer 7 SecureSpan Product Suite v4.1.

The SecureSpan Gateway component incorporates the Sun SCA 6000 cryptomodule, which has been validated to FIPS 140-2 Security Level 3 (certificate #778). The SecureSpan Gateway is pre-configured for FIPS mode of operation.

As a consequence of this validation, and in order to ensure the evaluated configuration of the TOE satisfies its security requirements, the following clarifications are noted:

- Only an Internal Identity Provider (IIP), for maintaining user security attributes of both TOE administrators and web consumers, is supported in the evaluated configuration. Support for Federated and LDAP Identity Providers is outside the scope of the evaluation
- The TOE has the capability to generate SNMP Trap and e-mail notifications as part of its policy processing capability. These require the presence in the IT environment of an SNMP server and an SMTP server respectively in order to be effective.
- The SecureSpan Gateway component is a hardware-based appliance and is assumed to be installed in a physically secure location.
- The SecureSpan Manager is a GUI-based Java application, running in the context of a Java Virtual Machine and supported on a Windows, Linux or Solaris operating system.

As such, it relies on its IT environment for protection from bypass and tampering and for provision of a reliable time stamp to manage its inactivity timeout capability.

- The SecureSpan Manager also relies on its environment for cryptographic support for its end of the SSL channel between itself and the SecureSpan Gateway.
- During configuration of the SecureSpan Gateway, the administrator needs to modify the file defining the cipher suites supported by the Gateway to ensure only the FIPS approved algorithms provided by the SCA 6000 will be used. This is described in the Administration Guide.

5 Architectural Information

The TOE comprises two components:

SecureSpan Gateway

The SecureSpan Gateway is a hardware-based XML firewall and service gateway designed to protect Web services, accelerate XML operations and mediate communications between client and services residing in different identity, security or middleware domains.

The SecureSpan Gateway provides runtime control over service level authentication, authorization, credentialing, integrity, confidentiality, schema validation, content inspection, data transformation, threat protection, routing, and logging. The SecureSpan Gateway enforces all security policies including an information flow policy for network traffic, as well as administrator's access to TSF data.

The SecureSpan Gateway interfaces with client-side applications that require communication with web services. Client systems send message requests intended for a web service to the SecureSpan Gateway. The SecureSpan Gateway then functions as a client-side proxy, applying necessary requirements such as identities, protocols, headers, and/or transformations to the message as required by the policy in use. Each web service is associated with its own policy, which is automatically applied by the SecureSpan Gateway to ensure that all subsequent messages conform to the policy.

SecureSpan Manager

The SecureSpan Manager application is a GUI application that provides the user with an administrative interface to manage the SecureSpan Gateway. The SecureSpan Gateway, as configured by Layer 7, will only allow communication with the manager on the network that has been designated as "internal". The SecureSpan Manager communicates over SSL, thus encrypting all communication. An Administrator uses SecureSpan Manager to construct web service and XML application policies, publish XML applications and web services, manage web service consumers, configure identity bridging, configure auditing and alerting, and monitor the performance of the SecureSpan Gateway. The SecureSpan Manager provides a set of security management roles that provide for fine-grained control of management privileges. The security management roles include the authorized Administrator, who has complete control of all management functions. Other roles defined by the TOE include Operators, Web Service Managers, Internal Users and Groups Manager, and View Audit Records and Logs.

6 Documentation

The guidance documentation examined during the course of the evaluation and therefore included in the TOE is as follows:

- SecureSpan Administrator Guidance, version 4.1CC, last modified May 26, 2010
- SecureSpan User Guidance, version 4.1CC, last modified May 26, 2010.

7 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 Layer 7 SecureSpan Product Suite 4.1.

Evaluation team testing was conducted at the vendor's development site in May 2010.

7.1 Developer Testing

The vendor's approach to testing for the SecureSpan Suite is based on testing the claimed security functions of the TOE as visible at the external TSFIs described in the functional specification. The vendor has compiled a test suite taken from its existing extensive set of functional and regression tests to demonstrate the correct behavior of the TSF at its external interfaces. The tests are a mix of manual and automated tests. Most of the automated tests can also be run manually if desired, since they are automations of previously manual tests, using the developer's own Autotest test tool.

The vendor addressed test depth by mapping SFRs to functionality in the low level design, which in turn was mapped to functional requirements in the functional specification. The vendor's tests are focused on demonstrating behavior as specified in the functional specification, which has in turn been mapped to the TSS and SFRs described in the Security Target.

The vendor ran the entire test suite on the TOE on the test configuration described in the test documentation and gave the evaluation team the actual results. The evaluation team verified the results demonstrated all vendor tests had passed.

7.2 Evaluation Team Independent Testing

The evaluation team executed a sample of the vendor test suite, including all automated tests, for the TOE per the evaluated configuration as described in the vendor's test documentation. Additionally, the evaluation team ran selected manual tests that had been identified in the developer's test records as having failed against earlier release candidates of the evaluated version. All tests run by the evaluation team passed.

The evaluation team performed the following additional functional tests covering the following aspects of the TSF:

- Audit record timestamp source
- Password structure and constraints enforcement
- Administrator logon
- Role aggregation
- Role classification
- Security management capabilities

- Role capabilities
- FTP(S) assertion properties
- Protected communications between SSM and SSG
- Disabling session termination
- SSM-implemented session termination
- Managing session termination.

As a result of the evaluation team's tests, some clarifications were made to the ST regarding the behavior of the TOE and some updates were made by the developer to the guidance documentation to ensure it was clear and complete.

7.3 Penetration Testing

The developer produced their own vulnerability analysis, including an open source search of public vulnerability databases. The developer's search did not identify vulnerabilities in the Layer 7 product, but did identify potential vulnerabilities in protocols handled by the TOE (e.g., WS-Security) or in third-party products included within the Gateway appliance to support the Layer 7 application. The developer's vulnerability analysis documented how each identified vulnerability was addressed, either by changes made to the TOE implementation or through analysis showing the vulnerability was not relevant to the TOE in its evaluated configuration.

The evaluation team conducted an open source search for vulnerabilities in the TOE. This search did not identify any public domain vulnerabilities in the TOE itself, but did identify vulnerabilities in third-party components that are packaged as part of the Gateway appliance, and in protocols handled by the TOE (e.g., SNMP). The evaluation team advised the developer of these vulnerabilities and the developer provided responses to each one as to why it was not relevant to the TOE.

In addition to the open source search, the evaluation team considered other potential vulnerabilities, based on a search of the evaluation evidence and consideration of the developer's own vulnerability analysis (including SOF and misuse analyses). This led to the evaluation team devising the following tests:

- Port scan of the Gateway appliance
- Malformed packets
- SSL configuration
- SSM logon behavior.

The evaluation team's penetration testing effort did not identify any vulnerabilities in the TOE.

8 Evaluated Configuration

The evaluated version of the TOE is Layer 7 SecureSpan Product Suite 4.1.

9 Results of the Evaluation

The evaluation was conducted based upon version 2.3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to

each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that a certificate rating of EAL4, augmented with ALC_FLR.2 be issued for Layer 7 SecureSpan Product Suite 4.1.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table:

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_FLR.2	Flaw reporting procedures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_MSU.2	Validation of analysis

Assurance Component ID	Assurance Component Name
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Independent vulnerability analysis

10 Validator Comments/Recommendations

The following capabilities of the SecureSpan Product Suite were not assessed as part of the evaluation and are excluded from the evaluated configuration:

- Support for Federated Identity Providers (FIPs) and LDAP Identity Providers (LIPs).
- Virtual partitions, where multiple Gateways can be configured on a single appliance.

The SecureSpan Manager component of the TOE is a GUI-based Java application, running in the context of a Java Virtual Machine and supported on a Windows, Linux or Solaris operating system. As such, it relies on its IT environment for protection from bypass and tampering and for provision of a reliable time stamp to manage its inactivity timeout capability.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **Layer 7 SecureSpan Product Suite 4.1 Security Target**, Version 1.0, dated 13 August 2010.

13 Glossary

Please consult the CC and CEM for definitions of abbreviations and terms used within this document.

14 Bibliography

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/common-criteria/)
- Layer 7 Networks, Inc. (http://www.layer7tech.com)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005
- *Common Evaluation Methodology for Information Technology Security*, version 2.3, August 2005.

Other Documents:

- *Layer 7 SecureSpan Product Suite Security Target*, Version 1.0, 13 August 2010.