National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

CA Layer 7 SecureSpan SOA Gateway v8.0

Report Number: CCEVS-VR-VID10530-2014

Dated: 30 May 2014

Version: 1.0

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

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin

Jerome Myers

Evaluation Team

Brian Pleffner

Cheryl Dugan

Richard Irizarry

Common Criteria Testing Laboratory

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076

Table of Contents

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the CA Layer 7 SecureSpan SOA Gateway v8.0, the Target of Evaluation (TOE), performed by Computer Sciences Corporation. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC) of Hanover, MD in accordance with the United States evaluation scheme and completed on May 30, 2014. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was written by Computer Sciences Corporation on behalf of CA Layer 7. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, dated July 2009 at Evaluation Assurance Level 1, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 3, July, 2009 and the Standard Protection Profile for Enterprise Security Management Policy Management, v1.4, 23 May 2012 (ESM Policy Manager PP) and Standard Protection Profile for Enterprise Security Management Access Control, v2.0, 22 February 2012 (ESM Access Control PP).

The SecureSpan SOA Gateway is an enterprise security management solution that provides centralized management and access control over SOAP web services. The TOE controls how SOAP web services are exposed to and accessed by external client applications.

The Evaluation Team performed an analysis of the international interpretations of the CC, CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before April 9, 2013.

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) evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP. The CCTLs are accredited to conduct security by the National Voluntary Laboratory Assessment Program (NVLAP).

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	CA Layer 7 SecureSpan SOA Gateway v8.0
Protection Profile	Standard Protection Profile for Enterprise Security Management Policy Management, v1.4, 23 May 2012 (ESM Policy Manager PP) Standard Protection Profile for Enterprise Security Management Access Control, v2.0, 22 February 2012 (ESM Access Control PP)
Security Target	CA Layer 7 SecureSpan SOA Gateway v8.0, Version 1.0, Revision 1.7, 28 May 2014
Dates of evaluation	April 9, 2013 – May 16, 2014
Evaluation Technical Report	CA Layer 7 SecureSpan SOA Gateway Assurance Activity Report, v1.2
Conformance Result	CC version 3.1 Release 3, July 2009 CC Part 2 extended CC Part 3 conformant Standard Protection Profile for Enterprise Security Management Policy Management, v1.4, 23 May 2012 (ESM Policy Manager PP) Standard Protection Profile for Enterprise Security Management Access Control, v2.0, 22 February 2012 (ESM Access Control PP)
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 3, July 2009
Common Evaluation Methodology (CEM) version	CEM version 3.1R3, July 2009
Sponsor	CA Layer 7
Developer	CA Layer 7
Evaluators	Brian Pleffner, Cheryl Dugan, Richard Irizarry
Validation Team	Daniel Faigin, Jerome F. Myers

3. SECURITY POLICY

The TOE enforces the following security policies:

- **Access Control Policy Definition.** The Policy Manager allows the TOE administrator to define detailed policies to enforce robust access control over web services.
- **Access Control Policy Enforcement.** The Gateway enforces the policies defined by the Policy Manager. The Gateway inspects messages sent between service clients (request messages) and service endpoints (response messages) to evaluate and enforce compliance with the defined policies.
- **Policy Security.** Communication between the Policy Manager and the Gateway is protected from disclosure and modification. A trusted channel is established to identify and authenticate each end point using TLS client / server authentication.
- **System Monitoring.** The TOE provides the ability to keep an audit/log trail to provide administrative insight into system management and operation, including identifying what policies are being defined and enforced.
- **Robust Administrative Access.** Administrative access to the TOE requires authentication and is governed by role based access control.
- **Continuity of Enforcement.** The Gateway will continue policy enforcement in the event of a loss of connectivity with the Policy Manager.

4. SECURITY PROBLEM DEFINITION

4.1. Assumptions

The ST identified the following security assumptions:

Table: Assumptions (ESM Policy Manager PP)

Identifier	Description
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.USERID	The TOE will receive identity data from the Operational Environment.
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.

Table: Assumptions (ESM Access Control PP)

Identifier	Description
A.AUDIT	A protected repository will exist in the Operational Environment to which audit data can be written.
A.POLICY*	The TOE will receive policy data from the Operational Environment.
A.USERID	The TOE will receive validated identity data from the Operational Environment.
A.TIMESTAMP	The TOE will receive a reliable timestamp from the Operational Environment.
A.INSTAL	There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.

4.2. Threats

The ST identified the following threats addressed by the TOE:

Table: Threats (ESM Policy Manager PP)

Identifier	Description
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.CONDTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.

T.FORGE	A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions.
T.WEAKPOL	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

Table: (ESM Access Control PP)

Identifier	**Description**
T.DISABLE	A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FALSIFY	A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
T.FORGE	A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.NOROUTE	A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
T.OFLOWS	A malicious user may attempt to provide incorrect Policy Management data to the TOE in order to alter its access control policy enforcement behavior.
T.UNAUTH	A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.

4.3. Organizational Security Policies

The ST identified the following OSPs addressed by the TOE:

Table: OSP (ESM Policy Manager PP)

Identifier	Description
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

Table: OSPs (ESM Access Control PP)

Identifier	Description
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

4.4. Clarification of Scope

The evaluation of the security provided by the product identified in the security target was limited to the functionality specified in the following protection profiles:

- Standard Protection Profile for Enterprise Security Management Policy Management, v1.4, 23 May 2012 (ESM Policy Manager PP)
- Standard Protection Profile for Enterprise Security Management Access Control, v2.0, 22 February 2012 (ESM Access Control PP)

Note that this product supports a large number of security assertions that are possible within an enforced policy. For the purpose of evaluation, the set of assertions covered by the evaluation was severely limited, and are described in Section 5.1.1. The additional assertions supported by the product may be used in the evaluated configuration, *but were not covered by the evaluation and were not tested for correctness.*

Any additional security functionality provided by the product was not included within the scope of this evaluation.

5. ARCHITECTURAL INFORMATION

5.1. Logical Scope and Boundary

The TOE logical scope and boundary consists of the security functions/features provided/controlled by the TOE. The TOE provides the following security features:

5.1.1. Access Control Policy Definition

The Policy Manager allows the TOE administrator to define detailed policies to enforce robust access control over web services. The following policy assertions are covered by the evaluation:

- **Access control assertions.** The following subset of access control assertions are evaluated:
  - **Authenticate User or Group.** Require specified users and/or groups to be authenticated against a selected identity provider. Applies the credentials collected by a ‘require’ assertion listed below to authenticate a user or group specified in this ‘authenticate’ assertion.
  - **Authenticate against Identity Provider.** Requires provided client credentials to be successfully authenticated against a selected identity provider. Applies the credentials collected by the ‘require’ assertions to be authenticated.
  - **Require HTTP Basic** (**Note:** should be used in conjunction with Require SSL or TLS). Require that incoming requests to contain HTTP basic authentication credentials.
  - **Require SAML Token Profile.** Requires incoming requests to contain a SAML (Security Assertions Markup Language) token. **Note:** The evaluated configuration defined in the *Secure Installation Guide* specifies a limited set of SAML attributes that may be used.
  - **Require SSL or TLS Transport with Client Authentication.** Requires clients to connect via SSL or TLS and optionally to provide a valid / trusted X.509 certificate. **Note:** This assertion appears in two different assertion palettes:
    - When accessed from the Access Control palette, this assertion is labeled "Require SSL or TLS Transport with Client Authentication" and has the Require Client Certificate Authentication check box selected by default.
    - When accessed from the Transport Layer Security palette, this assertion is labeled "Require SSL or TLS Transport" and does not have the Require Client Certificate Authentication check box selected by default.
  - **Require WS-Security Signature Credentials.** Requires that the web service target message includes an X.509 client certificate and has at least one element signed by that client certificate's private key as a proof of possession. **Note:** The evaluated configuration defined in the *Secure Installation Guide* specifies a limited set of attributes that may be used with this assertion – multiple signatures are not supported.

- **Service availability assertions.** The following subset of service availability assertions are evaluated:
  - **Limit Availability to Time/Days.** Enables restricting service access by a time and/or day interval. When the Gateway receives a request for the service, it will check the time and/or day restrictions before allowing the message to proceed.
  - **Restrict Access to IP Address Range.** Enables restricting service access based on the IP address of the requesting service client.
- **Policy logic assertions.** The following subset of policy logic assertions are evaluated in support of access control:
  - **All Assertions Must Evaluate to True.** All associated assertions must evaluate to true to achieve a 'success outcome'.
  - **At Least One Assertion Must Evaluate to True.** At least one associated assertion must evaluate to true to achieve a 'success outcome'.

The Policy Manager can detect inconsistencies in the application of policies so that policies are unambiguously defined.

The Policy Manager uniquely identifies the policies it creates so that it can be used to determine what policies are being implemented by remote products.

5.1.2. Access Control Policy Enforcement

The Gateway enforces the policies defined by the Policy Manager. The Gateway inspects messages sent between service clients (request messages) and service endpoints (response messages) to evaluate and enforce compliance with the defined policies.

5.1.3. Policy Security

Communication between the Policy Manager and the Gateway is protected from disclosure and modification. A trusted channel is established to identify and authenticate each end point using TLS client / server authentication.

The Gateway validates the integrity of the policy data it receives and rejects any invalid or replayed data. The Gateway generates evidence of receipt of policies.

The TOE protects the integrity of policy, identity, credential, attribute, and other security information obtained from other trusted IT entities.

5.1.4. System Monitoring

The TOE provides the ability to keep an audit/log trail to provide administrative insight into system management and operation, including identifying what policies are being defined and enforced. The TOE is capable of sending audit/log information to an external trusted entity.

The following policy assertions are used in support of system monitoring:

- **Audit Message in Policy.** Enables auditing of messages within a policy. It records events pertaining to the processing of a policy— e.g. assertion violations.

- **Add Audit Detail.** Allows the definition of a custom message that can enhance the context of an audit message.
- **Customize SOAP Fault Response.** Allows customization of the SOAP fault response on a policy-by-policy basis.

5.1.5. Robust Administrative Access

Administrative access to the TOE requires authentication and is governed by role based access control. The TOE protects against attacker attempts to illicitly authenticate using repeated guesses and enforces an administrator define password policy. The TOE displays a banner a login.

5.1.6. Continuity of Enforcement

The Gateway will continue policy enforcement in the event of a loss of connectivity with the Policy Manager.

5.2. Physical Scope and Boundary

The TOE consists of the following components:

- **Policy Manager (v8.0, Build: 4582).** The application software running on supported non-TOE operating systems.
- **Gateway (v8.0, Build: 4582).** The software including operating system, Java Virtual Machine (JDK 7u40) and database executing on supported non-TOE hardware and virtual appliances. Firmware executing on the appliance hardware is excluded from the physical boundary.

The various TOE form factors are marketed as (Policy Manager software included):

- **SecureSpan SOA Gateway Appliance.** Gateway ships on hardware.
- **SecureSpan SOA Gateway Soft Appliance.** Gateway ships as a virtual appliance (ssg-appliance-8.0-5).
- **SecureSpan SOA Gateway Software.** Gateway ships as software only for installation on client hardware (ssg-8.0-5).

In the evaluated configuration, the TOE is connected to one or more computers and shared peripherals as described in the User Guidance delivered with the TOE.

The following figure depicts the TOE and its environment.

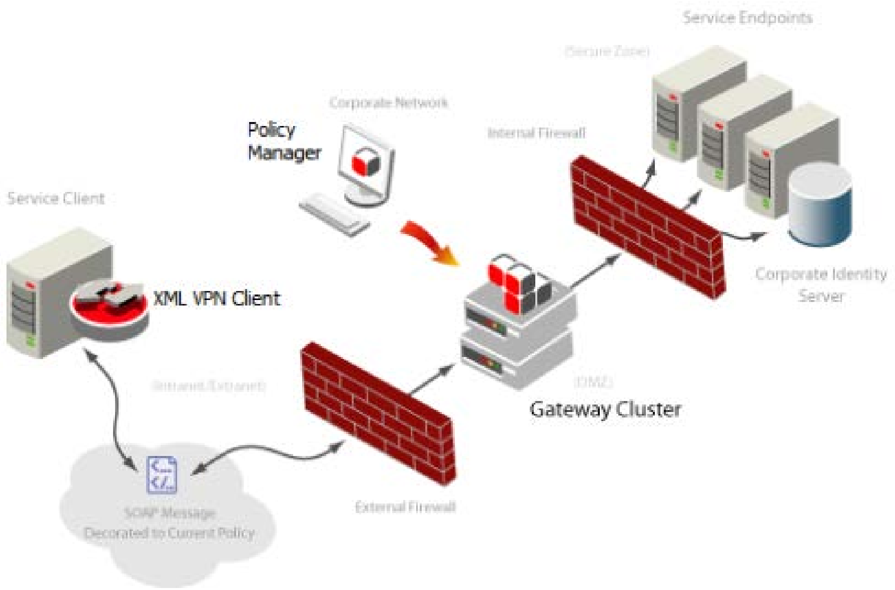

Figure 1: Depiction of TOE Deployment

6. DOCUMENTATION

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the CA Layer 7 SecureSpan SOA Gateway v8.0. Note that not all evidence is available to customers. The following documentation is available to the customer:

1. CA Layer 7 SecureSpan SOA Gateway v8.0 Installation and Maintenance Manual (Appliance Edition), v.0.8
2. CA Layer 7 SecureSpan SOA Gateway v8.0 Installation and Maintenance Manual (Software Edition), v.0.8
3. CA Layer 7 SecureSpan SOA Gateway v8.0 Policy Manager User Manual
4. CA Layer 7 SecureSpan SOA Gateway v8.0 Policy Authoring User Manual
5. CA Layer 7 SecureSpan SOA Gateway v8.0 Secure Installation Guide

The remaining evaluation evidence is described in the Assurance Activity Report developed by Computer Sciences Corporation.

7. IT PRODUCT TESTING

This section describes the testing efforts of the evaluation team.

7.1. Evaluation team independent testing

The evaluation team conducted independent testing at the CCTL lab facilities. For the testing at the CCTL, the TOE was delivered in accordance with the documented delivery procedures. The evaluation team installed and configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the developer's tests delivered to the lab as a basis for creating each of the Independent tests as required by the Assurance Activities. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the Assurance Activities under test

Each Assurance Activity was tested as required by the conformant Protection Profiles and the evaluation team verified that each test passed.

7.2. Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

8. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R3.

Computer Sciences Corporation (CSC) has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Standard Protection Profile for Enterprise Security Management Policy Management, v1.4, 23 May 2012 (ESM Policy Manager PP) and Standard Protection Profile for Enterprise Security Management Access Control, v2.0, 22 February 2012 (ESM Access Control PP). A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on May 16, 2014.

9. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the CA Layer 7 SecureSpan SOA Gateway v8.0 meets the claims stated in the Security Target. Only the security functionality specified within the Security Target was evaluated, all other functionality provided by the product needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation.

10. ANNEXES

None

11. SECURITY TARGET

- CA Layer 7 SecureSpan SOA Gateway v8.0 Security Target, Version 1.0, Revision 1.7, 28 May 2014.

12. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.
4. Common Evaluation Methodology for Information Technology Security Evaluation, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.
5. Standard Protection Profile for Enterprise Security Management Policy Management, v1.4, 23 May 2012 (ESM Policy Manager PP)
6. Standard Protection Profile for Enterprise Security Management Access Control, v2.0, 22 February 2012 (ESM Access Control PP)
7. CA Layer 8 SecureSpan SOA Gateway v8.0 Security Target, v1.7
8. Computer Sciences Corporation (CSC): CA Layer 7 SecureSpan SOA Gateway v8.0 Assurance Activity Report