National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Standard Protection Profile for Enterprise Security Management Policy Management, Version 1.4, May 23rd, 2012

Report Number: CCEVS-VR-PP-0010
Dated: 31 July 2015
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
Computer Sciences Corporation
Hanover, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Standard Protection Profile for Enterprise Security Management Policy Management, Version 1.4 (ESMPMPP14). It presents a summary of the ESMPMPP14 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the ESMPMPP14 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the CA Layer 7 SecureSpan SOA Gateway, version 8.0. The evaluation was performed by the Computer Sciences Corporation (CSC) Common Criteria Testing Laboratory (CCTL) in Hanover, Maryland, United States of America, and was completed in May 2014. This evaluation addressed the base requirements of the ESMPMPP.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the CSC CCTL.

The evaluation determined that the ESMPMPP14 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). The ST contains material drawn directly from the ESMPMPP14 as well as the Standard Protection Profile for Enterprise Security Management Policy Management. Performance of the majority of the ASE work units serves to satisfy the APE work units as well for both of these claimed PPs. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the ESMPMPP14 meets the requirements of the APE components. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the ESMPMPP14 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the CA Layer 7 SecureSpan SOA Gateway, Version 8.0, developed by CA, Inc. The evaluation was performed by the Computer Sciences Corporation Common

Criteria Testing Laboratory (CCTL) in Hanover, Maryland, United States of America, and was completed in May 2014.

The ESMPMPP14 contains a set of "base" requirements that all conformant STs must include and "additional" requirements that may or may not apply to a conformant TOE depending on its architecture and intended usage.

Because these optional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the ESMPMPP14 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the ESMPMPP14.

Protection Profile	*Standard Protection Profile for Enterprise Security Management Policy Management,, Version 1.4*
ST (Base)	CA Layer 7 SecureSpan SOA Gateway v8.0 Security Target, May 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (base)	Computer Sciences Corporation, Hanover, MD USA
CCEVS Validators (base)	Daniel Faigin, Aerospace Corporation Jerome Myers, Aerospace Corporation

3 ESMPMPP Description

This Protection Profile focuses on access control policy definition and management. ESM Policy Management products (PMs) will allow ESM Policy Administrators to configure and manage Access Control products in order to determine how objects should be protected throughout the enterprise. The output of this administrative action will be the production and distribution of policies to Access Control products. PMs should also be able to control the basic behavior of these products such as what events they audit, where they store audited event data, and how they should operate in the event of a loss of communications with the PM. A TOE that is compliant with the ESMPMPP is expected to exhibit the following behavior:

- Establish a trusted channel between itself and other Enterprise Security Management products
- Provide evidence of its identity to other Enterprise Security Management products
- Utilize organizational subject and attribute data to validate the identities and determine the authorities of Policy Administrators

- Provide a trusted remote or local interface for Policy Administrators to create and distribute policies
- Deconflict a policy that may contain contradictory data such as rules that both authorize and deny the same activity
- Provide the ability to configure the policy enforcement behavior of Access Control products
- Generate an audit trail of administrative behavior

In general, the ESM Policy Management PP exists to provide administrators with the ability to configure the behavior of products that claim conformance with the ESM Access Control PP, whether they are separate products or part of a composed solution.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: TOE Assumptions

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

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
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.WEAKIA	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control,

Threat Name	Threat Definition
	causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.WEAKPOL	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

4.3 Organizational Security Policies

Table 3: Threats

OSP Name	OSP Definition
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.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to examine human and IT entity user identity data received from the Operational Environment and determine the extent to which the claimed identity should be able to perform TSF management functions.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.
O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
O.EAVES	The TOE will either leverage a third-party cryptographic suite or contain the ability to utilize cryptographic algorithms to secure the communication channels to and from itself.
O.INTEGRITY	The TOE will contain the ability to assert the integrity of policy data.
O.POLICY	The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.

TOE Security Obj.	TOE Security Objective Definition
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.AUDIT	The Operational Environment will provide a remote location for storage of audit data
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
OE.USERID	The Operational Environment must be able to identify a user requesting access to the TOE.

5 Requirements

As indicated above, requirements in the ESMPMPP14 are comprised of the "base" requirements and additional requirements that are conditionally or strictly optional. The following are table contains the "base" requirements that were validated as part of the CA evaluation activity referenced above.

Requirement Class	Requirement Component
ESM: Enterprise Security Management	ESM_ACD.1: Access Control Policy Definition
	ESM_ACT.1: Access Control Policy Transmission
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SEL_EXT.1: External Selective Audit
	FAU_STG_EXT.1: External Audit Trail Storage
FCO: Communications	FCS_NRR.2: Enforced Proof of Receipt
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling
	FIA_SOS.1: Verification of Secrets
	FIA_UAU.2: User Authentication Before Any Action
	FIA_UID.2: User Identification Before Any Action
	FIA_USB.1: User-Subject Binding

Requirement Class	Requirement Component
FMT: Security Management	FMT_MOF_EXT.1: External Management of Functions Behavior
	FMT_MSA.1(1) Management of Security Attributes
	FMT_MSA.1(2) Management of Security Attributes
	FMT_MSA.3: Static Attribute Initialization
	FMT_MSA_EXT.5: Consistent Security Attributes
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Management Roles
FTA: TOE Access	FTA_TAB.1: TOE Access Banner
FTP: Trusted Path/Channels	FTP_ITC.1(1): Inter-TSF Trusted Channel
	FTP_ITC.1(2): Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path

The following table contains the optional requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
ESM: Enterprise Security Management	ESM_ATD.1: Object Attribute Definition	CA Layer 7 SecureSpan SOA Gateway Security Target, May 2014
	ESM_ATD.2: Subject Attribute Definition	CA Layer 7 SecureSpan SOA Gateway Security Target, May 2014
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	
	FCS_CKM_EXT.4: Cryptographic Key Zeroization	
	FCS_COP.1(1): Cryptographic Operation	
	FCS_COP.1(2): Cryptographic Operation	
	FCS_COP.1(3): Cryptographic Operation	
	FCS_COP.1(4): Cryptographic Operation	
	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	
FPT: Protection of the TSF	FPT_STM.1: Reliable Time Stamps	CA Layer 7 SecureSpan SOA Gateway Security Target, May 2014
FTA: TOE Access	FTA_SSL_EXT.1: TSF-Initiated Session Locking and Termination	CA Layer 7 SecureSpan SOA Gateway Security Target, May 2014
	FTA_SSL.3: TSF-initiated Termination	
	FTA_SSL.4: User-initiated Termination	CA Layer 7 SecureSpan SOA Gateway Security Target, May 2014
	FTA_TSE.1: TOE Session Establishment	

6 Assurance Requirements

The following are the assurance requirements contained in the ESMPMPP14:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Pass

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the ESMACPP Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

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

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

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Computer Sciences Corporation, *CA Layer 7 SecureSpan SOA Gateway v8.0 Security Target*, Version Unspecified. May, 2014.

[7] Standard Protection Profile for Enterprise Security Management Policy Management, Version 1.4, May 23, 2012.