Certification Report

Trustwave Network Access Control (NAC) Version 4.1 and Central Manager Software Version 4.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-249-CR
Version: 1.0
Date: 04 June 2014
Pagination: i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provide a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 04 June 2014, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

Trustwave Network Access Control (NAC) Version 4.1 and Central Manager Software Version 4.1 (hereafter referred to as Trustwave NAC v4.1), from Trustwave Holdings, Inc., is the Target of Evaluation. The results of evaluation demonstrate that Trustwave NAC v4.1 meets the requirements of Evaluation Assurance Level (EAL) 2 for the evaluated security functionality.

Trustwave NAC v4.1 enables network administrators to control which devices gain admission to their network and what network services they may invoke. The solution consists of a Central Manager (CM) and one or more Sensors. CM is used to configure the overall access policy for an enterprise and deploy it to Sensors. Sensors are connected to all the network segments that are controlled, and monitor all the network traffic to detect any violations of the network use policy configured by administrators.

As soon as a device attempts to gain access to the network, a Sensor immediately identifies the managed device and may be configured to run a policy check to determine if the device complies with the security policies in the network segment that it is trying to join.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 30 April 2014 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Trustwave NAC v4.1, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the Trustwave NAC v4.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

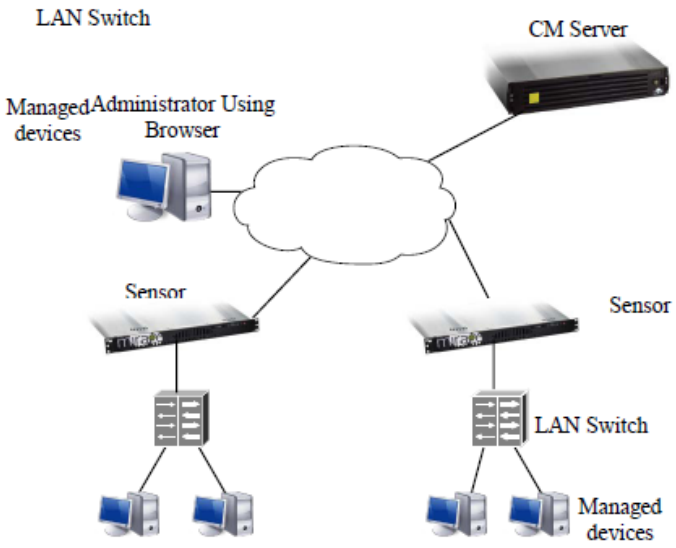
The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is Trustwave Network Access Control (NAC) Version 4.1 and Central Manager Software Version 4.1 (hereafter referred to as Trustwave NAC v4.1), from Trustwave Holdings, Inc..

2 TOE Description

Trustwave NAC v4.1 enables network administrators to control which devices gain admission to their network and what network services they may invoke. The solution consists of a Central Manager (CM) and one or more Sensors. CM is used to configure the overall access policy for an enterprise and deploy it to Sensors. Sensors are connected to all the network segments that are controlled, and monitor all the network traffic to detect any violations of the network use policy configured by administrators.

As soon as a device attempts to gain access to the network, a Sensor immediately identifies the managed device and may be configured to run a policy check to determine if the device complies with the security policies in the network segment that it is trying to join.

A diagram of the Trustwave NAC v4.1 deployment is as follows;



3 Security Policy

Trustwave NAC v4.1 implements a role-based access control policy to control administrative access to the system. In addition, Trustwave NAC v4.1 implements policies pertaining to the following security functional classes:

- *Identification and Authentication*
- *Management*
- *Network Access Control*

4 Security Target

The ST associated with this Certification Report is identified below:

Trustwave Network Access Control (NAC) Version 4.1 and Central Manager Software Version 4.1 Security Target v1.9, April 25, 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Trustwave NAC v4.1 is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following: ;*
   - *ALC_FLR.1*

b. *Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:*
   - IDS_SDC - System Data Collection
   - IDS_ANL - Analyser Analysis
   - IDS_RCT - Analyser React
   - IDS_RDR - Restricted Data Review
   - IDS_STG - System Data Storage

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of Trustwave NAC v4.1 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Managed devices will process received Address Resolution Protocol messages as specified in RFCs 826, 5227 and 5494;
- Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and ongoing; and
- The Administrator will install and configure the TOE according to the administrator guidance.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation; and
- There will be a segregated management network that supports communication between distributed components of the TOE. This network functions properly.

7 Evaluated Configuration

The evaluated configuration for Trustwave NAC v4.1 comprises:

The TOE software (Trustwave NAC v4.1) running on the following hardware;

Central Manager appliance

Item	**M-1**	**M-10**
Network Ports	Two 100 Mbps/ 1 Gbps Ethernet	
Storage Space	160 Gb	1 Tb
Maximum Sensors Managed	5	100

Sensor appliance

Item	**X-50**	**X-100**	**X-500**	**X-1000**	**X-2500**
Management Ports	One 100 Mbps/ 1 Gbps Ethernet	One 100 Mbps/ 1 Gbps Ethernet	Two 100 Mbps/ 1 Gbps Ethernet	Two 100 Mbps/ 1 Gbps Ethernet	Two 100 Mbps/ 1 Gbps Ethernet
Network Ports	Two 100 Mbps/ 1 Gbps Ethernet	Two 100 Mbps/ 1 Gbps Ethernet	Four 100 Mbps/ 1 Gbps Ethernet	Four 100 Mbps/ 1 Gbps Ethernet	Four or eight copper or fiber 1 Gbps
Monitored Traffic	Up to 1 Gb/s	Up to 1 Gb/s	Up to 1 Gb/s	Up to 1 Gb/s	Up to 1 Gb/s
Maximum VLANs	50	100	500	1000	2500

The X-series appliances shown above also support a Standalone configuration for hosting both NAC CM and Sensor functionality in a single appliance.

The publication entitled Trustwave Network Access Control (NAC) Version 4.1 Installation Supplement describes the procedures necessary to install and operate Trustwave NAC v4.1 in its evaluated configuration.

8 Documentation

The Trustwave Holdings, Inc. documents provided to the consumer are as follows:

a) *Trustwave NAC X-[50, 100, 500, 1000] Hardware Guide;*

b) *Trustwave NAC X-2500 Hardware Guide;*

c) *Trustwave NAC M-1/M-10 Hardware Guide;*

d) *Trustwave NAC 4.1 User Guide v2014-04-15, 15 April 2014;*

e) *Trustwave Central Manager Version 4.1 Getting Started Guide v2014-030-01, 3 January 2014; and*

a. *Trustwave Network Access Control (NAC) Version 4.1 Installation Supplement, v1.0, 31 January 2014.*

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Trustwave NAC v4.1, including the following areas:

Development: The evaluators analyzed the Trustwave NAC v4.1 functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the Trustwave NAC v4.1 functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the Trustwave NAC v4.1 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Trustwave NAC v4.1 configuration management system and associated documentation was performed. The evaluators found that the Trustwave NAC v4.1 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Trustwave NAC v4.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Trustwave NAC v4.1. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[1].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests; and

b. Account Management: The objective of this test goal is to test out the account management capabilities of the TOE such as creation, lockout, privileges, and limitations.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

b. Information leakage verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, login, and other scenarios using a packet sniffer; and

c. Heartbleed exploitation: The objective of this test goal is to determine if the TOE is vulnerable to the OpenSSL Heartbleed exploit and attempt to compromise the TOE using it.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

10.4 Conduct of Testing

Trustwave NAC v4.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the information Technology Security Evalaution and Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that Trustwave NAC v4.1 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Trustwave Network Access Control (NAC) Version 4.1 and Central Manager Software Version 4.1 Security Target v1.9, April 25, 2014.

e. ETR for EAL 2+ CC Evaluation of Trustwave Network Access Control (NAC) Version 4.1 and Central Manager Version 4.1, v1.1, 30 April 2014.