Certification Report

EAL 2+ Evaluation of Enterasys Netsight/Network Access Control v3.2.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-105-CR
Version: 1.0
Date: 31 may 2011
Pagination: i to iii, 1 to 8

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 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. This certification report, and its associated certificate, apply 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 Canada, 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 Canada, 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) provides 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 Canada.

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 DOMUS ITSL located in Ottawa, 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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 31 May 2011, 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

Enterasys Netsight/Network Access Control v3.2.2 (hereafter referred to as Enterasys Netsight/NAC), from Enterasys Networks, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Enterasys Netsight/NAC is a centralized network access control system that authenticates and authorizes end-system access to network resources. It ensures that only valid users and devices are permitted to connect to the network from the proper location and at the right time. The TOE supports three network access control functions: detection, authentication, and authorization. These three functions can be deployed in various combinations.

DOMUS ITSL is the CCEF that conducted the evaluation. This evaluation was completed on 11 April 2010, 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 Enterasys Netsight/NAC , the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security 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.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. The following augmentation is claimed:

- ALC_FLR.1 – Basic Flaw Remediation

Communications Security Establishment Canada, as the CCS Certification Body, declares that Enterasys Netsight/NAC 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is Enterasys Netsight/Network Access Control v3.2.2 (hereafter referred to as Enterasys Netsight/NAC), from Enterasys Networks, Inc.

2 TOE Description

Enterasys Netsight/NAC is a centralized network access control system that authenticates and authorizes end-system access to network resources. It ensures that only valid users and devices are permitted to connect to the network from the proper location and at the right time. The TOE supports three network access control functions: detection, authentication, and authorization. These three functions can be deployed in various combinations.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Enterasys Netsight/NAC is identified in Section 6 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Enterasys Networks, Inc. Netsight/Network Access Control v3.2.2
Version: 7
Date: 08 March 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*.

Enterasys Netsight/NAC is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 2 *augmented*, with all security the assurance requirements in the EAL 2 package, as well as the following:
   - ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

The Enterasys Netsight/NAC implements a role-based access control policy to control user access to what network resources they are allowed to access; details of this security policy can be found in Section 7 of the ST.

In addition, the Enterasys Netsight/NAC implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Enterasys Netsight/NAC 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- Authorized administrators who manage the TOE are non-hostile and are appropriately trained to use, configure, and maintain the TOE and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE resides in a physically controlled access facility that prevents unauthorized physical access; and
- The TOE and network devices shall be protected from MAC address spoofing and other disruptions of data and functions.

7.3 Clarification of Scope

The *Network Access Control Design Guide* and *NAC Manager Help* mention the following TOE functionality:

- TOE management via the Inventory Manager Console;
- MAC Locking;
- Identification and Authentication of administrators other than local;
- Identification and Authentication of end-users other than RADIUS;
- Assisted remediation; and
- End-system assessment and Automated Security Manager (ASM) additions to the NAC Manager blacklist.

It should be noted that the above functionality is not included within the evaluated configuration of the TOE.

8 Evaluated Configuration

The TOE is software-only defined as:

- Enterasys Netsight/Network Access Control v3.2.2 Build 48.

Two appliances are required components in the evaluated configuration, the NAC appliance and the NetSight appliance. Details on how these appliances are deployed can be found in section 1.3.2.1 of the ST.

The publication entitled Enterasys Networks, Inc. Netsight/Network Access Control v3.2.2 Guidance Documentation Supplement describes the procedures necessary to install and operate Enterasys Netsight/NAC in its evaluated configuration.

9 Documentation

The Enterasys documents provided to the consumer are as follows:

- Enterasys Network Access Control v3.2 ST v0.6;
- Enterasys Matrix® DFE-Platinum and Diamond Configuration Guide Firmware Version 6.11.xx;
- Enterasys NetSight® Network Access Control Gateway Appliance SNS-TAG-HPA / SNS-TAG-LPA Installation Guide;
- NetSight®Firmware Support;
- Enterasys® NAC Controller Hardware Installation Guide 2S4082-25-SYS 7S4280-19-SYS;
- Enterasys NetSight® Appliance SNS-NSS-A Installation Guide;
- Enterasys® Network Access Control Design Guide;
- Enterasys NetSight® Network Access Control Gateway Appliance NAC-A-20 Installation Guide;
- Enterasys NetSight® and NAC Virtual Appliance Installation Guide;
- CUSTOMER RELEASE NOTES Enterasys NetSight® Version 3.2.2.39 February, 2010;
- Enterasys Networks, Inc. Netsight/Network Access Control v3.2.2 Guidance Documentation Supplement;
- NetSight Console Help;
- NetSight® Suite Installation;
- NAC Manager Help; and
- Policy Manager Help.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Enterasys Netsight/NAC , including the following areas:

Development: The evaluators analyzed the Enterasys Netsight/NAC functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Enterasys Netsight/NAC security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Enterasys Netsight/NAC 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 Enterasys Netsight/NAC configuration management system and associated documentation was performed. The evaluators found that the Enterasys Netsight/NAC configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Enterasys Netsight/NAC during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Enterasys for Enterasys Netsight/NAC. 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.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Enterasys Netsight/NAC. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Enterasys Netsight/NAC potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the Enterasys Netsight/NAC in its operational environment.

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

11 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 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[2].

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.

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

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

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 DOMUS ITSL test goals:

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

b. Identification and Authentication: The objective of these tests is to ensure that access to the TOE is restricted to authorized users only;

c. Security Management: The objective of this test is to determine the correct operation of the remote interactions with the management server;

d. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data; and

e. Audit: The objective of these tests is to ensure that User Access Events Logging requirements have been met.

11.3 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:

- Network scanning by running port scanning tools and attempting to attack open ports;
- Network traffic monitoring and analysis by attempting to sniff network traffic;
- Bypass by attempting to exploit the capabilities of TOE interfaces in an unexpected way which could result in the violation of a TOE security policy.

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

11.4 Conduct of Testing

Enterasys Netsight/NAC was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS ITSL . 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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Enterasys Netsight/NAC behaves as specified in its ST and functional specification.

12 Results of the Evaluation

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

13 Evaluator Comments, Observations and Recommendations

The Evaluator recommends that the users read the ST and make sure the all the assumptions made regarding the environment are true in the intended environment of the TOE. The potential users of the TOE should also follow all the instructions and recommendations provided in the following documents during installation and configuration of the TOE.

Given the extensive set of user guidance, the evaluator strongly recommends users of the TOE consult the Guidance Documentation Supplement for references on relevant user guidance in order to configure the TOE in its evaluated configuration.

14 Acronyms, Abbreviations and Initializations

ASM	Automated Security Manager
CB	Certification Body
CC	Common Criteria
CCCS	Canadian Common Criteria Scheme
CCEF	Common Criteria Evaluation Facility
CEM	Common Methodology for Information Technology Security
CPL	Certified Products List
EAL	Evaluation Assurance Level
NAC	Network Access Control
SFRs	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. Enterasys Networks, Inc. Netsight/Network Access Control v3.2.2 Security Target, version 7, 8 March 2011

e. Evaluation Technical Report Enterasys Networks, Inc. Netsight/Network Access Control v3.2.2 , v1.0, 11 April 2011