Certification Report

EAL 4+ Evaluation of DefensePro Product Family Software Version 5.11

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-168-CR
Version: 1.0
Date: 22 May 2012
Pagination: i to iii, 1 to 9

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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. 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 EWA-Canada 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 22 May 2012, 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

DefensePro Product Family Software Version 5.11 (hereafter referred to as DefensePro), from Radware Ltd., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

DefensePro is a set of network devices that are deployed inline in the network, providing real-time network based Intrusion Detection/Prevention System (IDS/IPS) and anti-Denial of Service (DoS) protections for internal applications and infrastructure. A DefensePro device collects and analyzes network traffic flowing through the device, and can be configured to detect a wide set of attacks and suspected intrusion attempts. Detected events are recorded on the device, and can be configured to trigger reaction mechanisms such as blocking the suspected traffic and generating alarms.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 1 May 2012 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 DefensePro, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 4 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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.3 – Systematic Flaw Remediation.

DefensePro is conformant with the U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments, Version 1.7, July 25, 2007.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the DefensePro 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) 4 augmented evaluation is DefensePro Product Family Software Version 5.11 (hereafter referred to as DefensePro), from Radware Ltd.

2 TOE Description

DefensePro is a set of network devices that are deployed inline in the network, providing real-time network based Intrusion Detection/Prevention System (IDS/IPS) and anti-Denial of Service (DoS) protections for internal applications and infrastructure. A DefensePro device collects and analyzes network traffic flowing through the device, and can be configured to detect a wide set of attacks and suspected intrusion attempts. Detected events are recorded on the device, and can be configured to trigger reaction mechanisms such as blocking the suspected traffic and generating alarms.

A detailed description of the DefensePro architecture is found in Section 1 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for DefensePro is identified in Section 7 of the ST.

4 Security Target

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

Title: DefensePro Product Family Software Version 5.11 Security Target
Version: 0.4
Date: 26 Feb 2012

Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

DefensePro is:

a. *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.1 - System data collection;
   - IDS_ANL.1 - Analyser analysis;
   - IDS_RCT.1 - Analyser react;
   - IDS_RDR.1 - Restricted data review;
   - IDS_STG.1 - Guarantees of System data availability; and
   - IDS_STG.2 - Prevention of System data loss.

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

c. *Common Criteria EAL 4 augmented,* containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation

d. DefensePro is conformant with the U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments, Version 1.7, July 25, 2007.

5 Security Policy

DefensePro implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7 of the ST.

In addition, DefensePro implements policies pertaining to security audit, intrusion detection, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

Assumptions and Clarification of Scope

Consumers of DefensePro 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.

5.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE can only be accessed by authorized users.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

5.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE is scalable to the IT Systems it monitors.

5.3 Clarification of Scope

DefensePro offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. DefensePro is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

6 Evaluated Configuration

The evaluated configuration for DefensePro comprises:

DefensePro version 5.11.01 (build 39) software, running on one of the following supported Radware models:

• DefensePro DP-x412-NL-D-OZ device (2U with DME)

• DefensePro DP-x016-NL-Q devices (1U)

• DefensePro DP-x016-NL-D-Q devices (2U)

• DefensePro DP-x016-NL-D-QF devices (2U with DME)

The publication entitled DefensePro Product Family Common Criteria Evaluated Configuration Addendum, Software Version 5.11.01, v0.3 describes the procedures necessary to install and operate DefensePro in its evaluated configuration.

7 Documentation

The Radware Ltd. documents provided to the consumer are as follows:

a. DefensePro Product Family Common Criteria Evaluated Configuration Addendum, Software Version 5.11.01, v0.3;

b. DefensePro User Guide Software Version 5.11, RDWR-DP-V0511_UG1101; and

c. Radware Installation and Maintenance Guide, RDWR_IG_1101.

8 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of DefensePro, including the following areas:

Development: The evaluators analyzed the DefensePro functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the DefensePro security architectural description and determined that the initialization process is secure and 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 DefensePro 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 DefensePro configuration management system and associated documentation was performed. The evaluators found that the DefensePro configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorized access to the configuration items.

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

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the DefensePro design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Radware Ltd. for DefensePro. 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 DefensePro. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to DefensePro in its operational environment.

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

9 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

9.1 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 and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

9.2 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 EWA-Canada 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. Initialization: The objective of this test goal is to provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

c. Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met;

d. Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed;

[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.

e. Users and Roles: The objective of this test goal is to ensure the users and roles functionality is correct; and

f. IDS/IPS functionality: The objective of this test goal is to exercise the TOE's IDS/IPS functionality to ensure that the security claims may not be inadvertently compromised.

9.3 Independent Penetration Testing

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

a. Fail safe. This test attempts to compromise the TOE by forcing a failure state;

b. Vision client timeout. This test confirms that the timeout for an administration session can be changed to prevent unauthorized access; and

c. Leakage Verification. In this test case the TOE is monitored for information leakage during start-up and shutdown.

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

9.4 Conduct of Testing

DefensePro 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 EWA-Canada. 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.

9.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that DefensePro behaves as specified in its ST, functional specification, TOE design and security architecture description.

10 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

11 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
DME	DoS Mitigation Engine
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
ST	Security Target
TOE	Target of Evaluation

12 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 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments, Version 1.7, July 25, 2007.

e. DefensePro Product Family Software Version 5.11 Security Target, v0.4, 26 Feb 2012.

f. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of Radware Ltd. DefensePro version 5.11.01, v1.3, 1 May 2012.