Certification Report

EAL 2 + Evaluation of Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-50
Version: 1.0
Date: 17 October 2008
Pagination: i to iv, 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 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. 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 Standard 17025, General requirements for the accreditation of calibration and testing 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 IT Security Laboratory located in Ottawa, Ontario.

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 17 October 2008, 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 at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and http://www.commoncriteria.es.

This certification report makes reference to the following trademarks or registered trademarks:

- Dragon is a trademark or registered trademark of Enterasys Networks, Inc.;
- AIX is a trademark of IBM Corp.;
- SUSE is a trademark of Novell, Inc.;
- HP-UX is a registered trademark of Hewlett-Packard Company.;
- RED HAT is a registered trademark of Red Hat, Inc.;
- Solaris is a trademark of Sun Microsystems, Inc.; and
- Microsoft, Windows, Windows Vista are trademarks of Microsoft Corporation.

TABLE OF CONTENTS

Executive Summary

The Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances (hereafter referred to as Enterasys Dragon IDP), from Enterasys Networks, Inc. is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Enterasys Dragon IDP is an intrusion detection and prevention product that detects and responds to suspicious network activity based on collected forensic data. The system can alert administrators on an attack, drop offending packets, terminate sessions for TCP- and UDP-based attacks, and dynamically establish firewall rules that can keep the source of the threat off the network indefinitely or for a configurable period of time. The product provides both network-based and host-based intrusion detection/prevention.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 7 October 2008 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 Dragon IDP, 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 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.2 – Flaw reporting procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that Enterasys Dragon IDP 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 the Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances (hereafter referred to as Enterasys Dragon IDP), from Enterasys Networks, Inc.

2 TOE Description

Enterasys Dragon IDP is an intrusion detection and prevention product that detects and responds to suspicious network activity based on collected forensic data. The system will alert on an attack, drop offending packets, terminate sessions for TCP- and UDP-based attacks, and dynamically establish firewall rules that can keep the source of the threat off the network indefinitely or for a configurable period of time. The product provides both network-based and host-based intrusion detection/prevention.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Enterasys Dragon IDP is identified in Section 6 of the ST.

4 Security Target

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

Title: Enterasys Networks, Inc. Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances Security Target
Version: Version 2.0
Date: 6 October 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.3*.

The Enterasys Dragon IDP 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 – Analyzer Analysis;
   - IDS_RCT.1 – Analyzer React;
   - IDS_RDR.1 – Restricted Data Review;
   - IDS_STG.1 - Guarantee 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 2 augmented, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw reporting procedures.

6 Security Policy

Enterasys Dragon IDP implements a role-based access control policy to control user access to the system; details of this security policy can be found in Sections 5.1.3 and 6.1.3 of the ST.

In addition, Enterasys Dragon IDP implements policies pertaining to security audit, identification and authentication, security management, TOE self protection, and intrusion detection and prevention. Further details on these security policies are found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Enterasys Dragon IDP 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 Enterasys Dragon IDP.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE has access to all the IT System data it needs to perform its functions.
- 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 can only be accessed by authorized users.

7.3 Clarification of Scope

Enterasys Dragon IDP was designed and intended for use in a structured corporate environment. It cannot prevent authorized administrators from carelessly configuring the TOE such that the TOE security or the security of IT system monitored by the TOE is compromised.

The product provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

While the user guidance documents provides adequate advice for securing the operational environment, it is primarily the users' responsibility in ensuring that the networks and the systems which the Enterasys Dragon IDP is connected to, or installed on, are adequately protected.

8 Architectural Information

Enterasys Dragon IDP is an intrusion detection and prevention system that uses sensors to collect information about target systems and networks. The system includes an analyzer that interprets the information collected and initiates actions in response to the analysis.

EMS Server. The EMS Server is the central management server for the Enterasys Dragon IDP. The Server provides the Host Sensors, Network Sensors, and the Dragon Security Modules (collectively referred to as sensors) with current enforcement policies. The policies are created on, stored on, and deployed from, the Server. The sensors report event information back to the Server where it is consolidated, stored and analyzed for trends. Additionally, the Server maintains the list of users and user privileges for all system components. The Server grants permission to authorized users to view events generated by the sensors via a web-based reporting interface called Dragon Reporting. Dragon Reporting is a sub-component of the Server, that displays reports stored on the Server and provides summary information of attacks, activity graphs, summaries of rebuilt network sessions, and analysis of event trends. Dragon Reporting comprises four consoles available through a web browser: the Forensics Console, the Realtime Console, the Trending Console and the Executive Reporting Console.

EMS Client. The EMS Client is used to access the EMS Server. The Client provides a graphical user interface to manage users and their roles, enforcement policies, and network sensors.

Network Sensor. The Network Sensor is a network intrusion detection system (NIDS). This Sensor is deployed between subnets and collects network packets and analyzes them for suspicious activity. It can detect anomalies such as malformed network protocol headers and potentially malicious port scans. The Sensor can also provide SNMP alerts, enforcement of event-based policy, and reconstruction of packet and session traffic. It can also detect network patterns that may indicate probes, attacks, compromises, and other types of network abuse. In addition to typical intrusion detection capabilities, the Sensor employs active response techniques to block detected attacks. The Sensor can respond by terminating any sessions found to be potentially hostile and can reconfigure firewalls, switches, and routers to block attacks in progress. The Sensor can also analyze network-based attacks using forensic tools that capture packets and record complete session information. If an attack is suspected, the Sensor can take protective action. For example, the Sensor can create access control lists blocking certain IP addresses.

Dragon Security Module. The Dragon Security Module is also a NIDS. The Module is a Linux-based blade that provides NIDS functionality for the Matrix N-Series Enterasys Switch. The Module provides the same functionality as the Network Sensor.

Host Sensor. The Host Sensor is a software host-based IDS application that provides host-based intrusion prevention and detection functionality. This Sensor runs on the third party operating systems listed in the following Section 9 Evaluated Configuration.

9 Evaluated Configuration

Enterasys Dragon Intrusion Defense System Version 7.2.3 build 208 installs on the following operating systems: Windows 2000, Windows XP Professional, and Windows Server 2003 Server.

Enterasys Dragon Intrusion Defense System Version 7.2.3 build 273 installs on the following operating systems: AIX versions 5.2, 5.3; SUSE versions 9, 10; Fedora Core versions 3, 4, 5, 6; CentOS version 5; HP-UX versions 11, 11 with patch PHSS_33033 applied; Red Hat Enterprise Linux versions 4, 5; Solaris versions 9, 10 with latest jumbo patch applied; and Dragon ISO Slackware-based with a 2.6.14.3 kernel.

Enterasys Dragon Intrusion Defense System Version 7.2.3 build 273 installs on the following Dragon appliances:

DNSA-FE-TX	DSNSA7-GIG-SX	DSISA7-SX
DNSA-GE250-TX	DEPA	DSIPA7-FE-TX
DNSA-GE250-SX	DEMA-ME	DSIPA7-GE250-TX
DNSA-GE500-TX	DEMA-LE	DSIPA7-GE250-SX
DNSA-GE500-SX	DEMA-U	DSIPA7-GE500-TX
DNSA-GIG-TX (2U)	DEMA-RED-U	DSIPA7-GE500-SX
DNSA-GIG-SX (2U)	DEMA-6RED-U	DSIPA7-GIG-TX
DNSA-GIG-6P-TX (1U)	DSEPA7	DSIPA7-GIG-SX
DNSA-GIG-6P-SX (1U)	DSEMA7-ME	DIPA-FE-TX
DSNSA7-FE100-TX	DSEMA7-LE	DIPA-GE250-TX
DSNSA7-GE250-TX	DSEMA7-U	DIPA-GE250-SX
DSNSA7-GE250-SX	DSEMA7-RED-U	DIPA-GE500-TX
DSNSA7-GE500-TX	DISA-TX	DIPA-GE500-SX
DSNSA7-GE500-SX	DISA-SA	DIPA-GIG-TX
DSNSA7-GIG-TX	DSISA7-TX	DIPA-GIG-SX

10 Documentation

The Enterasys Networks, Inc. documents provided to the consumer are as follows:

- Enterasys Dragon® Intrusion Defense System Installation Guide, Part Number: 9034377 - 01 November 2007;
- Enterasys Dragon® Intrusion Defense System Installation Guide, Part Number: 9033997 - 13 September 2007;

- Dragon® Intrusion Defense System Appliance Quick Start, Part Number: 9034264 - 03 February 2007;
- Enterasys Dragon® Intrusion Defense System Configuration Guide, Part Number: 9033999 - 10 June 2007; and
- Enterasys Networks, Inc. Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances Common Criteria Administrative Guide Supplement, Document Version 0.5.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Enterasys Dragon IDP, including the following areas:

Configuration management: An analysis of the Enterasys Dragon IDP configuration management system and associated documentation was performed. The evaluators found that the Enterasys Dragon IDP 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.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Enterasys Dragon IDP during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the Enterasys Dragon IDP functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Enterasys Dragon IDP administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators reviewed the flaw remediation procedures used by Enterasys Networks, Inc. for Enterasys Dragon IDP. 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 Enterasys Dragon IDP ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for Enterasys Dragon IDP and found that it sufficiently described each

of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 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 accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 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 was the following list of DOMUS IT Security Laboratory 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. Audit: The objective of these tests is to ensure that User Access Events Logging requirements have been met;
c. Identification and Authentication: The objective of these tests is to ensure that access to the Enterasys Dragon IDP was restricted to authorized administrators only;
d. Security Management: The objective of these tests is to ensure that authorized administrators are able to manage and configure the Enterasys Dragon IDP and that the role access control are enforced;

[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. TOE Self Protection: The objective of these tests is to ensure that confidentiality of the data transmitted between different parts of the TOE is protected and that the TOE is able to protect itself from unwanted interference; and,
f. IDS Component Requirements: The objective of these tests is to ensure that the IDS requirements as specified in the ST are met by the TOE.

12.3 Independent Penetration Testing

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

- Application (Server, Client, Sensor) generic vulnerabilities;
- Server operating system generic vulnerabilities; and,
- Direct network based attacks.

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

12.4 Conduct of Testing

Enterasys Dragon IDP 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 IT Security Laboratory. 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.

12.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that Enterasys Dragon IDP behaves as specified in its ST and functional specification.

13 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.

14 Evaluator Comments, Observations and Recommendations

Enterasys Dragon IDP includes comprehensive guidance documents for the installation, configuration and operation of the product. Enterasys Dragon IDP should be operated in accordance with these documents.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CPL	Certified Products list
EMS	Enterprise Management Server
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDP	Intrusion Detection Prevention
IDS	Intrusion Detection System
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NIDS	Network Intrusion Detection System
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol

16 References

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

a. CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.

d. Enterasys Networks, Inc. Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances Security Target Version 2.0, 6 October 2008.

e. Evaluation Technical Report Version 1.2, Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances, EAL2+, 7 October 2008.