Certification Report

EAL 3+ Evaluation of Enterasys Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-81-CR
Version: 1.0
Date: 27 February 2009
Pagination: i to iv, 1 to 14

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 Information Technology 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/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 IT Security Laboratory, a division of NUVO Network Management, 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 27 February 2009, 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/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked or registered

trademarks:

- Enterasys and Matrix are registered trademarks of Enterasys Networks, Inc.

TABLE OF CONTENTS

Executive Summary

Enterasys Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 software, from Enterasys Networks, Inc. (hereafter referred to as Enterasys Matrix N v6.01 and Matrix X v1.6.4P4), is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 software support a product line of switch and router hybrid devices which are capable of applying access control filtering to routed traffic. These devices offer both layer 3 routing capabilities and higher speed layer 2 switching capabilities. Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 offer embedded security features that provide the ability to limit the applications on the network, and restrict the management of Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 to certain users.

DOMUS IT Security Laboratory, a division of NUVO Network Management, is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 14 January 2009, 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 Matrix N v6.01 and Matrix X v1.6.4P4, 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

[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.

sufficient evidence that it meets the EAL 3 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the Common Methodology for IT Security Evaluation, Version 2.3, for conformance to Common Criteria for IT Security Evaluation, version 2.3. The following augmentations are claimed:

ALC_FLR.1 – Basic flaw remediation

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 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) 3 *augmented* evaluation is the Enterasys Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 software, hereafter referred to as Enterasys Matrix N v6.01 and Matrix X v1.6.4P4, from Enterasys Networks, Inc.

2 TOE Description

Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 software support a product line of switch and router hybrid devices which are capable of applying access control filtering to routed traffic. These devices offer both layer 3 routing capabilities and higher speed layer 2 switching capabilities. Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 offer embedded security features that provide the ability to limit the applications on the network, and restrict the management of the TOE to certain users. The TOE may be installed on a network wherever routing and switching services are required, such as at the edge of the internal network, as part of a backbone, or as part of a data center.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 is identified in Section 5 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. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 Security Target

Version: 1.5

Date: August 29, 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.

Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 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 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following:
    - ALC_FLR.1 – Basic Flaw Remediation

6 Security Policy

Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 implement an access control policy on routed traffic through the application of Access Control Lists (ACLs). Further details on this security policy can be found in Section 5.1 of the ST.

In addition, Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 implements policies pertaining to security audit, identification and authentication, security management, and protection of the TOE security functions (TSF). Further details on these security policies may be found in Section 5.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 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 Matrix N v6.01 and Matrix X v1.6.4P4.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The TOE is installed on the appropriate, dedicated hardware and operating system. There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
- The TOE software will be protected from unauthorized modification.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE environment provides the security configuration required to allow the TOE to provide the administrator-intended secure routing and switching functions while connected to the network environment.
- The TOE is located within a controlled access facility.
- The IT environment provides the TOE with the necessary reliable timestamps.

For more information about the TOE security environment, refer to section 3 of the ST.

7.3 Clarification of Scope

The TOE 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 to violate system security, particularly from within the physical zone or domain of deployment. The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communications security.

Consumers of the TOE should be aware of the following features and/or functionality that were not included as part of the evaluated configuration:

- Telnet access to the Command Line Interface (CLI)
- Authentication mechanisms other than local authentication
- Remote Authentication Dial In User Service (RADIUS)
- Terminal Access Controller Access-Control System Plus (TACACS+)
- Request for Comment (RFC) 3580
- 802.1X authentication
- Port Web Authentication
- MAC Authentication
- Multiple Authentication
- WebView Management
- NetSight Manager
- Simple Network Management Protocol (SNMP) v1/v2 (i.e. SNMP must be used with v3 security features)
- Dynamic Host Configuration Protocol (DHCP)

In addition, all SNMP users must be configured with read-only access in the evaluated configuration of the TOE.

8 Architectural Information

Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 software support the action of either switching a packet or routing a packet. The Enterasys Matrix N v6.01 architecture includes the following subsystems to support this functionality:

- *Platform Subsystem* allows system administrators to manage and configure the Enterasys Matrix N v6.01 and review audit records.

- *SNMP Subsystem* provides SNMP support to the Enterasys Matrix N v6.01 in accordance with the SNMP version 3 Standard (Internet Engineering Task Force (IETF) Standard 62).

- *Routing Subsystem* provides the routing functionality and the application of access

control to routed packets.

- *Switching Subsystem* provides the switching services for the TOE.

The Matrix X v1.6.4P4 architecture includes the following subsystems:

- *Command Processor Subsystem* mediates access to the Matrix X v1.6.4P4. All requests between subsystems must go through the Command Processor Subsystem.
- *Command Line Interface Subsystem* allows system administrators to manage and configure the Matrix X v1.6.4P4 and review audit records.
- *SNMP Subsystem* provides SNMP support to the Matrix X v1.6.4P4 in accordance with the SNMP version 3 Standard (IETF Standard 62).
- *Host Services Subsystem* provides the interface between the embedded MontaVista Linux v3.1 OS and the Matrix X v1.6.4P4.
- *Configuration Manager Subsystem* is responsible for the persistent storage of data within the Matrix X v1.6.4P4.
- *Routing Subsystem* provides the routing functionality and the application of access control to routed packets.
- *Switching Subsystem* provides the switching services for the TOE.

Further details about Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 architecture are proprietary to the developer, and are not provided in this report.

9 Evaluated Configuration

The TOE is supported by an environment that includes one of several hardware appliance platforms manufactured by Enterasys. The TOE environment also includes the VxWorks v5.5.1 Operating System (OS) and MontaVista Linux v3.1 OS with Linux kernel v2.4.20. The combination of TOE software, underlying OS and hardware platforms for this evaluation are as follows:

- Enterasys Matrix N v6.01.01.0020 operating on the VxWorks v5.5.1 OS installed on the Matrix N1, Matrix N3, Matrix N5, Matrix N7, and Matrix N-Standalone hardware platforms.

- Enterasys Matrix X v1.6.4P4 operating on the MontaVista Linux v3.1 OS installed on the Matrix X4, Matrix X8, and Matrix X16 hardware platforms.

For evaluated configuration detail refer to Section 2.3 of the ST.

10 Documentation

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

- Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, and Matrix N, DFE Diamond Enterasys Networking System v6.01 - Common Criteria Administrative Guide Supplement.
- Enterasys Networks, Inc. Matrix X Enterasys Networking System v1.6.4P4 - Common Criteria Administrative Guide Supplement.
- Enterasys Matrix N1 7C111 Single-Slot Chassis Hardware Installation Guide (P/N 9034137-03).
- Enterasys Matrix N3 7C103 Chassis Hardware Installation Guide (P/N 9033824-05).
- Enterasys Matrix N5 POE (7C105-P) Chassis Hardware Installation Guide (P/N 9033943-03).
- Enterasys Matrix N7 7C107 Chassis Hardware Installation Guide (P/N 9033851-05).
- Enterasys Matrix N Series N-POE Power System Installation Guide (P/N 9033952-05).
- Enterasys Matrix X Secure Core Router X4-C Chassis Installation Guide (P/N 9034084-02).
- Enterasys Matrix X X8-C Secure Core Router X8-C Chassis Installation Guide (P/N 9034083-03).
- Enterasys Matrix X Secure Core Router X16-C Chassis Installation Guide (P/N 9034082-04).
- Enterasys Matrix DFE-Gold Series Configuration Guide Firmware Version 6.01.xx

(P/N 9033933-13).

- Enterasys Matrix DFE-Platinum and Diamond Series Configuration Guide Firmware Version 6.01.xx (P/N 9033800-16).
- Enterasys Networks, Inc. Enterasys Matrix N Standalone (NSA) Series Configuration Guide Firmware Version 6.01.xx (P/N 9034073-10).
- Enterasys Matrix X Secure Core Router Command Line Interface Reference Guide Firmware Version 1.6.x (P/N 9034085-09).
- Enterasys Matrix X Secure Core Router Configuration Guide Firmware Version 1.6.x (P/N 9034086-09).

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Enterasys Matrix N v6.01 and Matrix X v1.6.4P4, including the following areas:

Configuration management: An analysis of the Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 configuration management system and associated documentation was performed. The evaluators found that the Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 configuration items were clearly marked, and could be modified and controlled. 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 the Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 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 Matrix N v6.01 and Matrix X v1.6.4P4 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 Matrix N v6.01 and Matrix X v1.6.4P4 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 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 Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 design and implementation.

The evaluators reviewed the flaw remediation procedures used by Enterasys Networks, Inc. for Enterasys Matrix N v6.01 and Matrix X v1.6.4P4. 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 Matrix N v6.01 and Matrix X v1.6.4P4 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 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 EAL 3 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 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 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. Security Audit: The objective of this test goal is to verify the TOE's ability to generate, store and allow authorized viewing of audit records;

b. User Data Protection: The objective of this test goal is to verify the TOE's ability to enforce an access control policy on routed traffic;

c. Identification and Authentication: The objective of this test goal is to verify the TOE's ability to establish and verify a claimed user identity;

d. Security Management: The objective of this test goal is to verify the TOE's ability to manage aspects of the TOE Security Functions (TSF), including security function behaviour and TSF data; and

e. Protection of the TSF: The objective of this test goal is to verify the TOE's ability to provide integrity to and management of the mechanisms that provide the TSF.

[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.

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:

- Network scanning by running port scanning tools and attempting to attack open ports;
- Network traffic monitoring and analysis by attempting to sniff network traffic;
- Denial-of-service attack by launching SYN flood attacks; and
- 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 anticipated operating environment.

12.4 Conduct of Testing

Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 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 located in Ottawa, Ontario, 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.

12.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ 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

Consumers of Enterasys Matrix N v6.01 and Matrix X v1.6.4P4 should consider assumptions about usage and environmental settings, defined in the Section 3 of ST, and the TOE protection scope, clarified in the Section 7.3 of this document, as requirements for the product's installation and its operating environment.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
ACL	Access Control List
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
IETF	Internet Engineering Task Force
ETR	Evaluation Technical Report
IT	Information Technology
OS	Operating System
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
SNMP	Simple Network Management Protocol
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TOE	Target of Evaluation
TSF	TOE Security Function

16 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 2.3, August 2005.

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

d. Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 Security Target, version 1.5, August 29, 2008.

e. Evaluation Technical Report for EAL3+ Evaluation of the Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4, Version 0.8, January 14, 2009.