Certification Report

EAL 2 Evaluation of

Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches and E-Series Switch/Routers

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-102-CR
Version: 1.0
Date: 08 September 2009
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 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 EWA-Canada 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 08 September 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:

- Force10 Networks and E-Series are registered trademarks and Force10, C-Series, FTOS and S-Series are trademarks of Force10 Networks, Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches and E-Series Switch/Routers (hereafter referred to as FTOS 7.8), from Force10 Networks, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 evaluation.

FTOS 7.8 is an operating system that runs on specific hardware platforms (C-Series switches, S-Series switches, E-Series switch/routers). The TOE consists entirely of software while the hardware platforms form part of the operating environment for the TOE. The TOE provides management functions and switching/routing functionality (where applicable).

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 14 August 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 FTOS 7.8, 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 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.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that FTOS 7.8 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 evaluation is Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches and E-Series Switch/Routers (hereafter referred to as FTOS 7.8), from Force10 Networks.

2 TOE Description

FTOS 7.8 is an operating system that runs on specific hardware platforms (C-Series switches, S-Series switches, E-Series switch/routers). The TOE consists entirely of software while the hardware platforms form part of the operating environment for the TOE. The TOE provides management functions and switching/routing functionality (where applicable).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for FTOS 7.8 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: Security Target, Force10 Networks FTOS 7.8 for C-Series Switches, S-Series
           Switches, and E-Series Switch/Routers
Version: 1.4
Date: 28 July 2009

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.*

FTOS 7.8 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 conformant*, with all security the assurance requirements in the EAL 2 package.

6   Security Policy

FTOS 7.8 implements an information flow control policy to control the flow of network traffic through the TOE based upon the security parameters embedded within the information flow and rules established by the administrator of the TOE. Details of this security policy can be found in Section 6 of the ST.

In addition, the FTOS 7.8 implements policies pertaining to security audit, identification and authentication, and security management. Further details on these security policies may be found in Section 6 of the ST.

7   Assumptions and Clarification of Scope

Consumers of FTOS 7.8 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 Assumptions are listed in the ST:

- Administrators of the TOE are adequately trained, follow all relevant guidance and are trusted to perform their duties in a non-hostile manner.

7.2   Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is installed correctly in the network infrastructure such that it can effectively control information flows.

- The TOE is installed in an environment which provides physical security as well as uninterruptible electrical power and regulated temperature control.

- External authentication services and external time services are available to the TOE.

7.3   Clarification of Scope

Potential users of the TOE should note that while the TOE is only designed to run on designated hardware appliances from Force10 Networks, the TOE itself consists only of software. The hardware forms part of the operational environment of the TOE and as such was not subject to evaluation.

8   Architectural Information

FTOS 7.8 is a custom implementation of the Unix operating system based upon NetBSD. FTOS 7.8 consists of two subsystems which are the NetBSD/HAL kernel which implements a stable OS providing memory allocation, scheduling and hardware drivers, and the Process Space which provides the routing, switching and management functions specific to the TOE.

The NetBSD/HAL subsystem provides both standard operating system functionality (based on a custom implementation of NetBSD v1.6) as well as a hardware abstraction layer (HAL) which provides specific device drivers for the Force10 switches and switch/routers.

The Process Space subsystem implements processes which provide specific Force10 switching and routing functions on top of the NetBSD OS. The following processes are executed as part of the Process Space subsystem:

- Layer 2 switching protocols;

- Layer 3 routing protocols;

- System services and management functions ; and

- Security services and protocols.

9   Evaluated Configuration

The evaluated configuration for FTOS 7.8 consists of version 7.8.1.0 of the Force10 Operating System (FTOS) running on the hardware platforms:

- C-Series switches;

- S-Series switches; and

- E-Series switch/routers.

10 Documentation

The Force10 Networks documents provided to the consumer are as follows:

- FTOS Command Reference for the C-Series, Version 7.8.1.0, 11 March 2009, Edition 3;

- FTOS Configuration Guide for the C-Series, Version 7.8.1.0, 11 March 2009, Edition 3;

- Installing and Maintaining the C150 System. 5 June 2008, PN:100-00063-00;

- Installing and Maintaining the C300 System, 22 April 2008, PN:100-00057-00;

- FTOS Command Reference for the E-Series, Version 7.8.1.0, 11 March 2009, Edition 3;

- FTOS Configuration Guide for the E-Series, Version 7.8.1.0, 11 March 2009, Edition 3;

- Installing and Maintaining the E300 System, 14 March 2008, PN:100-00026-04;

- Installing and Maintaining the E600i System, April 2008, PN:100-00040-03;

- Installing and Maintaining the E1200i System, 11 February 2009, PN:100-00056-01;

- FTOS Command Reference for the S-Series, Version 7.8.1.0, 11 March 2009, Edition 3;

- FTOS Configuration Guide for the S-Series, Version 7.8.1.0, 11 March 2009, Edition 3;

- Installing S25N and S25V Systems, 15 December 2008, 100-00061-02;

- Installing the S25P System, 15 December 2008, 100-00058-02;

- Installing the S50 System, June 2007;

- Installing the S2410 System, 15 December 2008; and

- Operational User Guidance and Preparative Procedures Supplement, Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches and E-Series Switch/Routers, Version 1.1, 27 July 2009.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of FTOS 7.8, including the following areas:

Development: The evaluators analyzed the FTOS 7.8 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 FTOS 7.8 security architectural description and determined that the initialization process was 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 were correct.

Guidance Documents: The evaluators examined the FTOS 7.8 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the FTOS 7.8 configuration management system and associated documentation was performed. The evaluators found that the FTOS 7.8 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 FTOS 7.8 during distribution to the consumer.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of FTOS 7.8. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify FTOS 7.8 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the FTOS 7.8 in its operational environment.

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

12 ITS Product Testing

Testing at EAL 2 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 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,

---

[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.

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 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 complete the installation and configuration of the TOE ensuring that the tested TOE is in its evaluated configuration;

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; and

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

12.3 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:

- Reconnaissance;
- Port Scanning;
- Direct attacks; and
- Misuse.

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

12.4 Conduct of Testing

FTOS 7.8 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.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that FTOS 7.8 behaves as specified in its ST and functional specification.

13 Results of the Evaluation

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

14 Evaluator Comments, Observations and Recommendations

The TOE documentation includes a Command Reference Guide and a Configuration Guide specific to each platform type. Detailed installation guides are also provided for each specific platform model.

EWA-Canada performed a site visit to review the developer's life cycle processes with respect to Configuration Management (CM) and Delivery. The evaluators found that Force10 has comprehensive CM documentation and maintains rigorous control over their automated CM system.

15 Acronyms, Abbreviations and Initializations

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

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 3.1
        Revision 2, September 2007.

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

d.   Security Target, Force10 Networks FTOS 7.8 for C-Series Switches, S-Series
        Switches, and E-Series Switch/Routers, Version 1.4, 28 July 2009.

e.   Evaluation Technical Report for EAL 2 Common Criteria Evaluation of Force10
        FTOS 7.8 for C-Series Switches, S-Series Switches and E-Series Switch/Routers,
        Document No. 1596-000-D002, Version 1.4, 14 August 2009.