Certification Report

Fortigate UTM appliances running FortiOS 5.0 Patch Release 10

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment, 2015

Document number: 383-4-282-CR
Version: 1.0
Date: April 14, 2015
Pagination: i to iii, 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 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies 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, 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, 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) provide 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.

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 CGI IT Security Evaluation & Test Facility.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 14 April 2015, 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).

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

- FortiOS™ is a trademark of Fortinet, Inc.

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

TABLE OF CONTENTS

Executive Summary

Fortigate UTM appliances running FortiOS 5.0 Patch Release 10 (hereafter referred to as Fortigate UTM v5.0.10), from Fortinet, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Fortigate UTM v5.0.10 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 with the Stateful Traffic Filter Firewall Version 1.0 extended package (hereafter referred to as the NDPP).

Fortigate UTM v5.0.10 is a series of hardware security systems that are designed to protect computer networks from abuse. They reside between the network they are protecting and an external network such as the Internet, restricting the information flow between the networks to that permitted by a policy (set of rules) defined by an authorized administrator. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time.

The TOE is designed to provide firewall services ensuring network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks. The TOE is capable of robust filtering based on information contained in IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP headers as specified by their respective RFCs. Additionally the TOE is capable of content inspection of FTP and H.323 protocols to work with the dynamic nature of these protocols.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 14 April 2015 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 Fortigate UTM v5.0.10, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the Fortigate UTM v5.0.10 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

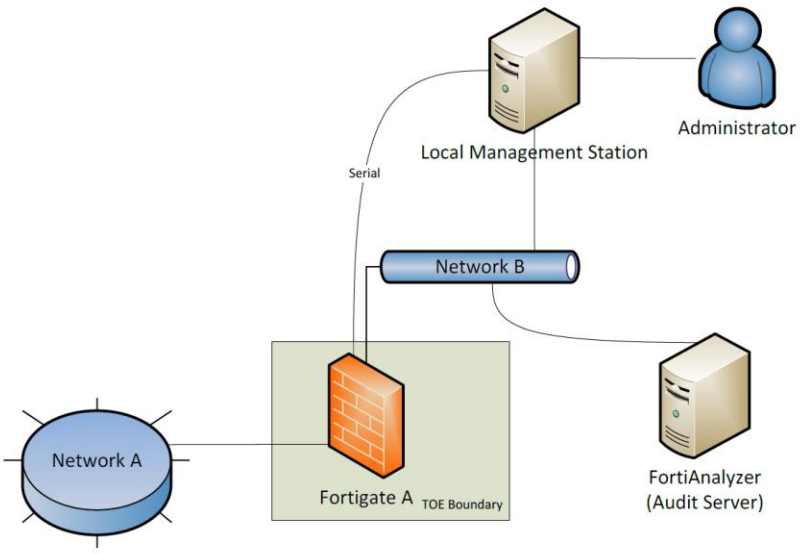
Fortigate UTM appliances running FortiOS 5.0 Patch Release 10 (hereafter referred to as Fortigate UTM v5.0.10), from Fortinet, Inc., is the Target of Evaluation. The Fortigate UTM v5.0.10 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 with the Stateful Traffic Filter Firewall Version 1.0 extended package (hereafter referred to as the NDPP).

2 TOE Description

Fortigate UTM v5.0.10 is a series of hardware security systems that are designed to protect computer networks from abuse. They reside between the network they are protecting and an external network such as the Internet, restricting the information flow between the networks to that permitted by a policy (set of rules) defined by an authorized administrator. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time.

The TOE is designed to provide firewall services ensuring network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks. The TOE is capable of robust filtering based on information contained in IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP headers as specified by their respective RFCs. Additionally the TOE is capable of content inspection of FTP and H.323 protocols to work with the dynamic nature of these protocols.

A diagram of the Fortigate UTM v5.0.10 architecture is as follows;



3 Security Policy

Fortigate UTM v5.0.10 implements a role-based access control policy to control administrative access to the system. In addition, Fortigate UTM v5.0.10 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Trusted Path/Channels
- Stateful Traffic Filtering

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Fortigate UTM v5.0.10:

Cryptographic Algorithm	Standard	Certificate #
Triple-DES (3DES)	FIPS 46-3	#1804, #1805, #1806, #1807 , #1808
Advanced Encryption Standard (AES)	FIPS 197	#3166, #3167, #3168, #3169, #3171
Rivest Shamir Adleman (RSA)	FIPS 186-2	#1604, #1605, #1606, #1607
Secure Hash Algorithm (SHA-1)	FIPS 180-2	#2619, #2620, #2621, #2622, #2624
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	#1994, #1995, #1996, #1997, #1999
Deterministic Random Bit Generator (DRBG)	SP 800-90A	#652

4 Security Target

The ST associated with this Certification Report is identified below:

Fortigate UTM appliances running FortiOS 5.0 Patch Release 10 Security Target, version 1.7, April 13, 2015.

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4,* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Fortigate UTM v5.0.10 is:

a. Conformant to the Protection Profile for Network Devices, v1.1, June 8, 2012 (Errata #2) with the Stateful Traffic Filter Firewall Version 1.0 extended package ,
b. *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:*

   - FAU_STG_EXT.1 - External audit trail storage
   - FCS_CKM_EXT.4 - Cryptographic key zeroization
   - FCS_RBG_EXT.1 - Cryptographic operation: random bit generation
   - FCS_HTTPS_EXT.1 - HTTPS
   - FCS_TLS_EXT.1 - TLS
   - FIA_PMG_EXT.1 - Password management
   - FIA_UIA_EXT.1 - User identification and authentication
   - FIA_UAU_EXT.2 - Password-based authentication mechanism
   - FPT_SKP_EXT.1 - Protection of TSF data
   - FPT_APW_EXT.1 - Protection of administrator passwords
   - FPT_TUD_EXT.1 - Trusted update
   - FPT_TST_EXT.1 - TSF testing
   - FTA_SSL_EXT.1 - TSF-initiated session locking
   - FFW_RUL_EXT.1 - Stateful Traffic Filtering

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

6 Assumptions and Clarification of Scope

Consumers of Fortigate UTM v5.0.10 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE;
- The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks. and
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

6.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

6.3 Clarification of Scope

Only the secure management and stateful packet filter firewall functionality of the TOE was evaluated, the TOE has other functionality that was not included as part of this evaluation.

7 Evaluated Configuration

The evaluated configuration for Fortigate UTM v5.0.10 comprises:

- The TOE firmware (FortiOS v5.0.10) running on the following platforms;

FortiGate-20C	FortiGate-111C	FortiGate-621B
FortiWiFi-20C	FortiGate-100D	FortiGate-800C
FortiGate-30D	FortiGate-140D	FortiGate-1000C
FortiWiFi-30D	FortiGate-140D-PoE	FortiGate-1000D
FortiWiFi-30D-PoE	FortiGate-200B	FortiGate-1200D
FortiGate-40C	FortiGate-200B-PoE	FortiGate-1240B
FortiWiFi-40C	FortiGate-200D	FortiGate-1500D
FortiGate-60C	FortiGate-240D	FortiGate-280D-PoE
FortiGate-60D	FortiGate-300C	FortiGate-3040B
FortiWiFi-60C	FortiGate-300D	FortiGate-3140B
FortiGate-80C	FortiGate-310B	FortiGate-3240C
FortiWiFi-80CM	FortiGate-311B	FortiGate-3600C
FortiGate-90D	FortiGate-500D	FortiGate-3700D
FortiGate-90D-PoE	FortiGate-600C	FortiGate-3950B
FortiGate-110C	FortiGate-620B	FortiGate-3951B

The TOE firmware can also be installed one of the following hardware blades;

- FortiGate-5001A
- FortiGate-5001B
- FortiGate-5001C
- FortiGate-5001D
- FortiGate-5101C
- FortiSwitch-5203B

The hardware blades themselves run on the following blade servers;

- FortiGate-5020 (2 Blade Slots)
- FortiGate-5060 (6 Blade Slots)
- FortiGate-5140B (14 Blade Slots)

The TOE requires the FTR-ENT1 USB token for the generation of random numbers.

The TOE requires a FortiAnalyzer appliance running FortiAnalyzer 5.0.7 firmware to act as an audit server in the environment.

The publication entitled FIPS 140-2 and Common Criteria Compliant Operation for FortiOS™ 5.0.10 01-510-267768-20150206 March 20, 2015 describes the procedures necessary to install and operate Fortigate UTM v5.0.10 in its evaluated configuration.

8 Documentation

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

a. FortiOS™ Handbook for FortiOS 5.0 01-5010-99686-20150219 February 19, 2015;

b. FortiGate™ Log Message Reference v5.0 Patch Release 10 01-510-112804-20150313 March 13, 2015;

c. FortiOS™ CLI Reference for FortiOS 5.0 01-509-99686-20150226 February 26, 2015;

d. FIPS 140-2 and Common Criteria Compliant Operation for FortiOS™ 5.0.10 01-510-267768-20150206 March 20, 2015;

e. FortiAnalyzer v5.0 Patch Release 9 Administration Guide 05-509-187572-20141020 October 20, 2014; and

f. *FortiGate Appliances with FortiOS 5.0 (NDPP Compliant) Product Architectural Description 0.3 February 6, 2015*.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Fortigate UTM v5.0.10, including the following areas:

Development: The evaluators analyzed the Fortigate UTM v5.0.10 functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the Fortigate UTM v5.0.10 functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the Fortigate UTM v5.0.10 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 Fortigate UTM v5.0.10 configuration management system and associated documentation was performed. The evaluators found that the Fortigate UTM v5.0.10 configuration items were clearly marked.

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

10 ITS Product Testing

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

10.1 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

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 test goals:

a. NDPP required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the NDPP to which the TOE is claiming conformance.

10.2 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:

a. NDPP required assurance activities. The evaluator performed the assurance activities mandated by the protection profile to which the TOE is claiming conformance; and
b. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

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

10.3 Conduct of Testing

Fortigate UTM v5.0.10 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evalution and Test Facility. 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.

10.4 Testing Results

The independent tests yielded the expected results, providing assurance that Fortigate UTM v5.0.10 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a NDPP conformance claim as claimed in Section 5. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 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
NDPP	Protection Profile for Network Devices
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Protection Profile for Network Devices, v1.1, June 8, 2012

e. Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall Version 1.0

f. Fortigate UTM appliances running FortiOS 5.0 Patch Release 10 Security Target, version 1.7, April 13, 2015

g. Fortinet, Inc. Fortigate UTM appliances running FortiOS 5.0 Common Criteria NDPP with Errata #2 and Stateful Traffic Firewall Extended Package Evaluation Technical Report v1.8, April 14, 2015.