Communications Security Establishment
Centre de la sécurité des télécommunications

COMMON CRITERIA CERTIFICATION REPORT

FortiAnalyzer™ Centralized Reporting Appliances running Firmware 5.2.4

11 July 2016

v1.0

383-4-360

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – 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 Canadian CC Scheme, 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.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the 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.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme, and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

FortiAnalyzer™ Centralized Reporting Appliances running Firmware 5.2.4 (hereafter referred to as the Target of Evaluation, or TOE), from Fortinet, Inc., was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE is a log collection and reporting device which aggregates log data from Fortinet devices and/or other syslog-compatible devices. Administrators can filter and review records, including traffic, event, virus, attack, Web content, and email. The TOE implements a FIPS 140-2 validated module to secure communications to trusted administrators and to secure audit logs in transit from another IT entity to the TOE.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 11 July 2016 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, 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 Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	**FortiAnalyzer™ Centralized Reporting Appliances running Firmware 5.2.4**
Developer	**Fortinet, Inc.**
Conformance Claim	**Protection Profile for Network Devices, v1.1, June 8, 2012, with Errata #3**

1.1 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.

1.2 TOE DESCRIPTION

The TOE is a log collection and reporting device which aggregates log data from Fortinet devices and/or other syslog-compatible devices. Administrators can filter and review records, including traffic, event, virus, attack, Web content, and email. The TOE implements a FIPS 140-2 validated module to secure communications to trusted administrators and to secure audit logs in transit from another IT entity to the TOE.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

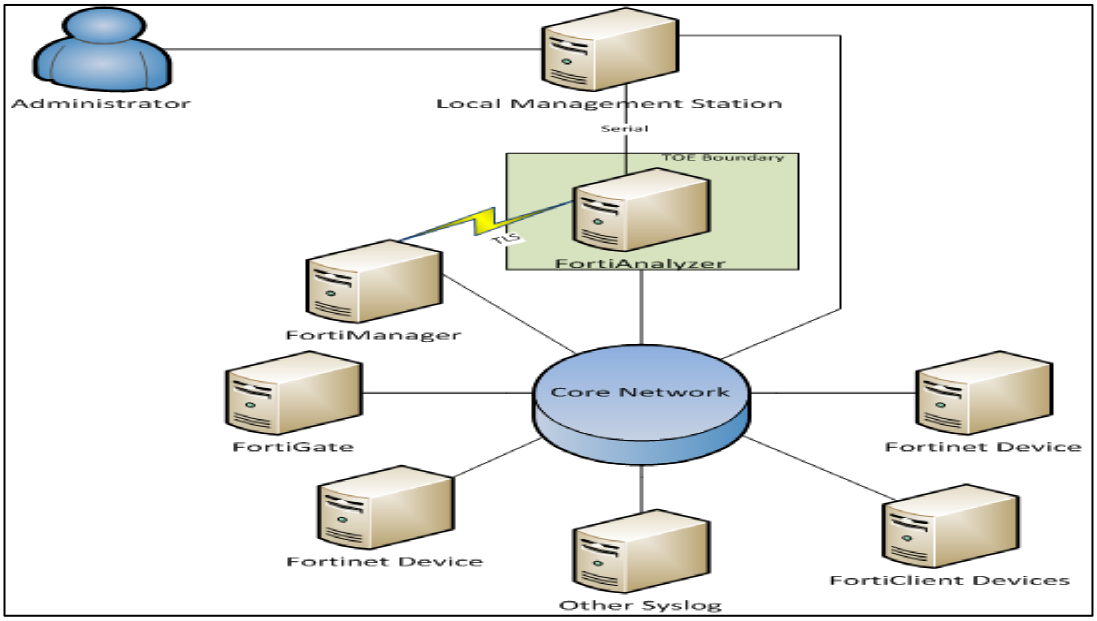

Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE 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

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic module was evaluated to the FIPS 140-2 standard by the CMVP and implemented in the TOE:

Table 1 Cryptographic Module

Cryptographic Module	Certificate Number
FortiAnalyzer 5.2 (Firmware Version: 5.2.4-build0738 150923)	2526

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- 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.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 CLARIFICATION OF SCOPE

The scope of the evaluation is limited to secure management functionality only.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises FortiAnalyzer 5.2.4 0738 FIPS/CC build running on the following hardware appliances:

- FAZ-200D
- FAZ-1000C
- FAZ-1000D
- FAZ-2000B
- FAZ-3000D
- FAZ-3000E
- FAZ-3500E
- FAZ-3900E
- FAZ-4000B

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a. FortiAnalyzer 5.2.4 Administration Guide 05-524-232167-20150922 September 22, 2015

b. FortiAnalyzer 5.2.4 CLI Reference 05-523-232152-201150923 September 23, 2015

c. FortiAnalyzer 5.2.4 Release Notes 05-524-292531-20151102 November 02, 2015

d. FortiAnalyzer 5.2.4 Upgrade Guide September 22, 2015

e. FortiAnalyzer Hardware Manual, September 26, 2013

f. FIPS 140-2 and Common Criteria Compliant Operation for FortiAnalyzer 5.2.4, July 7, 2016

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the TOE 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 TOE security architectural description and determined that the initialization process is 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 are correct.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

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

6 TESTING ACTIVITIES

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

6.1 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.

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.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 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. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP.

6.3.1 FUNCTIONAL TEST RESULTS

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

6.4 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and

b. SSH Backdoor Vulnerability: The objective of this test is to attempt to exploit a publicized SSH backdoor vulnerability.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
CCS Publication #4, Technical Oversight, Version 1.8, October 2010.
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
FortiAnalyzer™ centralized reporting appliances running Firmware 5.2.4 Security Target, Version 0.8, 14 June 2016.
FortiAnalyzer centralized reporting appliances running Firmware 5.2.4 Common Criteria NDPP Evaluation Technical Report, Version 1.7, 11 July 2016.