TLP:WHITE

Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Fortinet FortiAnalyzer 7.2.9

30 June 2025

596-EWA

V1.0

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). 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 Common Criteria Program, and the conclusions of the testing laboratory 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

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

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL 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, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the 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, 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 CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Fortinet FortiAnalyzer 7.2.9 (hereafter referred to as the Target of Evaluation, or TOE), from **Fortinet, Inc.** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

EWA-Canada is the CCTL that conducted the evaluation. This evaluation was completed on **30 June 2025** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the 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.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

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

Table 1: TOE Identification

TOE Name and Version	Fortinet FortiAnalyzer 7.2.9
Developer	Fortinet, Inc.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL4+ with ALC_FLR.3

1.2 TOE DESCRIPTION

The TOE, Fortinet ForiAnalyzer 7.2.9, is a stand-alone appliance that runs FIPS-CC firmware build. The TOE acts as an audit server that also offers vulnerability management functionality by analyzing logs collected from target hosts for known issues. In the evaluated configuration the TOE operates as the Analyzer with FIPS-CC mode enabled.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

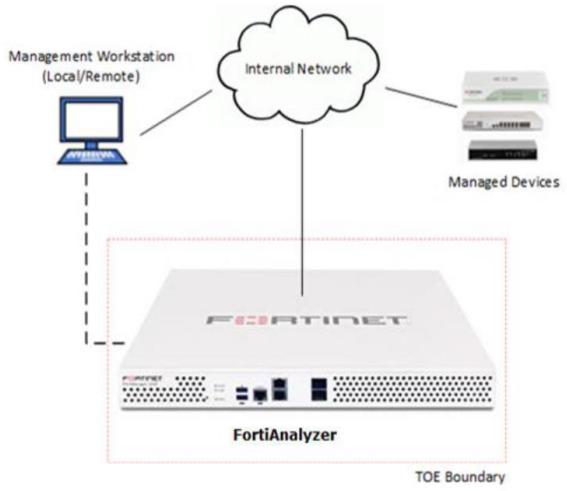

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path
- Data Collection and Reporting

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 implementations are used by the TOE and have been evaluated by the CAVP/CMVP:

Table 2: Cryptographic Implementation(s)

Cryptographic Implementation	Certificate Number
Fortinet FortiAnalyzer SSL Cryptographic Library v7.2	A6837
Fortinet FortiAnalyzer RBG Cryptographic Library v7.2	A6839

3 ASSUMPTIONS AND CLARIFICATION 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:

- The TOE will be located within controlled access facilities and protected from unauthorized physical modification.
- Authorized administrators are properly trained, not malicious, and follow all administrative guidance. Authorized administrators are trusted to administer the TOE correctly.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

3.2 CLARIFICATION OF SCOPE

The following features are excluded from this evaluation:

- Automated updates that do not require administrative action were not evaluated. Only manual updates using a Universal Serial Bus (USB) token are allowed in the evaluated configuration.
- FortiAnalyzer Collector Mode
- The following Representational State Transfer (REST) Application Programming Interfaces (APIs) are not included in the evaluation:
    - JavaScript Object Notation (JSON)
    - eXtensible Markup Language (XML)
    - Software Development Kit (SDK)
- FortiAnalyzer being managed by FortiManager using the FGFM protocol is currently excluded from the evaluation.
- The following protocol/interfaces are excluded from this evaluation:
    - SSH Client
    - DDNS
    - DHCP
    - HTTP
    - NTP
    - SNMP
    - SMTP

- Telnet
- TFTP Client
- LDAP
- RADIUS
- SYSLOG
- High Availability

- The following modules/services are excluded from this evaluation:
  - FortiView
  - FortiSoC
  - Trusted Platform Module (TPM)
  - FortiAnalyzer Cloud

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	Fortinet FortiAnalyzer 7.2.9 Build # 6429
TOE Hardware	FAZ-300G
Operational Environment	FortiGate v7.2.9

4.1 DOCUMENTATION

The following documentation is provided in Portable Document Format (PDF) format and is available at https://docs.fortinet.com/product/fortianalyzer/7.2 for download at to assist in the configuration and installation of the TOE:

a) FortiAnalyzer v7.2.9 Administration Guide, January 14, 2025
FortiAnalyzer-7.2.9-Administration_Guide.pdf

b) FortiAnalyzer v7.2.9 CLI Reference, December 11, 2024
FortiAnalyzer_7.2.9_CLI_Reference.pdf

c) FortiManager & FortiAnalyzer 7.2.9 Log Reference, December 11, 2024
FortiManager_&_FortiAnalyzer_7.2.9_Log_Reference.pdf

d) FortiAnalyzer v7.2.9 Release Notes, February 4, 2025
fortianalyzer-7.2.9-release-notes.pdf

The following Common Criteria Guidance Supplement is also available to customers upon request:

e) FortiAnalyzer 7.2, EAL4 Common Criteria Technote, February 19, 2025
FAZ 7.2 EAL4 CC Technote.pdf

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 documentation provided by the vendor; they determined that the security architecture description depicts the self-protection, domain separation, non-bypassability principles; the functional specification accurately describes and categorizes the TOE security functionality (TSF) interfaces, the implementation representation captures the detailed internal workings of the TSF, and the TOE design description provides appropriate level of decomposition. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

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 development security included appropriate security measures to protect the TOE and its parts, and an effective life-cycle model is in place.

The evaluators examined the delivery documentation and determined that it described all 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 tests, and performing a vulnerability analysis.

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 Evaluation Test Report (ETR). 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 TESTING

During this evaluation, the evaluator developed independent functional & penetration 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. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests

b. Cryptographic Implementation Verification: The evaluator confirmed that the claimed cryptographic implementation was present in the TOE

c. Independent Evaluator Tests: The evaluator examined SSH, HTTPS, and FGT to FAZ protocol implementations.

6.3.1 INDEPENDENT TESTING RESULTS

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

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **3 June 2025** and included the following search terms:

FortiAnalyzer	FortiOS Linux	Apache
Intel Core i3	OpenSSL	PostgreSQL
FOS Linux	OpenSSH	

Vulnerability searches were conducted using the following sources:

National Vulnerability Database https://nvd.nist.gov/vuln	PSIRT Advisories https://fortiguard.fortinet.com/psirt
CERT https://www.kb.cert.org/vuls/	CISA KEV https://www.cisa.gov/known-exploited-vulnerabilities-catalog

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Section 1.1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Fortinet FortiAnalyzer 7.2 Security Target v1.4, 25 June 2025
Evaluation Technical Report for Common Criteria Evaluation of Fortinet, Incorporated FortiAnalyzer 7.2 v1.4, 30 June 2025