Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

# COMMON CRITERIA CERTIFICATION REPORT

## Fortinet FortiGate™ Next Generation Firewalls with FortiOS 6.2.7

## 15 October 2021

## 515-EWA



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, 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 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 Project).

# TABLE OF CONTENTS



# LIST OF FIGURES



# LIST OF TABLES



# EXECUTIVE SUMMARY

**Fortinet FortiGate™ Next Generation Firewalls with FortiOS 6.2.7** (hereafter referred to as the Target of Evaluation, or TOE), from **Fortinet, Incorporated** , 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 15 October 2021 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 FortiGate™ Next Generation Firewalls with FortiOS 6.2.7 |
| **Developer** | Fortinet, Incorporated |

## 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:

EAL 4+ ALC_FLR.3 - Systematic Flaw Remediation

## 1.2 TOE DESCRIPTION

The TOE is a network appliance designed to provide firewall, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus protection, antispam protection and content filtering to provide network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks.

## 1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

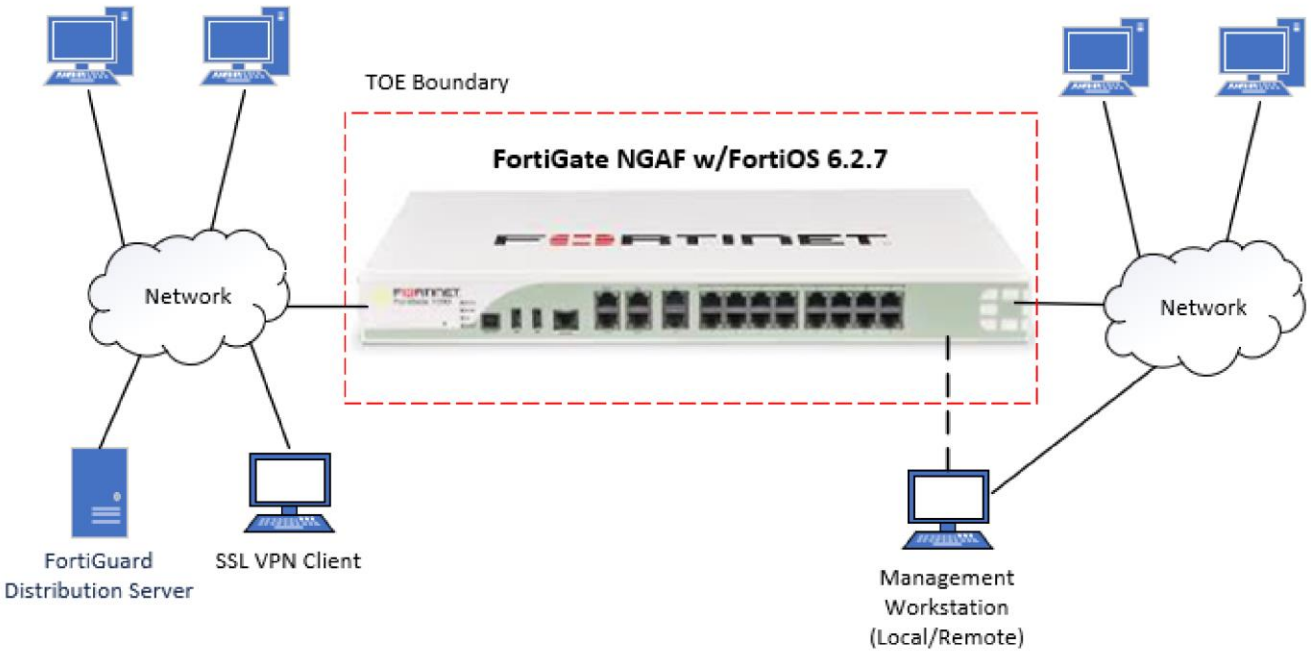


**Figure 1: TOE Architecture**

# 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
- Trusted Path/Channel
- Anti-Virus Actions
- Intrusion Prevention

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 implementation has been evaluated by the CMVP and is used by the TOE:

**Table 2: Cryptographic Implementation**

| Cryptographic Module | Certificate Number |
|---|---|
| FortiOS 6.0 and 6.2 | #3814 |

# 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 hardware appliances will be located within controlled access facilities and protected from unauthorized physical modification
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains
- Information cannot flow among the internal and external networks unless it passes through the TOE

## 3.2 CLARIFICATION OF SCOPE

The following TOE features are excluded from this evaluation:

- Centralized management of the TOE by FortiManager servers
- The TOE's antispam, content filtering and traffic shaping features
- The ICMP, SNMP, LDAP, Windows AD, NTP, Radius and Routing protocols
- The FortiGate REST API (not used in the evaluated configuration)
- FortiGuard-Antispam, Endpoint Control, and FortiSandbox services
- The TOE's DHCP, DDNS, or DNS server capabilities
- Traffic offloading to the FortiASIC NPx network processors

The following TOE features are disabled by default and are excluded from the scope of this evaluation:

- HTTP GUI
- The TOE acting as a telnet client or server
- The TOE acting as a TFTP client.

# 4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

<table>
<tr><td>TOE Software/Firmware</td><td>FortiOS 6.2.7 (Build # 5081)<br>Virtual Models<table>
<tr><td>FortiGate-VM00</td><td>FortiGate-VM08</td></tr>
<tr><td>FortiGate-VM01</td><td>FortiGate-VM16</td></tr>
<tr><td>FortiGate-VM02</td><td>FortiGate-VM32</td></tr>
<tr><td>FortiGate-VM04</td><td>FortiGate-VMUL</td></tr>
</table></td></tr>
<tr><td>TOE Hardware</td><td><table>
<tr><td>FWF-60E-DSL</td><td>FG-101F</td><td>FG-601E</td><td>FG-3200D</td></tr>
<tr><td>FG-60F</td><td>FG-140E</td><td>FG-900D</td><td>FG-3300E</td></tr>
<tr><td>FG-60F-3G4G</td><td>FG-140E-PoE</td><td>FG-1000D</td><td>FG-3301E</td></tr>
<tr><td>FG-61E</td><td>FG-200E</td><td>FG-1100E</td><td>FG-3400E</td></tr>
<tr><td>FG-61F</td><td>FG-201E</td><td>FG-1100E-DC</td><td>FG-3401E</td></tr>
<tr><td>FWF-60F</td><td>FG-300D</td><td>FG-1101E</td><td>FG-3600E</td></tr>
<tr><td>FWF-61E</td><td>FG-300E</td><td>FG-1200D</td><td>FG-3601E</td></tr>
<tr><td>FWF-61F</td><td>FG-301E</td><td>FG-1500D</td><td>FG-3700D</td></tr>
<tr><td>FG-80E</td><td>FG-400D</td><td>FG-1500DT</td><td>FG-3800D</td></tr>
<tr><td>FG-80E-PoE</td><td>FG-400E</td><td>FG-1500D-DC</td><td>FG-3810D</td></tr>
<tr><td>FG-81E</td><td>FG-401E</td><td>FG-2000E</td><td>FG-3815D</td></tr>
<tr><td>FG-81E-PoE</td><td>FG-500D</td><td>FG-2200E</td><td>FG-3960E</td></tr>
<tr><td>FG-100E</td><td>FG-500E</td><td>FG-2201E</td><td>FG-3980E</td></tr>
<tr><td>FG-100EF</td><td>FG-501E</td><td>FG2500E</td><td>FG-5001D</td></tr>
<tr><td>FG-100F</td><td>FG-600D</td><td>FG-3000D</td><td>FG-5001E</td></tr>
<tr><td>FG-101E</td><td>FG-600E</td><td>FG-3100D</td><td>FG-5001E1</td></tr>
<tr><td>FG-6301F</td><td>FGR-60F</td><td>FWF-30E</td><td>FWF-50E</td></tr>
<tr><td>FG-6501F</td><td>FGR-60F-3G4G</td><td>FG-40F</td><td>FG-51E</td></tr>
<tr><td>FGR-30D</td><td>FG-30E</td><td>FG-50E</td><td>FWF-51E</td></tr>
<tr><td>FG-52E</td><td>FG-60E</td><td>FG-60E-DSL</td><td>FG-60E-PoE</td></tr>
<tr><td>FWF-60E</td><td>FG-40F-3G4G</td><td></td><td></td></tr>
</table></td></tr>
</table>

| | |
|---|---|
| **Environmental Support** | • ESXi v6.7 (Virtual Models)<br>• FortiGuard Distribution Server<br>• Araneus Alea II Entropy token<br>• FortiAnalyzer Server v6.2.7 (Build 1398) |

## 4.1 DOCUMENTATION

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

a) FortiOS – CLI Reference, Version 6.2.7, February 9, 2021
b) FortiOS - Log Reference, Version 6.2.7, December 17, 2020
c) FortiOS - Cookbook, Version 6.2.7, February 10, 2021
d) FortiOS – Handbook, Version 6.0, June 17, 2020
e) FortiOS 6.2 and FortiGate NGFW Appliances, EAL4 Common Criteria Technote, May 25, 2021

# 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 design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. 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 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 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 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 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. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests

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

c. GUI Session Hijacking: The evaluator confirmed that the TOE is not susceptible to privilege escalation through cookie hijacking

d. Bypass of session lockout: The evaluator confirmed that the TOE enforces session lockouts across interfaces

e. GUI Control bypass: The evaluator confirmed that the TOE is not susceptible to privilege escalation through manipulation of the GUI implementation

### 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

The penetration testing effort 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 penetration testing effort.

### 6.4.1 PENETRATION TEST RESULTS

Type 1 & 2 searches were conducted on **4/19/2021** and included the following search terms:

| | | |
|---|---|---|
| FortiGate | FortiOS | Fortinet Firewall |
| CP8 | CP9 | CP9XLite |
| CP9Lite | FortiOS Cryptographic Library | |

Vulnerability searches were conducted using the following sources:

| | |
|---|---|
| National Vulnerability Database: https://nvd.nist.gov/vuln/search | Fortinet support: https://www.fortiguard.com/psirt |
| Google | |

The independent penetration testing did not uncover any 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 (CCCS). 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 Table 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 |
| CM | Configuration Management |
| CMVP | Cryptographic Module Validation Program |
| CSE | Communications Security Establishment |
| CCCS | Canadian Centre for Cyber Security |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| GC | Government of Canada |
| IT | Information Technology |
| ITS | Information Technology Security |
| 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. |
| Security Target Fortinet FortiGate™ Next Generation Firewalls with FortiOS 6.2.7, 12 October 2021, v1.10 |
| Evaluation Technical Report Fortinet FortiGate™ Next Generation Firewalls with FortiOS 6.2.7, 15 October 2021, v1.4 |