Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

FortiGate/FortiOS Version 6.2.7

14 January 2022

559-LSS

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

FortiGate/FortiOS Version 6.2.7 (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.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on 14 January 2022 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	FortiGate/FortiOS Version 6.2.7
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:

collaborative Protection Profile for Network Devices, v2.2e with the following PP-Modules:

- **PP-Module for Stateful Traffic Filter Firewalls, v1.4e;**
- **PP-Module for Virtual Private Network (VPN) Gateways, v1.1; and**
- **PP-Module for Intrusion Prevention Systems, v1.0**

1.2   TOE DESCRIPTION

The TOE is a firewall that includes Virtual Private Network (VPN) and Intrusion Prevention System (IPS) capabilities.
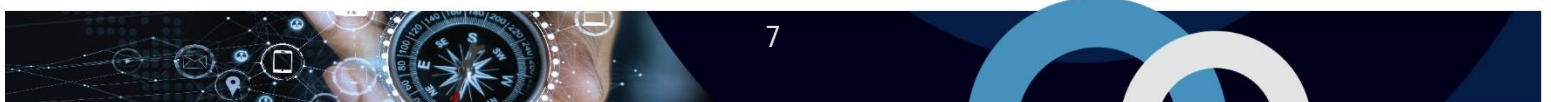
1.3   TOE ARCHITECTURE

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:
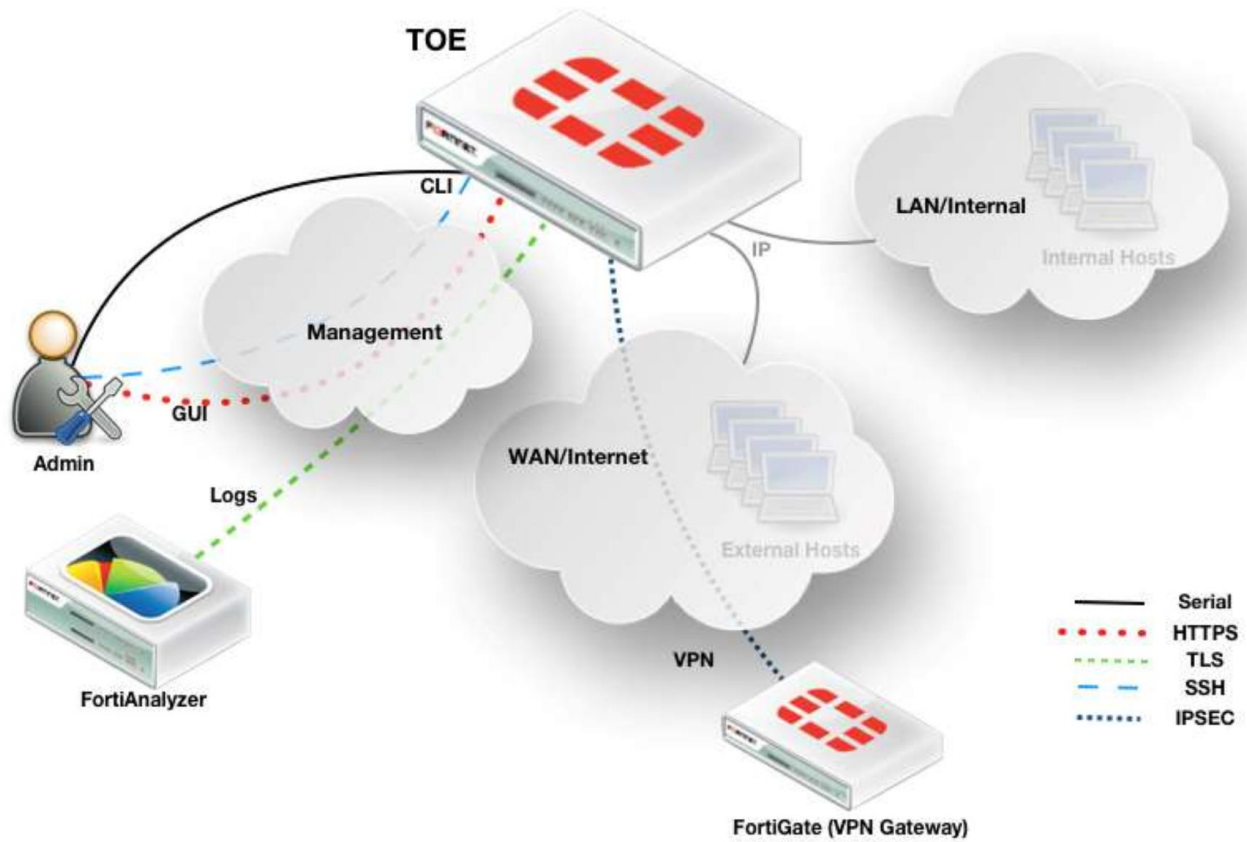
- Security Audit
- Cryptographic Support
- Residual Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels
- Stateful Traffic and Packet Filtering
- Intrusion Prevention

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

Table 2:   Cryptographic Implementation(s)

| Cryptographic Module/Algorithm	Certificate Number
Fortinet FortiOS FIPS Cryptographic Library v6.2	C1575
Fortinet FortiOS-VM FIPS Cryptographic Library v6.2	C2197, C2200
Fortinet FortiOS SSL Cryptographic Library v6.2	C1549, C1576
Fortinet FortiOS-VM SSL Cryptographic Library v6.2	C2140, C2199, C2201
Fortinet FortiOS RBG Cryptographic Library v6.2	C1573
Fortinet FortiOS-VM RBG Cryptographic Library v6.2	C2195, C2198
Fortinet CP8 Cryptographic Library	C1797
Fortinet FortiOS CP9 Cryptographic Library	C1578
Fortinet CP9Lite Cryptographic Library	C1798
Fortinet CP9XLite Cryptographic Library	A1253

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 Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.

- The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality

- A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

- The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

- For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g., offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

- The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

- The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.

- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

- The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device

- The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

- For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

- For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

- It is assumed that 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.

- This assumption defines the TOE's placement in a network such that it is able to perform its required security functionality.
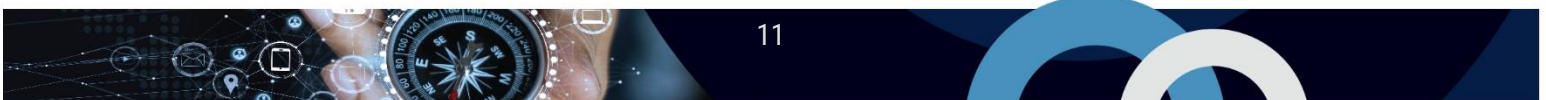
3.2   CLARIFICATION OF SCOPE

Only the functionality covered by the claimed protection profile and modules was evaluated.

The following features are not within scope of this evaluation:

a) High-Availability
b) FortiExplorer client
c) Anti-spam
d) Anti-virus
e) Content filtering
f) Web filtering
g) Use of syslog
h) FortiToken and FortiSSO Authentication
i) Stream Control Transmission Protocol (SCTP), BGP, RIP and DHCP protocols
j) Usage of the boot-time configuration menu to upgrade the TOE
k) Policy-based VPN
l) SSL VPN
m) Virtual domains (vdoms)
n) Logging to FortiCloud

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	FortiOS Version 6.2.7 Build 5067				
	Virtual Models				
	FortiGate-VM01			FortiGate-VM08	
	FortiGate-VM02			FortiGate-VM16	
	FortiGate-VM04			FortiGate-VM32	
	FortiGate-VMUL				
TOE Hardware	FG-30E	FWF-30E	FG-40F	FG-50E	FG-40F-3G4G
	FWF-50E	FG-51E	FWF-51E	FG-52E	FG-60E-DSLJ
	FG-60E	FG-60E-DSL	FG-60E-PoE	FG-60F	FG-60F
	FWF-60E	FWF-60E-DSL	FWF-60F	FG-61E	FG-61F
	FG-61F	FWF-61E	FWF-61F	FG-80E	FG-800D
	FG-80E-PoE	FG-81E	FG-81E-PoE	FG-100E	FWF-40F
	FG-100EF	FG-100F	FG-101E	FG-101F	FWF-40F-3G4G
	FG-140E	FG-140E-PoE	FG-200E	FG-201E	FWF-50E-2R
	FG-300D	FG-300E	FG-301E	FG-400D	FWF-60E-DSLJ
	FG-400E	FG-401E	FG-500D	FG-500E	FWF-60F
	FG-501E	FG-600D	FG-600E	FG-601E	FWF-61F
	FG-900D	FG-1000D	FG-1100E	FG-1101E	
	FG-1200D	FG-1500D	FG-1500D-DC	FG-1500DT	
	FG-2000E	FG-2200E	FG-2201E	FG-2500E	
	FG-3000D	FG-3100D	FG-3100D-DC	FG-3200D-DC	
	FG-3200D	FG-3300E	FG-3301E	FG-3400E	
	FG-3401E	FG-3600E	FG-3601E	FG-3700D	
	FG-3800D	FG-3810D	FG-3815D	FG-3960E	
	FG-3980E	FG-5001D	FG-5001E	FG-5001E1	
	FGR-30D	FGR-60F	FGR-60F-3G4G	FWF-61F	

Environmental Support	⊙ ESXi v6.7 (Virtual Models)
	⊙ Fortinet Entropy token (for models that require it)
	⊙ FortiAnalyzer 200D log server running v6.0.4 (build0292)
	⊙ CRL Webserver

4.1   DOCUMENTATION

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

a) FortiOS – Cookbook, Version 6.2.7, 01-627-538742-20210210

b) FortiOS 6.2 and FortiGate NGFW Appliances FIPS 140-2 and Common Criteria Technote, 01-627-672110-20210525

c) FortiOS 6.2.7 CLI Reference, 01-627-685877-20210209

d) FortiOS - Log Reference, Version 6.2.7, 01-627-538745-20201217

e) FortiOS - Hardening your FortiGate, Version 6.2.0, 01-620-554155-20201210

f) Custom IPS and Application Control Signature 3.6 Syntax Guide, 43-360-453749-20200225

g) FortiOS 6.2 Virtualization Reference, https://docs.fortinet.com/vm

h) FortiGate Virtual Appliances documentation https://docs.fortinet.com/document/fortigate-private-cloud/6.2.0/vmware-esxiadministration-guide/706376/about-fortigate-vm-on-vmware-esxi

i) FortiGate/FortiWiFi 30E/50E/51E 01-540-269598-20180808

j) FortiGate 52E 01-540-300075-20170907

k) FortiGate 60E/61E Series 01-540-367071-20181107

l) FortiGate 60E-DSL 01-560-442605-20200519

m) QuickStart Guide FortiGate/FortiWiFi 40F/40F-3G4G & 60F/61F Series, August 4, 2020

n) FortiGate 80E/81E 01-543-402959-20180808

o) FortiGate 80E/81E-POE 01-542-391830-20180314

p) FortiGate 100E/101E 01-540-366134-20170913

q) FortiGate 100EF 01-543-403497-20170907

r) QuickStart Guide FortiGate 100F/101F Series, April 14, 2020

s) FortiGate 140E/140E-PoE Series 01-543-404092-20180807

t) FortiGate 200E/201E 01-542-381079-20190912

u) FortiGate 300D 01-506-238488-20170824

v) FortiGate 300E/301E 01-560-440261-20191010

w) FortiGate 400D 01-523-277788-20170824

x) FortiGate 400E/401E 01-563-522532-20200427

y) FortiGate 500D 01-523-278008-20190408

z) FortiGate 500E/501E 01-560-440260-20191009

aa) FortiGate 600D 01-523-278008-20170907

bb) FortiGate 600E/601E 01-602-519311-20190726

cc) FortiGate 800D 01-540-273916-20200724

dd) FortiGate 900D 01-523-279315-20200406

ee) FortiGate 1000D 01-503-237227-20200406

ff)   FortiGate 1100E/1101E 01-620-24051-20190425

gg) FortiGate 1200D 01-540-306494-20190613

hh) FortiGate 2200E/2201E 01-600-231503-20200430

ii)   FortiGate 3000D 01-522-266144-20170907

jj)   FortiGate 3100D 01-5011-275737-20180711

kk) FortiGate 3200D 01-522-256537-20190321

ll)   FortiGate 1500D 01-523-211767-20200406

mm)   FortiGate 3300E/3301E 01-600-511354-20200430

nn) FortiGate 3400E/3401E Series 01-602-511354-20200225

oo) FortiGate 3600E/3601E Series 01-602-510285-20200225

pp) FortiGate 3700D 01-540-292415-20190501-M

qq) FortiGate 3800D 01-540-292415-20190828-M

rr)   FortiGate 3810D 01-522-261444-20170901-M

ss) FortiGate 3815D 01-540-292419-20170901-M

tt)   FortiGate-5001D 01-560-0242101-20170728

uu) FortiGate 2000E/2500E 01-540-306896 -20170907

vv) FortiGate 3960E/3980E 01-540-376285-20180807

ww)FortiGate-5001E System Guide 01-600-410512-20190709

xx)   FortiGate Rugged 30D Information 01-540-297736-20200812

yy)   FortiGate Rugged 60F/3G4G Series October 15, 2020

zz)   FortiGate 100F/101F Series QuickStart Guide December 11, 2020

aaa)   FortiGate 1500DT QSG Supplement 01-540-297032-20200728

bbb)   FortiGate 1500D QSG Supplement 01-523-211767-20200728

ccc)   FortiGate/FortiWiFi 40F & 60F Series QuickStart Guide August 4, 2020

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.
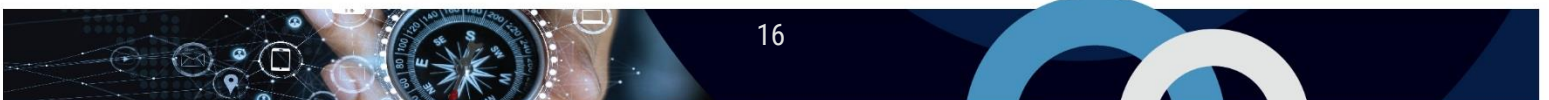
6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent 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. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP

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

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.
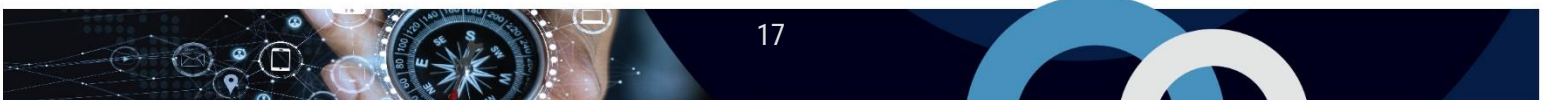
6.4   VULNERABILITY ANALYSIS

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 **6/14/2021** and included the following search terms:

Fortinet	CP8	CP9X-lite	Linux Kernel 3.2.16	Apache v2.4.41
FortiGate	CP9	Fortinet Entropy Token	OpenSSL 1.1.1	
FortiOS	CP9-lite	Araneus USB TRNG hardware Token	OpenSSH 7.1	

In addition to a standard web search, vulnerability searches were conducted using the following sources:

Fortinet FortiGuard Services: https://Fortiguard.com	Community (Symantec) security community: https://www.securityfocus.com/
NIST National Vulnerabilities Database: https://web.nvd.nist.gov/view/vuln/search	Tenable Network Security: http://nessus.org/plugins/index.php?view=search
Tipping Point Zero Day Initiative: http://www.zerodayinitiative.com/advisories	Offensive Security Exploit Database: https://www.exploit-db.com/
Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities	OpenSSL Vulnerabilities: https://www.openssl.org/news/vulnerabilities.html

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 (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.
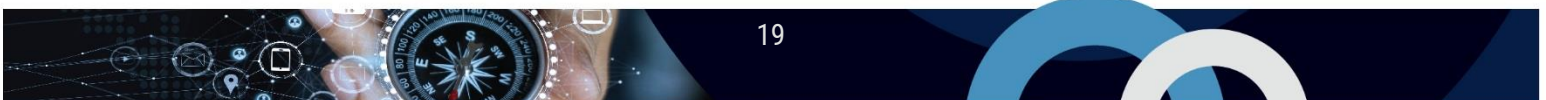
8 SUPPORTING CONTENT

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
IPS	Intrusion Prevention System
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
VPN	Virtual Private Network

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 FortiGate/FortiOS Version 6.2.7, 14 January 2021, v1.7
Evaluation Technical Report FortiGate/FortiOS Version 6.2.7, 14 January 2021, v1.7
Assurance Activity Report FortiGate/FortiOS Version 6.2.7, 14 January 2021, v1.6