Communications Security Establishment
Centre de la sécurité des télécommunications

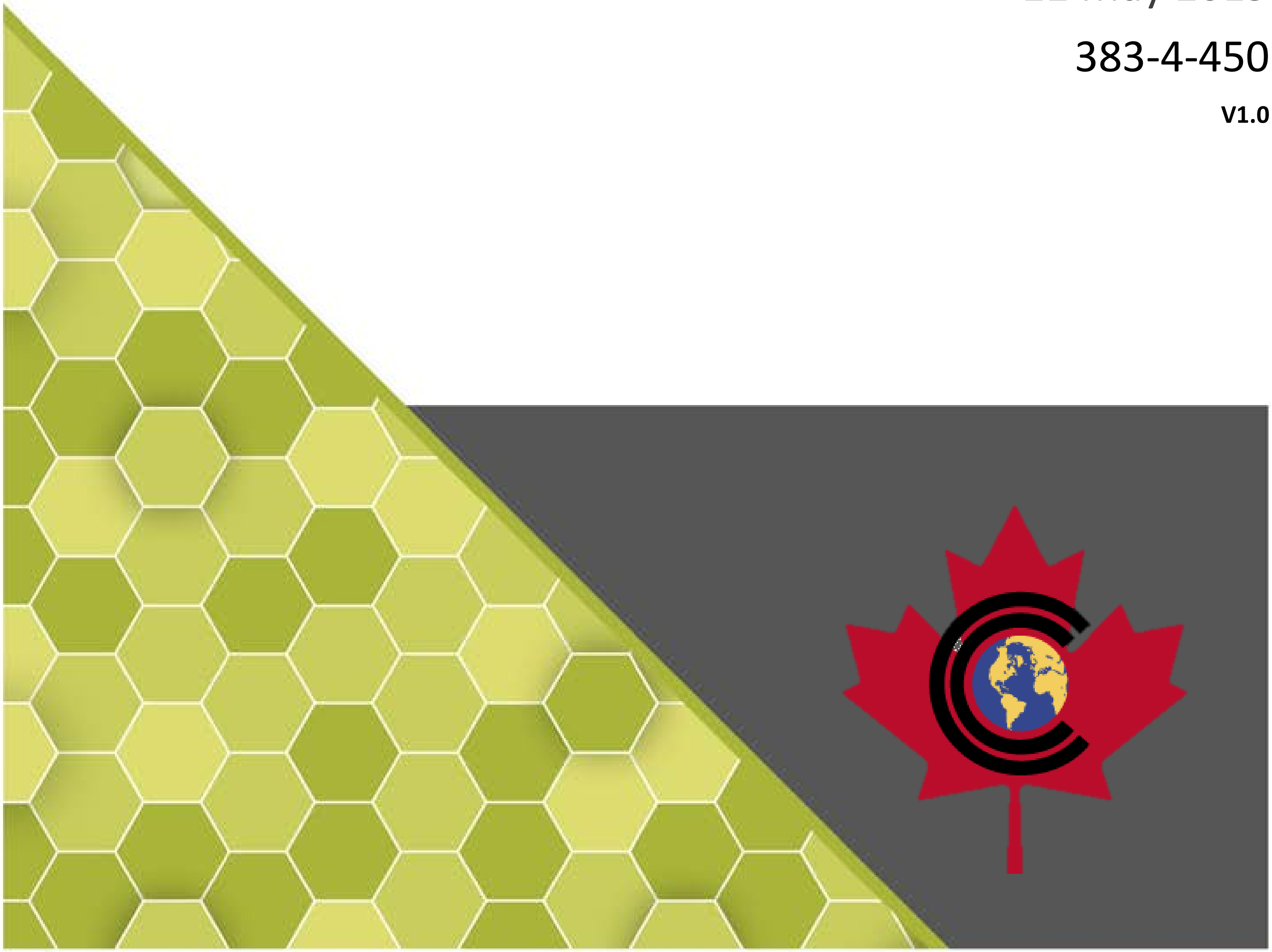
COMMON CRITERIA CERTIFICATION REPORT

Fortinet FortiGate w/ FortiOS v5.6.7

22 May 2019

383-4-450

V1.0



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.

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 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

Fortinet FortiGate w/ FortiOS v5.6.7 (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 TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

Lightship Security is the CCEF that conducted the evaluation. This evaluation was completed 22 May 2019 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 Canadian 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	Fortinet FortiGate w/ FortiOS v5.6.7
Developer	Fortinet, Inc.
Conformance Claim	collaborative Protection Profile for Stateful Traffic Filter Firewalls, v2.0e+20180314

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 firewall that includes Virtual Private Network (VPN) and Intrusion Prevention System (IPS) capabilities. The TOE is typically deployed as a gateway between two networks, such as an internal office network and the internet.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

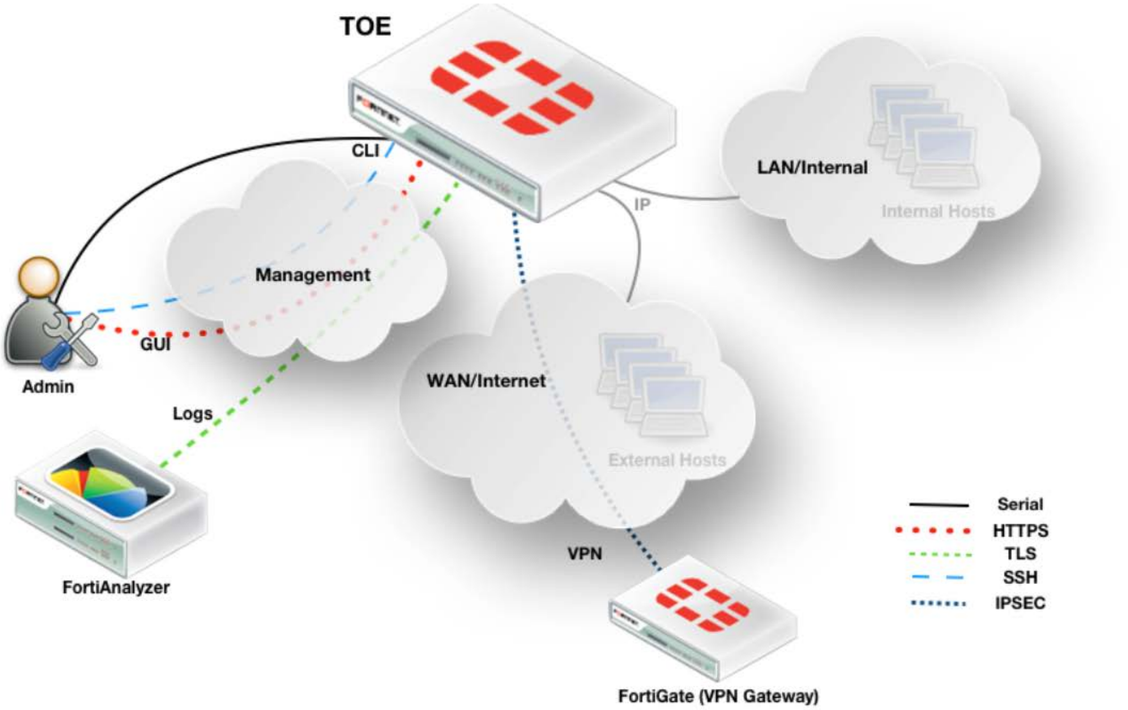


Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

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

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 Government of Canada approved cryptographic algorithms were evaluated by the CAVP and used by the TOE:

Table 2 Cryptographic Algorithm(s)

Cryptographic Algorithm	Standard	Certificate Number
Advanced Encryption Standard (AES)	FIPS 197	C468, C469, C530, C531, C610
Rivest Shamir Adleman (RSA)	FIPS 186-4	C468, C469, C530, C531, C610
Secure Hash Algorithm (SHS)	FIPS 180-3	C468, C469, C530, C531, C610
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	C468, C469, C530, C531, C610
Deterministic Random Bit Generation (DRBG)	SP 800-90A	C529
Key Agreement Scheme	SP 800-56A	C468, C530, C531
Component Validation List	SP 800-56A	C468, C530
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-4	C468, C530, C531, C610

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:

- The firewall device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the firewall’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the firewall and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the firewall that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the firewall.
- The firewall device is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the firewall device should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
- The Security Administrator(s) for the firewall device are assumed to be trusted and to act in the best interest of security for the organization. This includes being 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 firewall.
- The firewall device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the firewall device.
- The firewall 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 firewall are protected by the host 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 firewall equipment when the equipment is discarded or removed from its operational environment.

3.2 CLARIFICATION OF SCOPE

Due to the limitations of the current CCRA, only the stateful firewall functionality of the TOE was included in this version of the certification documents.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

The TOE firmware (FortiOS 5.6.7 Build 1653) on the any of the following hardware platforms;

FG-30E	FWF-60E-DSL	FG-201E	FG-1200D	FG-3810D
FWF-30E	FG-61E	FG-300D	FG-1500D	FG-3815D
FG-50E	FWF-61E	FG-300E	FG-2000E	FG-3960E
FWF-50E	FG-80E	FG-301E	FG-2500E	FG-3980E
FG-51E	FG-80E-PoE	FG-400D	FG-3000D	FG-5001D[1]
FWF-51E	FG-81E	FG-500D	FG-100E	FG-5001E
FG-52E	FG-81E-PoE	FG-500E	FG-100EF	
FG-60E	FG-101E	FG-501E	FG-3100D	
FG-60E-DSL	FG-140E	FG-600D	FG-3200D	
FG-60E-PoE	FG-140E-PoE	FG-900D	FG-3700D	
FWF-60E	FG-200E	FG-1000D	FG-3800D	

With support from the operating environment for;

- A FortiAnalyzer acting as an Audit Server
- CRL web Server capable of servicing up CRLs over HTTP

4.1 DOCUMENTATION

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

a. FIPS 140-2 and Common Criteria Compliant Operation for FortiOS 5.6, Doc No. 01-567-535352-20190122

b. FortiOS Handbook - CLI Reference version 5.6.7, 01-567-498240-20190131

c. FortiOS 5.6.7 Log Reference, Doc No. 01-565-414447-20181127

d. FortiOS Handbook version 5.6.7, Doc No. 01-567-497911-20190219

e. Fortinet IPS Signature Syntax Guide, Doc No. 00-108-229429-20140522

[1] Blade mounted in FortiGate 5144C rack mount ATCA chassis.

f. FG-30E / FWF-30E / FG-50E / FWF-50E / FG-51E / FWF-51E. FortiGate/FortiWiFi 30E/50E/51E Information, 01-540-269598-20180112

g. FG-52E. FortiGate 52E Information, 01-540-300075-20170907

h. FG-60E / FG-60E-PoE / FWF-60E / FG-61E / FWF-61E. FortiGate 60E/61E Series Information, 01-540-367071-20180314

i. FG-60E-DSL / FWF-60E-DSL. FortiGate 60E-DSL Information, 01-560-442605-20171026

j. FG-80E / FG-81E. FortiGate 80E/81E Information, 01-543-402959-20180314

k. FG-80E-PoE / FG-81E-PoE. FortiGate 80E/81E-POE Information, 01-542-391830-20180314

l. FG-100E / FG-101E. FortiGate 100E/101E Information, 01-540-366134-20170913

m. FG-100EF. FortiGate 100EF Information, 01-543-403497-20170907

n. FG-140E / FG-140E-PoE. FortiGate 140E Series Information, 01-543-404092-20170905

o. FG-200E / FG-201E. FortiGate 200E/201E Information, 01-542-381079-20170907

p. FG-300D. FortiGate 300D Information, 01-506-238488-20170824

q. FG-400D. FortiGate 400D Information, 01-523-277788-20170824

r. FG-600D. FortiGate 600D Information, 01-523-278008-20170907

s. FG-500E / FG-501E. FortiGate 500E/501E Information, 01-560-440260-20180522

t. FG-300E / FG-301E. FortiGate 300E/301E Information, 01-560-440261-20180522

u. FG-900D. FortiGate 900D Information, 01-523-279315-20171122

v. FG-1000D. FortiGate 1000D Information, 01-503-237227-20170907

w. FG-1200D. FortiGate 1200D Information, 01-540-306494-20170907

x. FG-3000D. FortiGate 3000D Information, 01-522-266144-20170907

y. FG-3100D. FortiGate 3100D Information, 01-5011-275737-20170824

z. FG-3200D. FortiGate 3200D Information, 01-522-256537-20170824

aa. FG-500D. FortiGate 500D Information, 01-523-278008-20170815

bb. FG-1500D. FortiGate 1500D Information, 01-523-211767-20170907

cc. FG-3700D. FortiGate 3700D Information, 01-540-292415-20171013-M

dd. FG-3800D. FortiGate 3800D Information, 01-540-292415-20170901-M

ee. FG-3810D. FortiGate 3810D Information, 01-522-261444-20170901-M

ff. FG-3815D. FortiGate 3815D Information, 01-540-292419-20170901-M

gg. FG-5001D. FortiGate-5001D Security System Guide, 01-560-0242101-20170728

hh. FG-2000E / FG-2500E. FortiGate 2000E/2500E Information, 01-540-306896-20170907

ii. FG-3960E / FG-3980E. FortiGate 3960E/3980E Information, 01-540-376285-20180423

jj. FG-5001E. FortiGate-5001E Security System Guide, 01-560-410512-201700905

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 (SFRs). 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 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 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 activity was 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 testing 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.

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 this 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 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 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.

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
CCEF	Common Criteria Evaluation Facility
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
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 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Security Target for Fortinet FortiGate v5.6.7, v1.3, 17/05/2019
Evaluation Technical Report for Fortinet FortiGate v5.6.7, v1.2, 22/05/2019