Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Fortinet FortiGate 6000 Series w/ FortiOS 5.6

Fortinet, Inc.

29 July 2020

383-4-491

V1.0

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 evaluation facility established under the Canadian Centre for Cyber Security (CCCS). 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 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 department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Contact Centre and Information Services
Edward Drake Building
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

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 Canadian Centre for Cyber Security.

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, 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 listed on the Certified Products list (CPL) for the Canadian CC Scheme and posted on the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Fortinet FortiGate 6000 Series w/ FortiOS 5.6 (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 Table 1 for the evaluated security functionality.

Lightship Security is the CCEF that conducted the evaluation. This evaluation was completed on 29 July 2020 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.

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 CC Scheme 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 6000 Series w/ FortiOS 5.6
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 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

The TOE claims the following conformance;

- collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 2.0 + Errata 20180314;
- Network Device collaborative Protection Profile Extended Package - VPN Gateway (VPN_EP), Version 2.1; and
- collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package for Intrusion Prevention Systems (IPS_EP), Version 2.11

1.2 TOE DESCRIPTION

The TOE is a firewall that includes Virtual Private Network (VPN) and Intrusion Prevention System (IPS) capabilities. Industry terms for this TOE type include Next-Generation Firewall (NGFW) and Unified Threat Management (UTM)

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

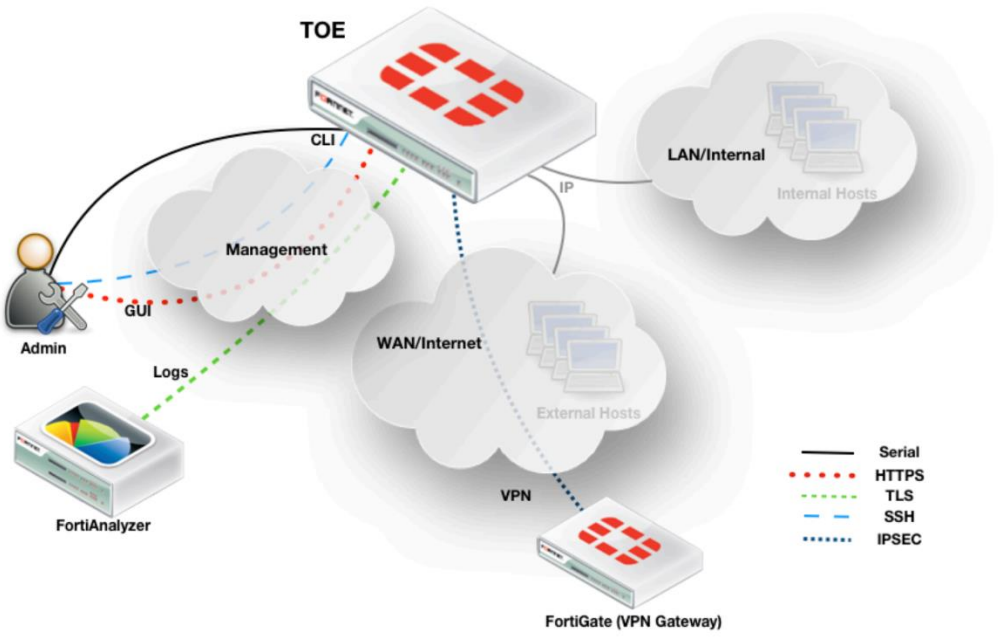

Figure 1: TOE Architecture

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
- 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 and are used by the TOE:

Table 2: Cryptographic Implementation(s)

Implementation	Certificate Number
Fortinet FortiOS SSL 6K series Cryptographic Library v5.6	C644
Fortinet FortiOS RBG 6K series Cryptographic Library v5.6	C613
Fortinet FortiOS FIPS 6K series Cryptographic Library v5.6	C599
Fortinet CP9 Cryptographic Library v5.6	C531

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 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 physicalinterconnections 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.
- 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.

3.2 CLARIFICATION OF SCOPE

The TOE incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

The FortiGate appliances are capable of a variety of functions and configurations which are not covered by the FWcPP and associated Eps(Extended packages). As such, the following features have not been examined as part 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) Use of NTP
o) Use of FortiCloud

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

The TOE firmware (**FortiOS 5.6 Version 5.6.6 Build 4265**) running on the following hardware platforms;

- FG-6300F
- FG-6301F
- FG-6500F
- FG-6501F

With support from the operating environment for;

- Audit server (Fortianalyzer)
- IPsec VPN endpoints
- CRL web server

4.1 DOCUMENTATION

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

a) FortiOS 5.6 and FortiGate NGFW Appliances FIPS 140-2 and Common Criteria Technote, 01-567-535352-20190122, July 14, 2020
b) FortiOS Handbook - CLI Reference version 5.6.10, 01-5610-498240-20190729
c) FortiOS Log Reference Version 5.6.8, Doc No. 01-568-414447-20190131
d) FortiOS Handbook version 5.6.11, Doc No. 01-5611-497911-20190820
e) Custom IPS and Application Control Signature - Syntax Guide, Version 3.6, 43-360-453749-20200225
f) FortiOS Handbook – FortiGate-6000, Version 5.6.7, 01-567-465651-20190416
g) FortiGate-6000F System Guide, 01-545-464766-2018052

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

b. Cryptographic Implementation Verification: The evaluators verified that the cryptographic implementation claimed is present in and used by the TOE.

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

The following sources of public vulnerabilities were considered in formulating the specific list of flaws to be investigated by the evaluators. Hypothesis sources for public vulnerabilities were:

- Fortinet security advisories (https://fortiguard.com/psirt)
- NIST National Vulnerabilities Database (can be used to access CVE and USCERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ ;https://www.cvedetails.com/vulnerability-search.php
- Community (Symantec) security community: https://www.securityfocus.com/
- US-CERT: http://www.kb.cert.org/vuls/html/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
- Google

Type 1 Hypothesis searches were conducted on July 6, 2020 and included the following search terms:

- Fortinet;
- FortiGate;
- FortiOS;
- Firewall;
- VPN Gateway;
- Intrusion Detection System;
- TCP
- TLS;
- IPSec;
- SSH;
- Linux Kernel;
- OpenSSL;
- OpenSSH;
- Apache;

There are no type 2 hypotheses identified for the NDcPP. The evaluation team developed Type 3 & 4 flaw hypotheses in accordance with Sections A.1.3, A.1.4, and A.2. The independent penetration testing did not uncover any residual 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 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 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.

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 CCCS or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CCCS 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.

This product is a complex UTM. Administrators are expected to be competent and trained in the concepts demanded by this product. Administrators are expected to understand X.509 certificates (and associated PKI requirements) and understand the security of those components. The custom IPS syntax should be properly tested before deploying. It is possible that administrators could benefit from product-specific training

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
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 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Security Target Fortinet FortiGate 6000 w/ FortiOS 5.6, 28 July 2020, v1.3
Evaluation Technical Report Fortinet FortiGate 6000 w/ FortiOS 5.6, 29 July 2020, v1.4
Assurance Activity Report Fortinet FortiGate 6000 w/ FortiOS 5.6, 29 July 2020, v1.5