Certification Report

EAL 4+ Evaluation of Fortinet FortiGate™ Unified Threat Management Solutions and FortiOS 4.0™ CC Compliant Firmware

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-133-CR
Version: 1.0
Date: 23 January 2012
Pagination: i to iii, 1 to 15

DISCLAIMER

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 Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply 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 CCS, 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 Canada, 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 Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) 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 CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS 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*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS 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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 23 January 2012, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks:

- FortiGate™ and FortiOS™ are trademarks of Fortinet, Incorporated.

TABLE OF CONTENTS

Executive Summary

Fortinet FortiGate™ Unified Threat Management Solutions and FortiOS 4.0™ CC Compliant Firmware (hereafter referred to as FortiGate 4.0), from Fortinet, Incorporated, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

FortiGate 4.0 is a family of stand-alone firewall appliances that reside between the network they are protecting and an external network such as the Internet, restricting the information flow between the networks to that permitted by a policy defined by an authorized administrator. FortiGate 4.0 implements firewall, web filtering, VPN[1], antivirus and intrusion detection/prevention functionality. FortiGate 4.0 supports secure remote administration using FIPS 140-2 validated cryptography.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 9 December 2011 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for FortiGate 4.0, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security 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 results documented in the Evaluation Technical Report (ETR)[2] for this product provide sufficient evidence that it meets the EAL 4 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.3 – Systematic Flaw Remediation.

FortiGate 4.0 is conformant with the *U.S. Government Protection Profile Intrusion Detection System Sensor For Basic Robustness Environments, Version 1.3, July 25, 2007*, the *U.S. Government Protection Profile for Application level Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007*, and the *U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007*.

[1] Virtual Private Network

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the FortiGate 4.0 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Fortinet FortiGate™ Unified Threat Management Solutions and FortiOS 4.0™ CC Compliant Firmware (hereafter referred to as FortiGate 4.0), from Fortinet, Incorporated.

2 TOE Description

FortiGate 4.0 is a family of stand-alone firewall appliances that reside between the network they are protecting and an external network such as the Internet, restricting the information flow between the networks to that permitted by a policy defined by an authorized administrator. FortiGate 4.0 implements firewall, web filtering, VPN, antivirus and intrusion detection/prevention functionality. FortiGate 4.0 supports secure remote administration using FIPS 140-2 validated cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for FortiGate 4.0 is identified in Sections 5 and 6 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
FortiGate-50B	*Pending* [3]
FortiGate-60C	*Pending*
FortiGate-80C	*Pending*
FortiGate-110C	*Pending*
FortiGate-200B	*Pending*
FortiGate-310B	*Pending*
FortiGate-311B	*Pending*
FortiGate-620B	*Pending*

[3] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

Cryptographic Module	**Certificate #**
FortiGate-1000A	*Pending*
FortiGate-1240B	*Pending*
FortiGate-3016B	*Pending*
FortiGate-3040B	*Pending*
FortiGate-3140B	*Pending*
FortiGate-3950B	*Pending*
FortiGate-3951B	*Pending*
FortiGate-5001SX	*Pending*
FortiGate-5001A-DW	*Pending*
FortiGate-5001A-SW	*Pending*
FortiGate-5001B	*Pending*
FortiWiFi-50B	*Pending*
FortiWiFi-60C	*Pending*
FortiWifi-80CM	*Pending*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in FortiGate 4.0:

Cryptographic Algorithm	**Standard**
Advanced Encryption Standard (AES) Remote Administration	FIPS 140-2 (Level 1)
Advanced Encryption Standard (AES) Encryption and decryption of VPN	FIPS PUB 197 (AES) and National Institute of Standards and Technology (NIST) SP 800-67 (TDEA)
RSA Digital Signature Algorithm (rDSA)	ANSI X9.31-1998
Secure Hash Algorithm (SHA-1) and HMAC	FIPS 140-2 PUB 180-2, and FIPS 140-2 PUB 198
ANSI X9.31 Appendix A Random Number Generation	ANSI X9.31

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Security Target for Fortinet FortiGate™ 50B, 60C, 80C, 110C, 200B, 310B, 311B, 620B, 1000A, 1240B, 3016B, 3040B, 3140B, 3950B, 3951B, 5001SX, 5001A-DW, 5001A-SW, 5001B and FortiWiFi-50B, 60C and 80CM Unified Threat Management Solutions and FortiOS 4.0 CC Compliant Firmware
Version: 2.1
Date: 6 December 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

FortiGate 4.0 is:

a. *Common Criteria Part 2 extended,* with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - FAV_ACT_EXT.1 - Anti Virus Actions;
   - IDS_COL_EXT.1 - Sensor data collection;
   - IDS_RDR_EXT.1 - Restricted data review;
   - IDS_STG_EXT.1 - Guarantee of sensor data availability; and
   - IDS_STG_EXT.2 - Prevention of sensor data loss.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

c. *Common Criteria EAL 4 augmented,* containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation.

d. FortiGate 4.0 is conformant with the *U.S. Government Protection Profile Intrusion Detection System Sensor For Basic Robustness Environments, Version 1.3, July 25, 2007*, the *U.S. Government Protection Profile for Application level Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007*, and the *U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007.*

6 Security Policies

FortiGate 4.0 implements firewall policies that determine the traffic that is allowed to flow through the FortiGate 4.0. In addition, FortiGate 4.0 implements policies pertaining to security audit, encryption, identification and authentication, security management, trusted channel/path, protection of the TOE, IDS[4], and antivirus. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of FortiGate 4.0 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

a. Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE;

b. There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains;

c. Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error;

d. Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks;

e. The TOE can only be accessed by authorized users; and

f. Authorized administrators may access the TOE from the internal and external networks.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE;

[4] Intrusion Detection System

b. The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access unauthorized physical modification;

c. The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low;

d. The TOE is physically secure;

e. The TOE does not host public data;

f. Information cannot flow among the internal and external networks unless it passes through the TOE;

g. Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks;

h. Authorized administrators may access the TOE remotely from the internal and external networks; and

i. The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

7.3 Clarification of Scope

FortiGate 4.0 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. FortiGate 4.0 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for FortiGate 4.0 comprises:

Product	Firmware Version	Hardware Version
FortiGate-50B	Build 8892,111128	C5GB38
FortiGate-60C	Build 8892,111128	C4DM93
FortiGate-80C	Build 8892,111128	C4BC61
FortiGate-110C	Build 8892,111128	C4HA15
FortiGate-200B	Build 8892,111128	C4CD24
FortiGate-310B	Build 8892,111128	C4ZF35
FortiGate-311B	Build 8892,111128	C4CI39
FortiGate-620B	Build 8892,111128	C4AK26
FortiGate-1000A	Build 8892,111128	C4WA49
FortiGate-1240B	Build 8892,111128	C4CN43
FortiGate-3016B	Build 8892,111128	C4XA14
FortiGate-3040B	Build 8892,111128	C4CX55 (AC) C4JH55 (DC)
FortiGate-3140B	Build 8892,111128	C4CX55
FortiGate-3950B	Build 8892,111128	C4DE23
FortiGate-3951B	Build 8892,111128	C4EL37
FortiGate-5001SX	Build 8892,111128	P4CF76
FortiGate-5001A-DW	Build 8892,111128	P4CJ36
FortiGate-5001A-SW	Build 8892,111128	P4CJ36
FortiGate-5001B	Build 8892,111128	P4EV74
FortiWiFi-50B	Build 8892,111128	C5WF27

Product	Firmware Version	Hardware Version
FortiWiFi-60C	Build 8892,111128	C4DM95
FortiWifi-80CM	Build 8892,111128	C4BD62

The products listed are collectively termed the FortiGate Series or FortiGate Family of Unified Threat Management (UTM) Solutions.

The document entitled *FortiOS Handbook v3 for FortiOS 4.0 MR3, Chapter 20 Certifications and Compliances* describes installing FortiGate 4.0 in its FIPS-CC evaluated configuration.

9 Documentation

The Fortinet documents provided to the consumer are as follows:

FortiGate-50B QuickStart Guide 01-30003-0361-20070419
FortiGate-60C QuickStart Guide 01-420-002122-20110128
FortiGate-80C QuickStart Guide 01-412-89805-20090615
FortiGate-110C QuickStart Guide 01-412-0468-20101119
FortiGate-200B QuickStart Guide 01-420-110056-20090910
FortiGate-310B QuickStart Guide 01-412-112401-20091020
FortiGate-311B QuickStart Guide 01-30007-97512-20090525
FortiGate-620B QuickStart Guide 01-420-112406-20110126
FortiGate-1000A/FA2 QuickStart Guide 01-30007-114859-20091203
FortiGate-1240B QuickStart Guide 01-30007-106971-20091117
FortiGate-3016B QuickStart Guide 01-30006-0402-20080328
FortiGate-3040B QuickStart Guide 01-413-125361-20101210
FortiGate-3140B QuickStart Guide 01-420-129377-20101210
FortiGate-3950B QuickStart Guide 01-413-124384-20100404

FortiGate-3951B QuickStart Guide 01-413-119330-20100210
FortiGate-5001SX Security System Guide 01-30000-0380-20070201
FortiGate-5001A Security System Guide 01-30000-83456-20081023 (applies to both 5001A-DW and 5001A-SW)
FortiGate-5001B Security System Guide 01-400-134818-20110118
FortiGate-WIFI-50B QuickStart Guide 01-30005-0399-20070830
FortiGate- WIFI-60C QuickStart Guide 19-420-002122-20110128
FortiGate- WIFI-80CM QuickStart Guide 01-412-89807-20090615
FortiGate Desktop Install Guide 01-400-95522-20090501
FortiGate 1U Install Guide 01-400-95523-20090501
FortiGate 2U Install Guide 01-400-95524-20090501
The FortiOS Handbook – The Complete Guide for FortiOS 4.0 MR3 01-430-99686-20110311
FortiGate 4.0 CLI Reference Guide, 01- 430-99686-20110318
FortiGate 4.0 MR3 HA Guide, 01-431-99686-20110623

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of FortiGate 4.0, including the following areas:

Development: The evaluators analyzed the FortiGate 4.0 functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TSF interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the FortiGate 4.0 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the FortiGate 4.0 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.

Life-cycle support: An analysis of the FortiGate 4.0 configuration management system and associated documentation was performed. The evaluators found that the FortiGate 4.0 configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorized access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of FortiGate 4.0 during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the FortiGate 4.0 design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Fortinet, Incorporated for FortiGate 4.0. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of FortiGate 4.0. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the FortiGate 4.0 in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 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[5].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of EWA-Canada test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Check FIPS-CC mode initial configuration. The purpose of this test case is to check the TOE's initial security configurations in FIPS-CC mode;

c. Backup and restore configuration using local USB interfaces. The purpose of this test case is to verify the TOE's configuration can be backed up to and restored from a USB drive through the TOE's local USB interfaces; and

d. Unauthorized admin user cannot access log data – CLI interface. The purpose of this test case is to verify an unauthorized admin user cannot access log data through CLI interface.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Port Scan. The purpose of this test case is to identify all open ports on the TOE;

[5] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

b. Information Leak. The purpose of this test is to see if the TOE is leaking any information that might be useful to an attacker;

c. Communications failure. This test verifies that the TOE can recover from a communications failure and operate as expected;

d. Session Management - Concurrent Admin Sessions. The purpose of this test is to ensure concurrent administrative sessions can be coordinated by the TOE;

e. Bypass – Session Management. This test verifies that once an administrative session has been closed it can't be reopened without first performing a login; and

f. Tampering – SQL Injection. The purpose of this test case is to try and bypass the normal authentication mechanism by injecting parameters.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

FortiGate 4.0 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that FortiGate 4.0 behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4 + level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The complete documentation for the FortiGate 4.0 includes a comprehensive Installation and Security Guide and a Users Guide. FortiGate 4.0 is straightforward to configure, use and integrate into a corporate network.

14 Acronyms, Abbreviations and Initializations

CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NIST	National Institute of Standards and Technology
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. U.S. Government Protection Profile Intrusion Detection System Sensor For Basic Robustness Environments, Version 1.3, July 25, 2007.

e. U.S. Government Protection Profile for Application level Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007.

f. U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007.

g. Security Target for Fortinet FortiGate™ 50B, 60C, 80C, 110C, 200B, 310B, 311B, 620B, 1000A, 1240B, 3016B, 3040B, 3140B, 3950B, 3951B, 5001SX, 5001A-DW, 5001A-SW, 5001B and FortiWiFi-50B, 60C and 80CM Unified Threat Management Solutions and FortiOS 4.0 CC Compliant Firmware, v2.1, 6 December 2011.

h. Evaluation Technical Report (ETR) Fortinet FortiGate™ 50B, 60C, 80C, 110C, 200B, 310B, 311B, 620B, 1000A, 1240B, 3016B, 3040B, 3140B, 3950B, 3951B, 5001SX, 5001A-DW, 5001A-SW, 5001B and FortiWiFi-50B, 60C and 80CM Unified Threat Management Solutions and FortiOS 4, EAL 4+ Evaluation, Common Criteria Evaluation Number: 383-4-133, Document No. 1660-000-D002, Version 1.1, 9 December 2011.