Certification Report

EAL 4+ Evaluation of Fortinet FortiGate™-200B and 620B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-184-CR
Version: 1.1
Date: 2 March 2011
Pagination: i to iii, 1 to 9

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, 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, Ontario.

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 2 March 2011, 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 registered trademark:

- FortiGate™ is a registered trademark of Fortinet, Incorporated.

TABLE OF CONTENTS

Executive Summary

Fortinet FortiGate™-200B and 620B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware (hereafter referred to as FortiGate™-200B and 620B), from Fortinet, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

FortiGate™-200B and 620B are stand-alone firewall appliances that implement stateful traffic filtering[1]. The appliances support secure local and remote administration using FIPS 140-2 validated cryptography.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 24 February 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 the FortiGate™-200B and 620B, 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.2 – Flaw Reporting procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the FortiGate™-200B and 620B 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] Only packets matching a known active connection will be allowed by the firewall; others will be rejected.

[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.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Fortinet FortiGate™-200B and 620B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware (hereafter referred to as FortiGate™-200B and 620B), from Fortinet, Incorporated.

2 TOE Description

FortiGate™-200B and 620B are stand-alone firewall appliances that implement stateful traffic filtering[3]. The appliances support secure local and remote administration using FIPS 140-2 validated cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the FortiGate™-200B and 620B is identified in Sections 5 & 6 of the Security Target (ST).

The following cryptographic module was evaluated to the FIPS 140-2 standard: FortiOS #1431.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in FortiGate™-200B and 620B:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	957, 962
Advanced Encryption Standard (AES)	FIPS 197	1404, 1409
Rivest Shamir Adleman (RSA)	FIPS 186-2	686
Secure Hash Standard (SHA-1)	FIPS 180-2	1274, 1279
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	825, 830
Random Number Generation (RNG)	FIPS 140-2	770

[3] Only packets matching a known active connection will be allowed by the firewall; others will be rejected.

4 Security Target

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

Title: Security Target for the Fortinet FortiGate™- 200B and 620B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware: EAL4+
Version: Version 1.0
Date: 18 February 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™-200B and 620B is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
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.2 - Flaw Reporting procedures.

6 Security Policy

FortiGate™-200B and 620B implements a stateful traffic filtering flow control policy. The default policy is restrictive, that is, until rules are configured by an administrator, no traffic can flow through the TOE.

In addition, FortiGate™-200B and 620B implements other policies pertaining to security audit, user data protection, identification and authentication, security management, and encryption. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions

Consumers of FortiGate™-200B and 620B 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 Assumption is listed in the ST:

- Authorized administrators are non-hostile and follow all administrator guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is physically secure;
- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE;
- The TOE does not host public data;
- Information can not flow among the internal and external networks unless it passes through the TOE; and
- Authorized administrators may access the TOE remotely from the internal and external networks.

8 Evaluated Configuration

The evaluated configuration for FortiGate™-200B and 620B includes:

Product	FortiOS Version	Hardware Version	Crypto Module
FortiGate-200B	FortiOS 4.0 build 6443, 110212	C4CD24	FortiOS #1431
FortiGate-620B	FortiOS 4.0 build 6443, 110212	C4AK26	FortiOS #1431

Documentation for the FortiGate-200B and 620B operated in Common Criteria mode consists of the standard FortiOS version 4.0 documentation set with the FIPS-CC-specific technical note.

9 Documentation

The Fortinet documents provided to the consumer are as follows:

- FortiGate Version 4.0 MR2 Administration Guide, 01-420-89802-20100326, 26 March 2010;
- FortiOS CLI Reference, 01-420-99686-20100811, 11 August 2010;
- FortiOS Handbook v2 for FortiOS 4.0 MR2, 01-420-99686-20101026, 26 October 2010;
- FortiGate 2U Install Guide, 01-400-95524-20090501, 1 May 2009;

- FortiGate Log Message Reference, 01-420-112804-20100824, 24 July 2010;
- FortiGate-200B Quickstart Guide, 01-420-110056-20090910, 10 September 2009; and
- FortiGate--620B Quickstart Guide, 01-420-112406-20091020, 20 October 2009.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the FortiGate™-200B and 620B, including the following areas:

Development: The evaluators analyzed the FortiGate™-200B and 620B functional specification, design documentation, and a subset of the implementation representation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the FortiGate™-200B and 620B security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the FortiGate™-200B and 620B preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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™-200B and 620B configuration management system and associated documentation was performed. The evaluators found that the FortiGate™-200B and 620B 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 unauthorised 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™-200B and 620B 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™-200B and 620B 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 for FortiGate™-200B and 620B. 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™-200B and 620B. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the FortiGate™-200B and 620B 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[4].

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 evaluators 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.

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

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 was the following list of EWA-Canada test goals:

a. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator's TOE installation; and

c. FIP-CC mode Testing: The objective of this test goal is to confirm FIPS-CC mode configuration.

11.3 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 tests focused on port scanning, communications failure, concurrent administrator logins, communications security, and secure session establishment.

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

11.4 Conduct of Testing

FortiGate™-200B and 620B 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 Procedures and Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the FortiGate™-200B and 620B 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™-200B and 620B includes comprehensive Evaluation, Installation, and Users Guides.

The developer has an extensive and robust test suite capable of insuring a proper working product.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
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
PALCAN	Program for the Accreditation of Laboratories Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

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 3.1R3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1R3, July 2009.

d. Security Target for the Fortinet FortiGate™- 200B and 620B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware: EAL4+, Version Version 1.0, 18 February 2011.

e. Evaluation Technical Report (ETR) for EAL3+ Common Criteria Evaluation of Fortinet FortiGate™-200B and 620B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware , Document No. 1708-000-D002, Version 1.3, 24 February 2011, Common Criteria Evaluation Number: 383-4-184.