



Certification Report

**EAL 4+ Evaluation of Fortinet FortiGate™ -50B, 200A,
300A, 310B, 500A, 800, 1000A, 3016B, 3600, 3600A,
3810A-E4, 5001SX, 5001FA2, 5001A-DW and FortiWiFi-
50B Unified Threat Management Solutions and FortiOS™
3.0 CC Compliant Firmware**

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© 2008 Government of Canada, Communications Security Establishment Canada

Document number: 383-4-51-CR
Version: 1.1
Date: 28 November 2008
Pagination: i to iv, 1 to 12



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 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. 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 Standard 17025, General requirements for the accreditation of calibration and testing 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 28 November 2008, 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 at: <http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html> and <http://www.commoncriteria.es/>

This certification report makes reference to the following trademarked names:

- FortiGate™ which is a trademark of Fortinet Incorporated.
- FortiOS™ which is a trademark of Fortinet Incorporated.
- FortiASIC™ which is a trademark of Fortinet Incorporated.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Disclaimer	i
Foreword.....	ii
Executive Summary	1
1 Identification of Target of Evaluation	2
2 TOE Description	2
3 Evaluated Security Functionality	3
4 Security Target.....	4
5 Common Criteria Conformance.....	4
6 Security Policy.....	5
7 Assumptions and Clarification of Scope.....	5
7.1 SECURE USAGE ASSUMPTIONS.....	6
7.2 ENVIRONMENTAL ASSUMPTIONS	6
7.3 CLARIFICATION OF SCOPE.....	6
8 Architectural Information	6
9 Evaluated Configuration.....	7
10 Documentation	7
11 Evaluation Analysis Activities	8
12 ITS Product Testing.....	9
12.1 ASSESSING DEVELOPER TESTS.....	9
12.2 INDEPENDENT FUNCTIONAL TESTING	9
12.3 INDEPENDENT PENETRATION TESTING.....	10
12.4 CONDUCT OF TESTING	11
12.5 TESTING RESULTS.....	11
13 Results of the Evaluation.....	11
14 Evaluator Comments, Observations and Recommendations	11
15 Acronyms, Abbreviations and Initializations.....	11

16 References..... **12**

Executive Summary

FortiGate™-50B, 200A, 300A, 310B, 500A, 800, 1000A, 3016B, 3600, 3600A, 3810A-E4, 5001SX, 5001FA2, 5001A-DW and FortiWiFi-50B Unified Threat Management Solutions and FortiOS™ 3.0 CC Compliant Firmware (hereafter referred to as FortiGate), from Fortinet Incorporated, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

FortiGate secures a wide range of network environments, from the remote office and branch office to the enterprise and the service provider. FortiGate detects and eliminates damaging, content-based threats from email and Web traffic such as viruses, worms, intrusion attempts, and inappropriate Web content in real-time without degrading network performance. FortiGate units can operate independently, as part of a cluster to provide high availability of services, or collectively with a centralized management system to provide multiple security enforcement points within large networks.

FortiGate units support the IPSec industry standard for Virtual Private Networks (VPN), allowing VPNs to be configured between a FortiGate unit and any compatible Internet Protocol Security (IPSec) VPN client, gateway, or firewall. FortiGate also provide Secure Sockets Layer (SSL) VPN gateway and tunneling services.

Firewall, IPSec VPN, antivirus, and intrusion prevention functionality are included in this evaluation; antispam, Web filtering, traffic shaping, SSL VPN and centralized management capabilities are excluded. Section 2 of the security target provides details on functionality included, and excluded, from this evaluation.

FortiGate incorporates FIPS PUB 140-2 validated cryptography.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 17 November 2008 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, 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)¹ 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 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. The following augmentation is claimed: ALC_FLR.3 – Systematic flaw remediation.

FortiGate is conformant with the Intrusion Detection System Sensor Protection Profile (IDSS PP) Version 1.2, April 27, 2005.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the FortiGate 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 FortiGate™-50B, 200A, 300A, 310B, 500A, 800, 1000A, 3016B, 3600, 3600A, 3810A-E4, 5001SX, 5001FA2, 5001A-DW and FortiWiFi-50B Unified Threats Management Solutions and FortiOS™ 3.0 CC Compliant Firmware (hereafter referred to as FortiGate), from Fortinet Incorporated.

2 TOE Description

FortiGate secures a wide range of network environments, from the remote office and branch office (ROBO) to the enterprise and the service provider. FortiGate detects and eliminates damaging, content-based threats from email and Web traffic such as viruses, worms, intrusion attempts, and inappropriate Web content in real-time without degrading network performance. FortiGate units can operate independently, as part of a cluster to provide high availability of services, or collectively with a centralized management system to provide multiple security enforcement points within large networks.

FortiGate units support the IPSec industry standard for Virtual Private Networks (VPN), allowing VPNs to be configured between a FortiGate unit and any compatible Internet Protocol Security (IPSec) VPN client, gateway, or firewall. FortiGate also provides Secure Sockets Layer (SSL) VPN gateway and tunneling services.

¹ The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Firewall, IPSec VPN, antivirus, and intrusion prevention functionality are included in this evaluation; antispam, Web filtering, traffic shaping, SSL VPN and centralized management capabilities are excluded. Section 2 of the security target provides details on functionality included, and excluded, from this evaluation.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the FortiGate is identified in Section 5 of the Security Target.

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

Cryptographic Module	Certificate #
FG-50B	945
FG-200A	807, 905
FG-300A	807, 905
FG-310B	1114
FG-500A	807, 905
FG-800	905
FG-1000A	810
FG-3016B	1098
FG-3600	810
FG-3600A	1098
FG-3810A-E4	1098
FG-5001SX	789
FG-5001FA2	789
FG-5001A-DW	1126
FortiWiFi-50B	1095

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

Cryptographic Algorithm	Standard	Certificate #
Triple-DES (3DES)	FIPS 46-3	486, 487, 489, 490, 582, 583, 584
Advanced Encryption Standard (AES)	FIPS 197	471, 472, 475, 476, 612, 613, 614
Rivest Shamir Adleman (RSA)	FIPS 186-2	193, 284, 285
Secure Hash Algorithm (SHA-1)	FIPS 180-2	539, 540, 543, 544, 660, 661, 662
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	228, 229, 232, 233, 315, 316, 317

4 Security Target

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

Title: Security Target for the FortiGate™-50B, 200A, 300A, 310B, 500A, 800, 1000A, 3016B, 3600, 3600A, 3810A-E4, 5001SX, 5001FA2, 5001A-DW and FortiWiFi-50B Unified Threat Management Solutions and FortiOS™ 3.0 CC Compliant Firmware: EAL 4+

Version: 0.25

Date: 17 November 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

FortiGate 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:
 - FAU_ARP_ACK_EXP.1 – Security Alarm Acknowledgement;

- FAV_ACT_EXP.1 – Anti Virus Actions;
 - FCS_BCM_EXP.1 – Baseline Cryptographic Module;
 - FIP_ACT_EXP.1 – Intrusion Prevention Actions;
 - IDS_COL_EXP.1 – Sensor Data Collection;
 - IDS_RDR_EXP.1 – Restricted Data Review;
 - IDS_STG_EXP.1 – Guarantee of Sensor Data Availability; and
 - IDS_STG_EXP.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 ALC_FLR.3 - Systematic flaw remediation.

6 Security Policy

The FortiGate implements four information flow control policies. These policies govern the following:

- unauthenticated information flow between the protected network and the external network;
- authenticated information flow between the protected network and the external network;
- access of unauthenticated users to services provided by the TOE; and
- establishment of a virtual private network between the TOE and an authenticated external entity.

A high level description of these security policies is found in Section 2 of the ST; a detailed description is found in Sections 5 and 6 of the ST.

In addition, FortiGate implements policies pertaining to security audit, self protection, identification and authentication, security administration, encryption and the use of trusted paths and channels. A high level description of these security policies is found in Section 2 of the ST; a detailed description is found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of FortiGate 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:

- Competent individuals are assigned to manage the TOE and these individuals are not careless, willfully negligent or hostile and will follow the instructions provided in the TOE documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be located in controlled access facilities thereby preventing unauthorized physical access to the TOE.
- The network which the TOE is intended to protect will be configured such that all information passing between the network and an external network must pass through the TOE.

For more information about the TOE security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

The FortiGate units provide a wide variety of services, not all of which were subject to evaluation. In particular, the following capabilities were excluded from the evaluation:

- dynamic routing;
- update of the FortiOS™ firmware;
- update of the FortiGate Anti-Virus and Intrusion Prevention System engines;
- spam filtering;
- traffic shaping; and
- web content filtering.

For a complete list of the capabilities both included and excluded from the evaluation, refer to Section 2 of the ST.

8 Architectural Information

FortiGate units comprise hardware and firmware components.

The FortiGate hardware comprises the processor, memory, the FortiASIC™ and the input/output (I/O) interfaces. The FortiASIC™ performs security and content processing. Different FortiGate models have different I/O capabilities. Refer to Section 2 of the ST for interface detail.

The FortiGate firmware comprises the custom FortiOS™ operating system.

Further details about the system architecture are proprietary to the developer, and are not provided in this report.

9 Evaluated Configuration

The FortiGate Security Target includes the following evaluated configurations of the TOE:

- FG-50B;
- FG-200A;
- FG-300A;
- FG-310B;
- FG-500A;
- FG-800;
- FG-1000A;
- FG-3016B;
- FG-3600;
- FG-3600A;
- FG-3810A-E4;
- FG-5001SX;
- FG-5001FA2;
- FG-5001A-DW; and
- FortiWiFi-50B.

Each of these units may be used either as a stand alone unit or along with other units of the same model in a high availability cluster.

10 Documentation

Fortinet documents provided to the consumer are as follows:

- a. FortiGate Installation Guide (one document available for each FortiGate model type);

- b. FortiGate Administration Guide, v3.0 MR4, 2 January 2007;
- c. FortiGate CLI Reference, v3.0, MR4, 1 March 2007;
- d. FortiGate HA Guide, FortiOS v3.0 MR3, 20 October 2006;
- e. FortiGate IPSec VPN User Guide, v3.0, MR5, 16 July 2007;
- f. FortiGate IPS User Guide, v3.0, MR4, 10 January 2007;
- g. FortiGate User Authentication User Guide, v3.0 MR4, 1 March 2007; and
- h. FortiGate FIPS-Common Criteria Compliant Operation Technical Note, FortiOS v3.0 MR4, 10 July 2008.

11 Evaluation Analysis Activities

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

Configuration management: An analysis of the FortiGate configuration management system and associated documentation was performed. The evaluators found that the FortiGate configuration items were clearly marked, and could be modified and controlled, and that the configuration management system supported generation of the TOE. The developer's configuration management system was observed during site visits, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of FortiGate during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the FortiGate functional specification, high-level design, low-level design, and a subset of the implementation representation; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the FortiGate user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators examined the development security procedures during site visits and determined that they detailed sufficient security measures for the development

environment to protect the confidentiality and integrity of FortiGate 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 the FortiGate. The evaluators determined that the procedures describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to product users. Additionally, the evaluators determined that the developer's procedures provide for the corrections of security flaws, for the receipt of flaw reports from product users, and for assurance that the corrections introduce no new security flaws.

Vulnerability assessment: The FortiGate ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for FortiGate and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

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

12.1 Assessing 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 ETR².

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation,

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.

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 was 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. Administration: The objective of this test goal is to confirm that FortiGate can be administered in a secure manner;
- c. Audit: The objective of this test goal is to confirm that the FortiGate audit functions meets the audit requirements listed in the ST;
- d. Firewall Services: The objective of this test goal is to confirm that FortiGate provides firewall policies that conform with the information flow control policies stated in the ST;
- e. Anti-virus Services: The objective of this test goal is to confirm that FortiGate provides anti-virus services as described by the explicit requirement listed in the security target;
- f. Intrusion Detection Services: The objective of this test goal is to confirm that the FortiGate detects attempted intrusion in accordance with the requirements listed in the claimed PP;
- g. Intrusion Prevention Services: The objective of this test goal is to confirm that the FortiGate prevents intrusions as described by the explicit requirement listed in the security target; and
- h. High Availability Services: The objective of this test goal is to confirm that a FortiGate cluster satisfies the high availability requirements described in the ST.

12.3 Independent Penetration Testing

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

- Generic vulnerabilities;
- Direct attacks; and
- Misuse.

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

12.4 Conduct of Testing

FortiGate 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.

12.5 Testing Results

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

13 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.

14 Evaluator Comments, Observations and Recommendations

Fortinet employs a rigorous testing process that tests the changes and fixes in each release of the FortiGate. Comprehensive regression testing is conducted for all releases.

15 Acronyms, Abbreviations and Initializations

<u>Acronym/Abbreviation/</u> <u>Initialization</u>	<u>Description</u>
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I/O	Input/Output
IPSec	Internet Protocol Security
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NIST	National Institute of Standards and

<u>Acronym/Abbreviation/ Initialization</u>	<u>Description</u>
PALCAN	Technology Program for the Accreditation of Laboratories Canada
SANS	SysAdmin, Audit, Network, Security
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network

16 References

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

- a. CCS Publication #4, Technical Oversight, Version 1.0.
- b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.
- c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.
- d. Security Target for the Fortinet FortiGate™-50B, 200A, 300A, 310B, 500A, 800, 1000A, 3016B, 3600, 3600A, 3810A-E4, 5001SX, 5001FA2, 5001A-DW and FortiWiFi-50B Unified Threat Management Solutions and FortiOS™ 3.0 CC Compliant Firmware: EAL 4+, Revision No. 0.25, 17 November 2008.
- e. Evaluation Technical Report (ETR) Fortinet FortiGate™-50B, 200A, 300A, 310B, 500A, 800, 1000A, 3016B, 3600, 3600A, 3810A-E4, 5001SX, 5001FA2, 5001A-DW and FortiWiFi-50B Unified Threat Management Solutions and FortiOS™ 3.0 CC Compliant Firmware, EAL 4+ Evaluation, Common Criteria Evaluation Number: 383-4-51, Document No. 1523-000-D002, Version 1.0, 17 November 2008.
- f. Intrusion Detection System Sensor Protection Profile (IDSS PP) Version 1.2, April 27, 2005.