Certification Report

EAL 2+ Evaluation of

Fortinet® FortiMail™ V3.0 MR5

Secure Messaging Platform

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-116-CR
Version: 1.0
Date: 4 June 2010
Pagination: i to iii, 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 3.1R2*, for conformance to the *Common Criteria for IT Security Evaluation, Version 3.1R2*. 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, 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 4 June 2010, 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 and the Common Criteria Portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

The FortiMail™ V3.0 MR5 Secure Messaging Platform (hereafter referred to as FortiMail™), from Fortinet®, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

FortiMail™ is a specialized email security system that provides multi-layered protection against blended threats comprised of spam, viruses, worms and malware. FortiMail™ implements a customized operating system that cleans emails through corresponding FortiMail™ antispam and antivirus engines. Its inbound filtering engine blocks spam and malware before it can clog a network and affect users. Its outbound inspection technology prevents outbound spam or malware from causing other antispam gateways to blacklist users. FortiMail™ 's dynamic and static user blocking and heuristics provides granular control over all policies and users. The high-performance threat filtering technology delivered by the FortiMail™ appliances processes and filters messages in real time.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 21 April 2010 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 FortiMail™, 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 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1R2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 3.1R2*. The following augmentation is claimed: ALC_FLR.1 - Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the FortiMail™ 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

[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.

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) 2 augmented evaluation is FortiMail™ V3.0 MR5 Secure Messaging Platform (hereafter referred to as FortiMail™), from Fortinet®.

2 TOE Description

FortiMail™ is a specialized email security system that provides multi-layered protection against blended threats comprised of spam, viruses, worms and malware. FortiMail™ implements a customized operating system that cleans emails through corresponding FortiMail™ antispam and antivirus engines. Its inbound filtering engine blocks spam and malware before it can clog a network and affect users. Its outbound inspection technology prevents outbound spam or malware from causing other antispam gateways to blacklist users. FortiMail™ 's dynamic and static user blocking and heuristics provides granular control over all policies and users. The high-performance threat filtering technology delivered by the FortiMail™ appliances processes and filters messages in real time.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the FortiMail™ is identified in Section 5 of the Security Target (ST).

As part of the CCS evaluation effort, the evaluator made use of the results generated under the Cryptographic Module Validation Program (CMVP). The cryptographic algorithms tested under the CMVP are:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES	FIPS 46-3	884
AES	FIPS 197	1231
HMAC SHA-1	FIPS 198	718
RSA	ANSI X9.31	591
RSA PKCS1	ANSI X9.31 Appendix A	591

4 Security Target

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

Title: Security Target for FortiMail™ V3.0 MR5 Secure Messaging Platform, Document Number ST0004
Version: 1.3
Date: 9 December 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1R2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1R2.*

The FortiMail™ is:

a. Common Criteria Part 2 extended, with functional requirements based on functional components in Part 2, except for the following explicitly stated requirement defined in the ST:
   - FSV_UPD_EXP.1. Antispam and Antivirus updates.
b. Common Criteria Part 3 conformant, with security assurance requirements based on assurance components in Part 3; and
c. Common Criteria EAL 2 augmented, with all the security assurance requirements in the EAL 2 package, as well as: ALC_FLR.1 – Basic flaw remediation.

6 Security Policy

The FortiMail™ implements the following four information flow control security functional policies:

- Unauthenticated Information Flow Control SFP (Security Function Policy) – describes the rules which the TOE uses when determining how to process unauthenticated email traffic;
- Authenticated Information Flow Control SFP – describes the rules which the TOE uses when determining how to process authenticated email traffic;
- Unauthenticated TOE Services SFP – describes the rules which the TOE uses to determine its response (if any) to ICMP (ping) requests; and,
- Authenticated TOE Services SFP – describes the rules which the TOE uses to process both administrative sessions (local and remote) as well as user requests for access to quarantined email.

In addition, the FortiMail™ implements policies pertaining to security audit, trusted paths and channels, user data protection, identification and authentication, security management, protection of TOE data, resource utilization, automated antispam and antivirus updates and unattended session termination. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the FortiMail™ product 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:

- One or more competent individuals are assigned to administer the TOE; and
- Administrators are not careless, willfully negligent or hostile and they follow the instructions contained within the TOE documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST.

- The TOE is located within a controlled access facility which prevents unauthorized physical access and modification; and,
- The facility in which the TOE is located provides a level of physical security which is commensurate with the value of the TOE and the data processed by the TOE.

7.3 Clarification of Scope

FortiMail™ units provide a mode of operation in which the unit acts as an email server. However the server mode of operation does not form part of the evaluated configuration of the TOE.

8 Architectural Information

The TOE consists of various appliances running FEOS, a customized version of the Linux operating system which is proprietary to Fortinet®. The TOE provides the following major functions:

- antispam and antivirus scanning;
- email content control;

- email access control;
- email quarantine;
- email archiving; and
- logging and reporting.

The hardware for each FortiMail™ appliance consists of a customized special purpose appliance. FortiMail™ models are functionally identical and differ only in their performance, disk capacity and redundancy features such as RAID and multiple power supplies.

Administration of the appliances may be performed locally using an administrative console or remotely using an encrypted connection. Both a command line interface and a web-based interface are provided for system administration.

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

9 Evaluated Configuration

The evaluated configuration of the TOE consists of the following FortiMail™ models operating in either gateway or transparent mode running the firmware FEOS v3.0 MR5 Build 529.

- FortiMail-100
- FortiMail-400
- FortiMail-400B
- FortiMail-2000A
- FortiMail-4000A

For evaluated configuration detail refer to Section 1 of the ST.

10 Documentation

The Fortinet® documents provided to the consumer are as follows:

a. FortiMail™ Secure Messaging Platform, Version 3.0 MR5 Patch 3, Install Guide, Revision 1, 25 September 2009;
b. FortiMail™ Secure Messaging Platform, Version 3.0 MR5 Patch 1, Administration Guide, Revision 1, 26 June 2009;
c. FortiMail™ Secure Messaging Platform, Version 3.0 MR5 Patch 3, CLI Reference, Revision 1, 14 September 2009;
d. FortiMail™ Secure Messaging Platform, Quick Start Guide (produced for each model of FortiMail™ appliance); and
e. FortiMail™ FIPS 140-2 Level 1 Security Policy for 3.0 MR5, V1.0, 3 December 2009.

11 Evaluation Analysis Activities

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

Development: The evaluators analyzed the FortiMail™ functional specification and design documentation; 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 FortiMail™ security architecture 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 FortiMail™ 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 FortiMail™ configuration management system and associated documentation was performed. The evaluators found that the FortiMail™ configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

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

The evaluators reviewed the flaw remediation procedures used by Fortinet® for FortiMail™. 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 FortiMail™. Additionally, the evaluators conducted a review of public domain vulnerability databases to identify FortiMail™ potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the FortiMail™ in its operational environment.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 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[2].

The evaluators analyzed the developer's test coverage 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, 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. 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. The evaluator created a test procedure for the installation of the TOE which describes:

   - unpacking the TOE from its shipping container, connecting the power and communications cables and installing hard drives,
   - initial boot of the device followed by loading of the evaluated firmware,
   - enabling of the FIPS mode of operation, and
   - configuring the TOE to operate in either of the evaluated modes of operation.

   The evaluator exercised this test procedure for all of the evaluated models of the TOE and found that the guidance documents were sufficient to install and configure the TOE in its evaluated configuration.

[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.

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. The evaluator repeated 71 of the developer's test cases. This represents approximately 40% of the test cases submitted by the developer for the evaluation. Test cases were selected from all of the functional areas of the TOE (Antispam, Antivirus, Content Control, Archive, High Availability, Logging, Mail Transfer, Policy, System, Users and Webmail). The tests (excluding High Availability tests) were performed on all of the TOE models in both of the evaluated modes of operation (transparent and gateway). Additionally two units of one model (FE-400) were configured as a High Availability cluster and the High Availability tests were performed using this configuration.

c. Independent Evaluator Testing: The objective of this test goal is to exercise the TOE's claimed functionality through evaluator independent testing and to augment any areas that were not covered during the repeat of developer testing. The evaluator developed independent test cases in the areas of Audit, Flow Control, User's and Roles, Security Management and TOE Protection. In addition to demonstrating that the TOE complied with its stated security policies, in many cases the evaluator's test were designed to demonstrate negative conditions. For example in the area of User's and Roles, the evaluator's test cases confirmed that the Read Only Administrator and the Read/Write Administrator were denied access to specific security functions in both the web based graphical user interface and the command line interface. This was an area that was not well covered by the developer's test cases.

12.3 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:

- Generic vulnerabilities;

  The evaluator conducted an open source search for vulnerabilities of the TOE. This search did not reveal any vulnerabilities applicable to the evaluated configuration of the TOE.

- Bypassing;

  During independent testing the evaluator confirmed that if configured correctly the TOE intercepts and processes all email traffic inbound to and outbound from the protected domains of the TOE. Correct configuration of the TOE's network environment is critical, particularly when operating in Gateway mode, and this fact is stressed in all of the guidance documents. Additionally, the evaluator extensively tested the restricted access features provided by the TOE, confirming that users without full administrative privileges cannot bypass their access restrictions.

- Tampering;

  The evaluator tested the response of the TOE in several failure modes (power failure, network failure) to confirm that the secure state of the TOE was maintained in the failure mode and after recovery from the failure.

- Direct attacks;

  The evaluator conducted port scans of all of the TOE models in both evaluated modes, looking for unnecessarily open ports which might be used for further probing. No unnecessarily open ports were found. Additionally, the evaluator sniffed the connection between a remote administrator and the TOE looking for unencrypted login credentials or leaked information which could be used to launch an attack against the TOE. The communications between the TOE and the remote administrator were encrypted and no useful information was gathered from this attempted attack.

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

12.4 Conduct of Testing

FortiMail™ 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 Testing (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 FortiMail™ behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ 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

The evaluator found the FortiMail™ to be straightforward to configure, use and integrate into a typical corporate network. The product is supported by comprehensive installation and administrative guidance as well as an exhaustive Command Line Interface guide.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HA	High Availability
HMAC SHA-1	Hash-based Message Authentication Code - Secure Hash Algorithm
ICMP	Internet Control Message Protocol
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
RAID	Redundant Array of Independent Disks
RSA	Rivest, Shamir and Aldeman Algorithm
SFP	Security Function Policy
SFR	Security functional requirements
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Triple – Data Encryption Standard
TSF	TOE Security Functionality

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS), CCS-Guide-004, Version 1.1, Technical Oversight for TOE Evaluation, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1R2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2, September 2007.

d. Security Target for FortiMail™ V3.0 MR5 Secure Messaging Platform, Document Number ST004, Revision No. 1.3, 9 December 2009.

e. Evaluation Technical Report (ETR) FortiMail™ V3.0 MR5 Secure Messaging Platform, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-116, Document No. 1593-000-D002, Version 1.0, 21 April 2010.