Certification Report

EAL 2 Evaluation of Symantec™ Mail Security 8300 Series Appliances Version 5.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-70-CR
Version: 1.0
Date: 22 August 2007
Pagination: i to iv, 1 to 11

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 Information Technology 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 (CSE), 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 CSE, 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 (CSE).

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 Electronic Warfare Associates-Canada, Ltd. 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 22 August 2007, 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.commoncriteriaportal.org/

This certification report makes reference to the following trademarked or registered trademarks:

- Symantec is a registered trademark of Symantec Corporation
- Linux is a registered trademark of Linus Torvalds. Inc.
- Red Hat is a registered trademark of Red Hat, Inc.

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **3**

2 TOE Description **3**

3 Evaluated Security Functionality **3**

4 Security Target **3**

5 Common Criteria Conformance **3**

6 Security Policy **4**

7 Assumptions and Clarification of Scope **4**

7.1 SECURE USAGE ASSUMPTIONS 4
7.2 ENVIRONMENTAL ASSUMPTIONS 4
7.3 CLARIFICATION OF SCOPE 4

8 Architectural Information **4**

9 Evaluated Configuration **5**

10 Documentation **5**

11 Evaluation Analysis Activities **6**

12 ITS Product Testing **7**

12.1 ASSESSMENT OF DEVELOPER TESTS 7
12.2 INDEPENDENT FUNCTIONAL TESTING 7
12.3 INDEPENDENT PENETRATION TESTING 8
12.4 CONDUCT OF TESTING 8
12.5 TESTING RESULTS 9

13 Results of the Evaluation **9**

14 Evaluator Comments, Observations and Recommendations **9**

15 Glossary **10**

15.1 ACRONYMS, ABBREVIATIONS AND INITIALIZATIONS 10
16 References 10

Executive Summary

The Symantec™ Mail Security 8300 Series Appliances Version 5.0, from Symantec Corporation (hereafter referred to as SMS 8300), is the Target of Evaluation for this Evaluation Assurance Level 2 evaluation.

The SMS 8300 provides high-performance, integrated mail protection against virus threats, spam, and other unwanted content at the earliest point of network entry, the Internet (SMTP) gateway. As mail flows into mail servers, the SMS 8300 analyzes and filters mail using a variety of techniques, incorporating up-to-the-minute filters from Symantec Security Response. Along with standard techniques such as heuristics and pattern matching, the SMS 8300 incorporates proprietary filtering methods such as advanced signature technologies and reputation-based source filters. Filters are continuously and automatically refreshed by Symantec Security Response to combat the latest spam and other email threats, and administrators can set up centralized policies to perform a variety of actions based on the verdict assigned to each message.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 21 August 2007 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 SMS 8300, 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 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*.

CSE, as the CCS Certification Body, declares that the SMS 8300 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that

[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.

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) 2 evaluation is the Symantec™ Mail Security 8300 Series Appliances Version 5.0 (hereafter referred to as SMS 8300), from Symantec Corporation.

2 TOE Description

The SMS 8300 provides high-performance, integrated mail protection against virus threats, spam, and other unwanted content at the earliest point of network entry, the Internet (SMTP) gateway. As mail flows into mail servers, the SMS 8300 analyzes and filters mail using a variety of techniques, incorporating up-to-the-minute filters from Symantec Security Response. Along with standard techniques such as heuristics and pattern matching, the SMS 8300 incorporates proprietary filtering methods such as advanced signature technologies and reputation-based source filters. Filters are continuously and automatically refreshed by Symantec Security Response to combat the latest spam and other email threats, and administrators can set up centralized policies to perform a variety of actions based on the verdict assigned to each message.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the SMS 8300 is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title: Security Target: Symantec™ Mail Security 8300 Series Appliances Version 5.0
Version: 1.6
Date: August 20, 2007

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*.

The SMS 8300 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 2 conformant, containing all security assurance requirements from EAL 2.

6 Security Policy

The SMS 8300 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Sections 2.4.3.1 and 2.4.3.2 of the ST, respectively.

In addition, the SMS 8300 implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the SMS 8300 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

Personnel authorized to install, configure, and operate the SMS 8300 possess appropriate training, are not hostile, and will adhere to the procedures for secure usage of the product.

7.2 Environmental Assumptions

The SMS 8300 resides within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

The SMS 8300 relies on the environment to provide it physical and logical protection. The SMS 8300 provides a level of protection that is appropriate for low robustness environments processing unclassified information. It offers protection against inadvertent or casual attempts to breach system security. It is not intended for situations in which hostile and well-funded attackers use sophisticated attacks from within the physical zone.

8 Architectural Information

The SMS 8300 is comprised of the following main components:

a. Control Center – enables Web-based configuration and administration of the TOE; and

b. Scanner – performs email filtering.

The Control Center enables Web-based configuration and administration of the TOE. With a single Control Center, the end user can centrally configure, monitor, and manage all the Scanners in the network. The Control Center also contains *Quarantine*, which is an optional storage area for caught spam.

Each TOE installation has exactly one Control Center. The Control Center communicates with the Agent on each Scanner. From the Control Center's Web-based graphical user interface, a TOE Administrator can:

- Configure, start and stop each Scanner.
- Specify email filtering options for groups of users or for all users at once.
- Monitor consolidated reports and logs for all Scanners.
- See summary information.
- Administer Quarantine.
- View online help for Control Center screens.

The Scanner component performs email filtering, and a TOE installation can have one or more Scanners. Each Scanner can reside on the same SMS 8300 appliance as the Control Center component or on a separate appliance.

9 Evaluated Configuration

The evaluated configuration for the SMS 8300 comprises:

- SMS 8380 Control Center running on SMS Version 5.0.0.36 with the Linux-based Operating System, Red Hat version 9.0 running Linux Kernel version 2.6.16; and
- SMS 8360 Scanner running on SMS Version 5.0.0.36 with the Linux-based Operating System, Red Hat version 9.0 running Linux Kernel version 2.6.16.

10 Documentation

The Symantec Corporation documents provided to the consumer are as follows:

a. Symantec Mail Security Appliance Installation Guide, PN 10747600, 2006;

b. Symantec Mail Security Appliance Administration Guide, PN 10747604, 2006; and

c. Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Mail Security 8300 Series Appliances Version 5.0.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the SMS 8300, including the following areas:

Configuration management: An analysis of the SMS 8300 CM system and associated documentation was performed. The evaluators found that the SMS 8300 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, 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 the SMS 8300 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 SMS 8300 functional specification and high-level design; 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 SMS 8300 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.

Vulnerability assessment: The SMS 8300 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the SMS 8300 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. Penetration testing was conducted by evaluators, which did not expose any residual vulnerabilities that would be exploitable in the intended operating environment for the TOE.

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].

Symantec employs a rigorous testing process that tests the changes and fixes in each release of the SMS 8300. Comprehensive regression testing is conducted for all releases.

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, 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. Initialization: The objective of this test goal is to provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

c. Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met;

d. Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed;

e. Users and Roles: The objective of this test goal is to ensure the users and roles functionality is correct;

f. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data; and

[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.

g. Basic Product Functionality: The objective of this test goal is to exercise the TOE's functionality to ensure that the security claims may not be inadvertently compromised.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's 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;
- Bypassing;
- Tampering; and
- Direct attacks

The evaluator conducted a port scan of the SMS 8300. The only ports found to be open were ones that would be expected to be. The evaluator used a publicly available tool to scan the SMS 8300 for weaknesses, and none were found. The evaluator also used a publicly available packet capture tool to examine output from the SMS 8300 during startup, shutdown and normal operations. The evaluator searched the captured results in an attempt to extract information which might be useful to a potential attacker; no useful information was uncovered.

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

12.4 Conduct of Testing

The Symantec™ Mail Security 8300 Series Appliances Version 5.0 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 Electronic Warfare Associates-Canada, Ltd. 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 Symantec™ Mail Security 8300 Series Appliances Version 5.0 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 complete documentation for the Symantec™ Mail Security 8300 Series Appliances Version 5.0 includes a comprehensive Installation and Security Guide and an Administrator's Guide.

The Symantec™ Mail Security 8300 Series Appliances Version 5.0 is straightforward to configure, use and integrate into a corporate network.

Symantec is strongly committed to secure practices, the CC effort and effective configuration management and delivery processes as evidenced by the high-quality of the CC evaluation evidence and its practical application for the Symantec™ Mail Security 8300 Series Appliances Version 5.0 project.

Though life-cycle support development security is not part of this evaluation, the evaluators observed that the Symantec is particularly conscious of security. There is a single point of access to the office. All visitors are required to report and sign-in on an automated sign-in/log system at the front entrance. Visitors are issued a pass and are escorted at all times in the facility by a Symantec employee. There is a video camera system providing additional security. There are lockable doors on the server rooms and access is limited to only essential authorized personnel. The office area is locked at night and a Pin code is also required for after-hours front door access. There is no wireless access within the Symantec office; there is just wired access. Remote connection is via secure VPN connection. The physical, procedural, and personnel security measures meet the assurance requirements of higher-level CC evaluations.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 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
CSE	Communications Security Establishment
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
SMS	Symantec Mail Security
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and 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: Symantec™ Mail Security 8300 Series Appliances Version 5.0, Revision No. 1.6, August 20, 2007.

e. Evaluation Technical Report (ETR) Symantec™ Mail Security 8300 Series Appliances Version 5.0, EAL 2 Evaluation, Common Criteria Evaluation Number: 383-4-70-CR, Document No. 1549-000-D002, Version 1.2, 21 August 2007.