Certification Report

EAL 2 Evaluation of SurfControl

E-mail Filter for SMTP

Version 5.0, Service Pack 2

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-39
Version:	1.0
Date:	16 September 2005
Pagination:	i to iv, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report has been evaluated using the *Common Methodology for Information Technology Security Evaluation, Version 2.2*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.2*. The evaluation was conducted by an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS). 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 16 September 2005, 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/en/services/common_criteria/trusted_products.html

This certification report makes reference to the following trademarked names: Windows XP®, Windows 2000®, and Windows Server 2003® which are registered trademarks of Microsoft® Corporation; and SurfControl® which is a registered trademark of SurfControl plc in the U.S.A. and other countries.

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

TABLE OF CONTENTS

Executive Summary

The SurfControl E-mail Filter for SMTP, Version 5.0, Service Pack 2 from SurfControl plc, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The E-mail Filter for SMTP is a server-based software application that enforces an acceptable usage policy for SMTP-based e-mail. The E-mail Filter for SMTP scans the content, origin, destination, attachments, and size of all SMTP-based e-mail to and from the Internet, and applies the policy rules established by the E-mail Filter for SMTP administrator.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed in September 2005 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 SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2, 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[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 2.2* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2*.

CSE, as the CCS Certification Body, declares that the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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.

[1] The evaluation technical report 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) 2 evaluation is the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2, from SurfControl plc.

2 TOE Description

The E-mail Filter for SMTP is a server-based software application that enforces an acceptable usage policy for SMTP-based e-mail. The E-mail Filter for SMTP scans the content, origin, destination, attachments, and size of all SMTP-based e-mail to and from the Internet, and applies the policy rules established by the E-mail Filter for SMTP administrator.

The E-mail Filter for SMTP comprises three core components: Message Administrator, Monitor, and Rules Administrator. Additional components that enhance the E-mail Filter for SMTP capabilities are: Dictionary Management, Scheduler, Web Administrator, and Queue View.

The E-mail Filter for SMTP components are accessible to administrators through three management and configuration interfaces:

- The graphical user interface application on the Windows server machine that is hosting the E-mail Filter for SMTP;

- The graphical user interface application client “SMTP Admin Client” running on a Windows machine on the protected network; and

- The web-based graphical user interface application which can be accessed from a web browser on a machine on the protected network.

Administrators are the only direct users of the E-mail Filter for SMTP.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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: SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2
Security Target Version: v1.04
Date: 19 September 2005

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2*.

The SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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 with the security assurance requirements in the EAL 2 package.

6 Security Policy

The SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 implements a discretionary access control policy and a discretionary information flow control policy. The complete policies are identified in the ST. The following statements are representative of the policies.

6.1 Discretionary Access Control Policy

The E-mail Filter for SMTP implements a discretionary access control policy such that only administrators can access and perform allowable operations on the SMTP e-mail messages stored in the various queues of the E-mail Filter for SMTP. The policy is configurable by administrators who have one or more of the following rights: All Permissions, Message Administration Permissions, Rules Administration Permissions or Dictionary Management Permissions.

6.2 Discretionary Information Flow Control Policy

The E-mail Filter for SMTP implements a discretionary information flow policy that is applied to SMTP-based e-mail as it flows through the E-mail Filter for SMTP. The policy filtering rules are defined by the administrators. Flow contol is based on e-mail header information, attachment type, attachment content, message content, presumed sender, receiver(s), presumed sending/relaying mail server IP address or domain, and/or time of day that message was sent/received.

7 Assumptions and Clarification of Scope

Consumers of the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 product should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

For purposes of this evaluation, the E-mail Filter for SMTP administrators are assumed to be trusted not to attack the TOE, intercept network traffic, or open up the trusted network to untrusted networks. The E-mail Filter for SMTP must be installed and configured using the guidance specified in the SurfControl plc document entitled *SurfControl Email Filter 5.0 for SMTP Installation Guide.*

7.2 Environmental Assumptions

The following assumptions are made about the operating environment of the E-mail Filter for SMTP:

a. the components of the E-mail Filter for SMTP are located within controlled access facilities that will prevent unauthorized physical access;

b. administrators are non-hostile and do not attempt to compromise the E-mail Filter for SMTP functionality; and

c. the E-mail Filter for SMTP will only be managed from within the protected network.

For more information about the E-mail Filter for SMTP security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

The administrator responsible for the E-mail Filter for SMTP must ensure that the E-mail Filter for SMTP is delivered, installed, configured, administered, and operated in a manner that maintains its security by following proper security procedures. Compromise of the integrity and/or availability of the E-mail Filter for SMTP may occur as a result of an administrator not following proper security procedures or unwittingly introducing malicious code (e.g., virus, trojan horse) into the system.

The product should be operated within the intended-operating environment as specified in the ST and guidance documentation.

In order to ensure that the E-mail Filter for SMTP properly enforces the security policies without leaving vulnerabilities due to rule set processing logic, it is important that administrators carefully read and understand the applicable administrative guidance information published by SurfControl plc.

8 Architectural Information

For this evaluation, the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 is deployed on a hardened server in a demilitarized zone (DMZ). The E-mail Filter for SMTP receives SMTP traffic from the unprotected network, filters the e-mail accordingly, and then routes it to the next host which is typically a mail server, gateway or bridgehead on the protected network.

The E-mail Filter for SMTP stores all configuration data and filtering policies in an SQL database called STEMConfig and all logging data in an SQL database called STEMLog. A dedicated database stores data for a single E-mail Filter for SMTP in a single database. The SQL database is resident on the protected network and is an essential component in the E-mail Filter for SMTP environment.

Administrators can access the E-mail Filter for SMTP through three interfaces:

- The graphical user interface application on the Windows server machine that is hosting the E-mail Filter for SMTP;
- The graphical user interface application client "SMTP Admin Client" running on a Windows machine on the protected network; and
- The web-based graphical user interface application which can be accessed from a web browser on a machine on the protected network.

For more information refer to Section 2 of the ST.

9 Evaluated Configuration

The evaluated configuration of the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 requires a fully licensed version of Microsoft® SQL Server on a separate, dedicated server.

The essential physical components for the proper operation of the E-mail Filter for SMTP in the evaluated configuration are Windows workstations (for SMTP Admin Client administration) and Web browser access (for Web Administration) inside the protected network.

The publication *SurfControl Email Filter 5.0 for SMTP Administrator's Guide* and *SurfControl Email Filter 5.0 for SMTP Installation Guide* describe the procedures necessary to install and operate the E-mail Filter for SMTP Version 5.0, Service Pack 2 in its evaluated configuration.

10 Documentation

The complete documentation for the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 can be obtained from the SurfControl plc public webserver. The SurfControl plc documents provided to the consumer are as follows:

a. SurfControl Email Filter for SMTP Version 5.0, Service Pack 2 IGS Readme Document Version 0.2;

b. SurfControl Email Filter for SMTP: Service Pack 2 README file;

c. SurfControl Email Filter v 5.0 for SMTP SurfControl plc README file;

d. SurfControl Email Filter 5.0 for SMTP Administrator's Guide; and

e. SurfControl Email Filter 5.0 for SMTP Installation Guide.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2, including the following areas:

Configuration management: An analysis of the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 development environment and associated documentation was performed. The evaluators found that the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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 SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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 SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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 SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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.

Vulnerability assessment: The SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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 (coverage, functional tests, independent testing): The evaluators examined the developer's testing activities and verified that the developer has met their testing responsibilities.

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 Evaluation Technical Report (ETR)[2].

SurfControl plc employs a rigorous testing cycle process that tests the changes and fixes in each release of the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 . 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.

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

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. Security Audit;

b. Identification and Authentication;

c. User Data Protection; and

d. Security Management.

Evaluator testing (executing a sample of the developer's test cases) was carried out on 8-12 August 2005 in Chatswood, Australia on the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2.

Independent evaluator tests (functional) were conducted using the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 at the EWA-Canada's Information Technology Security Evaluation and Testing (ITSET) Facility, Ottawa, Ontario.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, limited independent evaluator penetration testing was conducted. This testing confirmed that no exploitable vulnerabilities exist for the TOE.

12.4 Conduct of Testing

The SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 was subjected to a comprehensive suite of formally documented, independent functional tests. The testing took place at the SurfControl plc facility in Chatswood, Australia, and the ITSET facility at Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario. 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 the ETR and in a separate Test Results document.

12.5 Testing Results

The independent functional tests yielded the expected results, giving assurance that the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 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 SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 includes comprehensive Installation and Administrator Guides.

The SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 is straightforward to configure, use and integrate into a corporate network.

The SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 graphical user interface provided by the E-mail Filter for SMTP is intuitive and easy to use.

SurfControl plc Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

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
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 Accreditation of Laboratories Canada
QA	Quality Assurance

SFP	Security Function Policy
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation

References

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

a. Common Criteria for Information Technology Security Evaluation, Version 2.2, CCIMB-2004-01-001, -002 and -003.

b. Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.2, CCIMB-2004-01-004.

c. CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d. SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 Security Target, Document Version 1.04, 19 September 2005; and

e. Evaluation Technical Report (ETR) SurfControl® E-mail Filter for SMTP Version 5.0, Service Pack 2, Version 1.1, 9 September 2005.