National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

McAfee

Secure Content Management Appliance Version 4.0

Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG)

Report Number: CCEVS-VR-07-0031

Dated: 18 May 2007

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)

Jandria Alexander

Aerospace Corporation

Columbia, Maryland

Deborah Downs (Senior Validator)

Aerospace Corporation

El Segundo, California

Common Criteria Testing Laboratory

InfoGard Laboratories, Incorporated

San Luis Obispo, California

Table of Contents

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the McAfee® Secure Content Management Appliance 4.0, the target of evaluation (TOE), by InfoGard Laboratories, Inc. the Common Criteria Testing Laboratory (CCTL) that performed the evaluation. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation performed by InfoGard Laboratories, Inc., San Luis Obispo, CA in accordance with the United States evaluation scheme and was completed on April 2nd, 2007. The information in this report is largely derived from the ST, Evaluation Technical Report (ETR) and the functional testing report. The ST was written by InfoGard Laboratories. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, January 2004 Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.2, January 2004.

The TOE is an Anti-Virus technology type appliance that utilizes hardware and software in an integrated appliance to scan traffic between the WAN (Internet) and an internal (protected) network. Traffic flowing between the Wide Area Network (WAN) and the internal network is routed through the SCM Appliance where, through the intercept, scanning and reporting functions of the McAfee® SCM appliance, potentially malicious files of various types are detected, restricted content traffic is filtered, and restricted internet addresses (URLs) and email containing SPAM messages or Phish attempts are blocked. Following detection, the TOE can clean the affected file, delete the file, drop the associated traffic or quarantine the item pending review.

The appliance also blocks access to restricted web sites or those containing content indicated by the Administrator as prohibited. The TOE provides alerts and reports of suspicious activity to advise Administrators of traffic characteristics routed through the appliance. Scanning behavior and subsequent actions are configurable through a graphical user interface (GUI), allowing Administrators to tailor the appliance to the deployed environment. Three modes of operation are available for configuration of the appliance within the network: Explicit Proxy, Transparent Bridge or Transparent Router mode.

This Common Criteria evaluation requires configuration in either Transparent Bridge or Transparent Router mode only, which makes the appliance operation transparent to devices communicating through the TOE. The security functionality for both the transparent bridge mode and the transparent router mode are the same. The only difference is that in the transparent router mode, the appliance acts as a router and routes traffic between networks based on its routing table. In the transparent bridge mode, the appliance physically connects between two network segments and treats them as one logical network. **NOTE:** Explicit proxy mode was not part of the Common Criteria Evaluated configuration and should **not** be used in systems that require the Common Criteria evaluated configuration.

The TOE makes use of cryptographic modules in order to fulfill some security functions. The Cryptographic modules are certified by the vendor to operate correctly. No independent certification under National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 was performed on this product. In addition, the cryptographic functions of the TOE were not evaluated further during the CC evaluation. **NOTE:** Users should ensure that they select a product that meets their needs, including FIPS 140-2 compliance, if appropriate. Also, the algorithm suite that is used within the TOE (OpenSSL) is **not** a certified FIPS 140 cryptographic module.

The McAfee® Secure Content Management Appliance 4.0 product consists of the following components:

<table>
<tr><th>TOE/Environment</th><th colspan="2">Component Name Description of Component</th></tr>
<tr><td>TOE</td><td colspan="2">
<table>
<tr><th>SIG 3100</th><th>SIG 3200</th><th>SIG 3300</th><th>SMG 3300</th><th>SWG 3300</th><th>SWG 3400</th></tr>
<tr><td><b>A</b></td><td></td><td>▨</td><td>▨</td><td>▨</td><td>▨</td></tr>
<tr><td>▨</td><td><b>B</b></td><td>▨</td><td>▨</td><td>▨</td><td>▨</td></tr>
<tr><td>▨</td><td></td><td><b>C</b></td><td>▨</td><td>▨</td><td>▨</td></tr>
<tr><td>▨</td><td>▨</td><td>▨</td><td><b>D</b></td><td><b>D</b></td><td>▨</td></tr>
<tr><td>▨</td><td>▨</td><td>▨</td><td><b>E</b></td><td></td><td><b>E</b></td></tr>
</table>

<b>A) McAfee® 3100 Secure Internet Gateway Appliance (SIG)Version 4.0 (SKU: MAP-3100-SIG P/N: 610-1014-04-G5) [OR]</b>
<b>B) McAfee® 3200 Secure Internet Gateway Appliance (SIG)Version 4.0 (SKU: MAP-3200-SIG P/N: 610-1015-02-G5) [OR]</b>
<b>C) McAfee® 3300 Secure Internet Gateway Appliance (SIG)Version 4.0 (SKU: MAP-3300-SIG P/N: 610-1049-02-G5) [OR]</b>

<b>D) McAfee® 3300 Secure Messaging Gateway (SMG) Appliance Version 4.0 and McAfee® 3300 Secure Web Gateway (SWG) Appliance Version 4.0 (SKU: MAP-3300-SMG & MAP-3300-SWG, Hardware P/N:</b> 610-1016-02-G5 (SMG)<b>)</b> <b>(</b>610-1017-03-G5 (SWG)<b>)</b> <b>[OR]</b>

<b>E) McAfee® 3300 Secure Messaging Gateway (SMG) Appliance Version 4.0 (SKU MAP-3300-SMG Hardware P/N:</b> 610-1016-02-G5 (SMG)<b>) and McAfee® 3400 Secure Web Gateway (SWG) Appliance Version 4.0 (MAP-3400-SWG Hardware P/N:</b> 610-1018-02-G5<b>)</b>
</td></tr>
<tr><td>Environment</td><td>“Management Computer”</td><td>Requires:</td></tr>
</table>

	Configured for Administrator access to the TOE	PC with 300 megahertz (MHz) or higher processor clock speed recommended; 233-MHz minimum required;* Intel Pentium/Celeron family, AMD K6/Athlon/Duron family, or compatible processor recommended 128 megabytes (MB) of RAM or higher recommended (64 MB minimum supported; may limit performance and some features) 1.5 gigabyte (GB) of available hard disk space Super VGA (800 × 600) or higher resolution video adapter and monitor CD-ROM or DVD drive Keyboard and Microsoft Mouse or compatible pointing device
Environment	DNS Server component	Provides DNS service to the network
Environment	Router(s)	Routers as needed for network deployment
Environment	Switch(s)	Switches as needed for network deployment

Table 1: Physical Scope and Boundary: Hardware

The following table illustrates the differences between the four appliance hardware platforms:

Hardware Platform	3100	3200	3300	3400
SCM model(s)	**SIG**	**SIG**	**SIG, SMG, SWG**	**SWG**
RAM	512 K	1 GB	4 GB	4 GB
Hard Drive(s)	80 GB	73 GB x 2	73 GB x 2	73 GB x 2
Processor	Celeron® 2.8 GHz	Xeon® 2.8 GHz	Dual Xeon® 2.8 GHz	Dual Xeon® 2.8 GHz
Interfaces	2x Ethernet	2x Ethernet	2x Ethernet 2x Fiber Base SX	2x Ethernet 2x Fiber Base SX
Power Supply(s)	Single	Single	Dual	Dual
Misc				ASIC Accelerator

Table 2: Hardware Platform comparison

TOE or Environment	Component Name	Description of Component

TOE	Secure Content Management Software v.4.0 (identical for all deployment options, includes SCM operating system Redhat Linux 9, 2.4 Kernel with McAfee® customization) webshield-sag-7.0-948.200507201234.101.iso webshield-swg-7.0-948.200507201234.101.iso webshield-smg-7.0-948.200507201234.101.iso	SCM software package incl. O.S.
Environment	Windows 2000 SP4, Windows XP SP2	Operating system for Management Computer
Environment	Microsoft Internet Explorer 5.5, 6.0 or later with Secure Sockets Layer (SSL) v2 or v3 encryption, with ActiveX enabled	Web Browser Component on Management Computer for Administrator access to TOE

Table 3: Physical Scope and Boundary: Software

It is important to note that the following components/features are part of the SCM appliance product but were excluded from the TOE evaluation and ***should not be used in the evaluated configuration***:

- McAfee® E-Policy Orchestrator (software)
- Explicit Proxy Mode deployment
- The use of LDAP authentication servers
- Available provision within the TOE for exporting log records to an external server (i.e. syslog)
- Remote Access Card option for the 3300/3400 appliances (Enterprise)
- Administration from a remote location using the Remote Access Card
- SCM Client v 4.0 – Client software for Java based Admin interface
- ICAP server
- CLI usage except for initial installation of the CCE Compliant Installation Pack Installation – SCM Appliance version 4.0.

1.1. Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before June 6, 2006.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 2: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	A) McAfee® 3100 Secure Internet Gateway Appliance (SIG)Version 4.0 (SKU: MAP-3100-SIG P/N: 610-1014-04-G5) [OR] B) McAfee® 3200 Secure Internet Gateway Appliance (SIG)Version 4.0 (SKU: MAP-3200-SIG P/N: 610-1015-02-G5) [OR] C) McAfee® 3300 Secure Internet Gateway Appliance (SIG)Version 4.0 (SKU: MAP-3300-SIG P/N: 610-1049-02-G5) [OR] D) McAfee® 3300 Secure Messaging Gateway (SMG) Appliance Version 4.0 and McAfee® 3300 Secure Web Gateway (SWG) Appliance Version 4.0 (SKU: MAP-3300-SMG & MAP-3300-SWG, Hardware P/N: 610-1016-02-G5(SMG)) (610-1017-03-G5(SWG)) [OR] E) McAfee® 3300 Secure Messaging Gateway (SMG) Appliance Version 4.0 (SKU MAP-3300-SMG Hardware P/N: 610-1016-02-G5 (SMG)) and McAfee® 3400 Secure Web Gateway (SWG) Appliance Version 4.0 (MAP-3400-SWG Hardware P/N: 610-1018-02-G5)
Protection Profile	None
Security Target	*McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) EAL 2 Security Target* Version 1.1, May 7, 2007
Dates of evaluation	June 2006 through April 2007

Evaluation Technical Report	*Evaluation Technical Report McAfee® Secure Content Management Appliance Version 4.0, Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG)*, Version 1.1, May 7, 2007
Conformance Result	Part 2 and Part 3 conformant, EAL 2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.2, January 2004
Common Evaluation Methodology (CEM) version	CEM version 2.2, January 2004
Sponsor	McAfee
Developer	McAfee
Evaluators	Albert Chang and Clyde Sy of InfoGard Laboratories Incorporated
Validation Team	Deborah Downs, Mike Allen and Jandria Alexander of The Aerospace Corporation

3. SECURITY POLICY

The Security Functional Policies (SFPs) implemented by the McAfee® Secure Content Management Appliance 4.0 provide a mechanism so that only the identified/authenticated administrator has access to TOE resources, provides accountability for actions by logging security events, and a protection mechanism that provides the security policies.

Note: Much of the description of the McAfee® Secure Content Management Appliance 4.0 security policy has been extracted and reworked from the McAfee® Secure Content Management Appliance 4.0 Security Target [6.)].

The McAfee® Secure Content Management Appliance 4.0 performs the following security functionality:

- Anti-Virus
- ID and Authentication
- Filtering
- Action and Remediation
- Cryptographic Operations
- Audit
- Security Management
- Protection of TOE Functions

4. ASSUMPTIONS

4.1. Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the TOE hardware and software commensurate with the value of the IT assets. Specifically, the TOE is assumed to be located in a Server Room location providing physical protection and limited (Administrator only) access.

4.2. Personnel Security Assumptions

It is assumed that all authorized administrators are properly trained, not careless, not willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.3. Operational Security Assumptions

It is assumed that the McAfee® SCM Appliance is dedicated to its primary function and is not intended to provide any general purpose computing or storage capabilities. It is also assumed that information cannot flow between external and internal networks located in different enclaves without passing through the TOE. The Administrators will receive and install update signature files from the Anti-Virus Vendors and distribute the .dat and associated scanning engine updates to the TOE. Lastly, the administrator management computer used for remote security management purposes is assumed to be free from malware or other malicious software.

4.4. Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats:

T.AUDIT_ COMP A network user, attacker or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.

T.BAD_DAT A threat signature .dat file could be compromised during download to the TOE resulting in an inaccurate or corrupted threat signature file being used on the TOE.

T.UNID_ACTION An administrator may not have the ability to notice potential security violations, thus limiting the administrator’s ability to identify and take action against a possible security breach.

T.FLAW_CONFIG Unintentional or intentional errors in implementation of the TOE deployment may occur, leading to flaws that may be exploited by a malicious User or program.

T.MASQUERADE A malicious user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

T.MAL_AGENT A malicious agent may attempt to introduce a virus, malware, spyware, phish attempt, or SPAM onto a internal network resource via network traffic to compromise data or use that resource to attack other network nodes.

T.MAL_CONTENT Users within the internal network may attempt to access Network Policy prohibited URL addresses on the internet.

T.MAL_MSG Prohibited content may be received or sent through email resources within the protect network through the TOE appliance.

T.RESOURCE_X A malicious process or user may block others from TOE system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.

4.5. Organizational Security Policies

There are no applicable organizational security policies

5. ARCHITECTURAL INFORMATION

The McAfee® SCM Appliance architecture is divided into the following sections:

- Anti-Virus Module
- Anti-Spyware Module
- Anti-Phishing Module
- Anti-Spam Module
- URL Filtering Module
- Content Scan Module
- Quarantine Management Module
- ICAP support Module
- HTTP Scan Module
- SCM Security Management Operating System
- Statement of Non-Bypassibility of the TSF

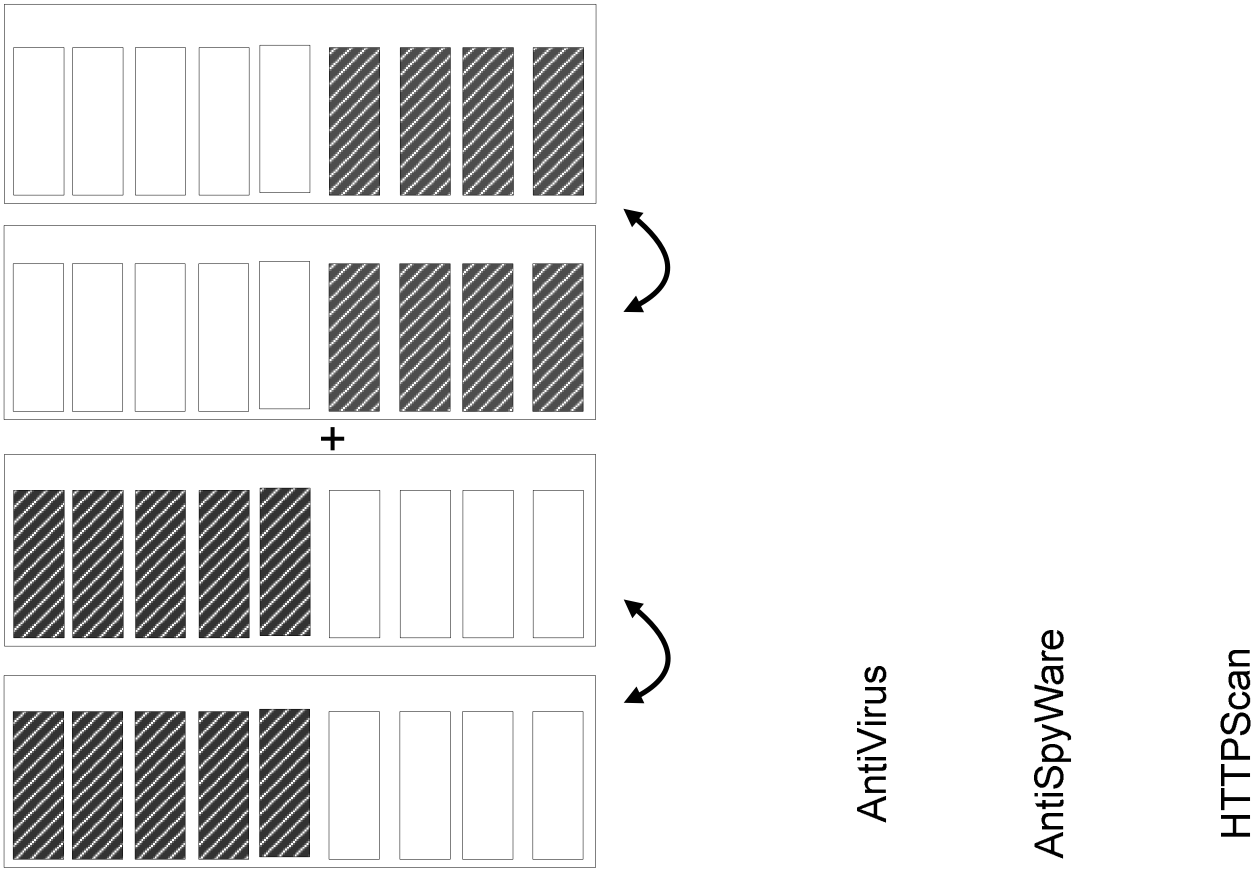


Figure 1: TOE Enterprise Option Hardware A & B combination

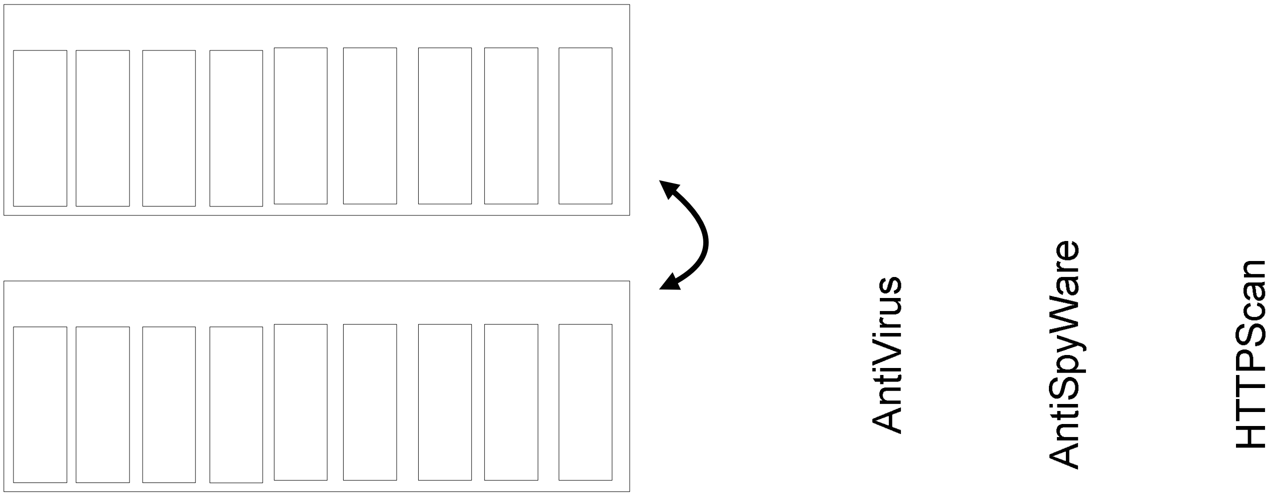


Figure 2: TOE Small Business Option Hardware C

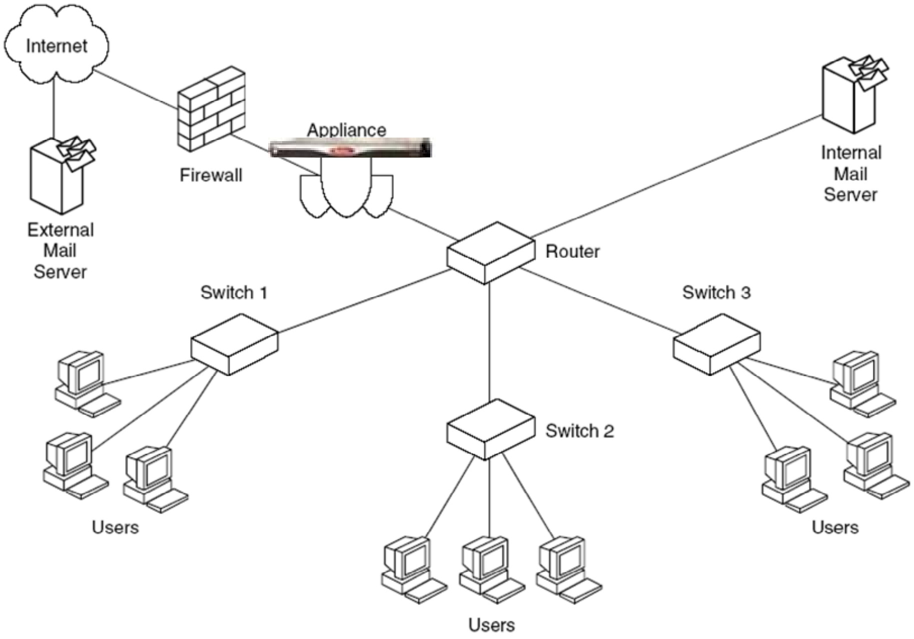


Figure 3: Architectural Diagram (network) SIG

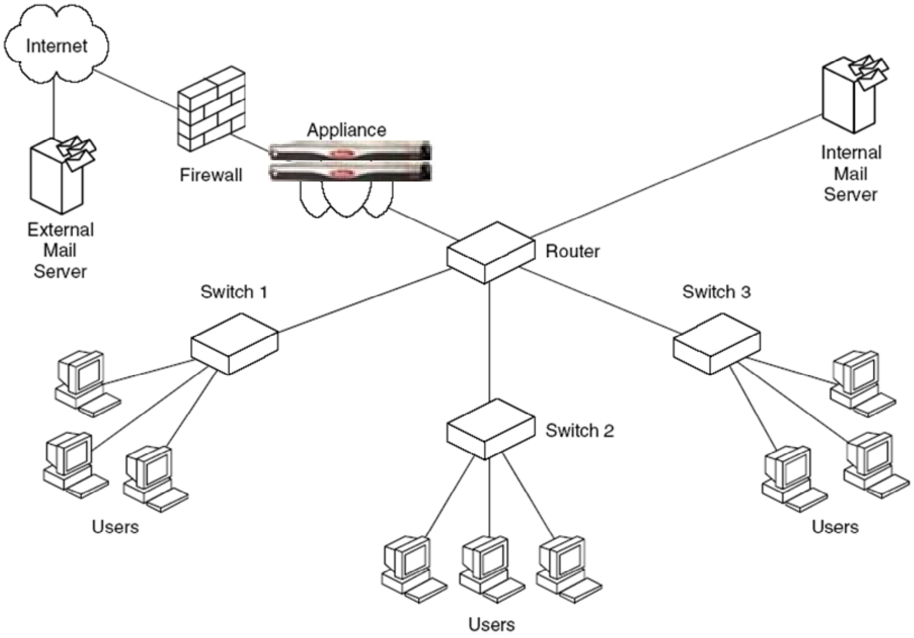


Figure 4: Architectural Diagram (network) SMG + SWG

5.1. Software Architectural Overview

The software of the McAfee® SCM appliance is identical among all shown configurations of the appliance. The service or functionality that is enabled is dependent upon the hardware platform deployed. In the case of the Secure Internet Gateway appliance all the software modules execute on that single hardware appliance. In the case of the Secure Messaging Gateway and Secure Web Gateway, those modules that correspond to the selected hardware platform are enabled based on that platform (either Messaging Related (email) or Web Gateway related (Internet)). In Figure 1, the modules shown that are darkened represents modules that are disabled due to the dedicated purpose of the appliance.

5.1.1. Anti-Virus Module

The Security Content Management application features an Anti-Virus module that provides protection through the SCM appliance from Viruses and Malicious programs. This module contains the essential scanning engine used for specific scans performed by other modules within the TOE.

The Anti-Virus module features automated scan processes that detect viruses and potential risks by comparing virus signature files, updated by McAfee® on a regular basis, to traffic flowing through the appliance. Email messages are scanned in the same manner to assure that attachments do not contain malicious software. Virus scanning is performed in real time by intercepting and reviewing network traffic. This function is provided by an Anti-Virus Scanning Engine and Virus Definition (.dat) files. The Anti-Virus Scanning Engine utilizes the updated .dat files to recognize Virus/Malware/Spyware files during scans based on their binary pattern. **NOTE:** The Common Criteria Evaluated configuration does not utilize the automated update function to update the base Program code to ensure the core software revision used for the CC evaluation remains unchanged. The only allowable updates are .dat signature files and anti-virus engine updates that are required to utilize the .dat files.

In addition to signature based detection, the anti-virus module also uses heuristic analysis to evaluate files to identify potentially harmful programs that have not yet been characterized with a signature file.

5.1.2. Anti-Spyware Module

The Anti-Spyware subsystem of the TOE utilizes the Anti-Virus Module's scanning functionality to identify potentially malicious programs called Spyware. Spyware can include programs intended to track network user browsing habits, establish keylogger programs or other local tracking programs on network user computers. These programs can also remotely administer workstations or applications. Adware is included within this definition and represents code that solicits advertising from internet sites by placing and polling tracking cookies on targeted workstations.

Another term for such programs referenced in the TOE is Potentially Unwanted Programs (PUPs). As with the Anti-Virus module, detection functions use Spyware signatures to identify potential Spyware programs.

5.1.3. Anti-Spam Module

The TOE provides protection from SPAM messages through the “Spamkiller” feature provided by the Anti-Spam Module of the Secure Content Management Suite. This functionality results in messages that meet pre-specified rules being separated from legitimate mail and forwarded to a specified location for review. The TOE uses 3 primary techniques to identify SPAM messages:

- Rules and scores

  A score is assigned for each aspect of a message, identified as suspicious, that may indicate a SPAM email message. These rules and score guidelines can be modified based on Administrators preferences. If a message reaches a certain score threshold it can be routed as SPAM.

- Bayesian learning

  The appliance uses Bayesian databases to calculate, using a scoring system, the probability that an e-mail message contains spam. This approach utilizes statistic probability and a database to determine if a message was likely SPAM.

- Blacklists and whitelists

  This technique uses Administrator created lists to either allow or disallow messages to be routed regardless of the SPAM score. Items from senders on a blacklist will be routed as SPAM, items from senders on a whitelist will be routed even if the score indicates it may be SPAM.

5.1.4. Anti-Phishing Module

The Anti-Phishing module leverages the scanning functionality of the Anti-Virus module in scanning email messages for characteristics typical of a Phishing attempt. These characteristics result in scoring as configured by the Administrator and may result in blocking of the messages if the threshold is reached and the network user is notified of a suspect email message. Alert warnings, action to be taken and reporting preferences may be configured by the Administrator.

5.1.5. URL Filtering Module

The TOE utilizes a URL filtering database that contains web site addresses with Administrator configured categories for use in filtering. The SIG application and SWG application utilize this Internet related functionality to filter which web sites are accessible through the TOE appliance. If a match is made between a URL requested from a network user and the restricted URL database, then access to that URL is blocked.

Based on this functionality and administrator configuration, specified web sites in various categories can be blocked, network users may be notified of the restricted nature of the site or access can be allowed based on established rules. This functionality is used to prevent access to offensive or non-business related web sites providing protection from liability and bandwidth preservation for the business.

5.1.6. Content Scan Module

This module uses content rules to prevent SMTP e-mail messages with unwanted content reaching their intended recipients. Based on Administrator configured rules, email messages are scanned by the TOE to determine if the content matches a restricted category or rule. Various parts of the email message may be scanned based on Administrator preferences and Administrators may receive a message that specifies which rule has been violated resulting in the blocking of a message. When rules are matched the message may be dropped, the SPAM score of the message can be adjusted based on characteristics or the message may be allowed but logged for administrator review.

5.1.7. Quarantine Management Module

McAfee® Quarantine Management is a software module that allows you to consolidate quarantine management and spam learning for the SCM appliance. This module can forward suspect messages or spam to a centralized server for disposition.

The TOE can be configured to send an e-mail message (known as a quarantine digest) to any network user that has quarantined e-mail messages. Depending on how the quarantine digest option has been configured, the quarantine digest e-mail message can contain:

- A list of e-mail messages that have been quarantined on behalf of that network user
- A URL link to a web site containing that information
- The list and the URL link

Network users can use the quarantine digests or a special McAfee® Quarantine Management network user interface to manage their own quarantined messages.

5.1.8. ICAP support Module (Not Applicable to the Evaluated Configuration)

ICAP support allows ICAP clients to pass HTTP messages to ICAP servers for some kind of processing or transformation (known as adaptation). The CC Evaluated configuration does **not** include the use of an ICAP server; therefore it should not be used.

5.1.9. HTTP Scan Module

The HTTP Scan Module provides the HTTP scanning functions to allow for the scanning of aspects of HTTP traffic to support other modules in detecting HTTP traffic characteristics that may indicate a malicious message or traffic. The appliance can be configured to scan:

- Request headers.
- Request bodies.
- Request cookies.
- Response headers.

- Response bodies.
- Response cookies.

5.1.10. SCM Security Management Operating System

SCM Operating System

The SCM operating system is a tailored version of Redhat Linux 9, Kernel 2.4 that integrates the operation of all McAfee® SCM support modules and provides the operational environment for executing the appliance's core functionality. This general application support, which is not explicitly represented by subsystems defined in previous sections, is referred to as the core SCM application. The core SCM application provides application level support to operational modules as well as security management support and audit log generation. The SCM Operating System also supports the administration of the appliance through an administrator management computer using an internal network connection to the appliance. This leverages the Apache Web Server within the SCM Operating System, which provides the User Interface for the SCM Appliance as well as ID and Authentication of Administrators for the appliance.

Security Management

Security Management functions are supported by the SCM Operating System and include an administrator interface, rendered by Apache Webserver, and functionality to allow for configuration and management of the Appliance. Administrator functions can be managed within the internal network through an administrator management computer or remotely in an encrypted form via HTTPS. The administrator management computer is a general purpose computing device and requires only a browser to communicate locally with the TOE appliance. The browser required for administrator management of the TOE is Microsoft Internet Explorer 5.5, 6.0 or later with Secure Socket Layer (SSL) v2 or v3 encryption, with ActiveX enabled. In addition, the Management Computer should be controlled and checked to ensure it is protected from installation of any Malware. Remote administration of the McAfee® SCM appliance is **not** included in the CC evaluated configuration and should not be used by CC customers

5.1.11. Statement of Non-Bypassibility of the TSF

Users should ensure that all WAN traffic can only enter or leave the protected network via the SCM appliance. That is, there should be no other routers (bridges) between the WAN and the protected network to ensure that the TOE security functions cannot be bypassed. All access to the TOE security functions requires Administrator level authentication to the TOE. The McAfee® SCM authentication process ensures that a valid username and password combination must be entered prior to allowing any changes to TSF settings.

5.2. TOE Boundaries

Figure 5 illustrates the McAfee® Secure Content Management Appliance 4.0 and its intended environment. Additionally, other components of the McAfee® Secure Content Management Appliance 4.0 product, as noted in the Introduction, are not part of the TOE.

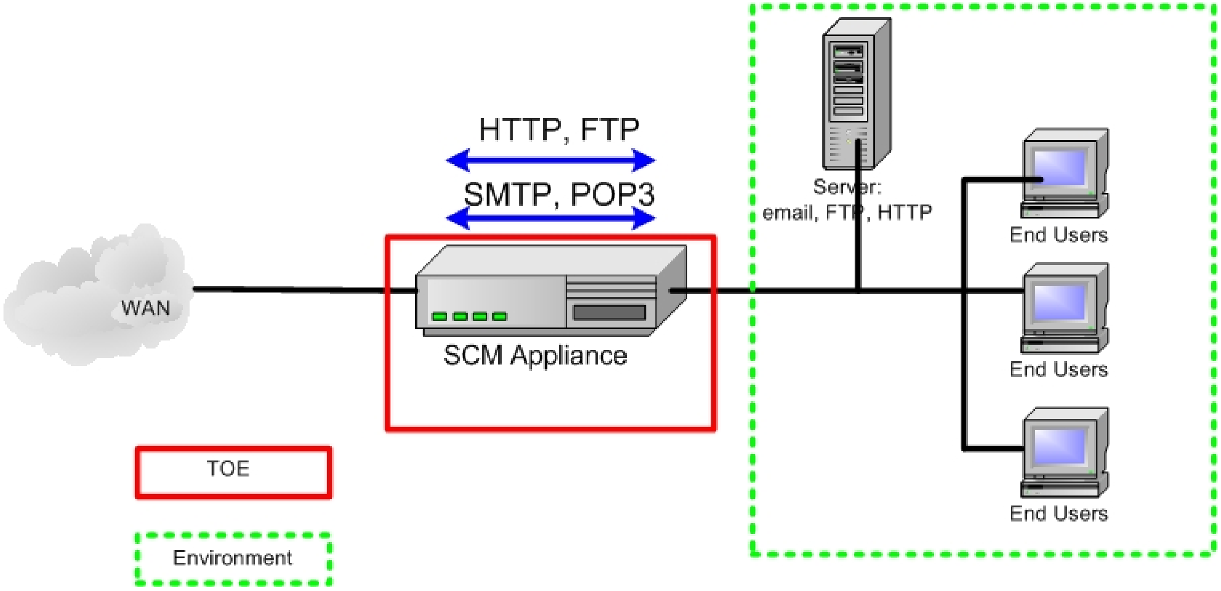


Figure 5: Physical Boundaries

In terms of logical boundaries, the following table enumerates the division between services provided *by* the TOE. The TOE itself does not rely on any services provided by the Operating Environment:

Functional Area	Services Provided *By* The TOE	Services Provided *To* The TOE By The Operating Environment
Anti-Virus	The Anti-Virus security function for the McAfee® SCM TOE provides the scanning functionality to detect specified traffic that may pose a threat to internal networks.	None
ID and Authentication	Access to the SCM appliance is gained through a network connection of an administrator management computer to the appliance and utilizes a browser based interface to gain access to the appliance management GUI.	None
Filtering	The Filtering security function of the McAfee® SCM appliance utilizes the core scanning capability described in the Anti-Virus security function to	None

	identify suspect email messages and/or email attachment and take specified action upon detection of restricted content.	
Action and Remediation	The Action and Remediation security function is provided by the Scanning Engine component (within the AntiVirus subsystem) and core application based on configuration settings that are passed to the Scanning Engine during the action/remediation configuration process by the SCM admin.	None
Cryptographic Operations	The only cryptographic operations within the TOE are the verification process for downloaded .dat threat signature files and for creating SSL sessions to access the Administrator management functions.	None
Audit	The McAfee® SCM Appliance generates audit records for security related events and all TSF configuration changes. The Audit security function is supported by a dedicated logging subsystem and the core application, both housed within the SCM Operating System.	None
Security Management	The McAfee® SCM TOE provides security management functions and tools to manage the TOE's security features. The Security Management interface is provided through a Graphical User Interface (GUI) hosted on the Apache web server component in conjunction with the core SCM application	None
Protection of TOE Functions	Protection of the TOE from physical and logical tampering is ensured by the physical security assumptions and by the domain separation requirements on the TOE. A secure session is required to be established prior to allowing TSF access and operating system based access	None

	controls restrict TSF access to Administrators only.	

Table 3: TOE Security Functions

6. DOCUMENTATION

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the McAfee® Secure Content Management Appliance 4.0.[1] Note that not all evidence is available to customers. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is *not* delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a bold title, but a hashed background.

The TOE is physically delivered to the end User. The guidance is part of the TOE components and is delivered with the TOE on CD labeled “Documentation CD”.

6.1. Design documentation

Document	Revision	Date
EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Version 4.0, Sections 3, and 4.	1.0	April 2, 2007
EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Section 5.	1.0	April 2, 2007
Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0, Section 1, 3, 4, and 5.	1.0	April 2, 2007
McAfee® Secure Content Management appliances product guide, version 4.0		August 2005

6.2. Guidance documentation

Document	Revision	Date
McAfee® Secure Content Management appliances product guide, version 4.0.(AGD_ADM)		August 2005

[1] This documentation list is based on the lists provided in the Evaluation Technical Report developed by InfoGard.

Document	Revision	Date
McAfee® Secure Content Management appliances concepts guide, version 4.0		August 2005
McAfee® SCM 3100 Installation Guide (English), version 4.0, 2005.		
McAfee® SCM 3200 Installation Guide (English), version 4.0, 2005		
McAfee® SCM 3300 and SCM 3400 Installation Guide (English), version 4.0, 2005.		
Quick Start Guide for McAfee® Secure Content Management Appliances version 4.0		
Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0, Sections 1, 2, 4, and 5.(ADO_IGS)	**1.0**	**April 2, 2007**
McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) Security Target	1.1	May 7, 2007

6.3. Configuration Management and Lifecycle

Document	Revision	Date
McAfee® Secure Content Management Appliance Version 4.0 EAL 2 Configuration Management Documentation, Version (ACM_CAP)	1.0	April 2, 2007
McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) Security Target	1.1	May 7, 2007

6.4. Delivery and Operation documentation

Document	Revision	Date
McAfee® Secure Content Manager Delivery Procedures for Common Criteria (ADO_DEL)	1.0	March 26, 2007
McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) Security Target	1.1	May 7, 2007
Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0, Sections 1, 2, 4, and 5.(ADO_IGS)	**1.0**	**April 2, 2007**

6.5. Test documentation

Document	Revision	Date
EAL 2 Test Activity ATE McAfee® Secure Content Management Appliances, Section 2 and Section 10. (ATE_COV.1)	1.0	April 2, 2007
EAL 2 Design Documentation McAfee® Secure Content Manager Appliance	1.0	April 2, 2007
McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) Security Target	1.1	May 7, 2007

6.6. Vulnerability Assessment documentation

Document	Revision	Date
McAfee® Secure Content Management Appliance Common Criteria Vulnerability Analysis AVA_VLA.1 EAL2.	1.0	April 2, 2007
McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) Security Target	1.1	May 7, 2007

EAL 2 Strength of Function Analysis McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG)	1.0	April 2, 2007
Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0	**1.0**	**April 2, 2007**
EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Version 4.0, Sections 1,2,3 and 4.	1.0	April 2, 2007

6.7. Security Target

Document	Revision	Date
McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG)	1.1	May 7, 2007

7. IT PRODUCT TESTING

This section describes the testing efforts of the Developer and the evaluation team.

7.1. Developer testing

Test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. During the evaluation of ATE_FUN.1, the evaluation team identified inconsistencies in the test cases and worked with the Developer to create accurate test cases.

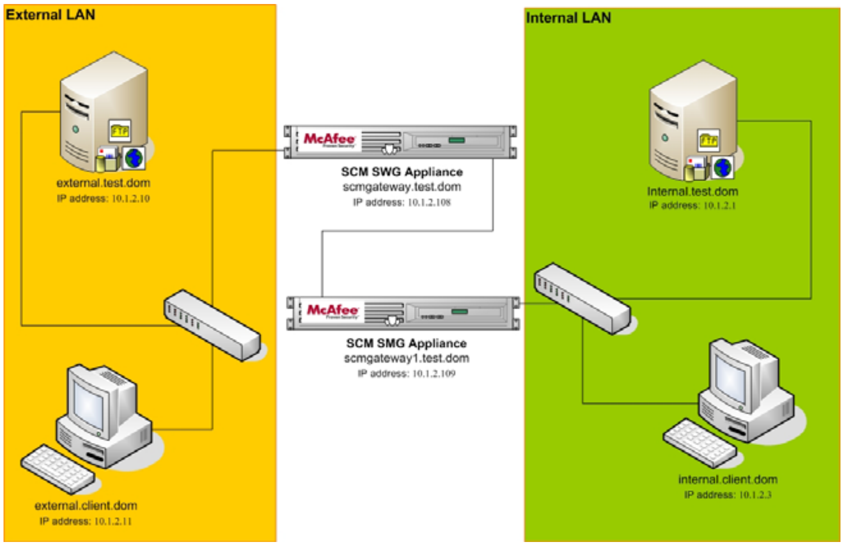
The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. Each test case was identified by a number that correlates to the expected test results in the TOE Test Plan.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

The following diagrams depict the test environment that was used by the Developers. The Evaluators assessed that the test environment used by the Developers was appropriate and mirror the test configuration during Independent testing.

Test Environment

SWG + SMG 3300 Transparent Bridge mode testing environment



Equipment:

Appliance: SWG and SMG 3200 SCM Version 4.0

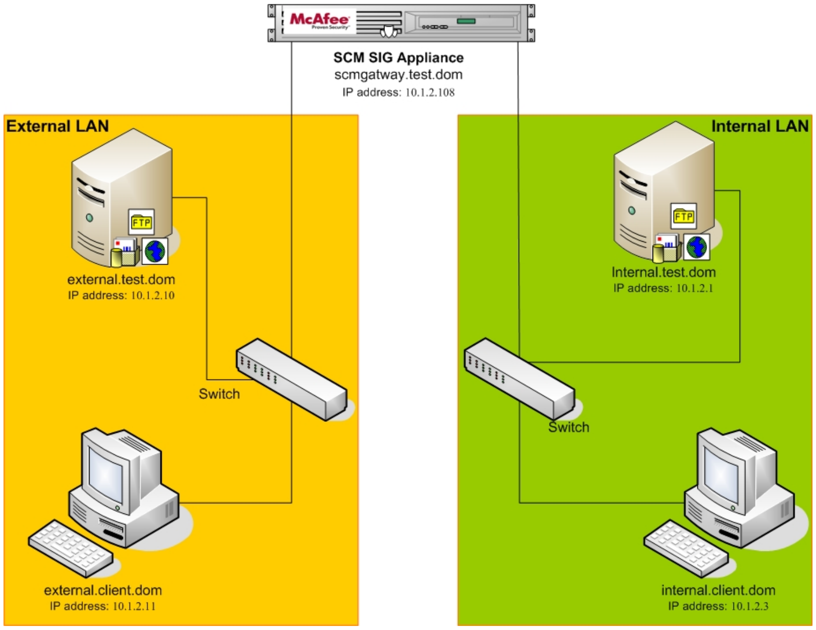
Switches: 10/100 Mbps 8 port Ethernet switch

Desktops/Servers: Pentium IV 2.4 GHz, 512 MB RAM, 40 GB Hard Disk, CD-ROM is the recommended configuration.

Cables: CAT5

Test Environment

SIG 3200 Transparent Bridge mode testing environment



Equipment:

Appliance: SIG 3200 SCM Version 4.0

Switches: 10/100 Mbps 8 port Ethernet switch

Desktops/Servers: Pentium IV 2.4 GHz, 512 MB RAM, 40 GB Hard Disk, CD-ROM is the recommended configuration.

Cables: CAT5

7.2. Evaluation team independent testing

The evaluation team conducted independent testing at the CCTL. The evaluation team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team repeated 50% of the Sponsor’s test cases and designed additional independent tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

The following were either not tested or partially tested by the evaluation team:

Not Tested/Partially Tested

SFR	**Rationale**
FAU_STG.3	The TOE audit storage capacity is fairly large and the evaluation team could not generate enough audit logs to take up 75% or more of the of the audit storage capacity.
FAU_STG.4	The TOE audit storage capacity is fairly large and the evaluation could not generate enough audit logs to take up 75% or more of the of the audit storage capacity.
FCS_CKM.1a	Partially tested by all the tests that utilized the Administrator Management GUI.
FCS_CKM.1b	Partially tested by all the tests that utilized the Administrator Management GUI.
FCS_CKM.1c	Partially tested by all the tests that utilized the Administrator Management GUI.
FSC_COP.1a	Implicitly tested via AntiVirus .dat update (TCS-201a,b).
FSC_COP.1b	Implicitly tested via AntiVirus .dat update (TCS-201a,b).
FCS_COP.1c	Partially tested by all the tests that utilized the Administrator Management GUI.
FCS_COP.1d	Partially tested by all the tests that utilized the Administrator Management GUI.
FMT_MSA.2.1	Implicitly tested through the management function interface as specified in FMT_SMF.1.

	The TOE generates exceptions/errors for any insecure or invalid security attributes values entered via GUI.

Table 4

7.3. Vulnerability analysis

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Developer Strength of Function analysis, the Developer Vulnerability Analysis, and the evaluation team's Vulnerability Analysis, and the evaluation team's performance of penetration tests.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerability in the product and to show that it is not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's Vulnerability Analysis, the evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with an expertise level of unsophisticated. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing to devise the penetration testing. This resulted in a set of three penetration tests:

- Attempt extra long passwords
- Test TOE's ability to recognize an updated .dat file
- Attempt to bypass the administrator's authentication

8. EVALUATED CONFIGURATION

The evaluated configuration of the McAfee® Secure Content Management Appliance 4.0, as defined in the Security Target, consists of the several components. Please refer to Tables 1 and 2 for the TOE's hardware and software components.

The McAfee® Secure Content Management Appliance 4.0 must be configured in accordance with the following Guidance Documents:

- Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0, Version 1.0, April 2, 2007

9. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

InfoGard Laboratories has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on April 2, 2007. A final Validation Oversight Review (VOR) was held on April 23, 2007 and final changes to the ST, ETR and VR were completed on May 7, 2007.

10. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) meet the claims stated in the Security Target. The validation team also wishes to add the following caveats to the use of the product and the evaluated configuration.

The TOE makes use of cryptographic modules in order to fulfill some security functions. The Cryptographic modules used in this product are certified by the vendor and **not** certified under the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2. Users of this product should ensure that their certification requirements can be satisfied by a product that does not include FIPS 140-2 certified encryption.

While extensive audit features are included in the evaluated TOE, it is important to note that the provision for exporting log records that can be used with the product was **not** evaluated and should not be used as part of a CC configuration.

The following features of the commercially available appliances were not included as part of the evaluation and should not be used in the CC configuration:

- McAfee® E-Policy Orchestrator (software)
- Explicit Proxy Mode deployment
- The use of LDAP authentication servers
- Available provision within the TOE for exporting log records to an external server (i.e. syslog)
- Remote Access Card option for the 3300/3400 appliances (Enterprise)
- Administration from a remote location using the Remote Access Card
- SCM Client v 4.0 – Client software for Java based Admin interface
- The ICAP server
- CLI usage except for initial installation of the CCE Compliant Installation Pack Installation – SCM Appliance version 4.0.

11. ANNEXES

None

12. SECURITY TARGET

McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) EAL 2 Security Target, Version 1.1, May 7, 2007

13. GLOSSARY

- **Administrator:** Role applied to user with full access to all aspects of the McAfee® Secure Content Management Appliance 4.0 appliance. Member of Administrative Users definition.
- **Administrative Users:** This term connotes within this ST an administrative user of the McAfee® Secure Content Management Appliance 4.0 appliance. Members of this grouping term include: Administrator, Operator and Guest.
- **Attack:** An attack is an exploited threat or an attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
- **Authentication:** Verification of the identity of a user.
- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so

forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. BIBLIOGRAPHY

1.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 2.2, January 2004. CCIMB-2004-01-0001.

2.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 2.2, January 2004. CCIMB-2004-01-002..

3.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 2.2, January 2004. CCIMB-2004-01-003.

4.) Common Criteria Project Sponsoring Organisations. Common Criteria Common Methodology for Information Technology Security Evaluation. January 2004 CCIMB-2004-01-004.

5.) Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

6.) InfoGard Laboratories. *McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) EAL 2 Security Target* Version 1.1, May 7, 2007

7.) InfoGard Laboratories. *Evaluation Technical Report McAfee® Secure Content Management Appliance Version 4.0, Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG)*, Version 1.1, May 7, 2007.