McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG)

EAL 2

Security Target

Release Date:	May 07, 2007
Document ID:	06-1094-R-0019
Version:	1.1

Prepared By: InfoGard Laboratories, Inc.

Prepared For:

McAfee
3965 Freedom Circle
Santa Clara, CA 95054

Table of Contents

List of Tables

List of Figures

Document History

Release Number	Date	Author	Details
1.1	5/7/07	InfoGard	Updates for final release version.

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification:

SIG 3100	SIG 3200	SIG 3300	SMG 3300	SWG 3300	SWG 3400
A					
	B				
		C			
			D	D	
			E		E

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)

ST Identification:	McAfee® Secure Content Management Appliance Version 4.0 Secure Internet Gateway (SIG)/Secure Messaging Gateway (SMG) + Secure Web Gateway (SWG) EAL 2 Security Target
ST Publication Date:	May 07, 2007
ST version number:	Version V1.1
Authors:	M. McAlister, InfoGard

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.2[1] Part 2 extended.

The TOE is Common Criteria (CC) Version 2.2 Part 3 conformant at EAL2.

The TOE is also compliant with all International interpretations with effective dates on or before June 06, 2006.

This TOE is not conformant to any Protection Profiles (PPs).

1.3 Overview

The Secure Content Management Appliance is a scalable hardware/software appliance that provides a comprehensive security solution for Internet and Email services. Through a series of security scanning, alert and configured actions and detailed content filtering options, the SCM appliance protects users and company IT resources from a variety of internet and email threats. Threats and resource liabilities such as Viruses, Spyware, Spam and Phishing attempts are identified and systematically blocked from protected IT resources. In addition, Content Filtering allows administrators to assure that inappropriate content or bandwidth usage is actively thwarted, further protecting the business from unnecessary costs or litigation.

Various hardware scalability options are available to tailor the SCM software solution to throughput requirements based on the size of the Enterprise and number of users. For small to medium sized businesses up to 1000 users, the SCM solution is implemented as the Secure Internet Gateway Appliance (SIG). This consolidated solution includes Internet and Email protection in a single appliance. For larger businesses, the SCM functionality is deployed as the Secure Web Gateway (SWG) appliance offering Internet Security features and the Secure Messaging Gateway (SMG) appliance providing Email protection features. The McAfee SCM Appliance utilizes the same software suite regardless of hardware platform selected.

[1] Common Criteria (CC) for Information Technology Security Evaluation – January 2004, Version 2.2.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet and the corresponding rationale.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE and the corresponding rationale.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides and the corresponding rationale.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.

Table 1: ST Organization and Description

1.5 Document Conventions

The CC defines four operations on security functional and assurance requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP interpretations are included in requirements, the changes from the interpretations are displayed as refinements.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***additions indicated with bold text and italics***

deletions indicated with strike-through ~~bold text and italics~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

The explicitly stated requirements claimed in this ST are denoted by the "_EXP" extension in the unique short name for the explicit security requirement.

1.6 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

1.6.1 ST Specific Terminology

Administrator	A user of the TOE appliance in the SCM Admin user role
Appliance	Within the context of this ST, the term "appliance" is synonymous with the TOE; the combination of hardware and software that is described within the TOE Boundary.
Bayesian Learning	Bayesian learning is a method of assigning scores to e-mail messages that could be spam. The TOE appliance uses Bayesian databases to calculate the probability that an e-mail message contains spam.
Blacklist	A list of e-mail addresses or domains that you create, which SpamKiller will always treat as spam. When the program detects an incoming message from an address or domain on the blacklist, it immediately assigns a very high score to that message.
Content Filtering	A process that uses rules to detect undesirable content, such as offensive words, in e-mail messages.
Denial of Service (DoS)	A means of attack, an intrusion, against a computer, server or network that disrupts the ability to respond to legitimate connection requests. A denial-of-service attack overwhelms its target with false connection requests, so that the target ignores legitimate requests.
Denied Connection	The term used by the TOE to denote traffic dropped in response to matching a Denial of Service Prevention policy as defined and configured by the TOE administrator.
Directory Harvest Attack	An attack on an email server that utilizes a script to identify and gather valid email addresses; utilized by spammers.
Explicit Proxy Mode	In Explicit Proxy mode some network devices must be set up to explicitly send traffic to the appliance. The appliance then works as a proxy, processing the traffic on behalf of these network devices.

Heuristic Analysis	A method of scanning that looks for patterns or activities that are virus-like, to detect new or previously undetected viruses.
Internal Network	Within the context of this ST, this refers to IT resources which are protected by the SCM appliance. The SCM appliance is installed between these IT resources and the WAN.
Keylogger	A computer program that captures the keystrokes of a computer user and stores them.
Network User	A remote user or process sending information to the workstation via a network protocol. This role only has the authority to Send information through the appliance from either the Internet or the internal network. Network users are unauthenticated users of the TOE.
Packers	Packers are compression tools that compress files and change the binary signature of the executable. They can be used to compress trojans and make them harder to detect.
Phishing	This category includes sites that typically arrive in hoax e-mail established only to steal users' account information. These sites falsely represent themselves as legitimate company Web sites in order to deceive and obtain user account information that can be used to perpetrate fraud or theft.
Potentially Unwanted Programs (PUPs)	A program that performs some unauthorized (and often harmful or undesirable) act such as viruses, worms, and Trojan horses.
Quarantine	Enforced isolation of a file or folder — for example, to prevent infection by a virus or to isolate a spam e-mail message — until action can be taken to clean or remove the item.
Scanning Engine	The mechanism that drives the scanning process.
Signature	The description of a virus, malware or attack methodology.
SMTP 250 command	Requested mail action okay, completed
Spam Score	A rating system used to indicate the likelihood that an e-mail message contains spam. The higher the score allocated to a message, the more likely it is to be spam.
Spyware	This category includes URLs that download software that covertly gathers

	user information through the user's Internet connection, without his or her knowledge, usually for advertising purposes. This may be considered a violation of privacy and may have bandwidth and security implications.
Transparent Mode	In either Transparent Router mode or Transparent Bridge mode the communicating devices are unaware of the intervention of the appliance — the appliance's operation is transparent to those devices.
Trojan Horse	A program that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Trojan horses are not technically viruses, because they do not replicate.
URL Filtering	A process that uses rules for blocking access to undesirable web sites on the basis of their Universal Resource Locators (URL).
Virus	A program that is capable of replicating with little or no user intervention, and the replicated program(s) also replicate further.
Whitelist	A list of e-mail addresses or domains that you create, which SpamKiller treats as non-spam. When SpamKiller detects an incoming message from an address or domain on the whitelist, it immediately assigns a very high negative score to that message.
Worm	A virus that spreads by creating duplicates of itself on other drives, systems, or networks.

1.6.2 Acronyms

CC	Common Criteria	SOF	Strength of Function
.dat	Virus Definition Data Files	SSL	Secure Socket Layer (denotes SSLv2 or SSLv3 only)
DHA	Directory Harvest Attack	SIG	Secure Internet Gateway
DoS	Denial of Service	SMG	Secure Messaging Gateway
FTP	File Transfer Protocol	SMTP	Simple Mail Transfer Protocol
HTTP	Hyper Text Transfer Protocol	SWG	Secure Web Gateway
HTTPS	Hyper Text Transfer Protocol over SSL	TOE	Target of Evaluation
ICAP	Internet Content Adaptation Protocol	TSF	TOE Security Function
POP3	Post Office Protocol 3	TSFI	TOE Security Function Interface
PUPs	Potentially Unwanted Programs	TSP	TOE Security Policy
SCM	Security Content Management	O.S.	Operating System
SFP	Security Function Policy		

2 TOE Description

2.1 Overview

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 to and from the Wide Area Network (WAN) to the internal network is first routed through the SCM Appliance where through the intercept, scanning and reporting functions, the McAfee SCM appliance can detect potentially malicious files of various types, filter traffic for restricted content, block access to restricted internet addresses (URLs) and email containing SPAM messages or Phish attempts.

Protocols included in scanning includes: HTTP, POP3, SMTP and FTP. Following detection of a potentially malicious file, the TOE can clean the affected file, delete the file, drop the associated traffic or quarantine the item pending review. The appliance also actively blocks access to restricted web sites or those containing content determined to be prohibited. The TOE provides comprehensive alerts and reports of suspicious activity to advise Administrators of traffic characteristic routed through the appliance. Scanning behavior and subsequent actions are highly configurable through a comprehensive graphic 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.

The Common Criteria Evaluation requires configuration in either Transparent Bridge or Transparent Router mode, which makes the appliance operation transparent to devices communicating through the TOE. Explicit proxy mode is not part of the Common Criteria Evaluated configuration.

2.2 Architecture Description

The McAfee SCM Appliance architecture is divided into the following sections in this ST:

- 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

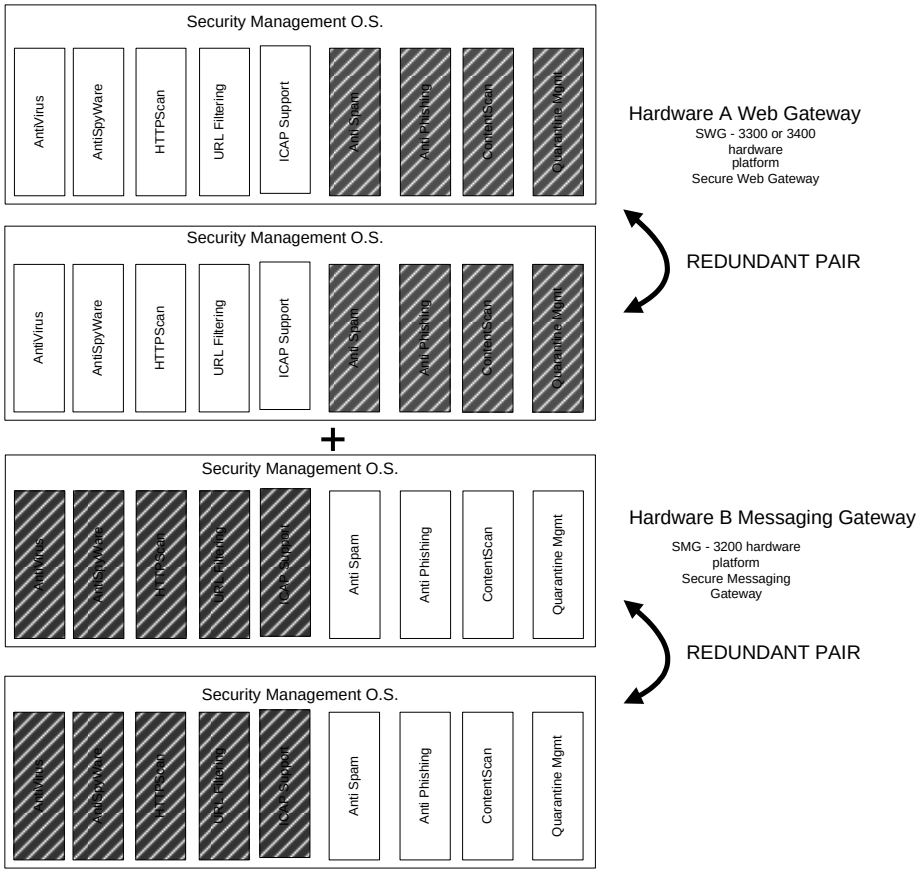

Figure 1: TOE Enterprise Option Hardware A & B combination

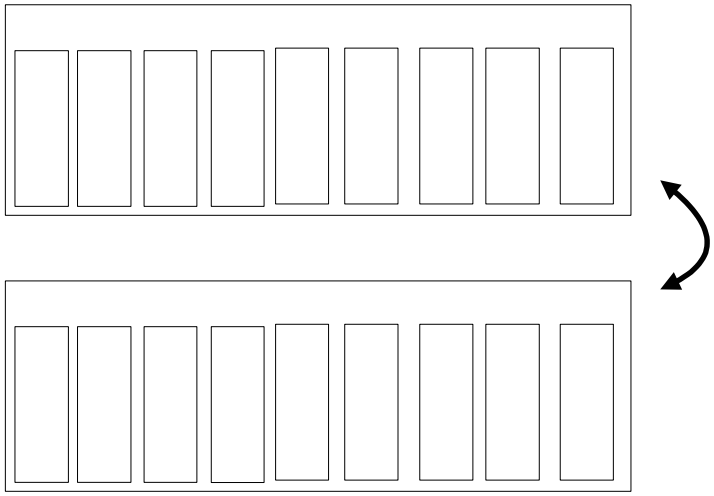

Figure 2: TOE Small Business Hardware C option

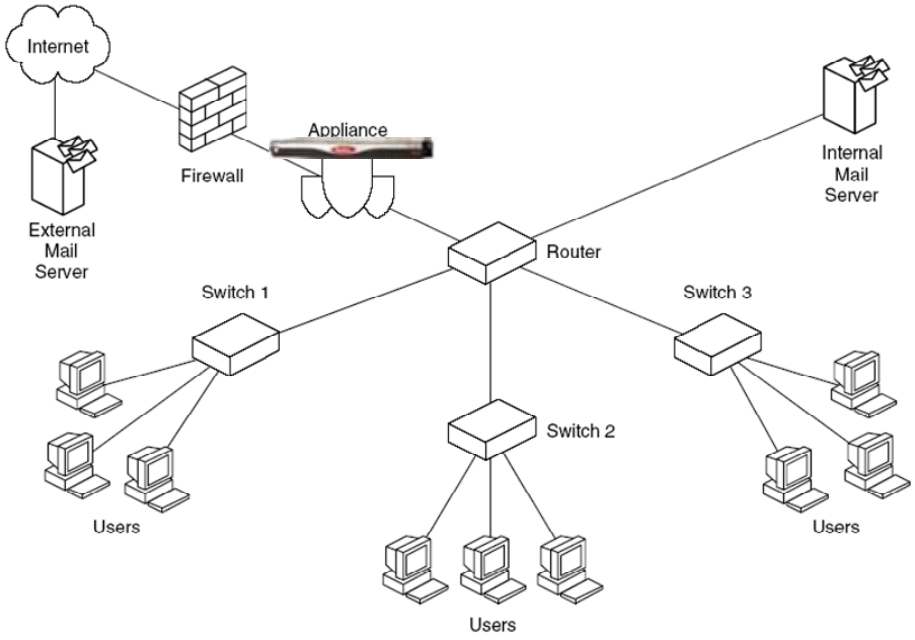

Figure 3: Architectural Diagram (network) SIG

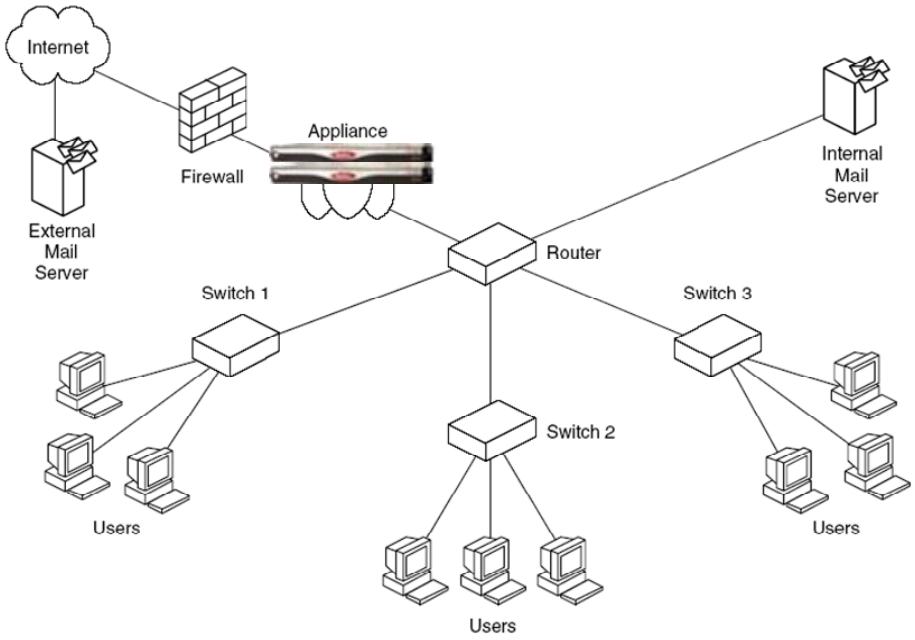

Figure 4: Architectural Diagram (network) SMG + SWG

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: TOE Enterprise Option Hardware A & B combination, the modules shown that are darkened represents modules that are disabled due to the dedicated purpose of the appliance.

2.2.1 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. The Common Criteria Evaluated configuration does not utilize the Update function to update the base Program code to preserve the core software revision used for CC. 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 utilizes heuristic analysis to evaluate files to identify potentially harmful programs that have not yet been characterized with a signature file.

2.2.2 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.

2.2.3 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.

2.2.4 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.

2.2.5 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.

2.2.6 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 is 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.

2.2.7 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.

2.2.8 ICAP support Module

ICAP support allows ICAP clients to pass HTTP messages to ICAP servers for some kind of processing or transformation (known as adaptation). This module in the TOE allows the use of an ICAP server to perform blocking or modification of HTTP requests that are presented to the appliance. The CC Evaluated configuration does not include the use of an ICAP server.

2.2.9 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.

2.2.10 SCM Security Management Operating System

2.2.10.1 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. Within this ST 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.

2.2.10.2 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. Remote administration of the McAfee SCM appliance utilizing the Remote Access Card option is not included in the CC evaluated configuration.

2.2.11 Statement of Non-Bypassibility of the TSF

TOE security functions cannot be bypassed. All access to TOE security functions requires Administrator level access 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.

2.3 Physical Boundaries

This section lists the hardware, software components and guidance documents of the product and denotes which are in the TOE and which are in the environment.

2.3.1 Hardware Components

The following table identifies the hardware components and indicates whether or not each component is in the TOE or the environment.

<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>A</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>B</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td>C</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td>D</td><td>D</td><td></td></tr>
<tr><td></td><td></td><td></td><td>E</td><td></td><td>E</td></tr>
</table>
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)
</td></tr>
<tr><td>Environment</td><td>Management Computer

Configured for Administrator access to the TOE</td><td>Requires:
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</td></tr>
<tr><td>Environment</td><td>DNS Server component</td><td>Provides DNS service to the network</td></tr>
<tr><td>Environment</td><td>Router(s)</td><td>Routers as needed for network deployment</td></tr>
<tr><td>Environment</td><td>Switch(s)</td><td>Switches as needed for network deployment</td></tr>
</table>

Table 2: Physical Scope and Boundary: Hardware

The following table illustrates the differences between the 4 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 3: Hardware Platform comparison

2.3.2 Software Components

The following table identifies the software components and indicates whether or not each component is in the TOE or the environment.

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,	Web Browser Component on Management Computer

	with ActiveX enabled	for Administrator access to TOE

Table 4: Physical Scope and Boundary: Software

2.3.3 Guidance Documents

The following guidance documents are provided with the TOE upon delivery in accordance with EAL 2 requirements:

- AGD_ADM - Administrator Guidance –
  - Secure Content Management appliances 4.0 Concepts Guide
  - Secure Content Management™ 4.0 Configuration Guide*
  - Secure Content Management appliances 4.0 Product Guide
  - Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0
- ADO_IGS –
  - McAfee SCM 3100 Installation Guide version 4.0 (English)
  - McAfee® SCM 3200 Installation Guide version 4.0 (English)
  - McAfee® SCM 3300 and SCM 3400 Installation Guide version 4.0 (English)
  - Quick Start Guide for McAfee® Secure Content Management appliances version 4.0
  - Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0

*The Secure Content Management 4.0 Configuration Guide is Not Applicable as it relates to use of the Orchestrator component which is excluded in the Common Criteria Evaluated Configuration.

All documentation delivered with the product is germane to and within the scope of the TOE as qualified by the Common Criteria document.

2.4 Logical Boundaries

This section contains the product features and denotes which are in the TOE.

Note: The Security Management O.S. supports all these functions by supporting the listed modules and providing Security Management functions to support configuration of these modules.

2.4.1 Anti-Virus

The following items make up the Anti-Virus security function:

2.4.1.1 Virus/Malware/Spyware Scanning

The McAfee SCM appliance provides comprehensive scanning capability that can be configured to identify and remove several types of Virus/Malware/Spyware. Traffic through the device is intercepted and scanned as configured prior to being forwarded to the internal network. The Anti-Virus module contains the scanning engine that is used for scanning for Viruses, Malware or Spyware. The Anti-Spyware module supports Spyware specific configuration and scanning options for both Malware and Spyware type files.

Email messages are evaluated by the Anti-Virus security function through the use of a scoring system that assigns a value to characteristics that may indicate a SPAM message. The scanning results are evaluated against a Bayesian database that uses a probability based technique to determine the likelihood that a message should be classified as SPAM.

The TOE Administrator can specify which protocol types and which ports are intercepted for scanning and can enable scanning for selected protocol types. Protocols included in scanning include: HTTP, POP3, SMTP and FTP. The Evaluated configuration requires that all protocol types are selected with scanning enabled.

Denial of Service Prevention configuration options allow administrators to set the threshold for determining when a DoS threat may be imminent and thereby drops packets to avoid exploit when the threshold is reached.

2.4.1.2 Comprehensive Traffic Scanning

The McAfee SCM TOE performs a thorough analysis of traffic routed through the appliance by implementing a module based scanning approach. Traffic is first intercepted as it traverses the appliance and it is processed for scanning. Based on protocol, specific scanning module processes are implemented to scan for various malicious file types, restricted content or access requests to restricted web site locations. The HTTP Scanning module provides the functionality used for traffic scanning. Denial of Service (DoS) attacks can also be identified and thwarted through the scanning function of the McAfee SCM appliance.

Protocols included in scanning include: HTTP, POP3, SMTP and FTP. All traffic types traversing the appliance are subject to scanning as configured for scanning by the TOE Administrator.

2.4.1.3 Alerts

The TOE utilizes policies that enforce action to be taken for specified events. Based on the

configuration of these policies, alerts may be specified that will notify the Administrator via email of events that match the parameters of the policy.

Alerts can be configured for specific Viruses/Malware/Spyware identified in scanning, content filtering events, and/or for identified behavior patterns seen in traffic analyzed that could be indicative of a network attack, such as a Denial of Service attempt. Alerts are supported by the SCM operating system and security management support provided by the O.S.

2.4.2 ID and Authentication

The McAfee SCM TOE requires that administrators of the TOE are identified and authenticated prior to gaining access to TSF data. Traffic through the device is evaluated based on the core functionality of the TOE, however, the network users of the traffic which travels through the appliance do not directly interact with the TOE appliance. These network users are only identified by the appliance by IP address, referring URL or email address. The TOE is transparent to network users passing traffic through the appliance.

The SCM Operating System supports the identification and password based authentication and requires that Administrators submit username and password prior to gaining access to the TOE appliance.

The SCM Appliance provides role based access controls to allow appliance administrators (SCM Admin) to establish multiple roles with configurable access options to assist in managing various functions within the appliance.

The TOE supports the use of external authentication servers such as LDAP, however, the use of external authentication servers is not included in the evaluated configuration.

2.4.3 Filtering

The Administrator can configure Content Scanning and Filtering to be applied to intercepted traffic to identify or restrict access where content matches prohibited characteristics, based on Administrator configured rules. The scanning engine can identify content within email messages or traffic that may be objectionable and pose risks to the operational environment. The Content Scan module and URL Filtering Module supports this functionality in conjunction with the HTTP scan module. These rules can be developed by the TOE Administrator based on protocol used, header layout, file type and/or keywords to quarantine or drop traffic or files based on the rule configured.

URL Filtering can also be configured to restrict access to URLs based on Administrator configurable rules. URL information is maintained in a database stored locally on the TOE that can be periodically updated based on new URL data.

2.4.3.1 Email Protection

The McAfee SCM TOE provides for full scanning of email traffic through the device to identify SPAM messages and Phishing attempts. Administrator configured rule sets are established within the appliance to set thresholds for which messages are identified as suspicious and deleted

or forwarded to a quarantine location. The Quarantine process functionality is provided by the Quarantine Management module. Evaluation of messages for characteristics that may indicate a Phish attempt is provided by the Anti-Phishing module. In addition, Administrator defined blacklists and whitelists allow administrators to set certain messages for immediately delivery (whitelist) or quarantine/deletion based on sender information. Through the "SPAMKiller" features set, Phish-attempts are thwarted through a series of configurable identifiers that assist administrators, in detecting and acting upon, fraudulent messages or information harvest attempts. The SPAMKiller feature set is provided by the functionality of the Anti-Spam module working in conjunction with the Quarantine Management module.

2.4.4 Action and Remediation

The TOE can be configured to take specific action upon identification of a Virus/Malware/Spyware when scanning traffic. Actions can eliminate the identified file entirely, attempt to clean the file from the payload, or provide only a notification that a potential Virus/Malware/Spyware has been identified. Various options are available for administrator configuration that specifies the actions to be taken for a variety of events. Cleaning actions are supported by the respective Anti-Virus or Anti-Spyware modules in conjunction with the SCM operating system management features.

2.4.5 Cryptographic Operations

When downloading updated Virus/Malware/Spyware signature files the McAfee SCM TOE performs MD5 hash message digest verification for signature files to ensure authenticity and file integrity. This functionality is supported by the core McAfee SCM operating system.

Administrator sessions with the McAfee SCM appliance are conducted through an Internet Explorer browser session from the Administrator management computer secured via SSLv2 or SSLv3 security protocols. These sessions are encrypted using RC4 (or) DES (or) 3DES (or) AES cryptographic algorithms and cryptographic key sizes 56 bits or greater (128 RC4).

Cryptography used within the TOE is not validated to the Federal Information Processing Standards (FIPS) requirements.

***note: Cryptographic functionality correctness represented by these claims and algorithm usage is based on McAfee assertion of product usage.**

2.4.6 Audit

The McAfee SCM TOE supports full logging of all Administrator actions that result in changes to the TSF. In addition, detailed audit logs are produced that identify TSF activities, traffic scans competed, Viruses/Malware/Spyware identified, actions taken and updates made to Virus/Malware/Spyware .dat signature files. Audit generation and related audit security functions are provided by the SCM Operating System. Audit Management features are provided

within the product software to allow for detailed review of audit records. There is also a provision within the TOE for exporting log records to an external server; however, this option is not included in the Common Criteria Evaluated Configuration.

2.4.7 Security Management

The Management interface provided by the TOE for administration requires only the use of Microsoft Internet Explorer 5.5, 6.0 or later on the administrator workstation through a configured HTTPS network management connection to the appliance. The administration of the TOE requires the use of an Administrator management computer and the specified Microsoft Internet Explorer browser with Active-X enabled. The Administrator management computer is only used for input and display purposes, the functions discussed herein are all implemented on the SCM TOE Appliance. The SCM Operating System provides the Management functions and coordinates with associated function-related module to provide configuration settings and actions.

Remote administration of the TOE is supported with the addition of remote access cards for Enterprise level deployments; however, the evaluated configuration does not include this option.

Access to Administrator functions and TSF resources within the SCM appliance requires identification by username and authentication through the SCM Appliance operating system enforced password.

An SCM client application is available that provides a Java based GUI Administrator interface to the appliance, however, this is not included in the Common Criteria Evaluated configuration in lieu of the browser based option described above.

2.4.8 Protection of TOE Functions

The McAfee SCM TOE provides protection to prevent unauthorized access to the TSF and prevent bypass of security functionality. Administrator access can only be gained through successful SSL session negotiation (Browser access). TSF access requires the Administrator to be positively identified by username and authenticated through the Administrator password.

The use of a firewall in conjunction with the McAfee SCM TOE is recommended, however, is not part of the evaluated configuration and is not required to meet the Security Functional Requirements claimed in this Security Target.

2.5 Items Excluded from the TOE

This section identifies any items that are specifically excluded from the TOE.

- 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 CC Evaluated configuration does not include the use of an ICAP server
- CLI usage except for initial installation of the CCE Compliant Installation Pack Installation – SCM Appliance version 4.0.

3 TOE Security Environment

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the IT environment.

3.1 Assumptions

The assumptions are ordered into three categories: personnel assumptions, physical environment assumptions, and operational assumptions.

3.1.1 Personnel Assumptions

A.ADMIN	The Administrators of the TOE are assumed to be non-hostile, competent, trustworthy and to follow the guidelines supplied in guidance documentation.

3.1.2 Physical Environment Assumptions

A.LOCATE	The TOE is assumed to be located in a Server Room location providing physical protection and limited (Administrator only) access.

3.1.3 Operational Assumptions

A. DEDICATED	The McAfee SCM Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.
A.NO_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
A.SEC_UPDATES	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.
A.NO_MALW	The administrator management computer used for remote security management purposes is assumed to be free from malware or other malicious software.

3.2 Threats

The TOE or IT environment addresses the threats identified in this section. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

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.

3.3 Organizational Security Policies

There are no Organizational Security Policies for this TOE.

4 Security Objectives

This chapter describes the security objectives for the TOE and the IT environment. The security objectives are divided between TOE Security Objectives (for example, security objectives addressed directly by the TOE) and Security Objectives for the IT Environment (for example, security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

O.AUDIT_GEN	The TOE creates audit records of security relevant events associated by user which caused the event.
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information
O.AUDIT_STOR	The TOE will provide a means for secure storage of the TOE audit log files.
O.CRYPT	The TOE shall use a cryptographic hash function to secure signature data files during transit.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the Administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MAL_CONTENT	The TOE shall provide the capability to block access to specific URL addresses through the device based on the Network Policy configured by the Administrator and to scan email traffic to detect and initiate actions to prevent transmission or delivery of restricted content.
O.RESOURCE_X	The TOE shall provide mechanisms that mitigate attempts to exhaust connection-oriented resources provided by the TOE.
O.TOE_ACCESS	The TOE will provide mechanisms that control administrator logical access to the TOE.
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the Administrator to set the time used for these time stamps.

O.SELF_PROT	The TSF will maintain logical domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.
O.SECURE_CHK	The TOE will detect and take action against viruses, malware, spyware, phish attempts and SPAM to protect network resources and block attempts to compromise network resources and/or to attack other network nodes or deny service.

4.2 Security Objectives for the Environment

The non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE (i.e., through procedural or administrative means):

OE.ADMIN	Sites using the TOE will ensure that the authorized administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow all administrative guidance.
OE.DEDICATED	Administrators will assure that the McAfee SCM Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.
OE.NO_BYPASS	The IT environment will ensure that the Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.NO_MALW	Administrators will assure that the administrator management computer used for remote security management purposes is free from malware or other malicious software.
OE.SEC_UPDATES	Sites using the TOE will ensure that authorized administrators will enable signature file updates when available to keep file signatures used for scanning current.
OE.LOCATE	Physical Security will be provided including a secure location for the TOE and related assets commensurate with the value of those assets.

4.3 Mapping of Threats to IT Security Objectives

The following table represents a mapping of the threats and assumptions to the security objectives defined in this ST.

	A.ADMIN	A.DEDICATED	A.LOCATE	A.NO_BYPASS	A.NO_MALW	A.SEC_UPDATES	T.AUDIT_COMP	T.BAD_DAT	T.MASQUERADE	T.MAL_CONTENT	T.MAL_MSG	T. RESOURCE_X	T.FLAW_CONFIG	T.UNID_ACTION	T.MAL_AGENT
O.AUDIT_GEN														☑	
O.AUDIT_PROTECT							☑								
O.AUDIT_REVIEW														☑	
O.AUDIT_STOR														☑	
O.CRYPT								☑							
O.MANAGE													☑		
O.MAL_CONTENT										☑	☑				
O.TIME_STAMPS														☑	
O.TOE_ACCESS									☑						
O.RESOURCE_X												☑			
O.SELF_PROT									☑						
O.SECURE_CHK															☑
OE.ADMIN	☑														
OE.DEDICATED		☑													
OE.LOCATE			☑												
OE.NO_BYPASS				☑											
OE.NO_MALW					☑										

	A.ADMIN	A.DEDICATED	A.LOCATE	A.NO_BYPASS	A.NO_MALW	A.SEC_UPDATES	T.AUDIT_COMP	T.BAD_DAT	T.MASQUERADE	T.MAL_CONTENT	T.MAL_MSG	T. RESOURCE_X	T.FLAW_CONFIG	T.UNID_ACTION	T.MAL_AGENT
OE.SEC_UPDATES						☑									

Table 5: Threats & IT Security Objectives Mappings

4.4 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.AUDIT_COMP O.AUDIT_PROTECT mitigates this threat by restricting access to audit records to authorized personnel.

T.BAD_DAT O.CRYPT mitigates this threat by providing for a message digest verification utilizing a cryptographic function.

T.UNID_ACTION O.AUDIT_GEN mitigates this threat by creating audit record data for any changes to TSF related functions and/or security related events. O.AUDIT_REVIEW mitigates this threat by providing resources for reviewing and sorting audit data, supporting the administrator's ability to detect potential security violations. O.AUDIT_STOR mitigates this threat by storing all audit record outputs from the TOE relating to security function related events within the TOE and making these logs available for review. O.TIME_STAMPS support the audit function by providing an accurate time stamp for audit records generated within the TOE.

T.MAL_AGENT O. SECURE_CHK further mitigates this threat by assuring that the TOE will detect and take action against known viruses and/or identified malicious software introduced to the appliance via network traffic.

T.MASQUERADE O.TOE_ACCESS mitigates this threat by providing mechanisms that control an administrator's logical access to the TOE. O.SELF_PROT mitigates this threat by providing TOE mechanisms that protects against external interference, tampering, or unauthorized disclosure through secure communication methods, domain separation and assuring that TSP enforcement mechanisms succeed prior to granting access to TSF resources.

T. MAL_CONTENT	O. MAL_CONTENT mitigates this threat by providing mechanisms that block prohibited URL addresses through the device.
T.MAL_MSG	O. MAL_CONTENT mitigates this threat by providing mechanisms that detect and take action to prevent prohibited content from being sent or received through email resources.
T.FLAW_CONFIG	O.MANAGE mitigates this threat by providing the functions and facilities necessary to support the Administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
T.RESOURCE_X	O.RESOURCE_X mitigates this threat by providing mechanisms within the TOE to identify and block or prevent Denial of Service attempts on the TOE appliance or protected resources.

4.5 Rationale For Organizational Policy Coverage

There are no Organizational Policies for this TOE.

4.6 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

A.ADMIN	This assumption is addressed in OE.ADMIN which ensures that the authorized administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow all administrative guidance.
A.DEDICATED	This assumption is restated in the form of OE.DEDICATED, assuring that the McAfee SCM Appliance is dedicated to its primary function.
A.LOCATE	This is assured through OE.LOCATE which assures that the TOE is deployed in a secure location for the TOE and related assets, commensurate with the value of those assets.
A.NO_BYPASS	OE.NO_BYPASS ensures that Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

A.NO_MALW	OE.NO_MALW ensures that the administrator management computer used for remote security management purposes is free from malware or other malicious software.
A.SEC_UPDATES	OE.SEC_UPDATES supports this assumption by stipulating that the Administrator will enable signature file updates when available to keep file signatures used for scanning current.

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST. These security requirements are defined in Sections 5.1 – 5.9.

TOE Security Functional Requirements (from CC Part 2)	
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User Identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1a	Selective audit – Protocol & Communication Events
FAU_SEL.1b	Selective audit – Detection Events
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1a	Cryptographic Key Generation – Administrator Sessions
FCS_CKM.1b	Cryptographic Key Generation – Asymmetric Keys
FCS_CKM.1c	Cryptographic Key Generation – Symmetric Keys
FCS_COP.1a	Cryptographic operation - .dat file verification
FCS_COP.1b	Cryptographic operation-Administrator Sessions
FCS_COP.1c	Cryptographic operation- Random Number Generator
FCS_COP.1d	Cryptographic operation- Diffie-Hellman
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_SOS.1	Verification of Secrets
FMT_MOF.1a	Management of security functions behaviour
FMT_MOF.1b	Management of security functions behaviour
FMT_MSA.2	Secure Security Attributes

FMT_MTD.1a	Management of TSF data
FMT_MTD.1b	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
FTA_SSL.3	TSF – initiated Termination
Explicitly Stated TOE Security Functional Requirements	
FSN_ACT_EXP.1	SCAN Actions
FSN_SCN_EXP.1	SCAN Operate
FSN_SAA_EXP.1	Real-Time Traffic Monitor

Table 6: Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.1.1 Class FAU: Security Audit

5.1.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take **action to notify the SCM Admin via email and generate an audit record** upon detection of a potential security violation.

5.1.1.2 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the not specified level of audit; and
c) Additional Events:

- **Success/Failure of Login to SCM Appliance User Interface**

- **Success/Failure of SCM Appliance Configuration Changes**
- **Identification of Virus/malware/spyware detection events**
- **Identification of SPAM/Phish detection events**
- **Identification of Directory Harvest detections**
- **Network level communication events**
- **Protocol processing events**
- **Unsuccessful attempts to Scan traffic or message**
- **Action Taken to remove or mitigate virus/malware/spyware**
- **Detection of Banned Content**
- **Identification of Banned URLs blocked**
- **Blocking of email messages**
- **Hardware/Software appliance settings incl. TSF settings**
- **.dat Updates**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **Logged data listed in Table 7: Audit Record logged events**

Identification	Subject	Description	Outcome	Logged Data	Security Attributes
User IP Address	Scanning Process	*Identification of Virus/malware/spyware Files	Success (Identification)	Virus/malware/spyware ID, Location	Detection Status
User IP Address	Scanning Process	*Unsuccessful attempts to Scan traffic or message	Failure (Scanning unsuccessful)	Identification of failed filename, email	Detection Status
User IP Address	Remediation Process	Action Taken to remove or mitigate virus/malware/spyware	Success, Failure (removal, mitigation)	Action taken, Result	Mitigation Status
User IP Address	Scanning Process	*Detection of Banned Content	Success, Failure (removal, mitigation)	Action taken, Result, Rule matched	Detection Status
User IP Address	Scanning Process	*Identification of Banned URLs blocked	Success, Failure (Blocking)	User Identification, URL (site location), Number of attempts to access	Detection Status
User IP Address	Scanning Process	*Blocking of email messages	Success, Failure (Blocking)	Sender/Recipient identification, Rule matched	Detection Status
Admin Username	TOE Administrator	TSF settings	Success, Failure (setting	Administrator logon to interface, TSF settings accessed/changes	TOE Configuration Status

	Configuration		changes)	made	
Admin Username	Update Process	.dat Updates	Success, Failure (updates installed)	Update filename installed, location of installation	Update Status
User IP Address	Protocol Scanning Process	Protocol Events created	Event results	Event details based on High, Mid, or all Events settings	Protocol Event Status

Table 7: Audit Record logged events

*indicates potential TSP violation events as described in FSN_SAA_EXP.1, Real-Time Traffic Monitor

5.1.1.3 FAU_GEN.2 User Identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity ***(IP Address or Username)*** of the user that caused the event.

5.1.1.4 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **SCM Admin** with the capability to read **audit information listed in** Table 7: Audit Record **logged** events**, including associated date/time stamps** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.5 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.6 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform searches, sorting of audit data based on Keyword (search), **Report Type, Date Range.**

5.1.1.7 FAU_SEL.1a Selective audit – Protocol & Communication Events

FAU_SEL.1.1a The TSF shall be able to include or exclude auditable events from the set

of audited events based on the following attributes:

a) event type

b) TSF rated severity of event – High Severity, Mid & High Severity, All, Off

5.1.1.8 FAU_SEL.1b Selective audit – Detection Events

FAU_SEL.1.1b The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type

b) **specific sub event type – AntiVirus, AntiSpam & Phish, Content Filter, other**

5.1.1.9 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

5.1.1.10 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **email the TOE Administrator (SCM Admin)** if the audit trail exceeds **75%, 90% of partition space allocated for audit logs**.

5.1.1.11 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall ignore auditable events and **generate an email to the SCM Admin** if the audit trail is full.

5.1.2 Class FCS: Cryptographic Functions*

5.1.2.1 FCS_CKM.1a Cryptographic key generation-Administrator Sessions

FCS_CKM.1.1a The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic

key sizes **RSA with key lengths of 1024** that meet the following: **PKCS #1.**

5.1.2.2 FCS_CKM.1b Cryptographic Key Generation – Asymmetric Keys

FCS_CKM.1b The TSF shall generate **Diffie-Hellman asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **a software random number generator (SHA-1, MD5 OpenSSL/OpenSSH based)** and specified cryptographic key sizes **default 1024 bits and maximum 4096 bits** that meets the following **none**.

5.1.2.3 FCS_CKM.1c Cryptographic Key Generation –Symmetric Keys

FCS_CKM.1c The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **a software random number generator (OpenSSL based)** and specified cryptographic key sizes **minimum 56 bits, (128 bits, RC4)** that meets the following **none**.

5.1.2.4 FCS_COP.1a Cryptographic operation - .dat file verification

FCS_COP.1.1a The TSF shall perform **calculate a message digest to verify the integrity of the signature files** in accordance with a specified cryptographic algorithm **MD5** and cryptographic key sizes (**not applicable**) that meet the following: **RFC 1321**.

Application Note: Message digests use hash functions, which do not have keys. Therefore, the assignment related to the cryptographic key size has been set to "not applicable".

5.1.2.5 FCS_COP.1b Cryptographic operation – Administrator Sessions

FCS_COP.1.1b The TSF shall perform **Administrator Session Encryption/Decryption** in accordance with a specified cryptographic algorithm **RC4 (or) DES (or) 3DES (or) AES** and cryptographic key sizes **56 bits or greater (128 RC4)** that **meet the following: RFC 4345 (RC4), RFC 2405(DES), FIPS 46.3 (3DES), RFC 3364 (AES).**

5.1.2.6 FCS_COP.1c Cryptographic operation - Random Number Generator

FCS_COP.1.1c The TSF shall perform **OpenSSL based pseudo random number generation functions** in accordance with a specified cryptographic algorithm **SHA, MD5** and cryptographic key size **not applicable** that meet the following **none.**

5.1.2.7 FCS_COP.1d Cryptographic operation – Diffie-Hellman

FCS_COP.1.1d The TSF shall perform **OpenSSL based Asymmetric Key Generation** in accordance with a specified cryptographic algorithm **Diffie-Hellman (Ephemeral-Ephemeral)** and cryptographic key size **default 1024 bits and maximum 4096 bits** that meet the following **none**.

***note: Cryptographic functionality correctness represented by these claims and algorithm usage is based on McAfee assertion of product usage.**

5.1.3 Class FIA: Identification and authentication

5.1.3.1 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.2 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

5.1.3.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **Administrator configured Password Management settings – 4 characters minimum and must contain either alphanumeric characters or special characters.**

5.1.4 Class FMT: Security management

5.1.4.1 FMT_MOF.1a Management of security functions behaviour

FMT_MOF.1.1a The TSF shall restrict the ability to modify the behaviour of, determine the behaviour of, disable, enable the functions:

a) Appliance audit logging

b) Real-time virus scanning

c) Enable and disable operation of the appliance

d) Update virus scan signatures

e) Acknowledge alert notifications from the appliance

to **the SCM Admin.**

5.1.4.2 FMT_MOF.1b Management of security functions behaviour

FMT_MOF.1.1b The TSF shall restrict the ability to modify the behaviour of, determine the behaviour of**,** the functions

a) Operational mode selection

b) Protocol Configuration

c) Content, Connection, Protocol Policies

d) Configure traffic scanning options on the appliance

to **the SCM Admin.**

5.1.4.3 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.4.4 FMT_MTD.1a Management of TSF data

FMT_MTD.1.1a The TSF shall restrict the ability to query, delete, the

a) Actions to be taken on traffic when a virus, Malware, SPAM, Spyware, Packers, Prohibited Content, Phishing Attempts or PUPs is detected,
b) Protocols to be intercepted and scanned automatically on the appliance,
c) Virus/Malware/Spyware scan signatures, and
d) Audit logs
e) Network Policy

to **the SCM Admin.**

5.1.4.5 FMT_MTD.1b Management of TSF data

FMT_MTD.1.1b The TSF shall restrict the ability to modify, the

a) Actions to be taken on traffic when a virus, Malware, SPAM, Spyware, Packers, Prohibited Content, Phishing Attempts or PUPs is detected,
b) Protocols to be intercepted and scanned automatically on the appliance,
c) Virus/Malware/Spyware scan signatures,
d) Audit settings
e) Scanning Options
f) Network Policy

to **the SCM Admin.**

5.1.4.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a. Enable and disable operation of the appliance

b. Configure traffic scanning options on the appliance

c. Update virus scan signatures

d. Acknowledge alert notifications from the appliance

e. Actions to take upon identification of a threat

f. Content filter settings incl. URL addresses

g. Query, Delete, Configure audit logs

5.1.4.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: **SCM Admin.**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Class FPT: Protection of the TSF

5.1.5.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

5.1.5.2 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **a single Message Authentication Code (MAC) error during transmission.**

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **resending of transmitted data** if modifications are detected.

5.1.5.3 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.4 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.5 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.6 Class FTA: TOE Access

5.1.6.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **15 Minutes.**

5.2 Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

5.2.1 Class FSN: SCAN functions (Explicit Class)

5.2.1.1 FSN_ACT_EXP.1 SCAN Actions

FSN_ACT_EXP.1.1 Upon detection of a file-based virus, the TSF shall perform the action(s) specified by the SCM Admin. Actions are administratively configurable on a per-Appliance basis and consist of:

a) Clean the virus from the file

b) Quarantine the file

c) Delete the file,

d) Protocol Specific Actions as specified in Table 8: Protocol Specific SCAN actions (as configured).

FSN_ACT_EXP.1.2 Upon detection of Malware, SPAM, Spyware, Packers, Prohibited Content, Phishing Attempts or PUPs the TSF shall perform the action(s) specified by the SCM Admin. Actions are administratively configurable on a per-Appliance basis and consist of: a) Protocol Specific Actions as specified in **Table 8: Protocol Specific SCAN actions (as configured)**.

Protocol	Primary Action taken (original)	Secondary Action taken (additional or copies)
(required settings for Common Criteria Evaluated Configuration)		
SMTP Scan	☒Accept and then drop the data	☒Deliver an annotated modified E-mail to a GUI defined recipient
POP3	☒Replace the content with an HTML alert	
HTTP	☒Delete the file and insert an HTML alert in it's place	
FTP	☒Refuse the original data (The file is rejected)	

Table 8: Protocol Specific SCAN actions (as configured)

5.2.1.2 FSN_SCN_EXP.1 SCAN Operate

FSN_SCN_EXP.1.1 The TSF shall perform real-time network traffic scans for viruses based upon known signatures and heuristic methods.

FSN_SCN_EXP.1.2 The TSF shall perform real-time network traffic scans for Malware, Spyware, SPAM, Phish attempts, Packers, Prohibited Content and PUPs based upon known signatures and heuristic methods.

FSN_SCN_EXP.1.3 The TSF shall filter URL addresses based on settings established by the SCM Admin, and thereby prevents access by users of the internal network to specified URLs/IP addresses through the SCM TOE appliance.

5.2.1.3 FSN_SAA_EXP.1 Real-Time Traffic Monitor

FSN_SAA_EXP.1.1 The TSF shall apply a set of rules in monitoring network traffic and based upon these rules indicate a potential violation of the TSP.

FSN_SAA_EXP.1.2 The TSF shall enforce the following rules for monitoring network traffic events:

a) Accumulation or combination of events as depicted ("*") in **Table 7: Audit Record logged events,** known to indicate a potential TSP violation, upon which an email is generated to the SCM Admin and an audit event is logged.

5.3 TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in the product are the password mechanism used to authenticate users and the cryptographic mechanisms. Strength of cryptographic algorithms is outside the scope of the Common Criteria.

The claimed minimum strength of function is SOF-basic. FIA_UAU.2 (authentication password) is the only non-cryptographic TOE security functional requirements that contain a permutational or probabilistic function.

The rationale for choosing SOF-basic is based on the low to moderate attack potential of the threats identified in this ST. While the TOE may be deployed in environments where WAN traffic is routed to internal network servers at a substantial rate, the TOE appliance is transparent to traffic users. Since the TOE appliance is transparent to these users and scanning functions are managed separately from TSF data (i.e.: Security Management functions), the attack potential of the TOE itself is considered to be low to moderate, therefore, leading to a basic strength of function claim.

5.4 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 as defined by the CC. The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design

Assurance Class	Assurance Components	
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance*
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 9: Assurance Requirements: EAL2

*Note: Product usage is transparent to network users therefore this requirement (AGD_USR.1) requirement is vacuously satisfied (ref: PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied)

5.4.1 ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.3 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.4.4 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages,

as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

5.4.5 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.6 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.7 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.8 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.9 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.10 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.11 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.4.12 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each

mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.4.13 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.5 Rationale For TOE Security Requirements

5.5.1 TOE Security Functional Requirements

	O.AUDIT_GEN	O.AUDIT_PROTECT	O. AUDIT_REVIEW	O.AUDIT_STOR	O.CRYPT	O.MANAGE	O.MAL_CONTENT	O.TIME_STAMPS	O.TOE_ACCESS	O.RESOURCE_X	O.SELF_PROT	O.SECURE_CHK
FAU_ARP.1												X
FAU_GEN.1	X											
FAU_GEN.2	X											
FAU_SAR.1			X									
FAU_SAR.2		X										
FAU_SAR.3			X									
FAU_SEL.1a	X											
FAU_SEL.1b	X											
FAU_STG.1				X								
FAU_STG.3			X									
FAU_STG.4			X									
FCS_CKM.1a					X							
FCS_CKM.1b					X							
FCS_CKM.1c					X							
FCS_COP.1a					X							
FCS_COP.1b					X							
FCS_COP.1c					X							
FCS_COP.1d					X							
FIA_UAU.2									X			
FIA_UID.2									X			
FIA_SOS.1									X			

	O.AUDIT_GEN	O.AUDIT_PROTECT	O. AUDIT_REVIEW	O.AUDIT_STOR	O.CRYPT	O.MANAGE	O.MAL_CONTENT	O.TIME_STAMPS	O.TOE_ACCESS	O.RESOURCE_X	O.SELF_PROT	O.SECURE_CHK
FMT_MOF.1a						X						
FMT_MOF.1b						X						
FMT_MSA.2					X							
FMT_MTD.1a						X						
FMT_MTD.1b						X						
FMT_SMF.1						X						
FMT_SMR.1						X						
FPT_ITC.1											X	
FPT_ITI.1											X	
FPT_RVM.1											X	
FPT_SEP.1											X	
FPT_STM.1								X				
FTA_SSL.3									X			
FSN_ACT_EXP.1							X			X		X
FSN_SCN_EXP.1							X			X		X
FSN_SAA_EXP.1												X

Table 10: SFR and Security Objectives Mapping

Security Objective	Mapping Rationale
O.AUDIT_GEN	FAU_GEN.1 specifies that the TOE generates audit records of security relevant events and information that audit records must contain. FAU_GEN.2 is selected to ensure that the audit records associate a network user identity with the event audited. FAU_SEL.1a specifies the audit log selection options for Protocol and Communication Events.

	FAU_SEL.1b specifies the audit log selection options for Detection Events.
O.AUDIT_PROTECT	FAU_SAR.2 ensures that audit records are protected from access by unauthorized personnel. Only authorized administrators may access TOE audit records. FAU_STG.3 specifies that the TOE will send emails to the SCM Admin upon reaching 75% and 90% of allocated space for audit logs. FAU_STG.4 specifies that the TOE will ignore audit records and email the SCM Admin when the allocated space on the appliance is exhausted.
O.AUDIT_REVIEW	FAU_SAR.1 is selected to specify that the TOE has provisions for the review of audit records for administrator review. FAU_SAR.3 is selected to specify that the TOE has provisions for selective review of audit records.
O.AUDIT_STOR	FAU_STG.1 ensures that the TOE provides for the storage of audit data in a manner that protects the data from unauthorized deletion and prevent unauthorized modification of TOE audit records.
O.CRYPT	FCS_COP.1a specifies that the TOE utilizes a cryptographic hash function to verify the integrity of .dat signature files. FCS_COP. b,c,d specifies the cryptographic algorithms and key sizes to be used for securing Administrator sessions. FCS_CKM.1a,b,c, specifies the key generation techniques and algorithms used for securing Administrator sessions. FMT_MSA.2 specifies that only secure values will be accepted for use by the TOE in support of cryptographic operations.
O.MANAGE	FMT_MOF.1a, FMT_MOF.1b provides that the TOE's management function can only be accessed and utilized by authorized personnel. FMT_MTD.1a, FMT_MTD.1b specifies the TSF data that can be queried, modified or deleted by use of the TOE's management functions. FMT_SMR.1 defines the roles provided by the TOE. FMT_SMF.1 specifies the management functions supported by the TOE.
O.MAL_CONTENT	FSN_SCN_EXP.1 specifies that the TOE provides scanning capability to detect prohibited content or prohibited URLs and FSN_ACT_EXP.1 specifies that the TOE takes actions upon detection of prohibited content and blocks prohibited URLs.
O.TIME_STAMPS	FPT_STM.1 specifies that the TOE provides accurate time stamps for use in audit records.
O.TOE_ACCESS	FIA_UID.2 specifies that the TOE requires identification before allowing access to TSF resources. FIA_UAU.2 specifies that the TOE requires authentication before allowing access to TSF resources. FTA_SSL.3 specifies that the TSF will log Administrator out (end session) after 15 minutes of inactivity. FIA_SOS.1 specifies that the TOE provides a mechanism to verify that secrets (passwords) are at least 4 characters including must contain either alphanumeric characters or special characters.

O.RESOURCE_X	FSN_SCN_EXP.1 specifies that traffic scanning activities are conducted that protect the TSF from Denial of Service threats by proactively identifying traffic attributes that are indicative of a resource exhaustion attempt. FSN_ACT_EXP.1 takes actions based on threats identified including blocking or dropping packets once a resource exhaustion attempt has been identified to protect the TSF and connected resources within the IT Environment.
O.SELF_PROT	FPT_SEP.1 specifies that the TOE will provide a secure domain for its execution and will enforce separation between subjects in the TSC. FPT_RVM.1 specifies that the TSF ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_ITC.1 specifies that the TOE will provide protection for TSF data from disclosure during data transfers to remote Trusted IT products. FPT_ITI.1 specifies that the TOE will detect modification during TSF data transfers to remote trusted IT products and take action upon detection of modification.
O.SECURE_CHK	FSN_SCN_EXP.1 specifies that the TOE will provide a scanning function used to detect viruses, spyware, malware or spam. FSN_ACT_EXP.1 specifies that the TOE takes specified actions to remediate the event identified in FSN_SCN_EXP.1. FAU_ARP.1 specifies that the TOE will provide alerts to the TOE administrator in the case an identified file has been detected. FSN_SAA_EXP.1 specifies that the TOE provides the capability to intercept and scan network traffic in real time in order to identify and take action on specified file types.

5.5.2 TOE Security Assurance Requirements

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

5.6 Rationale for Explicitly Stated Security Requirements

Table 11: Explicitly Stated SFR Rationale, presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FSN_ACT_EXP.1	SCAN Actions	This component defines the actions to be taken by the TOE when a viruses/spyware/malware is detected. Existing security policy SFRs (e.g., FDP_ACF and FDP_IFF) focus on the access to or flow of user data and are not suitable for the actions taken by Anti-Virus products.

Explicit Requirement	Identifier	Rationale
FSN_SCN_EXP.1	SCAN Operate	This component defines the scanning to be performed by the TOE to detect viruses/spyware/malware. Existing security policy SFRs (e.g., FDP_ACF and FDP_IFF) focus on the access to or flow of user data and are not suitable for the mechanisms used by Anti-Virus products.
FSN_SAA_EXP.1	Real-Time Traffic Monitor	This component defines the monitoring process that occurs through intercept of traffic on a real time basis. This explicit is necessary due to the fact that it is a real time function and not the result of audit records review - the TOE intercepts, scans and then passes the data; and generates an alarm (real time) based on this real time eval.

Table 11: Explicitly Stated SFR Rationale

5.7 Rationale For IT Security Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies that are not satisfied.

Functional Component	Dependency	Included/Rationale
FAU_ARP.1	FAU_SAA.1	Yes* via FSN_SAA_EXP.1
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1a	FAU_GEN.1, FAU_MTD.1	Yes
FAU_SEL.1b	FAU_GEN.1, FAU_MTD.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.3	FAU_STG.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_COP.1a,b,c,d	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	No, FCS_CKM.4
FCS_CKM.1a,b,c	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	Yes

Functional Component	Dependency	Included/Rationale
FIA_UAU.2	FIA_UID.1	Yes
FIA_UID.1	None	Yes
FIA_SOS.1	None	Yes
FMT_MOF.1a	FMT_SMF.1, FMT_SMR.1	Yes
FMT_MOF.1b	FMT_SMF.1, FMT_SMR.1	Yes
FMT_MSA.2	FDP_IFC.1, FMT_MSA.1 FMT_SMR.1	No, FDP_IFC.1, FMT_MSA.1
FMT_MTD.1a	FMT_SMF.1, FMT_SMR.1	Yes
FMT_MTD.1b	FMT_SMF.1, FMT_SMR.1	Yes
FMT_SMF.1	None	Yes
FMT_SMR.1	FIA_UID.1	Yes
FPT_ITC.1	None	Yes
FPT_ITI.1	None	Yes
FPT_RVM.1	None	Yes
FPT_SEP.1	None	Yes
FPT_STM.1	None	Yes
FTA_SSL.3	None	Yes
FSN_ACT_EXP.1	FSN_SCN_EXP.1, FMT_SMR.1	Yes
FSN_SCN_EXP.1	None	Yes
FSN_SAA_EXP.1	None	Yes

Table 12: SFR Dependencies

5.7.1 Rationale for Unsatisfied Dependencies

The following security requirements are depended upon by the security requirements for the TOE, yet were not included within this ST. These requirements and their justification is provided below.

FAU_ARP.1	FAU_SAA.1	The Explicit SFR: FSN_SAA_EXP.1 is modeled after FAU_SAA.1 and satisfies the dependency of FAU_SAA.1 on FAU_ARP.1.

FMT_MSA.2	FMT_MSA.1	FMT_MSA.2 was added to relate only to the use of secure cryptographic related security attributes. The appliance does not mediate information flow but rather scans traffic as it flows through the device – once completed, traffic continues as originally routed to the internal network.
FMT_MSA.2	FDP_IFC.1	FMT_MSA.2 was added to relate only to the use of secure cryptographic related security attributes. The appliance does not mediate information flow but rather scans traffic as it flows through the device – once completed, traffic continues as originally routed to the internal network.

Table 13: Rationale for Dependencies not met

5.8 Rationale for Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes all the SFRs provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in **Table 12: SFR Dependencies**
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.5
- including the SFRs FTA_SSL.3, FPT_RVM.1 and FPT_SEP.1 to protect the TSF
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely

5.9 Rationale for Strength of Function Claim

The rationale for choosing SOF-basic is based on the low to moderate attack potential of the threats identified in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE.

As noted in Section 5.3:

The rationale for choosing SOF-basic is based on the low to moderate attack potential of the threats identified in this ST. While the TOE may be deployed in environments where WAN traffic is routed to internal network servers at a substantial rate, the TOE appliance is transparent to traffic users. Since the TOE appliance is transparent to these users and scanning functions are managed separately from TSF data (i.e.: Security Management functions), the attack potential of the TOE itself is considered to be low to moderate, therefore, leading to a basic strength of

function claim.

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of 8 Security Functions:

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

6.1.1 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. The SCM Appliance is positioned in the network architecture to assure that all traffic routed through the device to the internal network and traffic from the internal network to external addresses is scanned by the TOE. The appliance first intercepts the traffic through a kernel extension within the underlying Operating System, and then passes the traffic to the core application where it is evaluated against configured scanning rules for the type of traffic/content intercepted. Based on these scanning rules, specific portions of the traffic are routed to the Scanning Engine where it is scanned and returned to the application along with the result. The content is then reconstructed and forwarded to the internal network destination.

The TOE can identify Viruses, Malware, or Spyware that is included in traffic passing through the device. This security function also works with other security functions by providing the scanning and files identification process. The TOE is configured to identify specific actions to be taken upon detection of a suspect file. In all cases when a suspect file or activity is detected, the TOE Administrator is notified by an email alert and an audit log entry is made (FAU_GEN.1).

Scanning levels can be set on the TOE based on security level desired:

- High — Most secure. Scans all files, including compressed files.
- Medium — Scan executables, Microsoft Office files, and compressed files.

- Low — Least secure. Scans executables and Microsoft Office files.
- Custom — Administrator chooses which types of file to scan and a range of scanning options.

The Custom option allows for scanning specific files types or a custom list of files and locations.

The TOE Administrator (SCM Admin) can specify which protocol types and which ports are intercepted for scanning and can enable scanning for selected protocol types. The Common Criteria Evaluated configuration stipulates that all protocols are enabled for scanning.

FSN_SCN_EXP.1 – Anti-Virus Scanning Processes

The McAfee SCM TOE performs traffic scanning in real time as traffic traverses the device. The TOE uses signature based detection methods that evaluates traffic for characteristics of known malicious files/data types. The types of data included in the scanning process includes Viruses, Malware, PUPs, Packers and Spyware that may be either embedded in legitimate files or be stand-alone code.

The scanning process also supports email system scanning that can identify Phish attempts and file attachments that may contain prohibited content or SPAM. SPAM detection utilizing the Anti-Virus scanning security function coordinates with Bayesian databases to assign scores to email characteristics based on Administrator configured rules. The Bayesian process evaluates the scoring to determine the likelihood that the message is SPAM as opposed to an email from a legitimate sender.

Heuristic based scanning is also employed within the TOE to identify files or malicious program data types that might not have signature files established but reveal a characteristic that may pose a threat to the network. Heuristic scanning employs additional scanning techniques that evaluate characteristics beyond .dat signatures and known profiles of Viruses, Malware etc. The use of heuristic scanning may be only enable or disabled; no configuration options are available. This feature is contained within the AntiVirus subsystem and is supported by the SCM Operating System subsystem in section SCM Security Management Operating System.

HTTP traffic scanning can be configured to scan various components of HTTP traffic such as headers, message bodies, and cookies.

Denial of Service attempts can be detected during the scanning process by identifying if the size of the header exceeds a pre-defined limit or the header line count exceeds a pre-defined limit. The administrator may also configure the appliance to close a connection if one or more of the following conditions occur:

- The average data throughput (message min. size setting) over a set interval is less

than a pre-defined value.

- The number of commands received before the appliance receives a successful DATA command is exceeded.
- The maximum command length permitted by the RFC standard is exceeded.
- The length of the SMTP conversation (defined as the time between the opening of the connection and receiving the final dot (.) command) exceeds a pre-set time.

The appliance can also identify a possible DoS attack and close the connection if:

- The AUTH phase of a communication exceeds a pre-defined limit (Transparent Bridge mode only).
- The maximum number of recipients allowed is exceeded. The appliance can sends the SMTP failure response and delay the response by a set amount of time.

When these limits are exceeded or requirements met, action is taken to prevent a DoS attack as described in Section 6.1.4.

FAU_ARP.1 – Security Alarms

The TOE generates alarms through email notifications to the Administrator for specified events in order to allow analysis to determine if a potential TSF violation has been detected. This functionality is supported through the scanning function (FSN_SCN_EXP.1) which scans traffic as it traverses through the appliance. Based on the events that trigger security alarms, data is provided for analysis and based on the rule set established in FSN_SAA_EXP.1 leads to specified alerts and actions.

Minimum events that generate security alarms include:

- Identification of Virus/Malware/Spyware files
- Unsuccessful attempts to Scan traffic or message
- Detection of Banned Content
- Identification of Banned URLs blocked
- Blocking of email messages
- Resource allocations becoming exhausted

FSN_SAA_EXP.1 –Traffic Monitoring Rules – Violation of the TSP

The TOE utilizes administrator configurable settings that can characterize how the TOE detects and reacts to events that may be potential violations of the TOE Security Policy. This includes

settings that specify the content and depth of what to scan and the specifications for what constitutes a violation event. For example, SPAM messages are specified based on a scoring system and the administrator determines the cumulative numerical value which indicates a notification event (email or annotation) vs. a remediation event such as blocking or deletion. In general, these settings specify the detection types, to which the action will apply and the actions that the TOE applies upon detection. These settings are applied while the appliance is monitoring traffic. These configuration settings are saved to an allocated location within the SCM Operating System. For each type of event that the appliance can detect, threshold settings are established by the administrator to indicate when the event has occurred and the appropriate action to take.

The monitoring of the TOE through FSN_SAA_EXP.1 is differentiated from scanning in that in that it applies settings and rules to the data that is scanned, applies a measure and determines when a specified event has occurred and what action to take. In contrast, Scanning (FSN_SCN_EXP.1) is the process by which the appliance intercepts traffic and applies detection rules to simply identify a target characteristic. FSN_SAA_EXP.1 provides input to FAU_ARP.1 as to when to generate an email alert.

Upon a security alarm as detailed in FAU_ARP.1, evaluation and configured action is conducted by the TOE. Once a potential violation of the TSF has been detected based on configured settings, the TOE generates an email alert to the Administrator and creates an audit record (FAU_GEN.1) of the event.

The following events at a minimum qualify as potential violation event and trigger an alert within the TOE to the Administrator (SCM Admin role):

- Identification of Virus/Malware/Spyware files
- Unsuccessful attempts to Scan traffic or message
- Detection of Banned Content
- Identification of Banned URLs blocked
- Blocking of email messages
- Resource allocations becoming exhausted

The actions taken by the TOE upon detection of files through the Anti-Virus are described in the Action and Remediation Security Function described in Section 6.1.4.

6.1.2 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. The User Interface for this purpose is provided by an Apache Web Server running within the SCM Operating System environment. The computer used for this purpose can be a general purpose machine running Microsoft Internet Explorer 5.5, 6.0 or

later with Secure Sockets Layer (SSL) v2 or v3 encryption, with ActiveX enabled.

FIA_UID.2, FIA_UAU.2 - Identification and Authentication

Administrators gain access to the TOE appliance by opening a secure browser session using HTTPS on the Administrator Management Computer. The SCM Operating System performs the Administrator authentication process. Upon entering the IP address of the TOE appliance, the administrator receives a logon dialog presented by the Apache web server component. The SCM Admin enters the applicable username and password, the password is hashed and compared with hashed password values within the TOE appliance database resource within the underlying operating system. If the hashed values match, then the SCM Admin is authenticated. The password mechanism utilized satisfies the Strength of Function claim of SOF-Basic. Communication between the Administrator Management Computer and TOE Appliance is secured via SSL.

FIA_SOS.1 - Verification of passwords

The password authentication mechanism is realized by a probabilistic or permutational security mechanism. By default, the McAfee TOE appliance requires that passwords used for TSF access contain greater than or equal to 4 characters and must contain either alphanumeric characters or any of the following special characters: ! @ # $ % ^ & * ( ) - +. This is enforced by the TOE through software based technical means within the appliance; only passwords which match the above policy will be accepted by the SCM appliance.

6.1.3 Filtering

The Filtering security function of the McAfee SCM appliance utilizes the core scanning capability described in the Anti-Virus security function to identify suspect email messages and/or email attachment and take specified action upon detection of restricted content. Content scanning scans email for indicators of restricted content, as specified by the administrator. URL filtering restricts access to URLs that may contain restricted data or meet restricted criteria as configured by the administrator.

FSN_SCN_EXP.1 – Content Scanning and URL Filtering

The Administrator can configure Content Scanning and Filtering to be enabled for scanned file types and to detail policies for handling of specified email file types. Content Scanning can also be extended to attachments contained in email messages.

URL Filtering can be configured to restrict access to URLs based on Administrator configurable rules. URL information is maintained in a database that can be periodically updated based on new URL data. Various reports are available to Administrators (SCM Admin) to view the URL requests that the TOE has blocked or filtered.

Email protection through the Filtering security function

The McAfee SCM TOE provides for full scanning of email traffic through the device to identify

SPAM messages and Phishing attempts. The Filtering security function interacts with various TOE modules to identify email attachments that may pose a risk to the internal network and filter them from traffic within the appliance.

Once files or data has been identified as potential SPAM or Phish attempts, they may be forwarded to a pre-configured quarantine location in order to assure Administrators can review them to assure they are safe prior to allowing them to be routed to the applicable destination.

6.1.4 Action and Remediation

FSN_ACT_EXP.1 – Actions taken upon detection

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. If cleaning of the detected virus is selected, the action is taken within the scanning engine. All other remediation activities, occur within the core SCM application. The McAfee SCM TOE has various settings that can be configured by the TOE Administrator to initiate specific actions to be taken based on the type of malicious file detected. These can be based on the traffic type, file type or classification within the TOE based on the file's signature or behavior. Upon detection of a file based virus the TOE Appliance can clean the file, quarantine the file, delete the file or take one of the following actions based on the protocol type:

- SMTP Accept and then drop the data; Deliver an annotated modified E-mail to the SCM Admin
- POP3 Replace the content with an HTML alert
- HTTP Delete the file and insert an HTML alert in its place
- FTP Refuse the original data (The file is rejected)

HTTP Traffic Scan actions

HTTP traffic that has an identified threat may be acted upon by:

- Replacing content with an HTML alert; effectively deleting the threat and notifying the recipient
- Allow through – typically for temporary use if a specific file type is expected that will trigger alerts. The events will be logged but the content not blocked or modified.

Content/URL Filtering Actions

For detections relating to Content and URL filtering, the available actions include the blocking of the URL or Content that matches the rules.

Spam messages can be rerouted, deleted or marked based on scoring parameters set by the TOE administrator.

Denial of Service Protection

If a Denial of Service (DoS) attack is identified, based on the configured Denial of Service Prevention policy, the connection will be dropped to prevent the threat. This is referred to in the TOE as a Denied Connection. The TOE administrator establishes this protection by configuring the appliance to not accept any new connections from the same address for a set period of time.

6.1.5 Cryptographic Operations*

The only cryptographic operations within the TOE are the verification process for downloaded .dat threat signature files. These files are verified for integrity using an MD5 hash function during the download and install process.

FCS_COP.1a - .dat file Message Digest verification

The threat signature files are used by the McAfee scanning engine in security function – Anti-Virus to identify potential malicious files and software. The characteristics of these known files or signatures are regularly updated to assure the latest threats are included in the scanning process. During the download process to the TOE Appliance these files utilize a 128 bit Hash cryptographic function utilizing the MD5 algorithm to assure that the files are unmodified, authentic and properly downloaded to the TOE.

Securing Administrator GUI browser sessions - FCS_COP.1b, FCS_COP.1c, FCS_COP.1d, FCS_CKM.1a, b, c

Administrator access to the SCM TOE is secured by through SSL sessions. Only HTTPS sessions are allowed for this purpose. The TOE utilizes the mod_ssl module within the Apache Web Server which hosts the GUI to provided cryptographic support for these sessions. Algorithm and key pairs used for these sessions are contained within OpenSSL libraries which mod_ssl accesses during session initiation. These open source modules are part of the SCM Operating System construct described within this ST. In order to successfully authenticate and create a session with the SCM appliance GUI the user must be properly authenticated by the underlying Operating System as described in ID and Authentication. The SCM appliance through its OpenSSL implementation supports the Cipher Suites listed in Appendix A for use in securing Administrator sessions with the TOE over HTTPS.

Administrative session keys are generated using an OpenSSL based software pseudo-random number generator which produces Diffie-Hellman asymmetric keys and symmetric keys based on the key pair definitions listed within Appendix A.

This represents the minimum for secure values accepted for SSL session negotiation with the management computer in the IT Environment.

*note: Cryptographic functionality correctness represented by these claims and algorithm usage is based on McAfee assertion of product usage.

6.1.6 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. The administrator accesses audit records through the administrator GUI console interface and can view audit records, delete audit records, perform keyword searches, sort records and create customized reports detailing security related event detected and action upon by the McAfee Appliance. Records are logged by network user information and contain details on traffic type, protocol in use; rule violated indicating a security event and the outcome of the event. Access to audit logs is restricted to authenticated administrators through the authentication mechanisms detailed in section 6.1.2.

FAU_GEN.1, FAU_GEN.2 – Audit Generation

The TOE generates audit records for the following events:

- Success/Failure of Login to SCM Appliance User Interface
- Success/Failure of SCM Appliance Configuration Changes
- Identification of Virus/malware/spyware detection events
- Identification of SPAM/Phish detection events
- Identification of Directory Harvest detections
- Network level communication events
- Protocol processing events
- Unsuccessful attempts to Scan traffic or message
- Action Taken to remove or mitigate virus/malware/spyware
- Detection of Banned Content
- Identification of Banned URLs blocked
- Blocking of email messages
- Hardware/Software appliance settings incl. TSF settings
- .dat Updates
- Activation or de-activation of the audit function

All Administrator changes to the TSF, including changes to security attributes, are reflected in audit records and can only be accessed by the authorized TOE administrator (SCM Admin) which is protected by the SCM Appliance Operating System.

Audit records include the network user and session attributes in use at the time of the logged event.

Selectable Audit – FAU_SEL.1a, FAU_SEL.1b

The TOE allows configuration of the audit generation function which specifies the type of events

and the level of logging to be implemented. For audit records relating to Protocol and Communication logs, the SCM Admin may configure that the TOE log High Severity events, Mid & High Security Events, All events or OFF (no events logged). For audit records relating to Detection Events, the SCM Admin may select any or all of the following events to be logged: AntiVirus, AntiSPAM & Phish, Content Filter, Other.

FPT_STM.1 – Audit records by accurate time stamps

An internal clock is provided within the McAfee SCM Appliance to provide a time reference for use by the TOE in recording accurate audit logs by the time of the event.

FAU_STG.1, FAU_STG.3, FAU_STG.4 – Storage and Protection of Audit Records

Audit records are stored within the McAfee SCM appliance through the use of a SQL compliant, open source object-relational database management system used within the McAfee SCM software. Audit logs are protected from access, deletion and modifications by the access control functionality described in the ID and Authentication section above. Only the Administrator (SCM Admin) may access appliance audit records. The SCM Appliance allocates 15 GB for audit log storage. The Administrator (SCM Admin) may configure two levels at which an email alert is send to the SCM Admin warning of a specified value of resource exhaustion. Also configurable is aging of audit records in days, where a "days old" value is set for audit records that, when reached, results in deletion of those audit records by the TSF. Alternatively, the SCM Admin may specify the value manually by entering "purge logs older than "X" days and pressing the purge logs button. By default, an email is sent when allocated logging resources used reach the 75% and 90% level. When the allocated space within the appliance is reached, audit events are no longer logged. If the audit trail becomes full, an email is sent to the SCM Admin for notification.

FAU_SAR.1, FAU_SAR.2, FAU_SAR.3 – Audit Review

The McAfee SCM appliance provides the Administrator full audit access through a Apache web server based GUI interface within the appliance to access audit records and activity logs for analysis. Access to read or search audit records are restricted to Administrators. The appliance allows searching based on keyword entered and/or sorting of audit records based on Report Type and Date Range.

Report Generation

Audit log data can be compiled by the TOE into a report format to support the review of events based on category of event. This detailed reporting capability allows administrators to customize

reports based on various characteristics of event types and actions taken. The TOE categorizes events using the following descriptors to assist in reporting:

Resource and System:	Network User and Network User Interface Events, Hardware and Resources Events Updates, Load Sharing and Bridging Events created, Mail digests Events.
Protocol:	Communication between the appliance and the clients/servers. Processing Events created by processing protocols, SMTP Transport Events
Communications:	Network Events created in network level communications. Scanner - If any of the scanning engines cannot scan an object.
Detection:	Virus Events, Content Events, Spam, URLs blocked, SMTP blocked, Actions taken.

6.1.7 Security Management

The McAfee SCM TOE provides security management functions and tools to manage the security features described within this security target. 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. Configuration data managed through this security function is managed and stored in the file system supported by the underlying SCM Operating System. Administrator access to the TOE is managed within the internal network via a web browser over a HTTPS protocol connection. The TOE enforces Identification and Authentication prior to allowing access to TOE Security Management functions.

FMT_SMR.1 Role Based Access

The TOE supports role based access to the SCM appliance through a single Administrator role of SCM Admin . No additional roles or users may be configured on the appliance, the SCM Admin is the only role provided.

FTA_SSL.3 TSF-initiated termination

Administrative access to the TOE is established using the administrative management computer via a supported web browser using an SSL session. The Administrator Management session may be closed manually by the Administrator through a logoff button on the GUI. To maintain security during management sessions, the session also automatically closes after an Administrator specified term of inactivity. The default setting enforces termination of sessions after 15 minutes of inactivity.

FMT_SMF.1 - Management Functions provided by the TOE

Various types of alerts can be configured by TOE Administrators to execute actions and notify administrators via email of security related events detected by the SCM appliance. Through this GUI based interface, administrators can acknowledge notification of events and actions taken to mitigate the identified file. Core TOE management functions include:

- Enable and disable operation of the appliance
- Configure traffic scanning options on the appliance
- Update virus scan signatures
- Acknowledge alert notifications from the appliance
- Actions to take upon identification of a threat
- Content filter settings incl. URL addresses
- Manage audit logs

Management of the TOE and Restrictions – FMT_MTD.1a, FMT_MTD.1b

Various operational modes and protocol configuration options can also be established through the management GUI that determine how the appliance intercepts traffic and integrates into the network architecture. Administrators with the SCM Admin role may also utilize the appliance management function to manage and update virus signature files that are used for scanning of traffic to specific malicious file structure characteristics.

The McAfee SCM appliance console allows the SCM Admin to configure and manage the audit/logging function, including searching and sorting of audit data and generation of reports based on various log parameters. The management GUI also allows administrators (SCM admin) to establish scanning options for traffic based on types of malicious files detected, traffic protocols and message header attributes.

Various policies can be established by the Administrator through the management GUI. These policies can define scanning options based on scan, connection and protocol type.

The TOE management function includes the ability to create events that initiate action based on prerequisites set configured by the administrator. Action taken by the TOE, through these Events, relating to a potentially malicious file or traffic indicator is configurable through the security management function.

The ability to query, delete or modify these security management functions of the TOE are restricted by the TSF to Administrators holding the SCM Admin role, properly authenticated by the SCM operating system.

FMT_MOF.1a, FMT_MOF.1b – TSF Control Over Management Functions

The TOE restricts the ability to access the Management GUI through the SCM operating system access controls. Administrator level access with the SCM Admin role is required to read, modify or enable/disable TOE Management functions. The TOE provides management functions that allow authorized administrators to enable or disable the Auditing and Scanning related functions. In addition, the TSF limits the ability to determine or modify the behavior of the auditing, scanning, operational mode, protocol configuration and policies that direct content, connection and protocol behavior to the SCM Admin. These limitations are supported by restricting Management GUI access as described in ID & Authentication in Section 6.1.2.

6.1.8 Protection of TOE Functions

FPT_SEP.1 - Domain Separation & FPT_RVM.1 - Non-bypassibility of the TSP

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 controls restrict TSF access to Administrators only.

The SCM Operating System and SCM Application subsystems provide separation between traffic intercepted and scanned by the device from TSF configuration data and settings which require SCM Admin level access. Administrative sessions are conducted over HTTPS and the HTTPS protocol is not scanned as part of traffic scanning, therefore the handling of these sessions and management within the appliance are discrete and separate.

In addition, actions taken on traffic flowing through the device by the TOE, such as scanning, are not run as the privileged root user.

FPT_ITC.1, FPT_ITI.1 – Protection of TSF data transfer during Administrator sessions

The TOE uses HTTPS for administrative management sessions to the Administrator Management Computer to protect the confidentiality of TSF data during transfer. This is supported by the Apache web server that hosts the Administrator Web GUI. SSL functionality is provided through the mod_ssl module within Apache working with OpenSSL libraries. The Administrative management computer communicates over the network to access the Administrator GUI and through the use of SSL session management, changes are detected if a single MAC authentication error is received and upon detection of modification, the message is requested to be resent.

6.2 Security Assurance Measures

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

Assurance Requirement	Assurance Components
ACM_CAP.2	The description of the configuration items is provided in McAfee Secure Content Management Appliance Version 4.0 EAL 2 Configuration Management Documentation Revision 1.0
ADO_DEL.1	The description of the delivery procedures is provided in McAfee Secure Content Manager Delivery Procedures For Common Criteria Document Number: 530-0001-01.0
ADO_IGS.1	The installation, generation, and start-up procedures are provided in: McAfee® SCM 3200 Installation Guide version 4.0 (English) McAfee® SCM 3300 and SCM 3400 Installation Guide version 4.0 (English) Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0
ADV_FSP.1	The informal functional specification is provided in EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Version 4.0 Version 1.0
ADV_HLD.1	The descriptive high-level design is provided in EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Version 4.0 Version 1.0
ADV_RCR.1	The informal correspondence demonstration is provided in EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Version 4.0 Version 1.0
AGD_ADM.1	The administrator guidance is provided in the following documents: Secure Content Management appliances 4.0 Concepts Guide Secure Content Management™ 4.0 Configuration Guide Quick Start Guide for McAfee® Secure Content Management appliances ver. 4.0 Secure Content Management appliances 4.0 Product Guide Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0 Version 1.0
AGD_USR.1	N/A – The only authenticated users of the TOE are Administrator's therefore User Guidance separate from Admin. Guidance is not provided.
ATE_COV.1	The evidence of coverage is provided in EAL 2 Tests Activity ATE McAfee® Secure Content Management Appliances Version 1.0
ATE_FUN.1	The functional testing description is provided in EAL 2 Tests Activity ATE McAfee® Secure Content Management Appliances Version 1.0
ATE_IND.2	The TOE and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_SOF.1	The strength of function analysis performed is provided in 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) Version 1.0

Assurance Requirement	Assurance Components
AVA_VLA.1	The vulnerability analysis performed is provided in McAfee® Secure Content Management Appliance Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2 Version 1.0

Table 14: Assurance Requirements: EAL2

6.3 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 6.1.

	Anti-Virus	ID and Authentication	Filtering	Action and Remediation	Cryptographic Operations	Audit	Security Management	Protection of TOE Functions
FAU_ARP.1	X							
FAU_GEN.1						X		
FAU_GEN.2						X		
FAU_SAR.1						X		
FAU_SAR.2						X		
FAU_SAR.3						X		
FAU_SEL.1a						X		
FAU_SEL.1b						X		
FAU_STG.1						X		

	Anti-Virus	ID and Authentication	Filtering	Action and Remediation	Cryptographic Operations	Audit	Security Management	Protection of TOE Functions
FAU_STG.3						X		
FAU_STG.4						X		
FCS_CKM.1a					X			
FCS_CKM.1b					X			
FCS_CKM.1c					X			
FCS_COP.1a					X			
FCS_COP.1b					X			
FCS_COP.1c					X			
FCS_COP.1d					X			
FIA_UAU.2		X						
FIA_UID.2		X						
FIA_SOS.1		X						
FMT_MOF.1a					X		X	
FMT_MOF.1b							X	
FMT_MSA.2					X			
FMT_MTD.1a							X	
FMT_MTD.1b							X	
FMT_SMF.1							X	
FMT_SMR.1							X	
FPT_ITC.1								X

	Anti-Virus	ID and Authentication	Filtering	Action and Remediation	Cryptographic Operations	Audit	Security Management	Protection of TOE Functions
FPT_ITI.1								X
FPT_RVM.1								X
FPT_SEP.1								X
FPT_STM.1						X		
FTA_SSL.3							X	
FSN_ACT_EXP.1				X				
FSN_SCN_EXP.1	X		X					
FSN_SAA_EXP.1	X							

Table 15: TOE Security Function to SFR Mapping

6.4 Appropriate Strength of Function Claim

The claim of SOF-basic for the Identification and Authentication security function is consistent with the claim of SOF-basic for the FIA_UAU.2 (authentication password) SFR that maps to that security function.

6.5 Rationale for Security Assurance Measures

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_CAP.2	McAfee Secure Content Management Appliance Version 4.0 EAL 2 Configuration Management Documentation Rev. 1.0	The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.
ADO_DEL.1	The description of the delivery procedures is provided in McAfee Secure Content Manager Delivery Procedures For Common Criteria Version 1.0	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer.
ADO_IGS.1	McAfee® SCM 3200 Installation Guide version 4.0 (English) McAfee® SCM 3300 and SCM 3400 Installation Guide version 4.0 (English) Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0 Version 1.0	The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.1	EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Version 4.0 Version 1.0	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADV_HLD.1	EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Version 4.0 Version 1.0	The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	EAL 2 Design Documentation McAfee® Secure Content Manager Appliance Version 4.0 Version 1.0	The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.
AGD_ADM.1	a. Secure Content Management appliances 4.0 Concepts Guide b. Secure Content Management™ 4.0 Configuration Guide c. Quick Start Guide for McAfee® Secure Content Management appliances ver. 4.0 d. Secure Content Management appliances 4.0 Product Guide e. Common Criteria Supplement EAL2 McAfee® Secure Content Manager Appliance Version 4.0	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	*N/A*	N/A – The only authenticated users of the TOE are Administrator's therefore User Guidance separate from Admin. Guidance is not provided.
ATE_COV.1	EAL 2 Tests Activity ATE McAfee® Secure Content Management Appliances Version 1.0	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_FUN.1	EAL 2 Tests Activity ATE McAfee® Secure Content Management Appliances Version 1.0	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	EAL 2 Test Activity ATE McAfee Secure Content Management Appliances Version 1.0	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.

Assurance Requirement	Assurance Measures	Assurance Rationale
AVA_SOF.1	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) Version 1.0	The strength of function analysis document provides the SOF argument for the password mechanism.
AVA_VLA.1	McAfee® Secure Content Management Appliance Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2 Version 1.0	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 16: Rationale for Security Assurance Measures

7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

8 Rationale

This Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

Sections 4.3 - 4.6 provide the security objectives, threats and assumptions rationale.

8.2 Security Requirements Rationale

Sections 5.5 - 5.9 provide the security requirements and strength of function rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provide the TOE summary specification and Security Measures rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.

9 Appendix A – OpenSSL Ciphers available for use in securing Adminstrator GUI sessions.

The SCM appliance support usage of any SSLv2, SSLv3 or TLS cipher suites supported by OpenSSL for securing Administrator GUI sessions.

CIPHER SUITE NAMES

The following lists give the SSL or TLS cipher suites names from the relevant specification and their OpenSSL equivalents. The SCMAppliance utilizes OpenSSL for generation of SSL session keys.

SSL v3.0 cipher suites.

SSL or TLS cipher suites names	OpenSSL equivalents
SSL_RSA_WITH_NULL_MD5	NULL-MD5
SSL_RSA_WITH_NULL_SHA	NULL-SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
SSL_RSA_WITH_RC4_128_MD5	RC4-MD5
SSL_RSA_WITH_RC4_128_SHA	RC4-SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5
SSL_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
SSL_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	Not implemented.
SSL_DH_DSS_WITH_DES_CBC_SHA	Not implemented.
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA	Not implemented.
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	Not implemented.
SSL_DH_RSA_WITH_DES_CBC_SHA	Not implemented.
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA	Not implemented.
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-CBC-SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA

SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	EXP-ADH-RC4-MD5
SSL_DH_anon_WITH_RC4_128_MD5	ADH-RC4-MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	EXP-ADH-DES-CBC-SHA
SSL_DH_anon_WITH_DES_CBC_SHA	ADH-DES-CBC-SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA	Not implemented.
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA	Not implemented.
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA	Not implemented.

TLS v1.0 cipher suites

TLS_RSA_WITH_NULL_MD5	NULL-MD5
TLS_RSA_WITH_NULL_SHA	NULL-SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
TLS_RSA_WITH_RC4_128_MD5	RC4-MD5
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	Not implemented.
TLS_DH_DSS_WITH_DES_CBC_SHA	Not implemented.
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Not implemented.
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	Not implemented.
TLS_DH_RSA_WITH_DES_CBC_SHA	Not implemented.
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	Not implemented.
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-CBC-SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	EXP-ADH-RC4-MD5
TLS_DH_anon_WITH_RC4_128_MD5	ADH-RC4-MD5
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	EXP-ADH-DES-CBC-SHA
TLS_DH_anon_WITH_DES_CBC_SHA	ADH-DES-CBC-SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA

Additional Export 1024 and other cipher suites

Note: these ciphers can also be used in SSL v3.

TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DES-CBC-SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	EXP1024-RC4-SHA
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DHE-DSS-DES-CBC-SHA
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA	EXP1024-DHE-DSS-RC4-SHA
TLS_DHE_DSS_WITH_RC4_128_SHA	DHE-DSS-RC4-SHA

SSL v2.0 cipher suites.

SSL_CK_RC4_128_WITH_MD5	RC4-MD5
SSL_CK_RC4_128_EXPORT40_WITH_MD5	EXP-RC4-MD5
SSL_CK_RC2_128_CBC_WITH_MD5	RC2-MD5
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	EXP-RC2-MD5
SSL_CK_IDEA_128_CBC_WITH_MD5	IDEA-CBC-MD5
SSL_CK_DES_64_CBC_WITH_MD5	DES-CBC-MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5	DES-CBC3-MD5

