McAfee® Email and Web Security Appliance Version 5.5 Patch 2 EAL 2 + ALC_FLR.2 Security Target

Release Date:	22 July 2010
Document ID:	
Version:	DRAFT 0.12

Prepared By:	Primasec Ltd.

Prepared For:	McAfee Inc. 3965 Freedom Circle Santa Clara, CA 95054

Table of Contents

1 INTRODUCTION 5
1.1 IDENTIFICATION 5
1.1.1 TOE Identification 5
1.1.2 ST Identification 5
1.2 TOE OVERVIEW 5
1.3 DOCUMENT CONVENTIONS 6
1.4 DOCUMENT TERMINOLOGY 6
1.4.1 ST Specific Terminology 6
1.4.2 Acronyms 8
1.5 TOE DESCRIPTION – OVERVIEW 10
1.6 ARCHITECTURE DESCRIPTION 10
1.6.1 Anti-Virus Module 12
1.6.2 PUP Module 13
1.6.3 Anti-Phishing Module 13
1.6.4 Anti-Spam Module 13
1.6.5 URL Filtering Module 14
1.6.6 Content Scan Module 14
1.6.7 Quarantine Management Module 14
1.6.8 ICAP support Module 15
1.6.9 HTTP Scan Module 15
1.6.10 EWS Security Management Operating System 15
1.7 STATEMENT OF NON-BYPASSIBILITY OF THE TSF 16
1.8 PHYSICAL BOUNDARIES 16
1.8.1 Hardware Components 16
1.8.2 Software Components 18
1.8.3 Guidance Documents 19
1.9 LOGICAL BOUNDARIES 20
1.9.1 Anti-Virus 20
1.9.2 ID and Authentication 21
1.9.3 Filtering 21
1.9.4 Email protection 22
1.9.5 Action and Remediation 22
1.9.6 Cryptographic Operations 22
1.9.7 Audit 22
1.9.8 Security Management 22
1.10 ITEMS EXCLUDED FROM THE TOE 23
2 CC CONFORMANCE CLAIM 24
3 TOE SECURITY PROBLEM DEFINITION 25
3.1 ASSUMPTIONS 25
3.1.1 Personnel Assumptions 25
3.1.2 Physical Environment Assumptions 25
3.1.3 Operational Assumptions 25
3.2 THREATS 25
3.3 ORGANIZATIONAL SECURITY POLICIES 26

4 SECURITY OBJECTIVES 27
4.1 SECURITY OBJECTIVES FOR THE TOE 27
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 28
4.3 MAPPING OF THREATS TO SECURITY OBJECTIVES 28
4.4 RATIONALE FOR THREAT COVERAGE 30
4.5 RATIONALE FOR ORGANIZATIONAL SECURITY POLICY COVERAGE 30
4.6 RATIONALE FOR ASSUMPTION COVERAGE 31
5 IT SECURITY REQUIREMENTS 32
5.1 EXTENDED COMPONENTS DEFINITION 33
5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS 35
5.2.1 Class FAU: Security Audit 35
5.2.2 Class FCS: Cryptographic Functions 38
5.2.3 Class FIA: Identification and authentication 38
5.2.4 Class FMT: Security management 38
5.2.5 Class FPT: Protection of the TSF 40
5.2.6 Class FTA: TOE Access 40
5.3 EXPLICITLY STATED TOE SECURITY FUNCTIONAL REQUIREMENTS 40
5.3.1 Class FDP: User data protection 41
5.4 TOE SECURITY ASSURANCE REQUIREMENTS 42
5.5 RATIONALE FOR TOE SECURITY REQUIREMENTS 43
5.5.1 TOE Security Functional Requirements 43
5.5.2 TOE Security Assurance Requirements 46
5.6 RATIONALE FOR EXPLICITLY STATED SECURITY REQUIREMENTS 46
5.7 RATIONALE FOR IT SECURITY FUNCTIONAL REQUIREMENT DEPENDENCIES 47
5.7.1 Rationale for unsatisfied dependencies 48
6 TOE SUMMARY SPECIFICATION 50
6.1 TOE SECURITY FUNCTIONS 50
6.1.1 Anti-Virus 50
6.1.2 ID and Authentication 53
6.1.3 Filtering 53
6.1.4 Action and Remediation 54
6.1.5 Cryptographic Operations 55
6.1.6 Audit 55
6.1.7 Security Management 57
6.2 RATIONALE FOR TOE SECURITY FUNCTIONS 58

Document History

Release Number	Date	Author	Details
0.1	9 July 09	Primasec	First draft version.
0.2	16 Aug 09	Primasec	Second draft version
0.3	28 Aug 09	Primasec	Incorporated peer review comments and comments from McAfee
0.4	9 Sept 09	Primasec	Incorporated initial evaluator comments
0.5	10 Sept 09	Primasec	Incorporated additional evaluator comments
0.6	4 Oct 09	Primasec	Incorporated OR1 and additional corrections
0.7	11 Oct 09	Primasec	Incorporated additional evaluator comments
0.8	14 Dec 09	Primasec	TOE version change and minor corrections
0.9	5 Jan 10	Primasec	Minor corrections
0.10	7 Jan 10	Primasec	Env Objectives added
0.11	23 Mar 10	Primasec	Update to TOE version
0.12	22 July 10	Primasec	Update to TOE version and add FIPS 140 details

1 Introduction

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

1.1 Identification

1.1.1 TOE Identification

The TOE is the McAfee Email and Web Security software v5.5 Patch 2 running on appliance models 3000, 3100, 3200, 3300, 3400, the Content Security Blade Server, and VMware Server.

Model identifiers:

Email and Web Security Appliance for the 3000 platform: SKU = EWS-3000-00A

Email and Web Security Appliance for the 3100 platform: SKU = EWS-3100-00A

Email and Web Security Appliance for the 3200 platform: SKU = EWS-3200-00A

Email and Web Security Appliance for the 3300 platform: SKU = EWS-3300-00A

Email Security Appliance for the 3400 platform: SKU = EWS-3400-SMA

Web Security Appliance for the 3400 platform: SKU = EWS-3400-SWA

Blade enclosure SKUs:	MCS-CH1P-M72 (M7 single phase power)
	MCS-CHDP-M7C (M7 DC power)
	MCS-CH3I-M72 (M7 3 phase international)
	MCS-CH3P-M72 (M7 DC international)
	MCS-CH1P-M31 (M3 single phase AC)
Blade SKUs:	Management MCS-MGMT-MXX
	Scanning MSC-BLDE-1XX
SKU for VMware	Not applicable – available as web download only

1.1.2 ST Identification

McAfee® Email and Web Security Appliance Version 5.5 Patch 2 EAL 2 + ALC_FLR.2 Security Target, Version 0.12.

1.2 TOE Overview

The Email and Web Security (EWS) 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 EWS appliance protects user and company IT resources from a variety of internet and email threats. Threats and resource liabilities such as Viruses, Potentially Unwanted Programs (including 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 EWS 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 EWS solution is implemented as the Email and Web Security Appliance. This consolidated solution includes Internet and Email protection in a single appliance. For larger businesses, the EWS functionality is deployed as the Web Security Appliance offering Internet Security features and the Email Security Appliance providing email protection features. In this case the requirements of this ST are met by the Web and Email appliances operating together, rather than by a single appliance. The McAfee EWS Appliance utilizes the same software suite regardless of hardware platform selected, although three different build images are available for the respective appliance functions.

1.3 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.

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)

1.4 Document Terminology

Please refer to CC Part 1 Section 4 for definitions of commonly used CC terms.

1.4.1 ST Specific Terminology

Administrator	A user of the TOE appliance in one of the predefined or user configured administrative roles. The predefined roles are Super Administrator, Email Administrator, Web Administrator and Reports Administrator. These predefined roles can be modified. The ST refers only to the “Administrator”, as the linkage of functions to roles is configurable.
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.
Blacklist	A list of e-mail addresses or domains that may be created, which the anti-spam module 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 EWS appliance. The EWS 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.
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 the anti-spam module treats as non-spam. When the anti-spam module 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.

1.4.2 Acronyms

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
.dat	Virus Definition Data Files
DHA	Directory Harvest Attack

DoS	Denial of Service
ESA	Email Security Appliance
EWS	Email and Web Security Appliance
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over SSL
ICAP	Internet Content Adaptation Protocol
O.S.	Operating System
POP3	Post Office Protocol 3
PUPs	Potentially Unwanted Programs
SFP	Security Function Policy
SSL	Secure Socket Layer (denotes SSLv3 only)
SIG	Secure Internet Gateway
SMG	Secure Messaging Gateway
SMTP	Simple Mail Transfer Protocol
SWG	Secure Web Gateway
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
TSP	TOE Security Policy
WSA	Web Security Appliance

1.5 TOE Description – Overview

The TOE is a security 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 EWS Appliance. Through the intercept, scanning and reporting functions, the McAfee EWS appliance can detect potentially malicious files of various types, filter traffic for restricted content, and block access to restricted internet addresses (URLs) and email containing spam messages or Phish attempts.

Protocols covered by scanning include: HTTP, ICAP, 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 characteristics 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.

Configuration in either Transparent Bridge or Transparent Router mode makes operation of the appliance transparent to devices communicating through the TOE.

1.6 Architecture Description

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

- Anti-Virus Module
- PUP Module (including Spyware)
- Anti-Phishing Module
- Anti-Spam Module
- URL Filtering Module
- Content Scan Module
- Quarantine Management Module
- ICAP support Module
- HTTP Scan Module
- EWS Security Management Operating System

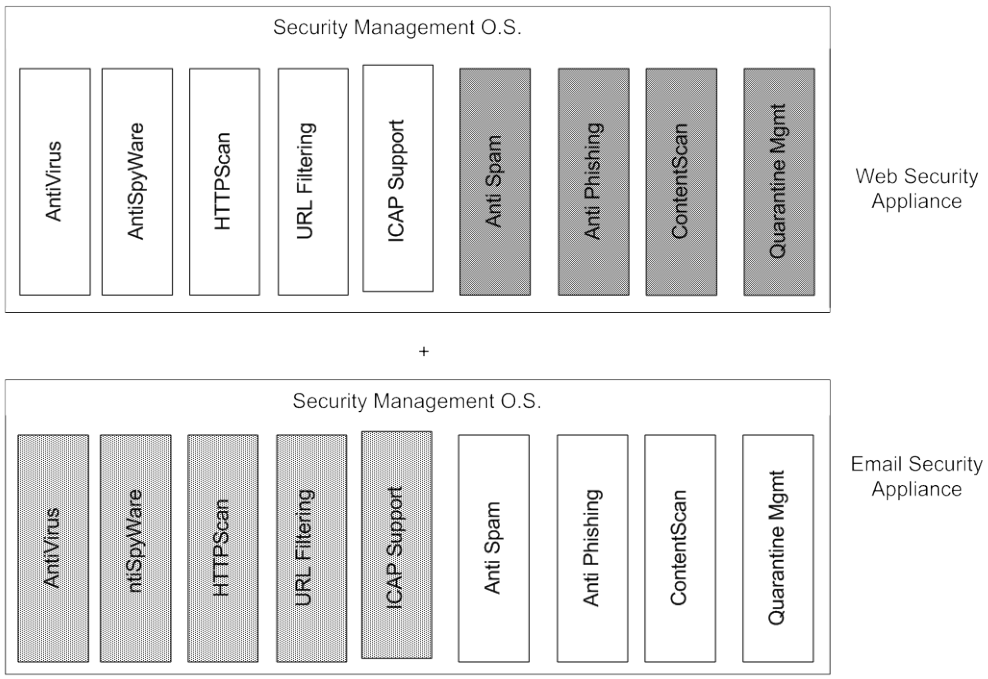


Figure 1: TOE Enterprise Option

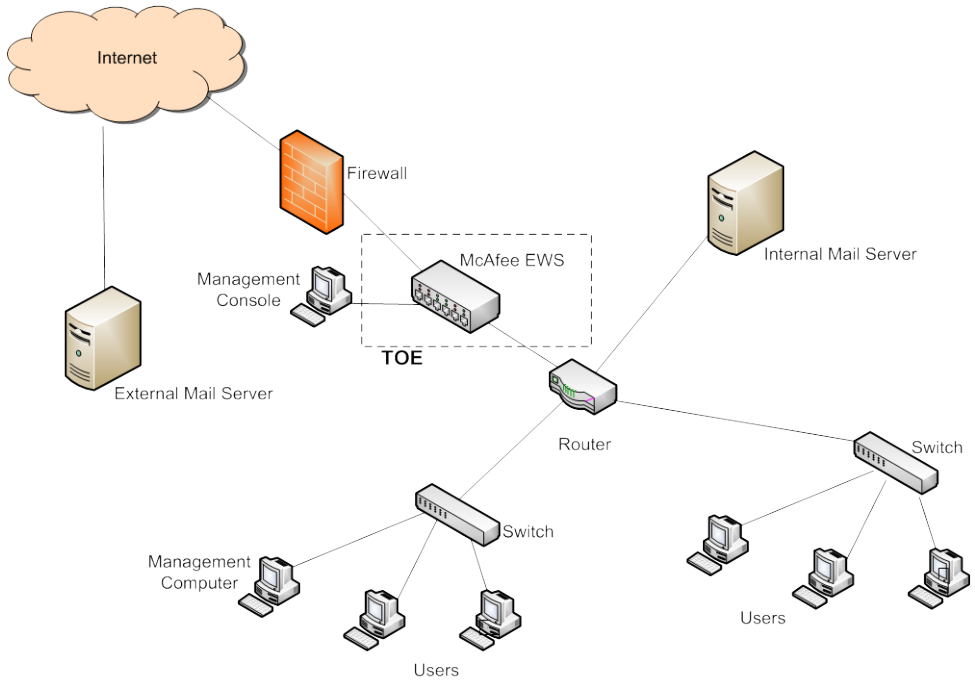


Figure 2: Architectural Diagram (placement in network)

Software Architectural Overview

The software of the McAfee EWS 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 Email and Web Security appliance all the software modules execute on that single hardware appliance. In the case of the Email Security Appliance and Web Security Appliance, those modules that correspond to the selected hardware platform are enabled based on that platform (either email or web). In Figure 1: TOE Enterprise Option, the modules shown that are darkened represent modules that are disabled due to the dedicated purpose of the appliance.

The EWS appliance allows creation of virtual hosts. Using virtual hosts, a single appliance can appear to behave like several appliances. Each virtual appliance can manage traffic within specified pools of IP addresses, enabling the appliance to provide scanning services to traffic from many sources or customers.

The EWS appliance also allows grouping of appliances into clusters. A cluster is a group of appliances that shares both its configuration and balances the network traffic. The cluster can contain:

- One cluster master. The master both synchronizes the configuration and balances the load of network traffic to the other cluster members.

and at least one of the following:

- One cluster failover. If the cluster master fails, the cluster failover will seamlessly take over the work of the cluster master.
- One or more cluster scanners. They scan traffic according to the policies synchronized from the master.

Note that the master and the failover can also scan traffic.

1.6.1 Anti-Virus Module

The Security Content Management application features an Anti-Virus module that provides protection through the EWS 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 of the engine, so as 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 new .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.

A further service is provided through use of Artemis technology. Where a file does not contain a recognised signature, but is suspicious (for example, the file is packed or encrypted), the appliance can send a small definition (or fingerprint) of that code to Artemis — an automated analysis system at McAfee.

McAfee compares the fingerprint against a database of fingerprints collected worldwide, and informs the appliance of the likely risk. Based on settings in the scanning policies, the appliance can then block, quarantine, or try to clean the threat. If McAfee later determines that the code is malicious, a DAT file is published as usual.

1.6.2 PUP Module

The Potentially Unwanted Programs (PUP) subsystem of the TOE utilizes the Anti-Virus Module's PUP scanning functionality to identify PUPs, including Spyware. PUPs 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.

As with the Anti-Virus module, detection functions use signatures to identify potential PUPs.

1.6.3 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.

1.6.4 Anti-Spam Module

The TOE provides protection from spam messages through the Anti-Spam Module of EWS. 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:

- Streaming Updates

  Streaming Updates are made available every five to ten minutes. This helps to raise detection rates and proactively protect against new types of spam email, including phishing, pharming and viruses.

- 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.

- 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.

1.6.5 URL Filtering Module

The TOE utilizes a URL filtering database that contains web site addresses with Administrator configured categories for use in filtering. This Internet related functionality is used to filter which web sites are accessible through the TOE appliance. Two types of filtering are provided:

- URL blacklist

  All web page requests are checked against an administrator established policy using a control list of pre-categorized web page URLs. If a match is made between a URL requested from a network user and the control list websites, then access to that URL can be blocked or audited. Administrators can customize their locally stored control lists by adding categories or sites, or exempting sites from the standard list.

- Site Advisor

  Site Advisor adds safety ratings (red, amber green) to browser and search engine results, providing a warning to users of potentially dangerous or unknown sites. These ratings are based on analysis done by McAfee.

This functionality is used to prevent access to offensive, non-business related or dangerous web sites, providing protection from liability, bandwidth preservation and reduced risk of infection for the business.

1.6.6 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.

Similar functionality is provided for HTTP and ICAP traffic.

1.6.7 Quarantine Management Module

McAfee® Quarantine Management is a software module that allows you to consolidate quarantine management and spam learning for the EWS 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.

1.6.8 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 acts an ICAP server to perform blocking or modification of HTTP requests that are presented to the appliance.

1.6.9 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.

1.6.10 EWS Security Management Operating System

1.6.10.1 EWS Operating System

The EWS operating system is a tailored version of Redhat Linux 9, Kernel 2.6.27.31 that integrates the operation of all McAfee EWS 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 EWS application. The core EWS application provides application level support to operational modules as well as security management support and audit log generation. The EWS 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 EWS Operating System, which provides the User Interface for the EWS Appliance as well as Identification and Authentication of Administrators for the appliance.

1.6.10.2 Security Management

Security Management functions are supported by the EWS Operating System, and include an administrator interface, rendered by Apache Webserver, and functionality to allow for configuration and management of the Appliance.

There are three methods of accessing the administrator interface:

1. Browser-based session on a web console machine from a connected network. This provides access to the graphical user interface used to configure all aspects of the appliance behaviour.
2. Serial port access. This provides access to a restricted console interface that can be used only to configure the limited settings of the appliance to allow access to configure the appliance over the network[1]. This serial based access is typically only used during installation for initial configuration, and use for any other purpose is not covered in the CC evaluated configuration.
3. Direct monitor/keyboard/pointing device connection. This provides access to the restricted console interface as described for serial port access above.

Regardless of the physical mode of accessing the appliance, administrators are provided with GUI access to:

1. The appliance configuration files;
2. The appliance console;
3. The logging subsystem, which manages access to appliance audit logs and reports.

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 either Microsoft Internet Explorer 6.0, 7.0 or 8.0, or Firefox 2.0, 3.0 or 3.5. The session uses HTTPS with Secure Socket Layer (SSL) v3.0 or Transport Layer Security (TLS) v1 encryption, using RC4 with cryptographic key size of 128-bits or 3DES with cryptographic key size of 112-bits. The SSLv2 protocol is explicitly disabled. ActiveX is enabled.

Note that use of SSL and HTTPS to secure the link to the administrator management computer is outside the scope of this evaluation. Remote administration of the McAfee EWS appliance utilizing the Remote Access Card option is also not included in the CC evaluated configuration.

1.7 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 EWS authentication process ensures that a valid username and password combination must be entered prior to allowing any changes to TSF settings.

1.8 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.

1.8.1 Hardware Components

The TOE includes both the EWS software image and the appliance on which it runs. The following tables

[1] The limited settings available via the console interface are those that can be configured in the Basic Settings using the standard setup wizard via the GUI; namely host name and domain, operational mode for the appliance, LAN1 and LAN2 settings, NIC settings (IP address, gateway and mask), gateway information and DNS server settings.

illustrate the differences between the appliance and blade hardware platforms:

Hardware Platform	3000	3100	3200	3300	3400
Users	120	300	600	1000	
Platform	Dell CR100	Dell CR100	Dell R200	Dell R610	Dell R610
Processor	Intel Celeron 440 Single Core	Intel Pentium E2160 Dual Core	Intel Xeon E3110 Dual Core	Intel Xeon E5530 Quad Core	2 x Intel Xeon E5560 Quad Core
RAM	2 GB	2 GB	4 GB	6 GB	12 GB
Hard Drive(s)	1 x 160 GB SATA	1 x 250 GB SATA	2 x 146 GB SAS	2 x 300 GB SAS (hot swappable)	2 x 300 GB SAS (hot swappable)
RAID	No	No	SAS6i – RAID 1	PERC6i – RAID 1	PERC6i – RAID 1
Network	2 Cu ports (on board)	2 Cu ports (on board)	2 Cu ports (on board)	4 Cu ports (on board) Optical – 2 Ports (PCI)	4 Cu ports (on board) Optical – 2 Ports (PCI)
Power Supply(s)	1 x 345W	1 x 345W	1 x 345W	2 x 670W (hot swappable)	2 x 670W (hot swappable)

Table 2: Appliance Hardware Platform comparison

	Enclosure Model	
	M7	M3
Platform	HP C7000	HPC3000
Blade slots	2 Management + 14 Scanning	2 Management + 6 Scanning
Onboard administrator	2	2
Network	4 x 4 Cu (1GB) port switches + 2 pairs SPF modules	4 x 4 Cu (1GB) port switches + 2 pairs SPF modules
Fans	10	6
Power supply	6 x 2250W DC or single phase AC or 3-phase Int/US	6 x 1200W DC or single phase AC
DVD	External USB	Internal

Blade	
Platform	HP BL460c
Processor	2 x Intel Xeon E5560 Quad Core
Memory	12GB
Hard disk	Two hot swappable 300GB (SCSI RAID 1)

Table 3: Blade Hardware Platform comparison

1.8.2 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	Email Web Security Software v.5.5 Patch 2 (identical for all deployment options, includes EWS operating system: Redhat Linux 9, 2.6.27.31 Kernel with McAfee customization) Email and Web Security Appliance: EWS-SIG-5.5-1531.117.iso (Models 3000,3100, 3200,3300 and Blade) Email Security Appliance: EWS-SMG-5.5-1531.117.iso (Model 3400) Web Security Appliance: EWS-SWG-5.5-1531.117.iso (Model 3400)	EWS software package incl. O.S.

	Content Security Blade Server: EWS-MULTI-5.5-1531.117.iso (single image for all blades, whether mail or gateway) Email and Web Security (Virtual Appliance): EWS-SIG-5.5-1531.117.VMBuy.zip	
Environment	Unspecified	Operating system for Management Computer
Environment	Microsoft Internet Explorer 6.0, 7.0 or 8.0, or Firefox 2.0, 3.0 or 3.5 with Secure Socket Layer (SSL) v3.0 or TLS 1.0 encryption, with ActiveX enabled	Web Browser Component on Management Computer for Administrator access to TOE
Environment	VMware Server 2	Virtual environment that can be used to run TOE

Table 4: Physical Scope and Boundary: Software

1.8.3 Guidance Documents

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

- AGD_PRE - Preparative guidance
  - Quick Start Guide for McAfee Email and Web Security Appliance v5.5
  - McAfee Email and Web Security Appliance 5.5 Installation Guide
  - McAfee Email and Web Security Virtual Appliance 5.5 Installation Guide
  - McAfee Email and Web Security Appliance (VMtrial) 5.5 Installation Guide
  - McAfee Email and Web Security Appliance 5.5 Migration Guide
  - Quick Start Guide for McAfee Content Security Blade Server (M3 chassis)
  - Quick Start Guide for McAfee Content Security Blade Server (M7 chassis)
  - McAfee Content Security Blade Server 5.5 (M3 chassis) Installation Guide
  - McAfee Content Security Blade Server 5.5 (M7 chassis) Installation Guide
- ADO_OPE – Operational guidance
  - McAfee Email and Web Security Appliance 5.5 Product Guide
  - Release Notes for McAfee Email and Web Security Appliance 5.5
  - McAfee Email and Web Gateway and McAfee ePolicy Orchestrator Integration Guide (out of scope of the TOE)

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

1.9 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.

1.9.1 Anti-Virus

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

1.9.1.1 Virus/Malware/Spyware Scanning

The McAfee EWS 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.

Where a file does not contain a recognised signature, but is suspicious (for example, the file is packed or encrypted), EWS can send a fingerprint to McAfee for analysis, and can act on results received.

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, ICAP, 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.

1.9.1.2 Comprehensive Traffic Scanning

The McAfee EWS 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 EWS appliance.

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

1.9.1.3 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 EWS operating system and security management support provided by the O.S.

1.9.2 ID and Authentication

The McAfee EWS 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 to the appliance by IP address, referring URL or email address. The TOE is transparent to network users passing traffic through the appliance.

The EWS 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 EWS Appliance provides role based access controls to allow appliance Administrators 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.

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

1.9.3 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 (HTTP and HTTPS) 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.

1.9.4 Email protection

The McAfee EWS 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 anti-spam 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 anti-spam feature set is provided by the functionality of the Anti-Spam module working in conjunction with the Quarantine Management module.

1.9.5 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 specify 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 EWS operating system management features.

1.9.6 Cryptographic Operations

When downloading updated Virus/Malware/Spyware signature files the McAfee EWS TOE performs SHA1 hash message digest verification for signature files to ensure authenticity and file integrity. This functionality is supported by the core McAfee EWS operating system.

1.9.7 Audit

The McAfee EWS 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 completed, 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 EWS 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, but this is outside the scope of the evaluation.

1.9.8 Security Management

The Management interface provided by the TOE for administration requires only the use of Microsoft Internet Explorer 6.0, 7.0 or 8.0, or Firefox 2.0, 3.0 or 3.5 on the administrator workstation through a configured HTTPS network management connection to the appliance, on an internal network. HTTPS is outside the scope of this evaluation. The administration of the TOE requires the use of an Administrator management computer and the specified Microsoft Internet Explorer browser with ActiveX enabled. The Administrator management computer is only used for input and display purposes, the functions discussed herein are all implemented on the EWS TOE Appliance. The EWS 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 EWS appliance requires identification by username and authentication through the EWS Appliance operating system enforced password.

The TOE allows creation of virtual hosts. Using virtual hosts, a single appliance can appear to behave like several appliances. Each virtual appliance can manage traffic within specified pools of IP addresses, enabling the appliance to provide scanning services to traffic from many sources or customers.

The EWS appliance also allows grouping of appliances into clusters. A cluster is a group of appliances that shares both its configuration and balances the network traffic.

1.10 Items Excluded from the TOE

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

- McAfee E-Policy Orchestrator (software)
- The use of LDAP or Kerberos authentication servers
- Scanning of TLS traffic
- Remote Access Card option for the 3300/3400 appliances (Enterprise)
- Administration from a remote location using the Remote Access Card
- Protection of the link to the management computer using HTTPS
- Export of log records to an external server

2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 3.1R3 Part 2 extended.

The TOE is Common Criteria (CC) Version 3.1R3 Part 3 conformant. The assurance level is EAL2 augmented with ALC_FLR.2.

This TOE is not conformant to any Protection Profiles (PPs) or security requirement packages.

3 TOE Security Problem Definition

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 EWS 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 Vendor 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 environment addresses the threats identified in this section. The primary assets to be protected are the integrity and availability of the resources and traffic on a network. There is also the concept of the network resources being used in line with organizational policy. 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.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 an 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 environment. The security objectives are divided between TOE Security Objectives (for example, security objectives addressed directly by the TOE) and Security Objectives for the 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 security objectives that are to be addressed by the TOE.

O.AUDIT_GEN	The TOE must create audit records of security relevant events associated by user which caused the event.
O.AUDIT_PROTECT	The TOE must provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE must provide the capability to selectively view audit information
O.AUDIT_STOR	The TOE must provide a means for secure storage of the TOE audit log files.
O.CRYPT	The TOE must secure signature data files during transit.
O.MANAGE	The TOE must 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 must 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 must provide mechanisms that mitigate attempts to exhaust connection-oriented resources provided by the TOE.
O.TOE_ACCESS	The TOE must provide mechanisms that control administrator logical access to the TOE.
O.TIME_STAMPS	The TOE must provide reliable time stamps and the capability for the Administrator to set the time used for these time stamps.
O.SECURE_CHK	The TOE must 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 security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE (i.e. through procedural, administrative or other technical means):

OE.ADMIN	Sites using the TOE must ensure that the authorized administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow all administrative guidance.
OE.DEDICATED	Administrators must assure that the McAfee EWS Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.
OE.NO_BYPASS	The TOE environment must ensure that the Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.NO_MALW	Administrators must 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 must ensure that authorized administrators will apply engine and signature file updates when available to keep file signatures used for scanning current.
OE.LOCATE	Physical Security must be provided including a secure location for the TOE and related assets commensurate with the value of those assets.
OE.ADMIN_SESSION	The integrity of the link between the TOE and management computer for Administrator sessions must be protected.
OE OE.NOSUB	The TOE environment must be able to protect against substitution attacks on the TOE data files during distribution.
OE.DECRYP	The TOE environment must provide for decryption of user data prior to analysis by the TOE.

4.3 Mapping of Threats to 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.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.SECURE_CHK														☑
OE.ADMIN	☑													
OE.DEDICATED		☑												
OE.LOCATE			☑											
OE.NO_BYPASS				☑										
OE.NO_MALW					☑									
OE.SEC_UPDATES						☑								
OE.ADMIN_SESSION									☑					
OE_NOSUB								☑						
OE_DECRYP											☑			☑

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. OE_NOSUB requires that the TOE environment also provides protection for the distributed files while in transit.
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. 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,
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. OE_DECRYP requires that the TOE environment provide decryption where necessary to allow access to the file content.
T.MASQUERADE	O.TOE_ACCESS mitigates this threat by providing mechanisms that control an administrator's logical access to the TOE. OE.ADMIN_ACCESS mitigates this threat by providing protection of the link to the management computer. O.MANAGE mitigates this threat by restricting access to management functions and facilities.
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. OE_DECRYP requires that the TOE environment provide decryption where necessary to allow access to the file content.
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 Security Policy Coverage

There are no Organizational Security 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 EWS 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 up to date.

5 IT Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST. New extended security functional components are defined in section 5.1. The security functional and assurance requirements are defined in Sections 5.2 and 5.3, respectively. The security functional requirements are listed in the table below.

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.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3a	Action in case of possible audit data loss
FAU_STG.3b	Action in case of possible audit data loss
FCS_COP.1	Cryptographic operation
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_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_STM.1	Reliable time stamps
FTA_SSL.3	TSF – initiated termination

Explicitly Stated TOE Security Functional Requirements	
FDP_MAM.1a	Scan operation
FDP_MAM.1b	Scan operation
FDP_MAM.1c	Scan operation
FDP_MAM.2a	Scan actions
FDP_MAM.2b	Scan actions
FDP_MAM.2c	Scan actions
FDP_MAM.3	Potential violation analysis

Table 6: Functional Requirements

5.1 Extended Components Definition

For this evaluation the Security Functional Requirements in CC Part 2 have been extended to cover part of the TOE functionality that cannot otherwise clearly be expressed.

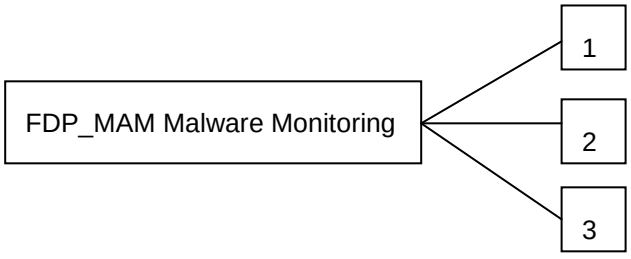
Three additional components have been defined. These have been placed in a new family named Malware Monitoring (FDP_MAM) within the Class FDP: User data protection. This choice has been made as the new components are all concerned with scanning and monitoring user data as it traverses the TOE. The decision was made to place this family within Class FDP, rather than Class FAU, since the latter class is concerned with monitoring the execution of the SFRs, rather than being a primary function of the TOE to protect user data, which is the case here.

Malware Monitoring (FDP_MAM)

Family behaviour

The requirements of this family relate to the monitoring of user data using specified methods in order to identify potential security violations.

Component leveling



Management: FDP_MAM.1

The following actions could be considered for the management functions in FMT:

a) Management of the type of monitoring conducted;

b) Management of the method used for monitoring.

Management: FDP_MAM.2

The following actions could be considered for the management functions in FMT:

a) Management of the list of security violations to be acted upon;

b) Management of the list of actions to be taken.

Management: FDP_MAM.3

The following actions could be considered for the management functions in FMT:

a) Management of the list of monitored events;

b) Management of the list of actions to be applied.

Audit: FDP_MAM.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Changes to the type of monitoring carried out.

Audit: FDP_MAM.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Identification of the security violation and action taken;

b) Basic: Changes to the list of identified security violations and changes to the list of actions to be taken.

Audit: FDP_MAM.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Identification of a monitored event and action taken;

b) Basic: Changes to the list of monitored events and changes to the list of rules.

FDP_MAM.1 Scan operation

Hierarchical to: No other components

Dependencies: No dependencies

FDP_MAM.1.1 The TSF shall perform [assignment: *type of monitoring*] based on [assignment: *monitoring method*].

FDP_MAM.2 Scan actions

Hierarchical to: No other components

Dependencies: FDP_MAM.1 Scan operation

FDP_MAM.2.1 Upon detection of [assignment: *list of identified security violations*] the TSF shall [assignment: list *of actions to be taken*].

FDP_MAM.3 Potential violation analysis

Hierarchical to: No other components

Dependencies: No dependencies

FDP_MAM.3.1 The TSF shall be able to apply [assignment*: list of rules*] in monitoring [assignment: *list of monitored events*], and based upon these rules indicate a potential security violation.

5.2 TOE Security Functional Requirements

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

5.2.1 Class FAU: Security Audit

5.2.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take **action to notify the Administrator via email and/or other alarm, and generate an audit record** upon detection of a potential security violation.

5.2.1.2 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 EWS Appliance User Interface**
- **Success/Failure of EWS 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 (if applicable), 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 Configuration	TSF settings	Success, Failure (setting changes)	Administrator logon to interface, TSF settings accessed/changes made	TOE Configuration Status
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 FDP_MAM.3, Potential violation analysis.

5.2.1.3 FAU_GEN.2 User Identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity ***(IP Address or Username)*** of the user that caused the event.

5.2.1.4 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator** with the capability to read **audit information listed in Table 4: 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.

5.2.1.5 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.

5.2.1.6 FAU_SAR.3 Selectable audit review

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

5.2.1.7 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all audited events based on the following attributes:

a) event type

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

c) specific sub event type – AntiVirus, AntiSpam & Phish, Content Filter, other.

5.2.1.8 FAU_STG.1 Protected audit trail storage

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

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

5.2.1.9 FAU_STG.3a Action in case of possible audit data loss

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

5.2.1.10 FAU_STG.3b Action in case of possible audit data loss

FAU_STG.3.1b The TSF shall **overwrite the oldest stored audit records** if the audit trail exceeds **available storage**.

5.2.2 Class FCS: Cryptographic Functions

5.2.2.1 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **calculate a message digest to verify the integrity of the engine and signature files** in accordance with a specified cryptographic algorithm **SHA1** and cryptographic key sizes (**not applicable**) that meet the following: **FIPS 180-3**.

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". The CAVP certificate number for this implementation of SHA1 is #SHS679.

5.2.3 Class FIA: Identification and authentication

5.2.3.1 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.

5.2.3.2 FIA_UID.2 User identification before any action

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

5.2.3.3 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 – 6 characters minimum and must contain either alphanumeric characters or special characters.**

5.2.4 Class FMT: Security management

5.2.4.1 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) Operation of the appliance

d) Update virus scan signatures

e) Configuration of alert notifications from the appliance

to **an Administrator.**

5.2.4.2 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) Traffic scanning options on the appliance

to **an Administrator.**

5.2.4.3 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 PUP is detected,

b) Protocols to be intercepted and scanned automatically on the appliance,

c) Virus/Malware/Spyware scan signatures,

d) Audit logs and

e) Network Policy

to **an Administrator.**

5.2.4.4 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 and

f) Network Policy

to **an Administrator.**

5.2.4.5 FMT_SMF.1 Specification of management functions

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

a. **Enable and disable operation of the appliance,**
b. **Configure traffic scanning options on the appliance,**
c. **Update virus scan signatures,**
d. **Configure alert notifications from the appliance,**
e. **Actions to take upon identification of a threat,**
f. **Content filter settings incl. URL addresses,**
g. **Query and configure audit logs.**

5.2.4.6 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: **Super Administrator, Email Administrator, Web Administrator, Reports Administrator and other configurable roles.**

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

5.2.5 Class FPT: Protection of the TSF

5.2.5.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.6 Class FTA: TOE Access

5.2.6.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **10 minute period of user inactivity.**

5.3 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. See section 5.1 for a definition of the extended components.

5.3.1 Class FDP: User data protection

5.3.1.1 FDP_MAM.1a Scan operation

FDP_MAM.1.1a The TSF shall perform **real-time network scans for viruses** based on **known signatures and heuristic methods**.

5.3.1.2 FDP_MAM.1b Scan operation

FDP_MAM.1.1b The TSF shall perform **real-time network scans for malware, spyware, Spam, phish attempts, packers, prohibited content and PUPS** based on **known signatures and heuristic methods**.

5.3.1.3 FDP_MAM.1c Scan operation

FDP_MAM.1.1c The TSF shall perform **filtering of URL addresses** based on **settings established by an Administrator**.

5.3.1.4 FDP_MAM.2a Scan actions

FDP_MAM.2.1a Upon detection of **a file-based virus** the TSF shall **perform the action(s) specified by an Administrator. 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.

5.3.1.5 FDP_MAM.2b Scan actions

FDP_MAM.2.1b Upon detection of **malware, spyware, spam, phish attempts, packers, prohibited content and PUPS** the TSF shall **perform the action(s) specified by the Administrator. Actions are administratively configurable on a per-Appliance basis and consist of protocol specific actions as specified in Table 8:**

Protocol	Primary Action taken (original)	Secondary Action taken (additional or copies)
SMTP Scan	**☒Accept and then optionally drop the data (based on configured options and scoring parameters)**	**☒Deliver an annotated modified E-mail to a GUI defined recipient (which may be the intended recipient or another)**
POP3	**☒Replace the content with an HTML alert**	
HTTP ICAP	**☒Delete the file and insert an HTML alert in its place**	

FTP	**☒Refuse the original data (The file is rejected)**

Table 8: Protocol Specific Scan actions

5.3.1.6 FDP_MAM.2c Scan actions

FDP_MAM.2.1c Upon detection of **a prohibited URL** the TSF shall **block access to the URL/IP address from the internal network**.

5.3.1.7 FDP_MAM.3 Potential violation analysis

FDP_MAM.3.1 The TSF shall be able to apply **the rules listed below** in monitoring **network traffic events**, and based upon these rules indicate a potential security violation.

On detection of an accumulation or combination of events as depicted ("*") in Table 7, known to indicate a potential TSP violation, an email is generated to the Administrator and an audit event is logged.

The TOE can be configured to not accept new connections from an IP address for a period of time following detection of a potential denial of service attack.

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 Evaluation Assurance Level 2 augmented by ALC_FLR.2, as defined by the CC. The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
ASE: Security target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction

Assurance Class	Assurance Components	
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 9: Assurance Requirements: EAL2+ALC_FLR.2

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.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.1	X										
FAU_STG.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.SECURE_CHK
FAU_STG.3a		X									
FAU_STG.3b		X									
FCS_COP.1					X						
FIA_UAU.2									X		
FIA_UID.2									X		
FIA_SOS.1									X		
FMT_MOF.1a						X					
FMT_MOF.1b						X					
FMT_MTD.1a						X					
FMT_MTD.1b						X					
FMT_SMF.1						X					
FMT_SMR.1						X					
FPT_STM.1								X			
FTA_SSL.3									X		
FDP_MAM.1a							X			X	X
FDP_MAM.1b							X			X	X
FDP_MAM.1c							X			X	X
FDP_MAM.2a							X			X	X
FDP_MAM.2b							X			X	X
FDP_MAM.2c							X			X	X
FDP_MAM.3											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.1 specifies the audit log selection options for protocol and communication events, and fordetection 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.3a specifies that the TOE will send emails to the Administrator upon reaching 75% and 90% of allocated space for audit logs. FAU_STG.3b specifies that the TOE will overwrite the oldest stored audit records 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.1 specifies that the TOE utilizes a cryptographic hash function to verify the integrity of .dat signature files.
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	FDP_MAM.1 specifies that the TOE provides scanning capability to detect prohibited content or prohibited URLs and FDP_MAM.2 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 10 minutes of inactivity. FIA_SOS.1 specifies that the TOE provides a mechanism to verify that secrets (passwords) are at least 6 characters including must contain either alphanumeric characters or special characters.
O.RESOURCE_X	FDP_MAM.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. FDP_MAM.2 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.SECURE_CHK	FDP_MAM.1 specifies that the TOE will provide a scanning function used to detect viruses, spyware, malware or spam. FDP_MAM.2 specifies that the TOE takes specified actions to remediate the event identified in FDP_MAM.1. FAU_ARP.1 specifies that the TOE will notify the TOE administrator via email and generate an audit record upon detection of a potential security violation. FDP_MAM.3 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.

Table 11: Security Objective Mapping Rationale

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. ALC_FLR.2 was added to provide assurance that the vendor will respond to reports of new threats and reported defects in the TOE.

5.6 Rationale for explicitly stated security requirements

Table 8: Explicitly Stated SFR Rationale, presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FDP_MAM.1	Scanoperation	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.
FDP_MAM.2	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.
FDP_MAM.3	Potential violation analysis	This component defines the monitoring process that occurs through intercept of traffic on a real time basis. This explicitly stated SFR 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 evaluation.

Table 12: Explicitly Stated SFR Rationale

5.7 Rationale for IT security functional 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 FDP_MAM.3
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.1	FAU_GEN.1, FAU_MTD.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.3a	FAU_STG.1	Yes

Functional Component	Dependency	Included/Rationale
FAU_STG.3b	FAU_STG.1	Yes
FCS_COP.1	FCS_CKM.1, FCS_CKM.4	No
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_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_STM.1	None	Yes
FTA_SSL.3	None	Yes
FDP_MAM.1a	None	Yes
FDP_MAM.1b	None	Yes
FDP_MAM.1c	None	Yes
FDP_MAM.2a	FDP_MAM.1	Yes
FDP_MAM.2b	FDP_MAM.1	Yes
FDP_MAM.2c	FDP_MAM.1	Yes
FDP_MAM.3	None	Yes

Table 13: 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 are provided below.

SFR	Dependency	Rationale

FAU_ARP.1	FAU_SAA.1	The Explicit SFR: FDP_MAM.3 is modeled after FAU_SAA.1 and satisfies the dependency of FAU_SAA.1 on FAU_ARP.1.
FCS_COP.1	FCS_CKM.1, FCS_CKM.4	The only cryptographic function is SHA1, which does not use a key.

Table 14: Rationale for Dependencies not met

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of 7 Security Functions:

- Anti-Virus
- ID and Authentication
- Filtering
- Action and Remediation
- Cryptographic Operations
- Audit
- Security Management

6.1.1 Anti-Virus

The Anti-Virus security function for the McAfee EWS TOE provides the scanning functionality to detect specified traffic that may pose a threat to internal networks. The EWS 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 are 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, FDP_MAM.3).

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 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.

FDP_MAM.1 – Anti-Virus Scanning Processes

The McAfee EWS TOE performs traffic scanning in real time as traffic traverses the device. The TOE uses signature based detection methods that evaluate traffic for characteristics of known malicious files/data types. The types of data included in the scanning process include 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, with streaming updates, coordinates with a rule and score system that assigns scores to email characteristics based on Administrator configured rules. The Administrator can also create black and white lists to disallow or allow messages to be routed, regardless of spam score.

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 enabled or disabled; no configuration options are available. This feature is contained within the AntiVirus subsystem and is supported by the EWS Operating System subsystem in section EWS Security Management Operating System.

Where a file does not contain a recognised signature, but is suspicious (for example, the file is packed or encrypted), the appliance can send a small definition (or fingerprint) of that code to Artemis — an automated analysis system at McAfee. McAfee informs the appliance of the likely risk. Based on settings in the scanning policies, the appliance can then block, quarantine, or try to clean the threat.

HTTP and ICAP 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 (FDP_MAM.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 FDP_MAM.3 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

FDP_MAM.3 –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 EWS 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 FDP_MAM.3 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 (FDP_MAM.1) is the process by which the appliance intercepts traffic and applies detection rules to simply identify a target characteristic. FDP_MAM.3 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 can trigger an alert within the TOE to the Administrator:

- 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 (e.g. for audit trail) 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 EWS 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 EWS Operating System environment. The computer used for this purpose can be a general purpose machine running Microsoft Internet Explorer 6.0, 7.0 or 8.0, or Firefox 2.0, 3.0 or 3.5 with SSL v3 or TLS v1 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 EWS 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 Administrator 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 Administrator is authenticated. Communication between the Administrator Management Computer and TOE Appliance is secured via SSL or TLS.

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. It is required in guidance that an Administrator sets this to a minimum of 6 characters. Only passwords with a minimum of 6 characters will be accepted by the EWS appliance in its evaluated configuration. The TOE enforces a 5 second delay between successive login attempts.

6.1.3 Filtering

The Filtering security function of the McAfee EWS 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.

FDP_MAM.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 to view the URL requests that the TOE has blocked or filtered.

Email protection through the Filtering security function

The McAfee EWS 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 have been identified as potential spam or Phish attempts, they may be forwarded to a pre-configured quarantine location. 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

FDP_MAM.2 – 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 Administrator. If cleaning of the detected unwanted content is selected, the action is taken within the scanning engine. All other remediation activities occur within the core EWS application. The McAfee EWS 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 Administrator;
- POP3 Replace the content with an HTML alert;
- HTTP Delete the file and insert an HTML alert in its place;
- ICAP Delete the file and insert an HTML alert in its place;
- FTP Refuse the original data (the file is rejected).

HTTP/ICAP Traffic Scan actions

HTTP or ICAP 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.

FDP_MAM.3 - Denial of Service Protection

If a Denial of Service (DoS) attack is identified, based on the configured Denial of Service Prevention policy, the connection can 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 operation within the TOE is the verification process for downloaded .dat threat signature files.

FCS_COP.1 - .dat file Message Digest verification

The threat signature files (.dat files) are verified for integrity using the SHA1 hash function during the download and install process. These 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. Hashing is used to assure that the files are unmodified, authentic and properly downloaded to the TOE. The SHA1 implementation is provided by RSA BSAFE Crypto-C Micro Edition (ME), version 2.1.0.2, FIPS 140-2 Cert#865, SHA1 Cert#679.

6.1.6 Audit

The McAfee EWS 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 EWS 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 EWS Appliance User Interface;

- Success/Failure of EWS 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 which is protected by the EWS 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.1

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 TOE Administrator 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 Administrator 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 EWS 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.3a, FAU_STG.3b – Storage and Protection of Audit Records

Audit records are stored within the McAfee EWS appliance through the use of a SQL compliant, open source object-relational database management system used within the McAfee EWS software. Audit logs are protected from access, deletion and modifications by the functionality described in the ID and Authentication section above. Only the Administrator may access appliance audit records. The EWS Appliance allocates space for audit log storage. The Administrator may configure two levels at which an email alert is sent to the Administrator warning of a specified value of resource exhaustion. By default, an email is sent when allocated logging resources used reach the 75% and 90% level, and an alarm can also be configured. When the allocated space within the appliance is reached, audit events overwritten, oldest first. If the audit trail becomes full, an email is sent to the Administrator for notification. Logs are rotated based on available disk size.

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

The McAfee EWS appliance provides the Administrator full audit access through an 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:

Scheduled reports	Reports which can be scheduled for delivery in either PDF, html, text; including a default report for overview, email, web and system;
Email Reports	All detections (totals and over time) including virus, spam, phish, sender authentication, content events, Status overview of the Email delivery status;
Web Reports	All detections (totals and over time) including virus, URLs, content events;
System Reports	System events including User Interface, updates, hardware and network events.

6.1.7 Security Management

The McAfee EWS 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 EWS application. Configuration data managed through this security function is managed and stored in the file system supported by the underlying EWS 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 EWS appliance through a number of default roles (which are configurable). It also provides the facility to create new user roles with defined limited responsibilities.

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 SSLv3 or TLSv1 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 10 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 EWS 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
- Query and configure 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 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 EWS appliance allows an Administrator 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 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 an 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 and 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 configuration parameters of the TOE is restricted by the TSF to Administrators holding the appropriate role, properly authenticated by the EWS 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 EWS operating system access controls. Administrator access 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 Administrator. These limitations are supported by restricting Management GUI access as described in ID & Authentication in Section 6.1.2.

6.2 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
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.1						X	
FAU_STG.1						X	
FAU_STG.3a						X	
FAU_STG.3b						X	
FCS_COP.1					X		
FIA_UAU.2		X					
FIA_UID.2		X					
FIA_SOS.1		X					
FMT_MOF.1a							X
FMT_MOF.1b							X

	Anti-Virus	ID and Authentication	Filtering	Action and Remediation	Cryptographic Operations	Audit	Security Management
FMT_MTD.1a							X
FMT_MTD.1b							X
FMT_SMF.1							X
FMT_SMR.1							X
FPT_STM.1						X	
FTA_SSL.3							X
FDP_MAM.1a	X		X				
FDP_MAM.1b	X		X				
FDP_MAM.1c			X				
FDP_MAM.2a				X			
FDP_MAM.2b				X			
FDP_MAM.2c				X			
FDP_MAM.3	X			X			

Table 15: TOE Security Function to SFR Mapping