McAfee® Email Gateway Appliance Version 7.0.1 EAL 2 + ALC_FLR.2 Security Target

Release Date:	16 October 2012
Version:	2.0

Prepared By:	Primasec Ltd.

Prepared For:	McAfee Inc. 2821 Mission College Blvd. Santa Clara, CA 95054

Table of Contents

TABLES

Document History

Release Number	Date	Author	Details
1.0	1 June 2011	Primasec	First release to evaluators
2.0	16 October 2012	Primasec	Final release for certification

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 Gateway (MEG) software v7.0.1, running on appliance models 4000-B, 4500-B, 5000(B, C & C-2U), 5500(B & C), and the Content Security Blade Server.

1.1.2 ST Identification

McAfee® Email Gateway Version 7.0.1 EAL 2 + ALC_FLR.2 Security Target, Version 2.0.

1.2 TOE Overview

MEG is a scalable hardware/software appliance that provides a comprehensive security solution for Email services. Through a series of security scanning, alert and configured actions and detailed content filtering options, the MEG appliance protects user and company IT resources from a variety of 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, Compliance 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 MEG software solution to throughput requirements based on the size of the enterprise and number of users. The McAfee MEG Appliance utilizes the same software suite regardless of hardware platform selected.

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 italicised text*
Selection:	indicated with underlined text
Refinement:	**additions indicated with bold text**
	deletions indicated with strike-through ~~bold text~~
Iteration:	indicated with typical CC requirement naming followed by the iteration number in parenthesis, e.g. (1), (2), (3).
Extension:	Extended components are identified by appending _EXT to the component name.

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 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.
Compliance	A process that uses rules to detect undesirable content, such as offensive words, in e-mail messages.
Data Loss Prevention (DLP)	Refers to systems that identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep content inspection and contextual security analysis of transactions (attributes of originator, data object, medium, timing, recipient/destination and so on).
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.
Encryption	Within the context of this ST, typically SWD, S/MIME or PGP.
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.
Image Filtering	A method of scanning that searches for inappropriate images in email traffic and performs a designated action on discovery.
Internal Network	Within the context of this ST, this refers to IT resources which are protected by the MEG appliance. The MEG 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.
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.

Table 1 - TOE Specific Terminology

1.4.2 Acronyms

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
.dat	Virus Definition Data Files
DHA	Directory Harvest Attack
DLP	Data Loss Prevention
DoS	Denial of Service
GTI	Global Threat Intelligence
HTTPS	Hypertext Transfer Protocol Secure
MEG	McAfee Email Gateway
O.S.	Operating System
PGP	Pretty Good Privacy
POP3	Post Office Protocol 3

PUPs	Potentially Unwanted Programs
SFP	Security Function Policy
SSL	Secure Socket Layer (denotes SSLv3 only)
SMTP	Simple Mail Transfer Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SWD	Secure Web Delivery
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
TSP	TOE Security Policy
WMC	Web Mail Client

Table 2 - Acronyms

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 MEG Appliance. Through the intercept, scanning and reporting functions, the MEG appliance can detect potentially malicious files of various types, filter traffic for restricted content, and email containing spam messages or Phish attempts.

Protocols covered by scanning include: POP3 and SMTP. 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 TOE provides comprehensive alerts and reports of suspicious activity to advise Administrators of traffic characteristics routed through the appliance. Scanning behaviour and subsequent actions are highly configurable through a comprehensive graphic user interface (GUI) allowing Administrators to tailor the appliance to the deployed environment.

The TOE supports options for mail to be accessed in a secure manner using a browser, using SWD. This is useful for situations where a user's mailbox is not trusted to maintain the confidentiality of stored mail.

The TOE provides mechanisms to support Data Loss Prevention (DLP), monitoring critical data in use and in transit, enforcing policies based upon the context of its use. It also employs image analysis techniques to filter mages in email that do not conform to policy guidelines.

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

1.6.1 Context

The software of the MEG appliance is identical among all shown configurations of the appliance. The following diagram shows placement of a MEG appliance within the network

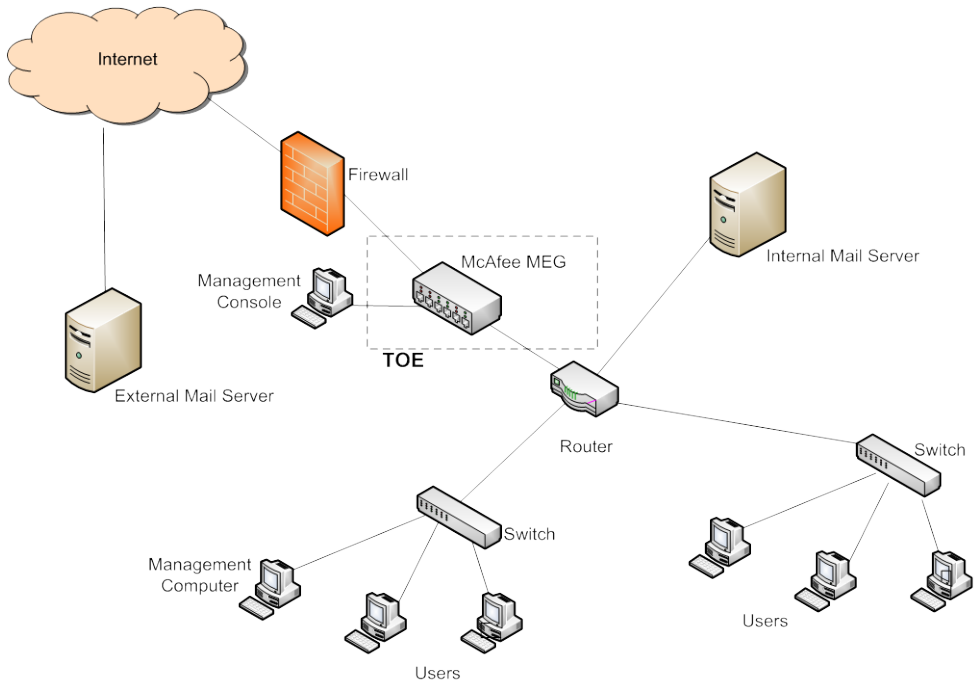


Figure 1: Architectural Diagram (placement in network)

1.6.2 Virtual hosts

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

1.6.3 Clustering

The MEG 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.

1.6.4 MEG Operating System

The MEG operating system is a tailored version of Redhat Linux 9, Kernel 2.6.27-31 that integrates the operation of all McAfee MEG support modules and provides the operational environment for executing the appliance's core functionality. The core MEG application provides application level support to operational modules as well as security management support and audit log generation. The MEG 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 MEG Operating System, which provides the User Interface for the MEG Appliance as well as Identification and Authentication of Administrators for the appliance.

1.7 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.

1.7.1 Hardware Components

The TOE includes both the MEG software image and the appliance on which it runs. The following tables illustrate the differences between the appliance and blade hardware platforms:

Hardware Platform	**4000-B**	**4500-B**	**5000-B** **5000-C** **5000-C-2U**	**5500-B** **5500-C**
Platform	Intel SR1530SH	Intel SR1630GPRX	Intel SR1625 URSASNA	Intel SR2625 URLXRNA
Processor	Intel Celeron E3400 Dual Core	Intel Core i3-540 Dual Core	Intel Xeon E5640 Quad Core	2 x Intel X5660 6-Core
RAM	4 GB	4 GB	6 GB	12 GB
Hard Drive(s)	1 x 500 GB	2 x 300 GB	2 x 300 GB	6 x 300 GB

	SATA	SAS (hot swappable)	SAS (hot swappable)	SAS (hot swappable)
RAID	No	SAS5iR – RAID 1	PERC6/i – RAID 1	PERC6/i – RAID 1
Network	2 Cu ports (on board)	2 Cu ports (on board)	B: 4 Cu ports (on board)	B: 4 Cu ports (on board)
			C & C-2U: 4 Cu ports (on board) Optical – 2 Ports (PCI)	C : 4 Cu ports (on board) Optical – 2 Ports (PCI)
Power Supply(s)	1 x 350W	1 x 400W	2 x 650W (hot swappable)	2 x 750W (hot swappable)

Table 3 - 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 – update
Processor	2 x Intel Xeon E5560 Quad Core
Memory	12GB
Hard disk	Two hot swappable 300GB (SCSI RAID 1)

Table 4 - Blade hardware platform comparison

1.7.2 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	McAfee Email Gateway Software v.7.0.1 (identical for all deployment options, includes MEG operating system: Redhat Linux 9, 2.6.27.31 Kernel with McAfee customization) McAfee Email Gateway Appliance: McAfee-MEG-7.0.1-2151.152.iso (Models 4000-B, 4500-B, 5000(B, C & 2U), 5500(B & C) and Content Security Blade Server)	MEG software package incl. O.S.
Environment	Unspecified	Operating system for Management Computer. Any operating system that can support one of the designated browsers can be used.
Environment	Microsoft Internet Explorer 7.0, 8.0 or 9.0, or Firefox 3.5, 3.6 or 4.0 with Secure Socket Layer (SSL) v3.0 or TLS 1.0 encryption, with ActiveX enabled	Web Browser Component on a general purpose Management Computer platform for Administrator access to TOE. Both platform and browser are outside the scope of the TOE.

Table 5 - Physical Scope and Boundary: Software

1.7.3 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 Gateway Appliance
  - McAfee Email Gateway Appliances (on Intel hardware) Installation Guide
  - Quick Start Guide McAfee Content Security Blade Server
  - McAfee Content Security Blade Server Installation Guide

- ADO_OPE – Operational guidance
    - Product Guide McAfee Email Gateway Appliances 7.0.0
    - Release Notes for McAfee Email Gateway Appliance7.0.1

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.

1.8 Logical Boundaries

The McAfee MEG TOE performs 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 or restricted content. Denial of Service (DoS) attacks can also be identified and thwarted through the scanning function of the McAfee MEG appliance.

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

The McAfee MEG logical description is divided into the following sections:

- Anti-Virus
    - Anti-Virus Scanning
    - GTI – File reputation
    - Packers
    - Potentially Unwanted Programs (including Spyware)
- Anti-Spam
    - Anti-Spam
    - Anti-Phishing
    - GTI Message Reputation
- Compliance
    - Compliance (Dictionaries)
    - Data Loss Prevention
    - Image Filtering
    - File Filtering
    - Mail Filtering
- Quarantine Management
- Secure Web Delivery - push/pull message delivery
- Security Management
- Audit and Alerts
- Action and Remediation

- Cryptographic Operations

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.

1.8.1 Anti-Virus

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

Anti-Virus Scanning

The TOE features an Anti-Virus module that provides protection 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 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.

The McAfee MEG 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), MEG 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: POP3 and SMTP. 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.

Global Threat Intelligence – File Reputation

A further service is provided through use of McAfee Global Threat Intelligence (GTI) file reputation technology. McAfee Global Threat Intelligence file reputation is McAfee's comprehensive, real-time, cloud-based file reputation service that enables McAfee products to protect customers against both known and emerging malware-based threats. McAfee's cloud-based system receives billions of file reputation queries each month and responds with a score that reflects the likelihood that the file in question is malware. The score is based not only on the collective intelligence from sensors querying the McAfee cloud and the analysis performed by McAfee Labs researchers and automated tools, but also on the correlation of cross-vector intelligence from web, email, and network threat data.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 GTI. McAfee compares the fingerprint against the database of fingerprints, and informs the appliance of the likely risk. The McAfee anti-malware engine — whether deployed as part of an endpoint anti-malware, gateway, or other solution — uses the score to determine action based on local policy. 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.

Packers

Packers compress files, which changes the binary structure of the executable. Packers can compress Trojan-horse programs and make them harder to detect. The TOE can be configured to take specified actions on detection of specific packer use. This can include blocking or unpacking and scanning.

Potentially Unwanted Programs (including Spyware)

The Potentially Unwanted Programs (PUP) (part of AV) 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.

1.8.2 Anti-Spam

Anti-spam

The McAfee MEG 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.

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

Anti-Phishing

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.

Global Threat Intelligence – Message Reputation

A further service is provided through use of McAfee Global Threat Intelligence (GTI) message reputation technology (see section 1.8.1.2 above). This service is applied also for spam and phishing detection.

1.8.3 Compliance

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.

Compliance (Dictionaries)

Dictionaries are provided that contain words or phrases that might cause offence. A library of predefined compliance rules is provided, or custom rules and dictionaries can be created to suit the needs of an organization. Compliance rules can vary in complexity from a straightforward trigger when an individual term within a dictionary is detected, to building on and combining score-based dictionaries which will only trigger when a certain threshold is reached.

Data Loss Prevention

The TOE provides mechanisms to support Data Loss Prevention (DLP), monitoring critical data in use and in transit, enforcing policies based upon the context of its use (SMTP only).

Image Filtering

The TOE has the capability to employ image analysis techniques to filter mages (i.e. pornography) in email that do not conform to specified policy guidelines.

File Filtering

The TOE allows for the creation of rules to allow control over the movement of files as email attachments according to their file name extension (e.g. .bmp, .exe), file format, name or size (SMTP only).

Mail Filtering

The TOE allows for the creation of rules to allow control over the movement of email according to the message size, attachment size or attachment count.

1.8.4 Quarantine Management

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.

1.8.5 Secure Web Delivery

The TOE provides users with a means to store and access emails securely in situations where the user's mail server does not provide sufficient assurance of confidentiality. Two approaches are supported for email traffic that policy has defined as sensitive, as follows:

Pull – MEG stores the emails in an encrypted form. An email is sent to the recipient that a sensitive email has arrived. The recipient sets up an account on MEG (if they do not have one already), and can then log in and view the email using a browser.

Push – MEG sends the email to the recipient's mail server in an encrypted form, together with a notification of its arrival. When the recipient selects the mail to be read, a browser login is performed, the email is sent back to MEG for decryption and is viewed via the browser.

1.8.6 Security Management

Management Interface

Security Management functions 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 (Out of band management) 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 7.0, 8.0 or 9.0, or Firefox 3.5, 3.6 or 4.0. The session uses HTTPS with Secure Socket Layer (SSL) v3.0 or Transport Layer Security (TLS) v1 encryption, using AES with cryptographic key size of 128-bits. The SSLv2 protocol is explicitly disabled. ActiveX is enabled. HTTPS is outside the scope of this evaluation.

The Administrator management computer is only used for input and display purposes: the functions discussed herein are all implemented on the MEG TOE Appliance.

TOE security functions cannot be bypassed. All access to TOE security functions requires Administrator level access to the TOE. The McAfee MEG authentication process ensures that a valid username and password combination must be entered prior to allowing any changes to TSF settings.

ID and Authentication

The McAfee MEG 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 MEG 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. It also supports use of Radius and AD enforced passwords.

[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.

The MEG 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 MEG 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.

Remote access cards may be used for remote administration for Enterprise level deployments. However, the evaluated configuration does not include this option.

1.8.7 Audit and Alerts

The McAfee MEG 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, and updates made to.dat signature files. Audit generation and related audit security functions are provided by the MEG 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.

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 and security management are supported by the MEG operating system.

1.8.8 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 configurations 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 MEG operating system management features.

Primary Action and Secondary Actions for any policy are defined. Primary actions are concerned with the immediate decision on how to process the traffic (e.g. block, allow, modify), and secondary actions are concerned with subsequent processing (e.g. quarantine, notifications).

1.8.9 Cryptographic Operations

File authentication and integrity

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

McAfee Agent 4.6 is used by the TOE to manage updates of the engine and .dat files.

S/MIME

The TOE also provides the capability to decrypt and scan mail and attachments that are encrypted withS/MIME, using preloaded keys and then re-encrypts them.

PGP

The TOE also provides the capability to decrypt and scan mail and attachments that are encrypted with PGP, using preloaded keys and then re-encrypts them.

TLS

Trusted communication with webmail clients is established using TLS to safeguard confidentiality and integrity.

1.9 Items Excluded from the TOE

This section identifies items not mentioned above that are specifically excluded from the TOE.

- McAfee E-Policy Orchestrator (software) management of appliances
- Remote Access Card option for the appliances
- Administration from a remote location using the Remote Access Card, including auto-configuration update

2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 3.1R4 Part 2 extended.

The TOE is Common Criteria (CC) Version 3.1R4 Part 3 conformant. The assurance level is EAL2 augmented with ALC_FLR.2.

This TOE is conformant to the Security Requirements for Network Devices Protection Profiles, Information Assurance Directorate, Version 1.1 [NDPP].

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 taken from [NDPP] with some TOE specific additions, as indicated. These additional assumptions do not diminish the security requirements for the [NDPP], and are related to the specific functionality of the TOE.

Source	Short name	Assumption
NDPP	A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
NDPP	A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
NDPP	A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
TOE Specific	A.NO_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
TOE Specific	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.
TOE Specific	A.NO_MALW	The administrator management computer used for remote security management purposes is assumed to be free from malware or other malicious software.

Table 6 - Assumptions

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.

The threats are taken from [NDPP] with some TOE specific additions.

Source	Threat Name	Threat Definition
NDPP	T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
NDPP	T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
NDPP	T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
NDPP	T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
NDPP	T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
NDPP	T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.
TOE Specific	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.
TOE Specific	T.BAD_DAT	An unidentified threat agent could compromise a threat signature .dat file during download to the TOE resulting in an inaccurate or corrupted threat signature file being

		used on the TOE.
TOE Specific	T.UNID_ACTION	An unidentified threat agent could effect a security violation on the protected network that goes unnoticed by the Administrator, thus limiting the Administrator's ability to identify and take action against a possible security breach.
TOE Specific	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.
TOE Specific	T.MAL_MSG	An unidentified threat agent could introduce prohibited content that could be received or sent through email resources within the protected network through the TOE appliance.

Table 7 - Threats

3.3 Organizational Security Policy

The organizational security policy is taken from [NDPP].

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

Table 8 - Organisational security policy

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

The table below defines the security objectives that are to be addressed by the TOE.

Source	TOE Security Objective Name	TOE Security Objective Definition
NDPP	O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
NDPP	O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
NDPP	O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
NDPP	O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
NDPP	O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
NDPP	O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
NDPP	O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
NDPP	O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
TOE Specific	O.AUDIT_PROTECT	The TOE must provide the capability to protect audit information.
TOE Specific	O.AUDIT_REVIEW	The TOE must provide the capability to selectively view audit information.
TOE Specific	O.MAL_CONTENT	The TOE must provide the capability to scan email traffic to detect and initiate actions to prevent

		transmission or delivery of restricted content.
TOE Specific	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.
TOE Specific	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.
TOE Specific	O.DECRYP	The TOE must provide for decryption of user data prior to analysis by the TOE.
TOE Specific	O.SECURE_MAIL	The TOE must provide a means to protect selected user email against unauthorized disclosure.

Table 9 - Security objectives for the TOE

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):

Source	TOE Security Objective Name	TOE Security Objective Definition
NDPP	OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
NDPP	OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
NDPP	OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
TOE Specific	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.
TOE Specific	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.

TOE Specific	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.
TOE Specific	OE.ADMIN_SESSION	The integrity of the link between the TOE and management computer for Administrator sessions must be protected.
TOE Specific	OE.NOSUB	The TOE environment must be able to protect against substitution attacks on the TOE data files during distribution.

Table 10 - Security objectives for the environment

4.3 Mapping of Security Problem Definition to Security Objectives

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

	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	A.NO_BYPASS	A.SEC_UPDATES	A.NO_MALW	T.ADMIN_ERROR	T.TSF_FAILURE	T.UNDETECTED_ACTIONS	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.USER_DATA_REUSE	T.AUDIT_ COMP	T.BAD_DAT	T.UNID_ACTION	T.MAL_AGENT	T.MAL_MSG	P.ACCESS_BANNER
O.PROTECTED_COMMUNICATIONS										X		X	X					
O.VERIFIABLE_UPDATES											X			X		X		
O.SYSTEM_MONITORING									X						X			
O.DISPLAY_BANNER																		X
O.TOE_ADMINISTRATION										X								
O.RESIDUAL_INFORMATION_CLEARING												X						
O.SESSION_LOCK										X								
O.TSF_SELF_TEST								X				X						
O.AUDIT_PROTECT									X				X		X			

	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	A.NO_BYPASS	A.SEC_UPDATES	A.NO_MALW	T.ADMIN_ERROR	T.TSF_FAILURE	T.UNDETECTED_ACTIONS	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.USER_DATA_REUSE	T.AUDIT_ COMP	T.BAD_DAT	T.UNID_ACTION	T.MAL_AGENT	T.MAL_MSG	P.ACCESS_BANNER
O.AUDIT_REVIEW									X						X			
O.MAL_CONTENT																	X	
O.TIME_STAMPS									X									
O.SECURE_CHK																X		
O.DECRYP																X		
O.SECURE_MAIL										X								
OE.NO_GENERAL_PURPOSE	X																	
OE.PHYSICAL		X																
OE.TRUSTED_ADMIN			X				X											
OE.NO_BYPASS				X														
OE.NO_MALW						X										X		
OE.SEC_UPDATES					X									X		X		
OE.ADMIN_SESSION										X								
OE.NOSUB											X			X		X		

Table 11 - Security Problem & 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.ADMIN_ERROR is addressed by OE.TRUSTED_ADMIN. The use of trusted administrators will help to reduce the likelihood of error.

T.TSF_FAILURE is addressed by O.TSF_SELFTEST. Self-testing will reduce the likelihood of undetected failures in TSF mechanisms compromising the security of the TOE.

T.UNDETECTED_ACTIONS is addressed by O.SYSTEM_MONITORING, O.AUDIT_PROTECT, O.AUDIT_REVIEW and O.TIME_STAMPS. The TOE will monitor and record selected events (O.SYSTEM_MONITORING, O.TIME_STAMPS), protect the stored records (O.AUDIT_PROTECT), and provide a capability to review the records (O.AUDIT_REVIEW).

T.UNAUTHORIZED_ACCESS is addressed by O.PROTECTED_COMMUNICATIONS, O.TOE_ADMINISTRATION, O.SESSION_LOCK, O.SECURE_MAIL and OE.ADMIN_SESSION. Communication channels are protected against interception (O. PROTECTED_COMMUNICATIONS, OE. ADMIN_SESSION). Login is controlled (O. TOE_ADMINISTRATION), and session locking is provided (O.SESSION_LOCK). A means for secure access to selected email is provided (O.SECURE_MAIL).

T.UNAUTHORIZED_UPDATE is addressed by O.VERIFIABLE _UPDATES and OE.NOSUB. The TOE will verify that updates are unaltered (O.VERIFIABLE _UPDATES), and the TOE environment will help safeguard files against substitution (OE.NOSUB).

T.USER_DATA_REUSE is addressed by O.PROTECTED_COMMUNICATIONS, O.RESIDUAL_INFORMATION_CLEARING and O.TSF_SELF_TEST. Protection against sending data to an incorrect destination is provided through protection of communication channels (O.PROTECTED_COMMUNICATIONS), clearing of information from objects before reuse (O.RESIDUAL_INFORMATION_CLEARING), and through self testing to ensure correct operation (O.TSF_SELF_TEST).

T.AUDIT_COMP is addressed by O.PROTECTED_COMMUNICATIONS and O.AUDIT_PROTECT. The TOE provides protection against the compromise of audit date through protection of communication channels (O.PROTECTED_COMMUNICATIONS), and protection of the audit trail records (O.AUDIT_PROTECT).

T.BAD_DAT is addressed by O.VERIFIABLE _UPDATES, OE_SEC_UPDATES and OE.NOSUB. Compromise of threat signature downloads is countered through use of verification of downloads (O.VERIFIABLE _UPDATES), and safeguards in the TOE environment (OE.NOSUB). Updates must also be applied when received (OE_SEC_UPDATES).

T.UNID_ACTION is addressed by O.SYSTEM_MONITORING, O.AUDIT_PROTECT and O.AUDIT_REVIEW. Administrators may not notice potential security violations, so the TOE will monitor these (O.SYSTEM_MONITORING) and record them securely for later review (O.AUDIT_PROTECT, O.AUDIT_REVIEW).

T.MAL_AGENT is addressed by O.VERIFIABLE _UPDATES, O.SECURE_CHK, OE.NO_MALW, OE.SEC_UPDATES, O.NOSUB and O.DECRYP. Protection against malware (O.SECURE_CHK) is provided through scanning of email traffic, including when encrypted (O.DECRYP). This capability is supported through protection of updates (O.VERIFIABLE _UPDATES, OE.SEC_UPDATES, OE.NOSUB), and protection of the administrator management computer by the TOE environment (OE.NO_MALW).

T.MAL_MSG is addressed by O.MAL_CONTENT. Protection against movement of restricted content is provided through scanning of emails.

4.5 Rationale for Organizational Security Policy Coverage

P.ACCESS_BANNER requires the display of an access banner. The TOE provides such a banner (O.DISPLAY_BANNER).

4.6 Rationale for Assumption Coverage

Each of the assumptions is addressed through provision of a correspondingly names objective for the TOE environment to assure that the assumptions are upheld in the TOE's operational environment.

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.

Functional Components	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User Identity association
FAU_STG_EXT.1	External audit trail storage
FAU_ARP.1 *	Security alarms
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.3 (1)*	Action in case of possible audit data loss
FAU_STG.3 (2)*	Action in case of possible audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM_EXT.4	Cryptographic key zeroisation
FCS_COP.1(1)	Cryptographic operation
FCS_COP.1(2)	Cryptographic operation
FCS_COP.1(3)	Cryptographic operation
FCS_COP.1(4)	Cryptographic operation
FCS_COP.1(5)*	Cryptographic operation
FCS_RBG_EXT.1	Cryptographic operation
FCS_SSH_EXT.1	SSH
FCS_TLS_EXT.1	TLS
FCS_HTTPS_EXT.1	HTTPS
FDP_RIP.2	Full residual information protection
FDP_CMM_EXT.1(1)*	Scan operation
FDP_CMM_EXT.1(2)*	Scan operation

FDP_CMM_EXT.1(3) *	Scan operation
FDP_CMM_EXT.1(4) *	Scan operation
FDP_CMM_EXT.2(1) *	Scan actions
FDP_CMM_EXT.2(2) *	Scan actions
FDP_CMM_EXT.2(3) *	Scan actions
FDP_CMM_EXT.2(4) *	Scan actions
FDP_IFC.1*	Subset information flow control
FDP_IFF.1*	Simple security attributes
FDP_UCT.1*	Basic data exchange confidentiality
FIA_PMG_EXT.1	Password management
FIA_UIA_EXT.1	User identification and authentication
FIA_UAU_EXT.2	Password-based authentication mechanism
FIA_UAU.7	Protected authentication feedback
FMT_MTD.1	Management of TSF data
FMT_MOF.1(1)	Management of security functions behaviour
FMT_MOF.1(2)	Management of security functions behaviour
FMT_MOF.1(3)	Management of security functions behaviour
FMT_SMF.1	Specification of management functions
FMT_SMR.2	Restrictions on security roles
FPT_ITT.1(1) *	Basic internal TSF data transfer protection
FPT_SKP_EXT.1	Protection of TSF data (for reading of all symmetric keys
FPT_APW_EXT.1	Protection of administrator passwords
FPT_STM.1	Reliable time stamps
FPT_TUD_EXT.1	Trusted update
FPT_TST_EXT.1	TSF testing
FTA_SSL_EXT.1	TSF-initiated session locking
FTA_SSL.3	TSF-initiated termination
FTA_SSL.4	User-initiated termination
FTA_TAB.1	Default TOE access banners
FTP_ITC.1	Inter-TSF trusted channel

FTP_TRP.1	Trusted path

Table 12 - TOE Security 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.

Two additional components have been defined for this ST. These have been placed in a new family named Compliance and Malware Monitoring (FDP_CMM_EXT) within the Class FDP: User data protection. This choice has been made as the new components are all concerned with scanning for undesirable content and determining compliance of 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.

The remaining extended components in this section are used in [NDPP]. The PP author has not provided definitions of these components, but it is considered appropriate to try to provide these definitions in this ST.

5.1.1 Compliance and Malware Monitoring (FDP_CMM_EXT)

Family behaviour

This new family is added to the class FDP. The requirements of this family relate to the monitoring of user data using specified methods in order to identify potential security violations.

Component levelling

Management: FDP_CMM_EXT.1

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

a) Management of the type of scan conducted;

b) Management of the rules used for scanning.

Management: FDP_CMM_EXT.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.

Audit: FDP_CMM_EXT.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 scanning carried out.

Audit: FDP_CMM_EXT.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.

FDP_CMM_EXT.1 Scan operation

Hierarchical to: No other components

Dependencies: No dependencies

FDP_CMM_EXT.1.1 The TSF shall perform [assignment: *type of scanning*] in accordance with [assignment: *scanning rules*].

FDP_CMM_EXT.2 Scan actions

Hierarchical to: No other components

Dependencies: FDP_CMM_EXT.1 Scan operation

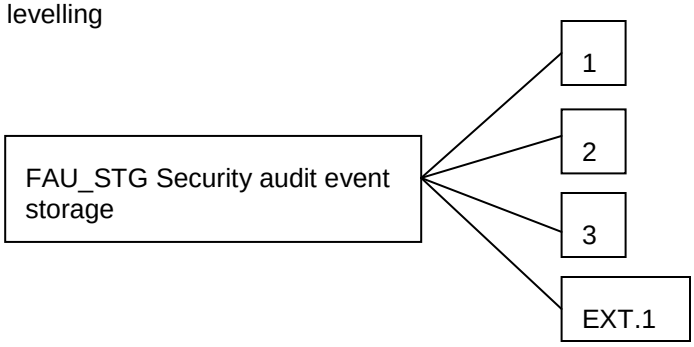
FDP_CMM.2.1 Upon detection of [assignment: *list of identified security violations*] the TSF shall [assignment: list *of actions to be taken*].

5.1.2 Security audit event storage (FAU_STG)

Family behaviour

This component is added to the existing family FAU_STG.

Component levelling



FAU_STG_EXT.1 requires the ability to transmit or receive audit data to or from a secure external IT entity.

Management: FAU_STG_EXT.1

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

a) Management of transmission/receipt of audit data.

Audit: FAU_STG_EXT.1

There are no auditable events foreseen.

FAU_STG_EXT.1 External audit trail storage

Hierarchical to: No other components

Dependencies: FTP_ITC.1 Inter-TSF trusted channel

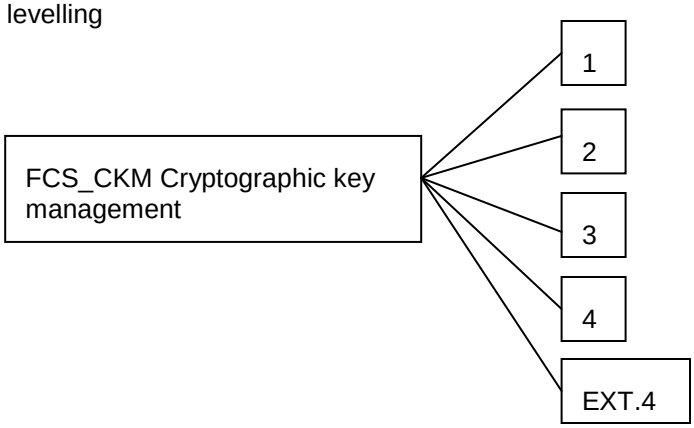
FAU_STG_EXT.1.1 The TSF shall be able to [selection: *transmit the generated audit data to an external IT entity, receive and store audit data from an external IT entity*] using a trusted channel implementing the [selection: *SSH, TLS, TLS/HTTPS*] protocol.

5.1.3 Cryptographic key management (FCS_CKM)

Family behaviour

This component is added to the existing family FCS_CKM.

Component levelling



FCS_CKM_EXT.4 requires the ability to zeroize cryptographic keys and critical security parameters (CSPs).

Management: FCS_CKM_EXT.4

There are no management activities foreseen.

Audit: FCS_CKM_EXT.4

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

a) Minimal: Failure of the activity.

FCS_CKM_EXT.4 Cryptographic key zeroization

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

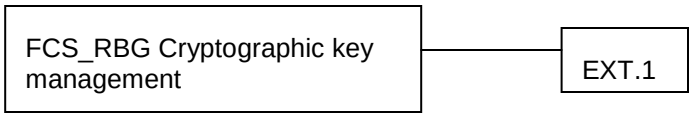
FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.1.4 Cryptographic operation: random bit generation (FCS_RBG)

Family behaviour

This family is added to the class FCS. This family deals with generation of random bit streams in support of cryptographic operations

Component levelling



FCS_RBG_EXT.1 requires generation of random bits in accordance with a selected standard..

Management: FCS_RBG_EXT.1

There are no management activities foreseen.

Audit: FCS_RBG_EXT.1

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

a) Minimal: Failure of the activity.

FCS_RBG_EXT.1 Cryptographic operation: random bit generation

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: *NIST Special Publication 800-90 using* [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES*] seeded by an entropy

source that accumulated entropy from [selection: *a software-based noise source, a TSF-hardware-based noise source*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

5.1.5 HTTPS (FCS_HTTPS)

Family behaviour

This family is added to the class FCS, and places specific requirements on the implementation of HTTPS.

Component levelling

FCS_HTTPS_EXT.1 places specific requirements on the implementation of HTTPS.

Management: FCS_HTTPS_EXT.1

There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1

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

a) Minimal: Failure to establish an HTTPS session,

b) Basic: Establishment and termination of an HTTPS session.

FCS_HTTPS_EXT.1 HTTPS

Hierarchical to: No other components

Dependencies: FCS_TLS_EXT.1 TLS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.1.6 SSH (FCS_SSH)

Family behaviour

This family is added to the class FCS, and places specific requirements on the implementation of SSH.

Component levelling

FCS_SSH_EXT.1 places specific requirements on the implementation of SSH.

Management: FCS_SSH_EXT.1

No management activities are foreseen.

Audit: FCS_SSH_EXT.1

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

a) Minimal: Failure to establish an SSH session,

b) Basic: Establishment and termination of an SSH session.

FCS_SSH_EXT.1 SSH

Hierarchical to: No other components

Dependencies: No dependencies

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [assignment: *timeout period*], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [assignment: *maximum number of attempts*] attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFS 4253, packets greater than [assignment: *number of bytes*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256 [*no other algorithms*].

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH-RSA and [selection: *PGP-SIGN-RSA, PGP-SIGN-DSS*, *no other public key algorithms*] as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that the data integrity algorithms used in SSH transport connection is [selection: *hmac-sha1, hmac-sha96, hmac-md5, hmac-md5-96*].

FCS_SSH_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.1.7 TLS (FCS_TLS)

Family behaviour

This family is added to the class FCS, and places specific requirements on the implementation of TLS.

Component levelling

FCS_TLS_EXT.1 places specific requirements on the implementation of TLS.

.

Management: FCS_TLS_EXT.1

There are no management activities foreseen.

Audit: FCS_TLS_EXT.1

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

a) Minimal: Failure to establish a TLS session,

b) Basic: Establishment and termination of a TLS session.

FCS_TLS_EXT.1 TLS

Hierarchical to: No other components

Dependencies: No dependencies

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: *TLS 1.0, (RFC 2346), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

Mandatory Ciphersuites

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Optional Ciphersuites:

[selection:

None

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA384].

5.1.8 Password management (FIA_PMG)

Family behaviour

This family is added to the class FIA, and deals with the specification of rules for password composition.

Component levelling

FIA_PMG_EXT.1 requires that passwords should conform to rules that are configurable by the system administrator.

Management: FIA_PMG_EXT.1

There are no management activities foreseen.

Audit: FIA_PMG_EXT.1

There are no auditable events foreseen.

FIA_PMG_EXT.1 Password management

Hierarchical to: No other components

Dependencies: FIA_UAU_EXT.2 Password-based authentication mechanism

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters [selection: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"*,[assignment: *other characters*]];

b) Minimum password length shall be settable by the security administrator, and support passwords of 15 characters or greater.

5.1.9 User identification and authentication (FIA_UIA)

Family behaviour

This family is added to the class FIA, and combines aspects of the existing CC families FIA_UID and FIA_UAU.

Component levelling

FIA_UIA_EXT.1 allows for specification of a limited set of actions to be permitted before a user is identified and authenticated.

Management: FIA_UIA_EXT.1

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

a) Management of the user identities;

b) Management of the authentication data by an administrator;

c) Management of the authentication data by the associated user;

b) If an authorised administrator can change the actions allowed before identification and authentication, the managing of the action lists.

Audit: FIA_UIA_EXT.1

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

a) Minimal: Unsuccessful use of the authentication mechanism;

b) Basic: All use of the authentication mechanism;

c) Detailed: All TSF mediated actions performed before identification and authentication of the user.

FIA_UIA_EXT.1 User identification and authentication

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;

- [selection: *no other actions*, [assignment: *list of services, actions performed by the TSF in response to non-TOE requests*]].

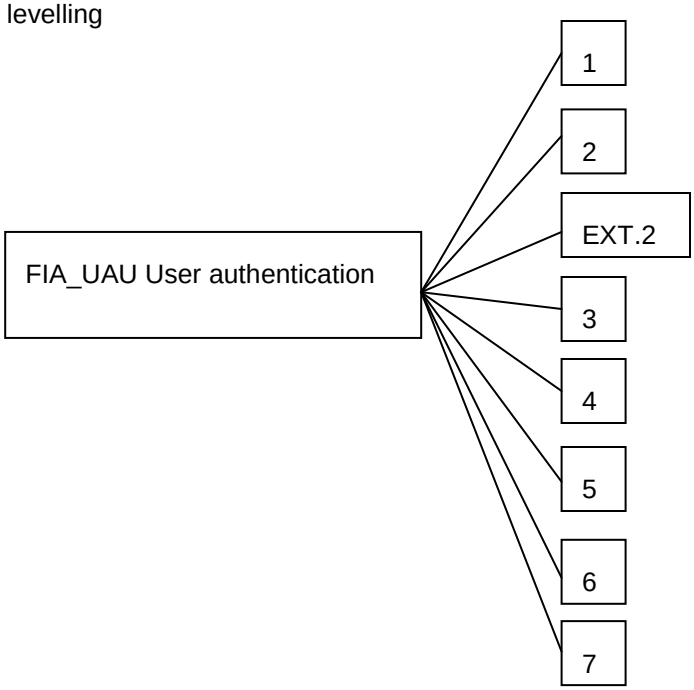
FIA_UIA_EXT.1.2 The TSF shall require each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.10 User authentication (FIA_UAU)

Family behaviour

This component is added to the existing CC family FIA_UAU, and covers use of a password for authentication.

Component levelling



FIA_UAU_EXT.2 allows for specification of password based and other authentication mechanisms.

Management: FIA_UAU_EXT.2

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

a) Resetting of the expired passwords.

Audit: FIA_UAU_EXT.2

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

a) Minimal: Unsuccessful use of the authentication mechanism;

b) Basic: All use of the authentication mechanism.

FIA_UAU_EXT.2 Password-based authentication mechanism

Hierarchical to: No other components

Dependencies: FIA_PMG_EXT.1 Password management

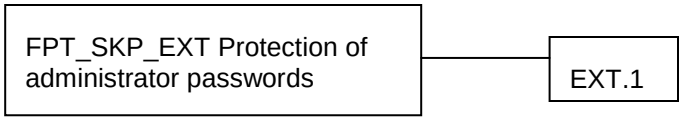
FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [selection: [assignment: *other authentication mechanism(s)*], *none*] to perform administrative user authentication.

5.1.11 Protection of TSF data (FPT_SKP)

Family behaviour

This family is added to the class FPT, and addresses the requirement to prevent reading of sensitive TSF data.

Component levelling



FPT_SKP_EXT.1 requires that sensitive cryptographic keys cannot be read.

Management: FPT_SKP_EXT.1

There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

There are no auditable events foreseen.

FPT_SKP_EXT.1 Protection of TSF data (for reading of all symmetric keys)

Hierarchical to: No other components

Dependencies: No dependencies

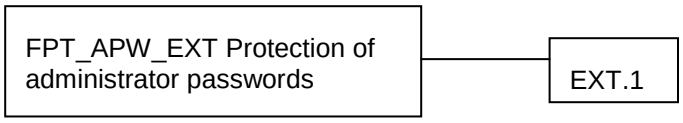
FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys and private keys.

5.1.12 Protection of administrator passwords (FPT_APW)

Family behaviour

This family is added to the class FPT, and addresses the requirement to prevent reading of plaintext passwords.

Component levelling



FPT_APW_EXT.1 requires that passwords are not stored in clear, and that no interface is provided to read them..

Management: FPT_APW_EXT.1

There are no management activities foreseen.

Audit: FPT_APW_EXT.1

There are no auditable events foreseen.

FPT_APW_EXT.1 Protection of administrator passwords

Hierarchical to: No other components

Dependencies: No dependencies

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.1.13 Trusted update (FPT_TUD)

Family behaviour

This family is added to the class FPT, and addresses the requirement to query the current version of the TOE, and to initiate and verify updates.

Component levelling

FPT_TUD_EXT.1 requires the ability to query the current TOE version, and to initiate and verify updates..

Management: FPT_TUD_EXT.1

There are no management activities foreseen.

Audit: FPT_TUD_EXT.1

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

a) Minimal: Initiation of any update to the TOE software/firmware.

FPT_TUD_EXT.1 Trusted update

Hierarchical to: No other components

Dependencies: No dependencies

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

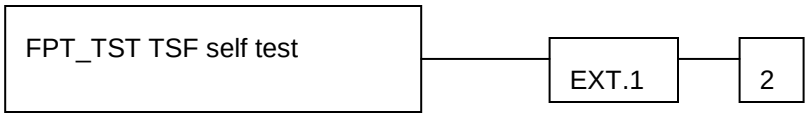
FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [selection: *digital signature mechanism, published hash*] prior to installing those updates.

5.1.14 TSF self test (FPT_TST)

Family behaviour

This component is added to the existing CC family FPT_TST.

Component levelling



FPT_TUD_EXT.1 requires the ability to query the current TOE version, and to initiate and verify updates.

Management: FPT_TST_EXT.1

There are no management activities foreseen.

Audit: FPT_TST_EXT.1

There are no auditable events foreseen.

FPT_TST_EXT.1 TSF testing

Hierarchical to: No other components

Dependencies: No dependencies

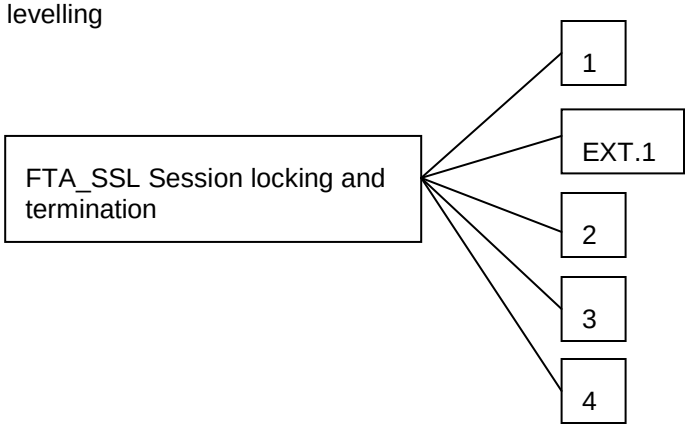
FPT_TST_EXT.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which a self test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of the TSF], the TSF*].

5.1.15 Session locking and termination (FTA_SSL)

Family behaviour

This component is added to the existing CC family FTA_SSL.

Component levelling



FTA_SSL_EXT.1 requires the ability to either lock or terminate a local interactive session.

Management: FTA_SSL_EXT.1

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

a) Specification of the time of user inactivity after which lock-out or termination occurs for an individual user;

b) Specification of the default time of user inactivity after which lock-out or termination occurs;

c) Management of the events that should occur prior to unlocking the session.

Audit: FTA_SSL_EXT.1

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

a) Basic: Any attempts at unlocking a locked interactive session.

FTA_SSL_EXT.1 TSF-initiated session locking

Hierarchical to: No other components

Dependencies: FIA_UIA_EXT.1 User identification and authentication

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection: *lock the session – disable any of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session; terminate the session*] after a security administrator-specified time period of inactivity.

5.2 Security Functional Requirements

5.2.1 Introduction

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3*, with additional extended functional components.

The TOE Security Functional Requirements that appear below in Table 1 are described in more detail in the following subsections. Items marked with * are additional to those contained in [NDPP].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None
FAU_GEN.2	None.	None
FAU_STG_EXT.1	None.	None
FAU_ARP.1 *	Actions taken due to potential security violations	No additional information.
FAU_SAR.1 *	None	None
FAU_SAR.2 *	None	None
FAU_SAR.3 *	None	None
FAU_SEL.1 *	All modifications to the audit configuration that occur while the audit collection functions are operating	No additional information.
FAU_STG.1*	None	None
FAU_STG.3 (1)*	None	None
FAU_STG.3 (2)*	None	None
FCS_CKM.1	None	None
FCS_CKM_EXT.4	None	None
FCS_COP.1(1)	None	None
FCS_COP.1(2)	None	None
FCS_COP.1(3)	None	None
FCS_COP.1(4)	None	None
FCS_COP.1(5)*	None	None
FCS_RBG_EXT.1	None	None
FCS_SSH_EXT.1	Failure to establish an SSH session, Establishment/Termination of an SSH session	Reason for failure, Non-TOE endpoint of connection (IP address) for both successes and failures
FCS_TLS_EXT.1	Failure to establish a TLS session, Establishment/Termination of a TLS session	Reason for failure, Non-TOE endpoint of connection (IP address) for both successes and failures
FCS_HTTPS_EXT.1	Failure to establish a HTTPS session, Establishment/Termination of a HTTPS session	Reason for failure, Non-TOE endpoint of connection (IP address) for both successes and failures

Requirement	Auditable Events	Additional Audit Record Contents
FDP_RIP.2	None.	None
FDP_CMM_EXT.1(1)*	Changes to the type of scanning carried out	No additional information.
FDP_CMM_EXT.1(2)*	Changes to the type of scanning carried out	No additional information.
FDP_CMM_EXT.1(3) *	Changes to the type of scanning carried out	No additional information.
FDP_CMM_EXT.1(4) *	Changes to the type of scanning carried out	No additional information.
FDP_CMM_EXT.2(1) *	Identification of the security violation and action taken	No additional information.
FDP_CMM_EXT.2(2) *	Identification of the security violation and action taken	No additional information.
FDP_CMM_EXT.2(3) *	Identification of the security violation and action taken	No additional information.
FDP_CMM_EXT.2(4) *	Identification of the security violation and action taken	No additional information.
FDP_IFC.1*	None.	No additional information.
FDP_IFF.1*	Decision to on request for information flow	No additional information.
FDP_UCT.1*	Use of data exchange mechanism	No additional information.
FIA_PMG_EXT.1	None.	None
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None
FMT_MOF.1(1)*	Modification to the function behaviour	None
FMT_MOF.1(2)*	Modification to the function behaviour	None
FMT_MOF.1(3)*	Modification to the function behaviour	None
FMT_MTD.1	None.	None
FMT_SMF.1	None.	None
FMT_SMR.2	None.	None
FPT_SKP_EXT.1	None	None
FPT_APW_EXT.1	None	None
FPT_ITT.1	None.	None
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond “success” or “failure”.

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session	No additional information.
FTA_TAB.1	None.	None
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 13 - TOE Security Functional Requirements and Auditable Events

5.2.2 Security Audit (FAU)

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 of the audit functions;
b) All auditable events for the [not specified] level of audit; and
c) [*All administrative actions*;
d) *Specifically defined auditable events listed in Table 13*].

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of Table 13*].

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 of the user that caused the event.

FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to [transmit the generated audit data to an external IT entity] using a trusted channel implementing the [SSH] protocol.

FAU_ARP.1 Security alarms*

FAU_ARP.1.1 The TSF shall take [*action to notify a specified email recipient via email and generate an audit record*] upon detection of a potential security violation.

FAU_SAR.1 Audit review*

FAU_SAR.1.1 The TSF shall provide [*Super Administrator, Reporting Administrator and applicable custom roles*] with the capability to read [*audit information listed in Table 13 - TOE Security Functional Requirements and Auditable* 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.

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.

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*].

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].

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.

FAU_STG.3(1) Action in case of possible audit data loss*

FAU_STG.3.1(1) The TSF shall [*email the Administrator*] if the audit trail exceeds [*75%, 90% of partition space allocated for audit logs*].

FAU_STG.3(2) Action in case of possible audit data loss*

FAU_STG.3.1(2) The TSF shall [*overwrite the oldest stored audit records*] if the audit trail exceeds [*available storage*].

5.2.3 Cryptographic Support (FCS)

Application Note: [NDPP] does not specify that correct cryptographic operation must be validated through compliance with FIPS 140. However, the Canadian Common Criteria Scheme requires that this is done, and so **compliance with FIPS 140 is considered implicit in the following cryptographic requirements**. Certificate numbers are provided in section 6.1.9.

FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with ~~**a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*]**~~ [

- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;
- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [P-521] (as defined in FIPS PUB 186-3, "Digital Signature Standard")
- NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]

and specified cryptographic key sizes [equivalent to, or greater than, a symmetric key strength of 112 bits] ~~**that meet the following:**~~.

FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

Application Note: zeroisation of CSPs (defined in FIPS 140-2 as "security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module") is the final task performed when the appliance is no longer required and the appliance is re-imaged to clear the CSPs.

FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1(1) The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in* [*CBC mode*]] and cryptographic key sizes ***128-bits, 256-bits*, and** [no other key sizes] that meet the following: ~~[~~

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **[**NIST SP 800-38A].

FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) The TSF shall perform [*cryptographic signature services*] in accordance with a ~~**specified cryptographic algorithm**~~ [

a) Digital Signature Algorithm (DSA) with a key size (modulus) of 2048 bits or greater, or

b) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater]

Application Note: Signatures are only used for signed emails (i.e. notifications)

~~**and cryptographic key sizes [assignment: *cryptographic key sizes*]**~~ that meet the following: [

Case: Digital Signature Algorithm

- *FIPS PUB 186-3, "Digital Signature Standard"*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-3, "Digital Signature Standard"*].

FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [SHA-1, SHA-256] and ~~**cryptographic key**~~ **message digest sizes** [160 bits, 256 bits] that meet the following: [*FIPS Pub 180-3, "Secure Hash Standard"*].

FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1(4) The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm **HMAC-**[SHA1, SHA-256] ~~**and cryptographic**~~ key sizes [*128, 256 bits],* **and message digest sizes** [160, 256] **bits** that meet the following: [*FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"*].

FCS_COP.1(5) Cryptographic Operation (for data encryption/decryption)*

FCS_COP.1.1(5) The TSF shall perform [*key wrapping*] in accordance with a specified cryptographic algorithm [*RSA*] and cryptographic key sizes [*1024 bits and 2048 bits*] that meets the following: [*PKCS#1 v2.1*].

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [FIPS Pub 140-2 Annex C: X9.31 Appendix A.2.4 using AES] seeded by an entropy source that accumulated entropy from [a TSF-hardware-based noise source].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

MEG 7 will make use of timer_entropyd on hardware which does not support hardware RNG.

FCS_SSH_EXT.1 SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [*120 seconds*], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [*3*] attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFS 4253, **large** packets **that could cause buffer overflows ~~greater than [*assignment: number of bytes*] bytes~~** in an SSH transport connection are dropped.[2]

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256 [*no other algorithms*].

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH-RSA and [*no other public key algorithms*] as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that the data integrity algorithms used in SSH transport connection is [hmac-sha1, hmac-sha96, hmac-md5, hmac-md5-96].

FCS_SSH_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

FCS_TLS_EXT.1 TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.0, (RFC 2346)] supporting the following ciphersuites:

Mandatory Ciphersuites

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Optional Ciphersuites:

[None].

FCS_HTTPS_EXT.1 HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.2.4 User Data Protection (FDP)

FDP_IFC.1 Subset information flow control*

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on [*subject identity, email, read request*].

FDP_IFF.1 Simple security attributes*

FDP_IFF.1.1 The TSF shall enforce the [information flow control SFP] based on the following types of subject and information security attributes: [*subject identity, password, email addressee list*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [the subject has successfully authenticated and requests access to email for which it is an addressee].

FDP_IFF.1.3 The TSF shall enforce the [use of an encrypted channel for the information flow].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*no additional rules*].

FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] all objects.

FDP_UCT.1 Basic data exchange confidentiality*

FDP_UCT.1.1 The TSF shall enforce the [*information flow control SFP*] to be able to [transmit] user data in a manner protected from unauthorised disclosure.

FDP_CMM_EXT.1(1) Scan operation (AV)*

FDP_CMM_EXT.1.1(1) The TSF shall perform [*real-time Anti Virus scan of traffic*] in accordance with [*specified policies*].

FDP_CMM_EXT.1(2) Scan operation (Spam, Phishing, Reputation)*

FDP_CMM_EXT.1.1(2) The TSF shall perform [*real-time scan of traffic for spam, phishing attempts and to determine message reputation*] in accordance with [*specified policies*].

FDP_CMM_EXT.1(3) Scan operation (Compliance)*

FDP_CMM_EXT.1.1(3) The TSF shall perform [*real-time scans of traffic to determine compliance with dictionaries and DLP*], in accordance with [*specified policies*].

FDP_CMM_EXT.1(4) Scan operation (Filtering, Image Analysis)*

FDP_CMM_EXT.1.1(4)d The TSF shall perform [*real-time scans of traffic to apply file filtering, email filtering and image analysis*] in accordance with [*specified policies*].

FDP_CMM_EXT.2(1) Scan actions (Virus)*

FDP_CMM_EXT.2.1(1) Upon detection of [*a file-based virus*] the TSF shall [*perform the Primary and Secondary action(s) specified by an Administrative user*:

a) *Primary:*
   - *Block/Replace Content/Clean/Allow*

b) *Secondary:*
   - *Quarantine*
   - *Notifications*]

FDP_CMM_EXT.2(2) Scan actions (Phishing, Reputation)*

FDP_CMM_EXT.2.1(2) Upon detection of [*spam, phishing attempts and bad message reputation*] the TSF shall [*perform the Primary and Secondary action(s) specified by an Administrative user:*

a) *Primary:*
   - *Block/[Modify/Add] Headers/Allow*

b) *Secondary:*
   - *Quarantine*
   - *Notifications*]

FDP_CMM_EXT.2(3) Scan actions (Dictionaries, DLP)*

FDP_CMM_EXT.2.1(3) Upon detection of [*non-compliance with dictionaries and DLP*] the TSF shall [*perform the Primary and Secondary action(s) specified by an Administrative user:*

a) *Primary:*
   - *Block/Replace Content/Allow*

b) *Secondary:*
   - *Quarantine*
   - *Notifications*]

FDP_CMM_EXT.2(4) Scan actions (Compliance, Filtering, Image Analysis)*

FDP_CMM_EXT.2.1(4) Upon detection of [*email content that does not comply with file filtering, email filtering and image analysis policies*] the TSF shall [*perform the Primary and Secondary action(s) specified by an Administrative user:*

a) *Primary:*
   - *Block/Replace Content/Allow*

b) *Secondary:*
   - *Quarantine*
   - *Notifications*]

5.2.5 Identification and Authentication (FIA)

*Application Note: These identification and authentication (FIA) SFRs applies to users (administrators) of services available from the TOE directly, and not services available by connecting through the TOE. Therefore, uses of the term "user" have been refined to "**administrative** user".*

FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters ["!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"];

b) Minimum password length shall settable by the **Super Administrator**, and support passwords of 15 characters or greater.

Application Note: The intent of this caveat is that the **Super Administrator** *is able to specify, for example, that passwords contain at least 1 upper case letter, 1 lower case letter, 1 numeric character, and 1 special character, and the TOE enforces this restriction.*

FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [No other actions].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

Application Note: This requirement applies to users (administrators) of services available from the TOE directly, and not services available by connecting through the TOE.

FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [none[3]] to perform administrative user authentication.

FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only [*obscured feedback*] to the administrative user while the authentication is in progress **at the local console**.

[3] The meaning of this selection in [NDPP] is not completely clear. Use of the selection "none" indicates that the local password-based authentication mechanism is the only one being addressed by this requirement.

5.2.6 Security Management (FMT)

Application Note: The term "Security Administrator" used in [NDPP] has been refined to reflect the term "Super Administrator" used in the TOE.

FMT_MTD.1 Management of TSF Data (for general TSF data)

FMT_MTD.1.1 The TSF shall restrict the ability to [*manage*] the [*TSF data*] to [the **Super Administrator**].

Application Note: The word "manage" includes but is not limited to create, initialize, view, change default, modify, delete, clear, and append. TSF data here is taken to mean all data that is used to support the correct operation of the TSF and can be modified through a provided interface.

FMT_MOF.1(1) Management of security functions behaviour (Reporting)

FMT_MOF.1.1(1) The TSF shall restrict the ability to [modify the behaviour of, determine the behaviour of] the functions[*:*

a) Appliance audit logging]

to [*the Reports Administrator, Super Administrator and applicable custom roles*].

FMT_MOF.1(2) Management of security functions behaviour (Maintenance)

FMT_MOF.1.1(2) The TSF shall restrict the ability to [modify the behaviour of, determine the behaviour of] the functions[*:*

a) Real-time virus scanning

b) Operation of the appliance

c) Update virus scan signatures]

to [*the Super Administrator and applicable custom roles*].

FMT_MOF.1(3) Management of security functions behaviour (Email Policies)

FMT_MOF.1.1(3) 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

e) Configuration of alert notifications from the appliance]

to [*the Email Administrator, Super Administrator and applicable custom roles*].

FMT_SMF.1 Specification of Management Functions

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

- [*Ability to administer the TOE locally and remotely;*
- *Ability to update the TOE, and to verify the updates using[published hash]*

capability prior to installing those updates;
- *Ability to configure the cryptographic functionality;*
- ***Ability to set the date and time***].

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- [*Super Administrator,*
- *Email Administrator,*
- *Reports Administrator*
- *other configurable roles*][4].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- [*Authorized Administrator role shall be able to administer the TOE locally;*
- *Authorized Administrator role shall be able to administer the TOE remotely;*]

are satisfied.

5.2.7 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure and modification] when it is transmitted between separate parts of the TOE.

FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_APW_EXT.1.1 Extended: Protection of administrator passwords

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

FPT_STM.1 Reliable Time Stamps

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

FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide **Super Administrators** the ability to query the current version of the TOE firmware/software.

[4] Note that the term "Authorized Administrator" from [NDPP] has been expanded, in this element only, to show the range of authorized administrator roles available in the TOE.

FPT_TUD_EXT.1.2 The TSF shall provide **Super Administrators** the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [published hash] prior to installing those updates.

FPT_TST_EXT.1 Extended: TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests [during initial start-up **(on power on)**] to demonstrate the correct operation of [the TSF].

5.2.8 TOE Access (FTA)

FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [terminate the session] after a **Super Administrator- or applicable custom administrator-**specified time period of inactivity.

FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate **a remote** interactive session after a [**Super Administrator -- or applicable custom administrator** *configurable time interval* ***between 3 and 30 minutes (with a default of 10 minutes)*** *of session inactivity*].

FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow **Administrator**-initiated termination of the **Administrator's** own interactive session.

FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing an **administrative user** session, the TSF shall display a **Super Administrator -- or applicable custom administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

5.2.9 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall **use [SSH, TLS] to** provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server(SSH), [authentication server(TLS)]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~**modification or**~~ disclosure **and detection of modification of the channel data**.

FTP_ITC.1.2 The TSF shall permit *the TSF*, ***or the authorized IT entities*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*all trusted communications with an IT peer*].

FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall **use [TLS/HTTPS] to** provide a **trusted** communication path between itself and [remote] ~~users~~ **administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure **and detection of modification of the communicated data**.

FTP_TRP.1.2 The TSF shall permit [remote ~~users~~ **administrators**] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial ~~user~~ **administrator** authentication *and all remote administrative actions*].

5.3 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
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition

Assurance Class	Assurance Components	
	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 14 - Assurance Requirements: EAL2+ALC_FLR.2

The assurance requirements listed above are hierarchical to those in [NDPP], providing compliance with the protection profile.

5.4 Rationale for TOE Security Requirements

5.4.1 TOE Security Functional Requirements

Security Objective	Mapping Rationale
O.PROTECTED_COMMUNICATIONS	Communications protection is provided through use of encrypted services for data transfer (FPT_ITT.1, FTP_ITC.1), and for administrator sessions (FTP_TRP.1). These services are supported by functions to manage encryption/decryption (FCS_COP.1(1)), key generation and management (FCS_CKM.1, FCS_CKM_EXT.4, FCS_RBG_EXT.1, FPT_SKP_EXT.1), digital signature FCS_COP.1(2), and hashing (FCS_COP.1(3), FCS_COP.1(4)). Specific services are provided for TLS, SSH and HTTPS (FCS_TLS_EXT.1, FCS_SSH_EXT.1, FCS_HTTPS_EXT.1). Encryption functions can be configured by an administrator (FMT_SMF.1).
O.VERIFIABLE_UPDATES	The TOE provides functionality to generate hash values (FMT_SMF.1, FCS_COP.1(3)) that can be used only (FMT_MOF.1(2)) by an administrator to check the validity of signature updates (FPT_TUD_EXT.1).
O.SYSTEM_MONITORING	The TOE generates audit records (FAU_GEN.1) that are attributable to users (FAU_GEN.2), and also generates alarms (FAU_ARP.1). The set of audit events is selectable (FAU_SEL.1). Only an administrator can configure audit (FMT_MOF.1(1)). Audit records may be exported for storage (FAU_STG_EXT.1).
O.DISPLAY_BANNER	The TOE generates a warning banner following login (FTA_TAB.1).

O.TOE_ADMINISTRATION	The TOE controls login (FIA_UIA_EXT.1) using passwords (FIA_PMG_EXT.1) that are not stored in clear (FPT_APW_EXT.1). Entered passwords are not displayed on screen (FIA_UAU.7). Protection is provided through session suspension or expiry (FTA_SSL_EXT.1, FTA_SSL.3), and protection of communication paths against modification or disclosure (FTP_TRP.1). A number of security management roles are defined (FMT_SMR.2), and the ability to manage TSF data is restricted (FMT_MTD.1).
O.RESIDUAL_INFORMATION_CLEARING	The TOE provides clearing of resources on allocation (FDP_RIP.2).
O.SESSION_LOCK	The TOE provides the capability to lock a local session following a period of inactivity (FTA_SSL_EXT.1), and also to terminate remote sessions after a period of inactivity (FTA_SSL.3, FTA_SSL.4).
O.TSF_SELF_TEST	The TOE runs a suite of self-tests following power on (FPT_TST_EXT.1).
O.AUDIT_PROTECT	The audit records are protected (FAU_STG.1), with safeguards against the audit trail becoming full (FAU_STG.3(1), FAU_STG.3(2). The TOE is also able to send storage records to external storage (FAU_STG_EXT.1). Only an administrator can configure audit (FMT_MOF.1(1)). The TOE also controls read access to the audit records (FAU_SAR.2).
O.AUDIT_REVIEW	The TOE provides the ability to review audit records (FAU_SAR.1), and to selectively search and sort the records (FAU_SAR.3). Access to this functionality is restricted (FMT_MOF.1(1)).
O.MAL_CONTENT	The TOE scans traffic to assure adherence to specified policies (FDP_CMM_EXT.1(3), FDP_CMM_EXT.1(4)). Upon detection of non-compliant traffic the TOE can be configured to take specified actions(FDP_CMM_EXT.2(3), FDP_CMM_EXT.2(4), FAU_ARP.1). Ability to configure the options is restricted (FMT_MOF.1(3)).
O.TIME_STAMPS	The TOE provides time stamps for audit records (FPT_STM.1), and the ability to set the date and time (FMT_SMF.1, FMT_MTD.1).
O.SECURE_CHK	The TOE scans traffic for unwanted and damaging traffic (FDP_CMM_EXT.1(1), FDP_CMM_EXT.1(2)). Upon detection of such traffic the TOE can be configured to take specified actions (FDP_CMM_EXT.2(1), FDP_CMM_EXT.2(2) , FAU_ARP.1).

	Ability to configure the options is restricted (FMT_MOF.1(3)).
O.DECRYP	The TOE has the ability to decrypt data prior to content inspection, and to re-encrypt it (FCS_COP.1(1), FCS_COP.1(5)).
O.SECURE_MAIL	The TOE has the ability to manage encrypted storage and transmission of email on behalf of registered users (FDP_IFC.1, FDP_IFF.1, FDP_UCT.1).

Table 15 - Security objective mapping rationale

5.4.2 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. Selection of this assurance package aims to support the assurance needs of McAfee customers.

5.5 Rationale for explicitly stated security requirements

Table 16 - Explicitly stated SFR rationale, presents the rationale for the inclusion of the explicit requirements found in this Security Target. No rationale is presented for explicitly stated requirements introduced by [NDPP], since their inclusion in [NDPP] is, in itself, the rationale for their inclusion in this ST.

Explicit Requirement	Identifier	Rationale
FDP_CMM_EXT.1	Scan operation	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_CMM_EXT.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.

Table 16 - Explicitly stated SFR rationale

5.6 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.

Items marked ^ are components defined by the [NDPP], which does not perform dependency analysis. The dependencies have therefore been inferred from an analysis of the new components.

Functional Component	Dependency	Included/Rationale
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1 is included. Dependency on FIA_UID.1 met by FIA_UIA_EXT.1, which includes that functionality.
FAU_STG_EXT.1^	FTP_ITC.1	Yes
FAU_ARP.1	FAU_SAA.1	Dependency is met using FDP_CMM_EXT.2, which includes that functionality.
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, FMT_MTD.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.3 (1)	FAU_STG.1	Yes
FAU_STG.3 (2)	FAU_STG.1	Yes
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Yes, through FCS_COP.1 and FCS_CKM_EXT.4
FCS_CKM_EXT.4^	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, using FCS_CKM.1
FCS_COP.1(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Yes, using FCS_CKM.1 and FCS_CKM_EXT.4 (which provides equivalent functionality to FCS_CKM.4)
FCS_COP.1(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Yes, using FCS_CKM.1 and FCS_CKM_EXT.4 (which provides equivalent functionality to FCS_CKM.4)
FCS_COP.1(3)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Yes, using FCS_CKM.1 and FCS_CKM_EXT.4 (although dependencies are not relevant as

		this component relates to hashing only)
FCS_COP.1(4)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Met using FCS_CKM.1 and FCS_CKM_EXT.4 (which provides equivalent functionality to FCS_CKM.4)
FCS_COP.1(5)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Partially met using FCS_CKM_EXT.4 (which provides equivalent functionality to FCS_CKM.4). The dependency on FDP_ITC.1 is considered inappropriate, since the elements are not relevant to the method of importing keys via a user interface (described under section 6.1.9)
FCS_RBG_EXT.1^	None	Yes
FCS_HTTPS_EXT.1^	FCS_TLS_EXT.1	Yes
FCS_SSH_EXT.1^	None	Yes
FCS_TLS_EXT.1^	None	Yes
FDP_RIP.2	None	Yes
FDP_CMM_EXT.1(1)	None	Yes
FDP_CMM_EXT.1(2)	None	Yes
FDP_CMM_EXT.1(3)	None	Yes
FDP_CMM_EXT.1(4)	None	Yes
FDP_CMM_EXT.2(1)	FDP_CMM_EXT.1	Yes
FDP_CMM_EXT.2(2)	FDP_CMM_EXT.1	Yes
FDP_CMM_EXT.2(3)	FDP_CMM_EXT.1	Yes
FDP_CMM_EXT.2(4)	FDP_CMM_EXT.1	Yes
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 is included. The information security attributes subject

		identity, password and email addressee list do not have default values, making FMT_MSA.3 unnecessary, and thereby satisfying the dependency.
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1, FDP_ACC.1 or FDP_IFC.1	Yes, using FTP_ITC.1 and FDP_IFC.1
FIA_PMG_EXT.1^	FIA_UAU_EXT.2	Yes
FIA_UIA_EXT.1^	None	Yes
FIA_UAU_EXT.2^	FIA_PMG_EXT.1	Yes
FIA_UAU.7	FIA_UAU.1	Dependency is met using FIA_UIA_EXT.1
FMT_MOF.1(1)	FMT_SMR.2, FMT_SMF.1	Yes
FMT_MOF.1(2)	FMT_SMR.2, FMT_SMF.1	Yes
FMT_MOF.1(3)	FMT_SMR.2, FMT_SMF.1	Yes
FMT_MTD.1	FMT_SMR.2, FMT_SMF.1	Yes
FMT_SMF.1	None	Yes
FMT_SMR.2	FIA_UID.1	Dependency is met using FIA_UIA_EXT.1
FPT_ITT.1	None	Yes
FPT_APW_EXT.1^	FIA_UAU_EXT.2	Yes
FPT_SKP_EXT.1(2)^	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, using FPT_CKM.1
FPT_STM.1	None	Yes
FPT_TUD_EXT.1^	None	Yes
FPT_TST_EXT.1^	None	Yes
FTA_SSL_EXT.1^	FIA_UIA_EXT.1	Yes
FTA_SSL.3	None	Yes
FTA_SSL.4	None	Yes
FTA_TAB.1	None	Yes
FTP_ITC.1	None	Yes
FTP_TRP.1	None	Yes

Table 17 - SFR dependencies

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of 8 Security Functions:

- Anti-Virus & Anti-Spam
- Compliance
- Quarantine Management
- Secure Web Delivery
- Security Management
- Audit and Alerts
- Action and Remediation
- Cryptographic Operations

6.1.1 Anti-Virus & Anti-Spam

The Anti-Virus security function for the McAfee MEG TOE provides the scanning functionality to detect specified traffic that may pose a threat to internal networks. The MEG 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.

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_CMM_EXT.1(1) and FDP_CMM_EXT.1(2) – Anti-Virus & Anti-Spam Scanning Processes

The McAfee MEG 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 Anti-Virus subsystem and is supported by the MEG 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 GTI File Reputation — 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.

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_CMM_EXT.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_CMM_EXT.2 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
- Blocking of email messages

FDP_CMM_EXT.2(1) and FDP_CMM_EXT.2(2) –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 MEG 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_CMM_EXT.2 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 primary and secondary actions to take. In contrast, Scanning (FDP_CMM_EXT.1) is the process by which the appliance intercepts traffic and applies detection rules to simply identify a target characteristic. FDP_CMM_EXT.2 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
- 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 6.1.7.

6.1.2 Compliance

This function uses content rules to prevent SMTP e-mail messages with unwanted content reaching their

intended recipients. It utilizes the core scanning capability described in the Anti-Virus security function to identify suspect email messages and/or email attachments and take specified action upon detection of restricted content. Content scanning scans email for indicators of restricted content, as specified by the administrator.

FDP_CMM_EXT.1(3), FDP_CMM_EXT.1(4), FDP_CMM_EXT.2(3) and FDP_CMM_EXT.2(4) – Content Scanning

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.

The TOE provides for full scanning of email traffic through the device to identify offensive language. This is achieved through provision of a library of dictionaries, and the ability to create custom dictionaries. The appliance can be configured to detect individual words, or crossing of a score based threshold, following which a defined action is taken.

The TOE can also be used to identify and monitor critical data on the TOE, and to take action when the data is detected in email traffic. The Data Loss Prevention interface allows the administrator to create a policy that assigns data loss prevention actions against the registered document categories. The Data Loss Prevention feature can be used to restrict the flow of sensitive information sent in email messages by SMTP through the appliance. For example, by blocking the transmission of a sensitive document such as a financial report that is to be sent outside of the organization. Detection occurs whether the original document is sent as an email attachment, or even as just a section of text taken from the original document.

The TOE has the capability to employ image analysis techniques to filter mages (e.g. pornography) in email that do not conform to specified policy guidelines. The technology uses a number of proprietary algorithmic based modules to analyse images. Initially the engine eliminates features in the image based upon colour; removing areas of colour which the software understands cannot be associated with skin. This engine allows for regional skin colour variations. A further module then enhances areas of interest within the image and using edge, curvature and body size algorithms produces a probability output as to whether the image is potentially pornographic.

The TOE allows for the creation of rules to allow control over the movement of files as email attachments according to their file name extension (e.g. .bmp, .exe), file format, name or size (SMTP only).

The TOE allows for the creation of rules to allow control over the movement of email according to the message size, attachment size or attachment count.

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 non-compliant with policy, 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.

6.1.3 Quarantine Management

FDP_CMM_EXT.2(1), FDP_CMM_EXT.2(2), FDP_CMM_EXT.2(3), FDP_CMM_EXT.2(4)

The TOE can be configured to apply two levels of actions when a detection is made.

Primary Action

In general, a client MTA sends an email to the TOE, and the TOE scans the message. If no detections are found, the message is delivered it to its intended recipients on the server MTAs. However, if a scanner triggers a detection, a number of primary and secondary actions can be applied to the message that contains the detection.

A primary action is defined as “What happens to the message coming from the client MTA to the server MTA?":

- Was it blocked?
- Was it modified and then delivered?
- Was it delivered to the recipient without modification?

The message is scanned by all scanners. If multiple scanners trigger, the primary action that has the highest priority is applied. For example, if the file filtering policy is set to Allow Through (Monitor), and the anti-spam policy was set to Accept and Drop the data (Block), then the Accept and Drop the data (Block) action applies.

Primary actions behaviour

Type	Action	Sender perspective	Recipient perspective	Kernel mode blocking
Blocking	Deny Connection	Message Rejected. Might receive notification that the message was delivered.	No message is received.	Yes
Blocking	Refuse the data and return an error code	Message Rejected. Might receive notification that the message was delivered.	No message is received.	No
Blocking	Accept and drop the data	Message Rejected. Might receive notification that the message was delivered.	No message is received.	No
Modify	Replace the content with an alert	Message Accepted. It appears to the sender that the message is delivered.	Replacement message (alert received)	No
Monitor	Allow Through	Message Accepted.	Message received	No

Secondary Action

A secondary action is defined as “What additional actions will happen due to the scanner triggering a detection?”. The message is scanned by all scanners. If multiple scanners trigger, the secondary actions are aggregated together. For example, if the file filtering policy is set to Annotate and deliver original to a list, and the anti-spam policy is set to Annotate and deliver original to a list, then only one notification is sent.

Available actions

If a scanner triggers a detection, these primary actions are available:

a) **Deny Connection (Block)** — Blocks the message from being delivered, returns a 550 SMTP code to the sending MTA, places the connecting IP address in the Kernel Mode Block list.

b) **Refuse the data and return an error code (Block)** — Blocks the message from being delivered, returns a 550 SMTP code to the sending MTA.

c) **Accept and Drop the data (Block)** — Blocks the message from being delivered, returns a 250 SMTP code to the sending MTA.

d) **Replace the content with an alert (Modify)** — Replaces any detected content with a configurable alert and delivers the modified Email to its intended recipients.

e) **Allow Through (Monitor)** — Lets the message pass to its intended recipients, but information is retained within the logs and reports.

The following *secondary* actions can also be configured:

Actions applied to the original message:

Quarantine — Quarantines the message in the scanner's quarantine queue (for example, the anti-virus scanner's quarantine).

Annotate and deliver the original to sender — McAfee Email Gateway sends an email to the original sender of the message that contains a configurable notification message and has the original message included as an attachment.

Annotate and deliver original to a list — McAfee Email Gateway sends an email to a configurable list of recipients that contains a configurable notification message, and has the original message as an attachment.

Notification actions :

a) Deliver to the sender of the original email.

b) Deliver to the recipient(s) of the original email.

c) Deliver a notification to a list.

Modification actions:

a) **Quarantine** — Quarantines the modified message in the scanner's quarantine queue (for example, the anti-virus scanner's quarantine).

b) **Forward modified to a list**.

c) **Annotate and deliver modified to a list** — The TOE generates an Email with a configurable notification, with the modified Email as an attachment. This is delivered to the original sender of the Email.

d) **Deliver to the sender of the original email**.

McAfee Quarantine Management allows consolidation of quarantine management and spam learning for the MEG 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.

6.1.4 Secure Web Delivery

FDP_UCT.1, FDP_IFC.1, FDP_IFF.1

The TOE provides users with a means to store and access emails securely in situations where the user's mail server does not provide sufficient assurance of confidentiality. This feature is known as Secure Web Delivery.Two approaches are supported for email traffic that policy has defined as sensitive, as follows:

Pull – MEG stores the emails in an encrypted form. An email is sent to the recipient that a sensitive email has arrived. The recipient sets up an account on MEG (if they do not have one already), and can then log in and view the email using a browser.

Push – MEG sends the email to the recipient's mail server in an encrypted form, together with a notification of its arrival. When the recipient selects the mail to be read, a browser login is performed, the email is sent back to MEG for decryption and is viewed via the browser.

Passwords for web mail users are not store in plaintext. They are hashed using a salted HMAC 256. The Web Mail Client has an increasing timeout of 2,4,8…64 (seconds) between login attempts.

6.1.5 Security Management

The McAfee MEG TOE provides security management functions and tools to manage the security features described within this security target.

There are three methods of accessing the User Interface framework:

1. Browser-based session on the web console machine. This provides access to the GUI 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. 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, the User Interface Framework provides the primary administrator interface into the TOE, providing TOE Administrators with GUI access to: the appliance configuration files; the appliance console (as described above); the logging subsystem, which manages access to appliance audit logs and reports; and the updater to download and apply signature files (and any necessary associated engine patches to run the .dat signature files).

The browser-based user interface is implemented in javascript and HTML, and connections (HTTP over SSL/TLS) are managed by Apache Web Server Software. SSL sessions are encrypted using a self-signed certificate. Commands and data are transferred over HTTPS using Direct Internet Message Encapsulation (DIME) as the encoding mechanism. An Apache module has been written specifically for the appliance to handle the decoding of DIME, and to invoke the appropriate system commands, to

update or retrieve configuration files and to retrieve audit records.

Configuration data managed through this security function is managed and stored in the file system supported by the underlying MEG Operating System. The TOE enforces Identification and Authentication prior to allowing access to TOE Security Management functions.

FTP_TRP.1 Trusted path

Administrator access to the TOE is managed within the internal or external network via a web browser over a HTTPS protocol connection. The secure connection helps to assure integrity and confidentiality.

FMT_SMR.2 Role Based Access

The TOE supports role based access to the MEG appliance through a number of default roles (which are configurable). These roles can be used both locally and remotely. It also provides the facility to create new user roles with defined limited responsibilities.

FTA_SSL.3 TSF-initiated termination, FTA_SSL.4 User-initiated termination, FTA_SSL_EXT.1 TSF-initiated session locking

Administrative access to the TOE is established via a supported web browser normally 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 (whether local or remote) also automatically closes after an Administrator specified term of inactivity (between 3 and 30 minutes). The default setting enforces termination of sessions after 10 minutes of inactivity.

FMT_SMF.1, FPT_TUD_EXT.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 MEG 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.

Selection of the About the Appliance tab allows the administrator to check the version of the current TOE software and the packages installed. The TOE can maintain effectiveness against current threats by obtaining updates from the McAfee website. Checks for updates can be scheduled to take place automatically at any time. Updates can be run immediately, or held for testing prior to deployment.

The following can be regularly downloaded:

- Anti-spam rules. These define what is spam. Some anti-spam rules are updated regularly, but McAfee also produces extra rules to combat sudden outbreaks of new types of spam. Anti-

phishing rules are also downloaded when the anti-spam rules are downloaded;

- Anti-spam engine. This uses anti-spam rules to scan email messages for spam;
- Anti-virus signatures in .dat files;
- Anti-virus engine. This uses the .dat files to scan email messages for viruses;
- Streaming updates. The appliance can also be updated with critical rules more frequently, possibly every few minutes.

Once a new file (e.g .dat or engine) is downloaded the TOE will extract the file (encoded using McAfee proprietary algorithms) and the associated hash value. The integrity of the downloaded file is then verified using the SHA1 hash function to compare the result with the hash value extracted from the encrypted file. This is performed before the file is made available to the relevant plugin for activation.

Management of the TOE and Restrictions – FMT_MTD.1

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 MEG 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 MEG operating system.

Initially, the appliance has one administrator account— the Super Administrator, scmadmin — which has access to all the appliance features. Using the scmadmin account, any number of other accounts can be created, including more Super Administrators. The appliance will probably be used by many people, where each user has a different requirement.

For example, two users may need full access to all the appliance features, while another four users need only to view the reports. This would require two user accounts that are like the Super Administrator, and four user accounts for administering reports. These type of requirements are referred to as roles.

The appliance has several roles already defined. A Super Administrator can see all the menus and buttons that are available from the interface. The other administrators can see fewer menus and buttons. As user accounts are created, each account is assigned a role. New roles can also be created.

FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3) – TSF Control Over Management Functions

The TOE restricts the ability to access the Management GUI through the MEG 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 6.1.5.2.

Only identified and authenticated administrators are able to manage TOE functions. The administrator must be assigned to a role with the necessary permission to manage the function:

a) An administrator with permissions 'Email Configuration' and 'Email policies' can configure the anti-virus scanning policies for emails.

b) Only an identified and authenticated administrator is able to enable/disable/modify the operation of the TOE, in accordance with the role to which they are assigned.

c) An administrator with permissions 'System Administration' and 'Component management' can select to automatically update the packages (including the virus scan signatures) and can use the Package Installer to install a specific file.

d) An administrator with permissions 'System Administration' and 'Access logging, alerting and SNMP' can select the level of logging and the individual events to be audited.

FCS_SSH_EXT.1 SSH

The administrator can configure the TOE to permit SSH client to be used for export of audit data.

FPT_TST_EXT.1 TSF Testing

At power-on the hardware will perform standard BIOS tests. This includes a check for the presence of memory. The TOE appliances make use of ECC RAM, and should there be an uncorrectable error the appliance will not boot.

The TOE executes a set of self-tests to demonstrate correct operation of the TSF. These tests cover cryptographic algorithm tests, software/firmware integrity test, and critical functions test. An MD5 hash is stored for each of the files that comprise the software TOE. At boot the hashes are recalculated and compared with the stored values.

FDP_RIP.2 Full residual information protection

Packets are processed within the Linux TCP socket send queue in a manner that ensures all residual data in the socket buffer is overwritten before the packet is sent. All drivers that do not explicitly clear frame data before use, or which may DMA or transfer data beyond the buffer end onto the wire, will call skb_pad to perform the requisite clearing of data. This function checks the buffer for trailing bytes, and where these exist they are overwritten with zeros. If the buffer already contains sufficient data to fill the frame it is untouched; otherwise it is extended.

6.1.6 Identification & Authentication

Access to the MEG 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 MEG Operating System environment. The computer used for this purpose can be a general purpose machine running Microsoft Internet Explorer 7.0, 8.0 or 9.0, or Firefox 3.0, 3.5 or 4.0 with SSL v3 or TLS v1 encryption, with ActiveX enabled.

FIA_UID_EXT.1, FIA_UAU_EXT.2, FIA_UAU.7, FPT_APW_EXT.1 - Identification and Authentication

Administrators gain access to the TOE appliance by opening a secure browser session using HTTPS on the Administrator Management Computer. The MEG 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. The entered password is not displayed on the screen. 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.

If the password has expired (after the configured number of days) the administrator is required to select and enter a new password, confirming the choice through re-entry of the old password.

Passwords for authentication are not stored in plaintext, and use a salted MD5 hash, protected by restricted file permissions.

Passwords for the administration interface are not stored in plaintext, and use a salted SHA1 (160 bits with the first 32 bits being the salt), protected by restricted file permissions.

FIA_PMG_EXT.1 – Password Management

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 8 characters. Only passwords with a minimum of 8 characters will be accepted by the MEG appliance in its evaluated configuration. The administrator is also able to specify through the Password Management interface the requirement to include a mix of upper and lower case letters, numbers an special characters within the password. The permitted special characters include "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". The administrator can also configure the maximum lifetime (in days) for the password, and the minimum number of characters that must be altered when the password is changed.

The TOE enforces a 5 second delay between successive login attempts.

FTA_TAB.1 – Default TOE access banners

The TOE will optionally display a configurable access banner when an administrator session is requested. The administrator must confirm acceptance of the banner before the logon screen is displayed.

6.1.7 Audit and Alerts

The McAfee MEG Appliance generates audit records and alarms 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 MEG 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 6.1.5.2.

FAU_GEN.1, FAU_GEN.2, FAU_ARP.1 – Audit Generation

The TOE generates audit records for the following events (see Table 13 for additional detail):

- Success/Failure of Login to MEG Appliance User Interface;
- Success/Failure of MEG 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;
- 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 MEG 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: Anti-Virus, Anti-Spam & Phish, Content Filter, Other.

FPT_STM.1 – Audit records by accurate time stamps

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

FAU_STG.1, FAU_STG.3(1), FAU_STG.3(2) – Storage and Protection of Audit Records

Audit records are stored within the McAfee MEG appliance through the use of a SQL compliant, open source object-relational database management system used within the McAfee MEG 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 MEG 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_STG_EXT.1 External Audit Trail Storage

The TOE provides a facility to export audit data to an external storage device for long term storage, using SSH. If the connection to external storage is lost the TOE will continue to store records on the TOE, overwriting the oldest stored audit records if the audit trail exceeds available storage.

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

The McAfee MEG 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 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, content events;
System Reports	System events including User Interface, updates, hardware and network events.

6.1.8 Action and Remediation

FDP_CMM_EXT.2(1), FDP_CMM_EXT.2(2), FDP_CMM_EXT.2(3), FDP_CMM_EXT.2(4) – 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 MEG application. The McAfee MEG 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.

Content Filtering Actions

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

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

FDP_CMM_EXT.2(1), FDP_CMM_EXT.2(2), FDP_CMM_EXT.2(3), FDP_CMM_EXT.2(4) - 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.

6.1.9 Cryptographic Operations

All cryptographic operations are provided by a FIPS 140 validated module.

FCS_COP.1(1)

AES in CBC mode is used to support encrypted communications for administrative access and mail operations. It is used to support the implementation of TLS and SSH. Keys are generated in accordance with ANSI X9.31 (see below FCS_RGB_EXT.1).

FCS_COP.1(2) Digital Signature

When using Secure Web Mail, the TOE generates a notification Email which it sends to the recipient which tells them that they have an Email that needs to be viewed. This notification can be S/MIME signed (using either DSA or rDSA) so that it does not get picked up as spam.

FCS_COP.1(4) Keyed Hash

A keyed hash (HMAC-SHA256) is used for integrity protection as part of the TLS, SSH and HTTP protocols.

FCS_COP.1(3) - .dat file Message Digest verification

The TOE provides a verification process for downloaded .dat threat signature files. 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.

FCS_COP.1(5), FCS_CKM.4 Cryptographic operation

The TOE provides the capability to decrypt and scan mail and attachments that are encrypted with PGP or S/MIME, using preloaded keys. Keys are imported into the TOE using the graphical user interface. This allows detail about the key to be entered (name, email address, passphrase), and the key to be loaded from a file. Since this operation is done under user control the dependency on FDP_ITC.1 is not appropriate. There is also an option to select and delete (zeroise) keys from the list.

FCS_HTTPS_EXT.1, FCS_TLS_EXT.1, FCS_COP.1, FCS_CKM.1, FCS_CKM_EXT.4

The TOE provides cryptographic services to support remote management using an HTTPS GUI.

Cryptographic keys are stored in clear text, and protected with restricted file permissions. There is no interface available for viewing them. Private asymmetric keys can be exported.

The TOE uses OpenSSL to generate asymmetric cryptographic keys using a domain parameter generator and a random number generator that meet ANSI X9.80 with an equivalent key strength of at least 112 bits (DSA and rDSA keys). Domain parameters used in finite field-based key establishment schemes meet NIST Special Publication 800-56A, and domain parameters used in RSA-based key establishment schemes meet NIST Special Publication 800-56B. These keys are used in support of the digital signature operations described under FCS_COP.1(2).

OpenSSL is used to clear keys on memory. The swap partition will be cleared on shutdown. Cryptographic key files on the appliance will be shredded/securely deleted when deleted. Secret keys when deleted from the appliance are zeroized by overwriting six times with a random pattern that is changed before each write. In FIPS mode, when the appliance is shutdown, the SWAP area is wiped such that secret key information that may of at some point been written out is no longer available. FIPS mode is disabled by reinstalling the appliance which removes all Key Security Parameters.

FCS_RBG_EXT.1

The RBG is the X9.31 compliant Linux kernel Random Number Generator. Currently the TOE uses version 2.6.27 of the Linux kernel. The TOE uses the Timer Entropy Daemon (TED) as a source of entropy. This uses as a source of entropy the difference between hardware and software clocks. Entropy is obtained by the TED. This program feeds the /dev/random device with entropy-data (random values) read from timers. It does this by measuring how much longer or shorter a sleep takes (this fluctuates by a few microseconds). The time for a sleep jitters because the frequency of the timer clocks change when they become colder or hotter (and a few other parameters). This process produces around 500 bits per second.

FCS_SSH_EXT.1 SSH

The SSH client is based upon the open source OpenSSH package (portable branch from www.openssh.org). The appliance maintains configuration for SSH client in ssh-settings section of network.xml. All attribute settings are configured. The default ciphers are: AES128-cbc and AES 256-cbc.

The scp command is used for copying off logs and configuration from the appliance to remote devices.

The open sshd daemon responds to rekey requests from the client as appropriate. The SSH client on the appliance is configured to rekey after 2^28 (256M) bytes of data. The value can be changed by modifying the appliance XML configuration.

If an erroneously large packet is received, the extraneous data is ignored.

The administrator can change the SSH (ssh client) algorithms by modifying the Ciphers and MAC attributes in the ssh-settings of network.xml and saving the appliance configuration.

DH group 14 key exchange is the default setting for SSH.

The available data integrity algorithms are hmac-sha1, hmac-sha96, hmac-md5, hmac-md5-96.

FCS_TLS_EXT.1

The TOE implements TLS 1.0 (RFC 2346)] supporting the following ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA.

There is an option for X509 Client Authentication (CAC device).

FCS_HTTPS_EXT.1

HTTPS (using TLS 1.0) is used to protect remote administrator sessions.

There is an option for X509 Client Authentication (CAC device), but otherwise Client-Authentication uses form based authentication over HTTPS.

For X509 authentication distinguished name attributes are mapped to on appliance roles, which allows for varying levels of authorization.

Radius and Kerberos authentication are supported as options.

FPT_SKP_EXT.1

All private cryptographic keys are secured against unauthorized disclosure. There are no pre-shared symmetric keys on the TOE. Private asymmetric keys are stored in clear text, and protected with restricted file permissions. These private keys can be exported, but there is no interface available for viewing them.

FPT_ITT.1 Internal TSF Data Transfer Protection

Data is transmitted between different parts of the TOE when clustering is used. Such communication is protected using TLS.

FCS_COP.2 Digital Signature

When using secure web mail, the TOE generates a notification Email which it sends to the recipient which tells them that they have an Email that needs to be viewed. This notification can be S/MIME signed so that it does not get picked up as spam.

FTP_ITC.1

Trusted communication with webmail clients is established using TLS to safeguard confidentiality and integrity. This is done through HTTPS to establish web mail sessions.

Trusted communication with an external audit server is achieved with the TOE acting as a SSH client.

FIPS Compliance

The table below shows algorithm test certificate numbers provided under the Cryptographic Algorithm Validation Program.

Algorithm	OpenSSL	RSA BSAFE	libgcrypt
AES	2013	TBS	2106
TDES	1299	TBS	1341
DSA	639	TBS	656
RSA	1042	TBS	1080
SHA	1763	TBS	1829
RNG	1055	TBS	1081

HMAC	1218	TBS	1280

Table 18 – CAVP Algorithm Certificates

MEG has been submitted for FIPS 140-2 validation under the Cryptographic Module Validation program. A certificate number will be provided when available.

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.

SFR	SFR Name	Security Function
FAU_GEN.1	Audit data generation	Audit
FAU_GEN.2	User Identity association	Audit
FAU_STG_EXT.1	External audit trail storage	Audit
FAU_ARP.1 *	Security alarms	Audit, Anti-Virus & Anti-Spam
FAU_SAR.1 *	Audit review	Audit
FAU_SAR.2 *	Restricted audit review	Audit
FAU_SAR.3 *	Selectable audit review	Audit
FAU_SEL.1 *	Selective audit	Audit
FAU_STG.1*	Protected audit trail storage	Audit
FAU_STG.3 (1)*	Action in case of possible audit data loss	Audit
FAU_STG.3 (2)*	Action in case of possible audit data loss	Audit
FCS_CKM.1	Cryptographic key generation	Cryptographic operations
FCS_CKM_EXT.4	Cryptographic key zeroisation	Cryptographic operations
FCS_COP.1(1)	Cryptographic operation	Cryptographic operations
FCS_COP.1(2)	Cryptographic operation	Cryptographic operations, Secure Web Mail
FCS_COP.1(3)	Cryptographic operation	Cryptographic Operations
FCS_COP.1(4)	Cryptographic operation	Cryptographic Operations
FCS_COP.1(5)*	Cryptographic operation	Cryptographic Operations
FCS_RBG_EXT.1	Cryptographic operation	Cryptographic operations
FCS_SSH_EXT.1	SSH	Cryptographic operations, Security

SFR	SFR Name	Security Function
		Management
FCS_TLS_EXT.1	TLS	Cryptographic operations
FCS_HTTPS_EXT.1	HTTPS	Cryptographic operations
FDP_IFC.1*	Subset information flow control	Secure Web Mail
FDP_IFF.1*	Simple security attributes	Secure Web Mail
FDP_RIP.2	Full residual information protection	Security Management
FDP_UCT.1*	Basic data exchange confidentiality	Secure Web Mail
FDP_CMM_EXT.1(1)*	Scan operation	Anti-Virus & Anti-Spam
FDP_CMM_EXT.1(2)*	Scan operation	Anti-Virus & Anti-Spam
FDP_CMM_EXT.1(3) *	Scan operation	Compliance
FDP_CMM_EXT.1(4) *	Scan operation	Compliance
FDP_CMM_EXT.2(1) *	Scan actions	Anti-Virus & Anti-Spam, Quarantine Management, Action & Remediation
FDP_CMM_EXT.2(2) *	Scan actions	Anti-Virus & Anti-Spam, Quarantine Management, Action & Remediation
FDP_CMM_EXT.2(3) *	Scan actions	Compliance, Quarantine Management, Action & Remediation
FDP_CMM_EXT.2(4) *	Scan actions	Compliance, Quarantine Management, Action & Remediation
FIA_PMG_EXT.1	Password management	Identification & Authentication
FIA_UIA_EXT.1	User identification and authentication	Identification & Authentication
FIA_UAU_EXT.2	Password-based authentication mechanism	Identification & Authentication
FIA_UAU.7	Protected authentication feedback	Identification & Authentication
FMT_MTD.1	Management of TSF data	Security Management
FMT_MOF.1(1)	Management of security functions behaviour	Security Management
FMT_MOF.1(2)	Management of security functions behaviour	Security Management

SFR	SFR Name	Security Function
FMT_MOF.1(3)	Management of security functions behaviour	Security Management
FMT_SMF.1	Specification of management functions	Security Management
FMT_SMR.2	Restrictions on security roles	Security Management
FPT_ITT.1*	Basic internal TSF data transfer protection	Cryptographic Operations
FPT_APW_EXT.1	Protection of administrator passwords	Identification & Authentication
FPT_SKP_EXT.1	Protection of TSF data	Cryptographic Operations
FPT_STM.1	Reliable time stamps	Audit
FPT_TUD_EXT.1	Trusted update	Security Management
FPT_TST_EXT.1	TSF testing	Security Management
FTA_SSL_EXT.1	TSF-initiated session locking	Security Management
FTA_SSL.3	TSF-initiated termination	Security Management
FTA_SSL.4	User-initiated termination	Security Management
FTA_TAB.1	Default TOE access banners	Identification & Authentication
FTP_ITC.1	Inter-TSF trusted channel	Secure Web Mail
FTP_TRP.1	Trusted path	Security Management

Table 19 - SFR to Security Functions mapping