McAfee® Email Gateway Appliance Version 7.0.1 NDPP Compliance Security Target

Release Date:	8 August 2013
Version:	2.3 niap

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
2.1 niap	19 June 2013	Primasec	NIAP PP compliance adjustments
2.2 niap	18 July 2013	Primasec	NIAP PP compliance adjustments
2.3 niap	8 August 2013	Primasec	NIAP PP compliance adjustments

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 NDPP Compliance Security Target, Version 2.3 niap.

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.

The McAfee MEG provides the following functionality:

- Anti-Virus
- Anti-Spam
- Compliance
- Quarantine Management
- Secure Web Delivery - push/pull message delivery
- Action and Remediation
- Security Management
- Identification and Authentication
- Audit and Alerts
- Cryptographic Operations

The first six of these are described below. The remaining items address the [NDPP] functionality and are described in Section 1.8.

1.2.1 Anti-Virus

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.

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.

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.

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.

1.2.2 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. This makes use of streaming updates, rules and scores, and blacklists/whitelists.

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..

Global Threat Intelligence: Message Reputation - A further service is provided through use of McAfee Global Threat Intelligence (GTI) message reputation technology. This service is applied also for spam and phishing detection.

1.2.3 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 in the blocking of a message. Compliance techniques include dictionary checks, data loss prevention, and image, file and mail filtering.

1.2.4 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.

1.2.5 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

browser access to email traffic that policy has defined as sensitive: **Pull** – where MEG stores the emails in an encrypted form; and **Push** – where MEG sends the email to the recipient's mail server in an encrypted form.

1.2.6 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.

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

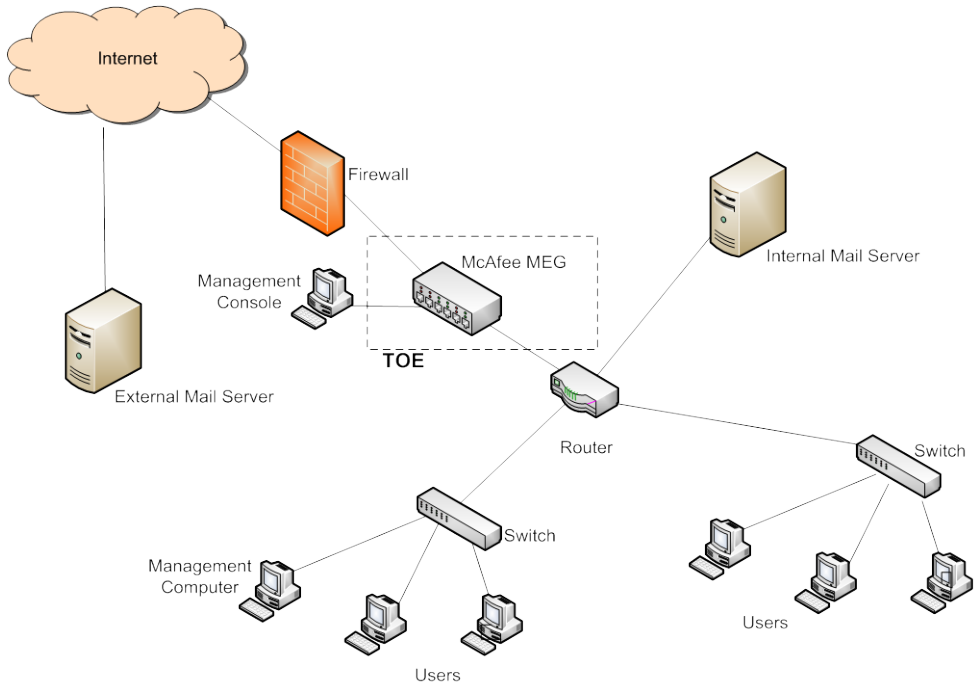


Figure 1: Architectural Diagram (placement in network)

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 SATA	2 x 300 GB SAS (hot swappable)	2 x 300 GB SAS (hot swappable)	6 x 300 GB 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	2 x 750W (hot swappable)

Hardware Platform	4000-B	4500-B	5000-B 5000-C 5000-C-2U	5500-B 5500-C
			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	MEG software package incl. O.S.

TOE or Environment	Component Name	Description of Component
	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)	
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 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:

- 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 TOE logical description is divided into the following sections:

- Security Management
- Identification and Authentication
- Audit and Alerts
- 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 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.

[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.

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 Transport Layer Security (TLS) v1 encryption, using AES with cryptographic key size of 128-bits. The SSLv2/v3 protocols are explicitly disabled. ActiveX is enabled.

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.

1.8.2 Identification 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.

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.

1.8.3 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.

1.8.4 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 with S/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.

This TOE is conformant to the Protection Profile for Network Devices, 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].

Short name	Assumption
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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

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 basic attack potential who possesses an average expertise, few resources, and low to moderate motivation.

The threats are taken from [NDPP].

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective

	security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
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.
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.
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.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

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.

TOE Security Objective Name	TOE Security Objective Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
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.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
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.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

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):

TOE Security Objective Name	TOE Security Objective Definition
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.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

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	T.ADMIN_ERROR	T.TSF_FAILURE	T.UNDETECTED_ACTIONS	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.USER_DATA_REUSE	P.ACCESS_BANNER
O.PROTECTED_COMMUNICATIONS							X		X	
O.VERIFIABLE_UPDATES								X		
O.SYSTEM_MONITORING						X				
O.DISPLAY_BANNER										X

	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	T.ADMIN_ERROR	T.TSF_FAILURE	T.UNDETECTED_ACTIONS	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.USER_DATA_REUSE	P.ACCESS_BANNER
O.TOE_ADMINISTRATION							X			
O.RESIDUAL_INFORMATION_CLEARING									X	
O.SESSION_LOCK							X			
O.TSF_SELF_TEST					X				X	
OE.NO_GENERAL_PURPOSE	X									
OE.PHYSICAL		X								
OE.TRUSTED_ADMIN			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 . The TOE will monitor and record selected events (O.SYSTEM_MONITORING).

T.UNAUTHORIZED_ACCESS is addressed by O.PROTECTED_COMMUNICATIONS, O.TOE_ADMINISTRATION and O.SESSION_LOCK. Communication channels are protected against interception (O. PROTECTED_COMMUNICATIONS). Login is controlled (O. TOE_ADMINISTRATION), and session locking is provided (O.SESSION_LOCK

T.UNAUTHORIZED_UPDATE is addressed by O.VERIFIABLE _UPDATES. The TOE will verify that updates are unaltered (O.VERIFIABLE _UPDATES)

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).

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 named 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
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_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
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_SMF.1	Specification of management functions
FMT_SMR.2	Restrictions on security roles
FPT_ITT.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

Functional Components	
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.

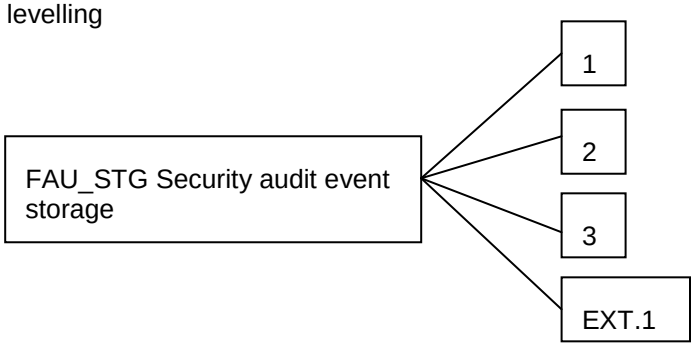
The extended components in this section are used in [NDPP]. The PP author has not provided definitions of these components, but it is considered appropriate to try to provide these definitions in this ST.

5.1.1 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

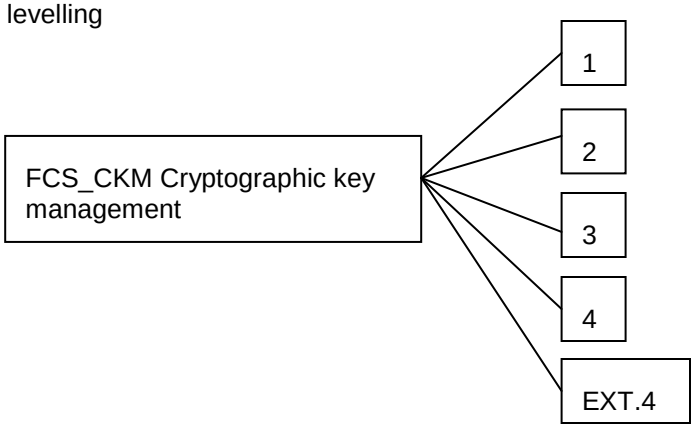
FAU_STG_EXT.1.1 The TSF shall be able to [selection: *transmit the generated audit data to an external IT entity, receive and store audit data from an external IT entity*] using a trusted channel implementing the [selection: *SSH, TLS, TLS/HTTPS*] protocol.

5.1.2 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]

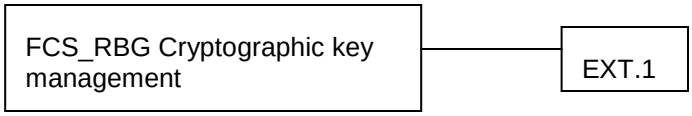
FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.1.3 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.

5.1.4 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.

5.1.5 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 protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: *number of bytes*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256 [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, *no other algorithms*].

FCS_SSH_EXT.1.5 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.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: *hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96*].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.1.6 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 2246), 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_256_CBC_SHA384].

5.1.7 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.

5.1.8 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*]].

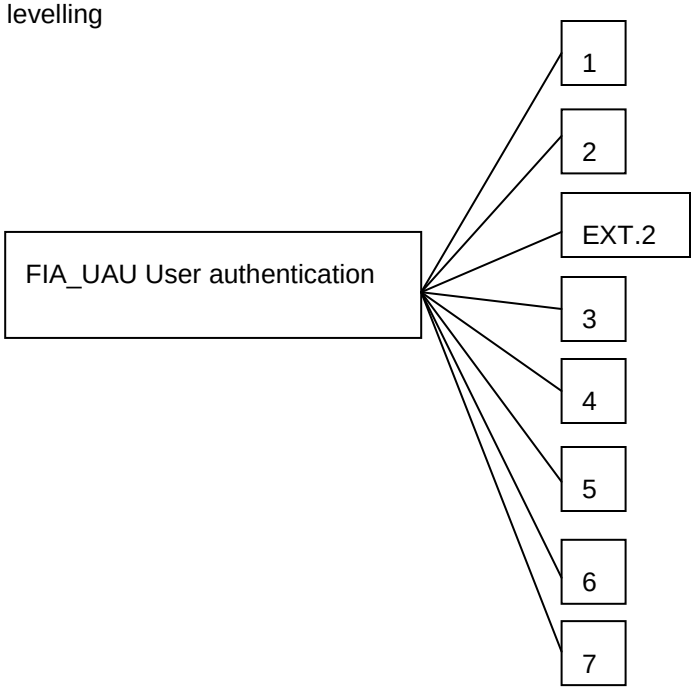
FIA_UIA_EXT.1.2 The TSF shall require each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.1.9 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

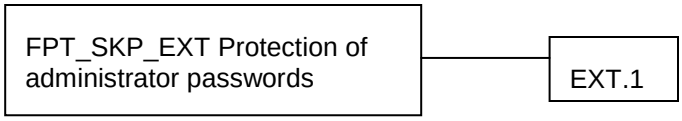
FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [selection: [assignment: *other authentication mechanism(s)*], *none*] to perform administrative user authentication.

5.1.10 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

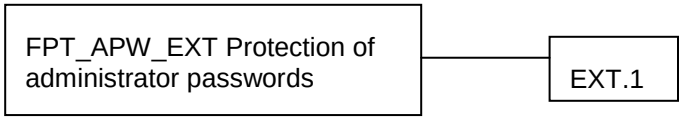
FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys and private keys.

5.1.11 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.

5.1.12 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.

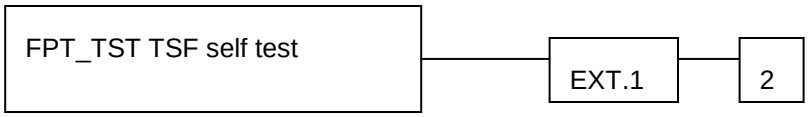
FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [selection: *digital signature mechanism, published hash*] prior to installing those updates.

5.1.13 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

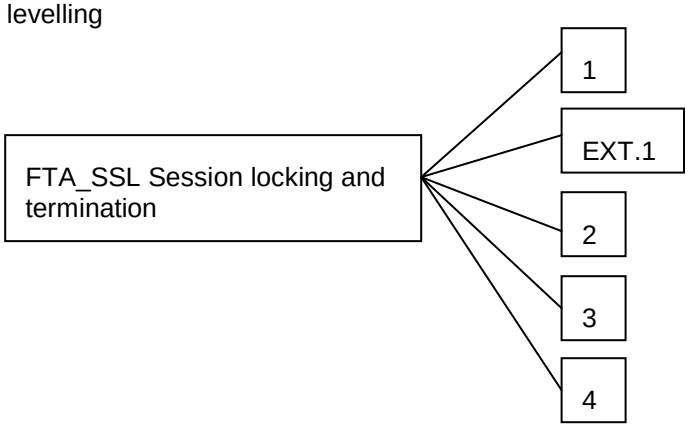
FPT_TST_EXT.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which a self test should occur]*] to demonstrate the correct operation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

5.1.14 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 4*, 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.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None
FAU_GEN.2	None.	None
FAU_STG_EXT.1	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_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
FDP_RIP.2	None.	None
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_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

Requirement	Auditable Events	Additional Audit Record Contents
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	None	None
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.

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 800-56B, "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.

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

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

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-2 or 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_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 [128 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

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 protocol implementation supports the following authentication methods as described in RFC 4252: public key based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253,packets greater than [*256k*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 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.1.5 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.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [hmac-sha1, hmac-sha1-96].

FCS_SSH_EXT.1.7 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 2246)] 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_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.

5.2.5 Identification and Authentication (FIA)

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 Security Administrator, and support passwords of 15 characters or greater.

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.

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] 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**.

5.2.6 Security Management (FMT)

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 Security Administrators*].

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*].

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- [Authorized *Administrator*].

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 detect its modification** when it is transmitted between separate parts of the TOE **through the use [TLS]**.

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 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 [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 Security 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 [Security 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 **Security 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] to** provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server(SSH), [no other capabilities]** 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 requirements listed below are those in [NDPP], providing compliance with the protection profile. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Assurance Class	Assurance Components	
ADV: Development	ADV_FSP.1	Basic functional specification
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
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_IND.1	Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1	Vulnerability survey

Table 14 - Assurance Requirements

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 by an administrator to check the validity of updates (FPT_TUD_EXT.1).
O.SYSTEM_MONITORING	The TOE generates audit records (FAU_GEN.1) that are attributable to users (FAU_GEN.2). 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

Security Objective	Mapping Rationale
	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).

Table 15 - Security objective mapping rationale

5.4.2 TOE Security Assurance Requirements

The TOE SARs are consistent with the threat environment, and are taken from [NDPP].

5.5 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.

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
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)

Functional Component	Dependency	Included/Rationale
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_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
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_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

Functional Component	Dependency	Included/Rationale
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 16 - SFR dependencies

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of 4 Security Functions:

- Security Management
- Identification and Authentication
- Audit
- Cryptographic Support

6.1.1 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); and the logging subsystem, which manages access to appliance audit logs and reports.

The browser-based user interface is implemented in javascript and HTML, and connections (HTTPS over TLS) are managed by Apache Web Server Software. 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 using a 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;
- 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 be updated with software hotfixes and patches. Prior to being applied, the integrity of hotfixes and patches is verified against the SHA-256 hashes provided on the McAfee website. For firmware updates (i.e. code embedded in the physical chips) such as the RAID controller, BIOS or network interface images, SHA-256 hashes are also provided.

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 ability to query, delete or modify the 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. In this default mode the Super Administrator is equivalent to the Security Administrator in [NDPP]. Using the scmadmin account, any number of other accounts can be created, including more Super Administrators or other less privileged roles. 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 types 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.

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

MEG self-tests are run during startup to ensure that the TOE is functioning properly to demonstrate correct operation of the TSF. 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 uses an Error Detection Code (EDC) for integrity over the firmware.
MEG performs a crypto module integrity check using HMAC-SHA-256, and it runs all approved algorithm cryptographic self-tests.
The BIOS performs power on self tests applicable to the hardware. The BIOS then boots the appliance OS, and verifies all of the files that form the software (using SHA-256). It verifies that the cryptographic engines used can function in FIPS mode, that the appliance configuration is compatible with FIPS mode, and that the configuration originated from a FIPS mode device.

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.

6.1.2 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 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 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, are obfuscated, and 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 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.

6.1.3 Audit

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 6.1.2.

FAU_GEN.1, FAU_GEN.2 – 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;
- Network level communication events;
- Protocol processing events;
- 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.

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_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.

6.1.4 Cryptographic Support

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 rDSA) so that it does not get picked up as spam.

FCS_COP.1(4) Keyed Hash

A keyed hash (HMAC-SHA-1, HMAC-SHA-256) is used for integrity protection as part of the TLS, SSH and HTTPS protocols.

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

The TOE provides a verification process for downloaded .dat threat signature and engine files. The threat signature files (.dat files) and engine 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_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. These private keys cannot be output on physical ports.

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 (rDSA keys). 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).

All cryptographic libraries include mechanisms 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 multiple 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 have at some point been written out is no

longer available. FIPS mode is disabled by reinstalling the appliance, which removes all Key Security Parameters.

The TOE has two methods for zeroizing keys and CSPs: a complete uninstall and reinstallation of the TOE and a zeroization function. The zeroization function uses a cleanup routine to remove keys and /or CSPs stored in RAM. The cleanup routine overwrites the RAM multiple times. This function is also called prior to uninstalling the MEG.

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.

The entropy bits are placed into a pool with a maximum size of 4000 bits. If there are insufficient bits in the pool the call from the RNG is halted until there are a sufficient number of bits for use. This ensures that there is sufficient entropy for any call made by the RNG to the pool. In addition, the entropy source has been tested to SP 800-90B tests and was found to be adequate.

When keys are being generated the RNG may be called repeatedly to ensure sufficient random bits are available, with no loss of entropy (e.g. in the case of AES-256 keys).

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: AES-CBC-128 and AES-CBC-256.

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 (in excess of 256k), 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-sha1-96.

FCS_TLS_EXT.1

The TOE implements TLS 1.0 (RFC 2246)] 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.

FCS_HTTPS_EXT.1

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

Client-Authentication uses form based authentication over HTTPS.

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 cannot be output on physical ports.

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	2281	2106
TDES	1299	1429	1341
RSA	1042	1172	1080
SHA	1763	1963	1829
RNG	1055	1134	1081
HMAC	1218	-	1280

Table 17 – 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
FCS_CKM.1	Cryptographic key generation	Cryptographic Support
FCS_CKM_EXT.4	Cryptographic key zeroisation	Cryptographic Support
FCS_COP.1(1)	Cryptographic operation	Cryptographic Support
FCS_COP.1(2)	Cryptographic operation	Cryptographic Support
FCS_COP.1(3)	Cryptographic operation	Cryptographic Support
FCS_COP.1(4)	Cryptographic operation	Cryptographic Support
FCS_RBG_EXT.1	Cryptographic operation	Cryptographic Support
FCS_SSH_EXT.1	SSH	Cryptographic Support, Security Management
FCS_TLS_EXT.1	TLS	Cryptographic Support
FCS_HTTPS_EXT.1	HTTPS	Cryptographic Support
FDP_RIP.2	Full residual information protection	Security Management
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_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	Cryptographic Support

SFR	SFR Name	Security Function
	protection	
FPT_APW_EXT.1	Protection of administrator passwords	Identification & Authentication
FPT_SKP_EXT.1	Protection of TSF data	Cryptographic Support
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	Audit
FTP_TRP.1	Trusted path	Security Management

Table 18 - SFR to Security Functions mapping