McAfee® Web Gateway
Version 7.2.0.1
EAL 2 + ALC_FLR.2
Security Target

Release Date:	5 October 2012
Version:	1.0
Prepared By:	Primasec Ltd.
Prepared For:	McAfee Inc. 3965 Freedom Circle Santa Clara, CA 95054

Document Introduction

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the McAfee Web Gateway Version 7.2.0.1. This Security Target (ST) defines a set of assumptions about the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which satisfy the set of requirements.

Revision History		
Revision	**Remarks**	**Date**
1.0	Issue for certification	5 October 2012

Table of Contents

1 SECURITY TARGET INTRODUCTION 6

1.1 PURPOSE 6
1.2 ST AND TOE IDENTIFICATION 6
1.3 CONVENTIONS, TERMINOLOGY, AND ACRONYMS 7
1.3.1 Conventions 7
1.3.2 Terminology 8
1.3.3 Acronyms 9
1.4 REFERENCES 9
1.5 COMMON CRITERIA CONFORMANCE CLAIMS 10

2 TOE DESCRIPTION 11

2.1 PRODUCT TYPE 11
2.2 PRODUCT DESCRIPTION 11
2.3 PRODUCT FEATURES 11
2.4 APPLICATION CONTEXT 12
2.5 SECURITY ENVIRONMENT TOE BOUNDARY 12
2.5.1 Security Features to be Evaluated 12
2.5.2 Features not to be Evaluated 12
2.5.3 Physical Scope and Boundary 14
2.5.4 Evaluated TOE Configuration 14

3 SECURITY PROBLEM DEFINITION 17

3.1 ASSUMPTIONS 17
3.2 THREATS 18
3.3 ORGANISATIONAL SECURITY POLICIES 19

4 SECURITY OBJECTIVES 20

4.1 SECURITY OBJECTIVES FOR THE TOE 20
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 21

5 TOE IT SECURITY REQUIREMENTS 23

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 23
5.2 TOE SECURITY ASSURANCE REQUIREMENTS 33

6 TOE SUMMARY SPECIFICATION 34

6.1 SECURITY MANAGEMENT [FMT] 34
6.1.1 Using Admin GUI [FMT_1] 34
6.1.2 MWG Administration [FMT_2] 35
6.1.3 URL/Application Filter Policy Configuration [FMT_3] 35
6.1.4 Anti-Malware Configuration [FMT_4] 35
6.1.5 Certificate Checking Configuration [FMT_5] 35
6.1.6 HTTPS Scanner Configuration [FMT_6] 36
6.1.7 Initial Configuration [FMT_7] 36
6.2 IDENTIFICATION AND AUTHENTICATION [FIA] 36
6.2.1 User Identification [FIA_1] 36
6.2.2 Authentication [FIA_2] 37
6.3 USER DATA PROTECTION [FDP] 37

6.3.1 URL Filter [FDP_1] *37*
6.3.2 Anti-Malware Filter [FDP_2] *38*
6.3.3 Certificate Checker [FDP_3] *38*
6.3.4 HTTPS Scanner [FDP_4] *38*
6.4 PROTECTION OF SECURITY FUNCTIONS [FPT] 38
6.4.1 Time Stamps [FPT_1] *38*
6.4.2 Trusted path [FPT_2] *39*
6.5 AUDIT [FAU] 39
6.5.1 Logging [FAU_1] *39*
6.5.2 Audit Reporting [FAU_2] *40*
6.5.3 Audit Data Protection [FAU_3] *40*

7 RATIONALE 41

7.1 RATIONALE FOR TOE SECURITY OBJECTIVES 41
7.2 RATIONALE FOR THE TOE OPERATING ENVIRONMENT SECURITY OBJECTIVES 42
7.3 RATIONALE FOR TOE SECURITY REQUIREMENTS 43
7.4 RATIONALE FOR ASSURANCE REQUIREMENTS 48
7.5 DEPENDENCY RATIONALE 48
7.6 RATIONALE FOR TOE SUMMARY SPECIFICATION 50

List of Tables

TABLE 1. ASSUMPTIONS FOR TOE OPERATIONAL ENVIRONMENT 17
TABLE 2. THREATS 18
TABLE 3. SECURITY OBJECTIVES FOR THE TOE 20
TABLE 4. SECURITY OBJECTIVES FOR THE TOE OPERATING ENVIRONMENT 21
TABLE 5. TOE SECURITY FUNCTIONAL REQUIREMENTS 23
TABLE 6. AUDITABLE EVENTS 31
TABLE 7. EAL2 PLUS ALC_FLR.2 ASSURANCE COMPONENTS 33
TABLE 8. MAPPING THREATS TO TOE SECURITY OBJECTIVES 42
TABLE 9. MAPPING THREATS TO TOE OPERATING ENVIRONMENT SECURITY OBJECTIVES 43
TABLE 10. MAPPING SFRS TO TOE SECURITY OBJECTIVES 47
TABLE 12. SFR/SAR DEPENDENCY EVIDENCE 49
TABLE 12. MAPPING OF SFRS TO SECURITY FUNCTIONS 50
TABLE 13. SUITABILITY OF SECURITY FUNCTIONS 52

List of Figures

FIGURE 1 MCAFEE WEB GATEWAY TOE SECURITY ENVIRONMENT 13

1 Security Target Introduction

1.1 Purpose

1 This security target has been written to support the evaluation of McAfee Web Gateway (MWG) software version 7.2.0.1. The primary purpose of MWG is to serve as a web gateway, mediating traffic between an enterprise and the internet.

2 This introductory section presents security target identification information and an overview of the security target structure. A brief discussion of the security target development methodology is also provided.

3 A security target provides the basis for the evaluation of a target of evaluation (TOE). A security target principally defines:

a) A set of assumptions about the security aspects of the environment, a list of threats which the product is intended to counter, and any known rules with which the product must comply (in Section 3, Security Problem Definition).

b) A set of security objectives and a set of security requirements to address that problem (in Sections 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet that set of requirements (in Section 6, TOE Summary Specification).

d) The security target rationale (Sections 7).

4 The structure and contents of this security target comply with the requirements specified in the CC, Part 1, Annex A, and Part 3, Chapter 11.

1.2 ST and TOE Identification

5 This section provides security target and TOE identification information.

ST Title:	McAfee Web Gateway Version 7.2.0.1 EAL2 +ALC_FLR.2 Security Target
ST Author:	Primasec Ltd.
ST Revision Number:	1.0

ST Date:	5 October 2012
TOE Identification:	Software: McAfee Web Gateway Software Version 7.2.0.1 Administrative Guidance for receiving, installing and managing the TOE Product Guide McAfee Web Gateway version 7.2 Quick Start Guide McAfee Web Gateway
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1r4, September 2012 (also known as ISO 15048)
Assurance Level:	EAL2, augmented with ALC_FLR.2
TOE Type:	Web Gateway

1.3 Conventions, Terminology, and Acronyms

6 This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.3.1 Conventions

7 This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this security target are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the security target reader.

8 The CC identifies four operations to be performed on functional requirements; *assignment*, *iteration*, *refinement*, and *selection* are defined by Part 2 of the CC.

a) The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security

requirements is denoted by **bold text** for additions and strike-through to indicate deletions.

b) The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.

c) The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].

d) The **iteration** operation is used when a component is repeated with varying operations. Showing the iteration number in parenthesis following the component identifier and element identifier (iteration_number) denotes iteration.

1.3.2 Terminology

9 In the Common Criteria, many terms are defined in Section 4.1 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the reader of the Security Target.

User/external entity	Any human or IT entity possibly interacting with the TOE from outside the TOE boundary. [N.B. in the context of this TOE a user may be an administrator with access to the TOE, or a network proxy user.]
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Identity	A representation (e.g. a string) uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE.
Authentication data	Information used to verify the claimed identity of a user.

10 In addition to the above general definitions, this Security Target provides the following specialized definition:

Authorized Administrator – A human user associated with a defined role that allows them to administer specified security parameters of the TOE. Such users are not subject to any additional access control requirements once authenticated to the TOE, and are therefore trusted to not compromise the security policy enforced by the TOE within their defined role.

1.3.3 Acronyms

11 The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
MLOS	McAfee Linux Operating System
MWG	McAfee Web Gateway
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions

1.4 References

12 The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1r4, CCMB-2012-09-001.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated September 2012, version 3.1r4, CCMB-2012-09-002.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated September 2012, version 3.1r4, CCMB-2012-09-003.
[CEM]	Common Methodology for Information

Technology Security Evaluation, dated September 2012, version 3.1r4, CCMB-2012-09-004.

1.5 Common Criteria Conformance Claims

13 The TOE does not claim conformance to any Protection Profile.

14 The TOE conforms to [CC_PART2] and [CC_PART3] conformant with the assurance level of EAL2, augmented with ALC_FLR.2.

2 TOE Description

15 McAfee Web Gateway (MWG) software is typically deployed as a web gateway between the internet and the enterprise. MWG provides filters which adapt traffic for various internet protocols including HTTP, HTTPS, and FTP. When it is installed in a system, every transaction is piped through it for filtering and malware scanning on the content.

2.1 Product Type

16 MWG functions as a web gateway to examine and adapt network traffic through a variety of filters to meet the needs of an enterprise. MWG protects against inbound threats such as malware hidden in blended content, and it protects organizations from outbound threats such as the potential loss of confidential information that can leak out on web protocols.

2.2 Product Description

17 The MWG product is available as a turn-key network appliance. The hardware platforms for the family of MWG appliance models are scaled to provide a range of performance capability to match the needs of the enterprise. The MWG appliances come completely preinstalled with software and a proven default configuration for rapid deployment. The software is self-contained and includes hardened OS features taken from McAfee Linux Operating System (MLOS) 1.0.

2.3 Product Features

18 MWG implements the following User Data Protection features:

- URL Filtering to control access to Web content
- Anti-Malware filtering for threats transported in Web and FTP traffic
- HTTPS scanning for malicious content hidden in encrypted internet protocol traffic
- Certificate Verification to control access to HTTPS content

19 The management features provided by MWG include the following:

- Granular Security Policy Management: A graphical user interface provides flexible and custom policy management.
- Audit Review: the graphical user interface provides authorized administrators with convenient access to audit information.

- Forensic Analysis: Report generation tools can be used to ascertain information about historical and current attacks.

2.4 Application Context

20 MWG operates in a network environment with web-based traffic. It provides gateway protection between at least two networks. Typically, one network is viewed as the inside of an organization, where there is some assumption of control over access to the computing network. The other network is typically viewed as an external network, such as the Internet, where there is no practical control over the actions of its processing entities. MWG's role is to examine and adapt traffic flowing between the two networks.

2.5 Security Environment TOE Boundary

2.5.1 Security Features to be Evaluated

21 The MWG scope of evaluation includes URL filtering, Anti-Malware, HTTPS scanning and Certificate verification. Other traffic filtering services provided by MWG are excluded from the scope of the evaluation.

2.5.2 Features not to be Evaluated

22 MWG provides the following functionality that is specifically excluded from the scope of this evaluation:

a) Instant Message Protocol

b) Cluster Management

c) High availability

d) ICAP

e) Transparent router and transparent bridge modes

f) Kerberos administration

g) Proxy auto-configuration

h) Authentication using cookies

i) Hybrid Policy Synchronisation

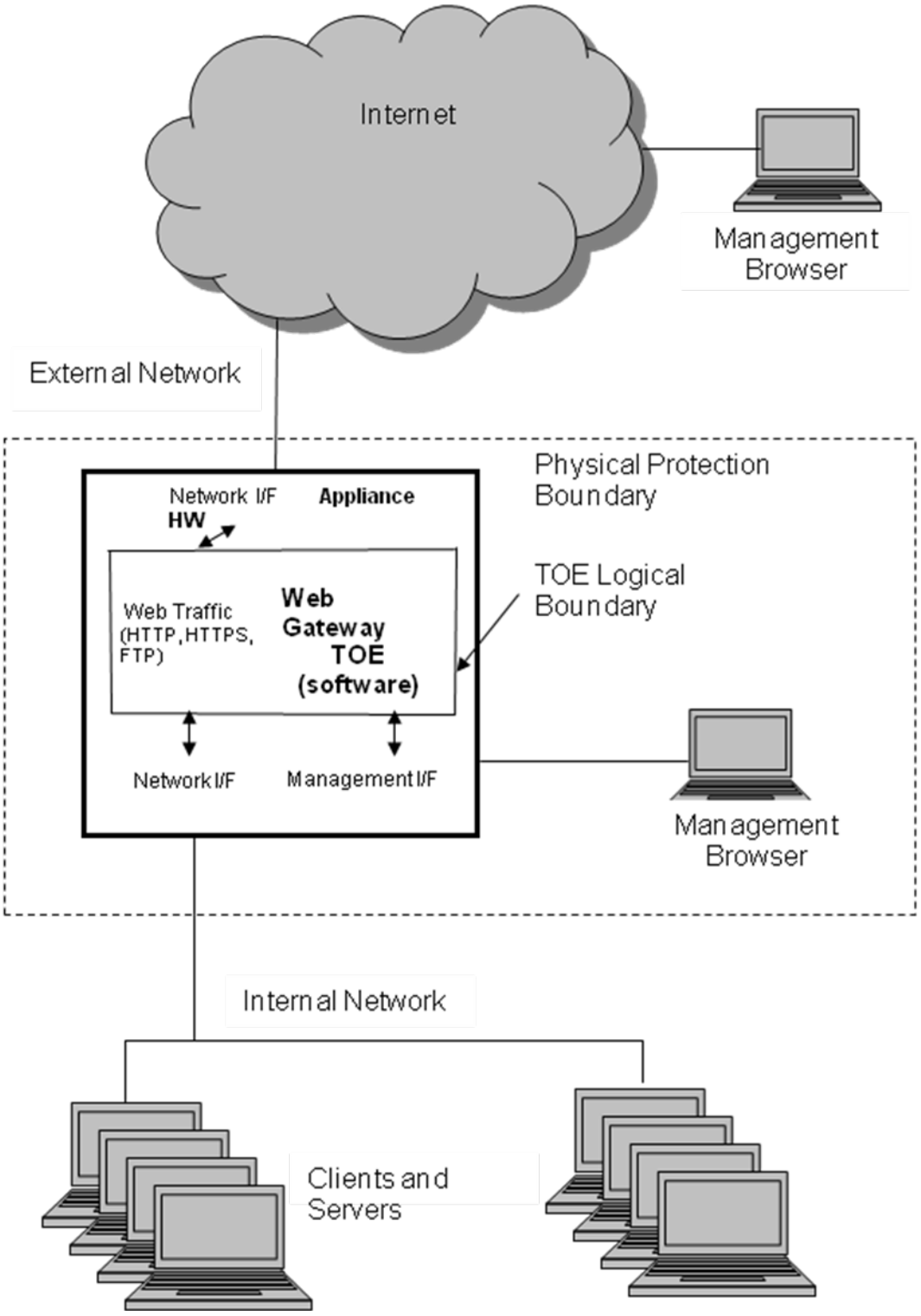

Figure 1 McAfee Web Gateway TOE Security Environment

2.5.3 Physical Scope and Boundary

23 The TOE consists of MWG Software Version 7.2.0.1. This software is fully integrated; it includes OS features that were built from MLOS, a Tomcat application server, and OpenSSL cryptographic capability. This software is obtained by purchasing a MWG appliance, or licence to download, from McAfee Corporation. The hardware appliance platform is not part of the TOE; it is part of the IT environment. The TOE includes a management GUI that can be accessed from a variety of commercially available Web browsers that can run HTTPS. The management browser software runs on a generic computing platform; however, the hardware platform, the browser, and the OS are not part of the TOE.

24 No extraordinary security demands are placed upon the hardware platforms and peripheral equipment used by the MWG software. This equipment or virtual environment is expected to meet the customary demands for reliable operation of typical Unix or Microsoft Servers as provided by standard Intel PC computing platforms. If any of the network interface cards support features such as wake-on LAN, special external command features, or special protocol processing, the hardware connections to support those features should not be connected. In the evaluated configuration, MWG will not enable any such special features.

2.5.4 Evaluated TOE Configuration

25 The MWG software is installed on a MWG appliance computing platform with at least three network interfaces. Two network communication interfaces are provided (generally to separate internal and external networks) and a third is typically used for communication with the management browser. MWG can communicate with a management browser on any connected network.

26 The TOE software version is available and executes properly across:

a) the entire family of MWG appliance models: WW500, WW1100, WW1900, WW2900, WG5000, WG5500, WG4000B, WG4500B, WG5000B, WG5500B;

b) a HP Proliant G6 Blade Server;

c) a virtual environment under VMware vSphere 4.1 or later.

27 The evaluated configuration is comprised of:

a) TOE software running on a MWG appliance, blade or virtual platform;

b) a generic computing platform with a vendor supported Windows or Linux operating system, running Java Runtime Environment (1.6 or later), and a browser (Microsoft Internet Explorer 7.0 or later, or Mozilla Firefox 2.0 or later); and

c) the associated network interconnections.

These components are maintained in a physically protected IT environment that prohibits unauthorized access.

2.5.4.1 Logical Scope and Boundary

28 The TOE with support from the IT environment provides the following security features:

a) Security Management [FMT]

b) Identification and Authentication [FIA]

c) User Data Protection [FDP]

d) Protection of Security Functions [FPT]

e) Audit [FAU]

2.5.4.2 Security Management [FMT]

29 An administrator uses a browser on a generic computing platform (part of the IT environment) to perform management functions on MWG. This administrative platform may be local or remote. New administrator roles can be created, each with a different set of access rights.

2.5.4.3 Identification and Authentication [FIA]

30 The MWG TOE, along with support from the IT environment, supports password authentication for administrative users. MWG consults its stored user information, determines the password's validity, and enforces the result of the validity check. MWG can also be configured to require client certificates for remote management sessions.

2.5.4.4 User Data Protection [FDP]

31 For the MWG TOE, user data refers only to internet protocol traffic passed through MWG. MWG rules implement a site's security policy and, ultimately, determine what filters will be applied to the IP traffic before it is allowed to flow to another network.

2.5.4.5 Protection of Security Functions [FPT]

32 The MWG TOE provides a reliable time mechanism which is of particular importance for audit and for the sequencing of security related activity.

2.5.4.6 Audit [FAU]

33 MWG provides an audit log to which key security processes may write audit data. MWG adds security relevant information, such as the time and the identity of the generating process, when logging audit data.

34 MWG audit includes administration activity as well as communication activity with results (traffic passes or not).

35 Only authorized administrators are allowed to read the audit data stream. MWG provides facilities to generate a few standard reports as well as a means to produce custom reports, or to view selected audit events. MWG also includes facilities to monitor and free up audit space at appropriate times.

3 Security Problem Definition

36 This section describes the security problem that the TOE is intended to solve. This includes information about the security aspects of the physical environment, personnel access, and network connectivity of the TOE.

37 Assumptions about the security aspects of the environment and manner of use are identified.

38 Known or assumed threats to the assets protected by the TOE or the TOE environment are described.

39 Organisational security policy (OSP) statements or rules to which the TOE must comply or implement are identified.

40 The TOE is intended to be used in environments in which sensitive information is processed, or where the sensitivity level of information in both the internal and external networks is different.

3.1 Assumptions

41 The TOE is assured to provide effective security measures when installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user/administrative guidance. Only authorized administrators are allowed physical access to the TOE and its management browser. The TOE, the management computing platform, and the administrative communication path are all managed in a physically secure environment.

42 The assumptions for the TOE are given in the table below:

Table 1. Assumptions for TOE Operational Environment

Assumption Identifier	Assumption Description
A.PHYSEC	The TOE and administration platform are physically secure.
A.PUBLIC	The TOE and administration platform do not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information cannot flow between the internal and external networks unless it passes through the TOE.

Assumption Identifier	Assumption Description
A.PROLIN	The communication path between the TOE and the management browser is physically or cryptographically protected.
A.NOREMO	Human users who are not authorized administrators cannot directly or remotely access the management platform.
A.BENIGN	The operating system running on the management platform will provide necessary computing services, but will not tamper with browser communications with the TOE.

3.2 Threats

43 This section helps define the nature and scope of the security problem by identifying assets that require protection, as well as threats to those assets.

44 The TOE addresses all threats listed in the following table. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

Table 2. Threats

Threat Identifier	Threat Description.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being

Threat Identifier	Threat Description.
	recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

3.3 Organisational Security Policies

45 This ST does not identify any OSPs.

4 Security Objectives

46 The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both. The CC identifies two categories of security objectives:

a) Security objectives for the TOE, and

b) Security objectives for the Operating Environment

4.1 Security Objectives for the TOE

47 The TOE accomplishes the following security objectives:

Table 3. Security Objectives for the TOE

Objective Identifier	Objective Description
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting them access to TOE functions.
O.MEDIAT	The TOE must mediate the flow of all information between IT devices located on internal and external networks governed by the TOE, disallowing passage of data identified as inappropriate.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

Objective Identifier	Objective Description
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

4.2 Security Objectives for the Environment

48 All the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE software. They will be satisfied largely through application of procedural or administrative measures.

Table 4. Security Objectives for the TOE Operating Environment

Objective Identifier	Objective Description
OE.PHYSEC	The TOE is physically secure.
OE.PUBLIC	The TOE does not host public data.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
OE.PROLIN	The communication path between the TOE and the management browser is physically or cryptographically protected.
OE.NOREMO	Human users who are not authorized administrators must not directly or remotely access the management platform.

Objective Identifier	Objective Description
OE.BENIGN	The OS running on the management platform must provide necessary computing services, but must not tamper with browser communications with the TOE.

5 TOE IT Security Requirements

49 This section provides functional and assurance requirements that must be satisfied by a security target-compliant TOE.

5.1 TOE Security Functional Requirements

50 The security functional requirements for this Security Target consist of the following components from Part 2 of the CC, summarized in Table 5. TOE Security Functional Requirements. The SFRs are provided in their entirety in the subsequent paragraphs.

Table 5. TOE Security Functional Requirements

Functional Components	
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FDP_IFC.1 (1)	Subset information flow control (1)
FDP_IFC.1 (2)	Subset information flow control (2)
FDP_IFC.1 (3)	Subset information flow control (3)
FDP_IFC.1 (4)	Subset information flow control (4)
FDP_IFF.1 (1)	Simple security attributes (1)
FDP_IFF.1 (2)	Simple security attributes (2)
FDP_IFF.1 (3)	Simple security attributes (3)
FDP_IFF.1 (4)	Simple security attributes (4)
FCS_COP.1 (1)	Cryptographic operation (1)
FCS_COP.1 (2)	Cryptographic operation (2)
FCS_CKM.1 (1)	Cryptographic key generation (1)
FCS_CKM.1 (2)	Cryptographic key generation (2)
FCS_CKM.4	Cryptographic key destruction
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization

Functional Components	
FMT_MTD.1 (1)	Management of TSF data (1)
FMT_MTD.1 (2)	Management of TSF data (2)
FMT_MTD.1 (3)	Management of TSF data (3)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FPT_STM.1	Reliable time stamps
FTP_TRP.1	Trusted path

Application note: The SFRs related to identification and authentication apply to administrative users attempting direct access to the TOE functions. They also apply to network proxy users in cases where the TOE has been configured to require authentication before allowing access *through* the TOE.

FIA_ATD.1 User attribute definition

51 FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;

b) association of a human user with the authorized administrator role;

c) and password].

FIA_UID.2 User identification before any action

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

FIA_UAU.2 User authentication before any action

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

FIA_UAU.5 Multiple authentication mechanisms

54 FIA_UAU.5.1 – The TSF shall provide [password, client certificate] to support user authentication.

55 FIA_UAU.5.2 – The TSF shall authenticate any user's claimed identity according to the [rule: authentication shall be by the method configured by an authorized administrator].

56 Requirements Overview: This Security Target consists of multiple information flow control Security Function Policies (SFPs). The CC allows multiple policies to exist, each having a unique name. This is accomplished by iterating FDP_IFC.1 for each of the four named information flow control policies.

57 The first policy is called the URL SFP. The subjects under control of this policy are external IT entities on an internal or external network sending HTTP traffic that is passed through the TOE prior to being forwarded to other external IT entities. This traffic may be filtered based upon the designated URLs.

58 The second policy is called the MALWARE SFP. The subjects under control of this policy are external IT entities sending IP traffic content that is passed through the TOE prior to being forwarded to other IT entities. This content may be filtered for malware.

59 The third policy is called the CERTIFICATE SFP. The subjects under control of this policy are external IT entities sending IP traffic content that is passed through the TOE prior to being forwarded to other IT entities. This content may be filtered for certificate characteristics.

60 The fourth policy is called the HTTPS SFP. The subjects under control of this policy are external IT entities on an internal or external network sending HTTPS traffic that is passed through the TOE prior to being forwarded to other external IT entities. This traffic may be decrypted for processing by the other SFPs, prior to being re-encrypted and forwarded.

61 The information flowing between subjects in these policies is traffic with attributes, defined in FDP_IFF.1.1. The rules that define each information flow-control SFP are found in FDP_IFF.1.2. Component FDP_IFF.1 is iterated to correspond to each of the iterations of FDP_IFC.1.

FDP_IFC.1 Subset information flow control (1)

62 FDP_IFC.1.1(1) - The TSF shall enforce the [URL SFP] on:

a) [subjects: external IT entities that send and receive information that is passed through the TOE to one another;

b) information: web traffic passed through the TOE; and

c) operation: pass information].

FDP_IFC.1 Subset information flow control (2)

63 FDP_IFC.1.1(2) - The TSF shall enforce the [MALWARE SFP] on:

a) [subjects: external IT entities that send and receive IP traffic content that is passed through the TOE to one another;

b) information: web traffic content passed through the TOE; and

c) operation: pass information].

FDP_IFC.1 Subset information flow control (3)

64 FDP_IFC.1.1(3) - The TSF shall enforce the [CERTIFICATE SFP] on:

a) [subjects: external IT entities that send and receive IP traffic content that is passed through the TOE to one another;

b) information: HTTP traffic content passed through the TOE; and

c) operation: pass information].

FDP_IFC.1 Subset information flow control (4)

65 FDP_IFC.1.1(4) - The TSF shall enforce the [HTTPS SFP] on:

a) [subjects: external IT entities that send and receive HTTPS traffic that is passed through the TOE to one another;

b) information: HTTPS traffic passed through the TOE; and

c) operation: decrypt information for filtering by other SFPs].

FDP_IFF.1 Simple security attributes (1)

66 FDP_IFF.1.1(1) - The TSF shall enforce the [URL SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- Presumed address;

b) information security attributes:

- presumed address of source subject;
- application;
- URL requested in HTTP message; and
- Category of the requested URL].

67 FDP_IFF.1.2(1) - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

68 [all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from combinations of the values of the information flow security attributes, created by the authorized administrator].

69 FDP_IFF.1.3(3) - The TSF shall enforce the [none].

70 FDP_IFF.1.4(4) - The TSF shall explicitly authorize an information flow based on the following rules: [none].

71 FDP_IFF.1.5(5) - The TSF shall explicitly deny an information flow based on the following rules: [none].

FDP_IFF.1 Simple security attributes (2)

72 FDP_IFF.1.1(2) - The TSF shall enforce the [MALWARE SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- none;

b) information security attributes:

- Traffic content].

73 FDP_IFF.1.2(2) - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

74 [traffic content does not violate any Anti-Malware searches that have been activated by the authorized administrator].

75 FDP_IFF.1.3(2) - The TSF shall enforce the [none].

76 FDP_IFF.1.4(2) - The TSF shall explicitly authorize an information flow based on the following rules: [none].

77 FDP_IFF.1.5(2) - The TSF shall explicitly deny an information flow based on the following rules: [none].

FDP_IFF.1 Simple security attributes (3)

78 FDP_IFF.1.1(3) - The TSF shall enforce the [CERTIFICATE SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- none;

b) information security attributes:

- Certificate Characteristics (validity, lifetime, name, chain)].

79 FDP_IFF.1.2(3) - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

80 [certificate characteristics satisfies the rules established by the authorized administrator].

81 FDP_IFF.1.3(3) - The TSF shall enforce the [none].

82 FDP_IFF.1.4(3) - The TSF shall explicitly authorize an information flow based on the following rules: [none].

83 FDP_IFF.1.5(3) - The TSF shall explicitly deny an information flow based on the following rules: [none].

FDP_IFF.1 Simple security attributes (4)

84 FDP_IFF.1.1(4) - The TSF shall enforce the [HTTPS SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- none;

b) information security attributes:

- Traffic content].

85 FDP_IFF.1.2(4) - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

86 [the authorized administrator has activated HTTPS termination and the decrypted message satisfies all other security policies that have been specified by the authorized administrator].

87 FDP_IFF.1.3(4) - The TSF shall enforce the [none].

88 FDP_IFF.1.4(4) - The TSF shall explicitly authorize an information flow based on the following rules: [none].

89 FDP_IFF.1.5(4) - The TSF shall explicitly deny an information flow based on the following rules: [none].

90 Application Note: MWG uses OpenSSL FIPS Object Module Version 1.1.2 for https encryption and decryption. MWG virual and appliance cryptographic modules are undergoing FIPS 140 validation, and reports are awaiting review by CMVP (Block 2).

FCS_COP.1 Cryptographic operation (1)

91 FCS_COP.1.1(1) – The TSF shall perform [symmetric encryption and decryption] in accordance with a specified cryptographic algorithm [3DES or AES] and cryptographic key sizes [168 bits 3DES or up to 256 bits AES] that meet the following: [NIST Special Publication 800-67 (3DES) or FIPS 197 (AES)].

FCS_COP.1 Cryptographic operation (2)

92 FCS_COP.1.1(2) – The TSF shall perform [asymmetric encryption and decryption] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [up to 2048 bits] that meet the following: [PKCS#1 v2.1].

FCS_CKM.1 Cryptographic key generation (1)

93 FCS_CKM.1.1(1) – The TSF shall generate **symmetric** cryptographic keys in accordance with a specified key generation algorithm [FIPS Approved random number generator] and specified cryptographic key sizes [168 bits 3DES or up to 256 bits AES] that meet the following: [ANSI X9.31].

FCS_CKM.1 Cryptographic key generation (2)

94 FCS_CKM.1.1(2) – The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified key generation algorithm [FIPS Approved random number generator] and specified cryptographic key sizes [up to 2048 bits] that meet the following: [ANSI X9.62].

FCS_CKM.4 Cryptographic key destruction

95 FCS_CKM.4.1– The TSF shall destroy cryptographic keys in accordance with a specified key destruction method [overwriting] that meets the following: [FIPS 140-2].

FMT_MOF.1 Management of security functions behaviour

96 FMT_MOF.1.1 - The TSF shall restrict the ability to *enable***,** *disable* the functions:

a) [start-up and shut-down of the TOE; and

b) Backup of audit trail data] to [an authorized administrator].

FMT_MSA.1 Management of security attributes

97 FMT_MSA.1.1 - The TSF shall enforce the [URL SFP, MALWARE SFP, CERTIFICATE SFP, and HTTPS SFP] to restrict the ability to [delete and create] the security attributes [information flow rules described in FDP_IFF.1(1-4)] to [the authorized administrator].

FMT_MSA.3 Static attribute initialization

98 FMT_MSA.3.1 - The TSF shall enforce the [URL SFP, MALWARE SFP, CERTIFICATE SFP, and HTTPS SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

99 FMT_MSA.3.2 - The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

100 Application Note: Following TOE installation, the default configuration is to restrict traffic using URL filtering and malware filtering.

FMT_MTD.1 Management of TSF data (1)

101 FMT_MTD.1.1(1) - The TSF shall restrict the ability to *query, modify, delete,* [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

FMT_MTD.1 Management of TSF data (2)

102 FMT_MTD.1.1(2) - The TSF shall restrict the ability to *modify* the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

FMT_MTD.1 Management of TSF data (3)

103 FMT_MTD.1.1(3) - The TSF shall restrict the ability to *modify* the [network proxy user passwords] to [the authorized administrator].

FMT_SMF.1 Specification of Management Functions

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

a) [delete and create the security attributes (information flow rules) described in FDP_IFF.1(1-4);
b) override default values for security attributes described in FMT_MSA.3 when an object or information is created;
c) query, modify, delete, and assign the user attributes defined in FIA_ATD.1.1;
d) modify the time and date used to form the timestamps in FPT_STM.1.1;
e) modify network proxy user passwords;
f) start-up and shut-down of the TOE; and
g) backup of audit trail data].

FMT_SMR.1 Security roles

105 FMT_SMR.1.1 - The TSF shall maintain the roles [defined set of authorized administrator roles with allocated privileges].

106 FMT_SMR.1.2 - The TSF shall be able to associate **administrative** users with the roles.

FAU_GEN.1 Audit data generation

107 FAU_GEN.1.1 - The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [the events in Table 6. Auditable Events].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 6. Auditable Events].

Table 6. Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.
FIA_UAU.2	Any use of the authentication mechanism	The user identities provided to the TOE.
FDP_IFF.1	All decisions on requests for information flow.	None
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_MOF.1	Use of the functions listed in this requirement	The identity of the authorized administrator performing the operation.

Functional Component	Auditable Event	Additional Audit Record Contents
	pertaining to audit.	
FMT_SMF.1	Use of the management functions	The identity of the authorized administrator performing the operation.

FAU_SAR.1 Audit review

109 FAU_SAR.1.1 - The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

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

FAU_STG.1 Protected audit trail storage

111 FAU_STG.1.1 - The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

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

FPT_STM.1 Reliable time stamps

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

114 Application Note: The word “reliable” in the above requirement means that the order of the occurrence of auditable events is preserved. Time stamps include both date and time information that are included in audit records.

FTP_TRP.1 Trusted path

115 FTP_TRP.1.1 – The TSF shall provide a communication path between itself and *remote* **administrative** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification and disclosure*.

116 FTP_TRP.1.2 – The TSF shall permit *remote **administrative** users* to initiate communication via the trusted path.

117 FTP_TRP.1.3 – The TSF shall require the use of the trusted path for [remote administration].

5.2 TOE Security assurance requirements

118 The TOE claims compliance to EAL 2 plus ALC_FLR.2. The security assurance requirements are identified in the following table.

Table 7. EAL2 plus ALC_FLR.2 Assurance Components

Assurance class	Assurance components
Class ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_FSP.2 Security enforcing functional specification
	ADV_TDS.1 Basic design
	ADV_ARC.1 Security architecture description
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample

6 TOE Summary Specification

119 This section presents a functional overview of the TOE and the security functions implemented by the TOE.

120 The TOE implements the following security functions:

- SECURITY MANAGEMENT
- IDENTIFICATION AND AUTHENTICATION
- USER DATA PROTECTION
  - URL/APPLICATION FILTER
  - ANTI-MALWARE
  - CERTIFICATE CHECKING
  - HTTPS SCANNER
- PROTECTION OF SECURITY FUNCTIONS
- AUDIT

121 TOE security functions are described in the following sections, with references to the particular SFRs that are addressed by those functions.

6.1 Security Management [FMT]

122 The TOE provides a web-based management interface required for an administrator to manage the MWG and utilize its security features. The interface also provides administrators access to audit information.

123 The TOE also supports the use of Representational State Transfer (REST) as an additional interface for certain management functions. This allows authenticated clients to make management requests to the MWG server.

6.1.1 Using Admin GUI [FMT_1]

124 Before an administrator may perform any management functions on a MWG they must establish a connection to MWG from a web browser on a local or remote generic computing platform. This connection is established via HTTPS. MWG downloads a Java applet to the browser to support use of the interface.

125 MWG maintains an authorized administrator role. MWG keeps a list that associates particular user identities with a defined authorized administrator role. When a user attempts to sign in at the GUI, the list is

consulted and a user on the list is given the administrative privileges. Only authorized administrators can read system configuration data and examine audit data.
(FMT_SMR.1, FPT_TRP.1)

6.1.2 MWG Administration [FMT_2]

126 A MWG administrator can manage all other administrative users of the system. On initialisation a single administrative user role is created with all privileges. Additional administrator roles can be created with access to any combination of the following: dashboard, policy rules, policy lists, policy settings, configuration, accounts and log files.

127 Only an authorized administrator is permitted to query, modify, delete or assign individual user attributes such as identity and password. Only an authorized administrator can start up and shut down the operation of the MWG, change the system time and date, and backup the audit trail.
(FMT_MTD.1 (1) & (2), FMT_MOF.1, FMT_SMF.1)

6.1.3 URL/Application Filter Policy Configuration [FMT_3]

128 The administrator manages the rules for filtering URL and application traffic which comprise the URL Policy. Only an authorized administrator is permitted to delete, modify, or add to the filter rules, and to the object definitions that are used in writing policy rules.
(FMT_MSA.1, FMT_SMF.1)

6.1.4 Anti-Malware Configuration [FMT_4]

129 The administrator manages the rules for MWG Anti-Malware filtering which comprise the Malware Policy. Only an authorized administrator is permitted to delete, modify, or add to the malware rules, and to the object definitions that are used in writing policy rules. (FMT_MSA.1, FMT_SMF.1)

6.1.5 Certificate Checking Configuration [FMT_5]

130 The administrator manages the rules for certificate checking which comprise the Certificate Policy. Only an authorized administrator is permitted to delete, modify, or add to the certificate checking rules, and to the object definitions that are used in writing policy rules.
(FMT_MSA.1, FMT_SMF.1)

6.1.6 HTTPS Scanner Configuration [FMT_6]

131 The administrator manages the rules for performing HTTPS decryption which comprise the HTTPS Policy. Only an authorized administrator is permitted to delete, modify, or add to the HTTPS rules, and to the object definitions that are used in writing policy rules. (FMT_MSA.1, FMT_SMF.1)

6.1.7 Initial Configuration [FMT_7]

132 The default TOE configuration restricts traffic flow. An authorized administrator must override initial information flow security attributes to deactivate URL filtering or Anti-malware filtering in order to allow more data to flow. (FMT_MSA.3, FMT_SMF.1)

6.2 Identification and Authentication [FIA]

133 The MWG management function provides an administrative interface protected by an identification and authentication mechanism. The TOE requires administrative users to provide unique identification (user IDs) and authentication data (passwords) before any access to the TOE is granted.

6.2.1 User Identification [FIA_1]

134 MWG supports administrative users. The identification information for each MWG administrative user includes the following (FIA_ATD.1):

- The user login name (identity)
- Association of the user with the authorized administrator role
- The password required to login.

135 MWG requires any potential user to provide identification information before it will allow any security relevant activity on behalf of that user. (FIA_UID.2)

136 Other individuals or external IT entities that send inter-network communications mediated via MWG are not considered MWG users. They cannot log into MWG and have no direct access to MWG. However, the TOE can be configured to require network proxy users to be identified.

6.2.2 Authentication [FIA_2]

137 MWG requires successful password (and optionally client certificate) authentication before allowing administrative user access. MWG consults its own or external user policy storage to determine if the provided authentication credentials are valid (e.g. Radius, LDAP). MWG supports reusable passwords with a minimum size of 8 characters. A delay of 5 seconds is introduced following each unsuccessful login attempt. (FIA_UAU.2, FIA_UAU.5)

138 The TOE can be configured to require authentication of network proxy users. (FIA_UAU.2, FMT_MTD.1(3))

6.3 User Data Protection [FDP]

139 MWG provides URL Filter, Anti-Malware, Certificate Checking and HTTPS Scanning capabilities to examine and filter IP traffic for inappropriate or harmful content. Corresponding policies, or rule sets, are configured to determine what information to watch for and how to react if it is detected. The filters can access various knowledge bases to identify potential threats that might be present in the IP traffic (HTTP, HTTPS and FTP).

6.3.1 URL Filter [FDP_1]

140 On MWG, the flow of HTTP, HTTPS and FTP information through the system is determined by key subject and information security attributes. In particular, the authorized administrator can set up URL filter rules that depend upon the presumed source subject address, the URL requested and the category that can be attributed to the URL. MWG consults its URL Global Threat Intelligence database (that has organized URLs into predefined categories) in order to filter the HTTP/HTTPS/FTP traffic according to the rules. Full support is provided for IPv6.

141 Rules can make use of lists. For example a blocking rule may make use of a list of URLs related to online shopping. Such lists can be created by an administrator, obtained by subscription to McAfee, or from external sources over HTTPS or FTP. The TOE supports the use of live enquiries to external lists, avoiding the need to maintain static lists on the TOE.

142 The TOE also makes use of a McAfee database to identify and filter specific applications (e.g. Facebook), based on known characteristics of the application traffic.
(FDP_IFC.1 (1), FDP_IFF.1 (1))

6.3.2 Anti-Malware Filter [FDP_2]

143 Anti-Malware filtering is turned on by an authorized MWG administrator. Following activation, MWG invokes specific Anti-Malware searches (including engines from McAfee and Avira) to examine the IP traffic to look for malware. When a malware match is identified, MWG performs the configured actions to allow or disallow the traffic flow. (FDP_IFC.1 (2), FDP_IFF.1 (2))

6.3.3 Certificate Checker [FDP_3]

144 Certificate Checking is turned on by an authorized MWG administrator. Following activation, MWG examines the IP traffic to look for a certificate with characteristics such as validity, lifetime, name and chain. MWG then uses that information to determine whether to perform the configured actions to allow or disallow the traffic to flow to the HTTPS Scanner or content filters. (FDP_IFC.1 (3), FDP_IFF.1 (3))

6.3.4 HTTPS Scanner [FDP_4]

145 Upon activation by an authorized administrator, MWG will decrypt HTTPS traffic prior to forwarding the clear-text content to the MWG URL and Anti-Malware filter functions. Such messages, if they pass the filters, will be re-encrypted prior to being forwarded to their intended destinations. MWG uses OpenSSL FIPS Object Module Version 1.1.2 for HTTPS encryption and decryption. MWG virual and appliance cryptographic modules are undergoing FIPS 140 validation, and reports are awaiting review by CMVP (Block 2). (FDP_IFC.1 (4), FDP_IFF.1 (4), FCS_COP.1 (1), FCS_COP.1 (2), FCS_CKM.1 (1), FCS_CKM.2 (2), FCS_CKM.4)

6.4 Protection of Security Functions [FPT]

146 The TOE provides an accurate time source which is needed to ensure that the sequence of reported security actions and security decisions is correct.

6.4.1 Time Stamps [FPT_1]

147 The hardware platform, part of the IT environment, includes a battery-backed real time clock (RTC) which maintains the time when the platform is shut down.

148 The software, with its McAfee Linux OS features, reads the RTC (or its representation in VMware) at bootup and maintains its own time stamp

throughout operation. The software provides the reliable time stamp to any processes that request the time. Also, the software manages any changes to the time and determines the access requirements for administrative users or processes desiring to modify the time. Once the software has changed the time, it updates the RTC. The software provides the time stamp during TOE operation, while the RTC maintains the time when the platform is shut down. (FPT_STM.1)

6.4.2 Trusted path [FPT_2]

149 The TOE makes use of HTTPS as a secure communication path between the administrative browser and the server. This protects the confidentiality and integrity of the management traffic over a potentially untrusted network. (FPT_TRP.1)

6.5 Audit [FAU]

150 The TOE generates two different types of audit records. System audit records cover activities related to the administration and management of the TOE, while traffic audit records provide a log of information flowing through the MWG's filtering operations. The TOE collects both the system audit and traffic log information into a data store, which is part of the TOE. MWG records attempts to access the system itself, such as successful and failed authentication, as well as the actions taken by the user once authenticated. Auditable actions include addition or deletion of administrators, changes to the filtering rules and decisions made by the filtering functions. Authorized administrators are allowed to review audit data.

6.5.1 Logging [FAU_1]

151 MWG provides information to identify the type of auditable event and entities related to the event as described in Table 7. Auditable Events. The information includes both success and failure outcomes for the auditable events. MWG augments that audit event with a time stamp. (FAU_GEN.1)

152 MWG accumulates the audit and access events into log files. The authorized administrator may remove audit data to manage the storage space, but nobody is allowed to modify the content of the audit files. The format of new entries to the access logs can be modified. (FAU_STG.1)

153 MWG audit is separated into an “audit log” which covers administrative activities and an “access log” which covers communication requests and the result (traffic passes or not).

6.5.2 Audit Reporting [FAU_2]

154 The MWG management application allows an authorized administrator to review and interpret the audit data using a browser on a generic computing platform. The selected audit records are sorted in time sequence order and are displayed in a readable format. (FAU_SAR.1)

6.5.3 Audit Data Protection [FAU_3]

155 MWG provides mechanisms which allow an authorized administrator to manage the audit storage to minimize the risk of losing data. The authorized administrator can cause MWG to automatically rotate, delete and push audit data off box to ensure adequate space for new records while making existing records available for review. Audit data cannot be deleted from the system without authorisation. (FAU_STG.1)

7 Rationale

7.1 Rationale for TOE Security Objectives

156 O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH because it requires that administrators be uniquely identified before accessing the TOE.

157 O.MEDIAT This security objective is necessary to counter the threat: T.MEDIAT that has to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE.

158 O.SECSTA This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

159 O.SELPRO This security objective is necessary to counter the threats: T.SELPRO, T.NOAUTH, and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. In particular, it counters attempts from an attacker to bypass the TSF to gain access to the TOE or the assets it protects. It also counters attempts to exhaust the audit trail and thereby bypass the audit security function.

160 O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search the information contained in the audit trail.

161 O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

162 O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

Table 8. Mapping Threats to TOE Security Objectives

	T.NOAUTH	T.MEDIAT	T.AUDACC	T.SELPRO	T.AUDFUL
O.IDAUTH	X				
O.MEDIAT		X			
O.SECSTA	X			X	
O.SELPRO	X			X	X
O.AUDREC			X		
O.ACCOUN			X		
O.SECFUN	X				X

7.2 Rationale for the TOE Operating Environment Security Objectives

163 OE.PHYSEC The TOE is physically secure. This objective is needed to ensure that unauthorized individuals have no physical access to the computing platform running the TOE software. This precludes such individuals from performing such activities as restarting the system or loading software that changes the security function operations.

164 OE.PUBLIC The TOE does not host public data. This objective helps ensure that the computing platform is dedicated to the TOE software and related data, thus precluding any possible adverse effects of foreign data.

165 OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error. This objective ensures that the administrators are trusted, competent and take no malicious actions.

166 OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE. This objective ensures that the filtering function of the TOE cannot be bypassed as traffic flows between the networks.

167 OE.GUIDAN This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

168 OE.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC because it ensures that authorized administrators receive the proper training.

169 OE.PROLIN The communication path between the TOE and the management browser is physically or cryptographically protected. This objective ensures that no-one can gain access to the TOE by connecting a rogue IT device to this communication line.

170 OE.NOREMO Human users who are not authorized administrators can not directly or remotely access the management platform. This objective ensures that such users have neither local nor remote access to the TOE via the management platform.

171 OE.BENIGN The OS running on the management platform will provide necessary computing services, but will not tamper with browser communications to the TOE. This objective ensures that OS does not contain inappropriate features or vulnerabilities that might adversely affect browser communications with the TOE and thereby change the TOE security policy enforcement.

Table 9. Mapping Threats to TOE Operating Environment Security Objectives

	T.TUSAGE	T.AUDACC
OE.GUIDAN	X	X
OE.ADMTRA	X	X

172 The remaining security objectives for the environment are, in part, a re-statement of the security assumptions. Each of these security objectives traces to the corresponding assumption with a similar name. Objective OE.PHYSEC traces to assumption A.PHYSEC, for example.

7.3 Rationale for TOE Security Requirements

173 The functional and assurance requirements presented in this ST are mutually supportive and their combination meets the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. Table 13. Mapping SFRs to TOE Security Objectives illustrates the mapping between the TOE security requirements and the TOE security objectives. Table 11. Mapping Threats to TOE Security Objectives demonstrates the relationship between the TOE threats and the TOE security objectives. Together these tables demonstrate the completeness and sufficiency of the requirements.

FMT_SMR.1 Security roles

174 Each of the CC class FMT components in this ST depend on this component. It requires the ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

175 This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with an administrative user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

FIA_UID.2 User identification before any action

176 This component ensures that before anything occurs on behalf of a user, the user's identity is available to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_UAU.2 User authentication before any action

177 This component was chosen to ensure that authentication mechanisms are used appropriately in all attempts to access the TOE. An additional metric for this requirement is defined to ensure that the mechanisms are of adequate strength to protect against authentication data compromise. This component traces back to and aids in meeting the following objective: O.IDAUTH.

FIA_UAU.5 Multiple authentication mechanisms

178 This component allows an authorized administrator to specify a range of authentication methods for network proxy and administrative users. This component traces back to and aids in meeting the following objective: O.IDAUTH.

FDP_IFC.1 Subset information flow control (1) – (4)

179 This component identifies the entities involved in the URL, MALWARE, Certificate and HTTPS SFPs (IP information flowing between networks). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes (1) – (4)

180 This component identifies the attributes of the users sending information, as well as the attributes for the information itself. Each information flow policy is defined by saying under what conditions information is

permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FCS_COP.1 Cryptographic operation (1) – (2)

181 These components provide symmetric and asymmetric encryption and decryption services to support the mediation of HTTPS traffic. These components trace back to and aid in meeting the following objective: O.MEDIAT.

FCS_CKM.1 Cryptographic key generation (1) – (2)

182 These components provide symmetric and asymmetric key generation services to support the mediation of HTTPS traffic. These components trace back to and aid in meeting the following objective: O.MEDIAT.

FCS_CKM.4 Cryptographic key destruction

183 This component provides key destruction services to support the mediation of HTTPS traffic. This component traces back to and aid in meeting the following objective: O.MEDIAT

FMT_MSA.1 Management of security attributes

184 This component ensures the TSF enforces the four information flow security function policies to restrict the ability to add, delete, and modify within a rule those security attributes that are listed in section FDP_IFF.1 (1) - (4). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.3 Static attribute initialization

185 This component ensures that there is a predictable, restrictive, policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.

FMT_MTD.1 Management of TSF data (1)

186 This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN

FMT_MTD.1 Management of TSF data (2)

187 This component ensures that the TSF restrict abilities to modify the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.1 Management of TSF data (3)

188 This component ensures that only an authorized administrator can modify a network proxy user password. This component traces back to and aids in meeting the following objective: O.IDAUTH.

FPT_STM.1 Reliable time stamps

189 FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_GEN.1 Audit data generation

190 This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

191 This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

192 This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator, and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECSTA and O.SECFUN.

FMT_MOF.1 Management of security functions behaviour

193 This component was to ensure the TSF restricts the ability to modify the behaviour of functions such as audit trail management to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA and O.SECFUN.

FMT_SMF.1 Specification of Management Functions

194 This component is a necessary prerequisite for and supports the following SFRs that have been rationalized above: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2) and FMT_MOF.1. This component addresses the same security objectives.

FTP_TRP.1 Trusted path

195 This component requires the use of a trusted path for remote administrator access, protecting the integrity and confidentiality of the communication path. The component traces back to and aids in meeting O.IDAUTH.

Table 10. Mapping SFRs to TOE Security Objectives

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN
FMT_SMR.1							X
FIA_ATD.1	X						X
FIA_UID.2	X					X	
FIA_UAU.2	X						
FIA_UAU.5	X						
FDP_IFC.1 (1)		X					
FDP_IFC.1 (2)		X					
FDP_IFC.1 (3)		X					
FDP_IFC.1 (4)		X					
FDP_IFF.1 (1)		X					
FDP_IFF.1 (2)		X					
FDP_IFF.1 (3)		X					
FDP_IFF.1 (4)		X					
FCS_COP.1 (1)		X					
FCS_COP.1 (2)		X					
FCS_CKM.1 (1)		X					
FCS_CKM.1 (2)		X					
FCS_CKM.4		X					

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN
FMT_MSA.1		X	X				X
FMT_MSA.3		X	X				
FMT_MTD.1 (1)							X
FMT_MTD.1 (2)							X
FMT_MTD.1(3)	X						
FPT_STM.1					X		
FAU_GEN.1					X	X	
FAU_SAR.1					X		
FAU_STG.1			X	X			X
FMT_MOF.1			X				X
FMT_SMF.1		X	X				X
FPT_TRP.1	X						

7.4 Rationale for Assurance Requirements

196 The EAL 2 level of assurance is consistent with best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2. Augmentation with ALC_FLR.2 provides customers with added confidence that any reported security flaws in the TOE will be addressed.

7.5 Dependency Rationale

197 The following table is provided as evidence that all dependencies have been satisfied in this ST.

Table 11. SFR/SAR Dependency Evidence

SFR/SAR	Dependencies	Satisfied?
FMT_SMR.1	FIA_UID.1	Yes, using FIA_UID.2
FIA_ATD.1	NONE	N/A
FIA_UID.2	NONE	N/A
FIA_UAU.2	FIA_UID.1	Yes, using FIA_UID.2
FIA_UAU.5	NONE	N/A
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes Yes
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FCS_CKM.4	Yes
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 and FCS_CKM.4	Yes
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	 Yes Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes Yes
FPT_STM.1	NONE	N/A
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_SMF.1	None	N/A
FPT_TRP.1	None	N/A

SFR/SAR	Dependencies	Satisfied?
ACM_CMC.2	ACM_CMS.1	Yes
ACM_CMS.2	None	N/A
ALC_DEL.1	None	N/A
ALC_FLR.2	None	N/A
ADV_FSP.2	ADV_TDS.1	Yes
ADV_TDS.1	ADV_FSP.2	Yes
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	Yes Yes
AGD_OPE.1	ADV_FSP.1	Yes
AGD_PRE.1	None	N/A
ATE_COV.1	ADV_FSP.1 ATE_FUN.1	Yes Yes
ATE_FUN.1	NONE	N/A
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 AGD_COV.1 ATE_FUN.1	Yes Yes Yes Yes Yes

7.6 Rationale for TOE Summary Specification

198 This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

199 The specified TOE security functions work together to satisfy the TOE security functional requirements. Section 6.1 includes in the descriptions of security functions a mapping to SFRs to show that each security function is traced to at least one SFR. Table 15. Mapping of SFRs to Security Functions demonstrates that each SFR is covered by at least one security function.

Table 12. Mapping of SFRs to Security Functions

Functional Components		Security Function
FMT_SMR.1	Security roles	FMT
FIA_ATD.1	User attribute definition	FIA
FIA_UID.2	User identification before any action	FIA
FIA_UAU.2	User authentication before any action	FIA
FIA_UAU.5	Multiple authentication mechanisms	FIA

Functional Components		Security Function
FDP_IFC.1	Subset information flow control (1) – (4)	FDP
FDP_IFF.1	Simple security attributes (1) – (4)	FDP
FMT_MSA.1	Management of security attributes	FMT
FMT_MSA.3	Static attribute initialization	FMT
FMT_MTD.1	Management of TSF data (1)	FMT
FMT_MTD.1	Management of TSF data (2)	FMT
FMT_MTD.1	Management of TSF data (3)	FIA
FPT_STM.1	Reliable time stamps	FPT
FAU_GEN.1	Audit data generation	FAU
FAU_SAR.1	Audit review	FAU
FAU_STG.1	Protected audit trail storage	FAU
FMT_MOF.1	Management of security functions behaviour	FMT
FMT_SMF.1	Specification of Management Functions	FMT
FTP_TRP.1	Trusted path	FPT

200 Table16 provides rationale that the security functions are suitable to meet the SFRs.

Table 13. Suitability of Security Functions

Security Function	SFR Identifier	Justification
FMT	FMT_SMR.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 (1) FMT_MTD.1 (2) FMT_MOF.1 FMT_SMF.1	The FMT security function provides an authorized administrator, as appropriate, with the capability to manage the operation of MWG. A user acting in the administrator role is allowed to control the operation of the TOE, manage user attributes and modify the system time and date. Authorized administrators are also provided with the capability to manage the flow of information through MWG. This includes complete control of all information flow security attributes. Authorized administrators are provided the capability to selectively review audit data and may remove old audit records.
FIA	FIA_ATD.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.5 FMT_MTD.1(3)	The FIA security function provides the capability to determine and verify the identity of users, determine their authority to interact with the TOE, and associate the proper security attributes for each authorized user. Also, it ensures that user identification and authentication precede any TSF-mediated actions on behalf of a user and provides for password and certificate based authentication.
FDP	FDP_IFC.1 (1) FDP_IFC.1 (2) FDP_IFC.1 (3) FDP_IFC.1 (4) FDP_IFF.1 (1) FDP_IFF.1 (2) FDP_IFF.1 (3) FDP_IFF.1 (4) FCS_COP.1 (1) FCS_COP.1 (2) FCS_CKM.1 (1) FCS_CKM.1 (2) FCS_CKM.4	The FDP security function mediates information flows through MWG. It controls IP traffic flow, allowing for URL and Anti-Malware filtering. In addition, the authorized administrator may activate certificate checking and HTTPS decryption so that clear text information can be provided as input to the other filters.
FPT	FPT_STM.1 FPT_TRP.1	The FPT security function provides a reliable time stamp that is essential for TOE security audits. The reliable time stamp provides critical information for monitoring user activities and for detecting real, potential or imminent violations of the TOE's security policy. FPT also provides a trusted path for remote administrators to communicate with the TOE in a secure manner.
FAU	FAU_GEN.1 FAU_SAR.1 FAU_STG.1	The FAU security function generates audit records related to security relevant events. It provides the capability to review audit logs. Audit records are protected from modification and

Security Function	SFR Identifier	Justification
		unauthorized deletion.

201 Because the security functions trace to SFRs, which were shown to be mutually supportive, and Table 16 justifies that the security functions implement all the SFRs, it is concluded that the security functions work together to satisfy the SFRs.