McAfee® Web Gateway
Version 7.0.1.1
EAL 2 + ALC_FLR.2
Security Target

Release Date:	September 2010
Document ID:	
Version:	Draft J
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 7.0.1.1. 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**
86-0948031-A	Initial version for evaluation of MWG version 7.0.	February 14, 2008
86-0948031-B	Minor Corrections after OR.	April 14, 2008
86-0948031-C	Add SMF requirement and respond to validator OR	May 2, 2008
86-0948031-D	Product name change	May 12, 2008
86-0948031-E	Removed IM + other minor changes for consistency	July 30, 2008
86-0948031-F	Removed IM + other minor changes for consistency	September 12, 2008
86-0948031-G	Minor changes for CB comments	November 12, 2008
86-0948031-H	Product name change, version update and other minor changes	July 2010
86-0948031-I	Internal McAfee review	August 2010
86-0948031-J	To address CCS Instruction #4	September 2010

Table of Contents

1 SECURITY TARGET INTRODUCTION 1

1.1 ST AND TOE IDENTIFICATION 1
1.2 CONVENTIONS, TERMINOLOGY, AND ACRONYMS 2
1.2.1 Conventions 2
1.2.2 Terminology 3
1.2.3 Acronyms 3
1.3 REFERENCES 4
1.4 COMMON CRITERIA CONFORMANCE CLAIMS 4

2 TOE DESCRIPTION 5

2.1 PRODUCT TYPE 6
2.2 PRODUCT DESCRIPTION 6
2.3 PRODUCT FEATURES 6
2.4 APPLICATION CONTEXT 6
2.5 SECURITY ENVIRONMENT TOE BOUNDARY 7
*2.5.1 Security Features to be Evaluated ..... **Error! Bookmark not defined.***
*2.5.2 Features not to be Evaluated ..... **Error! Bookmark not defined.***
2.5.3 Physical Scope and Boundary 9
2.5.4 Evaluated TOE Configuration 9
2.5.5 Logical Scope and Boundary 10

3 TOE SECURITY ENVIRONMENT 12

3.1 ASSUMPTIONS 12
3.1.1 TOE Assumptions 12
3.2 THREATS 13
3.2.1 Threats Addressed by the TOE 13
3.2.2 Threats Addressed by the TOE Operating Environment 14
3.3 ORGANIZATIONAL SECURITY POLICIES 14

4 SECURITY OBJECTIVES 15

4.1 SECURITY OBJECTIVES FOR THE TOE 15
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 16

5 TOE IT SECURITY REQUIREMENTS 17

5.1 TOE SECURITY REQUIREMENTS 17
5.1.1 TOE Security Functional Requirements 17
5.2 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 26
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 26
5.3.1 Additional Security Assurance Requirements 27

6 TOE SUMMARY SPECIFICATION 30

6.1 TOE SECURITY FUNCTIONS 30
6.1.1 Security Management [FMT] 30
6.1.2 Identification and Authentication [FIA] 32
6.1.3 User Data Protection [SW_FDP] 32
6.1.4 Protection of Security Functions [FPT] 33
6.1.5 Audit [FAU] 34
6.2 ASSURANCE MEASURES 35
6.2.1 Configuration Management 35
6.2.2 Delivery and Operation 35

6.2.3 Development *36*
6.2.4 Guidance *36*
6.2.5 Life-cycle Support *36*
6.2.6 Test *37*
6.2.7 Vulnerability Assessment *37*

7 PP CLAIMS **38**

8 RATIONALE **39**

8.1 RATIONALE FOR TOE SECURITY OBJECTIVES 39
8.2 RATIONALE FOR THE TOE OPERATING ENVIRONMENT SECURITY OBJECTIVES 40
8.3 RATIONALE FOR TOE SECURITY REQUIREMENTS 41
8.4 RATIONALE FOR TOE IT ENVIRONMENT SECURITY REQUIREMENTS 45
8.5 RATIONALE FOR ASSURANCE REQUIREMENTS 46
8.6 SOF RATIONALE 46
8.7 DEPENDENCY RATIONALE 46
8.8 INTERNAL CONSISTENCY AND MUTUALLY SUPPORTIVE RATIONALE 48
8.9 RATIONALE FOR EXPLICIT REQUIREMENTS 48
8.10 RATIONALE FOR TOE SUMMARY SPECIFICATION 48
8.10.1 TOE Security Requirements *49*
8.10.2 TOE Assurance Requirements *51*

List of Tables

TABLE 1. ASSUMPTIONS FOR TOE OPERATIONAL ENVIRONMENT 12
TABLE 2. THREATS ADDRESSED BY THE TOE 13
TABLE 3. THREATS ADDRESSED BY THE TOE OPERATING ENVIRONMENT 14
TABLE 4. SECURITY OBJECTIVES FOR THE TOE 15
TABLE 5. SECURITY OBJECTIVES FOR THE TOE OPERATING ENVIRONMENT 16
TABLE 6. TOE SECURITY FUNCTIONAL REQUIREMENTS 17
TABLE 7. AUDITABLE EVENTS 24
TABLE 8 FUNCTIONAL COMPONENTS OF THE IT ENVIRONMENT 26
TABLE 9 ADDITIONAL SAR TO AUGMENT EAL2 27

List of Figures

FIGURE 1 TYPICAL MCAFEE WEB GATEWAY APPLICATION 5
FIGURE 2 MCAFEE WEB GATEWAY TOE SECURITY ENVIRONMENT 8

1 Security Target Introduction

1 This Security Target has been written to support the evaluation of McAfee Web Gateway (MWG) software version 7.0.1.1. 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 (ST) identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

3 A ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., target of evaluation (TOE)). An ST 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 Environment).

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 which meet that set of requirements (in Section 6, TOE Summary Specification).

d) Protection Profile claims and overall ST rationale (Sections 7 and 8, respectively).

4 The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex B, and Part 3, Chapter 10.

1.1 ST and TOE Identification

5 This section provides ST and TOE identification information.

ST Title:	McAfee Web Gateway Version 7.0.1.1 EAL2 +ALC_FLR.2 Security Target
ST Author:	Primasec Ltd.
ST Revision Number:	86-0948031-J
ST Date:	Sep 2010
TOE Identification:	Software:
	McAfee Web Gateway Software Version 7.0.1.1

	Administrative Guidance for receiving, installing and managing the TOE Product Guide McAfee Web Gateway version 7.0.1 Quick Start McAfee Web Gateway, part number 700-2513A00
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (also known as ISO 15048)
Assurance Level:	EAL2, augmented with ALC_FLR.2

1.2 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.

1.2.1 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 ST 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.

1.2.2 Terminology

9 In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Human user	Any person who interacts with the TOE.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
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 an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
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 definitions:

Authorized Administrator – A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

1.2.3 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
IGS	Installation, Generation and Startup
IT	Information Technology

MLOS	McAfee Linux Operating System
MWG	McAfee Web Gateway
OSP	Organizational 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
TSP	TOE Security Policy

1.3 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 August 2005, version 2.3, CCMB-2005-08-001.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, version 2.3, CCMB-2005-08-002.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, version 2.3, CCMB-2005-08-003.
[CEM]	Common Methodology for Information Technology Security Evaluation – August 2005, version 2.3, CCMB-2005-08-004.

1.4 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 an FTP system, every transaction is piped through it for filtering and malware scanning on the content.

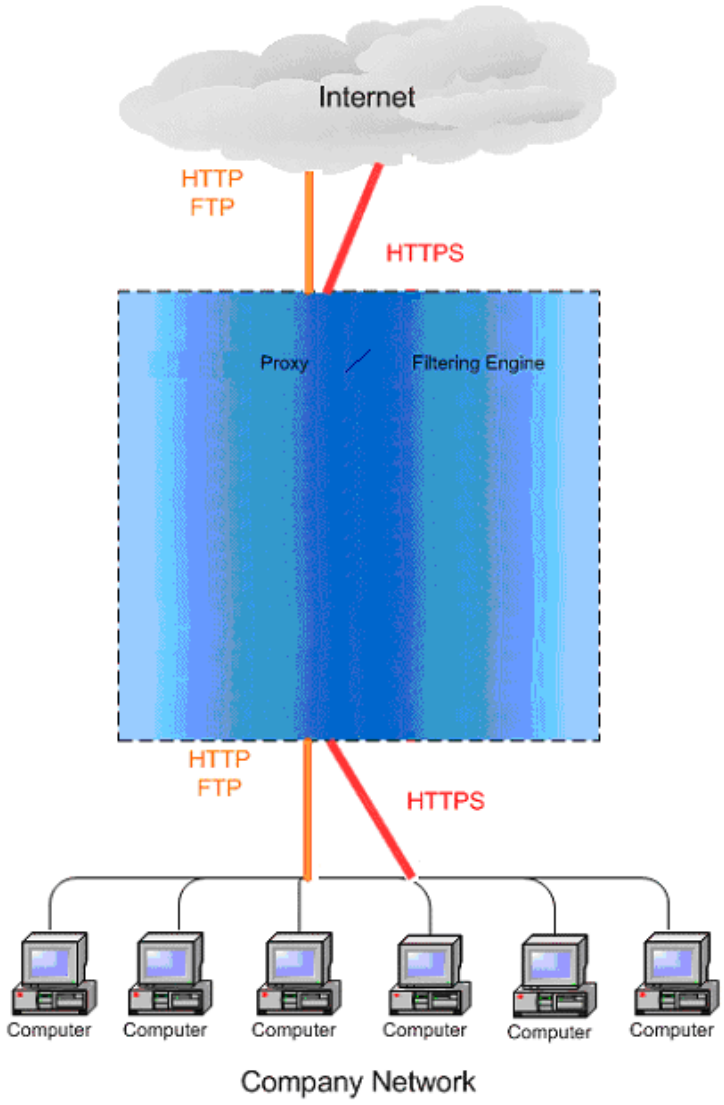

Figure 1 Typical McAfee Web Gateway Application

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) Remote administration from connected networks

c) Cluster Management

d) Multiple Authentication Mechanisms

e) High availability

f) ICAP

g) Transparent router and transparent bridge modes

h) Use of multiple administrator roles

i) Use of ePolicy Orchestrator

j) Kerberos administration

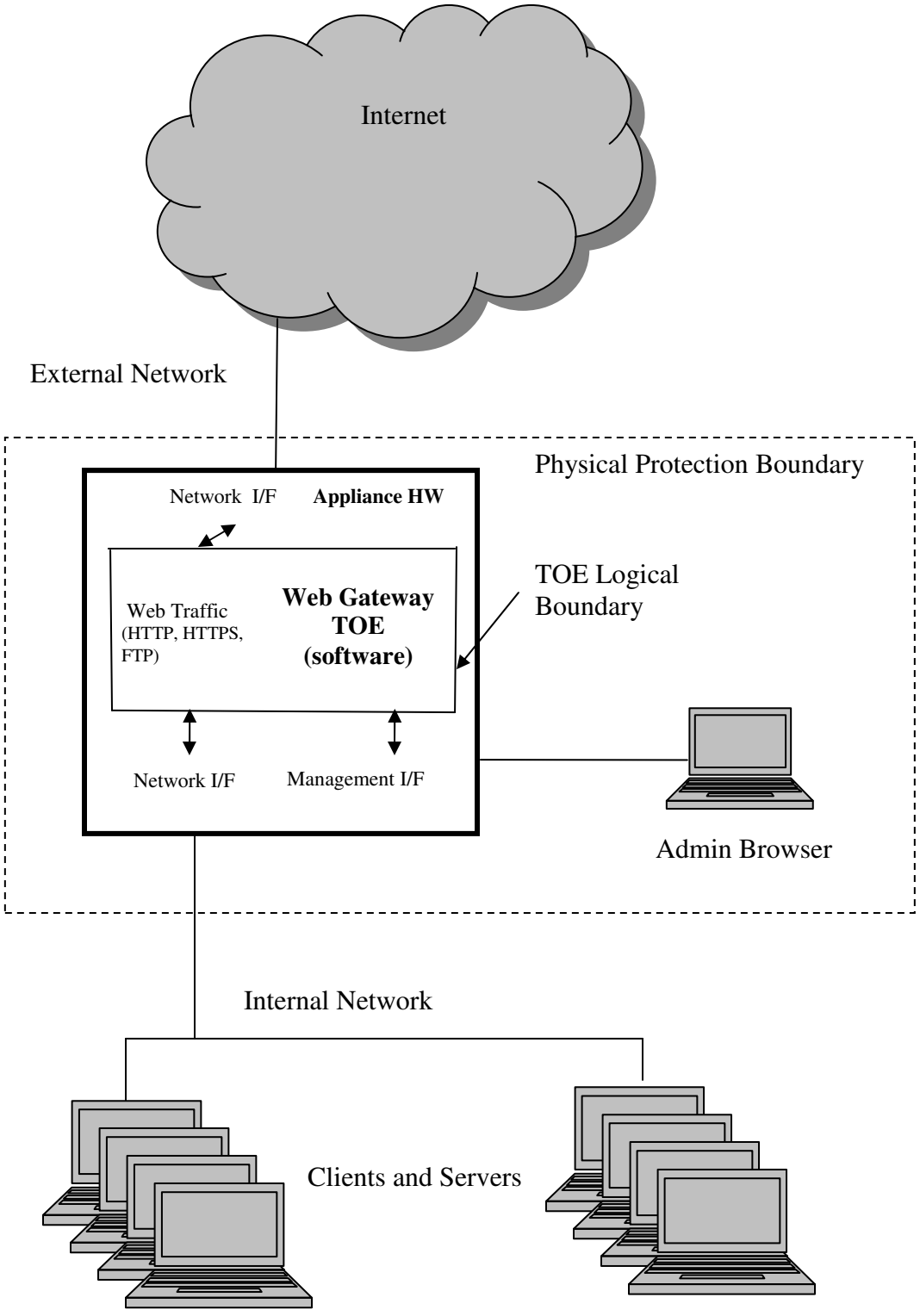

Figure 2 McAfee Web Gateway TOE Security Environment

2.5.3 Physical Scope and Boundary

23 The TOE consists of MWG Software Version 7.0.1.1. 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 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 local, generic computing platform with a Windows operating system; however, the platform, the browser, and the Windows OS are not part of the TOE.

2.5.4 Evaluated TOE Configuration

24 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. Even though MWG can communicate with an administrative browser on any connected network; the evaluated configuration binds administration to the isolated management network (or to the internal network if the appliance hardware only includes two network connections).

25 The TOE software version is available and executes properly across the entire family of MWG appliance models: WW500, WW1100, WW1900, WW2900, WG5000 and WG5500. The software also executes properly in a virtual environment under VMware ESX, ESXi or VMware Workstation (version 5.5 or later).

26 The evaluated configuration is comprised of TOE software running on a MWG appliance or virtual platform, the generic Windows based administrative workstation running Firefox, and the associated network interconnections. These components are maintained in a physically protected IT environment that prohibits unauthorized access.

2.5.4.1 Hardware Security Considerations

27 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.

2.5.5 Logical Scope and Boundary

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

a) Security Management [SW_FMT]

b) Identification and Authentication [SW_FIA]

c) User Data Protection [SW_FDP]

d) Protection of Security Functions [SW_FPT]

e) Audit [SW_FAU]

2.5.5.1 Security Management [FMT]

29 An administrator uses a browser running on a Windows computer (part of the IT environment) to perform management functions on MWG. This administrative workstation communicates with MWG via one of the networks connected to MWG.

2.5.5.2 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.

2.5.5.3 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.

2.5.5.4 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.

.

2.5.5.5 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 TOE Security Environment

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 IT and operating environments are described.

39 Organization 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 workstation. The TOE, the management workstation, and the administrative communication path are all managed in a physically secure environment with no remote access.

3.1.1 TOE Assumptions

42 The TOE claims the assumptions in the table below:

Table 1. Assumptions for TOE Operational Environment

Assumption Identifier	Assumption Description
A.PHYSEC	The TOE and local administration platform are physically secure.
A.PUBLIC	The TOE and local 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 can not flow between the internal and external networks unless it passes through the TOE.
A.PROLIN	The communication path between the TOE

Assumption Identifier	Assumption Description
	and the local administration workstation (browser) is physically protected.
A.NOREMO	Human users who are not authorized administrators cannot directly or remotely access the local administration platform.
A.BENIGN	The Windows OS running on the local administration 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 Threats may be addressed by the TOE or by the TOE operating environment.

3.2.1 Threats Addressed by the TOE

45 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 Addressed by the TOE

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.

Threat Identifier	Threat Description.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.

3.2.2 Threats Addressed by the TOE Operating Environment

46 The following threats are addressed by the TOE operating environment.

Table 3. Threats Addressed by the TOE Operating Environment

Threat Identifier	Threat Description.
TE.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

3.3 Organizational Security Policies

47 This ST does not identify any OSPs.

4 Security Objectives

48 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

49 The TOE accomplishes the following security objectives:

Table 4. Security Objectives for the TOE

Objective Identifier	Objective Description
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user 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.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized

Objective Identifier	Objective Description
	administrators are able to access such functionality.

4.2 Security Objectives for the Environment

50 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 5. 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 local administration workstation (browser) is physically protected.
OE.NOREMO	Human users who are not authorized administrators must not directly or remotely access the local administration platform.
OE.BENIGN	The Windows OS running on the local administration platform must provide necessary computing services, but must not tamper with browser communications with the TOE.

5 TOE IT Security Requirements

51 This section provides functional and assurance requirements that must be satisfied by a Security Target-compliant TOE.

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

52 The security functional requirements for this Security Target consist of the following components from Part 2 of the CC, summarized in Table 6. TOE Security Functional Requirements. The SFRs are provided in their entirety in the subsequent paragraphs.

Table 6. TOE Security Functional Requirements

Functional Components	
FMT_SMR.1	Security roles
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FDP_IFC.1	Subset information flow control (1)
FDP_IFC.1	Subset information flow control (2)
FDP_IFC.1	Subset information flow control (3)
FDP_IFC.1	Subset information flow control (4)
FDP_IFF.1	Simple security attributes (1)
FDP_IFF.1	Simple security attributes (2)
FDP_IFF.1	Simple security attributes (3)
FDP_IFF.1	Simple security attributes (4)
FCS_COP.1	Cryptographic operation (1)
FCS_COP.1	Cryptographic operation (1)
FCS_CKM.1	Cryptographic key generation (1)
FCS_CKM.1	Cryptographic key generation (2)
FCS_CKM.4	Cryptographic key destruction
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data (1)

Functional Components	
FMT_MTD.1	Management of TSF data (2)
FPT_STM.1	Reliable time stamps
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FMT_MOF.1	Management of security functions behavior
FMT_SMF.1	Specification of Management Functions

5.1.1.1 Comprehensive Listing of all TOE SFRs

FMT_SMR.1 Security roles

53 FMT_SMR.1.1 - The TSF shall maintain the ~~roles~~ **role** [authorized administrator].

54 FMT_SMR.1.2 - The TSF shall be able to associate users with the ~~roles~~ **role**.

FIA_ATD.1 User attribute definition

55 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

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

FIA_UAU.2 User authentication before any action

57 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.

58 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.

59 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.

60 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.

61 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.

62 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.

63 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)

64 FDP_IFC.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)

65 FDP_IFC.1.1 - 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)

66 FDP_IFC.1.1 - 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)

67 FDP_IFC.1.1 - 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)

68 FDP_IFF.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;
- URL requested in HTTP message; and
- Category of the requested URL].

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

70 [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].

71 FDP_IFF.1.3 - The TSF shall enforce the [none].

72 FDP_IFF.1.4 - The TSF shall provide the following [none].

73 FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

74 FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules: [none].

FDP_IFF.1 Simple security attributes (2)

75 FDP_IFF.1.1 - 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].

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

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

78 FDP_IFF.1.3 - The TSF shall enforce the [none].

79 FDP_IFF.1.4 - The TSF shall provide the following [none].

80 FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

81 FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules: [none].

FDP_IFF.1 Simple security attributes (3)

82 FDP_IFF.1.1 - 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)].

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

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

85 FDP_IFF.1.3 - The TSF shall enforce the [none].

86 FDP_IFF.1.4 - The TSF shall provide the following [none].

87 FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

88 FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules: [none].

FDP_IFF.1 Simple security attributes (4)

89 FDP_IFF.1.1 - 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].

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

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

92 FDP_IFF.1.3 - The TSF shall enforce the [none].

93 FDP_IFF.1.4 - The TSF shall provide the following [none].

94 FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

95 FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules: [none].

96 Application Note: MWG uses OpenSSL FIPS Object Module Version 1.1.2 (FIPS 140-2 certificate 918) for https encryption and decryption.

FCS_COP.1 Cryptographic operation (1)

97 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)

98 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 4096 bits] that meet the following: [PKCS#1 v2.1].

FCS_CKM.1 Cryptographic key generation (1)

99 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)

100 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 4096 bits] that meet the following: [ANSI X9.62].

FCS_CKM.4 Cryptographic key destruction

101 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_MSA.1 Management of security attributes

102 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

103 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.

104 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.

105 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)

106 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)

107 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].

FPT_STM.1 Reliable time stamps

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

109 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.

FAU_GEN.1 Audit data generation

110 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 7. Auditable Events].

111 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 7. Auditable Events].

Table 7. 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 pertaining to audit.	The identity of the authorized administrator performing the operation.
FMT_SMF.1	Use of the management	The identity of the authorized

Functional Component	Auditable Event	Additional Audit Record Contents
	functions	administrator performing the operation.

FAU_SAR.1 Audit review

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

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

FAU_STG.1 Protected audit trail storage

114 FAU_STG.1.1 - The TSF shall protect the stored audit records from unauthorized deletion.

115 FAU_STG.1.2 - The TSF shall be able to *prevent* unauthorized modifications to the audit records in the audit trail. [1]

FMT_MOF.1 Management of security functions behavior

116 FMT_MOF.1.1(1) - The TSF shall restrict the ability to *enable*, *disable* the functions:

a) [operation of the TOE; and

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

117 Application Note: By "Operation of the TOE" in a) above, we mean having the TOE start up (enable operation) and shut down (disable operation).

FMT_SMF.1 Specification of Management Functions

118 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) operation of the TOE; and

f) backup of audit trail data].

[1] **This wording of this requirement has been modified to reflect Common Criteria International Interpretation #141.**

5.1.1.2 SFRs With Strength of Function (SOF) Declarations

119 The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism. In the case of this security target, this minimum level shall be SOF-basic.

120 Specific strength of function metrics are defined for the following requirement:

121 FIA_UAU.2 - Strength of function shall be demonstrated for the password authentication mechanism to show that it meets SOF-basic, as defined in Part 1 of the CC.

5.2 Security Requirements for the IT Environment

122 The security functional requirements allocated to the IT Environment consist of the following components from Part 2 of the CC, summarized in Table 8. The SFRs are provided in their entirety in the subsequent paragraphs.

Table 8 Functional Components of the IT Environment

Functional Components	
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation

FPT_RVM.1 Non-Bypassability of the TSP

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

FPT_SEP.1 TSF Domain Separation

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

125 FPT_SEP.1.2 - The ~~TSF~~ **IT Environment** shall enforce separation between the security domains of subjects in the TSC.

5.3 TOE Security Assurance Requirements

The TOE claims compliance to EAL 2 level of assurance. The security assurance requirements (SARs) for this Security Target include the EAL 2 SARs in Part 3 of the CC. The EAL 2 SARs are identified in the following

Table 9. EAL2 Assurance **Components**:

Table 9. EAL2 Assurance Components

Assurance class	Assurance components
Class ACM: Configuration management	ACM_CAP.2 Configuration Items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery Procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1Administrator guidance
	AGD_USR.1 User guidance
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

5.3.1 Additional Security Assurance Requirements

126 This section describes one security assurance requirement from the CC Part 3 that the TOE must satisfy in addition to the previously listed EAL2 SARs.

127 In particular, ALC_FLR.2 for flaw reporting procedures that are designed to help ensure that reported defects in the TOE are addressed by the developer is added. ALC_FLR.2 is not included in any EAL. This additional SAR is restated verbatim from the CC.

Table 9 Additional SAR to Augment EAL2

Assurance class	Assurance components

Class ALC: Life cycle support	ALC_FLR.2 Flaw Reporting Procedures

5.3.1.1 ALC_FLR.2 Flaw Reporting Procedures

128 **Developer action elements:**

129 ALC_FLR.2.1D – The developer shall provide flaw remediation procedures addressed to TOE developers.

130 ALC_FLR.2.2D – The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

131 ALC_FLR.2.3D – The developer shall provide flaw remediation guidance addressed to TOE users.

132 **Content and presentation of evidence elements:**

133 ALC_FLR.2.1C – The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

134 ALC_FLR.2.2C – The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

135 ALC_FLR.2.3C – The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

136 ALC_FLR.2.4C – The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

137 ALC_FLR.2.5C – The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

138 ALC_FLR.2.6C – The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

139 ALC_FLR.2.7C – The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

140 ALC_FLR.2.8C – The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

141 **Evaluator action elements:**

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

6 TOE Summary Specification

143 This section presents a functional overview of the TOE, the security functions implemented by the TOE, and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

144 The TOE implements the following security functions:

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

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

6.1.1 Security Management [FMT]

146 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.

6.1.1.1 Using Admin Workstation [FMT_1]

147 Before an administrator may perform any management functions on a MWG they must establish a connection to MWG from a web browser on the administration workstation.

148 MWG maintains an authorized administrator role. MWG keeps a list which associates particular user identities with the 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)

6.1.1.2 MWG Administration [FMT_2]

149 A MWG administrator can manage all other administrative users of the system. 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)

6.1.1.3 URL Filter Policy Configuration [FMT_3]

150 The administrator manages the rules for filtering URL 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)

6.1.1.4 Anti-Malware Configuration [FMT_4]

151 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)

6.1.1.5 Certificate Checking Configuration [FMT_5]

152 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)

6.1.1.6 HTTPS Scanner Configuration [FMT_6]

153 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)

6.1.1.7 Initial Configuration [FMT_7]

154 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)

155

6.1.2 Identification and Authentication [FIA]

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

6.1.2.1 User Identification [FIA_1]

157 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.

158 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)

159 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.

6.1.2.2 Authentication [FIA_2]

160 MWG requires successful password authentication before allowing administrative user access. MWG consults its user policy storage to determine if the provided password matches the user's valid password. MWG supports reusable passwords with a minimum size of 8 characters. The permutational mechanism as applied in the evaluated configuration meets the standard of SOF-basic. A delay of 5 seconds is introduced following each unsuccessful login attempt. (FIA_UAU.2)

6.1.3 User Data Protection [SW_FDP]

161 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).

6.1.3.1 URL Filter [FDP_1]

162 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 trusted source database (that has organized URLs into predefined categories) in order to filter the HTTP traffic according to the rules. (FDP_IFC.1 (1), FDP_IFF.1 (1))

6.1.3.2 Anti-Malware Filter [FDP_2]

163 Anti-Malware filtering is turned on by an authorized MWG administrator. Following activation, MWG invokes specific Anti-Malware searches 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))

6.1.3.3 Certificate Checker [FDP_3]

164 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))

6.1.3.4 HTTPS Scanner [FDP_4]

165 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 (FIPS 140-2 certificate 918) for HTTPS encryption and decryption. (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)

6.1.4 Protection of Security Functions [FPT]

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

6.1.4.1 Time Stamps [FPT_1]

167 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.

168 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 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)

6.1.5 Audit [FAU]

169 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 users are allowed to review audit data.

6.1.5.1 Logging [FAU_1]

170 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)

171 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)

172 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).

6.1.5.2 Audit Reporting [FAU_2]

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

6.1.5.3 Audit Data Protection [FAU_3]

174 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. Unauthorized users can not delete audit data from the system. (FAU_STG.1)

6.2 Assurance Measures

175 This section identifies the Configuration Management, Delivery/Operation, Development, Guidance Documents, Life-cycle Support, Test, and Vulnerability Assessment measures applied by McAfee to satisfy CC assurance requirements.

176 The security assurance requirements for this Security Target include the requirements taken from Part 3 of the CC, augmented by, ALC_FLR.2. These assurance components are described in Section 5.3.

6.2.1 Configuration Management

177 The Configuration Management measures applied by McAfee include unique identification for configuration items, proper labeling, tracking of configuration items and tracking of security flaws. These configuration management measures are documented within the following McAfee documents:

- MWG Configuration Management Plan
  Assurance Requirements Satisfied: ACM_CAP.2

6.2.2 Delivery and Operation

178 McAfee provides measures to ensure that the TOE is delivered without modification and that it is installed, generated, and started in a way that will lead to the evaluated configuration. These delivery and operation measures are documented within the following McAfee documents:

- MWG Delivery Procedure
- MWG Installation and Configuration Guide
- Common Criteria Evaluated Configuration Guide (CCECG)

Assurance Requirements Satisfied: ADO_DEL.1 and ADO_IGS.1

6.2.3 Development

179 McAfee provides increasingly refined descriptions of the TOE security functionality starting with this Security Target. Design documentation consists of a functional specification and a high level design. In addition, there is a representation correspondence that maps the various representations of the TOE to one another and to this Security Target. This information is provided by the following McAfee documents:

- MWG Security Target
- MWG Functional Specification
- MWG High-Level Design
- MWG Security Functions Correspondence Analysis

Assurance Requirements Satisfied: ADV_FSP.1, ADV_HLD.1, and ADV_RCR.1.

6.2.4 Guidance

180 McAfee provides administrator guidance to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. The guidance includes warnings about functions and privileges that should be controlled in a secure processing environment. These guidance measures are documented within the following McAfee documents:

- MWG Administration Guide
- Common Criteria Evaluated Configuration Guide (CCECG)[2]

Assurance Requirements Satisfied: AGD_ADM.1 and AGD_USR.1

6.2.5 Life-cycle Support

181 McAfee provides information describing internal and user procedures to handle reports of TOE security flaws. This information is documented within the following McAfee documents:

- MWG Security Flaw Reporting Procedures[3]
- Common Criteria Evaluated Configuration Guide (CCECG)[4]

Assurance Requirements Satisfied: ALC_FLR.2

---

[2] **The CCECG provides administrative guidance for running Web Gateway in the configuration that was evaluated for Common Criteria.**

[3] **These are the internal developer procedures for fixing any flaws that might be reported.**

[4] **A section of this document provides the user guidance for reporting flaws.**

6.2.6 Test

182 McAfee performs extensive testing of MWG to ensure that it behaves as specified in the design documentation and in accordance with the security functional requirements specified in the ST. Test coverage analysis is performed to confirm that the testing is sufficiently extensive. These tests and analyses are presented in the following McAfee documents:

- MWG Test Plan/Coverage Analysis
- MWG Test Procedures and Results

Assurance Requirements Satisfied: ATE_COV.1, ATE_FUN.1, and ATE_IND.2

6.2.7 Vulnerability Assessment

183 In addition to the design and testing process, McAfee performs vulnerability assessment of the TOE. Strength of function analysis is performed on the administrator authentication mechanism in order to gain more confidence in the overall security functionality of the TOE. Finally, a systematic analysis of the TOE deliverables is performed to identify any flaws or weaknesses that could be exploited by an attack. These vulnerability assessment activities are documented within the following McAfee documents:

- MWG Strength of Function Analysis
- MWG Vulnerability Analysis

Assurance Requirements Satisfied: AVA_SOF.1, and AVA_VLA.1

7 PP Claims

184 The ST does not claim conformance with any PP.

8 Rationale

8.1 Rationale for TOE Security Objectives

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

186 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.

187 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.

188 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.

189 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.

190 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.

191 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 11. 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

8.2 Rationale for the TOE Operating Environment Security Objectives

192 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.

193 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.

194 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.

195 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 can not be bypassed as traffic flows between the networks.

196 OE.GUIDAN This non-IT security objective is necessary to counter the threat: TE.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.

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

198 OE.PROLIN The communication path between the TOE and the local administration workstation (browser) is physically protected. This objective ensures that a non-authorized user can not gain access to the TOE by connecting a rogue IT device to this communication line.

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

200 OE.BENIGN The Windows OS running on the local administration 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 12. Mapping Threats to TOE Operating Environment Security Objectives

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

201 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.

8.3 Rationale for TOE Security Requirements

202 The functional and assurance requirements presented in this ST are mutually supportive and their combination meet 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.

203 The rationale for the SOF is based on the low attack potential identified in this ST, augmented by the need to protect against more than casual attempted breaches of security. SOF-basic is therefore selected. The

security objectives imply the need for probabilistic or permutational security mechanisms.

FMT_SMR.1 Security roles

204 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

205 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 a 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

206 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

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

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

208 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)

209 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)

210 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)

211 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

212 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

213 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

214 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)

215 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)

216 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.

FPT_STM.1 Reliable time stamps

217 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

218 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

219 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

220 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 behavior (1)

221 This component was to ensure the TSF restricts the ability to modify the behavior 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

222 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.

Table 13. 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_AFL.1				**X**			
FIA_UAU.2	**X**						
FDP_IFC.1 (1)		**X**					
FDP_IFC.1 (2)		**X**					
FDP_IFC.1 (3)		**X**					

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN
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					
FMT_MSA.1		X	X				X
FMT_MSA.3		X	X				
FMT_MTD.1 (1)							X
FMT_MTD.1 (2)							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

8.4 Rationale for TOE IT Environment Security Requirements

FPT_RVM.1 Non-bypassability of the TSP

223 This component ensures that the TOE security policy enforcement functions can not be bypassed when data flows between the internal and external networks under its control. This component traces back to and aids in meeting the following objective: OE.SINGEN.

FPT_SEP.1 TSF Domain Separation

224 This component ensures that untrusted subjects cannot interfere with or tamper with the operation of the TSF. This component traces back to and aids in meeting the following objectives: OE.GUIDAN.

8.5 Rationale for Assurance Requirements

225 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.

8.6 SOF Rationale

226 The rationale for the chosen level of SOF-basic is related to the intended TOE environment. The low attack potential described in the TOE assumptions and the attack potential of the identified threat agents requires at least SOF-basic. The security objectives for the TOE imply probabilistic or permutational security mechanisms. The metrics defined are the minimal "industry" standard accepted for passwords.

8.7 Dependency Rationale

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

Table 14. SFR/SAR Dependency Evidence

SFR/SAR	Dependencies	Satisfied?
FMT_SMR.1	FIA_UID.1	Yes, FIA_UID.2
FIA_ATD.1	NONE	N/A
FIA_UID.2	NONE	N/A
FIA_UAU.2	FIA_UID.1	Yes, FIA_UID.2
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

SFR/SAR	Dependencies	Satisfied?
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_RVM.1	NONE	N/A
FPT_SEP.1	NONE	N/A
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
ACM_CAP.2	None	N/A
ADO_DEL.1	None	N/A
ADO_IGS.1	AGD_ADM.1	Yes
ADV_FSP.1	ADV_RCR.1	Yes
ADV_HLD.1	ADV_FSP.1 ADV_RCR.1	Yes Yes
ADV_RCR.1	NONE	N/A
AGD_ADM.1	ADV_FSP.1	Yes
AGD_USR.1	ADV_FSP.1	Yes
ALC_FLR.2	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.1 AGD_ADM.1 AGD_USR.1	Yes Yes Yes

SFR/SAR	Dependencies	Satisfied?
	ATE_FUN.1	Yes
AVA_SOF.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes
AVA_VLA.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes
	AGD_ADM.1	Yes
	AGD_USR.1	Yes

8.8 Internal Consistency and Mutually Supportive Rationale

228 The set of security requirements identified in this ST for MWG form a mutually supportive and internally consistent whole as evidenced by the following:

a) The choice of security requirements is justified as shown in Sections 8.3, 8.4, and 8.5. The choice of SFRs and SARs was made based on the assumptions and threats identified in Section 3 and the objectives identified in Section 4. Sections 8.1 and 8.2 of this ST provide evidence the security objectives counter threats to the TOE. Also, Section 8.2 demonstrates that the assumptions and objectives counter threats to the TOE operating environment.

d) The security functionality as described in the TOE Summary Specification satisfies the SFRs. All SFR dependencies have been met as shown in Section 8.7, Table 14.

e) The SOF claims are valid. The chosen SOF-basic level meets the attack potential identified in Section 3 of this ST. The identified metrics and SOF claim are commensurate with the EAL 2 level of assurance.

f) The SARs are appropriate for the assurance level of EAL 2 and are satisfied by MWG as demonstrated in Section 6.2 of this ST.

8.9 Rationale for Explicit Requirements

229 There are no explicit requirements.

8.10 Rationale for TOE Summary Specification

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

8.10.1 TOE Security Requirements

231 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 15. 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
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
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 behavior	FMT
FMT_SMF.1	Specification of Management Functions	FMT

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

Table 16. 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	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 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	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.
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 unauthorized deletion.

233 Because the security functions trace to SFRs, which were shown to be mutually supportive in Section 8.8, 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.

8.10.2 TOE Assurance Requirements

234 Table 17 is provided to demonstrate that each TOE SAR is adequately addressed by at least one assurance measure.

Table 17. Assurance Measure Suitability

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
ACM_CAP.2	MWG Configuration Management Plan	The Configuration Management Plan provides for unique identification of the TOE and all related configuration items.
ADO_DEL.1	MWG Delivery Procedure	This procedure describes mechanisms, which ensure that the TOE is delivered securely to customers.
ADO_DEL.1	Common Criteria Evaluated Configuration Guide (CCECG)	This document contains delivery procedures followed in the delivery of the TOE.
ADO_IGS.1	Quick Start McAfee Web Gateway, part number 700-2513A00	This document describes the procedures for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1	Common Criteria Evaluated Configuration Guide (CCECG)	This document supplements the installation procedures provided in the MWG Startup Guide.
ADV_FSP.1	MWG Functional Specification	This document describes the TSF and its external interfaces using an informal style.
ADV_HLD.1	MWG High-Level Design	The high-level design files describe the structure of the TSF in terms of subsystems and the functionality each provides. It also describes the interfaces to the subsystems.
ADV_RCR.1	MWG Security Functions Correspondence Analysis	This analysis document provides the correspondence between all adjacent pairs of TSF representations that are provided.
AGD_ADM.1	Product Guide McAfee Web Gateway version 7.0.1	These two documents provide guidance to those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. They include warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1	Common Criteria Evaluated Configuration Guide (CCECG)	This document supplements and supports the guidance provided in the MWG Installation and Configuration Guide.

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
AGD_USR.1	MWG Administration Guide	This document also suffices to cover user guidance. Only administrative users are allowed to directly control MWG.
ALC_FLR.2	MWG Security Flaw Reporting Procedures	This document defines the security flaw handling procedures to be followed by the developer.
ALC_FLR.2	Common Criteria Evaluated Configuration Guide (CCECG)	This document contains information on security flaw reporting procedures
ATE_COV.1	MWG Test Coverage Analysis	This document shows the correspondence between tests and the security functions.
ATE_FUN.1	MWG Test Plan, Procedures and Results	This functional test documentation includes test procedure descriptions, expected test results and actual test results.
AVA_SOF.1	MWG Strength of Function Analysis	Strength of function analysis is performed on the administrator authentication mechanism in order to gain more confidence in the overall security functionality of the TOE. The results of the analysis are documented.
AVA_VLA.1	MWG Vulnerability Analysis	An analysis of the TOE deliverables is performed to identify any flaws or weaknesses that could be exploited by an attack. The analysis results are documented.