SECURITY TARGET

FOR

FORTIMAIL™ V3.0 MR5 SECURE MESSAGING PLATFORM

Document No. ST0004

Version: 1.3, 9 December 2009

Prepared for:

Fortinet, Incorporated

326 Moodie Drive

Ottawa, Ontario

Canada, K2H 8G3

Prepared by:

Electronic Warfare Associates-Canada, Ltd.

55 Metcalfe St., Suite 1600

Ottawa, Ontario

K1P 6L5

SECURITY TARGET

FOR

FORTIMAIL™ V3.0 MR5 SECURE MESSAGING PLATFORM

Document No. ST0004

Version: 1.3, 9 December 2009

<Original> Approved by:

Project Engineer:	S. Jackson	9 December 2009
Project Manager:	G. Gibbs	9 December 2009
Program Director:	E. Connor	9 December 2009
	(Signature)	(Date)

TABLE OF CONTENTS

1 INTRODUCTION 1
1.1 DOCUMENT ORGANIZATION 1
1.2 SECURITY TARGET REFERENCE 1
1.3 TARGET OF EVALUATION REFERENCE 1
1.4 FORTIMAIL™ V3.0 MR5 SECURE MESSAGING PLATFORM OVERVIEW 2
1.5 TARGET OF EVALUATION DESCRIPTION 3
1.5.1 Physical Scope 3
1.5.1.1 Physical Configuration 3
1.5.1.2 Physical Interfaces 3
1.5.1.3 TOE Boundary - Single-Unit Configuration 4
1.5.1.4 TOE Boundary - High-Availability Configuration 5
1.5.2 Logical Scope 6
1.5.2.1 Logical Interfaces 6
1.5.2.2 Functions Included in the TOE 7
1.5.3 Security Functional Policies 9

2 CONFORMANCE CLAIMS 11

3 SECURITY PROBLEM DEFINITION 12
3.1 THREATS 12
3.2 ORGANIZATIONAL SECURITY POLICIES 13
3.3 ASSUMPTIONS 14

4 SECURITY OBJECTIVES 15
4.1 SECURITY OBJECTIVES FOR THE TOE 15
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 17
4.3 SECURITY OBJECTIVES RATIONALE 18
4.3.1 T.ADMIN_ERROR 21
4.3.2 T.ADMIN_ROGUE 21
4.3.3 T.AUDIT_COMPROMISE 21
4.3.4 T.FLAWED_DESIGN 22
4.3.5 T.FLAWED_IMPLEMENTATION 22
4.3.6 T.IMPROPER_CONFIGURATION 23
4.3.7 T.INFLUX 23

4.3.8 T.LOSSOF 23
4.3.9 T.MALICIOUS_ACTIVITY 23
4.3.10 T.MISUSE 23
4.3.11 T.NOHALT 24
4.3.12 T.POOR_TEST 24
4.3.13 T.PRIVILEGE 24
4.3.14 T.UNATTENDED_SESSION 24
4.3.15 T.UNAUTHORIZED_ACCESS 24
4.3.16 T.VIRUS 25
4.3.17 P.ACCESS 25
4.3.18 P.ACCOUNTABILITY 25
4.3.19 P.ADMIN_ACCESS 26
4.3.20 P.DETECT 26
4.3.21 P.INTEGRITY 26
4.3.22 P.MANAGE 26
4.3.23 P.PROTECT 26
4.3.24 P.VULNERABILITY_ANALYSIS_TEST 26
4.3.25 A.LOCATE 27
4.3.26 A.MANAGE 27
4.3.27 A.NOEVIL 27
4.3.28 A.PHYSICAL 27
4.3.29 A.PROTECT 27
4.4 SECURITY REQUIREMENTS RATIONALE 28
4.4.1 O.ACCESS 33
4.4.2 O.ADMIN_ROLE 33
4.4.3 O.AUDIT_GENERATION 33
4.4.4 O.AUDIT_PROTECTION 33
4.4.5 O.AUDIT_REVIEW 33
4.4.6 O.AUDITS 33
4.4.7 O.CHANGE_MANAGEMENT 33
4.4.8 O.EFFECTIVE_ADMIN 33
4.4.9 O.INTEGRITY 33
4.4.10 O.MAIL 33

4.4.11 O.MANAGE 34
4.4.12 O.OVERFLOWS 34
4.4.13 O.PROTECT 34
4.4.14 O.ROBUST_ADMIN_GUIDANCE 34
4.4.15 O.ROBUST_TOE_ACCESS 34
4.4.16 O.SECURE_UPDATES 34
4.4.17 O.SELF_PROTECTION 34
4.4.18 O.SOUND_DESIGN 35
4.4.19 O.SOUND_IMPLEMENTATION 35
4.4.20 O.THOROUGH_FUNCTIONAL_TESTING 35
4.4.21 O.TIME_STAMPS 35
4.4.22 O.TRUSTED_CHANNEL 35
4.4.23 O.TRUSTED_PATH 35
4.4.24 O.VIRUS 35
4.4.25 O.VULNERABILITY_ANALYSIS_TEST 35
4.5 DEPENDENCY RATIONALE 35

5 EXTENDED COMPONENTS DEFINITION 38
5.1 CLASS FSV: ANTISPAM AND ANTIVIRUS UPDATES 38
5.1.1 Antispam and Antivirus Updates (FSV_UPD_EXP) 38
5.1.1.1 Family Behaviour 38
5.1.1.2 Component levelling 38
5.1.1.3 Management 38
5.1.1.4 Audit 38
5.1.1.5 FSV_UPD_EXP.1 (Antispam and antivirus updates) 38

6 SECURITY REQUIREMENTS 38
6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 39
6.1.1 Security Audit (FAU) 41
6.1.1.1 FAU_ARP.1(1) Security Alarms (antispam) 41
6.1.1.2 FAU_ARP.1(2) Security Alarms (antivirus) 41
6.1.1.3 FAU_ARP.1(3) Security Alarms (content filtering) 41
6.1.1.4 FAU_ARP.1(4) Security Alarms (other events) 41
6.1.1.5 FAU_GEN.1 Audit data generation 42

6.1.1.6 FAU_GEN.2 User identity association 46
6.1.1.7 FAU_SAA.1(1) Potential violation analysis (antispam)..... 46
6.1.1.8 FAU_SAA.1(2) Potential violation analysis (antivirus) 46
6.1.1.9 FAU_SAA.1(3) Potential violation analysis (content filtering)..... 46
6.1.1.10 FAU_SAA.1(4) Potential violation analysis (other events) 47
6.1.1.11 FAU_SAR.1 Audit review..... 47
6.1.1.12 FAU_SAR.3 Selectable audit review 47
6.1.1.13 FAU_SEL.1 Selective audit..... 47
6.1.1.14 FAU_STG.1 Protected audit trail storage..... 48
6.1.1.15 FAU_STG.4 Prevention of audit data loss 48
6.1.2 Cryptographic Support (FCS)..... 48
6.1.2.1 FCS_CKM.1 Cryptographic key generation..... 48
6.1.2.2 FCS_CKM.4(1) Cryptographic key Destruction (Keys and CSPs) 48
6.1.2.3 FCS_CKM.4(2) Cryptographic key Destruction (RNG Seed Key)..... 48
6.1.3 FCS_COP.1 Cryptographic operation 49
6.1.4 User Data Protection (FDP)..... 49
6.1.4.1 FDP_ETC.2 Export of user data with security attributes..... 49
6.1.4.2 FDP_IFC.1(1) Subset information flow control (unauthenticated information flow) 50
6.1.4.3 FDP_IFC.1(2) Subset information flow control (authenticated information flow) 50
6.1.4.4 FDP_IFC.1(3) Subset information flow control (unauthenticated TOE services) 50
6.1.4.5 FDP_IFC.1(4) Subset information flow control (authenticated TOE services).... 50
6.1.4.6 FDP_IFF.1(1) Simple security attributes (unauthenticated information flow policy) 51
6.1.4.7 FDP_IFF.1(2) Simple security attributes (authenticated information flow policy) 51
6.1.4.8 FDP_IFF.1(3) Simple security attributes (unauthenticated TOE services policy). 52
6.1.4.9 FDP_IFF.1(4) Simple security attributes (authenticated TOE services policy)..... 52
6.1.5 Identification and Authentication (FIA)..... 53
6.1.5.1 FIA_UAU.1(1) Timing of authentication (SMTP/SMTPS traffic)..... 53
6.1.5.2 FIA_UAU.1(2) Timing of authentication (for TOE services) 53
6.1.5.3 FIA_UAU.2(1) User authentication before any action (SMTP/SMTPS traffic) ... 54
6.1.5.4 FIA_UAU.2(2) User authentication before any action (administrators)..... 54

6.1.5.5 FIA_UAU.2(3) User authentication before any action (end users) 54
6.1.5.6 FIA_UID.2(1) User identification before any action (SMTP/SMTPS traffic) 54
6.1.5.7 FIA_UID.2(2) User identification before any action (administrators) 54
6.1.5.8 FIA_UID.2(3) User identification before any action (end users[1]) 54
6.1.6 Security Management (FMT) 54
6.1.6.1 FMT_MOF.1(1) Management of security functions behaviour (FAU_SAR, FAU_SEL, FAU_STG, FRU_RSA) 54
6.1.6.2 FMT_MOF.1(2) Management of security functions behaviour (FTA_SSL) 54
6.1.6.3 FMT_MOF.1(3) Management of security functions behaviour (antispam, antivirus, content filtering) 54
6.1.6.4 FMT_MOF.1(4) Management of security functions behaviour (antispam and antivirus updates) 55
6.1.6.5 FMT_MOF.1(5) Management of security functions behaviour (administrator reports) 55
6.1.6.6 FMT_MSA.1 Management of security attributes 55
6.1.6.7 FMT_MSA.3 Static attribute initialisation 55
6.1.6.8 FMT_MTD.1(1) Management of TSF data (default administrator) 55
6.1.6.9 FMT_MTD.1(2) Management of TSF data (read and write administrator) 56
6.1.6.10 FMT_MTD.1(3) Management of TSF data (read only administrator) 57
6.1.6.11 FMT_SMR.1 Security roles 57
6.1.7 Protection of the TSF (FPT) 57
6.1.7.1 FPT_FLS.1 Failure with preservation of secure state 57
6.1.7.2 FPT_ITT.1 Basic internal TSF data transfer protection 57
6.1.7.3 FPT_STM.1 Reliable time stamps 57
6.1.8 Fault Tolerance (FRU) 58
6.1.8.1 FRU_FLT.1 Degraded fault tolerance 58
6.1.8.2 FRU_RSA.1 Maximum quotas 58
6.1.9 Antivirus Updates (FSV) 58
6.1.9.1 FSV_UPD_EXP.1 Antispam and Antivirus Updates 58
6.1.10 TOE Access (FTA) 58
6.1.10.1 FTA_SSL.3 TSF-initiated termination 58
6.1.11 Trusted Path/Channels (TRP) 58
6.1.11.1 FTP_ITC.1 Inter-TSF trusted channel 58
6.1.11.2 FTP_TRP.1 Trusted Path 59

6.2 TOE SECURITY ASSURANCE REQUIREMENTS 59

7 TOE SUMMARY SPECIFICATION 60
7.1 TOE SECURITY FUNCTIONS 60
7.1.1 F.Audit 60
7.1.2 F.Authentication 61
7.1.3 F.InformationFlow 62
7.1.4 F.Protection 63
7.1.5 F.SecurityManagement 64

8 CONVENTIONS AND TERMINOLOGY 67
8.1 CONVENTIONS 67
8.2 TERMINOLOGY AND ACRONYMS 68
8.2.1 Terminology 68
8.2.2 Acronyms 71

LIST OF FIGURES

Figure 1 – Single Unit FortiMail Configuration 4
Figure 2 – FortiMail High Availability Configuration (Active-passive Mode) 5

LIST OF TABLES

Table 1 - TOE Identification Details 1
Table 2 - FortiMail Interfaces 3
Table 3 - FortiMail Logical Interfaces 7
Table 4 - FortiMail Features 9
Table 5- Mapping Between SFPs and SFRs 11
Table 6 - Mapping Between Objectives, Threats, Policies, and Assumptions 20
Table 7 - Mapping of SFRs to Security Objectives and Assurance Requirements 32
Table 8 - Functional Requirement Dependencies 37
Table 9 - Summary of Security Functional Requirements 41
Table 10 - Auditable Events 45
Table 11 - Cryptographic Key Generation 48
Table 12- Cryptographic Operation 49
Table 13 - Default Administrator Management of TSF Data 56
Table 14 - Read and Write Administrator Management of TSF Data 56
Table 15 - Read Only Administrator Management of TSF Data 57
Table 16 - EAL 2 Assurance Requirements 60
Table 17- Mapping of Security Functions to SFRs 67

1 INTRODUCTION

1.1 DOCUMENT ORGANIZATION

Section 1, Introduction, provides the Security Target (ST) reference, the Target of Evaluation (TOE) reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, **Security Problem Definition**, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition

Section 5, Extended Components Definition, defines the extended components defined in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.

Section 7, TOE Summary Specification, describes the security functions and assurance measures that are included in the TOE to enable it to meet the IT security functional and assurance requirements.

Section 8, Conventions and Terminology, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

This document, version 1.3, dated 9 December 2009, is the Security Target for the FortiMail™ v3.0 MR5 Secure Messaging Platform.

1.3 TARGET OF EVALUATION REFERENCE

The Target of Evaluation for this Security Target is identified in Table 1.

Product	Firmware Version	Hardware ID
FortiMail	v3.0 MR5 build number 529	see Table 2

Table 1 - TOE Identification Details

1.4 FORTIMAIL™ V3.0 MR5 SECURE MESSAGING PLATFORM OVERVIEW

FortiMail is a specialized email security system that provides multi-layered protection against blended threats comprised of spam, viruses, worms and spyware. The FortiMail system relies on a customized operating system that cleans emails through corresponding FortiMail antispam and antivirus. Email content policies must be enforced and good email must be archived for compliance purposes. Unique to inbound risks, are DHA (Directory Harvest Attacks) and DOS (Denial of Service) attacks, which must be part of a multi-layered email security strategy. For outbound risks an email security solution must ensure that infected zombie PCs that relay spam do not lead to a legitimate enterprise network becoming added to a Real-Time Black List (RBL). To ensure up to date email protection, FortiMail relies on Fortinet FortiGuard™ antispam and antivirus security subscription services.

Administration of the system may be performed locally through the Command Line Interface (CLI) using an administrator console or remotely via a network management station through the FortiMail Web-based manager or the CLI through an SSH connection. Access to the FortiMail administrative functions including audit data is restricted to authenticated Administrators.

FortiMail supports two high availability modes. Config-only mode provides load balancing and allows up to 25 FortiMail units to share a common configuration, but operate as separate FortiMail units. In Active-passive mode a second (passive) FortiMail unit can be configured as a failover device if the primary (active) FortiMail unit fails. All data from the active unit, except for the Bayesian database, is duplicated to the passive unit. Both modes are within the scope of this evaluation.

FortiMail supports three modes of operation: gateway mode, transparent mode and server mode. Gateway mode and transparent mode are within the scope of this evaluation. In gateway mode the FortiMail unit provides antivirus, antispam, content filtering, email routing and email archiving functionality with only minor changes to existing networks. When operating in gateway mode, all of the unit's interfaces are on different IP subnets and the FortiMail acts as a router for SMTP/SMTPS traffic only. FortiMail transparent mode allows the unit to be placed into an existing network without making any changes. When operating in transparent mode, all of the unit's interfaces are on the same IP subnet and the FortiMail unit effectively acts as a bridge.

The FortiMail supports local authentication and authentication using IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS servers. Administrators are authenticated locally. End users are authenticated using remote servers. FortiMail also supports TLS for encryption of the tunnel between the sending MTA/client and the receiving mail server. FortiMail is being validated to FIPS 140-2.

1.5 TARGET OF EVALUATION DESCRIPTION

1.5.1 Physical Scope

1.5.1.1 Physical Configuration

The FortiMail unit is a stand-alone appliance that does not require supporting hardware. The FortiMail unit consists of custom hardware and firmware, including the following major components: firmware, processor, memory, disk storage and I/O interfaces. The firmware is being validated to FIPS 140-2.

1.5.1.2 Physical Interfaces

The FortiMail unit has the interfaces defined in Table 2.

Product	Interfaces				Total Hard Drive Capacity	Hardware ID
	Ethernet Interfaces		Administrator Interfaces			
	No.	Speed	Local Console	Network		
FortiMail-100	4	4 x 10/100 Ethernet (RJ-45)	RS232/DB-9	Yes	250 GB	C4TQ29
FortiMail-400	4	2 x 10/100/1000 and 2 2 x 10/100 Ethernet (RJ-45)	RS232/RJ-45	Yes	500 GB	C4PW86
FortiMail-400B	4	10/100/1000 Ethernet (RJ-45)	RS232/RJ-45	Yes	2 x 500GB drives	C4AH53
FortiMail-2000A	4	10/100/1000 Ethernet (RJ-45)	RS232/DB-9	Yes	Up to 6 x 250GB or 400GB drives	C2FE89
FortiMail-4000A	4	10/100/1000 Ethernet (RJ-45)	RS232/DB-9	Yes	Up to 12 x 250GB or 400GB drives	C4FE37

Table 2 - FortiMail Interfaces

The FortiMail units may be securely administered over the external or internal networks or locally within the secure area. The FortiMail unit provides the following administration options:

- The FortiMail unit has a dedicated console RS232 port with RJ-45 connector. When connected to a terminal which supports VT100 emulation, the console port allows access to the FortiMail unit via the CLI. This Local Console CLI permits an authenticated Administrator to configure the FortiMail unit, monitor its operation and examine the audit logs that are created.

- Remote administration may be performed via any network port that has been configured by an Administrator to allow HTTPS (for the Network Web-Based GUI) and SSH (for the Network CLI) traffic. When connected to a Network Management Station, this port provides remote access to the Network CLI or to the Network Web-Based GUI and allows an authenticated Administrator to configure the FortiMail unit, monitor its operation and examine the audit logs that are created; and

- The Administrator may configure automatic antivirus updates from the FortiGuard Distribution Server.

The FortiMail units are designed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

1.5.1.3 TOE Boundary - Single-Unit Configuration

In the Single-Unit configuration, the TOE consists of a single FortiMail. Figure 1 – Single Unit FortiMail Configuration shows an example of a single FortiMail unit, in gateway mode, routing SMTP/SMTPS traffic between networks. One of the networks provides access to the FortiGuard Distribution Server, which permits antivirus updates to be downloaded.

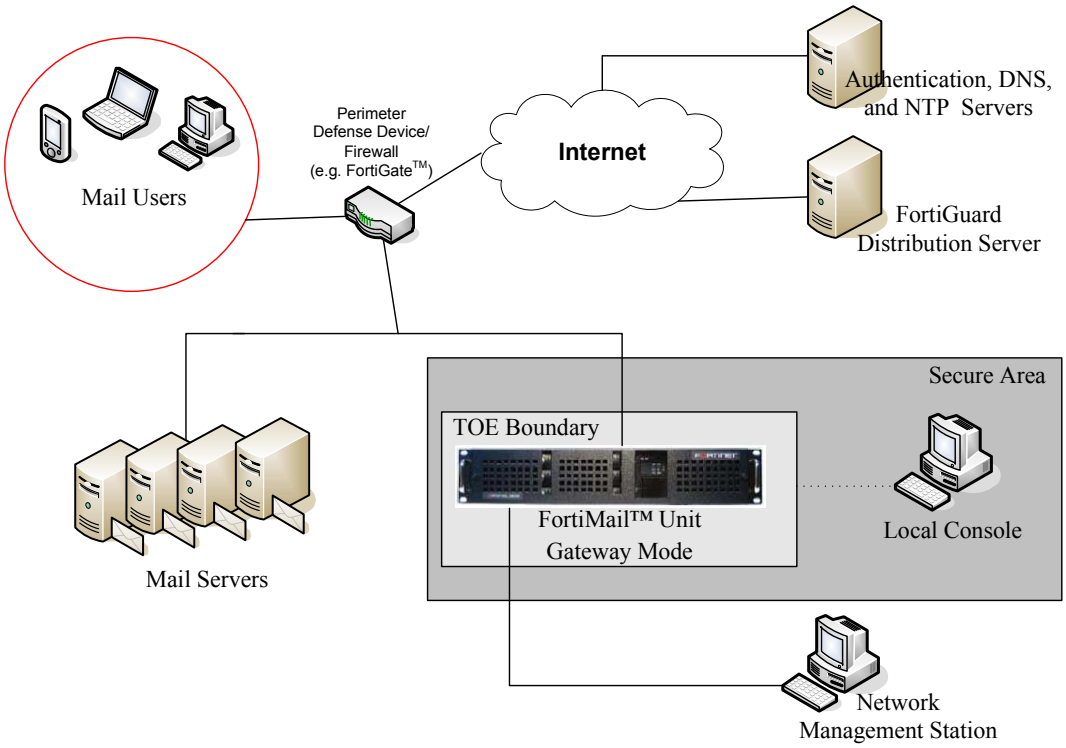

Figure 1 – Single Unit FortiMail Configuration

The Local Console, located within a Secure Area, is a terminal or general purpose computer with a standard serial interface and optional ethernet interfaces. A serial port is required to administer the TOE via the Local Console CLI.

The Network Management Station is a terminal or general purpose computer with a standard network interface which is used to remotely administer the TOE using the Network Web-Based GUI or Network CLI.

1.5.1.4 TOE Boundary - High-Availability Configuration

In the Active-passive High-Availability (HA) configuration, the TOE consists of a two FortiMail units interconnected to form a FortiMail HA group. A FortiMail Active-passive HA group consists of two FortiMail units, one functioning as a primary unit (also called the master) and the other as a backup unit (also called the slave). All FortiMail units in an HA group must be the same FortiMail model and must be running the same firmware build. The primary and backup units are configured separately and then joined together to form the FortiMail HA group. Figure 2 shows an example of FortiMail units in an HA group for Active-passive mode.

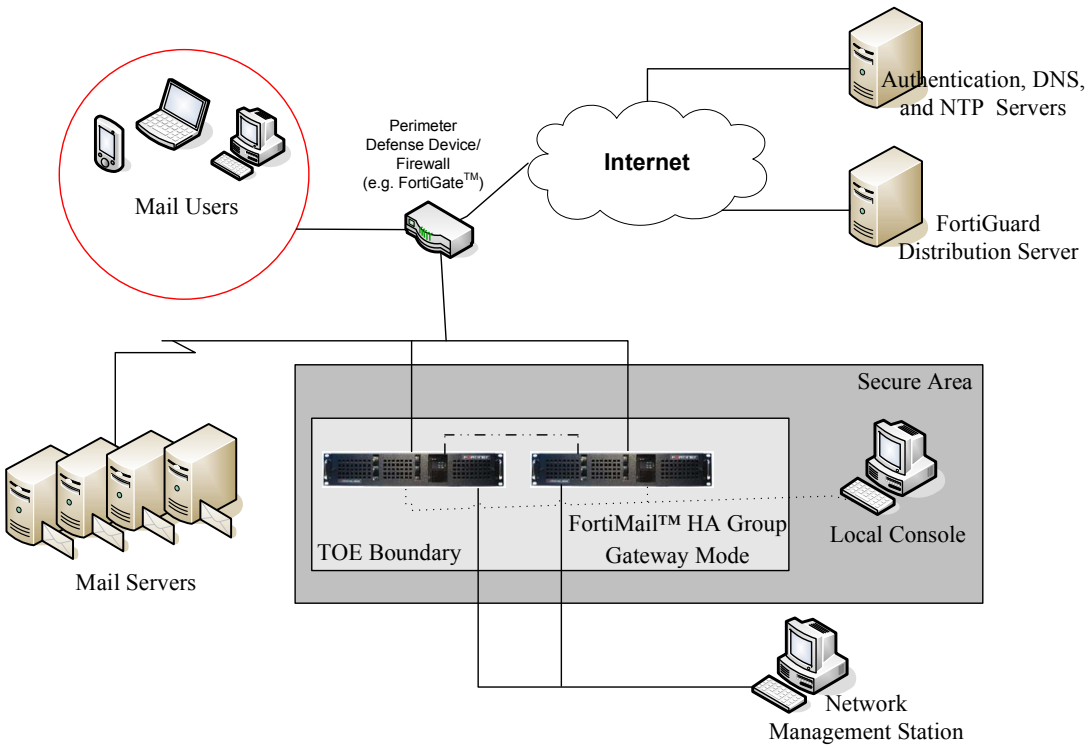

Figure 2 – FortiMail High Availability Configuration (Active-passive Mode)

In the Config-only HA configuration up to 25 FortiMail units can be configured to share the same configuration but operate independently. All FortiMail units in the group have the same configuration except for network settings and the FortiMail unit host name and SMTP/SMTPS system information.

The Local Console, located within a Secure Area, is a terminal or general purpose computer with a standard serial interface and optional ethernet interfaces. A serial port is required to administer the TOE via the Local Console CLI.

The Network Management Station is a terminal or general purpose computer with a standard network interface to remotely administer the TOE using the Network Web-Based GUI or Network CLI.

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary.

1.5.2.1 Logical Interfaces

Table 3 - FortiMail Logical Interfaces describes each of the interfaces that are included in the TOE in terms of the external entity to which it connects, the interface data that is transferred, the purpose of the interface and the protocol used for the transfer.

External Entity	Interface Data	Interface Purpose	Protocol(s)
Authentication - IMAP	Authentication Data	Authenticate users	IMAP/IMAPS
Authentication - LDAP	Authentication Data	Authenticate users	LDAP/LDAPS
Authentication - POP3	Authentication Data	Authenticate users	POP3/POP3S
Authentication - RADIUS	Authentication Data	Authenticate users	RADIUS
Authentication - SMTP	Authentication Data	Authenticate users	SMTP/SMTPS
FortiMail HA Group	HA Data	Exchange data to configure and synchronize the FortiMail that form a HA group.	TCP/IP (proprietary)
Fortinet's FortiGuard Distribution Server	Antispam and Antivirus Updates	Provided that the customer has subscribed to the service, Fortinet provides antispam and antivirus updates from Fortinet to the FortiMail unit.	proprietary protocol over SSL

External Entity	Interface Data	Interface Purpose	Protocol(s)
Local Console	Administration Data	Allow local administration using the CLI command interface	Serial
Mail Servers	Email	Send and receive email to/from mail servers.	SMTP/SMTPS
Mail Users	Email Data	Send and receive user email to/from the Network Users.	SMTP/SMTPS
Mail Users	Webmail	Retrieve the quarantined messages.	HTTP/HTTPS, IMAP/IMAPS, POP3/POP3S
Network Management Station	Administration Data	Allow remote administration using the CLI command interface	SSH
Network Management Station	Administration Data	Allow administration using the Web-Based GUI.	HTTPS
NTP Server	Time	Update time from NTP server	NTP

Table 3 - FortiMail Logical Interfaces

1.5.2.2 Functions Included in the TOE

Table 4 summarizes the FortiMail features that are included in the TOE.

Feature	Description
Access Control	The FortiMail provides a role-based access control capability to ensure that only authorized administrators are able to administer the FortiMail unit.
Administration (Local Console CLI)	The FortiMail provides management capabilities via a text-based Local Console CLI.
Administration (Network CLI)	The FortiMail provides management capabilities via a text-based Network CLI interface.
Administration (Network Web-Based GUI)	The FortiMail provides a Network Web-Based GUI, accessed via HTTPS, for system management and configuration.
Alert Email	Alert Email enables the FortiMail unit to monitor logs for specific log messages, and notifies you by email when they appear.

Feature	Description
Antispam, Antivirus	The FortiMail provides antispam and antivirus protection for email (Simple Mail Transfer Protocol (SMTP/SMTPS)) content as it passes through the FortiMail unit. Antivirus protection also includes protection from spyware and worms.
Archiving	The FortiMail provides the ability to archive email.
Audit Reporting	The TOE can collate information collected from its log files and present the information in tabular and graphical reports and email to an administrator.
Authentication - Administrator	For administration, the TOE supports local authentication using a username and password mechanism.
Authentication - SMTP/SMTPS Traffic	For SMTP/SMTPS traffic, the TOE supports authentication via IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, and SMTP/SMTPS servers.
Authentication - Users	For users accessing quarantine email, the TOE supports authentication via IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, and SMTP/SMTPS servers.
Backup/Restore	The TOE provides for configuration backup and restore.
Content Filtering	The FortiMail provides content filtering for email (Simple Mail Transfer Protocol (SMTP/SMTPS), Post-Office Protocol Version 3 (POP3/POP3S), and Internet Message Access Protocol (IMAP/IMAPS) content as it passes through the FortiMail unit.
DHA	The TOE protects against directory harvest attacks (DHA) by providing the ability to discard email messages based on the sender's reputation.
DOS	The TOE protects against denial of service by providing the ability to limit resource utilization.
Email routing	In Transparent mode, the FortiMail unit uses proxy servers to pick up, scan, and relay the emails not destined to the FortiMail unit.
FortiGuard Distribution Server	The TOE provides for updates to the antispam and antivirus signatures from the FortiGuard Distribution Server.
High Availability (FortiMail group)	The FortiMail provides a high availability capability. Both Config-only HA (load balancing) and Active-passive HA (failover protection) between two or more identical units are supported.
ICMP	The FortiMail responds to Internet Control Message Protocol (ICMP) pings, to verify installations and for testing, without requiring that the user be authenticated.
Logging (recording)	Logging is performed and data written to hard disk.

Feature	Description
Profiles / Policies	Profiles / Policies are used configure antispam, antivirus, authentication, content, and other settings to filter email and email attachments and to control email account settings
Quarantine	The FortiMail provides the capability of quarantining email.
Time	The FortiMail maintains internal time on a system clock, settable by the Administrator, or updated via NTP. This clock is used when time stamps are generated.
Webmail	End users use Webmail to access quarantined or archived email in both gateway and transparent modes.

Table 4 - FortiMail Features

1.5.3 Security Functional Policies

The TOE enforces information flow control and TOE services security functional policies (SFPs) that control access to TOE functionality and resources. The SFPs are as follows:

- UNAUTHENTICATED INFORMATION FLOW SFP;
- AUTHENTICATED INFORMATION FLOW SFP;
- UNAUTHENTICATED TOE SERVICES SFP; and
- AUTHENTICATED TOE SERVICES SFP.

The UNAUTHENTICATED INFORMATION FLOW SFP addresses the TOE's routing of email between a client and an email server under the TOE's ownership. This SFP may be disabled by the administrator whereby email routing is controlled by the AUTHENTICATED INFORMATION FLOW SFP. The subjects under control of this policy are the TOE interfaces that connect to unauthenticated users on an internal or external network sending information through the TOE to other destinations on the internal or external network. The information flowing between subjects in the policy is traffic with attributes, defined in FDP_IFF.1.1(1), including source and destination addresses. The rules that define the SFP are found in FDP_IFF.1.2(1). FMT_MSA.3 requires that these rules be assigned restrictive initial values. FMT_MSA.1 ensures that the rules are subsequently managed only by the administrator. Information is allowed to flow without authentication by FIA_UAU.1(1).

The AUTHENTICATED INFORMATION FLOW SFP addresses the TOE's routing of email between an authenticated client and an email server under the TOE's ownership. Authentication is via an IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS server as described in FIA_UAU.2(1) and FIA_UID.2(1). The information flowing between subjects in the policy is traffic with attributes, defined in FDP_IFF.1.1(2), including source and destination addresses. The rules that define the SFP are found in FDP_IFF.1.2(2). FMT_MSA.3 requires that these rules be assigned

restrictive initial values. FMT_MSA.1 ensures that the rules are subsequently managed only by the administrator.

The UNAUTHENTICATED TOE SERVICES SFP addresses the TOE's response to ping requests. The subjects under control of this policy are the TOE interfaces that connect unauthenticated users on an internal or external network sending information to or receiving information from the TOE. The information flowing between subjects in the policy is traffic with attributes, defined in FDP_IFF.1.1(3), including source and destination addresses. The rules that define the SFP are found in FDP_IFF.1.2(3). FMT_MSA.3 requires that these rules be assigned restrictive initial values. FMT_MSA.1 ensures that the rules are subsequently managed only by the administrator. Ping requests are allowed by FIA_UAU.1(2).

The AUTHENTICATED TOE SERVICES SFP addresses user access to quarantine email via Webmail (HTTP/HTTPS), POP3/POP3S or IMAP/IMAPS with credentials stored on an IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS server. User authentication is addressed by FIA_UAU.2(3) and FIA_UID.2(3). The information flowing between subjects in the policy is traffic with attributes, defined in FDP_IFF.1.1(4), including source and destination addresses. The rules that define the SFP are found in FDP_IFF.1.2(4). FMT_MSA.3 requires that these rules be assigned restrictive initial values. FMT_MSA.1 ensures that the rules are subsequently managed only by the administrator.

A mapping between the SFPs and the authentication, identification, and information flow SFRs is provided in the following table.

SFP	**SFR Identifier**	**SFR Name**
AUTHENTICATED INFORMATION FLOW SFP	FDP_IFC.1(2)	Subset information flow control (authenticated information flow)
	FDP_IFF.1(2)	Simple security attributes (authenticated information flow)
	FIA_UAU.2(1)	User authentication before any action (SMTP/SMTPS traffic)
	FIA_UID.2(1)	User identification before any action (SMTP/SMTPS traffic)
AUTHENTICATED TOE SERVICES SFP	FDP_IFC.1(4)	Subset information flow control (authenticated TOE services)
	FDP_IFF.1(4)	Simple security attributes (authenticated TOE services)

	FIA_UAU.2(3)	User authentication before any action (end users)
	FIA_UID.2(3)	User identification before any action (end users)
UNAUTHENTICATED INFORMATION FLOW SFP	FDP_IFC.1(1)	Subset information flow control (unauthenticated information flow)
	FDP_IFF.1(1)	Simple security attributes (unauthenticated information flow)
	FIA_UAU.1(1)	Timing of authentication (SMTP/SMTPS traffic)
UNAUTHENTICATED TOE SERVICES SFP	FDP_IFC.1(3)	Subset information flow control (unauthenticated TOE services)
	FDP_IFF.1(3)	Simple security attributes (unauthenticated TOE services)
	FIA_UAU.1(2)	Timing of authentication (for TOE services)

Table 5- Mapping Between SFPs and SFRs

2 CONFORMANCE CLAIMS

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, CCMB-2006-09-001 September 2006 Revision 1, CCMB-2007-09-002 September 2007 Revision 2 and CCMB-2007-09-003 September 2007 Revision 2.

The Target of Evaluation (TOE) for this ST is conformant with the functional requirements specified in Part 2 as well as two explicitly-defined functional requirements. The Target of Evaluation (TOE) for this ST, the FortiMail™ v3.0 MR5 Secure Messaging Platform, is therefore conformant with CC Part 2 extended.

The TOE for this ST is conformant to the CC Part 3 assurance requirements for EAL 2, augmented with ALC_FLR.1 Basic flaw remediation.

The TOE for this ST does not claim conformance with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

The threats discussed below are addressed by the TOE. The threat agents are either authorized TOE users, unauthorized persons, or external IT entities not authorized to use the TOE itself. The threat agents are assumed to have a low attack potential and are assumed to have a moderate level of resources and access to all publicly available information about the TOE and potential methods of attacking the TOE. It is expected that the FortiMail units will be protected to the extent necessary to ensure that they remain connected to the networks they protect.

T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
T.ADMIN_ROGUE	An administrator's intentions may become malicious resulting in user or TOE Security Function (TSF) data being compromised.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.FLAWED_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.
T.FLAWED_IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.
T.IMPROPER_CONFIGURATION	The TOE may be susceptible to improper configuration by any user, causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected by the TOE.
T.MALICIOUS_ACTIVITY	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System which may result in the TOE being affected by unauthorised users.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System which may result in the TOE being affected by unauthorised users.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE's functionality by halting execution of the TOE.
T.POOR_TEST	The developer may not produce sufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) resulting in the TOE being affected by unauthorized users due to incorrect TOE behaviour being undiscovered thereby causing potential security vulnerabilities.
T.PRIVILEGE	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
T.VIRUS	A malicious agent may attempt to pass a virus through or to the TOE.

3.2 ORGANIZATIONAL SECURITY POLICIES

The TOE must address the organizational security policies described below.

P.ACCESS	All data collected by the TOE shall only be used for authorized purposes.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.DETECT	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.INTEGRITY	Data collected by the TOE shall be protected from modification.
P.MANAGE	The TOE shall be manageable only by authorized users.
P.PROTECT	The TOE shall be protected from unauthorized accesses and disruptions of activities.
P.VULNERABILITY_ANALYSIS_TEST	The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a low attack potential.

3.3 ASSUMPTIONS

The specific conditions below are assumed to exist in the TOE environment.

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means). The mapping of security objectives to assumptions, threats and organizational security policies along with the rationale for this mapping is found in Section 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

This section defines the security objectives that are to be addressed by the TOE and its environment.

O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ADMIN_ROLE	The TOE will provide administrator roles to isolate administrative actions, and to make the administrative functions available locally and remotely.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions.
O.CHANGE_MANAGEMENT	The configuration of, and all changes to, the TOE and its development evidence will be analyzed, tracked, and controlled throughout the TOE's development.

O.EFFECTIVE_ADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.INTEGRITY	The TOE must ensure the integrity of all audit data.
O.MAIL	The TOE must handle email traffic providing the necessary filtering.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.OVERFLOWS	The TOE must appropriately handle potential audit data storage overflows.
O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.ROBUST_ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure delivery and management.
O.ROBUST_TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.
O.SECURE_UPDATES	The TOE shall provide a secure mechanism for the receipt of spam and virus signature updates.
O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure. The TSF will provide a High Availability configuration which allows for continued operation of the TOE in the event of a single unit failure.
O.SOUND_DESIGN	The design of the TOE will use sound design principles and techniques.
O.SOUND_IMPLEMENTATION	The implementation of the TOE will be an accurate instantiation of its design, and is adequately and accurately documented.
O.THOROUGH_FUNCTIONAL_TESTING	The TOE will undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements.

O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
O.TRUSTED_CHANNEL	The TOE shall ensure that data sent between the TOE and administrators, users, and external entities is protected from unauthorized disclosure and modification.
O.TRUSTED_PATH	The TOE shall maintain a trusted path for administrator and user identification and authentication.
O.VIRUS	The TOE will detect and block viruses contained within an information flow which arrives at any of the TOE network interfaces.
O.VULNERABILITY_ANALYSIS_TEST	The TOE will undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE does not allow attackers with low attack potential to violate the TOE's security policies.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means.

OE.CREDENTIALS	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organisational policies identified for the TOE.

	T.ADMIN_ERROR	T.ADMIN_ROGUE	T.AUDIT_COMPROMISE	T.FLAWED_DESIGN	T.FLAWED_IMPLEMENTATION	T.IMPROPER_CONFIGURATION	T.INFLUX	T.LOSSOF	T.MALICIOUS_ACTIVITY	T.MISUSE	T.NOHALT	T.POOR_TEST	T.PRIVILEGE	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.VIRUS	P.ACCESS	P.ACCOUNTABILITY	P.ADMIN_ACCESS	P.DETECT	P.INTEGRITY	P.MANAGE	P.PROTECT	P.VULNERABILITY_ANALYSIS_TEST	A.LOCATE	A.MANAGE	A.NOEVIL	A.PHYSICAL	A.PROTECT
O.ACCESS						X		X			X		X				X												
O.ADMIN_ROLE		X																	X										
O.AUDIT_GENERATION																		X											
O.AUDIT_PROTECTION		X	X																										
O.AUDIT_REVIEW															X														
O.AUDITS									X	X										X									
O.CHANGE_MANAGEMENT				X	X																								
O.EFFECTIVE_ADMIN						X																X							
O.INTEGRITY								X													X								

	T.ADMIN_ERROR	T.ADMIN_ROGUE	T.AUDIT_COMPROMISE	T.FLAWED_DESIGN	T.FLAWED_IMPLEMENTATION	T.IMPROPER_CONFIGURATION	T.INFLUX	T.LOSSOF	T.MALICIOUS_ACTIVITY	T.MISUSE	T.NOHALT	T.POOR_TEST	T.PRIVILEGE	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.VIRUS	P.ACCESS	P.ACCOUNTABILITY	P.ADMIN_ACCESS	P.DETECT	P.INTEGRITY	P.MANAGE	P.PROTECT	P.VULNERABILITY_ANALYSIS_TEST	A.LOCATE	A.MANAGE	A.NOEVIL	A.PHYSICAL	A.PROTECT
O.MAIL							X		X	X						X													
O.MANAGE	X																												
O.OVERFLOWS							X																X						
O.PROTECT								X					X				X					X							
O.ROBUST_ADMIN_GUIDANCE	X																												
O.ROBUST_TOE_ACCESS														X				X											
O.SECURE_UPDATES																X													
O.SELF_PROTECTION			X												X														
O.SOUND_DESIGN				X																									
O.SOUND_IMPLEMENTATION					X																								
O.THOROUGH_FUNCTIONAL_TESTING					X							X																	
O.TIME_STAMPS																		X											

	T.ADMIN_ERROR	T.ADMIN_ROGUE	T.AUDIT_COMPROMISE	T.FLAWED_DESIGN	T.FLAWED_IMPLEMENTATION	T.IMPROPER_CONFIGURATION	T.INFLUX	T.LOSSOF	T.MALICIOUS_ACTIVITY	T.MISUSE	T.NOHALT	T.POOR_TEST	T.PRIVILEGE	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.VIRUS	P.ACCESS	P.ACCOUNTABILITY	P.ADMIN_ACCESS	P.DETECT	P.INTEGRITY	P.MANAGE	P.PROTECT	P.VULNERABILITY_ANALYSIS_TEST	A.LOCATE	A.MANAGE	A.NOEVIL	A.PHYSICAL	A.PROTECT
O.TRUSTED_CHANNEL																							X						
O.TRUSTED_PATH																							X						
O.VIRUS																X													
O.VULNERABILITY_ANALYSIS_TEST				X	X							X												X					
OE.CREDENTIALS																											X		
OE.INSTAL																											X		
OE.PERSON		X																								X	X		
OE.PHYSICAL																								X				X	X

Table 6 - Mapping Between Objectives, Threats, Policies, and Assumptions

4.3.1 T.ADMIN_ERROR

O.MANAGE also contributes to mitigating this threat by providing administrators the capability to view configuration settings. For example, if the administrator made a mistake when configuring the ruleset, providing them the capability to view the rules affords them the ability to review the rules and discover any mistakes that might have been made.

O.ROBUST_ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner and to provide the administrator with instructions to ensure the TOE was not corrupted during the delivery process. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure.

4.3.2 T.ADMIN_ROGUE

O.ADMIN_ROLE mitigates this threat to a limited degree by limiting the functions available to an administrator. The TOE supports the following roles: Default Administrator, Read and Write Administrator, and Read Only Administrator. Though the Default Administrator role has full access to the system, the Read and Write Administrator and Read Only Administrator roles have limited privileges.

O.AUDIT_PROTECTION contributes to mitigating this threat by controlling access to the audit trail. Though the Default Administrator and the Read and Write Administrator can delete the audit trail the TOE audits deletion of audit data and no one is allowed to modify audit records. This ensures that the Default Administrator's actions are audited and the records can be viewed by another user.

OE.PERSON ensures that personnel are carefully selected thereby reducing the likelihood of a rogue administrator.

4.3.3 T.AUDIT_COMPROMISE

O.AUDIT_PROTECTION contributes to mitigating this threat by controlling access to the audit trail. No one is allowed to modify audit records, the Default Administrator and the Read and Write Administrator are the only ones allowed to delete the audit trail. The TOE has the capability to prevent auditable actions from occurring if the audit trail is full.

O.SELF_PROTECTION contributes to countering this threat by ensuring that the TSF can protect itself from users. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the audit trail. Likewise, ensuring that the functions that protect the audit trail are always invoked is also critical to the mitigation of this threat.

4.3.4 T.FLAWED_DESIGN

O.CHANGE_MANAGEMENT plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. This includes controlling physical access to the TOE's development area, and having an automated configuration management system that ensures changes made to the TOE go through an approval process and only those persons that are authorized can make changes to the TOE's design and its documentation.

O.SOUND_DESIGN counters this threat, to a degree, by requiring that the TOE be developed using sound engineering principles. By accurately and completely documenting the design of the security mechanisms in the TOE the design of the TOE can be better understood, which increases the chances that design errors will be discovered.

O.VULNERABILITY_ANALYSIS_TEST ensures that the design of the TOE is independently analyzed for design flaws. Having an independent party perform the assessment ensures an objective approach is taken and may find errors in the design that would be left undiscovered by developers that have a preconceived incorrect understanding of the TOE's design.

4.3.5 T.FLAWED_IMPLEMENTATION

O.CHANGE_MANAGEMENT plays a role in mitigating this threat in the same way that the flawed design threat is mitigated. By controlling who has access to the TOE's implementation representation and ensuring that changes to the implementation are analyzed and made in a controlled manner, the threat of intentional or unintentional errors being introduced into the implementation are reduced.

In addition to documenting the design so that implementers have a thorough understanding of the design, O.SOUND_IMPLEMENTATION requires that the developer's tools and techniques for implementing the design are documented. Having accurate and complete documentation, and having the appropriate tools and procedures in the development process helps reduce the likelihood of unintentional errors being introduced into the implementation.

Although the previous two objectives help minimize the introduction of errors into the implementation, O.THOROUGH_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation (with respect to the functional specification, high level, and low-level design) will be discovered through testing.

O.VULNERABILITY_ANALYSIS_TEST helps reduce errors in the implementation that may not be discovered during functional testing. Ambiguous design documentation and the fact that exhaustive testing of the external interfaces is not required may leave bugs in the implementation undiscovered in functional testing. Having an independent party perform a vulnerability analysis and conduct testing outside the scope of functional testing increases the likelihood of finding errors.

4.3.6 T.IMPROPER_CONFIGURATION

O.ACCESS contributes to the mitigation of this threat by limiting user access to appropriate functions and data.

O.EFFECTIVE_ADMIN mandates that the TOE include functions to effectively manage its functions and data, thereby reducing the likelihood of improper configuration.

4.3.7 T.INFLUX

O.MAIL mitigates this threat by ensuring that the TOE only processes legitimate email traffic thereby minimizing the TOE's workload.

O.OVERFLOWS mitigates this threat by ensuring that the TOE can handle potential audit data storage overflows.

4.3.8 T.LOSSOF

Since O.ACCESS only allows authorized users to access only appropriate TOE functions and data, it contributes to reducing the threat of unauthorized users accessing TOE data.

The objective O.INTEGRITY requires that the TOE ensure the integrity of all audit data. An audit trail assists the administrator in ensuring that unauthorized access has not occurred.

O.PROTECT requires that the TOE protect itself from unauthorized modifications and access to its functions and data, thereby contributing to the mitigation of loss of TOE data.

4.3.9 T.MALICIOUS_ACTIVITY

O.AUDITS requires that audit records exist for data accesses and use of the TOE functions. Administrator monitoring of the audit records can serve to deter or detect malicious activity.

O.MAIL contributes to the mitigation of this threat by filtering email reducing the likelihood of an IT System being affected by unauthorised users.

4.3.10 T.MISUSE

O.AUDITS requires that audit records exist for data accesses and use of the TOE functions. Administrator monitoring of the audit records can serve to deter or detect unauthorized activity.

O.MAIL contributes to the mitigation of this threat by filtering email reducing the likelihood of an IT System being affected by unauthorised users.

4.3.11 T.NOHALT

Since O.ACCESS only allows authorized users to access only appropriate TOE functions and data, it ensures that unauthorized users can not affect the TOE's execution.

4.3.12 T.POOR_TEST

Design analysis determines that TOE's documented design satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE. O.THOROUGH_FUNCTIONAL_TESTING ensures that adequate functional testing is performed to ensure the TSF satisfies the security functional requirements and demonstrates that the TOE's security mechanisms operate as documented. While functional testing serves an important purpose, it does not ensure the TSFI cannot be used in unintended ways to circumvent the TOE's security policies.

O.VULNERABILITY_ANALYSIS_TEST addresses this concern by requiring a vulnerability analysis be performed in conjunction with testing that goes beyond functional testing. This objective provides a measure of confidence that the TOE does not contain security flaws that may not be identified through functional testing.

4.3.13 T.PRIVILEGE

O.ACCESS only allows authorized users to access only appropriate TOE functions and data. It contributes to reducing the threat of unauthorized users accessing the TOE.

O.PROTECT requires that the TOE protect itself from unauthorized modifications and access to its functions and data, thereby contributing to the mitigation of misuse of system privileges.

4.3.14 T.UNATTENDED_SESSION

O.ROBUST_TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on user's sessions. Local administrator's sessions are locked and remote sessions are dropped after an administrator defined time period of inactivity. Locking the local administrator's session reduces the opportunity of someone gaining unauthorized access the session when the console is unattended. Dropping the connection of a remote session (after the specified time period) reduces the risk of someone accessing the remote machine where the session was established, thus gaining unauthorized access to the session.

4.3.15 T.UNAUTHORIZED_ACCESS

O.AUDIT_REVIEW requires that the TOE provide the capability to selectively view audit information, and alert the administrator of identified potential security violations. This mitigates the risk of unauthorized users accessing TOE services or sending data through the TOE by

providing the administrator the ability to detect activity that may indicate a desire to obtain unauthorized access.

O.SELF_PROTECTION contributes to countering this threat by ensuring that the TSF can protect itself from users. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control.

4.3.16 T.VIRUS

O.MAIL contributes to the mitigation of this threat by filtering email reducing the likelihood of an IT System being affected by unauthorised users.

O.SECURE_UPDATES requires that the TOE provide a secure mechanism for the receipt of virus signature updates. Ensuring that updates are received securely reduces the threat of viruses.

O.VIRUS ensures that the TOE will detect and block viruses contained within an information flow which arrives at any of the TOE network interfaces, thereby contributing to the mitigation of T.VIRUS.

4.3.17 P.ACCESS

O.ACCESS only allows authorized users to access only appropriate TOE functions and data, and contributes to the enforcement of the policy by ensuring that only authorized users can access the TOE.

O.PROTECT requires that the TOE protect itself from unauthorized modifications and access to its functions and data, and therefore contributes to meeting the objective that all TOE data is only used for authorized purposes.

4.3.18 P.ACCOUNTABILITY

O.AUDIT_GENERATION addresses this policy by providing the Administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.).

O.ROBUST_TOE_ACCESS supports this policy ensuring that all authorized users are identified.

O.TIME_STAMPS plays a role in supporting this policy by requiring the TOE to provide a reliable time stamp (configured by the Administrator). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred.

4.3.25 A.LOCATE

OE.PHYSICAL provides for the physical protection of the TOE.

4.3.26 A.MANAGE

OE.PERSON ensures all authorized administrators are qualified and trained to manage the TOE.

4.3.27 A.NOEVIL

OE.CREDENTIALS ensures that all access credentials are protected by the users in a manner which is consistent with IT security.

OE.INSTAL ensures that the TOE is properly installed and operated.

OE.PERSON ensures that authorized administrators are carefully selected and trained.

4.3.28 A.PHYSICAL

OE.PHYSICAL provides for the physical protection of the TOE hardware and software.

4.3.29 A.PROTECT

OE.PHYSICAL provides for the physical protection of the TOE hardware and software.

4.4 SECURITY REQUIREMENTS RATIONALE

The following table provides a mapping between the SFRs and Security Objectives or assurance requirements.

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUDITS	O.CHANGE_MANAGEMENT	O.EFFECTIVE_ADMIN	O.INTEGRITY	O.MAIL	O.MANAGE	O.OVERFLOWS	O.PROTECT	O.ROBUST_ADMIN_GUIDANCE	O.ROBUST_TOE_ACCESS	O.SECURE_UPDATES	O.SELF_PROTECTION	O.SOUND_DESIGN	O.SOUND_IMPLEMENTATION	O.THOROUGH_FUNCTIONAL_TESTING	O.TIME_STAMPS	O.TRUSTED_CHANNEL	O.TRSUTED_PATH	O.VIRUS	O.VULNERABILITY_ANALYSIS_TEST
FAU_ARP.1(1)										X															
FAU_ARP.1(2)										X														X	
FAU_ARP.1(3)										X															
FAU_ARP.1(4)										X			X												
FAU_GEN.1			X			X																			
FAU_GEN.2			X			X																			
FAU_SAA.1(1)										X															
FAU_SAA.1(2)										X															
FAU_SAA.1(3)										X															
FAU_SAA.1(4)										X															
FAU_SAR.1					X																				
FAU_SAR.3					X																				
FAU_SEL.1			X																						

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUDITS	O.CHANGE_MANAGEMENT	O.EFFECTIVE_ADMIN	O.INTEGRITY	O.MAIL	O.MANAGE	O.OVERFLOWS	O.PROTECT	O.ROBUST_ADMIN_GUIDANCE	O.ROBUST_TOE_ACCESS	O.SECURE_UPDATES	O.SELF_PROTECTION	O.SOUND_DESIGN	O.SOUND_IMPLEMENTATION	O.THOROUGH_FUNCTIONAL_TESTING	O.TIME_STAMPS	O.TRUSTED_CHANNEL	O.TRSUTED_PATH	O.VIRUS	O.VULNERABILITY_ANALYSIS_TEST
FAU_STG.1				X																					
FAU_STG.4				X					X			X													
FCS_CKM.1																						X	X		
FCS_CKM.4 (1)																						X	X		
FCS_CKM.4 (2)																						X	X		
FCS_COP.1																						X	X		
FDP_ETC.2										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															
FIA_UAU.1(1)	X														X										

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUDITS	O.CHANGE_MANAGEMENT	O.EFFECTIVE_ADMIN	O.INTEGRITY	O.MAIL	O.MANAGE	O.OVERFLOWS	O.PROTECT	O.ROBUST_ADMIN_GUIDANCE	O.ROBUST_TOE_ACCESS	O.SECURE_UPDATES	O.SELF_PROTECTION	O.SOUND_DESIGN	O.SOUND_IMPLEMENTATION	O.THOROUGH_FUNCTIONAL_TESTING	O.TIME_STAMPS	O.TRUSTED_CHANNEL	O.TRSUTED_PATH	O.VIRUS	O.VULNERABILITY_ANALYSIS_TEST
FIA_UAU.1(2)	X														X										
FIA_UAU.2(1)	X														X										
FIA_UAU.2(2)	X										X				X										
FIA_UAU.2(3)	X														X										
FIA_UID.2(1)	X														X										
FIA_UID.2(2)	X										X				X										
FIA_UID.2(3)	X														X										
FMT_MOF.1(1)								X			X														
FMT_MOF.1(2)								X			X														
FMT_MOF.1(3)								X			X														
FMT_MOF.1(4)								X			X														
FMT_MOF.1(5)								X			X														
FMT_MSA.1								X			X														
FMT_MSA.3								X			X														
FMT_MTD.1(1)								X			X														
FMT_MTD.1(2)								X			X														

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUDITS	O.CHANGE_MANAGEMENT	O.EFFECTIVE_ADMIN	O.INTEGRITY	O.MAIL	O.MANAGE	O.OVERFLOWS	O.PROTECT	O.ROBUST_ADMIN_GUIDANCE	O.ROBUST_TOE_ACCESS	O.SECURE_UPDATES	O.SELF_PROTECTION	O.SOUND_DESIGN	O.SOUND_IMPLEMENTATION	O.THOROUGH_FUNCTIONAL_TESTING	O.TIME_STAMPS	O.TRUSTED_CHANNEL	O.TRSUTED_PATH	O.VIRUS	O.VULNERABILITY_ANALYSIS_TEST
FMT_MTD.1(3)								X			X														
FMT_SMR.1		X																							
FPT_FLS.1																	X								
FPT_ITT.1													X												
FPT_STM.1													X								X				
FRU_FLT.1																	X								
FRU_RSA.1															X										
FSV_UPD_EXP.1																X									
FTA_SSL.3													X				X								
FTP_ITC.1																						X			
FTP_TRP.1																							X		
ALC_CMS.2							X																		
AGD_OPE.1														X											
AGD_PRE.1														X											
ADV_FSP.2												X					X	X	X						
ADV_TDS.1																	X	X	X						

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUDITS	O.CHANGE_MANAGEMENT	O.EFFECTIVE_ADMIN	O.INTEGRITY	O.MAIL	O.MANAGE	O.OVERFLOWS	O.PROTECT	O.ROBUST_ADMIN_GUIDANCE	O.ROBUST_TOE_ACCESS	O.SECURE_UPDATES	O.SELF_PROTECTION	O.SOUND_DESIGN	O.SOUND_IMPLEMENTATION	O.THOROUGH_FUNCTIONAL_TESTING	O.TIME_STAMPS	O.TRUSTED_CHANNEL	O.TRSUTED_PATH	O.VIRUS	O.VULNERABILITY_ANALYSIS_TEST
ATE_FUN.1																				X					
ATE_IND.2																				X					
AVA_VAN.2																									X

Table 7 - Mapping of SFRs to Security Objectives and Assurance Requirements

4.4.1 O.ACCESS

This objective is met by FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.2(3), FIA_UID.2(1), FIA_UID.2(2), and FIA_UID.2(3) which address ping requests, SMTP/SMTPS traffic, administrator, and end user authentication.

4.4.2 O.ADMIN_ROLE

The TOE provides administrator roles via FMT_SMR.1.

4.4.3 O.AUDIT_GENERATION

This objective is addressed by FAU_GEN.1, FAU_GEN.2, and FAU_SEL.1 which handle audit data generation.

4.4.4 O.AUDIT_PROTECTION

This objective is addressed by FAU_STG.1 and FAU_STG.4 which ensure that audit information is protected.

4.4.5 O.AUDIT_REVIEW

Through FAU_SAR.1 and FAU_SAR.3 the TOE will provides the capability to selectively view audit information, thereby alerting the administrator of potential security violations.

4.4.6 O.AUDITS

This objective is addressed by FAU_GEN.1 and FAU_GEN.2 which handle audit data generation.

4.4.7 O.CHANGE_MANAGEMENT

Configuration control of the TOE and its development evidence is addressed by ALC_CMS.2.

4.4.8 O.EFFECTIVE_ADMIN

The necessary management functions are defined by FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), and FMT_MTD.1(3). FMT_MOF.1(1), FMT_MOF.1(2), and FMT_MOF.1(3) limit changes to security functions to the administrator. FMT_MOF.1(4) limits changes to the antispam and antivirus signature databases to the administrator. FMT_MOF.1(5) limits changes to the administrator reports to the administrator. FMT_MSA.1 and FMT_MSA.3 control who can change the security attributes and their default values. FMT_MTD.1 limits access to TSF data.

4.4.9 O.INTEGRITY

FAU_STG.4 defines the requirement for the TOE to provide protected audit trail storage.

4.4.10 O.MAIL

FAU_ARP.1(1), FAU_ARP.1(2), FAU_ARP.1(3), and FAU_SAA.1 ensure that the TOE provides an appropriate response when filtering email and FDP_IFC.1(1), FDP_IFC.1(2),

FDP_IFF.1(1), and FDP_IFF.1(2) provide the necessary functions to handle the email flows. FDP_IFC.1(3) and FDP_IFF.1(3) address the TOE's response to ICMP requests. FDP_IFC.1(4) and FDP_IFF.1(4) address user access to their email quarantine. FDP_ETC.2 addresses archiving of email. FAU_ARP.1(4) addresses the sending of an alert email upon detection of a security violation.

4.4.11 O.MANAGE

FIA_UAU.2(2) and FIA_UID.2(2) ensure that the management functions are restricted to administrators. The necessary management functions are defined by FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), and FMT_MTD.1(3). FMT_MOF.1(1), FMT_MOF.1(2), and FMT_MOF.1(3) limit changes to security functions to the administrator. FMT_MOF.1(4) limits changes to the antispam and antivirus signature databases to the administrator. FMT_MOF.1(5) limits changes to the administrator reports to the administrator. FMT_MSA.1 and FMT_MSA.3 control who can change the security attributes and their default values. FMT_MTD.1(1), FMT_MTD.1(2), and FMT_MTD.1(3) limit access to TSF data.

4.4.12 O.OVERFLOWS

The objective for the TOE to handle audit data storage overflows is addressed by FAU_STG.4.

4.4.13 O.PROTECT

The TOE protects itself from unauthorized modifications and access to its functions and data through the FPT_STM.1 and FTA_SSL.3 requirements. Time stamps serve to show actual or potential violations and session termination ensures that unattended administrator sessions are terminated. FPT_ITT.1 ensures that data transferred between components is protected in the HA configuration. FAU_ARP.1(4) ensures that an administrator can receive an email alert when a potential security violation is detected thereby assisting in protecting the TOE.

4.4.14 O.ROBUST_ADMIN_GUIDANCE

This objective is addressed by the AGD_OPE.1 and AGD_PRE.1 assurance requirements.

4.4.15 O.ROBUST_TOE_ACCESS

This objective is met by FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.2(1), FIA_UID.2(1), FIA_UAU.2(2), FIA_UID.2(2), FIA_UAU.2(3), FIA_UID.2(3) which address ping requests, SMTP/SMTPS traffic, administrator, and end user authentication and FRU_RSA.1 which help ensure that users do not misuse TOE services.

4.4.16 O.SECURE_UPDATES

The TOE provides for antispam and antivirus signature updates via FSV_UPD_EXP.1.

4.4.17 O.SELF_PROTECTION

The ADV_FSP.2 and ADV_TDS.1 assurance requirements contribute to the ability of the TOE to protect itself from external interference, tampering, or unauthorized disclosure. FTA_SSL.3

also contributes to this by ensuring that inactive administrator sessions are terminated. The requirement for an HA configuration is addressed by FRU_FLT.1 and FPT_FLS.1.

4.4.18 O.SOUND_DESIGN

The objective that the TOE is of sound design is addressed by the ADV_FSP.2 and ADV_TDS.1 assurance requirements.

4.4.19 O.SOUND_IMPLEMENTATION

The objective that the TOE is implemented correctly is addressed by the ADV_FSP.2 and ADV_TDS.1 assurance requirements.

4.4.20 O.THOROUGH_FUNCTIONAL_TESTING

The ATE_FUN.1 and ATE_IND.2 assurance requirements address the objective that the TOE undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements.

4.4.21 O.TIME_STAMPS

FPT_STM.1 defines the requirement for the TOE to provide time stamps.

4.4.22 O.TRUSTED_CHANNEL

FCS_CKM.1, FCS_CKM.4(1), FCS_CKM.4(2), and FCS_COP.1 provide the necessary cryptographic support for the trusted channel objective while FTP_ITC.1 implements the trusted channel.

4.4.23 O.TRUSTED_PATH

FCS_CKM.1, FCS_CKM.4(1), FCS_CKM.4(2), and FCS_COP.1 provide the necessary cryptographic support for the trusted path objective while FTP_TRP.1 implements the trusted path.

4.4.24 O.VIRUS

The ability of the TOE to detect and block viruses contained within an information flow is addressed by FAU_ARP.1(2).

4.4.25 O.VULNERABILITY_ANALYSIS_TEST

AVA_VAN.2 addresses the requirement for independent vulnerability analysis and penetration testing.

4.5 DEPENDENCY RATIONALE

Table 8 - Functional Requirement Dependencies identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

SFR	Dependencies	Dependency Satisfied?	Notes
FAU_ARP.1	FAU_SAA.1	Yes	FAU_SAA.1 is in the ST
FAU_GEN.1	FPT_STM.1	Yes	FPT_STM.1 is in the ST
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes	FAU_GEN.1 and FIA_UID.2 are in the ST
FAU_SAA.1	FAU_GEN.1	Yes	FAU_GEN.1 is in the ST
FAU_SAR.1	FAU_GEN.1	Yes	FAU_GEN.1 is in the ST
FAU_SAR.3	FAU_SAR.1	Yes	FAU_SAR.1 is in the ST
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Yes	FAU_GEN.1 and FMT_MTD.1 are in the ST
FAU_STG.1	FAU_GEN.1	Yes	FAU_GEN.1 is in the ST
FAU_STG.4	FAU_STG.1	Yes	FAU_STG.1 is in the ST
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4		FCS_COP.1 and FCS_CKM.4 are in the ST
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes	FCS_CKM.1 is in the ST
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Yes	FCS_CKM.1 and FCS_CKM.4 are in the ST
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Yes	FDP_IFC.1 is in the ST
FDP_IFC.1	FDP_IFF.1	Yes	FDP_IFF.1 is in the ST
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes	FDP_IFC.1 and FMT_MSA.3 are in the ST
FIA_UAU.1	FIA_UID.1	Yes	FIA_UID.2 is in the ST
FIA_UAU.2	FIA_UID.1	Yes	FIA_UID.2 is in the ST
FIA_UID.2	None	Yes	
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes	FMT_SMR.1 is in the ST See note below table regarding FMT_SMF.1

SFR	Dependencies	Dependency Satisfied?	Notes
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Yes	FDP_IFC.1 and FMT_SMR.1 are in the ST See note below table regarding FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes	FMT_MSA.1 and FMT_SMR.1 are in the ST
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes	FMT_SMR.1 is in the ST See note below table regarding FMT_SMF.1
FMT_SMF.1	None	Yes	See note below table.
FMT_SMR.1	FIA_UID.2	Yes	FIA_UID.2 is in the ST
FPT_FLS.1	None	Yes	
FPT_ITT.1	None	Yes	
FPT_STM.1	None	Yes	
FRU_FLT.1	FPT_FLS.1	Yes	FPT_FLS.1 is in the ST
FRU_RSA.1	None	Yes	
FSV_UPD_EXP.1	FAU_GEN.1 FMT_MOF.1	Yes	FAU_GEN.1 and FMT_MOF.1 are in the ST
FTA_SSL.3	None	Yes	
FTP_ITC.1	None	Yes	
FTP_TRP.1	None	Yes	

Table 8 - Functional Requirement Dependencies

Note: Although the FMT_SMF.1 requirement is a dependency of FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1, FMT_SMF.1 has not been included in this ST. The requirements FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 express the functionality required by the TSF to provide the specified functions to manage TSF data, security attributes and management functions. These requirements make it clear that the TSF has to provide the functions to manage the identified data, attributes and functions. Therefore FMT_SMF.1 is not necessary.

5 EXTENDED COMPONENTS DEFINITION

5.1 CLASS FSV: ANTISPAM AND ANTIVIRUS UPDATES

Antispam and antivirus updates provide the ability to update the antispam and antivirus signature databases. Updates to the antispam and antivirus signature databases are not addressed by existing CC components.

This class consists of one family / component; FSV_UPD_EXP.1 Antispam and Antivirus Updates.

5.1.1 Antispam and Antivirus Updates (FSV_UPD_EXP)

5.1.1.1 Family Behaviour

This family defines the requirements for antispam and antivirus signature database updates.

5.1.1.2 Component levelling

FSV_UPD_EXP.1 provides for the ability to securely update the antispam and antivirus signature databases.

5.1.1.3 Management

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

Changes to the update configuration.

5.1.1.4 Audit

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

Basic: Changes to the configuration and updates to the antispam and antivirus signature databases.

5.1.1.5 FSV_UPD_EXP.1 (Antispam and antivirus updates)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation and FMT_MOF.1 Management of functions in TSF

This component will provide for the ability to securely update the antispam and antivirus signature databases.

FSV_UPD_EXP.1.1 - The TSF shall provide a secure mechanism to update the antispam and antivirus signatures used by the TSF.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, an extended requirement, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 9 - Summary of Security Functional Requirements.

Identifier	Name
FAU_ARP.1(1)	Security alarms (antispam)
FAU_ARP.1(2)	Security alarms (antivirus)
FAU_ARP.1(3)	Security alarms (content filtering)
FAU_ARP.1(4)	Security alarms (other events)
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1(1)	Potential violation analysis (antispam)
FAU_SAA.1(2)	Potential violation analysis (antivirus)
FAU_SAA.1(3)	Potential violation analysis (content filtering)
FAU_SAA.1(4)	Potential violation analysis (other events)
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4(1)	Cryptographic key destruction (Keys and CSPs)
FCS_CKM.4(2)	Cryptographic key destruction (RNG Seed Key)
FCS_COP.1	Cryptographic operation
FDP_ETC.2	Export of user data with security attributes
FDP_IFC.1(1)	Subset information flow control (unauthenticated information flow)
FDP_IFC.1(2)	Subset information flow control (authenticated information flow)
FDP_IFC.1(3)	Subset information flow control (unauthenticated TOE services)
FDP_IFC.1(4)	Subset information flow control (authenticated TOE services)

Identifier	Name
FDP_IFF.1(1)	Simple security attributes (unauthenticated information flow)
FDP_IFF.1(2)	Simple security attributes (authenticated information flow)
FDP_IFF.1(3)	Simple security attributes (unauthenticated TOE services)
FDP_IFF.1(4)	Simple security attributes (authenticated TOE services)
FIA_UAU.1(1)	Timing of authentication (SMTP/SMTPS traffic)
FIA_UAU.1(2)	Timing of authentication (for TOE services)
FIA_UAU.2(1)	User authentication before any action (SMTP/SMTPS traffic)
FIA_UAU.2(2)	User authentication before any action (administrators)
FIA_UAU.2(3)	User authentication before any action (end users)
FIA_UID.2(1)	User identification before any action (SMTP/SMTPS traffic)
FIA_UID.2(2)	User identification before any action (administrators)
FIA_UID.2(3)	User identification before any action (end users)
FMT_MOF.1(1)	Management of security functions behaviour (FAU_SAR, FAU_SEL, FAU_STG, FRU_RSA)
FMT_MOF.1(2)	Management of security functions behaviour (FTA_SSL)
FMT_MOF.1(3)	Management of security functions behaviour (antispam, antivirus, content filtering)
FMT_MOF.1(4)	Management of security functions behaviour (antispam and antivirus updates)
FMT_MOF.1(5)	Management of security functions behaviour (administrator reports)
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1(1)	Management of TSF data (default administrator)
FMT_MTD.1(2)	Management of TSF data (read and write administrator)
FMT_MTD.1(3)	Management of TSF data (read only administrator)
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_ITT.1	Basic internal TSF data transfer protection

Identifier	Name
FPT_STM.1	Reliable time stamps
FRU_FLT.1	Degraded fault tolerance
FRU_RSA.1	Maximum quotas
FSV_UPD_EXP.1	Antispam and antivirus updates
FTA_SSL.3	TSF-initiated termination
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

Table 9 - Summary of Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_ARP.1(1) Security Alarms (antispam)

FAU_ARP.1.1(1) The TSF shall take [

a) *Tag Email in subject line;*
b) *Tag Email with Header; and*
c) *(Reject, Discard, Quarantine, Replace email with replacement message, or Forward to email address)*

] upon detection of ~~a potential security violation~~ an email message qualifying as spam.

6.1.1.2 FAU_ARP.1(2) Security Alarms (antivirus)

FAU_ARP.1.1(2) The TSF shall take [

a) *Reject, Discard, Quarantine, Replace email with replacement message; and*
b) *send an alert email to specified email addresses*

] upon detection of ~~a potential security violation~~ an email containing a virus.

6.1.1.3 FAU_ARP.1(3) Security Alarms (content filtering)

FAU_ARP.1.1(3) The TSF shall take [

a) *Treat as spam, Reject, Discard, Replace email with replacement message, Quarantine or Forward to an email address; and*
b) *send an alert email to specified email addresses*

] upon detection of ~~a potential security violation~~ specified content in an email.

6.1.1.4 FAU_ARP.1(4) Security Alarms (other events)

FAU_ARP.1.1(1) The TSF shall take [

a) *send an alert email to specified email addresses*

] upon detection of a potential security violation.

6.1.1.5 FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [basic] level of audit; and
c) [*All auditable events listed in Table 10 - Auditable Events, which is a complete list, including those required by the basic level of audit*].

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 ST, [*information specified in column 3 of Table 10 - Auditable Events below*].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ARP.1(1)	Action taken due to detection of spam	Profile/policy that was matched and message details
FAU_ARP.1(2)	Action taken due to detection of virus	Profile/policy that was matched and message details
FAU_ARP.1(3)	Action taken due to content filtering	Profile/policy that was matched and message details
FAU_ARP.1(4)	Potential security violation detected	Identification of event
FAU_GEN.1	Start-up and shutdown of audit	
FAU_GEN.2	None	
FAU_SAA.1(1)	Action taken due to detection of antispam filtering rules met	Profile/policy that was matched and message details
FAU_SAA.1(2)	Action taken due to detection of antivirus rules met	Profile/policy that was matched and message details
FAU_SAA.1(3)	Action taken due to detection of content filtering rules met	Profile/policy that was matched and message details

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SAA.1(4)	Action taken	Identification of event
FAU_SAR.1	Reading of information from the audit records (Opening the audit trail)	The identity of the Administrator performing the function
FAU_SAR.3	None	
FAU_SEL.1	All modifications to the audit configuration that occur while he audit collection functions are operating	The identity of the Administrator performing the function
FAU_STG.1	None	
FAU_STG.4	None	
FCS_CKM.1	Failure of the activity	
FCS_CKM.4(1)	None	
FCS_CKM.4(2)	None	
FCS_COP.1	Failure of cryptographic operation	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information
FDP_ETC.2	None	
FDP_IFC.1(1)	None	
FDP_IFC.1(2)	None	
FDP_IFC.1(3)	None	
FDP_IFC.1(4)	None	
FDP_IFF.1(1)	None	
FDP_IFF.1(2)	None	
FDP_IFF.1(3)	None	
FDP_IFF.1(4)	None	
FIA_UAU.1(1)	All use of authentication mechanisms	Claimed identity of the user using the authentication mechanism
FIA_UAU.1(2)	None	

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU.2(1)	All use of authentication mechanisms	Claimed identity of the user using the authentication mechanism
FIA_UAU.2(2)	All use of authentication mechanisms	Claimed identity of the user using the authentication mechanism
FIA_UAU.2(3)	All use of authentication mechanisms	Claimed identity of the user using the authentication mechanism
FIA_UID.2(1)	All use of the user identification mechanism used for authorized users (that is, those that authenticate to the TOE)	Claimed identity of the user using the identification mechanism, location
FIA_UID.2(2)	All use of the user identification mechanism used for authorized users (that is, those that authenticate to the TOE)	Claimed identity of the user using the identification mechanism, location
FIA_UID.2(3)	All use of the user identification mechanism used for authorized users (that is, those that authenticate to the TOE)	Claimed identity of the user using the identification mechanism, location
FMT_MOF.1(1)	All modifications in the behaviour of the functions in the TSF	The identity of the Administrator performing the function
FMT_MOF.1(2)	All modifications in the behaviour of the functions in the TSF	The identity of the Administrator performing the function
FMT_MOF.1(3)	All modifications in the behaviour of the functions in the TSF	The identity of the Administrator performing the function
FMT_MOF.1(4)	All modifications in the behaviour of the functions in the TSF	The identity of the Administrator performing the function
FMT_MOF.1(5)	All modifications in the behaviour of the functions in	The identity of the Administrator performing the

Requirement	Auditable Events	Additional Audit Record Contents
	the TSF	function
FMT_MSA.1	All manipulation of the security attributes	The identity of the Administrator performing the function
FMT_MSA.3	None	
FMT_MTD.1(1)	All deletions of audit data	The identity of the Administrator performing the function
FMT_MTD.1(2)	All deletions of audit data	The identity of the Administrator performing the function
FMT_MTD.1(3)	None	
FMT_SMR.1	Modifications to the group of users that are part of a role	The identity of the Administrator performing the function
FPT_FLS.1	Failure of the TSF	
FPT_ITT.1	None	
FPT_STM.1	Changes to the time	The identity of the Administrator performing the function (if applicable)
FRU_FLT.1	Failure of the TSF	
FRU_RSA.1	limit reached	mail server and email address or IP address
FSV_UPD_EXP.1	Updates to the antispam and antivirus signature databases	The identity of the administrator or FortiGuard Distribution Server who performed the update
FTA_SSL.3	session termination	Identify of the administrator
FTP_ITC.1	All attempted uses of the trusted channel functions	Identification of the initiator and target of all trusted channels
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of the claimed user identity

Table 10 - Auditable Events

6.1.1.6 FAU_GEN.2 User identity association

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

6.1.1.7 FAU_SAA.1(1) Potential violation analysis (antispam)

FAU_SAA.1.1(1) The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2(1) The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*spam detected based on results of FortiGuard-Antispam scan, forged IP scan, greylist scan, DNSBL scan, deep header scan, SURBL scan, bayesian scan, heuristic scan, dictionary scan, banned word scan, image scan, sender reputation scan*] known to indicate a potential security violation.

Note: Definitions of the terms used are provided in Section 8.2.1.

6.1.1.8 FAU_SAA.1(2) Potential violation analysis (antivirus)

FAU_SAA.1.1(2) The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2(2) The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*virus detected based on results of FortiGuard-Antivirus scan, and heuristic scan*] known to indicate a potential security violation.

Note: Definitions of the terms used are in Section 8.2.1.

6.1.1.9 FAU_SAA.1(3) Potential violation analysis (content filtering)

FAU_SAA.1.1(3) The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2(3) The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*content questionable based on results of message filtering, attachment file type filtering*] known to indicate a potential security violation.

6.1.1.10 FAU_SAA.1(4) Potential violation analysis (other events)

FAU_SAA.1.1(4) The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2(4) The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*other events consisting of system error, disk is full, remote archiving fails, HA event, disk quota of an account is exceeded, dictionary is corrupted, system quarantine quota is full, and deferred emails # over n, interval time n minutes*] known to indicate a potential security violation.

6.1.1.11 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [*default administrator, read and write administrator, and read only administrator*] with the capability to read [*all audit information*] from the audit records.

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

6.1.1.12 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*selection and searches*] of audit data based on [

a) *selection of log type, subtype, and severity level;*
b) *searches by keyword (all log types);*
c) *searches by email subject (history log type);*
d) *searches by email from, to, message (history, antispam, and antivirus log types);*
e) *searches by session ID (all log types);*
f) *searches by log ID (all log types);*
g) *searches by client name (history log type); and*
h) *searches by date/time (all log types);*].

6.1.1.13 FAU_SEL.1 Selective audit

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

a) [severity level]; and

b) [*none*].

Note: The CC allows selection based on 'event type'. The TOE has predefined 'severity levels' which are equivalent. The severity levels are defined in the TSS.

6.1.1.14 FAU_STG.1 Protected audit trail storage

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

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

6.1.1.15 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [at the discretion of the administrator ignore audited events or overwrite the oldest stored audit records] and [*none*] if the audit trail is full.

Note: This requirement has been refined since the CC only allows one selection.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*as listed below*] and specified cryptographic key sizes [*as listed bel*ow] that meet the following: [*standards listed below*].

Algorithm	**Key Size**	**Standard**
Diffie Hellman	1024	RSA PKCS3
RSA PKCS1	2048	ANSI X9.31

Table 11 - Cryptographic Key Generation

6.1.2.2 FCS_CKM.4(1) Cryptographic key Destruction (Keys and CSPs)

FCS_CKM.4.1(1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [keys and CSPs are zeroized when a factory reset is performed via the web-manager, CLI, or console] that meets the following: [FIPS PUB 140-2 Key Management Security Level 1].

6.1.2.3 FCS_CKM.4(2) Cryptographic key Destruction (RNG Seed Key)

FCS_CKM.4.1(2) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [RNG seed key is zeroized when a

factory reset is performed via the web-manager, CLI, or console followed by a firmware update] that meets the following: [no standard].

6.1.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified below*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified below*] and cryptographic key sizes [*cryptographic key sizes specified below*] that meet the following: [*standards listed below*].

Operation	**Algorithm**	**Key Size or Digest Length**	**Standard**
Encryption and Decryption	Triple-DES	168	FIPS 46-3
	AES	256	FIPS 197
Message authentication coding	HMAC SHA-1	128, 224, 256, 384, 512	FIPS 198
Hashing	SHA-1	160	FIPS 180-3
Random Number Generation	RSA PKCS1	2048	ANSI X9.31 Appendix A
Digital Signatures	RSA	2048	ANSI X9.31

Table 12- Cryptographic Operation

6.1.4 User Data Protection (FDP)

6.1.4.1 FDP_ETC.2 Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the [*UNAUTHENTICATED INFORMATION FLOW SFP, AUTHENTICATED INFORMATION FLOW SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE:

a) [*email messages are archived based on administrator configurable parameters consisting of sender's email address, recipient's email address, keyword in subject, keyword in body, or attachment file name; and*

b) *Quarantine summary reports can be emailed to end users*].

6.1.4.2 FDP_IFC.1(1) Subset information flow control (unauthenticated information flow)

FDP_IFC.1.1(1) The TSF shall enforce the [*UNAUTHENTICATED INFORMATION FLOW SFP*] on

a) [*source subject: TOE interface on which information is received;*

b) *destination subject: TOE interface to which information is destined;*

c) *information: network packets and email messages; and*

d) *operations: route network packets and email messages*].

6.1.4.3 FDP_IFC.1(2) Subset information flow control (authenticated information flow)

FDP_IFC.1.1(2) The TSF shall enforce the [*AUTHENTICATED INFORMATION FLOW SFP*] on

a) [*source subject: TOE interface on which information is received;*

b) *destination subject: TOE interface to which information is destined;*

c) *information: network packets and email messages; and*

d) *operations: route network packets and email messages*].

6.1.4.4 FDP_IFC.1(3) Subset information flow control (unauthenticated TOE services)

FDP_IFC.1.1(3) The TSF shall enforce the [UN*AUTHENTICATED TOE SERVICES SFP*] on

a) [*source subject: TOE interface on which information is received;*

b) *destination subject: TOE interface to which information is destined;*

c) *information: network packets; and*

d) *operations: route network packets*].

6.1.4.5 FDP_IFC.1(4) Subset information flow control (authenticated TOE services)

FDP_IFC.1.1(4) The TSF shall enforce the [*AUTHENTICATED TOE SERVICES SFP*] on

a) [*source subject: TOE interface on which information is received;*

b) *destination subject: TOE interface to which information is destined;*

c) *information: network packets; and*

d) *operations: route network packets*].

6.1.4.6 FDP_IFF.1(1) Simple security attributes (unauthenticated information flow policy)

FDP_IFF.1.1(1) The TSF shall enforce the [*UNAUTHENTICATED INFORMATION FLOW SFP*] based on the following types of subject and information security attributes:

a) [*Source subject security attributes: presumed IP address and email address;*
b) *Destination subject security attributes: destination IP address and (email address);*
c) *Information security attributes: email message*].

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

a) [*the source IP address is not blocked; and*
b) *message does not violate antispam, antivirus, content filtering potential violation analysis rules defined in FAU_SAA.1(1), FAU_SAA.1(2), and FAU_SAA.1(3)*].

.

FDP_IFF.1.3(1) – The TSF shall enforce the [*in Transparent Mode the TSF shall pass, drop or intercept connections destined for the IP address of an SMTP/SMTPS server associated with the protected domain*].

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [

a) *The TOE shall ignore requests where the email address domain is not owned by the TSF; and*
b) *The TOE shall ignore all traffic except SMTP/SMTPS*].

6.1.4.7 FDP_IFF.1(2) Simple security attributes (authenticated information flow policy)

FDP_IFF.1.1(2) The TSF shall enforce the [*AUTHENTICATED INFORMATION FLOW SFP*] based on the following types of subject and information security attributes:

a) [*Source subject security attributes: presumed IP address and email address;*
b) *Destination subject security attributes: destination IP address and (email address);*
c) *Information security attributes: email message*].

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

a) [*the source IP address is not blocked;*

b) *user is authenticated using IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS servers; and*

c) *message does not violate antispam, antivirus, content filtering potential violation analysis rules defined in FAU_SAA.1(1), FAU_SAA.1(2), and FAU_SAA.1(3)*].

.

FDP_IFF.1.3(2) The TSF shall enforce the [*no additional rules*].

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

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [

a) *The TOE shall ignore requests where the email address domain is not owned by the TSF; and*

b) *The TOE shall ignore all traffic except SMTP/SMTPS*].

6.1.4.8 FDP_IFF.1(3) Simple security attributes (unauthenticated TOE services policy)

FDP_IFF.1.1(3) The TSF shall enforce the [*UNAUTHENTICATED TOE SERVICES SFP*] based on the following types of subject and information security attributes:

a) [*Source subject security attributes: presumed IP address;*

b) *Destination subject security attributes: destination IP address;*

c) *Information security attributes: ICMP message type and code as specified in RFC 792*].

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

a) [*the source IP address is not blocked; and*

b) *the identity of the destination subject is the TOE*].

.

FDP_IFF.1.3(3) – The TSF shall enforce the [*no additional rules*].

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

FDP_IFF.1.5(3) The TSF shall explicitly deny an information flow based on the following rules: [

a) *The TOE shall ignore all traffic except ICMP*].

6.1.4.9 FDP_IFF.1(4) Simple security attributes (authenticated TOE services policy)

FDP_IFF.1.1(4) The TSF shall enforce the [*AUTHENTICATED TOE SERVICES SFP*] based on the following types of subject and information security attributes:

a) [*Source subject security attributes: presumed IP address;*
b) *Destination subject security attributes: none;*
c) *Information security attributes: none*].

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

a) [*the source IP address is not blocked;*
b) *user is authenticated to an IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS server*].

.

FDP_IFF.1.3(4) The TSF shall enforce the [*no additional rules*].

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

FDP_IFF.1.5(4) The TSF shall explicitly deny an information flow based on the following rules: [

a) *The TOE shall ignore requests where the email address domain is not owned by the TSF; and*
b) *The TOE shall ignore all traffic except Webmail (HTTP/HTTPS), POP3/POP3S, and IMAP/IMAPS*].

6.1.5 Identification and Authentication (FIA)

6.1.5.1 FIA_UAU.1(1) Timing of authentication (SMTP/SMTPS traffic)

FIA_UAU.1.1(1) The TSF shall allow [*SMTP/SMTPS traffic to flow with mediation through the TOE unless the administrator requires authentication for SMTP/SMTPS traffic as defined by FIA_UID.2(1) and FIA_UAU.2(1)*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(1) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.2 FIA_UAU.1(2) Timing of authentication (for TOE services)

FIA_UAU.1.1(2) The TSF shall allow [*ICMP*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(2) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.3 FIA_UAU.2(1) User authentication before any action (SMTP/SMTPS traffic)

FIA_UAU.2.1(1) The TSF shall require each user to be successfully authenticated to an IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS server before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.4 FIA_UAU.2(2) User authentication before any action (administrators)

FIA_UAU.2.1(2) The TSF shall require each user to be successfully authenticated locally before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.5 FIA_UAU.2(3) User authentication before any action (end users[1])

FIA_UAU.2.1(3) The TSF shall require each user to be successfully authenticated to an IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS server before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.6 FIA_UID.2(1) User identification before any action (SMTP/SMTPS traffic)

FIA_UID.2.1(1) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.7 FIA_UID.2(2) User identification before any action (administrators)

FIA_UID.2.1(2) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.8 FIA_UID.2(3) User identification before any action (end users[1])

FIA_UID.2.1(3) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.6 Security Management (FMT)

6.1.6.1 FMT_MOF.1(1) Management of security functions behaviour (FAU_SAR, FAU_SEL, FAU_STG, FRU_RSA)

FMT_MOF.1.1(1) The TSF shall restrict the ability to [enable, disable, determine, and modify the behaviour of] the functions [*security audit (FAU_SAR), security audit (FAU_SEL), maximum quota (FRU_RSA)]* to [*the default administrator, read and write administrator*].

6.1.6.2 FMT_MOF.1(2) Management of security functions behaviour (FTA_SSL)

FMT_MOF.1.1(2) The TSF shall restrict the ability to [determine, modify the behaviour of] the functions [*session termination (FTA_SSL)]* to [*the default administrator*].

6.1.6.3 FMT_MOF.1(3) Management of security functions behaviour (antispam, antivirus, content filtering)

[1] End users use Webmail, POP3, or IMAP to access quarantined or archived email.

FMT_MOF.1.1(3) The TSF shall restrict the ability to [modify the behaviour of] the functions [*specified in FAU_ARP.1(1), FAU_ARP.1(2), FAU_ARP.1(3), FAU_ARP.1(4), and FAU_SAA.1(1), FAU_SAA.1(2), FAU_SAA.1(3), FAU_SAA.1(4), FDP_ETC.2]* to [*the default administrator, read and write administrator*].

6.1.6.4 FMT_MOF.1(4) Management of security functions behaviour (antispam and antivirus updates)

FMT_MOF.1.1(4) The TSF shall restrict the ability to [modify the behaviour of] the functions [*specified in FSV_UPD_EXP.1]* to [*the default administrator, and read and write administrator*].

6.1.6.5 FMT_MOF.1(5) Management of security functions behaviour (administrator reports)

FMT_MOF.1.1(5) The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*presenting and emailing to the administrator tabular and graphical reports of audit data*] to [*the default administrator, read and write administrator*].

6.1.6.6 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*UNAUTHENTICATED INFORMATION FLOW SFP, AUTHENTICATED INFORMATION FLOW SFP, UNAUTHENTICATED TOE SERVICES SFP, and AUTHENTICATED TOE SERVICES SFP*] to restrict the ability to [change_default, query, modify, delete] the security attributes [*referenced in the indicated polices*] to [*default administrator, read and write administrator*].

6.1.6.7 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [*UNAUTHENTICATED INFORMATION FLOW SFP, AUTHENTICATED INFORMATION FLOW SFP, UNAUTHENTICATED TOE SERVICES SFP, and AUTHENTICATED TOE SERVICES SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*default administrator, read and write administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.8 FMT_MTD.1(1) Management of TSF data (default administrator)

FMT_MTD.1.1(1) The TSF shall restrict the ability to [*perform the operations identified in Table 13 - Default Administrator Management of TSF Data on*] the [*TSF data identified in Table 13 - Default Administrator Management of TSF Data*] to [*the default administrator*].

Operation	**TSF Data**
view, add, edit, and delete	administrator accounts of all levels
view and change	all parts of the FortiMail unit configuration,

Operation	TSF Data
	including functions defined by FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.1(3), FAU_SEL.1, and FDP_ETC.2
manually update	firmware, antivirus definitions
download or upload	system setting
restore the FortiMail unit to factory defaults	not applicable
restart the FortiMail unit	not applicable
shut down the FortiMail unit	not applicable
delete	audit data
set	time and date used to form the time stamps in FPT_STM.1
backup and restore	TOE configuration

Table 13 - Default Administrator Management of TSF Data

6.1.6.9 FMT_MTD.1(2) Management of TSF data (read and write administrator)

FMT_MTD.1.1(2) The TSF shall restrict the ability to [*perform the operations identified in Table 14 - Read and Write Administrator Management of TSF Data on*] the [*TSF data identified in Table 14 - Read and Write Administrator Management of TSF Data*] to [the *read and write administrator*].

Operation	TSF Data
view	administrator accounts
view and change	FortiMail unit configuration at the system and domain levels, including functions defined by FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.1(3), FAU_SEL.1, AND FDP_ETC.2
change	own administrator account password
release and delete	quarantined messages for all domains
delete	audit data
set	time and date used to form the time stamps in FPT_STM.1
backup and restore	TOE configuration

Table 14 - Read and Write Administrator Management of TSF Data

6.1.6.10 FMT_MTD.1(3) Management of TSF data (read only administrator)

FMT_MTD.1.1(3) The TSF shall restrict the ability to [*perform the operations identified in Table 15 - Read Only Administrator Management of TSF Data on*] the [*TSF data identified in Table 15 - Read Only Administrator Management of TSF Data*] to [the *read only administrator*].

Operation	TSF Data
view	FortiMail unit configuration at the system and domain levels
manage	mail queues
backup	TOE configuration

Table 15 - Read Only Administrator Management of TSF Data

6.1.6.11 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [*default administrator, read and write administrator, and read only administrator*].

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

6.1.7 Protection of the TSF (FPT)

6.1.7.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*failure of a unit in a* FortiMail *Active-passive HA Group is detected*].

Application Note: The FPT_FLS.1 requirement is only implemented in the Active-passive High Availability configuration of the TOE.

6.1.7.2 FPT_ITT.1 Basic internal TSF data transfer protection

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

Application Note: The FPT_ITT.1 requirement only applies to the High Availability configuration of the TOE. To address this requirement a separate HA interface between units is used, with the cable being within the TOE boundary (as shown in Figure 2 – FortiMail High Availability Configuration*).*

6.1.7.3 FPT_STM.1 Reliable time stamps

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

6.1.8 Fault Tolerance (FRU)

6.1.8.1 FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of [*all TOE functionality*] when the following failures occur: [*complete failure of primary unit, failure of primary unit to accept SMTP/SMTPS service, failure of primary unit to accept POP service (POP3/POP3S), and failure of primary unit to accept Web service (HTTP/HTTPS) connections*].

Application Note: The FRU_FLT.1 requirement is only implemented in the Active-passive High Availability configuration of the TOE. Though all TOE functionality is provided by the passive unit if the primary unit fails, the Bayesian database is not duplicated to the passive unit.

6.1.8.2 FRU_RSA.1 Maximum quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [*connections*] that [individual user, defined group of users] can use [simultaneously, over a specified period of time].

6.1.9 Antivirus Updates (FSV)

6.1.9.1 FSV_UPD_EXP.1 Antispam and Antivirus Updates

FSV_UPD_EXP.1.1 The TSF shall provide a secure mechanism to update the antispam and antivirus signatures used by the TSF.

Application Note: Virus signature updates consist of updates to both the virus signature database and the processing engine for the detection of virus attacks. The TOE provides specific guidance to administrators noting that in the evaluated configuration of the TOE, only the virus signature database updates may be applied to the TOE.

6.1.10 TOE Access (FTA)

6.1.10.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an ~~interactive~~ **administrative** session after an [*administrator specified time interval of user inactivity*].

6.1.11 Trusted Path/Channels (TRP)

6.1.11.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **the FortiGuard Distribution Server** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*Antispam and Antivirus Updates*].

6.1.11.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] 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, disclosure].

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication].

6.2 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Basic Flaw Remediation (ALC_FLR.1). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.1 augmentation since there are a number of areas where current Fortinet practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in the Table 16 - EAL 2 Assurance Requirements below.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage

Assurance Class	Assurance Components	
	Identifier	**Name**
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 16 - EAL 2 Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 F.Audit

The TOE creates audit records for administrative events, potential TSP violations and information flow decisions. The TOE records time of the event, the identity of the administrator or user who caused the event, and details of the event as they occur. The administrator can review and search the audit records. The audit records are stored locally. The administrator can also control the events that are audited based on severity level. Old audit records are overwritten

if the audit trail is full or logging stops if that option has been chosen by the administrator. Audit records can not be modified and can only be deleted by the default or read and write administrator. In addition to being time stamped, each audit record is also assigned a sequential event ID. The timestamps originate from the TOE's system clock. The administrator can set the system clock. Changes to the date/time are audited.

The audit information is contained in four types of logs consisting of the event log, virus log, spam log, and history log. The event log contains management activity and events, such as administration and HA activity. The virus and spam logs record events related to virus and spam detection. The history log contains information flow records.

The administrator can view audit information based on the following parameters:

- log type consisting of history, event, antispam, and antivirus;
- sub type consisting of (ALL, Configuration, Admin User, Webmail, System, HA, Update Failure, Update Success, POP3, IMAP, SMTP, OTHERS);
- keyword (all log types);
- email subject (history log type);
- email from, to, message (history, antispam, and antivirus log types);
- session ID (all log types);
- log ID (all log types);
- client name (history log type); and
- date/time (all log types).

Information from log files can also be presented in tabular and graphical reports and can be emailed to administrators.

The administrator can control the information that is audited by on severity level consisting of:

- 0 - Emergency The system has become unusable.
- 1 - Alert Immediate action is required.
- 2 - Critical Functionality is affected.
- 3 - Error An error condition exists and functionality could be affected.
- 4 - Warning Functionality could be affected.
- 5 - Notification Information about normal events.
- 6 - Information General information about system operations.

7.1.2 F.Authentication

In order to protect the TOE data and services, the TOE requires identification and authentication for all administrative access via the network interfaces. Identification and authentication is always enforced on the serial interface (Local Console). The identification and authentication

mechanism is a username and password combination. The accounts are created by the Default Administrator or the Read and Write Administrator over the serial or network interfaces. The TOE maintains administrator accounts locally.

In addition the TOE supports authentication for information flows and TOE services (AUTHENTICATED INFORMATION FLOW SFP and AUTHENTICATED TOE SERVICES SFP). Supported authentication methods are IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, and SMTP/SMTPS servers.

7.1.3 F.InformationFlow

The TOE operates in accordance with four information flow security functional policies.

For the UNAUTHENTICATED INFORMATION FLOW SFP and the AUTHENTICATED INFORMATION FLOW SFP, the subjects under control of this policy are the TOE interfaces that connect to unauthenticated and authenticated users on an internal or external network sending information through the TOE to other destinations on the internal or external network. Unless the administrator requires authentication for SMTP/SMTPS traffic, the UNAUTHENTICATED INFORMATION FLOW SFP allows unauthenticated SMTP/SMTPS traffic to pass information through the TOE. The AUTHENTICATED INFORMATION FLOW SFP allows the administrator to restrict the passing of SMTP/SMTPS traffic through the TOE to users authenticated using IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS.

For the UNAUTHENTICATED TOE SERVICES SFP, the subjects under control of this policy are the TOE interfaces that connect unauthenticated users on an internal or external network sending information to or receiving information from the TOE. The UNAUTHENTICATED TOE SERVICES SFP allows the TOE to respond to ICMP requests.

For the AUTHENTICATED TOE SERVICES SFP, the subjects under control of this policy are the TOE interfaces that connect authenticated users on an internal or external network sending information to or receiving information from the TOE. The AUTHENTICATED TOE SERVICES SFP allows end users to access quarantine email via Webmail (HTTP/HTTPS), POP3/POP3S, or IMAP/IMAPS using credentials stored on an IMAP/IMAPS, LDAP/LDAPS, POP3/POP3S, RADIUS, or SMTP/SMTPS server.

The TOE provides the ability to archive emails (UNAUTHENTICATED INFORMATION FLOW SFP and AUTHENTICATED INFORMATION FLOW SFP) based on administrator controlled settings. Incoming and outgoing messages can exported outside the TOE based on sender's email address, recipient's email address, keyword in subject, keyword in body, or attachment file name.

The TOE allows the Administrator to view all information flows allowed by the information flow policy rules before the rules are applied. For information to pass through the TOE, it must match one of the Administrator specified rules which permit the information flow. The TOE provides filtering based on the content of the information flows. The TOE can perform antivirus, antispam, and content filtering. The TSF immediately enforces changes to the information flow policy rules when applied.

For antivirus filtering, the SMTP/SMTPS protocol is subject to filtering. The Administrator can also select the specific antivirus filtering techniques which are applied. If a virus is detected in an information flow the TOE can optionally, as specified by the Administrator, quarantine the information flow for further analysis and replace the information flow content containing the virus with a 'replacement message' the content of which is specified by the Administrator.

Antispam filtering is applied to information flows which use the SMTP/SMTPS, POP3/POP3S and IMAP/IMAPS protocols. The Administrator can select the antispam filtering techniques which are applied to these protocols. These techniques include FortiGuard-Antispam scan, forged IP scan, greylist scan, DNSBL scan, deep header scan, SURBL scan, bayesian scan, heuristic scan, dictionary scan, banned word scan, and image scan. The Administrator can also specify the action to be taken when spam is detected in an information flow and can also specify a replacement message.

Content filtering is applied to information flows which use the SMTP/SMTPS, POP3/POP3S and IMAP/IMAPS protocols and filters non-spam content such as words and file attachments that are not permitted by an organization's network usage policy. Content filtering can check for words in messages and/or filter attachments based on file type. If desired a replacement message can be specified by the administrator.

For messages which are quarantined as a result of filtering, the TOE, at the discretion of the administrator, can be configured to email quarantine summary reports to end users.

The TOE also performs ongoing analysis and will notify the administrator if significant system events occur that may indicate a potential security violation. These events include system error, disk is full, remote archiving fails, HA events, disk quota of an account is exceeded, dictionary is corrupted, system quarantine quota is full, and deferred emails exceed a specified limit.

For antispam filtering, the Administrator can configure the TOE to connect with a FortiGuard Distribution Server in order to determine whether or not an information flow contains spam. For antispam and antivirus filtering, the Administrator can configure the TOE to periodically download antispam and antivirus signature information from a FortiGuard Distribution Server. All communications between the TOE and the FortiGuard Distribution Server use a trusted channel which is provided by the TOE.

The TOE minimizes directory harvest attacks (DHA) tracking SMTP/SMTPS client behaviour and limits deliveries of those clients sending excessive spam messages, infected email, or messages to invalid recipients. Should clients continue delivering these types of messages, their connection attempts will be rejected. Sender reputation is managed by the FortiMail unit and requires no administration.

7.1.4 F.Protection

The TOE maintains an isolated security domain for its own execution. No other applications can be loaded onto the TOE. Administrators and users do not have access to the operating system or the file system (there are no root/system level users). The TOE stores all security and configuration data in segregated configuration files. The TOE only provides identification, authentication and information flow services to non-administrative users. To protect

administrative sessions the TOE terminates unattended sessions and uses cryptography to ensure that the administrator's credentials and sessions are protected.

The TOE provides high availability features to allow load balancing (Config-only HA) or failover protection (Active-passive HA). For failover protection the TOE preserves a secure state and ensures that mail data is synchronized. Data transmitted between units in a HA cluster is protected through the use of a separate HA interface and by physically protecting the cable.

The TOE provides a time stamp which is provided by the hardware.

The TOE protects against denial of service attacking by providing the ability to limit the number and duration of client (IP address or email server) connections.

The TOE can also send alert emails to the administrator when system related events occur including:

- critical events (the FortiMail unit detects a system error that may affect its operation);
- the hard disk of the FortiMail unit is full;
- remote archiving failures;
- HA events;
- disk quota of an account is exceeded; and
- system quarantine quota is full.

The TOE provides the administrator the ability to enforce limits on the connections that users or groups of users can use simultaneously or over a period of time. Connections can be controlled by IP address or by email domains.

7.1.5 F.SecurityManagement

Administrative access to the TOE is restricted to authorised administrators and is controlled through a set of pre-defined roles (default administrator, read and write administrator, and read only administrator). The roles permit specific types of administrative activities to be performed. The activities are shown in Table 13 - Default Administrator Management of TSF Data, Table 14 - Read and Write Administrator Management of TSF Data, and Table 15 - Read Only Administrator Management of TSF Data.

The TOE allows both local and remote administration. Local administration is performed using the Local Console. Remote administration is performed using the Network Web-Based GUI or Network CLI interfaces.

The TOE provides the default administrator and read and write administrator with the ability to backup and restore the configuration via the Network CLI or Network Web-Based GUI interfaces. The configuration backup consists of several parts which include the following:

- core configuration file;
- Bayesian databases;
- dictionary database;

- mail queues;
- black/white list database; and
- email user's address books.

The configuration backup does not include email archives stored locally, log files, and generated report files.

The TOE restricts changing the default, viewing, modifying, and deleting information flow and TOE services settings to the default administrator and the read and write administrator. Unless changed by the administrator, by default information flows are restrictive and email messages are rejected. By default the TOE responds to ICMP requests unless changed by the administrator. Authenticated services require end user accounts.

The TOE restricts the ability to present and email tabular and graphical reports of audit data to the default administrator and the read and write administrator.

	F.Audit	F.Authentication	F.InformationFlow	F.Protection	F.SecurityManagement
FAU_ARP.1(1)			X		
FAU_ARP.1(2)			X		
FAU_ARP.1(3)			X		
FAU_ARP.1(4)				X	
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAA.1(1)			X		
FAU_SAA.1(2)			X		
FAU_SAA.1(3)			X		
FAU_SAA.1(4)			X		
FAU_SAR.1	X				
FAU_SAR.3	X				
FAU_SEL.1	X				

	F.Audit	F.Authentication	F.InformationFlow	F.Protection	F.SecurityManagement
FAU_STG.1	X				
FAU_STG.4	X				
FCS_CKM.1			X	X	
FCS_CKM.4(1)			X	X	
FCS_CKM.4(2)			X	X	
FCS_COP.1			X	X	
FDP_ETC.2			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		
FIA_UAU.1(1)		X			
FIA_UAU.1(2)		X			
FIA_UAU.2(1)		X			
FIA_UAU.2(2)		X			
FIA_UAU.2(3)		X			
FIA_UID.2(1)		X			
FIA_UID.2(2)		X			
FIA_UID.2(3)		X			
FMT_MOF.1(1)					X
FMT_MOF.1(2)					X

	F.Audit	F.Authentication	F.InformationFlow	F.Protection	F.SecurityManagement
FMT_MOF.1(3)					X
FMT_MOF.1(4)					X
FMT_MOF.1(5)	X				X
FMT_MSA.1					X
FMT_MSA.3					X
FMT_MTD.1(1)					X
FMT_MTD.1(2)					X
FMT_MTD.1(3)					X
FMT_SMR.1					X
FPT_FLS.1				X	
FPT_ITT.1				X	
FPT_STM.1	X			X	
FRU_FLT.1				X	
FRU_RSA.1				X	
FSV_UPD_EXP.1			X		
FTA_SSL.3				X	
FTP_ITC.1			X	X	
FTP_TRP.1			X	X	

Table 17- Mapping of Security Functions to SFRs

8 CONVENTIONS AND TERMINOLOGY

8.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2 are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item]. To improve readability selections of [none] are generally not shown.

- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*]. To improve readability assignments of [*none*] are generally not shown.

- Refinement: Refined components are identified by using underlining additional information, or ~~strikeout~~ for deleted text.

- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_IFC.1(1), Subset information flow control (unauthenticated information flow policy)' and 'FDP_IFC.1(2) Subset information flow control (unauthenticated TOE services policy)'.

8.2 TERMINOLOGY AND ACRONYMS

8.2.1 Terminology

The following terminology is used in this ST:

Administrator	An Administrator is responsible for administering the TOE. The TOE has three administrative roles; default administrator, read and write administration, and read only administrator. Administration is performed using the administrator interfaces which consist of the Local Console, Network Web-Based GUI, and Network CLI.
Attack Potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
Banned word scanning	The administrator can specify a list of banned words as part of an antispam profile. If the FortiMail unit detects any of the banned words in the email body or header, it flags the email as spam.
Bayesian scanning	Bayesian scanning is one of the methods that the FortiMail Gateway uses to filter email for spam. Bayesian filters are the latest in spam filtering technology. The filters recognize spam by looking at the words (or "tokens") in email. A Bayesian filter starts with two collections of email, one of spam and one of legitimate email. For every word in the emails, it calculates a spam probability based on the proportion of spam occurrences. Scanning is performed using information from the TOE's Bayesian Database.

Deep header scanning	Deep header scanning involves two separate checks. Black IP checking examines the “Received” fields of the email header. The FortiMail unit then extracts any URIs or IPs from the header and passes them to the FortiGuard Antispam service, DNSBL, or SURBL servers for spam checking. Header analysis examines the entire message header for spam characteristics.
DNSBL scanning	In addition to supporting Fortinet’s FortiGuard Antispam DNSBL service, the FortiMail unit supports administrator-defined, third-party DNS Blacklist servers.
Forged IP scanning	When the FortiMail unit receives an email message, it converts the sender's IP address to a canonical host name. The FortiMail unit then compares all of the officially listed IP addresses for that host name with the sender's IP address. If the sender's IP address is not found, the FortiMail unit considers the IP address and host name to be forged and treats the email as spam.
FortiGuard Antispam DNSBL	To achieve up-to-date real-time identification, the FortiGuard Antispam service uses globally distributed spam probes that receive over one million spam messages per day. The FortiGuard Antispam service uses multiple layers of identification processes to produce an up-to-date list of spam origins. To further enhance the service and streamline performance, the FortiGuard Antispam service continuously retests each of the “known” identities in the list to determine the state of the origin (active or inactive). If a known spam origin has been decommissioned, the FortiGuard Antispam service removes the origin from the list, thus providing customers with both accuracy and performance.
FortiGuard Antispam service	The FortiGuard Antispam service is a Fortinet-managed service that provides a three-element approach to screening email messages. The first element is a DNS Block List (DNSBL) which is a “living” list of known spam origins. The second element is an in-depth email screening based on a Uniform Resource Identifier (URI) contained in the message body – commonly known as Spam URI Realtime Blackhole Lists (SURBLs). The third element is the FortiGuard Antispam Spam Checksum Blocklist (SHASH) feature. Using SHASH, the FortiMail unit sends a hash of an email to the FortiGuard Antispam server which compares the hash to hashes of known spam messages stored in the FortiGuard Antispam database. If the hash results match, the email is flagged as spam

FortiGuard Antispam SURBL	To detect spam based on the message body URIs (usually web sites), Fortinet uses FortiGuard Antispam SURBL technology. Complementing the DNSBL component, which blocks messages based on spam origin, SURBL technology blocks messages that have spam hosts mentioned in message bodies. By scanning the message body, SURBL is able to determine if the message is a known spam message regardless of origin. This augments the DNSBL technology by detecting spam messages from spam source that may be dynamic, or a spam source that is yet unknown to the DNSBL service. The combination of both technologies provides a superior managed service with higher detection rates than traditional DNSBLs or SURBLs alone.
Greylist scanning	Greylist scanning blocks spam based on the behavior of the sending server, rather than the content of the messages. When receiving an email from an unknown server, the FortiMail unit will temporarily reject the message. If the mail is legitimate, the originating server will try to send it again later, at which time the FortiMail unit will accept it.
Heuristic scanning	The FortiMail unit includes rules the heuristic filter uses. Each rule has an individual score used to calculate the total score for an email. An upper and lower limit threshold for the heuristic filter is set for each antispam profile. To determine if an email is spam, the heuristic filter examines an email message and adds the score for each rule that applies to get a total score for that email. If the total is greater than or equal to the upper threshold, the filter classifies the email as spam and processes it accordingly. If the total is less than or equal to the lower threshold, the email is not spam. If the total is between the two thresholds, then the heuristic filter cannot determine whether the email is spam or not spam determination.
Image spam scanning	Spammers attempt to get their email messages past spam safeguards by replacing the message body with an image file. This image file displays a graphic of the desired text. Since the message body contains no real text, scanners designed to examine the message body find nothing to work with. However, the FortiMail unit's image spam scan is equipped to examine and identify GIF, JPEG, and PNG graphics used in image spam.
Local Console	A management console (may be a computer workstation or VT100 type terminal) connected directly to the TOE. Although the Local Console falls outside the TOE Boundary it is located in the same physical location as the TOE and therefore is provided with the same physical protection as is provided for the TOE.
Network Management Station	A computer located remotely from the TOE but which is able to establish a network connection to the TOE. The Network Management Station falls outside the TOE Boundary.

Presumed Address	The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a 'presumed address' is used to identify source and destination addresses.
SURBL scanning	In addition to supporting Fortinet's FortiGuard Antispam SURBL service, the FortiMail unit supports administrator-defined, third-party Spam URI Realtime Block Lists servers.
Whitelist word scanning	You can specify a white list of words as part of an antispam profile. If the FortiMail unit detects a whitelist word, it treats the message as non-spam and cancels further antispam scanning.

8.2.2 Acronyms

The following acronyms are used in this ST:

AES	Advanced Encryption Standard
CLI	Command Line Interface
DES	Data Encryption Standard
DHA	Directory Harvest Attacks
DNS	Domain Name Server
DNSBL	DNS Black List (see DNS above)
DOS	Denial of Service
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HA	High-Availability
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Over Secure Socket Layer
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
IMAPS	Internet Message Access Protocol Over Secure Socket Layer
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Over Secure Socket Layer
PKCS	Public-Key Cryptography Standards
POP3	Post Office Protocol

POP3S	Post Office Protocol Over Secure Socket Layer
RADIUS	Remote Authentication Dial In User Service
RBL	Real-Time Black List
RNG	Random Number Generator
SFP	Security Functional Policy
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Over Secure Socket Layer
SSH	Secure Shell
ST	Security Target
SURBL	Spam URI Realtime Block Lists (see URI below)
TOE	Target of Evaluation
TSF	TOE Security Function
URI	Uniform Resource Identifier