Part Number 86-0947956-G

Version Date 8 April 2008

IronMail® Email Security Gateway v6.7 HF2

SECURITY TARGET

Prepared by:

Secure Computing Corporation

2340 Energy Park Drive

Saint Paul, Minnesota 55108

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the IronMail® Secure Email Gateway v6.7 HF2. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

ST Title:	IronMail® Secure Email Gateway v6.7 HF2 Security Target
ST Author:	Dwight D. Colby
ST Revision Number:	86-0947956-G
ST Date:	April 8, 2008

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC	COMMON CRITERIA
DNS	DOMAIN NAME SYSTEM
EAL2	EVALUATION ASSURANCE LEVEL 2
IMAP	INTERNET MESSAGE ACCESS PROTOCOL
IT	INFORMATION TECHNOLOGY
MIME	MULTIPURPOSE INTERNET MAIL EXTENSIONS
NIAP	NATIONAL INFORMATION ASSURANCE PARTNERSHIP
PP	PROTECTION PROFILE
POP	POST OFFICE PROTOCOL
SF	SECURITY FUNCTION
SFP	SECURITY FUNCTION POLICY
SMTP	SIMPLE MAIL TRANSFER PROTOCOL
SOF	STRENGTH OF FUNCTION
ST	SECURITY TARGET
TOE	TARGET OF EVALUATION
TSC	TSF SCOPE OF CONTROL
TSF	TOE SECURITY FUNCTIONS
TSFI	TSF INTERFACE
TSP	TOE SECURITY POLICY

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the IronMail® Secure Email Gateway v6.7 HF2. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) and international interpretations through June 29, 2006. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the IronMail® Secure Email Gateway v6.7 HF2 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

IronMail® Secure Email Gateway v6.7 HF2 Security Target.

1.1.2 TOE Reference

IronMail® Secure Email Gateway v6.7 HF2.

1.1.3 Security Target Evaluation Status

This ST is currently being written for acceptance into the Common Criteria Evaluation scheme.

1.1.4 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2 augmented with ALC_FLR.2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.1.5 Keywords

Email, Spam filtering, Content analysis.

1.2 TOE Overview

This Security Target forms the basis of evaluation for the IronMail® Secure Email Gateway v6.7 HF2. The TOE resides in an all-inclusive device positioned at the network gateway and is used for protecting organisations from email threats such as spam, liabilities arising from offensive content present in email messages and general mail policy violations. The TOE processes incoming messages through a number of filtering queues, which check the content of the messages for compliance against relevant organisational policies. Only those messages that have not been filtered by any queue are delivered to their destination. Messages may be selectively forwarded, quarantined or saved in order to facilitate forensic examination by third party tools.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the IronMail® Secure Email Gateway v6.7 HF2 to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

This Security Target is compliant with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9,* and all National Information Assurance Partnership (NIAP) and international interpretations through June 28, 2006. This Security Target is functional requirements (Part 2 of CC) conformant and assurance requirements (Part 3 of CC) conformant for EAL2, augmented with ALC_FLR.2.

1.4 Protection Profile Conformance

The IronMail® Secure Email Gateway v6.7 HF2 Security Target does not claim conformance to any registered Protection Profile.

1.5 Document Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).

    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
    - Explicitly stated Security Functional Requirements are indicated with "(EXP)".
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

CHAPTER 2

2. TOE Description

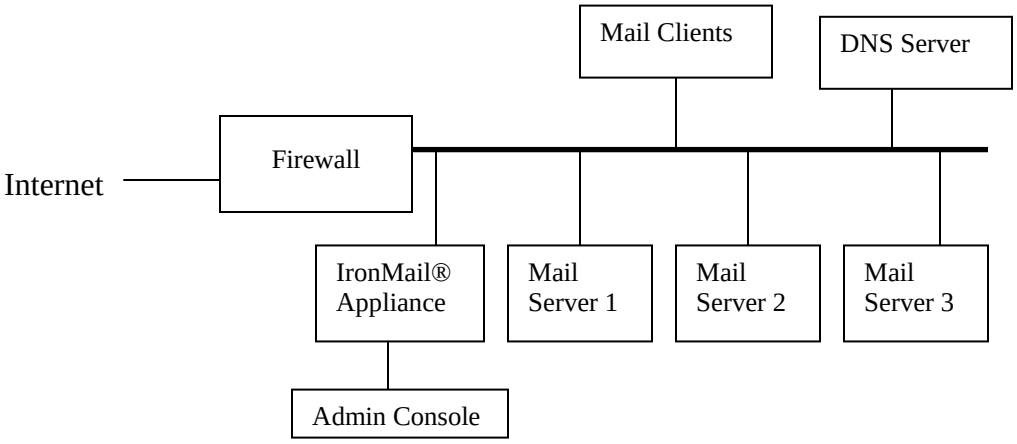
This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 IronMail® Secure Email Gateway v6.7 HF2 TOE Description

The TOE software provides an approach for limiting exposure of resources to threats inherent in a network infrastructure that supports sending and delivering electronic mail. The TOE is capable of scanning inbound and outbound email for unsolicited commercial email (aka Spam), offensive content, and violations of policies that are configured by authorized administrators.

The TOE is physically contained within a special purpose computer with a limited physical interface. This computer device is hereafter referred to as the IronMail® appliance. RFC 822, Multipurpose Internet Mail Extensions (MIME) encoded messages are checked for policy violations and the presence of offensive content. Any message that violates the TOE's notion of security is isolated and acted upon so as to mitigate any threat being posed by it before it reaches the internal network. The TOE is also able to detect and curtail the flow of spam into the internal network in order to ensure the availability of system resources such as storage space and CPU time.

Figure 1 - Typical TOE deployment



Typically the TOE is not in the physical path between the various participants in email exchanges (mail clients and servers, both internal and external). However, logically the IronMail® Appliance mediates all email exchanges. This requires the clients and servers to be configured to forward all email traffic through the IronMail® Appliance, routers and firewalls to redirect all email traffic through the IronMail® Appliance, or a combination of both.

The TOE is based on a fully functional mail server engine and a queuing architecture designed to quickly parse and analyze messages for policy violations. Once accepted by the SMTP interface, messages are written to the hard disk and meta data are inserted into the database. A management and scheduling process known as the “Super Queue” accepts responsibility for each message at this point. Super Queue will spawn multiple

copies of itself (based on the hardware model) each with a single processing engine thread that breaks down the message into parts and parses each of them for violations of rules or policies that have been configured by an authorized administrator.

The constituent queues that comprise the Super Queue are:

1. Rip Queue
2. Spam Queue (or Anti-Spam Queue)
3. Content Analysis Queue (or Content Filtering Queue)
4. Envelope Analysis Queue (or Mail Monitoring Queue)
5. Join Queue

TOE queues are components that process messages in an ordered fashion. The queuing architecture scrutinises every message received for harmful content. Once a message has successfully passed the scrutiny of each queue (assuming that no queue had to quarantine, drop, re-route, or take some other action on the message) the message is reassembled and provided to the organization's internal mail server(s) for delivery to its intended recipient. Each of the queues can be configured to take some action based on a set of rules in the event that a message fails to pass the security policy enforced by the queue.

The Spam Queue technology relies on information obtained from DNS; the DNS server is considered part of the IT environment and can reside on any host on the internal network. It is assumed to always provide reliable information to the TOE.

The TOE can be configured to recognise multiple administrators, each of whom can be granted privileges to configure selected components of the TOE. Administrators access the TOE using a graphical user interface (GUI) through a secured web connection and the administrator is authenticated by the TOE. Once authenticated, administrators can configure the behaviour of different TOE components by defining rules that identify spam, malicious content, confidential information and policy violations. Rules may also be defined to allow specific messages to bypass the various filtering queues.

The TOE provides a logging component that allows the authorised administrator of the TOE to monitor the behaviour of the TOE and its different components. Log records are generated for events such as policy matches and configuration changes made on the TOE.

The IronMail® appliance uses a variant of FreeBSD as its base operating system. The FreeBSD operating system has been pared down to its essential components and only provides the services necessary for supporting the TOE software. In addition, OpenSSL version 0.9.8g is included in the appliance to support SSL communication. Both the OS and OpenSSL are part of the IT environment and are not included in the TOE.

2.1.1 Physical and Logical Boundaries

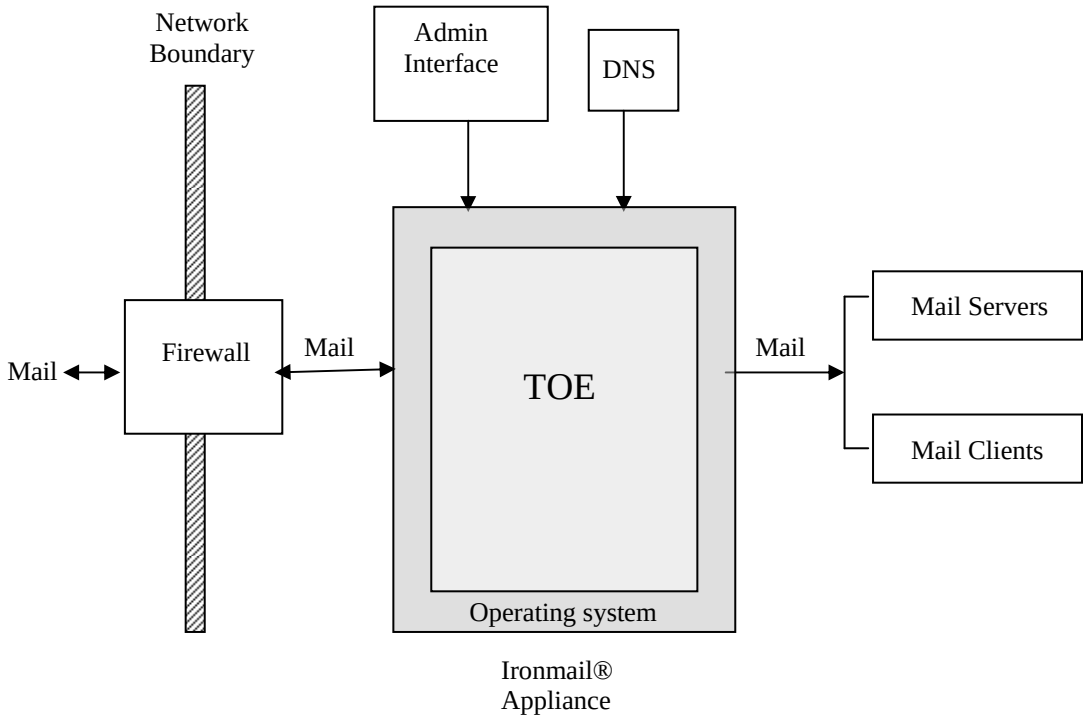
The TOE is a software product that is physically contained within a computer having limited physical interfaces. The computer is configured as a special purpose device or appliance, intended solely to serve as a host for the TOE software.

The logical relationship between the TOE and the various network components is depicted in Figure 2. The TOE is logically positioned at the network gateway between the

firewall and the mail servers. Every email that enters the internal network first passes through the TOE. Similarly, only the TOE can deliver outgoing messages.

The IT environment is configured such that the TOE is the only entry point for all incoming email messages (destined to internal network) to the mail servers. Similarly, the TOE is the only exit point for all outgoing email messages (destined to external network).

Figure 2 - Physical and Logical Boundary



The TOE runs over a hardened operating system and includes a MySQL database that ensures high integrity and speed. The database provides a storage and retrieval mechanism for configuration information, message meta data and statistical data for reporting purposes.

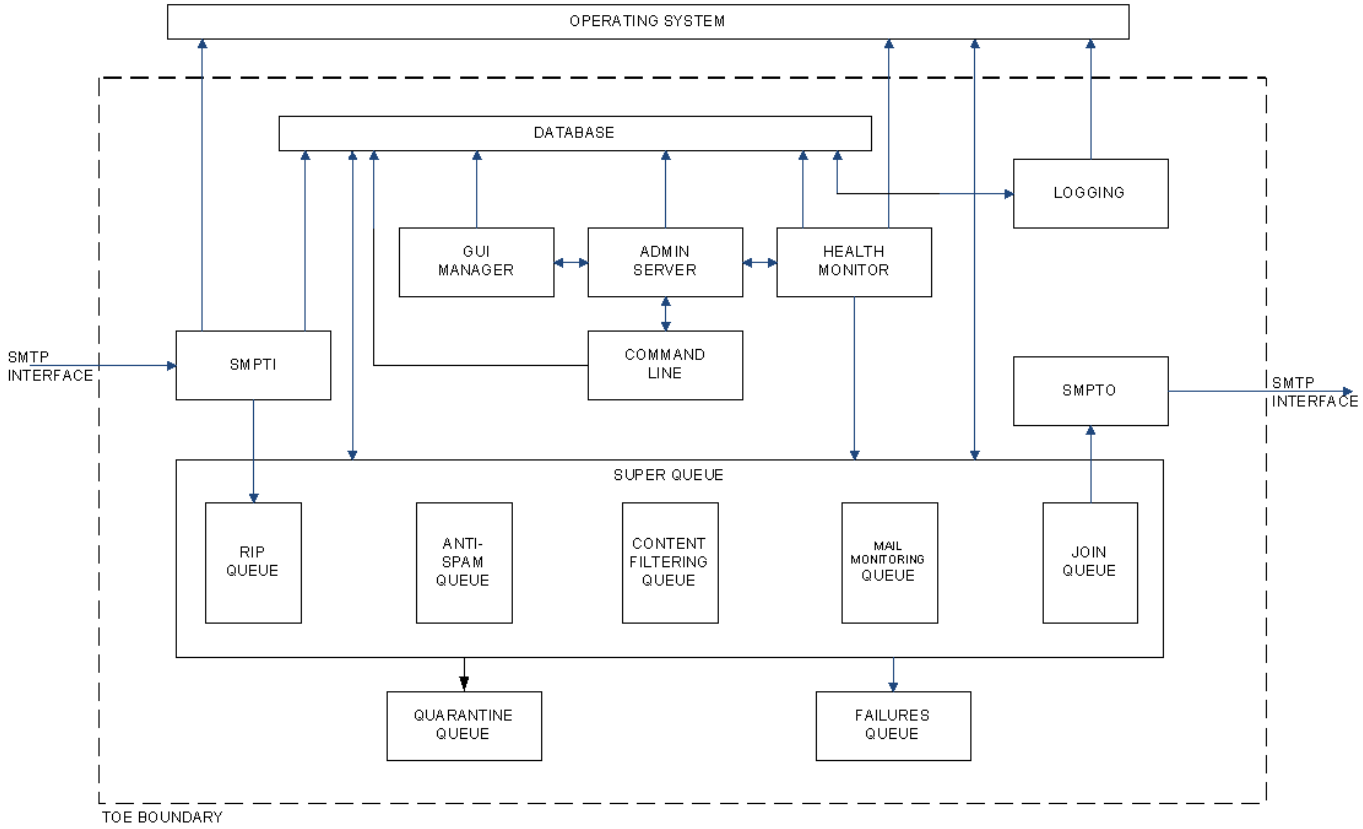
Administrators connect to the IronMail® appliance using a secure HTTPS connection from a web browser in order to maintain and monitor the TOE's operation. HTTPS is supported by cryptographic services in the IT environment. Authentication services are provided by the TOE.

2.1.2 Logical Boundary

The logical boundary of the TOE is as shown in Figure 3. The essential TOE components which provide the security functionality of the TOE are: SMTPI, Super Queue (Rip

Queue, Spam Queue, Content Filtering Queue, Mail Monitoring Queue, Join Queue), SMTPO, Logging and GUI Manager.

Figure 3 - TOE Internal Logic



These components essentially represent TOE Security Functions (TSFs) and are described below. The other internal TOE components represented are not responsible for any Security Function Policy (SFP).

- **SMTPI** is the only external interface to receive email in the TOE. It accepts the email as per RFC 2821. It also evaluates all administrator configured whitelisting rules for the message and sets up processing order that the other queues follow.
- **Super Queue** is the email processing engine of the TOE. It is tasked with handling all the sub-queues and acts as a facilitator for the message hand-off between the sub-queues. The sub-queues evaluate various administrator configured rules and handover the results to Super Queue which then is responsible for the final action (if any) on the message based on a pre-determined precedence rules among the actions.
    - The **Rip Queue** is the first to process an email message. It is tasked to “rip” (or break down) the message into its constituent MIME parts. Messages that cannot be parsed can be configured to be either dropped or repackaged and sent to the original or an alternate email address or it can be further processes but with only a subset of TOE functionality.

- The **SPAM Queue** inspects messages for characteristics of spam. When a message is found to be spam-like, an administrator-defined action such as drop, quarantine or rename can be performed on it.
- The **Content Filtering Queue** inspects messages for the presence of inappropriate content. Content analysis is also enforced over the message attachments to ensure that messages containing specified attachment types do not pass through the TOE.
- The **Mail Monitoring Queue** allows the monitoring of messages over selection criteria such as the sender, recipient, size and subject information.
- The **Join Queue** is the last to process an email message. Its task is to reassemble the message back into a whole. If any of the intermediate sub-queues perform a message altering action, the Join Queue reassembles the message from the TOE-edited parts and sends it to the SMTPO for final delivery.

- The **SMTPO** Service is responsible for delivering messages out of the TOE. It is the only means by which messages can be sent out of the network domain. It delivers email conforming to RFC 2821.
- The **GUI MANAGER** component provides graphical interfaces for the authorised users of the TOE to configure and maintain the TOE.
- The **Logging** component provides auditing support for the TOE.

2.2 IronMail® Secure Email Gateway Software Version 6.7 HF2 Evaluated Configuration

The evaluated configuration includes an IronMail® appliance that is logically situated between the firewall and the internal mail servers/clients, configured in a manner which ensures that every message that is sent into or out of the internal network always passes through it. The TOE and the Admin workstation and the connection between them are maintained in a physically secure environment.

IronMail® uses "hardened" FreeBSD as its Operating System; the OS is not included in the TOE Scope of Control (TSC). IronMail® provides additional functionality for Anti-virus, Webmail Protection, and Corporate Compliance but these are specifically excluded from the scope of evaluation.

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) Information Technology related threats to the organisation countered by the TOE.

C) Environmental threats requiring controls to provide sufficient protection.

D) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies assumptions (A), threats (T) and organisational security policies (P).

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

3.2.1 Connectivity Assumptions

A.DNS	DNS information received by the TOE is reliable.
A.COMM_PROTECT	The IT Environment will protect communication to and from the TOE from unauthorized disclosure or modification.

3.2.2 Personnel Assumptions

A.NO_EVIL_ADMIN	Authorized administrators are non-hostile and are appropriately trained to use, configure and maintain the TOE.

3.2.3 Physical Assumptions

A.PHYSICAL_SECURITY	The TOE resides in a physically controlled access facility that prevents unauthorized physical access.

3.3 Threats

3.3.1 Threats against the TOE

T.BYPASS	A threat agent may bypass one or more of the TOE's security functions and send malicious data to mail servers being protected by the TOE.
T.CONTENT	A threat agent may circulate dirty, offensive or proprietary information in violation of the TOE policy.

T.NEW_EXPLOITS	A threat agent may modify the message content suitably or use variants in the sender or recipient information in order to defeat the protection services offered by the TOE.
T.NO_AUDIT	A threat agent may perform security relevant operations on the TOE without being held accountable for it.
T.NO_REGULATE	A threat agent may try to violate the mail dissemination policy of the TOE by sending information that the TOE may not want to forward or receive, either because of its origin, destination or subject content.
T.OPAQUE	A threat agent may send malicious content in an encrypted form in order to violate the TOE's content distribution policy.
T.RESOURCE_CONSUME	Threat agents may flood the TOE with spam, consuming resources such as memory, bandwidth, processor time and data storage and thus limit the TOE's ability to execute its security functions efficiently.
T.UNTRUSTED_CODE	A threat agent may download untrusted code to the TOE causing abnormal processes to be executed, which violate the integrity and availability of system assets.
T.BRUTE_FORCE	A threat agent may repeatedly try and guess authentication data in order to gain unauthorized access to the TOE.
T.IA	A threat agent may attempt to compromise the TOE by attempting actions that it is not authorized to perform on the TOE.

3.4 Organisational Security Policies

None

CHAPTER 4

4. Security Objectives

4.1 Security Objectives for the TOE

The objectives listed in this section ensure that all of the TOE security threats listed in Chapter 3 have been countered. The security objectives (O) for the IronMail® Secure Email Gateway v6.7 HF2 are:

O.CONFIGURABILITY	The TOE shall provide administrative tools to enable authorised administrators to effectively configure and maintain the TOE.
O.CONTENT_FILTER	The TOE shall take specified action on incoming messages based on their message or attachment content and content patterns.
O.LOG	The TOE shall generate logs of all the security-relevant operations performed on the TOE.
O.MAIL_POLICY	The TOE shall be able to prevent specific types of information sent to or from specific entities, from passing through the TOE.
O.REF_MEDIATION	All inbound or outbound mail into or out of the TOE, unless explicitly allowed by the TOE administrator, shall be examined by each of the TOE's configured filters before being forwarded to its destination.
O.SPAM_FILTER	The TOE shall be able to define characteristics for spam and take configured action when such characteristics are recognised.
O.AUTHENTICATION	The TOE shall require that users of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.
O.BOUNDED_AUTH	The TOE shall bound the number of failed authentication attempts to some configurable value in order to prevent brute force attacks against the TOE.

4.2 Security Objectives for the IT Environment

The objectives in this section are designed to address security assumptions and threats from Chapter 3.

O.E.DOMAIN_SEP	The IT Environment shall ensure that the execution of code within the TOE cannot be interfered with or tampered by any untrusted subject.

O.E.COMM_PROTECT	The IT Environment shall protect communication to and from the TOE from unauthorized disclosure or modification.
O.E.LOG	The IT environment will provide a means to store the TOE's audit log and protect it from unauthorised modification
O.E.TRUSTED_ENV	The TOE shall reside at a physically secure location, safe from compromise by malicious insiders or outsiders.
O.E.TRUSTED_INFO	The integrity of the information received by the TOE from trusted external subsystems shall never be compromised.
O.E.TS_INTEGRITY	The IT Environment shall ensure the reliability of timestamps exported to the TOE.

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

5.1 TOE Security Functional Requirements

Table 1 - Functional Components of the TOE

CC Component	Name	Dependency
FAU_ARP.1(a)	Security Alarms **for Spam Detection**	FAU_SAA.1(a)
FAU_ARP.1(b)	Security Alarms **for Content Match**	FAU_SAA.1(b)
FAU_ARP.1(c)	Security Alarms **for Mail Policy Violation**	FAU_SAA.1(c)
FAU_ARP.1(d)	Security Alarms **for Encrypted Mail Policy Violation**	FAU_SAA.1(d)
FAU_ARP.1(e)	Security Alarms **for Email Attachment Policy Violation**	FAU_SAA.1(e)
FAU_GEN.1	Audit Data Generation	FPT_STM.1, satisfied in the environment
FAU_SAA.1(a)	Potential Violation **Analysis for Spam Detection**	FAU_GEN.1
FAU_SAA.1(b)	Potential Violation Analysis **for Content Match**	FAU_GEN.1
FAU_SAA.1(c)	Potential Violation Analysis **for Mail Policy**	FAU_GEN.1
FAU_SAA.1(d)	Potential Violation Analysis **for Encrypted Mail Policy**	FAU_GEN.1
FAU_SAA.1(e)	Potential Violation Analysis **for Email attachment policy Match**	FAU_GEN.1
FAU_SAR.1	Audit Review	FAU_GEN.1
FAU_SEL.1	Selective Audit	FAU_GEN.1 FAU_MTD.1
FIA_AFL.1	Authentication failure handling	FIA_UAU.1 (included as part of FIA_UAU.2)

FIA_UAU.2	User authentication before any action	FIA_UID.1 (included as part of FIA_UID.2)
FIA_UID.2	User identification before any action	None
FMT_MOF.1(a)	Management of Security Functions behavior	FMT_SMR.1
FMT_MOF.1(b)	Management of Security Functions behavior	FMT_SMR.1
FMT_MTD.1	Management of TSF data	FMT_SMR.1
FMT_SMF.1	Specification of Management Functions	None
FMT_SMR.1	Security Roles	FIA_UID.1 (included as part of FIA_UID.2)
FPT_RVM.1	Non-bypassability of the TSP	None

Table 1 lists the Security Functional Requirements and all functional dependencies associated with the components.

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* with the exception of italicised and/or bolded items listed in brackets and refinements indicated in bold. The bracketed items include either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces. Iterations are indicated with typical CC requirement naming followed by a letter in parenthesis for each iteration.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_ARP.1(a) Security Alarms for Spam Detection

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [**one of the following actions***:*

a) **Drop the message**.

b) **Deliver the original message but also send a copy to an alternate email address.**

c) **Forward the message to an alternate email address instead of the original recipient.**

d) **Add additional information to the message (subject and/or new X-header) to indicate a match.**

e) **Quarantine the message for a specified number of days into an administrator-specified quarantine area.**

f) **Reroute message to alternate IT device.**

And log the message.]

upon ~~detection of a potential security violation~~ **detecting that the email message qualifies as spam.**

Dependencies: FAU_SAA.1(a) Potential violation analysis **for Spam Detection**.

Application note: Alternate IT device would be a mail transfer agent or special "quarantine server".

5.1.1.2 FAU_ARP.1(b) Security Alarms for Content Match

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [**one of the following actions:**

a) **Drop the message.**

b) **Reroute the message to alternate IT device.**

c) **Quarantine the message for the specified number of days into an administrator-specified quarantine area.**

d) **Deliver the original message but also send a copy to an alternate email address.**

e) **Drop the attachment from the email.**

f) **Add information to the message subject to indicate a match for the given content.**

g) **Replace matched content with alternate text.**

And log the message and optionally notify an alternate recipient about the content match.]

upon detection ~~of a potential security violation~~ **of specific content in email messages or their attachments.**

Dependencies: FAU_SAA.1(b) Potential Violation Analysis **for Content Match**.

5.1.1.3 FAU_ARP.1(c) Security Alarms for Mail Policy Violation

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [**one of the following actions:**

a) **Drop the message.**

b) **Reroute the message to alternate IT device.**

c) **Quarantine the message for the specified number of days into an administrator-specified quarantine area.**

d) **Deliver the original message but also send a copy to an alternate email address.**

e) **Forward the message to an alternate email address instead of the original recipient.**

f) **Add information to the message subject to indicate a policy violation.**

And log the message and optionally notify an alternate recipient about the policy match.]

upon detection of a potential security violation **in mail policy.**

Dependencies: FAU_SAA.1(c) Potential Violation Analysis **for Mail Policy**.

5.1.1.4 FAU_ARP.1(d) Security Alarms for Encrypted Mail Policy Violation

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [**one of the following actions:**

a) **Drop the encrypted message.**

b) **Drop the plain message.**

c) **Allow the encrypted message.**

d) **Allow the plain message.**

e) **Quarantine the encrypted message for a specified number of days into an administrator-specified quarantine area.**

f) **Quarantine the message to alternate IT device.**

And log the message and optionally notify an alternate recipient about the policy match.]

upon detection of a potential security violation **in encrypted mail policy**.

Dependencies: FAU_SAA.1(d) Potential Violation Analysis **for Encrypted Mail Policy**.

5.1.1.5 FAU_ARP.1(e) Security Alarms for Email Attachment Policy Violation

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [**one of the following actions:**

a) **Drop the message.**

b) **Drop the attachment.**

c) **Rename the attachment.**

d) **Reroute the message to alternate IT device.**

e) **Quarantine the message for the specified number of days into an administrator-specified quarantine area.**

f) **Deliver the original message but also send a copy to an alternate email address.**

g) **Add information to the message subject to indicate a policy violation.**

And log the message and optionally notify an alternate recipient about the policy match.]

upon detection of a potential security violation **in mail policy.**

Dependencies: FAU_SAA.1(e) Potential Violation Analysis **for Email attachment Policy**.

5.1.1.6 **FAU_GEN.1** Audit Data Generation

Hierarchical to: No other components.

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

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

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

c) [**events listed in Table 2**].

Table 2 - Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents
FAU_ARP.1(a)	Actions taken due to detection of spam	Policy that was matched, message details
FAU_ARP.1(b)	Actions taken due to content match	Policy that was matched, message details
FAU_ARP.1(c)	Actions taken due to imminent security violations in mail policy	Policy that was matched, message details
FAU_ARP.1(d)	Actions taken due to imminent security violations in encrypted mail policy	Policy that was matched, message details
FAU_ARP.1(e)	Actions taken due to imminent security violations in Email Attachment policy.	Policy that was matched, message details
FAU_GEN.1	Startup and Shutdown of audit	None
FAU_SAA.1(a)	Enabling and disabling of the spam queue or individual spam tools	None
FAU_SAA.1(b)	Enabling and disabling of the content filtering queue or individual rules	None
FAU_SAA.1(c)	Enabling and disabling of the mail policy queue or	None

	individual rules	
FAU_SAA.1(d)	Enabling and disabling of the encrypted mail policy rules	None
FAU_SAA.1(e)	Enabling and disabling of the email attachment policy rules	None
FAU_SAR.1	None	None
FAU_SEL.1	All modifications to the Audit configuration while audit collection function is operating	None
FIA_AFL	Success and failure of authentication attempts.	None
FIA_UAU.2	User Authentication data	None
FIA_UID.2	User Identification data	None
FMT_MOF.1(a)	None	None
FMT_MOF.1(b)	None	None
FMT_MTD.1	None	None
FMT_SMF.1	Use of the management functions	None
FMT_SMR.1	Modification to the group of users that are part of a role	None
FPT_RVM.1	None	None

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**additional audit record contents specified in Table 2**].

Dependencies: FPT_STM.1 Reliable Time Stamps.

5.1.1.7 **FAU_SAA.1(a)** Potential Violation Analysis **for Spam Detection**

Hierarchical to: No other components.

FAU_SAA.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 TSP.

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

a) Accumulation or combination of [**the following events:**

i) **Messages explicitly identified as spam.**

ii) **Message headers containing a specific value in the given field.**

iii) **Unknown or inconsistent source or destination addresses for the message]**

known to indicate a potential security violation**;**

b) **[additional rules as follows:**

i) **Deny any messages determined to be spam based on it exceeding one or more predefined threshold values.**

ii) **Permit any message that is explicitly allowed to bypass the spam filtering component.**].

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.8 **FAU_SAA.1(b)** Potential Violation Analysis **for Content Match**

Hierarchical to: No other components.

FAU_SAA.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 TSP.

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

a) Accumulation or combination of [**the following events:**

i) **Presence of dirty or offensive words in messages.**

]

known to indicate a potential security violation;

b) [**additional rules as follows:**

i) **Permit any message that is explicitly allowed to bypass the content filtering component.**].

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.9 **FAU_SAA.1(c)** Potential Violation Analysis **for Mail Policy**

Hierarchical to: No other components.

FAU_SAA.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 TSP.

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

a) Accumulation or combination of [**the following events:**

i) **Messages sent by a specific user, group or domain.**

ii) **Messages destined to a specific user, group or domain.**

iii) **Messages containing specific text in the subject line.**

iv) **Messages with its size that violates configured thresholds.**]

known to indicate a potential security violation;

b) [**additional rules as follows:**

i) **Permit any message that is explicitly allowed to bypass the Mail Policy filtering component.**].

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.10 FAU_SAA.1(d) Potential Violation Analysis for Encrypted Mail Policy

Hierarchical to: No other components.

FAU_SAA.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 TSP.

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

a) Accumulation or combination of [**the following events:**

i) **Encrypted messages sent from a specific user, group or domain**

ii) **Encrypted messages destined to a specific user, group or domain**

iii) **Plain messages sent from a specific user, group or domain**

iv) **Plain messages destined to a specific user, group or domain**]

known to indicate a potential security violation;

b) [**additional rules as follows:**

i) **Permit any encrypted or plain message that is explicitly allowed to bypass the Mail Policy filtering component.**].

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.11 FAU_SAA.1(e) Potential Violation Analysis for Email attachment policy Match

Hierarchical to: No other components.

FAU_SAA.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 TSP.

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

a) Accumulation or combination of [**the following events:**

i) **Presence of specific attachment types in messages.**

ii) **Presence of specific attachment names in messages**]

known to indicate a potential security violation;

b) [**additional rules as follows:**

i) **Permit any message that is explicitly allowed to bypass the attachment filtering component.**].

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.12 **FAU_SAR.1** Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [**authorised administrators**] with the capability to read [**email usage and traffic patterns**] 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.

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.13 **FAU_SEL.1** Selective Audit

Hierarchical to: No other components.

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

a) [**event type**].

b) [**log level**].

Dependencies: FAU_GEN.1 Audit Data Generation,

FMT_MTD.1 Management of TSF Data.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 **FIA_AFL.1** Authentication Failure Handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [**five**] unsuccessful authentication attempts occur related to [**authorized administrator authentication**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**disable the account**].

Dependencies: FIA_UAU.1 Timing of Authentication.

5.1.2.2 **FIA_UAU.2** User Authentication before any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication.

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

Dependencies: FIA_UID.1 Timing of Identification.

5.1.2.3 **FIA_UID.2** User Identification before any Action

Hierarchical to: FIA_UID.1 Timing of Identification.

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

Dependencies: No dependencies.

5.1.3 Security Management (FMT)

5.1.3.1 **FMT_MOF.1(a)** Management of Security Functions Behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [***enable***] the functions [

a) **Spam Filter**

b) **Content Filter**

c) **Mail Policy Filter**

d) **Encrypted email policy filter**

e) **Email attachment policy filter**

to [**authorised administrators**].

Dependencies: FMT_SMR.1 Security Roles.

5.1.3.2 **FMT_MOF.1(b)** Management of Security Functions Behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable***] the functions [

a) **Spam Filter**

b) **Content Filter**

c) **Mail Policy Filter**

d) **Encrypted email policy filter**

e) **Email attachment policy filter**

to [**authorised administrators**].

Dependencies: FMT_SMR.1 Security Roles.

5.1.3.3 **FMT_MTD.1** Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [***perform operations as specified in Table 3*** [***and no other operation***]] the [**list of TOE data as specified in Table 3**] to [**authorised administrators**].

Dependencies: FMT_SMR.1 Security Roles.

Table 3 - Management of TOE data

Functional Component	**Operation**	**TOE Data**
FAU_ARP.1(a)	Modify	Action taken when spam is detected
FAU_ARP.1(b)	Modify	Action taken when specific content is matched
FAU_ARP.1(c)	Modify	Action taken when mail policy rules are matched
FAU_ARP.1(d)	Modify	Action taken when encrypted mail policy rules are matched
FAU_ARP.1(e)	Modify	Action taken when email attachment policy rules are matched
FAU_SAA.1(a)	Add, remove, modify Add, remove	Rules that identify spam Rules that allow bypass of the anti-spam feature
FAU_SAA.1(b)	Add, remove, modify Add, remove	Rules that match specific content Rules that allow bypass of the content filtering feature
FAU_SAA.1(c)	Add, remove, modify Add, remove	Rules that match specific mail policy rules Rules that allow bypass of

		the mail policy feature
FAU_SAA.1(d)	Add, remove, modify Add, remove	Rules that match specific encrypted mail policy rules Rules that allow bypass of the encrypted mail policy feature
FAU_SAA.1(e)	Add, remove, modify Add, remove	Rules that match specific email attachment policy rules Rules that allow bypass of the email attachment policy feature
FAU_SAR.1	Add, remove, modify	Group of users allowed to read audit records
FAU_SEL.1	Modify	Rights to view or change audit events
FIA_UAU.2 FIA_UID.2	Create, Modify	User identification and authentication data
FMT_MOF.1(a)	Add, remove, modify	Users that can interact with the TSF
FMT_MOF.1(b))	Add, remove, modify	Users that can interact with the TSF
FMT_MTD.1	Add, remove, modify	Users that can interact with the TSF data
FMT_SMR.1	Add, remove, modify	Users that are part of a role

5.1.3.4 **FMT_SMF.1** Specification of Management Functions

Hierarchical to: No other components.

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

a) **Add, remove and modify rules that identify messages that qualify as spam.**

b) **Add, remove and modify rules that identify inappropriate content in messages.**

c) **Add, remove and modify rules that identify mail policy violations.**

d) **Add, remove and modify rules that identify messages that violate the TOE's encryption policy for the given sender and receiver.**

e) **Add, remove and modify rules that identify Email attachment policy violations.**

f) **Add and remove rules that allow specific messages to bypass/whitelist any of the spam, content filtering, mail policy, encrypted mail policy or email attachment policy features.**

g) **Enable and Disable the Spam Filter, the Content Filter, the Mail Policy Filter, encrypted email policy filter and email attachment policy filter.**

h) **Select the action taken when rules for spam filtering, content filtering, mail policy, encrypted mail policy and email attachment policy are matched.**

i) **Add, remove and modify the users that are part of a role for viewing or modifying audited events and accessing TSF data and functions.**]

Dependencies: No Dependencies.

5.1.3.5 **FMT_SMR.1** Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [**super administrator**, **authorized administrators**].

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

Dependencies: FIA_UID.1 Timing of Identification.

5.1.4 Protection of the TSF (FPT)

5.1.4.1 **FPT_RVM.1** Non-Bypassability of the TSP

Hierarchical to: No other components.

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

Dependencies: No dependencies.

5.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarised in Table 4.

Table 4 - Assurance Requirements

Assurance Class	Component ID	Component Title	Dependencies
Configuration	ACM_CAP.2	Configuration Items	None

Assurance Class	Component ID	Component Title	Dependencies
Management			
Delivery and Operation	ADO_DEL.1	Delivery Procedures	None
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures	AGD_ADM.1
Development	ADV_FSP.1	Informal Functional Specification	ADV_RCR.1
Development	ADV_HLD.1	Descriptive High-Level Design	ADV_FSP.1, ADV_RCR.1
Development	ADV_RCR.1	Informal Correspondence Demonstration	None
Guidance Documents	AGD_ADM.1	Administrator Guidance	ADV_FSP.1
Guidance Documents	AGD_USR.1	User Guidance	ADV_FSP.1
Life Cycle Support	ALC_FLR.2	Flaw reporting procedures	None
Tests	ATE_COV.1	Evidence of Coverage	ADV_FSP.1, ATE_FUN.1
Tests	ATE_FUN.1	Functional Testing	None
Tests	ATE_IND.2	Independent Testing - Sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation	ADV_FSP.1, ADV_HLD.1
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

5.3 Strength of Function Claim of the TOE

The claimed minimum strength of function is SOF-basic.

The objectives defined in section 4 counter the threats in section 3.3 that arise from attackers with a low attack potential.

5.4 Security Requirements for the IT Environment

Table 5 - Functional Components of the IT Environment

CC Component	Name	Dependency
FCS_CKM.1	Cryptographic key generation	FCS_COP.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1, FMT_MSA.2
FCS_COP.1a – d	Cryptographic operation	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FMT_MSA.2	Secure security attributes	FMT_MSA.1, ADV_SPM.1
FAU_STG.1	Protected Audit Trail Storage	FAU_GEN.1
FPT_SEP.1	TSF Domain Separation	None
FPT_STM.1	Reliable Time Stamps	None

5.4.1 Security Audit (FAU)

5.4.1.1 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

FAU_STG.1.1 The ~~TSF~~ **IT Security Environment** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The ~~TSF~~ **IT Security Environment** shall be able to [***prevent***] unauthorised modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit Data Generation.

5.4.2 Cryptographic Support (FCS)

5.4.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The ~~TSF~~ **IT Environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA**] and specified cryptographic key sizes [**not specified**] that meet the following: [**ANSI X9.31**].

Dependencies: FCS_COP.1 Cryptographic operation, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

5.4.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The ~~TSF~~ **IT Environment** shall destroy cryptographic keys in accordance with a specified key destruction method [**zeroize**] that meets the following: [**US FIPS 140-2 key zeroize requirement**].

Dependencies: FCS_CKM.1 Cryptographic key generation, FMT_MSA.2 Secure security attributes.

5.4.2.3 FCS_COP.1a Cryptographic operation (AES encrypt / decrypt)

Hierarchical to: No other components.

FCS_COP.1a.1 The ~~TSF~~ **IT Environment** shall perform [**encrypt and decrypt**] in accordance with a specified cryptographic algorithm [**AES CBC mode**] and cryptographic key sizes [**256 bits**] that meet the following: [**FIPS 197**].

Dependencies: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

5.4.2.4 FCS_COP.1b Cryptographic operation (RSA signature / verification)

Hierarchical to: No other components.

FCS_COP.1b.1 The ~~TSF~~ **IT Environment** shall perform [**signature generation and signature verification**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**not specified**] that meet the following: [**ANSI X9.31**].

Dependencies: FCS_COP.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

5.4.2.5 FCS_COP.1c Cryptographic operation (SHA-1)

Hierarchical to: No other components.

FCS_COP.1c.1 The ~~TSF~~ **IT Environment** shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes [**not specified**] that meet the following: [**FIPS 180-2**].

Dependencies: FCS_COP.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

5.4.2.6 FCS_COP.1d Cryptographic operation (Random number generation)

Hierarchical to: No other components.

FCS_COP.1d.1 The ~~TSF~~ **IT Environment** shall perform [**Random number generation**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes [**not specified**] that meet the following: [**ANSI X9.31**].

Dependencies: FCS_COP.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

5.4.3 Security Management (FMT)

5.4.3.1 **FMT_MSA.2** Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1.1 The ~~TSF~~ **IT Environment** shall ensure that only secure values are accepted for security attributes.

Dependencies: FMT_MTD.1 Management of TSF data, ADV_SPM.1 Informal TOE security policy. Assurance requirement ADV_SPM.1 is a dependency to FMT_MSA.2, related to the cryptographic support (FCS) requirements included in the ST. The rationale for not including this dependency in the ST is CC Part 2 paragraph 1020 states that if the developer provided a clear definition of the secure values and the reason why they should be considered secure, the dependency from FMT_MSA.2 Secure security attributes to ADV_SPM.1 Informal TOE security policy model can be argued away. In the case of this TOE, there are no secure security values entered into the TOE; the IT Environment generates and destroys keys by zeroizing the generated key. No values are entered by the administrator, therefore this requirement is not applicable.

5.4.4 Protection of the TSF (FPT)

5.4.4.1 **FPT_SEP.1 TSF** Domain Separation

Hierarchical to: No other components.

FPT_SEP.1 The ~~TSF~~ **IT Security Environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

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

Dependencies: No dependencies.

5.4.4.2 **FPT_STM.1** Reliable Time Stamps

Hierarchical to: No other components.

FPT_STM.1.1 The ~~TSF~~ **IT Security Environment** shall be able to provide reliable time stamps for ~~its own~~ **the TOE's** use.

Dependencies: No dependencies.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

The TOE security functions are described below under the corresponding TOE component or component through which they are implemented:

6.1.1 SMTPI

SMTPI is the only external interface to receive email in the TOE. It accepts the email as per RFC 2821. It also evaluates all administrator configured whitelisting rules for the message and sets up processing order that the other queues follow.

6.1.2 Super Queue

Super Queue is the email processing engine of the TOE. It is tasked with handling all the sub-queues and acts as a facilitator for the message hand-off between the sub-queues. The sub-queues evaluate various administrator configured rules and handover the results to Super Queue which then is responsible for the final action (if any) on the message based on a pre-determined precedence rules among the actions.

6.1.2.1 Rip Queue

The Rip Queue is the first to process an email message. It is tasked to “rip” (or break down) the message into its constituent MIME parts. Messages that cannot be parsed can be configured to be either dropped or repackaged and sent to the original or an alternate email address or it can be further processes but with only a subset of TOE functionality. It is also responsible for document identification and text extraction from the attachments in a message.

6.1.2.2 Spam Queue

The Spam Queue inspects messages for characteristics of spam. When a message is found to be spam-like, an administrator-defined action such as drop quarantine or rename can be performed on it. It uses a multitude of identification mechanisms to score the message against each of these mechanisms. A correlation engine then digests the score and based on the confidence level assigned to each mechanism by the administrator, identifies the message as spam or ham.

6.1.2.3 Content Filtering Queue

The Content Filtering Queue is responsible for two basic functionalities of the TOE –

a) Inspect messages and attachments for the presence of inappropriate content using dictionary and regex searches.

b) Inspect the attachments of the message for any violations of Email attachment policy.

6.1.2.4 Mail Monitoring Queue

The Mail Monitoring Queue is responsible for two basic functionalities of the TOE –

a) Inspect messages for any violations of Mail policy. It is accomplished by monitoring messages over selection criteria such as the sender, recipient, size and subject information.

b) Inspect messages for any violations of encrypted mail policy. The TOE recognizes S/MIME and PGP encryption and filters encrypted mail based on the policy set for encryption.

6.1.2.5 Join Queue

The Join Queue is the last to process an email message. Its task is to reassemble the message back into a whole. If any of the intermediate sub-queues perform a message altering action, the Join Queue reassembles the message from the TOE-edited parts and sends it to the SMTPO for final delivery.

6.1.3 SMTPO

The SMTPO Service is responsible for delivering messages out of the TOE. It is the only means by which messages can be sent out of the network domain. It delivers email conforming to RFC 2821. Delivery can fail if there is a network error, if the receiving MTA is unreachable, if the receiving domain is invalid or if either the sender or recipient is refused. Multiple delivery attempts will be made if the receiving MTA is unreachable.

6.1.4 GUI Manager

The GUI Manager provides a web-based browser interface for the administrators to identify and authorise themselves to the TOE and to configure and maintain the TOE. Users may access the GUI Manager through a web browser by connecting to the IronMail® appliance's configured address using the secure HTTP (or HTTPS) protocol. The TOE provides a unified compliance manager through the GUI Manager. This allows administrators to define, monitor and enforce email policy across all email servers within the organization.

6.1.5 Logging

The Logging component provides auditing support for the TOE. The logging framework allows the administrator to control the output logs and configure them externally through customisable log levels and output mechanisms. The IT environment of the TOE, namely the operating system, stores and prevents modification to the audit records.

The TOE generates detailed logs of events generated by each one of its components. Important fields from the message and the rules that they match are saved in these log records. Activities of users who access the Web Administration interface are also recorded.

6.2 TOE Security Function Rationale

Table 6 demonstrates the correspondence between the security functional requirements identified in Sections 5.1 and the TOE security functions identified in Section 6.1.

Table 6 - Mappings Between TOE Security Functional Requirements and TOE Security Functions represented by the TOE components that provide these functions

	SMTPI	SPAM Queue	Content Filtering Queue	Mail Monitoring	SMTPO	GUI MANAGER	Logging
FAU_ARP.1 (a)		X					
FAU_ARP.1 (b)			X				
FAU_ARP.1 (c)				X			
FAU_ARP.1 (d)				X			
FAU_ARP.1 (e)			X				
FAU_GEN.1	X	X	X	X	X	X	X
FAU_SAA.1(a)		X					
FAU_SAA.1(b)			X				
FAU_SAA.1(c)				X			
FAU_SAA.1(d)				X			
FAU_SAA.1(e)			X				
FAU_SAR.1							X
FAU_SEL.1							X
FIA_AFL.1						X	
FIA_UAU.2						X	
FIA_UID.2						X	
FMT_MOF.1(a)						X	
FMT_MOF.1(b)						X	
FMT_MTD.1						X	
FMT_SMF.1						X	
FMT_SMR.1						X	
FPT_RVM.1	X				X		

The SMTPI ensures that every email message passes through the TOE before being forwarded to its destination by the SMTPO. The queuing architecture of the TOE ensures that no mail bypasses any filtering queue unless the TOE administrator explicitly configures it as such. The ability of the TOE to monitor and process every incoming mail helps satisfy FPT_RVM.1.

The SPAM Queue, Content Filtering Queue, and Mail Monitoring Queue automatically detects and respond to conditions that are met when the message contains specific data -- the Spam Queue detects spam, the Content Filtering Queue detects inappropriate or unwanted content and attachments in the message and the Mail Monitoring Queue detects monitored header information (sender, recipient, size or subject line content). In each case, the defined set of responses corresponds with the appropriate requirement.

The TOE provides integrated policy definition capability through the GUI Manager Interface. These components allow the authorised administrator to enable, disable and configure the different features, thus satisfying FMT_MOF.1(a) and FMT_MOF.1(b), manage the different authorised roles and their privileges for configuring TOE components, thus satisfying FMT_SMR.1, and configure the TSF data shown in Table 7 below. The ability to configure the above parameters helps satisfy requirements for FMT_SMF.1 and FMT_MTD.1.

Table 7 - Management of TOE data

Operation	TOE Data	Satisfies FMT_MTD.1 requirements for the following
Modify	Log level	FAU_SEL.1
Add, Delete	Whitelist rules	FAU_SAA.1(a), FAU_SAA.1(b), FAU_SAA.1(c), FAU_SAA.1(d), FAU_SAA(e)
Add, Remove, Modify	User Account data	FIA
Add, Remove, Modify	Envelope Analysis Rules	FAU_SAA.1(c), FAU_ARP.1(c)
Add, Remove, Modify	Encrypted Mail monitoring Rules	FAU_SAA.1(d), FAU_ARP.1(d)
Add, Remove, Modify	email attachment monitoring Rules	FAU_SAA.1(e), FAU_ARP.1(e)
Add, Remove, Modify	Spam Rules,	FAU_SAA.1(a), FAU_ARP.1(a)
Modify	Spam Confidence threshold, Enterprise Spam Trap addresses	FAU_SAA.1(a)
Add, remove, modify	Content Analysis Rules,	FAU_SAA.1(b), FAU_ARP.1(b)

Operation	TOE Data	Satisfies FMT_MTD.1 requirements for the following
Add, remove, modify	List of users assigned read or write privileges for configuring various TOE functionality	FAU_SAR.1, FMT_MOF.1(a), FMT_MOF.1(b), FMT_MTD.1, FMT_SMR.1

Logs are generated by every component of the system whenever some security relevant action is performed, which corresponds to the FAU_GEN.1 requirement. The Logging engine provides the ability to selectively view and generate events including all auditable events listed in Table 2, which satisfies FAU_SAR.1 and FAU_SEL.1 requirements. The log records are stored in the IT environment and only the authorised administrator is able to view or delete these records.

6.3 Assurance Measures

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented with ALC_FLR.2 from part 3 of the Common Criteria.

Table 8 demonstrates the correspondence between the security assurance requirements listed in Sections 5.2 to the developer evidence.

Table 8 - Assurance Correspondence

Component ID	Developer Evidence
ACM_CAP.2	Configuration Management Document
ADO_DEL.1	IronMail® Delivery Procedures
ADO_IGS.1	IronMail® Startup Guide
ADV_FSP.1	Functional Specification
ADV_HLD.1	High-Level Design Document
ADV_RCR.1	Representation Correspondence Document
AGD_ADM.1	IronMail® Administration Guide
AGD_USR.1	N/A, covered in AGD_ADM.1
ALC_FLR.2	IronMail® Flaw Remediation Procedures

Component ID	Developer Evidence
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Functional Test Procedures and Results
ATE_IND.2	Independent testing performed by Evaluation Lab
AVA_SOF.1	Strength of Function Analysis
AVA_VLA.1	Vulnerability Analysis

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 8

8. Rationale

Tables 9 and 10 demonstrate the correspondence between the security objectives listed in Sections 4.1 - 4.2 to the assumptions, threats and policies identified in Sections 3.2, 3.3 and 3.4.

8.1 Security Objectives Rationale

Table 9 - Correspondence between Assumptions, Threats and Policies to Objectives

Policies/Threats/ Assumptions	Objectives
A.DNS	O.E.TRUSTED_INFO
A.COMM_PROTECT	O.E.COMM_PROTECT
A.NO_EVIL_ADMIN	O.E.TRUSTED_ENV
A.PHYSICAL_SECURITY	O.E.TRUSTED_ENV
T.BYPASS	O.REF_MEDIATION
T.CONTENT	O.CONTENT_FILTER
T.NEW_EXPLOITS	O.CONFIGURABILITY
T.NO_AUDIT	O.LOG, O.E.TS_INTEGRITY, O.E.LOG
T.NO_REGULATE	O.MAIL_POLICY
T.OPAQUE	O.MAIL_POLICY
T.RESOURCE_CONSUME	O.SPAM_FILTER
T.UNTRUSTED_CODE	O.E.DOMAIN_SEP
T.BRUTE_FORCE	O.BOUNDED_AUTH
T.IA	O.AUTHENTICATION

Table 10 - Correspondence between Objectives and Assumptions, Threats and Policies

Objectives	Policies/Threats/ Assumptions
O.CONFIGURABILITY	T.NEW_EXPLOITS
O.CONTENT_FILTER	T.CONTENT
O.LOG	T.NO_AUDIT
O.MAIL_POLICY	T.OPAQUE, T.NO_REGULATE
O.REF_MEDIATION	T.BYPASS
O.SPAM_FILTER	T.RESOURCE_CONSUME

Objectives	Policies/Threats/ Assumptions
O.AUTHENTICATION	T.IA
O.BOUNDED_AUTH	T.BRUTE_FORCE
O.E.COMM_PROTECT	A.COMM_PROTECT
O.E.DOMAIN_SEP	T.UNTRUSTED_CODE
O.E.LOG	T.NO_AUDIT
O.E.TRUSTED_ENV	A.NO_EVIL_ADMIN, A.PHYSICAL_SECURITY
O.E.TRUSTED_INFO	A.DNS
O.E.TS_INTEGRITY	T.NO_AUDIT

8.1.1 Rationale for TOE Security Objectives

8.1.1.1 T.BRUTE_FORCE

A threat agent may attempt brute force attacks against the TOE authentication mechanism by repeatedly trying to guess authentication data for valid uses of the TOE. The TOE can counter T.BRUTE_FORCE by bounding the number of failed authentication attempts and take appropriate actions when this threshold is met, which is O.BOUNDED_AUTH.

8.1.1.2 T.BYPASS

T.BYPASS is the threat of a malicious entity bypassing one or more of the TOE's security functions in order send malicious data to the internal mail servers without the TOE detecting it. O.REF_MEDIATION ensures that every inbound our outbound mail that reaches the TOE, unless specifically allowed by the TOE administrator, must pass through each of its configured filters before being forwarded onto their respective destinations. The combination of the above objectives successfully counters T.BYPASS.

8.1.1.3 T.CONTENT

This is the threat of dirty, offensive, proprietary or otherwise inappropriate content being sent through the TOE. By implementing O.CONTENT_FILTER the TOE can take specific action on such messages, thus directly countering the above threat.

8.1.1.4 T.IA

T.IA is the threat of TOE compromise arising due to not doing any identification or authentication of users before giving them access to the TOE. It can be directly countered by O.AUTHENTICATION, which requires that the Authorized Administrator be identified and authenticated before being allowed to perform any TSF-mediated activities.

8.1.1.5 T.NEW_EXPLOITS

T.NEW_EXPLOITS is the threat where a malicious sender may modify the message content suitably or use variants in the sender or recipient information in order to defeat the protection services offered by the TOE. By implementing O.CONFIGURABILITY, the TOE administrator

can ensure that an up-to-date knowledge base of known malicious entities or variants in messages that constitute policy violations is installed on the TOE.

8.1.1.6 T.NO_AUDIT

T.NO_AUDIT is the threat of the TOE administrator not being able to detect compromise of the TOE due to lack of any accounting information. The above threat is countered by implementing O.LOG, which ensures that the TOE maintains a log of all the security-relevant operations performed on the TOE.

In order to be able to reliably correlate events there must be some temporal attribute or a timestamp associated with every audit record. The TOE environment must additionally implement O.E.TS_INTEGRITY to ensure that the timestamps used in the audit records are reliable.

The TOE environment must also implement O.E.LOG to ensure that the audit records are protected from unauthorized modification.

8.1.1.7 T.NO_REGULATE

This is the threat of an entity attempting to send content that the TOE may not want to receive, either because of its origin, destination, attachments, or subject content. This threat can be countered by implementing O.MAIL_POLICY, which allows the TOE to configure specific actions to be taken on incoming mail based on its sender, its recipient, its attachments, or its subject content.

8.1.1.8 T.OPAQUE

Inappropriate content such as proprietary information for an organization may be sent as encrypted data thus escaping detection by the content filter. This threat is countered by enforcing a policy that allows only specific users, groups or domains to send and receive encrypted information, which is covered by O.MAIL_POLICY.

8.1.1.9 T.RESOURCE_CONSUME

Spam is the primary cause for consumption of resources such as memory, bandwidth, processor time and data storage on the TOE. The TOE can counter T.RESOURCE_CONSUME by being able to define characteristics for identifying spam and take appropriate action when such characteristics are recognized, which is O.SPAM_FILTER.

8.1.1.10 T.UNTRUSTED_CODE

This is the threat that untrusted code could execute in the TOE and violate the integrity or availability of system assets. This threat can be countered by implementing O.E.DOMAIN_SEP which ensures that normal TOE operation can not be interfered with by an untrusted subject.

8.1.2 Rationale for IT Environment Security Objectives

8.1.2.1 A.DNS

O.E.TRUSTED_INFO ensures that the integrity of the information received by the TOE from trusted external components is never compromised. This addresses A.DNS, or the assumption that information received through DNS is reliable.

8.1.2.2 A.COMM_PROTECT

O.E.COMM_PROTECT ensures that communication to and from the TOE is protected from unauthorized disclosure or modification.

8.1.2.3 A.NO_EVIL_ADMIN

If O.E.TRUSTED_ENV is achieved then the TOE cannot be compromised by inside entities. This includes compromise by the administrators of the TOE who are then assumed to be are non-hostile and appropriately trained to use, configure and maintain the TOE, which is A.NO_EVIL_ADMIN.

8.1.2.4 A.PHYSICAL_SECURITY

If O.E.TRUSTED_ENV is achieved then the TOE cannot be physically compromised malicious entities. This includes the assumption that the TOE resides in a physically controlled access facility that cannot be physically compromised by unauthorized entities including malicious insiders, which is A.PHYSICAL_SECURITY.

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements Rationale for the TOE

Tables 11 and 12 demonstrate the correspondence between the security objectives listed in Sections 4.1 to the security functional requirements identified in Sections 5.1.

Table 11 - Mappings Between TOE Security Objectives and TOE Security Functional Requirements

Objectives	Requirements
O.AUTHENTICATION	FIA_UAU.2, FIA_UID.2
O.BOUNDED_AUTH	FIA_AFL.1, FIA_UAU.2
O.CONFIGURABILITY	FMT_MOF.1(a), FMT_MOF.1(b), FMT_MTD.1, FMT_SMR.1
O.CONTENT_FILTER	FAU_SAA.1(b), FAU_ARP.1(b)
O.LOG	FAU_GEN.1, FAU_SEL.1, FAU_SAR.1
O.MAIL_POLICY	FAU_ARP.1(c), FAU_SAA.1(c), FAU_ARP.1(d), FAU_SAA.1(d), FAU_ARP.1(e), FAU_SAA.1(e)
O.REF_MEDIATION	FPT_RVM.1
O.SPAM_FILTER	FAU_ARP.1(a), FAU_SAA.1(a),

Table 12 - Mappings Between TOE Security Functional Requirements and TOE Security Objectives

Requirements	Objectives
FAU_ARP.1(a)	O.SPAM_FILTER
FAU_ARP.1(b)	O.CONTENT_FILTER
FAU_ARP.1(c)	O.MAIL_POLICY
FAU_ARP.1(d)	O.MAIL_POLICY
FAU_ARP.1(e)	O.MAIL_POLICY
FAU_GEN.1	O.LOG
FAU_SAA.1(a)	O.SPAM_FILTER
FAU_SAA.1(b)	O.CONTENT_FILTER
FAU_SAA.1(c)	O.MAIL_POLICY
FAU_SAA.1(d)	O.MAIL_POLICY
FAU_SAA.1(e)	O.MAIL_POLICY
FAU_SAR.1	O.LOG
FAU_SEL.1	O.LOG
FIA_AFL.1	O.BOUNDED_AUTH
FIA_UAU.2	O.AUTHENTICATION
FIA_UID.2	O.AUTHENTICATION
FMT_MOF.1(a)	O.CONFIGURABILITY
FMT_MOF.1(b)	O.CONFIGURABILITY
FMT_MTD.1	O.CONFIGURABILITY
FMT_SMF.1	O.CONFIGURABILITY
FMT_SMR.1	O.CONFIGURABILITY
FPT_RVM.1	O.REF_MEDIATION

8.2.1.1 O.AUTHENTICATION

The identification and authentication requirements for O.AUTHENTICATION are implemented in the TOE by FIA_UAU.2 User authentication before any action, and FIA_UID.2 User identification before any action respectively.

8.2.1.2 O.BOUNDED_AUTH

O..BOUNDED_AUTH is implemented in the TOE by FIA_AFL.1 Authentication failure handling. The assignment in this component defines the action that the IT Security Environment

must take when a brute force attack at guessing passwords is made by a malicious entity. FIA_UAU.2 User Authentication before any action supports the above requirement by ensuring that the no action is allowed on behalf of the user before that user is authenticated.

8.2.1.3 O.CONFIGURABILITY

To implement O.CONFIGURABILITY, the TOE must provide administrative tools that allow the administrator to enable, disable, and configure specific functionality in the TOE. This objective is implemented in the TOE using the management components FMT_MOF.1(1) and FMT_MOF.1(2) Management of security functions behavior, and FMT_MTD.1 Management of TSF data. The assignments in these components list the specific functionality that can be enabled or disabled and the actions that can be taken for managing specific TOE data. The requirement FMT_SMR.1 Specification of management functions ensures that TOE provides these management functions to the administrators of the TOE.

8.2.1.4 O.CONTENT_FILTER

FAU_ARP.1(b) Security alarms for content match, and FAU_SAA.1(b) Potential violation analysis for content match, implement a detect-response mechanism in the TOE for detection of inappropriate content and/or content patterns in the email or its attachments. The assignments in these components list the types of events that indicate a match, including those events that are explicitly bypassed from this analysis and the appropriate action to be taken if such events are detected.

8.2.1.5 O.LOG

O.LOG is implemented in the TOE using relevant functional components from the audit family. FAU_GEN.1 Audit data generation, FAU_SEL.1 Selective audit, and FAU_SAR.1 Audit review ensure that audit records can be reliably and selectively generated and viewed, thus satisfying the objective O.LOG.

8.2.1.6 O.MAIL_POLICY

FAU_ARP.1(c), Security alarms for Mail Policy Violation, and FAU_SAA.1(c) Potential violation analysis for mail policy implement a detect-response mechanism in the TOE for detecting violation of TOE policy for mail sent from or received by specific users, groups or domains, or messages containing specific subject line content and content patterns. The assignments in these components list the types of events that indicate a match, including those events that are explicitly bypassed from this analysis and the appropriate action to be taken if such events are detected.

The detect-response mechanism provided by FAU_ARP.1(d), Security alarms for Encrypted Mail Policy Violation, and FAU_SAA.1(d) Potential violation analysis for encrypted mail policy, include the rules for accepting or denying encrypted mail sent from or received by specific users, groups or domains.

The detect-response mechanism provided by FAU_ARP.1(e), Security alarms for Email Attachment Policy Violation, and FAU_SAA.1(e) Potential violation analysis for email attachment policy, include the rules for accepting or denying mail based on attachment types and names.

8.2.1.7 O.REF_MEDIATION

O.REF_MEDIATION requires that inbound or outbound mail passing through the TOE unless explicitly bypassed, be examined by each of the TOE's configured filters before being forwarded to its destination. The component FPT_RVM.1 Non-bypassability of the TSP, directly implements this objective.

8.2.1.8 O.SPAM_FILTER

FAU_ARP.1(a) Security alarms for spam detection, and FAU_SAA.1(a) Potential violation analysis for spam detection, implement O.SPAM_FILTER as a detect-response mechanism in the TOE. The assignments in these components list the types of events that indicate the presence of spam, including those events that are explicitly bypassed from this analysis and the appropriate action to be taken if such events are detected.

8.2.2 Security Functional Requirements Rationale for the IT Environment

Tables 13 and 14 demonstrate the correspondence between the security objectives listed in Sections 4.2 to the security functional requirements identified in Sections 5.3.

Table 13 - Mappings Between IT Environment Security Objectives and IT Environment Security Functional Requirements

Objectives	Requirements
O.E.COMM_PROTECT	FCS_CKM.1, FCS_CKM.4, FCS_COP.1 (all iterations), FMT_MSA.2
O.E.TS_INTEGRITY	FPT_STM.1
O.E.DOMAIN_SEP	FPT_SEP.1
O.E.LOG	FAU_STG.1

Table 14 - Mappings Between IT Environment Security Functional Requirements and IT Environment Security Objectives

Requirements	Objectives
FAU_STG.1	O.E.LOG
FCS_CKM.1	O.E.COMM_PROTECT
FCS_CKM.4	O.E.COMM_PROTECT
FCS_COP.1 (all iterations)	O.E.COMM_PROTECT
FMT_MSA.2	O.E.COMM_PROTECT
FPT_SEP.1	O.E.DOMAIN_SEP
FPT_STM.1	O.E.TS_INTEGRITY

8.2.2.1 O.E.COMM_PROTECT

O.E.COMM_PROTECT is implemented in the IT environment by FCS_CKM.1, FCS_CKM.4, and all iterations of FCS_COP.1. The IT environment includes the OpenSSL cryptographic module, which provides support for communication via SSL. FMT_MSA.2, Secure security values, is a dependency of the FCS requirements and ensures that secure security values are provided to cryptographic functions.

8.2.2.2 O.E.DOMAIN_SEP

O.E.DOMAIN_SEP is implemented in the IT environment by FPT_SEP.1 TSF domain separation. The requirements of this component directly implement the objective.

8.2.2.3 O.E.TS_INTEGRITY

O.E.TS_INTEGRITY or the objective of enforcing reliable time stamps is implemented in the IT environment by FPT_STM.1 Reliable Time Stamps. The requirements directly implement the objective.

8.2.2.4 O.E.LOG

O.E.LOG is implemented in the IT environment by FAU_STG.1 which ensures that the audit records are stored and are protected from unauthorized deletion and modification.

8.2.3 Security Assurance Requirements Rationale

The rationale for the Security Assurance Requirements is defined in Chapter 6, Section 6.3.

8.2.4 Rationale for Satisfaction of Strength of Function Claim

SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." Because this ST identifies threat agents with low attack potential, the claimed minimum strength of function for the TOE is SOF-basic.

This SOF-basic claim also applies to the TOE's authentication mechanism which is based on user passwords.

8.3 TOE Summary Specification Rationale

The rationale for the TOE Summary Specification is defined in Chapter 6, Section 6.2.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.