Security Target: Symantec™ Mail Security 8300 Series Appliances Version 5.0

ST Version 1.6

August 20, 2007

Prepared For:

Symantec Corporation

20330 Stevens Creek Blvd.

Cupertino, CA 95014

www.symantec.com

Prepared By:

Apex Assurance Group, LLC

5448 Apex Peakway Drive, Ste. 101

Apex, NC 27502

www.apexassurance.com

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Symantec™ Mail Security 8300 Series Appliances Version 5.0. 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.

Document Revision History

REVISION	DATE	DESCRIPTION
1.0	October 25, 2006	Release to Symantec for review
1.1	November 2, 2006	Incorporate comments from Symantec
1.2	November 9, 2006	Incorporate comments from Symantec and submit to laboratory
1.3	January 15, 2007	Address initial round of verdicts
1.4	June 22, 2007	Include build number, resolve TBDs, minor revisions
1.5	July 13, 2007	Close verdicts
1.6	August 20, 2007	Update with certifier comments

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), conformance claims, Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

This section provides information necessary to identify and control this ST and its Target of Evaluation.

ST Title:	Security Target: Symantec™ Mail Security 8300 Series Appliances Version 5.0
ST Revision:	1.6
ST Publication Date:	August 20, 2007
TOE Identification:	Symantec™ Mail Security 8300 Series Appliances Version 5.0
Vendor:	Symantec Corporation
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.3 August 2005 (ISO/IEC 15408:2005).
Author:	Apex Assurance Group
Keywords:	Symantec™, anti-spam, anti-virus, security appliance

1.2 Overview

The TOE is Symantec™ Mail Security 8300 Series Appliances Version 5.0, which prevents unwanted emails from entering the network. Robust management and audit capabilities support advanced filtering of all incoming SMTP traffic for spam and viruses. Symantec™ Mail Security 8300 Series Appliances Version 5.0 may hereafter also be referred to as the 8300 Series Appliances or the TOE in this document.

1.3 CC Conformance Claim

The TOE is Common Criteria Version 2.3 Part 2 and Part 3 conformant at EAL2.

1.4 Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the Security Target
2	TOE Description	Defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
3	TOE Security Environment	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE and the TOE environment
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE
6	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.
7	PP Claims	Specifies Protection Profile conformance claims of the TOE
8	Rationale	Provides a rationale to demonstrate that the security objectives satisfy the threats; provides justifications of dependency analysis and strength of function issues

Table 1 – ST Organization and Description

1.5 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.3 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in paragraph 2.1.4 of Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by <u>*underlined italicized*</u> text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.6 Document Terminology

The following table provides a list of acronyms used within this document:

TERM	DEFINITION
CC	Common Criteria version 2.3 (ISO/IEC 15408:2005)
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MTA	Mail Transfer Agent
NTP	Network Time Protocol
OSP	Organizational Security Policy
SFR	Security Functional Requirement
SFP	Security Function Policy
SOF	Strength Of Function
SMS	Symantec™ Mail Security
SMTP	Simple Mail Transfer Protocol
SPF	Sender Policy Framework
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target Of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

Table 2 – Acronyms Used in Security Target

2 TOE Description

This section describes the Target of Evaluation (TOE), the provided security functionality (logical boundaries), and the physical TOE boundaries.

2.1 Overview and Mail Flow Summary

Symantec™ Mail Security 8300 Series appliances offer enterprises an easy-to-deploy, comprehensive gateway-based email security solution through the following:

- TCP-Layer Traffic Shaping – This feature analyzes email sources over time, classifying them as either legitimate or illegitimate. It slows the rate at which email leaves attackers' networks, thereby saving resources, reducing volume, and penalizing spammers.
- Email Firewall – This early response feature can vastly improve message throughput by analyzing incoming SMTP connections and enabling the end user to refuse connections or email messages from hosts it perceives to be hostile.
- Antispam technology – Symantec's state-of-the-art antispam filters assess and classify email as it enters the end user's site.
- Antivirus technology – Antivirus definitions and engines protect end users from email-borne viruses.
- Content Control – These features help administrators enforce corporate email policies, reduce legal liability, and ensure compliance with regulatory requirements.
- Group policies and filter policies – An easy-to-use authoring tool lets administrators create powerful and flexible ad hoc filters for individuals and groups.

The TOE provides high-performance, integrated mail protection against virus threats, spam, and other unwanted content at the earliest point of network entry, the Internet email (SMTP) gateway. As mail flows into mail servers, the TOE analyzes and filters mail using a variety of techniques, incorporating up-to-the-minute filters from Symantec Security Response. Along with standard methods such as heuristics and pattern matching, the TOE incorporates many proprietary filtering methods, such as advanced signature technologies and reputation-based source filters. Filters are continuously and automatically refreshed by Symantec Security Response to combat the latest spam and other email threats. Administrators can set up centralized policies to perform a variety of actions based on the verdict assigned to each message. For example, administrators can immediately delete spam identified by the TOE or choose to route spam to a central Web-based quarantine for a specific set of users.

2.2 Architecture Overview

The Symantec™ Mail Security 8300 Series appliances process a mail message as follows (the scenario discussed below assumes a sample message passes through the Filtering Engine to the Transformation Engine without being rejected):

- At the gateway, TCP-Layer Traffic Shaping checks the message's IP address to determine if it comes from a known source of spam or email-borne viruses.
- The incoming connection arrives at the inbound MTA via TCP/IP.
- Before accepting the connection, the inbound MTA sends the message's IP address to

the Email Firewall to check whether it is a known source of spam or email-borne viruses. If it is not, the inbound MTA accepts the connection and moves the message to its inbound queue.

- The Filtering Hub accepts a copy of the message for filtering.
- The Filtering Hub consults the LDAP Synchronization Service directory to expand the message's distribution list.
- The Filtering Engine determines each recipient's filtering policies.
- The Email Firewall checks the message's SMTP From field and IP address against Sender Group, Spam Attack, Directory Harvest Attack, and Virus Attack settings which the administrator configured via the Control Center. In addition, the message is checked against Blocked/Allowed Senders Lists defined by end users. The Email Firewall tries to authenticate the message using the Sender Policy Framework (SPF).
- Antivirus and configurable heuristic filters determine whether the message is infected.
- Content Compliance filters scan the message for restricted attachment types or words, as defined in configurable dictionaries.
- Antispam filters compare message elements with current filters published by Symantec Security Response to determine whether the message is spam. At this point, the message may also be checked against end-user defined Language settings.
- The Transformation Engine performs actions based on filtering results and configurable Group Policies.

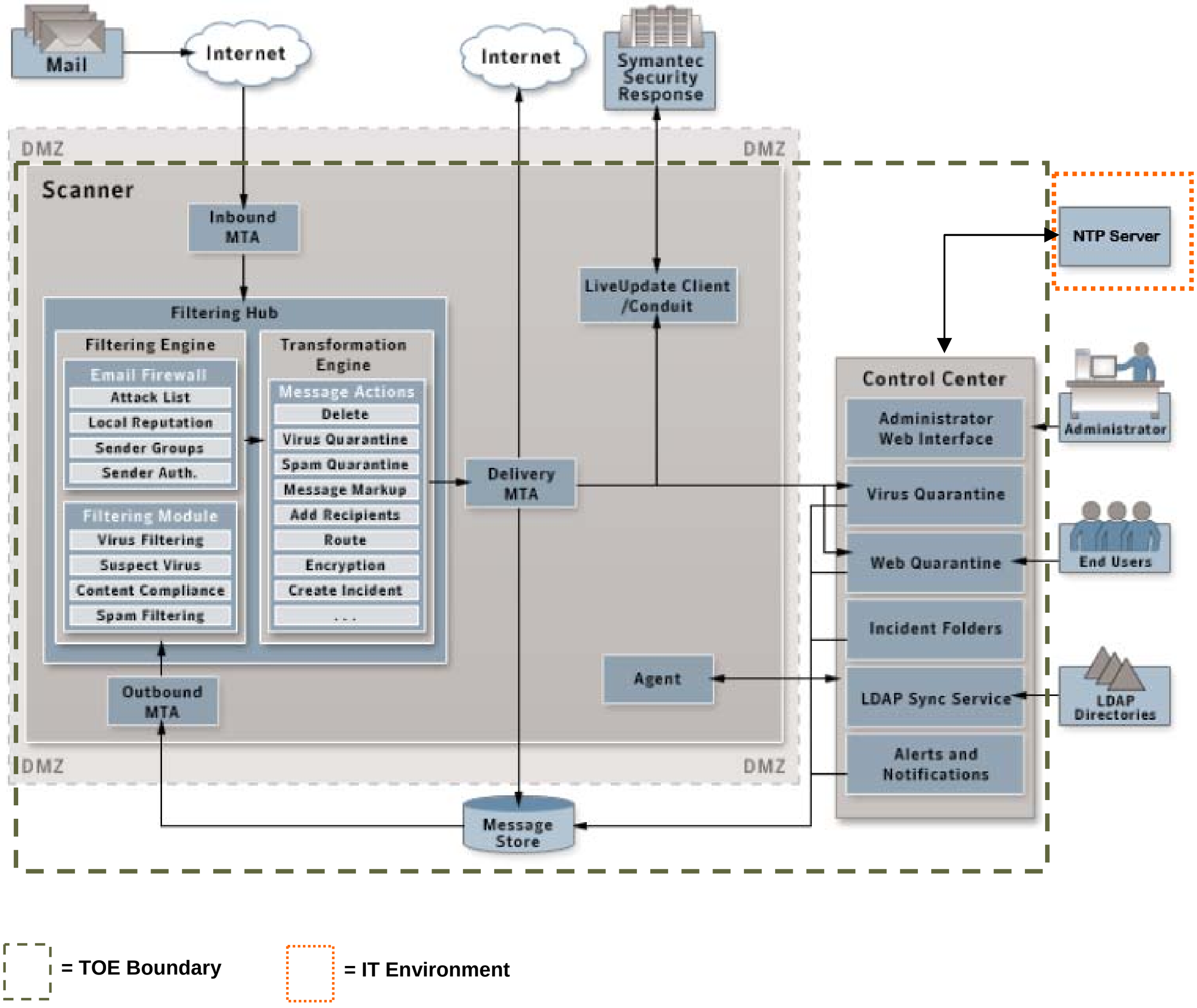

Figure 1 – Architecture Overview and TOE Boundaries

2.3 TOE Components

The TOE is Symantec™ Mail Security 8300 Series appliances, which are flexible units that can perform several different functions, depending on the size of the end user network and email processing needs. Each Symantec™ Mail Security 8300 Series appliance can act as a Scanner, a Control Center, or both. The TOE boundary is indicated with a dashed green line in Figure 1 and includes the components listed in the sections below.

2.3.1 Control Center

The Control Center enables Web-based configuration and administration of the TOE. With a single Control Center, the end user can centrally configure, monitor, and manage all the Scanners in the network. The Control Center also contains Quarantine, which is an optional storage area for caught spam.

Each TOE installation has exactly one Control Center. The Control Center communicates with the Agent on each Scanner. From the Control Center's Web-based graphical user interface[1], a TOE Administrator can:

- Configure, start and stop each Scanner.
- Specify email filtering options for groups of users or for all users at once.
- Monitor consolidated reports and logs for all Scanners.
- See summary information.
- Administer Quarantine.
- View online help for Control Center screens.

The Control Center subcomponents and functionality are described in Table 3 – Description of Components within the TOE Boundary.

2.3.2 Scanner

The Scanner component performs email filtering, and a TOE installation can have one or more Scanners. Each Scanner can reside on the same 8300 appliance as the Control Center component or on a separate appliance. The Scanner subcomponents and functionality are described in Table 3 – Description of Components within the TOE Boundary.

2.3.3 Subcomponent Descriptions

The table below provides a description of each subcomponent in the TOE boundary as referenced in Figure 1 – Architecture Overview and TOE Boundaries:

COMPONENT	DESCRIPTION
Inbound MTA	Receives inbound mail and forwards it to the Filtering Hub for processing.
Filtering Hub	Manages message filtering processes
Filtering Engine	Performs message filtering
Transformation Engine	Performs actions on messages
Outbound MTA	Receives outbound mail and forwards it to the Filtering Hub for processing.
Delivery MTA	Sends inbound and outbound messages that have already been filtered to their required destinations using the filtering results and the configuration settings for relaying inbound and outbound mail.
Live Update Client / Conduit	Retrieves new and updated filters from Symantec Security Response through secure HTTPS file transfer. Once retrieved, the Conduit authenticates filters, and then alerts the Filter Hub that new filters are to be received and implemented. Finally, the Conduit manages statistics for use by Symantec Security Response and for generating reports.

[1] The Administrator configures and manages the TOE with a workstation communicating with the TOE via SSL

COMPONENT	DESCRIPTION
Agent	Facilitates communicating configuration information between the Control Center and each Scanner.
Administrative Web Interface	Allows configuration as well as review of configuration settings and reports
Virus Quarantine	Holds messages suspected of containing viruses
Web Quarantine	Stores email messages separately from the normal message flow and allows access to those messages[2].
Incident Folders	Holds incident notifications
LDAP Synch Service	Provides automated synchronization between LDAP directory sources and Symantec Mail Security. Enables alias expansion, facilitates application of filtering policies to users and groups, and provides enhanced performance.
Alerts and Notifications	Sends email to the sender, recipients, or other email addresses when a specified condition is met (such as stripping .exe attachments). Also sends periodic email messages to users, providing a summary of their spam.
Message Store	Database in the Control Center that stores configuration information, logs, reports, and Quarantined messages (if using Quarantine).

Table 3 – Description of Components within the TOE Boundary

2.4 TOE Boundaries

2.4.1 Physical Boundaries

The TOE is a combined hardware/software TOE and is defined as the Symantec™ Mail Security 8300 Series Appliances Version 5.0. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Version 5.0.0-36
TOE Hardware	Symantec™ Mail Security 8380
	Symantec™ Mail Security 8360

Table 4 – Evaluated Configuration for the TOE

The Linux-based Operating System (Red Hat version 9.0 running Linux Kernel version 2.6.16) for each appliance is included as part of the TOE software and is installed when the appliance is provisioned. As such, the Operating System on the TOE hardware is included in the evaluation.

[2] The User accesses their quarantined messages with a workstation communicating with the TOE via SSL

2.4.2 Logical Boundaries

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

At a high level, the logical boundaries of the TOE are the functions of the TOE interfaces, including audit of security functions, authentication for the administrative functions, the management of the security configurations, controlling the flow of SMTP traffic, and the self-protection of the TOE itself.

2.4.2.1 Security Audit

The TOE provides spam reports and virus reports to provide the Administrator with insight on the filtering activity. Additionally, the TOE supports the provision of log data from each system component and supports the ability to notify an Administrator when a specific event is triggered.

2.4.2.2 User Data Protection

The spam detection, virus detection, monitoring, and managing capabilities of the TOE ensure that the information received by the network is free of potential risks.

2.4.2.3 Identification and Authentication

The TOE supports identity-based Identification and Authentication of an Operator. Operators authenticate via a Web-based GUI connected to the Control Center, and operators can assume a role of Administrator or Limited Administrator.

2.4.2.4 Security Management

The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to Security Audit, SMTP Information Flow Control, and Component Services. Administrators configure the TOE via web-based connection.

2.4.2.5 TSF Protection

The TOE provides various protection mechanisms for its security functions, including the enforcement of the information flow control policy and authentication rules at the applicable interfaces.

2.4.3 TOE Security Functional Policies

The TOE supports the following Security Functional Policies:

2.4.3.1 Administrative Access Control SFP

The TOE implements an access control SFP named *Administrative Access Control SFP*. This SFP determines and enforces the privileges associated with operator roles. An authorized administrator can define specific services available to administrators and users via the Control Center. The Administrator can also configure LDAP support, view/configure Syslog data, and backup/restore configurations via FTP. All administration takes place via Web-based HTTPS GUI connected to the TOE via SSL-protected session.

2.4.3.2 SMTP Information Flow Control SFP

The TOE implements an information process flow policy named *SMTP Information Flow Control SFP*. This SFP determines the procedures utilized to process information entering the TOE and the action taken when a security violation occurs. The security violations are defined as messages containing viruses or classified as spam. The actions taken at the occurrence of a violation is configurable by an authorized administrator via the Control Center.

3 TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply

3.1 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The assumptions are ordered into three groups: personnel, physical environment, and operational assumptions.

The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance. The following specific conditions are assumed to exist in an environment where the TOE is employed.

3.1.1 Personnel Assumptions

A.MANAGE Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.

A.NOEVIL Administrators of the TOE are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.1.2 Physical Environment Assumptions

A.LOCATE The processing platform on which the TOE resides is assumed to be located within a facility that provides controlled access.

3.1.3 Operational Assumptions

A.CONFIG The TOE is configured to handle all SMTP traffic flow.

A.TIMESOURCE The TOE has a trusted source for system time

3.2 Threats

The TOE or IT environment addresses the threats identified in the following sections.

3.2.1 Threats Addressed by the TOE

The TOE addresses the following threats:

T.ATTACK An attacker directs malicious network traffic against the network monitored by the TOE.

T.FALSEPOS An email message that contains virus or is classified as spam may not be flagged malicious or may not be reviewed by the intended recipient.

T.NOAUTH An unauthorized user may gain access to the TOE and alter the TOE configuration, causing malicious/unwanted traffic to enter the network.

T.NOPRIV An authorized user of the TOE exceeds his/her assigned security privileges resulting in the illegal modification of the TOE configuration and/or data.

3.2.2 Threats Addressed by Operating Environment

The TOE Operating Environment is not required to explicitly address any threats, although the TOE Operating Environment is constrained by the assumptions made above in the Assumptions section.

3.3 Organizational Security Policies

The organizational security policies relevant to the operation of the TOE are as follows:

P.INCOMING All incoming network traffic via SMTP shall be able to be monitored for malicious/undesired email.

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).

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

O.AUDIT The TOE shall record the necessary events to provide information on SMTP traffic and the results of the TOE’s detection/filtering functions.

O.DETECT The TOE shall be able to correctly detect emails classified as spam or containing viruses.

O.QUARANTINE The TOE shall establish a quarantine area for user review of messages flagged as spam or containing viruses.

O.SEC_ACCESS The TOE shall ensure that only those authorized users and applications are granted access to the security functions, configuration and associated data.

O.TOE_PROTECT The TOE operating system shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.

4.2 Security Objectives for the IT Environment

The IT security objectives for the IT environment are addressed below:

OE.TIME The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).

4.3 Security Objectives for the Non-IT Environment

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

ON.PERSONNEL Authorized administrators are non-hostile and follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any administrator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

ON.PHYSEC The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility.

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table. These security requirements are defined in Sections 5.1 - 5.4.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Data Generation
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
	FDP_ITC.1	Import of User Data Without Security Attributes
Identification and Authentication	FIA_UAU.2	User Authentication before Any Action
	FIA_UID.2	User Identification before Any Action
Security Management	FMT_MSA.1(1)	Management of Security Attributes
	FMT_MSA.1(2)	Management of Security Attributes
	FMT_MSA.3(1)	Static Attribute Initialization
	FMT_MSA.3(2)	Static Attribute Initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF Domain Separation

Table 5 – TOE Security Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are derived from Part 2 of the CC.

5.1.1 Security Audit (FAU)

5.1.1.1 *FAU_ARP.1 Security Alarms*

FAU_ARP.1.1 The TSF shall take [action to notify the administrator's designated personnel via email and generate an audit record] upon detection of a potential security violation.

5.1.1.2 *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 *not specified* level of audit; and

c) [Startup and shutdown of TOE services

d) System Status including

- Whether anti-virus or anti-spam filtering is enabled or disabled
- Whether Servers are accessible
- Whether the filters are current
- Quarantine disk space usage

e) Reports listed in Table 8 – Available Spam and Virus Reports

]

FAU_GEN.1.2 The TSF shall record within each audit record at last 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, [no other information].

5.1.1.3 *FAU_SAA.1 Potential Violation Analysis*

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 [detection of information process flow policy violation] known to indicate a potential security violation;

b) [No additional rules].

5.1.1.4 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all audit data generated within the TOE] 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.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [Administrative Access Control SFP] on [

Subjects: All users

Objects: System reports, component audit logs, Scanner/Controller configurations, operator account attributes

Operations: all user actions]

5.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following: [

Subjects: All users

Objects: System reports, component audit logs, Scanner/Controller configurations, operator account attributes

Operations: all user actions]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [See Table 6 – Management Actions and Available Services].

MANAGEMENT ACTIONS	AVAILABLE SERVICES
Full Administrative Privileges	Access to the Policies Tab Access to the Status Tab Access to the Reports Tab Access to the Compliance Tab Access to the Quarantine Tab Access to the Administration Tab Access to all links on the Settings Tab
Manage Quarantine	Access to the Quarantine Tab Access to the Administration Tab with the following links only • Administrators

MANAGEMENT ACTIONS	AVAILABLE SERVICES
	Access to the Settings Tab with the following links only: • LDAP • Quarantine
Manage Status and Logs	Access to the Status Tab Access to the Administration Tab with the following links only • Administrators Access to the Settings Tab with the following links only: • Hosts • Logs • LDAP
Manage Reports	Access to the Reports Tab Access to the Administration Tab with the following links only • Administrators Access to the Settings Tab with the following links only: • Reports
Manage Group Policies	Access to the Policies Tab Access to the Administration Tab with the following links only • Administrators

Table 6 – Management Actions and Available Services

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [no additional explicit denial rules].

5.1.2.3 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [SMTP Information Flow Control SFP] on [

Subjects: External IT entities attempting to send SMTP traffic through the TOE

Information: Mail messages to the internal network

Operations: Deliver, Delete, Quarantine, Forward]

5.1.2.4 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [SMTP Information Flow Control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes: IP Address, Allowed Senders List, Blocked Senders List

Information Security Attributes: Message structure type (i.e., virus, spam, mass-mailing worm)]

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

[Monitoring option is enabled for the service and information structure type and:

1. No malicious code is detected
2. Malicious code is detected and the following actions are configured:
    a. See Table 10 – Email Handling Verdicts and Available Actions

].

FDP_IFF.1.3 The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [no explicit authorization rules].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [no explicit denial rules].

5.1.2.5 FDP_ITC.1 Import of User Data Without Security Attributes

FDP_ITC.1.1 The TSF shall enforce the [SMTP Information Flow Control SFP] when importing user data, controlled under the SFP, from outside the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [no additional importation control rules].

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_UAU.2 User Authentication before Any Action

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.

5.1.3.2 FIA_UID.2 User Identification before Any Action

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.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MSA.1(1) Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [SMTP Information Flow Control SFP] to restrict the ability to *modify, delete*, **and** [filter] the security attributes [TSF data] to [Administrator].

5.1.4.2 FMT_MSA.1(2) Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to *modify* **and** *delete* the security attributes [Administrator accounts, Limited Administrator accounts, privileges for Limited Administrators] to [Administrator].

5.1.4.3 FMT_MSA.3(1) Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [SMTP Information Flow Control 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 [Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.4 FMT_MSA.3(2) Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Administrative Access Control 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 [Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.5 FMT_SMF.1 Specification of Management Functions

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

- [Create user accounts
- Modify user accounts
- Define privilege levels
- Export syslog data to external syslog server

- Backup or restore configurations via FTP
- Determine the behavior of the SMTP Information Flow Control SFP
- Modify the behavior of the SMTP Information Flow Control SFP].

5.1.4.6 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, Limited Administrator].

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

5.1.5.2 FPT_RVM.1 Non-bypassability of the TSP

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.

5.1.5.3 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF 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 shall enforce separation between the security domains of subjects in the TSC.

5.2 Security Functional Requirements for the IT Environment

5.2.1 Protection of the TSF (FPT)

5.2.1.1 FPT_STM.1 Reliable time stamps

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

5.3 Security Requirements for the Non-IT Environment

There are no security requirements for the non-IT environment.

5.4 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

ASSURANCE CLASS	ASSURANCE COMPONENTS	
Configuration Management	ACM_CAP.2	Configuration items
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 7 – Security Assurance Requirements at EAL2

6 TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 5.1 – TOE Security Functional Requirements. The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- User Data Protection
- Security Management
- TSF Protection

6.1.1 Security Audit

The TOE provides Spam Reports and Virus reports to provide the Administrator with insight on the filtering activity. Additionally, the TOE supports the provision of log data from each system component and supports the ability to notify an Administrator when a specific event is triggered.

6.1.1.1 Event-Based Reporting

The TOE generates audit data for various events, and this audit data is aggregated into a series of pre-defined reports. The Administrator can query the following reports:

REPORT TYPE	DATA DISPLAYED	REQUIRED REPORT DATA STORAGE OPTIONS (REPORTS SETTINGS PAGE)
Mail Summary	A summary of total mail.	None.
SPAM REPORTS		
Detection	A summary of total detected messages (spam, blocked, allowed and suspected spam messages). Also reports false positives.	None
Top Sender Domains	The domain names of the senders of detected messages.	Sender domains
Top Senders	The email addresses of the top senders of filtered messages.	Senders
Specific Senders	Detected messages filtered by specific	Senders

REPORT TYPE	DATA DISPLAYED	REQUIRED REPORT DATA STORAGE OPTIONS (REPORTS SETTINGS PAGE)
	senders.	
Top Sender HELO Domains*	Domain names of the SMTP HELO servers from which messages have been received.	Sender HELO domains
Top Sender IP Connections*	The top IP connections from which spam has been received.	Senders
Top Recipients Domains	The domain names of the recipients of detected messages.	Recipient Domains
Specific Recipients	The filtering activity for specific email addresses.	Recipients
Top Recipients	The email addresses of the top recipients of detected messages.	Recipients
VIRUS REPORTS		
Detection	A summary of total viruses and worms	None
Top Sender Domains	The domain names of the senders of viruses and worms.	Senders Sender domains
Top Senders	The email addresses of the top senders of viruses and worms.	Senders Sender domains
Specific Senders	Number of viruses and worms by specified senders	Senders Sender domains
Top Sender HELO Domains*	Domain names of the SMTP HELO servers from which viruses and worms have been received.	Sender HELO domains
Top Sender IP Connections*	The top IP connections from which viruses and worms have been received	Senders Sender domains
Top Recipients Domains	The domain names of the recipients of viruses and worms.	Recipient Domains
Specific Recipients	The filtering activity for specific email addresses.	Recipients
Top Recipients	The email addresses of the top recipients of viruses and worms.	Recipients

Table 8 – Available Spam and Virus Reports

* If running any Scanners in internal relay configurations, the `SMTP HELO` name or `IP connection address` could be the name or connection of the gateway machine, rather than the Internet address that might be expected.

The Administrator can filter reports via the following parameters:

- Time Range

  - Preset Range (i.e., Past Hour, Past Day, Past Week, and Past Month)
  - Customized range (i.e., Administrator enters Start and End Dates)
- Grouping (i.e., by Hour, Day, Week, or Month)

The TOE also supports robust system logging capability, including the following:

- System Status Summary
  - View at a glance how Symantec Anti-Spam is performing.
  - View the graphs for recent spam and virus filtering statistics.
  - View summary status about filters and enabled components.
- System Status
  - Whether anti-virus or anti-spam filtering is enabled or disabled
  - Whether Servers are accessible
  - Whether filters are current
  - Quarantine disk space usage

6.1.1.2 Component Logging

Each component of the TOE processes logging data[3], and the Administrator can designate the severity of errors to be written to the log files. The TOE provides five logging levels, with each successive level including all errors from the previous levels:

- Errors
- Warnings (the default)
- Notices
- Information
- Debug

6.1.1.3 Alerts and Notifications

The TOE can be configured to automatically send email alerts to Administrators when certain operating conditions arise. The conditions that generate alerts are the following:

[3] Logs can be viewed via the Web Interface available to the Administrator or via Syslog messages

ALERT SETTING	EXPLAINATION
Send From	The email address that will appear in the notification's `From:` header.
System detected *n* viruses in the past interval	An alert is sent because the system detects that the number of virus outbreaks occurring over a certain time period exceeds a set limit.
Spam filters are older than	An alert is sent because of the age of the spam filters. Spam filters update periodically, at different intervals for different types of filters.
Virus filters are older than	An alert is sent because of the age of the virus filters. Virus filter updates typically occur several times a week.
New virus filters are available	An alert is sent because new virus rules are available for download from Symantec Security Response. New virus rules are updated daily, and Rapid Response rules are updated hourly.
A message queue is larger than	An alert is sent when the size of a message queue exceeds the size specified next to the alert description. Message queues include Inbound, Outbound and Delivery. Queues can grow if the MTA has stopped, or if an undeliverable message is blocking a queue.
Available Spam Quarantine is less than	An alert is sent when the size of the Quarantine exceeds a certain number.
Available Content Compliance Folder is less than	An alert is sent when the size of the Content Compliance Folder exceeds a certain number.
LDAP Synchronization errors	An alert is sent because of LDAP synchronization errors. These errors are caused by problems in directory synchronization. Only messages that log at the error level cause alerts.
LDAP scanner replication errors	An alert is sent because of replication errors. These errors are caused by problems in the replication of LDAP data from the Control Center to attached and enabled Scanners. Only messages that log at the error level cause alerts.
Symantec Premium Content Control license expired	An alert is sent when the PCC license is approaching expiration. Another alert is sent when the license expires.
Symantec Antivirus license expired	An alert is sent when the antivirus license is approaching expiration. Another alert is sent when the license expires.
Symantec Antispam license expired	An alert is sent when the antispam license is approaching expiration. Another alert is sent when the license expires.
Software Updates license expired	An alert is sent when the software update license is approaching expiration. Another alert is sent when the license expires.
SSL/TLS certificate expiration warning	An alert is sent when a certificate expires. The first expiration warning is sent seven days prior to the expiration date. A second warning is sent one hour later. No more than two warnings per certificate are sent.
New software release update available	An alert is sent when a new software update release is available
A component is not responding or working	An alert is sent because of a non-responsive component. Relevant components include the Conduit, Filtering Hub, MTA, and LiveUpdate.
Hardware failures	An alert is sent due to fan or disk failure.
Service start after improper shutdown	An alert is sent because a service restarted after an improper shutdown.

ALERT SETTING	EXPLAINATION
Service shutdown	An alert is sent because a service was shut down normally.
Service start	An alert is sent because a service was started.
UPS status	Selecting the UPS status check box on the Alert Settings page generates a device alert that indicates the uninterruptible power supply status has changed. This alert can be potentially generated every 7 minutes.

Table 9 – Alert Settings and Descriptions

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_ARP.1
- FAU_GEN.1
- FAU_SAA.1
- FAU_SAR.1
- FPT_STM.1

6.1.2 User Data Protection

6.1.2.1 Information Process Flow

The spam detection, virus detection, monitoring, and managing capabilities of the TOE ensure that the information received by the network is free of potential risks. The TOE implements a policy for SMTP information flow control to enforce actions upon detection of undesired email messages, which may be spam or which may contain viruses. This policy is configured by the Administrator and supported by mechanisms within the TOE to identify such undesired email messages. Upon detection of such messages, the TOE will either delete them or move them to the Quarantine component for further review. Additionally, the TOE will notify an Administrator when certain events occur.

The following table maps the available actions[4] to the email handling verdicts:

ACTION	DESCRIPTION	VERDICT				
		Directory Harvest Attack	Virus Attack	Virus	Spam, Suspected Spam	Content Compliance

[4] Additional notes on filtering actions apply, including the capability to perform multiple actions for particular verdicts. For more details, please review the Symantec Mail Security Appliance Administration Guide.

Add a Header	Add an X-header to the message.	✓	✓	✓	✓	✓
Add annotation	Insert predefined text into the message (a disclaimer, for example).	✓	✓	✓	✓	✓
Add BCC recipients	Blind carbon copy the message to the designated SMTP address(es).	✓	✓	✓	✓	✓
Archive the message	Deliver the original message and forward a copy to the designated SMTP address, and, optionally, host.	✓	✓	✓	✓	✓
Clean the message	Delete unrepairable virus infections and repair repairable virus infections.			✓		
Create an incident	Create a record of a compliance or regulatory violation.					✓
Defer SMTP connection	Using a 4xx SMTP response code, tell the sending MTA to try again later.	✓	✓			
Delete the message	Delete the message.	✓	✓	✓	✓	✓
Deliver the message normally	Deliver the message. Viruses and mass-mailing worms are neither cleaned nor deleted.	✓	✓	✓	✓	✓
Deliver the message to the recipient's Spam folder	Deliver the message to end-user Spam folder(s). Requires use of the Symantec Spam Folder Agent for Exchange or the Symantec Spam Folder Agent for Domino.	✓	✓	✓	✓	✓
Deliver the message with TLS protocol	According to some regulatory requirements (HIPAA and GLBA) send an protected message containing sensitive data.					✓

Forward the message	Forward the message to designated SMTP address(es).	✓	✓	✓	✓	✓
Hold message in Spam Quarantine	Send the message to the Spam Quarantine.	✓	✓	✓	✓	✓
Hold message in Suspect Virus Quarantine	Hold the message in the Suspect Virus Quarantine for a configured number of hours (default is six hours), then re-filter using new virus definitions, if available. Only available for the suspicious attachment verdict.			✓		
Modify the Subject line	Add a tag to the message's `Subject:` line.	✓	✓	✓	✓	✓
Reject SMTP Connection	Using a 5xx SMTP response code, notify the sending MTA that the message is not accepted.	✓	✓			
Remove invalid recipients	If a directory harvest attack is taking place, remove each invalid recipient rather than sending a bounce message to the sender.	✓				
Route the message	Route the message using the designated SMTP host.	✓	✓	✓	✓	✓
Send a bounce message	Return the message to its `From:` address with a custom response, and deliver it to the recipient. Optionally, the original message can be included.	✓	✓	✓	✓	✓
Send notification	Deliver the original message and send a predefined notification to designated SMTP address(es) with or without attaching the original message.	✓	✓	✓	✓	✓

Strip and hold in Suspect Virus Quarantine	Remove all message attachments and hold the message in the Suspect Virus Quarantine for a configured number of hours (default is six hours). Then refilter, with new virus definitions, if available. Only available for the suspicious attachment verdict.			✓		
Strip Attachments	Remove all message attachments.			✓	✓	✓
Treat as blocked sender	Process the message using the action(s) specified in the domain-based Blocked Senders List. Applies even if the domain-based Blocked Senders List is disabled, and applies to inbound messages only.					✓
Treat as mass-mailing worm	Process the message using the action(s) specified in the associated worm policy. The message is delivered normally if the worm policy is disabled or does not apply because of message direction.					✓
Treat as an allowed sender	Process the message using the action(s) specified in the domain-based Allowed Senders List. Applies even if the domain-based Allowed Senders List is disabled, and applies to inbound messages only.					✓

Treat as a virus	Process the message using the action(s) specified in the associated virus policy. The message is delivered normally if the virus policy is disabled or does not apply because of message direction.					✓
Treat as spam	Process the message using the action(s) specified in the associated spam policy. The message is delivered normally if the spam policy is disabled or does not apply because of message direction.					✓
Treat as suspected spam	Process the message using the action(s) specified in the associated suspected spam policy. The message is delivered normally if the suspected spam policy is disabled or does not apply because of message direction.					✓

Table 10 – Email Handling Verdicts and Available Actions

The TOE supports the import of user data without security attributes. Imported user data includes virus definitions and spam filters that are imported from Symantec Security Response, a team of dedicated intrusion experts, security engineers, virus hunters, threat analysts, and global technical support teams that work in tandem to provide extensive coverage for enterprise businesses and consumers. User data is imported from Symantec Security Response via SSL session to the Live Update Client / Conduit in the Scanner component of the TOE.

6.1.2.2 Access Control

The TOE provides access control functionality to prevent unauthorized users from accessing reports, component logs, or component configuration details. The Administrator can create additional administrator accounts, granting each administrator the desired level of management privileges for different components of the TOE (e.g., an Administrator might want to delegate management of Quarantine to another administrator, who will only be able to modify Quarantine settings.). When granting limited privileges, the Administrator can assign any or all of the following management actions:

- Manage Quarantine
- Manage TOE Status and Component Logs

- Manage Reports
- Manage Group Policies

The User Data Protection function is designed to satisfy the following security functional requirements:

- FAU_ARP.1
- FDP_IFC.1
- FDP_IFF.1
- FDP_ITC.1
- FMT_MSA.1(1)
- FMT_MSA.3(1)

6.1.3 Identification and Authentication

The TOE enforces individual identification and authentication and provides a centralized authentication mechanism. Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE (whether those actions are reviewing reports/component logs, managing user accounts, or configuring TOE components). Identification and Authentication occurs via web-based management GUI interfacing with the Control Center component.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_UAU.2
- FIA_UID.2
- FMT_MSA.1(2)
- FMT_MSA.3(2)

6.1.4 Security Management

The functionality in the TOE requires management to ensure proper configuration control. These pieces of Security Management functionality are described in the following subsections:

6.1.4.1 Security Audit

A TOE Administrator can view system reports and specific component logs. The Administrator can further define lifespans for the storage of reports/logs and can view, print, save, schedule, and delete them as part of the Security Audit capabilities.

6.1.4.2 Information Process Flow

The Administrator configures the TOE components to meet the Security Objectives. IN addition to configuring the default policies for spam and virus detection, the Administrator can customize detection filters to:

- Specify Allowed and Blocked senders
- Adjust Spam scoring
- Enable language identification
- Adjust anti-virus settings
- Create custom filters (e.g., by message size, specific subject, etc.)

6.1.4.3 Access Control

The Administrator manages the creation and enforcement of different levels of access within the TOE, and each level of access has set of services available. The Administrator can define services available to various privilege levels/roles without granting full Administrator privileges.

6.1.4.4 Component Services

The Administrator can configure the TOE to support several services, including the Quarantine component and multiple Scanners. Typical managed services for these components include:

- Configuring Administrative access to Quarantine
- Setting the lifespan for messages in Quarantine retention
- Adding, testing, enabling, disabling, and deleting Scanners

The Security Management function is designed to satisfy the following security functional requirements:

- FDP_ACC.1
- FDP_ACF.1
- FMT_MSA.1(1)
- FMT_MSA.1(2)
- FMT_MSA.3(1)
- FMT_MSA.3(2)
- FMT_SMF.1
- FMT_SMR.1

6.1.5 TSF Protection

The TOE is integrated into a network, and all SMTP traffic flowing into the network must pass through the services provided by the TOE. Only an approved, authenticated Administrator can install, configure, and modify the TOE components (and all TOE Security Functions), which provides a protected domain for the TSFs.

The TOE can be implemented in a distributed manner, where one appliance running as a Control Center communicated with multiple appliances running as Scanners. In this case, communications between the Scanners and the Control center appliances are protected via SSL tunnel.

The TSF protection function is designed to satisfy the following security functional requirements:

- FPT_ITT.1
- FPT_RVM.1
- FPT_SEP.1

6.2 Security Assurance Measures

This section identifies the Configuration Management, Delivery/Operation, Development, Guidance Documents, Test, and Vulnerability Assessment measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
ACM_CAP.2	**CM_DOC**	**Configuration items: The implementation and documentation of procedures for the development of the TOE, including a configuration list of uniquely identified items.** **Evidence Title:** ***Configuration Management Processes and Procedures: Symantec™ Mail Security 8300 Series Appliances Version 5.0***
ADO_DEL.1	**DEL_DOC**	**Delivery procedures: The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner.** **Evidence Title:** ***Secure Delivery Processes and Procedures: Symantec™ Mail Security 8300 Series Appliances Version 5.0***
ADO_IGS.1	**IGS_DOC**	**Installation, generation, and start-up procedures: Documentation provided to the end users instructing the end users how to install and configure the TOE in a secure manner.** **Evidence Titles:** ***Symantec™ Mail Security Appliance Installation Guide*** ***Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Mail Security 8300 Series Appliances Version 5.0***
ADV_FSP.1	**FUN_SPEC**	**Informal functional specification: Functional Specification for the TOE describing the TSF and the TOE's external interfaces.** **Evidence Title:** ***Functional Specification: Symantec™ Mail Security 8300 Series Appliances Version 5.0***
ADV_HLD.1	**HLD_DOC**	**Descriptive high-level design: System Design for the TOE providing descriptions of the TSF structure in the form of subsystems and the functionality of each subsystem.** **Evidence Title:** ***High Level Design and Representation Correspondence Analysis: Symantec™ Mail Security 8300 Series Appliances Version 5.0***
ADV_RCR.1	**RCR_DOC**	**Informal correspondence demonstration: The documentation of the correspondence between the TSS,**

		FSP and HLD in specifically provided deliverables. Evidence Title: *High Level Design and Representation Correspondence Analysis: Symantec™ Mail Security 8300 Series Appliances Version 5.0*
AGD_ADM.1	ADMIN_GUIDE	Administrator guidance: Documentation provided to the customers instructing the customer how to configure the TOE in a secure manner. Evidence Title: *Symantec™ Mail Security Appliance Administration Guide* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Mail Security 8300 Series Appliances Version 5.0*
AGD_USR.1	USER_GUIDE	User guidance: Documentation provided to the customers instructing the users how to use the TOE. Evidence Title: *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Mail Security 8300 Series Appliances Version 5.0*
ATE_COV.1	TEST_COV	Evidence of coverage: Documented correspondence between the security functions and tests. Evidence Title: *Test Plan and Coverage Analysis: Symantec™ Mail Security 8300 Series Appliances Version 5.0*
ATE_FUN.1	TEST_DOC	Functional testing: The implementation and documentation of the test procedures including expected and actual results. Evidence Title: *Test Plan and Coverage Analysis: Symantec™ Mail Security 8300 Series Appliances Version 5.0*
AVA_SOF.1	SOF_DOC	Strength of TOE security function evaluation: The documentation for the Strength of Function Assessment. Evidence Title: *Security Target for Common Criteria Evaluation: Symantec™ Mail Security 8300 Series Appliances Version 5.0*
AVA_VLA.1	VLA_DOC	Developer vulnerability analysis: Vulnerability Assessment of the TOE and its deliverables is performed and documented to ensure that identified security flaws are

		countered. **Evidence Title:** ***Security Target for Common Criteria Evaluation: Symantec™ Mail Security 8300 Series Appliances Version 5.0***

Table 11 – Assurance Measures (EAL2)

7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

8 Rationale

8.1 Rationale for Security Objectives of the TOE, IT Environment, and Non-IT Environment

8.1.1 Summary Mapping of Security Objectives

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

OBJECTIVE THREATS/ ASSUMPTIONS	O.AUDIT	O.DETECT	O.QUARANTINE	O.SEC_ACCESS	O.TOE_PROTECT	OE.TIME	ON.PERSONNEL	ON.PHYSEC
ASSUMPTIONS								
A.MANAGE				✓			✓	
A.NOEVIL							✓	
A.LOCATE								✓
A.CONFIG		✓					✓	
A.TIMESOURCE						✓		
THREATS								
T.ATTACK	✓	✓						
T.FALSEPOS		✓	✓					
T.NOAUTH				✓	✓		✓	✓
T.NOPRIV				✓				
OSPs								
P.INCOMING	✓	✓				✓	✓	

Table 12 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

8.1.2 Rationale for Security Objectives of the TOE

A.MANAGE	This assumption is addressed by O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.

A.CONFIG

This assumption is addressed by O.DETECT, which ensures that the TOE will correctly detect emails classified as spam or containing viruses.

T.ATTACK

This threat is countered by the following:

- O.AUDIT, which ensures that the TOE monitors SMTP network traffic to allow the administrator to query detailed reports information (including spam and virus messages detected/filtered) and
- O.DETECT, which ensures that the TOE will correctly detect emails classified as spam or containing viruses.

T.FALSEPOS

This threat is countered by the following:

- O.DETECT, which ensures that the TOE will correctly detect emails classified as spam or containing viruses and
- O.QUARANTINE, which ensures that the TOE establishes a special area (known as a Quarantine area) for user review of messages flagged as spam or containing viruses.

T.NOAUTH

This threat is countered by the following:

- O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications and
- O.TOE_PROTECT, which provides mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.

T.NOPRIV

This threat is countered by O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.

P.INCOMING

This organizational security policy is enforced by the following:

- O.AUDIT, which ensures that the TOE monitors SMTP network traffic to allow the administrator to query detailed reports information (including spam and virus messages detected/filtered) and
- O.DETECT, which ensures that the TOE will correctly detect emails classified as spam or containing viruses

8.1.3 Rationale for Security Objectives of the IT Environment

The IT security objectives for the IT environment are addressed below:

A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.
P.INCOMING	OE.TIME provides support for enforcement of this policy by ensuring the provision of an accurate time source.

8.1.4 Rationale for Security Objectives of the Non-IT Environment

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

A.MANAGE	This assumption is addressed by ON.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.
A.NOEVIL	This assumption is addressed by ON.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.
A.CONFIG	This assumption is addressed by ON.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.
A.LOCATE	This assumption is addressed by ON.PHYSEC, which ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated.
T.NOAUTH	This threat is countered by the following: • ON.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security

aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.

- ON.PHYSEC, which ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated.

P.INCOMING ON.PERSONNEL provides support for the enforcement of this policy by ensuring that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.

8.2 Security Requirements Rationale

8.2.1 Summary of TOE Security Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE SFR	O.AUDIT	O.DETECT	O.QUARANTINE	O.SEC_ACCESS	O.TOE_PROTECT	OE.TIME
FAU_ARP.1	✓					
FAU_GEN.1	✓					
FAU_SAA.1	✓					
FAU_SAR.1	✓					
FDP_ACC.1				✓		
FDP_ACF.1				✓		
FDP_IFC.1		✓	✓			
FDP_IFF.1		✓	✓			

OBJECTIVE SFR	O.AUDIT	O.DETECT	O.QUARANTINE	O.SEC_ACCESS	O.TOE_PROTECT	OE.TIME
FDP_ITC.1		✓				
FIA_UAU.2	✓			✓		
FIA_UID.2	✓			✓		
FMT_MSA.1(1)		✓				
FMT_MSA.1(2)				✓		
FMT_MSA.3(1)		✓				
FMT_MSA.3(2)				✓		
FMT_SMF.1	✓	✓				
FMT_SMR.1		✓				
FPT_ITT.1					✓	
FPT_RVM.1		✓				
FPT_SEP.1		✓		✓	✓	
FPT_STM.1	✓					✓

Table 13 – Mapping of TOE Security Functional Requirements and Objectives

8.2.2 Sufficiency of Security Requirements

This section confirms that the security requirements are sufficient to satisfy the TOE security objectives, whether in a principal or supporting role.

OBJECTIVE	ARGUMENT TO SUPPORT SUFFICIENCY OF SECURITY REQUIREMENTS
O.AUDIT	The objective to ensure that the TOE monitors SMTP network traffic to allow the administrator to query detailed reports information (including spam and virus messages detected/filtered) is met by the following security requirements: • FAU_ARP.1 provides a notification capability, which is utility to keep the administrator updated on SFP violations. • FAU_GEN.1, FAU_SAA.1, and FAU_SAR.1 defines the auditing capability for SMTP information flow and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • FIA_UAU.2 and FIA_UID.2 require the TOE to enforce identification and

OBJECTIVE	ARGUMENT TO SUPPORT SUFFICIENCY OF SECURITY REQUIREMENTS
	authentication of all users • FMT_SMF.1 supports the security management functions relevant to the TOE, including the configuration of SMTP information flow control and user monitoring parameters • FPT_STM.1 requires the provision of reliable time stamps that can be associated with security-relevant events
O.DETECT	The objective to ensure that the TOE will correctly detect emails classified as spam or containing viruses is met by the following security requirements: • FDP_IFC.1, FDP_IFF.1 defines the SFP that ensures that all inbound information is analyzed for SFP violations and that appropriate action is taken. • FDP_ITC.1 allows the import of user data from outside the TSC (such as spam filters and virus definitions from Symantec Security Response) to help ensure the latest threats are detected. • FMT_MSA.1(1) restricts the ability to modify, delete, or filter incoming SMTP traffic to an authorized administrator • FMT_MSA.3(1) ensures that the default values of security attributes are restrictive in nature and enforce specification of initial configuration parameters to the Administrator • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role • FPT_RVM.1 ensures that the TOE is not bypassed (all SMTP information flows through the TOE) • FPT_SEP.1 ensures that the a separate execution domain is maintained by the TOE to avoid intentional (or otherwise) tampering with the TOE security functions and configuration data by un-trusted agents
O.QUARANTINE	The objective to ensure that the TOE establishes a special area for user review of messages flagged as spam or containing viruses is met by the following security requirements: • FDP_IFC.1, FDP_IFF.1 defines the SFP that ensures that all inbound information is analyzed for SFP violations and that appropriate action is taken.
O.SEC_ACCESS	This objective ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user privilege level and their allowable actions • FIA_UAU.2 and FIA_UID.2 require the TOE to enforce identification and authentication of all users prior to configuration of the TOE • FMT_MSA.1(2) specifies that only privileged administrators can access the TOE security functions and related configuration data

OBJECTIVE	ARGUMENT TO SUPPORT SUFFICIENCY OF SECURITY REQUIREMENTS
	• FMT_MSA.3(2) ensures that the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE • FPT_SEP.1 ensures that a separate execution domain is maintained by the TOE to help prevent unauthorized access to the TOE
O.TOE_PROTECT	The objective to ensure that the TOE provides mechanisms to isolate the TOE Security Functions (TSF) and assures that TSF components cannot be tampered with or bypassed is met by the following: • FPT_ITT.1 ensures that communications between TOE components in a distributed environment are protected via SSL tunnel. • FPT_SEP.1 ensures that the TOE is protected from untrusted processes that could attempt to tamper with or bypass the TOE.
OE.TIME	The objective to ensure that the TOE operating environment provides an accurate timestamp is met by the following: • FPT_STM.1 requires the provision of reliable time stamps that can be associated with security-relevant events
ON.PERSONNEL	The objective to ensure that authorized administrators are non-hostile and follow all administrator guidance and that the TOE is delivered, installed, managed, and operated in a secure manner is met by the following: • A.MANAGE assumes Administrators of the TOE are appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner. • A.NOEVIL assumes the Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. • A.LOCATE assumes the processing platform on which the TOE resides is assumed to be located within a facility that provides controlled access.
ON.PHYSEC	The objective to ensure that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility is met by the following: • A.LOCATE assumes the processing platform on which the TOE resides is assumed to be located within a facility that provides controlled access.

Table 14 – Sufficiency of Security Requirements

8.3 TOE Summary Specification Rationale

The following table provides a mapping of Security Functional Requirements to IT Security Functions:

IT SECURITY FUNCTION / SFR	SECURITY AUDIT	IDENTIFICATION AND AUTHENTICATION	USER DATA PROTECTION	SECURITY MANAGEMENT	TSF PROTECTION
FAU_ARP.1	✓		✓		
FAU_GEN.1	✓				
FAU_SAA.1	✓				
FAU_SAR.1	✓				
FDP_ACC.1				✓	
FDP_ACF.1				✓	
FDP_IFC.1			✓		
FDP_IFF.1			✓		
FDP_ITC.1			✓		
FIA_UAU.2		✓			
FIA_UID.2		✓			
FMT_MSA.1(1)			✓	✓	
FMT_MSA.1(2)		✓		✓	
FMT_MSA.3(1)			✓	✓	
FMT_MSA.3(2)		✓		✓	
FMT_SMF.1				✓	
FMT_SMR.1				✓	
FPT_ITT.1					✓
FPT_RVM.1					✓
FPT_SEP.1					✓
FPT_STM.1	✓				

Table 15 – Mapping of Security Functional Requirements to IT Security Functions

8.3.1 Sufficiency of IT Security Functions

This section provides appropriate justification that the IT Security Functions are suitable to meet the TOE Security Functional Requirement and that when implemented, contributes to meeting that requirement.

SFR	RATIONALE TO SUPPORT SUFFICIENCY OF SECURITY FUNCTION
FAU_ARP.1	This TOE SFR is satisfied by the Security Audit functions and the User Data Protection functions. The TOE provides a method of alerting the select personnel of the occurrence of the policy violation and the actions taken. It then records the incident in an audit log. The notification is triggered by the user protection function that invokes the information process flow policy.
FAU_GEN.1	This TOE SFR is satisfied by the Security Audit function, which generates audit logs from the audit of a variety of security events.
FAU_SAA.1	This TOE SFR is satisfied by the Security Audit function, which provides the authorized administrator with the ability to review the number of violation occurrences via reviews of audit logs. The log viewing utility provides the total number of violations per service type and per date.
FAU_SAR.1	This TOE SFR is satisfied by the Security Audit function by enabling only authorized users to review and query the audit logs based on the certain criteria.
FDP_ACC.1	This TOE SFR is satisfied by the Security Management function, which permits each user to be assigned a privilege level and the respective privileges for that level.
FDP_ACF.1	This TOE SFR is satisfied by the Security Management function by permitting TOE access based on the privileges assigned a specific privilege level.
FDP_IFC.1	This TOE SFR is satisfied by the User Data Protection function, which utilizes the information process flow policy to monitor and process the information entering the system. The policy encourages the analysis of the information for potential violations and takes appropriate steps to rectify the presence of a violation, based on the administrator configuration.
FDP_IFF.1	This TOE SFR is satisfied by the User Data Protection function, which utilizes the information process flow policy to monitor and process the information entering the system. The policy encourages the analysis of the information for potential violations and takes appropriate steps to rectify the presence of a violation, based on the administrator configuration.
FDP_ITC.1	This TOE SFR is satisfied by the User Data Protection function, which utilizes the information process flow policy to monitor and process the information entering the system. The policy allows the import of user data from outside the TSC (in this case, spam filters and virus definitions from Symantec Security Response) to help ensure the latest threats are detected.
FIA_UAU.2	This TOE SFR is satisfied by the Identification and Authentication security function by requiring users to successfully authenticate themselves using a unique identifier and password prior to performing any action on the TOE.
FIA_UID.2	This TOE SFR is satisfied by the Identification and Authentication security function by requiring users to successfully identify themselves using a unique identifier.
FMT_MSA.1(1)	This TOE SFR is satisfied by Security Management and User Data Protection function, which provides the TOE Administrator with full authority to configure the TOE to uphold SMTP information flow control policies.
FMT_MSA.1(2)	This TOE SFR is satisfied by Security Management and Identification and Authentication functions, which provides the TOE Administrator with full authority and ability to define user groups and their privileges. These security functions also provide complete control (via configuration) over the security functions of the TOE.
FMT_MSA.3(1)	This TOE SFR is satisfied by Security Management and User Data Protection functions, which allow the TOE Administrator to change default settings for how the

SFR	RATIONALE TO SUPPORT SUFFICIENCY OF SECURITY FUNCTION
	TOE enforces the SMTP information flow controls.
FMT_MSA.3(2)	This TOE SFR is satisfied by Security Management and Identification and Authentication functions, which allow the TOE Administrator to change default settings for each user and privilege level.
FMT_SMF.1	This TOE SFR is satisfied by Security Management function by providing the TOE Administrator the capability to enable, and disable the information process flow policy, select the actions that would be taken upon the violation of the policy and select the method and type of notification of violations. It provides the capability for the administrator to select the type of information structure with respect to selected services to be monitored and processed, and the ability to install and configure the TOE services to ensure that the information entering the system is subjected to the information process flow policy. The Security Management function also provides the capability to modify user accounts and privilege levels.
FMT_SMR.1	This TOE SFR is satisfied by Security Management function, which assigns each user to the role of Administrator or Limited Administrator, the latter of which has a subset of Administrator services. These subset services are defined by the Administrator at the time the account is created.
FPT_ITT.1	This TOE SFR is satisfied by the TSF Protection security functions by ensuring that communications between a Control Center and a Scanner in a distributed implementation are protected with SSL protocol.
FPT_RVM.1	This TOE SFR is satisfied by the TSF Protection security functions by ensuring that all information traffic is subjected to the information process flow policy.
FPT_SEP.1	The TOE provides protection mechanisms for its security functions, such as the restricted ability that only TOE Administrators can perform administrative actions on the TOE.
FPT_STM.1	This IT Environment SFR is satisfied by the TOE’s connection to an NTP server to ensure that each audited event contains a date and time stamp for that event.

Table 16 – Sufficiency of IT Security Functions

8.4 Rationale for Explicitly Stated Security Requirements

The TOE does not support any explicitly stated security requirements; therefore, this section does not apply.

8.5 Rationale for IT Security Requirement Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_ARP.1	No other components.	FAU_SAA.1	Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_SAA.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components.	FDP_ACC.1	Satisfied
		FMT_MSA.3	Satisfied by FMT_MSA.3(2)
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components.	FDP_IFC.1	Satisfied
		FMT_MSA.3	Satisfied by FMT_MSA.3(1)
FDP_ITC.1	No other components	FDP_IFC.1	Satisfied
		FMT_MSA.3	Satisfied by FMT_MSA.3(1)s
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FIA_UID.2	FIA_UID.1	None	Not applicable
FMT_MSA.1(1)	No other components.	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	Satisfied
FMT_MSA.1(2)	No other components.	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Satisfied
FMT_MSA.3(1)	No other components.	FMT_SMR.1	Satisfied
		FMT_MSA.1	Satisfied by FMT_MSA.1(1)
FMT_MSA.3(2)	No other components.	FMT_SMR.1	Satisfied
		FMT_MSA.1	Satisfied by FMT_MSA.1(2)
FMT_SMF.1	No other components.	None	Not applicable
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FPT_ITT.1	No other components	None	Not applicable
FPT_RVM.1	No other components.	None	Not applicable
FPT_SEP.1	No other components.	None	Not applicable
FPT_STM.1	No other components.	None	Not applicable

Table 17 – TOE SFR Dependency Rationale

8.6 Rationale for Strength of Function Claim

The TOE is targeted at a generalized IT environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a low attack potential. As such, minimum and explicit strength of function claims is "SOF-basic" which is appropriate for the intended environment. Note that the only applicable mechanisms (i.e., those that are probabilistic or permutational yet not cryptographic) are related to the identification and authentication security function and specifically to the following security functional requirements: FIA_UAU.2, FIA_UID.2.

8.7 Rationale for Security Assurance

The assurance documentation listed in Table 11 – Assurance Measures (EAL2) meets the developer action and content and presentation of evidence elements for each assurance requirement defined in the CC. EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.8 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles