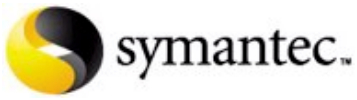


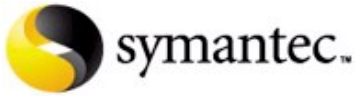
Security Target

Symantec Brightmail™ Gateway 9.0.1

Document Version 1.4

December 23, 2010

Prepared For:



Symantec Corporation

350 Ellis Street

Mountain View, CA 94043

www.symantec.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Brightmail™ Gateway 9.0.1. 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.

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 ST Reference

ST Title	Security Target: Symantec Brightmail™ Gateway 9.0.1
ST Revision	1.4
ST Publication Date	December 23, 2010
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Symantec Brightmail™ Gateway 9.0.1

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 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 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 and a change in text color, 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 *underlined italicized* 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, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

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

1.5 Document Terminology

The following table[1] describes the terms and acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria version 3.1 (ISO/IEC 15408)
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

[1] Derived from the IDSPP

TERM	DEFINITION
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 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

The TOE is Brightmail™ Gateway 9.0.1, which prevents unwanted email and IM messages from entering a customer's network. Robust management and audit capabilities support advanced filtering of all incoming SMTP and IM traffic for spam and viruses. Brightmail™ Gateway 9.0.1 may hereafter also be referred to as the 8300 Series Appliances, Brightmail Gateway, Brightmail Gateway Virtual Edition, or the TOE in this document.

1.7 TOE Description

1.7.1 Overview and Mail Flow Summary

Symantec™ Brightmail Gateway Series appliances and Brightmail Gateway Virtual Edition offer enterprises a comprehensive gateway-based message-security solution. Symantec Brightmail Gateway provides a solution that integrates email security and IM security capabilities in one appliance. Symantec Brightmail Gateway does the following to protect the customer environment:

- Detects spam, denial-of-service attacks, and other inbound email threats.
- Leverages a global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections.
- Secures and protects public instant messaging communications with the same management console that it uses to secure and protect email.
- Obtains visibility into messaging trends and events with minimal administrative burden.

As mail and instant messaging traffic flow into the customer network, the TOE analyzes and filters the traffic 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 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.

1.7.2 TOE Functionality Overview

The TOE processes a mail message as follows:

1. At the gateway, Connection Classification classifies the sending IP address into one of 9 classes based on local reputation. It either accepts or defers the connection based on class membership. New senders are placed in a tenth, default class. Symantec Brightmail Gateway also checks the IP address to determine if it belongs to a good sender group or bad sender group. It then blocks or permits the connection accordingly.

2. Before the gateway accepts the message, it checks the domain address and email address. The gateway determines if the message belongs to the Local Good Sender Domains or Local Bad Sender Domains groups. If the message belongs to either, the gateway applies the configured action to the message. If appropriate, the gateway moves the message to its inbound queue.

3. The Brightmail Gateway consults the LDAP SyncService directory to expand the message's distribution list.

4. The Brightmail Gateway determines each recipient's filtering policies.

5. Antivirus filters determine whether the message is infected.

6. Content filtering policy filters scan the message for restricted attachment types or words, as defined in configurable dictionaries.

7. If the sending IP address is granted a pass by Fastpass, antispam filtering is bypassed. If not, the antispam filters that use the latest rules from Symantec Security Response determine whether the message is spam. The message may also be checked against user-defined Language settings.

8. The gateway performs actions according to filtering results and configurable policies and applies them to each recipient's message based on group membership.

The TOE processes IM messages as follows:

1. IM traffic enters the customer network and is redirected to the IM proxy by enterprise DNS servers.

2. The IM proxy filters IM traffic according to customer settings and compares the traffic with the current filters Symantec Security Response publishes. These filters determine whether a message is spim or contains a virus. If a message is determined to contain spim or a virus, the traffic can be blocked.

3. The IM traffic reaches the internal user's IM client.

4. If customers have enabled outbound IM filtering, outbound messages are routed through the IM proxy before they are sent to an external user's IM client.

1.7.3 Physical Boundary

The TOE is a software TOE and is defined as the Brightmail™ Gateway 9.0.1. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Brightmail™ Gateway 9.0.1
IT Environment	For Virtual Edition: general purpose server workstation running VMware ESX Server Version 3.5 and meeting the requirements specified in Table 4 – Hardware and Software Requirements for the SBG Virtual Edition For the appliances: 8380, 8360, 8340 appliances running a customized version of Linux with kernel version 2.6.28

Table 3 – Evaluated Configuration for the TOE

The TOE boundary is shown below:

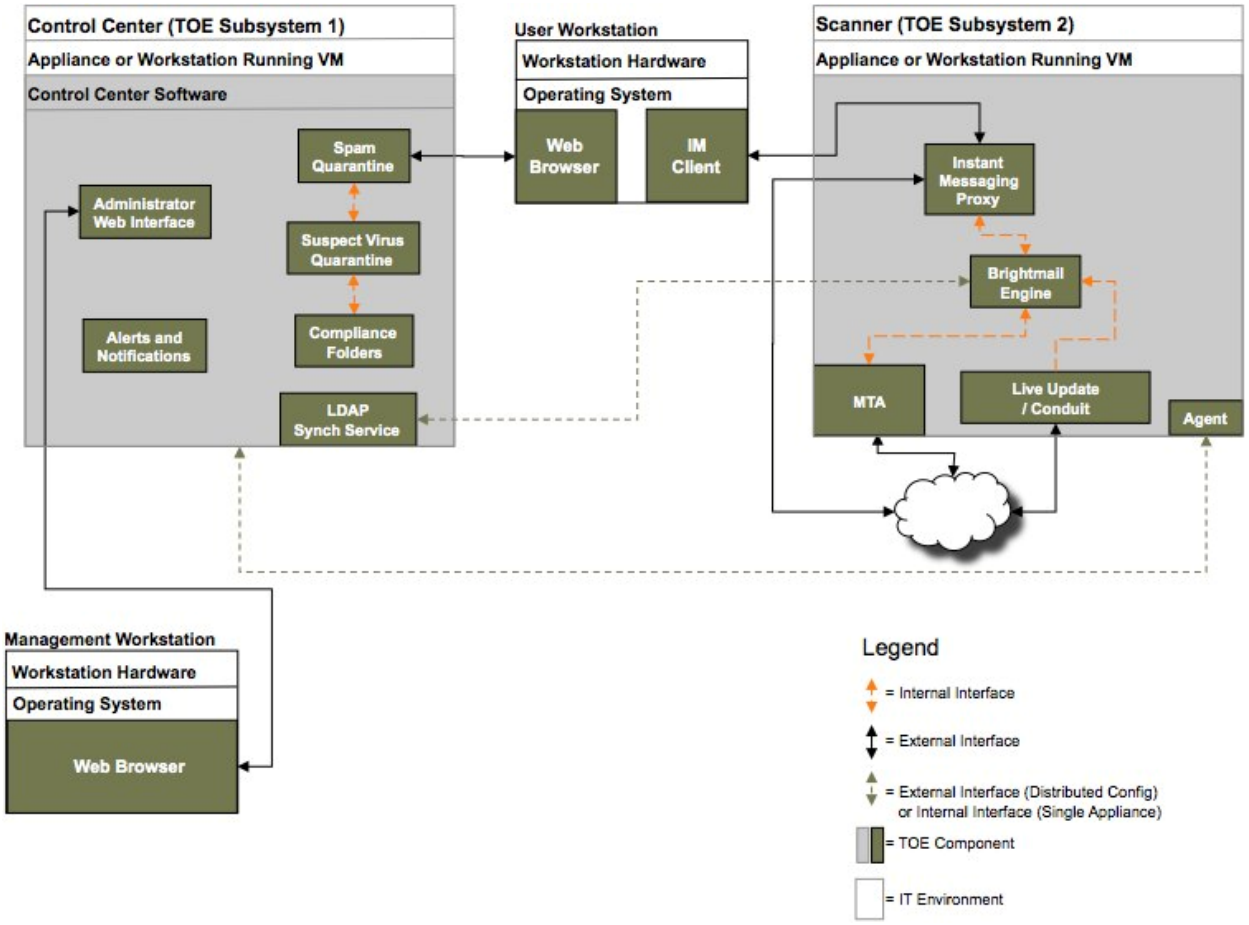


Figure 1 – TOE Boundary

The TOE interfaces include the following:

1. Software interfaces for connection to internal TOE components and external IT products.
2. Software interfaces to receive and process traffic from internal TOE components and external IT products.
3. Management interface to handle administrative actions.

The TOE's evaluated configuration requires one or more instances of a Scanner, one instance of a Control Center, and one or more instances of a workstation for management. Each TOE component runs on a dedicated appliance/workstation; applications not essential to the operation of the TOE are not installed on the workstation.

The TOE is integrated into a network, and all SMTP and Instant Messaging traffic flowing into the network must pass through the services provided by the TOE. The TOE can be implemented in a distributed manner, where one appliance running as a Control Center communicates with multiple appliances running as Scanners. In this case, communications between the Scanners and the Control center appliances are protected via SSL tunnel, provided by the Operational Environment.

1.7.4 Hardware and Software Supplied by the IT Environment

The following table identifies the minimum hardware and software requirements for components provided by the IT Environment:

Component	Minimum Requirement
Processor	2 processors
OS Environment	VMware ESX Server or ESXi Server Version 3.5 and later running a customized version of Linux with kernel version 2.6.28
Memory	2GB
Disk Space	30GB
Network card	1 10/100/1000 card required for network connectivity

Table 4 – Hardware and Software Requirements for the SBG Virtual Edition

1.7.5 Logical Boundary

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.

TSF	DESCRIPTION
Security Audit	The TOE generates 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.

TSF	DESCRIPTION
User Data Protection	The spam detection, virus detection, monitoring, and managing capabilities of the TOE ensure that the information received by the customer network is free of potential risks.
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.
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.

Table 5 – Logical Boundary Descriptions

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. The TOE ensures that the security policy is applied and succeeds before further processing is permitted. Whenever a security relevant interface is invoked: incoming network IP traffic is inspected before the packets are acted upon by higher-level protocol handlers, and management actions are limited to the permissions of the authenticated users. Non-security relevant interfaces do not interact with the security functionality of the TOE. The OS ensures that the security relevant interfaces are invoked. All incoming network packets are delivered to the TOE for inspection.

1.9 TOE Security Functional Policies

1.9.1 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 provided by the Operational Environment.

1.9.2 Message Information Flow Control SFP

The TOE implements an information process flow policy named *Message 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 are configurable by an authorized administrator via the Control Center.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 2.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

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

- 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.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.ATTACK	An attacker directs malicious network traffic against the network monitored by the TOE.
T.FALSEPOS	An email message or instant 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.

Table 6 – Threats Addressed by the TOE

3.2 Organizational Security Policies

The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.INCOMING	All incoming network traffic via SMTP or Instant Messaging protocols shall be able to be monitored for malicious/undesired email.

Table 7 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. 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 following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
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.
A.LOCATE	The processing platform on which the TOE resides is assumed to be located within a facility that provides controlled access.
A.CONFIG	The TOE is configured to handle all SMTP and instant messaging traffic flow.
A.TIMESOURCE	The TOE has a trusted source for system time.
A.SECURE_COMMS	The processing platform on which the TOE resides provides SSL/TLS functionality for secure communication to a Web browser.

Table 8 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.AUDIT	The TOE shall record the necessary events to provide information on SMTP and IM traffic and the results of the TOE's detection/filtering functions.
O.DETECT	The TOE shall be able to correctly detect emails or IMs 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.

Table 9 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.TIME	The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).
OE.SECURE_COMMS	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.
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

Table 10 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

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

Table 11 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
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.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.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.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
A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.SECURE_COMMS	This assumption is addressed by OE.SECURE_COMMS, which ensures the provision of SSL/TLS functionality.
T.ATTACK	This threat is countered by the following: • O.AUDIT, which ensures that the TOE monitors SMTP and IM 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 and IMs 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 and IMs 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 O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications
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 and IM 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 and IMs classified as spam or containing viruses.

Table 12 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

This evaluation does not include any extended components.

6 Security Requirements

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

6.1 Security Functional Requirements

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:

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

Table 13 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 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.

6.1.1.2 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 Section 7.2 - Security Audit

]

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].

6.1.1.3 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 enforcement of the SFRs.

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].

6.1.1.4 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.

6.1.2 User Data Protection (FDP)

6.1.2.1 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, TOE configuration, operator account attributes

Operations: all user actions]

6.1.2.2 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, TOE configuration, 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 14 – Management Actions and Available Services].

MANAGEMENT ACTIONS	AVAILABLE SERVICES
Full Administrative Privileges	Manage Status and Logs
	Manage Reports
	Manage Policies
	Manage Settings
	Manage Administration
	Manage Quarantine

Table 14 – 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].

6.1.2.3 FDP_IFC.1 Subset Information Flow Control

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

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

Information: Mail messages and Instant Messages to the internal network

Operations: Deliver, Delete, Quarantine, Forward]

6.1.2.4 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [Message 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 20 - Verdicts and Actions for Email Messages and Table 21 - IM Filtering Actions by Verdict Category.

].

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

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no explicit authorization rules].

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

6.1.2.5 FDP_ITC.1 Import of User Data Without Security Attributes

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

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

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

6.1.3 Identification and Authentication (FIA)

6.1.3.1 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.

6.1.3.2 FIA_UID.2 User Identification before Any Action

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

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MSA.1(1) Management of security attributes

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

6.1.4.2 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].

6.1.4.3 FMT_MSA.3(1) Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Message 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.

6.1.4.4 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.

6.1.4.5 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 Message Information Flow Control SFP
- Modify the behavior of the Message Information Flow Control SFP].

6.1.4.6 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.

6.2 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:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 15 – Security Assurance Requirements at EAL2

6.2.1 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2. EAL2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

SFR \ OBJECTIVE	O.AUDIT	O.DETECT	O.QUARANTINE	O.SEC_ACCESS
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		✓		

Table 16 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE

OBJECTIVE	RATIONALE
O.AUDIT	The objective to ensure that the TOE monitors SMTP and IM 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 a 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 and IM 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 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
O.DETECT	The objective to ensure that the TOE will correctly detect emails and IMs 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 and IM 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
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.

OBJECTIVE	RATIONALE
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 • 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

Table 17 – Rationale for Mapping of TOE SFRs to Objectives

6.4 Dependency Rationale

Table 18 – TOE SFR Dependency Rationale identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_ARP.1	No other components.	FAU_SAA.1	Satisfied
FAU_GEN.1	No other components.	FPT_STM.1	See note below table
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

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
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

Table 18 – TOE SFR Dependency Rationale

Note: Although the FPT_STM.1 requirement is a dependency of FAU_GEN.1, it has not been included in this ST because the timestamping functionality is provided by the IT Environment. The audit mechanism within the TOE uses this timestamp in audit data, but the timestamp function is provided by the operating system in the IT Environment.

6.4.1 Security Assurance Requirements

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

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: Symantec Brightmail™ Gateway 9.0.1
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: Symantec Brightmail™ Gateway 9.0.1
ADV_TDS.1: Basic Design	Basic Design: Symantec Brightmail™ Gateway 9.0.1
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Symantec Brightmail™ Gateway 9.0.1
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Symantec Brightmail™ Gateway 9.0.1
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: Symantec Brightmail™ Gateway 9.0.1
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: Symantec Brightmail™ Gateway 9.0.1
ALC_DEL.1: Delivery Procedures	Delivery Procedures: Symantec Brightmail™ Gateway 9.0.1
ATE_COV.1: Evidence of Coverage	Security Testing: Symantec Brightmail™ Gateway 9.0.1
ATE_FUN.1: Functional Testing	Security Testing: Symantec Brightmail™ Gateway 9.0.1
ATE_IND.2: Independent Testing – Sample	Security Testing: Symantec Brightmail™ Gateway 9.0.1

Table 19 – Security Assurance Rationale and Measures

7 TOE Summary Specification

7.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 6.1 – Security Functional Requirements. The security functions performed by the TOE are as follows:

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

7.2 Security Audit

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

The TOE provides for the following types of summary reports from the Administration console:

- Executive: Overview of the security profile, which includes total messages and threats processed, and virus and content filtering summaries.
- Content Filtering: Overview of the content filtering violations and trends affecting the organization. Includes number of policies triggered, and percentage of policies triggered versus total processed messages.
- Email Messages: Overview of email message threat counts and types of threats.
- Instant Messages: There is no Summary report for Instant Messages.
- Invalid Recipients: Overview of invalid recipient data.
- IP Connections: Overview of the IP connections of email entering the system.
- Spam: Overview of the email message spam.
- Virus: Overview of the current viral threats to the organization. Includes a message summary, virus summary, suspect virus outcomes, and separate tables showing stats for known and potential viral threats.

Each of these reports can be expanded to a considerable level of granular detail described in the "Working with reports" section of the *Symantec Brightmail Gateway 9.0 Administration Guide.*

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

- System
  - Dashboard
    - View the Dashboard to obtain a dynamic view of product status and filtering activity for various timeframes.
  - Hosts
    - Monitor the status of hardware and the size and volume of message queues and also view information about the hardware, software, and services that are installed.
  - Logs
    - Symantec Brightmail Gateway logs information about the Control Center, Spam Quarantine, directory data service, and each Scanner (local and remote). The Administrator can view these logs to monitor the status of the product and troubleshoot issues.
- SMTP
  - Message audit logs
    - Symantec Brightmail Gateway provides a message auditing component that allows message searching to find out what has happened to them. You can view the message audit log to determine the trail of messages that Scanners accept and process.
  - Message queues
    - A message queue is a temporary holding area for messages before they reach their destination. You can view the messages that are queued in any of the message queues.
- Instant Messaging
  - Active users
    - View all of the registered and unregistered IM users that are currently signed on.
  - Network status
    - View the connection status of each IM network that is supported from each Scanner that is in the corporate network.

Each component of the TOE processes logging data[2], 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: Provides the most important information.
- Warnings: Provides warning and Errors level data. This level is the default log level for all Scanner components (local and remote).

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

- Notices: Provides notice information and Warnings and Errors level data.
- Information: Provides informational messages and Warnings, Errors, and Notices data.
- Debug: Provides debugging information and Warnings, Errors, Notices, and Information data. This level provides the greatest amount of log information and should only be used after contacting Symantec.

7.3 User Data Protection

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

- FDP_IFC.1
- FDP_IFF.1
- FDP_ITC.1

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 and IM information flow control to enforce actions upon detection of undesired email messages or instant 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/instant 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[3] to the email handling verdicts:

Action	Description	Attacks	Virus	Spam	Content Filtering	Sender Groups
Add a header	Add an email header.	✓	✓	✓	✓	✓
Add annotation	Insert predefined text (a disclaimer, for example).	✓	✓	✓	✓	✓
Add BCC recipients	Blind carbon copy to the designated SMTP address(es).	✓	✓	✓	✓	✓
Archive the message	Forward a copy to the designated SMTP address and, optionally, host.	✓	✓	✓	✓	✓
Bypass content filtering policy	Do not filter spam messages for content filtering policies. You can choose all content filtering policies or specify the policies to bypass.			✓		✓
Bypass spam scanning	Do not scan messages that meet this policy for spam. Cannot be added to the list of approved or rejected actions.				✓	

[3] Additional notes on filtering actions apply, including the capability to perform multiple actions for particular verdicts. For more details, please review the *Symantec Brightmail Gateway 9.0 Administration Guide*.

Action	Description	Attacks	Virus	Spam	Content Filtering	Sender Groups
Clean the message	Repair repairable virus infections and delete unrepairable virus infections. Only available for the virus verdict.		✓			
Create an incident	Create a record of a content filtering policy incident. Optionally, hold for review and defer certain actions.				✓	
Defer SMTP connection	Using a 4xx SMTP response code, tell the sending MTA to try again later. Cannot be used with the Local Bad Sender Domains or Local Good Sender Domains groups.	✓				✓
Delete message	Delete the message.	✓	✓	✓	✓	✓
Deliver 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 to end-user Spam folder(s). Requires use of the Symantec Spam Folder Agent for Exchange or the Symantec Spam Folder Agent for Domino. Note: Symantec no longer provides technical support for the Symantec Spam Folder Agent for Exchange and the Symantec Spam Folder Agent for Domino.	✓	✓	✓	✓	✓
Deliver message with content encryption	Deliver via the designated encryption host over a mandatory TLS channel.				✓	
Deliver message with TLS encryption	Send the message over an encrypted channel.				✓	
Forward a copy of the message	Copy the message to designated SMTP address(es), and also deliver the original message to the recipient.	✓	✓	✓	✓	✓
Hold message in Spam Quarantine	Send to the Spam Quarantine.	✓	✓	✓	✓	✓
Hold message in Suspect Virus Quarantine	Hold in the Suspect Virus Quarantine for a configured number of hours (default is six), then refilter for viruses only, using the latest virus definitions. Only available for the suspicious attachment verdict.		✓			
Modify the Subject line	Add a tag to the message's Subject: line.	✓	✓	✓	✓	✓
Reject messages failing bounce attack validation	If a message fails bounce attack validation, reject the message. Only available for the Failed bounce attack validation verdict.			✓		

Action	Description	Attacks	Virus	Spam	Content Filtering	Sender Groups
Reject SMTP connection	Using a 5xx SMTP response code, notify the sending MTA that the message is not accepted. Cannot be used with the Local Bad Sender Domains or Local Good Sender Domains groups.	✓				✓
Remove unresolved recipients (for Directory Harvest Attacks only)	If a directory harvest attack is taking place, remove each unresolved recipient rather than sending a bounce message to the sender.	✓				
Route the message	Deliver via 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, with or without attaching the original message.	✓	✓	✓	✓	✓
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 Delay in Suspect Virus Quarantine	Remove all non-text content and deliver the stripped message immediately. Hold the complete message in Suspect Virus Quarantine for a configured number of hours (default is six hours), then release and rescan. Only available for the Suspicious Attachment verdict.		✓			
Strip attachments	Remove all attachments according to a specific attachment list. Cannot be used with sender authentication.		✓	✓	✓	
Treat as a bad sender	Process using the action(s) specified in the Local Bad Sender Domains group. Applies even if the Local Bad Sender Domains group is disabled.				✓	
Treat as a mass-mailing worm	Process using the action(s) specified in the associated worm policy.				✓	
Treat as a good sender	Process using the action(s) specified in the Local Good Sender Domains group. Applies even if the Local Good Sender Domains group is disabled. When used in a content filtering policy, messages that match the policy will not be scanned for spam.				✓	
Treat as a virus	Process using the action(s) specified in the associated virus policy.				✓	
Treat as spam	Process using the action(s) specified in the associated spam policy.				✓	
Treat as suspected spam	Process using the action(s) specified in the associated suspected spam policy.				✓	

Table 20 - Verdicts and Actions for Email Messages

The following table maps the available actions to the instant message handling verdicts:

Action	Description	Virus	Spim
Add annotation	Add an annotation to an IM message informing the recipient that the message contains spim or suspected spim.		✓
Allow file transfer	Allow an infected, encrypted, or unscannable file to be transferred to its recipient.	✓	
Block file transfer	Block an infected, encrypted, or unscannable file from being transferred to its recipient.	✓	
Delete the message	Delete an IM message that contains spim or suspected spim.		✓
Deliver message normally	Deliver an IM message that contains spim or suspected spim.		✓
Send notification	Send a predefined notification to the sender of an IM message that contains spim or an infected file informing the sender of the action.	✓	✓

Table 21 - IM Filtering Actions by Verdict Category

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 provided by the Operational Environment to the Scanner component of the TOE.

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 Status and Logs
- Manage Reports
- Manage Policies
- Manage Settings
- Manage Administration
- Manage Quarantine

7.4 Identification and Authentication

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)

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.

7.5 Security Management

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

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

7.5.1 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.

7.5.2 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.)

7.5.3 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.

7.5.4 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