Symantec Messaging Gateway Version 10.6 Security Target

Version 1.6
October 11, 2016

Prepared for:
Symantec Corporation

350 Ellis Street
Mountain View, CA 94043
http://www.symantec.com

Prepared by:

Leidos Inc.
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Symantec Messaging Gateway Version 10.6.1-4 provided by Symantec Corporation. The Symantec Messaging Gateway enables organizations to secure their email and productivity infrastructure with effective and accurate real-time antispam and antimalware protection, targeted attack protection, advanced content filtering, data loss prevention, and optional email encryption.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Rationale (Section 7)

1.1 Security Target, TOE and CC Identification

ST Title – Symantec Messaging Gateway Version 10.6 Security Target

ST Version – Version 1.6

ST Date – October 11, 2016

TOE Identification – Symantec Messaging Gateway Version 10.6.1-4 running on one or more Symantec appliances listed below:

Hardware Appliance

- 8340
- 8360
- 8380

Virtual Machine Appliance

- Symantec Messaging Gateway Version 10.6.1-4

TOE Developer – Symantec Corporation

Evaluation Sponsor – Symantec Corporation

CC Identification – *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012*

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, July 2012.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, July 2012.

- Part 3 Conformant
- Assurance Level: EAL 2

1.3 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

1.4 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FDP_ACC.1 (1) and FDP_ACC.1 (2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (for example, [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (for example, [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (for example, [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (for example, "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.5 Glossary

Acronym	Description
BBC	Blind carbon copy
DDS	Directory Data Service
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
FTP	File Transfer Protocol
LDAP	Lightweight Directory Access Protocol
MTA	Mail Transfer Agent
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PDF	Portable Document Format
SFR	Security Functional Requirement
SFP	Security Function Policy
SMG	Symantec Messaging Gateway

Acronym	Description
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

1.6 Terminology

The terminology below is described in order to clarify the terms used in the ST as well as those used in the TOE product documentation.

Term	Definition
4xx	4xx is a series of SMTP error codes. Any error code in the 400's is a temporary error. You can infer from this that your outgoing mail server will continue to try and send the email in the hopes that it can be delivered at a later time.
5xx	The 5xx is a series of SMTP error codes. Error codes in the 500's are permanent errors. When a 5xx error is encountered the outgoing mail server should immediately stop trying to send the email and send a bounce message, usually from mailer-daemon, letting you know that the email could not be delivered.
Agent	A component that facilitates communicating configuration information between the Control Center and each Scanner.
Bad Sender	A sender from whom you do not want to accept email messages. A Bad Sender is a member of at least one of the following groups: Local Bad Sender Domains, Local Bad Sender IPs, Third Party Bad Senders, or Symantec Global Bad Senders.
Bounce	An action that can be performed on an email message by a mail server. The action returns the message to it's `From:` address with a custom response.
Bounce Attack Prevention	A feature of Symantec Messaging Gateway that eliminates the bounced messages that are a result of redirection, while still allowing legitimate bounce message notification.
Brightmail Engine	The Symantec Messaging Gateway component that scans email and attachments and file transfers for malware, spam, and content filtering according to polices that you configure.
Conduit	A component that retrieves new and updated filters from Symantec Security Response through secure HTTPS file transfer. Once the filters are retrieved, the Conduit authenticates filters. It then alerts the Brightmail Engine that new filters are to be received and implemented. Finally, the Conduit manages statistics for use by Symantec Security Response and for generating reports.
Control Center	A Web-based configuration and administration center. Each site has one Control Center. The Control Center also houses Spam Quarantine and supporting software. You can configure and monitor all of your Scanners from the Control Center.
Directory Data Service	A Symantec Messaging Gateway service that permits the use of the information in your Lightweight Directory Access Protocol (LDAP) directories for Symantec Messaging Gateway features.
Directory Data Source	An LDAP query configuration that enables particular features in Symantec

Term	Definition
Function	Messaging Gateway. Symantec Messaging Gateway provides four directory data source functions: authentication, address resolution, routing, and recipient validation.
Directory Harvest Attack	A tactic that spammers use to determine valid email addresses. A directory harvest attack occurs when a spammer sends a large quantity of possible email addresses to a site.
Disarm	Disarm scans email attachments for Microsoft Office and PDF documents that may contain potentially malicious content.
False Positive	A piece of legitimate email that is mistaken for spam and classified as spam by Symantec Messaging Gateway.
Filter	A method for analyzing email messages, used to determine what action to take on each message.
Good Sender	A sender from whom you want to accept email messages. A Good Sender is a member of at least one of the following groups: Local Good Sender Domains, Local Good Sender IPs, Third Party Good Senders, or Symantec Global Good Senders.
HTTPS	HTTPS (also called HTTP over TLS, HTTP over SSL, and HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.
LDAP (Lightweight Directory Access Protocol)	A software protocol that enables anyone to locate organizations, individuals, and other resources (such as files and devices). These resources can be located whether on the Internet or on a corporate intranet. LDAP is a lightweight version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
Malware	Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.
Messaging Gateway	The outermost point in a network where mail servers are located. All other mail servers are downstream from the mail servers that are located at the messaging gateway.
MTA (Mail Transfer Agent)	A generic term for programs such as Sendmail, postfix, or qmail that send and receive mail between servers using SMTP. The MTA in each Symantec Messaging Gateway Scanner routes the inbound messages and outbound messages to the Brightmail Engine for processing. Then the MTA delivers filtered messages to their internal destinations or to remote destinations.
PDF	Portable Document Format (PDF) is a file format used to present and exchange documents reliably, independent of software, hardware, or operating system.
SMTP (Simple Mail Transfer Protocol)	The protocol that allows email messages to be exchanged between mail servers. Then, clients retrieve email, typically through the POP protocol or IMAP protocol.
SSL (Secure Sockets Layer)	A protocol that allows mutual authentication between a client and server. The protocol allows for the establishment of an authenticated and encrypted connection, thus ensuring the secure transmission of information over the Internet. See also TLS.
Spam	1. Unsolicited commercial bulk email. 2. An email message that is identified as spam by Symantec Messaging Gateway, using its filters.

Term	Definition
Symantec Security Response	Symantec global technical support team that provides extensive coverage for enterprise businesses and consumers to leverage threat and early warning systems to provide customers with comprehensive expertise regarding viruses, malware, worms, Trojan horses, bots, and other malicious code.
TLS (Transport Layer Security)	A protocol that provides communications privacy over the Internet that uses symmetric cryptography with connection-specific keys and message integrity checks. TLS provides some improvements over SSL in security, reliability, interoperability, and extensibility. See also SSL.
Reject	An action that an MTA receiving an email message can take. The action consists of using a 5xx SMTP response code to tell the sending MTA that the message is not accepted.
Unscannable	In Symantec Messaging Gateway, a message can be unscannable for viruses for a variety of reasons. For example, unscannable files exceed the maximum file size or maximum scan depth that is specified. They can also consist of malformed MIME attachments.
URL	A URL is one type of Uniform Resource Identifier (URI); the generic term for all types of names and addresses that refer to objects on the World Wide Web. The term "Web address" is a synonym for a URL that uses the HTTP or HTTPS protocol.
Virus	A piece of programming code inserted into other programming to cause some unexpected and, for the victim, usually undesirable event.
Worm	A special type of virus. A worm does not attach itself to other programs like a traditional virus, but creates copies of itself, which create even more copies.

2. TOE Description

The Target of Evaluation (TOE) is Symantec Messaging Gateway Version 10.6.1-4.

2.1 TOE Overview

Symantec Messaging Gateway offers enterprises a comprehensive gateway-based message-security solution. Symantec Messaging Gateway delivers inbound and outbound messaging security, real-time antispam and antivirus protection, advanced content filtering, and data loss prevention in a single platform. Symantec Messaging Gateway does the following to protect the customer environment:

- Detects spam, denial-of-service attacks, and other inbound email threats.
- Uses Symantec Disarm technology to detect and remove potentially malicious content from many common email attachments, including Microsoft Office documents and Adobe PDFs. Potentially malicious content types include macros, scripts, Flash movies, and other exploitable content. Disarm deconstructs the attachment, strips the exploitable content, and reconstructs the document, preserving its visual fidelity. You can choose the types of documents and types of potentially malicious content to Disarm. You can also choose whether to archive the original unaltered documents in case administrators or end users need access to them.
- Provides outbound sender throttling to protect against outbound spam attacks from compromised internal users.
- Leverages a global sender reputation and local sender reputation analysis, including expanded URL reputation-based filtering, to block spam, malware and phishing message and to reduce email infrastructure costs by restricting unwanted connections.
- Filters email by policies to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email.

- Gives you the option to enforce TLS encryption on inbound messages from specific domains, to allow more secure communication with trusted partners and senders.
- Provides granular policies and verdicts for mail that cannot be scanned, so you can take different actions depending on the reasons why a message is unscannable. Reports that focus on unscannable messages allow you to isolate and interpret statistical information about unscannable mail and attachments.
- Provides visibility into messaging trends and events with minimal administrative burden.
- Provides secure remote administration using HTTPS.

The TOE implements additional security functions such as identification and authentication of TOE users; auditing; user data protection; security management; and trusted path.

2.2 TOE Architecture

The Symantec Messaging Gateway Series appliances and Symantec Messaging Gateway Virtual Edition are composed of two components that can be combined on appliances or deployed with multiple appliances depending on network needs. Customers may deploy any appliance model as a combined control center / scanner, dedicated scanner, or dedicated control center.

Component	Description
Control Center	A Control Center lets you configure and manage Symantec Messaging Gateway from a Web-based interface. From a single Web-based console, administrators can easily manage multiple Messaging Gateway appliances to view trends, attack statistics, and noncompliance incidents. Lightweight Directory Access Protocol (LDAP) credentials can be used to authenticate administrative access and configure groups and policies. One Control Center must be configured for your site. One Control Center controls one or more Scanners.
Scanner	Scanners can perform all of the following tasks: • Process the inbound messages and outbound messages and route messages for delivery. • Download virus definitions, spam signatures, and other security updates from Symantec Security Response. • Run filters, render verdicts, and apply actions to messages in accordance with the appropriate policies and settings. You can configure one or more Scanners.
Control Center and Scanner	Performs both functions. This configuration is suitable for smaller installations.

Table 1 - TOE Components

The TOE's evaluated configuration requires one or more instances of a Scanner and one instance of a Control Center. The TOE is integrated into a network, and all SMTP 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.

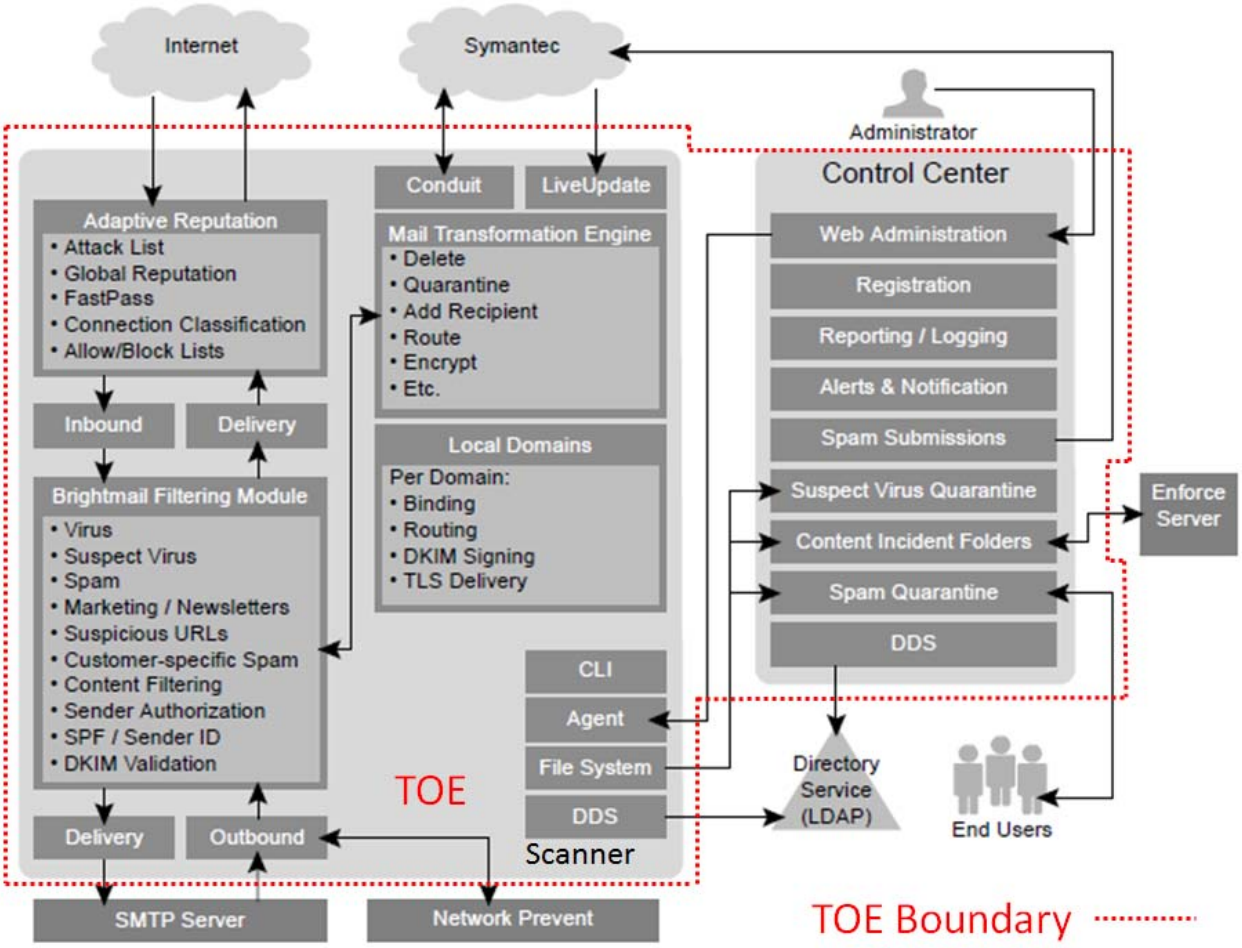

Figure 1 - Symantec Messaging Gateway Architecture

Figure 1 shows how Symantec Messaging Gateway processes an email message. This diagram assumes that the message passes through the Brightmail Filtering Module to the Mail Transformation Engine without being rejected.

The path an email message takes is as follows:

1. At the gateway, global reputation determines if the sending IP is a Good Sender or a Bad Sender. It accepts or rejects the connection based on the distinction.
2. Connection Classification classifies the sending IP into one of 10 classes based on local reputation. It either accepts or defers the connection based on class membership.
3. Before the MTA accepts the message, it checks the domain address and email address. The MTA determines if it belongs to the Local Good Sender Domains or Local Bad Sender Domains group. If it does, it applies the configured action to the message. If appropriate, the MTA moves the message to its inbound queue.
4. The Brightmail Filtering Module consults the directory data service to expand the message's distribution list and determines policy group membership.
5. The Brightmail Filtering Module determines each recipient's filtering policies.
6. Antivirus filters determine whether the message is infected.
7. Spam filters determine whether the message is spam or suspected spam.
8. Unwanted mail filters (including marketing newsletters, redirect URLs, and customer-specific spam) determine whether the message is unwanted.

9. Content filtering policy filters scan the message and attachments for restricted content.
10. The Mail Transformation Engine performs actions according to filtering results and configurable policies and applies them to each recipient's message based on policy group membership.
11. Messages may be held in quarantine for review based on policy configuration. Messages in content incident folders can be remediate through the console.
12. Messages are then inserted into the delivery queue for delivery by the MTA.

Note: Symantec Messaging Gateway does not filter any messages that do not flow through the SMTP gateway. For example, it does not filter the messages that are sent between mailboxes on the same Microsoft Exchange Server or within an Exchange organization.

The administrator connects via HTTPS to the Control Center through a Web browser to configure and manage the TOE. New administrators can be added based on attributes and group memberships that are found in LDAP directory structures. Administrative policies can be configured and assigned to specific LDAP-based groups. The TOE relies upon a NTP server in the operational environment to provide accurate timestamps.

2.2.1 Physical Boundaries

2.2.1.1 Included Product Components

The Symantec Messaging Gateway can be deployed on a family of Symantec 8300 Series hardware appliances that can scale across organizations from small businesses to large enterprises. There is also a virtual appliance option, the Messaging Gateway virtual edition, which offers the same software, features, and functionality, deployed on VMware or Microsoft Hyper-V environments. Appliances can be deployed as dedicated control centers, scanners, or combined control center/scanners.

Appliance Model	8340	8360	8380
Organization	Small and Medium Businesses	Enterprise / Large Enterprise	Enterprise/Large Enterprise
Typical Deployment*	Control Center/Scanner	Dedicated Scanner or Control Center	Dedicated Scanner or Control Center
Form Factor	1RU Rack Mount	1RU Rack Mount	1RU Rack Mount
Power Supply	Single	Redundant, hot-plug, auto-switching, universal power supply	Redundant, hot-plug, auto-switching, universal power supply
CPU	Single Quad-Core Processor	Dual Quad-Core Processors	Dual 6-Core Processors
Hard Drive / RAID	2 x 1TB SAS RAID 1	2 x 146GB Serial-Attach SCSI (hot-swappable) RAID 1	6 x 300GB Serial-Attach SCSI (hot-swappable) RAID 10
NIC	Two Gigabit Ethernet Ports	Two Gigabit Ethernet Ports	Four Gigabit Ethernet Ports
* Customers may deploy any appliance model as a combined control center/scanner, dedicated scanner, or dedicated control center			

Table 2 – Hardware Appliance Models

Description	Recommended	Minimum	Notes
VMware ESX	ESXi Version 5.5	Version 5.0	Supported versions are

Description	Recommended	Minimum	Notes
Server	or later		ESXi/vSphere 5.0/5.1/5.5/6.0 server. Processor on the host must support VT and have this setting enabled in the BIOS prior to installation to support the 64-bit kernel that is required by Symantec Messaging Gateway.
Disk type	Fixed Disk	----	Symantec Messaging Gateway installed on a flexible disk on a virtual machine is not supported.
Disk space	For more information, consult the Symantec Knowledge Base article, *Disk Space Recommendations for Symantec Messaging Gateway Virtual Edition*.	120 GB	For Scanner-only virtual machines.
		120 GB	For Control Center - only virtual machines.
		120 GB	For combined Scanner and Control Center virtual machines.
Memory	16 GB	8 GB	A minimum of 8 GB is necessary to run Symantec Messaging Gateway and the virtual machine.
CPUs	8	4	Symantec recommends allocating eight or more CPUs, based on workload demands and hardware configuration. Note: the environment must support 64-bit applications.
NICs	2	1	Only one network interface card is required per virtual machine. Note: The maximum number of NICs that are supported is 2.

Table 3 - Supported Configurations for Symantec Messaging Gateway Virtual Edition on VMware

Description	Recommended	Minimum	Notes
Microsoft Hyper-V	Windows 2012 Datacenter Edition	Windows 2008 Standalone	Processor on host must support VT and have this setting enabled in the BIOS prior to installation to support the 64-bit kernel.
Disk type	Fixed Disk	----	Symantec Messaging Gateway does not support installation on a virtual machine with a dynamic disk.
Disk space	For more	120 GB	For Scanner-only virtual machines.

Description	Recommended	Minimum	Notes
	information, consult the Symantec Knowledge Base article, *Disk Space Recommendations for Symantec Messaging Gateway Virtual Edition.*	120 GB	For Control Center–only virtual machines.
		120 GB	For combined Scanner and Control Center virtual machines.
Memory	16 GB	8 GB	A minimum of 8 GB is necessary to run Symantec Messaging Gateway and the virtual machine.
CPUs	8	4	Symantec recommends allocating four or more CPUs, based on workload demands and hardware configuration. Note: The environment must support 64-bit applications.
NICs	2	1	Only one network interface card is required per virtual machine. Symantec Messaging Gateway supports the use of synthetic NICs only. Note: The maximum number of NICs that are supported is 2.

Table 4 - Supported Configurations for Symantec Messaging Gateway Virtual Edition on Hyper-V

2.2.1.2 Services and Products in the Operational Environment

The TOE relies on the following services and products in operational environment:

1. Hypervisor: provides virtualization for Symantec Messaging Gateway Virtual Edition. The hypervisor is VMware ESX Server Version 4.1, VMware ESXi Server Version 5.0/4.x, or Microsoft Hyper-V - Windows 2012 Datacenter Edition or Windows 2008 Standalone.
2. The Control Center supports the following Web browsers:
    a. Microsoft Internet Explorer 9 or later
    b. Mozilla Firefox 28 or later
    c. Chrome 34 or later
3. Symantec Messaging Gateway supports the following LDAP directory types:
    a. Windows 2012 Active Directory® (both LDAP and Global Catalog)
    b. Windows 2008 Active Directory (both LDAP and Global Catalog)
    c. Oracle® Directory Server Enterprise Edition 11.1.1.7
    d. Oracle Directory Server Enterprise Edition 11.1.1.6.0
    e. Oracle Directory Server Enterprise Edition 11.1.1.5.0

f. Sun™ Directory Server 7.0

g. IBM® Domino® (formerly Lotus Domino) LDAP Server 8.5.3

h. IBM LDAP Server 8.5.2

i. IBM Domino LDAP Server 8.5

j. IBM Domino LDAP Server 8.0

k. IBM Domino LDAP Server 7.0

l. OpenLDAP 2.4

m. OpenLDAP 2.3

n. Symantec Messaging Gateway is LDAP v.3 compliant and can be configured to work with other directory server types.

4. Syslog server: In addition to viewing logs using the Control Center, some Scanner logs can be sent to syslog on a remote server.

5. Network Time Protocol Server

2.2.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- User data protection
- Identification and authentication
- Security management
- Trusted path/channels

2.2.2.1 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.

2.2.2.2 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.

2.2.2.3 Identification and authentication

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

2.2.2.4 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.

2.2.2.5 Trusted path/channels

The TOE requires remote users to initiate a trusted communication path using HTTPS/TLSv1.2 for initial user authentication. The TOE also requires that the trusted path be used for the transmission of all Symantec Messaging Gateway administrative communication. HTTPS/TLSv1.2 ensures the administrative session communication pathway is secured from disclosure and modification.

2.3 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.

2.4 TOE Security Functional Policies

2.4.1 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 SCP or FTP. All administration takes place via Web-based HTTPS GUI connected to the TOE.

2.4.2 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.

2.5 TOE Documentation

Symantec has a number of administration and configuration guides for the Symantec Messaging Gateway which include the following:

- Symantec Messaging Gateway 10.6 Administration Guide, Documentation Version 10.6
- Symantec Messaging Gateway 10.6 Getting Started Guide, Documentation Version 10.6
- Symantec Messaging Gateway 10.6 Installation Guide, Documentation Version 10.6

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 section 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 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 inappropriately view, modify, or delete 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 5 - Threats

3.2 Organizational Security Policies

The following Organizational Security Policies apply to the TOE:

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

Table 6 - 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.

ASSUMPTION	DESCRIPTION
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 traffic flow.
A.TIMESOURCE	The TOE has a trusted source for system time.

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 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.PROTECTED_COMMS	The TOE will provide a protected communication channel for remote administrators to TOE device communications.

Table 7 - Security Objectives for the TOE

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

Table 8 - Operational Environment Security Objectives

5. IT Security Requirements

The security requirements for the TOE have been drawn from Parts 2 and 3 of the Common Criteria. The security functional requirements have been selected to correspond to the actual security functions implemented by the TOE while the assurance requirements have been selected to offer a low to moderate degree of assurance that those security functions are properly realized.

5.1 Extended Components Definition

This evaluation does not include any extended components.

5.2 TOE Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, of which are summarized in the following table:

Class Heading	Class Family	Description
FAU: Security Audit	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Data Generation
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
FDP: 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
FIA: Identification and Authentication	FIA_UAU.2	User Authentication before Any Action
	FIA_UID.2	User Identification before Any Action
FMT: 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
FTP: Trusted path/channels	FTP_TRP.1	Trusted path

Table 9 - TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 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.

5.2.1.2 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

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**

Reports listed in Section 6.1 - 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]**.

5.2.1.3 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]**.

5.2.1.4 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.

5.2.2 User Data Protection (FDP)

5.2.2.1 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]

5.2.2.2 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 10**Management Actions and Available Services].

Management Action	Available Services
Full Administrative Privileges	Manage Status and Logs Manage Reports Manage Policies Manage Settings Manage Administration Manage Quarantine

Table 10 - 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]**.

5.2.2.3 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 traffic through the TOE

Information: Mail messages to the internal network

Operations: Deliver, Delete, Quarantine, Forward].

5.2.2.4 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 12 - Verdicts and Actions for Email Messages].**

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]**.

5.2.2.5 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]**.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 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.

5.2.3.2 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.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MSA.1(1) Management of security attributes

FMT_MSA.1.1(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 **[Administrators]**.

5.2.4.2 FMT_MSA.1(2) Management of security attributes

FMT_MSA.1.1(2) The TSF shall enforce the **[Administrative Access Control SFP]** to restrict the ability to **[*modify, delete*]** the security attributes **[Administrator accounts, Limited Administrator accounts, privileges for Limited Administrators]** to **[Administrators]**.

5.2.4.3 FMT_MSA.3(1) Static Attribute Initialization

FMT_MSA.3.1(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(1) The TSF shall allow the **[Administrator]** to specify alternative initial values to override the default values when an object or information is created.

5.2.4.4 FMT_MSA.3(2) Static Attribute Initialization

FMT_MSA.3.1(2) 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(2) The TSF shall allow the **[Administrator]** to specify alternative initial values to override the default values when an object or information is created.

5.2.4.5 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]**.

5.2.4.6 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.

5.2.5 Trusted path/channels (FTP)

5.2.5.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **[*remote*]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[*modification, disclosure*].**

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **[*initial user authentication, [remote administrative access to the TOE]*].**

5.3 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:

Requirement Class	Requirement Component
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: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
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 11 - Security Assurance Requirements at EAL2

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1d The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2d The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3d The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1c The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2c The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3c The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4c The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5c The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Security-enforcing functional specification (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.

ADV_FSP.2.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1c The functional specification shall completely represent the TSF.

ADV_FSP.2.2c The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3c The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4c For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5c For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Basic design (ADV_TDS.1)

ADV_TDS.1.1d The developer shall provide the design of the TOE.

ADV_TDS.1.2d The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1c The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2c The design shall identify all subsystems of the TSF.

ADV_TDS.1.3c The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4c The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.1.5c The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6c The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

ADV_TDS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2e The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance documents (AGD)

5.3.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.

AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle support (ALC)

5.3.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1d The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2d The developer shall provide the CM documentation.

ALC_CMC.2.3d The developer shall use a CM system.

ALC_CMC.2.1c The TOE shall be labelled with its unique reference.

ALC_CMC.2.2c The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3c The CM system shall uniquely identify all configuration items.

ALC_CMC.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1d The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1c The configuration list shall include the following: The TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2c The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2d The developer shall use the delivery procedures.

ALC_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4c	The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.3 Independent testing — sample (ATE_IND.2)

ATE_IND.2.1d	The developer shall provide the TOE for testing.
ATE_IND.2.1c	The TOE shall be suitable for testing.
ATE_IND.2.2c	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3e	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability assessment (AVA)

5.3.5.1 Vulnerability analysis (AVA_VAN.2)

AVA_VAN.2.1d	The developer shall provide the TOE for testing.
AVA_VAN.2.1c	The TOE shall be suitable for testing.
AVA_VAN.2.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2e	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.2.3e	The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
AVA_VAN.2.4e	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.3.6 Security Target Evaluation (ASE)

5.3.6.1 – Conformance claims (ASE_CCL.1)

ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Extended components definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

5.3.6.3 ST introduction (ASE_INT.1)

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

5.3.6.4 Security objectives (ASE_OBJ.2)

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

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

5.3.6.5 Derived security requirements (ASE_REQ.2)

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

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

5.3.6.6 Security problem definition (ASE_SPD.1)

ASE_SPD.1.1D	he developer shall provide a security problem definition.
ASE_SPD.1.1C	The security problem definition shall describe the threats.
ASE_SPD.1.2C	All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C	The security problem definition shall describe the OSPs.
ASE_SPD.1.4C	The security problem definition shall describe the assumptions about the operational environment of the TOE.
ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.7 TOE summary specification (ASE_TSS.1)

ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

6. TOE Summary Specification

The security functions described in the following subsections fulfill the security requirements that are defined in **Section 5.2 TOE Security Functional Requirements**. The security functions performed by the TOE are as follows:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of Management Functions
- Trusted Path/Channels

6.1 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 generates audit records for the following auditable events:

- Start-up and shutdown of the audit function
- Start-up and shutdown of TOE services 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

Each audit record includes the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Logs can be viewed via the Web Interface available to the authorized Administrator or via Syslog messages (if configured). The authorized administrator can sort log data, create log reports, and clear log files from the database.

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.
- Invalid Recipients: Overview of invalid recipient data.
- IP Connections: Overview of the IP connections of email entering the system.
- Spam and Unwanted Email: Overview of the spam and unwanted email.
- Submissions: Overview of spam submissions.
- Malware: Overview of the current malware threats to the organization. Includes a message summary, malware summary, suspect malware outcomes, and separate tables showing stats for known and potential malware threats.
- Disarm: Overview of the potentially malicious content containers and types detected and removed from email attachments.

Each of these reports can be expanded to a considerable level of granular detail described in the "Creating reports" section of the *Symantec Messaging Gateway 10.6 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 your hardware and the size and volume of your message queues and also view information about the hardware, software, and services that are installed.
    - Logs
        - Symantec Messaging Gateway logs information about the Control Center, Spam Quarantine, directory data service, and logs on each Scanner. The administrator can view these logs to monitor the status of your product and troubleshoot issues.
- SMTP
    - Message audit logs
        - Symantec Messaging Gateway provides a message auditing component that allows searching for messages to find out what has happened to them. The administrator 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.

Each component of the TOE processes logging data[1], 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).
- 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.

Upon detection of a potential security violation; automatic email notifications are sent to inform administrators of the conditions that potentially require attention.

6.2 User data protection

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

- FDP_ACC.1
- FDP_ACF.1
- 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 the Message Information Flow Control policy for SMTP and flow control to enforce actions such as adding the email to the Allowed Senders List or the Blocked Senders List. Email may be added to the Allowed Senders List if no malicious code is detected. Undesired mail may be identified to be spam or 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 such that an administrator may possibly add them to the Blocked Senders List. If the TOE detects a specified number of infected messages from an IP address, email virus attack prevention can then defer further connections and prevent additional infections.

Additionally, the TOE will notify an Administrator when certain events occur.

The following table maps the available actions[2] to the email handling verdicts:

Action	Description	Attacks	Malware	Spam	Unwanted Email	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.	✓	✓	✓	✓	✓	✓

[1] Logs can be viewed via the Web Interface available to the Administrator or via Syslog messages.
[2] Additional notes on filtering actions apply, including the capability to perform multiple actions for particular verdicts. For more details, please review the *Symantec Messaging Gateway 10.6 Administration Guide*.

Action	Description	Attacks	Malware	Spam	Unwanted Email	Content Filtering	Sender Groups
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 Disarm	Do not scan attachments for Potentially malicious content.					✓	
Bypass spam scanning	Do not scan messages that meet this policy for spam. Cannot be added to the list of approved or rejected actions.					✓	
Clean the message	Repair repairable virus infections and delete unrepairable virus infections. Only available for the virus verdict.		✓				
Create an informational incident	Create a record for the incident in the informational incident folder that you specify.			✓	✓	✓	
Create a quarantine incident	Hold the message for review in the content quarantine folder that you specify. When you select this option, you must also specify actions for the following sub-options: Approve, Rejected, and Custom action.			✓	✓	✓	
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 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.					✓	

Action	Description	Attacks	Malware	Spam	Unwanted Email	Content Filtering	Sender Groups
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 re-filter 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.			✓			
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 potentially malicious content (Disarm)	Scan message attachments for Specified document types, remove specified types of potentially malicious content, and reconstruct attachments.		✓				
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.	✓	✓	✓	✓	✓	✓

Action	Description	Attacks	Malware	Spam	Unwanted Email	Content Filtering	Sender Groups
Send a bounce message	Return the message to it's "`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.					✓	

Action	Description	Attacks	Malware	Spam	Unwanted Email	Content Filtering	Sender Groups
Treat as suspected spam	Process using the action(s) specified in the associated suspected spam policy.					✓	

Table 12 - Verdicts and Actions for Email Messages

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

The TOE enforces the Administrative Access Control Policy to prevent unauthorized users from accessing system reports, component audit logs, or component configuration details. The Administrator can create additional administrator accounts and control the account attributes by 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 Spam Quarantine
- Manage Virus Quarantine

6.3 Identification and authentication

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

- FIA_UAU.2
- FIA_UID.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.

6.4 Security management

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

- 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.

6.4.1 Manage User Accounts

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

Users are managed through policy groups. These groups of users can be configured according to email addresses, domain names, or LDAP groups. Then you can apply filtering policies to specific policy groups.

The TOE maintains the roles of administrator and limited administrator. An administrator with Full Administration Rights can view, access, and modify any page in the Control Center.

Administrators can grant administrators Limited Administration Rights with the following access:

- None - Administrators do not have any rights to perform the selected task and cannot view the corresponding pages.
- View - Administrators can view appropriate pages, but cannot manage them.
- Modify - Administrators have full rights to view and modify tasks.

Each type of Limited Administration Rights grants the administrator the ability to view a subset of the pages of the Control Center. You can grant Limited Administration Rights to the following functions:

- Status and Logs
- Reports
- Policies
- Settings
- Administration
- Spam Submissions
- Quarantine

6.4.2 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. The administrator may configure the TOE to send Scanner log data to a remote syslog server.

6.4.3 Backup and Restore

The administrator can backup or restore the configuration data via FTP. The configuration data includes all modifiable settings in the Control Center, the spam submission submitter ID, and the submitters list and policies.

6.4.4 Information Process Flow

The administrator may configure and modify the behavior of the Message Information Flow Control SFP to set the policies for spam and virus detection. Upon installation, one default policy for each spam or virus verdict is assigned by default to the default group. Other default policies for spam and virus are provided but initially not assigned to any group. The administrator can create additional policies of any type.

6.4.5 Administrative Access Control

The Symantec Messaging Gateway installs with a Default policy group that consists of all of the users. The administrator may configure and modify the behavior of the Administrative Access Control SFP to set the privilege level of users.

6.5 Trusted Path/Channels

The Trusted Path/Channels function is designed to satisfy the following security functional requirement:

- FTP_TRP.1

The TSF provides a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.

The TOE requires an HTTPS/TLSv1.2 connection for remote users to authenticate to the TOE from a browser that is part of the environment. To successfully establish an interactive administrative session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to access the GUI interface.

7. Rationale

The security functions described in the following subsections

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Requirement Dependencies;
- TOE Summary Specification.

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

7.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the 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 (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.PROTECTED_COMMS	O.SEC_ACCESS	OE.TIME	OE.PERSONNEL	OE.PHYSEC
A.MANAGE							✓	
A.NOEVIL							✓	

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

Table 13 - 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 OE.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 OE.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 OE.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 OE.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
T.ATTACK	This threat is countered by the following: • O.AUDIT, which ensures that the TOE monitors SMTP 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 • O.PROTECTED_COMMS, which ensures that remote communication to the TOE is protected from unauthorized disclosure and modification by using HTTPS.
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 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.

Table 14 - Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

7.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note: **Table 15 - Mapping of TOE SFRs to Security Objectives** indicates the requirements that effectively satisfy the individual objectives.

7.2.1 Security Functional Requirements Rationale

All of the Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

SFR \ OBJECTIVE	O.AUDIT	O.DETECT	O.QUARANTINE	O.PROTECTED_COMMS	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		✓			
FTP_TRP.1				✓	

Table 15 - 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 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 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 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
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.PROTECTED_COMMS	The objective to ensure that the TOE provides a protected communication channel for remote administrators to TOE device communications is met by the following security requirement: • FTP_TRP.1 The TOE is required to protect communication between itself and its remote administrative users from disclosure and detect the modification of those communications. The TOE is required to use HTTP over TLSv1.2 to provide these protections.

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 16 - Rationale for Mapping of TOE SFRs to Objectives

7.2.2 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.

The table below 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 Messaging Gateway 10.6
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: Symantec Messaging Gateway 10.6
ADV_TDS.1: Basic Design	Basic Design: Symantec Messaging Gateway 10.6
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Symantec Messaging Gateway 10.6
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Symantec Messaging Gateway 10.6
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: Symantec Messaging Gateway 10.6
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: Symantec Messaging Gateway 10.6
ALC_DEL.1: Delivery Procedures	Delivery Procedures: Symantec Messaging Gateway 10.6
ATE_COV.1: Evidence of Coverage	Security Testing: Symantec Messaging Gateway 10.6
ATE_FUN.1: Functional Testing	Security Testing: Symantec Messaging Gateway 10.6
ATE_IND.2: Independent Testing – Sample	Security Testing: Symantec Messaging Gateway 10.6

Table 17 - Security Assurance Rationale and Measures

7.3 Requirement Dependency Rationale

The table below 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
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
FTP_TRP.1	No other components.	None	Not applicable

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 time stamping 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.

7.4 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 19 - Mapping of TOE SFRs to Security Functions** the relationship between security requirements and security functions.

OBJECTIVE / SFR	Security Audit	User Data Protection	Identification and Authentication	Security Management	Trusted path/channels
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				✓	
FTP_TRP.1					✓

Table 19 - Mapping of TOE SFRs to Security Functions