SurfControl
E-mail Filter for SMTP Version 5.0, Service Pack 2

Security Target

Document Version 1.04

Prepared for:

SurfControl plc
5550 Scotts Valley Drive
Scotts Valley CA, 95066
Phone: (831) 440-2500
Fax: (831) 440-2740
http://www.surfcontrol.com/

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com/

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2, and will hereafter be referred to as the TOE throughout this document. The TOE is a server-based software application which filters Simple Mail Transfer Protocol (SMTP)-based email messages. It protects internal networks by filtering email flowing in from and out to the internet and enhances security by detecting spam and enforcing an acceptable usage policy for e-mail within an organization.

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish, or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile (PP) claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terms used within this ST.

1.1 Security Target, TOE and CC Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

ST Title	SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 Security Target
ST Version	Version 1.04
Author	Corsec Security, Inc. (http://www.corsec.com/) Nathan Lee and Shyam Enjeti
TOE Identification	SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.2 Revision 326, December 2004 (aligned with ISO/IEC 15408:2004); Parts 2 and 3 Interpretations from the Interpreted Common Methodology for Information Technology Security Evaluation (CEM) as of February 3, 2005 were reviewed, No interpretations apply to the claims made in this ST.
PP Identification	None
Assurance Level	Evaluation Assurance Level (EAL) 2
Keywords	E-mail Filter, Secure Messaging, Mail Scanning.

1.2 Conventions, Acronyms, and Terminology

1.2.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for several operations to be performed on security requirements; *assignment*, *refinement*, *selection* and *iteration*. All of these operations are used within this ST. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [<u>*underlined italicized text within brackets*</u>].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

1.2.2 Acronyms and Terminology

The acronyms and terms used within this ST are described in Section 9 – “Acronyms and Terms.”

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security requirements provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The TOE is a server based software application that enables implementation of an acceptable usage policy for SMTP based e-mail within an organization.

The TOE enforces an acceptable usage policy for SMTP based e-mail within an organization by scanning the content, sender, destination, attachments and size of all SMTP based e-mail to and from the Internet then applying rules that have been established by authorized administrators of the TOE to support the established acceptable usage policy.

For this evaluation, the configuration given below is proposed:

- The TOE is deployed in the DMZ (demilitarized zone).

Short for ***dem****ilitarized* ***z****one*, the DMZ consists of a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

In essence, a DMZ is a controlled area outside of the trusted network that falls between the internal zone and the external zone (the term internal zone is the same as the trusted network). By design, a DMZ exists to compartmentalize security access. A DMZ is not a secure zone. The main objective is to reduce the risk of malicious users gaining access to an organization’s most valuable resources. In other words, it exists to protect internal resources from external users.

In this configuration the TOE is installed on a hardened server in the DMZ. In this configuration the TOE receives SMTP traffic for the organization, filter the e-mail accordingly, then route it to the next host, which is typically a mail server, gateway or bridgehead on the protected network.

The TOE stores all configuration data and filtering policies in a SQL database called STEMConfig and all logging data in a SQL database called STEMLog. The evaluated configuration requires a fully licensed version of SQL onto a separate, dedicated server. A dedicated database stores data for a single TOE in a single database. The SQL database is resident on the protected network and is an essential component in the TOE Environment.

Because of its placement in a DMZ, installation of the TOE should be done onto a hardened Windows 2000 or Windows 2003 Server, following Microsoft’s Operating System (OS) hardening recommendations for a stand-alone server.

Figure 1 below shows the details of the deployment configuration of the TOE:

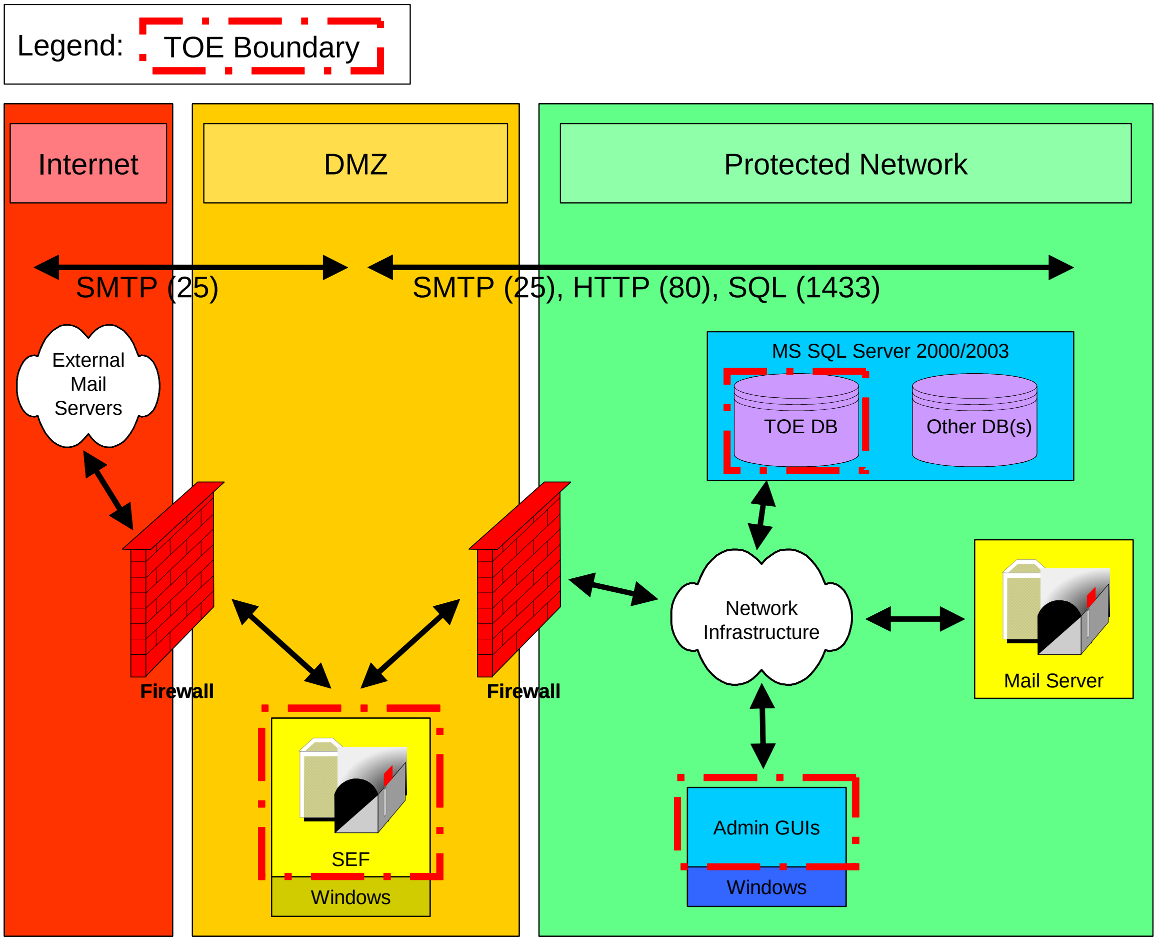

Figure 1 - Deployment Configuration of the TOE

As an SMTP based E-mail filter, the TOE also offers various other services, mainly:

- Dictionary-based message and attachment scanning
- Lexical-analysis-based message and attachment scanning
- MIME-format analysis
- Email loop detection
- Message size analysis
- Message destination (inbound/outbound) analysis
- Message recipient analysis
- Message sender analysis
- Number-of-recipients analysis
- URL scanning and analysis
- Message archiving
- Isolation of messages for administrative review
- Delayed delivery of messages
- Deletion of messages
- Appending of banners and/or footers to messages
- Message header modification
- Stripping HTML from messages
- Compressing attachments within messages
- Stripping attachments from messages
- Email notification

- Automated “blind carbon copy” of messages to defined recipients

2.2 Product Description

This section details the overall TOE solution, the various components of the TOE that are a part of this evaluation and their brief descriptions, the modes of configuration and management available in the TOE and the E-mail filtering process in the TOE.

The TOE enforces an acceptable usage policy for SMTP based e-mail within an organization by scanning the content, sender, destination, attachments and size of all SMTP based e-mail to and from the Internet then applying rules that have been established by authorized administrators of the TOE to support the established acceptable usage policy.

The TOE primarily comprises three core components

- Message Administrator
- Monitor
- Rules Administrator

In addition to the three core components the TOE comprises additional components which enhance the TOE's capabilities.

- Dictionary Management
- Scheduler
- Web Administrator
- Queue View

The various components of the TOE are available to an authorized administrator with the appropriate privileges from the three modes of configuration and management available in the TOE.

The three modes for the configuration and the management of the TOE are;

- A graphical user interface application on the Windows server machine that is hosting the TOE.
- A graphical user interface application client namely “SMTP Admin Client” running on a Windows machine on the protected network
- A web-based graphical user interface application which can be accessed from a web browser on a machine on the protected network.

Given below is a complete list of the various features of the TOE available for configuration and administration using the three modes.

- Server Application on the Windows server machine hosting the TOE:
    - Web Administrator
    - Rules Administrator
    - Monitor
    - Message Administrator
    - Dictionary Management
    - Scheduler
    - Queue View
    - Utilities
    - Documentation
    - Virtual Learning Agent
- GUI Application on a Windows machine on the protected network:
    - Web Administrator

  - Rules Administrator
  - Monitor
  - Message Administrator
  - Dictionary Management
  - Documentation
- Web-based GUI application that can be accessed from a web browser on a Windows machine on the protected network.
  - Dictionary Management
  - Message Administrator
  - Rules Log
  - System Log
  - Traffic Log
  - Help

The authorized administrators are the only direct users of the TOE. They can access and manipulate the configuration parameters of the TOE, define filtering rules, view e-mails in the various queues and view status information.

These direct users are divided into seven distinct roles with each role having predefined set of privileges. Users of the internal and external networks that send information through the TOE are considered external (unprivileged) users of the TOE, they have no access to the TOE Security Functions. Table 2 clearly demonstrates the various administrators and their privileges.

Table 2 - Administrator Privileges and Activities

Privileges	Administrative Activities and Security Attributes
All Permissions	• All administrative activities on all applicable security attributes
Message Administration	• View, edit, release, delete isolated emails
Rules Administration	• View, create, edit, delete, apply, disable email filter rules
Systems Administration	• View the real-time progress of emails passing through the TOE • Configure the TOE
Dictionary Management	• View, create, edit, delete dictionaries
View Logs	• View audit logs
User Management	• View, create, edit, delete administrative users and administrative user permissions

A TOE user is herein defined as a direct user of the TOE. Unless explicitly stated otherwise a TOE user is an authorized administrator of the TOE assigned to one the roles defined above in Table 2.

2.2.1 Brief Description of the Various Components of the TOE

In this section a brief description of the various components of the TOE is provided:

Message Administrator: The Message Administrator displays isolated e-mails so that an authorized administrator can release, move, or delete e-mails. Activity logs can also be viewed from the Message Administrator.

Monitor: The Monitor is used to display the progress of e-mails through the TOE in real time.

Rules Administrator: The Rules Administrator is used to set up rules by authorized administrators to meet the needs of an organization's Acceptable Use Policy.

Dictionary Management: Dictionaries are used in rules to detect particular kinds of content; the Dictionary Management tool can be used by administrators to configure Dictionaries to suit the rules.

Scheduler: The Scheduler tool is used to automate tasks such as

- Anti-Spam Agent
- URL Category List
- Database Maintenance
- Queue Synchronization

Queue View: Queue View tool is used to display information about messages currently held in queues.

Web Administrator: The Web Administrator is used to

- Manage isolated e-mails
- View logs
- Manage dictionaries from a remote location

2.2.2 The E-mail Filtering Process

The TOE's E-mail filter functionality is managed by four software services:

- The Receive Service
- The Rules Service
- The Send Service
- The Administration Service

The email filtering process is synopsized in the following paragraphs and detailed in the flowchart shown in Figure 2. When a mail server or firewall wishes to send an email to the TOE, the Receive Service on the TOE first pre-screens the e-mail's "envelope" and header against certain pre-screening criteria (for instance, to see if it originated from a "black-holed" mail server belonging to a known spammer); the email will be allowed to continue through the email filtering process if it does not meet any of the pre-screening criteria, otherwise it will be rejected.

If the email successfully passes through the pre-screening process, it is given to the Rules Service for filtering against the filtering rules. The email may cause one or more rules to be triggered, depending on each rule's criteria; rules that are triggered might cause the email to be isolated (where it will wait for review by the TOE administrator), have its delivery delayed for some set amount of time, be edited, be discarded, or be immediately delivered.

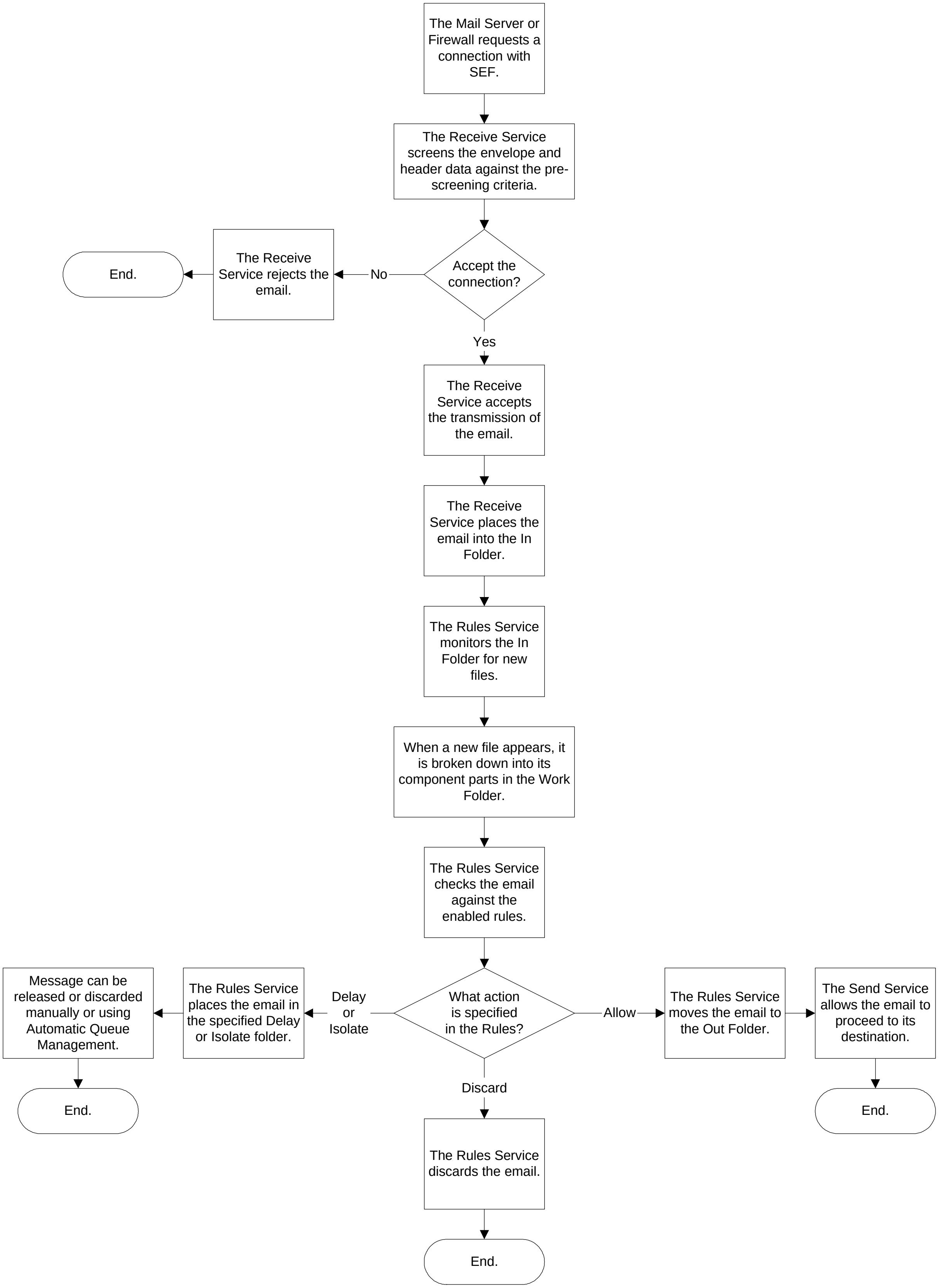
The Mail Server or Firewall requests a connection with SEF.
The Receive Service screens the envelope and header data against the pre-screening criteria.
Accept the connection?
No
The Receive Service rejects the email.
End.
Yes
The Receive Service accepts the transmission of the email.
The Receive Service places the email into the In Folder.
The Rules Service monitors the In Folder for new files.
When a new file appears, it is broken down into its component parts in the Work Folder.
The Rules Service checks the email against the enabled rules.
What action is specified in the Rules?
Delay or Isolate
The Rules Service places the email in the specified Delay or Isolate folder.
Message can be released or discarded manually or using Automatic Queue Management.
End.
Allow
The Rules Service moves the email to the Out Folder.
The Send Service allows the email to proceed to its destination.
End.
Discard
The Rules Service discards the email.
End.

Figure 2 - Filtering Process Flow Chart

2.3 TOE Boundaries and Scope

This section will primarily address what physical and logical components of the TOE are included in evaluation.

2.3.1 Physical Boundary

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is a Windows server based software application which runs on a hardened Windows server compliant to the minimum software and hardware requirements as listed in Table 3 below. The TOE is installed in a DMZ environment as depicted in the figure below. The essential physical components for the proper operation of the TOE in the evaluated configuration are

- SMTP Admin Clients running on Windows machines compliant to minimum requirements as stated in Table 3 inside the protected network.
- Web browser access inside the protected network for Web Administration of the TOE compliant to the minimum requirements as stated in Table 3.
- A fully licensed version of SQL database on a dedicated Windows server inside the protected network (This component is a part of the TOE Environment and hence discussed in Section 2.3.1.2)

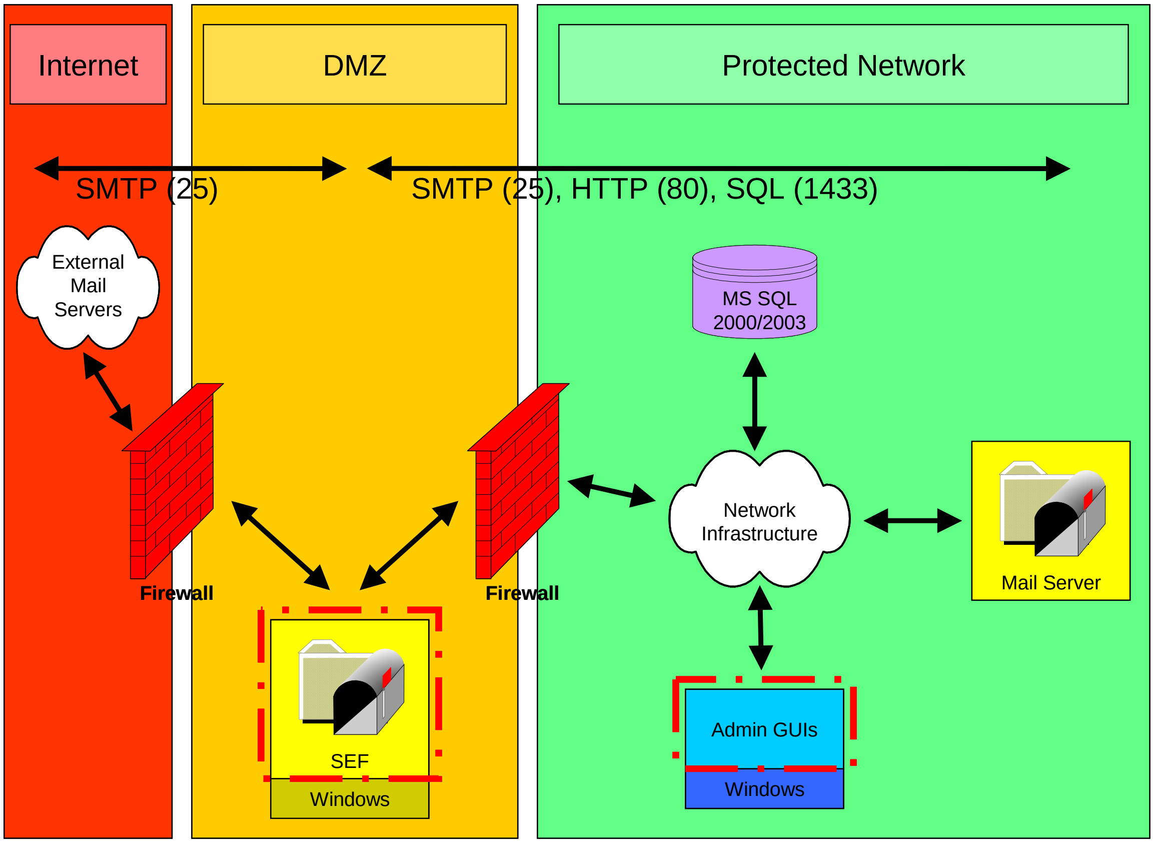

Figure 3 - Physical TOE Boundary

2.3.1.1 TOE Software

The TOE is a server based software application which runs on a Windows-based Server Operating System. Table 3 below specifies the minimum system requirements for the proper operation of the TOE.

Table 3 - TOE Minimum Requirements

Category	Requirement
Memory	• 512MB RAM; 1024 MB RAM recommended
Processor	• Intel Pentium III Processor 600MHz or higher
Operating Systems	• Windows 2000 Server with SP4 • Windows 2000 Advanced Server with SP4 • Windows Server 2003 Standard Edition • Windows Server 2003 Enterprise Edition • Windows XP SP1 (Remote Client only)
Disk Space	• 1 GB Minimum
Display	• Super VGA (800 x 600) or higher resolution video adaptor and monitor
MDAC	• Microsoft Data Access Components (MDAC) 2.7 (SP 2) or later
Other Requirements	• TCP/IP installed and configured with dedicated Internet connection • Internal or External DNS configured • E-mail system with SMTP gateway or Mail Transport Agent (MTA) installed • Web Browser Access: Microsoft Internet Explorer 5.0 or higher

2.3.1.2 TOE Environment

The TOE is deployed in a DMZ and works in conjunction with the essential components in an Email system such as:

- Windows 2000 or Windows 2003 Server Operating Systems for the installation of the TOE.
- Windows 2000, Windows 2003, or Windows XP Operating Systems for the installation of the TOE Component "**SMTP Admin Client**."
- Workstations on the protected network equipped with Microsoft Internet Explorer 5.0 or higher.
- A mail server, Gateway or a Bridgehead
- A fully licensed SQL Server which is dedicated for the TOE. The TOE stores all configuration data and filtering policies in a SQL database called STEMConfig and all logging data in a SQL database called STEMLog. The dedicated database stores data for a single TOE in a single database. The SQL database is resident on the protected network and is an essential component in the TOE Environment.

In the TOE environment the DMZ is segregated from the Internet by a firewall configured to allow only SMTP traffic inbound on port 25 to enter the DMZ and travel to the TOE's IP address. The DMZ is segregated from the protected network by a second, internal firewall. This firewall has a tunnel configured for port 25 from the e-mail Host to the TOE (in the DMZ). A tunnel on port 25 from the TOE to the e-mail host is also configured. The firewall rules permit the TOE to communicate with the SQL Server resident on the protected network over port 1433. The TOE uses the SQL Server for policy management and logging. The firewall rules permit the TOE to communicate with the management workstation resident on the protected network over port 80.

2.3.1.2.1 Security Considerations in the TOE Environment:

Because of the placement of the TOE in a DMZ, the TOE should be installed onto a hardened Windows 2000 or Windows 2003 server, following Microsoft's OS hardening recommendations for a stand-alone server. The TOE operates as a stand-alone server (nor part of a domain) and uses local accounts for services. When communicating with the SQL database, the TOE uses SQL authentication.

2.3.1.3 TOE Services

There are four software services running on the TOE which implement the TOE's E-mail filter functionality.

2.3.1.3.1 The Receive Service

The Receive Service accepts SMTP traffic on port 25 and checks each e-mail against a series of pre-screening criteria. The pre-screening criteria are based on:

- Protected Domains
- Trusted IP addresses (Relay Sources: IP addresses of mail servers allowed to relay mail)
- Blacklist (domains or e-mail addresses blocked from sending mail)
- Reverse DNS Lookup (Checking if IP address of the connection matched IP address returned from a DNS lookup of the HELO domain)
- Real-time Blackhole List (Checking if connecting IP address matches to any IP address in the specified real-time blackhole lists)
- Directory Harvest Detection (Detecting brute-force attempts to access mailboxes)
- Denial of Service Detection (Detecting attempts to use all system resource)
- Remote User Authentication (Allow remote e-mail clients (for example, dial-up users) to relay mail from non-trusted IP addresses).

If the message passes the pre-screening checks E-mail Filter accepts the message and hands it over to it to the Rules Service for further processing.

2.3.1.3.2 The Rules Service

The TOE works by checking e-mails against the rules specified by authorized administrators of the TOE with appropriate privileges, to enforce the organization’s Acceptable Use Policy. The Rules Service controls how e-mails are checked and processed. The main Rules Service branch in the Rules Administrator component of the TOE controls the Rules service properties. The Rules Service has two sub-branches namely Configuration and Queue Management.

Configuration:

The Rules Service Properties settings affect the folders used by the Rules service to access, hold and act upon e-mails, and how the actions of the service are logged.

There are three folders used by the Rules service to receive, store and act upon e-mail:

- **Rules Mail pick-up folder**: The Rules service monitors this folder for incoming e-mail. (C:\Program Files\SurfControl E-mail Filter\In)
- **Work folder**: The Work folder is where e-mails are held while they are being checked against the rules. (C:\Program Files\SurfControl E-mail Filter\Work)
- **Processed mail drop off folder**: If an e-mail has been checked against the rules and allowed to proceed it will be placed in the “Processed mail drop off folder” If it has been delayed or isolated it will be placed in the folder specified by the rule it triggered. (C:\Program Files\SurfControl E-mail Filter\Out)

The Rules service logging options control how the actions of the Rules service are recorded and where they are displayed:

- Real-time console: The actions of the Rules service are displayed in the real-time console
- The status of the Rules service is displayed in the System Log in Message Administrator. For example, if you add and activate a new rule, you will see a message saying that the rules configuration has been reloaded.

The Rules Service Configuration branch deals with

- Specifying the number of Rules Processing threads: Specify the number of messages that the Rules service can process at any one time. (For example, using the default setting of 4 means that the Rules service can check 4 e-mails at the same time. The default setting is 4, the maximum is 16. Each extra thread added requires approximately 16MB of memory above the minimum system requirement of 512MB RAM.)

- Dealing with Corrupted e-mail messages: If an e-mail has been corrupted, the Rules service may not be able to check it against the enabled rules. An authorized administrator with the appropriate privileges can specify how the TOE acts in the event that an e-mail becomes corrupted:
    - Release corrupted messages: The corrupted e-mail will not be checked by the Rules service, and will be sent directly to its recipient. A copy of the e-mail will be left in the **In** folder.
    - Move corrupted messages to folder: The corrupted e-mail will be moved to the folder you specify. The administrator should specify the path of the folder, or browse to the destination and select.
    - Copy to folder and send corrupted message: The TOE will take a copy of the corrupted e-mail and save it in the folder specified by the administrator, and then send the original to its recipient. The administrator should specify the path of the folder, or browse to the destination and select.

Queue Management:

The Rules service checks the e-mail against the list of enabled rules, starting at the top of the window and working through the enabled rules in order until the message triggers a rule. There are four automatically managed actions the TOE can take:

- Discard the e-mail
- Release the e-mail
- Isolate the e-mail
- Delay the e-mail

E-mails that are **isolated** or **delayed** are held in dedicated queue folders until they are either discarded or released and sent to their recipient. The TOE is installed with 11 pre-configured queues for easy management of e-mail, but an authorized administrator can set up others to suit the needs of the deployment.

The four actions objects – Allow, Delay, Discard, and Isolate are **terminating actions**. Once the TOE performs a terminating action on an e-mail, no further processing takes place If an e-mail passes all the rules checks without being isolated, delayed or discarded it is placed in the Out folder for delivery to its destination.

Rules Objects: Rules Objects are the basic logical units that are available to authorized administrators to create a rule. There are five types of Rules object – the order in which they are provided in the Rules Administrator component of the TOE the logical order in which they should be added to a rule. The five types of Rules Objects are:

- A **Who** Object
- A **What** Object
- An **Operations** Object
- A **Notify** Object
- An **Actions** Object

A **Who** object in a rule affects who the rule applies to. The available options are:

- From Users and Groups
- Inbound/Outbound Mail
- To Users and Groups

If a Who object in a rule is not specified it will apply to everybody sending and receiving e-mail in and out of the protected domain.

A **What** object in a rule checks the characteristics of the e-mail against the criteria specified. The available options are:

- Anti-Spam Agent
- Dictionary Threshold
- File Attachment

- Illegal Mime Format
- LexiMatch
- Loop Detection
- Number of recipients
- URL Category List
- When

An **Operations** object in a rule will modify the e-mail in the way specified. The available options are:

- Archive Message
- Compress Attachments
- Footers and Banners
- Header Modification
- HTML Stripper
- Strip Attachments

A **Notify** object in a rule will send an e-mail to the user you specify to notify them that a rule has been triggered. The available options are:

- Blind Copy
- E-mail Notification

An **Actions** object in a rule will perform an action on the e-mail. Once an action is carried out, no further processing takes place on the e-mail. The available options are:

- Allow Message
- Delay Message
- Discard Message
- Isolate Message

2.3.1.3.3 The Send Service

The Send Service controls what happens to e-mails after they have been allowed to proceed through the TOE by the Rules Service.

The main Send Service branch of the Server Configuration console controls general Send Service settings. It also has three sub-branches:

- Connections
- Routing
- Requeuing scheme

When an e-mail has been checked and allowed to proceed, it is placed in the Send Mail Pickup Folder (the **Out** folder), where the Send Service can pick it up for delivery. By default the path is: C:\Program files\SurfControl E-mail Filter\Out. When an e-mail is moved to the Out folder for delivery, you can log the action in two places: The real-time console and the system log.

The Connections branch of the Send Service controls the type and number of connections that the TOE can make when it is sending e-mails. There are three kinds of Connections settings that an authorized administrator can configure:

- Connections
- SMTP Options
- SMTP EHLO/HELO command

In the Routing branch of the Send Service an authorized administrator can define the TOE's routing tables. The routing table defines the location of your mail servers so that TOE can identify where to send e-mail within the protected domain.

If the TOE cannot send a message (for example because it cannot connect to a remote mail host), it will store the message in a queue and try to send it again at intervals. An authorized administrator can specify how often these attempts to resend messages take place.

It can be configured based on:

- How many times the TOE will try to send the message
- The length of time between each attempt.

2.3.1.3.4 Administration Service:

The Administration branch controls general system settings. It has one sub branch, Configuration, where you can configure remote administrative access to the TOE.

E-mail Administrator's Address: When an administrator sets up a protected domain he is are prompted to specify the e-mail address of the system administrator for that domain. If the TOE needs to send a notification it examines each recipient of the message and checks each domain against the Protected Domains list. As soon as it finds a recipient in a protected domain, the TOE will send the notification from the administrator of that domain. If none of the recipients are in any of the protected domains, the TOE will send the notification from the e-mail address specified in the Administration Settings.

Print Configuration: An authorized administrator with the appropriate privileges can print a record of the TOE configuration by clicking **Print Configuration**. A text file will display showing all the Server Configuration settings.

The administrators branch is where an authorized administrator with the appropriate privileges can configure access to remote administration of TOE. There are two methods of remote access:

- **Web Administrator**: The TOE's Web Administrator is a Web-based application that gives remote access to selected TOE functions from any computer on the protected network via a Web browser.
- **TOE Administration Clients**: The TOE's Administration Clients can be installed on a remote computer on the protected network and used to access selected TOE functions.

Remote Administration Permissions

Table 4 below shows the remote administration permissions that can be set, and which method of remote access can be used for each permission setting.

Table 4 - Remote Administration Permissions

Permission Setting	Access	Access Method	
		Web Administrator	SMTP Administration Client
All Permissions	All of the permissions in the lists below.		
Message Administration	View and work with isolated messages using Message Administrator functions	✓	✓
Rules Administration	Create and manage rules to enforce organizations Appropriate Use Policy (AUP) using Rules Administrator functions.		✓

Permission Setting	Access	Access Method	
		Web Administrator	SMTP Administration Client
Systems Administration	View the progress of emails through E-mail Filter in real time. Configure E-mail Filter using the Server Configuration console.		✓
Dictionary Management	Manage Dictionaries and their content.	✓	✓
View Logs	View the Traffic, Rules, and System logs from a remote computer.	✓	✓
User Management	Set administrative access to E-mail Filter.		✓

Adding/Editing/Deleting a Remote Administrator Account: In order to enable Remote Administration an authorized administrator with the appropriate privileges can add/delete/edit administrator accounts and set their permissions from the Server Configuration Console. If there are no administrator accounts, Remote Administration will be unavailable.

The TOE logical boundary in Figure 4 below depicts a detailed representation of the different logical components of the TOE:

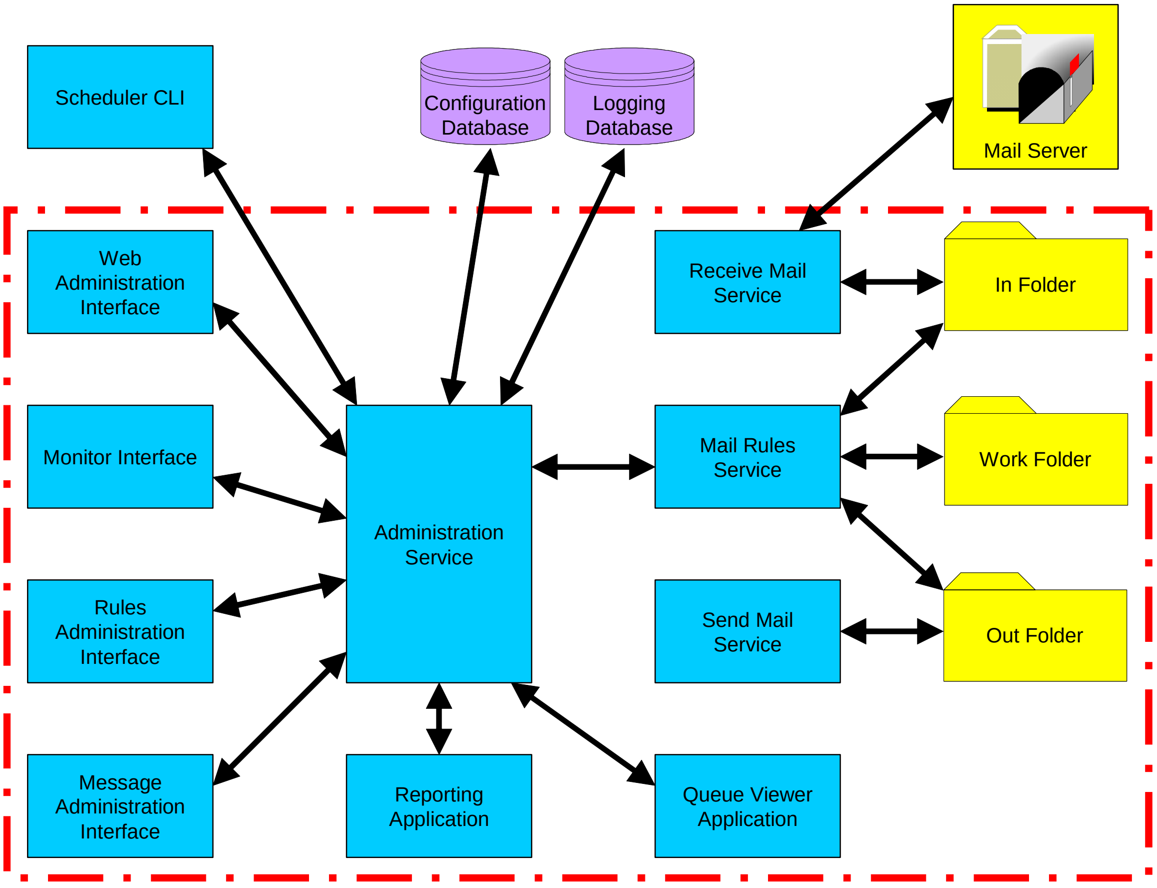

Figure 4 - TOE Logical Boundary

2.3.2 Logical Boundary

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

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

2.3.2.1 Security Audit

One of the primary functions performed by the TOE is the auditing/logging of critical events. All audit data is stored in the System Log database. The System Log contains the records of regular operations and exceptions from various components of the system including information about the start-up and shutdown of the audit functions and all audited events listed in FAU_GEN.1. The TOE also records for each event the date and time an event occurred, the type and outcome of the event, and the subject identity.

2.3.2.2 User Data Protection

The TOE controls the flow of incoming and outgoing SMTP messages, which are processed by the TOE. They are defined as User Data for the purpose of this evaluation. The TOE enforces information flow policies on the SMTP messages as they are processed by the TOE. Through the creation of information flow control policies, traffic flows across an interface can be controlled by defining the types of traffic permitted to pass from one security zone to another within the TOE. The information flow policy is supported by allowing a TOE user to define information flow policies that specify which SMTP messages are allowed to be processed by the TOE, which should be rejected and which should require additional handling. Additionally, the TOE controls access to all messages that are stored within the TOE by a defined access control policy.

The TOE allows TOE users who possess the appropriate privileges to define filters on email sent and email to be received by external senders and receivers. As an email advances through the pipeline it is checked against a successive set of filters. Depending on the filter, various rules can be implemented and several actions could be taken. Rules define the collection of SMTP messages that the filter can act upon (messages from a certain IP address or within a range of IP addresses, messages with a message body size bigger than a predefined value, messages destined to a certain domain etc.) whereas actions define the operation or operations to be performed on the SMTP message (deliver, drop, quarantine, archive etc.).

2.3.2.3 Identification and Authentication

TOE Users must identify themselves and authenticate to the TOE in order to gain access to the various services provided by the TOE. There are four graphical user interfaces (GUIs) which allow TOE Users to interact with the TOE: the Web Administrator, the Rules Administrator, the Monitor, and the Message Administrator. TOE Users are authorized only to initiate the authentication process prior to identification and authentication. Before a TOE user is successfully identified and authenticated, no other TSF-mediated actions can be performed on behalf of the user.

The username and password of the TOE user are verified by the Administration Service. The Administration Service receives the username and password from the GUIs. The username and password provided are compared to the entries in the configuration database, and if a match is found then the user is assigned a role (or roles) and can access the TOE. The privileges which are assigned to the user depends on the roles to which the TOE user belongs (All Permissions, Message Administration, Rules Administration, Systems Administration, Dictionary Management, View Logs, User Management). If no match is found then access is not granted and the user is offered the chance to login again.

2.3.2.4 Security Management

The TOE lets an authorized administrator of the TOE with appropriate privileges perform various management functions. Specifically, the TOE provides several functions through the TOE server application and TOE remote administrator components for the management and administration of the TOE.

The TOE user is provided with four Graphical User Interface (GUI) components to perform configuration, management, and troubleshooting tasks. The GUIs offer several graphical commands for management and administration. These commands can be issued by an administrator with the appropriate privileges. The TOE maintains various administrator roles based on permissions as detailed in Table 2. These roles together are referred to as TOE Users. The GUIs offer various tools and “wizards” for the TOE Users by which various configuration and management tasks can be performed.

2.3.2.5 TOE Self Protection

Non-bypassability of the TOE is provided by a combination of the basic configuration and enforcement of the security policy rules. The assumed secure basic configuration maintaining physical and logical isolation supports the Protection of Security Functions (PSF). The functions that enforce the TOE Security Policy (TSP) will always be invoked, before any function within the TSF Scope of Control is allowed to proceed. The TOE can be accessed through the GUI applications on the server hosting the TOE, through the SMTP Admin Clients from a Windows machine on the protected network, or from a web browser on a machine resident on the protected network. These are the only three avenues of user interaction to the TOE.

Some of the TOE self-protection (e.g., against physical tampering) is ensured by the TOE environment. In particular, it is assumed that the Windows server hosting the TOE and the remote administration components of the TOE on the protected network will remain attached to the physical connections made by an authorized administrator responsible for the proper installation of the TOE so that the TOE cannot be bypassed.

The security functions are physically separated from the unauthenticated external IT entities which send and receive SMTP messages through the TOE. The TOE configuration protects its management functions by isolating them using identification and authentication and by limiting them exclusively to the port assigned to accept SMTP based e-mail traffic.

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- The ability to scan emails for viruses using the Anti-Virus Agent
- The ability to scan image attachments for pornographic content using the Virtual Image Agent
- The External Program Plugin object to integrate the TOE with an external executable or batch file
- The Virtual Learning Agent (VLA) which is a content development tool that can be used to train to understand and recognize business-confidential content
- SQL database services

3 Security Environment

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects
- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies the TOE must comply with

3.1 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

A.FIREWALL All ports needed for proper operations of the TOE will be opened at the firewall.

A.INSTALL The TOE is delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.

A.MANAGE There will be one or more competent TOE user(s) assigned to manage the TOE and the security functions it performs.

A.INTMANG It is assumed that the TOE environment will only be managed from within the protected network.

A.NO_EVIL A TOE user is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation.

A.PHYSICAL The TOE will be physically protected to prevent hostile individuals engaging in theft, implantation of devices, or unauthorized alteration of the physical configuration of the TOE (e.g. bypassing the TOE altogether by connecting the corporate and hostile networks together).

A.TRANSFER All SMTP traffic between networks connected to the TOE will be transferred through the TOE.

A.TRUSTED The users of the internal network from which administration of the TOE is performed are trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks.

A.HARDENED The underlying operating systems will be hardened to remove all mechanisms and services that are not required by the TOE.

A.AUDFUL The authorized user of the machine used to store audit data must ensure that the audit data is archived and that the storage space does not become exhausted.

A.TIMESTMP It is assumed that the IT environment will provide the TOE with the necessary reliable timestamps.

3.2 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are however assumed not to be willfully hostile to the TOE)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 - Security Objectives.

3.2.1 Threats Addressed by the TOE

The following threats are to be addressed by the TOE:

T.SEND The attempts of an attacker to send harmful SMTP traffic (e-mail) may go undetected posing a threat to the protected network.

T.MEDIAT An attacker who is not a TOE user may send impermissible information through the TOE which results in the exploitation of resources on the internal network or undesired SMTP messages being delivered.

T.OPENRELAY An attacker who is not a TOE user may send multiple SMTP messages to the TOE, where those messages are addressed to recipients whose e-mail addresses fall outside the set of address for which the TOE handles e-mail. The intent of this attack is to utilize the resources of the TOE to deliver bulk e-mail on behalf of the originator.

T.REMCONN An attacker who is not a TOE user may exploit network protocol(s) based vulnerabilities and compromise TOE services and data assets by establishing a remote connection to the TOE.

T.UNSOLICT An attacker who is not a TOE user may send unsolicited bulk mail where the content of those messages falls outside of a defined acceptable use policy posing a threat to the effective processing of other SMTP messages.

T.USRDATA An attacker who is not a TOE user could access individual e-mail messages stored on the TOE, by viewing, sorting, releasing, deleting or moving to (queue) the queued e-mails stored on the TOE.

3.2.2 Threats Addressed by the TOE Environment

The following threats are to be addressed by the TOE environment:

TE.AUDFUL An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity.

3.3 Organization Security Policies

There are no organizational Security Policies specified for the TOE.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

The principal security objective of this TOE is to reduce the vulnerabilities of a corporate email system exposed to a hostile network by preventing any direct connections from a hostile network to any potentially vulnerable components of that email system. Additionally, the TOE has the objectives of providing message integrity checks, message filtering, and message routing services to provide a secured delivery channel for validated messages. The specific security objectives are as follows:

O.ADMIN The TOE must provide a secure method of administrative control of the TOE, ensuring that TOE users with the appropriate privileges, and only these TOE users, can exercise such control.

O.AUDIT The TOE shall provide a means to detect and collect SMTP traffic events for all e-mails flowing through the TOE.

O.DIRECT The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to the TOE.

O.MESACC The TOE shall enforce an access control policy on TOE users who wish to access queued SMTP e-mails stored within the TOE.

O.MAILRVW The TOE shall review all incoming and outgoing SMTP messages to determine that the defined policies are enforced and the appropriate actions are performed on every message.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

OE.HARDENED The underlying operating system will be hardened to remove all mechanisms and services that are not required by the TOE.

OE.TIMESTMP The TOE operating environment shall be able to generate reliable timestamps for the TOE's use.

OE.FIREWALL The Firewall must have all ports needed for proper operations of the TOE opened.

OE.TRANSFR The TOE must be installed between networks wishing to transfer SMTP messages. This must be the only connection between the networks permitting the flow of SMTP traffic.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

NOE.AUDIT Authorized users of the audit facilities must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.

NOE.DELIV Those responsible for the TOE must ensure that it is delivered, installed, managed, and operated in accordance with documented delivery and installation/setup procedures.

NOE.MANAGE A TOE user is assigned with responsibility for day to day management and configuration of the TOE, including the management of the audit trail.

NOE.INTMANG The TOE can only be managed from the protected network and cannot be managed from the external network.

NOE.NOEVIL TOE users are non-hostile and follow all administrator guidance.

NOE.PHYSIC The TOE must be physically protected so that only TOE users who possess the appropriate privileges have access.

NOE.REVIEW The configuration of the TOE will be inspected on a regular basis to ensure that the configuration continues to meet the organization’s security policies in the face of:

- Changes to the TOE configuration
- Changes in the security objectives
- Changes in the threats presented by the hostile network
- Changes (additions and deletions) in the services available between the hostile network and the corporate network

NOE.TRAIN Those responsible for the TOE must train TOE users to establish and maintain sound security policies and practices.

NOE.TRUSTED The users of the network from which the TOE will be administered must be trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks.

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.2.1.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 5 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 5 - TOE Security Functional Requirements

SFR ID	Description	ST Operation			
		Selection	Assignment	Refinement	Iteration
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Restricted audit review				
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		✓	✓	
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1 (a)	Management of security functions behaviour	✓	✓		✓
FMT_MOF.1 (b)	Management of security functions behaviour	✓	✓		✓
FMT_MOF.1 (c)	Management of security attributes	✓	✓		✓
FMT_MOF.1 (d)	Management of security attributes	✓	✓		✓
FMT_MSA.1 (a)	Management of security attributes	✓	✓	✓	✓
FMT_MSA.1 (b)	Management of security attributes		✓	✓	✓
FMT_MSA.3 (a)	Static attribute initialization	✓	✓	✓	✓
FMT_MSA.3 (b)	Static attribute initialization	✓	✓	✓	✓
FMT_MTD.1 (a)	Management of TSF data	✓	✓		✓
FMT_MTD.1 (b)	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1	Non-bypassability of the TSP				

Section 5.1 contains the functional components from the CC Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.2.1.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit 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 the Receive Service; Startup and shutdown of the Rules Service; Startup and shutdown of the Send Service; Reload of the Rules configuration*].

FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

FAU_SAR.1.1

The TSF shall provide [*the applicable authorized roles listed in Table 2*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1

The TSF shall provide the ability to perform [*searches, sorting, and/or ordering*] of audit data based on [*Date, Event, Server DN, Server Name, and/or System Log ID*].

Dependencies: FAU_SAR.1 Audit review

5.1.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

FDP_ACC.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] on

[

- *Subjects: identified and authenticated TOE users;*
- *Objects: information (email) in the queues;*
- *Operations: view, sort, release, delete, Move to (queue)*

].

Dependencies: FDP_ACF.1 Security attribute based access control.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the [Discretionary Access Control SFP] to objects based on the following:

[

- *Subjects: identified and authenticated TOE users*
  - *Username*
  - *Password*
  - *Email address*
  - *Roles*
  - *Role permissions*
- *Objects: information (email) in the quarantine*
  - *Presumed sender IP*
  - *Recipient IP*
  - *Subject*
  - *Date*
  - *Message Size*

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*a TOE user can access the queues and perform operations on information (email) in the queue if he has the required privileges as defined in Table 2;*].

FDP_ACF.1.3

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

FDP_ACF.1.4

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

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1

The TSF shall enforce the [*discretionary information flow control SFP*] on

[

- *Subjects: presumed external IT entities that send and receive SMTP based e-mails through the TOE to one another;*
- *Information: SMTP traffic (e-mail) sent through the TOE from one subject to another;*
- *Operation: Archive Message, Compress Attachments, Add Footers and Banners, Header Modification, Strip HTML, Strip Attachments, Blind Copy, E-mail Notification, Allow Message, Delay Message, Discard Message, Isolate Message*

].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1

The TSF shall enforce the [*discretionary information flow control SFP*] based on the following types of subject and information security attributes: [*email header information, attachment type, attachment content, message content, presumed sender, receiver(s), presumed sending/relaying mail server IP address or domain, and/or time of day that message was sent/received*].

[

- *Subject security attribute:*
  - *Sender's presumed IP address*
  - *Recipient IP address*
- *Information:*
  - *E-mail header information*
  - *Attachment type*
  - *Attachment content*
  - *Message content*
  - *Presumed sender*
  - *Receiver(s)*
  - *Presumed sending/relaying mail server IP address or domain*
  - *Time of day that message was send/received*

].

FDP_IFF.1.2

The TSF shall permit an information flow between a **source subject and a destination subject** ~~controlled subject and controlled information~~ via a controlled operation if the following rules hold: [*subject's information can flow through the TOE if all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information security attributes, created by an administrator who possesses the appropriate privileges*].

FDP_IFF.1.3

The TSF shall enforce the [*no additional rules*].

FDP_IFF.1.4

The TSF shall provide the following [*no additional capabilities*].

FDP_IFF.1.5

The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.6

The TSF shall explicitly deny an information flow based on the following rules: [*none*].

Dependencies: FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialization

5.1.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

[

- *Username*
- *Password*
- *Email address*
- *Roles*
- *Role permissions*

].

Dependencies: No dependencies

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.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UID.2 User identification before any action

FIA_UID.2.1

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

Dependencies: No dependencies.

5.1.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 (a)

The TSF shall restrict the ability to [*modify the behavior of*] the functions [*TOE Management Functions*] to [*an administrator with All Permissions or System Administration Permissions*].

FMT_MOF.1.1 (b)

The TSF shall restrict the ability to [*disable, enable, and/or modify the behavior of*] the functions [*Information Flow Control Functions*] to [*an administrator with All Permissions, Message Administration Permissions, Rules Administration Permissions or Dictionary Management Permissions*].

FMT_MOF.1.1 (c)

The TSF shall restrict the ability to [*modify the behavior of*] the functions [*Access Control Functions*] to [*an administrator with All Permissions or User Management Permissions*].

FMT_MOF.1.1 (d)

The TSF shall restrict the ability to [*modify the behavior of*] the functions [*Audit Functions*] to [*an administrator with All Permissions or View Logs Permissions*].

Dependencies: FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 (a)

The TSF shall enforce the [*discretionary access control SFP*] to restrict the ability to [*modify*] the security attributes [*username, password, e-mail address, permissions*] to [*an administrator with All Permissions or User Management Permissions*].

FMT_MSA.1.1 (b)

The TSF shall enforce the [*discretionary information flow control SFP*] to restrict the ability to [*query, modify, delete, [create]*] the **information flow control policy rulesets** ~~security attributes~~ to [*an administrator with All Permissions, Message Administration Permissions, Rules Administration Permissions or Dictionary Management Permissions*].

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control], FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 (a)

The TSF shall enforce the [*discretionary access control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (a)

The TSF shall allow the [*an administrator with All Permissions or User Management Permissions*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1 (b)

The TSF shall enforce the [*discretionary Information Flow Control SFP*] to provide [*permissive*] default values for the **information flow control policy rulesets** ~~security attributes~~ that ~~are~~ **is** used to enforce the *SFP*.

FMT_MSA.3.2 (b)

The TSF shall allow the [*no one*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 (a)

The TSF shall restrict the ability to [*view, sort*] the [*audit data*] to [*an administrator with All Permissions or View Logs Permissions*].

FMT_MTD.1.1 (b)

The TSF shall restrict the ability to [*modify*] the [*configuration*] to [*an administrator with All Permissions or System Administration Permissions*].

Dependencies: FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

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

[

- *TOE Management Functions*
- *Information Flow Control Functions*
- *Access Control Functions*
- *Audit Functions*

].

Dependencies: No dependencies

FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the roles [*listed in Table 2*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.5 Class FPT: Protection of TOE Security Functions

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1

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

Dependencies: No dependencies.

5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirements for its IT environment. The stated Security Functional Requirement on the IT Environment of the TOE presented in this section has been drawn from Part 2 of CC Version 2.2 and hence conformant to CC Version 2.2 Part 2.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

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

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1

The **IT Environment hosting the TOE** shall provide reliable time stamps for **the TOE's** use.

FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1

The **IT Environment hosting the TOE** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2

The **IT Environment hosting the TOE** shall be able to [*prevent*] modifications to the audit records.

6 TOE Summary Specification

This section presents information to detail how the TOE meets the functional and assurance requirements described in previous sections of this ST.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

The TOE records logs of critical events in the System Log table in a database. These records can be reviewed from within the TOE. The TOE also provides a mechanism to archive and purge the System Log as a means to prevent audit data storage exhaustion.

The System Log contains the records of regular operations and exceptions from various components of the system including information about the start-up and shutdown of the audit functions and all audited events listed in FAU_GEN.1. The TOE also records for each event the date and time an event occurred, the type and outcome of the event, and the subject identity. Each audit record includes the "subject identity" allowing a viewer to associate each event with the person that caused the event. The time that is used to time stamp all the audit records is always pulled from the same source: the SQL server hardware.

The TOE audit records contain the following information:

Table 6 - Audit Record Contents

Field	Content
Date	Date and time that the event occurred
Event	The type of the event being logged (service started or stopped, rules configuration reloaded)
System Log ID	Unique record number for the audit record
Server Name	The name of the server which reported the event
Server DN	The domain name of the server which reported the event

TOE Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, and FAU_SAR.3.

6.1.2 User Data Protection

For the purpose of this evaluation User Data is defined as the SMTP based e-mail messages that are processed by the TOE, as these messages are owned by the external IT entities sending the emails and are clearly not required system data as defined by Common Criteria. The TOE provides a discretionary information flow policy of the SMTP based e-mail messages (user data) as they flow through the various filtering mechanisms of the TOE. Additionally, the TOE provides a discretionary access control policy that enforces the policy in such a way that only identified and authenticated TOE users can access the User Data (SMTP e-mail messages) stored in the various queues of the TOE. Further the discretionary access control policy allows TOE users who possess the appropriate privileges to access User Data in the queues and perform allowable operations on the User Data stored in the queues.

The TOE allows TOE users who possess the appropriate privileges to define discretionary information flow control policies on SMTP based e-mail sent and to be received by external senders and receivers as primarily identified by their IP addresses. The TOE scheme on which the information flow control policies are based depends on a series of successive filtering mechanisms in the form of three primary services. The receive service, the rules service and the send service. As an e-mail flows through the various services it is checked initially against pre-screening criteria in the receive service subsequently the e-mail is subject to filtering by rules defined by rule objects in the rules service. These rules are collection of criteria that an e-mail will be checked against,

Rules define the collection of criteria that a filter can act upon (Anti-Spam Agent, Dictionary Threshold, File Attachment, Illegal Mime Format, LexiMatch, Loop Detection, Number of recipients, URL Category List, When) whereas actions define the operation or operations to be performed on these messages (Archive Message Compress Attachments Footers and Banners Header Modification HTML Stripper Strip Attachments, Blind Copy, E-mail Notification, Allow Message, Delay Message, Discard Message, Isolate Message). Once an action is carried out, no further processing takes place on the e-mail. The Send Service controls what happens to e-mails after they have been allowed to proceed through the TOE by the Rules Service. When an e-mail has been checked and allowed to proceed, it is placed in the Send Mail Pickup Folder (the Out folder), where the Send Service can pick it up for delivery. If the TOE cannot send a message (for example because it cannot connect to a remote mail host), it will store the message in a queue and try to send it again at intervals. An authorized administrator can specify how often these attempts to resend messages take place.

TOE Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, and FDP_IFF.1.

6.1.3 Identification & Authentication

There are four Graphical User Interfaces (GUIs) which allow the TOE users to interact with the TOE: the Web Administrator, the Rules Administrator, the Monitor, and then Message Administrator. Each GUI collects TOE user identification and authentication credentials from the TOE users. Before a user is successfully identified, no other TSF-mediated actions can be performed on behalf of the user. Similarly, before a user is successfully authenticated, no other TSF-mediated actions can be performed on behalf of the user.

The username and password of the TOE user are verified by the Administration Service. The Administration Service receives the username and password from the GUIs. The username and password provided are compared to the entries in the configuration database, and if a match is found then the user is assigned a role (or roles) and can access the TOE. The privileges which are assigned to the user depends on the roles to which the TOE user belongs (All Permissions, Message Administration, Rules Administration, Systems Administration, Dictionary Management, View Logs, User Management). If no match is found then access is not granted and the user is offered the chance to login again.

User accounts have the following attributes: username, password, email address, roles, and the specific permissions for a particular role . These attributes are stored in the configuration database.

The Monitor GUI provides TOE users who possess the appropriate privileges with a means to view and edit user attributes, including the password and the assigned role(s)..

The TOE incorporates user defined authentication tokens (i.e. passwords) that can be analyzed via probabilistic or permutational means. The TOE requires that the minimum password length used be equal to or greater than 6 alphanumeric characters. Passwords are also case sensitive. The number of possible passwords is therefore 56,800,235,584. On average a brute force attack will have to try half of these values before finding the correct password. The probability of guessing a password is low enough to be considered consistent with safe practice measures at EAL2. For this reason a strength of function rating of SOF-basic is claimed for this TOE.

TOE Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.2, and FIA_UID.2.

6.1.4 Security Management

The TOE lets a TOE user who possesses the appropriate privileges perform various management functions. Specifically, the TOE provides several commands for the management and administration of the TOE.

6.1.4.1 User accounts

The TOE imposes no limit to the number of user accounts that can be created for the system and maintains seven roles: All Permissions, Message Administration, Rules Administration, System Administration, Dictionary Management, View Logs, and User Management. For each new user account created, a username and an email address need to be specified, and the user needs then to be assigned to one or more of the seven possible roles. User-specific permissions must also be assigned within each role to which the user is assigned (except the “All Permissions” role); these permissions determine upon which message queues and functions the user may exercise the privileges granted by his role(s). The roles are detailed in Table 2. Each role is an administrative role – there are no non-administrative users of the TOE.

Users with the role “All Permissions” can perform any action and exercise any functionality which the TOE provides. Users with roles other than “All Permissions” can perform some subset of actions and exercise some subset of functionality provided by the TOE, depending upon the roles to which they are assigned, up to and including the equivalent privileges of the “All Permissions” role if they happen to be assigned to all of the other roles.

Only an user with the “All Permissions” or “User Management” role can create and/or manage user accounts. These two roles are the only roles that have the privileges to modify the behavior of the access control functions. Such an administrator can modify the behavior of the access control functions by querying, modifying, and deleting the role and password security attributes of a TOE user and by querying, modifying, or creating an account’s “User Name” security attribute.

6.1.4.2 Management Commands

The audit log may be viewed via the Message Administrator GUI by TOE users with the “All Permissions” or “View Logs” roles. The TOE itself may be managed by users with the “All Permissions” or “System Administration” roles.

The right to issue mail flow control commands is reserved to users with the “All Permissions,” “Message Administration,” “Rules Administration,” and “Dictionary Management” roles. These commands give TOE administrators the ability to enable, disable or modify the behavior of the mail flow policy and query, modify, delete or create new filters and rulesets. However, no one has any control over any of the e-mail’s security attributes.

By default, when no policy is yet created, the TOE will permit all email traffic to flow through the TOE.

TOE Functional Requirements Satisfied: FMT_MOF.1 (a), FMT_MOF.1 (b), FMT_MOF.1 (c), FMT_MOF.1 (d), FMT_MSA.1 (a), FMT_MSA.1 (b), FMT_MSA.3 (a), FMT_MSA.3 (b), FMT_MTD.1 (a), FMT_MTD.1 (b), FMT_SMF.1, and FMT_SMR.1.

6.1.5 TOE Self Protection

Non-bypassability of the TOE is provided by a combination of the basic configuration and enforcement of the security policy rules. The assumed secure basic configuration maintaining physical and logical isolation supports the Protection of Security Functions (PSF). The functions that enforce the TOE Security Policy (TSP) will always be invoked, before any function within the TSF Scope of Control is allowed to proceed. The TOE can be accessed through the GUI application on the server hosting the TOE, through the SMTP Admin Client from a Windows machine on the protected network or from a web browser on a machine resident on the protected network. These are the only three avenues of user interaction to the TOE.

The SMTP Admin Client and the Web Administrator, are located on the protected network, they have to access the TOE server application and successfully authenticates themselves to perform any security management or policy changes to the TOE. In addition to this Remote Administration is enabled only on the Server Console which aids in the strengthening of the Identification and Authentication function. The security policy rules enforced by the TOE are applied to every SMTP based e-mail and no e-mail can bypass this filtering mechanism.

The TOE server application resident in the DMZ does not host any configuration or management information, the same is protected in a dedicated database resident inside the protected network. Only the services necessary for the proper operation of the TOE are enabled on the firewall such as Port 25 for SMTP (for transfer of user data (SMTP e-mails)), Port 1433 for SQL, and Port 80 for HTTP (for management). The configuration information is passed on to the SQL database from the TOE server application using SQL authentication mechanisms and the same mechanisms are used for loading of configuration information from the database to the TOE server application. Thus ensuring confidentiality and integrity of the data transfer. The TOE runs only processes that are needed for its proper execution and does not run any other user processes. In the process of filtering SMTP based e-mail the TOE runs only the policy rulesets that are enabled and doesn't provide a provision to run any other executables (so long as the "External Program Plugin" rules object is not used). This implementation provides the required TSF domain separation.

Some of the TOE self-protection (e.g., against physical tampering) is ensured by the TOE environment. In particular, it is assumed that the Windows server hosting the TOE and the remote administration components of the TOE on the protected network will remain attached to the physical connections made by an authorized administrator responsible for the proper installation of the TOE so that the TOE cannot be bypassed.

The security functions are physically separated from the unauthenticated external IT entities which send and receive SMTP messages through the TOE. The TOE configuration protects its management functions by isolating them using identification and authentication and by limiting them exclusively to the port assigned to accept SMTP based e-mail traffic.

TOE Functional Requirements Satisfied: FPT_RVM.1

6.2 TOE Security Assurance Measures

EAL2 was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2 level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 7 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	[ACM_CAP.2] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - Configuration Management Document v0.4
ADO_DEL.1	[ADO_DEL.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - Secure Delivery Procedure Document v0.4
ADO_IGS.1	[ADO_IGS.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - Installation and Setup Procedure Document v0.2
ADV_FSP.1	[ADV_FSP.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence v0.4
ADV_HLD.1	[ADV_HLD.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence v0.4

Assurance Component	Assurance Measure
ADV_RCR.1	[ADV_RCR.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence v0.4
AGD_ADM.1	[AGD_ADM.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - Administrator Guides
AGD_USR.1	[AGD_USR.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - User Guides
ATE_COV.1	[ATE_COV.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 – Functional Tests and Coverage v0.3
ATE_FUN.1	[ATE_FUN.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 – Functional Tests and Coverage v0.3
AVA_SOF.1	[AVA_SOF.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 – Vulnerability Assessment v0.1
AVA_VLA.1	[AVA_VLA.1] SurfControl E-mail Filter for SMTP Version 5.0, Service Pack 2 - Vulnerability Assessment v0.1

6.2.1 ACM_CAP.2: Configuration Management Document

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at SurfControl. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.2 ADO_DEL.1: Delivery and Operation Document

The Delivery and Operation document provides a description of the secure delivery procedures implemented by SurfControl to protect against TOE modification during product delivery. The Installation Documentation provided by SurfControl details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE Users(s) on configuring the TOE and how they affect the TSF.

6.2.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE.

The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The User Guidance documentation provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they need to be exercised.

6.2.4 ADV_FSP.1: Informal Functional Specification, ADV_HLD.1: High Level Design, ADV_RCR.1: Representation Correspondence.

The SurfControl design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

6.2.5 ATE_COV.1: Test Coverage Analysis, ATE_FUN.1: Functional Testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

6.2.6 AVA_VLA.1: Vulnerability Analysis, AVA_SOF.1: Strength of Function Analysis

A Vulnerability Analysis is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks.

The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. Table 8 demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 8 - Relationship of Security Threats to Objectives

Objectives Threats, Assumptions			TOE Objectives					Environmental Objectives												
								IT				Non-IT								
			O.ADMIN	O.AUDIT	O.DIRECT	O.MESACC	O.MAILRVW	OE.HARDENED	OE.TIMESTMP	OE.FIREWALL	OE.TRANSFER	NOE.AUDIT	NOE.DELIV	NOE.MANAGE	NOE.INTMANG	NOE.NOEVIL	NOE.PHYSIC	NOE.REVIEW	NOE.TRAIN	NOE.TRUSTED
Threats	TOE	T.SEND	✓	✓								✓								
		T.MEDIAT					✓													
		T.OPENRELAY					✓													
		T.REMCONN	✓		✓															
		T.UNSOLICT					✓													
		T.USRDATA			✓	✓														
	Env	TE.AUDFULL										✓		✓						
Assumptions		A.FIREWALL								✓										
		A.INSTALL											✓							
		A.MANAGE										✓		✓				✓		
		A.INTMANG													✓					
		A.NO_EVIL														✓			✓	
		A.PHYSICAL											✓				✓			
		A.TRANSFER									✓									
		A.TRUSTED																		✓
		A.HARDENED						✓												
		A.AUDFUL										✓		✓						
		A.TIMESTMP							✓											

T.SEND **The attempts of an attacker to send harmful SMTP traffic (e-mail) may go undetected posing a threat to the protected network.**

The TOE detects and collects all security relevant events related to the SMTP traffic (O.AUDIT) and offers functionality to collect SMTP related audit information, to view audit records, and to restrict these two functions to only TOE users with the appropriate privileges (O.ADMIN). TOE users with the appropriate privileges should regularly inspect the logs generated to detect unauthorized activity (NOE.AUDIT).

O.AUDIT and O.ADMIN combined ensure that this threat is removed. NOE.AUDIT supplements the TOE security objectives in removing this threat.

T.MEDIAT **An attacker who is not a TOE user may send impermissible information through the TOE which results in the exploitation of resources on the internal network or undesired SMTP messages being delivered.**

The TOE reviews all incoming and outgoing SMTP messages and blocks or queues all messages that violate any of the defined policies to prevent the delivery of a harmful or unwanted SMTP message (O.MAILRVW).

O.MAILRVW removes this threat.

T.OPENRELAY **An attacker who is not a TOE user may send multiple SMTP messages to the TOE, where those messages are addressed to recipients whose e-mail addresses fall outside the set of address for which the TOE handles e-mail. The intent of this attack is to utilize the resources of the TOE to deliver bulk e-mail on behalf of the originator.**

The TOE limits the SMTP messages accepted, to those messages addressed to recipients within the address set of the Mail Firewall (O.MAILRVW).

O.MAILRVW removes this threat.

T.REMCONN **An attacker who is not a TOE user may exploit network protocol(s) based vulnerabilities and compromise TOE services and data assets by establishing a remote connection to the TOE.**

The TOE controls access to hosts and limits security functions available from the network interfaces to TOE users who possess the appropriate privileges (O.ADMIN). Any connection requests with the TOE must be successfully identified and authenticated before access is permitted (O.DIRECT) and will be protected to ensure only TOE users with the appropriate rights can read or modify transmitted data (O.ADMIN).

O.DIRECT and O.ADMIN combined ensure that this threat is removed.

T.UNSOLICT **An attacker who is not a TOE user may send unsolicited bulk mail where the content of those messages falls outside of a defined acceptable use policy posing a threat to the effective processing of other SMTP messages.**

The TOE will detect and take action against unsolicited bulk e-mail that matches the rule definitions and will not allow SMTP messages for delivery if the content of the message falls outside the defined policy (O.MAILRVW).

O.MAILRVW ensures that this threat is removed.

T.USRDATA **An attacker who is not a TOE user could access individual e-mail messages stored on the TOE, by viewing, sorting, releasing, deleting or moving to (queue) the queued e-mails stored on the TOE.**

The TOE provides an identification and authentication mechanism that prevents external entities not defined as TOE users from accessing the TOE (O.DIRECT) and ensures that only TOE users with the appropriate privileges have access to the quarantine or to the messages stored within the TOE (O.MESACC).

O.DIRECT and O.MESACC combined ensure that this threat is removed.

TE.AUDFUL **An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity.**

An authorized user is assigned with responsibility for day to day management of the audit trail (NOE.MANAGE). The authorized user must ensure that the audit facilities are used and managed effectively and that the audit logs are archived in a timely manner to ensure that the machine does not run out of audit log data storage space (NOE.AUDIT).

NOE.MANAGE and NOE.AUDIT combined ensure that this threat is diminished.

A.FIREWALL **All ports needed for proper operations of the TOE will be opened at the firewall.**

The Firewall must have all ports needed for proper operations of the TOE opened (OE.FIREWALL).

OE.FIREWALL satisfies this assumption.

A.INSTALL **The TOE hardware and software have been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.**

Those responsible for the TOE must ensure that it is delivered, installed, managed, and operated in accordance with documented delivery and installation/setup procedures (NOE.DELIV).

NOE.DELIV satisfies this assumption.

A.MANAGE **There will be one or more competent TOE user(s) assigned to manage the TOE and the security functions it performs.**

A TOE user is assigned with responsibility for day to day management and configuration of the TOE, including the management of the audit trail (NOE.MANAGE). Users of the TOE who possess the appropriate privileges must ensure that the audit functionalities are used and managed effectively (NOE.AUDIT). The configuration of the TOE will be inspected on a regular basis to ensure that the configuration continues to meet the organization's security policies (NOE.REVIEW).

NOE.MANAGE, NOE.AUDIT and NOE.REVIEW combined satisfy this assumption.

A.INTMANG **It is assumed that the TOE environment will only be managed from within the protected network.**

The TOE can only be managed from the protected network and cannot be managed from the external network (NOE.INTMANG).

NOE.INTMANG satisfies this assumption.

A.NO_EVIL **A TOE user is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation.**

TOE users are non-hostile and follow all administrator guidance (NOE.NOEVIL). Those responsible for the TOE must train TOE users to establish and maintain sound security policies and practices (NOE.TRAIN).

NOE.NOEVIL and NOE.TRAIN combined satisfy this assumption

A.PHYSICAL The TOE will be physically protected to prevent hostile individuals engaging in theft, implantation of devices, or unauthorized alteration of the physical configuration of the TOE (e.g. bypassing the TOE altogether by connecting the corporate and hostile networks together).

The TOE must be physically protected so that only TOE users who possess the appropriate privileges have access (NOE.PHYSIC). Those responsible for the TOE must ensure that it is delivered, installed, managed, and operated in a manner that maintains the security policy (NOE.DELIV).

NOE.PHYSIC and NOE.DELIV combined satisfy this assumption.

A.TRANSFER All SMTP traffic between networks connected to the TOE will be transferred through the TOE.

The TOE must be installed between networks wishing to transfer SMTP mail messages. This must be the only connection between the networks permitting the flow of SMTP traffic (OE.TRANSFR).

OE.TRANSFR satisfies this assumption.

A.TRUSTED The users of the internal network from which administration of the TOE is performed are trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks.

The users of the network from which the TOE will be administered must be trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks (NOE.TRUSTED).

NOE.TRUSTED satisfies this assumption.

A.HARDENED The underlying operating systems will be hardened to remove all mechanisms and services that are not required by the TOE.

The underlying operating system will be hardened to remove all mechanisms and services that are not required by the TOE (OE.HARDENED).

OE.HARDENED satisfies this assumption.

A.AUDFUL The authorized user of the machine used to store audit data must ensure that the audit data is archived and that the storage space does not become exhausted.

An authorized user is assigned with responsibility for day to day management of the audit trail (NOE.MANAGE). The authorized user must ensure that the audit facilities are used and managed effectively and that the audit logs are archived in a timely manner to ensure that the machine does not run out of audit log data storage space (NOE.AUDIT).

NOE.MANAGE and NOE.AUDIT combined satisfy this assumption.

A.TIMESTMP It is assumed that the IT environment will provide the TOE with the necessary reliable timestamps.

The TOE operating environment shall be able to generate reliable timestamps for the TOE's use (OE.TIMESTMP).

8.2 Security Functional Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

Table 9 - Relationship of Security Requirements to Objectives

	Objectives	TOE					Env	
	Requirements	O.ADMIN	O.AUDIT	O.DIRECT	OMESACC	O.MAILRVW	OE.TIMESTMP	NOE.AUDIT
TOE	FAU_GEN.1		✓					
	FAU_SAR.1	✓						
	FAU_SAR.3	✓						
	FDP_ACC.1				✓			
	FDP_ACF.1				✓			
	FDP_IFC.1					✓		
	FDP_IFF.1					✓		
	FIA_ATD.1			✓				
	FIA_UAU.2	✓		✓				
	FIA_UID.2	✓		✓				
	FMT_MOF.1 (a)	✓						
	FMT_MOF.1 (b)	✓						
	FMT_MOF.1 (c)	✓						
	FMT_MOF.1 (d)	✓						
	FMT_MSA.1 (a)	✓				✓		
	FMT_MSA.1 (b)	✓				✓		
	FMT_MSA.3 (a)					✓		
	FMT_MSA.3 (b)					✓		
	FMT_MTD.1 (a)	✓						
	FMT_MTD.1 (b)	✓						
	FMT_SMF.1	✓						
	FMT_SMR.1	✓						
	FPT_RVM.1	✓	✓	✓		✓		
Env	FPT_SEP.1	✓	✓	✓		✓		
	FPT_STM.1		✓				✓	
	FAU_STG.1							✓

O.ADMIN **The TOE must provide a secure method of administrative control of the TOE, ensuring that TOE users with the appropriate privileges, and only these TOE users, can exercise such control.**

The TOE maintains authorized administrators with appropriate privileges as defined in Table 2 (FMT_SMR.1)

The TOE provides administrators with the capability to manage the users of the TOE (FMT_MSA.1) and assures that no one can override the restrictive default values assigned to a new user at creation (FMT_MSA.3).

Identification and authentication of the requesting administrator provide a secure mechanism to enforce an access control to the management functions of the TOE (FIA_UID.2, FIA_UAU.2).

The TOE also provides administrators with the capability to view system log, traffic logs and rules log and read the audit records (FAU_SAR.1). It also provides the ability to perform searching, sorting, and/or ordering of audit data based on date, event, server domain name, and/or system log ID(FAU_SAR.3). Only TOE users with the appropriate privileges may manage the configuration (FMT_MTD.1) and manage the audit files (FMT_SMF.1) by modifying the behavior of the audit functions (FMT_MOF.1).

The identification and authentication process and the management functions will be performed for every request received and cannot be bypassed or be interfered with by other processes (FPT_RVM.1, FPT_SEP.1).

O.AUDIT **The TOE shall provide a means to detect and collect all security-relevant events as defined by a TOE user (who possesses the appropriate privileges) into the audit records with accurate dates and times.**

The TOE defines and audits security-relevant events that need to be logged (FAU_GEN.1). The TOE depends on the environment for reliable time stamps and associates each audit record with the time and date the event occurred (FPT_STM.1). Audit functions will be performed for every request received, as the TSP enforcement functions are started and terminated in a specific order, and cannot be bypassed or be interfered with by other processes (FPT_RVM.1, FPT_SEP.1).

O.DIRECT **The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to the TOE.**

The TOE maintains the security attributes belonging to individual authorized administrators (FIA_ATD.1) and uniquely identifies and authenticates access to the TOE using an identification and authentication process before allowing any other TSF-mediated actions on behalf of that user (FIA_UID.2, FIA_UAU.2). This process will be performed for every request received and cannot be bypassed or be interfered with by other processes (FPT_RVM.1, FPT_SEP.1).

O.MESACC **The TOE shall enforce an access control policy on TOE users who wish to access quarantined messages stored within the TOE.**

The TOE enforces the discretionary access control policy on TOE users, restricting the ability to access the queues and the messages stored within the TOE (in the queues) to only TOE users who possess or were giving the appropriate privileges (FDP_ACC.1, FDP_ACF.1).

O.MAILRVW **The TOE shall review all incoming and outgoing SMTP messages to determine that the defined policies are enforced and the appropriate actions are performed on every message.**

The TOE verifies all incoming and outgoing SMTP message and ensures that the defined policies are enforced and the appropriate actions are taken on every message (FDP_IFC.1, FDP_IFF.1). These checks will be performed for every request received and cannot be bypassed or be interfered with by other processes (FPT_RVM.1, FPT_SEP.1).

By default, restrictive policies are in place and can be modified in accordance with the Acceptable Use Policy by TOE users who possess the appropriate privileges (FMT_MSA.1, FMT_MSA.3).

OE.TIMESTMP **The TOE operating environment shall be able to generate reliable timestamps for the TOE's use.**

The TOE environment provides reliable time stamps for use by the TOE.

OE.HARDENED **The underlying operating system will be hardened to remove all mechanisms and services that are not required by the TOE.**

The operating system of the server upon which the TOE software runs is hardened according to the guidance previously referred to in this document.

OE.FIREWALL **The Firewall must have all ports needed for proper operations of the TOE opened.**

The firewall is configured to pass traffic on ports 25, 80, and 1433 to and from the TOE.

OE.TRANSFR **The TOE must be installed between networks wishing to transfer SMTP messages. This must be the only connection between the networks permitting the flow of SMTP traffic.**

The only two networks with which the TOE environment is configured to allow the TOE to communicate with are the external “untrusted” network and the internal “trusted” network.

NOE.AUDIT **Authorized users of the audit facilities must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.**

The IT environment hosting the TOE shall protect the stored audit records from unauthorized deletion and will prevent any modification to the stored audit records.

8.3 Security Assurance Requirements Rationale

The TOE is designed as a server based software application for filtering SMTP based E-mail that protects the internal network from E-mail non conformant to the Acceptable Use Policy of the organization. It is intended to be protected by a firewall product that would intercept and block a significant number of network attacks. An assurance level of EAL 2, structurally tested, was selected as the threat to the system resources and to the internal network security is considered to be unsophisticated attackers. It is felt that an evaluation at this level provides evidence that the TOE functions in a manner consistent with its documentation and that it provides useful protection against the identified threats.

8.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 10 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 10 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FAU_SAR.3	FAU_SAR.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_ATD.1	No Dependencies		
FIA_UAU.2	FIA_UID.1	✓ (FIA_UID.2)	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FIA_UID.2	No Dependencies		
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No Dependencies		
FMT_SMR.1	FIA_UID.1	✓ (FIA_UID.2)	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FPT_RVM.1	No Dependencies		

8.5 TOE Summary Specification Rationale

8.5.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these 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 the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 11 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the Strength of Function, refer to Strength of Function (SOF) Rationale section.

Table 11 - Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR	Rationale
Security Audit	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3	The TOE records logs of critical events in the System Log table in a database. These records can be reviewed from within the TOE. In addition TOE also provides a mechanism to archive and purge the System Log as a means to prevent audit data storage exhaustion. The System Log contains the records of regular operations and exceptions from various components of the system including information about the start-up and shutdown of the audit functions and all audited events listed in FAU_GEN.1. The TOE also records for each event the date and time an event occurred, the type and outcome of the event, and the subject identity. Each audit record includes the "subject identity" allowing a viewer to associate each event with the person that caused the event. The time that is used to time stamp all the audit records is always pulled from the same source: the IT environment of the TOE.
User Data Protection	FDP_ACC.1 FDP_ACF.1 FDP_IFC.1 FDP_IFF.1	SMTP based e-mail messages that are owned by the external IT entities are processed by the TOE. The TOE provides a discretionary information flow policy of the SMTP based e-mail messages (user data) as they flow through the various filtering mechanisms of the TOE. Additionally, the TOE provides a discretionary access control policy that enforces the policy in such a way that only identified and authenticated TOE users can access the User Data (SMTP e-mail messages) stored in the various queues of the TOE. Further the discretionary access control policy allows TOE users who possess the appropriate privileges to access User Data in the queues and perform allowable operations on the User Data stored in the queues. The TOE scheme on which the information flow control policies are based depends on a series of successive filtering mechanisms in the form of three primary services. The receive service, the rules service and the send service. As an e-mail flows through the various services it is checked initially against pre-screening criteria in the receive service subsequently the e-mail is subject to filtering by rules defined by rule objects in the rules service. These rules are collection of criteria that an e-mail will be checked against. The Send Service controls what happens to e-mails after they have been allowed to proceed through the TOE by the Rules Service. When an e-mail has been checked and allowed to proceed, it is placed in the Send Mail Pickup Folder by the Send Service.
Identification & Authentication	FIA_ATD.1 FIA_UAU.2 FIA_UID.2	To gain access to the TOE data and functionality the authorized users must successfully identify and authenticate themselves (FIA_UAU.2, FIA_UID.2). The TOE uses the maintained account information of the TOE user to make authentication decisions. The account information the TOE maintains is the username, the password of the user, attributes and email address (FIA_ATD.1)

TOE Security Function	SFR	Rationale
Security Management	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	The TOE lets a TOE user who possesses the appropriate privileges perform various management functions. Specifically, the TOE provides several commands for the management and administration of the TOE. The TOE imposes no limit to the number of user accounts that can be created for the system and maintains seven roles. For each new user account created, a username and an email address need to be specified, and the user needs then to be assigned to one or more of the seven possible roles. User-specific permissions must also be assigned within each role to which the user is assigned (except the "All Permissions" role); these permissions determine upon which message queues and functions the user may exercise the privileges granted by his role(s). The roles are detailed in Table 2. Each role is an administrative role – there are no non-administrative users of the TOE. The audit log may be viewed via the Message Administrator GUI by TOE users with the "All Permissions" or "View Logs" roles. The TOE itself may be managed by users with the "All Permissions" or "System Administration" roles. The right to issue mail flow control commands is reserved to users with the "All Permissions," "Message Administration," "Rules Administration," and "Dictionary Management" roles. These commands give TOE administrators the ability to enable, disable or modify the behavior of the mail flow policy and query, modify, delete or create new filters and rulesets. However, no one has any control over any of the e-mail's security attributes. By default, when no policy is yet created, the TOE will permit all email traffic to flow through the TOE.
TOE Self Protection	FPT_RVM.1	Non-bypassability of the TOE is provided by a combination of the basic configuration and enforcement of the security policy rules. The assumed secure basic configuration maintaining physical and logical isolation supports the Protection of Security Functions (PSF). The functions that enforce the TOE Security Policy (TSP) will always be invoked, before any function within the TSF Scope of Control is allowed to proceed. Some of the TOE self-protection (e.g., against physical tampering) is ensured by the TOE environment. In particular, it is assumed that the Windows server hosting the TOE and the remote administration components of the TOE on the protected network will remain attached to the physical connections made by an authorized administrator responsible for the proper installation of the TOE so that the TOE cannot be bypassed. The security functions are physically separated from the unauthenticated external IT entities which send and receive SMTP messages through the TOE. The TOE configuration protects its management functions by isolating them using identification and authentication and by limiting them exclusively to the port assigned to accept SMTP based e-mail traffic.

8.5.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2 was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. The chosen assurance level was also selected for conformance with the client's needs.

8.5.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used at the SurfControl. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.5.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by SurfControl to protect against TOE modification during product delivery. The Installation Documentation provided by SurfControl details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

8.5.2.3 Development

The SurfControl design documentation consist of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Correspondence Demonstration

8.5.2.4 Guidance Documentation

The SurfControl Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. SurfControl provides single versions of documents which address the administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

8.5.2.5 Tests

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. SurfControl Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

8.5.2.6 Vulnerability and TOE Strength of Function Analyses

A Vulnerability Analysis is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Strength of TOE Security Function analysis
- SurfControl Vulnerability Analysis

8.6 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL 2 assurance requirements, this SOF is sufficient to resist the threats identified in Section 3. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information.

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Sections 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements.

The relevant security functions and security functional requirements which have probabilistic or permutational functions are:

FIA_UAU.2	User Authentication before any action

The only mechanisms within the TOE that are probabilistic and permutational in nature are the passwords used to authenticate users to the TOE. The TOE requires that the minimum password length used to authenticate an entity would be equal to or greater than six case-sensitive alphanumeric characters, for a total character set of 62 characters.

A six-character case-sensitive alphanumeric password yields:

62^6 = 56,800,235,584 possible password permutations

Where each character is selected independently of the others, order is relevant, and characters can be repeated within a password.

The expected number of attacker attempts will be one-half of the total possible attempts:

56,800,235,584 * (½) = 28,400,117,792 expected attempts

Based on the above calculations for a worst-case scenario, an attacker would have to enter 28,400,117,792 passwords before entering the correct password.

Attackers are assumed to possess a low skill level and limited resources, considering it would take 3 seconds in order to attempt authentication, the number of attempts that could be made in 1 month = (20 attempts in a one min) * (60 min in an hour) * (24 hours in a day) * (30 day in a month) = 864,000.

So, the average of months required to guess the password is

= average no of attempts / number of attempts per month

= 10,967,424,000 * (1/864,000)

= 12,693.78 months ~ 1,057.815 years

In accordance with annex B.8 in the CEM, this elapsed time of attack results in a strength of function rating exceeding SOF-basic.

9 Acronyms and Terms

Table 12 - Acronyms and Terms

Acronym	Definition
AUP	Appropriate Use Policy
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
DMZ	Demilitarized Zone
DNS	Domain Name Server
EAL	Evaluation Assurance Level
Env	Environment / Environmental
GB	Gigabyte
GUI	Graphical User Interface
HTTP	Hypertext Transport Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MB	Megabyte
MDAC	Microsoft Data Access Components
MHz	Megahertz
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transport Agent
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
SAR	Security Assurance Requirement
SEF	SurfControl E-mail Filter
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
SP	Service Pack
SQL	Structured Query Language
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	Target of Evaluation (TOE) Security Function
TSP	Target of Evaluation (TOE) Security Policy
URL	Uniform Resource Location

Acronym	Definition
VGA	Video Graphics Array
VLA	Virtual Learning Agent