WATCHGUARD XCS SERVER V9.2

SECURITY TARGET

Evaluation Assurance Level: 4+

Augmented with ALC_FLR.2

Version: 1.9

WatchGuard Technologies Inc 505 Fifth Avenue South, Suite 500 Seattle, WA 98104 United States of America Tel: +1.206.613.6600 Fax: +1.206.521.8342	WatchGuard Canada 50 Burnhamthorpe Road West, Suite 500 Mississauga, Ontario, L5B 3C2 Canada Tel: +1.905.804.1855 Fax: +1.905.804.1865

http://www.watchguard.com/

History of Changes

Version	Date	Description
1.8	November 7, 2011	Backup/Restore and Patch Update support added. P.SYSTEM_DATA, OE.SYSTEM_DATA
1.9	December 8, 2011	Resolved references

Table of Contents

List of Figures

List of Tables

References

Reference	Publication Source
[CC]	CCMB-2009-07-001, CCMB-2009-07-002 and CCMB-2009-07-003 Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, July 2009

1 Security Target Introduction (ASE_INT)

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the software running on the WatchGuard XCS Server v9.2 and will hereafter be referred to as the TOE throughout this document.

The TOE is a software product designed to provide e-mail content security. The TOE protects corporate e-mail client and server components by providing screening and protecting of the content of e-mails sent via corporate e-mail systems.

1.1 Purpose

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 ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem Definition (Section 3) – Describes the threats, organizational security policies, 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.
- Extended Components Definition (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terminology (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1-1 ST and TOE References

Reference	Description
ST Title	WatchGuard XCS Server v9.2 Security Target
ST Author	Ross Williams
ST Revision	1.9
ST Publication Date	December 8, 2011
TOE Reference	WatchGuard XCS Server v9.2 Extended version = WTI-XCS92-090611 Build Date = 090611

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is the software running on the “XCS Series” family of appliances.

The WatchGuard XCS Series provides corporations with an enterprise-class email security, privacy and compliance solution that protects against inbound threats and controls outbound information to prevent data loss.

WatchGuard XCS Series provides defense-in-depth spam and malware security for email, web and data loss prevention.

WatchGuard XCS Series offers defense from email and web based threats including spam, viruses, malware, spyware, URL filtering, blended threats, and network attacks.

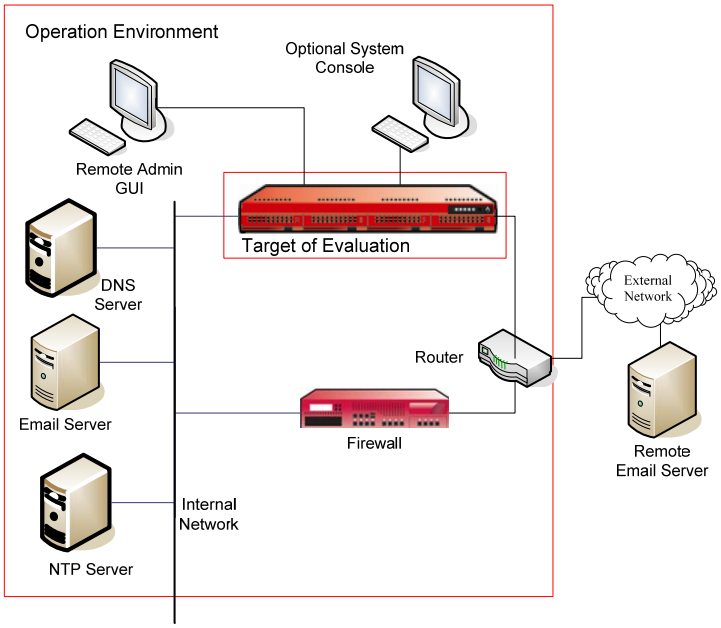

Figure 1-1 – Typical Operational Environment for the TOE

A typical Operational Environment would be to use two network interfaces as shown in Figure 1-1. In this configuration the TOE is deployed in parallel with a general purpose Firewall. The TOE will process all inbound and outbound e-mail for the protected organization.

The router is configured to direct all email traffic to the TOE and the general purpose Firewall is configured to block all email traffic from entering or leaving the protected organization.

This configuration ensures that a highly specialized email server will offer a significant increase in the overall level of security to the organization by deep inspection of the data content of the email messages.

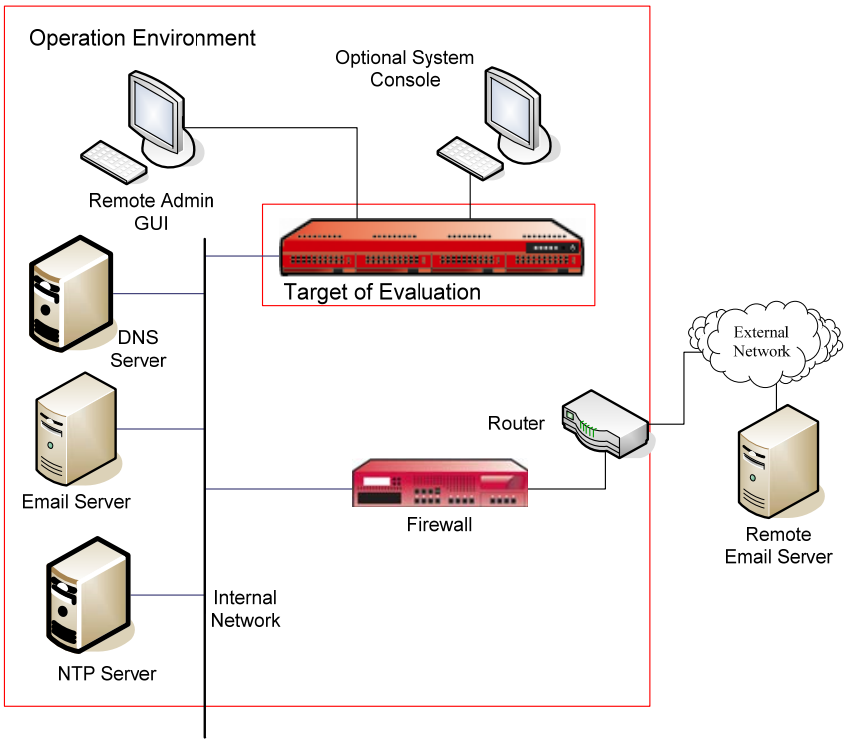

Figure 1-2 – Secondary Operational Environment for the TOE

A secondary Operational Environment exists for organizations where the local security policy prohibits the deployment of the TOE in parallel with an existing general purpose Firewall as in Figure 1-2. The TOE would be deployed with a single network interface that is connected to the network segment protected by the Firewall.

The router would direct all data traffic to the Firewall and the Firewall's forwarding policy would be required to direct all inbound e-mail protocol connections to the TOE. While this configuration is within the scope of the TOE, it is recommended only for organizations whose policies prohibit any device to be connected in parallel with the Corporate Firewall.

1.3.1 TOE Components

The TOE comprises multiple components which work together to implement the e-mail security functions and supporting services.

The following components compose the TOE.

1.3.1.1 S-CORE Operating System

The TOE is built on the WatchGuard S-CORE operating system. S-CORE is a hardened operating system that has been specifically designed by WatchGuard Technologies Inc and is derived from BSD Unix.

S-CORE has all non-essential functions removed and is further optimized for security and throughput. The purpose-designed operating system provides a separate domain of execution for each critical subsystem and implements kernel-level packet filtering to ensure that only valid IP datagrams reach the application servers running on the TOE. IP Datagrams for any protocol or port not supported and enabled are dropped by the kernel-level packet filtering module.

Management, monitoring and audit functions. The TOE includes all management monitoring and audit functions implemented by the TOE.

1.3.1.2 SMTP Server

The SMTP server is running by default and will accept connections on TCP port 25 on all network interfaces. The SMTP server accepts both clear text on port 25 and TLS encrypted connections (not included in the scope of the evaluation). The server may be disabled by stopping the Mail Service. This is normally done for administrative purposes only.

Key features of the SMTP Server are:

Store and forward mail relay - The TOE is responsible for the delivery of all inbound e-mail from an external network to one or more mail severs located on a corporate network and for the delivery of all outbound e-mail from those corporate mail servers to external destinations. Messages are *relayed* via a mail queue maintained on the TOE. Delivery of messages via a store and forward relay prevents any direct SMTP connections between corporate e-mail servers and external e-mail sources and destinations. Corporate e-mail servers are therefore protected against the wide range of threats and vulnerabilities associated with such connections. Where the TOE is deployed in conjunction with an existing Firewall, the Firewall's configuration may be modified to block all inbound and outbound SMTP connections, increasing the level of protection afforded to corporate e-mail systems.

Mail address aliasing and mapping - The TOE can optionally modify the sender and/or recipient address of processed messages based on alias rules or on address mapping rules. This ensures that internal e-mail addresses and servers maintain a degree of anonymity from external mail servers.

Mail Routing - The TOE can operate as a mail router, determining the next hop delivery destination for e-mail messages based on the domain component of an e-mail address, on the user name component or on both components. Mail routing operates on sender and recipient addresses after any transformations required by aliasing or mapping rules.

Source Address Filtering - The TOE can selectively reject, trust or relay messages received from a pre-defined IP address or from a local subnet. Trust means that messages received from the defined IP addresses will be treated as if they originate from a trusted network, may be relayed to any destination and will be used as examples of legitimate email for the Spam control functions (not included in TOE). Relay means that messages may be relayed to any destination. A local subnet is defined as any range of IP addresses that includes one or more of the TOE's active interfaces. The Trust and Relay functions are needed to ensure correct handling of outbound e-mail from a corporate mail server.

Mail Relay controls - The TOE enforces controls on mail relay, limiting the ability for other e-mail systems to send messages to the TOE for onward relay to the destination. These controls are designed to prevent the protected mail systems from operating as an *open relay* and unwittingly forwarding unsolicited commercial e-mail (UCE or Spam).

Mail access and filtering - Specific file name extensions against which an SMTP message are permitted or denied can be configured.

1.3.1.3 Authentication Server

The Authentication Server validates attempts to authenticate as an administrator in the establishment of a session with the Management/Configuration Server (MCS) interface.

1.3.1.4 Management/Configuration Server (MCS)

The TOE implements two management interfaces.

The primary management interface is Web based. The Management/Configuration server that provides this interface is permanently running and may be configured to accept connections on all network interfaces on TCP port 80 (HTTP) and TCP port 443 (HTTPS). Connections to port 80 may optionally be re-directed to port 443. This forces all web server connections to be encrypted using SSL.

By default, the MCS will accept connections only on the first network interface which has an assigned IP address during the installation process. It is recommended that this interface be physically connected to the internal (protected) network.

MCS connections may be enabled on other interfaces. These MCS connections on TCP Ports 80 or 443 must be authenticated by the web server. (Only connections on Port 80 (HTTP) are within the scope of the evaluation.)

The TOE provides a second management interfaces called the System Console. It is made available via a keyboard/monitor connection to the server or dedicated serial interface. This interface has limited functionality and is mainly used for network diagnostics and system reset. The Console is user/password protected in the same fashion as the Web based management interface.

1.3.1.5 Web Server

The Web server supports the provision of the MCS interface.

1.3.1.6 Ping Server

The Ping server is permanently running and supports the Internet Control Message Protocol (ICMP) Echo request/reply network diagnostic. During installation the ping server is enabled on the first interface. Other interfaces must be separately enabled from the MCS. When enabled, the Ping server will respond with an ICMP echo reply for each echo request received up to a maximum of 200 per second. When an interface is disabled, the firewall access control rules also known as IPFW rules are written to deny ICMP packets on that interface.

1.3.1.7 Syslog Client

The Syslog client forms part of the S-CORE operating system (OS) and supports the generation of records of specified system/configuration events. These records are stored in audit logs. This server cannot be disabled, and the records generated are always stored locally on the TOE. Records for events other than those generated by the web server can also, optionally, be directed to an external syslog server running a syslog daemon, to provide a secondary storage of records.

1.3.1.8 SMTP Client

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail). The SMTP client is responsible for the onward delivery of messages when the mail routing function determines that the delivery end-point for the message is a mailbox located on an external e-mail server.

1.3.1.9 DNS Client

The Domain Name System (DNS) is a service that stores, translates, and retrieves the numerical IP address equivalents of familiar host names that you use every day for example www.watchguard.com translates to 206.191.171.104.

The DNS client is used by the TOE to look up Mail Exchange Records (MX Records) for domains to determine the next hop delivery for e-mail messages and to resolve domain names into IP addresses.

1.3.1.10 NTP Client

NTP stands for Network Time Protocol, and it is an Internet protocol used to synchronize the clocks of computers connected to a reference time source.

The NTP client is used to synchronize the TOE's system clock with an identified and trusted time source.

1.3.2 TOE Excluded Components

The TOE excludes the following features that are either standard components of the WatchGuard XCS Server or are provided as additional cost options.

1.3.2.1 Virus Scanning Option

This is an additional cost option which scans all inbound and outbound messages for known viruses.

Kaspersky Anti-virus;

McAfee Anti-virus;

Outbreak control;

Malformed Mail;

and Spyware.

1.3.2.2 Spam Features

The following Spam features are excluded:

Reputation Enabled Defense (RED);

Connection Control - Reject on unknown recipients, RED connection, DNSBL, Backscatter;

Threat Prevention;

Backscatter Detection;

DNS Block Lists;

DomainKeys;

Mail Anomalies;

Spam Rules;

Spam Words;

Sender Policy Framework (SPF);

Token Analysis;

URL Block List;

and BrightMail Spam optional feature.

1.3.2.3 Content Control

The following Content Control features are excluded:

Content Scanning;

Attachment Control;

Content Rules;

Pattern Filters;

Objectionable Content;

Document Fingerprinting;

Dictionaries & Lists;

Custom Actions;

and Attachment Size Limits.

1.3.2.4 Mail Features

Message Quarantine

Policies

SMTP Authenticated Relay

Specific Access Patterns (SAP) - using Envelope-From, Envelope-To and HELO access

1.3.2.5 Accounts

All local Accounts with the exception of the Admin (TOE admin);

Mirror Accounts;

Relocated Users;

Delegated Domains;

Vacations;

SecurID;

And Remote Authentication

1.3.2.6 Web mail services

The following Web mail services are excluded.

Unprivileged Web mail user account on the XCS Mail Server required for mail boxes hosted on the server.

POP and IMAP connections which are associated with Web mail services.

The use of local mailboxes on the TOE is excluded.

1.3.2.7 E-mail encryption services

Third party encryption services such as

Voltage SecureMail;

Cisco CRES/PostX;

TLS;

and configurable third party servers.

1.3.2.8 External Authentication Services

The following authentication services are excluded:

Lightweight Directory Access Protocol (LDAP)

SecurID authentication tokens;

Authentication methods relying on an external Radius server for authenticating Web Mail and Web Admin logins;

Secure Tokens cards including CryptoCard, Safeword Gold 3000 and Platinum

Administration sessions on non-dedicated/isolated TOE network connections

Administration sessions using SSL Certificates

1.3.2.9 Non-System Administration

Centralized Administration, Tiered Administration and Dedicated Domain Administration (DDA), including vacation notification are excluded

1.3.2.10 Cloud Services

All aspects of WatchGuard Reputation Authority or RED services for IP and WEB services are excluded.

1.3.2.11 Network features

Web proxy also known as http/https proxy.

Transparent Mode, Bridging Mode, Virtual Interfaces

Performance – web, webmail, and custom pull-down lists

1.3.2.12 Server Features

The use of automatic software update features using the security connection service.

Backup and restore and re-install mode using ftp and scp servers.

Enabling ICMP ping and redirect feature during operational deployment

Archiving

Web proxy features

Frequent Tasks QMS Integration and Data Loss Prevention Wizards

Hardware Intelligent Platform Management Interface (IPMI) Ethernet interface

External attached USB Hard Drives, floppy drives and DVD/CD-ROM drives

1.3.2.13 Multiple System Management and Configuration

Centralized Management feature

Clustering feature

SMTP Queue Replication feature

Simple Network Management Protocol (SNMP) Agent

Automatic Feature Key Updating is excluded (Manual update is supported)

SSL Certificate

1.3.2.14 System Utilities

Web based utilities – Flush Web Cache, Flush URL from Web Cache, Flush Web Single Sign On Sessions, Web RED URL Lookups

Policy Trace

1.3.3 TOE Environment

The TOE is a software product designed to run on Intel x86/EM64T based server grade hardware. The XCS Series is an appliance product which combines the TOE software with the server hardware. The minimum environment requirements are in Table 1-2.

Table 1-2 TOE Environment

CPU	Memory	Network Interface	Hard Disk(s)	Web UI Browser
Dual Core E1200	2 GB	Intel(R) 1000BaseT 2 minimum	160 GB SATA II	Internet Explorer 7, or Mozilla Firefox 3

1.4 TOE Description

1.4.1 Physical Scope

Figure 1-3 below 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 software-only TOE designed to fulfill the e-mail security needs.

The software components which make up the TOE are installed on a single host computer that is compliant with the minimum requirements as listed in Table 1-2. The non-TOE servers and devices are service resources which require operational environment as depicted in Figure 1-3 below. There are no hardware components that are provided with the TOE.

Components of the Physical TOE are outlined in red and filled in with green.

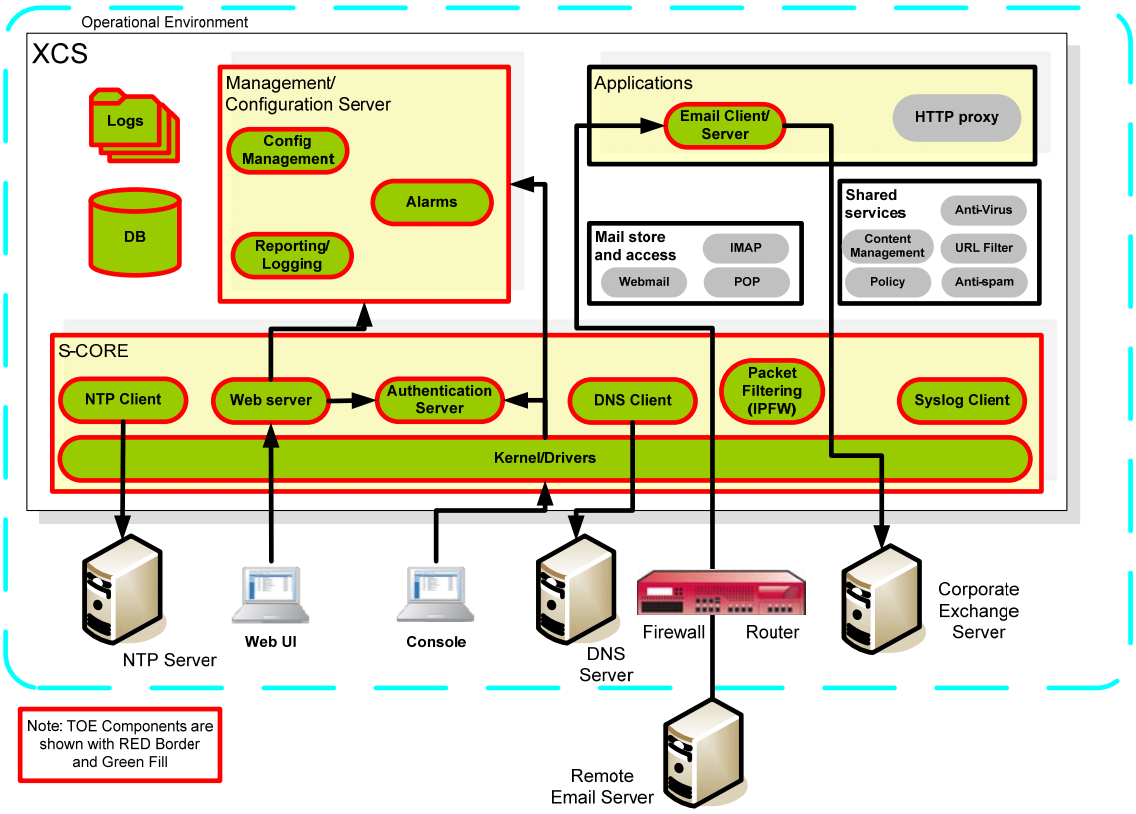

Figure 1-3 – Physical Scope for the TOE

1.4.1.1 TOE Software

The TOE is an application and S-CORE operating system software running on one of the approved XCS Series appliances. The TOE is software only; the appliance hardware is not part of the TOE.

1.4.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

Guides	Title
Release Notes	WatchGuard XCS v9.2 Release Notes – June 14, 2011
Preparatory Guide	WatchGuard XCS Preparatory Guide – v1.2
User Guide	WatchGuard XCS v9.2 User Guide – 6/15/2011
Field Guide	WatchGuard XCS v9.2 Field Guide – 6/13/11
Hardware Guide	WatchGuard XCS Hardware Guide – 170,370,570,770 and 770R models – P.N. 275-3727-003 WatchGuard XCS Hardware Guide – 970 and 1170 models – P.N. 275-3728-001
Quick Start Guide	WatchGuard XCS Quick Start Guide – 170,370,570,770 and 770R models - P.N. 352-3707-003 WatchGuard XCS Quick Start Guide – 970 and 1170 models - P.N. 352-3708-002

Table 1-3 TOE Guidance Documents

1.4.2 Logical Scope

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
- Protection of the TOE Security Functions
- TOE Access

1.4.2.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation of audit records. As administrators manage and configure the TOE, their activities are automatically logged. All security-relevant configuration settings and changes are recorded to ensure accountability of the administrator's actions.

1.4.2.2 User Data Protection

The User Data Protection function implements functionality for TOE security functions and TOE security function policies related to protecting user data. The user data that the TOE is protecting is the secure transport of email between the external and corporate servers.

The TOE has the ability to define compliancy policies which will make available the end-user data to compliancy department or individuals as identified within the organizations policy.

It is the responsibility of the organizations appropriate use policy to ensure that the system administrator adheres to these policies.

1.4.2.3 Identification and Authentication

The Identification and Authentication function identifies and authenticates users to the TOE. End users must identify and authenticate themselves to the TOE anytime they wish to access a resource protected by the TOE.

Authentication Server provides its own internal authentication mechanism for identifying and authenticating users to the TOE. It does this by validating the user's username and password against the User Data store. The TOE can integrate with several external authentication types such as LDAP as well as maintain its own data store.

Additionally, each system administrator must identify and authenticate himself before he can administer the TOE.

1.4.2.4 Security Management

The Security Management features provide management and administration functions of the TOE for its administrators. The TSF is capable of associating users with roles. The TOE uses customizable user roles. The System Administrator is the only user who can elevate a user to an admin status. The enabling of subordinate administrators such as Delegate Doman Administrators (DDA), and tiered administrators are excluded from the TOE.

1.4.2.5 Protection of the TOE Security Functions

The System Administrator is the sole role capable of modifying and verifying the TOE configuration policy.

1.4.2.6 TOE Access

The System Administrator is required to be trained on corporate policy regarding appropriate use of organizational resources. Access to the TOE Management/Configuration Console implies awareness of appropriate use.

The TOE Management/Configuration Web User interface is excluded from being enabled on the Insecure External Network connection.

The TOE will lock-out the User interface for a period of 30 minutes after five failed attempts to login correctly.

1.4.2.7 Security Considerations in the TOE Environment:

The hardware that the TOE is installed upon must be maintained in a secure server room where physical access is limited to employees with appropriate security clearance for the server room as defined by the organizations access policy.

If the optional system console is attached to the TOE appliance, it will be physically located in the secure server room.

The Web based configuration browser is required to be located on a secure network which is dedicated for use by the TOE and the approved system administrator.

Use of the Backup and Restore facility provided by the MCS will use the Local Disk Backup and Restore method only. FTP and SCP modes are not recommended to be used. The Backup options supported for EAL4 deployments are:

Encrypt backup, Backup System Configuration and Backup Statistical Token Analysis (STA) Data are recommended to be enabled.

Reporting database and Quarantine mail are strongly recommended to be disabled due to size restrictions with the Local Disk Backup method.

Software Patch and image updating on the system is supported. The image and patches must be acquired from the WatchGuard LiveSecurity Web site. The LiveSecurity Web site will clearly identify which images and patches are Common Criteria compliant. The TOE admin will follow appropriate backup procedures prior to updating the software. These procedures are described in the user manual.

2 Conformance Claim (ASE_CCL)

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2-1 CC and PP Conformance Claim

Identification	Claim
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 3 conformant; CC Part 2 conformant
PP Identification	PP claim: none
Evaluation Assurance Level	EAL4 (Augmented with Flaw Remediation (ALC_FLR.2))

3 Security Problem Definition (ASE_SPD)

This section provides the statement of the TOE security environment, which identifies and explains all:

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

3.1 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.

3.1.1 Threats countered by the TOE

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 be hostile and possess a moderate skill level and 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 services provided by, and data accessible via, hosts on the corporate (private) network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 - Security Objectives.

The following specific threats are applicable:

Table 3-1 Threats

Name	Description
T.CONN	An unauthorized person may attempt to establish a connection across the TOE between networks or hosts to compromise the corporate network and data assets. This threat includes but is not limited to SMTP protocol attacks on e-mail servers.
T.MEDIAT	An unauthorized person may attempt to send impermissible information through the TOE to exploit services on the internal network.
T.REM_CONN	A remote connection established to the TOE that could be exploited by an attacker to compromise the TOE service and data assets.
T.REPEAT	An unauthorized person may repeatedly attempt to guess authentication data to gain access to the TOE.
T.DETECT	An attacker succeeds in compromising network, data and TOE service assets without being detected.
T.SOURCE	An attacker may attempt to initiate a service from an unauthorized source, by sending an IP packet with a fake source address.

Name	Description
T.CONFIG	An attacker on the corporate/hostile network may attempt to exploit an insecure configuration of the TOE in order to gain access to the restricted resources/data on the protected network not in accordance with the chosen network security policy.
T.OS_FAC	An attacker on the corporate/hostile network may attempt to use operating system facilities on the TOE server in order to gain access to the restricted resources/data on the protected network not in accordance with the chosen network security policy.
T.OPEN_RELAY	An unauthorized e-mail source may utilize the TOE as a bulk e-mail delivery system which will compromise the acceptable use policy for the TOE; and negatively affect the global reputation of the company's ability to sending valid email. Bulk e-mail falls outside the acceptable use policy for the TOE when the recipients of the e-mail are outside the set of addresses for which the TOE normally handles.
T.SELPRO	An unauthorized person may read, modify or destroy security critical TOE configuration data.
T.OLDINF	An unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.UNSOLICITED	An unauthorized e-mail source may send unsolicited bulk mail where the content of those messages falls outside of a defined acceptable use policy or where the volume of messages is considered to pose a threat to the effective processing of other e-mail messages.
T.USAGE	The TOE may be inadvertently or maliciously configured, used and administered in an insecure manner by either authorized or unauthorized persons.
T.VIOLATE	Careless or willfully negligent system administrators may violate network security policies by inappropriate action or inaction required on the TOE.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

Table 3-2 Organizational Security Policies

Name	Description
P.WEB_BROWSER	The TOE requires a secure and isolated network for administrators WEB UI Console to configure and manage the TOE.
P.SERVICES	The TOE will have access to physically and logically secure support services such as NTP and DNS.
P.SYSTEM_DATA	The TOE requires the admin to treat the generated backup/restore file as organizationally confidential data and provide appropriate secure storage measures. The TOE admin must acquire and install approved EAL4 software patches made available from the WatchGuard LiveSecurity Web site.

3.3 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.

Table 3-3 Assumptions

Name	Description
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 mail Server (e.g. bypassing the mail Server altogether by connecting the corporate and hostile networks together). Note: The threat of theft relates to theft of the TOE or other critical components resulting in interruption of the email service. The threat of device implantation relates to attaching devices to network equipment, keyboard ports or other points of physical vulnerability that could result in the unauthorized monitoring of authentication or configuration information.
A.TRANSFER	All SMTP email traffic between networks connected to the TOE will be transferred through the TOE. (If a firewall is in place in parallel to the TOE, then all ports relating to SMTP email traffic will be blocked at that firewall.)
A.USAGE	The TOE system administrator will adhere to the secure guidance provided for the operation of the TOE.
A.TRUSTED	The users of the internal network from which administration of the TOE is performed are trusted to be not willfully hostile to the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks.
A.SCALABLE	The TOE environment is appropriately scalable to provide support to the IT Systems in the organization it is deployed.

4 Security Objectives (ASE_OBJ)

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

The mapping of the objectives to the threats, OSPs, and assumptions included in the security problem definition can be found in Section 8. This mapping also provides rationale for how the threats, OSPs, and assumptions are effectively and fully addressed by the security objectives.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 4-1 Security Objectives for the TOE

Name	Description
O.ADDRESS	The TOE must limit the valid range of addresses expected on each of the network interfaces.
O.PORTS	The TOE must limit the hosts and service ports that can be accessed from each network interface.
O.DIRECT	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to the MCS.
O.MEDIATE	The TOE must mediate all access between clients and servers on the internal and external networks governed by the TOE, invoking a proxy to prevent direct connections through the TOE, and must ensure that residual information from previous information flow is not transmitted in any way.
O.MAILCTL	The TOE must only accept mail for onward delivery for recipients within the address set of the TOE, and accept mail that falls within specified content controls.
O.ATTEMPT	The TOE must provide a facility for monitoring successful and unsuccessful attempts at connections between the networks where those connections fall within the scope of the TOE (i.e. connections established to deliver or to attempt to deliver email messages).
O.NOREP	The TOE must prevent repeated attempts to guess authentication data in order to authenticate as an administrator.
O.AUDREC	The TOE must provide a means to record a readable trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ADMIN	The TOE must provide a secure method of administrative control of the TOE, ensuring that the authorized administrator, and only the authorized administrator, can exercise such control.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit use of TOE security functions by an unauthorized external entity.
O.GW	The TOE is designed or configured solely to act as a TOE and must not provide any operating system user services (e.g. login shell) to any user (including administrators). Only administrators have direct access to the TOE, i.e. can interact with the TOE management interface. Network users can only use the TOE transparently.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

Table 4-2 IT Security Objectives

Name	Description
OE.DNS	If the TOE is configured to use the DNS service, the IT environment will provide a redundant, reliable and secure Domain Name Server to the TOE.
OE.NTP	If the TOE is configured to use the NTP service, the IT environment will provide a redundant, reliable and secure Network Time Protocol Server to the TOE.
OE.SCALABLE	The TOE will be deployed with the appropriately sized hardware to ensure that the anticipated mail volume can be handled in a timely manner for the organization.
OE.USER_DATA	The administrator of the TOE must follow the organizational Security Policies regarding the viewing and modification of end-user mail. In particular, Policies can be setup which will allow carbon copy and blind carbon copy of messages to the administrator of the system. End-user mail may be modified to provide header warnings and quarantined from reaching the end-user.
OE.WEB_BROWSER	The IT environment will provide a secure and non-hostile environment for the MCS http or https connection to the TOE.
OE.SYSTEM_DATA	The IT environment will provide a secure means to store the Backup & Restore files generated during 'local' backup and restore processes using the MCS. The TOE Administrator will ensure that the Software patches and images are retrieved from the WatchGuard Live Security as identified in the supported Security Target.

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.

Table 4-3 Non-IT Security Objectives

Name	Description
OD.DELIV	Those responsible for the TOE must ensure that it is delivered, installed, managed and operated in a manner that maintains the security policy.
OD.TRAIN	Those responsible for the TOE must train administrators to establish and maintain sound security policies and practices.
OD.AUDIT	The administrator of the TOE must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Furthermore, appropriate archive action must be taken to ensure security logs archived by the TOE are not overwritten before they are inspected.
OD.MANAGE	A TOE administrator is assigned with responsibility for day to day management of configuration audit trail of the TOE.
OD.PHYSICAL	The TOE must be physically protected so that only administrators have access.
OD.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.
OD.TRANSFER	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.
OD.TRUSTED	The network from which the TOE will be administered must be trusted.

5 Extended components definition (ASE_ECD)

There are no extended components.

6 Security Requirements (ASE_REQ)

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used with respect to the Common Criteria standard. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- 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 parentheses 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.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 6-1 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

S- Selection statements; A- Assignment statements; R-Refinement statements; I-Iteration statements

Table 6-1 TOE Security Functional Requirements

Name	Description	S	A	R	I
FIA_UID.2	User identification before any action				
FIA_UAU.2	User authentication before any action				
FIA_AFL.1	Authentication failure handling	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.2	Secure security attributes		✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_SMR.1	Security roles		✓		
FMT_SMF.1	Specification of management functions		✓		
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FPT_STM.1	Reliable time stamps				
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FDP_RIP.2	Full residual information protection	✓			

6.2.1 Class FIA: Identification and Authentication

This section addresses the requirements for functions to establish and verify a claimed user identify. This includes identification of any actions that the TOE may complete on the user's behalf prior to identification or authentication.

There is one type of direct user of the TOE (within the evaluated configuration); the authorized administrator who can access and manipulate the configuration parameters. The TOE administrator is subject to identification and authentication checks.

There are also indirect, unprivileged users who send requests for connection through the TOE. These connection requests are not subject to identification and authentication. These are controlled by the UNAUTHENTICATED information flow policy.

6.2.1.1 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. [1]

6.2.1.2 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

6.2.1.3 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*five*] unsuccessful authentication attempts occur related to [*an authentication attempt by an administrator via the MCS*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*lock the account for 30 minutes; and log the unsuccessful authentication attempt*].

[1] A 'recent activity' screen and a license summary screen are available at the MCS prior to successful identification and authentication of an administrator. However, these screens do not display any TSF data or permit any TSF mediated actions (or any other administrator interaction with the administration interface).

6.2.2 Class FMT: Security management

This section defines requirements for the management of security attributes that are used to enforce the SFP.

6.2.2.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*TOE Administrator*].

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

6.2.2.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control, FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the
[*TOE administration Access Control SFP*] to restrict the ability to
[*change_default, query, modify and delete*] the security attributes *[the rules to permit or deny traffic flow*];
[*modify*] the security attributes [*TOE administrator account*];
[*change_default, query, modify*] the security attributes [*SMTP mail server configuration*];
[*change_default, query, modify*] the security attributes [*NTP server configuration*];
[*change_default, query, modify*] the security attributes [*DNS configuration*];
[*change_default, query, modify*] the security attributes [*syslog server configuration*];
[query, modify] the security attributes [*system time*];
[*query*] the security attributes [*system event log records*]
to [the TOE Administrator].

6.2.2.3 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control, FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [*security attributes*[2]].

[2] The secure value of some attributes requires consideration of the Administrator (e.g. the IP address of a DNS server). These are explained in the product user interfaces and guidance document as applicable. Other secure values are constrained by the interface (e.g. selection of a toggle switch or menu selection).

6.2.2.4 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 The TSF shall enforce the [*System Administration Access Control and Information Flow Control SFPs*[3]] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*TOE Administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.2.5 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions[4]: [

Admin account management
modifying the administrator password, user id and email address;
Network management
Configuring host and domain name and the NICs addresses and whether remote administration is permitted;
Configure static routes;
Configure the web server;
Configure mail delivery (SMTP server), including mail access/filtering, mail mapping, virtual mapping; relocated users; mail aliases; delivery settings and mail routing;
Configure the syslog server to which system event records are to be sent for storage;
Offloading and query of the audit logs[5] *stored on the TOE;*

]

[3] There is an apparent overlap with the specification of both the access control and information flow control SFPs to enforce default values. The restrictive defaults for information flow control prevent traffic from being passed through the TOE. However, the creation of Information Flow Control configuration objects relies upon the access control policy, permitting administrators to configure the information flow control parameters. The restrictive defaults for access control and information flow control are detailed in Guidance documents.

[4] The type of configuration for many of the items is explained in FMT_MSA.1.

[5] The security relevant events are stored in one of : Mail Transport log, Authentication log, Web Server Access log, Web Server Errors log, Messages log or Kernel log.

6.2.3 Class FAU: Security audit

This section involves recognizing, recording and storing information related to security relevant activities.

6.2.3.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

start-up and shutdown of the audit functions[6];
All auditable events for the [*not specified*] level of audit; and
[Every successful inbound and outbound connection;
Every unsuccessful connection;
Every successful administrator authentication attempt;
Every unsuccessful administrator authentication attempt;
Every admin command to modify the configuration].

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

Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*required destination address, and Application layer protocol for network connections*].

6.2.3.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*TOE Administrator*] 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.

6.2.3.3 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

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

[6] The start-up and shutdown of the audit trail is synonymous to the startup and shutdown of the Mail/SMTP function, as the auditing cannot be disabled.

6.2.4 Class FPT: Protection of the Trusted Security Functions

This section specifies functional requirements that relate to the integrity and management of the mechanisms providing the TSF and the TSF data.

6.2.4.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps**.**

6.2.5 Class FDP: User data protection

This section specifies requirements for TOE security functions and TOE security function policies relating to protecting user data. These are used to ensure a secure channel for administration and the control of user traffic through the TOE. The policies selected for the control of user traffic will depend on the number of interfaces configured in the TOE.

Access to the TOE internal data is controlled by the identification and authentication of a TOE Administrator at the TOE console. Once this has been completed, according to the requirements specified by the FIA class of components, an administrative user is able to access all TSF data.

There are two types of information flow:

AUTHENTICATED – remote access to the TOE requiring the source subject to be identified and authenticated as a TOE Administrator.

UNAUTHENTICATED – indirect users of the TOE who send requests for connections to specified services provided by the TOE and IT entities that respond to connection requests from the TOE.

Note: In the specification of FDP_IFF.1.2 below, the subsections of the requirement listed as ‘a)’, ‘b)’, ‘c)’, etc. are to be read as “or” operators and the bullets ‘□’ within these subsections are to be read as “and” operators.

6.2.5.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*TOE administration Access Control SFP*] on
[Subjects: identified and authenticated TOE Administrator;
Objects: TSF data (i.e. system time, event logs), security attributes;
Operations: change_default, delete, modify, query]

6.2.5.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control; FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*TOE administration Access Control SFP*] to objects based on the following:
[Subjects: identified and authenticated TOE Administrator;
Objects: TSF data (i.e. system time, event logs), security attributes;
Operations: change_default, delete, modify, query]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[identified and authenticated TOE Administrator, to change_default, modify, delete and query TSF data and security attributes (as specified in FMT_MSA.1) and query and delete items in the mail queue and quarantine queue].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the: [*Subject (indirect user) not being an identified and authenticated TOE Administrator*].

6.2.5.3 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*AUTHENTICATED and UNAUTHENTICATED information flow control SFPs*] on [*Subjects: external IT entities that send and receive information through the TOE to one another, or external IT/human entities that send and receive information to/from the TOE; Information: traffic sent through the TOE from one subject to another, or traffic sent to/from the TOE; Operation: permit or deny information through the TOE or permit or deny information to terminate at the TOE*].

6.2.5.4 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [*UNAUTHENTICATED and AUTHENTICATED information flow control SFPs*] based on the following types of subject and information security attributes:

[*Subject security attributes:*
Presumed address,
Information security attributes:
Presumed address of source subject;
Presumed address of destination subject;
Transport layer protocol;
TOE interface on which traffic arrives and departs;
Services requested.]

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

a) Subjects can cause information to flow through the TOE to another connected network according to the UNAUTHENTICATED information flow control SFP only if :
- *All information security attributes are unambiguously permitted by the connection policy rules, where such rules are composed of the combination of the security attributes [7]relating to information flow created by the administrator*
- *A proxy server (SMTP) is configured to service the request;*

b) Subjects can cause information to flow between the TOE (Web Server) and the administrator according to the AUTHENTICATED information flow control SFP only if:

[7] As detailed in FMT_MSA.1

- *All information security attributes are unambiguously permitted by the connection policy rules, where such rules are composed of the combination of the security attributes[8] relating to information flow created by the administrator.*

c) The TOE can cause information to flow between itself and external IT entities according to the UNAUTHENTICATED information flow control SFP only if:

- *A client (NTP, DNS) is configured on the TOE to initiate and service the request.*

]

FDP_IFF.1.3 The TSF shall enforce the [additional information flow control SFP rules: a) none].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*no additional rules to authorize information flow*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [
There are no rules which explicitly allow it;
If any of the attributes identified in FDP_IFF.1.1 do not match].

FDP_RIP.2 Full residual information protection

Hierarchical to: FDP_RIP.1 Subset residual information protection
Dependencies: No dependencies.

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to*] all objects.

[8] As detailed in FMT_MSA.1

6.3 Security Assurance Requirements

The assurance requirements for this Security Target, taken from Part 3 of the CC, compose the EAL4 level of assurance, augmented with the Flaw Remediation assurance component and with vulnerability analysis component. The assurance components are summarized in the following table.

Table 6-2 Assurance Requirements: EAL4 Augmented by ALC_FLR.2

Assurance Class	Assurance components	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.2	Basic flaw reporting procedures
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

Further information on these assurance components can be found in [CC] Part 3.

7 TOE Summary Specification (ASE_TSS)

7.1 TOE Security Functions

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the WatchGuard XCS Server in Section 5.1. These are grouped into the following categories:

Identification and authentication;

Management;

Audit;

and Communication Control.

7.1.1 Identification and Authentication

A single administrator account is supported by the TOE.

The TOE Administrator must be identified and authenticated before able to access any data managed by the TOE or access any TOE functions. When accessing the TOE through the system console, the TOE Administrator is authenticated using a username and password. When accessing the TOE remotely using the web administration interface (MCS), the TOE Administrator is authenticated through a username/password mechanism.

The administrator account is locked for 30 minutes following 5 unsuccessful authentication attempts via the MCS.

7.1.2 Management

The TOE includes a standard Apache Web server, through which the TOE Administrator can configure the TOE. This will provide a restrictive interface, constraining the accepted input.

The following attributes of the TOE Administrator account can be configured by the TOE Administrator: password, user id and email address to receive any email directed towards the system administrator.

The following network settings of the TOE can be configured by the TOE Administrator:

IP addresses and whether Admin login is permitted from that interface. (Also, for the purposes outside the scope of the evaluation, whether the interface is trusted, access to a POP3 server is permitted and access to Web mail is permitted).

The address of the NTP server providing source data for clock maintained by the TOE.

The Administration GUI should be enabled on an interface connected to a local network. The web mail and POP services are outside the scope of the TOE and should not be enabled. When an interface is marked as trusted, this means that email messages received from any IP address contained within that interface's subnet are considered to be from a trusted source.

The TOE Administrator can configure static routes where the corporate mail server to which mail must be delivered is on another corporate network.

The TOE Administrator can configure mail delivery (SMTP server), including:

mail access/filtering - add/modify/delete the access patterns permitted/denied;

mail mapping - add/modify/delete the mapping between external and internal mail addresses;

virtual mapping - add/modify/delete the incoming and redirected addresses;

attachment control - specify whether attachments of file types (.pif, .ps, .psd, .rtf, .scr, .snd, .sys, .tif, .vbe, .vbs) are permitted or blocked;

relocated users - add/modify/delete new contact details for obsolete email addresses;

mail aliases - add/modify/delete alias for email address;

delivery settings - add/modify/delete values of parameters for maximum time in mail queue; time delay warning; time to retain undelivered mail, strip received headers; masquerade addresses, relay to, ignore MX file, copy mail to, send errors to, modify annotation, delivery failure notification, delivery delay warning.

The TOE administrator can view details (headers, etc) and delete items in the mail queue and the quarantine queue. The Administrator can also flush the mail queue.

The TOE Administrator defines the domains (mail routing) for which the TOE should accept mail. Accepted mail will be forwarded to corporate SMTP server(s) (in the TOE environment) using Mail routing, aliasing and mail mapping.

The TOE Administrator can configure the system time either manually or using an NTP service.

The TOE Administrator can configure the status and utility functions and DNS functions;

The TOE Administrator can configure the secondary syslog server (in the IT environment) to which copies of event records may be directed.

The TOE Administrator can reboot and shutdown of the TOE.

The TOE Administrator can update the software of the system using the WatchGuard LiveSecurity web site and guidance from the TOE Reference section of the latest XCS Common Criteria Security Target.

The TOE Administrator can backup and restore configuration data using the Local Disk method with the MCS system.

7.1.3 Audit

The following logs will always be maintained by the TOE, recording security relevant events relating to access to the TOE and traffic through the TOE:

Mail Transport - log all inbound/outbound mail;

Web Server Access and Web Server Errors logs - log all successful and unsuccessful connections through browser interface, all attempted administrator commands to modify the configuration (http commands);

Authentication log - log all TOE Administrator access (authentication) attempts and start-up and shut-down of the TOE;

Messages log - log all NTP client activity;

Kernel log - log all kernel messages.

The following data is always recorded in the log files for each record:

Date, time and type of the event, subject identity (source address) and outcome of the event.

The following data is recorded in the log files for network connection requests:

Required destination address and application level protocol.

A web browser interface is provided for the TOE Administrator to inspect the logs. This interface is constrained to permit either read-only access to the contents of the log file or deletion of the complete log file.

7.1.4 Communication Control

The types of communication with the TOE are described in section 1.3. The methods and controls used for this communication are then described in Section 1.3.1 of this document. This information is not reproduced here, and Section 1.3 is considered to form part of the TOE Summary Specification. The rationale for the completeness of the information is provided in Section 8.5.4, along with the rationale for the other aspects of the TOE Summary Specification.

Any padding required for data packets transmitted on the network interfaces will be randomly generated.

7.2 Assurance Measures

Deliverables will be produced to comply with the Common Criteria Assurance Requirements for EAL4, augmented with ALC_FLR.2.

8 RATIONALE

8.1 Conformance Claims Rationale

This Security Target conforms to part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 rev 2.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Section 8.2.1, 8.2.2, 8.2.3 demonstrates the mappings between the threats, policies, and assumptions to the security objectives. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

Table 8-1 Mapping of TOE Security Objectives to Threats, Policies and Assumptions

Security Objectives / Threats, Policies, Assumptions	TOE Objectives											Environmental Objectives													
												Non-IT								IT					
	O.ADDRESS	O.PORTS	O.DIRECT	O.MEDIATE	O.MAILCTL	O.ATTEMPT	O.NOREP	O.AUDREC	O.ADMIN	O.LIMEXT	O.GW	OD.DELIV	OD.TRAIN	OD.AUDIT	OD.MANAGE	OD.PHYSCIAL	OD.REVIEW	OD.TRANSFER	OD.TRUSTED	OE.SCALABLE	OE.USER_DATA	OE.DNS	OE.NTP	OE.WEB_BROWSER	OE.SYSTEM_DATA
Threats																								
T.CONN	✓	✓		✓	✓																			
T.MEDIAT		✓	✓	✓																				
T.REM_CONN	✓	✓	✓	✓					✓	✓														
T.REPEAT							✓																	
T.DETECT						✓		✓	✓															
T.SOURCE	✓	✓																						
T.CONFIG	✓	✓																						
T.OS_FAC	✓	✓		✓							✓													
T.OPEN_RELAY					✓																			
T.SELPRO			✓		✓			✓	✓	✓	✓													
T.OLDINF	✓	✓		✓																				
T.UNSOLICITED					✓																			
T.USAGE									✓							✓	✓							
T.VIOLATE												✓	✓	✓	✓									

Security Objectives / Threats, Policies, Assumptions	TOE Objectives											Environmental Objectives											
												Non-IT								IT			
	O.ADDRESS	O.PORTS	O.DIRECT	O.MEDIATE	O.MAILCTL	O.ATTEMPT	O.NOREP	O.AUDREC	O.ADMIN	O.LIMEXT	O.GW	OD.DELIV	OD.TRAIN	OD.AUDIT	OD.MANAGE	OD.PHYSCIAL	OD.REVIEW	OD.TRANSFER	OD.TRUSTED	OE.SCALABLE	OE.USER_DATA	OE.DNS	OE.NTP	OE.WEB_BROWSER	OE.SYSTEM_DATA
Policies																								
P.SERVICES																					✓	✓		
P.WEB_BROWSER																							✓	
P.SYSTEM_DATA																								✓

Security Objectives / Threats, Policies, Assumptions	TOE Objectives											Environmental Objectives											
												Non-IT								IT			
	O.ADDRESS	O.PORTS	O.DIRECT	O.MEDIATE	O.MAILCTL	O.ATTEMPT	O.NOREP	O.AUDREC	O.ADMIN	O.LIMEXT	O.GW	OD.DELIV	OD.TRAIN	OD.AUDIT	OD.MANAGE	OD.PHYSCIAL	OD.REVIEW	OD.TRANSFER	OD.TRUSTED	OE.SCALABLE	OE.USER_DATA	OE.DNS	OE.NTP	OE.WEB_BROWSER	OE.SYSTEM_DATA
Assumptions																								
A.PHYSICAL												✓				✓								
A.TRANSFER																		✓						
A.USAGE												✓	✓	✓	✓	✓	✓	✓			✓			
A.TRUSTED																			✓					
A.SCALABLE																				✓				

8.2.1 Security Objectives Rationale Relating to Threats

The following table describes the mapping of threats to objectives.

Table 8-2 Threats: Objectives Mapping

Threats	Objectives	Rationale
T. CONN An unauthorized person may attempt to establish a connection across the TOE between networks or hosts to compromise the network and data assets. This threat includes but is not limited to SMTP protocol attacks on e-mail servers.	O.PORTS The TOE must limit the hosts and service ports that can be accessed from each network interface.	The TOE controls the information flow between the networks. The TOE limits the hosts and service ports, the address ranges and the recipient address of the mail message. The TOE will not permit any direct connections through the TOE, by providing proxy services for all permitted connections.
	O.ADDRESS The TOE must limit the valid range of addresses expected on each of the network interfaces.	
	O.MAILCTL The TOE must only accept mail for onward delivery for recipients within the address set of the TOE, and accept mail that falls within specified content controls.	
	O. MEDIATE The TOE must mediate all access between clients and servers on the internal and external networks governed by the TOE.	
T.MEDIAT An unauthorized person may attempt to send impermissible information through the TOE to exploit services on the internal network.	O. MEDIATE The TOE must mediate all access between clients and servers on the internal and external networks governed by the TOE.	The TOE mediates flow of all information between clients and servers on internal and external networks. The TOE restricts the information flow between the networks to permissible types of flow only by limiting the hosts and service ports. The TOE will not permit any direct connections through the TOE, by providing proxy services for all permitted connections. Any connection requests to the TOE must be successfully identified and authenticated before access is permitted.
	O.PORTS The TOE must limit the hosts and service ports that can be accessed from each network interface.	
	O.DIRECT The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to the MCS.	

Threats	Objectives	Rationale
T.REM_CONN A remote connection established to the TOE that could be exploited by an attacker to compromise the TOE service and data assets.	O.PORTS The TOE must limit the hosts and service ports that can be accessed from each network interface.	The TOE limits the hosts and service ports, address ranges and functions available from the network interfaces. The TOE will not permit any direct connections through the TOE, by providing proxy services for all permitted connections. Any connection requests with the TOE must be successfully identified and authenticated before access is permitted and will be protected to ensure only the administrator can read or modify transmitted data.
	O.ADDRESS The TOE must limit the valid range of addresses expected on each of the network interfaces.	
	O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit use of TOE Server security functions by an unauthorized external entity.	
	O. MEDIATE The TOE must mediate all access between clients and servers on the internal and external networks governed by the TOE.	
	O.DIRECT The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to the MCS	
	O.ADMIN The TOE must provide a secure method of administrative control of the TOE.	
T.REPEAT An unauthorized person may repeatedly attempt to guess authentication data to gain access to the TOE.	O.NOREP The TOE must prevent repeated attempts to guess authentication data in order to authenticate as an administrator.	The TOE provides controls at point of authentication to prevent the repeated attempts to guess authentication information.

Threats	Objectives	Rationale
T.DETECT An attacker succeeds in compromising network, data and TOE service assets without being detected.	O.ATTEMPT The TOE must provide a facility for monitoring successful and unsuccessful attempts at connections between the networks where those connections fall within the scope of the TOE.	The TOE provides a facility to monitor successful and unsuccessful connections requests between networks. The authorized administrator should regularly inspect the logs generated by this facility to detect unauthorized activity.
	O.AUDREC The TOE must provide a means to record a readable trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.	
	O.ADMIN The TOE must provide a secure method of administrative control of the TOE.	
	OD.AUDIT The administrator of the TOE must ensure that the audit facilities are used and managed effectively	
T.SOURCE An attacker may attempt to initiate a service from an unauthorized source, by sending an IP packet with a fake source address.	O.ADDRESS The TOE must limit the valid range of addresses expected on each of the network interfaces.	The TOE controls the information flow between the networks. TOE limits the address ranges expected on each network interface and the services available at each interface.
	O.PORTS The TOE must limit the hosts and service ports that can be accessed from each network interface.	
T.CONFIG An attacker on the corporate/hostile network may attempt to exploit an insecure configuration of the TOE in order to gain access to the restricted resources/data on the protected network not in accordance with the chosen network security policy.	O.PORTS The TOE must limit the hosts and service ports that can be accessed from each network interface.	The TOE controls the information flow between the networks. The TOE limits the hosts and service ports and address ranges. The TOE will not permit any direct connections through the TOE, by providing proxy services for all permitted connections. The configuration of the TOE should be inspected regularly by the administrator to ensure it meets the security objectives for the network.
	O.ADDRESS The TOE must limit the valid range of addresses expected on each of the network interfaces.	

Threats	Objectives	Rationale
	O. MEDIATE The TOE must mediate all access between clients and servers on the internal and external networks governed by the TOE.	
	OD.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	
T.OS_FAC An attacker on the corporate/hostile network may attempt to use operating system facilities on the TOE server in order to gain access to the restricted resources/data on the protected network not in accordance with the chosen network security policy.	O.GW The TOE is designed or configured solely to act as a XCS Server and must not provide any operating system user services (e.g. login shell) to any user (including administrators). Only administrators have direct access to the TOE, i.e. can interact with the TOE management interface. Network users can only use the TOE transparently.	The TOE does not provide any operating system services to any user of the TOE (there is no command line access provided). The TOE controls the information flow between the networks. TOE limits the hosts and service ports and address ranges. The TOE will not permit any direct connections through the TOE, by providing proxy services for all permitted connections.
	O. MEDIATE The TOE must mediate all access between clients and servers on the internal and external networks governed by the TOE.	
	O.PORTS The TOE must limit the hosts and service ports that can be accessed from each network interface.	
	O.ADDRESS The TOE must limit the valid range of addresses expected on each of the network interfaces.	

Threats	Objectives	Rationale
T.OPEN_RELAY An unauthorized e-mail source may utilize the TOE as a bulk e-mail delivery system which will compromise the acceptable use policy for the TOE; and negatively affect the global reputation of the company's ability to sending valid email. Bulk e-mail falls outside the acceptable use policy for the TOE when the recipients of the e-mail are outside the set of addresses for which the TOE normally handles.	O.MAILCTL The TOE must only accept mail for onward delivery for recipients within the address set of the TOE, and accept mail that falls within specified content controls.	The TOE limits the mail messages accepted, to those messages addressed to recipients within the address set of the TOE.
T.SELPRO An unauthorized person may read, modify or destroy security critical TOE configuration data.	O.DIRECT The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to the MCS O.ADMIN The TOE must provide a secure method of administrative control of the TOE. O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit use of TOE Server security functions by an unauthorized external entity. O.GW The TOE is designed or configured solely to act as a XCS Server and must not provide any operating system user services (e.g. login shell) to any user (including administrators). Only administrators have direct access to the TOE, i.e. can interact with the TOE management interface. Network users can only use the TOE transparently.	The TOE enforces controls to ensure only the TOE Administrator can access and amend the configuration. The TOE does not provide any operating system services to any user of the TOE (there is no command line access provided), preventing alternative routes to attempt to access and modify security critical TOE configuration data. TOE will monitor attempts to initiate connections at the network interfaces, including attempts to initiate a remote administration session. The logs of connection attempts should be inspected on a regular basis and configuration of the TOE should be inspected regularly by the administrator to ensure it meets the security objectives for the network.

Threats	Objectives	Rationale
	O.ATTEMPT The TOE must provide a facility for monitoring successful and unsuccessful attempts at connections between the networks where those connections fall within the scope of the TOE.	
	O.AUDREC The TOE must provide a means to record a readable trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.	
	OD.AUDIT The administrator of the TOE must ensure that the audit facilities are used and managed effectively.	
	OD.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	
T.OLDINF An unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.	O.ADDRESS The TOE must limit the valid range of addresses expected on each of the network interfaces.	The TOE mediates information flow and ensures no residual information is transmitted.
	O.PORTS The TOE must limit the hosts and service ports that can be accessed from each network interface.	
	O. MEDIATE The TOE must mediate all access between clients and servers on the internal and external networks governed by the TOE.	

Threats	Objectives	Rationale
	O.MAILCTL The TOE must only accept mail for onward delivery for recipients within the address set of the TOE, and accept mail that falls within specified content controls.	
T.UNSOLICITED An unauthorized e-mail source may send unsolicited bulk mail where the content of those messages falls outside of a defined acceptable use policy or where the volume of messages is considered to pose a threat to the effective processing of other e-mail messages.	O.MAILCTL The TOE must only accept mail for onward delivery for recipients within the address set of the TOE, and accept mail that falls within specified content controls.	The TOE will not accept messages for onward delivery or delivery to TOE hosted mailboxes if the content of the message falls outside the content configuration controls.
T.USAGE The TOE may be inadvertently or maliciously configured, used and administered in an insecure manner by either authorized or unauthorized persons.	OD.PHYSICAL The TOE must be physically protected so that only administrators have access.	The TOE will be physically protected to prevent unauthorized persons from altering the physical configuration. The configuration of the TOE will be regularly inspected by the authorized administrator to ensure the configuration upholds the organization's security policies.
	O.ADMIN The TOE must provide a secure method of administrative control of the TOE.	
	OD.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	
T.VIOLATE Careless or willfully negligent system administrators may violate network security policies by inappropriate action or inaction required on the TOE.	OD.DELIV Those responsible for the TOE must ensure that it is delivered, installed, managed and operated in a manner that maintains the security policy.	The administrator of the TOE is trusted to install, manage and operate (including using and managing the audit facilities) the TOE in a manner consistent with the security policy. The TOE Administrator should be provided with the appropriate training.

Threats	Objectives	Rationale
	OD.MANAGE A TOE administrator is assigned with responsibility for day to day management of configuration audit trail of the TOE.	The logs generated by this facility should be regularly inspected by the authorized administrator to detect unauthorized activity.
	OD.TRAIN Those responsible for the TOE must train administrators to establish and maintain sound security policies and practices.	
	O.ADMIN The TOE must provide a secure method of administrative control of the TOE.	
	OD.AUDIT The administrator of the TOE must ensure that the audit facilities are used and managed effectively.	

8.2.2 Security Objectives Rationale Relating to Policies

Table 8-3 Policies: Objectives Mapping

Policies	Objectives	Rationale
P.WEB_BROWSER The administrator will use the http/https MCS access in a secure room on a secure network.	**OE.WEB_BROWSER** The IT environment will provide a secure and non-hostile environment for the http or https connection to the TOE.	The OE.WEB_BROWSER objective ensures the protection of TOE and user data from unauthorized access and modification.
P.SERVICES The TOE will have access to physically and logically secure support services such as NTP and DNS**.**	**OE.DNS** If the TOE is configured to use the DNS service, the IT environment will provide a redundant, reliable and secure Domain Name Server to be used by the TOE.	The TOE may be configured to use external servers which provide network services like Domain Name Services or Network Time. These services are optional for operation of the TOE, however if they are enabled, it is the responsibility of the security organization to ensure that the server is maintained in a reliable and secure manner.
	OE.NTP If the TOE is configured to use the NTP service, the IT environment will provide a redundant, reliable and secure Network Time Protocol Server to be used by the TOE.	
P.SYSTEM_DATA The administrator will securely store the backup & restore file generated by the TOE. The administrator will acquire approved EAL4 software patches and images (identified in the released Security Target) from the WatchGuard LiveSecurity Web site.	**OE.SYSTEM_DATA** The IT environment will provide a secure means to store the Backup & Restore files generated during 'local' backup and restore processes using the MCS access. The TOE administrator will ensure that the Software Patches and images are retrieved from the WatchGuard Live Security as identified in the supported Security Target.	The Backup file generated contains sensitive configuration data which must be treated as confidential information for the enterprise. The WatchGuard LiveSecurity Web site is the only approved site for retrieving software patches and documentation. Any software patches applied to the system must be identified in the latest Security target's TOE reference.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

The following table describes the mapping of assumptions to objectives.

Table 8-4 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
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).	OD.DELIV Those responsible for the TOE must ensure that it is delivered, installed, managed and operated in a manner that maintains the security policy.	The OD.DELIV objective provides access control to the TOE during delivery.
	OD.PHYSICAL The TOE must be physically protected so that only administrators have access.	The OD.PHYSICAL objective provides access control to the TOE during operation.
A.TRANSFER All SMTP email traffic between networks connected to the TOE will be transferred through the TOE. (If a firewall is in place in parallel to the TOE, then all ports relating to SMTP email traffic will be blocked at that firewall.)	OD.TRANSFER 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.	The OD.TRANSFER objective provides assurance that all mail traffic between interconnected networks will pass through the TOE.
A.USAGE The TOE Administrator will adhere to the secure guidance provided for the operation of the TOE.	OD.DELIV Those responsible for the TOE must ensure that it is delivered, installed, managed and operated in a manner that maintains the security policy.	In seeking to achieve the procedural and environment objectives specified for the non-IT environment, the administrator will be following the secure guidance for the operation of the TOE.
	OD.TRAIN Those responsible for the TOE must train the administrator to establish and maintain sound security policies and practices.	
	OD.AUDIT The administrator of the TOE must ensure that the audit facilities are used and managed effectively.	
	OD.MANAGE A TOE administrator is assigned with responsibility for day to day management of configuration audit trail of the TOE.	

Assumptions	Objectives	Rationale
	OD.PHYSICAL The TOE must be physically protected so that only administrators have access.	
	OD.TRANSFER 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.	
	OD.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.	
	OE.USER_DATA The administrator of the TOE must follow the organizational Security Policies regarding the viewing and modification of end-user mail.	
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.	OD.TRUSTED The network from which the TOE will be administered must be trusted.	The OD.TRUSTED objective supports this assumption by preventing physical access to unauthorized entities from accessing the administrator function of the TOE.
A.SCALABLE The TOE environment is appropriately scalable to provide support to the IT Systems in the organization it is deployed.	OE.SCALABLE The TOE will be deployed with the appropriately sized hardware to ensure that the anticipated mail volume can be handled in a timely manner for the organization	The OE.SCALABLE objective supports this assumption by ensuring the administrator has evaluated the organization usage and has acquired the necessary hardware appliance to meet the organizations needs.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended SFRs for this evaluation of the TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs for this evaluation of the TOE.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

The following table describes the mapping of objectives to SFRs.

Table 8-5 Objectives: SFRs Mapping

Objective	Requirements addressing the Objective	Rationale
O.ADDRESS The TOE must limit the valid range of addresses expected on each of the network interfaces.	FDP_IFC.1 Subset information flow control	The range of addresses expected on the corporate and hostile network are limited by the control of information flow through the TOE. Information flow control is based on the security of attributes of the request, including the source address of the request. This address is linked to the interface on which the request was received to ensure it is an address expected on that interface. These checks 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.
	FDP_IFF.1 Simple security attributes	
O.PORTS The TOE must limit the hosts and service ports that can be accessed from each network interface.	FDP_IFC.1 Subset information flow control	The TOE must limit the corporate hosts and service ports that can be accessed from each network interface. The TOE controls information flow between interfaces by allowing or denying traffic through: presumed address of source subject; presumed address of destination subject; transport layer protocol; TOE interface on which traffic arrives and departs; and services requested.
	FDP_IFF.1 Simple security attributes	

Objective	Requirements addressing the Objective	Rationale
	FMT_MSA.3 Static attribute initialization	The TOE will deny any information flows for which no rule is defined and defaults to deny all information flows through the TOE. These checks 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.
O.MEDIATE The TOE must mediate all access between clients and servers on the internal and external networks governed by the TOE, invoking a proxy to prevent direct connections through the TOE, and must ensure that residual information from previous information flow is not transmitted in any way.	FMT_MSA.3 Static attribute initialization	The TOE controls information flows between interfaces. For requests to pass information through the TOE, the TOE only forwards the information if the administrator has configured a proxy server to service the request.
	FDP_RIP.2 Subset residual information protection	The TOE will ensure that neither the information associated with previous flows through the TOE nor any internal TOE data is used as padding for information flow.
O.DIRECT The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to the MCS.	FIA_UID.2	The TOE controls information flows between interfaces, as described above (O.ADDRESS, O.PORTS and O. MEDIATE). These rules implement the UNAUTHENTICATED and AUTHENTICATED information flow policies. Any user requesting to manipulate the TOE configuration or access the audit trails, must be identified and authenticated as a TOE Administrator before access is permitted.
	FIA_UAU.2	
O.MAILCTL The TOE must only accept mail for onward delivery for recipients within the address set of the TOE, and accept mail that falls within specified content controls.	FDP_IFC.1 Subset information flow control	The TOE must limit the corporate hosts and service ports that can be accessed from each network interface. The TOE controls information flow between interfaces by allowing or denying traffic through based on: presumed address of source subject; presumed address of destination subject; transport layer protocol (if SMTP, presumed recipient of mail message is checked against those hosted within corporate network); TOE interface on which traffic arrives and departs; Service requested.
	FDP_IFF.1 Simple security attributes	
O.ATTEMPT The TOE must provide a facility for monitoring successful and unsuccessful attempts at connections between the networks where those connections fall within	FMT_SMR.1 Security Roles	TOE only maintains one type of direct user: TOE Administrator – able to manipulate the configuration of the TOE and view the audit trail data; A constrained interface ensures the administrator only has access to those administration functions necessary to operate and maintain the TOE, preventing direct
	FMT_MSA.1 Management of security attributes	

Objective	Requirements addressing the Objective	Rationale
the scope of the TOE (i.e. connections established to deliver or to attempt to deliver email messages).	FMT_MSA.2 Secure security attributes FMT_MSA.3 Static Attribute initialization FIA_UID.2 User identification before any action FIA_UAU.2 User authentication before any action FDP_ACC.1 Subset access control FDP_ACF.1 Security attribute based access control	interaction with the operating system. Identification and authentication of the requesting user provides an access control mechanism to the management functions of the TOE.
O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit use of TOE security functions by an unauthorized external entity.	FAU_GEN.1 Audit data generation FAU_SAR.1 Audit review FAU_STG.1 Protected audit trail storage	The TOE provides an accounting mechanism that cannot be disabled. The start-up and shutdown of the audit function is synonymous with the start-up and shutdown of the TOE. Start-up and shutdown of the TOE is recorded in the audit log. All inbound and outbound connection attempts can be recorded with their associated data. The TOE provides the facility for the TOE Administrator to view the audit trail with read-only access) Accounting and audit functions will be completed as appropriate 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
O.NOREP The TOE must prevent repeated attempts to guess	FIA_UID.2 User Identification before any action	Repeated attempts to authenticate are prevented by locking the administrator account for 30 minutes following 5 failed authenticated attempts.

Objective	Requirements addressing the Objective	Rationale
authentication data in order to authenticate as an administrator.	FIA.UAU.2 User authentication before any action	
	FIA_AFL.1 Authentication failure handling	
O.AUDREC The TOE must provide a means to record a readable trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.	FAU_GEN.1 Audit Data Generation	The TOE provides an accounting mechanism that cannot be disabled. The start-up and shutdown of the audit function is synonymous with the start-up and shutdown of the TOE. Start-up and shutdown of the TOE is recorded in the audit log. The following events can be recorded with their associated data: All inbound and outbound connection attempts; Every successful and unsuccessful administrator authentication; Change of administrator password; The TOE provides the facility for the TOE Administrator to view the audit trail (read-only access) .
	FPT_STM.1 Reliable time stamps	
	FIA_AFL.1 Authentication failure handling	
	FIA_UID.2 User Identification before any action	
	FIA_UAU.2 User authentication before any action	
	FAU_SAR.1 Audit review	
	FAU_STG.1 Protected audit trail storage	
O.ADMIN The TOE must provide a secure method of administrative control of the TOE, ensuring that the authorized administrator, and only the authorized administrator, can exercise such control.	FMT_SMF.1 Specification of management functions	TOE provides an interface through which the administrator can administer the TOE, controlling access an unauthorized user has through the TOE.

Objective	Requirements addressing the Objective	Rationale
O.GW The TOE is designed or configured solely to act as a TOE and must not provide any operating system user services (e.g. login shell) to any user (including administrators). Only administrators have direct access to the TOE, i.e. can interact with the TOE management interface. Network users can only use the TOE transparently.	FDP_IFF.1 Simple security attributes	The TOE is designed to provide no operating system user services by ensuring the information flows do not access the operating system and that separate domains are provided in which to process security functions and controlling the invocation of subsequent functions. As it can be seen in the descriptions above, all objectives are satisfied by at least one SFR and all SFRs are required to meet at least one objective. Therefore, all SFRs specified for the TOE are appropriate to counter the threats and meet the objectives of the TOE.

8.5.2 Security Requirements Rationale for Refinement

There are no refinements of Security Requirements for this evaluation of the TOE.

8.5.3 Security Assurance Requirements Rational

EAL4, augmented with ALC_FLR.2 was chosen to provide a moderate to high level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment.

In the Internet area of IT new exploits are continually being discovered and published, which the TOE will be expected to protect the corporate network against. It is therefore considered to be appropriate to augment the EAL4 assurance requirements for the TOE with the ALC_FLR.2 assurance component. This will provide additional assurance that new vulnerabilities identified and reported in the services the product supports, or in the product itself, are addressed in a controlled and suitable manner.

8.5.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. The following table 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 8-6 Functional Requirements Dependencies

SFR	Dependency	Dependency Met	Rationale
FIA_AFL.1	FIA_UAU.1	✓	satisfied by hierarchical FIA_UAU.2 component
FIA_UAU.2	FIA_UID.1	✓	FIA_UAU.2 is hierarchal to FIA.UAU.1 Dependency satisfied by hierarchical FIA_UID.2 component
FIA_UID.2	none	N/A	FIA_UID.2 is hierarchal to FIA_UID.1
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1,	✓	

SFR	Dependency	Dependency Met	Rationale
	FMT_SMF.1, FDP_IFC.1		
FMT_MSA.2	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1, FDP_IFC.1	✓	
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	✓	
FMT_SMR.1	FIA_UID.1	✓	Dependency satisfied by hierarchical FIA_UID.2 component
FMT_SMF.1	none	N/A	
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FPT_STM.1	none	N/A	
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	✓	
FDP_RIP.2	none	N/A	FDP_RIP.2 is hierarchal to FDP_RIP.1

As demonstrated in the table above, each of the SFRs identified as dependencies have been stated as Functional Components of the TOE. Therefore, all dependencies have been satisfied.

9 Acronyms

Acronym	Definition
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol, Secure
IP	Internet Protocol
IT	Information Technology
MCS	Management/Configuration Server
OSP	Organization Security Policy
POP	Post Office Protocol
PP	Protection Profile
SFP	Security Function Policy
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
UCE	Unsolicited Commercial E-mail
UDP	User Datagram Protocol
WWW	World Wide Web
XCS	Extensible Content Security