BorderWare™
Security that works.

Security Target for

BorderWare MXtreme Appliance Models MX-200, MX-400 & MX-800, and specified OEM Appliances, running MXtreme **Mail Firewall V3.1**

Reference: ST

August 2004

Version: 3.0

North America:
50 Burnhamthorpe Rd. W.
Suite 502
Mississauga
Ontario
Canada L5B 3C2

Europe:
Vista Business Centre
50 Salisbury Rd
Hounslow
Middlesex
TW4 6JQ   U.K.

DOCUMENT AUTHORISATION

DOCUMENT TITLE	Security Target for BorderWare MXtreme Appliance Models MX-200, MX-400 & MX-800, and specified OEM Appliances, running MXtreme Mail Firewall 3.1

Version	Date	Description
1.0	October 2002	Release for review
2.0	December 2003	Updated to ensure TSS is consistent with SFRs
2.5	March 2004	Further updates to clarify scope and minor editorial changes
2.6	April 2004	Updated to add OEM hardware to scope, addressed CB comments
2.7	April 2004	Address CB comments
2.8	April 2004	Address CB comments
2.9	April 2004	Clarify OEM Hardware
3.0 draft C	May 2004	Draft for CR issue
3.0	August	Final version incorporating comments generated by CR

Contents

REFERENCES

[CC]	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (aligned with ISO 15408), with Final Interpretations as at 31 October 2003
[ECG]	BorderWare MXtreme Mail Firewall v3.1, EAL4 Configuration Guide, Release 9

GLOSSARY AND TERMS

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
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

1 Introduction to the Security Target

1.1 Security Target Identification

Title: Security Target for BorderWare MXtreme Appliance Models MX-200, MX-400 & MX-800, and specified OEM Appliances, running MXtreme Mail Firewall 3.1

Assurance Level: EAL4, augmented with ALC_FLR.1 and AVA_VLA.3

1.2 Security Target Overview

BorderWare MXtreme Mail Firewall is a uniquely designed inclusive SMTP, POP and IMAP server that secures Internet e-mail and protects corporate mail systems.

Deployment is simple. MXtreme is delivered as an appliance installs in minutes and is immediately ready for use as a high security mail server that can be deployed anywhere on the corporate network or on the Internet.

Security is based on BorderWare's S-Core technology, which is at the heart of the BorderWare Firewall Server, and which provides a complete, secure OS.

Administration requires no specialised IT knowledge or experience. BorderWare S-Core supplies a secure platform that requires no intervention. Administration is carried out via an intuitive browser interface. Following the simple initial set-up, user accounts can be added, mail maps and aliases specified, and parameters such as mail routes and anti-virus regimes defined.

This ST is structured according to the families of the ASE class as indicated by the Contents section. The rationales are contained in Section 8.

1.3 CC Conformance Claim

This TOE has been developed to conform to the functional components as defined in the Common Criteria version 2.1 [CC] part 2, with the assurance level of EAL4, augmented with ALC_FLR.1 and AVA_VLA.3 as identified in part 3 of [CC]. Assurance gained during this evaluation will be maintained under an assurance maintenance scheme.

2 TOE Description

2.1 MXtreme Features

The BorderWare MXtreme Mail Firewall is designed as a comprehensive e-mail security solution protecting the client and server components used in corporate e-mail systems, screening the content of e-mails sent via corporate e-mail systems and protecting the confidentiality of information sent and received by corporate e-mail systems. The TOE is designed to be deployed as a dedicated device securing e-mail applications only. The TOE will normally form part of an organisation's network security defences with other components such as a general purpose Firewall securing other applications.

The TOE provides a range of features designed to implement the security functions and to provide supporting services. The feature set includes:

1. 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.

2. 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.

3. 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.

4. 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 address(es) 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.

5. 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).

6. Management, monitoring and audit functions. The TOE includes all management monitoring and audit functions implemented by the MXtreme Mail Firewall.

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

The TOE supports between two and four network interface depending on the model deployed. At least one interface must be configured with an appropriate IP address for remote administration, two for receiving and forwarding traffic between networks. Interfaces that are not configured with an IP address will not be used by the TOE (no servers will accept connections on those interfaces and no clients will attempt to establish connections through those interfaces). A typical configuration would be to use two network interfaces as shown in Figure 2-1. In this configuration the TOE is normally deployed in parallel with a general purpose Firewall. The TOE will process all inbound and outbound e-mail for the protected organisation. As the Firewall no longer needs to permit connections for e-mail protocols the existing Firewall's configuration may be modified by blocking the passage of mail protocols through the Firewall. Moving all e-mail traffic from a general purpose Firewall which is likely to do little more that simply permit or deny e-mail protocol connections to a specialist dedicated device that can examine the data content of these protocols offers a net increase in the overall level of security

If local security policy prohibits the deployment of the TOE in parallel with an existing Firewall, the TOE may be deployed with a single network interface that is connected to the network segment protected by the Firewall. The Firewall would then 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 organisations whose policies prohibit any device to be connected in parallel with the Corporate Firewall.

Regardless of the number of network interfaces installed, the TOE treats each network interface as untrusted. (The networks are only designated as "trusted" during configuration for the purpose of SPAM controls, which are outside the scope of the evaluation.) If more than two network interfaces are installed, the additional network interfaces may be used to connect additional e-mail servers or may be used to provide extra links to remote networks. The TOE is built on the S-CORE operating system. S-CORE is a hardened operating system that has been specifically designed by BorderWare Technologies Inc and is derived from BSD 4.2 Unix. S-CORE has all non-essential functions removed and is further optimised 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.

The TOE provides two management interfaces:

- System console (via the keyboard/monitor connected to the computer or a dedicated serial interface) which is used only for initial configuration and network diagnostics;

- Web based GUI that is implemented via a Management Configuration Server (MCS), which supports local and remote connections.

2.2 Application Servers

The functionality described in section 2.1 is delivered by a number of application servers implemented in the TOE, which are protected by the S-CORE hardened operating system. These application servers include:

1. 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 and TLS encrypted connections (not included in the scope of the evaluation) on port 25. The server may be disabled by stopping the Mail Service. This is normally done for administrative purposes only.

2. Management/Configuration Server (MCS). The TOE implements a Web based management interface. 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 (not included within the scope of the evaluation). By default the MCS will accept connections only the first network interface to the assigned an IP address (via the system console). It is recommended that this interface is 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.)

3. The Ping Server. The Ping server supports the ICMP Echo request/reply network diagnostic. By default this server is disabled and must be separately enabled for each network interface. When enabled the Ping server will send an ICMP echo reply for each echo request received.

4. The Authentication Server. The Authentication Server validates attempts to authenticate as an administrator in the establishment of a session with the MCS interface.

5. The Web Server. The Web server supports the provision of the MCS interface.

2.3 Application Clients

The TOE includes a number of application clients that provide supporting services for the application servers. These clients include:

1. Syslog Client. The Syslog client forms part of the kernel and supports the generation of records of specified events. These records are stored in one of the 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 another syslog server running a syslog daemon, to provide a secondary storage of records.

2. SMTP Client. 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 e-mail server external to the TOE.

3. DNS Client. 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.

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

2.4 Remote Administration

All administration functions (with the exception of the initial definition of IP addresses and the definition of local time zone) are provided via a remote web based interface. Connection requests to this interface are processed by the Management Configuration Server (MCS). This server accepts HTTP and HTTPS connections. The use of HTTPS is not within the scope of the evaluation. HTTP connections to the MCS are suitable for use from the internal (protected) network only, for this reason the TOE is limited to the use of remote administration from the internal network.

2.5 TOE Branding Module

The TOE includes a Branding Module, which allows BorderWare to brand a functionally identical version of the TOE with the identity of an OEM partner. Details of the Branding Module are provided in Appendix 1.

2.6 TOE Scope

The scope of the evaluation is the TOE software and the underlying hardware on which it runs. The TOE software is MXtreme v3.1 (as branded by BorderWare), which is also the uniquely identified software object "3.1 (BTI_MX31-013004)" that can be branded by an OEM-partner, with the patch "mx31_allowhttp".

Therefore, the same TOE can be provided to the consumer in one of the following two forms:

1. The first is that MXtreme hardware and software shipped as an appliance. The hardware options for this form of the TOE are detailed in Table 2-1. The TOE software is MXtreme v3.1, which also contains the unique identifier "3.1 (BTI_MX31-013004)" together with the patch " `mx31_allowhttp`".

2. The second is an appliance shipped by an OEM partner, integrating the branded "3.1 (BTI_MX31-013004)" software and the patch " `mx31_allowhttp`" with the OEM hardware, an example of which is detailed in Table 2-2.

2.7 TOE Exclusions

The TOE excludes the following features that are either standard components of the BorderWare MXtreme Mail Firewall or are provided as additional cost options.

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

2. E-mail mime content filters and Unsolicited Commercial Email (UCE or Spam) controls, including Realtime Blackhole List, Distributed Checksum Clearinghouse and Statistical Token Analysis.

3. The Brightmail Spam control option.

4. Web mail services (unprivileged BorderPost user account on the MXtreme Mail Firewall required for mail boxes hosted on the Firewall are also excluded, thereby also excluding POP and IMAP connections which are associated with these services).

5. E-mail encryption services (both POP and SMTP).

6. Use of SecurID authentication tokens or authentication methods relying on an external Radius server for authenticating Web Mail and Web Admin logins. Both of these are supported by the MXtreme Mail Firewall but are excluded from the TOE because they rely on external authentication servers.

7. CryptoCard and the Safeword Gold 3000 and Platinum authentication tokens.

8. Encrypted administration sessions (HTTPS, TLS, including SSL Certificate Handling).

9. The use of local mailboxes on the TOE.

10. LDAP Server.

11. Centralised Administration and Tiered Administration, including vacation notification.

12. The use of software update features (Security connection and manually applied patches, except `mx31_allowhttp`, which is detailed in [ECG]), backup and restore and re-install mode.

13. Enabling ICMP server during operational deployment.

2.8 TOE Hardware Options

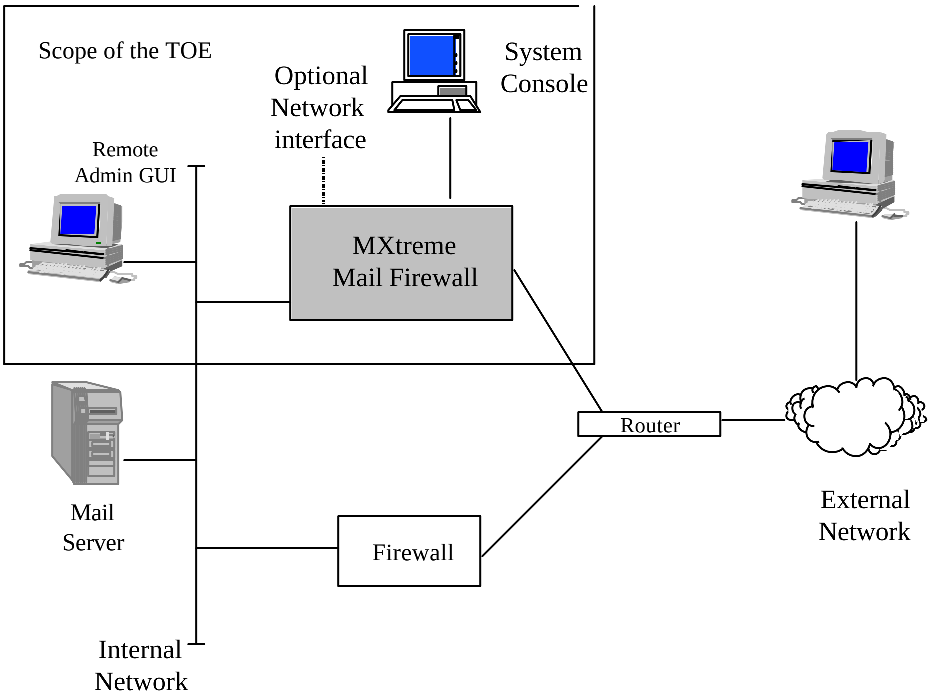

Figure 2-1- Overview of MXtreme Mail Firewall

The MXtreme Mail Firewall is delivered pre-loaded on IA32 hardware. Three models are available (with two variants of two models), all of which are included in the TOE. The specification of the TOE hardware is summarised in Table 2-1.

The TOE can also be integrated to form an OEM branded versions of the Mail Firewall (see section 2.5 and Appendix 1). Branded versions of the TOE run on hardware that meets or exceeds the specifications summarised in Table 2-1. Supported OEM hardware includes the Sun Microsystems SunFire V60 and V65 range of products. The specification of the SunFire V60 and V65 are summarised in Table 2-2.

Model	**CPU**	**Ram**	**NICs**	**Hard Disk(s)**
MX-200 (Serial Number: mmyyssssssnnnn)	P4 1.4 GHz	256 Mbytes Memory	1x Intel Pro/100 Ethernet 1x Intel Pro 10/100B/100+ Ethernet Interfaces: fxp0, fxp1	20 Gbyte Hard Drive
MX-400 (Serial Number: mmyyssssssnnnn)	P4 1.7 GHz	512 Mbytes Memory	1 Intel Pro 10/100B/100+ Ethernet 1 Intel Pro 10/100B/100+ Ethernet 1 Intel PRO/1000 Network Connection, version 1.3.8 Interfaces: fxp0, fxp1, em0	2 x 40 Gbyte Hard Drives, configured as Raid Level 1
MX-400 (new) (Serial Number: NNGyyyywwnnnnn)	P4 1.7 GHz	512 Mbytes Memory	3x Intel Pro/1000 Network Connection Interfaces: fxp0, fxp1, em0	2 x 40 Gbyte Hard Drives, configured as Raid Level 1
MX-800 (Serial Number: mmyyssssssnnnn)	P4 2.0 GHz	1 Gbyte Memory	2 Intel Pro/100B/100+ Ethernet 2 Intel PRO/1000 Network Connection, version 1.3.8 Interfaces: fxp0, fxp1, em0, em1	4 x 40 Gbyte Drives, configured as Raid Level 2
MX 800 (new) (Serial Number: NNGyyyywwnnnnn)	P4 2.0 GHz	1 Gbyte Memory	4 Intel PRO/1000 Network Connection, version 1.3.8 Interfaces: fxp0, fxp1, em0, em1	4 x 40 Gbyte Drives, configured as Raid Level 2

Table 2-1 TOE Hardware Options

For explanation of the serial number formats, see Appendix 2.

Model	CPU	Ram	NICs	Hard Disk(s)
SunFire V60 (Serial Number AZCWnnnnnnn)	P4 2.0 GHz	1 Gbyte Memory	4x Intel Pro/1000 Network Connection Interfaces: em0, em1, em2, em3	36 Gbye Hard Drive
SunFire V65 (Serial Number AZSWnnnnnnn)	P4 2.0 GHz	2 Gbyte Memory	4 Intel PRO/1000 Network Connection, version 1.3.8 Interfaces: em0, em1, em2, em3	36 Gbye Hard Drive and 72 Gbye Hard Drive

Table 2-2 Sample OEM Hardware Specification

2.9 Hardware and Software Requirements for Admin Interfaces

Basic initial configuration of the TOE (assignment of network addresses and system names) is carried out from the system console, using a simple menu-driven Admin GUI. Initial configuration of the TOE requires a monitor and keyboard to allow access to the system console functions. These items are not included in the product package. Once the initial configuration is complete the TOE will operate without the screen and keyboard**.**

The MX-400 and MX-800 applicances include an LCD display. The only function of this LCD is to shut-down the system, permitting shutdown in an orderly fashion when phyiscally located with the Mail firewall without having to connect a screen and keyboard.

All other administration is carried out using a web admin interface. Connections from the web browser to the TOE may be made using HTTP or HTTPS (HTTPS not included in the scope of the evaluation). Standard or non-standard ports may be used. The TOE includes the web server component; any compatible web browser (i.e. Mozilla or Internet Explorer) on any supported operating system may be used to establish the connections. The Web admin interface requires that Javascript is enabled in the Browser (Java and ActiveX should NOT be enabled). No bespoke code is required at the machine accessing the remote administration GUI (MCS). The web browser used by the administrator is simply pointed to the TOE IP address/URL.

3 Security Environment

3.1 Introduction

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;
- organisational security policies the TOE must comply with;
- assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

3.2 Threats

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

3.2.1 Threats countered by the TOE

The IT assets requiring protection are the services provided by, and data accessible via, hosts on the corporate (private) network.

The general threats to be countered are:

- attackers on any network gaining unauthorised access to the corporate mail servers located on other networks where the TOE provides the only link for e-mail protocols;
- mail relay attacks.

The following specific threats are countered:

T.CONN	An unauthorised 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 unauthorised 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 unauthorised 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 unauthorised source, by sending an IP packet with a fake source address.

T.CONFIG An attacker on the corporate/hostile network may exploit an insecure configuration of the TOE (i.e. 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.

T.OPEN_RELAY An unauthorised e-mail source may send multiple messages to the TOE, where those messages are addressed to recipients whose e-mail addresses fall outside the set of address for which the TOE handles e-mail. The intent of this attack is to utilise the resources of the TOE to deliver bulk e-mail on behalf of the originator.

T.SELPRO An unauthorised person may read, modify or destroy security critical TOE configuration data.

T.OLDINF An unauthorised 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 unauthorised 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.

3.2.2 Threats countered by the Operating Environment

The following is a list of threats that must be countered by technical and/or non-technical measures in the IT environment, or must be accepted as potential security risks.

TE.VIOLATE Violation of network security policy as a result of inaction, or action taken, by careless or wilfully negligent system administrators.

TE.USAGE	The mail firewall may be inadvertently or maliciously configured, used and administered in an insecure manner by either authorised or unauthorised persons.

3.3 Organisational Security Policies

There are no organisational security policies or rules with which the TOE must comply.

3.4 Assumptions

The following assumptions describe security aspects of the environment in which the TOE will be used or is intended to be used. This includes information about the intended usage of the TOE and the environment of use of the TOE.

A.PHYSICAL	The Mail Firewall will be physically protected to prevent hostile individuals engaging in theft, implantation of devices, or unauthorised alteration of the physical configuration of the Mail Firewall (e.g. bypassing the Mail Firewall altogether by connecting the corporate and hostile networks together). Note: The threat of theft relates to theft of the Mail Firewall 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 unauthorised monitoring of authentication or configuration information.
A.TRANSFER	All SMTP email traffic between networks connected to the MXtreme Mail Firewall will be transferred through the MXtreme Mail Firewall. (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.USEAGE	The Mail Firewall administrator will adhere to the secure guidance provided for the operation of the Mail Firewall.
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.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

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

> All SMTP mail traffic between networks must be directed through the TOE and must be prevented from passing through any network barrier protection devices, such as firewalls, placed in parallel with the TOE.

The specific IT security objectives are as follows:

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 mail firewall functions, specifically 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.SELPRO The TOE must protect itself against attempts by unauthorised users to bypass, deactivate, or tamper with mail firewall security functions.

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 authorised administrator, and only the authorised administrator, can exercise such control

O.LIMEXT The TOE must provide the means for an authorised administrator to control and limit use of mail firewall security functions by an unauthorised external entity.

O.GW The TOE is designed or configured solely to act as an E-Mail Firewall 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.

4.1.2 Non-IT Security Objectives

There are no non-IT security objectives to be satisfied by the TOE.

4.2 Environment Security Objectives

4.2.1 IT Security Objectives

There are no IT environment security objectives to be provided for the TOE.

4.2.2 Non-IT Security Objectives

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

NOE.DELIV Those responsible for the TOE must ensure that it is delivered, installed, managed and operated in a manner that maintains the security policy.

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

NOE.AUDIT Administrators 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

NOE.MANAGE A TOE administrator is assigned with responsibility for day to day management and configuration of the TOE. Including the management of the audit trail.

NOE.PHYSICAL The TOE must be physically protected so that only administrators have access.

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

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

NOE.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.

NOE.TRUSTED The network from which the TOE will be administered must be trusted.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

The functional security requirements for this Security Target are discussed in detail below. The following table summarises those security requirements.

Functional Components	
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 initialisation
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_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
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.1	Subset residual information protection

Table 5-1 Functional Requirements

Emboldened text within a component identifies a refinement of a component (FDP_IFF.1.2).

5.1.1 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 Mail Firewall (within the evaluated configuration); the authorised administrator who can access and manipulate the configuration parameters. The Mail Firewall 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.

FIA_UID.2 **User identification before any action**

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

FIA_UAU.2 **User authentication before any action**

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

Application Note: The "user" referred to in the SFRs above relates to a MXtreme Mail Firewall administrative user (administrator at the MXtreme Mail Firewall console or using the MCS on a corporate client) only.

FIA_AFL.1 **Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [5] 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 or surpassed, the TSF shall [lock the account for 30 minutes and log the unsuccessful authentication attempt].

5.1.2 Security Management

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

[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).

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Mail Firewall Administrator].

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

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [MXtreme Mail Firewall 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 [Mail Firewall Administrator account];
- [change_default, query, modify] the security attributes [SMTP mail server configuration];
- [query and delete]
- [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, clear] the security attributes [system event log records]

to the [Mail Firewall Administrator].

FMT_MSA.2 Secure security attributes

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).

FMT_MSA.3 Static attribute initialisation

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

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security 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;
- clearing and query of the audit logs[5] stored on the TOE;
- manipulation of the mail queue and quarantine message queue;
- configuration of status and utility functions, DNS functions; including system time and NTP server;
- reboot and shutdown of the Mail Firewall].

[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 bullet items is explained in FMT_MSA.1.

[5] The security relevant events are stored in one of : Mail Transport log, Authentication log, Web

5.1.3 Security Audit

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

FAU_GEN.1 Audit data generation

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

a) start-up and shutdown of the audit functions[6];

b) All auditable events for the [not specified] level of audit; and

c) [Every successful inbound and outbound connection;

Every unsuccessful connection;

Every successful and 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:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [required destination address, and Application layer protocol for network connections].

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [Mail Firewall 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.

FAU_STG.1 Protected audit trail storage

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

Server Access log, Web Server Errors log, Messages log or Kernel log.

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

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

5.1.4 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.

FPT_RVM.1 Non-Bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.5 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 Mail Firewall. The policies selected for the control of user traffic will depend on the number of interfaces configured in the TOE.

Access to the MXtreme Mail Firewall internal data is controlled by the identification and authentication of a Mail Firewall Administrator at the MXtreme Mail Firewall 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.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [MXtreme Mail Firewall Administration Access Control SFP] on

1. [subjects: identified and authenticated Mail Firewall Administrator;
2. objects: TSF data (i.e. system time, event logs), security attributes;
3. operations: change_default, delete, modify, query].

FDP_ACF.1 Security attribute based access control

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

- [the user being an identified and authenticated Mail Firewall Administrator].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. [identified and authenticated Mail Firewall 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 Mail Firewall Administrator].

There are two types of information flow:

a) AUTHENTICATED – remote access to the MXtreme Mail Firewall requiring the source subject to be identified and authenticated as a Mail Firewall Administrator.

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

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.

FDP_IFC.1 Subset information flow control

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

a) [subjects: external IT entities that send and receive information through the Mail Firewall to one another, or external IT/human entities that send and receive information to/from the Mail Firewall;

b) information: traffic sent through the Mail Firewall from one subject to another, or traffic sent to/from the Mail Firewall;

c) operation: permit or deny information through the Mail Firewall or permit or deny information to terminate at the Mail Firewall].

FDP_IFF.1 Simple security attributes

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:

a) [subject security attributes:

presumed address,

b) information security attributes:

presumed address of source subject;

presumed address of destination subject;

transport layer protocol;

Mail Firewall interface on which traffic arrives and departs;

service requested].

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

a) [subjects can cause information to flow through the Mail Firewall 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:

- 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 SFP rules:

a) none].

FDP_IFF.1.4 The TSF shall provide the following [None];

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules [no additional rules to authorise information flow]

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

a) [there is no rule which explicitly allows it;

b) if any of the attributes identified in FDP_IFF.1.1 do not match].

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] the following objects [all objects].

[7] As detailed in FMT_MSA.1

[8] As detailed in FMT_MSA.1

Application Note: For example, if the TOE pads information with bits in order to properly prepare the information before sending it out on an interface, these 'bits' would be considered a 'resource'. The intent of this requirement is that these bits should not include any remains of information that has previously passed through the TOE.

5.2 TOE 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 AVA-VLA.3, both identified in Part 3. The assurance components are summarised in the following table.

Assurance Class	**Assurance Components**	
Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance

Assurance Class	Assurance Components	
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately resistant

Table 5-2 Assurance Requirements: EAL4 Augmented by ALC_FLR.1 and AVA_VLA.3

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

5.3 Security Requirements for the IT Environment

There are no security functional requirements on the IT environment for the TOE, as the underlying hardware is considered to form part of the TOE.

5.4 Strength of Function Claim

A Strength of Function (SoF) claim of SOF-MEDIUM is made for the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the BorderWare MXtreme Mail Firewall in Section 5.1. These are grouped into the following categories:

- Identification and authentication;
- Management;
- Audit;
- Communication Control.

6.1.1 Identification and Authentication

1. A single administrator account is supported by the Mail Firewall.
2. The Mail Firewall Administrator must be identified and authenticated before able to access any data managed by the Mail Firewall or access any Mail Firewall functions. When accessing the Mail Firewall through the system console, the Mail Firewall Administrator is authenticated using a username and password. When accessing the Mail Firewall remotely using the web administration interface (MCS), the Mail Firewall Administrator is authenticated through a username/password mechanism.
3. The administrator account is locked for 30 minutes following 5 unsuccessful authentication attempts via the MCS.

6.1.2 Management

1. The Mail Firewall includes a standard Apache Web server, through which the Mail Firewall Administrator can configure the Mail Firewall. This will provide a restrictive interface, constraining the accepted input.
2. The following attributes of the Mail Firewall Administrator account can be configured by the Mail Firewall Administrator: password, user id and email address to receive any email directed towards the system administrator.
3. The following network settings of the MXtreme Mail Firewall can be configured by the Mail Firewall 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 BorderPost is permitted).
   - The address of NTP server providing source data for clock maintained by the Mail Firewall.

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

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

5. The Mail Firewall 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.

6. The Mail Firewall 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.

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

8. The Mail Firewall Administrator can configure the system time either manually or using an NTP service.

9. The Mail Firewall Administrator can configure the status and utility functions and DNS functions;

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

11. The Mail Firewall Administrator can reboot and shutdown of the Mail Firewall.

6.1.3 Audit

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

   - 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 Mail Firewall 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.

2. 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.

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

   - required destination address and application level protocol.

4. A web browser interface is provided for the Mail Firewall 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.

6.1.4 Communication Control

1. The types of communication with the TOE are described in section 2.1. The methods and controls used for this communication are then described in Sections 2.2 and 2.3 of this document. This information is not reproduced here, and Sections 2.1, 2.2 and 2.3 are considered to form part of the TOE Summary Specification. The rationale for the completeness of the information is provided in Section 8.3.5, along with the rationale for the other aspects of the TOE Summary Specification.

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

6.2 Assurance Measures

Deliverables will be produced to comply with the Common Criteria Assurance Requirements for EAL4, augmented with ALC_FLR.1 and AVA_VLA.3

6.3 Permutational IT Security Functions

Permutation IT security functions are used to implement the following mechanism:

- static password authentication

The administrator connecting via the administration Web GUI uses this mechanism. The Strength of function claim for this mechanism is SOF-MEDIUM.

The encryption (for password storage) mechanisms are implemented in accordance with publicly known algorithms. Therefore, no strength of function claim is made for this mechanism.

7 Protection Profiles Claims

There are no Protection Profile Claims.

8 Rationale

8.1 Introduction

This section identifies the rationale for the adequacy of the security functional requirements and the security assurance requirements in addressing the threats and meeting the objectives of the TOE.

8.2 Security Objectives for the TOE and Environment Rationale

The coverage of the threats and assumptions countered by the TOE is discussed in the subsections below.

T. CONN - An unauthorised 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.

The MXtreme Mail Firewall controls the information flow between the networks. MXtreme Mail Firewall limits the hosts and service ports (O.PORTS), the address ranges (O.ADDRESS) and the recipient address of the mail message (O.MAILCTL). The Mail Firewall will not permit any direct connections through the Mail Firewall, by providing proxy services for all permitted connections (O.MEDIATE).

T.MEDIAT - An unauthorised person may attempt to send impermissible information through the TOE to exploit services on the internal network.

The MXtreme Mail Firewall mediates flow of all information between clients and servers on internal and external networks (O.MEDIATE). The Mail Firewall restricts the information flow between the networks to permissible types of flow only by limiting the hosts and service ports (O.PORTS). The Mail Firewall will not permit any direct connections through the Mail Firewall, by providing proxy services for all permitted connections (O.MEDIATE). Any connection requests to the Mail Firewall must be successfully identified and authenticated before access is permitted (O.DIRECT).

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.

The MXtreme Mail Firewall limits the hosts and service ports (O.PORTS), address ranges (O.ADDRESS) and functions (O.LIMEXT) available from the network interfaces. The Mail Firewall will not permit any direct connections through the Mail Firewall, by providing proxy services for all permitted connections (O.MEDIATE). Any connection requests with the Mail Firewall must be successfully identified and authenticated before access is permitted (O.DIRECT) and will be protected to ensure only the administrator can read or modify transmitted data (O.ADMIN).

T.REPEAT - An unauthorised person may repeatedly attempt to guess authentication data to gain access to the TOE.

The MXtreme Mail Firewall provides controls at point of authentication to prevent the repeated attempts to guess authentication information (O.NOREP).

T.DETECT - An attacker succeeds in compromising network, data and TOE service assets without being detected.

The Mail Firewall provides a facility to monitor successful and unsuccessful connections requests between networks (O.ATTEMPT). The authorised administrator should regularly inspect the logs generated by this facility (O.AUDREC, O.ADMIN) to detect unauthorised activity (NOE.AUDIT).

T.SOURCE - An attacker may attempt to initiate a service from an unauthorised source, by sending an IP packet with a fake source address.

The MXtreme Mail Firewall controls the information flow between the networks. MXtreme Mail Firewall limits the address ranges expected on each network interface (O.ADDRESS) and the services available at each interface (O.PORT).

T.CONFIG - An attacker on the corporate/hostile network may exploit an insecure configuration of the TOE (i.e. not in accordance with the chosen network security policy).

The MXtreme Mail Firewall controls the information flow between the networks. MXtreme Mail Firewall limits the hosts and service ports (O.PORTS) and address ranges (O.ADDRESS). The Mail Firewall will not permit any direct connections through the Mail Firewall, by providing proxy services for all permitted connections (O.MEDIATE). The configuration of the Mail Firewall should be inspected regularly by the administrator to ensure it meets the security objectives for the network (NOE.REVIEW). (O.SELPRO)

T.OS_FAC - An attacker on the corporate/hostile network may attempt to use operating system facilities on the TOE server.

The MXtreme Mail Firewall does not provide any operating system services to any user of the MXtreme Mail Firewall (there is no command line access provided) (O.GW). The Mail Firewall will protect itself against attempts to bypass, deactivate or tamper with security functions (O.SELPRO). The MXtreme Mail Firewall controls the information flow between the networks (O.MEDIATE). MXtreme Mail Firewall limits the hosts and service ports (O.PORTS) and address ranges (O.ADDRESS). The Mail Firewall will not permit any direct connections through the Mail Firewall, by providing proxy services for all permitted connections (O.MEDIATE).

T.OPEN_RELAY - An unauthorised e-mail source may send multiple messages to the TOE, where those messages are addressed to recipients whose e-mail addresses fall outside the set of address for which the TOE handles e-mail. The intent of this attack is to utilise the resources of the TOE to deliver bulk e-mail on behalf of the originator.

The MXtreme Mail Firewall limits the mail messages accepted, to those messages addressed to recipients within the address set of the Mail Firewall (O.MAILCTL).

T.SELPRO - An unauthorised person may read, modify or destroy security critical TOE configuration data.

The MXtreme Mail Firewall enforces controls to ensure only the Mail Firewall administrator can access and amend the configuration (O.DIRECT, O.ADMIN, O.LIMEXT, O.SELPRO). The Mail Firewall does not provide any operating system services to any user of the MXtreme Mail Firewall (there is no command line access provided) (O.GW), preventing alternative routes to attempt to access and modify security critical Mail Firewall configuration data.

MXtreme Mail Firewall will monitor attempts to initiate connections at the network interfaces, including attempts to initiate a remote administration session (O.ATTEMPT, O.AUDREC). The logs of connection attempts should be inspected on a regular basis (NOE.AUDIT) and configuration of the Mail Firewall should be inspected regularly by the administrator to ensure it meets the security objectives for the network (NOE.REVIEW).

T.OLDINF - An unauthorised 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.

The MXtreme Mail Firewall mediates information flow through the firewall (O.ADDRESS, O.PORTS, O. MEDIATE, O.MAILCTL) and ensures no residual information is transmitted (also O.MEDIATE).

T.UNSOLICITED - An unauthorised 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.

The MXtreme Mail Firewall will not accept messages for onward delivery or delivery to Mail Firewall hosted mailboxes if the content of the message falls outside the content configuration controls (O.MAILCTL).

TE.USAGE – The mail firewall may be inadvertently or maliciously configured, used and administered in an insecure manner by either authorised or unauthorised persons.

The MXtreme Mail Firewall will be physically protected to prevent unauthorised persons from altering the physical configuration (NOE.PHYSICAL). The configuration of the MXtreme Mail Firewall will be regularly inspected by the authorised administrator (O.ADMIN) to ensure the configuration upholds the organisation's security policies (NOE.REVIEW).

TE.VIOLATE - Violation of network security policy as a result of inaction, or action taken, by careless or wilfully negligent system administrators.

The administrator of the MXtreme Mail Firewall is trusted to install, manage and operate (including using and managing the audit facilities) the MXtreme Mail Firewall in a manner consistent with the security policy (NOE.DELIV, NOE.MANAGE). The MXtreme Mail Firewall administrator should be provided with the appropriate training in order to complete this (NOE.TRAIN). The logs generated by this facility should be regularly inspected by the authorised administrator (O.ADMIN) to detect unauthorised activity (NOE.AUDIT)

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

Access to the Mail Firewall must be controlled during delivery (NOE.DELIV) and operation (NOE.PHYSICAL).

A.TRANSFER - All SMTP email traffic between networks connected to the MXtreme Mail Firewall will be transferred through the MXtreme Mail Firewall. (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.)

All mail traffic between interconnected networks will pass through the MXtreme Mail Firewall (NOE.TRANSFER).

A.USEAGE - The Mail Firewa ll administrator will adhere to the secure guidance provided for the operation of the Mail Firewall.

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 (NOE.DELIV, NOE.TRAIN, NOE.AUDIT, NOE.MANAGE, NOE.PHYSICAL, NOE.TRANSFER and NOE.REVIEW).

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

The network from which the TOE is administered is to be a trusted network (NOE.TRUSTED).

8.3 Security Requirements Rationale

8.3.1 TOE require ments are appropriate

The following text identifies which SFRs satisfy the Objectives defined in Section 4.1.1.

O.ADDRESS - The TOE must limit the valid range of addresses expected on each of the network interfaces.

The range of addresses expected on the corporate and hostile network are limited by the control of information flow through the MXtreme Mail Firewall. 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 (FDP_IFC.1, FDP_IFF.1). 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 (FPT_RVM.1, FPT_SEP.1).

O.PORTS - The TOE must limit the hosts and service ports that can be accessed from each network interface.

The MXtreme Mail Firewall must limit the corporate hosts and service ports that can be accessed from each network interface. The MXtreme Mail Firewall controls information flow between interfaces by allowing or denying traffic through based on (FDP_IFC.1, FDP_IFF.1):

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service requested.

The MXtreme Mail Firewall will also deny any information flows for which no rule is defined and defaults to deny all information flows through the TOE (FMT_MSA.3).

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 (FPT_RVM.1, FPT_SEP.1).

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.

The MXtreme Mail Firewall controls information flows between interfaces, as described above (O.ADDRESS and O.PORTS). 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 (FMT_MSA.3).

The Mail Firewall will ensure that neither information associated with previous flows through the Mail Firewall nor any internal Mail Firewall data is used as padding for information flow (FDP_RIP.1).

O.DIRECT - The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to mail firewall functions, specifically the MCS.

The MXtreme Mail Firewall 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 Mail Firewall Administrator before access is permitted (FIA_UID.2, FIA_UAU.2,).

O.SELPRO - The TOE must protect itself against attempts by unauthorised users to bypass, deactivate, or tamper with mail firewall security functions.

Processing within the MXtreme Mail Firewall will be protected through the provision of separate domains in which to process security functions (FDP_SEP.1) and control of the invocation of subsequent functions (FDP_RVM.1).

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 MXtreme Mail Firewall must limit the corporate hosts and service ports that can be accessed from each network interface. The MXtreme Mail Firewall controls information flow between interfaces by allowing or denying traffic through based on (FDP_IFC.1, FDP_IFF.1):

- 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.

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).

The MXtreme Mail Firewall 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 Mail Firewall. 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 (FAU_GEN.1,).

The MXtreme Mail Firewall provides the facility for the MXtreme Mail Firewall administrator to view the audit trail (read-only access) (FAU_SAR.1, FAU_STG.1).

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 (FPT_RVM.1, FPT_SEP.1).

O.NOREP - The TOE must prevent repeated attempts to guess authentication data in order to authenticate as an administrator.

Identification and authentication functions will meet the requirements for SOF-Medium (AVA_SOF). Repeated attempts to authenticate are prevented by locking the administrator account for 30 minutes following 5 failed authenticated attempts (FIA_UID.2, FIA.UAU.2, FIA_AFL.1).

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.

The MXtreme Mail Firewall 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 Mail Firewall. Start-up and shutdown of the TOE is recorded in the audit log. The following events can be recorded with their associated data (FAU_GEN.1, FPT_STM.1, FIA_AFL.1, FIA_UID.2, FIA_UAU.2):

- All inbound and outbound connection attempts;
- Every successful and unsuccessful administrator authentication;
- Change of administrator password;

The MXtreme Mail Firewall provides the facility for the MXtreme Mail Firewall administrator to view the audit trail (read-only access) (FAU_SAR.1, FAU_STG.1).

O.ADMIN - The TOE must provide a secure method of administrative control of the TOE, ensuring that the authorised administrator, and only the authorised administrator, can exercise such control.

MXtreme Mail Firewall only maintains one type of direct user (FMT_SMR.1, FMT_MSA.1, FMT_MSA.3):

- Mail Firewall Administrator – able to manipulate the configuration of the Mail Firewall 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 Mail Firewall, preventing direct interaction with the operating system.(FMT_MSA.2).

Identification and authentication of the requesting user provides an access control mechanism to the management functions of the MXtreme Mail Firewall (FIA_UID.2, FIA_UAU.2, FDP_ACC.1, FDP_ACF.1,).

O.LIMEXT - The TOE must provide the means for an authorised administrator to control and limit use of mail firewall security functions by an unauthorised external entity.

MXtreme Mail Firewall provides an interface through which the administrator can administer the TOE (FMT_SMF.1), controlling access an unauthorised user has through the TOE.

O.GW - The TOE is designed or configured solely to act as an E-Mail Firewall 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 MXtreme Mail Firewall is designed to provide no operating system user services by ensuring the information flows do not access the operating system (FDP_IFF.1) and that separate domains are provided in which to process security functions (FDP_SEP.1) and controlling the invocation of subsequent functions (FDP_RVM.1).

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.

8.3.2 Requirements for the IT environment are appropriate

There are no requirements for the IT environment for the TOE.

8.3.3 Security Requirement dependencies are satisfied

Functional Component	Dependencies
FIA_AFL.1	FIA_UAU.1 (satisfied by hierarchical FIA_UAU.2 component)
FIA_UAU.2	FIA_UID.1 (satisfied by hierarchical FIA_UID.2 component)
FIA_UID.2	none
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1, FMT_MSA.1, FMT_SMR.1

Functional Component	Dependencies
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_SMR.1	FIA_UID.1 (satisfied by hierarchical FIA_UID.2 component)
FMT_SMF.1	none
FAU_GEN.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1
FPT_RVM.1	none
FPT_SEP.1	none
FPT_STM.1	none
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.1	none

Table 8-1 Mapping of SFR Dependencies

Those SFRs with a dependency on FIA_UID.1 and FIA_UAU.1 have been met through inclusion of the components FIA_UID.2 that is hierarchical to FIA_UID.1 and FIA_UAU.2 that is hierarchical to FIA_UAU.1, respectively.

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.

8.3.4 Security Requirements are mutually supportive

The only interactions between the security requirements specified for the MXtreme Mail Firewall are those which are identified in the CC Part 2 as dependencies between the SFRs. These dependencies are documented and demonstrated to be satisfied in Section 8.3.3. These interactions are specified in the CC Part 2, with one minor refinement to FDP_IFF.1 to support the interactions between controlled subjects and are therefore mutually supportive

8.3.5 ST complies with the referenced PPs

This Security Target does not claim compliance with a Protection Profile.

8.3.6 IT security functions satisfy SFRs

Mapping of Section 6 IT functions to SFRs (Section 5.1).

Security Functional Requirement	IT Function(s)	Coverage of SFR(s) by IT Function
FIA_UID.2	6.1.1/1, 6.1.1/2	Mail Firewall Administrator must be identified before any access to data or functions on the Mail Firewall is provided. The process of a person identifying and authenticating themselves as a TOE administrator is achieved through the same mechanism. As there is only one Administrator, and therefore successful entry of the administrator account password identifies and authenticates the person accessing the TOE as the TOE administrator.
FIA_UAU.2	6.1.1/2	Mail Firewall Administrator must be authenticated at either the console or the GUI before any access to data or functions on the Mail Firewall is provided. This is performed through entering a password
FIA_AFL.1	6.1.1/3, 6.1.3/1	The administrator account will be locked for 30 minutes following 5 unsuccessful authentication attempts via the remote web administration GUI. Authentication Log records all (successful and) unsuccessful attempts to authenticate as the Mail Firewall administrator.

FMT_MSA.1	• 6.1.2/3, /4, /5 • 6.1.2/2 • 6.1.2/5, /4 • 6.1.2/8, /3 • 6.1.2/9 • 6.1.2/10 • 6.1.2/8, /3 • 6.1.3./4	Mail Firewall Administrator can: • Configure the permissible traffic to and through the Mail Firewall; • Manage the Administrator account; • Configure the Mail Firewall SMTP Mail Server(s). • Configure the NTP server; • Configure the DNS server; • Configure the syslog server; • Configure the system time; • Query the system events logs.
FMT_MSA.2	6.1.2/1	The Mail Firewall will only accept input of particular types and values according to the prompt.
FMT_MSA.3	6.1.2	The Mail Firewall permits the Administrator to specify values for the Mail Firewall configuration parameters. When an object (such as a static route) is created, the default values of that object can be modified by the administrator.
FMT_SMR.1	6.1.1/1, /2 6.1.2/2	The Mail Firewall maintains 1 role Administrator.
FMT_SMF.1	6.1.2, 6.1.3/4	Administration functions are provided to maintain the configuration of the Mail Firewall.
FAU_GEN.1	6.1.3/1, 6.1.3/2, 6.1.3/3	The Mail Firewall records details of all events in the Mail Transport log, the Web Server Access log, Web Server Errors log, Messages log, Kernel log and the Authentication log.
FAU_SAR.1	6.1.3/4	The Mail Firewall administrator can view the Mail transport log, Mail Transport log, Web Server Access log, Web Server Errors log, Messages log, Kernel log and the Authentication log.
FAU_STG.1	6.1.3/4, 6.1.2/1	The administrator is constrained to read only access of the accounting log entries, or delete permission of the log file.

FPT_RVM.1	6.1.1, 2.2, 2.1 All	Functions invoked must succeed before other functions can proceed. • No other administrator functions can be performed before identification and authentication of the user is completed; • The Mail Firewall 'rules' (configuration settings) must be parsed before the connection is permitted.
FPT_SEP.1	6.1.1, 6.1.2, 6.1.3, 2.2, 2.3, 2.1	Different domains of execution are maintained, enforcing separation between human initiated processes and the Mail Firewalls internal process threads. Separation of network traffic is also supported through the provision of separate servers and separate clients to process the various types of traffic received by the TOE.
FPT_STM.1	6.1.2/8, /3	The Mail Firewall administrator can select to configure the Mail Firewall clock manually or using an NTP service.
FDP_ACC.1	6.1.2, 6.1.1	The Mail Firewall restricts/permits access to functions according to the role.
FDP_ACF.1	6.1.2	The Mail Firewall administrator is able to manipulate the Mail Firewall configuration parameters.
FDP_IFC.1	2.1, 2.2, 2.3, 6.1.4/1	The Mail Firewall permits/denies connections according to the identification and authentication associated with the request.

FDP_IFF.1	2.2/1 (2.1/1-5), 2.3/2, 2.3/3, 2.3/4, 6.1.4/1 2.2/2, 6.1.4/1, 6.1.1/2	The Mail Firewall permits connections to servers according to the configured 'rules' (parameters) without identification and authentication of the originator. The Mail Firewall permits remote access to the Mail Firewall according to the 'rules' (parameters) only after successful identification and authentication of the originator.
FDP_RIP.1	6.1.4/2	All padding used in packets will be randomly generated, and will not contain either content of previous transmission or TSF data.

Table 8-2 Mapping of IT Functions to SFRs

SFR FAU_GEN1.1 part b requires no IT Functions.

SFRs FDP_ACF.1.3 FDP_IFF.1.3 , FDP_IFF.1.4 and FDP_IFF.1.5 have not been translated into IT security functions, as they specify that no rules are required in addition to those specified in other elements of the respective components.

Therefore, as demonstrated all Security Functional Requirements of the TOE are fully provided by the IT security functions specified in the TOE Summary Specification.

Also demonstrated in Table 8-2, all IT Security Functions identified for the TOE in the TOE Summary Specification are required to meet the TOE Security Functional Requirements.

8.3.7 IT security functions mutually supportive

The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 8.3.4), as each of the IT functions can be mapped to one or more SFRs, as demonstrated on Table 8-2.

8.3.8 Strength of Function claims are appropriate

The SoF claim made by the TOE is SOF-MEDIUM, which is defined in the CC Part 1 as "resistance to attackers possessing a moderate attack potential".

AVA_VLA.3, , which determines that "the TOE is resistant to penetration attacks performed by attackers possessing a medium attack potential" (CC Part 3). Therefore, a SoF claim of SOF-MEDIUM demonstrates that the functions with an associated SoF would be suitable to resist such attackers.

This product is to be used in environments such as government organisations to protect internal networks when connecting to external networks. The security objectives for the TOE imply probabilistic or permutational security mechanisms. The metrics defined are the minimal "industry" standard accepted for single use authentication mechanisms and are acceptable to protect information to EAL4.

Therefore, the claim of SOF-MEDIUM made by MXtreme Mail Firewall is viewed to be appropriate for this use.

8.3.9 Justification of assurance requirements

EAL4 is defined in the CC as “methodically designed, tested and reviewed”.

Products such as MXtreme Mail Firewall are used in a variety of environments, and used to connect networks with different levels of trust in the users. The Evaluation Assurance Level is viewed as good commercial practice, which is a suitable level for the MXtreme Mail Firewall.

The assurance requirements also permit the identity and integrity of an OEM-distributed TOE to be maintained across different platforms. The delivery assurance requirements (ADO_DEL.2) will address delivery of the appliance to the consumer for the MX-TOE and the delivery of the TOE software to the OEM partners. The installation assurance requirements (ADO_IGS.1) will address the guidance provided to the consumer for the installation and configuration of the TOE and the guidance provided to the OEM partners for the installation and configuration of the TOE software on the OEM hardware platforms.

In the Internet area of IT new exploits are continually being discovered and published, which the MXtreme Mail Firewall will be expected to protect the corporate network against. It is therefore considered to be appropriate to augment the EAL4 assurance requirements for the MXtreme Mail Firewall with the ALC_FLR.1 and AVA_VLA.3 assurance components. 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.

9 Appendix 1: TOE Branding Module

The TOE branding module allows OEMs to brand the MXtreme™ Mail Firewall and market the product under a different name. The TOE includes a build identifier, which is displayed on the Web Admin GUI (see the user documentation for the BorderWare MXtreme Mail Firewall v3.1). This identifier is common to all branded and non branded variants of a product build, and provides assurance that the branding has been applied to an evaluated release. Therefore, the branding process retains the identity of the MXtreme Mail Firewall Software.

The branding module is used only by BorderWare Technologies Inc. The branding module enables a customised product image to be generated. The Branding module reads a configuration file that specifies the location of alternate product name strings and graphics files that are incorporated into the product image. These product name strings and logos are then displayed on the Web Admin GUI.

The OEM partners are provided with guidance from BorderWare to ensure the assurance on the MXtreme software is retained during the branded appliance build process. This guidance also instructs the OEM partners to use hardware commensurate with that integrated in the MXtreme appliances. Particular note should be taken of the following:

Processor	A single processor from the Intel Architecture-32 (IA32), minimum speed 1.4GHz.
Memory	Minimum 256 Mbytes
Network interface cards	The selection of network cards should be made in awareness of the information provided at http://www.kb.cert.org/vuls/id/412115, to ensure the network cards integrated in the appliance do not introduce vulnerabilities. NICs tested: • Intel Pro /100Ethernet; • Intel Pro 10/100B/100+ Ethernet; • Intel Pro/1000 Network Connection, version - 1.3.8.
Hard disk	Minimum 20Gbytes
BIOS	The types of BIOS considered within this evaluation were: • Intel Bios WD84510A.86B.0003.P02 • FastTrak TX100 (used by Promise TX100 Raid Controller) • FastTrak TX2000 BIOS v2.00.0.28 (used by Promise TX2000 RAID controller) • ATI Rage SDRAM Bios (ATI Video controller), P/N GR-

	XLINTS3Y.09a -4.332 • Adaptec SCSI BIOS V41001S2 (used by Disk controller (AIC-7902) • SuperMicro X5DPR-8G2 Bios Rev. 1.5 • Amibios version 8.00, swv25.86b1161.p02

Borderware also provide the OEM partners with details of controls to be used during delivery. A statement of adherence to these controls by the OEM partner in their delivery documents would provide OEM consumers with a level of confidence that the security of the product has been maintained.

10 Appendix 2: Appliance Serial Numbers

This section provides details of the serial number formats used for the MXtreme appliances.

10.1 Format

For the original MXtreme MX-400 and MX-800 appliances, the serial number format has additional digits, but follows the format shown where:

- mm = month
- yy = year
- sssssss = sales order (our purchase order) number
- nnnn = an incremental number assigned to each system built against BTI sales order.

For the updated MXtreme MX-400 and MX-800 appliances, the serial number always starts with NNG, format:

- NNG = Network Engines
- yyyy = year
- ww = week (e.g. week 14)
- nnnnn = an incremental number assigned to each system (regardless of who it is for) that is manufactured in that week.