UK IT SECURITY EVALUATION AND
CERTIFICATION SCHEME

UKAS
PRODUCT
CERTIFICATION

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P204

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

Issue 1.0

July 2004

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham, GL51 0EX
United Kingdom

ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

[*] This statement applies to the Evaluation Assurance Level EAL4 augmented with ALC_FLR.1, this assurance having been confirmed in accordance with the methods quoted in paragraph 26. However, neither the Arrangement nor this statement extend to the AVA_VLA.3 augmentation.

Trademarks:

The following trademarks are acknowledged:

Apache is a trademark of the Apache Software Foundation.

BorderWare, MXtreme and S-CORE are trademarks of BorderWare Technologies Inc.

Intel, Celeron and Pentium are trademarks of Intel Corporation.

Sun Fire is a trademark of Sun Microsystems Inc.

All other product or company names are used for identification purposes only and may be trademarks of their respective owners.

CERTIFICATION STATEMENT

BorderWare Technologies' MXtreme Mail Firewall is a high security e-mail firewall that secures SMTP-based e-mail and protects corporate e-mail systems. The MXtreme Mail Firewall, incorporating the S-CORE hardened operating system, is pre-installed in BorderWare MXtreme Appliance Models MX-200, MX-400 and MX-800, and specified OEM Appliances, and is deployable on a corporate network as part of an organisation's network security defences.

BorderWare MXtreme Appliance Models MX-200, MX-400 and MX-800, and specified OEM Appliances, running MXtreme Mail Firewall Version 3.1 have been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and have met the Common Criteria Part 3 augmented requirements, incorporating Evaluation Assurance Level EAL4, ALC_FLR.1 (basic flaw remediation) and AVA_VLA.3 (moderately resistant vulnerability analysis) for the specified Common Criteria Part 2 conformant functionality in the environment specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body, UK IT Security Evaluation and Certification Scheme
Date authorised	30 July 2004

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

BIOS	Basic Input/Output System
CC	Common Criteria
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
DNS	Domain Name Server
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol, Secure
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MCS	Management/Configuration Server
NIC	Network Interface Card
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
POP	Post Office Protocol
QA	Quality Assurance
RAC	Release Acceptance Criteria
RAID	Redundant Array of Inexpensive Disks
RBL	Realtime Blackhole List
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SoF	Strength of Function
SPL	Seachange Programming Language
SSL	Secure Socket Layer
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UCE	Unsolicited Commercial E-mail
UKSP	United Kingdom Scheme Publication
UPS	Uninterruptible Power Supply
WWW	World Wide Web

(This page is intentionally left blank)

REFERENCES

a. Security Target for BorderWare MXtreme Appliance Models MX-200, MX-400 & MX-800, and specified OEM Appliances, running MXtreme Mail Firewall V3.1,
BorderWare Technologies (UK),
ST, Version 3.0, July 2004.

b. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

e. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

f. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CEM-099/045, Version 1.0, August 1999.

h. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Interpretations Management Board ,
CCIMB-2004-01-004, Version 2.2, Revision 256, January 2004.

i. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2001/0015R, Version 1.1, February 2002.

j. Evaluation Technical Report, Common Criteria EAL4 Evaluation of BorderWare MXtreme Mail Firewall V3.1,
BT Syntegra CLEF,
LFS/T362/ETR, Issue 1.0, 21 May 2004.

k. User Guide, MXtreme Mail Firewall 3.1,
BorderWare Technologies (UK),
15 March 2004.

l. Configuration Management and Delivery Procedures for BorderWare Technologies Inc.,
BorderWare Technologies (UK),
CMP, Version 1.14, May 2004.

m. BorderWare MXtreme Mail Firewall, OEM Branding Guide,
BorderWare Technologies (UK),
September 2003.

n. BorderWare MXtreme Mail Firewall Version 3.1, EAL4 Configuration Guide,
BorderWare Technologies (UK),
Release 14, July 2004.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of BorderWare MXtreme Mail Firewall Version 3.1 to the Sponsor, BorderWare Technologies (UK), and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The versions of the products evaluated were:

- BorderWare MXtreme Appliance Models MX-200, MX-400 and MX-800
- Specified Original Equipment Manufacturer (OEM) Appliances

each running MXtreme Mail Firewall Version 3.1, also uniquely identified as “3.1 (BTI-MX31-013004)” with patch Mx31_allowhttp.

These products are also described in this report as the Target of Evaluation (TOE). The Developer of the MXtreme Appliances and the MXtreme Mail Firewall software was BorderWare Technologies Inc. The Developer of the evaluated OEM Appliances was Sun Microsystems Inc.

4. The BorderWare MXtreme Mail Firewall is an e-mail firewall protecting client and server components used in corporate e-mail systems, screening the content of e-mails and protecting the confidentiality of information sent and received. The TOE is a dedicated device securing e-mail applications and will normally only form part of an organisation’s network security defences.

5. The TOE implements a range of Security Functions and supporting services including:

a. Store and forward mail relay. The TOE is responsible for the delivery of all inbound e-mail from external networks to mail servers located on a corporate network and for the delivery of all outbound e-mail from 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.

b. 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.

c. 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 both. Mail routing operates on sender and recipient addresses after any transformations required by aliasing or mapping rules.

d. Source Address Filtering. The TOE can selectively reject, trust or relay messages received from a pre-defined IP address or from a local subnet. The Trust and Relay functions ensure correct handling of outbound e-mail from a corporate mail server.

e. 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 a 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).

f. Management, monitoring and audit functions.

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

6. The TOE supports between two and four network interfaces, depending on the model deployed. At least one interface must be configured with an appropriate IP address for remote administration, the remainder for receiving and forwarding traffic between networks as appropriate. Each appliance is pre-installed with all required hardware, including the network interfaces.

7. Administration is provided by two management interfaces: the System Console, which is used only for initial configuration and network diagnostics, and the web-based Remote Admin Graphical User Interface (GUI), implemented via the Management/Configuration Server (MCS), which supports local and remote connections.

8. Functionality is implemented in the TOE as a number of application servers, including:

- SMTP server
- MCS
- Ping server
- Web server
- Authentication server

9. The TOE includes application clients providing supporting services for the application servers, including:

- Domain Name Server (DNS) client
- Network Time Protocol (NTP) client

10. 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 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 unsupported or disabled protocols and ports are dropped by the kernel-level packet filtering module. S-CORE only permits administrator logins to the TOE.

11. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

12. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

13. The scope of the evaluation is the TOE software and the underlying appliance hardware on which it runs, as identified in Annex A. The MXtreme Mail Firewall software is pre-installed and pre-configured on Intel IA-32 compatible hardware, except for the evaluated patch. The TOE software includes a Branding Module that allows BorderWare to brand a functionally identical version of the TOE with the identity of BorderWare or an OEM partner, while retaining the identity of the MXtreme Mail Firewall software. Therefore, the same TOE can be provided to the consumer in one of two forms:

a. MXtreme hardware and BorderWare-branded TOE software shipped as an MXtreme Appliance Model. The five MXtreme Appliance Models within the scope of the TOE are detailed in Annex A.

b. OEM hardware and OEM-branded TOE software shipped as an OEM Appliance. The two OEM Appliances within the scope of the TOE are detailed in Annex A.

14. The TOE explicitly excludes the following features or components:

a. Virus scanning option.

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

c. The Brightmail Spam control option.

d. Web mail services (including unprivileged BorderPost user account together with POP and IMAP connections).

e. E-mail encryption services – both POP and SMTP.

f. SecurID authentication tokens or authentication methods relying on an external Radius server for authenticating Web Mail and Web Admin logins.

g. CryptoCard, Safeworld Gold 3000 and Platinum authentication tokens.

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

i. The use of local mailboxes on the TOE.

j. LDAP Server.

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

l. The use of software update features, backup, restore and reinstall mode.

m. Enabling ICMP server during operational use.

15. Various aspects of the hardware development of the MXtreme and OEM Appliances were the responsibility of the hardware subcontractor and OEM partner respectively, rather than BorderWare. Other than BorderWare's procedures for delivery to the hardware subcontractor or OEM partner and BorderWare's First Article Acceptance testing process, aspects, such as delivery of OEM Appliances, were excluded from the evaluation. (See paragraph 55 for details.)

16. The following assumptions regarding security aspects of the IT environment in which the TOE will be used have been made:

a. The firewall will be physically protected to prevent theft, the implantation of devices or the unauthorised alteration of the physical configuration.

b. All SMTP e-mail traffic between networks connected to the TOE will pass through the TOE and not bypass it via some other route e.g. by some other firewall connected in parallel to the TOE.

c. The guidelines [k, n] for ensuring secure operation of the TOE will be followed.

d. The users of the internal network, from which TOE administration is performed, are trusted not to attack the TOE, to intercept network traffic, or to introduce any uncontrolled network connections.

Protection Profile Conformance

17. The Security Target [a] did not claim conformance to any protection profile.

Assurance

18. The Security Target [a] specified the assurance requirements for the evaluation. The assurance incorporated predefined Evaluation Assurance Level EAL4, augmented by ALC_FLR.1 (basic flaw remediation) and AVA_VLA.3 (moderately resistant vulnerability analysis). Common Criteria Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

19. The minimum Strength of Function (SoF) claimed for the TOE was SoF-medium which applied to one mechanism: the password space for administrator-selected passwords. This mechanism provided password-based administrator authentication at the System Console and Remote Admin GUI. The SoF claim did not extend to the algorithm used to protect stored passwords, as the MD5 hash algorithm is publicly known and it is the policy of the national authority for cryptographic mechanisms, CESG, for no claim to be made on the appropriateness or strength of publicly known hashing algorithms. Note that stored passwords are also protected by the S-CORE access control mechanisms.

Security Policy

20. The TOE security policies are evident from the TOE Security Functional Requirements (SFRs) detailed in section 5.1 of the Security Target [a].

21. There are two types of information flow policy:

a. AUTHENTICATED – administrative access to the TOE, via the local System Console and the web-based Remote Admin GUI, requires the source subject to be identified and authenticated as a firewall administrator; and

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

22. There are no Organisational Security Policies with which the TOE must comply.

Security Claims

23. The Security Target [a] fully specifies the TOE's security objectives, the threats which these objectives counter and the SFRs and Security Functions to elaborate the objectives. All of the SFRs, including one refined SFR (FDP_IFF.1.2), are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

24. Security functionality claims were made for the following 4 categories of IT Security Functions:

- Identification and Authentication
- Management
- Audit
- Communication Control

Evaluation Conduct

25. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [e, f]. The Scheme has established a Certification Body which is

managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the CC Mutual Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement, except in respect of AVA_VLA.3. (See paragraph 27 below.)

26. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for the CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [d], the Common Evaluation Methodology (CEM) [g] and the applicable CC Interpretations, including those international interpretations now incorporated in the annotated CEM [h]. In addition, the TOE was evaluated against the CEM Supplement on Flaw Remediation [i], which is also now incorporated in CEM [h].

27. There is no mutually recognised methodology for AVA_VLA.3. The Certification Body agreed that the Evaluators should determine that the Developer's vulnerability analysis was systematic by demonstrating that a predetermined, planned approach was employed in producing the analysis and by demonstrating that the analysis was complete. The methodology agreed for the moderate attack potential used the guidance in CEM [g] Annex B and was based on the methodology for AVA_VLA.2 at EAL4.

28. The Certification Body monitored the evaluation which was carried out by the BT Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [j] to the Certification Body in May 2004. The Certification Body then produced this Certification Report.

General Points

29. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

30. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the products and what assurance exists for such patches.

31. The issue of a Certification Report is not an endorsement of a product.

II. EVALUATION FINDINGS

Introduction

32. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [j] under the CC Part 3 [d] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Delivery

33. The procedures for the secure delivery of the evaluated TOE to consumers, and the initial checks that should be performed on the delivered TOE, are described in the guidance documentation [k, n] detailed in Annex A. (References [k, n] are available from the BorderWare website at http://dgsupport.borderware.com. A hardcopy of the User Guide [k] is delivered with the appliance as described below.) The procedures in [l, m] address the secure delivery of TOE software to the MXtreme hardware manufacturer and OEM partners and the secure delivery of first production Appliance Models to BorderWare. The Evaluators audited a sample delivery and were satisfied that these procedures were adequately documented and applied. Summarised below are the delivery aspects that are relevant to consumers.

34. Following installation of the TOE software by the appliance manufacturer, all appliances detailed in the "Evaluated Configuration" are delivered from the manufacturer using similar delivery procedures, but with minor differences between MXtreme and OEM Appliances as summarised below.

35. During manufacture, each appliance is labelled, with model number, appliance serial number and an appliance logo, and fitted with a tamper-resistant seal. (The appliance logo reflects either the BorderWare MXtreme or the OEM Model as appropriate.) It is then securely stored at the manufacturing site.

36. Following receipt of an order for an MXtreme Appliance, the appliance, together with the User Guide [k] and licence pack, is packed in a box that is then tape sealed and a packing list attached. (The packing list details the contents of the box, including the appliance model and serial numbers.) No separate software media is included within the package as BorderWare will normally provide any subsequent technical support. BorderWare notify the consumer of the approximate delivery date by including this information on the shipping note that is sent in advance. Delivery of the MXtreme package to the consumer is undertaken by a commercial courier (e.g. FedEx or DHL) direct from the hardware manufacturer.

37. The delivery procedure for OEM-branded appliances is identical to that for MXtreme-branded appliances, except in respect of the following. Following receipt of an order for an OEM Appliance, the appliance, together with the media kit (i.e. User Guide [k], self-adhesive Branded logo and a System Recovery CD-ROM) and licence pack, is packed in a box that is then tape sealed and a packing list attached. The System Recovery CD-ROM may be used by the customer to restore the system in the event of a disk failure. (The System Recovery CD-ROM contains the same build image that is used to load the hardware appliance.) OEM partners notify

the consumer of the approximate delivery date by including this information on the shipping note that is sent in advance.

38. On receipt of the MXtreme package, it is recommended that the consumer checks that the security of the TOE has not been compromised in delivery by checking that the package is as described above and that there is no obvious evidence of tampering. The contents of the box should match the system ordered and the contents of the packing list. Suspected tampering should be reported to the supplier prior to any further installation, as detailed in the Configuration Guide [n].

39. The licence pack within the package contains a ReadMe First leaflet, an introductory letter and a licence serial number. The consumer must contact BorderWare and use this serial number to obtain an activation key for the TOE as directed in the User Guide [k]. BorderWare maintains a record of licence serial numbers that is used to check the MXtreme and OEM Appliances delivered to and registered with consumers. This activation procedure ensures that a third-party could not masquerade as the Developer and supply potentially malicious software.

40. Consumers can check that an evaluated version of the TOE software has been supplied by examining the software identification string, which includes the version number of the TOE, that is displayed on the Web GUI Status and Utility menu (on the Remote Admin GUI). All evaluated appliances have the identification string “3.1 (BTI-MX31-013004)”. The only software difference between the MXtreme and OEM-branded appliances is that the background graphics to the user interface (System Console and Remote Admin GUI) will reflect the appliance branding.

41. Consumers can check that an evaluated version of the hardware appliance has been supplied by examining the labels physically attached to the appliance. The appliance has the Model Number and an appliance logo displayed on the front of the appliance and an appliance serial number on the back. The appliance serial number is correlated to the appliance model type as indicated in the Security Target and in the table in Annex A. The serial number is used to distinguish between within-model upgrades that include different versions of hardware (e.g. motherboard or BIOS). Note that whilst the appliance hardware may be checked by physically opening the appliance, this will damage the tamper-resistant seal and may invalidate the warranty and/or support.

42. To recreate the evaluated configuration of the TOE software by disabling SSL, the consumer must request the evaluated patch (“patch_Mx_31_allowhttp”) from BorderWare as described in the Configuration Guide [n]. Consumers should note that delivery of this patch is optionally by CD-ROM or by download (via a machine that is not the TOE) from the BorderWare website detailed above. Both methods of patch delivery use the same digital signature and MD5 checksum mechanisms to protect patch integrity and authenticity. When requested by the consumer, the CD-ROM, with BorderWare logo applied to the CD-ROM within a plain jewel case, is tape sealed in a package and delivered direct from BorderWare to the consumer by a commercial courier (e.g. FedEx or DHL). Using a standard MD5 hash utility, the consumer is recommended to check that the checksum of the patch file mx_31allowhttp.pf delivered via CD-ROM or website download is e6a48e4eb00ccd6104f8a33b56fd1b, as detailed on the BorderWare website and in the Configuration Guide.

Installation and Guidance Documentation

43. The installation procedures are described in [k, n]. The “3.1 (BTI-MX31-013004)” TOE software is pre-installed on the hardware prior to delivery to consumers, except for the evaluated patch (“patch_Mx_31_allowhttp”), which needs to be installed by the consumer as described in the Configuration Guide [n]. The User Guide Appendix B [k] is relevant to consumers who may need to reinstall an OEM Appliance using the System Recovery CD-ROM.

44. The procedures for the secure configuration of the TOE are described in [k] and [n]. Initial configuration of the appliance is performed using the System Console, which includes setting the disk space allocations, initial network addresses and time zone parameters. Thereafter, the appliance is managed remotely via the web-based GUI, except when network troubleshooting. The GUI is also used to complete the initialization phase, which includes accepting the licence agreement. Consumers should note that default passwords, excepting BIOS passwords, should be changed during installation in accordance with the guidance in [k]. BorderWare does not recommend applying BIOS passwords as the TOE is designed to operate continuously as a server and needs to re-start automatically if rebooted remotely from the GUI, or by a UPS following a power failure.

45. The procedures for the secure administration of the TOE are described in [k] and [n]. The procedures include explanations of how the firewall administrator can: configure mail delivery, including network settings, static routes, mail routes, mail delivery settings, mail filtering and mail aliases; archive mail; produce reports; and manage the appliance. The appliance should be configured to match the specific security policy requirements of the organisation. The administrator should follow the guidance documentation in order to ensure that the TOE operates in a secure manner.

46. On delivery the POP and Web mail services are disabled by default and need to remain disabled for consistency with the evaluated configuration. The SMTP, HTTP and HTTPS services are enabled by default but cannot be used until each is assigned to an IP address. The guidance documentation describes how to configure these services, but the HTTPS service should be disabled, as described in [n], to maintain an evaluated configuration.

47. Note that the Configuration Management and Delivery Procedures [l] and Branding Guide [m] are relevant only to the MXtreme hardware manufacturer and OEM partners during the appliance manufacturing stage.

Strength of Function

48. The SoF claim for the TOE is identified above under “Strength of Function Claims”. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that the only probabilistic or permutational mechanisms in the TOE related to the authentication of administrator passwords (i.e. the password space for administrator-selected passwords) and that the SoF claim of SoF-medium was upheld. Consumers should note that guidance on the construction of appropriate passwords to meet the SOF claim is provided in [k].

Vulnerability Analysis

49. The Evaluators' systematic vulnerability analysis of the software, firmware and hardware was based on public domain sources, the Sponsor's vulnerability analysis and the visibility of the TOE given by the evaluation process. The Evaluator's vulnerability analysis identified some potential software vulnerabilities in addition to those described in the Sponsor's analysis. These additional vulnerabilities are described in the ETR [j]. The Evaluators identified no additional potential firmware or hardware vulnerabilities.

50. The Evaluators developed and performed penetration tests, under CESG guidance, based on their vulnerability analysis. The Evaluators did not identify any exploitable or residual vulnerability from their penetration tests and were therefore satisfied that the TOE, in its intended environment, is resistant to an attacker possessing a moderate attack potential, which is consistent with the requirements of AVA_VLA.3.

Assurance Maintenance and Re-evaluation Issues

51. The Evaluators confirmed that the flaw remediation procedures documentation was satisfactory. Any product issue reported by a customer or Developer is first investigated by the BorderWare Technical Support Team. Any residual issue is passed via e-mail to the Escalation Manager, who investigates the problem with the Software Development Manager and Quality Assurance (QA). Where appropriate, residual issues are entered into the automatic bug tracking system, which records flaw related information such as category (e.g. affected product area), affected product versions, severity (e.g. serious or critical), description (including flaw overview and any interim workarounds) and status (Fixed, Closed or Open).

52. BorderWare notifies the customer of the outcome of investigations into the reported issue. Where a patch is required, it is produced and tested by the development team and QA in line with the evaluated development procedures. Any corrective action taken is recorded in the bug tracking system. Any updated software modules are entered back into the Configuration Management System and, following testing, the flaw status is appropriately updated in the bug tracking system. The patch is then distributed to all BorderWare customers with the necessary retrieval and installation instructions (Release Notes) via the BorderWare website (http://www.borderware.com). However, all patches, except that detailed in the "Evaluated Configuration", are currently outside the scope of the evaluation.

53. Consumers should note that assurance in derivatives of the TOE may be maintained under the UK Assurance Maintenance Process. Details of any product releases or patches covered by that process would be provided on the UK Scheme website.

Hardware Issues

54. The TOE hardware is identified in Annex A. All hardware appliances built by the hardware manufacturer or the OEM partners are built to BorderWare-defined hardware specifications and procedures. The TOE software is designed to run on standard Intel IA-32 compatible hardware that meets or exceeds the minimum specification summarised in Annex B, but otherwise does not rely on specific processor speed, RAM size or disk size. The specific hardware dependencies are summarised in Annex B.

55. The TOE software was developed, branded and delivered to the hardware manufacturer (a subcontractor), or the OEM partner as appropriate, using BorderWare procedures. The software includes a standard set of hardware drivers that are identical for each type of appliance model and no other drivers can be loaded. After installation of the TOE software, the first production model of an appliance type is delivered to BorderWare for checking and First Article Acceptance testing against the hardware specification. The Evaluators audited this BorderWare process and were satisfied that it provided an appropriate level of hardware checking and acceptance testing. The Evaluators also took delivery of an MXtreme Appliance for use in various evaluation activities. (The Evaluators performed no examination of the specific MXtreme hardware subcontractor or OEM partner hardware development environment, including configuration management, integration, testing and delivery.)

56. During the evaluation, the BorderWare MXtreme Appliance Models MX-400 and MX-800 were updated to include different motherboard, BIOS and network interface attributes. The appliance serial number is used to identify such hardware variations and a specific appliance hardware configuration may be identified as detailed in the Security Target [a] Appendix 2 and as summarised in Annex A.

57. The security testing of the appliance models is summarised in Annex C. BorderWare extensively tested 3 MXtreme Appliance models, while the Evaluators tested the same 3 MXtreme models, together with the Sun Fire V60 and the updated versions of 2 of the MXtreme Appliance models. For each appliance, the Evaluators confirmed that the TOE software operated securely on the hardware.

58. The Sun Fire V65 differs from the Sun Fire V60 only in terms of the size of the RAM and hard disk - the Sun Fire V65 has larger RAM and hard disk sizes than the latter (see Annex A). There were only 4 SFRs that relied on specific hardware functionality, as summarised in Annex B. As this hardware functionality had been exercised during the Sun Fire V60 tests, there was no requirement to perform any further tests on the Sun Fire V65.

59. The Sponsor provided the Evaluators with a rationale to demonstrate that the UK Scheme hardware interpretations for each of the assurance components had been met for the claimed range of appliances. The hardware rationale included information as detailed under this section and under “Hardware and Firmware Dependencies” in Annex B. The basis of the rationale was that, except for minor graphics branding differences, identical TOE software, including identical hardware drivers, runs on Intel IA-32 compatible hardware. The rationale referenced publicly-available design details of the on-board Intel P4 clock, the Intel 845 chipset memory and the IA-32 processor architecture.

60. The hardware rationale noted that the smallest memory size would be the most susceptible to memory conflicts due to the limited memory space. The Developer and Evaluator tests therefore ensured that the TOE with the smallest memory space adequately addressed this issue. The internal clock relies on a processor speed of at least 66MHz, which is far exceeded in all appliances within the evaluated configuration. However, there were no known issues with the accuracy of clocks due to increased processor speed. (The Intel P4 range of processors are designed to perform operations in a consistent manner and differences in clock speed were not known to introduce any potential security or functional errors.) The Developer and Evaluator

tests addressed the minimum and maximum processor speeds within the evaluated set of appliances and no inconsistencies were detected.

61. Any alternative hardware configurations to those identified in Annex A, or any use of hardware components different to those in the table of Annex A (identified by a different appliance serial number), will require assessment to determine whether further testing or other evaluation activity is warranted. Any such hardware configurations and components will need to meet the minimum hardware requirements specified in Annex B under “Hardware and Firmware Dependencies”. Note that none of the TOE configurations include multi-processor or Celeron configurations.

III. EVALUATION OUTCOME

Certification Result

62. After due consideration of the ETR [j], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that the BorderWare MXtreme Appliance Models MX-200, MX-400 and MX-800, and specified OEM Appliances, running BorderWare MXtreme Mail Firewall Version 3.1 meet the CC Part 3 conformant requirements of Evaluation Assurance Level EAL4, augmented with ALC_FLR.1 and AVA_VLA.3, for the specified CC Part 2 conformant functionality, in the environment specified in Annex A.

63. The Certification Body has also determined that the TOE meets the minimum SoF claim of SoF-medium given above under “Strength of Function Claims”.

Recommendations

64. Prospective consumers of BorderWare MXtreme Appliance Models MX-200, MX-400 and MX-800, and specified OEM Appliances, running MXtreme Mail Firewall Version 3.1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

65. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under “TOE Scope” and “Evaluation Findings”.

66. The TOE should be delivered, installed, configured and used in accordance with the supporting guidance documentation detailed in Annex A.

67. The above “Evaluation Findings” include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE hardware is identified as one of the following appliances:

- BorderWare MXtreme Appliance Model MX-200 (serial number: mmyyssssssnnnn)
- BorderWare MXtreme Appliance Model MX-400 (serial number: mmyysssssnnnn)
- BorderWare MXtreme Appliance Model MX-400 (serial number: NNGyyyywwnnnnn)
- BorderWare MXtreme Appliance Model MX-800 (serial number: mmyysssssnnnn)
- BorderWare MXtreme Appliance Model MX-800 (serial number: NNGyyyywwnnnnn)
- Sun Fire V60 (serial number: AZCWnnnnnnn)
- Sun Fire V65 (serial number: AZSWnnnnnnn)

2. The table overleaf provides details of the hardware configurations of the appliances that are included in the evaluated configuration. The rationale for the inclusion of the Sun Fire V65 Appliance is summarized under “Hardware Issues” above. The MXtreme Appliance serial numbers, which enable different types of appliance hardware to be identified, are explained in the Security Target [a], Appendix 2.

3. Details of the hardware dependencies, including the minimum hardware specification, are provided in Annex B under “Hardware and Firmware Dependencies”.

4. The TOE software is identified as:

- BorderWare MXtreme Mail Firewall Version 3.1, also identified uniquely as "3.1 (BTI-MX31-013004)" with patch Mx_31_allowhttp, which includes BorderWare’s hardened S-CORE operating system

5. Annex C provides details of the appliances used in the Developer and Evaluator tests. It also provides details of the test configuration.

TOE Documentation

6. The supporting TOE guidance documents evaluated were:

- MXtreme Mail Firewall 3.1, User Guide [k]
- Configuration and Delivery Procedures for BorderWare Technologies Inc. [l]
- BorderWare MXtreme Mail Firewall, OEM Branding Guide [m]
- BorderWare MXtreme Mail Firewall Version 3.1, EAL4 Configuration Guide [n]

7. Further discussion of these guidance documents is provided above under “Installation and Guidance Documentation”.

System	Processor	RAM	Bios Version	Motherboard	Network Interface Cards	Hard Disk
MX-200 mmyysssssssnnnn	Intel Pentium P4 (IA-32 architecture) 1.4 GHz	256 Mb	Phoenix AwardBios v6.00PG	TYAN S2425	fxp0: Intel Pro/100 Ethernet fxp1: Intel Pro 10/100B/100+ Ethernet	20 Gb
MX-400 mmyyssssssnnnn	Intel Pentium P4 (IA-32 architecture) 1.7 GHz	512 Mb	Intel Bios WD84510A.86B.0003.P02 FastTrak TX100 (used by Promise TX100 Raid Controller)	Intel Entry Server S845WD1-E	fxp0: Intel Pro 10/100B/100+ Ethernet fxp1: Intel Pro 10/100B/100+ Ethernet em0: Intel PRO/1000 Network Connection, Version - 1.3.8	2 x 40 Gb (RAID 1)
MX-400 NNGyyyywwnnnnn	Intel Pentium P4 (IA-32 architecture) 1.7 GHz	512 Mb	FastTrak TX2000 (used by Promise TX2000 RAID controller) SuperMicro X5DPR-8G2 Bios Rev. 1.5	SuperMicro X5DPR-1G2+	em0: Intel PRO/1000 Network Connection, Version - 1.3.8 em1: Intel PRO/1000 Network Connection, Version - 1.3.8 em2: Intel PRO/1000 Network Connection, Version - 1.3.8	2 x 40 Gb (RAID 1)
MX-800 mmyyssssssnnnn	Intel Pentium P4 (IA-32 architecture) 2.0 GHz	1 Gb	Intel Bios WD84510A.86B.0003.P02 FastTrak TX100 (used by Promise TX100 Raid Controller)	Intel Entry Server S845WD1-E	fxp0: Intel Pro 10/100B/100+ Ethernet fxp1: Intel Pro 10/100B/100+ Ethernet em0: Intel PRO/1000 Network Connection, Version - 1.3.8 em1: Intel PRO/1000 Network Connection, Version - 1.3.8	4 x 40 Gb (RAID 2)
MX-800 NNGyyyywwnnnnn	Intel Pentium P4 (IA-32 architecture) 2.0 GHz	1 Gb	FastTrak TX2000 (used by Promise TX2000 RAID controller) SuperMicro X5DPR-8G2 Bios Rev. 1.5	SuperMicro X5DPR-1G2+	em0: Intel PRO/1000 Network Connection, Version - 1.3.8 em1: Intel PRO/1000 Network Connection, Version - 1.3.8 em2: Intel PRO/1000 Network Connection, Version - 1.3.8 em3: Intel PRO/1000 Network Connection, Version - 1.3.8	4 x 40 Gb (RAID 2)
Sun Fire V60 AZCWnnnnnnn	Intel Pentium P4 (IA-32 architecture) 2.0 GHz	1 Gb	ATI Rage SDRAM Bios (ATI Video controller) Amibios swv25.86b1161.p02 Adaptec SCSI BIOS V4100S2 (used by	Intel Server Board SE7501WV2	em0: Intel PRO/1000 Network Connection, Version - 1.3.8 em1: Intel PRO/1000 Network Connection, Version - 1.3.8 em2: Intel PRO/1000	36 Gb

System	Processor	RAM	Bios Version	Motherboard	Network Interface Cards	Hard Disk
			Disk controller (AIC-7902)		Network Connection, Version - 1.3.8 em3: Intel PRO/1000 Network Connection, Version - 1.3.8	
Sun Fire V65 AZSWnnnnnnn Not tested by Syntegra	Intel Pentium P4 (IA-32 architecture) 2.0 GHz	2 Gb	ATI Rage SDRAM Bios (ATI Video controller) Amibios swv25.86b1161.p02 Adaptec SCSI BIOS V4100S2 (used by Disk controller (AIC-7902)	Intel Server Board SE7501WV2	em0: Intel PRO/1000 Network Connection, Version - 1.3.8 em1: Intel PRO/1000 Network Connection, Version - 1.3.8 em2: Intel PRO/1000 Network Connection, Version - 1.3.8 em3: Intel PRO/1000 Network Connection, Version - 1.3.8	1 x 36 Gb, 1 x 72 Gb

TOE Configurations

8. The evaluated TOE configurations consist of the above hardware appliances running the above TOE software. The TOE software may also run on other branded appliances (i.e. hardware that meets the minimum specifications for the MXtreme Appliances listed above), as detailed in [n]. The Sun Fire V60 and V65 are examples of OEM-branded versions of the TOE. However, only the Sun Fire V60 and V65 are included in the evaluated configuration as detailed above. None of the TOE configurations include multi-processor or Celeron configurations.

9. The TOE has the following configuration options:

- Allocating the disk space allocations, such as log file storage, mail storage, backup area and database area
- Allocating the available Network Interface Cards (NICs) to the internal and external networks

10. A minimum of 2 NICs must be configured and up to 4 NICs can be supported, dependent on the type of appliance.

11. The TOE should be configured in accordance with the supporting guidance documents identified above under "TOE Documentation".

Environmental Configuration

12. The TOE's operational environment includes:

- A local interface to the System Console
- Interfaces to between 2 and 4 networks, depending on appliance model
- A host on an internal network containing a web browser
- A mail server on an internal network
- An optional boundary device (e.g. firewall) in parallel with the TOE for non-SMTP traffic

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

2. The 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 TOE application servers. IP datagrams for any protocol or port not supported and enabled are dropped by the kernel-level packet-filtering module.

3. The TOE performs the following Security Functions:

a. Identification and Authentication, using username and password, via the System Console or Remote Admin GUI.

b. Access Control for management, monitoring and audit functions, after successful identification and authentication.

c. Management of the firewall, via an Apache Web Server, allowing:

- Setting administrator attributes
- Setting firewall network addresses
- Defining static routes
- Defining mail delivery options
- Defining mail routing, aliasing and mapping
- Setting system time
- Defining status, utility and DNS functions
- Configuring the secondary syslog server
- Viewing, deleting and flushing items in the mail queue
- Rebooting or shutting down the Mail Firewall
- Mail access/filtering
- Relocated users
- Attachment control

d. Audit of security-relevant events, including maintenance of the six security logs.

e. Control of information flow i.e. mail delivery, using packet filtering.

f. Separation of security-related processes.

4. The Security Functions are provided by the following components:

a. Software: MXtreme Mail Firewall Version 3.1 (BTI-MX31-013004) with patch Mx31_allowhttp, as detailed in Annex A.

b. Network interface connections.

c. The System Console allows initial configuration and diagnostics.

d. The Remote Admin GUI provides administration other than that provided by the System Console.

e. Application servers:

i. The SMTP server accepts clear text and TLS encrypted connections on port 25, although the latter is out of scope of the evaluation.

ii. The MCS may be configured to accept connections on ports 80 and 443, although only connections on port 80 are within scope.

iii. The ICMP (Ping) server supports the ICMP Echo request/reply network diagnostic via the MCS.

iv. The Apache Web Server allows administration of the firewall via the MCS and allows users to access their mailboxes, although the latter is out of scope.

v. The Authentication server authenticates administrators before they are able to access the MCS and access any other HTML pages provided by the MXtreme firewall.

f. Application clients:

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

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

TSF Interfaces

5. The TOE has the following external TOE Security Functions Interface (TSFI):

- The System Console interface
- The Remote Admin GUI
- 2 to 4 Network Interfaces

Design Subsystems

6. The TOE consists of the following TSP-enforcing or TSP-supporting subsystems:

- Kernel
- Configuration Database (PostgreSQL)
- System Console
- Management/Configuration Server (MCS)
- Web Server (Apache WWW)
- Authentication Server
- Inbound Mail Server
- Outbound Message Processing
- Mail Delivery
- NTP Client
- DNS Client

7. With the exception of the Configuration Database and the DNS Client subsystems, all the TOE subsystems are TSP-enforcing. The Kernel provides the environment in which process and subsystems execute. The process environment provides controlled access to file storage, memory, IP stack and other processes (including ICMP).

8. The Configuration Database provides information storage and retrieval to other subsystems.

9. The System Console provides a user interface for the firewall administrator for initial configuration of the firewall and for diagnostic utilities during its operation.

10. The MCS (a set of SPL scripts) allows an administrator to manage the firewall from a remote PC, using the Web Server interface.

11. The Web Server provides management of the firewall (as described in 3.c), via the MCS.

12. The Authentication Server authenticates administrators before they are able to access any other HTML pages provided by the firewall via the MCS.

13. The Inbound Mail Server processes mail passed to the firewall using the SMTP protocol.

14. The Outbound Message Processing subsystem forwards mail to an external mail server during mail relay.

15. The Mail Delivery subsystem takes the incoming mail traffic from the SMTP server input queue. It then processes the mail according to the Realtime Blackhole List (RBL), routing and alias configurations before placing the mail in the output queue for onward delivery by the SMTP Client. (RBL is outside the scope of the evaluation.)

16. The NTP Client is used by the firewall to synchronize its own internal clock with reference to sources on the Internet.

17. The DNS Client forwards Domain Name address lookup requests to a configured Domain Name Server, and caches the results.

Hardware and Firmware Dependencies

18. The TOE relies on the hardware for the following system functions:

- User and Kernel Mode
- Interrupts and Exceptions
- Processor Execution Levels
- Memory Allocation
- System Clock

19. The TOE is dependent on the hardware for the following CC Security Functional Requirements:

a. FPT_SEP.1 – the separation of memory and processes rely upon the memory controller and system bus.

b. FPT_RVM.1 – the non-bypassability of the TOE is enforced through the control of system interrupts and exception handling, and the implementation of processor execution levels by the processor.

c. FPT_STM.1 – the provision of the reliable timestamp relies on the clock provided by the Intel Pentium 4 motherboard.

d. FPT_RIP.1 – the padding of packets is implemented by software mechanisms (the driver being part of the operating system); the hardware (NIC) is relied upon to transmit the packet passed from the operating system stack. Therefore, although the hardware (NIC) is ultimately relied upon for transmission of the packet, it is not relied upon for the provision of any security functionality, as this is all addressed within software.

20. The TOE does not rely on firmware features for the provision of Security Functions. However, if an alternative BIOS is used within the hardware, it should comply with the requirements for Intel 845 chipset compatibility detailed in:

- http://www.intel.com/design/chipsets/applnots/platintwhite.pdf?iid=ipp_845chpst+info_whtppr&

21. The minimum hardware requirements are detailed in [n] and are summarised as:

- One or more Intel Celeron or Intel P4 processors (Intel 845 chipset or fully compatible alternatives) with minimum speed of 1.4GHz
- A minimum of two network interfaces, using NICs detailed in the table under "Evaluated Configuration"
- A minimum of 256Mb RAM
- At least one hard disk with a minimum of 20Gb space

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The TSF addressed by the product testing is described in Annex B, under "Architectural Features". The TSFI is described in Annex B, under "TSF Interfaces". The design subsystems tested are described in Annex B, under "Design Subsystems".

2. The following appliance types were used for functional testing by the Developers:

- MX-200 (serial number: mmyysssssssnnnn)
- MX-400 (serial number: mmyysssssssnnnn)
- MX-800 (serial number: mmyysssssssnnnn)

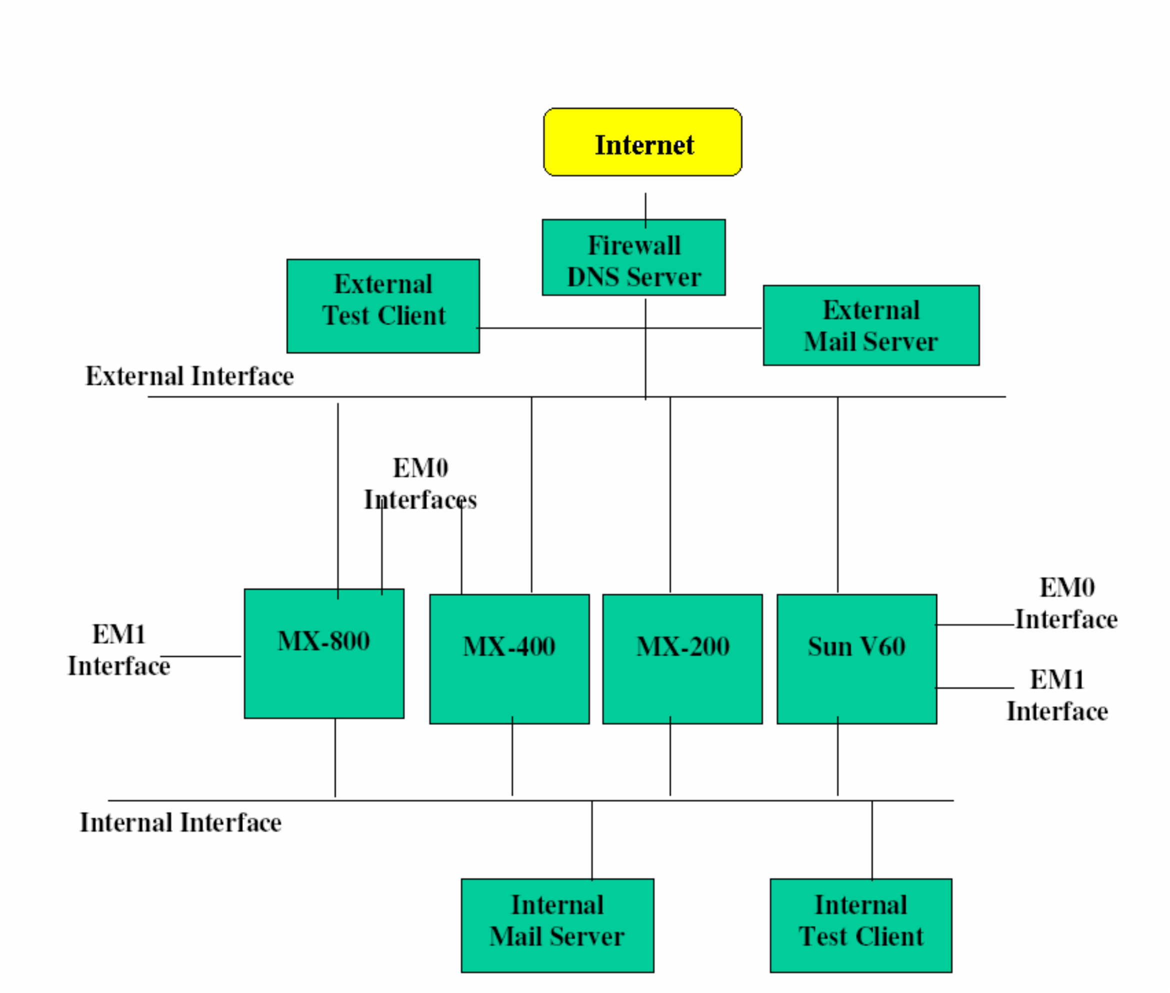
3. The following appliance types were used for functional and vulnerability testing by the Evaluators:

- MX-200 (serial number: mmyysssssssnnnn)
- MX-400 (serial number: mmyyssssssnnnn)
- MX-400 (serial number: NNGyyyywwnnnnn)
- MX-800 (serial number: mmyyssssssnnnn)
- MX-800 (serial number: NNGyyyywwnnnnn)
- Sun-V60 (serial number: AZCWnnnnnnn)

4. For the Evaluator and the Developer tests, the following test equipment was connected to each of the appliances.

- External Test Client via an external interface
- DNS Server via an external interface
- External Mail Server via an external interface
- Internal Mail Server via an internal interface
- Internal Test Client via an internal interface

5. The test configuration used by the Developer and Evaluators is shown in the Test Configuration Schematic overleaf:



Test Configuration Schematic

6. The following tools were used for functional testing:

- Ethereal Version 0.10.0
- Kiwi syslog server Version 7.03

7. The following types of test were carried out by the Developer:

- Verification of correct installation and configuration
- Verification of each Security Function
- Stress testing

8. The Developer's testing was primarily designed to test the TOE Security Functions provided by the high-level design subsystems identified in Annex B. For each design subsystem,

Unit Tests were used as the basis for testing the TOE's IT security objectives, and other objectives such as usability and performance.

9. The testing of the TOE's external interfaces as specified in the TOE's Functional Specification was performed by the Unit Tests that were mapped to the Security Functions in the Functional Specification.

10. The Developer's test procedures included Sanity Tests, Release Acceptance Criteria (RAC) Tests and Unit Tests. Sanity Tests had to be passed before RAC Tests, and then Unit Tests, were performed. A RAC test is defined for each software product release and consists of a pre-defined subset of Unit Tests designed to check that the basic objectives of the build are met. A Unit Test is defined for a particular module of the product, or for a particular set of functions or features and consists of one or more test scripts that exercise all the relevant features of the product.

11. The following types of test were carried out by the Evaluators:

- Confirmation of the TOE configuration.
- Repetition of a 35% sample of Developer's security tests, including representative tests involving different functional areas, different design subsystems and different test engineers, covering all TOE design subsystems and external TSF interfaces.
- Verification of password Strength of Function analysis.
- Tests for known public domain weaknesses associated with this type of TOE, i.e. firewalls, mail gateways and BSD UNIX operating system.
- Tests for potential vulnerabilities determined during the evaluation.
- Additional Security Function tests.
- Confirmation that the guidance documents describe how to mitigate against misuse: insecure installation, configuration or mode of operation.
- Tests of the hardware drivers relevant to the security claims.

Coverage of the various types of hardware platform was as described below.

12. The following tools were used for vulnerability testing:

- Port Flooding Tool Version 1.062 from 7th Sphere
- Bftelnet Version 1.5 – Telnet client
- Kiwi syslog server Version 7.03
- Internet Security Scanner (ISS) Version 7.0
- Nmap Version 3.48
- Ethereal Version 0.10.0
- Hping Version 2.0
- Nessus Version 2.0.10a
- Perl Scripted DNS Server Version 0.1

13. The Evaluators repeated subsets of the 35% sample of Developer tests, as described below:

- All of the sample tests were repeated on the MX-800 (mmyyssssssnnnn)
- Half of the sample tests were repeated on the MX-200 (mmyyssssssnnnn)

- Half of the sample tests repeated on the MX-200 (mmyyssssssnnnn) were repeated on the MX-400 (mmyyssssssnnnn)
- All of the tests repeated on the MX-400 (mmyyssssssnnnn) were repeated on the Sun Fire V60

14. Any Developer test related to a Security Function that was partially provided by hardware or firmware was repeated by the Evaluators on the MX-400 (NNGyyyywwnnnnn). This was to verify that the change in motherboard and BIOS hardware between MXtreme models with serial numbers mmyyssssssnnnn and NNGyyyywwnnnnn had no effect on security functionality. As these hardware variations in the MX-400 Appliance Models were identical to those in the MX-800, there was no requirement to repeat these tests on the MX-800 (NNGyyyywwnnnnn).

15. The Evaluator's additional Security Function tests comprised 10 tests, which were performed as follows:

- All tests were performed on the MX-800 (mmyyssssssnnnn)
- 8 tests were repeated on the MX-200 (mmyyssssssnnnn)
- 9 were repeated on the MX-400 (mmyyssssssnnnn)
- 6 were repeated on the Sun Fire V60

16. Of the 15 penetration tests, all were performed on the MX-800 (mmyyssssssnnnn) and MX-400 (mmyyssssssnnnn), 14 were repeated on the MX-200 (mmyyssssssnnnn) and 10 were repeated on the Sun Fire V60.

17. The Sun Fire V65 was not tested in the evaluation – see "Hardware Issues" above for rationale.

18. The Evaluators checked all of the Developer security test results and found that they were consistent with the expected results. The Evaluators also found that the actual results recorded during all of the Evaluator's functional and penetration tests were consistent with the expected results and no problems were detected. Identical test results were obtained for each test repeated on a different appliance model, which, after previous analysis, satisfactorily demonstrated that the hardware variations did not impact the Security Functions of the TOE.