UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

CERTIFICATION REPORT No. P144

MailGuard Bastion

Release 1.0.0

including Trusted Solaris 2.5.1
running on Sun Ultra SPARC-1/170 Workstation

Issue 1.0

June 2000

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

RECOGNITION AGREEMENT OF
INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Agreement Group and as such:

- indicates that it is the issuer's claim that this certificate is a conformant certificate as defined in this Agreement; and

- therefore gives grounds for confidence, though it cannot in itself guarantee, that the certificate is a conformant certificate and that it will in practice be recognised by the other Members of the Agreement Group.

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.

CERTIFICATION STATEMENT

NET-TEL Computer Systems Limited's MailGuard Bastion Release 1.0.0 is a messaging relay or messaging firewall, and is designed primarily to be used between incompatible or mutually mistrusting networks where free exchange of any form of network traffic (eg e-mail messages) cannot be permitted.

MailGuard Bastion Release 1.0.0 including functionality from the certified Trusted Solaris 2.5.1 operating system has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the requirements of ITSEC Assurance Level E3 when running on a Sun Ultra SPARC-1/170 Workstation as specified in Annex B.

Originator	**CESG** Certifier
Approval	**CESG** Technical Manager of the Certification Body
Authorisation	**CESG** Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	2 June 2000

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CLEF	Commercial Evaluation Facility
DMZ	De-Militarised Zone
ETR	Evaluation Technical Report
IP	Internet Protocol
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
MAC	Mandatory Access Control
MGB	MailGuard Bastion
MTA	Message Transfer Agent
RPC	Remote Procedure Call
SEF	Security Enforcing Function
SMTP	Simple Mail Transfer Protocol
SoM	Strength of Mechanisms
TCP	Transmission Control Protocol
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Trusted Solaris 2.5.1 Certification Report No. P104,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, October 1998.

b. Scheme Information Notice No. 052, F-B1 Functionality Class,
UK IT Security Evaluation and Certification Scheme,
SIN No. 052, Issue 2.0, 28 January 1997.

c. MGB TSOL Configuration Details,
NET-TEL Computer Systems Limited,
DN11027/1, Issue 1.0, May 2000.

d. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 3.0, 2 December 1996.

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

f. MailGuard Bastion 1.0.0 Security Target,
NET-TEL Computer Systems Limited,
DN10460/8, Issue 8.0, July 1999.

g. Harmonised Information Technology Security Evaluation Criteria,
Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

h. Information Technology Security Evaluation Manual,
Commission of the European Communities,
Version 1.0, 10 September 1993.

i. Manual of Computer Security Evaluation, Part I, Evaluation Procedures,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 3.0, October 1994.

j. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 2.0, 30 July 1997.

k. ITSEC Joint Interpretation Library (ITSEC JIL),
Joint Interpretation Working Group,
Version 2.0, November 1998.

l. LFA/T135 Evaluation Technical Report 1.0, Admiral Management Services Limited, 7123A/T15/1, Version 1.0, May 2000.

m. MailGuard Bastion Administrator's Guide, NET-TEL Computer Systems Limited, DN10690/7-UM, Issue 7.0, April 2000.

n. Release Notice, NET-TEL Computer Systems Limited, DN10691/5, Issue 5.0, April 2000.

o. Installation Guide MailGuard Bastion (MGB), NET-TEL Computer Systems Limited, DN10725/5, Issue 5.0, June 2000.

I. INTRODUCTION

Intended Audience

1. This Certification Report states the outcome of the IT security evaluation of MailGuard Bastion (MGB) Release 1.0.0 to the Sponsor, NET-TEL Computer Systems Limited, and is intended to assist potential users when judging the suitability of the product for their particular requirements.

Identification of Target of Evaluation

2. The version of the product evaluated was:

MailGuard Bastion Release 1.0.0.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was NET-TEL Computer Systems Limited.

3. The TOE acts as a messaging relay or messaging firewall, and is designed primarily to be used between incompatible or mutually mistrusting networks where free exchange of any form of network traffic (eg e-mail messages) cannot be permitted.

4. The TOE includes the Trusted Solaris 2.5.1 Compartmented Mode Workstation (see Certification Report No. P104 [Reference a]) certified to ITSEC E3 with the F-B1 functionality class [b] (which includes Mandatory Access Control, MAC). Trusted Solaris 2.5.1 is installed in its evaluated configuration with minor changes subsequently made to the configuration of Trusted Solaris 2.5.1 components, audit parameters and startup scripts to harden the TOE by removing vulnerable applications and services and thus increase the security of the TOE. This was confirmed by the Evaluators during the course of the evaluation. Details of the changes to Trusted Solaris 2.5.1 are detailed in the Trusted Solaris Configuration Details document [c] available from the Sponsor.

5. Trusted Solaris 2.5.1 provides two of the TOE's Security Enforcing Functions (SEFs), viz SEF7 (System Auditing) and SEF8 (Administration Access Control) and supports four other SEFs, viz SEF1-SEF4 (Domain Separation, Network Separation, Assured Message Handling and Assured Message Channels).

6. The TOE has several predefined administrative roles, all of which apart from Tms and Cots are standard roles of Trusted Solaris 2.5.1. They are as follows:

a. **Security Administrator (secadmin)** is used for all security issues including setting passwords for other roles and for the auditing of the file system security.

b. **System Administrator (admin)** is used to perform non-security related system management, such as account creation and management.

c. **Tms** is a TOE specific role which is used for starting and stopping the TOE and has access to all compartments, including those for message archiving.

d. **Cots** is a TOE specific role which is used solely for administering the untrusted subsystems, eg those running the Message Transfer Agents (MTAs).

e. **Root** is used for examining the system log**.**

f. **Oper** is a non-administrative role used for backing up files and mounting removal media.

7. The TOE includes a number of De-Militarised Zones (DMZs) which use the Trusted Solaris 2.5.1 MAC functionality to provide protected compartments in which message archiving and vetting software can be executed. The MailGuard Bastion provides a trusted mover security enforcing component with mandatory access control override privilege which moves messages from one DMZ to the next. Other than Trusted Solaris 2.5.1, the only other security enforcing component of the TOE is the proprietary archiving subsystem which archives copies of all messages received. The TOE supports security irrelevant proprietary vetting software and security irrelevant proprietary MTAs (see Annex B for further details). The product can be configured to use other vetting modules and MTAs, but these need to be configured in such a way as to remain security irrelevant (see the "Rationale for Security Irrelevant Subsystems" section of this report).

8. Additional vetting modules that support the processing of messages before messages can be rejected or accepted and forwarded on to the opposing network (eg label mediators, virus scanners, content filters, etc) must be pre-configured by NET-TEL Computer Systems Limited (or equivalently trained staff) before delivery of the TOE. However, the evaluation testing did not include any additional vetting modules (see Annex B for details of non-evaluated software components).

9. Annex B provides further details of the evaluated configuration of the TOE.

Evaluation

10. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UKSP 01 and UKSP 02 [d, e]. The Scheme has established a Certification Body which is jointly managed by the Communications-Electronics Security Group and the Department of Trade and Industry on behalf of Her Majesty's Government.

11. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [f], which prospective users are advised to read. The criteria against which the TOE was judged are described in the IT Security Evaluation Criteria (ITSEC) [g]. This describes how the degree of assurance is expressed in terms of the levels E0 to E6 where E0 represents no assurance. The methodology used is described in the IT Security Evaluation Manual (ITSEM) [h], UKSP 05 Parts I and III [i, j] and the ITSEC Joint Interpretation Library [k].

12. The Certification Body monitored the evaluation which was carried out by the Admiral Commercial Evaluation Facility (CLEF). The evaluation was completed in May 2000 when the

CLEF submitted an Evaluation Technical Report (ETR) [l] to the Certification Body which, in turn, produced this Certification Report.

13. The Target Assurance Level for the product, as required by the Security Target [f], was E3.

14. The claimed Strength of Mechanisms (SoM) for the TOE was High since all passwords were generated by the certified Trusted Solaris 2.5.1 operating system and there were no other critical mechanisms.

General Points

15. Prospective users of the TOE are reminded that the security functionality evaluated is that claimed in the Security Target [f]. This functionality may not necessarily meet all the threats that a user has identified in a particular operating environment. The assumed threats, intended method of use and environment are as stated in the Security Target. The TOE should only be used in its evaluated configuration (as indicated in Annex B) and in accordance with the recommendations contained in this report. It is the responsibility of purchasers to ensure that MailGuard Bastion Release 1.0.0 meets their requirements.

16. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) 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. Users (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 product and whether such patches have been evaluated and certified. Users are reminded of the security dangers inherent in downloading 'hot-fixes' where these are available, and that the UK Certification Body provides no assurance whatsoever for patches obtained in this manner. More up to date information on known security vulnerabilities within individual certified products can be found on the IT Security Evaluation and Certification Scheme web site www.itsec.gov.uk.

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

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

18. The evaluation of MailGuard Bastion Release 1.0.0 followed the generic Evaluation Work Programme described in the ITSEM [h] with work packages structured around the evaluator actions described in the ITSEC [g]. The results of this work were reported in the ETR [l] under the ITSEC headings. This Certification Report summarises the assurance results in relation to the security functionality claimed in the Security Target [f].

Correctness - Construction

19. This aspect of the evaluation examined both the development process (ie the Security Target, the Architectural and Detailed Designs and the Implementation) and the development environment. The results were as follows:

a. The final version of the Security Target [f] described the SEFs provided by the TOE, and contained a Product Rationale and intended environment; it also described how the product's functionality was appropriate for that method of use and was adequate to counter the assumed threats.

b. The Architectural Design properly described the general structure of the TOE, together with any external interfaces and supporting hardware (see Annex A for representative diagrams); it also clearly detailed how the SEFs of the TOE are provided and how the TOE is separated into security enforcing and other components.

c. The final version of the Detailed Design specified all basic components, identified all security mechanisms, described all SEFs and other security relevant functions, mapped SEFs to mechanisms and components, documented interfaces adequately and enabled the relationships between levels of specification to be identified.

d. The correctness of the implementation was satisfactory, ie all security enforcing and security relevant functions offered in the Detailed Design were identifiable in the source code and test documentation and the associated tests were repeatable.

e. Repeating an agreed sample of 30 per cent of the Developer's functional tests on the hardware platform (see Annex B) used in the certified configuration of Trusted Solaris 2.5.1 (see Certification Report No. P104 [a]) produced no differences in the test results. After confirmation from Sun Microsystems, Inc. and the Logica CLEF, the Certification Body was satisfied that the hardware platform used for Developer's and Evaluators' testing was identical to the platform identified in the certified configuration of Trusted Solaris 2.5.1.

f. The configuration control, programming standards and security aspects of the Developer's working environment were satisfactory. As part of their evaluation of the development environment, the Evaluators confirmed that the Developer securely

transferred backups of the TOE to an off-site location. The Evaluators were satisfied that the transfer and storage of backups were performed in a secure fashion.

20. SEF5 (Acknowledged Message Processing) requires that there is some form of acknowledgement from a process running within the compartment that the message has been detected and processed when a message leaves the compartment. It is the Certification Body's view that the use of the term 'acknowledgement' is not ideal in this instance as the TOE does not provide any acknowledgement to the TOE's administrative roles. The Sponsor has explained that SEF5 is intended to provide assurance that the flow of messages through the compartments requires the active participation of a process within every compartment. This is achieved by ensuring that the inqueues and outqueues are distinct (so that a message must be moved by an independent process). The Evaluators confirmed that the TOE performed acknowledgement in the sense explained by the Sponsor. The Certification Body confirms that SEF5 meets the Scheme requirements in terms of testability and adequate clarity.

21. The Evaluators concluded that the TOE met the requirements for ITSEC E3 in respect of its Security Target, Architectural and Detailed Designs, Implementation and Development Environment.

Correctness - Operation

22. The Evaluators checked and confirmed that:

a. the operational documentation [m-o] adequately described the SEFs relevant to administrators and how to operate the TOE in a secure manner;

b. the delivery and configuration documentation described the delivery arrangements from the development environment to the customer and the required system generation aspects;

c. the startup and operation documentation adequately described the procedures for secure startup and operation and, where relevant, for the deactivation or modification of SEFs; and

d. the information supplied described how these procedures maintain the security of the TOE.

23. The Evaluators found that the TOE installation and configuration procedures [o] were not customer deliverables as the TOE is pre-configured and pre-installed by NET-TEL Computer Systems Limited (or equivalently trained) staff. When the TOE has been delivered, customers need to follow the configuration guidance in the Release Notes [n] and the Administrator's Guide [m] to administer the TOE.

24. The minimum and maximum number of DMZs was not checked during the Evaluators' independent testing, but the Evaluators examined the `label_encodings` file and found that there were 4 vetting compartments in each direction and examined the source code to confirm that the TOE could be configured to have no vetting compartments, 8 vetting compartments and 2 archiving compartments (the maximum number configured) and all values in between. The

number of DMZs tested was 2 archive compartments with vetting from Red (the external network) to Blue (the internal network). The Evaluators checked the configuration of the TOE and the Developer's testing of the maximum number of DMZ. Therefore the certified configuration includes the maximum number of DMZs.

25. Developer's testing demonstrated that SEFs specified in the Security Target [f] continued to hold during startup and shutdown of the TOE.

26. The Evaluators concluded that the Operational Documentation and the Operational Environment met the requirements for ITSEC E3.

Effectiveness - Construction

27. This aspect of the evaluation dealt with:

a. the suitability of the TOE's SEFs to counter the threats identified in the Security Target [f];

b. the ability of the SEFs and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

c. the ability of the TOE's security mechanisms to withstand direct attack;

d. the question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security; and

e. the presence of covert channels in the TOE, ie communication channels that are not designed to be used as such.

28. The Evaluators were satisfied that:

a. the Suitability Analysis confirmed that all the threats listed in the Security Target [f] were adequately countered by one or more of the stated SEFs and mechanisms;

b. the Binding Analysis demonstrated that it was not possible for any SEF or mechanism to conflict with or contradict the intent of any other SEF or mechanism;

c. the procedural measures in the Sponsor's Security Target [f] and the Developer's operational documentation [m-o] were sufficient to prevent all known construction vulnerabilities from being exploited;

d. the Construction Vulnerability Analysis revealed no covert channels that could be exploited;

e. the independent vulnerability analysis and penetration testing did not reveal any exploitable vulnerabilities in the TOE that were not satisfactorily corrected or neutralised; and

f. no exploitable vulnerabilities associated with the use of the TOE beyond 2000 AD were identified.

29. The Security Target of TOE [f] does not claim to counter denial of service attacks or buffer overflows. However, during penetration testing the Evaluators confirmed that any attempt to access the TOE via the network resulted in access to the MTA compartment only (ie sensitivity label [MGB MTA1] or [MGB MTA2]). Since all compartments are disjoint and all processes executing in, or executable from, an MTA compartment were observed to be unprivileged, any attempt to access a process with an administrative sensitivity label would fail and would give no administrative access to the TOE. By exploiting a buffer overflow in an application the attacker could at most gain access to the MTA compartment, which contains no security enforcing or security relevant functionality.

30. The TOE runs with Transmission Control Protocol (TCP) ports open for rpc.bind (Sun Remote Procedure Call (RPC) portmapper), rpc.ttdbserverd (Sun ToolTalk database server daemon) and sadmind (Sun system administration daemon), which are needed because Trusted Solaris 2.5.1 will not function unless these ports are open. This was not considered to introduce any vulnerabilities into the TOE because these processes run unprivileged at the ADMIN_HIGH sensitivity label, which is not accessible from the compartments (which have incompatible sensitivity labels).

31. The Evaluators confirmed that Trusted Solaris 2.5.1 (see Certification Report No. P104 [a]) is preconfigured in the certified configuration with minor configuration changes that harden the TOE by removing vulnerable applications and services and thus increase the security of the TOE (see Annex B), and by adding roles (viz Tms and Cots) to those installed as part of the certified installation process of Trusted Solaris 2.5.1.

32. The Evaluators confirmed that the MTAs required the Trusted Solaris 2.5.1 `net_privaddr` privilege in order to have access to the privileged ports which they require in order to perform their function and that the use of the `net_privaddr` conformed to the principle of least privilege.

33. The Evaluators confirmed the following:

a. Administrator documentation contained details on how to prepare the pre-configured single user account for normal operation, how to add more user accounts (and to re-assign roles) if other administrative users are to have access to the TOE, and how to change passwords for administrative role accounts.

b. The Trusted Solaris 2.5.1 configuration in use applied the principle of least privilege to components, audit parameters and changes to startup scripts and other minor changes to the configuration of Trusted Solaris 2.5.1.

34. The TOE is configured so that all passwords are generated by Trusted Solaris 2.5.1 operating system (see Certification Report No. P104 [a]) and the SoM is therefore High as claimed.

35. The Evaluators concluded that the TOE met the requirements for ITSEC E3 in respect of Suitability, Binding, SoM and Construction Vulnerability.

Effectiveness - Operation

36. This work involved:

a. checking that the TOE can be used in a secure manner and assessing whether known vulnerabilities in its operation could, in practice, compromise its security; and

b. checking the List of Known Vulnerabilities in the operation of the TOE, as supplied by the Sponsor, and assessing the impact of these vulnerabilities and the measures proposed to counter their effects.

37. The evaluation confirmed that:

a. the TOE could not be configured or used in a manner which was insecure but which an administrator would reasonably believe to be secure;

b. the countermeasures proposed by the Sponsor in the List of Known Vulnerabilities in Operational Use were entirely satisfactory; and

c. a number of exploitable vulnerabilities, revealed by comprehensive penetration testing, were successfully overcome by procedural measures documented in the Security Target [f] and the operational documentation [m-o].

38. The Evaluators concluded that the TOE met the requirements for ITSEC E3 in respect of Ease of Use and Operational Vulnerability.

Specific Functionality

39. The Evaluators concluded that all of the claimed functionality in the Security Target [f] had been met. This included security enforcing functionality claims for:

- Domain Separation
- Network Separation
- Assured Message Handling
- Assured Message Channels
- Acknowledged Message Processing
- Message Archives
- System Auditing
- Administration Access Control

Rationale for Security Irrelevant Subsystems

40. The Evaluators confirmed that vetting and MTA subsystems were identified as security irrelevant since they did not implement any SEFs and did not support any components that implements a SEF.

41. The following rationale explains how alternative vetting and MTA software can be installed and run on the TOE without affecting any SEFs and thus maintain their security

irrelevant status. It is provided as information to potential purchasers who wish to ensure that the certification of the TOE is not invalidated by the use of alternative software.

42. Key requirements that must be met by the vetting and MTA subsystems to maintain their security irrelevant status are as follows:

a. The vetting and MTA subsystems must be packaged such that all the software can be installed and configured pre-delivery, by NET-TEL Computer Systems Limited staff or equivalently trained staff using standard installation procedures as documented in the TOE Installation and Configuration procedures [o].

b. It must be possible to install and run the vetting and MTA subsystems without alteration to the evaluated subsystems of the TOE.

c. The vetting subsystem must run completely unprivileged as a non-root application.

d. The MTA subsystem must run as a non-root application with no Trusted Solaris 2.5.1 privileges other than that of `net_privaddr` to allow access to one of the reserved network ports.

e. The vetting subsystem must not require the use of any network connection.

f. The procedures covered in the vetting and MTA specific application notes (where provided) do not compromise or contradict any of the procedures defined in the TOE Administration Guide [m] covering the administration of the security-enforcing components of TOE.

g. The procedures covered in the vetting and MTA specific application notes (where provided) do not compromise or contradict any of the TOE environmental assumptions listed in the Security Target [f].

Unresolved Issues

43. Although the Developer's test specification contained test steps, in a number of the tests the description of the test steps did not uniquely specify or reference how each test step was to be performed. This was raised by the Evaluators as an unresolved problem report. Although the Evaluators were able to repeat a sample of the Developer's tests and the assurance in the TOE was not therefore affected, it is recommended for any future re-evaluation that test scripts are prepared for each test which explicitly identify the sequence of commands that are needed to perform the test.

III. CONCLUSIONS

Certification Result

44. After due consideration of the ETR [l], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that MailGuard Bastion Release 1.0.0 running on certified Trusted Solaris 2.5.1 (see Certification Report No. P104 [a]) meets the requirements of ITSEC Assurance Level E3 and a minimum SoM of High.

Recommendations

45. The product should only be used in accordance with the intended environment and method of use assumptions described in the Security Target [f]. Particular care should be taken that the product is configured and used in accordance with the operational documentation [m-n].

46. It is recommended that the TOE is installed with an uninterruptible power supply to help prevent data loss or data corruption in the event of a power failure.

47. The TOE Administrator's Guide [m] advises that audit logs, including the archive log, are checked every day to ensure they are not full and that they are backed up or deleted if they are becoming large. If the audit log space should fill completely, the TOE will cease forwarding messages until the audit logs are either removed or reduced to a manageable size.

48. Potential purchasers of the TOE should be aware that the effective administration of the TOE requires experience of Trusted Solaris 2.5.1. However, the Evaluators found the TOE Administrator's Guide [m] to be clear and easy to follow.

49. Potential purchasers of the TOE should be aware that hosts on the networks mediated by the TOE must be identified in the `/etc/hosts` and the `/etc/security/tsol/tnrhdb` files. Hosts with unknown IP addresses cannot transfer data via the TOE. Potential purchasers of the TOE should also be aware that the TOE will only accept one host IP address on either network interface; it does not perform a routing function.

50. To help counter additional threats, such as denial of service attacks, it is recommended that network level packet filters or screening routers are placed between the TOE and a hostile network to block access to the open ports described in paragraph 30.

51. The Certification Body recommends that the wording of SEF5 is amended for any future re-evaluation to indicate that no explicit message acknowledgement is provided by the TOE. The Certification Body also recommends that any vetting software provides logging functionality to identify rejected data.

52. The Certification Body recommends that any security patches to Trusted Solaris 2.5.1 evaluated under the Certificate Maintenance Scheme are applied to future versions of the TOE if they are relevant to the TOE's security functionality or counter vulnerabilities relevant to the TOE's configuration.

53. The Certification Body recommends that the issue identified in the "Unresolved Issues" section above is resolved in accordance with the recommendation specified in that section.

54. Potential purchasers of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [f]. Only the relevant evaluated product network configuration, as identified in Annex B, should be installed as described in Annex A.

ANNEX A: SUMMARY OF THE SECURITY TARGET

Introduction

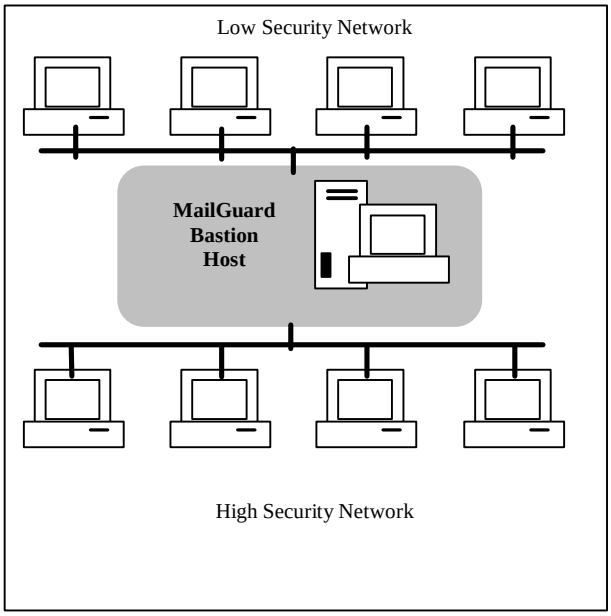
1. The Security Target is given in [f].

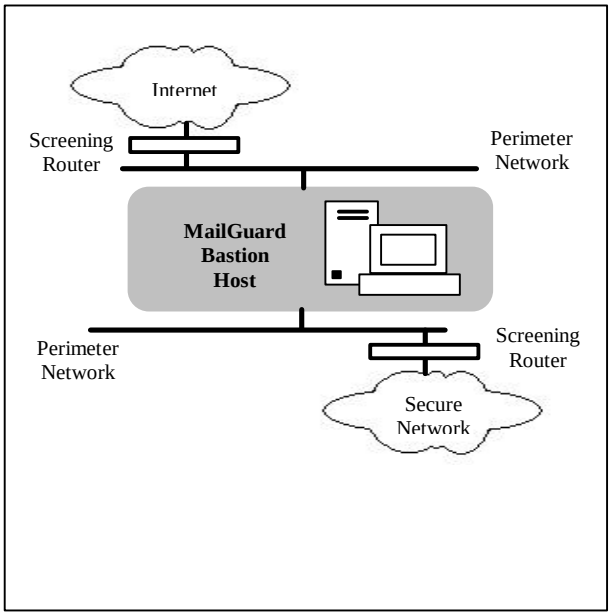
Product Rationale

Intended Method of Use

2. The TOE is intended for use as an electronic messaging relay, or messaging firewall, between two distinct networks where one or both networks require complete accountability of all traffic passing through the relay.

3. Where beneficial, network level packet filters or screening routers should be used between the two networks being connected to filter out superfluous network traffic and to add an extra layer of protection between the. See diagrams below.





4. The TOE is particularly intended for use between incompatible or mutually mistrusting networks where free exchange of e-mail cannot be permitted and extra controls on message flow need to be enforced at the interface between the two networks. To this end, the product offers a protected environment, referred to as the DMZ compartment, into which additional processing modules can be plugged to implement the necessary controls on the messages flowing in each direction.

5. The product guarantees that each processing module embedded within the DMZ has the opportunity to inspect, process and accept or reject each message before the message is forwarded on to the opposing network. Typical processing modules that could be supported in this manner include virus-scanners, content-filters, sensitivity-label checkers and digital-signature checkers. These need not be trusted or evaluated but must meet the requirements of the

rationales supporting security irrelevant functionality (see "Rationale for Security Irrelevant Subsystems" in the main body of this report.

Assumed Threats

6. The assumed threats are summarised as follows:

   a. A network-based attacker attempts to establish an independent network connection across the TOE that bypasses the TOE software.

   b. A network-based attacker overruns one or both of the MTAs and then attempts to use the established MTA network connection(s) to bypass the remaining TOE software.

   c. A locally- or network-based attacker attempts to modify or overrun the TOE mechanisms that ensures all e-mail passes through each of the DMZ compartments defined by the TOE configuration, and thus enables e-mail to bypass one or more of the DMZ processing modules.

   d. Locally- or network-based attack attempts remain undetected allowing an attacker to eventually defeat the TOE security objectives.

   e. An attack by a locally-based unauthorised user to the system, or abuse of trusted privilege by an authorised user.

   f. A deliberate or accidental attempt by a network user to send an e-mail message in the wrong direction across the TOE.

   g. An IP 'spoofing' attack from an external network using a source IP address of a host based on the internal network to try and connect to the internal MTA.

Summary of Security Features

7. The primary security features of the TOE are as follows:

   a. An electronic mail (X.400 or Simple Mail Transfer Protocol, SMTP) messaging gateway between two networks connected to, and separated by, the TOE.

   b. Archiving of all messages passing through the TOE (optional).

   c. A plug-in software interface that allows additional processing checks to be applied to each message as it passes through the TOE. This mechanism can be used to apply import/export sanctions, or to enforce additional elements of network security policy such as (but not limited to) virus scanning, content filtering, filtering based on sensitivity labels or digital signature verification.

   d. Separate channels for managing the message flow in each direction (allowing differing import or export sanctions and/or network security policy to be applied in each direction).

e. Administrator identification and authentication, along with system auditing, provided by Trusted Solaris 2.5.1 (See Certification Report No. P104 [a]).

Target Assurance Level

8. The Target Assurance Level for the product, as defined in the Security Target [f], was E3 as defined in ITSEC [g].

Claimed Minimum Strength of Mechanisms

9. The TOE is configured such that all passwords are generated by the Trusted Solaris 2.5.1 operating system. The minimum SoM claimed for the password encryption and authentication algorithms was High.

(This page is intentionally left blank)

ANNEX B: EVALUATED CONFIGURATION

Hardware

1. The evaluation results apply to the certified platform of Trusted Solaris 2.5.1, viz a Sun Ultra SPARC-1/170 Workstation running at 167MHz with 64MB memory, 1GB hard disk and UltraWide SCSI CD-ROM. The platform was fitted with 2 network cards to enable 2 MTAs running on the same machine to communicate with 2 distinct networks.

Firmware

2. The TOE has no firmware components other than those evaluated as part of the Trusted Solaris 2.5.1 evaluation (see Certification Report No. P104 [a]).

Software

3. The TOE consists of MailGuard Bastion Release 1.0.0 from the Master CD Number 16 and includes Trusted Solaris Version 2.5.1 (CD part no. 704-8118-10 Revision 50).

4. No Sun Solaris or Trusted Solaris patches were installed on the TOE's implementation of certified Trusted Solaris 2.5.1. Reasons for this were as follows:

   a. they were not applicable to the certified version of Trusted Solaris 2.5.1; or

   b. they related to threats not covered by the TOE security objectives; or

   c. they were unnecessary due to modifications made to the configuration of Trusted Solaris 2.5.1 during system hardening.

5. The source code version numbers of the security enforcing components other than Trusted Solaris 2.5.1 are as follows:

   a. archrun.sh –Revision 1.7
   b. build – Revision 1.3
   c. confgen – Revision 1.11
   d. makefile.unx – Revision 1.3
   e. mgb.h – Revision 1.4
   f. mgbarchive.sh – Revision 1.9
   g. mgbarchtidy.sh – Revision 1.10
   h. mgblaunch.c – Revision 1.13
   i. mgbtm.c – Revision 1.8
   j. misc.c – Revision 1.8
   k. S91mgb – Revision 1.7

l. tmsrun.c – Revision 1.12

6. The revision numbers of the remaining security relevant and security irrelevant source code are documented in the build tree referenced by the Concurrent Versions System tag mgb1_00a9.

7. The X.400 MTA used during the Evaluators' testing was the proprietary mgbmtax package based on Route400 MHS Release 3.6.1 for Solaris SPARC.

8. The TOE was tested by the Developer in the following configurations:

a. SMTP MTA with the archiving subsystem and SMTP vetting with 1 to 4 vetting compartments active;

b. SMTP MTA with the archiving subsystem;

c. SMTP MTA with the SMTP vetting subsystem;

d. SMTP MTA;

e. X.400 MTA with the archiving subsystem and X.400 vetting with 1 to 4 vetting compartments active;

f. X.400 MTA with the archiving subsystem;

g. X.400 MTA with the X.400 vetting subsystem; and

h. X.400 MTA.

9. The SMTP MTA used during Developer's testing was the proprietary mgbmtas package based on Sendmail Version 8.9.1. The X.400 MTA used during the Developer's testing was the proprietary mgbmtax package based on Route400 MHS Release 3.6.1 for Solaris SPARC. The SMTP vetting subsystem used during Developer's testing was the proprietary mgbvets package based on NET-TEL's VETSMTP utility Version 0.00.01. The X.400 vetting subsystem used during Developer's testing was the proprietary mgbvetx package based on NET-TEL's VETASN utility Version 0.00.03.

10. Subject to the conditions in the Developer's rationale (summarised in the main body of this report), the MTA and vetting software is security irrelevant.

11. The modifications made to Trusted Solaris 2.5.1 to harden the TOE are detailed in the TSOL Configuration Details document [c] available from the Sponsor.

Non-evaluated Components

Hardware

12. An optional tape drive, used for backup purposes only, may be purchased with the TOE from NET-TEL Computer Systems Limited.

Software

13. All additional vetting modules (eg label mediators, virus scanners, content filters, etc) were outside the scope of the evaluation.

14. All Sun patches to Trusted Solaris 2.5.1 were outside the scope of the evaluation.

15. The security irrelevant vetting software and the MTAs were not tested by the Evaluators, although a vetting script was used to forward messages from the inqueue to the outqueue.

(This page is intentionally left blank)