UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P150

CyberGuard Firewall for UnixWare / Premium Appliance Firewall

Release 4.3

running on SCO UnixWare 2.1.3

Issue 2.0

February 2003

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

**ARRANGEMENT ON THE
MUTUAL 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. *

* Whilst the Arrangement has not yet been extended to address ALC_FLR.1 (basic flaw remediation), a working agreement exists amongst Parties to the Arrangement to recognise the Common Evaluation Methodology ALC_FLR supplement (Reference [w] in this report) and the resultant inclusion of ALC_FLR.1 elements in certificates issued by a Qualified Certification Body.

Trademarks:

The following trademarks are acknowledged:

CyberGuard is a registered trademark of CyberGuard Corporation.
Intel and Pentium are registered trademarks of Intel Corporation.
PowerEdge is a trademark of Dell Computer Corporation.
UNIX is a registered trademark of The Open Group.
UnixWare is a registered trademark of SCO Corporation.

All other products or services mentioned herein are trademarks of their respective owners.

The following Copyright is acknowledged:

CERTIFICATION STATEMENT

CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 4.3 is a dynamic (stateful inspection) packet filter and application level proxy firewall that runs on a Multi-Level Secure Unix operating system. It enables organisations to safeguard information held on their internal network by using IP packet filtering and application-level proxies to control the access that external network users have to the internal network. The CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 4.3 can also control the access that internal network users have to the external network. The product was evaluated in a multi-homed configuration, mediating between up to 32 networks and having a network address on each. The product was evaluated as a standard CyberGuard Firewall for UnixWare installation and as a Premium Appliance Firewall installation. The scope of the certificate therefore extends to KnightSTAR (ie KS) Release 4.3, a member of the Premium Appliance Firewall family, and to both FireSTAR (ie FS) Release 4.3 and STARLord (ie SL) Release 4.3, which are derivatives of KnightSTAR.

CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 4.3 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL4, augmented with ALC_FLR.1, for the specified Common Criteria Part 2 conformant functionality in the specified environment when running on SCO UnixWare 2.1.3 and the Intel Pentium hardware platforms as specified in Annex A.

Certification to the EAL4 Evaluation Assurance Level was previously completed in December 2000. This certification has now been updated to include the ALC_FLR.1 (basic flaw remediation) augmentation. Details of the certification update are given by Annex C (other points within the report are those made at the time of the original EAL4 certification).

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorised	25 February 2003

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

AMA	Maintenance of Assurance Class
ASP	Application Service Provider
CC	Common Criteria
CD-ROM	Compact Disk - Read Only Memory
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
CLI	Command Line Interface
CMS	Certificate Maintenance Scheme
DAC	Discretionary Access Control
DAT	Digital Audio Tape
DNS	Domain Name Server
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IDE	Integrated Device Electronics
IP	Internet Protocol
ISP	Internet Service Provider
ISS	Internet Security Scanner
ITSEC	Information Technology Security Evaluation Criteria
MD5	Message Digest 5
NNTP	Network News Transfer Protocol
PCI	Protocol Control Information
PSU	Product Software Update
RAM	Random Access Memory
SCSI	Small Computer Standard Interface
SFR	Security Functional Requirement
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
SoF	Strength of Function
SPM	Security Policy Model
TCP	Transfer Control Protocol
TELNET	TELecommunications NETworking Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Common Criteria Security Target,
Logica UK Ltd,
CLEF.EC25402.40.1, Issue 2.0, 24 August 2000.

b. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.

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

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

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

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

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

h. Endorsed Interpretation UK/2.1/003,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, January 2000.

i. LFL/T133 Evaluation Technical Report 1,
Logica CLEF,
CLEF.25402.30.1, Issue 1.0, 5 September 2000.

j. LFL/T133 Evaluation Technical Report 2,
Logica CLEF,
CLEF.25402.30.2, Issue 1.0, 7 November 2000.

k. Evaluation Technical Report 2 Comments,
Logica CLEF, Logica UK Limited,
CLEF.25402.34.03, 5 December 2000.

l. Security Hardening in the CyberGuard Firewall for UnixWare,
CyberGuard Corporation,
EV030-001, Issue 1.0, 10 December 1998.

m. CyberGuard Firewall Platform Compliance and Certification,
CyberGuard Corporation,
Version 2.0, April 1998.

n. Certification Report No. P117, CyberGuard Firewall for UnixWare, Release 4.1, running on UnixWare 2.1.3,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, March 1999.

o. CyberGuard Firewall for UnixWare Security Target (E3),
CyberGuard Corporation,
EV002-008, Issue 1.8, 10 December 1998.

p. Delivery and Configuration,
CyberGuard Corporation,
EV024-001, 26 June 2000.

q. CyberGuard 4.3 Installation Guide,
CyberGuard Corporation,
IN001-040, June 2000.

r. CyberGuard Firewall Release Notes,
CyberGuard Corporation,
RN001-4-3, June 2000.

s. CyberGuard Firewall Manual (Volumes I, II, III),
CyberGuard Corporation,
FW001-050, June 2000.

t. Impact of Additional Interfaces on TOE Security Functions,
CyberGuard Corporation,
15 December 2000.

u. Common Criteria Certification Report No. P150, CyberGuard Firewall for UnixWare / Premium Appliance Firewall, Release 4.3, running on SCO UnixWare 2.1.3,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, December 2000.

v. Common Criteria Security Target,
Logica UK Ltd,
CLEF.EC25402.40.1, Issue 3.0, 5 February 2003.

w. 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.

x. Task LFL/T145 Certificate Maintenance Scheme Audit Report,
Logica CLEF,
CLEF.26874.CMS/7.2/3, Issue 1.0, 22 January 2002.

y. AMS for Task LFL/T145,
Logica CLEF,
CLEF.26874/5.1/3, 18 March 2002.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) evaluation of CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 4.3 to the Sponsor, CyberGuard Corporation, 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 version of the product evaluated was:

- CyberGuard Firewall for UnixWare Release 4.3

The product is also described in this report as the Target of Evaluation (TOE) and is known in its pre-configured, pre-packaged derivatives as the Premium Appliance Firewall Release 4.3. The Developer was CyberGuard Corporation.

4. The TOE is a dynamic (stateful inspection) packet filter and application level proxy firewall that runs on a Multi-Level Secure UNIX operating system. It enables organisations to safeguard information held on their internal network by controlling the access that external network users have to that network. The TOE is intended to protect the integrity, availability, authentication data and anonymity of the internal network. The TOE can also control the access that internal network users have to the external network.

5. The product supports a number of connection topologies. The evaluation addressed the product when configured in a multi-homed configuration providing both IP packet filtering and application-level proxies. No distinction is made between external and internal networks, although the evaluated configuration included at least one external network. Additional network interfaces (up to the maximum of 32) provide DeMilitarised Zones or further internal / external network connections.

6. The TOE comprised the CyberGuard Firewall for UnixWare Release 4.3 software and the UnixWare kernel as modified by the installation of the CyberGuard Firewall for UnixWare Release 4.3 software and excluded any unchanged operating system functionality.

7. The underlying Multi-Level Secure UNIX-based operating system has secure configuration options enforced during TOE installation (as described in the security hardening document [l]) which provide mandatory access control functionality used by the TOE to ensure separation between network services and the operating system. However, there were no Security Functional Requirements (SFRs) associated with any of the security hardening measures.

8. Further identification of the evaluated TOE, including the Intel Pentium platforms on which it was evaluated, follows below under “TOE Scope”.

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

10. An overview of the TOE’s security architecture can be found in Annex B.

TOE Scope

11. CyberGuard Firewall for UnixWare Release 4.3 was evaluated running on the UnixWare 2.1.3 operating system, both as a standard installation and as a KnightSTAR Premium Appliance Firewall Release 4.3 (hereinafter “KnightStar Release 4.3”) installation. KnightSTAR Release 4.3 is a fully pre-configured, pre-packaged TOE and a member of the Premium Appliance Firewall family that uses multiple Intel Pentium III processors. The TOE also includes other members of the Premium Appliance Firewall family, such as FireSTAR and STARLord, which are derivatives of KnightSTAR in alternative packaging as follows:

a. FireSTAR is available as a compact 1U size unit and is designed for use in mid-size, growing network environments;

b. KnightSTAR is available as a 2U or 5U size unit and is designed to provide powerful protection for enterprises, data centres and service providers; and

c. STARLord is available as a 4U size unit and is designed to provide comprehensive security for high-bandwidth data centres, web hosting and ISP / ASP markets.

12. All these variants of the Premium Appliance Firewall family utilise CyberGuard Firewall for UnixWare Release 4.3. Each platform variant incorporates identical TOE software and has the same Release number as the incorporated CyberGuard Firewall for UnixWare product. The only differences between variants is the alternative packaging and marketing name, together with the processor type and configuration of the network interface cards. (In general, the minimum requirements for each platform component changes with each TOE variant.) The initial configuration of each variant is identical (ie the network security policy is to DENY everything).

13. The TOE was evaluated with the following application proxies installed as part of the TOE:

- TELNET
- FTP for file transfer services
- SMTP for e-mail
- HTTP for the World Wide Web
- NNTP for electronic news

14. The following security features of the TOE were addressed by the evaluation:

a. Connection level Access Control for IP packets eg permit / deny source and destination addresses or ports, divert IP packets to a proxy process (FTP, HTTP, SMTP, NNTP, TELNET);

b. Accounting, auditing and statistics of firewall traffic and security related events;

c. Alerts (eg log-file, e-mail, SNMP traps) for security events;

d. Network Address Translation facility for networks and hosts; and

e. Split Domain Name Server (DNS).

15. None of the following security features were evaluated:

- Functionality of UnixWare 2.1.3 not modified by the installation of the TOE
- Virtual Private Networks
- Authentication of Firewall Administrators and network users
- Remote administrator login
- The generic SOCKS proxy and all other proxies not explicitly mentioned above
- Secure Remote Management
- Centralised Management
- Central Audit
- Client Level Authentication System (Passport-1)
- Tarantella
- High-Availability CyberGuard

16. The TOE was evaluated on an Intel Pentium II dual processor server as representative of the following supported Intel Pentium hardware platforms that are members of the Intel IA-32 family of processors which use the same basic (4-ring) protection architecture and that are compatible with Intel Specification MP1.1 or MP1.4:

- Single- or multi-processor Intel Pentium, Pentium Pro, Pentium II, Pentium III and Pentium III Xeon servers with a minimum clockspeed of 133MHz.

17. Additional platform hardware includes network interface cards, disk storage device, memory, CD-ROM Player and a tape drive. The TOE can run with a minimum of 2 and a maximum of 32 network interface cards. In the minimum configuration, the TOE is connected to one internal network and one external network.

18. Platform verification is performed according to CyberGuard's Platform Compliance and Certification process [m]. A fuller discussion of the consideration given to hardware platforms is detailed below under "Platform Issues".

Protection Profile Conformance

19. The Security Target [a] did not claim conformance to any Protection Profile.

Assurance Requirement

20. CC Part 3 [f] describes the scale of assurance given by predefined Evaluation Assurance Levels (EALs) on the scale EAL1 to EAL7 (where EAL0 represents no assurance). An overview of CC is given in CC Part 1 [d]. The assurance requirement for the TOE, as defined in the Security Target [a], was EAL4. No augmented assurance requirements were defined.

Strength of Function Claims

21. The minimum Strength of Function (SoF) was SoF-Medium. This was claimed as being commensurate with an Evaluation Assurance Level of EAL4. There were no IT Security Functions that had an associated SoF claim.

22. The authentication mechanism for the Firewall Administrator local login and for the FTP and TELNET proxies used by the TOE was provided by the underlying UnixWare operating system. The operating system is outside the scope of the TOE and as such the SoF claims did not extend to the password authentication mechanism.

Security Policy

23. The TOE security policy is evident from Sections 1 to 6 of the Security Target [a]. There are no Organisational Security Policies with which the TOE must comply.

Security Functionality Claims

24. The Security Target [a] specifies the TOE's security objectives, the threats that these objectives counter and the SFRs and IT Security Functions that elaborate these objectives. All are fully specified in the Security Target.

25. All of the SFRs are taken from CC Part 2 [e]; use of this standard facilitates comparison with other evaluated products.

26. Security functionality claims are made for IT Security Functions grouped under the following 3 categories:

- Identification and Authentication
- Discretionary Access Control (DAC)
- Accountability and Audit

27. The consumer familiar with CyberGuard Firewall for UnixWare Release 4.1, which was previously certified by the UK IT Security Evaluation and Certification Scheme to the Information Technology Security Evaluation Criteria (ITSEC) assurance level E3 [n], will observe that the security claims of CyberGuard Firewall for UnixWare Release 4.3 are equivalent to those specified in the CyberGuard Firewall for UnixWare Release 4.1 Security Target [o]. However, there is some variation in the expression of the claims in order to comply with CC requirements.

Evaluation Conduct

28. 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 [b, c]. The Scheme has established a Certification Body which is managed by the Communications-Electronics Security Group on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Mutual Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

29. 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 a 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 [f] and the Common Evaluation Methodology (CEM) [g].

30. The TOE Security Functions (TSF) and security environment, together with much of the supporting evaluation deliverables, remained unchanged from that of CyberGuard Firewall for UnixWare Release 4.1, which had previously been certified by the IT Security Evaluation and Certification Scheme to the ITSEC E3 assurance level [n]. For the evaluation of CyberGuard Firewall for UnixWare Release 4.3, the Evaluators addressed every CEM [g] EAL4 work unit but made some use of CyberGuard Firewall for UnixWare Release 4.1 evaluation results where these were valid for both CyberGuard Firewall for UnixWare Release 4.3 and the CEM requirements.

31. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the final Evaluation Technical Report (ETR) [j] to the Certification Body in November 2000. Following the CLEF response [k] to a request for further information, the Certification Body produced Issue 1.0 of this Certification Report [u].

Certification Result

32. For the certification result see the "Evaluation Outcome" chapter.

General Points

33. 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.

34. 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 the original EAL4 certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since Issue 1.0 of 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.

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

36. The certification applies to the CyberGuard Firewall for UnixWare software and the UnixWare kernel as modified by the installation of the CyberGuard Firewall for UnixWare software and excludes any unchanged operating system functionality. No evaluation of the unmodified functionality of the underlying operating system, SCO UnixWare 2.1.3, was undertaken, apart from functionality tested as part of the functional and penetration testing of the TOE.

II. EVALUATION FINDINGS

Introduction

37. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETRs [i, j] under the CC Part 3 [f] 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.

Security Policy Model

38. UK interpretation UK/2.1/003 [h] was followed, allowing the Security Target [a] to be taken as providing the Informal Security Policy Model (SPM). The Evaluators confirmed that the SPM clearly articulated the security behaviour of the TOE. They noted that although the CEM [g] does not require a check of the internal consistency of the informal SPM, the evidence for such was provided as part of the Security Target evaluation.

Delivery

39. On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

40. All TOE software components identified in Annex A are available on CD-ROM and all TOE components and documentation are delivered to the customer using FedEx, a standard trusted commercial carrier with next day delivery.

41. The following measures provide security for the TOE delivery:

a. each CD-ROM carries a proprietary photographic quality printed logo and graphics of CyberGuard Corporation and has a CyberGuard Corporation business card attached;

b. each CD-ROM is supplied in a CD-ROM case with tamper-resistant seals;

c. each CD-ROM case, together with hardcopy manuals and licence agreement is packed in a box that is sealed with CyberGuard tape;

d. each box and hardcopy document has photographic quality printed logo and graphics of CyberGuard Corporation;

e. small CyberGuard stickers displaying the software release number and site identifier are placed on the CD-ROM sleeve, CD-ROM case and box, together with blank labels (with CyberGuard logos) for customer use (eg subsequent audits);

f. the packing slip accompanying each delivery includes the separately-supplied purchase order or invoice number;

g. the delivery is performed by the carrier previously notified by CyberGuard;

h. the hardware, labelled with a unique serial number, is shipped directly from the manufacturer to the customer and the associated packing slip includes a customer reference number, the hardware serial number, the site identifier and initial password; and

i. the delivery of the hardware is previously notified to the customer by e-mail, any e-mail also including the site identifier.

42. A purchase order is required for any TOE upgrade and Product Software Updates (PSUs) are obtainable on CD-ROM.

43. There is also a CyberGuard FTP site (ftp.cybg.com), where security is enforced by requiring a login, site identifier and valid e-mail address. (N.B. This was only evaluated under ALC_FLR. See Annex C update.)

Installation and Guidance Documentation

44. Procedures for the secure installation, generation and configuration of the TOE are described in the Delivery and Configuration document [p]. Further documentation is provided in the form of the CyberGuard 4.3 Installation Guide [q] and the CyberGuard Firewall Release Notes [r].

45. The CyberGuard 4.3 Installation Guide [q] explains the procedures for the preparation and initial setup of a CyberGuard Firewall for UnixWare / Premium Appliance Firewall. It describes the software and procedures for installing and configuring a firewall, including how to install SCO UnixWare 2.1.3 and CyberGuard Firewall for UnixWare Release 4.3.

46. The SCO UnixWare 2.1.3 kernel is modified during the CyberGuard installation process by security hardening, as fully described in [l]. Therefore, whenever the system is re-booted, the TOE will startup securely.

47. Secure operation of the CyberGuard Firewall for UnixWare / Premium Appliance Firewall by a Firewall Administrator is fully described in [s]. There is no end-user documentation as there are no end-users of the TOE.

48. A collection of issues specific to the operation of CyberGuard Firewall for UnixWare / Premium Appliance Firewall and its components are also documented in the CyberGuard Answer Book available on the CyberGuard website (http://www.cyberguard.com). (N.B. This was only evaluated under ALC_FLR. See Annex C update.)

Strength of Function

49. The SoF claim for the TOE was as given above under “Strength of Function Claims”. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE and that the SoF claim of SoF-Medium was therefore upheld.

50. The Evaluators noted the following related dependency:

- Identification and authentication for the FTP and TELNET proxies is provided by the SCO UnixWare 2.1.3 operating system, which is outside the scope of the TOE.

Vulnerability Analysis

51. The Developer's vulnerability analysis described all known currently open vulnerabilities detailed in the CyberGuard Problem Report Database, including security irrelevant vulnerabilities.

52. The only security relevant potential vulnerability is as follows:

- The SMTP Proxy is designed to rewrite internal addresses if they are specified on the header of the mail message but not those contained in the "CC" field, "BCC" field, or body of the message. The Evaluators confirmed that the guidance documentation [s] describes the operation of the SMTP Proxy. In addition, the Answer Book advises that internal users should not specify any internal host addresses in the "CC" field, "BCC" field, or body of the message.

53. The Evaluators' vulnerability analysis considered both public domain sources (for TOE and SCO UnixWare 2.1.3 vulnerabilities on 9 different websites) and the visibility of the TOE given by the evaluation process, but was mainly based on information from the previous ITSEC E3 evaluation [n]. The analysis considered potential vulnerabilities (and penetration tests) under the categories of implementation errors, bypassing, tampering, direct attack and misuse. The Evaluators confirmed that the Developer's vulnerability analysis was complete and consistent with the Security Target [a] and the countermeasures detailed in the guidance documentation [q-s]. The Developer's analysis did not contain anything new with respect to the previous ITSEC E3 evaluation, which had satisfactorily tested the SMTP Proxy header rewriting potential vulnerability for "CC" and "BCC" fields.

54. The Evaluators confirmed that there were no exploitable vulnerabilities or residual vulnerabilities in the TOE.

Testing

55. The correspondence between the tests specified in the Developer's test documentation and the IT Security Functions specified in the Security Target [a], low-level design modules and source code was completely specified in the low level design. The product security functionality and tests had not changed since the previous ITSEC E3 evaluation [n].

56. The test documentation included the test plan, which detailed the test setup, network topologies and configuration required for the tests, and the test specifications, which detailed all the test descriptions, input and output parameters, test steps (applicable mainly to a few manual tests which were outside the scope of the TOE) and the expected results. The documentation also provided a summary of the results of the tests, all of which passed. The Evaluators noted that the test environment was consistent with the security environment assumptions stated in the Security Target [a].

57. The Developer's testing was performed using a largely automated test suite, comprising both fully automated tests and the few tests prompting for manual input which needed to be made before return of control to the test suite. The test suite recorded the test results. The Developer's testing was very thorough and used a range of Intel Pentium platforms (Firewalls LARRY, KOKO, DMAN and JEDI) and network interface cards in the 4 test environments specified in Annex B. All IT Security Functions and the TSF Interface were exercised during the testing and were addressed under the following topics:

- Network Address Translation
- Remote Authentication Proxies
- TELNET Proxy
- FTP Proxy
- Address Hiding Proxies
- SMTP Proxy
- NNTP Proxy
- HTTP Proxy
- Split DNS
- CyberGuard Rule Set
- Auditing and Alerts

58. The Evaluators used the same test facilities as the Developer to perform the following independent testing:

a. Each test configuration was checked for correct installation and known state of the TOE.

b. Two example installations of a TOE (a standard installation and a KnightStar installation) were repeated to check for installation errors, including errors in the installation procedures. The standard installation includes the TOE and SCO UnixWare 2.1.3. The KnightStar installation is a very fast automated installation from the KnightStar 4.3 CD-ROM that utilises Norton Ghost 6.01 to install a fully pre-configured TOE and SCO UnixWare 2.1.3 in less than 30 minutes.

c. A test for each IT Security Function specified in the Security Target [a], different from those performed by the Developer, was devised wherever possible. Only 10 independent functional tests were thus performed due to the thoroughness of the Developer's tests.

d. All the TOE-specific Developer tests were repeated to validate the Developer's functional testing.

59. The Evaluators repeated all 18 penetration tests that had been performed in the previous ITSEC E3 evaluation [n], including the Year 2000 tests. They also devised and performed 4 new penetration tests to confirm the non-exploitability of potential vulnerabilities that had been noted in the course of the evaluation. This included testing for several hundred potential vulnerabilities, using the automatic Internet Security Scanner (ISS), SAINT and Nessus tools,

and a denial of service potential vulnerability, using the jolt2.c tool. (The jolt2.c tool was one of several freeware versions available on the Internet. It included a minor CyberGuard modification prior to compilation for running on Linux. This attack tool attempts to cause CPU utilisation to reach 100% preventing incoming packets from being handled and causing the platform to cease functioning. Although denial of service functionality is not specified within the scope of the Security Target, the attack was successfully detected and the tool did not succeed in causing the CyberGuard Firewall to become sluggish or inactive.)

60. The Evaluators confirmed that the TOE implemented correctly all IT Security Functions detailed in the Security Target [a] and that there were no exploitable vulnerabilities in the TOE. In addition, no potential vulnerabilities or errors were detected by the Evaluators when using the Graphical User Interface (GUI) to perform their functional and penetration tests.

61. Test coverage of the hardware platforms was as outlined below under "Platform Issues".

Platform Issues

62. Secure operation of the TOE on the range of hardware platforms discussed above under "TOE Scope" was performed by both analysis and testing of a sample platform. In addition, a KnightSTAR Premium Appliance Firewall Release 4.3 installation was performed to check for TOE correctness and to search for errors in the installation procedures. The Evaluators concluded that the TOE, the KnightSTAR derivative and their documentation were consistent and correct.

63. In the previous ITSEC E3 evaluation [n], the Evaluators had confirmed that the product relied upon no known hardware or firmware dependencies and hence were satisfied that, subject to the Developer's requirements documented in the CyberGuard Firewall Platform Compliance and Certification [m], the product would operate on any hardware platform supported by the underlying operating system. The Evaluators confirmed that these findings remained valid for the TOE.

64. The Developer ran their full test suite on Firewall LARRY (a 200MHz Intel Pentium II dual processor server with 3 network interface cards) in the Evaluation Test Stand as detailed in Annex A.

65. The following point is noted:

- A minimum memory of 128MB and a minimum disk size of 4GB are recommended.

66. In the previous ITSEC E3 evaluation [n], the Evaluators also provided a multi-interface rationale for the product justifying its use with up to 16 network interfaces, whether internal or external. The rationale confirmed that the Developer had performed testing on up to 16 network interfaces, and addressed the behaviour of the TOE's Security Functions and mechanisms under increased loading by a description of the management of the memory and the operating system network stack. This rationale can be summarised as follows:

a. The CyberGuard packet filter works in conjunction with the operating system kernel level TCP/IP network stack. Packets are inspected for network stack processing as they arrive from the TOE's network interface controllers. During this processing the information on each configured interface is maintained in a separate dynamically allocated table of negligible size in terms of kernel memory. The main interaction between the packet filter and additional interfaces involves maintaining and looking up interface tables to gather routing information about them.

b. The addition of interfaces slightly increases the utilisation of kernel memory to establish additional lookup tables. However, this does not impact the functionality of the routines that use these lookup tables. This fact, in addition to the fact that there are no software imposed limitations in terms of static arrays or other hard coded limits, ensures that the TOE can be configured to support a maximum of 16 interfaces without impacting on the functionality of the TOE's Security Functions.

67. The Developer provided an updated rationale [t] to address 32 network interfaces and confirmed that the TOE had been successfully performance tested with 24 network interfaces. The Developer was unable to test the TOE with 32 network interfaces because of a hardware platform limitation: there is a maximum of 6 PCI slots in the PCs currently available.

68. In the Developer's performance testing configuration (which used the Smartbits traffic generator product), a STARLord firewall was configured to give the maximum of 24 interfaces. This was achieved by inserting a quad port network card into each of the 6 PCI slots. Various issues related to Smartbits were tested using all of the 24 interfaces, chosen randomly. No formal test documentation has been retained, although the Developer's performance laboratory testing ensures that the maximum possible network interface configuration has been tested when the related software limit is increased in each release of the TOE. The multi-interface rationale [t], together with the additional developer testing, thus satisfactorily demonstrated that the product would support 32 network interfaces.

Assurance Maintenance and Re-evaluation Issues

69. The development environment assessment gave primary focus to the development site in Fort Lauderdale, Florida, USA. The Evaluators confirmed that the CyberGuard development security procedures were sufficient to maintain the confidentiality and integrity of the TOE design and implementation and that the procedures were being actively applied.

70. Consumers should note that assurance in derivatives of the TOE is maintained under the UK Assurance Maintenance Process. Details of the product releases and PSUs currently covered by this process are provided on the UK Scheme website.

III. EVALUATION OUTCOME

Certification Result

71. After due consideration of the ETRs [i, j], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 4.3 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 conformant functionality in the specified environment when running on SCO UnixWare 2.1.3 and the Intel Pentium platforms as specified in Annex A.

72. 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

73. Prospective consumers of CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 4.3 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should only be used in accordance with the environmental considerations as specified in the Security Target.

74. 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”.

75. The TOE should only be configured and used in accordance with the supporting guidance documentation included in the evaluated configuration detailed in Annex A.

76. The above “Evaluation Findings” include a number of recommendations relating to the secure delivery and receipt of the TOE, together with guidance in respect of a potential vulnerability in the SMTP Proxy and the minimum sizes for RAM and hard disk.

77. As the security hardening documentation [l] is referenced from the Security Target [a], the Sponsor should make it available to the same audience as the Security Target or provide the information relevant to TOE administrators in other documents.

78. Potential consumers and administrators of the product should note the following general points with regard to the firewall:

a. a network security policy should be defined prior to any attempted installation or implementation of the firewall;

b. only the approved Firewall Administrators should have physical access to the firewall hardware;

c. the firewall should be configured in accordance with the intended method of use and environment stated in the Security Target [a, l], together with the defined network security policy;

d. to maintain an evaluated configuration, the default configuration of the operating system and network software must not be subject to any changes that would affect the firewall's security objectives; and

e. the network connections to the firewall should be controlled and periodically checked to prevent any firewall bypass connection from being installed.

79. Potential consumers of the TOE should ensure that the SoF of the authentication mechanism provided by the underlying operating system for the Firewall Administrator local login and for the FTP and TELNET proxies is adequate for their needs.

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of :

- CyberGuard Firewall for UnixWare Release 4.3

2. The CyberGuard Firewall for UnixWare Release 4.3 is provided on the following CD-ROM:

- CyberGuard Firewall Release 4.3, 1903

3. The pre-configured, pre-packaged FireSTAR Premium Appliance Firewall Release 4.3 variant is installed from the following CD-ROM:

- CyberGuard Firewall Release 4.3, 1903FS

4. The pre-configured, pre-packaged KnightSTAR Premium Appliance Firewall Release 4.3 variant is installed from the following CD-ROM:

- CyberGuard Firewall Release 4.3, 1903

5. The pre-configured, pre-packaged STARLord Premium Appliance Firewall Release 4.3 variant is installed from the following CD-ROM:

- CyberGuard Firewall Release 4.3, 1903SL

6. The supporting guidance documents for all TOE variants evaluated were:

- Delivery and Configuration, EV024-001, 26 June 2000 [p]
- CyberGuard 4.3 Installation Guide, IN001-040, June 2000 [q]
- CyberGuard Firewall Release Notes, RN001-4-3, June 2000 [r]
- CyberGuard Firewall Manual (Volumes I, II, III), FW001-050, June 2000 [s]
- Security Hardening in the CyberGuard Firewall for UnixWare, EV030-001, Issue 1.0, 10 December 1998 [l]

7. Further discussion of the supporting guidance material is given above under “Installation and Guidance Documentation”.

TOE Configuration

8. The TOE had the following configuration options:

   a. loading the TOE software from the CD-ROM as a standard installation or delivery of the pre-configured, pre-packaged Premium Appliance Firewall (FireSTAR, KnightSTAR or STARLord); and

b. allocating the number of network interface cards in the standard installation.

9. The TOE can be configured with a minimum of 2 and a maximum of 32 network interface cards for internal and external networks. In all cases, at least one internal and one external network card are installed.

10. Prior to changes for the tests that checked the proxies and network security policy rules, the following initial product configuration was used for the developer and evaluator tests:

a. configuration of TOE and UnixWare 2.1.3 operating system as defined in the Delivery and Configuration document [p];

b. 3 network interfaces: one internal network and 2 external networks;

c. all proxies disabled except FTP, HTTP, SMTP, NNTP and TELNET; and

d. network security policy (the CyberGuard Rule Set) set to DENY all.

Environmental Configuration

11. The TOE was evaluated on the Intel Pentium platform and UNIX-based operating system specified below. The correct installation of both a standard (CyberGuard Firewall for UnixWare Release 4.3) installation on that platform, and a KnightSTAR Premium Appliance Firewall Release 4.3 installation, was checked as discussed above under “Platform Issues”.

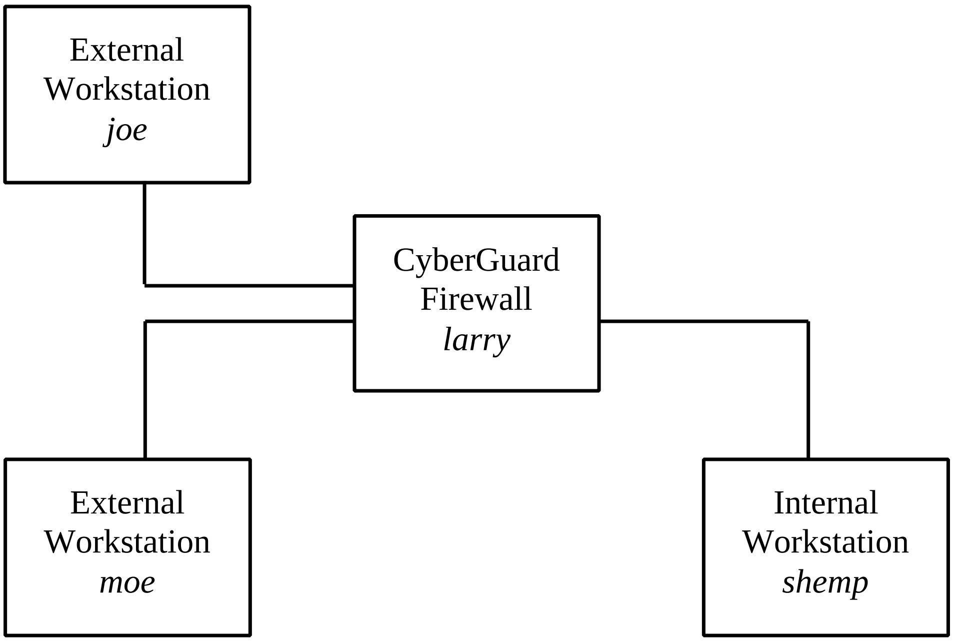
12. The TOE is designed to operate on Intel Pentium hardware platforms. It includes device drivers to support the range of commonly used disk controllers (IDE and SCSI) and the network interface cards supported by the operating system. The TOE does not rely on specific processor speed or RAM size and therefore will operate on any Intel Pentium processor that satisfies the hardware dependencies as detailed in the Platform and Compliance and Certification document [m]. In addition, the TOE does not rely on the network interface cards and therefore will operate on any network interface card supported by the UnixWare 2.1.3 operating system.

13. The main developer and evaluator tests, together with the jolt2 tests, were performed on the Evaluation Test Stand. This Test Stand included Firewall LARRY, whose specification was as follows:

- 200MHz Intel Pentium II dual processors
- 4GB Seagate Model ST32171W hard drive
- 128MB RAM
- 32X CD-ROM player
- Archive Python 238388 DAT tape drive
- 3 Cogent Em1/0 TX PCI 10/100 Fast Ethernet network interface cards

14. The following diagram illustrates the main test environment used for both the developer and evaluator tests located in the CyberGuard Corporation HQ development laboratory. The test

platform included the CyberGuard Firewall for UnixWare Release 4.3 installation running on the SCO UnixWare 2.1.3 operating system.


External Workstation *joe*
CyberGuard Firewall *larry*
External Workstation *moe*
Internal Workstation *shemp*

15. The test environment included unique IP addresses for the following hosts:

- External Workstation *moe*
- External Workstation *joe*
- CyberGuard Firewall *larry* (internal network address for Workstation *shemp*)
- CyberGuard Firewall *larry* (external network address for Workstation *moe*)
- CyberGuard Firewall *larry* (external network address for Workstation *joe*)
- Internal Workstation *shemp*

16. The workstations representing hosts on the internal and external networks used the Slackware Linux Revision 3.5 or RedHat Linux Version 6.2 operating systems and were connected via Ethernet using 10BaseT network connections (RJ45 interface).

17. Some supporting tests were run by the Developers and Evaluators on the Performance Test Stand I. This Test Stand had a similar environmental configuration as detailed above for LARRY, but used only one external workstation. Both internal and external workstations used RedHat Linux Version 6.2. This configuration was used to test the installation of both CyberGuard Firewall for UnixWare Release 4.3 (on Firewall KOKO) and KnightSTAR Release 4.3 (by replacing the Firewall KOKO with KnightSTAR). This Test Stand was also used in the tests that used the scanning tools (such as Nessus, Saint and ISS). The specification of Firewall KOKO used in the Performance Test Stand I was as follows:

- 166MHz Intel Pentium Pro dual processors
- 4GB Seagate Model ST32171W hard drive
- 32MB RAM
- 32X CD-ROM player
- Archive Python 238388 DAT tape drive
- 3 x 3COM, DEC-compatible network interface cards

18. The specification of the KnightSTAR Premium Appliance Firewall Release 4.3 used in Performance Test Stand II (ie Performance Test Stand I, with Firewall KOKO replaced by KnightSTAR) was as follows:

- 700MHz Intel Pentium II dual processors
- 9.2GB Seagate Barracuda 18XL ST39236LC hard drive
- 128MB RAM
- 48X CD-ROM player
- Single D-Link quad port network interface card

19. Some supporting automated tests were run with multiple network ports and the results verified by the Developers on the Test Automation I Stand. This Test Stand had a similar environmental configuration as detailed above for LARRY, but used only one external workstation. Both internal and external workstations used RedHat Linux Version 6.2. This configuration was used to test CyberGuard Firewall for UnixWare Release 4.3 in Firewall DMAN. The specification of Firewall DMAN was as follows:

- 180MHz Intel Pentium Pro single processor
- 4GB Seagate Model ST32171W hard drive
- 128MB RAM
- 32X CD-ROM player
- Archive Python 238388 DAT tape drive
- 2 Adaptec quad port ANA-6944A/TX 10/100 Fast Ethernet network interface cards

20. Some supporting automated tests were continually run by the Developers on the Test Automation II Stand. This Test Stand had a similar environmental configuration as detailed above for LARRY, but used only one external workstation. Both internal and external workstations used RedHat Linux Version 6.2. This configuration was used to test CyberGuard Firewall for UnixWare Release 4.3 in Firewall JEDI. The specification of Firewall JEDI used in the Test Automation II Stand was as follows:

- Dell PowerEdge 1300 base with 600MHz Intel Pentium IIIK dual processors
- 8.4GB hard drive
- 256MB RAM
- 40X IDE, CD-ROM player for Dell PowerEdge 1300 Servers
- 1.44MB 3.5" Floppy Drive for Dell PowerEdge 1300 Servers
- Archive Python 238388 DAT tape drive
- Single D-Link model DFE-570TX quad port network interface card

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the 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.

Major Architectural Features

Trusted Components and Privilege

2. The CyberGuard Firewall for UnixWare product consists of a set of bespoke CyberGuard application subsystems running on the UnixWare operating system and a set of additional CyberGuard subsystem modules for the operating system kernel. The application subsystems include the proxies, which are network services that are executed on the firewall on behalf of an internal network machine. All subsystems are security enforcing, except for the Administrative Interface subsystem which contains the GUI. The Administrative Interface subsystem is security irrelevant as the GUI does not provide a direct external interface to the TSF. (For further details, see next subsection.)

3. Although the operating system is part of the definition of the TOE, the security features of the CyberGuard Firewall for UnixWare are being implemented without using known UnixWare specific security measures. The network security measures are provided independently of the operating system. For the packet filtering process and Network Address Translation, the add-on subsystem modules are compiled into the operating system kernel. The UnixWare kernel is changed to call 2 CyberGuard modules, one for packet filtering and one for address translation. For the proxies, redirection of IP packets is performed in these modules. All other security measures are applications running independent of the operating system.

4. Issues that play a role are file system controls, user identification and authentication and network reliability. There are no claims about the security of these modules. Also, the operating system is SCO UnixWare 2.1.3, which is unevaluated. The security claims only relate to the CyberGuard Firewall for UnixWare and its 2 operating system modules.

5. CyberGuard Firewall for UnixWare has only one class of user who is the Firewall Administrator. The Firewall Administrator has local or remote access to the TOE, but remote access is outside the scope of the TOE. Users of the application proxies have limited rights and privileges and cannot log on to the firewall.

External Interfaces

6. The external interfaces that comprise the TSF Interface are as follows:

- Command Line Interface (CLI)
- Network Interface

7. The GUI is an indirect interface to the TSF as all GUI communication with the TSF is via the CLI. The GUI and CLI provide a method by which the Firewall Administrator can configure

the packet filtering and proxy services. The Network Interface is required because the firewall controls traffic between an *internal* and *external* network. All the functions in the GUI, and more, are available in the CLI. The CLI directly accesses all subsystems of the TSF, whereas the GUI calls the appropriate CLI functions on behalf of the Firewall Administrator. There can be a maximum of 32 physical network interfaces on the TOE.

Design Subsystems

8. CyberGuard Firewall for UnixWare is decomposed into several high-level design subsystems as detailed in the table below.

Subsystem	**Interface Specification**
Administrative Interface	This is the graphical user interface that is used by the Firewall Administrator to configure and maintain the firewall.
Netguard	This is the packet filtering component. For every packet passing through the firewall, netguard will either permit, deny, or proxy that packet according to the packet filtering rules that have been configured.
Network Address Translation	This component allows the firewall to hide the hosts and networks on the internal side of the firewall from the hosts and networks on the external side of the firewall.
Proxies	Proxies are network services that are executed on the firewall on behalf of the corresponding service on an internal network machine. A proxy may restrict service functionality, hide host and network information and provide stronger user authentication.
Split DNS	The split DNS component of the TOE entails the separation of DNS services for the internal and external networks. The hosts on the internal networks will be able to utilise the internal or external DNS server. However, hosts on the external network will only be able to utilise the external DNS server.
Audit & Alerts	This component monitors and records events on the firewall, as specified by the Firewall Administrator. The Firewall Administrator can configure alerts to be triggered on certain events that occur on the TOE. An alert could be a message to the console, a message by email, a message by pager, a log file entry or the result of a custom shell script.

9. The TOE subsystems identified as TOE Security Policy enforcing within the scope of the evaluation are detailed below.

Netguard (NET)

10. All IP packets entering the firewall from a network interface will be checked against the Netguard rules at the kernel level. An IP packet may be subject to a PERMIT, PROXY or DENY rule. A PERMIT rule entails that the IP packet is passed to the appropriate interface. A PROXY rule entails that the IP packet is passed up the TCP/IP protocol stack on the firewall. A DENY rule entails that the IP packet is dropped and ignored completely. In the cases where an IP packet appears on an interface where it could not have possibly originated (eg an IP packet with an apparently external address on an internal interface), then the packet is dropped if the Validate Source Address option has been set.

11. The UnixWare kernel is modified, by the installation of the TOE, to perform the packet filtering. A packet filtering rule can be *static* (ie defined in `netguard.conf`) or *dynamic* (ie created as necessary by the firewall in operation, usually in response to proxy traffic).

Network Address Translation (NAT)

12. NAT hides internal network addresses from external hosts but allows services to function normally. NAT translates the source address/port of outbound IP packets to a registered external IP address and translates the destination address/port of inbound IP packets to the appropriate internal host.

13. NAT is located in the kernel between NET and the network access layer on the TCP/IP protocol stack. A system command called `nat` allows the administration of static and dynamic NAT. In dynamic NAT, all internal addresses are changed to the firewall's address. In static NAT, all internal addresses are changed to a configured registered global address (not necessarily the firewall's address).

Proxies (PRO)

14. PRO provides network services on the firewall on behalf of corresponding services on a local host. A proxy helps to restrict the functionality of a service, hide internal names and addresses, provide authentication at the firewall and interfaces with standard clients and servers.

TELNET Proxy

15. The TOE ensures that user identification and password authentication is provided by the TELNET proxy, although the Identification and Authentication mechanism is outside the scope of the TOE. Note that token authentication is also out of scope because it is third party functionality. The `/etc/passwd` file is used to support identification based on a user login account name and the `/etc/shadow` file supports authentication based on the user's password. The usual password management characteristics can be defined, such as length, locking, expiry etc. Any TELNET connection request from an external host to an internal host is held on the firewall and passed to the TELNET proxy which will mediate the connection and subsequent session to the internal host. As a security precaution, users cannot login to the firewall itself and cannot TELNET to the firewall.

16. The packet filtering rules that are contained in the operating system file `/etc/security/firewall/ng_inet/netguard.conf` determine whether TELNET itself or the TELNET proxy is activated, and which networks or hosts are permitted. On successful identification and authentication, the final destination will be requested (ie a login shell is not provided at this point). The user then provides the identification and authentication (not necessarily the same as that at the firewall) required at the destination.

17. TELNET can be configured with authentication *at* the firewall or (the default) *through* the firewall. In the first instance, the user will be prompted for the destination. In the second instance, the destination is already known. In both cases it is the firewall itself which performs the authentication before the session is established.

FTP Proxy

18. The description for the FTP proxy is the same as already outlined for the TELNET proxy, with the following additional functionality:

- A subset of the FTP commands can be defined on a per user basis. This is additional (and separate) to the control provided by the netguard packet filtering rules in `netguard.conf`

- Anonymous FTP is supported, although it is not allowed in the evaluated configuration since identification and authentication is not possible

SMTP Proxy

19. The SMTP proxy filters email between 2 hosts and ensures that headers of mail messages are rewritten so that internal names and addresses are hidden. SMTP is used by Mail Transfer Agent programs such as sendmail and User Agent programs such as elm, pine and mailx. SMTP consists of 4 letter commands with arguments and 3 digit numbers with a character string. Commands are preceded by “S:” and replies are preceded by “R:”.

20. The firewall can be configured to permit, proxy or deny SMTP communication inbound/outbound between any specified hosts. In outgoing mail, the SMTP proxy will change the domain name in the “FROM:” argument to the domain name of the firewall. All “Received:” lines will be deleted except for the last. In incoming mail, the SMTP proxy will change the “To:” path from its external representation to the valid internal path. The SMTP proxy only allows the following commands: HELO, MAIL, RCPT, DATA and QUIT. *The other commands such as EXPN, HELP, NOOP, RSET, SAML, SEND, SOML, TRUN and VRFY are not allowed.*

NNTP Proxy

21. The NNTP proxy filters news messages between 2 hosts and ensures that the headers are rewritten so that internal names and addresses are hidden.

22. The firewall can be configured to permit, proxy or deny NNTP communication inbound/outbound between any specified hosts. In outgoing news messages, the NNTP proxy will change the domain name to the domain name of the firewall. Incoming news messages are left unchanged. The NNTP protocol does not support user authentication so the TOE does not require user authentication. However, access can be controlled to a certain extent via the netguard packet filtering rules, in conjunction with the NAT functionality.

HTTP Proxy

23. The HTTP proxy ensures that information is displayed according to the file `httpd-proxy.conf` and can be used with and without NAT. Some of the features are: controlled access to internal servers, configurable list of prohibited sites, default HTML document when unable to access internal server, default HTML document on attempt to access a prohibited site. Proxy operation is transparent to the user and HTTP clients (such as Netscape Navigator and Microsoft Internet Explorer) do not need to be modified.

Split DNS

24. Split DNS protects against a malicious external attacker discovering the IP addresses (and other information) on an internal network by probing a DNS server. Split DNS provides 2 DNS servers on one machine (the firewall). There is one server for the internal network and one for the external network. The internal server receives and returns requests from the internal network. The internal server sends and receives requests to the external server. The external server receives and returns requests from the internal server. The external server sends and receives requests to the external network. The external server receives and sends requests from the external network; however, it will only be able to respond to queries about the firewall host.

25. The internal and external DNS servers use the same executable but the starting script points them to distinct configuration and host database files, which are located in distinct directories. The internal DNS server will use the external DNS server as its primary, and the external DNS server database will not contain any information about the internal DNS server.

Audit & Alerts (AAM)

26. When an auditable event occurs, the process collects the necessary audit information and generates an audit record. All such audit records are stored in a file for future processing. The TOE uses the UnixWare auditing subsystem to record auditable events for the network, system and user. An alert management system provides notification (by message box, email, pager or custom script) of configured alert-events in the TOE. Various types of audit reports can be generated by the TOE from the binary audit log files.

27. The following audit trail commands are supported: `auditlog`, `auditlogd`, `auditon`, `auditoff`, `auditrpt`, `auditset`, `auditmap`, `audit_compress`, `audit_init_log and alert_log_tidy_up`. The default audit configuration file is `/etc/default/audit`. The following files are generated by `auditlogd`:

- `ForwardD` - IP packet forwarding
- `NetguardD` - packet denied by a rule
- `NetguardI` - packet denial due to interface spoof
- `NetguardM` - packet denial due to failure to match rule
- `NetguardP` - packet permitted by a rule
- `NetguardS` - all packet processing events
- `NetguardT` - session summary on data transfer completion
- `Portscan` - packet denial due to network port scan attempts

28. The TOE has user level auditing and kernel level auditing.

29. For kernel level auditing, NET and NAT use the UnixWare audit system to write audit records to audit buffers. Kernel audit buffers are written to binary audit log files in `/var/audit`, where file names are of the form MMDDxxx (MM = month, DD = day, xxx = sequence number).

30. For user level auditing, NET and PRO use the `auditdmp` command which executes the same kernel routines and functions as in the kernel level process.

31. The alert component notifies security personnel of possible attacks and the trace component produces reports. Alerts are based on the netguard and alert configuration files as follows:

- `/etc/security/firewall/ng_inet/netguard.conf`
- `/etc/security/cyber/alert.conf`

32. The `alert.conf` file has lines of the form alert_name parameter=value

33. When a suspicious event occurs, `auditlogd` does one of the following: it triggers a specified action, it increments/decrements/resets the specified alarm count or it stops monitoring an audit trail for a specific alarm condition.

Administrative Interface

34. The Administrative Interface (the GUI) is claimed to be security irrelevant since anything the GUI can do is covered by the security functionality of the CLI. The Administrative Interface is merely a way in which the TOE can be configured in a high-level user-friendly well-structured manner, without recourse to the CLI.

35. However, not all aspects of the Administrative Interface are relevant to the evaluated configuration of the TOE, eg centralised management, secure remote management, high availability, etc. One point of interest is that the GUI functionality does perform error checking on the input fields of configuration windows.

Discretionary Access Control (DAC)

36. DAC is not a separate subsystem of the TOE. It implements the network security policy rules as configured by the Firewall Administrator using the CLI. The firewall uses a set of rules known as “Netguard rules” which govern how IP packets move through the firewall. Each rule keeps track of source, destination, service and protocol of an IP packet. IP packets flowing through the firewall are processed on the basis of these defined rules. These packet filtering rules are specified in the form:

Operator Service/Protocol SourceAddress DestinationAddress Options

37. Operator can be PERMIT, PROXY or DENY. Service is any name or number in the operating system file `/etc/inet/services`. Protocol is any name or number in the operating system file `/etc/protocols`. The SourceAddress and DestinationAddress values are names or addresses of hosts or networks. The Options can include the following: enable_reply, dont_audit, no_if_check, time_out, established, rpc_program, rpc_proc and rpc_user. Several keywords are also defined so that the packet filtering rules can be user friendly and hence understood quickly.

Operating System Dependencies

38. The FTP and TELNET proxies for CyberGuard Firewall for UnixWare Release 4.3 use the operating system’s authentication mechanism in conjunction with the firewall’s own authentication database to verify the user’s access. Users of these proxies have limited rights and privileges and cannot log on to the firewall. The Firewall Administrator local login uses the operating system’s authentication mechanism, via the contents of the UnixWare password database, in conjunction with the firewall’s own authentication database, to verify the Administrator’s access to the firewall. The auditing subsystem of the CyberGuard Firewall is an extension to the UnixWare auditing subsystem. The additional auditing functionality enhances some of the existing UnixWare kernel level auditing routines and provides additional new routines.

Hardware and Firmware Dependencies

39. The TOE has no firmware components. There were no firmware dependencies affecting the evaluation.

40. The hardware was relied upon to provide general supporting protection mechanisms.

(This page is intentionally left blank)

ANNEX C: FLAW REMEDIATION AUGMENTATION

Introduction

1. This annex gives an overview of the ALC_FLR evaluation that was performed concurrently with AMA Audit No 1 in January and March 2002.

Assurance Requirement

2. The assurance requirement for the TOE, as defined in the updated Security Target [v], was EAL4 augmented with ALC_FLR.1 (basic flaw remediation).

Evaluation Conduct

3. As part of the UK Assurance Maintenance Process, the ALC_FLR component was evaluated by the Logica CLEF in accordance with the latest guidance detailed in the CEM Supplement on Flaw Remediation [w]. Following the submission in March 2002 of an AMA Audit Report [x, y] that addressed Flaw Remediation, the Certification Body issued an updated Certificate. The Certification Body subsequently produced Issue 2.0 of this Certification Report to confirm the Flaw Remediation outcome stated in that AMA Audit Report.

General Points

4. Certification of a Flaw Remediation Process acknowledges that there is no guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after an original certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether such patches have been:

- applied in accordance with the evaluated flaw remediation procedures,
- incorporated into a later assurance maintained derivative, or
- evaluated and certified.

Delivery

5. The measures providing security during delivery are summarised in the main body of this report. In respect of delivery via the CyberGuard FTP site (ftp.cybg.com), MD5 checksum functionality is provided to detect tampering en route from CyberGuard to a customer. The relevant checksum is provided by courier to the customer (ie separate from the release or PSU download) to permit comparison against the checksum information derived from the TOE or TOE derivative after download. Note, however, that whilst the possibility of using the MD5 checksum functionality has been evaluated as a delivery procedure, it is the Vendor’s current practice to use a CD-ROM delivery procedure.

Flaw Remediation Procedures

6. The Evaluators confirmed [x, y] that the flaw remediation procedures documentation was satisfactory. CyberGuard monitors the public domain vulnerabilities provided by CERT Summaries (from CERT Co-ordination Center Incident Response Team), together with websites and mailing lists, such as Bugtrack and ICSA Firewall Product Vendor Consortium mailing list. Vulnerabilities relevant to all CyberGuard products are also tracked via phone calls from customers or field personnel to the Hot Line personnel. Any unresolved problem from the Support Calls database is forwarded to the CyberGuard software developers and logged in the Problem Report database, which records all problems related to the product, including the status of each security flaw. The Tracking Database, a web-based tool, tracks all changes requested for each new release. A Tracking Sheet for each new release details the associated problem reports.

7. Updated product releases and PSUs are distributed to consumers using the measures described under “Delivery”. Existing customers are notified of each security flaw and associated fix, and the method for obtaining an updated product release or PSU, by a variety of methods:

a. The README file, associated with each product release or PSU, is available on CD-ROM and the CyberGuard website and contains details of each change, including any resolved security flaws, related to that release or PSU.

b. The Answer Book describes product flaws and the identity of the product release or PSU that addresses each flaw. The Answer Book is an on-line database on the CyberGuard website (http://www.cyberguard.com) that is available only to current CyberGuard customers. The Answer Book provides a detailed explanation of these flaws and provides Firewall Administrators and support staff with direct access to live documentation which is quickly updated with the latest information and advice.

c. The Hot Line personnel notify fixes to existing customers who have reported specific problems.

d. Customer Support disseminates appropriate security flaw information to the customer community via the regular CyberGuard Security Bulletin, e-mail or the CyberGuard website.

Certification Result

8. After due consideration of the AMA Audit Report [x, y], produced by the Evaluators, and the visibility of the Flaw Remediation Process given to the Certifier, the Certification Body has determined that CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 4.3 meets the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL4, augmented with ALC_FLR.1, for the specified Common Criteria Part 2 conformant functionality in the specified environment when running on SCO UnixWare 2.1.3 and the Intel Pentium platforms as specified in Annex A.