

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

CERTIFICATION REPORT No. P136

BorderWare Firewall Server

Version 6.1.1

running on specified Intel platforms

Issue 1.0

January 2000

© Crown Copyright 2000

Reproduction is authorised provided the report
is copied in its entirety

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 Arrangement of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.*

*Mutual recognition applies to EAL4 but not to ALC_FLR.1 (basic flaw remediation).

The following trademarks are acknowledged:

BorderWare Firewall Server is a trademark of BorderWare Technologies Inc.

Windows and Windows NT are trademarks of Microsoft Corporation.

PowerEdge is a trademark of Dell Computer Corporation.

Intel, Pentium and Celeron are trademarks of Intel Corporation.

All other product names mentioned herein are trademarks of their respective owners.

CERTIFICATION STATEMENT

BorderWare Technologies' BorderWare Firewall Server is a secure Internet gateway designed to implement secure Internet or intranet connections. The BorderWare Firewall Server incorporates a hardened operating system based on FreeBSD UNIX.

BorderWare Firewall Server Version 6.1.1 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 incorporating Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 conformant functionality in the specified environment when running on the platforms described in Annex A.

Originator	Dr. A W Powell Certifier
Approval	Dr. R Pizer Head of the Certification Body
Authorisation	P M Seeviour Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	28 January 2000

(This page is intentionally left blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT	iii
TABLE OF CONTENTS	v
ABBREVIATIONS	vii
REFERENCES	ix
I. EXECUTIVE SUMMARY	1
Introduction	1
Evaluated Product	1
TOE Scope	2
Protection Profile Conformance	3
Assurance Level	3
Strength of Function	3
Security Claims	3
Threats Countered	3
Threats and Attacks not Countered	4
Environmental Assumptions and Dependencies	5
IT Security Objectives	5
Non-IT Security Objectives	6
Security Functional Requirements	6
Security Function Policy	7
Evaluation Conduct	8
Certification Result	8
General Points	8
II. EVALUATION FINDINGS	11
Security Policy Model	12
Delivery and Installation	13
User Guidance	14
Misuse	14
Developer's Tests	14
Evaluators' Tests	15
III. EVALUATION OUTCOME	17
Certification Result	17
Recommendations	17
ANNEX A: EVALUATED CONFIGURATION	19
ANNEX B: PRODUCT SECURITY ARCHITECTURE	23

(This page is intentionally left blank)

ABBREVIATIONS

ATA	Advanced Technology Attachment
BSD	Berkeley Software Development
BWAPI	BorderWare Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
DES	Data Encryption Standard
DNS	Domain Name Server
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDE	Integrated Drive Electronics
IP	Internet Protocol
NNTP	Network News Transmission Protocol
POP	Post Office Protocol
RAC	Release Acceptance Criteria
SCSI	Small Computer System Interface
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SoF	Strength of Function
SSN	Secure Servers Network
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UKSP	United Kingdom Scheme Publication
URL	Uniform Resource Locator
WWW	World Wide Web

(This page is intentionally left blank)

REFERENCES

- a. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 3.0, 2 December 1996.
- b. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.
- c. Security Target for BorderWare 6.1.1,
BorderWare Technologies Inc.,
ST, Version 2.3, January 2000.
- d. Common Criteria Part 1,
Common Criteria Implementation Board,
CCIB-98-026, Version 2.0, May 1998.
- e. Common Criteria Part 2,
Common Criteria Implementation Board,
CCIB-98-027, Version 2.0, May 1998.
- f. Common Criteria Part 3,
Common Criteria Implementation Board,
CCIB-97-028, Version 2.0, May 1998.
- g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
Version 1.0, CEM-99/045, August 1999.
- h. Manual of Computer Security Evaluation, Part III, Evaluation Tools and Techniques,
UK IT Security Evaluation and Certification Scheme,
USKP 05, Version 2.0, 30 July 1997.
- i. Manual of Computer Security Evaluation, Part V, Generic Potential Vulnerabilities,
UK IT Security Evaluation and Certification Scheme,
USKP 05, Version 1.0, 30 July 1997.
- j. Evaluation Technical Report,
Common Criteria EAL4 Augmented Evaluation of BorderWare 6.1.1,
Syntegra CLEF,
LFS/T274/ETR, Issue 1.0, 24 January 2000.

- k. Installation and Administrative Guide,
BorderWare Technologies Inc.,
Version 1.1, December 1999.
- l. BorderWare Firewall Server 6.1.1 Reference Guide,
BorderWare Technologies Inc.,
December 1999.
- m. BWClient Help GUI,
BorderWare Technologies Inc.,
Version 1.1b, December 1999.
- n. EAL4 Configuration Guide for BorderWare 6.1.1,
BorderWare Technologies Inc.,
December 1999.
- o. TOE Security Policy Model For BorderWare 6.1.1,
BorderWare Technologies Inc.,
SPM, Version 1.1, December 1999.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the IT security evaluation of BorderWare Firewall Server Version 6.1.1 to the Sponsor, BorderWare Technologies Inc., and is intended to assist potential consumers when judging the suitability of the product for their particular requirements.

2. The prospective consumer is advised to read the report in conjunction with the Security Target [Reference c], which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

BorderWare Firewall Server Version 6.1.1.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was BorderWare Technologies Inc. Details of the evaluated configuration, including the product's supporting guidance documentation, are given in Annex A.

4. The BorderWare Firewall Server is a secure Internet gateway. It provides a set of ancillary services necessary to implement Internet and intranet connections. The TOE provides 3 layers of security: packet filtering, circuit level gateways and application level gateways.

5. The TOE incorporates a bespoke hardened FreeBSD UNIX-based operating system. The operating system provides a separate domain of execution for each security critical subsystem and implements kernel level packet filtering.

6. The following TOE subsystems are TOE Security Policy (TSP)-enforcing:

- C BorderWare Application Programming Interface (BWAPI)
- C UNIX Kernel
- C Database
- C System console
- C Administration Graphical User Interface (GUI)
- C Proxies
- C File Transfer Protocol (FTP) Server
- C Web Server

7. The Admin GUI is provided by the BWClient remote administration application installed on a Win32 machine on the internal network. Further details of the BWClient are provided in Annex A to this report.

8. The following TOE subsystems are TSP-supporting:

- C Domain Name Server (DNS)
- C Mail Server
- C Finger Server
- C Ident Server
- C Traceroute Response Server
- C Ping Server

9. The proxies manage connections for TCP/IP applications, provided by the servers such as DNS and mail relay. A complete list of the proxies within the scope of this evaluation is provided in Annex B to this report. The TOE provides dual DNS and Network Address Translation to ensure separation between internal and external networks. The mail relay service protects e-mail servers by allowing mail dispatch and delivery without permitting a connection between the server and an untrusted network.

10. Details of the TOE's architecture can be found in Annex B to this report.

TOE Scope

11. The scope of the certification applies to the TOE running on any standard Intel platform as the TOE does not rely on specific processor speed or RAM size and therefore will operate on any Intel processor that satisfies the hardware dependencies. See Annex A for details of the platforms on which the TOE was tested.

12. The TOE can run with a maximum of 3 and a minimum of 2 network interface cards. These are used to connect the firewall to the internal, external and (if there is a third network interface card) the Secure Servers Network (SSN), which is a demilitarised zone.

13. The proxies and services within the scope of the evaluation are detailed in Annex B to this report.

14. The evaluation of BorderWare Firewall Server Version 6.1.1 **excludes** the following functionality, which has not been considered by the Evaluators:

- C Third party authentication (eg Crypto Card for administrator authentication or Secure inbound FTP and Telnet proxies)
- C Virtual Private Network capability
- C User Defined Proxies
- C Uniform Resource Locator (URL) Filtering (ie SmartFilter)
- C Secure remote administration of the firewall from an external (unprotected) network
- C Support access for patches and upgrades

Protection Profile Conformance

15. The Security Target [c] did not claim conformance to any protection profiles.

Assurance Level

16. The Security Target [c] specifies the assurance requirements for the resultant evaluation. The assurance incorporated predefined evaluation assurance level EAL4 augmented by ALC_FLR.1 (basic flaw remediation). Common Criteria Part 3 [f] describes the scale of assurance given by predefined evaluation assurance levels EAL1 to EAL7. EAL0 represents no assurance.

Strength of Function

17. The TOE contained the permutational cryptographic functions to provide administrator password-based authentication at the system console and FTP-user passwords to meet the “timing of authentication” Security Functional Requirement (SFR) FIA_UAU.1. The minimum Strength of Function (SoF) claim for the TOE was SOF-medium. This claim referred to the strength of the password file encryption mechanism using the Data Encryption Standard (DES) which was additionally protected by operating system access control. DES is publicly known and as such it is the policy of the national authority for cryptographic functions, the Communications-Electronics Security Group (CESG), not to comment on its appropriateness or strength. The minimum SoF claim also applied to the administrator password and FTP-Admin authentication mechanisms.

Security Claims

18. The Security Target [c] fully specifies the TOE’s security objectives, and threats which these objectives counter and functional requirements and security functions to elaborate the objectives. The Security Target does not mandate compliance with any Organisational Security Policies. All of the functional requirements were taken from Common Criteria (CC) Part 2 [e]; use of this standard facilitates comparison with other evaluated products. An overview of CC is given in CC Part 1 [d].

Threats Countered

19. The threats that the TOE is to counter are as follows:
- a. Attackers on the external network may gain inappropriate access to the internal network.
 - b. Users on the internal network may inappropriately expose data or resources to the external network.
 - c. An attacker on the external network may try to connect to services other than those expressly intended to be available in accordance with the security policy.
 - d. An attacker on the internal network may try to connect to services other than those expressly intended to be available.
 - e. An attacker on the internal or external network may attempt to initiate a service from an unauthorised source.

- f. An attacker on the internal or external network may exploit a configuration not in accordance with the chosen network security policy of the firewall.
- g. Unauthorised changes to the configuration may be completed without being identified.
- h. An attacker on the internal or external network may attempt to use operating system facilities on the firewall server.

Threats and Attacks not Countered

- 20. Protection against violation of network security policy as a result of inaction or action taken by careless, willfully negligent or external system administrators must be supplied by measures in the TOE's environment or accepted as potential security risks.
- 21. The TOE does not claim to resist all denial-of-service attacks, although during testing the TOE was found to be resistant to all of the denial-of-service attacks performed by the Evaluators.
- 22. Potential consumers should note that it is not possible for any firewall to counter all types of Internet Protocol (IP) source address spoofing attack, although all network traffic appearing on an interface is denied by the packet filtering rules, other than that which is implied by the relevant IP packet source address. It should be noted that the threat of the internal or external masquerade variant of IP address source address spoofing (ie masquerade of an internal IP source address on an internal network or of an external IP source address on the external network) is not countered.
- 23. Potential consumers should note that the firewall, in common with similar TOEs, does not counter the threat of Session Hi-jacking (ie an external attacker taking over an authenticated session initiated by another external host).
- 24. Potential consumers should be aware that the TOE does not differentiate between HyperText Markup Language (HTML) and embedded active content such as Java or ActiveX that may be transmitted using the HyperText Transfer Protocol (HTTP).
- 25. Potential consumers should be aware that the TOE does not detect viruses.
- 26. Potential consumers should be aware that in general the TOE does not counter the attack of tunnelling one protocol inside another.

Environmental Assumptions and Dependencies

27. The TOE's environment must also satisfy the following assumptions:
- a. The firewall must be physically protected to prevent hostile individuals engaging in theft, implantation of devices or unauthorised alteration of the physical configuration of the firewall.
 - b. The firewall will only limit the access to resources and data between an internal and external network.
28. The TOE has no software or firmware dependencies. The TOE has the following hardware dependencies:
- C User and Kernel mode
 - C Interrupts and Exceptions
 - C Processor Execution levels
 - C Memory Allocation
 - C System clock

IT Security Objectives

29. The IT security objectives in the Security Target [c] are as follows:
- a. The firewall must limit the valid range of addresses expected on each of the external and internal networks.
 - b. The firewall must limit the hosts and service ports that can be accessed from the external network.
 - c. The firewall must limit the hosts and service ports that can be accessed from the internal network.
 - d. The TOE must provide authentication of the end-user prior to establishing a through connection, in accordance with the security policy enforced on the TOE. (The policy is to ensure that no services are allowed for inbound connections.)
 - e. The firewall must provide facility for monitoring successful and unsuccessful attempts at connections between networks.
 - f. The firewall must provide a secure method of administrative control of the firewall, ensuring that only the authorised administrator can exercise such control.
 - g. The firewall must provide separate areas in which to process security functions and service requests. The processing of a security function must be completed prior to the invocation of subsequent security functions.

- h. The firewall is designed and configured solely to act as a firewall and does not provide any operating system user services to any network users; administrators have access to the firewall via the administration GUI.

Non-IT Security Objectives

30. The non-IT security objectives in the Security Target [c], which are met by procedural or administrative measures in the TOE's environment, are as follows:

- a. Those responsible for the firewall must ensure that it is delivered, installed and managed in a manner that maintains the security policy.
- b. Those responsible for the firewall must train administrators to establish and maintain sound security policies and practices.
- c. Administrators of the firewall must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis and appropriate action should be taken on detection of breaches of security or events that are likely to lead to a breach in future. Furthermore, appropriate archive action must be taken to ensure security logs archived by the firewall are not overwritten before they are inspected.
- d. The firewall must be configured as the only network connection between the internal network and the external network.
- e. A firewall administrator is assigned the responsibility for day-to-day management and configuration of the firewall, including management of the audit trail.
- f. The firewall must be physically protected so that only administrators have access. The firewall must only be administered via the dedicated management port on the firewall or by using the administration GUI on the internal network.
- g. The configuration of the firewall will be reviewed on a regular basis to ensure that the configuration continues to meet the organisation's security policies in the face of changes to the firewall configuration, changes in the security objectives, changes to the threats from the external network, and changes in the hosts and services made available to the external network by the internal network.

Security Functional Requirements

31. The TOE provides security functions to satisfy the following SFRs:

- C Timing of identification (FIA_UID.1)
- C Timing of authentication (FIA_UAU.1)
- C Authentication failure handling (FIA_AFL.1)
- C Management of security attributes (FMT_MSA.1)
- C Static attribute initialisation (FMT_MSA.3)
- C Security Roles (FMT_SAR.1)

- C Management of TOE Security Functions' (TSF) data (FMT_MTD.1)
- C Security audit data generation (FAU_GEN.1)
- C Security alarms (FAU_ARP.1)
- C Security audit analysis (FAU_SAA.1)
- C Security audit review (FAU_SAR.1)
- C Protected audit trail storage (FAU_STG.1)
- C Non-bypassability of the TSP (FPT_RVM.1)
- C TSF domain separation (FPT_SEP.1)
- C Reliable time stamps (FPT_STM.1)
- C Subset access control (FDP_ACC.1)
- C Security attribute based access control (FDP_ACF.1)
- C Subset information flow policy (FDP_IFC.1)
- C Information flow functions based on simple security attributes (FDP_IFF.1)

Security Function Policy

32. The TOE has an explicit access control Security Function Policy defined in the FDP_ACC.1 SFR and an explicit information flow policy defined in the FDP_IFC.1 SFR. A summary of each of these policies is provided below, and more details can be found in the "Security Policy Model" section and in paragraph 11 of Annex B to this report.

33. Access to the firewall's internal data is controlled by the identification and authentication of an administrator at the firewall console. Once this has been completed, according to the requirements specified by the FIA class of components, an administrative user is able to access all TSF data. Access to data stored in the FTP server is controlled according to whether the user has successfully provided the necessary authentication information. An "anonymous" or "FTP" FTP user can only access a subset of the information that the FTP Admin user is able to access.

34. There are 3 main types of information flow:

- a. AUTHENTICATED – traffic from the internal network to the firewall, providing access to the firewall for a remote administrator on the internal network, which requires the source subject to be identified and authenticated as an administrator of the firewall.
- b. UNAUTHENTICATED – outbound traffic, of which the source subject is identified, but not authenticated. Also, inbound traffic from the external network to the SSN, and inbound traffic from the SSN to the internal network as this is a controlled flow from a known source.
- c. UNIDENTIFIED – outbound traffic, of which the source subject is not identified, and inbound traffic from the external network to the SSN.

Evaluation Conduct

35. 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 [a, b]. The Scheme has established a Certification Body which is jointly managed by CESG and the Department of Trade and Industry on behalf of Her Majesty's Government.

36. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [c]. To ensure that the Security Target gave an appropriate baseline for a Common Criteria evaluation, it was first itself evaluated, as outlined by CC Part 3 [f].

37. The evaluation was performed against the EAL4 assurance package and assurance component ALC_FLR.1 (basic flaw remediation) defined in CC Part 3 [f]. The Common Evaluation Methodology (CEM) [g] was used as the methodology for the evaluation.

38. The Evaluators conducted sampling during the evaluation, as required for the relevant work-units for EAL4. Guidance provided in the CEM [g], Annex B, Section B.2, was followed in all cases. The Evaluators also confirmed the sample size and approach with the Certifier in all cases. For the testing, the Evaluators repeated a minimum sample of 20% of the Developer tests and checked that the sample covered all of the security functions of the TOE. Where the sampling related to gaining evidence that a process such as configuration control was being followed, the Evaluators sampled sufficient information to gain reasonable confidence that this was the case.

39. The Evaluators used software tools during independent testing. The Evaluators used these tools in accordance with guidance from the Certification Body and from UKSP 05 Part III [h] Chapter 12.

40. The Certification Body monitored the evaluation which was carried out by the Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed in January 2000 when the CLEF submitted the final Evaluation Technical Report (ETR) [j] to the Certification Body which, in turn, produced this Certification Report.

Certification Result

41. For the evaluation result see the "Evaluation Outcome" section.

General Points

42. 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. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether such patches have been evaluated and certified. Consumers 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 and systems can be found on the IT Security Evaluation and Certification Scheme web site www.itsec.gov.uk.

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

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

(This page is intentionally left blank)

II. EVALUATION FINDINGS

45. The Evaluators examined the following assurance classes and components taken from CC Part 3 [f]:

Assurance class	Assurance components
Configuration management	Partial configuration management automation (ACM_AUT.1)
	Generation support and acceptance procedures (ACM_CAP.4)
	Problem tracking configuration management coverage (ACM_SCP.2)
Delivery and operation	Detection of modification (ADO_DEL.2)
	Installation, generation and startup procedures (ADO_IGS.1)
Development	Fully defined external interfaces (ADV_FSP.2)
	Security enforcing high-level design (ADV_HLD.2)
	Subset of the implementation of the TOE Security Functions (ADV_IMP.1)
	Descriptive low-level design (ADV_LLD.1)
	Informal correspondence demonstration (ADV_RCR.1)
	Informal TOE Security Policy (ADV_SPM.1)
Guidance documents	Administrator guidance (AGD_ADM.1)
	User guidance (AGD_USR.1)
Life cycle support	Identification of security measures (ALC_DVS.1)
	Basic flaw remediation (ALC_FLR.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Well defined development tools (ALC_TAT.1)
Security Target	TOE description (ASE_DES)
	Security Environment (ASE_ENV)
	Security Target introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	Protection Profile claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	TOE summary specification (ASE_TSS)

Assurance class	Assurance components
Tests	Analysis of coverage (ATE_COV.2)
	Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability Assessment	Misuse: validation of analysis (AVA_MSU.2)
	Strength of TOE security function evaluation (AVA_SOF.1)
	Independent vulnerability analysis (AVA_VLA.2)

46. All assurance classes were found to be satisfactory and were awarded an overall “pass” verdict.

47. There are a number of aspects of the evaluation that are relevant to consumers. These are summarised in the sections that follow.

Security Policy Model

48. The Security Policy Model [o] identifies 5 types of security policies in the TOE, which completely define the conditions under which a user and administrator can interact with the TOE. These policy types are as follows:

- C Information flow control security policies
- C Identification and authentication security policy
- C Access control security policy
- C Separation security policy
- C Audit security policy

49. The TOE provides a flow control mechanism for all connection requests received by the firewall on one of its network interfaces. The TOE processes incoming requests for services and will permit or deny the request according to the rules set by the administrator. The initial default policy is to deny connection requests that are not covered by an explicit rule. Information flows can be either UNAUTHENTICATED (identification only), AUTHENTICATED (identification and authentication) or UNIDENTIFIED (no identification or authentication). Details of the services belonging to each category are provided in paragraph 11 of Annex B to this report.

50. Only TOE administrators are allowed to login at the system console and the remote administration GUI on the internal network. The TOE does not perform any other source authentication within the scope of the evaluation. Source authentication on FTP and Telnet IP packets entering the firewall from the external network and the SSN was outside the scope of the evaluation. However, the TOE performs source authentication on FTP IP packets from the internal network with the user identifier “FTP Admin”. The claimed source address is verified against the address of the network interface card on which it was received, disallowing the packet if the results of the check are not consistent. A password-based scheme is used.

51. All TOE administrators have the same access rights. Administrators set the security policy by modifying the configuration of the TOE, modifying the rules specifying permissible traffic, by creating and updating administrator accounts, by configuring the events to be accounted and by enabling audit alarms and configuring audit parameters. The FTP administrator can access the administration area of the FTP server and may be granted access to download audit logs from the FTP server. The FTP administrator can read, copy and delete the audit trails archived to the administration area of the FTP server. Unprivileged users of the TOE interact with the TOE only through proxies and have no access to privileged files and processes.

52. TOE functions operate independently with no interaction between processes. Process separation is provided by separation of domains imposed by the operating system supported by the underlying hardware. The partitioning of the file areas is performed by the hardware. A domain is a partitioned file system area containing only the file system resources needed for a process to run. Each process will be assigned its own working directory with access rights limited to that process.

53. The TOE ensures that the TSP functions are invoked and succeed before any related operation is allowed to proceed. Packet filtering must always be performed and completed on any packet received before any further action is performed. In the same way, authentication of the administrator must be performed and completed prior to the administrator being able to invoke system management.

54. The TOE detects and records the occurrences of security relevant events. Audit logs cannot be modified and the audit mechanism cannot be turned off. System startup/shutdown, administrator logon/logoff, GUI startup/shutdown, changes to an administrator account by an administrator, changes to a rule by an administrator, audit log rollover, authentication of an unprivileged user, change of administrator password, prohibited IP packets, and changes of system time/date are always recorded in the audit log. It is also possible to configure auditing of rejected packets, establishment or termination of a connection, attempted use of FTP commands and alarms sent. The date and time of the event, type of event, subject identity, event outcome, requested destination address and port number are recorded in each case.

Delivery and Installation

55. The consumer receives the TOE as a shrink wrapped package clearly labelled as BorderWare Firewall Server Version 6.1.1. This will ensure that interference with the TOE will be detectable. It is sent by a shipping company (usually Federal Express) to the consumer. A licence pack is sent to the consumer with the TOE software package. This licence pack contains a serial number which the consumer has to use to obtain a product activation key from the Developer. This ensures that a third-party could not masquerade as the Developer and supply potentially malicious software.

56. The TOE has a number of configuration options which the consumer must perform in order to use the TOE. These options are described in the Administrative and Installation Guide [k]. The Evaluators were satisfied that all configuration options lead to a secure installation of the TOE.

User Guidance

57. User documentation was not relevant to the TOE.

58. The firewall administrator can configure the packet filtering rules, the proxies, servers and alarms. These should be configured to match the requirements of the Security Target [c] and the specific requirements of the organisation. The administrator should follow the guidance in the administration guidance documentation [k-n] in order to ensure that the TOE operates in a secure manner.

Misuse

59. The Evaluators found that the TOE provided a warning and alarm system documented in the BWClient GUI Help document [m] to notify the TOE administrator of a potentially insecure state. Regular examination of the TOE's audit logs would also help detect a potentially insecure state. The TOE also includes facilities to guard against failure caused by operational error due to power failure, log overflow and overflow attack and provides safeguards in the event of these errors occurring. Administrators should follow the guidance in the administration guidance documentation [k-n] in order to ensure that the TOE operates in a secure manner.

Developer's Tests

60. The TOE was installed and tested on 4 hardware platforms as specified in Annex A. The Evaluators agreed with the Certification Body prior to testing that tests should be conducted across all 4 platforms to test whether the hardware platform variations impact on the TOE security functions. In some cases the same test was repeated on all 4 hardware platforms. In these cases the Evaluators noted that the same results were achieved across all platforms. The Evaluators were satisfied that the hardware platform did not impact on the security functions of the TOE.

61. The TOE is designed to operate on Intel platforms. It does not rely on specific processor speed or RAM size, and therefore should operate on any Intel processor that provides the necessary security support services for FreeBSD UNIX in the following areas:

- C User and Kernel mode
- C Interrupts and Exceptions
- C Processor Execution levels
- C Memory Allocation
- C System clock

62. See Annex A to this report for the minimum recommended hardware specification of the TOE.

63. The Developer's testing was designed to test the security functions that are provided by or which relate to the use of the high-level design subsystems of the TOE. Unit tests were designed based on the high-level design subsystems of the product. For each high-level design subsystem the unit tests tested the TOE's IT security objectives and other objectives such as usability and performance.

64. The testing of the TOE's external interfaces as specified in the TOE's functional specification was performed by a subset of the unit tests which were mapped to the security functions in the functional specification. See Annex A to this report for details of the Developer's test environment.

65. The Developer's testing procedures started with master runs, then described Release Acceptance Criteria (RAC), followed by unit tests and then individual tests using test scripts. For each product release, a master run is defined. The master run consisted of an RAC test and one or more unit tests. An RAC test is defined for each type of product release, and consists of a pre-defined set of unit tests. A unit test is defined for a particular module of the product, or for a particular set of functions or features. The unit tests consisted of one or more test scripts.

66. The Evaluators examined all of the test scripts and confirmed that the actual test results were consistent with the expected test results. The expected results were also consistent with the actual results of the Evaluators' repeated sample of the Developer's tests.

Evaluators' Tests

67. The Evaluators sampled 37% of the Developer's tests. Tests were repeated for each high-level design subsystem and security mechanism using every external TOE interface. Known public domain vulnerabilities relevant to firewalls were also tested.

68. Each TOE security function was tested by at least one additional test devised by the Evaluators. During testing the Evaluators devised additional tests to check that it is not possible for Admin FTP to be used from an external network and that Admin FTP cannot be used to change file permissions on the FTP area on the server.

69. The Evaluators used the following tools during independent testing:

- C FreeBSD boot program
- C DOS 6.22 boot program
- C NMAP Version 2.3Beta8

70. NMAP Version 2.3Beta8 is a remote scanning tool used to aid the testing using its automated scanning capability. The results of the tests were verified manually.

71. The configuration of the Evaluators' test environment is described in Annex A.

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

72. After due consideration of the ETR [j], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that BorderWare Firewall Server Version 6.1.1, running on Intel platforms in the environment specified in Annex A, meets the specified CC Part 3 [f] augmented requirements incorporating Evaluation Assurance Level EAL4 for the specified CC Part 2 [e] conformant functionality in the specified environment.

73. The TOE contained 3 permutational cryptographic functions: password file encryption provided by DES and the administrator password and FTP-Admin authentication mechanisms. The administrator password and FTP-Admin authentication mechanisms were found to meet SoF-medium. DES is publicly known and as such it is the policy of the national authority for cryptographic functions, CESG, not to comment on its appropriateness or strength. Nevertheless, as the password file is protected by operating system access control, the password file is adequately protected and the encryption mechanism is not directly attackable.

Recommendations

74. Prospective consumers of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [c].

75. The TOE provides some features that were not within the scope of the evaluation as identified in the "TOE Scope" section above. The secure use of these features has thus not been considered in the evaluation. It is recommended that these features should not be used if the TOE is to comply with the evaluated configuration.

76. Only the evaluated product configuration, specified in Annex A, should be installed. The product should be used in accordance with its guidance documentation [k-n].

77. The product should only be used in accordance with the environmental considerations outlined in the Security Target [c].

78. Consumers should consider the threats not countered by the TOE when devising their Organisational Security Policy and may need to consider additional products to provide content checking and virus checking functionality not provided by the TOE.

79. The TOE is designed to operate on Intel processors (without reliance on the processor speed or RAM size). However, it is recommended that the TOE should be installed and operated on at least the minimum hardware specification identified in Annex A to this report.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

BorderWare Firewall Version 6.1.1

2. The supporting guidance documents evaluated were:

- C Installation and Administrative Guide [k]
- C BorderWare Firewall Server 6.1.1 Reference Guide [l]
- C BWClient Help GUI [m]
- C EAL4 Configuration guide for BorderWare 6.1.1 [n]

TOE Configuration

3. The TOE had the following configuration options:

- a. loading the TOE software from the CD-ROM or from the network; and
- b. allocating the size of the disk partition in which to install the TOE.

4. The TOE can be configured with 2 or 3 network interface cards for the internal and external networks and the SSN respectively. If the third network card is not installed, only the internal and external networks are installed.

5. The Evaluators concluded that no TOE configuration options affected the security of the TOE.

Environmental Configuration

6. The Developer's test environment consisted of a total of 6 systems. Each system comprised:

- C Intel processor, ranging from 400 MHZ Celeron to 600 MHZ Pentium III using 64, 128 or 256 MB RAM
- C Hard drives, ranging in capacity from 2.2 GB to 13 GB, including Small System Computer Interface (SCSI) and Integrated Drive Electronics (IDE) adapters
- C CD-ROM
- C 3.5 diskette drive
- C Monitor
- C Keyboard

- C Network cards, including popular 3COM cards and NE2000 compatibles

7. The Developer's test environment was located on its own network, and was connected to internal and external networks, supporting all of the possible test procedures and scenarios. For the purpose of testing the SSN feature of the firewall, a separate sub-network existed, to which one or more servers and workstations were connected as required.

8. The Developer's quality assurance department had several Microsoft Windows 95, Windows 98 and NT systems available for use both as clients and servers. Test clients were required to run BWClient, and to simulate normal client activity. Test servers were required to test passing traffic through the firewall. Both the test servers and test clients were connected on the internal, external or SSN networks connected to the test firewalls.

9. The specific configurations of the machines used during the Evaluators' tests for the TOE were:

- C Compaq Deskpro with 400 MHZ Intel Celeron processor, 64 MB RAM and 6 GB IDE hard disk
- C Compaq Proliant with 600 MHZ Intel Pentium III processor, 128 MB RAM and 9 GB SCSI hard disk
- C Dell Dimension L466C with 466MHz Celeron processor, 64 MB RAM and 6 GB IDE hard disk
- C Dell PowerEdge 1300 with 500 MHZ Pentium III processor, 256 MB RAM and 9 GB SCSI hard disk

10. The TOE is designed to operate on standard Intel hardware platforms. It includes device drivers to support the range of commonly used disk controllers (IDE, ATA and SCSI) and the majority of network interface cards on the market. The TOE does not rely on specific processor speed or RAM size and therefore, will operate on any Intel processor that satisfies the hardware dependencies.

11. The minimum recommended hardware specification for the TOE is as follows:

- C Intel Pentium Processor (133 MHZ)
- C 32 MB RAM
- C 1 Gbyte Hard Disk (SCSI or IDE)
- C 2 or 3 Network Interface cards from the supported list
- C CD-ROM drive
- C 3.5 inch floppy disk drive

12. The BWClient does not have any special requirements. It is a Windows based application that runs on any Win32 operating system (Windows 95, Windows 98 or Windows NT Version 4.0). As the BWClient communicates over the network to the BorderWare Firewall Server, it requires that the machine on which it is installed to have networking capability. It is recommended that Windows

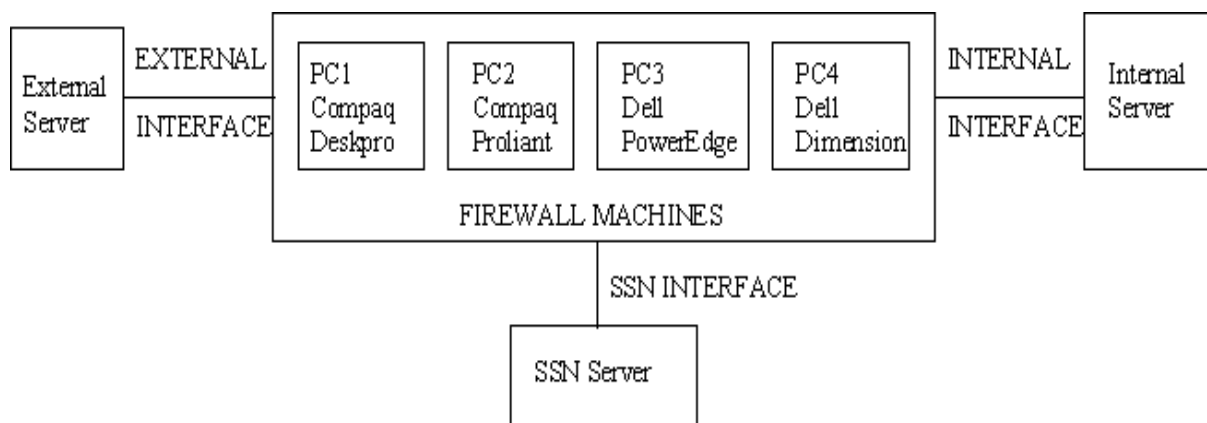
NT systems are patched to at least Service Pack 3. A copy of BWClient is included on the TOE distribution CD-ROM. In this evaluation BWClient was installed on the internal interface machine which ran Windows NT Version 4.0 Server with Service Pack 3 on a Compaq Deskpro machine with the following specification:

- C Intel Pentium Processor (200 MHZ)
- C 32 MB RAM
- C 1 Gbyte Hard Disk (SCSI)
- C 3 Network Interface cards from the supported list
- C CD-ROM drive
- C 3.5 inch floppy disk drive

13. The machine used during Evaluators' testing as representing the internal network had 32 MB of RAM and used the Microsoft Windows NT 4.0 Server Version 4.0 operating system with Service Pack 3. The machine representing the external network had 8 MB of RAM and used the Unix FreeBSD Version 3.2 operating system. The machine representing the SSN had 16 MB of RAM and also used the Unix FreeBSD Version 3.2 operating system.

14. The diagram below shows the architectural layout of the machines used for Evaluators' independent testing:

15. The firewall machines in the above diagram are not in series; only one firewall was used at a time. The machines represent the choices of firewall available.



(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. The TOE is an application-level firewall. It mediates information flows between clients and servers located on internal and external networks governed by the TOE. The TOE employs proxies to screen information flows. Proxy servers on the TOE, for inbound services such as FTP and Telnet, require authentication at the TOE by client users before requests for such services can be authorised. Thus, only valid requests are relayed by the proxy server to the actual server on the internal network.

2. The TOE delivers three security layers:

- C packet filtering
- C circuit level gateways
- C application level gateways

3. The packet filtering controls are performed at the operating system kernel level. By default, these security policy rules deny all inbound information flows. Only an authorised administrator has the authority to change the security policy rules.

4. The BorderWare Firewall Server operating system does not permit any operating system user logins. All direct interaction with the TOE to perform configuration and administration tasks is performed on the firewall server console, or via the Admin GUI on a client connected to the internal, protected network. The administrator is the only user who is able to directly interact with the TOE. Interaction with the TOE is transparent to all other users.

5. The administrator is able to perform basic configuration and administration of the firewall using the firewall server console, via the "Admin menu". Access to the console is physically protected and logically controlled through password protection. Full administration services are only provided through use of the Admin GUI at a client workstation. Use of the Admin GUI is protected by use of a password. A challenge/response Crypto Card authentication token (56 bit DES encryption) may be used, but this is outside the scope of the evaluation.

6. The outbound gateway provides transparent services to the user on the internal network. Multiple Address Translation is provided for inbound traffic received at the firewall to enable a number of IP addresses to be specified for servers within the SSN area, the de-militarised zone.

7. Transparent address translation is performed for all outbound traffic. Requests for connections from a client on the internal network to a server on the external network are directed by the client to the server's actual IP address. If the TOE is configured correctly, as the only connection between the internal and external networks, then the appropriate proxy for the requested service will be activated by the TOE (subject to successfully passing any appropriate identification, authentication or access controls) to handle that request. The proxy will ensure that the apparent source address of that connection is set to that of the TOE's external interface before any IP datagrams are transmitted on the external network. Inbound address translation is not transparent. An external entity must direct all traffic to an address assigned to the TOE's external interface. Subject to successful identification and authentication, this traffic can be relayed to an entity on the internal network. The address translation is augmented by the separate DNSs, which ensure that internal addresses are never disclosed to an external entity by domain name lookup.

8. When recorded, the audit trail data is stamped with the date and time information. Audit events include:

- C Every successful inbound and outbound connection
- C Every unsuccessful connection
- C Every successful and unsuccessful administrator authentication attempt

9. If the audit trail becomes filled, then the trail will be archived and a new audit trail initialised. If the limit of archived audit trails is reached, the oldest archive will be deleted to allow the current audit trail to be archived. This mechanism ensures that the partition on the TOE's disk reserved for audit information never becomes full, an event that could lead to failure to record audit information.

10. The TOE has predefined proxies and built-in servers. The following tables identify the predefined proxies and built in servers that are included within the scope of the evaluation.

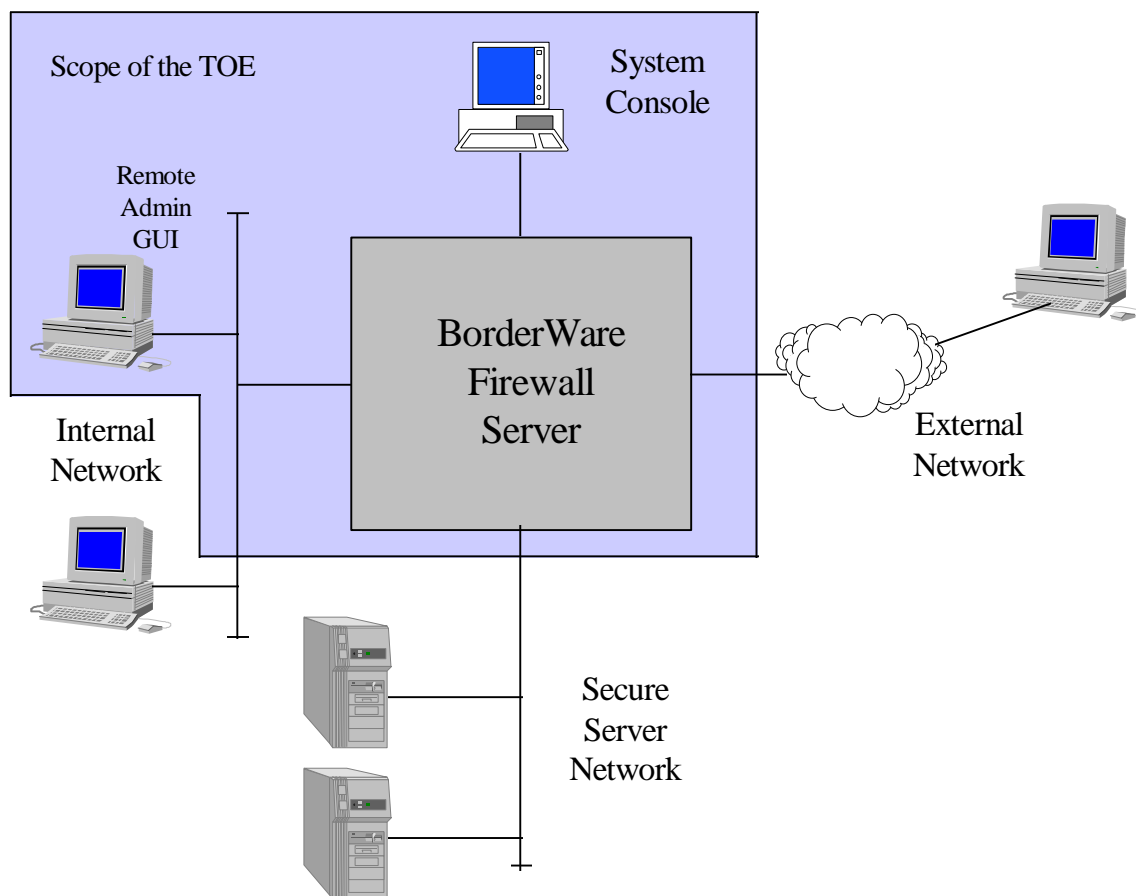
11. Services provided by predefined proxies that can be configured on the TOE within the scope of the evaluation are specified in the table below. The table heading identifies the direction of information flow provided by the services and the relevant information flow security policies. Only the Admin GUI on the internal network is subject to the AUTHENTICATED information flow security policy.

Internal->External (UNAUTHENTICATED or UNIDENTIFIED)	Internal->SSN (UNAUTHENTICATED or UNIDENTIFIED)	External-> SSN (UNAUTHENTICATED or UNIDENTIFIED)	SSN->External (UNAUTHENTICATED or UNIDENTIFIED)
America On-line	Finger	Anonymous FTP	FTP
Finger	FTP	Finger	Finger
FTP	Gopher	Ident	Ident
Gopher	Ident	NNTP	Ping
Ident	NetShow	SMTP Mail	POP Mail
NetShow	NNTP	WWW	SMTP Mail
NNTP	Ping		WWW
Ping	POP Mail		
POP Mail	RealAudio		
RealAudio	SMTP Mail		
Telnet	WWW		
Whois			
WWW			

12. Services provided by servers that can be configured on the TOE server within the scope of the evaluation are provided in the table below.

Internal	External	SSN
Finger	Anonymous FTP	Anonymous FTP
FTP	Finger	Finger
Ident	Ident	Ident
Ping	Ping	Ping
POP Mail	SMTP Mail	POP Mail
SMTP Mail	Traceroute response	SMTP Mail
Traceroute response	WWW	Traceroute response
WWW		WWW

13. The figure below provides an architectural overview of the BorderWare Firewall Server. It identifies the network interfaces and the management interfaces via the system console and Remote Admin GUI. The shaded area provides the scope of the TOE covered by the evaluation.

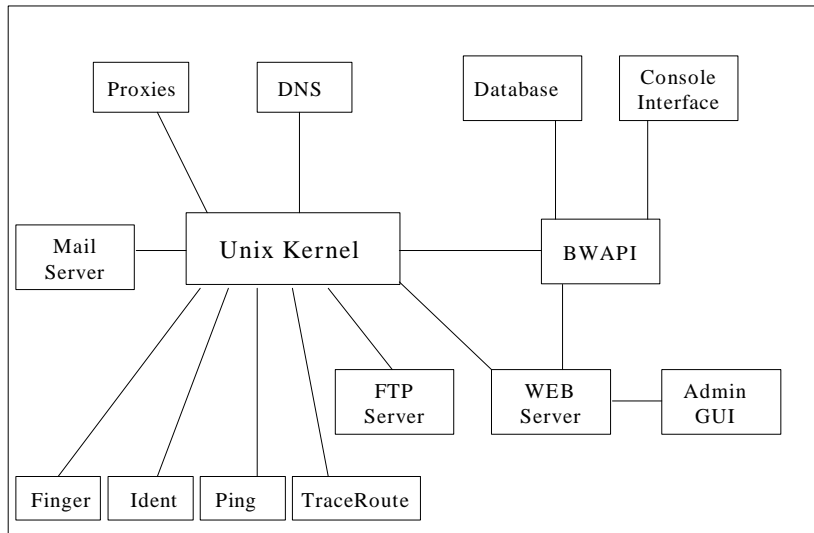


14.
 The
 TOE

includes the operating system based on FreeBSD-3.3-Release. The kernel has all redundant devices

removed including shell access and UNIX login prompt. The TOE is comprised of a number of subsystems described in the high level design. Each subsystem is further refined into modules in the low level design.

15. The following diagram shows the subsystems described in the high level design and relationships between them:



16. The BWAPI subsystem is used to handle requests for firewall management functions from the console interface and the remote Administration GUI. Management functions are functions used to modify or view the firewall configuration, run diagnostic tests and view log files.

17. The kernel provides the environment in which processes and subsystems execute. The process environment provides controlled access to files, the IP stack and other processes. The IP stack includes a packet filter that discards or redirects packets. It is responsible for passing data between proxy and server subsystems and other hosts on the network. The kernel also provides Transmission Control Protocol (TCP) connection state, TCP option negotiation, TCP flow control, resending of unacknowledged TCP packets, and handling and generation of Internet Control Message Protocol (ICMP or “ping”) error messages.

18. The database subsystem provides a means of information storage and retrieval for other subsystems.

19. The system console subsystem provides a user interface for the firewall administrator to configure and maintain the other subsystems.

20. The Administration GUI subsystem is a Windows 95, 98 or NT application that allows an administrator to manage the BorderWare Firewall Server from a remote PC. Remote management includes the configuration of firewall servers such as DNS and Mail, proxies, authorised remote administration and examination of logs and diagnostic information.

21. The Proxies subsystem exchanges IP traffic between the TOE’s network interfaces. Where appropriate, traffic is filtered or reinterpreted.

22. The DNS subsystem provides translation between Internet host names and addresses. It also provides other resource records on hosts and domains.
23. The FTP Server subsystem provides a secure public file sharing system and allows an administrator to upload and download certain configuration to the firewall.
24. The Web Server subsystem provides 2 distinct services on the firewall to allow remote management access to public static HTML documents.
25. The Mail Server subsystem comprises a Simple Mail Transfer Protocol (SMTP) mail server and a Post Office Protocol (POP) mail server. The SMTP server is used to provide a secure means of passing SMTP mail from the Internet to the internal network, and it may be used as a default mail gateway to pass mail from the internal network to the Internet. The POP mail server is used for relaying Internet mail.
26. The Finger Server subsystem implements the finger protocol and provides a static, configurable information message. The finger service does not provide any information about individual users.
27. The Ident Server subsystem is used to allow the TOE to process requests for the identity of users on external networks. The TOE does not implement an Ident client to identify the TOE or users on the internal network.
28. The Traceroute Response Server enables the TOE to respond to Traceroute requests (for routing information of an IP packet). The TOE does not allow Traceroute probes to pass from one network interface to another.
29. The Ping Server subsystem provides responses to ICMP echo requests. Ping is a low level diagnostic tool designed to test if a system is reachable and responding.

(This page is intentionally blank)