

UK ITSEC SCHEME CERTIFICATION REPORT No. P123

VCS Firewall

Version 3.0

running on specified Intel platforms

Issue 1.0

March 1999

© Crown Copyright 1999

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.

Trademarks:

VCS Firewall is a trademark of The Knowledge Group.
Pentium is a registered trademark of Intel Corporation.
Ethernet is a registered trademark of Xerox Corporation.

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

CERTIFICATION STATEMENT

The Knowledge Group's VCS Firewall is an Internet firewall providing both packet filtering and application proxies. It is a product designed to manage access between trusted and untrusted networks which can mediate communications between up to 4 networks and can manage traffic between all pairs of networks.

As detailed in this report, VCS Firewall Version 3.0 has been evaluated under the terms of the UK ITSEC Scheme and has met the specified CC Part 3 requirements of Evaluation Assurance Level EAL1, augmented by ACM_CAP.2 for the specified CC Part 2 extended functionality when running on the specified Intel platforms in the specified environment.

Originator	CESG Certifier
Approval	CESG Head of the Certification Body
Authorisation	CESG Senior Executive UK ITSEC Scheme
Date authorised	31 March 1999

(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

 Product Environment 2

 Protection Profile Conformance 2

 Evaluation 3

 General Points 4

II. EVALUATION OUTCOME 5

 Certification Result 5

 Recommendations 5

ANNEX A: EVALUATED CONFIGURATION 9

ANNEX B: SECURITY ARCHITECTURE 13

(This page is intentionally left blank)

ABBREVIATIONS

BIOS	Basic Input/Output System
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ITSEC	Information Technology Security Evaluation Criteria
MIME	Multipurpose Internet Mail Extensions
NVRAM	Non-Volatile Random Access Memory
OSP	Organisational Security Policy
SMTP	Simple Mail Transfer Protocol
SoF	Strength of Function
TCP	Transmission Control Protocol
TELNET	TELEcommunications NETwork Protocol
TOE	Target of Evaluation
UDP	Universal Datagram Protocol
UKSP	United Kingdom Scheme Publication
VCS	Very Clever Software

(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. VCS Firewall EAL1 Security Target,
The Knowledge Group,
GE298FC/ST, Issue 1.3, 18 December 1998.
- d. Common Criteria Part 1,
Common Criteria Implementation Board,
CCIB-97/081R, Version 2.0, Draft, 19 December 1997.
- e. Common Criteria Part 2,
Common Criteria Implementation Board,
CCIB-97/082R, Version 2.0, Draft, 19 December 1997.
- f. Common Criteria Part 3,
Common Criteria Implementation Board,
CCIB-97/083R, Version 2.0, Draft, 19 December 1997.
- g. LFF/T140 Evaluation Technical Report,
IBM Global Services CLEF,
Issue 1.0, 15 January 1999.
- h. Common Methodology for Information Technology Security Evaluation,
Part I: Introduction and General Model,
Common Evaluation Methodology Editorial Board,
Version 0.6, CEM-97/017, September 1997.
- i. Common Methodology for Information Technology Security Evaluation,
Part II: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
Version 0.6, CEM-99/008, January 1999.
- j. Interim CC Evaluation Manual,
Common Evaluation Methodology UK Support Group,
UKSP05.CCINT, Version 2.0, 19 June 1998.
- k. Harmonised Information Technology Security Evaluation Criteria,

Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

- l. Information Technology Security Evaluation Manual,
Commission of the European Communities,
Version 1.0, 10 September 1993.
- m. Manual of Computer Security Evaluation, Part I, Evaluation Procedures,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 3.0, October 1994.
- n. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 2.0, 30 July 1997.
- o. VCS Firewall for Windows System Guide,
The Knowledge Group,
Version 3, Revision 3, 6 April 1998.
- p. VCS Firewall Proxy Functional Specification,
The Knowledge Group,
VCS/PROXY/FS/01, Issue 003, 26 January 1998.
- q. VCS Firewall Multi-Platform Rationale,
The Knowledge Group,
VCS/FW/MPR/01, Issue 001, 10 March 1998.
- r. The Intel Architecture Software Developer's Manual, Volume 1 (Basic Architecture),
Intel Corporation,
Order No: 243190, <ftp://download.intel.com/design/PentiumII/manuals/24319001.pdf>.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the IT security evaluation of VCS Firewall Version 3.0 to the Sponsor, The Knowledge Group, and is intended to assist potential consumers when judging the suitability of the product for their particular requirements.

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

Evaluated Product

3. The version of the product evaluated was:

VCS Firewall Version 3.0.

The evaluated configuration, including the product's supporting guidance documentation [o], is detailed more fully in Annex A. This product is also described in this report as the Target of Evaluation (TOE). The Developer was The Knowledge Group.

4. The TOE is an Internet firewall providing both packet filtering and application proxies. It is a product designed to manage access between trusted and untrusted networks which can mediate communications between up to 4 networks and can manage traffic between all pairs of networks.

5. The TOE includes a minimal installation of RedHat Linux Version 5.2 with Netscape Navigator Version 2.0. This software is supplied as part of the TOE.

6. Packet filtering for TCP/IP, UDP and ICMP is performed using the Linux Packet Filter package. The built-in support for strong authentication is outside the scope of the evaluation.

7. The TOE provides proxies for TELNET, HTTP, FTP and Mail Store and Forward. A generic proxy is also provided. The TOE has audit logging and alarm raising capabilities and is accessed either locally or remotely at a specified IP address via a Graphical User Interface.

8. The Security Target [c] specifies the TOE's security environment, including the threats, Organisational Security Policy (OSP) requirements, TOE environment and secure usage assumptions. The Security Target also fully specifies the security objectives that counter these threats, together with the functional requirements and security functions that implement these objectives.

9. Most of the functional requirements are taken from Common Criteria (CC) Part 2 [e]; use of this standard facilitates comparison with other evaluated products. Some of the functional requirements are extended functional requirements, not taken from CC Part 2. These were specified for captive user logons, audit log file and audit alarms. An overview of CC is given in CC Part 1 [d].

10. The security policy operated by the TOE is enforced by the security functions and is thus evident from them. The Security Target [c] confirms that the OSP for any system using the TOE should include statements to cover the following secure usage assumptions:

- a. procedures will exist in the OSP to ensure that users do not bypass the TOE by connecting directly to a remote network; and
- b. procedures will exist in the OSP to ensure that an attempt to access the TOE by an unauthorised individual will be detected.

11. The TOE implements re-usable passwords, generated by the user, in the cryptographic function that meets functional requirement FIA_UAU.2 (User Authentication Before Any Action).

12. The product's security architecture is outlined in Annex B.

Product Environment

13. The TOE was evaluated with reference to its specified environment. The secure usage assumptions and environmental objectives for the TOE are specified in the Security Target [c]. In addition to those detailed in paragraph 10 above, the secure usage assumptions are:

- a. The passwords required to access the Administrator account on the VCS Firewall and the Linux root account should be recorded and stored in a secure location. This record should be kept up to date when the password is changed. Access to the Administrator account should only be granted to the Firewall Administrator and access to the Linux root account should only be granted to the System Administrator.
- b. The PC on which the VCS Firewall is running should not be used for any other purpose.

14. The TOE is designed to run on any IBM-compatible PC containing an Intel 80486 or higher processor. Support is provided for any IBM-compatible PC Network Interface Card that can operate in conjunction with the Linux RedHat Version 5.2 operating system and TCP/IP.

15. To demonstrate the required assurance, the TOE was evaluated on a RESEDA Pentium 166 and on a 350 MHz AMD K6-2 platform. The platform configuration used to support the evaluation is given in Annex A. Other than for supporting protection mechanisms, the security functions of the VCS Firewall place no reliance on any security functionality provided by the PC or Network Interface Cards.

Protection Profile Conformance

16. The Security Target did not claim conformance to any Protection Profile.

Evaluation

17. 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 the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry on behalf of Her Majesty's Government.

18. 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 in CC Part 3 [f].

19. The Security Target [c] specifies the assurance requirements for the resultant evaluation. The assurance incorporated predefined Evaluation Assurance Level EAL1 augmented by ACM_CAP.2 (configuration management). CC Part 3 [f] describes the scale of assurance given by predefined Evaluation Assurance Levels EAL0 to EAL7, where EAL0 represents no assurance.

20. As the only operators of the TOE were administrators, user guidance documentation was not required and user guidance (AGD_USR.1) was therefore not applicable.

21. The specified assurance of EAL1 does not require the Strength of Function (SoF) to be assessed for cryptographic functions. No minimum SoF claim was therefore appropriate and no cryptographic assessment of the Linux RedHat Version 5.2 password mechanism was performed.

22. Testing addressed the following to the EAL1 assurance requirements:

- a. security functions specified by the Security Target;
- b. potential vulnerabilities of which there is knowledge in the public domain;
- c. potential vulnerabilities associated with the password functionality;
- d. potential vulnerabilities associated with the use of the TOE beyond 2000 AD; and
- e. other potential vulnerabilities which became evident during the course of the evaluation.

23. The TOE was tested on the RESEDA platform identified in Annex A in a configuration which consisted of one external network and one internal network. The Intel clone identified in Annex A was used to specifically test the TOE for potential vulnerabilities associated with the use of the TOE beyond 2000 AD. The Evaluators were satisfied that VCS Firewall Version 3.0 supports up to 4 Network Interface Cards as claimed in the Security Target [c].

24. The evaluation included the examination of the VCS Firewall Multi-Platform Rationale [q] to assess the claims related to the hardware platforms. Architectural details of the platforms are provided in Annex B. The evaluation confirmed that the TOE will run on any IBM-compatible PC containing an Intel 80486 or higher processor. The evaluation also confirmed that the TOE supports

any IBM-compatible PC Network Interface Card that supports Linux RedHat Version 5.2 and TCP/IP as listed in Annex A.

25. Although the TOE was evaluated against assurance criteria taken from those agreed internationally in CC Part 3 [f], the evaluation was performed prior to the finalisation of the Common Evaluation Methodology (CEM). To ensure an appropriate application of the criteria, available drafts of CEM [h, i] were consulted and the current UK CC interpretations in the Interim CC Evaluation Manual [j] were checked. Also, as the CC are broadly equivalent in many respects to those of the IT Security Evaluation Criteria (ITSEC) [k], the IT Security Evaluation Manual [l], as elaborated in UKSP 05 [m, n], was followed where appropriate. Otherwise, the criteria were applied in a manner consistent with both this basis and the overall objectives of EAL1 stated in CC Part 3.

26. The Certification Body monitored the evaluation which was carried out by the IBM Global Services Commercial Evaluation Facility (CLEF). The evaluation was completed in January 1999 when the CLEF submitted the final Evaluation Technical Report (ETR) [g]. Further information relevant to testing the use of the TOE beyond 2000 AD was required before this Certification Report could be produced by the Certification Body.

General Points

27. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) that exploitable vulnerabilities remain undiscovered.

28. The evaluation addressed the security functional requirements and security functions claimed in the Security Target [c], with reference to the assumed environment specified in the Security Target. The evaluated configuration 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.

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

II. EVALUATION OUTCOME

Certification Result

30. After due consideration of the ETR [g], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that VCS Firewall Version 3.0, running on the specified Intel platforms in the specified environment, meets the specified CC Part 3 requirements of Evaluation Assurance Level EAL1, augmented by ACM_CAP.2 for the specified CC Part 2 [e] extended functionality.

Recommendations

31. The product should only be used in accordance with the environmental considerations outlined in the Security Target [c], which details the TOE environment and secure usage assumptions. Particular care should be taken that the product is configured and used in accordance with the guidance documentation [o].

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

- a. an OSP should be defined prior to any attempted installation or implementation of the firewall;
- b. only an approved group of administrators should have physical access to the firewall hardware;
- c. the firewall should be configured in accordance with the OSP; and
- d. to maintain an evaluated configuration, the default configuration of the operating system must not be subject to any changes that would affect the firewall's security objectives.

33. Potential consumers should note that the specified assurance of EAL1 does not require the SoF to be assessed for cryptographic functions and that the SoF of the Linux RedHat Version 5.2 password mechanism has therefore not been assessed. Although the evaluation included some tests for obvious potential vulnerabilities, consumers should confirm that this password mechanism is adequate to meet the intended use of the product prior to purchase.

34. Potential administrators should consider carefully the use of remote administration and re-usable passwords, particularly in relation to their use over an untrusted external network. Re-usable passwords should only be configured and used over a network when there is sufficient protection on the network to prevent eavesdropping (electronically or visually) of such passwords. The Certification Body recommends that the OSP specifies procedures for the use of remote administration and re-usable passwords, including the frequency of password changes and the method of password selection (for example, passwords to be alphanumeric and of minimum length 8 characters). General guidance on passwords is provided in the guidance documentation [o].

35. Administrators should note that it is essential that the passwords for the Linux root and firewall Administrator accounts are stored securely to avoid unauthorised changes to the configuration of the TOE.
36. Administrators should be aware that the firewall does not prevent hostile users on the internal network colluding with hostile attackers on the external network if the user is authorised to access and send the information to external hosts.
37. Potential administrators should note that any traffic on the internal network not routed through the firewall falls outside the administrator's control. Thus the firewall will not counter threats to the security of the internal network from authorised users of the internal network.
38. Administrators should be aware that the TOE does not counter the threat that the firewall could be bypassed by connecting together the internal network directly to an external network. It is recommended that the TOE is placed in a physically secure environment to which only authorised personnel have access and that internal users are prevented from connecting their workstations or servers to the external network by any link (eg a modem) that does not pass through the firewall (see the Security Target [c], secure usage assumption U.BYPASS).
39. The Security Target recommends that it is useful to check regularly that there has been no tampering with the network connections. The Certification Body also recommends that physical protection of the TOE is provided to minimise the risks associated with tampering of the TOE and its environment (ie hardware platform, including the PC Basic Input/Output System (BIOS)).
40. Potential consumers should note that the administrators of the firewall are assumed to be trusted individuals who are appropriately vetted and trained. The TOE does not counter threats from careless, negligent or hostile administrators. It is recommended that appropriate measures, including regular, independent audits of the firewall configuration, be taken to counter these threats.
41. Firewall flow policies are complex and they need to be tailored to fit specific requirements. Consumers of the TOE should ensure that administrators are competent to determine the firewall flow policies to be implemented or have access to people who are competent to determine such policies.
42. Potential consumers of the TOE should be aware that 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.
43. Potential consumers should note that it is not possible for any firewall to counter all types of 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.

44. 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). This threat should be considered when defining the OSP.
45. To reduce the potential impact of IP source address spoofing and Session Hi-jacking, it is recommended that the OSP states what executable software is authorised to be received through the firewall from the external network. Corresponding operational procedures to quarantine such software may also be required.
46. To detect whether IP source address spoofing or Session Hi-jacking has affected the firewall, it is recommended that a backup of the firewall in its initial operational configuration is retained and used for comparison at periodic intervals. The OSP should state when this comparison is to be made.
47. Potential consumers should be aware that the TOE does not differentiate between HTML and embedded active content such as Java or ActiveX that may be transmitted using HTTP. The decision on whether to allow HTML, Java or ActiveX through the firewall must be specified in the OSP. If active content is to be prevented from being imported from the external network, the HTTP proxy should be disabled, unless alternative security measures are available to counter any content-based threat.
48. Potential consumers should be aware that the TOE does not detect viruses. It is recommended that executable programs attached to incoming mail messages should be virus checked. Automatic explosion or execution of MIME-encoded attachments within mail messages should also be disabled.
49. It is recommended that the firewall audit log is inspected on a regular basis (eg during each operational day) and that the frequency of inspection is stated in the OSP. Appropriate action must be taken to ensure that there is sufficient free disk space to allow audit logging to continue without any loss of audit records. It is also recommended that the firewall is regularly monitored for audit alarms and that the OSP states the action to be taken when such alarms are detected.
50. Prospective consumers of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [c]. Only the evaluated product configuration, specified in Annex A, should be installed on a single platform and used as described in the Security Target.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:
 - VCS Firewall Version 3.0.
2. The supporting guidance document evaluated was:
 - C VCS Firewall for Windows System Guide [o]

TOE Configuration

3. The specific software configuration of VCS Firewall Version 3.0 included:
 - C RedHat Linux Version 5.2, Kernel Version 2.0.36
 - C Netscape Navigator Version 2.0
4. The TOE is delivered with Netscape Navigator and with the operating system already set to the minimal configuration. No other software, including any other Linux software, must be added to this configuration.

Environmental Configuration

5. The specific hardware configuration of the machine used for the Evaluators' tests included:
 - C RESEDA 166 MHz Pentium processor
 - C 64 MB RAM
 - C 2 GB IDE drive
 - C 2 3Com 3C509 Network Interface Cards (Ethernet adapters)
6. The environmental configuration included any IBM-compatible PC containing an Intel 80486 or higher processor. The environmental configuration also included any IBM-compatible PC Network Interface Card that supports RedHat Linux Version 5.2 and TCP/IP as listed in paragraph 11 below. An evaluated configuration may include a maximum of 4 such Network Interface Cards.
7. In an evaluated configuration, the PC hardware must include RAM in the range of 32 - 512 MB. The PC hardware must include at least 1GB of disk storage.
8. There is no limit to the total system disk storage within the evaluated configuration. Disk configurations of any size showing more than 1024 (mapped) cylinders via the BIOS require the /boot directory to be created in a separate filesystem partition, contained entirely at addresses below logical cylinder number 1024. The relevant installation procedures are described in the System Guide [o].

9. The evaluated configuration includes any Intel Pentium variant and clone that is a member of the IA-32 family complying with the architecture specified in The Intel Architecture Software Developer's Manual, Volume 1 (Basic Architecture) [r]. Details of the current processors complying with this architecture are available in the Developer Manuals supplied by Intel.

10. For Year 2000 testing of the TOE, the TOE was installed on an Intel clone platform which fell within the evaluated configuration. The specific hardware configuration was:

- C 350 MHz AMD K6-2 processor
- C 128 MB RAM
- C 4 GB SCSI drive
- C 1 SMC Ultra Network Interface Card (Ethernet adapter)

Network Interface Cards

11. The evaluated configuration includes the following Network Interface Cards:

- C 3Com: 3c503 3c505 3c507 3c509 3c515 3c590 3c592 3c595 3c597 3c900 3c905
- C Allied Telesis AT1700
- C Fujitsu FMV-181/182/181A/182A/183/184/183A/184A
- C KINGSTON
- C Linksys
- C ZNYX342
- C SMC8432
- C SMC9332 (w/new SRAM)
- C ZNYX31[45]
- C ZNYX346 10/100 4 port
- C D-Link de600
- C D-Link de620
- C DEC: DE425 TP/COAX EISA
- C DE434 TP PCI
- C DE435 TP/COAX/AUI PCI
- C DE450 TP/COAX/AUI PCI
- C DE500 10/100 PCI Fasternet
- C DC21040 (no SRAM)
- C DC21041[A]
- C DC21140[A]
- C DC21142
- C DC21143
- C DEPCA
- C DE100
- C DE101
- C DE200 Turbo
- C DE201 Turbo
- C DE202 Turbo
- C DE203 Turbo
- C DE204 Turbo

C	DE205 Turbo
C	DE210
C	DE422
C	Digi RightSwitch SE-X
C	Cabletron E2100 series
C	HP PC-LAN
C	Hewlett Packard PC LAN (27****) plus
C	HP J2585B 10/100 Mbit/s PCI Busmaster
C	HP J2585A 10/100 Mbit/s PCI
C	HP J2970 10 Mbit/s PCI Combo 10base-T/BNC
C	HP J2973 10 Mbit/s PCI 10base-T
C	HP J2573 10/100 ISA
C	Compex ReadyLink ENET100-VG4 10/100 Mbit/s PCI / EISA
C	Compex FreedomLine 100/VG 10/100 Mbit/s ISA / EISA /
C	Intel EtherExpress 16
C	Intel EtherExpress Pro/10
C	Intel EtherExpress Pro 100B
C	Allied Telesis AT1500 and HP J2405
C	NE2100/NE2500
C	NE1000 and clones
C	NE2000 and clones
C	PCnet32
C	PCnetPCI
C	RTL8129
C	RTL8139 PCI
C	SMC EtherPower II 9432 PCI adapter
C	SMC Ultra
C	SMC EtherEZ
C	SMC Ultra32C
C	SMC 9000 series
C	ThunderLAN
C	Digital "Tulip"-based cards (21*4* chipset)
C	WD8003
C	WD8013
C	Packet Engines G-NIC PCI Gigabit Ethernet adapter

Non-Evaluated Components

12. The following features of the TOE were outside the scope of the evaluation:

C	Strong Authentication (SecurID)
C	Radius

(This page is intentionally left blank)

ANNEX B: SECURITY ARCHITECTURE

TOE Architecture

1. VCS Firewall Version 3.0 exists as a single, self contained component, as viewed by the user in its installation and operation. Its internal security architecture was not visible at the EAL1 level of assurance.

2. The interfaces to the TOE were as follows:

C	Partition Command interface
C	Network interface cards
C	External Domain Name Service
C	User Authentication Method
C	Mail proxy
C	FTP and TELNET services
C	HTTP proxy
C	Generic proxy
C	Packet filtering

3. The TOE Security Functions were identified in the Functional Specification [p] and System Guide [o] as comprising the following 6 programs which form the packet filtering and proxy system:

C	tcpaddvral	-	address validation for incoming connection
C	telnet-proxy	-	the TELNET proxy
C	ftp-proxy	-	the FTP proxy
C	connect-through	-	a "plug-through" proxy
C	smtp	-	incoming mail handler
C	smtp-deliver	-	which passes the incoming mail queue to the mail delivery agent

Platform Variations

4. There are 2 main variations across different IBM-compatible PCs that could potentially affect software security - the PC BIOS type and the processor type. The BIOS provides the functions of system configuration (stored in NVRAM), system diagnosis, stage 1 of bootstrapping an operating system, I/O functions and timer functions available to the operating system once running.

5. System configuration is concerned with hard disk type, memory size, I/O address and interrupt setting for on-board peripherals and time setting. There are no variations across processor type that are security relevant to the VCS Firewall.

6. System diagnosis on IBM-compatible PCs is basic and generally consists of a memory check and verification that key peripherals such as keyboard and hard disk drive are operational. System diagnosis is not security relevant to the VCS Firewall.

7. The operating system bootstrap contained in PC BIOSs is simple and fairly standardised. Since there are 2 further bootstrap programs loaded from hard disk (installed by the VCS Firewall installation) before the operating system is fully loaded, different first-stage bootstrap programs are not security relevant to the VCS Firewall.

8. The I/O and timer functions are, in general, unused by the Linux operating system under which the VCS Firewall operates, and therefore any variations can be excluded from the evaluation. The one exception to this is acquiring system time at startup, which (as long as the correct time has been set) has no impact on VCS Firewall security.

9. All Intel processors from the 80386 and upwards are members of the IA-32 family of Intel processors that utilise the same basic (4 ring) protection architecture. The Linux operating system is built on this architecture and all Intel and instruction-set compatible processors implement this architecture. The only other security relevant variation between processors is in their handling of illegal or unimplemented instructions, but no such instructions are known to exist in VCS Firewall.

10. A wide range of network interface cards are supported by the VCS Firewall. This has been achieved by the design of a common interface to the operating system or PC BIOS for all card drivers. This interface is as close to the physical interface as possible while allowing for different interface cards. None of the supported network interface card drivers modify the data passed to or from the external connector. The drivers are only responsible for driving the network controller providing error detection and recovery and arbitration of data to be transmitted. The use of a common interface at such a low level avoids changes in cards having any effect on system security as evaluated by the EAL1 process.

11. No VCS Firewall security functionality is implemented in the network interface card or driver. The VCS Firewall packet filters and proxies are all implemented in software that runs on the PC processor. The network interface card and driver is only responsible for the implementation of the TCP/IP communications.