UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P185

Sidewinder™ G_2 Firewall™

Version 6.0
running on specified platforms

Issue 1.0

May 2003

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

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

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

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

* Whilst the Arrangement has not yet been extended to address ALC_FLR.2, a working agreement exists amongst Parties to the Arrangement to recognise the Common Evaluation Methodology ALC_FLR supplement (reference [h] in this report) and the resultant inclusion of ALC_FLR.2 elements in certificates issued by a Qualified Certification Body.

Trademarks:

CERTIFICATION STATEMENT

Sidewinder G_2 Firewall, from Secure Computing Corporation, is a software firewall incorporating a hardened operating system. It provides access control of communication and information flow between two or more networks, using application-level proxy and packet-filtering technology.

Sidewinder G_2 Firewall Version 6.0 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 with ALC_FLR.2, for the specified Common Criteria Part 2 extended functionality when running on the specified platforms.

Sidewinder G_2 Firewall Version 6.0 has also met the requirements of the US DoD Application-level Firewall Protection Profile for Basic Robustness Environments when running on the specified platforms.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body, UK IT Security Evaluation and Certification Scheme
Date authorised	19 May 2003

(This page is intentionally blank)

TABLE OF CONTENTS

(This page is intentionally blank)

ABBREVIATIONS

ACL	Access Control List
BSD	Berkeley Software Distribution
CC	Common Criteria
CCIMB	Common Criteria Interpretation Management Board
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CLI	Command Line Interface
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IDE	Integrated Drive Electronics
IP	Internet Protocol
MMU	Memory Management Unit
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
PCI	Peripheral Component Interconnect
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SCSI	Small Computer System Interface
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SoF	Strength of Function
SSH	Secure Shell
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UDP	User Datagram Protocol
UKSP	United Kingdom Scheme Publication
URL	Uniform Resource Locator
VPN	Virtual Private Network

(This page is intentionally blank)

REFERENCES

a. Sidewinder G_2 Firewall Version 6.0 Security Target,
Secure Computing Corporation,
PN 00-0937193-G, 12 May 2003.

b. Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Common Criteria Interpretation Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements,
Common Criteria Interpretation Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
Common Criteria Interpretation Management Board,
CCIMB-99-033, Version 2.1, August 1999.

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

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

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
CEM-99/045, Version 1.0, August 1999.

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

i. Evaluation Technical Report, Sidewinder G_2 Firewall Version 6.0,
Syntegra CLEF,
LFS/T446/ETR, Issue 1.0, 11 March 2003.

j. Sidewinder G_2 Firewall Startup Guide,
Secure Computing Corporation,
PN SWOP-MN-STRT60-A, January 2003.

k. Sidewinder G_2 Firewall Version 6.0 -
EAL4+ Common Criteria Evaluated Configuration Guide,
Secure Computing Corporation,
PN 86-0937726-D, March 2003.

l. Sidewinder G_2 Firewall Administration Guide,
Secure Computing Corporation,
PN SWOP-MN-ADMN60-A, January 2003.

m. US DoD Application-level Firewall Protection Profile for Basic Robustness Environments,
Version 1.0, 22 June 2000.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Sidewinder G_2 Firewall Version 6.0 to the Sponsor, Secure Computing 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 evaluated product consists of :

- SecureOS (an operating system)
- a firewall application
- COBRA (a firewall administration Graphical User Interface (GUI) application)

4. The version of the product evaluated is Sidewinder G_2 Firewall Version 6.0.

5. The product is also described in this report as the Target of Evaluation (TOE) and as 'Sidewinder'. The Developer was Secure Computing Corporation.

6. The TOE is a software firewall incorporating a hardened operating system. It provides access control of communication and information flow between 2 or more networks, using application-level proxy and packet-filtering technology.

7. The TOE contains SecureOS, which is an extended version of the Berkeley Software Distribution (BSD) UNIX operating system employing Secure Computing Corporation's Type Enforcement security technology. Type Enforcement protects the TOE by separating all processes and services. The COBRA GUI runs on a separate Microsoft Windows NT or Windows 2000 workstation, connected to the firewall platform by a dedicated and physically protected network.

8. Sidewinder is a network security gateway that allows an organisation to connect to the Internet, while protecting the systems on its internal network from unauthorised users and network attackers. The TOE is aware of application-specific protocols, and can filter data based on content. It also has packet filter capability, to restrict traffic based upon source and destination address. It provides a set of Internet services and proxies.

9. Annex A provides details of the evaluated configuration of the TOE.

10. Annex B provides an overview of the TOE's security architecture.

TOE Scope

11. The FTP, HTTP (non-caching), SMTP, Telnet, Generic TCP (finger and daytime) and Generic UDP (daytime) proxies are all included within the scope of the evaluation.

12. Other protocol aware proxies provided by the product were excluded from the scope of the evaluation.

13. The product also provides the following functionality that was specifically excluded from the scope of the evaluation:

- cryptographically protected remote administration[1]
- on console administration[2]
- direct login to a Sidewinder via Telnet or Secure Shell (SSH)
- Virtual Private Network (VPN)
- cloning
- failover
- Uniform Resource Locator (URL) Filtering
- mail filtering
- policy acceleration network cards
- built-in servers (e.g. SSH Daemon (SSHD) server)

14. The evaluation platform for the firewall is an Intel Pentium processor based computing platform (discussed further below under the heading 'Platform Issues') with three network interfaces as follows:

a. two to communicate with the networks for which the firewall mediates communication and information flow; and

b. one to communicate with the platform hosting the COBRA GUI.

15. The recommended evaluation platform hardware configuration requirements are identified on the Developer's website (www.securecomputing.com) as follows:

- CPU type: Intel Pentium II (minimum), Pentium III, Pentium 4 or Xeon
- CPU speed: 600MHz (minimum)
- RAM: 512MB (minimum)
- hard disk: SCSI 9GB (minimum)
- CD-ROM drive: IDE or SCSI (used to install the TOE software)
- 3.5? 1.44MB floppy disk drive (used to create a backup of the configuration)
- network: 2 network connections (minimum)

[1] The evaluation included remote administration across a dedicated, physically protected network. Remote administration over physically unprotected networks was excluded from the scope of the TOE.

[2] The console is required for installation of the firewall. However the console Command Line Interface (CLI) was excluded from the scope of the TOE, as the COBRA GUI was included to support all post-installation administrator functionality.

- SVGA video (display monitor)
- US keyboard

16. The TOE's operational environment includes:

a. a commercially-available, single-use authentication server that is compatible with Sidewinder (eg SafeWord from Secure Computing Corporation); and

b. an Intel Pentium processor based computing platform with Windows 2000 or Windows NT operating system, that supports the COBRA GUI.

Protection Profile Conformance

17. The Security Target [a] claims conformance to the US DoD Application-level Firewall Protection Profile for Basic Robustness Environments [m]. Section 7 of the Security Target discusses various PP conformance issues; the most significant of these are as follows:

a. Single use authentication of FTP and Telnet traffic, rather than being included in the TOE (as recommended in the PP), must be provided by using a separate authentication server. The UK Certification Body agreed this approach with the PP authors, the US National Information Assurance Partnership (NIAP).

b. The PP requirements relating to cryptographic remote administration are not applicable to the TOE because of the assumption that the administrator workstation must be connected by a dedicated and physically protected network.

c. The TOE assurance requirement of Evaluation Assurance Level EAL4 exceeded the EAL2 requirement of the Protection Profile (PP).

Assurance

18. The Security Target [a] specified the assurance requirements for the evaluation. The predefined Evaluation Assurance Level EAL4 was used, augmented by ALC_FLR.2.

19. CC Part 3 [d] describes an increasing scale of assurance given by predefined assurance levels EAL1 to EAL7.

20. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

21. Security Functional Requirement (SFR) FIA_UAU.5 d) requires a re-usable password authentication mechanism for administrator access to the TOE (ie from the COBRA GUI). The following strength claims were made in respect of this mechanism:

a. minimum strength of Function (SoF) of SoF-medium; and

b. the specific metric of the probability that authentication data can be guessed being no greater than one in two to the fortieth (2 ^ 40).

22. In addition, SFR FIA_UAU.4 requires the TOE's IT environment to provide a single-use authentication mechanism for FTP and Telnet traffic. This mechanism is outside the scope of the evaluation. (SFR FIA_UAU.8, which is within the scope of the TOE, merely ensures that a single-use authentication server is invoked.)

23. The TOE uses DES encryption for protecting reusable administrator passwords. The DES cryptographic mechanism is publicly known and as such it is the policy of the UK national authority for cryptographic mechanisms, Communications-Electronics Security Group (CESG), not to comment on its appropriateness or strength.

Security Policy

24. The TOE security policy is provided in the Security Target [a].

25. The Security Target [a] states that there are no Organisational Security Policies with which the TOE must comply.

Security Claims

26. The Security Target [a] fully specifies the TOE's security objectives, the threats that the objectives counter, and the SFRs and TOE Security Functions (TSF) to elaborate the objectives.

27. With the exception of FIA_UAU.8, all of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products. FIA_UAU.8 is fully defined in the Security Target [a].

28. Security functionality claims are made for IT security functions grouped under the following 5 categories:

- security management
- identification and authentication
- user data protection
- protection of security functions
- audit

Evaluation Conduct

29. The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication (UKSP) 01 [e] and UKSP 02 [f]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Mutual Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

30. 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.

31. To ensure that the Security Target [a] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline.

32. The evaluation was performed in accordance with CC Part 3 [d], the Common Evaluation Methodology (CEM) [g], the CEM supplement on Flaw Remediation [h] and the appropriate interpretations.

33. The Certification Body monitored the evaluation, which was performed by the Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [i] to the Certification Body in March 2003. The Certification Body then produced this report.

General Points

34. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target.

35. The evaluated configuration is specified in Annex A. Prospective consumers are advised to check that it matches their identified requirements, and to give due consideration to the recommendations and caveats of this Certification Report.

36. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification.

37. 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. However see the discussion below under the heading 'Flaw Remediation' regarding the application of patches generated as a result of the Developer's flaw remediation procedure.

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

(This page is intentionally blank)

II. EVALUATION FINDINGS

Introduction

39. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [i] under the CC Part 3 [d] headings.

40. The following sections note considerations of particular relevance to consumers.

Delivery

41. On receiving the TOE, the consumer is recommended to check that it is the evaluated version and to check that the security of the TOE has not been compromised during delivery.

42. Verification of secure delivery is described in the Common Criteria Evaluated Configuration Guide [k]. Consumers can verify the authenticity of the TOE by following the instructions detailed in that document.

43. The consumer must download the Common Criteria Evaluated Configuration Guide [k], using Secure Sockets Layer (SSL) encryption, from the Developer's website (www.securecomputing.com) where it is provided as a Portable Document Format (PDF) file.

44. Copies of the product (CD-ROMs in protective packaging) with manuals and associated components are packed and boxed, with a tamper evident seal or shrink-wrapped, in the Developer's production facility.

45. The TOE is shipped to the consumer by the Developer's preferred carrier (ie UPS), unless the consumer makes a special request to use an alternative service (eg FedEx, DHL). The order can be tracked by using part number, serial number, shipping tracking number and barcodes; all of these numbers and codes are visible to the consumer from the product and its packaging.

46. The serial number is required to activate the product. If the media and the serial number do not match, then there is reason to query the delivery.

Installation and Guidance Documentation

47. Secure installation, generation and startup of the TOE are described in the Startup Guide [j] and the Common Criteria Evaluated Configuration Guide [k].

48. The Common Criteria Evaluated Configuration Guide [k] should be read first, as it details the steps that must be followed to install the TOE in its evaluated configuration. That guide references out to the Startup Guide [j] and the Administration Guide [l], as appropriate.

49. Administrator guidance for the TOE is provided in the Startup Guide [j], the Common Criteria Evaluated Configuration Guide [k] and the Administration Guide [l].

50. There are no non-privileged users or direct users of the TOE. All human interaction with the TOE is by authorised administrators. Hence user guidance is not applicable to the TOE.

Strength of Function

51. The SoF claim for the TOE is identified above under the heading 'Strength of Function Claims'. SoF was demonstrated for the password authentication mechanism such that the probability that authentication data can be guessed is no greater than one in two to the fortieth (2^40).

52. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no other probabilistic or permutational mechanisms in the TOE.

53. The Evaluators also confirmed that the SoF claim of SoF-medium for the TOE is upheld.

Vulnerability Analysis

54. The Developer's vulnerability analysis describes the disposition of all known vulnerabilities relating to the TOE identified by design analysis and an extensive search of public domain sources of vulnerability.

55. The Evaluators' vulnerability analysis considered public domain sources on a wide range of different recognised websites, but found no vulnerabilities beyond those considered in the developer's analysis. The Evaluators' analysis also considered the evaluation deliverables for potential vulnerabilities. The Evaluators confirmed that the Developer's vulnerability analysis was consistent with the Security Target and with the countermeasures detailed in the Common Criteria Evaluated Configuration Guide [k] and the Administration Guide [l]. This analysis resulted in the identification of penetration tests, which were then executed by the evaluators. No exploitable vulnerabilities were identified.

Platform Issues

56. The recommended hardware configuration for the firewall platform is quoted above under 'TOE Scope'.

57. The Developer has a programme of compliance testing to determine the compatibility of specific hardware platforms, with specific hardware components, for the firewall. Details of the specific, compatible hardware platforms and the specific, compatible hardware components are provided on the Developer's website (www.securecomputing.com/index.cfm?sKey=734).

58. The Evaluators confirmed that the Developer's programme of compliance testing ensures the correct operation of the product on the specific hardware platforms and the specific hardware components, identified as compatible on the Developer's website. However consumers should note that the Evaluators' independent testing did not consider the full range of specific hardware platforms and specific hardware components that are identified as compatible on the Developer's website. Strictly therefore the firewall evaluation platforms comprise only those specified in Annex C.

59. The evaluated configuration excluded other hardware options, eg use of multiple CPUs and alternative Network Interface Cards (NIC). There may be a risk in the use of hardware components incorporating special processing or external command features (eg wake-on LAN) that are not disabled.

60. The TOE was evaluated for a configuration of the COBRA GUI installed on the following operating systems:

- Windows 2000 with Service Pack 2;
- Windows NT 4.0 with Service Pack 6a; and
- Windows NT 4.0 with Service Pack 4.

61. The focus given to the hardware evaluation platforms primarily involved:

a. confirmation that the Developers' and Evaluators' testing gave rise to no results which could be attributed to problems in the platforms;

b. consideration, in the course of the various development representation activities, of the way in which the firewall harnessed the functionality of the platform; and

c. analysis of potential hardware effects which might undermine the security of the firewall (eg whether the packets passed to NICs were of sufficient length to prevent those NICs from introducing Etherleak problems).

Flaw Remediation

62. Procedures for reporting flaws, and for requesting that a known flaw is corrected, are described in the Common Criteria Evaluated Configuration Guide [k].

63. A consumer who reports a flaw is notified of the solution.

64. If the solution requires a software patch, all purchasers of the product are notified.

65. If the solution does not require a software patch (eg if the flaw is resolved by a procedural workaround or will be addressed in the next release of the product), details are provided on the Developer's website (www.securecomputing.com) and are also available from the Developer's customer support. The consumer should check for the appearance of such details, in accordance with good industry practice for firewall administrators.

66. Details of the above notification process are provided in the Common Criteria Evaluated Configuration Guide [k].

67. The Startup Guide [j] directs consumers to the Developer's website to obtain patches. See the discussion below under the heading 'Recommendations' regarding the application of patches generated as a result of the Developer's flaw remediation procedure.

(This page is intentionally blank)

III. EVALUATION OUTCOME

Certification Result

68. After due consideration of the ETR [i] produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that Sidewinder G_2 Firewall Version 6.0 meets the Common Criteria Part 3 [d] augmented requirements of Evaluation Assurance Level EAL4 with ALC_FLR.2, for the specified Common Criteria Part 2 [c] extended functionality, when running on the specified platforms.

69. The TOE meets the requirements of the US DoD Application-level Firewall Protection Profile for Basic Robustness Environments [m], when running on the specified platforms.

70. The TOE meets the minimum SoF claim of SoF-medium and the metric given above under the heading 'Strength of Function Claims'.

Recommendations

71. Prospective consumers of the TOE should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a].

72. The TOE should be used in accordance with a number of environmental considerations, as specified in the Security Target [a].

73. The TOE should be delivered, installed, configured and used in accordance with the supporting guidance documentation [j- l] included in the evaluated configuration.

74. Only the evaluated TOE configuration should be installed. That for which EAL4 assurance has been demonstrated is specified in Annex A, with further relevant information given above under the headings 'TOE Scope' and 'Evaluation Findings'.

75. Strictly, whilst ALC_FLR.2 gives confidence in the Developer's flaw remediation procedure, this will not maintain the full EAL4 assurance if the TOE configuration is changed by the application of patches. Nevertheless the application of patches generated under this procedure is recommended, if and where the patches fix exploitable vulnerabilities discovered since this report was issued.

76. Further recommendations are provided above under the heading 'Evaluation Findings'.

(This page is intentionally blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as Sidewinder G_2 Firewall Version 6.0.

TOE Documentation

2. The guidance documents evaluated were:

- Sidewinder G_2 Firewall Startup Guide [j]
- Common Criteria Evaluated Configuration Guide [k]
- Sidewinder G_2 Firewall Administration Guide [l]

3. Further discussion of the guidance documents is provided above under the heading 'Installation and Guidance Documentation'.

TOE Configuration

4. The TOE should be configured in accordance with the guidance documents identified in paragraph 2 above.

Platform Configuration

5. The firewall evaluation platform is discussed above under the headings 'TOE Scope' and 'Platform Issues', and in Annex B under the heading 'Hardware and Firmware'.

6. Annex C provides details of the specific platforms used for the evaluation.

(This page is intentionally blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the product's main 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 this report and in Annex A.

Architectural Features

2. The TOE provides a hybrid firewall solution that supports both application-level proxy and packet filtering.

3. The TOE contains SecureOS. SecureOS is an extended version of the BSD UNIX operating system, which employs Secure Computing Corporation's Type Enforcement security technology, additional network separation control, network level packet filtering support and improved auditing facilities. SecureOS also provides the secured computing environment in which all of the TOE's firewall application layer processing is done.

4. The application layer firewall components include the network service monitor processes, network proxy applications, the firewall Access Control List (ACL) daemon, audit monitors and the system management functions.

5. The TOE operates in an environment where it provides a single point of connectivity between at least 2 networks. One network is typically viewed as the inside of an organisation, where there is some assumption of control over access to the computing network. The other network is typically viewed as an external network, similar to the Internet, where there is no practical control over the actions of its processing entities. The role of the TOE is to limit and control all information flow between the networks.

6. Administration of the firewall is performed using the COBRA GUI, which runs on either the Windows 2000 or Windows NT operating system, on a separate workstation connected to the firewall by a physically secure network connection.

Design Subsystems

7. The TOE consists of the following subsystems:

   a. SecureOS Kernel Subsystem. This consists of the BSD UNIX kernel with the TOE's unique security enhancements.

   b. SecureOS Utilities Subsystem. This provides the processing elements that complete the system startup, provide support for administrator login control and initiate a number of system daemons which make the system usable.

   c. Firewall Management Subsystem. This includes the daemons and commands which respond to firewall administrator input to define, modify and examine all aspects of the firewall security policy and the firewall configuration.

   d. Firewall Policy Subsystem. This deals with controlling network communications to and through the firewall.

e. Firewall Communications Control Subsystem. This provides the facilities required for the TOE to move network communication data from one 'burb' (ie combination of IP addresses and network interfaces) to another, under the control of the firewall security policy.

f. System Utilities Subsystem. This provides facilities (eg C library files, user shells) to the other subsystems and provides the non-blocking name resolver facilities which are unique to the TOE.

Hardware and Firmware

8. No extraordinary security demands are placed upon the hardware platforms and peripheral equipment used by the TOE.

9. The firewall is designed to operate on generic Intel Pentium based platforms with minimum processor speed, RAM size and hard disk size, as specified above under the heading 'TOE Scope'. Further discussion of compatible hardware platforms and compatible hardware components is provided above under the heading 'Platform Issues'.

10. The security features required to be present and operational on the firewall hardware platform include:

a. A CPU that provides a 2-state processing model to support the separation of the kernel processing from the application processing.

b. A CPU (and/or supporting motherboard) that provides a Memory Management Unit (MMU) to support memory spaces for the kernel and each process.

c. A system motherboard that provides a battery backup for the clock to maintain time information when the system is shut down. Also the CPU or ancillary hardware must provide a periodic cycle time operating at a minimum of 100Hz to support the internal time management within the kernel.

11. The COBRA GUI is also designed to operate on a generic Intel Pentium based hardware platform capable of supporting the Windows 2000 or Windows NT operating system.

TSF Interface

12. The following external TOE Security Functions Interface (TSFI) is identified for the TOE:

a. Administrator Interface. This defines the relationship between an administrator and the TOE management facilities. It is used to manage all aspects of operation of the TOE.

b. Network Interface. This supports the exchange of information from the physical network wire to elements of the TOE responsible for controlling the exchange of information between attached networks.

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The Evaluators performed independent functional testing on the TOE to confirm that it operates as specified. They also repeated a sample of 31% of the Developer's tests to confirm the adequacy of the Developer's testing of all of the TSF, subsystems and TSFI.

2. The Evaluators then performed penetration testing which confirmed the SoF claimed in the Security Target [a] for the password authentication mechanism. The penetration testing also confirmed that all identified potential vulnerabilities in the TOE have been addressed, ie that the TOE in its intended environment has no exploitable vulnerabilities.

3. During their testing, the Evaluators used both the COBRA GUI and the Sidewinder Console Command Line Interface (CLI). However, they used the CLI only to facilitate the gathering of test data.

4. The single-use authentication server used by the TOE during testing was the SafeWord authentication server.

Platform Issues

5. To meet the CC Part 3 [d] class ATE assurance requirements, the Developer provided evidence of testing the firewall on the following evaluation platforms:

a. Dell PowerEdge 1650 Server consisting of:
- two Intel Pentium III processors (only one enabled) running at 1.26GHz
- 512KB L2 cache
- 1GB RAM
- two Dell 36GB Ultra3 15,000 rpm SCSI hard disks
- embedded Dell PERC 3/Di RAID Controller, configured with 'container' entities rather than 'RAID' entities
- CD-ROM drive
- 3.5" 1.44MB floppy disk drive
- Compaq V700 17" monitor[3]
- keyboard
- two embedded Intel Pro/1000XT 1Gbit/s NICs (82544EI chip, driver version 1.3.8) - to communicate with the networks for which the firewall mediates communication and information flow
- one Intel Pro/100+ server adapter PCI single-port NIC (PILA8470B, driver version 1.8.2.1) - to communicate with the platform hosting the COBRA GUI

[3] The Developer's website recommended a Dell 17" monitor for installing the firewall on Dell PowerEdge 1650, 2650 and 6650 platforms. A Compaq V700 17" monitor was used to install the TOE on the evaluation platforms identified in paragraphs 5.a, 5.b and 5.c. The Evaluators confirmed that the monitor had no impact on the security of the TOE on those platforms and that, once the TOE was installed, the monitor could be removed if necessary.

b. Dell PowerEdge 2650 Server consisting of:
- one Intel Xenon processor running at 2.6GHz
- 512KB L2 cache
- 1GB RAM
- one Dell 36GB Ultra3 15,000 rpm SCSI hard disk
- embedded Dell PERC 3/Di RAID Controller (disabled on this platform)
- CD-ROM drive
- 3.5" 1.44MB floppy disk drive
- Compaq V700 17" monitor[3]
- keyboard
- two embedded Broadcom NetXtreme 1Gbit/s server adapter NICs (BCM5701, driver version 1.0.0) - to communicate with the networks for which the firewall mediates communication and information flow
- one Intel Pro/100+ server adapter PCI single-port NIC (PILA8470B, driver version 1.8.2.1) - to communicate with the platform hosting the COBRA GUI

c. Dell PowerEdge 6650 Server consisting of:
- four Intel Xenon processors (only one enabled) running at 1.9GHz
- 512KB L2 cache
- 1GB RAM
- four Dell 18GB Ultra3 15,000 rpm SCSI hard disks
- Dell PERC 3/DC RAID Controller, configured as 51GB RAID 5
- CD-ROM drive
- 3.5" 1.44MB floppy disk drive
- Compaq V700 17" monitor[3]
- keyboard
- two embedded Broadcom NetXtreme 1Gbit/s server adapter NICs (BCM5700, driver version 1.0.0) - to communicate with the networks for which the firewall mediates communication and information flow
- one Intel Pro/1000XT server adapter NIC (PWLA8490XT, driver version 1.8.2.1) - to communicate with the platform hosting the COBRA GUI

6. The Evaluators performed their independent testing of the firewall on the Dell PowerEdge 1650 and 2650 evaluation platforms in paragraphs 5.a and 5.b above. The Evaluators' testing on those platforms formed part of their examination of the Developer's programme of compliance testing (discussed above under 'Platform Issues').

7. For the above testing, each of the firewall evaluation platforms was located on its own administration network, and was connected to internal and external networks, providing services to support all of the possible test procedures and scenarios.

8. Developer testing was performed with the COBRA GUI installed on Windows 2000 Service Pack 2 and installed on Windows NT 4.0 Service Pack 6a. In each case the following hardware platform was used:

Dell Dimension 4550 consisting of:
- one Intel Pentium 4 processor running at 2.4GHz

- 256MB RAM
- 30GB Ultra ATA/100 7200rpm hard disk
- 3.5" 1.44MB floppy disk drive
- CD-ROM drive
- SVGA video and display
- serial mouse
- US keyboard
- one embedded Intel Pro/100VE network connection - to communicate with the firewall evaluation platform

9. Evaluator testing was performed with the COBRA GUI installed on Windows 2000 Service Pack 2 on the hardware platform specified in paragraph 8 above, and installed on Windows NT 4.0 Service Pack 4 on the following hardware platform:

Compaq Deskpro EN Series consisting of:

- Intel Pentium III running at 500MHz
- 128Mb RAM
- 1.5GB hard disk
- 3.5" 1.44MB floppy disk drive
- CD-ROM drive
- SVGA video and display
- PS/2 mouse
- keyboard
- 3Com EtherLink 10/100 PCI 3C905B-Combo NIC - to communicate with the firewall evaluation platform

10. Evaluators considered that:

a. the testing performed was sufficient overall to cover operation on the Windows 2000 Service Pack 2, Windows NT4.0 Service Pack 6a and Windows NT4.0 Service Pack 4 operating systems; and

b. the differences between hardware on which the COBRA GUI was installed for Developer and Evaluator testing had no impact on the security of the TOE.

(This page is intentionally blank)