122-B

COMMON CRITERIA CERTIFICATION REPORT No. CRP239

Sidewinder™ G_2 Firewall™ Version 6.1.2.03

(Sidewinder G_2 Security Appliance Model 2150D and Sidewinder G_2 Software v 6.1.2.03)

Issue 1.0

May 2007

UK Certification Body
CESG, Hubble Road
Cheltenham, GL51 0EX
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.

CERTIFICATION STATEMENT

The products detailed below have been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and have met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	**Secure Computing Corporation**
Product and Version	**Sidewinder G_2 Firewall Version 6.1.2.03**
Description	Sidewinder is a firewall and access control security platform suitable for enterprise deployment.
CC Part 2	**extended**
CC Part 3	**conformant**
EAL	**EAL4** augmented by ALC_FLR.3
Protection Profile	U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, FINAL
CLEF	**BT**
Date authorised	**31 May 2007**

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 ([a] - [c]). The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [d], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [e], CC Part 2 [f], CC Part 3 [g], the Common Evaluation Methodology (CEM) [h], and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Sidewinder G_2 Firewall Version 6.1.2.03 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 [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The versions of the product evaluated were:

   Sidewinder G_2 Security Appliance Model 2150D
   and Sidewinder G_2 Software v 6.1.2.03.

   These are collectively referred to as **Sidewinder G2 Firewall Version 6.1.2.03** throughout this report.

4. The Developer was Secure Computing Corporation.

5. Sidewinder G_2 Firewall, from Secure Computing Corporation, is a software firewall incorporating a hardened operating system. It is available either as a software only upgrade for existing customers or installed on Sidewinder hardware appliances. It provides access control of communication and information flow between two or more networks, using application-level proxy and packet filtering technology.

6. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration'.

7. The evaluated configuration relies on the TOE being physically secure and accessed only by trusted personnel. Additionally, the same physical and personnel security requirements must also apply to the administration console machine and any external authentication server.

8. An overview of the product and its security architecture can be found in Chapter IV 'Product Security Architecture'.

Protection Profile Conformance

9. **The Security Target [d] is certified as achieving conformance to the following protection profile:**

   U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, FINAL [n].

10. Section 7 of the Security Target [d] discusses various PP conformance issues. The most significant of these are as follows:

    - 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).

    - 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.

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

Security Claims

11. The Security Target [d] fully specifies the TOE's security objectives, the threats which these objectives counter and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives. Most of the SFRs are taken from CC Part 2 [f]; use of this standard facilitates comparison with other evaluated products. Section 5.1 of the Security Target [d] details the one explicitly stated SFR.

12. The TOE security policies are detailed in Paragraph 82 of the Security Target [d].

Strength of Function Claims

13. **The minimum Strength of Function (SoF) was SoF-Medium**. This was claimed for security function SW_FIA with a metric where the password authentication mechanism is such that the probability that authentication data can be guessed is no greater than one in two to the fortieth (2 ^ 40). This is based on guidance given on Page 9 of the Common Criteria Evaluated Configuration Guide [k]. **The Certification Body has determined that these claims were met.**

Evaluation Conduct

14. The TOE Security Functions and security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of Sidewinder G_2 Firewall Version 6.1, which had previously been certified by the UK Certification Body to the CC EAL4 augmented by ALC_FLR.3 assurance level [i]. For the evaluation of Sidewinder G_2 Firewall Version 6.1.2.03, the Evaluators made some use of Sidewinder G_2 Firewall Version 6.1 evaluation results where appropriate.

15. The Certification Body monitored the evaluation which was carried out by the BT Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [d]. The results of this work, completed in May 2007, were reported in the ETR [j].

Conclusions and Recommendations

16. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

17. **Prospective consumers of Sidewinder G_2 Firewall Version 6.1.2.03 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [d]**. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

18. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III 'Evaluated Configuration'.

19. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II 'Product Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

20. **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. 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 these patches have further assurance. The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product.

II. PRODUCT SECURITY GUIDANCE

Introduction

21. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

22. **On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery**.

23. 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.

24. 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.

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

26. 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.

27. 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

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

29. 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 [l] and the Administration Guide [m], as appropriate.

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

31. 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.

III. EVALUATED CONFIGURATION

TOE Identification

32. The TOE consists of:

- Sidewinder G_2 Firewall Software (Version 6.1.2.03), delivered on a bootable CDROM from the Sponsor or with an appliance from an authorised reseller;
- Sidewinder G_2 Management Tools (Version 6.1.2), delivered on a CDROM from the Sponsor or with an appliance from an authorised reseller;
- Sidewinder G_2 Security Appliance Model 2150D (Part Number SW612-2950A-2150D-A), delivered from the Sponsor or authorised resellers.

TOE Documentation

33. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'. The Startup Guide [l] and the Administration Guide [m] are provided on the Management Tools CDROM. The Common Criteria Evaluated Configuration Guide [k] must be downloaded, see Paragraph 24, above.

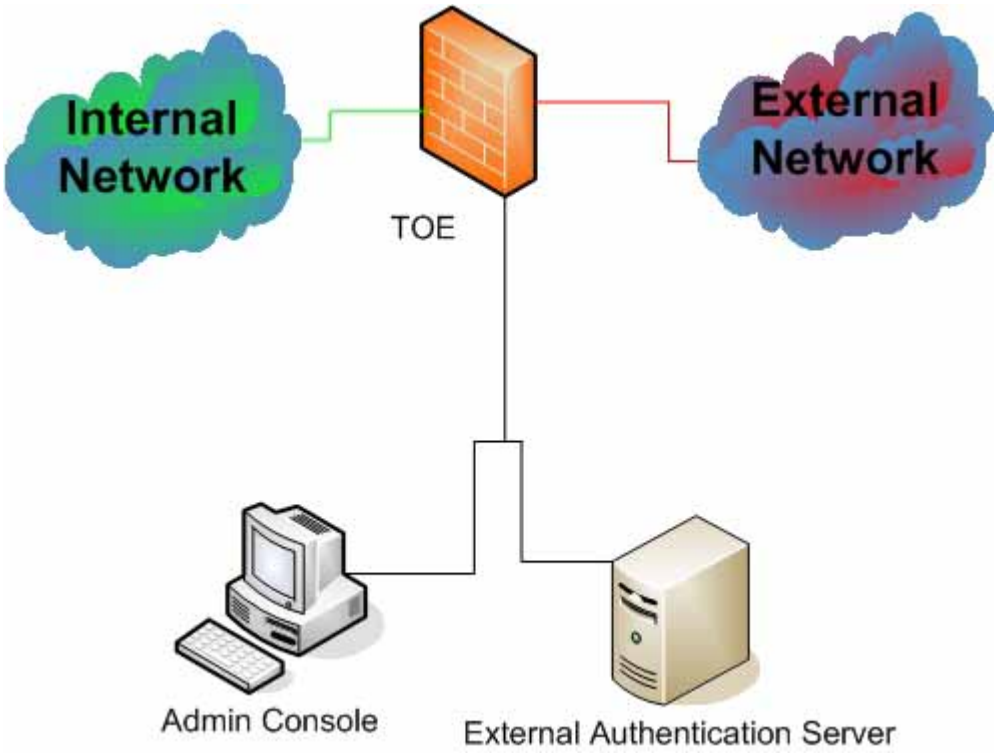
TOE Scope

34. Sidewinder provides the following functionality that is specifically excluded from the scope of this evaluation:

- On-console Administration;
- Virtual Private Network (VPN);
- Failover/High Availability;
- Anti-Virus;
- URL Filtering;
- Mail Filtering;
- Policy Acceleration Network Cards;
- SSL Termination;
- Direct login to a Sidewinder via Telnet or ssh;
- Firewall policy cloning;
- Remote administration from external networks;
- Built-in servers (e.g. SSHD).

TOE Configuration

35. The evaluated TOE configuration is as detailed in Section 2 of the Security Target [d]. The TOE is be deployed within a network architecture as shown in the following diagram:



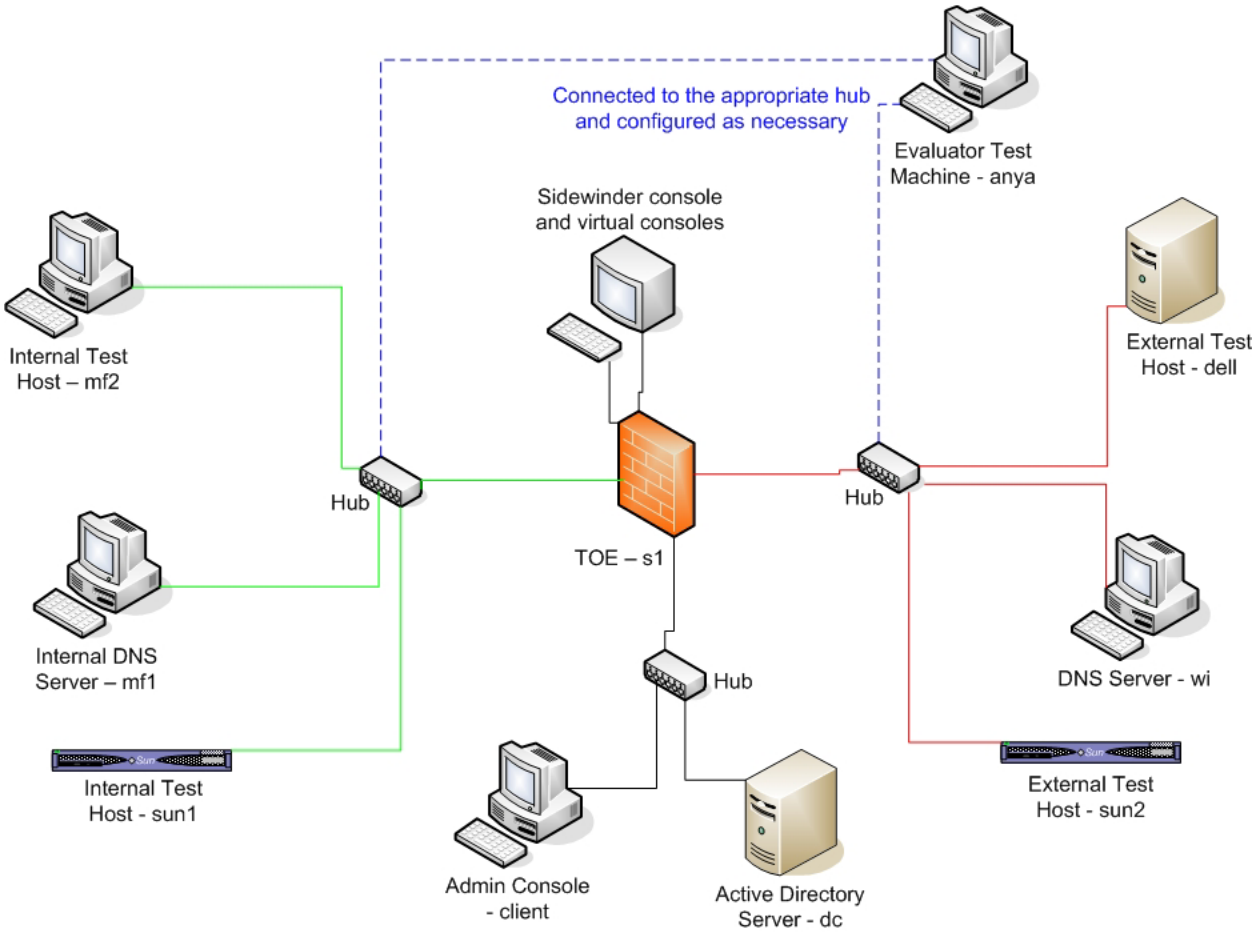
Environmental Requirements

36. The environmental configuration is as described within Sections 2.2, 2.3, 3.1 and 4.2 of the Security Target [d].

37. The diagram in Paragraph 35 above shows, in outline, the position of the various items within the TOE's environment.

Test Configuration

38. The configuration in the diagram below was used for testing. The TOE was installed and configured according to the Common Criteria Evaluated Configuration Guide [k] referencing out to the Startup Guide [l] and the Administration Guide [m] when necessary. The Sidewinder console and virtual consoles were used to facilitate testing and are not required for normal operation once installation is complete. The TOE was tested using a 2150D Appliance (hostname s1) that was re-imaged from a bootable CDROM that was received separately from the Sponsor. Hence, the test results are applicable to any supported hardware.



39. The Admin Console platform was a Compaq DeskPro EN with Pentium 3, 866 MHz, 384 Mb RAM, Embedded Intel 10/100 NIC and 15Gb HDD running Windows XP Professional with SP2.

40. The Active Directory Server (used as the External Authentication Server) was a Compaq ProLiant DL380 with Pentium 3, 1.266 GHz, 1 Gb RAM, 2 Embedded NC3163 10/100 NICs and 50Gb HDD (RAID, 3x18Gb) running Windows 2003 Server R2.

IV. PRODUCT SECURITY ARCHITECTURE

Introduction

41. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

42. An overview of the TOE and the TOE architecture is described in Section 2 of the Security Target [d].

43. The diagram in Paragraph 35 above shows the outline network topology that is applicable to the TOE.

44. The TOE security policies (i.e. the UNAUTHENTICATED SFP and the AUTHENTICATED SFP) are detailed in Paragraph 82 of the Security Target [d]. Specific parameter settings are detailed within the Common Criteria Evaluated Configuration Guide [k].

45. The main security protection mechanisms of the TOE are :

    a. Identification and Authentication – the TOE invokes local or external identification and authentication mechanisms;

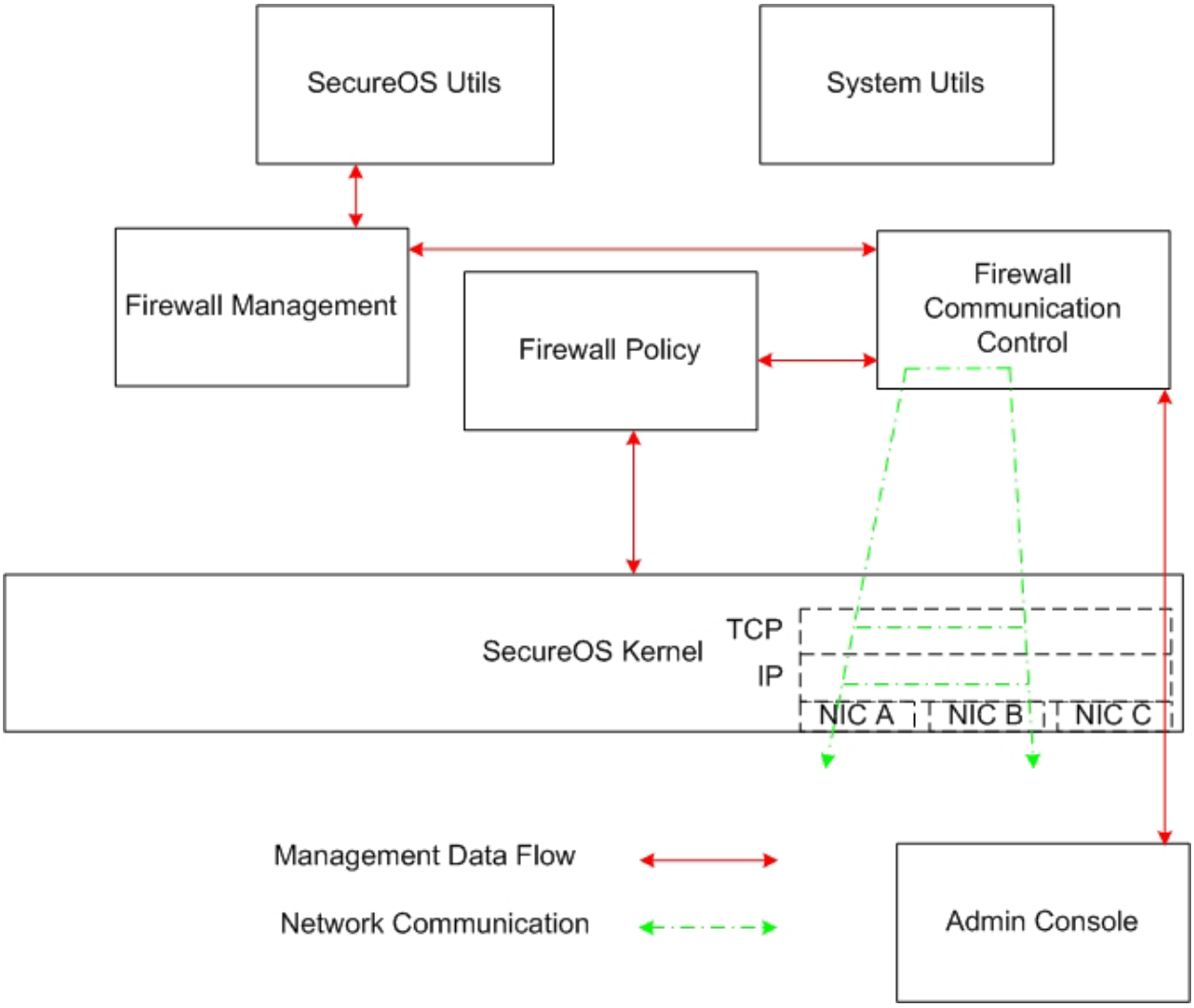
    b. Traffic Flow Control – the TOE only allows specific traffic to pass through when it has been configured to allow that traffic to pass;

    c. Traffic Separation – the TOE prevents leakage between one traffic stream and another;

    d. Secure Operating System – the TOE operating system has been designed to be highly resistant to both malicious and accidental attack.

Design Subsystems

46. The subsystems of the TOE are shown in the diagram below. The System Utils subsystem provides support to the other subsystems but does not affect any of the security functionality of the TOE nor does directly handle any Management Data during startup or operation.



Hardware and Firmware Dependencies

47. The TOE's hardware and firmware dependencies are detailed in Paragraph 32 and Section 2.3.4.2 of the Security Target [d]

Product Interfaces

48. There are two external TSF interfaces (the Administrator Interface and the Network Interface). The Administrator Interface facilitates the relationship between an administrator and the TOE management facilities. It is used to manage all aspects of operation of the TOE. This is via the Cobra GUI. The Network Interface supports the exchange of information from the physical network wire to elements of the Sidewinder responsible for controlling the exchange of information between attached networks and between the TOE and the workstation hosting the Cobra GUI.

V. PRODUCT TESTING

IT Product Testing

49. The evaluators confirmed that the developer testing covered all security functions in the Security Target [d], subsystems and interfaces documented in Chapter IV 'Product Security Architecture', paragraphs 47 and 49 respectively.

50. 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. The evaluators performed this testing between March 2nd and 14th 2007 at the BT CLEF lab in Fleet, Hampshire, UK, except for functional test 2, which was carried out on the 18th April 2007 at the BT CLEF lab in Aldershot, Hampshire, UK.

51. The evaluators then performed penetration testing which confirmed the SoF claimed in the Security Target [d] for the password authentication mechanism. The penetration testing also confirmed that all identified potential vulnerabilities in the TOE have been addressed, i.e. that the TOE in its intended environment has no known exploitable vulnerabilities. The evaluators performed penetration testing between 18th and 20th April 2007, at the BT CLEF lab in Aldershot.

52. During their testing the evaluators used both the Admin Console GUI and the Sidewinder Console Command Line Interface. However, they used the Command Line Interface only to facilitate the gathering of test data.

53. The evaluators used the following tools during the testing sub-activities:

- Packit v0.7 (obtained from http://packit.sourceforge.net);
- Fragroute v1.2 (obtained from http://monkey.org/~/dugsong/fragroute/);
- Wireshark v.99.5 (obtained from http://heanet.dll.sourceforge.net/sourceforge/wireshark/);
- Nmap v4.20 (obtained from http://insecure.org);
- Siege v2.59b3 (obtained from BT CLEF Test Tools Live CD).

54. Other than these no specialist tools or techniques were employed.

Vulnerability Analysis

55. 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 vulnerabilities.

56. The evaluators' vulnerability analysis, which preceded penetration testing, 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 evaluator's analysis also considered the evaluation deliverables for

potential vulnerabilities. The evaluators confirmed that the developer's vulnerability analysis was consistent with the Security Target [d] and with the countermeasures detailed in the Common Criteria Evaluated Configuration Guide [k] and the Administration Guide [m]. This analysis resulted in the identification of penetration tests, which were executed by the evaluators. No exploitable vulnerabilities were identified.

Platform Issues

57. Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration'.

58. The Developer provided evidence of testing the firewall on the following platform:

    a. Sidewinder G_2 Security Appliance model 2150D with the following components:

    - CDROM;
    - Monitor Port;
    - USB port (for console keyboard);
    - Two embedded 1 GB Ethernet Ports (not supported by Secure Computing);
    - 1 PCI NIC supplying 6 Intel PRO 1000 Ethernet ports.

59. For the above testing, the TOE was located on its own network (ADMIN), and was connected to internal and external networks, providing services to support all of the possible test procedures and scenarios.

60. The Evaluators re-ran the developer test sample using the same configuration as the developers, with the exception of the SafeWord Server. As a SafeWord server was not available to the evaluators it was replaced by a Microsoft Active Directory Server. However, this change did not affect the test results in any way.

61. The Active Directory Server (used as the External Authentication Server) was a Compaq ProLiant DL380 with Pentium 3, 1.266 GHz, 1 Gb RAM, 2 Embedded NC3163 10/100 NICs and 50Gb HDD (RAID, 3x18Gb) running Windows 2003 Server R2.

62. The Evaluators performed their independent testing of the firewall on the following platform:

    a. Sidewinder G_2 Security Appliance model 2150D consisting of:

    - Two 2.66 GHz CPUs;
    - 2 Gbytes RAM;
    - 4 x 36 Gbytes Hard Disks; and
    - 2 Embedded 6 Intel PRO/1000 ethernet ports.

63. The Admin Console platform was a Compaq DeskPro EN with Pentium 3, 866 MHz, 384 Mb RAM, Embedded Intel 10/100 NIC and 15Gb HDD running Windows XP Professional with SP2.

VI. REFERENCES

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[b] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

[d] Sidewinder G2 Security Appliance Model 2150D and Sidewinder G2 Software v 6.1.2 Security Target,
Secure Computing Corporation,
Part Number 00-0946372-D, 29 March 2007.

[e] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-001, Version 2.3, August 2005.

[f] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-002, Version 2.3, August 2005.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-003, Version 2.3, August 2005.

[h] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2005-08-004, Version 2.3, August 2005.

[i] Common Criteria Certification Report No P206,
Sidewinder G2 Firewall, Sidewinder G2 Security Appliance Models 210, 310, 315, 410, 415, 510, 515, 1100, 1150, 2150, 4150 and Sidewinder G2 Software v 6.1,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, July 2004.

[j] Evaluation Technical Report, Common Criteria EAL4 Augmented Evaluation of Sidewinder G2 Security Appliance Model 2150D and Sidewinder G2 Software Version 6.1.2,
BT CLEF,
LFS/T534/ETR, Issue 1.0, 11 May 2007.

[k] Common Criteria Evaluated Configuration Guide,
Secure Computing Corporation,
PN 00-0946376-B.

[l] Startup Guide Sidewinder G2,
Secure Computing Corporation,
SWOP-MN-STRT61-D, February 2006.

[m] Sidewinder Administrator Guide,
Secure Computing Corporation,
SWOP-MN-ADMN61-D, March 2006.

[n] U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments,
Version 1.0, FINAL.