UK IT sec

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UKAS PRODUCT CERTIFICATION

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P175

Sidewinder™ Firewall

Version 5.2.1
running on specified platforms

Issue 1.0

September 2002

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 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 Firewall Version 5.2.1 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2, augmented by ALC_FLR.2, for the specified Common Criteria Part 2 extended functionality when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body UK IT Security Evaluation Certification Scheme
Date authorised	30 September 2002

(This page is intentionally blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT iii

TABLE OF CONTENTS v

ABBREVIATIONS vii

REFERENCES ix

I. EXECUTIVE SUMMARY 1

Introduction 1
Evaluated Product 1
TOE Scope 2
Protection Profile Conformance 3
Assurance 3
Strength of Function Claims 3
Security Policy 3
Security Claims 3
Evaluation Conduct 4
General Points 4

II. EVALUATION FINDINGS 7

Introduction 7
Delivery 7
Installation and Guidance Documentation 7
Strength of Function 8
Vulnerability Analysis 8
Platform Issues 8
Flaw Remediation 8

III. EVALUATION OUTCOME 9

Certification Result 9
Recommendations 9

ANNEX A: EVALUATED CONFIGURATION 11

ANNEX B: PRODUCT SECURITY ARCHITECTURE 13

ANNEX C: PRODUCT TESTING 17

(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
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
MMU	Memory Management Unit
NIC	Network Interface Card
SFR	Security Functional Requirement
SOF	Strength of Function
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 Version 5.2.1 Security Target,
Secure Computing Corporation,
00-0937063-E, 27 September 2002.

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 4.0, February 2000.

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 Secure Server Version 5.2.1,
Syntegra CLEF,
LFS/T246/ETR, Issue 1.0, 22 August 2002.

j. Sidewinder Delivery Procedures,
Secure Computing Corporation,
PN 00-0935143-F, 2 August 2002.

k. Sidewinder Installation and Configuration Guide,
Secure Computing Corporation,
SWOP-MN-INST52-B, May 2002.

l. Common Criteria Evaluated Configuration Guide,
Secure Computing Corporation,
PN 86-0935509-L.

m. Sidewinder Administrator Guide,
Secure Computing Corporation,
PN-SWOP-MN-ADMN52-B, May 2002.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Sidewinder Firewall Version 5.2.1 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

The version of the product evaluated is Sidewinder Firewall Version 5.2.1.

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

4. 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.

5. The operational environment for the Sidewinder software is a typical Intel-based architecture Pentium PC hardware platform. The TOE contains SecureOS, which is an extended version of the Berkeley Software Distribution (BSD) UNIX operating system that employs Secure Computing Corporation’s Type Enforcement security technology. Type Enforcement protects the TOE by separating all processes and services on the firewall.

6. 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. It provides a comprehensive set of Internet services and proxies.

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

8. Annex B provides an overview of the TOE’s security architecture.

TOE Scope

9. The FTP, HTTP (non-caching), Telnet, Generic TCP (finger and daytime) and Generic UDP (daytime) proxies are all included within the scope of the evaluation. Other protocol aware proxies provided by Sidewinder were excluded from the scope of the evaluation.

10. Sidewinder also provides the following functionality that was specifically excluded from the scope of the evaluation:

- Remote Administration
- Virtual Private Network (VPN)
- 3rd Party Authentication
- User Defined Proxies
- Cloning
- Failover
- Uniform Resource Locator (URL) Filtering
- Mail Filtering
- Policy Acceleration Network Cards
- Built-in Servers

11. The TOE's operational environment includes:

a. a generic Intel Pentium processor based computing platform, with 2 network interfaces, that executes the software to control the flow of IP traffic between those interfaces; and

b. a commercially-available, single-use authentication server that is compatible with Sidewinder (eg SafeWord from Secure Computing Corporation, or any RADIUS server).

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

- CPU type: Intel Pentium II, Pentium III, Pentium IV or Pentium XEON
- CPU speed: 300MHz minimum
- RAM: 192 MB minimum
- hard disk storage: 8 GB minimum
- 3.5? 1.44 MB floppy disk drive
- CD-ROM drive
- DAT drive (optional)
- network: 2 (Ethernet) network interfaces
- SVGA video and display monitor
- PS/2 compatible 3-button mouse
- US keyboard

Protection Profile Conformance

13. The Security Target [a] did not claim conformance to any protection profile.

Assurance

14. The Security Target [a] specified the assurance requirements for the evaluation. The predefined Evaluation Assurance Level EAL2 was used, augmented by ALC_FLR.2.

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

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

Strength of Function Claims

17. Section 6.1.2.2 of the Security Target [a] states that "passwords are implemented by means of a permutational mechanism that meets the standard of SOF-medium". Section 5.1.1.1 of the Security Target states that this is realised by FIA_UAU.5 and provides its specific Strength of Functions (SOF) metric, as follows:

> FIA_UAU.5 - "Strength of function shall be 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). The password authentication mechanism must demonstrate SOF-medium as defined in Part 1 of the CC."

18. In addition, FIA_UAU.4 requires the TOE operating environment to provide a single-use authentication mechanism. This mechanism is outside the scope of the evaluation (Security Functional Requirement (SFR) FIA_UAU.8, which is within the scope of the TOE, merely ensures that a single-use authentication server is invoked).

19. The TOE uses DES encryption for protecting reusable 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

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

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

Security Claims

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

23. 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 Section 5.1.1 of the Security Target [a].

24. 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

25. 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 jointly managed by CESG and the Department of Trade and Industry 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.

26. 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.

27. 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.

28. Both parts of the evaluation were performed in accordance with CC Part 3 [d], the Common Evaluation Methodology (CEM) [g], the CEM supplement on Flaw Remediation [h] and the appropriate Common Criteria Interpretation Management Board (CCIMB) interpretations numbered 3, 8, 27, 32, 38, 43, 49, 51, 64, 75, 84, 85, 116, 127 and 128.

29. 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 August 2002. The Certification Body then produced this Certification Report.

General Points

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

31. 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.

32. 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 such patches have been evaluated and certified. However, see paragraph 60 of this Certification Report regarding the application of patches generated as a result of the Developer's flaw remediation procedure.

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

(This page is intentionally blank)

II. EVALUATION FINDINGS

Introduction

34. 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.

35. The following sections note considerations of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Delivery

36. Secure delivery of the TOE is described in the Delivery Procedures [j], which describe the process of releasing the TOE to consumers.

37. Copies of the product (CD-ROMs in protective packaging), along with manuals and associated components are packed, boxed and shrink-wrapped in the Developer's Production Facility.

38. 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 alternate service (eg FedEx, DHL).

39. The consumer must download the Common Criteria Evaluated Configuration Guide [l], using SSL encryption, from the Developer's website (www.securecomputing.com) where it is provided in the form of a PDF file.

40. 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.

Installation and Guidance Documentation

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

42. The Common Criteria Evaluated Configuration Guide [l] 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 Installation and Configuration Guide [k] and the Administrator Guide [m], as appropriate.

43. When the installation of the TOE is complete, the Man Pages can then be accessed.

44. Administrator guidance for the TOE is provided in the Installation and Configuration Guide [k], the Common Criteria Evaluated Configuration Guide [l], the Administrator Guide [m] and the Man Pages.

45. 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.

46. Although the Security Target [a: 2.3.1] states that " ... authorised administrators shall be allowed physical access to the Sidewinder console and its hardware computing platform for such purposes as starting the system and loading new software", the administrators should follow the guidance in the Installation and Configuration Guide [k] and the Common Criteria Evaluated Configuration Guide [l].

Strength of Function

47. The SOF claim for the TOE is identified above under the heading 'Strength of Function Claims'.

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

49. The Evaluators also confirmed that the SOF claim of SOF-medium for the TOE is upheld.

Vulnerability Analysis

50. The Evaluators' vulnerability analysis was based on public domain sources and the visibility of the TOE given by the evaluation process.

Platform Issues

51. The TOE was evaluated on the hardware platforms specified in Annex A. Therefore, the evaluated configuration excluded other hardware options, eg Network Interface Cards (NIC).

52. The Developer has a programme of compliance testing to determine the compatibility of specific hardware platforms, with specific hardware components, for the product. 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).

53. 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 evaluated EAL2 configuration is that running on the hardware platforms specified in Annex C. There may be a risk in the use of other hardware components incorporating special processing or external command features (eg wake-on LAN) that are not disabled.

Flaw Remediation

54. Procedures for reporting flaws are described in the Common Criteria Evaluated Configuration Guide [l]. The Installation and Configuration Guide [k] directs consumers to the Developer's website (www.securecomputing.com) to obtain patches. See paragraph 60 of this Certification Report regarding the application of patches generated as a result of the Developer's flaw remediation procedure.

III. EVALUATION OUTCOME

Certification Result

55. 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 Firewall Version 5.2.1 meets the Common Criteria Part 3 [d] conformant requirements of Evaluation Assurance Level EAL2, augmented by ALC_FLR.2, for the specified Common Criteria Part 2 [c] extended functionality, when running on the platforms specified in Annex A.

56. The Certification Body has also determined that the TOE meets the minimum SOF claim of SOF-medium and metric given above under the heading ‘Strength of Function Claims’.

Recommendations

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

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

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

60. Only the evaluated TOE configuration should be installed. That for which EAL2 assurance has been demonstrated is specified in Annex A, with further relevant information given above under the headings ‘TOE Scope’ and ‘Evaluation Findings’. Strictly, whilst ALC_FLR.2 gives confidence in the Developer’s flaw remediation procedure, this will not maintain the full EAL2 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.

61. 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 Firewall Version 5.2.1.

TOE Documentation

2. The guidance documents evaluated were:

- Sidewinder Delivery Procedures [j]
- Sidewinder Installation and Configuration Guide [k]
- Common Criteria Evaluated Configuration Guide [l]
- Sidewinder Administrator Guide [m]

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.

Environmental Configuration

5. Details of the TOE’s environmental configuration are provided above under the headings ‘Evaluated Product’ and ‘TOE Scope’. This includes the platforms (including hardware, firmware and software) covered by the scope of the evaluation of the TOE.

6. Further details of the hardware requirements are provided in Annex B under the heading ‘Hardware and Firmware Dependencies’.

7. Annex C provides details of the test configuration.

(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, operating on a commercially available Intel Pentium class hardware platform with 2 network interfaces, provides a hybrid firewall solution that supports both application-level proxy and packet filtering.

3. The TOE contains SecureOS, which is an extended version of the BSD UNIX operating system that 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.

Design Subsystems

6. 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 IP addresses and network interfaces combination) 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 Dependencies

7. No extraordinary security demands are placed upon the hardware platform and peripheral equipment used by the TOE. The equipment is expected to meet the customary demands for reliable, secure operation of typical operating systems as provided by standard Intel PC computing platforms.

8. The TOE requires a minimum processor speed and RAM size, and is designed to operate on generic Intel Pentium platforms, as specified above under the heading ‘TOE Scope’.

9. The TOE also requires specific graphics cards that are compatible with the X-Windows used by the Console Graphical User Interface (GUI). The list of compatible graphics cards is provided on the Developer’s website (www.securecomputing.com/index.cfm?sKey=734).

10. Further discussion of compatible hardware platforms and compatible hardware components is provided above under the heading ‘Platform Issues’.

11. The security features assumed to be present and operational on the hardware platform include:

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

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

c. A system motherboard providing 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 100 Hz to support the internal time management within the kernel.

12. If any of the network interface cards support wake-on LAN, or special external command features, the hardware connections to support those features should not be connected.

TSF Interface

13. 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. Typically this is via the Console GUI, Console Command Line and Remote GUI Client (Cobra).

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.

(This page is intentionally blank)

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 Sidewinder Console GUI and the Sidewinder Console Command Line. In addition, the single-use authentication server used by the TOE during testing was the SafeWord authentication server.

Platform Issues

4. The Evaluators noted that the environment used for the Developer's testing of the TOE comprised the following hardware:

- hardware: Compaq Proliant ML370
- CPU: Intel Pentium III, 733 MHz
- RAM: 512 MB
- hard disk: Compaq 9 GB SCSI drive
- 3.5" floppy disc drive
- network interfaces: 2 Intel 10/100 cards
- CD-ROM
- monitor
- keyboard

5. The above test environment was located on its own network, and was connected to internal and external networks, providing services to support all of the possible test procedures and scenarios.

6. The Evaluators performed their independent testing of the TOE on the above hardware platform and on one additional hardware platform from the list recommended on the Developer's website (www.securecomputing.com/index.cfm?sKey=734) as follows:

- hardware: Dell PowerEdge 2650
- CPU: twin Intel XEON, each 2,200 MHz - testing used only 1 CPU
- RAM: 1 GB
- hard disk: Seagate 18GB SCSI drive
- network interfaces: 2 Intel Pro cards
- CD-ROM
- monitor
- keyboard

7. The Evaluators' tests on the hardware platforms identified in paragraph 6 above formed part of their examination of the Developer's programme of compliance testing.