National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Secure Computing Corporation, 2340 Energy Park Drive, Saint Paul, Minnesota 55108

Sidewinder Version 7.0.0.02

Report Number:	**CCEVS-VR-VID10089-2007**
Dated:	**9 November 2007**
Version:	**1.1**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Santosh Chokhani
Scott Shorter
Orion Security Solutions
McLean, VA

Common Criteria Testing Laboratory

Manuel Cintron
Tammy Compton
David McDermitt
Catherine Sykes
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of SCC Sidewinder (henceforth referred to as Sidewinder). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in October 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.3.

Sidewinder is a network security gateway that allows an organization to connect to the Internet while protecting the systems on its internal network from unauthorized users and network attackers. Sidewinder 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. Sidewinder provides a comprehensive set of Internet services and proxies.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.3) have been met.

The technical information included in this report was obtained from the Sidewinder Version 7.0.0.02 Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	• Software: o Sidewinder Software Version 7.0.0.02 o Sidewinder 7.0 Management Tools • Hardware for Sidewinder appliances: o Models 110D/210D: SW70-845A-B/B-B o Models 410D/510D: SW70-860A-A/B-A o Model 1100D: SW70-1950A-A o Models 2100D/2150D: SW70-2950B-A/A-A o Model 4150D: SW70-2900A-A o Model RM700: SW70-860C-A

Item	Identifier
	o Model TNG: SW70-TNGA-A Note – Model TNG is also identified as the TNG(Fw), Tactical Network-Layer Gateway (Firewall) and MESHnet Firewall
Protection Profile	U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 22, 2000
ST:	Sidewinder Version 7.0 Security Target, Part Number 00-0944961-I, 09-November 2007
Evaluation Technical Report	Evaluation Technical Report for SCC Sidewinder, (Proprietary), Version 4.0, October 26, 2007 Science Applications International Corporation. *Evaluation Technical Report for Secure Computing Sidewinder (Non-proprietary)*, Version 1.0, October 26, 2007
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2 Part 2: Evaluation Methodology, Supplement: ALC_FLR- Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Secure Computing Corporation
Developer	Secure Computing Corporation.
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Santosh Chokhani, Orion Security Solutions, McLean VA Scott Shorter, Orion Security Solutions, McLean VA

3 Architectural Information

The TOE consists of a Sidewinder appliance with Sidewinder Software Version 7.0. The TOE also includes the Admin Console client software (the Sidewinder 7.0 Management Tools). This software is provided with every Sidewinder appliance; it is also provided as a separate part of every Sidewinder Software version 7.0 product distribution. The administration client software runs on a local, generic computing platform with a Windows operating system; however, the platform and Windows OS are not part of the TOE.

3.1 Proxy agents to be Evaluated

The FTP, HTTP (non-caching), SMTP, Telnet, and Generic proxy agents are all included within the scope of the evaluation. Other protocol-aware proxy agents and services provided by Sidewinder are excluded from the scope of the evaluation.

3.2 Evaluated TOE Configuration

The Sidewinder is configured to control the flow of TCP/IP traffic between two network interfaces. Its Intel-processor-based computing platform includes at least three network interfaces. The environment includes a commercially available, single-use authentication server that is compatible with Sidewinder such as SafeWord PremierAccess[1] or any RADIUS server. The environment also includes a generic administrative workstation platform running on a Windows operating system.

1. The hardware configuration requirements are as follows:
    1. CPU: Intel, 1Ghz or greater
    2. RAM: 512 MB minimum
    3. Media:
        - Minimum of 8 GB of disk storage
    4. Network: At least 3 network interfaces
    5. SVGA video and display (optional)
    6. US Keyboard (optional)
2. Additional information concerning key hardware components can be found under Sidewinder "hardware" category on the Secure Computing website (www.securecomputing.com/hardware).
3. In addition, a second hardware platform is required in the IT environment for the local administration workstation running the Sidewinder 7.0 Admin Console software. The minimum configuration required for this platform is as follows:
    1. CPU: Intel, 1GHz
    2. RAM: 512 MB
    3. OS: MS Windows 2000 Workstation, 2000 Server, or Windows XP
    4. Media:
        - Minimum of 300 MB of available disk storage
        - CD drive
    5. Network: One network interface
    6. SVGA video and display
    7. PS/2 or Serial Mouse
    8. US Keyboard

4 Security Policy

Sidewinder provides the following security features:

[1] Safeword PremierAccess is a Secure Computing Product

4.1 User Data Protection

For the Sidewinder TOE, user data refers only to a user's communication that is transferred through the firewall via one of the many TCP/IP protocols. Sidewinder's Access Control List (ACL) is the key mechanism that implements a site's security policy and, ultimately, determines what user data is allowed to flow. The ACL database rules establish the parameters for data movement, including both authenticated and unauthenticated security policies.

User data is protected by different facilities depending upon the protocol and stage of processing. While user data is within the network stack, it is part of the kernel memory space and, as such, is protected from all user state processing elements on the system. While user data is in the control of a proxy process, it is protected by the SecureOS processing model and type enforcement facilities.

Sidewinder network stack processing ensures that there is no leakage of residual information from previous packets to new packets as they are transferred through the firewall. The memory and file handling systems zero storage blocks as they are reused to prevent residual information leakage.

4.2 Identification and Authentication

The Sidewinder TOE, along with support from the IT environment, supports standard UNIX password authentication and the use of several single-use authentication mechanisms, including the SafeWord Premier Access Authentication Server. Identification attributes are assigned to each administrative user and each user of authenticated protocol services through the firewall.

In either the case of a one time or reusable password, Sidewinder gathers data from the user and the associated service connection and consults the rules to determine if and what form of authentication is required for the service. In the case of passwords, Sidewinder consults its stored user information, determines the password’s validity, and enforces the result of the validity check. In the case of single-use authentication, Sidewinder interacts with the appropriate external authentication server and enforces the results of the password check performed by the remote authentication server.

4.3 Security Management

An administrator uses the Sidewinder Admin Console client (part of the TOE) running on a Windows computer (part of the IT environment) to perform management functions on the Sidewinder. This administrative workstation communicates with the Sidewinder via one of the networks connected to the Sidewinder.

4.4 Protection of the TOE Security Functions

Sidewinder, with its SecureOS operating system, has been designed to be highly resistant to both malicious and accidental attack. It includes system elements that provide several levels of protection for its security functions.

The lowest level of protection is provided by the computing platform Central Processing Unit (CPU). The CPU provides a two-state processing model that limits access to certain privileged instructions to the SecureOS kernel. The SecureOS kernel provides a second layer of protection by limiting user mode access to kernel memory. SecureOS also extends the normal BSD UNIX network stack processing with additional separation control to restrict inter-process communication to certain interfaces.

SecureOS includes Secure Computing Corporation's patented Type Enforcement facilities that enforce mandatory security policy control over all user state processing. The Type Enforcement policy data is loaded onto the system during installation and cannot be modified on an operational system. Type Enforcement ensures that critical data is accessible only via programs designed to use the data and that the impact of any failure will be confined in scope.

The last layer of protection is the controlled access to system services. Administrators must be authenticated to gain access to the system before they are allowed to perform any administrative functions, including the establishment of access control policy for Sidewinder's network services. Subsequent attempts to access Sidewinder via network connections are controlled by that policy.

4.5 Security Audit

SecureOS supplements the normal UNIX Syslog Facilities by providing an audit device to which all processes and the kernel may write audit data. The SecureOS audit device increases the integrity of the audit data, by adding security relevant information, such as the time and the identity of the generating process, to the audit data when it passes through the device within the kernel.

Only those entities with a "need-to-know" are allowed to read the audit data stream. Audit logging daemons are provided to read the audit data stream and log it to a database to facilitate subsequent administrator review and report generation. Also, special administrator-configurable daemons, called audit-bots, monitor the audit data stream for specified events and initiate defined response actions. Sidewinder provides an administrator with great flexibility to define an extensive set of responses, with an optional "Strikeback" response. Type Enforcement is used to prevent the stored audit data from being modified by anyone, including administrators.

Sidewinder provides facilities to generate standard reports as well as a means to produce custom reports, or to view selected audit events. Sidewinder also includes facilities to monitor and free up audit space at appropriate times.

5 Assumptions

The following assumptions were made during the evaluation of Sidewinder:

- It shall be newly installed and configured in accordance with the directives contained in the Installation, Generation and Startup (IGS) documentation.

- Physical access to the configured Sidewinder shall be controlled.

- The configured Sidewinder shall be connected only to networks between which it controls information flow and to a separate network for administrative control.

- The configured Sidewinder shall manage traffic for at least two (2) networks, at least one of which is designated as internal and one is designated as external.

- The configured Sidewinder shall also support a separate network interface that is used exclusively for communications between the TOE, an administration workstation and a single-use authentication device.

- The configured Sidewinder shall support administrative operations via a GUI application, known as Admin Console, running on a Windows system.

- The configured Sidewinder shall require a single-use authentication mechanism for human users sending or receiving FTP or Telnet information. The single-use authentication device, itself, is outside the TOE.

- The configured Sidewinder shall be connected to its administrative workstation and to the single-use authentication device via a separate isolated network that is physically protected from unauthorized access.

- The evaluated configuration does not include remote administration; the TOE is administered by means of a local workstation that is physically protected.

- Only authorized administrators shall be allowed physical access to the Sidewinder hardware computing platform or to the administrative workstation for such purposes as starting the system.

6 Documentation

The following documentation was used as evidence for the evaluation of the Sidewinder:

6.1 Configuration Management

1. Sidewinder Configuration Management Plan, Part Number 00-0944963-A, Version Date 20 June 2005

6.2 Delivery and Operation

1. Sidewinder Delivery Procedures, Part Number 00-0944962-A, 30 October 2005
1. Sidewinder v7.0 Startup Guide, SWOP-MN-STRT70-A, March 2007
2. Common Criteria Evaluated Configuration Guide, 86-0947005-B, July 2007

6.3 Design Documentation

1. Functional Specification for Sidewinder Security Server, v 1.24 2007/05/04
2. Man pages for Version 7.0
3. Design Document for the Sidewinder System, SCC, v1.22, 2006/02/03
4. Sidewinder Source Code Subset Rationale.doc
5. Source code identified in Sidewinder Source Code Subset Rationale.doc
6. Sidewinder Security Policy Model, revision 00-0945999-A, 2006/07/24.

6.4 Guidance Documentation

1. Sidewinder v7.0 Startup Guide, SWOP-MN-STRT70-A, March 2007
2. Common Criteria Evaluated Configuration Guide, 86-0947005-B, July 2007
3. Sidewinder v7.0 Administration Guide, SWOP-MN-ADMN70-A, March 2007
4. Sidewinder v7.0 Re-imaging without a CD-ROM drive, 89-0946851-A, March 2007

6.5 Life Cycle

1. Secure Computing Product Life Cycle Guide, Document # 00-0931955-E, 31 December 2003
2. Sidewinder Life-Cycle Model, Part Number 00-0944976-A, Version Date 6 July 2005, Common Criteria Assurance Family ALC_LCD.1
3. Sidewinder Development Security Description, Part Number 00-0944975-A, Version Date 12 August 2005, Common Criteria Assurance Family ALC_DVS.
4. Sidewinder G2 Version 7.0 Development Tools Definition, Part Number 00-0944977-B, Version Date 16 December 2005, Common Criteria Assurance Family ALC_TAT.1

6.6 Testing

1. Sidewinder Network Gateway Test Plan for Sidewinder Version 7.0-00-0944971-C, June 15, 2007.
2. Sidewinder v7.0.0.02 Test Coverage Analysis-00-0944966-A, June 1, 2007.
3. Sidewinder v7.0.0.02 Test Depth Analysis-00-0944967-B, June 1, 2007.
4. Sidewinder v.7.0.02 Test Package-00-0944968-E, July 25, 2007
5. Sidewinder Network Gateway Security Version 7.0.0.02 Test Report-00-0944969-C, July 25, 2007.
6. CC00100: Sidewinder Proxy Rule Attribute Verification Test Procedure, v 1.23, June 14, 2007.
7. CC00200: Rule Protection Test Procedure, v 1.10, May 10, 2007.
8. CC00300: Sidewinder Audit Data Generation Test Procedure, v 1.7, April 16, 2007.
9. CC00400: Sidewinder Prevention of Audit Data Loss Test Procedure, v 1.15, June 14, 2007.
10. CC00500: Sidewinder Protected Audit Trail Test Procedure, v 1.12, June 18, 2007.
11. CC00600: Audit Review Test Procedure, v 1.11, April 27, 2007.
12. CC00700: Multiple Authentication Test Procedure, v 1.10, May 16, 2007.
13. CC00800: Authentication Failure, v 1.17, May 17, 2007.
14. CC00900: Domain Separation Test Procedure, v 1.10, May 17, 2007.
15. CC01000: System Integrity Test Procedure, v 1.9, May 18, 2007.
16. CC01100: Residual Data Test Procedure, v 1.11, April 27, 2007.
17. CC01200: Sidewinder Time Processing Test Procedure, v 1.8, April 16, 2007.
18. CC01300: Sidewinder Time Stamp Test Procedure, v 1.8, May 21, 2007.
19. CC01400: Sidewinder FTP Permissions Test Procedure, v 1.11, June 14, 2007
20. CC01500: Sidewinder HTTP Permissions Test Procedure, v 1.11, May 21, 2007.
21. CC01600: Sidewinder Generic TCP Proxy Procedure, v 1.14, June 6, 2007.
22. CC01700: Sidewinder Generic UDP Proxy Procedure, v 1.13, June 6, 2007.
23. CC01800: Static Attribute Initialization Test Procedure, v 1.12, June 6, 2007.

24. CC01900: Sidewinder User Validation Test Procedure, v1.14, June 14, 2007.
25. CC02000: Sidewinder Security Function Management Test Procedure, v 1.14, June 14, 2007.
26. CC02100: Sidewinder UDB Protection Test Procedure, v 1.12, July 24, 2007.
27. CC02200: Sidewinder Users and Roles Test Procedure, v 1.13, June 11, 2007.
28. CC02300: Proxy Authentication Test Procedure, v 1.8, May 24, 2007.
29. SY00600: Sidewinder TCP-based IP Filter Procedure, v 1.12, June 14, 2007.
30. SY00700: Sidewinder UDP-based IP Filter Procedure, v 1.13, June 14, 2007.
31. KE00400: Sidewinder ICMP processing and port not reachable test procedure, v 1.10, April 27, 2007.
32. KE00800: Penetration Test Procedure, v 1.6, April 16, 2007
33. Actual Test Results

6.7 Vulnerability Assessment

- Sidewinder Guidance Documentation Analysis, April 9, 2007
- Sidewinder G2 Security Appliance Models with Sidewinder G2 Software Version 7.0 Strength of Function Analysis, 31 May 2006
- Sidewinder Network Gateway Security Version 7.0 Vulnerability Analysis, Part Number 00-0944972-B, July 10, 2007

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the SCC Sidewinder, Version 1, August 27, 2007.

Note that the security functions as described in section 4 above are provided by the TOE application with support from the environment. The hardware, operating system, and type enforcement capabilities do not provide TOE Security Function Interface (TSFI) and thus the evaluation of the coverage of testing of those components was not performed.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification and high level design. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces in the design. These security functions include:

- Security Audit
  - Application proxy connections audited
  - Audit review and filtering capability
  - Audit storage response capability
  - Proper security management of audit configuration
- Identification and Authentication
  - Lockout
  - Single use passwords
  - Administrator I&A and application proxy I&A
- User Data Protection
  - Traffic filtering on type of IP packet
  - Redirection capability
  - Application proxy syntax validation

- Security Management
    - Restriction of management to authorized administrators
- Protection of the TSF
    - Timestamp
    - Discretionary access control settings for system integrity

7.2 Evaluation Team Independent Testing

The evaluation team installed the product according the Evaluated Configuration Guide, reran all developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

Functional tests confirmed that:

- Changes to the security attributes of roles are properly audited,
- Password length and complexity requirements are enforced,
- Firewall configuration files and type enforcement policy files cannot be modified through the filesystem to bypass audit requirements, and
- IPv4 packets with a broadcast source address are rejected.

The vulnerability testing confirmed that:

- No open source vulnerability reports are applicable to the current version,
- IPv4 packets with loopback source are logged and rejected,
- UDP fragments are logged and rejected when the firewall is configured to permit only telnet,
- IPv4 packets with source routing are logged and rejected,
- Attempts by external hosts to use a spoofed source address of an internal host is logged and rejected,
- Attempts to perform TCP SYN scans through the TOE are logged and rejected, and
- Application passwords are protected from buffer overflow attacks.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is as follows:

- Software:
    - Sidewinder Software Version 7.0.0.02
    - Sidewinder 7.0 Management Tools
- Hardware for Sidewinder appliances:

- Models 110D/210D: SW70-845A-B/B-B
- Models 410D/510D: SW70-860A-A/B-A
- Model 1100D: SW70-1950A-A
- Models 2100D/2150D: SW70-2950B-A/A-A
- Model 4150D: SW70-2900A-A
- Model RM700: SW70-860C-A
- Model TNG: SW70-TNGA-A.

To use the product in the evaluated configuration, the product must be configured as specified in Common Criteria Evaluated Configuration Guide, 86-0947005-B, July 2007 and Sidewinder v7.0 Startup Guide, SWOP-MN-STRT70-A, March 2007.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.3 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.2] and CEM version 1.0 [5], [6]. The evaluation determined the SCC Sidewinder TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.3 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Sidewinder product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from SCC and performed a CM audit.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.3 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

- Note there is non-trivial functionality omitted from the evaluation and testing, including IKE/IPSec and IPv6, anti-virus, SSL termination, and others. Refer to the Security Target for more information.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as Sidewinder Version 7.0.0.02 Security Target, Part Number 00-0944961-I, 09 November 2007.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.2, January 2004.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.2, January 2004.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.2, January 2004.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

[6] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[7] Science Applications International Corporation. *Evaluation Technical Report for Secure Computing Sidewinder (Non-proprietary)*, Version 1.0, October 26, 2007.

[8] Science Applications International Corporation. *Evaluation Technical Report for Secure Computing Sidewinder (Proprietary)*, Version 4.0, October 26, 2007.

[9] Science Applications International Corporation. *Evaluation Team Test Report for the Secure Computing Sidewinder (SAIC and SCC Proprietary)*, Version 2.0, October 30, 2007.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Sidewinder Version 7.0.0.02 Security Target, Part Number 00-0944961-I, 09 November 2007