National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Sidewinder G2 Security Appliance Models
EAL4+ with Basic and Medium PP Compliance

Report Number: **CCEVS-VR-05-0130**
Dated: **October 27, 2005**
Version: **1.0**

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

Kathy Cunningham
NSA

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Commercial Licensed Evaluation Facility (CLEF)

BT Syntegra
United Kingdom

Table of Contents

1 Executive Summary

The Delta Evaluation of Sidewinder G2 Security Appliance Model 410 EAL4+ with Basic and Medium PP Compliance was performed by Science Applications International Corporation (SAIC) in the United States and was completed on October 10, 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.2 and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

The Delta Evaluation consisted of an assessment of the evaluation efforts perform in the United Kingdom by BT Syntegra CLEF to confirm the mutual recognition claim, and the associated U.S. Department of Defense Application-level Firewall Protection Profiles for Basic and Medium Robustness modifications to the Security Target to include the additional AVA_VLA.3 and ALC_FLR.3 requirements.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.2) 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 adduced. This Validation Report is not an endorsement of the Sidewinder G2 Security Appliance Model 410 EAL4+ with Medium PP Compliance product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team reviewed the activities of the evaluation teams, the SAIC Delta ETR, the National Security Agency (NSA) testing results, and provided guidance on technical issues and evaluation processes. 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 evaluation completed by BT Syntegra in the UK supports the mutual recognition claims and that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.3 and AVA_VLA.3) have been met.

1.1 Evaluation Details

Evaluation Completion: October 20, 2005

Evaluated Product: Sidewinder G2 Security Appliance Model 410 EAL4+ with Medium PP Compliance

Software: Sidewinder G2 Software Version 6.1.0.05.E51
Sidewinder G2 6.1 Management Tools

Hardware: Model 410: SW61-750A-8-B

Developer: Secure Computing Corporation
2675 Long Lake Road
Saint Paul, Minnesota 55113

CCTL: Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

CLEF: BT Syntegra
Sentinel House, Harvest Crescent
Ancells Park, Fleet
Hampshire, GU51 2UZ

Validation Team: Kathy Cunningham
National Security Agency (NSA)
9800 Savage Rd
Ft. Meade, MD 20755

Evaluation Class: EAL 4 augmented with ALC_FLR.3 and AVA_VLA.3

Completion Date: October 27, 2005

1.2 Interpretations

The Evaluation Team determined that no CCIMB Interpretations were applicable to this evaluation.

The Validation Team concurred with the Evaluation Team that no CCIMB Interpretations were applicable to this evaluation.

1.3 Threats to Security

The Security Target identifies the following threats for the evaluated product.

T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T. MODEXP	An attacker with moderate attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.

The Security Target also identifies the following threats for the IT environment of the TOE:

TE.DOMSEP	An unauthorized person may attempt to bypass the security mechanism in order to launch attacks on the TOE.
TE.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
TE.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
TE.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

The following PP Threat was omitted from this ST because remote administration is not part of the evaluated configuration.

T.PROCOM: An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

2 Identification

2.1 ST and TOE Identification

ST: Sidewinder G2 Security Appliance Models EAL4+ with Medium PP Compliance Security Target, Part Number 00-09843554-J, Date 3 October 2005

TOE Identification:

Software:

- Sidewinder G2 Software Version 6.1.0.05.E51
- Sidewinder G2 6.1 Management Tools

Hardware for Sidewinder G2 Security Appliances:

- Model 410: SW610750A-8-B

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004, ISO/IEC 15408.

Protection Profile (PP) Identification – The TOE claims conformance to PP's:

- U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 22, 2000
- U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, January 2004, version 2.2, CCIMB-2004-01-004

2.2 TOE Overview

The TOE is any Sidewinder G2 Security Appliance Model with Sidewinder G2 Software Version 6.1.0.05.E51. Sidewinder is a firewall and access control security platform for the enterprise. Enabling the implementation of "safe, secure extranets for e-business," Sidewinder configured in its operational environment delivers strong security while maintaining performance and scalability. It provides access control of communication and information flow between two or more networks using application-level proxy and packet

filtering technology. The operational environment for the Sidewinder software is a typical Intel-based architecture Pentium PC computing platform. The configured Sidewinder provides the highest levels of security by using SecureOS™, an enhanced UNIX operating system that employs Secure Computing's patented Type Enforcement™ security technology. Type Enforcement technology protects Sidewinder by separating all processes and services on the firewall.

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. Section 2.3.2 of the ST identifies the proxies included in the Sidewinder evaluated configuration.

2.3 IT Security Environment

Sidewinder operates in an environment where it provides a single point of connectivity between at least two networks. Typically one network is viewed as the inside of an organization, 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. Sidewinder's role is to limit and control all information flow between the networks.

2.3.1 Physical Boundaries

The TOE consists of a Sidewinder G2 Security Appliance with Sidewinder Software Version 6.1.0.05.E51. The TOE also includes the Admin Console client software (the Sidewinder G2 6.1 Management Tools). This software is provided with every Sidewinder G2 Security Appliance; it is also provided as a separate part of every Sidewinder Software version 6.1 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.

2.3.2 Logical Boundaries

The logical boundaries of the TOE can be described in the terms of the security functions that the TOE provides.

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.

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 ACL 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.

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 establishes the rules 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.

Protection of 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.

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 security "alarms", each with its corresponding "strikeback" responses. Type Enforcement is used to prevent the stored audit data from being modified by anyone, including administrators.

Sidewinder provides facilities to generate a variety of 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.

3 Security Policy

The Security Target does not identify any Security Policies for the evaluated product.

The following PP Organizational Security Policy was omitted from this ST because remote administration is not part of the evaluated configuration.

P.CRYPTO: Triple DES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1).

4 Assumptions

4.1 TOE Assumptions

The following TOE assumptions are identified in the Security Target:

A.PHYSEC	The TOE is physically secure.
A.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.PROLIN	The communication path between the TOE (i.e., authentication client) and the single-use authentication server is physically protected. The communication path between the TOE and the administrator Windows computer is physically protected, also.

The following PP Assumption was omitted from this ST because remote administration is not part of the evaluated configuration.

A.REMACC: Authorized administrators may access the TOE remotely from the internal and external networks.

4.2 Environment Assumptions

The following assumptions are identified for the Authentication server and the local administration platform in the Security Target:

A.ASPHYSEC	The authentication server and local administration platform are physically secure.
A.ASMODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities in the authentication server and local administration platform is considered moderate.
A.ASGENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the authentication server or on the local administration platform.
A.ASPUBLIC	The authentication server and local administration platform do not host public data.
A.ASNOEVIL	Authorized administrators of the authentication server and local administration platform are non-hostile and follow all administrator

	guidance; however, they are capable of error.
A.ASNOREMO	Human users who are not authorized administrators cannot directly or locally access the authentication server or the local administration platform.
A.BENIGN	The Windows OS running on the local administration platform will provide necessary computing services to the TOE, but will not tamper with it.

5 Architectural Information

Sidewinder operating with three network interfaces provides a hybrid firewall solution that supports both application-level proxy and packet filtering. The Sidewinder software consists of a collection of integrated components. The base component is SecureOS™, a secure operating system. This OS is an extended version of the BSD UNIX operating system. It includes Secure Computing's patented 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 Sidewinder firewall application layer processing is done. 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.

Sidewinder is configured to control the flow of TCP/IP traffic between two network interfaces. Its Pentium processor-based computing platform includes at least three network interfaces, floppy drive and CD ROM drive. The environment includes a commercially available, single-use authentication server that is compatible with Sidewinder such as SafeWord PremierAccess1 or any RADIUS server. The environment also includes a generic administrative workstation running the Sidewinder 6.1 Admin Console software on a Windows operating system.

6 Documentation

Purchasers of Sidewinder G2 v 6.1.0.05.E51 will receive the following documentation:

- Administrative Guidance for receiving, installing and managing the TOE
- Startup Guide Sidewinder G2 Firewall, PN SWOP-MN-STRT61-A, February 2004
- Common Criteria Evaluated Configuration Guide, PN 00-0943795-G, May 2005
- Sidewinder G2 Firewall Administration Guide, PN SWOP-MN-ADMN61-A, February 2004

7 IT Product Testing

Evaluation team testing at NSA, heretofore referred to as "the NSA evaluation team," was completed in October 20, 2005. Using the results of the VLA.2 evaluation by the BT Syntegra evaluation team, the NSA evaluation team performed the following activities during testing:

1. Installation of the TOE in its evaluation configuration
2. Vulnerability Testing (AVA_VLA.3)

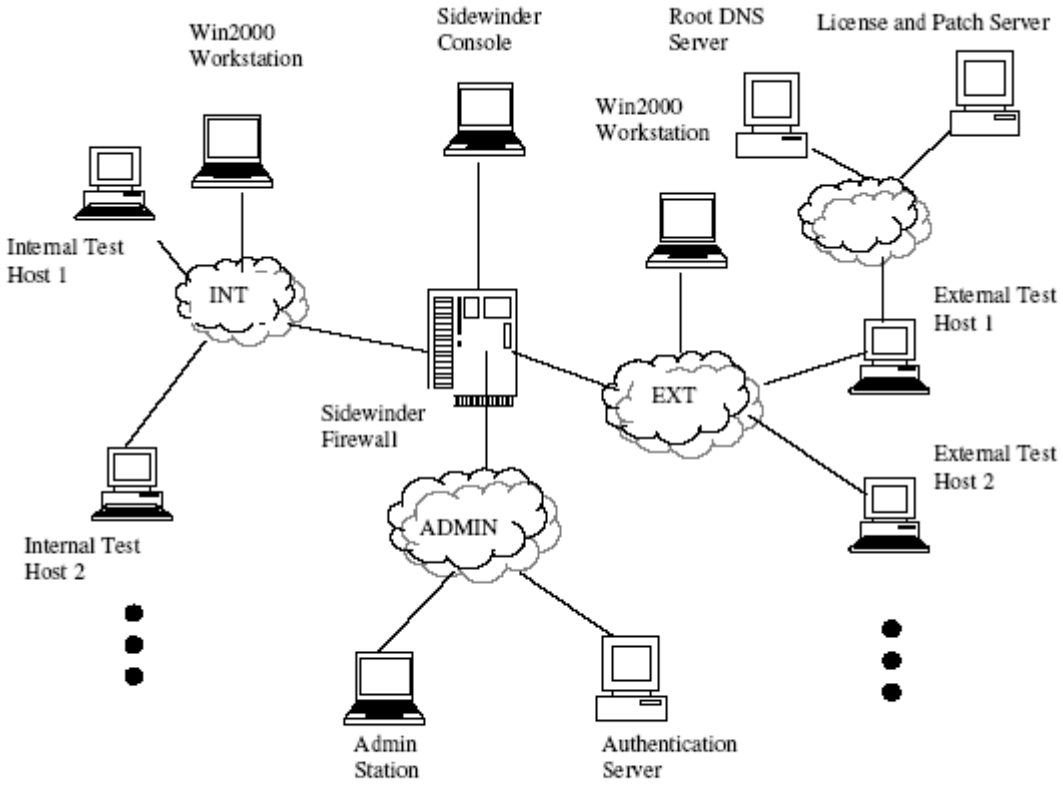
Tools employed by the NSA evaluation team for independent testing included the same category of tools employed by the BT Syntegra evaluation team, as well as in-house developed tools, which assisted in determining that the TOE was resistant to penetration attacks performed by attackers possessing a moderate attack potential. Numerous In-house tools were developed to stress network protocols. The tools developed specifically targeted the application layer of the protocol stack. The team also developed packet generators, (TCP, UDP, ICMP), denial of service (DoS) tools, small programs, and shells designed for a specific purpose.

The results of the evaluation team tests and the evaluation penetration tests demonstrated the Sidewinder G2 Appliance behaved as claimed in the Security Target. The testing found that the product was implemented as described in the functional specification.

8 Evaluated Configuration

8.1 BT Syntegra Evaluation Configuration

The TOE version 6.1 software was provided on a CD. The evaluators installed it on the specified hardware platforms. The TOE was also supplied as hardware appliances, onto which the TOE version 6.1 software was installed. Figure 3-1 below shows the architectural layout of the test environment used by the evaluators.



Developer test environment network diagram

The specific configurations of the hardware platforms used during evaluator tests were as follows:

Hardware	CPU	RAM	Hard Disk	Network Interfaces
Dell PowerEdge 1750	Two 2.8 GHz CPUs	2 Gbytes memory	36 Gbytes	2 Embedded 4 Intel Pro/1000 MT
Dell PowerEdge 2650	Two 3.066 GHz CPUs	2 Gbytes memory	4 x 36 Gbytes	2 Embedded 8 Intel Pro/1000 MT
Dell PowerEdge 6650	Four 2.5 GHz CPUs	2 Gbytes memory	4 x 36 Gbytes	2 Embedded 12 Intel Pro/1000 MT
Appliance 210	One 2.6 GHz CPU	512 Mbytes memory	40 Gbytes	1 Embedded 2 Intel Pro/1000 MT
Appliance 310	One 2.8 GHz CPU	512 Mbytes memory	36 Gbytes	2 Embedded 4 Intel Pro/1000 MT
Appliance 515	Two 2.8 GHz CPU	2 Gbytes memory	2 x 36 Gbytes	2 Embedded 4 Intel Pro/1000 MT
Appliance 2150	Two 3.066 GHz CPU	2 Gbytes memory	4 x 36 Gbytes	2 Embedded 8 Intel Pro/1000 MT
Appliance 4150	Four 2.5 GHz CPU	2 Gbytes memory	4 x 36 Gbytes	2 Embedded 24 Intel Pro/1000 MT

8.2 The NSA Evaluation Team Configuration

A Sidewinder G2 Model 410, preloaded with Version 6.1.0.05.E51 of the software was tested for security vulnerabilities. The testing environment consisted of two networks, one a protected internal network and the other an external network comprised of attacking machines. Each network had a mix of machines, running an assortment of operating systems. These networks were separated by a Sidewinder G2 firewall. The firewall was configured to allow FTP, TELNET, HTTP, DAYTIME (UDP/TCP), and SMTP traffic to traverse the firewall. All other services were blocked.

9 Results of the Evaluation

SAIC reviewed the Secure Computing Corporation (SCC) provided Evaluation Technical Reports produced by the Syntegra U.K. Commercial Laboratory Evaluation Facility (CLEF) and associated U.S. Department of Defense Application-level Firewall Protection Profiles for Basic and Medium Robustness modifications to the Security Target for the Customer's Sidewinder G2 Security Appliance v6.1. SAIC reviewed the Syntegra Evaluation Technical Report (ETR) to assess if the evaluation conclusions for each work unit appear to be correct and substantiated by the rationale provided to support each conclusion. Additionally SAIC evaluated the updated Security Target to ensure compliance with the Basic and Medium Robustness Application-level Firewall Protection Profiles.

The Evaluation Team accomplished the Delta Evaluation by providing Notes, Comments, or Vendor Actions to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

Section 4 SAIC Assessment Team Observations in the Evaluation Team's CCEVS report states"

> "Overall ETR Descriptions – For the most part, SAIC found the amount of evaluator rationale to be very similar to the amount of rationale its evaluation team's put into ETRs. The rationale varied on particular work units but the overall trend was similar. This supports the mutual recognition claims"

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the NSA evaluation team applied the AVA_VLA.3 CEM work units. The NSA 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 NSA evaluation team's misuse analysis, vulnerability analysis, and the performance of penetration tests demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 22, 2000 and the U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000 allow for remote administration. The evaluated configuration of the TOE did not include remote administration; therefore the following PP components were omitted from this evaluation:

1. A. REMACC Assumption
2. P.CRYPTO OSP
3. O.ENCRYPT TOE Objective
4. O.REMACC TOE Environment Objective
5. FCS_COP.1 SFR
6. T.PROCOM Threat

11 Security Target

The Security Target is identified as Sidewinder G2 Security Appliance Models EAL4+ with Medium PP Compliance Security Target, Part Number 00-09843554-J, Date 3 October 2005.

The document identifies the security functional requirements necessary to implement Information Flow Protection and TOE Self Protection security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.3 and AVA_VLA.3

12 Glossary

The following definitions are used throughout this document:

User: Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Human User: Any person who interacts with the TOE.

External IT entity: Any IT product or system, untrusted or trusted, outside the TOE that interacts with the TOE.

Role: A predefined set of rules establishing the allowed interactions between a user and the TOE

Identity: A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Authentication Data: Information used to verify the claimed identity of a user.

Authorized Administrator: A role which human users may be associated with to administer the security parameters of the TOE.

Authorized External IT entity: Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE.

Password: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Software: The programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE): An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

13 Abbreviations

Abbreviations	Long Form
ACL	Access Control List
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CEM	Common Evaluation Methodology
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IATF	Information Assurance Technical Framework
IGS	Installation, Generation and Startup
IT	Information Technology
ITSEC	IT Security Evaluation Criteria
I&A	Identification and Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OR	Observation Report
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
QA	Quality Assurance
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTAP/CCEVS	Trusted Technology Assessment Program / Common Criteria Evaluation and Validation Scheme

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[4] Common Evaluation Methodology for Information Technology Security Evaluation, dated January 2004, version 2.2, CCIMB-2004-01-004.

[5] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[6] U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 22, 2000

[7] U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000