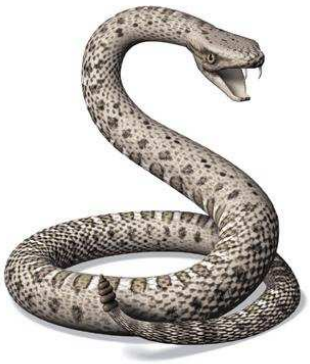
Part Number 00-0937063-E

Version Date 27 September 2002

SIDEWINDER Version 5.2.1

SECURITY TARGET



Prepared by:

Secure Computing Corporation

2675 Long Lake Road

Saint Paul, Minnesota 55113

Table of Contents

List of Tables

1 Security Target Introduction

1 This introductory section presents security target (ST) identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

2 A ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., target of evaluation (TOE)). An ST principally defines:

a) A set of assumptions about the security aspects of the environment, a list of threats which the product is intended to counter, and any known rules with which the product must comply (in Section 3, Security Environment).

b) A set of security objectives and a set of security requirements to address that problem (in Sections 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE which meet that set of requirements (in Section 6, TOE Summary Specification).

3 The ST for a TOE is a basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation. Because the audience for a ST may include not only evaluators but also developers and "those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE,"[1] this ST minimizes terms of art from the Common Criteria for Information Technology Security Evaluation (CC).

4 The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

5 This section provides ST and TOE identification information.

ST Title:	Sidewinder Version 5.2.1 Security Target
ST Author:	Dwight D. Colby
ST Revision Number:	00-0937063-E
ST Date:	September 27, 2002
TOE Identification:	Sidewinder Version 5.2.1
CC Identification:	Common Criteria for Information Technology

[1] ***Common Criteria for Information Technology Security Evaluation*** **(CC), Part 1, Annex C, par. C.1, par 2.**

	Security Evaluation, Version 2.1, August 1999 (also known as ISO 15048)
Assurance Level:	EAL2, augmented with ALC_FLR.2
ST Evaluation:	Syntegra
Keywords:	Proxies, application-level, information flow control, firewall, packet filter, network security, traffic filter, security target

1.2 Conventions, Terminology, and Acronyms

6 This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.2.1 Conventions

7 This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

8 The CC identifies four operations to be performed on functional requirements; *assignment*, *iteration*, *refinement*, and *selection* are defined in paragraph 2.1.4 of Part 2 of the CC.

a) The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

b) The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.

c) The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].

d) The **iteration** operation is used when a component is repeated with varying operations. Showing the iteration number in parenthesis following the component identifier and element identifier (iteration_number) denotes iteration.

9 Explicitly stated requirements are identified by ***bold italic*** with an ***(EXP)*** extension.

1.2.2 Terminology

10 In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

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 of 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.

11 In addition to the above general definitions, this Security Target provides the following specialized definitions:

Authorized Administrator – A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized external IT entity – Any IT product or system, outside the scope of the TOE that may identify and authenticate itself for the purpose of communicating with the TOE.

Note, the evaluated TOE does not communicate with authorized external IT entities, but it does provide management control related to such entities. .

1.2.3 Acronyms

12 The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IGS	Installation, Generation and Startup
IT	Information Technology
OSP	Organizational Security Policy

PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13

14 The following abbreviations are also used in this Security Target:

ACL	Access Control List

1.3 Security Target Overview

15 Sidewinder is a software 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 hardware 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.

16 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 identifies the proxies included in the Sidewinder evaluated configuration.

17 The evaluated TOE only includes the Sidewinder software.

1.4 References

18 The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1, CCIMB-99-031.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033.
[CEM_PART1]	Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, version 0.6.
[CEM_PART2]	Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.
[CC/CEM_FLR]	Common Methodology for Information Technology Security – Part 2 Evaluation Methodology, Supplement: ALC_FLR Flaw Remediation, dated February 2002, version 1.1, CEM-2001/0015R

1.5 Common Criteria Conformance Claims

19 The TOE conforms to the security functional components as defined in [CC_PART2], with the assurance level of EAL2, augmented with ALC_FLR.2 as identified in [CC_PART3]

20

2 TOE Description

21 This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

22 Sidewinder software operating on a commercially available Intel Pentium class hardware platform with two 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.

2.2 Application Context

23 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 Evaluation Application Context

2.3.1 Physical and Logical Boundaries

24 The following physical and logical boundaries are drawn around the above mentioned configurations to scope the TOE evaluation:

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

b) Physical access to the configured Sidewinder shall be controlled.

c) The configured Sidewinder shall be connected only to networks between which it controls information flow.

d) The configured Sidewinder shall support two (2) networks, one designated as internal and one designated as external.

e) The configured Sidewinder shall support administrative operations on the system console only. The system console consists of a video display, mouse, and keyboard directly connected to the hardware computing platform running Sidewinder software. Only authorized administrators are allowed to use the mouse and keyboard to interact with the TOE.

f) The configured Sidewinder shall require a single-use authentication mechanism for human users sending or receiving FTP or Telnet information.

g) Only authorized 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.

2.3.2 Proxies to be Evaluated

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

2.3.3 Features not to be Evaluated

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

a) Remote Administration

b) Virtual Private Network (VPN)

c) 3rd Party Authentication

d) User Defined Proxies

e) Cloning

f) Failover

g) URL Filtering

h) Mail Filtering

i) Policy Acceleration Network Cards

2.3.4 Physical Scope and Boundary

27 The TOE consists of the Sidewinder Software Version 5.2.1.

2.3.4.1 Evaluated TOE Configuration

28 The software TOE is configured in the following IT environment. The TOE IT environment includes a generic computing platform that executes the software to control the flow of IP traffic between two network interfaces. The platform is comprised of a generic Pentium processor-

based computing platform with 2 network interfaces, floppy drive, CD ROM drive, video display, mouse and keyboard. The environment also includes a commercially available, single-use authentication server that is compatible with Sidewinder such as Safeword[2] or any RADIUS server.

29 The hardware configuration requirements are as follows:

a) CPU: Intel Pentium II, Pentium III, Pentium IV, or Pentium XEON

b) RAM: 192 MB minimum

c) Media:

- Minimum of 4 GB of disk storage
- 3.5" Floppy drive
- CD ROM drive
- DAT drive (optional)

d) Network: 2 network interfaces (Ethernet)

e) SVGA video and display

f) PS/2 or Serial Mouse

g) US Keyboard

30 Additional information concerning key hardware components can be found under Sidewinder "hardware requirements" category on the Secure Computing website (www.securecomputing.com). To the extent that this product information identifies specific components that have been tested, such components shall be used.

2.3.4.2 Hardware Security Considerations

31 No extraordinary security demands are placed upon the hardware platform and peripheral equipment used by the Sidewinder software TOE. This equipment is expected to meet the customary demands for reliable, secure operation of typical Unix or Microsoft Servers as provided by standard Intel PC computing platforms. The security features assumed to be present and operational on the hardware platform include:

a) The CPU must provide a two state processing model to support the separation of the kernel processing from the application processing.

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

c) The system motherboard must provide a battery backup for the clock to maintain time information when the system is shut down. Also the CPU

[2] **Safeword is a Secure Computing Product**

or ancillary hardware must provide a periodic cycle time operating at a minimum of 100Hz to support the internal time management within the kernel.

d) 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. The Sidewinder software drivers will not enable any such special features.

2.3.5 Logical Scope and Boundary

32 The TOE with support from the IT environment provides the following security features:

a) Security Management [SW_FMT]

b) Identification and Authentication [SW_FIA]

c) User Data Protection [SW_FDP]

d) Protection of Security Functions [SW_FPT]

e) Audit [SW_FAU]

2.3.5.1 Security Management [SW_FMT]

33 An administrator logged in at the Sidewinder console accomplishes management of the Sidewinder TOE. Typically, the administrator manages all aspects of system operation using Sidewinder's graphical management interface known as Cobra.

2.3.5.2 Identification and Authentication [SW_FIA]

34 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 Authentication Server. Identification attributes are assigned to each administrative user and each user of authenticated protocol services through the firewall. Authentication attributes are assigned to services.

35 In the case of passwords, Sidewinder gathers data from the user, determines its validity and enforces the result of the validity check. In the case of single-use authentication, Sidewinder gathers data, determines the required authentication facility, interacts with the external authentication server and enforces the results of the policy check performed by the remote authentication server.

2.3.5.3 User Data Protection [SW_FDP]

36 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.

37 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.

38 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.

2.3.5.4 Protection of Security Functions [SW_FPT]

39 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.

40 The lowest level of protection is provided by the computing platform Central Processing Unit (CPU), required as part of the operational environment for the TOE software. 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.

41 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.

42 The last layer of protection is the controlled access to system services. Administrators must log into the system console and be authorized 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.

2.3.5.5 Audit [SW_FAU]

43 SecureOS extends the normal UNIX Syslog facilities and specific application audit facilities by providing a system 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 to the audit data when it passes through the device within the kernel.

44 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.

45 Sidewinder provides a rich capability for audit reporting. A variety of standard and custom reports can be generated. Sidewinder also includes the capability to monitor and free up audit space at appropriate times.

3 TOE Security Environment

46 This section describes the security problem that the TOE is intended to solve. This includes information about the security aspects of the physical environment, personnel access, and network connectivity of the TOE.

47 Assumptions about the security aspects of the environment and manner of use are identified.

48 Known or assumed threats to the assets protected by the TOE or the TOE IT and operating environments are described.

49 Organization security policies (OSP) statements or rules to which the TOE must comply or implement are identified.

50 The TOE is intended to be used in environments in which, at most, sensitive but unclassified information is processed, or where the sensitivity level of information in both the internal and external networks is equivalent.

3.1 Assumptions

51 The TOE is assured to provide effective security measures in a cooperative, non-hostile environment when installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user/administrative guidance.

3.1.1 TOE Assumptions

52 The TOE claims the assumptions in the table below:

Table 1. Assumptions for TOE Operational Environment

Assumption Identifier	Assumption Description
A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
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

Assumption Identifier	Assumption Description
	authentication server is either physically or logically protected.

3.1.2 Additional Environment Assumptions

53 Because the authentication server plays a critical role in the TOE's ability to enforce its security policy, the following condition are assumed to exist with respect to the authentication server.

Table 2. Assumptions for the Authentication Server

Assumption Identifier	Assumption Description
A.ASPHYSEC	The authentication server is physically secure.
A.ASLOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities in the authentication server is considered low.
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.
A.ASPUBLIC	The authentication server does not host public data.
A.ASNOEVIL	Authorized administrators of the authentication server 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 remotely access the authentication server..

3.2 Threats

54 This section helps define the nature and scope of the security problem by identifying assets that require protection, as well as threats to those assets.

55 Threats may be addressed by the TOE or by the TOE operating environment.

3.2.1 Threats Addressed by the TOE

56 The TOE addresses all threats listed in the following table. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

Table 3. Threats Addressed by the TOE

Threat Identifier	Threat Description.
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 attackers actions.
T. LOWEXP	An attacker with low attack potential may

Threat Identifier	Threat Description.
	attempt to bypass the TSF to gain access to the TOE or the assets it protects.

3.2.2 Threats Addressed by the TOE Operating Environment

57 The following threats are addressed by the TOE operating environment.

Table 4. Threats Addressed by the TOE Operating Environment

Threat Identifier	Threat Description.
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.

3.3 Organizational Security Policies

58 This ST does not identify any OSPs.

4 Security Objectives

59 The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both. The CC identifies two categories of security objectives:

a) Security objectives for the TOE, and

b) Security objectives for the Operating Environment

4.1 Security Objectives for the TOE

60 The TOE accomplishes the following security objectives:

Table 5. Security Objectives for the TOE

Objective Identifier	Objective Description
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols and ensuring that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions,

Objective Identifier	Objective Description
	and must ensure that only authorized administrators are able to access such functionality.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

4.2 Security Objectives for the Environment

61 All the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the non-IT security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE software. They will be satisfied largely through application of procedural or administrative measures.

Table 6. Security Objectives for the TOE Operating Environment

Objective Identifier	Objective Description
O.PHYSEC	The TOE must be physically secure.
O.LOWEXP	The TOE's operating environment must protect itself against malicious attacks from an attacker with low attack potential, aimed at discovering exploitable vulnerabilities.
O.PUBLIC	The TOE must not host public data.
O.NOEVIL	Authorized administrators must be non-hostile and follow all administrator guidance; however, they are capable of error.
O.SINGEN	Information must not flow among the internal and external networks unless it passes through the TOE.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
O.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
O.ADMTRA	Authorized administrators must be trained as to establishment and maintenance of security policies and practices.
O.DOMSEP	The TOE's operating environment must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

Objective Identifier	Objective Description
O.PROLIN	The communication path between the TOE (i.e., authentication client) and the single-use authentication server must be either physically or logically protected.
O. ASPHYSEC	The authentication server must be physically secure.
O.ASLOWEXP	The TOE's operating environment must protect itself against malicious attacks from an attacker possessing low attack potential, aimed at discovering exploitable vulnerabilities in the authentication server.
O.ASGENPUR	There must be no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the authentication server.
O.ASPUBLIC	The authentication server must not host public data.
O.ASNOEVIL	Authorized administrators of the authentication server must be non-hostile and follow all administrator guidance; however, they are capable of error.
O.ASNOREMO	Human users who are not authorized administrators must not directly or remotely access the authentication server.

5 TOE IT Security Requirements

5.1 TOE Security Requirements

62 This section provides functional and assurance requirements that must be satisfied by a Security Target-compliant TOE.

5.1.1 TOE Security Functional Requirements

63 The security functional requirements for this Security Target consist of the following components from Part 2 of the CC, summarized in the following Table 7. In addition to the CC Part 2 SFRs, one explicitly stated requirement is also identified in the table. The SFRs are provided in their entirety in the subsequent paragraphs.

Table 7. TOE Security Functional Requirements

Functional Components	
FMT_SMR.1	Security roles
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_AFL.1	Authentication failure handling
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.8 (EXP)	Invocation of authentication mechanisms
FDP_IFC.1	Subset information flow control (1)
FDP_IFC.1	Subset information flow control (2)
FDP_IFF.1	Simple security attributes (1)
FDP_IFF.1	Simple security attributes (2)
FMT_MSA.1	Management of security attributes (1)
FMT_MSA.1	Management of security attributes (2)
FMT_MSA.1	Management of security attributes (3)
FMT_MSA.1	Management of security attributes (4)
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data (1)
FMT_MTD.1	Management of TSF data (2)
FDP_RIP.1	Subset residual information protection
FPT_RVM.1	Non-bypassability of the TSP

Functional Components	
FPT_SEP.1	TSF domain separation (1)[3]
FPT_STM.1	Reliable time stamps (1)[4]
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of security functions behavior (1)
FMT_MOF.1	Management of security functions behavior (2)

FMT_SMR.1 Security roles

64 FMT_SMR.1.1 - The TSF shall maintain the roles [authorized administrator].

FMT_SMR.1.2 - The TSF shall be able to associate **human** users with **the authorized administrator** role.

FIA_ATD.1 User attribute definition

65 FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;

b) association of a human user with the authorized administrator role;

c) and password].

FIA_UID.2 User identification before any action

66 FIA_UID.2.1 - The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1 Authentication failure handling

67 FIA_AFL.1.1 - The TSF shall detect when **four** unsuccessful authentication attempts occur related to **authorized TOE administrator access**.

68 FIA_AFL.1.2 - When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **add increasing time**

[3] **The second iteration of this requirement is found in the environment section.**
[4] **The second iteration of this requirement is found in the environment section.**

delays and, after ten successive failed attempts, terminate that login session.

FIA_UAU.5 Multiple authentication mechanisms

69 FIA_UAU.5.1 - The TSF shall provide [a password mechanism] to support user authentication.

70 FIA_UAU.5.2 - The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rule:

a) reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator].

71 Application Note: The password mechanism in this requirement can be considered one of "multiple" mechanisms because it operates in conjunction with the following requirement, FIA_UAU.8, which invokes a single-use authentication mechanism.

FIA_UAU.8 (EXP) Invocation of authentication mechanism

72 ***FIA_UAU.8.1(EXP) - The TSF shall invoke the single-use authentication server to authenticate a user's claimed identity according to the [following rules:***

a) single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user.]

73 Requirements Overview: This Security Target consists of multiple information flow control Security Function Policies (SFPs). The CC allows multiple policies to exist, each having a unique name. This is accomplished by iterating FDP_IFC.1 for each of the two named information flow control policies. The first policy identified is called the UNAUTHENTICATED SFP. The subjects under control of this policy are external IT entities on an internal or external network sending information through the TOE to other external IT entities. The second policy identified is called the AUTHENTICATED SFP. The subjects under control of this policy are human users on an internal or external network who must be authenticated at the TOE before using the services in FIA_UAU.5. The information flowing between subjects in both policies is traffic with attributes, defined in FDP_IFF.1.1, including source and destination addresses. The rules that define each information flow control SFP are found in FDP_IFF.1.2. Component FDP_IFF.1 is iterated twice to correspond to each of the two iterations of FDP_IFC.1.

FDP_IFC.1 Subset information flow control (1)

74 FDP_IFC.1.1 - The TSF shall enforce the [UNAUTHENTICATED SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another; and

c) operation: pass information].

FDP_IFC.1 Subset information flow control (2)

75 FDP_IFC.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] on:

a) [subjects: a human user or external IT entity that sends and receives FTP and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.5;

b) information: FTP and Telnet traffic sent through the TOE from one subject to another; and

c) operation: initiate service and pass information].

FDP_IFF.1 Simple security attributes (1)

76 FDP_IFF.1.1 - The TSF shall enforce the [UNAUTHENTICATED SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address; and
- no other subject attributes ;

b) information security attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- Service; and
- destination service port range].

77 FDP_IFF.1.2 - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

78 FDP_IFF.1.3 - The TSF shall enforce the [none].

79 FDP_IFF.1.4 - The TSF shall provide the following [none].

80 FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

81 FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules:

a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed

address of the source subject is an external IT entity on the loopback network;

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) The TOE shall provide an HTTP protocol filtering proxy that provides administrative control over a specific set of command requests from the commonly used HTTP protocol.]

FDP_IFF.1 Simple security attributes (2)

82 FDP_IFF.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address; and
- no other subject attributes;

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service (i.e., FTP and Telnet);
- security relevant service command; and
- destination service port range].

83 FDP_IFF.1.2 - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- the human user initiating the information flow authenticates according to FIA_UAU.4;
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

- the presumed address of the source subject, in the information, translates to an internal network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- the human user initiating the information flow authenticates according to FIA_UAU.4;
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

84 FDP_IFF.1.3 - The TSF shall enforce the [none].

85 FDP_IFF.1.4 - The TSF shall provide the following [none].

86 FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

87 FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules:

a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) The TOE shall provide Telnet and FTP protocol filtering proxies that support user authentication. The FTP proxy provides administrative control over a specific set of command requests from the commonly used FTP protocol.]

88 Application Note: The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a "presumed address" is used to identify source and destination addresses. A "service", listed in FDP_IFF.1.1(b), could be identified, for example, by a source port number and/or destination port number. A "service command", also mentioned FDP_IFF.1.1(b), could be identified, for example, in the case of the File Transport Protocol (FTP) service as an FTP STOR or FTP RETR.

FMT_MSA.1 Management of security attributes (1)

89 FMT_MSA.1.1 (1) - The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(1)] to [the authorized administrator].

FMT_MSA.1 Management of security attributes (2)

90 FMT_MSA.1.1(2) - The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(2)] to [the authorized administrator].

FMT_MSA.1 Management of security attributes (3)

91 FMT_MSA.1.1(3) - The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to ***delete*** [and create] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the authorized administrator].

FMT_MSA.1 Management of security attributes (4)

92 FMT_MSA.1.1(4) - The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to ***delete*** [and create] the security attributes [information flow rules described in FDP_IFF.1(2)] to [the authorized administrator].

FMT_MSA.3 Static attribute initialization

93 FMT_MSA.3.1 - The TSF shall enforce the [UNAUTHENTICATED_SFP and AUTHENTICATED_SFP] to provide

restrictive default values for **information flow** security attributes that are used to enforce the SFP.

94 FMT_MSA.3.2 - The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

95 Application Note: Following TOE installation, the default configuration is to allow no traffic through the firewall.

FMT_MTD.1 Management of TSF data (1)

96 FMT_MTD.1.1(1) - The TSF shall restrict the ability to *query, modify, delete,* [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

FMT_MTD.1 Management of TSF data (2)

97 FMT_MTD.1.1(2) - The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

FDP_RIP.1 Subset residual information protection

98 FDP_RIP.1.1 - The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects: [process memory and network message buffers].

99 Application Note: This requirement is met by zeroing all newly allocated memory pages and by ensuring that the network traffic packet processing is based upon the actual packet size as reported by the NIC hardware.

FPT_RVM.1 Non-bypassability of the TSP

100 FPT_RVM.1.1 - The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation (1)

101 FPT_SEP.1.1 - The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

102 FPT_SEP.1.2 - The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable time stamps (1)

103 FPT_STM.1.1 - The TSF shall be able to provide reliable time stamps for its own use.

104 Application Note: The word “reliable” in the above requirement means that the order of the occurrence of auditable events is preserved

FAU_GEN.1 Audit data generation

105 FAU_GEN.1.1 - The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [the events in Table 8].

106 FAU_GEN.1.2 - The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 8].

Table 8. Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
	Unsuccessful attempts to authenticate the authorized administrator role.	The user identity and the role.
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.
FIA_UAU.5	The final decision on authentication.	The user identity and the success or failure of the authentication.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts	The identity of the offending user
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1(1)	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_MOF.1	Use of the functions listed	The identity of the authorized

Functional Component	Auditable Event	Additional Audit Record Contents
	in this requirement pertaining to audit.	administrator performing the operation.

FAU_SAR.1 Audit review

107 FAU_SAR.1.1 - The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

108 FAU_SAR.1.2 - The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

109 FAU_SAR.3.1 - The TSF shall provide the ability to perform *searches and sorting* of audit data based on:

a) [user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times; and

e) ranges of addresses].

FAU_STG.1 Protected audit trail storage

110 FAU_STG.1.1 - The TSF shall protect the stored audit records from unauthorized deletion.

111 FAU_STG.1.2 - The TSF shall be able to *prevent* modifications to the audit records.

FAU_STG.4 Prevention of audit data loss

112 FAU_STG.4.1. - The TSF shall *prevent auditable events, except those taken by the authorized **administrator*** and [shall limit the number of audit records lost] if the audit trail is full.

FMT_MOF.1 Management of security functions behavior (1)

113 FMT_MOF.1.1(1) - The TSF shall restrict the ability to *enable and disable* the functions:

a) [operation of the TOE; and

b) multiple use authentication as described in FIA_UAU.5]

to [an authorized administrator].

114 Application Note: By “Operation of the TOE” in a) above, we mean having the TOE start up (enable operation) and shut down (disable

operation). By "multiple use" in b) above, we mean the management of password and single-use authentication mechanisms.

FMT_MOF.1 Management of security functions behavior (2)

115 FMT_MOF.1.1(2) - The TSF shall restrict the ability to *enable, disable, determine and modify the behaviour of* the functions:

a) [audit trail management; and

b) communication of authorized external IT entities with the TOE]

to [an authorized administrator].

116 Application Note: Determine and modify the behavior of element b (communication of authorized external IT entities with the TOE) is intended to cover functionality such as providing a range of addresses from which the authorized external entity can connect.

5.1.1.1 SFRs With Strength of Function (SOF) Declarations

117 The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism. In the case of this security target, this minimum level shall be SOF-medium.

118 Specific strength of function metrics are defined for the following requirement:

119 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 mechanisms must demonstrate SOF-medium, as defined in Part 1 of the CC.

5.2 Security Requirements for the IT Environment

120 The TOE has the following security requirements allocated to its IT environment.

Table 9. Functional Requirements for IT Environment

Functional Components	
FIA_UAU.4	Single-use authentication mechanisms
FPT_SEP.1	**TOE operating environment** domain separation (2)
FPT_STM.1	Reliable time stamps (2)

FIA_UAU.4 Single-use authentication mechanisms

121 FIA_UAU.4.1 – The **TOE operating environment** shall prevent reuse of authentication data related to [the authentication mechanism employed to authenticate: human users sending or receiving information through the TOE using FTP or Telnet].

FPT_SEP.1 **TOE operating environment** domain separation (2)

122 FPT_SEP.1.1 – The **TOE operating environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

123 FPT_SEP.1.2 – The **TOE operating environment** shall enforce separation between the security domains of subjects in the **TOE operating environment's scope of control.**

FPT_STM.1 Reliable time stamps (2)

124 FPT_STM.1.1 - The **Hardware Platform** shall be able to provide reliable time stamps for its own use.

5.3 TOE Security Assurance Requirements

125 The TOE claims compliance to EAL 2 level of assurance. The security assurance requirements (SARs) for this Security Target include the EAL 2 SARs in Part 3 of the CC. These SARs are identified in the following Table 10:

Table 10. EAL2 Assurance Components

Assurance class	Assurance components
Class ACM: Configuration management	ACM_CAP.2 Generation support and acceptance procedures
Class ADO: Delivery and operation	ADO_DEL.1 Delivery Procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal Functional Specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1Administrator guidance
	AGD_USR.1 User guidance
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

5.3.1 Additional Security Assurance Requirement

126 This section describes the maintenance assurance requirements from the CC Part 3 that the TOE must satisfy in addition to the previously listed EAL 2 SARs.

127 In particular, ALC_FLR.2 for flaw reporting procedures that are designed to help ensure that reported defects in the TOE are addressed by the developer is added. ALC_FLR.2 is not included in any EAL. This single additional SAR needed for the Security Target is restated verbatim from the CC.

Table 11. Additional SAR to Augment EAL 2

Assurance class	Assurance components
Class ALC: Life cycle support	ALC_FLR.2 Flaw reporting procedures

128

5.3.1.1 ALC_FLR.2 Flaw reporting procedures

129 **Developer action elements:**

130 ALC_FLR.2.1D – The developer shall provide flaw remediation procedures addressed to TOE developers.

131 ALC_FLR.2.2D – The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

132 ALC_FLR.2.3D – The developer shall provide flaw remediation guidance addressed to TOE users.

133 **Content and presentation of evidence elements:**

134 ALC_FLR.2.1C – The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

135 ALC_FLR.2.2C – The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

136 ALC_FLR.2.3C – The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

137 ALC_FLR.2.4C – The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

138 ALC_FLR.2.5C – The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.l

139 ALC_FLR.2.6C – The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

140 ALC_FLR.2.7C – The procedures for processing reported security flaws shall provide safeguards that any corrections to these flaws do not introduce any new flaws.

141 ALC_FLR.2.8C – The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

142 **Evaluator action elements:**

143 ALC_FLR.2.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6 TOE Summary Specification

144 This section presents a functional overview of the TOE, the security functions implemented by the TOE, and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

145 The TOE implements the following security functions:

a) Security Management [SW_FMT]

b) Identification and Authentication [SW_FIA]

c) User Data Protection [SW_FDP]

d) Protection of Security Functions [SW_FPT]

e) Audit [SW_FAU]

6.1.1 Security Management [SW_FMT]

146 The Cobra graphical user interface (GUI) provides the external interfaces required for an administrator to manage the Sidewinder firewall and utilize its security features. Cobra windows-oriented, point-and-click features are used to turn services on or off and to select configuration options.

147 Administrators are also provided with convenient access to a wide variety of audit files and reports. The action of reviewing audit logs is accomplished via the *acat* and *asort* commands at the console or an xterm window. Other command line features such as *cd* to change directories and *ls* to list the files in a directory are available, but these are only used for convenience; they are not required to manage security features and are not being evaluated.

6.1.1.1 Using Cobra

148 At startup, the administrative user responds to the login prompt for name and password, activates the x-windows environment via the *startx* command, and clicks an icon to start Cobra. At this point, the administrator can use Cobra to administer the firewall. Each individual administrative user is assigned one or more of the administrator roles supported by Sidewinder. When an administrator establishes a login session on the console, their initial command environment operates in a Type Enforcement domain appropriate for a generic user. Once they have logged into the system, an administrator may change their operational role to any of the other roles they are authorized to use. The role change is accomplished via the GUI authentication. An administrator may operate in only one role at a time. (FMT_SMR.1)

149 The management interface software associated with the GUI function initiates an appropriate action in response for the administrator's data input. The major Cobra command menu selections are:

- Firewall Policy Configuration
- Services Configuration
- Reports and Monitoring
- Firewall Administration

6.1.1.2 Firewall Policy Configuration

150 The administrator manages the rules for access control and IP filtering which comprise the Firewall Policy. The authorized administrator is permitted to delete, modify, or add rules to the Firewall Policy. Sidewinder protects the ACL rule database via Type Enforcement and administrator roles. Only software operating in the correct Type Enforcement domain and under control of an authenticated administrator may initiate changes to the ACL database. (FMT_MSA.1).

151 Only an authorized administrator is allowed to query, modify, delete and assign the user attributes for individual users. Sidewinder protects the user database information via Type Enforcement and administrator management roles. (FMT_MTD.1).

6.1.1.3 Services Configuration

152 The authorized administrator can start up and shut down the Sidewinder as well as manage the password and single-use authentication mechanisms that are enforced. The authorized administrator also enables, disables and controls the behavior of communication between authorized external IT entities and Sidewinder. In addition, the authorized administrator manages the operation of the audit trail. Only individuals authorized to operate in the administrator role are allowed to manage the audit trail, to enable and disable services, or to change the configuration information related to these services. (FMT_MOF.1).

153 An authorized administrator, and only an authorized administrator, is allowed to create and delete the security attributes controlling the flow rules for information passing through the Sidewinder. (FMT_MSA.1)

6.1.1.4 Reports and Monitoring

154 Audit reporting is provided through the use of commands entered at the command line outside of Cobra. After login, the administrative user changes to the administrative role with the *srole* command, and uses the *acat* and *asort* commands to access audit files. Only individuals

authorized to operate in the administrative role can examine and manage the audit trail information. (FMT_MOF.1)

6.1.1.5 Firewall Administration

155 After TOE installation is complete, default values for ACLs and IP filter rules are restrictive and do not allow inbound or outbound information flows. Thereafter, the administrator may choose to change the flow rules by specifying new values or by accepting values that are pre-selected by the GUI. (FMT_MSA.3)

156 Sidewinder permits the authorized administrator to manage the list of administrators, shutdown the system and change the system date and time stamp. Access to operations such as changing the system time is controlled via the Sidewinder Type Enforcement policy. Access is restricted to software initiated by input from an authenticated administrator. (FMT_MTD.1)

157 **Functional Requirements Satisfied by TOE:** FMT_MOF.1 (1) & (2); FMT_MSA.1 (1), (2), (3), & (4); FMT_MSA.3; FMT_MTD.1 (1) & (2); and FMT_SMR.1

6.1.2 Identification and Authentication [SW_FIA]

6.1.2.1 Sidewinder Users

158 Sidewinder supports two classes of users. Those that are administrators and those that are network communication users. The identification information for each Sidewinder administrative user includes the following information (FIA_ATD.1):

- The user login name
- User data including full name, office number, phone, home phone, their home directory and default login shell
- The hashed version of the password required to login to the console or via telnet, assuming the relevant ACL rules call for password authentication.
- List of roles in which the individual is allowed to operate.

159 Communication users are those individuals identified within the Firewall user database for the purpose of defining control over who may utilize specific firewall inter-network communication services. These users cannot log into the Sidewinder and have no direct access to the Sidewinder. In response to specific access control rules, the Sidewinder may interact with these users to require an authentication action to assure that policy required expressed in the access control rule are satisfied before the user is allowed to utilize the communication protocol through the firewall. For network communication users, the following information is retained.

- The user's name
- User description
- The user's employee ID value
- The user's organization
- up to 4 other information fields
- Users password, which is stored in an encrypted form,
- Users group membership.

160 The only human users that Sidewinder recognizes are administrators; only administrators are allowed to directly control the behavior of Sidewinder. Administrative users have to identify and authenticate themselves to Sidewinder before they can take any TSF-mediated actions. (FIA_UID.2).

161 External IT entities are identified by IP address and network interface, or "burb", to which they are connected. Communication user access from external IT entities to Sidewinder proxies and services is controlled by the policy specified in the form of an Access Control List (ACL). When a communication user requests a network connection, Sidewinder checks the ACL entries to determine whether to make the requested connection on behalf of the user or to deny the request.

162 Sidewinder includes the processing elements that establish administrative login sessions. All processing that establishes an administrator-controlled session, must perform the following functions.

- Consult the access control list to determine whether the specific request is to be allowed or denied.
- Perform the method of authentication as required in the controlling access control list entry in the firewall security policy.
- Establish an administrator login session upon completion of a successful authentication exchange.

6.1.2.2 Password Authentication

163 During system installation, an initial administrator ID and password are established. Following installation, the initial administrator is allowed to login to the console by providing the correct ID and password. (FIA_ATD.1)

164 For each administrative user, Sidewinder maintains typical UNIX identification information including UNIX user name, login password, identification data, login shell and allowed administrative roles. This "weak" authentication merely requires a user to enter a predefined password at login time (FIA_UAU.5). Passwords are implemented by

means of a permutational mechanism that meets the standard of SOF-medium.

165 After four unsuccessful password authentication attempts for a UNIX password, Sidewinder takes actions to decrease the rate at which additional password guesses are allowed. After a total of 10 authentication failures, the login session is terminated. (FIA_AFL.1)

6.1.2.3 Strong Authentication

166 Strong authentication requires a user to enter a unique, one-time, response to a logon challenge or special code presented by the authentication server. The user must provide a one-time, or single-use, authentication value during the logon process. A "warder" in Sidewinder communicates with the authentication server to authenticate a user when an ACL specifies that form of authentication.

167 Sidewinder, as configured for evaluation, requires single-use authentication for network users of Telnet and FTP services. On Sidewinder, the type of authentication used for an authentication-controlled service is determined by the appropriate service related ACL rule in the site-specific firewall security policy. Sidewinder supports external single-use password authentication facilities such as SafeWord™ Authentication Server, RADIUS, SecurID, or SNK. The Sidewinder TOE operating environment includes an authentication server to perform the single-use password authentication. (FIA_UAU.4)

168 Sidewinder communicates with the authentication server to ascertain that network users have successfully authenticated with the single-use password mechanism as a prerequisite for using Telnet and FTP. (***FIA_UAU.8 (EXP)***). Sidewinder detects unsuccessful authentication attempts and generates audit records.

169 **Functional Requirements Satisfied by TOE:** FIA_AFL.1; FIA_ATD.1; FIA_UAU.5, ***FIA_UAU.8(EXP)***, and FIA_UID.2

170 **Functional Requirements Satisfied by TOE Environment:** FIA_UAU.4

6.1.3 User Data Protection [SW_FDP]

6.1.3.1 Residual Information Protection

171 The Sidewinder virtual memory system within the kernel ensures that as physical memory pages are taken from a free list and added to a given process's memory space they are zeroed and that there is no residual data passed between processes.

172 Data read from and written to the network is managed in kernel message buffers, mbufs and mbuf clusters. The kernel does not zero these buffers prior to reuse for reading a new buffer. Rather the avoidance of data leakage from one network message to another is managed by keeping

track of the amount of data placed in the message. The network interface controller provides the data count to the driver. This information is maintained in the mbuf header information, separate from the message data. The kernel network stack code maintains the integrity of this critical data element and ensures that when a subsequent message is transmitted on another network interface card or the message is transferred to a memory buffer in user space, the correct number of data bytes are moved. (FDP_RIP.1)

6.1.3.2 Information Flow Control

173 For information protocols supported by Sidewinder, the information flow is determined by the relevant network protocol connection attributes established by the administrator. In most cases, the access control rules do not allow specification of an authentication requirement.

174 On Sidewinder, the telnet and FTP proxies can also be configured to require user authentication to utilize the service. In this case, an administrator must define the service users in the user database and establish ACL rules for telnet and FTP which specify that the service is contingent upon successful authentication. The ACL specifies the particular type of single-use authentication mechanism that is to be used. (FDP_IFC.1)

6.1.3.3 Security Attributes

175 On Sidewinder, the flow of information through the system is affected by key information security attributes. In particular, the flow rules depend upon the presumed source and destination addresses, the Sidewinder interface (burb) on which the traffic arrives or departs, and the requested service. Sidewinder employs the burb concept as a convenience that allows administrators to refer to one or more network interfaces from the same security point of view when defining flow rules. On Sidewinder there is no mandatory distinction between internal networks and external networks; they are just separate burbs. The allowed flow between any two networks is determined by the services enabled and the state of the ACL rules in the firewall security policy. (FDP_IFF.1.1)

176 In addition to specific ACL rules, Sidewinder uses these security attributes to enforce some general flow rules that are described in subsequent paragraphs. (FDP_IFF.1.2 and FDP_IFF.1.6)

177 Sidewinder deals with address spoofing issues at two levels. First the nss validates that a source address matches the burb from which the packet is received. Failures of this check are reported as an attack audit event. Also the proxies can determine the burb associated with the connection socket and make ACL policy decisions based on this information independent of the stated source address.

178 By default the Sidewinder IP stack processing rejects IP packets that have a broadcast address as their source address.

179 The Sidewinder IP stack processing rejects IP packets that have a source address on a loop-back network but where received on a non loop-back device.

180 The Sidewinder rejects all IP packets containing source route information and generates a net-probe audit message.

181 Sidewinder processing for HTTP and FTP connections provides controls to check for bad service requests. For HTTP and FTP, the ACL can specify which specific protocol service requests are allowed.

6.1.3.4 Access Control List

182 The Access Control List (ACL) is a Sidewinder mechanism that implements a site's security policy and determines the flow of user data. When an internal or external user requests a network connection, the appropriate proxy or server checks the ACL entries to determine whether to allow the requested connection. The ACL can be configured to allow access from one burb to another, where a burb is a type enforced network area used to isolate network interfaces from each other. Once a particular service connection is allowed by the applicable ACL entry, the flow of data related to that service connection is determined by the specific configuration of that proxy or service capability. Administrative access to the Sidewinder is also determined by means of the ACL.

6.1.3.5 Internet Service Configuration

183 The Sidewinder provides two means of controlling network communications. The first is the more secure application level session based control. The second is a less secure, typical, packet filtering mechanism that operates at the IP network layer of the network stack. The administrator determines which form of control to use for various communication flows when they establish the firewall security policy.

184 Sidewinder includes the network protocol proxies required to transfer communication between networks. These elements are responsible for establishing the network connections, transferring or arranging for the transfer of data between networks, and enforcing firewall security policy decisions.

185 Sidewinder provides proxies for controlling connections to standard network services.

186 Sidewinder supports and controls transfer of data between connected networks via a wide range of Internet application layer protocols. No connection is allowed unless all of the criteria specified in the firewall security policy are satisfied and the firewall policy queries all state that the connection is allowed. All protocol proxies must support network address

translation and service address translation as specified by the response to an ACL query. This supports hiding the structure of one Sidewinder burb from another. The Sidewinder installation includes proxies that support the application layer protocols. It also provides generic TCP and UDP proxies.

6.1.3.6 Data Processing Protection

187 While user data is physically present on Sidewinder, the information is protected by different facilities depending on the protocol, the selected mode of data transfer, and the stage of processing. As the data moves through the firewall, it is either in the control of the network stack or a proxy.

188 A network packet resides in a network message buffer structure, which contains the IP header of the packet. This data is always within the kernel address space and is not subject to modification by any non-kernel processing. The network stack ensures that no residual data from previous packets is leaked to new packets as they flow through the firewall.

189 When the data packet is in the proxy, it resides within memory buffers in that proxy's memory space. The operating system memory management facilities ensure the separation of memory space for each process. The memory and file handling systems ensure there is no residual data leakage by zeroing storage blocks as they are allocated for a new use. (FDP_RIP.1)

190 **Functional Requirements Satisfied by TOE:** FDP_IFC.1 (1) & (2); FDP_IFF.1 (1) & (2); and FDP_RIP.1

6.1.4 Protection of Security Functions [SW_FPT]

191 On Sidewinder the basic integrity of system operation is provided by Sidewinder's Type Enforcement facilities. Type enforcement is used to define a mandatory security policy that specifies the range of operations that may be performed by each process. All Type Enforcement decisions and enforcement are performed at appropriate spots in normal processing sequence of the SecureOS kernel. Since all Sidewinder processing operations are ultimately dependent on kernel services, it provides strong control over system operation that can not be bypassed. This mechanism is used to control which executables, programs, may be used to perform specific Sidewinder functions. Also the Sidewinder Type Enforcement security policy is defined to ensure that no system executable may be modified on an operational system. (FPT_RVM.1)

192 The current Sidewinder Type Enforcement security policy provides approximately 86 different operational domains in which various parts of the system operate. The actions allowed for each of these domains is fully defined by the content of the Type Enforcement security policy. The general design guideline is to provide minimal permission to accomplish the task (FPT_SEP.1 (1)). Type Enforcement controls:

- system-level actions e.g. change clock or reboot, the domain can perform,
- new programs that can execute in the same operational domain,
- process signals that can be sent to other domains,
- object operations that may be performed on the various object types such as files and sockets, and
- network burbs a given domain may interact with.

193

6.1.4.1 Secure Operating System

194 Sidewinder employs a two state CPU processing model that limits access to certain privileged instructions to the SecureOS kernel. The SecureOS kernel limits user mode access to kernel memory. SecureOS also extends the normal BSD UNIX network stack processing with additional separation control to restrict inter-network communication to certain interfaces.

195 Each process has its own address space, which cannot be accessed by other processes, unless they are specifically designed to share memory. Application programs gain access to kernel services, such as opening files or creating new processes, via a well defined set of system calls provided by the kernel.

196 The Sidewinder SecureOS kernel retains the current time value by reading a hardware provided battery-backed real-time clock during system boot. Subsequently it maintains the system time, which can be read by all system processes via cpu supported facilities.

197 Access to the system calls that can alter time values is a restricted action, by an administrator, and one of the two system daemons provided to assist in maintaining the system time. This access is specified in the Sidewinder type enforcement security policy and is enforced by the kernel. (FPT_STM.1 (1))

198 The hardware platform (part of the TOE environment) provides the accurate physical time keeping mechanisms needed by the software TOE to maintain the system time. (FPT_STM.1 (2))

6.1.4.2 Type Enforcement

199 The Type Enforcement mechanism enforces 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. On a normally operating Sidewinder, Type Enforcement provides increased integrity to

data. It also ensures that potential adverse effects of any processing element failure are confined in scope.

200 Type enforcement is based on the least privilege principle whereby any program executing on the system is given only the privileges it needs to accomplish its tasks. When a shell or application is running on Sidewinder, it is executing in a specific domain, which is distinct from other application domains. The various system components are placed in separate domains, user access to these domains is strictly controlled, and the processes running in the domain are only allowed to access specific files.

201 Type enforcement cannot be bypassed; it controls all interactions between domains and file types. Domains must have explicit permission to access specific file types, communicate with other domains, or to access system functions. Any attempts to the contrary fail as if the files never existed.

6.1.4.3 TOE Operating Environment

202 In addition to the Sidewinder hardware platform, the TOE operating environment includes an external authentication server that provides the single-use authentication for FTP and Telnet traffic flowing through Sidewinder.

203 The TOE operating environment is relied upon to maintain a security domain for its own execution that protects it from interference and tampering by untrusted users. This protection is needed, in particular, for the authentication server and its interface to the Sidewinder hardware platform. (FPT_SEP.1 (2))

204 **Functional Requirements Satisfied by TOE:** FPT_RVM.1; FPT_STM.1 (1), and FPT_SEP.1 (1)

205 **Functional Requirements Satisfied by TOE Environment:** FPT_SEP.1 (2) and FPT_STM.1 (2)

6.1.5 Audit [SW_FAU]

206 The Sidewinder generates audit to mark the starting and stopping of the firewall services, including the audit facilities. Audit is also generated to capture pertinent information related to security policy decisions made by Sidewinder. The audit event type and operation specific information is provided in the audit record by the generator before it is written to the Sidewinder audit device. The kernel provides the time stamp and identification information about the audit generator as the audit message passes through the Sidewinder audit device. (FAU_GEN.1)

207 Access to the Sidewinder audit files and audit database are controlled by the Type Enforcement security policy. Audit files are given Type Enforcement attributes that limit access to those processing elements with need to access the data. (FAU_STG.1)

6.1.5.1 Logging

208 SecureOS extends the common UNIX "Syslog" facilities and specific application audit facilities by providing a system audit device to which all processes and the kernel may write audit data. The use of an audit device allows the kernel to add relevant security information to the audit data, such as the identification of the process that initiated the message, its Type Enforcement security attributes, and the system time when the message was sent. The audit data, augmented by this additional security relevant information, cannot be modified or changed. Even an administrator is not allowed to modify current data on the system, although they do have the capability to remove old audit data.

209 Sidewinder logs include extensive information about system usage. It records who is using the system and which services they are using. In general, this tracking is based on the IP addresses of computers, rather than the individuals using the computers. Sidewinder knows which machine is making the request and which machine is the destination of the request. In the case of authenticated telnet and ftp, the user's identity is also collected in the audit logs.

6.1.5.2 Audit Reporting

210 Sidewinder provides special *acat* and *asort* commands for viewing audit files and creating reports. The raw audit files can be searched and sorted, if necessary, to explore issues related to a complex security problem or an attack.

211 Sidewinder authorized administrators can use the *acat* and *asort* commands to review both the live audit and stored audit files. The *acat* command converts the raw audit information into a readable format that can be easily understood by the administrator. (FAU_SAR.1) Sidewinder provides sorting via the *asort* command and special audit filters that allow the administrator to search and select the audit information according to user identity, address, date and time. Sidewinder has an audit filter language, *sacap_filter,* which allows the administrator to specify filter expressions directly within the acat command. (FAU_SAR.3)

6.1.5.3 Audit Data Retention

212 The Sidewinder audit facilities monitor the state of the audit storage area. Based on an administrator configurable setting, when the storage area reaches one threshold it triggers an audit event. At another threshold the system will either terminate operation to avoid any audit loss or remove the oldest audit files and continue to collect the most recent audit.

213 At appropriate times, Sidewinder will act to "roll" the data files, which will compress existing files to free space for more audit. Log files can be

scheduled for a regular daily "roll-over" at a prescribed time, usually at night. However, the action will take place sooner if one of the hourly checks indicates that the logs have exceeded a configured size limit. The "roll-over" consists of producing reports for the newest files, condensing the files (zipping) and "aging" the files to become one generation older. A configured number of previous generations of each log file are kept and then, finally, the oldest files are deleted. Sidewinder can be configured to stop normal operations in the event that the audit data storage area is exhausted. (FAU_STG.4)

214 **Functional Requirements Satisfied by TOE:** FAU_GEN.1; FAU_SAR.1; FAU_SAR.3; FAU_STG.1; and FAU_STG.4

6.2 Assurance Measures

215 This section identifies the Configuration Management, Delivery/Operation, Development, Guidance Documents, Life-cycle Support, Test, and Vulnerability Assessment measures applied by Secure Computing to satisfy CC assurance requirements.

216 The security assurance requirements for this Security Target include the requirements taken from Part 3 of the CC, augmented by, ALC_FLR.2. These assurance components are described in Section 5.3.

6.2.1 Configuration Management

217 The Configuration Management measures applied by Secure Computing include unique identification for configuration items, proper labeling, tracking of configuration items. These configuration management measures are documented within the following Secure Computing documents:

- Sidewinder Configuration Management Plan

Assurance Requirements Satisfied: ACM_CAP.2

6.2.2 Delivery and Operation

218 Secure Computing provides measures to ensure that the TOE is delivered without modification and that it is installed, generated, and started in a way that will lead to the evaluated configuration. These delivery and operation measures are documented within the following Secure Computing documents:

- Sidewinder Delivery Procedure
- Sidewinder Installation and Configuration Guide
- Common Criteria Evaluated Configuration Guide (CCECG)

Assurance Requirements Satisfied: ADO_DEL.1 and ADO_IGS.1

6.2.3 Development

219 Secure Computing provides increasingly refined descriptions of the TOE security functionality. Design documentation consists of a functional specification, which describes the external interfaces of the TOE and a high-level design. In addition, there is a representation correspondence that maps the various representations of the TOE to one another and to this Security Target. This information is provided by the following Secure Computing documents:

- Sidewinder Functional Specification (information files)
- Sidewinder High-Level Design (information files)
- Sidewinder Security Functions Correspondence Analysis

Assurance Requirements Satisfied: ADV_FSP.1, ADV_HLD.1 and ADV_RCR.1.

6.2.4 Guidance

220 Secure Computing provides administrator guidance to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. The guidance includes warnings about functions and privileges that should be controlled in a secure processing environment. These guidance measures are documented within the following Secure Computing documents:

- Sidewinder Installation and Configuration Guide
- Sidewinder Administration Guide
- Common Criteria Evaluated Configuration Guide (CCECG)

Assurance Requirements Satisfied: AGD_ADM.1 and AGD_USR.1

6.2.5 Life-cycle Support

221 Secure Computing provides information describing the procedures that are used to handle reports of security flaws in the TOE. This information is documented within the following Secure Computing document:

- Sidewinder Security Flaw Reporting Procedures
- Common Criteria Evaluated Configuration Guide (CCECG)

Assurance Requirements Satisfied: ALC_FLR.2

6.2.6 Test

222 Secure Computing performs extensive testing of Sidewinder to ensure that it behaves as specified in the design documentation and in accordance with the security functional requirements specified in the ST. Test coverage evidence is provided to demonstrate the extent of testing, and to show that the TOE conforms to its functional specification. These tests

and evidence are presented in the following Secure Computing documents:

- Sidewinder Test Plan/Coverage Analysis
- Sidewinder Test Procedures and Results
- Sidewinder TOE (this is product software, not a document)

Assurance Requirements Satisfied: ATE_COV.1, ATE_FUN.1, and ATE_IND.2

6.2.7 Vulnerability Assessment

223 In addition to the design and testing process, Secure Computing performs vulnerability assessment of the TOE. Firstly, a strength of function analysis is performed on the administrator authentication mechanism in order to gain more confidence in the overall security functionality of the TOE. Secondly, an analysis of the TOE deliverables is performed to identify any flaws or weaknesses that could be exploited by an attack. These vulnerability assessment activities are documented within the following Secure Computing documents:

- Sidewinder Strength of Function Analysis
- Sidewinder Vulnerability Analysis

224 **Assurance Requirements Satisfied:** AVA_SOF.1, and AVA_VLA.1

7 PP Claims

225 This ST makes no PP conformance claims.

8 Rationale

8.1 Rationale for TOE Security Objectives

226 O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

227 O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF that have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

228 O.SECSTA This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

229 O.SELPRO This security objective is necessary to counter the threats: T.SELPRO, T.NOAUTH, T.AUDFUL and T.LOWEXP because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. In particular, it counters attempts from an attacker with low attack potential to bypass the TSF to gain access to the TOE or the assets it protects.

230 O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

231 O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

232 O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

233 O.LIMEXT This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.

Table 12. Mapping Threats to TOE Security Objectives

	T.NOAUTH	T.ASPOOF	T.MEDIAT	T.OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL	T.LOWEXP
O.IDAUTH	X							
O.MEDIAT		X	X	X				
O.SECSTA	X					X		
O.SELPRO	X					X	X	X
O.AUDREC					X			
O.ACCOUN					X			
O.SECFUN	X						X	
O.LIMEXT	X							

8.2 Rationale for the TOE Operating Environment Security Objectives

234 O.PHYSEC The TOE is physically secure.

235 O.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

236 O.PUBLIC The TOE does not host public data.

237 O.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

238 O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

239 O.SINUSE This security objective is necessary to counter the threats TE.REPEAT and TE.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.

240 O.GUIDAN This non-IT security objective is necessary to counter the threat: TE.TUSAGE and T.AUDACC because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

241 O.ADMTRA This non-IT security objective is necessary to counter the threat: TE.TUSAGE and T.AUDACC because it ensures that authorized administrators receive the proper training.

242 O.DOMSEP This non-IT security objective is necessary to counter the threat: TE.DOMSEP because it requires that the TOE's operating environment protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

243 O.PROLIN The communication path between the TOE(.e., authentication client) and the single-use authentication server is either physically or logically protected.

244 O.ASPHYSEC The authentication server is physically secure.

245 O.ASLOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities in the authentication server is considered low.

246 O.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.

247 O.ASPUBLIC The authentication server does not host public data.

248 O.ASNOEVILAuthorized administrators of the authentication server are non-hostile and follow all administrator guidance; however, they are capable of error.

249 O.ASNOREMO Human users who are not authorized administrators can not directly or remotely access the authentication server.

Table 13. Mapping Threats to TOE Operating Environment Security Objectives

	TE.TUSAGE	T.AUDACC	TE.DOMSEP	TE.REPEAT	TE.REPLAY
O.GUIDAN	**X**	**X**			
O.ADMTRA	**X**	**X**			
O.SINUSE				**X**	**X**
O.DOMSEP			**X**		

250 The remaining security objectives for the environment are, in part, a re-statement of the security assumptions. Each of these security objectives traces to the corresponding assumption with a similar name. Objective O.PHYSEC traces to assumption A.PHYSEC, for example.

8.3 Rationale for TOE Security Requirements

251 The functional and assurance requirements presented in this ST are mutually supportive and their combination meet the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. Table 14 illustrates the mapping between the TOE security requirements and the TOE security objectives. Table 12 demonstrates the relationship between the TOE threats and the TOE security objectives. Together these tables demonstrate the completeness and sufficiency of the requirements.

252 The rationale for the SOF is based on the low attack potential identified in this ST, augmented by the need to protect against more than casual attempted breaches of security. SOF-medium is therefore selected. The security objectives imply the need for probabilistic or permutational security mechanisms.

FMT_SMR.1 Security roles

253 Each of the CC class FMT components in this ST depend on this component. It requires the ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

254 This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

FIA_UID.2 User identification before any action

255 This component ensures that before anything occurs on behalf of a user, the users identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_AFL.1 Authentication failure handling

256 This component ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After a specified number of failures, the user is first delayed and then his login session is terminated. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_UAU.5 Multiple authentication mechanisms

257 This component was chosen to ensure that multiple authentication mechanisms are used appropriately in all attempts to authenticate at the TOE from an internal or external network. An additional SOF metric for this requirement is defined to ensure that the mechanisms are of adequate probabilistic strength to protect against authentication data compromise.

This component traces back to and aids in meeting the following objective: O.IDAUTH.

FIA_UAU.8 (EXP) Invocation of authentication mechanism

258 ***This component was chosen to ensure that the TOE invokes the authentication server to authenticate all human users using FTP and Telnet. This component traces back to and aids in meeting the following objective: O.SELPRO.***

FDP_IFC.1 Subset information flow control (1)

259 This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 Subset information flow control (2)

260 This component identifies the entities involved in the AUTHENTICATED information flow control SFP (i.e., users of the services FTP or Telnet sending information to servers and vice versa). The users of these services must be authenticated at the TOE. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes (1)

261 This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes (2)

262 This component identifies the attributes of the users sending and receiving the information in the AUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FMT_MSA.1 Management of security attributes (1)

263 This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to add, delete, and modify within a rule those security attributes that are listed in section FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (2)

264 This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to add, delete, and modify within a rule those security

attributes that are listed in section FDP_IFF.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (3)

265 This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to create and delete rules for security attributes that are listed in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (4)

266 This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to create and delete rules for security attributes that are listed in FDP_IFF.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECFUN, and O.SECSTA.

FMT_MSA.3 Static attribute initialization

267 This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.

FMT_MTD.1 Management of TSF data (1)

268 This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN

FMT_MTD.1 Management of TSF data (2)

269 This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FDP_RIP.1 Subset residual information protection

270 This component ensures that neither information that had flown through the TOE, nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FPT_RVM.1 Non-bypassability of the TSP

271 This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO and O.SECSTA.

FPT_SEP.1 TSF domain separation (1)

272 This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps (1)

273 FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_GEN.1 Audit data generation

274 This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

275 This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review

276 This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

277 This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator, and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECSTA and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

278 This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECSTA and O.SECFUN.

FMT_MOF.1 Management of security functions behavior (1)

279 This component ensures that the TSF restricts the ability of the TOE start up and shut down operation and multiple authentication function to the

authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN, and O.LIMEXT.

FMT_MOF.1 Management of security functions behavior (2)

280 This component was to ensure the TSF restricts the ability to modify the behavior of functions such as audit trail management and communication of authorized external IT entities with the TOE to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN, and O.LIMEXT.

Table 14. Mapping SFRs to TOE Security Objectives

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FMT_SMR.1							**X**	
FIA_ATD.1	**X**						**X**	
FIA_UID.2	**X**					**X**		
FIA_AFL.1				**X**				
FIA_UAU.5	**X**							
FIA_UAU.8 (EXP)				**X**				
FDP_IFC.1 (1)		**X**						
FDP_IFC.1 (2)		**X**						
FDP_IFF.1 (1)		**X**						
FDP_IFF.1 (2)		**X**						
FMT_MSA.1 (1)		**X**	**X**				**X**	
FMT_MSA.1 (2)		**X**	**X**				**X**	
FMT_MSA.1 (3)		**X**	**X**				**X**	
FMT_MSA.1 (4)		**X**	**X**				**X**	
FMT_MSA.3		**X**	**X**					
FMT_MTD.1 (1)							**X**	
FMT_MTD.1 (2)							**X**	
FDP_RIP.1		**X**						
FPT_RVM.1			**X**	**X**				
FPT_SEP.1 (1)				**X**				
FPT_STM.1 (1)					**X**			

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FAU_GEN.1					**X**	**X**		
FAU_SAR.1					**X**			
FAU_SAR.3					**X**			
FAU_STG.1			**X**	**X**			**X**	
FAU_STG.4			**X**	**X**			**X**	
FMT_MOF.1 (1)			**X**				**X**	**X**
FMT_MOF.1 (2)			**X**				**X**	**X**

Added Analysis for FAU_STG.4

281 Requirement FAU_STG.4 requires that the TSF shall limit the number of audit records lost if the audit trail is full. Sidewinder provides a number of capabilities for managing audit information to protect against losing data in the event of a storage failure, exhaustion and/or attack. In the event of exhaustion, or an attack, which leads to audit data exhaustion, Sidewinder can be expected to lose no data. Sidewinder should be configured to halt normal operation upon hitting a threshold capacity on the audit files. This will stop most new audit events long before the remaining storage capacity is exhausted and prevent all data loss. In the event of any storage failure, the loss of audit data is also limited by the automatic capabilities of Sidewinder to format audit data and export the data on a scheduled basis. In this case, the worst-case lose of data is limited to the amount of time since the last regularly scheduled export, typically 24 hours or less.

8.4 Rationale for TOE IT Environment Security Requirements

282 The environmental objective O.DOMSEP is necessary to counter the environmental threat TE.DOMSEP because it ensures the TOE environment's security functions are not bypassed, deactivated, or tampered with by unauthorized users. The environmental requirement FPT_SEP.1 (2) is necessary in order for the TOEs operating environment (the authentication server) to maintain a security domain for its own execution that protects it from interference and tampering by untrusted users. The environment requirement FPT_STM.1 (2) is necessary to provide the hardware platform timekeeping capability needed for reliably marking audit records with the correct time and date.

283 The environmental objective O.SINUSE is necessary to counter the environmental threats TE.REPEAT and TE.REPLAY because it ensures

that authentication data cannot be reused by an attacker attempting to authenticate to the TOE from a connected network. The environmental requirement FIA_UAU.4 is necessary to ensure single-use authentication for human users sending or receiving information through the TOE using FTP or Telnet.

8.5 Rationale for Assurance Requirements

284 The EAL 2 level of assurance was chosen to provide a moderate level of independently assured security, including confidence that the TOE will not be tampered with during delivery. Augmentation with ALC_FLR.2 will also help to ensure that any reported security flaws in the TOE are addressed. This level of assurance will provide sufficient security to protect unclassified information such as that found in government organizations. Information with this importance is assumed, by nature, to have a greater threat for disclosure and/or corruption by unauthorized parties.

8.6 SOF Rationale

285 The rationale for the chosen level of SOF-medium is related to the intended TOE environment. The low attack potential described in the TOE assumptions and the attack potential of the identified threat agents is consistent with the SOF-medium, since protection against greater than casual (as offered by SOF-Basic) attempted breaches of the authentication mechanism is generally required. The security objectives for the TOE imply probabilistic or permutational security mechanisms. The metrics defined are the minimal “industry” standard accepted for passwords.

8.7 Dependency Rationale

286 The following table is provided as evidence that all dependencies have been satisfied in this ST.

Table 15. SFR/SAR Dependency Evidence

SFR/SAR	Dependencies	Satisfied?
FMT_SMR.1	FIA_UID.1	Yes, FIA_UID.2
FIA_ATD.1	NONE	N/A
FIA_UID.2	NONE	N/A
FIA_AFL.1	FIA_UAU.1	No, however FIA_UAU.5 provides the mechanism that is referred to in AFL.1 and can be used to satisfy the dependency.
FIA_UAU.4	NONE	N/A
FIA_UAU.5	NONE	N/A
FIA_UAU.8	FIA_UAU.4	Yes

SFR/SAR	Dependencies	Satisfied?
(EXP)		
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1	 Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_MTD.1	FMT_SMR.1	Yes
FDP_RIP.1	NONE	N/A
FPT_RVM.1	NONE	N/A
FPT_SEP.1	NONE	N/A
FPT_STM.1	NONE	N/A
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FMT_MOF.1	FMT_SMR.1	Yes
ACM_CAP.2	NONE	N/A
ADO_DEL.1	NONE	N/A
ADO_IGS.1	AGD_ADM.1	Yes
ADV_FSP.1	ADV_RCR.1	Yes
ADV_HLD.1	ADV_FSP.1 ADV_RCR.1	Yes Yes
ADV_RCR.1	NONE	N/A
AGD_ADM.1	ADV_FSP.1	Yes
AGD_USR.1	ADV_FSP.1	Yes
ALC_FLR.2	NONE	N/A
ATE_COV.1	ADV_FSP.1 ATE_FUN.1	Yes Yes
ATE_FUN.1	NONE	N/A
ATE_IND.2	ADV_FSP.1 AGD_ADM.1	Yes Yes

SFR/SAR	Dependencies	Satisfied?
	AGD_USR.1	Yes
	ATE_FUN.1	Yes
AVA_SOF.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes
AVA_VLA.1	ADV_FSP.1	Yes
	AGD_ADM.1	Yes
	ADV_HLD.1	Yes
	AGD_USR.1	Yes

8.8 Internal Consistency and Mutually Supportive Rationale

287 The set of security requirements identified in this ST for Sidewinder 5.2.1 form a mutually supportive and internally consistent whole as evidenced by the following:

a) The choice of security requirements is justified as shown in Sections 8.3, 8.4, and 8.5. The choice of SFRs and SARs was made based on the assumptions and threats identified in Section 3 and the objectives identified in Section 4. Sections 8.1 and 8.2 of this ST provide evidence the security objectives counter threats to the TOE. Also, Section 8.2 demonstrates that the assumptions and objectives counter threats to the TOE operating environment.

b) The security functionality as described in the TOE Summary Specification satisfies the SFRs. All SFR dependencies have been met as shown in Section 8.7, Table 15.

c) The SOF claims are valid. The chosen SOF-medium level is consistent with the attack potential and general level of threats identified in Section 3 of this ST. The identified metrics and SOF claim is commensurate with the EAL 2 level of assurance.

d) The SARs are appropriate for the assurance level of EAL 2 and are satisfied by Sidewinder 5.2.1 as demonstrated in Section 6.2 of this ST.

8.9 Rationale for Explicit Requirements

288 Although single-use authentication (FIA_UAU.4) is in the operating environment in this ST, an explicit requirement, ***FIA_UAU.8 (EXP)*** has been added to the TOE for clarification. ***FIA_UAU.8 (EXP)*** requires the TOE to provide support for invoking an authentication server prior to granting access to the TOE. This requirement ensures that the authentication server will successfully authenticate a user's claimed identity (e.g., humans using FTP and Telnet) before allowing any other TSF-mediated actions on behalf of that user.

8.10 Rationale for TOE Summary Specification

289 This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

8.10.1 TOE Security Requirements

290 The specified TOE security functions work together to satisfy the TOE security functional requirements. Section 6.1 includes in the descriptions of security functions a mapping to SFRs to show that each security function is traced to at least one SFR. Table 16 demonstrates that each SFR is covered by at least one security function.

Table 16. Mapping of SFRs to Security Functions

Functional Components		Security Function
FMT_SMR.1	Security roles	SW_FMT
FIA_ATD.1	User attribute definition	SW_FIA
FIA_UID.2	User identification before any action	SW_FIA
FIA_AFL.1	Authentication failure handling	SW_FIA
FIA_UAU.4	Single-use authentication mechanisms	SW_FIA
FIA_UAU.5	Multiple authentication mechanisms	SW_FIA
FIA_UAU.8 (EXP)	Invocation of authentication mechanisms	SW_FIA
FDP_IFC.1	Subset information flow control (1)	SW_FDP
FDP_IFC.1	Subset information flow control (2)	SW_FDP
FDP_IFF.1	Simple security attributes (1)	SW_FDP
FDP_IFF.1	Simple security attributes (2)	SW_FDP
FMT_MSA.1	Management of security attributes (1)	SW_FMT

Functional Components		**Security Function**
FMT_MSA.1	Management of security attributes (2)	SW_FMT
FMT_MSA.1	Management of security attributes (3)	SW_FMT
FMT_MSA.1	Management of security attributes (4)	SW_FMT
FMT_MSA.3	Static attribute initialization	SW_FMT
FMT_MTD.1	Management of TSF data (1)	SW_FMT
FMT_MTD.1	Management of TSF data (2)	SW_FMT
FDP_RIP.1	Subset residual information protection	SW_FDP
FPT_RVM.1	Non-bypassability of the TSP	SW_FPT
FPT_SEP.1	TSF domain separation (1)	SW_FPT
FPT_SEP.1	**TOE operating environment** domain separation (2)	SW_FPT
FPT_STM.1	Reliable time stamps (1)	SW_FPT
FPT_STM.1	Reliable time stamps (2)	SW_FPT
FAU_GEN.1	Audit data generation	SW_FAU
FAU_SAR.1	Audit review	SW_FAU
FAU_SAR.3	Selectable audit review	SW_FAU
FAU_STG.1	Protected audit trail storage	SW_FAU
FAU_STG.4	Prevention of audit data loss	SW_FAU
FMT_MOF.1	Management of security functions behavior (1)	SW_FMT

Functional Components		Security Function
FMT_MOF.1	Management of security functions behavior (2)	SW_FMT

291 Table 17 provides rationale that the security functions are suitable to meet the SFRs.

Table 17. Suitability of Security Functions

Security Function	SFR Identifier	Justification
SW_FMT	FMT_SMR.1 FMT_MSA.1 (1) FMT_MSA.1 (2) FMT_MSA.1 (3) FMT_MSA.1 (4) FMT_MSA.3 FMT_MTD.1 (1) FMT_MTD.1 (2) FMT_MOF.1 (1) FMT_MOF.1 (2)	The SW_FMT security function provides an authorized administrator, as appropriate, with the capability to manage the operation of the Sidewinder. An administrator is allowed to control the operation of the TOE, manage user attributes, perform audit management, set the system time and date, and manage authentication failure responses. Authorized administrators are also provided with the capability to manage the flow of information through the Sidewinder. This includes complete control of all information flow security attributes.
SW_FIA	FIA_ATD.1 FIA_UID.2 FIA_AFL.1 FIA_UAU.4 FIA_UAU.5 ***FIA_UAU.8 (EXP)***	The SW_FIA security function provides the capability to determine and verify the identity of users, determine their authority to interact with the TOE, and associate the proper security attributes for each authorized user. Also, it ensures that user identification and authentication precede any TSF-mediated actions on behalf of a user, responds to unsuccessful authentication attempts, and provides for both password and single-use authentication mechanisms.
SW_FDP	FDP_IFC.1 (1) FDP_IFC.1 (2) FDP_IFF.1 (1) FDP_IFF.1 (2) FDP_RIP.1	The SW_FDP security function implements the information flow and mediates all flows through the Sidewinder. It controls traffic flows from unauthenticated IT entities and also controls FTP and Telnet flows which require the human user initiating the flow to be authenticated. Safeguards are provided to ensure that residual data from a previous packet is not leaked to new packets as they flow through the Sidewinder.

Security Function	SFR Identifier	Justification
SW_FPT	FPT_RVM.1 FPT_SEP.1 (1) FPT_SEP.1 (2) FPT_STM.1 (1) FPT_STM.1 (2)	The SW_FPT security function provides unbypassable mechanisms for policy enforcement; separate security domains to preclude observation and tampering by untrusted subjects; and a reliable time stamp.
SW_FAU	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3 FAU_STG.1 FAU_STG.4	The SW_FAU security function generates audit records related to security relevant events. It provides the capability to review audit logs using tools for sorting and searching. Audit records are protected from modification and unauthorized deletion. If the audit trail becomes full, appropriate safeguards are applied to prevent audit data loss.

292 Because the security functions trace to SFRs, which were shown to be mutually supportive in Section 8.8, and Table 17 justifies that the security functions implement all the SFRs, it is concluded that the security functions work together to satisfy the SFRs.

8.10.2 TOE Assurance Requirements

293 Table 18 is provided to demonstrate that each TOE SAR is adequately addressed by at least one assurance measure.

Table 18. Assurance Measure Suitability

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
ACM_CAP.2	Sidewinder Configuration Management Plan	The Configuration Management Plan provides for unique identification of the TOE and all related configuration items.
ADO_DEL.1	Sidewinder Delivery Procedure	This procedure describes mechanisms, which ensure that the TOE is delivered securely to customers. It addresses how unauthorized modifications can be detected.

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
ADO_DEL.1	Common Criteria Evaluated Configuration Guide (CCECG)	This document contains delivery procedures followed in the delivery of the TOE.
ADO_IGS.1	Sidewinder Installation and Configuration Guide	This document describes the procedures for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1	Common Criteria Evaluated Configuration Guide (CCECG)	This document supplements the installation procedures provided in the Sidewinder Installation and Configuration Guide.
ADV_FSP.1	Sidewinder Functional Specification (consists of information files, not a formal document)	This document describes the TSF and its external interfaces using an informal style.
ADV_HLD.1	Sidewinder High-Level Design (consists of information files, not a formal document)	The high-level design files describe the structure of the TSF in terms of subsystems and the functionality each provides. It also describes the interfaces to the subsystems.
ADV_RCR.1	Sidewinder Security Functions Correspondence Analysis	This analysis document provides the correspondence between all adjacent pairs of TSF representations that are provided.
AGD_ADM.1	Sidewinder Administration Guide Sidewinder Installation and Configuration Guide	These two documents provide guidance to those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. They include warnings about functions and privileges that should be controlled in a secure processing environment.

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
AGD_ADM.1	Common Criteria Evaluated Configuration Guide (CCECG)	This document supplements and supports the guidance provided in the Sidewinder Installation and Configuration Guide.
AGD_USR.1	Sidewinder Administration Guide	This document also suffices to cover user guidance. Only administrative users are allowed to directly control the Sidewinder.
ALC_FLR.2	Sidewinder Security Flaw Reporting Procedures	This document defines the security flaw handling procedures to be followed by the developer.
ALC_FLR.2	Common Criteria Evaluated Configuration Guide (CCECG)	This document contains information on security flaw reporting procedures
ATE_COV.1	Sidewinder Test Plan/Coverage Analysis	This document shows the correspondence between tests and the security functions.
ATE_FUN.1	Sidewinder Test Procedures and Results	This functional test documentation includes test procedure descriptions, expected test results and actual test results.
ATE_IND.2	Sidewinder TOE (this is product software, not a document)	This is a copy of the TOE that is suitable for independent testing by evaluators.
AVA_SOF.1	Sidewinder Strength of Function Analysis	Strength of function analysis is performed on the administrator authentication mechanism in order to gain more confidence in the overall security functionality of the TOE. The results of the analysis are documented.

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
AVA_VLA.1	Sidewinder Vulnerability Analysis	An analysis of the TOE deliverables is performed to identify any flaws or weaknesses that could be exploited by an attack. The analysis results are documented.