Part Number 00-0944961-I

Version Date 9 November 2007

Sidewinder Version 7.0.0.02

SECURITY TARGET

Prepared by:

Secure Computing Corporation

2340 Energy Park Drive

Saint Paul, Minnesota 55108

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 7.0.0.02 Security Target
ST Author:	Dwight D. Colby
ST Revision Number:	00-0944961-I
ST Date:	November 9, 2007
TOE Identification:	Software:

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

Sidewinder Software Version 7.0.0.02

Sidewinder 7.0 Management Tools

Hardware for Sidewinder appliances:

Models 110D/210D: SW70-845A-B/B-B

Models 410D/510D: SW70-860A-A/B-A

Model 1100D: SW70-1950A-A

Models 2100D/2150D: SW70-2950B-A/A-A

Model 4150D: SW70-2900A-A

Model RM700: SW70-860C-A

Model TNG: SW70-TNGA-A

Note – Model TNG is also identified as the TNG(Fw), Tactical Network-Layer Gateway (Firewall) and MESHnet Firewall.

Administrative Guidance for receiving, installing and managing the TOE

Sidewinder v7.0 Startup Guide, SWOP-MN-STRT70-A, March 2007

Common Criteria Evaluated Configuration Guide, 86-0947005-B, July 2007

Sidewinder v7.0 Administration Guide, SWOP-MN-ADMN70-A, March 2007

Sidewinder v7.0 Re-imaging without a CD-ROM drive, 89-0946851-A, March 2007

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004 (also known as ISO 15048)

Assurance Level:	EAL4, augmented with ALC_FLR.3
PP Identification:	U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 22, 2000
ST Evaluation:	SAIC
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. An authorized administrator can both read and write TOE security parameters.

Authorized external IT entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities 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.

Note, the evaluated TOE does not communicate with authorized external IT 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 Any Sidewinder appliance model with Sidewinder Software Version 7.0.0.02 will be identified hereafter as Sidewinder. Sidewinder is a firewall and access control security platform for the enterprise. Enabling the implementation of “safe, secure extranets for e-business,” Sidewinder configured in its operational environment delivers strong security while maintaining performance and scalability. It provides access control of communication and information flow between two or more networks using application-level proxy and packet filtering technology. The operational environment for the Sidewinder software is a typical Intel-based architecture Pentium PC computing platform. The configured Sidewinder provides the highest levels of security by using SecureOS ™, an enhanced UNIX operating system that employs Secure Computing's

patented Type Enforcement™ security technology. Type Enforcement technology protects Sidewinder by separating all processes and services on the firewall.

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

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 January 2004, version 2.2, CCIMB-2004-01-001.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, version 2.2, CCIMB-2004-01-002.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, version 2.2, CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation – January 2004, version 2.2, CCIMB-2004-01-004.
[ALFPP_BAS]	U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, dated June 22, 2000.

1.5 Common Criteria Conformance Claims

19 The TOE conforms to the U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, dated June 22, 2000 [ALFPP_BAS]. This Protection Profile defines the minimum security requirements for firewalls used by U. S. Government organizations handling unclassified information in a low-risk environment.

20 The TOE conforms to [CC_PART2] extended and [CC_PART3] conformant with the assurance level of EAL4, augmented with ALC_FLR.3.

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 operating with three network interfaces provides a hybrid firewall solution that supports both application-level proxy and packet filtering. The Sidewinder software consists of a collection of integrated components. The base component is SecureOS™, a secure operating system. This OS is an extended version of the BSD UNIX operating system. It includes Secure Computing's patented Type Enforcement security technology, additional network separation control, network-level packet filtering support and improved auditing facilities. SecureOS also provides the secured computing environment in which all Sidewinder firewall application layer processing is done. The application-layer firewall components include the network service monitor processes, network proxy applications, the firewall Access Control List (ACL) daemon, audit monitors and the system management functions.

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 and to a separate network for administrative control.

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

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

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

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

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

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

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

2.3.2 Proxy agents to be Evaluated

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

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) On-console Administration

b) Virtual Private Network (VPN)

c) Failover/High Availability

d) Anti-Virus

e) URL Filtering

f) Mail Filtering

g) Policy Acceleration Network Cards

h) SSL Termination

i) Direct login to a Sidewinder via Telnet or SSH

j) Firewall policy cloning/One-to-Many

k) Remote administration from external networks

l) Built-in servers (e.g. SSHD)

2.3.4 Physical Scope and Boundary

27 The TOE consists of a Sidewinder appliance with Sidewinder Software Version 7.0.0.02. The TOE also includes the Admin Console client software (the Sidewinder 7.0 Management Tools). This software is provided with every Sidewinder appliance; it is also provided as a separate part of every Sidewinder Software version 7.0.0.02 product distribution. The administration client software runs on a local, generic computing platform with a Windows operating system; however, the platform and Windows OS are not part of the TOE.

2.3.4.1 Evaluated TOE Configuration

28 The Sidewinder is configured to control the flow of TCP/IP traffic between two network interfaces. Its Intel-processor-based computing platform includes at least three network interfaces. The environment includes a commercially available, single-use authentication server that is compatible with Sidewinder such as SafeWord PremierAccess[2] or any RADIUS server. The environment also includes a generic administrative workstation platform running on a Windows operating system.

29 The hardware configuration requirements are as follows:

a) CPU: Intel, 1Ghz or greater

b) RAM: 512 MB minimum

c) Media:

- Minimum of 8 GB of disk storage

d) Network: At least 3 network interfaces

e) SVGA video and display (optional)

f) US Keyboard (optional)

30 Additional information concerning key hardware components can be found under Sidewinder "hardware" category on the Secure Computing website (www.securecomputing.com/hardware).

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

31 In addition, a second hardware platform is required in the IT environment for the local administration workstation running the Sidewinder 7.0 Admin Console software. The minimum configuration required for this platform is as follows:

a) CPU: Intel, 1GHz

b) RAM: 512 MB

c) OS: MS Windows 2000 Workstation, 2000 Server, or Windows XP

d) Media:

- Minimum of 300 MB of available disk storage
- CD drive

e) Network: One network interface

f) SVGA video and display

g) PS/2 or Serial Mouse

h) US Keyboard

2.3.4.2 Hardware Security Considerations

32 No extraordinary security demands are placed upon the hardware platforms and peripheral equipment used by the Sidewinder software. This equipment is expected to meet the customary demands for reliable 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 platforms 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 or ancillary hardware must provide a periodic timer to support the internal time management within the kernel.

d) If any of the network interface cards support features such as wake-on LAN, special external command features, or special protocol processing, the hardware connections to support those features should not be connected. In the evaluated configuration, Sidewinder will not enable any such special features.

2.3.5 Logical Scope and Boundary

33 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]

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

2.3.5.2 Identification and Authentication [SW_FIA]

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

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

2.3.5.3 User Data Protection [SW_FDP]

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

38 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.

39 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 system zeros storage blocks as they are reused to prevent residual information leakage.

2.3.5.4 Protection of Security Functions [SW_FPT]

40 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.

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

42 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.

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

2.3.5.5 Audit [SW_FAU]

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

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

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

3 TOE Security Environment

47 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.

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

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

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

51 The TOE is intended to be used in environments in which sensitive information is processed, or where the sensitivity level of information in both the internal and external networks is different.

3.1 Assumptions

52 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

53 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 authentication server is physically protected.

Assumption Identifier	Assumption Description
	The communication path between the TOE and the administrator Windows computer is physically protected, also.

3.1.2 Additional Environment Assumptions

54 Because the authentication server and the local administration platform play a critical role in the TOE's ability to enforce its security policy, the following conditions are assumed to exist with respect to them.

Table 2. Assumptions for the Authentication Server and Local Administration Platform

Assumption Identifier	Assumption Description
A.ASPHYSEC	The authentication server and local administration platform are physically secure.
A.ASLOWEXP	The authentication server and local administration platform are not connected to any other IT entities, only the TOE.
A.ASGENPUR	No extraneous applications, beyond authentication services and TOE administration, are installed on the authentication server or on the local administration platform.
A.ASPUBLIC	The authentication server and local administration platform do not host public data.
A.ASNOEVIL	Authorized administrators of the authentication server and local administration platform are non-hostile and follow all administrator guidance; however, they are capable of error.
A.ASNOREMO	There is no remote access to the authentication server or the local administration platform.

3.2 Threats

55 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.

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

3.2.1 Threats Addressed by the TOE

57 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 attacker's actions.
T. LOWEXP	An attacker with low attack potential may 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

58 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

59 This ST does not identify any OSPs.

4 Security Objectives

60 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

61 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.

Objective Identifier	Objective Description
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, 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

62 All the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the 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 is physically secure.
O.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
O.PUBLIC	The TOE does not host public data.
O.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
O.SINGEN	Information cannot 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 are trained as to establishment and maintenance of security policies and practices.

Objective Identifier	Objective Description
O.DOMSEP	The TOE's operating environment must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.PROLIN	The communication path between the TOE (i.e., authentication client) and the single-use authentication server must be physically protected. The communication path between the TOE and the administrator Windows computer must be physically protected, also.
O. ASPHYSEC	The authentication server and local administration platform must be physically secure.
O.ASLOWEXP	The authentication server and local administration platform must not be connected to any other IT entities, only the TOE.
O.ASGENPUR	There must be no extraneous applications, beyond authentication services and TOE administration, installed on the authentication server or on the local administration platform.
O.ASPUBLIC	The authentication server and the local administration platform must not host public data.
O.ASNOEVIL	Authorized administrators of the authentication server and the local administration platform must be non-hostile and follow all administrator guidance; however, they are capable of error.
O.ASNOREMO	There must be no remote access to the authentication server or the local administration platform.

5 TOE IT Security Requirements

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

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

64 The security functional requirements for this Security Target consist of the following components from Part 2 of the CC, summarized in Table 7. TOE Security Functional Requirements. 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)
FMT_MTD.2	Management of limits on TSF data

Functional Components	
FDP_RIP.1	Subset residual information protection
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
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)

5.1.1.1 Static PP SFRs

65 *Static PP SFRs* are those PP security functional requirements with which the ST claims compliance and for which no additional operations are to be performed. These PP SFRs apply verbatim, the complete statement of which can be found in Section 5 of the [ALFPP_BAS] and are repeated later in this ST. The following Table 8 identifies the Static PP SFRs.

Table 8. Static PP SFRs

Functional Components	
FIA_AFL.1	Authentication failure handling
FIA_UID.2	User identification before any action
FDP_IFC.1	Subset information flow control (1)
FDP_IFC.1	Subset information flow control (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)

Functional Components	
FMT_MTD.1	Management of TSF data (2)
FMT_MTD.2	Management of limits on TSF data
FDP_RIP.1	Subset residual information protection
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
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)

5.1.1.2 Omitted PP SFRs

66 The FCS_COP.1 SFR has been omitted from this ST because remote administration is not part of the evaluated configuration.

5.1.1.3 Tailored PP SFRs

67 *Tailored PP SFRs*: those PP security functional requirements that contain operations to be completed in PP-compliant security targets. Table 9 identifies those SFRs. The justification for the tailored SFRs is provided in Section 7, which contains the PP conformance claims. The tailored SFRs are provided in their entirety in the following paragraphs.

Table 9. Tailored SFRs

Functional Components		Operation(s)
FMT_SMR.1	Security roles	assignment, refinement
FIA_ATD.1	User attribute definition	security target writer, assignment
FIA_UAU.5	Multiple authentication mechanisms	assignment
FDP_IFF.1	Simple security attributes (1)	security target writer, refinement
FDP_IFF.1	Simple security attributes (2)	security target writer, refinement

Functional Components		Operation(s)
FAU_GEN.1	Audit data generation	refinement, assignment
FAU_SAR.1	Audit review	assignment

5.1.1.4 Non-PP SFR

68 The TOE includes one security requirement beyond the PP to clarify that the TSF must invoke the single-use authentication mechanism which is included in the IT environment.

Table 10. Non-PP Requirements

Functional Components	
FIA_UAU.8 (EXP)	Invocation of authentication mechanism

69

5.1.1.5 Comprehensive Listing of all TOE SFRs

FMT_SMR.1 Security roles

70 FMT_SMR.1.1 - The TSF shall maintain the roles [authorized administrator and read only administrator].

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

FIA_ATD.1 User attribute definition

72 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 or with the read only administrator role;

c) and password].

FIA_UID.2 User identification before any action

73 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

74 FIA_AFL.1.1 - The TSF shall detect when [a non-zero number determined by the authorized administrator]of unsuccessful

authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access].

75 FIA_AFL.1.2 - When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question].

FIA_UAU.5 Multiple authentication mechanisms

76 FIA_UAU.5.1 - The TSF shall provide [a password and single-use authentication mechanism] to support user authentication.

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

a) single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;

b) single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity;

c) 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;

d) reusable password mechanism shall be used for authorized administrators or read only 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].

78 Application Note: Rules a and b are not applicable because the TOE does not provide for remote administrator access or for authorized external IT entities. The use of the single-use authentication mechanism is provided in conjunction with the following requirement, FIA_UAU.8, which invokes a single-use authentication mechanism from the TOE operating environment. This approach is consistent with the industry view that a firewall supplier should not mandate selection of a single (possibly weak) single-use authentication product, but should allow choice of state of the art products from a range of third party vendors. The "directly connected terminal" for authorized administrator access is provided by an administration workstation connected to the TOE via a protected local area network.

FIA_UAU.8 (EXP) Invocation of authentication mechanism

79 ***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.]

80 Requirements Overview: This Security Target consists of two 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)

81 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)

82 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)

83 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].

84 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.]

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

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

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

88 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) For the HTTP and SMTP application protocols, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC). This shall be accomplished through protocol filtering proxies that are designed for that purpose.]

89 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.

90 Application Note: The generalized wording of the FDP_IFF.1.6f) requirement has been modified from the PP to make it clear that only HTTP and SMTP are included in the TOE (while DNS and POP3 application-level proxies are not included in the TOE).

FDP_IFF.1 Simple security attributes (2)

91 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].

92 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.5;[3]
- 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.5;
- 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.]

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

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

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

96 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 reject Telnet or FTP command requests that do not conform to generally accepted published protocol definitions (e.g., RFCs).

97 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)

98 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)

99 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)

100 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)

101 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

102 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.

103 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.

104 Application Note: Following TOE installation, the default configuration is to allow no traffic through the firewall. The default values for the information flow control security attributes appearing in FDP_IFF.1 (1) and FDP_IFF.1 (2) are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

FMT_MTD.1 Management of TSF data (1)

105 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].

106 Application Note: The ability to perform all of the listed actions is restricted to the authorized administrator, however the read only administrator is allowed to view the user attributes. A proxy user who has successfully authenticated via the password mechanism, may also change his or her own password.

FMT_MTD.1 Management of TSF data (2)

107 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].

FMT_MTD.2 Management of limits on TSF data

108 FMT_MTD.2.1 - The TSF shall restrict the specification of the limits for [the number of authentication failures] to [the authorized administrator].

109 FMT_MTD.2.2 - The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions specified in FIA_AFL.1.2].

FDP_RIP.1 Subset residual information protection

110 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* [all objects].

111 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

112 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

113 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.

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

FPT_STM.1 Reliable time stamps

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

116 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

117 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 11. Auditable Events].

118 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 11. Auditable Events].

Table 11. 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 or read only administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the administrator role.
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.

Functional Component	Auditable Event	Additional Audit Record Contents
FIA_UAU.5	Any use of the authentication mechanism	The user identities provided to the TOE.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorized administrator of the users capability to authenticate.**	The identity of the offending user and the authorized administrator.
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation.

FAU_SAR.1 Audit review

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

120 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

121 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].

122 Application Note: Sorting is to be provided by predefined report formats.

FAU_STG.1 Protected audit trail storage

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

124 FAU_STG.1.2 - The TSF shall be able to *prevent* unauthorized modifications to the audit records in the audit trail. [4]

FAU_STG.4 Prevention of audit data loss

125 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)

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

a) [operation of the TOE; and

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

to [an authorized administrator].

127 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. The single-use authentication mechanism can be changed while the TOE is running. The ability to change the mechanism is also restricted to an authorized administrator.

FMT_MOF.1 Management of security functions behavior (2)

128 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;

b) backup and restore for TSF data, information flow rules, and audit trail data; and

c) communication of authorized external IT entities with the TOE] to [an authorized administrator].

129 Application Note: Determine and modify the behavior of element c (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.

5.1.1.6 SFRs With Strength of Function (SOF) Declarations

130 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.

[4] **This wording of this requirement has been modified from that in the PPs to reflect Common Criteria International Interpretation #141.**

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

132 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

133 The TOE has the following non-PP security requirement allocated to its IT environment (authentication server and Admin Console hardware platform).

Table 12. Functional Requirements for IT Environment

Functional Components	
FIA_UAU.4	Single-use authentication mechanisms

FIA_UAU.4 Single-use authentication mechanisms

134 FIA_UAU.4.1 – The TSF 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].

5.3 TOE Security Assurance Requirements

135 The TOE claims compliance to EAL 4 level of assurance. The security assurance requirements (SARs) for this Security Target include the EAL 4 SARs in Part 3 of the CC. The EAL 4 SARs are identified in the following Table 13:

Table 13. EAL4 Assurance Components

Assurance class	Assurance components
Class ACM: Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Class ADO: Delivery and operation	ADO_DEL.2 Detection of Modification
	ADO_IGS.1 Installation, generation, and start-up procedures

Assurance class	Assurance components
Class ADV: Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Class AGD: Guidance documents	AGD_ADM.1Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

5.3.1 Additional Security Assurance Requirements

136 This section describes the maintenance assurance requirements from the CC Part 3 that the TOE must satisfy in addition to the previously listed EAL 4 SARs.

137 In particular, ALC_FLR.3 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.3 is not included in any EAL. This additional SAR is restated verbatim from the CC.

Table 14. Additional SARs to Augment EAL 4

Assurance class	Assurance components
Class ALC: Life cycle support	ALC_FLR.3 Systematic Flaw Remediation

5.3.1.1 ALC_FLR.3 Systematic Flaw Remediation

138 **Developer action elements:**

139 ALC_FLR.3.1D – The developer shall provide flaw remediation procedures addressed to TOE developers.

140 ALC_FLR.3.2D – The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

141 ALC_FLR.3.3D – The developer shall provide flaw remediation guidance addressed to TOE users.

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

143 ALC_FLR.3.1C – The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

144 ALC_FLR.3.2C – 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.

145 ALC_FLR.3.3C – The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

146 ALC_FLR.3.4C – The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

147 ALC_FLR.3.5C – 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.

148 ALC_FLR.3.6C – The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

149 ALC_FLR.3.7C – The procedures for processing reported security flaws shall provide safeguards that any corrections to these flaws do not introduce any new flaws.

150 ALC_FLR.3.8C – The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

151 ALC_FLR.3.9C – The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

152 ALC_FLR.3.10C – The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

153 ALC_FLR.3.11C – The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

154 **Evaluator action elements:**

155 ALC_FLR.3.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6 TOE Summary Specification

156 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

157 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]

158 The Admin Console graphical user interface (GUI) provides the external interfaces required for an administrator to manage the Sidewinder firewall and utilize its security features. Admin Console windows-oriented, point-and-click features are used to turn services on or off and to select configuration options. A keyboard is used enter configuration parameters to augment the point-and-click Admin Console operation.

159 The Admin Console also provides administrators access to audit information and system usage reports.

6.1.1.1 Using Admin Console [SW_FMT_1]

160 Before an administrator may perform any management functions on a Sidewinder they must establish a connection between the Admin Console client operating on a network-connected Windows system. This requires that the administrator identify the Sidewinder to be managed, and to provide identification and authentication information for an administrative user recognized by the Sidewinder. The authentication method, reusable password or specific type of one-time-password check, is determined by the current state of the rule controlling the management service from the Windows system being used. Reusable password is the default authentication mechanism for the initial administrator.

161 Sidewinder maintains an authorized administrator role. Sidewinder keeps a list which associates particular user identities with the authorized administrator role and also identifies the type of administration activities they are allowed to perform, as either Read/Write or Read Only. When a user attempts to sign in at the GUI, the list is consulted and a user on the list is given the administrative privileges associated with their

identity. All authorized administrators can access system configuration data, but only an authorized administrator with Read/Write permission can change the security configuration of Sidewinder. (FMT_SMR.1)

162 The major Admin Console command menu selections are:

- Monitor (review audit and system operation)
- Policy (configure rules for firewall policy and services)
- Network (establish networking configuration)
- Maintenance (administer firewall operation)

6.1.1.2 Firewall Policy Configuration [SW_FMT_2]

163 The administrator manages the rules for access control and packet filtering which comprise the Firewall Policy. Only an authorized administrator is permitted to delete, modify, or add to the proxy and filter rules, and to the object definitions, such as groups of network addresses, individual network users, groups of users, etc. that are used in writing policy rules. Only an authorized administrator is permitted to query or update individual user attributes such as identity, role and password. However, a proxy user is allowed to change his or her own password after successfully authenticating via the password mechanism. (FMT_MSA.1 (1), (2), (3) & (4), FMT_MTD.1 (1)).

6.1.1.3 Services Configuration [SW_FMT_3]

164 An authorized administrator may use the GUI to enable, disable and configure all Sidewinder services. This includes network protocol communication proxies, remote authentication services, and remote administration services. Since the default TOE configuration prohibits traffic flow, an administrator must override initial information flow security attributes to allow traffic. (FMT_MSA.3)

6.1.1.4 Reports and Monitoring [SW_FMT_4]

165 After establishing a connection to a Sidewinder, an authorized administrator may review the audit logs and generate system operation and usage reports.

166 Only an authorized administrator may initiate actions to remove old audit records.

6.1.1.5 Firewall Administration [SW_FMT_5]

167 Only an authorized administrator is allowed to create, delete or make changes to the Sidewinder system configuration information such as number of network interfaces, network addresses, security attributes and the information flow rules described later in Section 6.1.3.3 for both unauthenticated and authenticated SFPs. This includes providing the identification attributes and role attributes for sidewinder administrators.

(FMT_SMR.1, FMT_MSA.1 (1), (2), (3) & (4)) The administrator can also use the GUI to establish the limit for authentication failures before a user is no longer allowed to authenticate and the ability to take actions permitting the user to authenticate once again. (FMT_MTD.2)

168 Only an authorized administrator is allowed to enable or disable the use of reusable and single-use authentication mechanisms, to manage the audit trail, to control security data backup and restore, and to control any external IT entity communication with Sidewinder.

169 On Sidewinder, the authentication mechanisms are independently enabled and disabled. Turning one mechanism on or off has no effect on the status of another mechanism. Thereafter, specific proxies or services can be configured to require the use of an enabled mechanism.

170 Only an authorized administrator can shut down the operating Sidewinder or change the system time and date via the GUI. Also, only an individual with physical access to the Sidewinder computing platform may start or stop a Sidewinder via the power and reset controls. (FMT_MOF.1 (1) & (2), FMT_MTD.1 (2))

171 **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); FMT_MTD.2; and FMT_SMR.1

6.1.2 Identification and Authentication [SW_FIA]

6.1.2.1 Sidewinder Users [SW_FIA_1]

172 Sidewinder supports two classes of users: those who are administrators and those who 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 rules call for password authentication.
- The role in which the individual is allowed to operate.

173 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 before the user is allowed to utilize the communication protocol through the

firewall. For network communication users, the following information is retained. Only the user's name, group and password (if required) are security relevant; the other fields are optional.

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

174 Administrative users must first identify and authenticate themselves before they can directly control the behavior of Sidewinder. (FIA_UID.2)

175 During system installation, an initial authorized administrator ID and password are established. Following installation, the initial administrator is allowed to establish a connection from an Admin Console by providing the correct ID and password. (FIA_ATD.1)

176 In addition to human users, external IT entities are identified by IP address, network interface to which they are connected, and the communications protocol being used. These security attributes are provided in the network communication packets and the Sidewinder's TCP/IP network processing.

6.1.2.2 Authentication [SW_FIA_2]

177 Sidewinder provides support for both single-use and multi-use passwords. The decision on which form to use is dictated by the content of the rule associated with the service being accessed. The type of authentication required may also be configured on a user-by-user basis. Multiple authentication capability applies to both administrative access and network communication services. In either case, the function consults the appropriate authenticator which operates on the Sidewinder being accessed. Sidewinder supports SafeWord, LDAP/Active Directory, NT Domain, and Radius authentication servers. (FIA_UAU.5)

178 In the case of reusable passwords, the authenticator consults the user information maintained on the Sidewinder to determine if the provided password matches the user's valid password. Reusable passwords, with lengths from 12 to 64, combine letters, numbers and special characters to provide a permutational mechanism that meets the standard of SOF-medium. The probability that the password can be guessed is less than one in two to the fortieth (2^40). In the case of single-use passwords, the

relevant warder consults the remote authentication server to determine if the provided authentication data is valid. (FIA_UAU.4, FIA_UAU.8)

179 Authentication control is supported for all forms of administrative access to the Sidewinder, and for the FTP and Telnet proxies.

6.1.2.3 Authentication Failure Processing [SW_FIA_3]

180 An authorized administrator can define an authentication failure limit. After that defined number of consecutive unsuccessful password authentication attempts by a user trying to establish an administrator connection or trying to employ FTP and Telnet, Sidewinder prevents that user from successfully authenticating. The user is prevented from successful authentication until an authorized administrator takes action to restore the user's rights. (FIA_AFL.1)

181 In all cases, an audit event recording connection denial due to the authentication failure is generated.

182 **Functional Requirements Satisfied by TOE:** FIA_AFL.1; FIA_ATD.1; FIA_UAU.5, FIA_UAU.8 and FIA_UID.2

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

6.1.3 User Data Protection [SW_FDP]

6.1.3.1 Residual Information Protection [SW_FDP_1]

184 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. Thus newly allocated memory pages are zeroed.

185 A second situation arises when using kernel message buffers for managing data read from and written to the network. Since these buffers have previously been allocated, they are not zeroed again. 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 message buffer 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 is moved. (FDP_RIP.1)

6.1.3.2 Information Flow Control [SW_FDP_2]

186 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 rules do not allow specification of an authentication requirement.

187 On Sidewinder, the Telnet and FTP proxies can also be instructed to require user authentication to utilize the service. In this case, an administrator must define the service users in the user database and establish rules for Telnet and FTP which specify that the service is contingent upon successful authentication. The rule specifies the particular type of single-use authentication mechanism that is to be used. (FDP_IFC.1 (1) & (2))

6.1.3.3 Security Attributes [SW_FDP_3]

188 On Sidewinder, the flow of information through the system for both the unauthenticated and the authenticated SFPs is determined by key subject and information security attributes. In particular, the flow rules depend upon the presumed source subject and destination subject addresses, the Sidewinder interface (burb) on which the traffic arrives or departs, the requested service, and destination service port range. In the case of authenticated policy, the attributes that determine flow also include the user identity and security relevant service commands for Telnet and FTP. In the case of unauthenticated policy, the attributes that determine flow also include security relevant service commands for HTTP and SMTP.

189 Sidewinder employs the burb concept to allow 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. In the evaluated configuration, one or more networks are designated as internal, while one or more other networks are designated as external. The administrator would set up corresponding internal and external burbs with distinct, non-overlapping IP address spaces to serve as the basis for policy enforcement. The allowed flow between any two networks is determined by the services enabled and the state of the rules in the firewall security policy.

190 In addition to specific rules, Sidewinder uses these security attributes to enforce other flow rules that are described in subsequent paragraphs.

191 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 policy decisions based on this information independent of the stated source address.

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

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

194 The Sidewinder rejects all IP packets containing source route information and generates a netprobe audit message.

195 Sidewinder processing for HTTP, SMTP, Telnet, and FTP connections provides controls to check for and reject bad service requests. For HTTP and FTP, the rule can specify which specific protocol service requests are allowed. (FDP_IFF.1 (1) & (2))

6.1.3.4 Access Control List [SW_FDP_4]

196 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, server, or filter agent checks the rules to determine whether to allow the requested connection. The ACL rules can be configured to allow access from one presumed source address to a presumed destination address. In addition, burbs may be used to aggregate multiple addresses within the rules. The rules can also be configured to specify the transport layer protocol, the service, the interface on which traffic arrives and departs, and the destination service port range. (FDP_IFF.1 (1) & (2))

6.1.3.5 Internet Service Configuration [SW_FDP_5]

197 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.

198 Sidewinder includes the network protocol proxies and network protocol servers 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.

199 Sidewinder provides proxy services for controlling connections to standard network services.

200 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 a rule. This supports hiding the structure of one Sidewinder burb from another. The Sidewinder installation includes proxy services that support the application-layer protocols. It also provides generic proxy services that can be configured on both TCP and UDP ports. FDP_IFC.1 (1) & (2)

6.1.3.6 Data Processing Protection [SW_FDP_6]

201 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 agent.

202 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.

203 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 system ensures there is no residual data leakage by zeroing storage blocks as they are allocated for a new use. (FDP_RIP.1)

204 **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]

205 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.

6.1.4.1 Secure Operating System [SW_FPT_1]

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

207 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. The separation of process address spaces is dependent on the Memory Management Unit provided by the hardware platform. (FPT_SEP.1)

208 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 through the use of the CPU cycle counters provided by the hardware platform. Access to the system calls that can alter time values is controlled by Type Enforcement policy and mechanism. (FPT_STM.1)

209 Since all Sidewinder processing operations are ultimately dependent on kernel services, SecureOS provides strong control over system operation that cannot be bypassed. This mechanism is used to control which executable 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)

6.1.4.2 Type Enforcement [SW_FPT_2]

210 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 processes running 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.

211 The Type Enforcement policy 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 an application is running on Sidewinder, it is executing in a specific domain, which is distinct from other application domains. The various system components run in separate domains providing strong separation of the Sidewinder processing elements.

212 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.

213 The current Sidewinder Type Enforcement security policy provides approximately 100 different domains in which the system's programs operate. The actions allowed for each of these domains is fully defined by the content of the Type Enforcement security policy. (FPT_SEP.1)

6.1.4.3 Sidewinder Hardware Platform [SW_FPT_3]

214 The Sidewinder hardware platform provides two-state processing and memory management to separate kernel processing from application processing. (FPT_SEP.1) The hardware platform also provides the battery-backed real-time clock and the CPU cycle counters which allow the SecureOS kernel to maintain the time. (FPT_STM.1)

215 **Functional Requirements Satisfied by TOE:** FPT_RVM.1, FPT_STM.1 , and FPT_SEP.1

6.1.5 Audit [SW_FAU]

216 The Sidewinder generates audit to mark the starting and stopping of the firewall itself, and also starting and stopping of individual services, including the audit facilities. Audit is generated to capture pertinent information related to the use of the authentication facilities, use of network communication services, establishment of administrative connections, changes to the security policy and security relevant changes to the system configuration. Sidewinder's Type Enforcement mandatory security policy protects the audit file contents from change.

6.1.5.1 Logging [SW_FAU_1]

217 The audit event generator provides information to identify the type of auditable event and entities related to the event as described in Table 11. The information includes both success and failure outcomes for the auditable events. The audit generator writes the audit event to the Sidewinder audit device. The SecureOS kernel augments that audit event with a time stamp, identification information about the audit generator, such as the process ID value, the process's TE security attributes, and the name of the command that generated the audit event. The audit event is then made available to the audit logging and audit monitor processes via the audit device. (FAU_GEN.1)

218 Sidewinder provides an audit-logging daemon, named auditd, which reads all audit events from the audit device and records them into log files. An authorized administrator may remove audit files to manage the storage space, but nobody is allowed to modify the content of the audit files.

219 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)

6.1.5.2 Audit Reporting [SW_FAU_2]

220 The Sidewinder GUI allows the administrator to search and sort audit data according to user identity, presumed subject address, as well as ranges of dates, times and addresses. Two different mechanisms are provided for accessing the audit data. The first method allows the administrator to review complete audit records for selected types of audit events, over a specified range of time. The administrator may select one of the predefined record filters, or define their own filter, to select the records they want to review. The selected audit records are sorted in time sequence order and are displayed in a readable format. (FAU_SAR.1)

221 The second method is to use one of the predefined report formats to present summary information based on the raw audit records. The administrator may choose from a list of reports that includes the administrative user connections to the system sorted by time, network probes sorted by source address and probed region, traffic usage reports sorted by service name, and rule usage sorted by rule name. Several of the reports allow the administrator to specify a specific host address or user name, which is then used to select records for the report. (FAU_SAR.3)

6.1.5.3 Audit Data Retention [SW_FAU_3]

222 The Sidewinder audit facilities monitor the state of the audit storage area to minimize the risk of loss of data. On a daily basis it will "roll" the data files. This means that the current audit file is compressed (zipped) and rotated, named to indicate order of generation, and a new current log file is created. This frees up disk space and allows more audit data to be stored. The audit "roll" mechanism is implemented so that no data is lost during the transition from the current audit file to the new audit file.

223 Every 5 minutes Sidewinder checks the status of the available audit space. When the used storage space exceeds a defined threshold it triggers an audit event. When the used storage exceeds a second threshold the system will, by default, stop inter-network communications to avoid loss of audit data. (FAU_STG.4)

224 **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

225 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.

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

6.2.1 Configuration Management

227 The Configuration Management measures applied by Secure Computing include automated tools to generate the TOE, acceptance procedures for authorizing changes to configuration items, unique identification for configuration items, proper labeling, tracking of configuration items and tracking of security flaws. These configuration management measures are documented within the Sidewinder Configuration Management Plan.

Assurance Requirements Satisfied: ACM_AUT.1, ACM_CAP.4 and ACM_SCP.2

6.2.2 Delivery and Operation

228 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.2 and ADO_IGS.1

6.2.3 Development

229 Secure Computing provides increasingly refined descriptions of the TOE security functionality starting with this Security Target. The Security Target describes the security policies enforced by the TOE and provides the information to meet the Security Policy Model requirement. Design documentation consists of a functional specification, which describes the external interfaces of the TOE, a high-level design, a low-level design and source code. 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 Security Target
- Sidewinder Functional Specification (information files)
- Sidewinder High-Level Design (information files)
- Sidewinder Low-Level Design (information files)
- Sidewinder Security Functions Correspondence Analysis
- Sidewinder Code Subset (source code files; this is not a document)

Assurance Requirements Satisfied: ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1 and ADV_SPM.1.

6.2.4 Guidance

230 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 Startup Guide
- Sidewinder Administration Guide
- Common Criteria Evaluated Configuration Guide (CCECG)[5]

Assurance Requirements Satisfied: AGD_ADM.1 and AGD_USR.1

6.2.5 Life-cycle Support

231 Secure Computing provides information describing the procedures that are used during the development and maintenance of the TOE. These procedures include the security measures used throughout TOE development, the life-cycle model used by the developer, the tools used by the developer throughout the life cycle of the TOE, as well as the internal and user procedures used to handle reports of TOE security flaws. This information is documented within the following Secure Computing documents:

- Sidewinder Development Security Description
- Sidewinder Life-Cycle Model
- Sidewinder Development Tools Definition

[5] **The CCECG provides administrative guidance for running Sidewinder in the configuration that was evaluated for Common Criteria.**

- Sidewinder Security Flaw Reporting Procedures[6]
- Common Criteria Evaluated Configuration Guide (CCECG)[7]

Assurance Requirements Satisfied: ALC_DVS.1, ALC_FLR.3, ALC_LCD.1 and ALC_TAT.1

6.2.6 Test

232 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 analysis is performed to confirm that the testing is sufficiently extensive, and test depth analysis demonstrates that the tests verify the correct behavior of the high-level design. These tests and analyses are presented in the following Secure Computing documents:

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

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

6.2.7 Vulnerability Assessment

233 In addition to the design and testing process, Secure Computing performs vulnerability assessment of the TOE. The guidance documents are examined and an analysis is documented to ensure that the documents are sufficient to allow an administrator to move a delivered system to a secure operational state. 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. Finally, a systematic 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 Guidance Documentation Analysis
- Sidewinder Strength of Function Analysis
- Sidewinder Vulnerability Analysis

Assurance Requirements Satisfied: AVA_MSU.2, AVA_SOF.1, and AVA_VLA.2

[6] **These are the internal developer procedures for fixing any flaws that might be reported.**
[7] **A section of this document provides the user guidance for reporting flaws.**

7 PP Claims

234 This section provides the PP conformance claims statements.

7.1 PP References

235 The TOE conforms to the security functional requirements and to the security assurance requirements within the following PPs:

- U. S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environment, Version 1.0, Final [ALFPP_BAS].

7.2 PP Refinements

236 The following SFRs were refined from the [ALFPP_BAS]. The changes from the PP and the justifications for the changes are presented for each SFR.

a) FIA_ATD.1 User attribute definition

Change: "password" is added as a security attribute.

Justification: The PP allows for additional attributes to be determined by the security target writer.

Change: the “read only administrator role” was added.

Justification: this additional role was added to reflect the product implementation which includes this role.

b) FDP_IFF.1 Simple security attributes (1)

Change: The requirement includes "no other subject attributes" and "destination service port range" as an information security attribute.

Justification: The PP allows for additional security attributes to be determined by the security target writer.

c) FDP_IFF.1 Simple security attributes (2)

Change: The requirement includes "no other subject attributes" and "destination service port range" as an information security attribute.

Justification: The PP allows for additional security attributes to be determined by the security target writer.

d) FAU_GEN.1 Audit data generation

Change: The auditable events table has been changed. The entry related to FCS_COP.1 was eliminated.

Justification: No audit event entries are needed for FCS_COP.1 because that requirement is not applicable to the TOE.

Change: the “read only administrator role” was added

Justification: this additional role was added to reflect the product implementation which includes this role.

e) FAU_SAR.1 Audit Review

Change: the “read only administrator role” was added

Justification: this additional role was added to reflect the product implementation which includes this role.

f) FIA_UAU.5 Multiple authentication mechanisms

Change: the “read only administrator role” was added

Justification: this additional role was added to reflect the product implementation which includes this role.

g) FMT_SMR.1 Security roles

Change: the “read only administrator role” was added.

Justification: this additional role was added to reflect the product implementation which includes this role.

7.3 PP Changes

237 The generalized wording of FDP_IFF. (1) 1.6f) has been modified from the PP to make it clear that only HTTP and SMTP are included in the TOE. The Application Note in the PP for this requirement clearly states that rule f) only applies when an application-level proxy is provided for the DNS, HTTP, SMTP, and POP3 protocols.

238 The Strength of Function metrics defined in the Security Target for FIA_UAU.5 have been modified from the Strength of Function metrics in the PP. The ST removes the metric related to the single-use authentication mechanism because that mechanism is not totally provided with the TOE.

239 O.SINUSE has been removed as an objective for the TOE and inserted as an objective for the environment. This reflects the fact that the authentication server is part of the environment.

240 Changed the wording of FAU_STG.1.2 to be consistent with version 2.2 of the CC which went into effect after the PP was validated.

7.4 PP Additions

241 This section entitled *PP Additions* describes elements of the ST that are not part of the PPs. In particular, this section describes SFRs, SARs, and security objectives that are not found in the PPs, but were added by the ST author for the reasons described herein.

242 The FIA_UAU.4 Single-use Authentication Mechanisms SFR was added and allocated to the environment because the single-use authentication server is included in the environment, but not within the TOE. Another SFR, FIA_UAU.8.1 (EXP) Invocation of Authentication Mechanism, was added to clarify the role of the TOE to invoke and enforce the use of the single-use authentication mechanism for FTP and Telnet users.

243 The assurance level of EAL2 in the [ALFPP_BAS] PP was augmented with additional SARs to bring the overall level of assurance up to EAL 4, augmented with ALC_FLR.3. The purpose of the additional EAL4 assurance requirements is to provide a meaningful increase in assurance beyond the PP by requiring more design description, more complete testing coverage, and improved mechanisms and/or procedures that provide more confidence that the TOE will not be tampered with during development or delivery. The assurance was further augmented by adding ALC_FLR.3 to help ensure that reported defects in the TOE are addressed by the developer.

244 O.DOMSEP has been included because the local administration platform and authentication server have been moved to the environment. In the PP, O.SELPRO applies to both the firewall and the authentication server; but as this is not the case in Sidewinder, a corresponding objective has been added to the environment.

245 O.PROLIN has been included because the Authentication Server has been moved to the environment. In the PP, O.PHYSEC applies to both the firewall and the authentication server. Since this is not the case for Sidewinder, O.ASPHYSEC has been added to the environment to protect communications between the TOE and the administrator Windows computer and, also, between the TOE and the Authentication Server.

246 O.ASLOWEXP, O.ASGENPUR, O.ASPUBLIC, O.ASNOEVIL, and O.ASNOREMO have been added as objectives for the environment as a result of moving the authentication server and remote administration platform to the environment. They have the same intent as corresponding objectives in the PPs.

7.5 PP Omissions

247 The following PP components were omitted from this ST because remote administration is not part of the evaluated configuration.

a) A.REMACC Assumption
b) P.CRYPTO OSP
c) O.ENCRYP TOE Objective
d) O.REMACC TOE Environment Objective
e) FCS_COP.1 SFR
f) T.PROCOM Threat

248 A.GENPUR and A.NOREMO have been removed from the list of assumptions for the TOE, although they remain in place for the local administration platform and authentication server in the environment. Similarly O.GENPUR and O.NOREMO have been removed from the list of objectives for the TOE, although they remain in place for the local administration platform and authentication server in the environment.

249 O.GENPUR has been removed because the use of Type Enforcement means the objective is implicit within the TOE.

250 O.NOREMO has been removed because there is no remote access allowed in the TOE and the way the objective is phrased can be interpreted such that authorized administrators can access the TOE remotely.

251 O.EAL has been removed for clarity as this is a requirement on the TOE itself, rather than an objective that it must achieve.

252 O.DIRECT has been omitted from the TOE as its intent is covered entirely by O.PHYSEC, O.ASPHYSEC, O.NOEVIL and O.ASNOEVIL.

253 The ST omits FIPS PUB 140-1 compliance from its FIA_UAU.5 strength of function declaration, since single-use authentication is done in the environment.

8 Rationale

8.1 Rationale for TOE Security Objectives

254 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.

255 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.

256 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.

257 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.

258 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.

259 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.

260 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.

261 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 15. 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

262 O.PHYSEC The TOE is physically secure.

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

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

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

266 O.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.

267 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.

268 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.

269 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.

270 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.

271 O.PROLIN The communication path between the TOE(.e., authentication client) and the single-use authentication server is physically protected. Similarly, the communication path between the TOE and the administrator Windows computer is physically protected.

272 O.ASPHYSEC The authentication server and local administration platform are physically secure.

273 O.ASLOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities in the authentication server or the local administration platform is considered low as a result of having no connections with IT entities other than the TOE.

274 O.ASGENPUR There are no extraneous applications, beyond authentication services and TOE administration, on the authentication server or on the local administration platform.

275 O.ASPUBLIC The authentication server and local administration platform do not host public data.

276 O.ASNOEVIL Authorized administrators of the authentication server and the local administration platform are non-hostile and follow all administrator guidance; however, they are capable of error.

277 O.ASNOREMO There is no remote access to the authentication server or the local administration platform.

Table 16. 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**		

278 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

279 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 17. Mapping SFRs to TOE Security Objectives illustrates the mapping between the TOE security requirements and the TOE security objectives. Table 15. Mapping Threats to TOE Security Objectives demonstrates the relationship between the TOE threats and the TOE security objectives. Together these tables demonstrate the completeness and sufficiency of the requirements.

280 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

281 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

282 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

283 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

284 This component ensures that human users who are not authorized administrators cannot endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable from the point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_UAU.5 Multiple authentication mechanisms

285 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

286 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)

287 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)

288 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)

289 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)

290 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)

291 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)

292 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)

293 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)

294 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

295 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)

296 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)

297 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.

FMT_MTD.2 Management of limits on TSF data

298 This component ensures that the TSF restrict the specification of limits of the number of unauthenticated failures to the authorized administrator and specifies the action be taken if limits on the TSF data are reached or exceeded. This component traces back to and aids in meeting the following objective: O.SECFUN.

FDP_RIP.1 Subset residual information protection

299 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

300 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

301 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

302 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

303 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

304 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

305 This component ensures that a variety of searches and sortscan 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

306 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

307 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)

308 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)

309 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 17. 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**						

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
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	
FMT_MTD.2							X	
FDP_RIP.1		X						
FPT_RVM.1			X	X				
FPT_SEP.1				X				
FPT_STM.1					X			
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

310 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.

Rational for Not Including FMT_SMF.1

311 Common Criteria version 2.2 [CC_PART2] introduces a dependency for FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 requirements to include a new FMT_SMF.1 requirement. This ST does not include that requirement. The ST was written to be consistent with two DoD firewall PPs that predate CC version 2.2 and don't include the extra requirement. In each case, the MOF.1, MSA.1 and MTD.1 requirements "restrict" certain management functions to an authorized administrator and this has been interpreted within this ST as requiring that those management functions exist in the TOE. Section 6.1.1, the TOE Summary Specification, includes these management functions.

8.4 Rationale for TOE IT Environment Security Requirements

312 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

313 The EAL 4 level of assurance was chosen to provide a moderate to high level of independently assured security, including confidence that the TOE will not be tampered with during development or delivery. Augmentation with ALC_FLR.3 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 sensitive 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

314 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

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

Table 18. 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	Yes, FIA_UAU.5 provides the timing of authentication
FIA_UAU.4	NONE	N/A
FIA_UAU.5	NONE	N/A
FIA_UAU.8 (EXP)	NONE	N/A
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 FMT_SMF.1	 Yes Yes No – see Section 8.3
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes No – see Section 8.3
FMT_MTD.2	FMT_SMR.1 FMT_MTD.1	Yes Yes
FDP_RIP.1	NONE	N/A
FPT_RVM.1	NONE	N/A
FPT_SEP.1	NONE	N/A

SFR/SAR	Dependencies	Satisfied?
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 FMT_SMF.1	Yes No – see Section 8.3
ACM_AUT.1	ACM_CAP.3	Yes, ACM_CAP.4
ACM_CAP.4	ALC_DVS.1	Yes
ACM_SCP.2	ACM_CAP.3	Yes, ACM_CAP.4
ADO_DEL.2	ACM_CAP.3	Yes, ACM_CAP.4
ADO_IGS.1	AGD_ADM.1	Yes
ADV_FSP.2	ADV_RCR.1	Yes
ADV_HLD.2	ADV_FSP.1 ADV_RCR.1	Yes, ADV_FSP.2 Yes
ADV_IMP.1	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	Yes Yes Yes
ADV_LLD.1	ADV_HLD.2 ADV_RCR.1	Yes Yes
ADV_RCR.1	NONE	N/A
ADV_SPM.1	ADV_FSP.1	Yes, ADV_FSP.2
AGD_ADM.1	ADV_FSP.1	Yes, ADV_FSP.2
AGD_USR.1	ADV_FSP.1	Yes, ADV_FSP.2
ALC_DVS.1	NONE	N/A
ALC_FLR.3	NONE	N/A
ALC_LCD.1	NONE	N/A
ALC_TAT.1	ADV_IMP.1	Yes
ATE_COV.2	ADV_FSP.1 ATE_FUN.1	Yes, ADV_FSP.2 Yes
ATE_DPT.1	ADV_HLD.1 ATE_FUN.1	Yes, ADV_HLD.2 Yes
ATE_FUN.1	NONE	N/A
ATE_IND.2	ADV_FSP.1	Yes, ADV_FSP.2

SFR/SAR	Dependencies	Satisfied?
	AGD_ADM.1	Yes
	AGD_USR.1	Yes
	ATE_FUN.1	Yes
AVA_MSU.2	ADO_IGS.1	Yes
	ADV_FSP.1	Yes, ADV_FSP.2
	AGD_ADM.1	Yes
	AGD_USR.1	Yes
AVA_SOF.1	ADV_FSP.1	Yes, ADV_FSP.2
	ADV_HLD.1	Yes, ADV_HLD.2
AVA_VLA.2	ADV_FSP.1	Yes, ADV_FSP.2
	ADV_HLD.2	Yes
	ADV_IMP.1	Yes
	ADV_LLD.1	Yes
	AGD_ADM.1	Yes
	AGD_USR.1	Yes

8.8 Internal Consistency and Mutually Supportive Rationale

316 The set of security requirements identified in this ST for Sidewinder 7.0.0.02 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 18.

c) The SOF claims are valid. The chosen SOF-medium level is consistent with the attack potential identified in Section 3 of this ST. The identified metrics and SOF claim is commensurate with the EAL 4 level of assurance.

d) The SARs are appropriate for the assurance level of EAL 4 and are satisfied by Sidewinder 6.1 as demonstrated in Section 6.2 of this ST.

8.9 Rationale for Explicit Requirements

317 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

318 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

319 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 19. Mapping of SFRs to Security Functions demonstrates that each SFR is covered by at least one security function.

Table 19. 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, SW_FMT
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
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
FMT_MTD.2	Management of Limits on TSF data	SW_FMT

Functional Components		Security Function
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	SW_FPT
FPT_STM.1	Reliable time stamps	SW_FPT
FAU_GEN.1	Audit data generation	SW_FAU
FAU_SAR.1	Audit review	SW_FAU, SW_FMT
FAU_SAR.3	Selectable audit review	SW_FAU, SW_FMT
FAU_STG.1	Protected audit trail storage	SW_FAU, SW_FMT
FAU_STG.4	Prevention of audit data loss	SW_FAU
FMT_MOF.1	Management of security functions behavior (1)	SW_FMT
FMT_MOF.1	Management of security functions behavior (2)	SW_FMT

320 Table 20 provides rationale that the security functions are suitable to meet the SFRs.

Table 20. 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_MTD.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. A user acting in the administrator role is allowed to control the operation of the TOE, manage user attributes, 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 and setting the limit for authentication failure handling. Authorized administrators are provided the capability to selectively review audit data and may remove old audit records.
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.
SW_FPT	FPT_RVM.1 FPT_SEP.1 FPT_STM.1	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 searching and sorting. Audit records are protected from modification and unauthorized deletion. If the audit trail becomes full, appropriate safeguards are applied to prevent audit data loss.

321 Because the security functions trace to SFRs, which were shown to be mutually supportive in Section 8.8, and Table 20 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

322 Table 21 is provided to demonstrate that each TOE SAR is adequately addressed by at least one assurance measure.

Table 21. Assurance Measure Suitability

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
ACM_AUT.1	Sidewinder Configuration Management Plan	The Configuration Management Plan describes automated tools used in the CM system. These automated mechanisms support the generation of the TOE and ensure that only authorized changes are made.
ACM_CAP.4	Sidewinder Configuration Management Plan	The Configuration Management Plan provides for unique identification of the TOE and all related configuration items. It also describes the controls used to ensure that any creation or modification of configuration items is authorized. It describes the procedures used to accept modified or new configuration items as part of the TOE.
ACM_SCP.2	Sidewinder Configuration Management Plan	The Configuration Management Plan describes the scope of items that are managed by the CM system. It describes the tracking of the TOE implementation, security flaws, and documentation used for evaluation.
ADO_DEL.2	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.
ADO_DEL.2	Common Criteria Evaluated Configuration Guide (CCECG)	This document contains delivery procedures followed in the delivery of the TOE.
ADO_IGS.1	Sidewinder Startup Guide	This document describes the procedures for the secure installation, generation, and start-up of the TOE.

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
ADO_IGS.1	Common Criteria Evaluated Configuration Guide (CCECG)	This document supplements the installation procedures provided in the Sidewinder Startup Guide.
ADV_FSP.2	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.2	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_IMP.1	Sidewinder Code Subset (source code files; this is not a document)	Code files for a selected subset of the TSF are provided.
ADV_LLD.1	Sidewinder Low-Level Design (consists of information files, not a formal document)	The low-level design files describe the TSF in terms of modules. These files include the purpose, security functionality, and interface identification.
ADV_RCR.1	Sidewinder Security Functions Correspondence Analysis	This analysis document provides the correspondence between all adjacent pairs of TSF representations that are provided.
ADV_SPM.1	Sidewinder Security Target	This document provides a security policy model that corresponds to the security functions in the functional specification.
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.
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.

Assurance Component ID	Assurance Measure (a document, unless otherwise noted)	Justification
ALC_DVS.1	Sidewinder Development Security Description	This document describes the physical, procedural, personnel and other security procedures that are used during the development and maintenance of the TOE.
ALC_FLR.3	Sidewinder Security Flaw Reporting Procedures	This document defines the security flaw handling procedures to be followed by the developer.
ALC_FLR.3	Common Criteria Evaluated Configuration Guide (CCECG)	This document contains information on security flaw reporting procedures
ALC_LCD.1	Sidewinder Life-Cycle Model	This document defines the life-cycle model applied to develop and maintain the TOE.
ALC_TAT.1	Sidewinder Development Tools Definition	This document defines the development tools used for the TOE.
ATE_COV.2	Sidewinder Test Plan/Coverage Analysis	This document shows the correspondence between tests and the security functions.
ATE_DPT.1	Sidewinder Test Depth Analysis	This document describes the testing of the high-level design in terms of its subsystems.
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, not a document)	This is a copy of the TOE that is suitable for independent testing by evaluators.
AVA_MSU.2	Sidewinder Guidance Documentation Analysis	The guidance documents are examined and an analysis is performed to ensure that the documents are sufficient to allow an administrator to move a delivered system to a secure operational state. The analysis results are documented.
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.2	Sidewinder Vulnerability Analysis	A systematic 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.