Gauntlet 6.0

Security Target

Version 3.1

Prepared By:

CSC Australia

Prepared For:

Secure Computing Corporation

http://www.securecomputing.com/

Table of Contents

List of Tables

0 - Security Target Introduction

This introductory section presents *Security Target (ST)* identification information and an overview of the ST structure.

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

- 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).

- A set of security objectives and a set of security requirements to address the threats and assumptions (in Sections 4 and 5, Security Objectives and IT Security Requirements, respectively).

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

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 presents a user-oriented document that minimises reference to other material that might not be readily available to the ST users.

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

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

0.1 - Identification

ST Title: Gauntlet 6.0 Security Target, Version 3.1, February 2002

TOE Identification: Gauntlet 6.0, Build Numbers: Firewall - 0226a (kernel 0731d);

GUI – 0226a.

Patches:

Patch	**Version**	**Patch**	**Version**
authsvr.patch	1	crfwcert.patch	1
crontab.patch	1	edatupdate.patch	1
Ednload.patch	1	Espmc.patch	1
Espmd.patch	1	Frequentcheck.patch	2
ftp-pdk.patch	2	Fwregister.patch	1
Getroot.patch	1	Gfw.patch	2
Gui.patch	2	http-pdk.patch	3
Iiop-pdk.patch	2	Ipe-patch	1
ipfs.patch	1	jre.patch	1
login-sh.patch	1	mmp.patch	1
oracle.patch	1	plug-pdk.patch	2
proxymgr.patch	1	rootusr.patch	3
rtsp-pdk.patch	2	snmp.patch	1
socks5-gw.patch	1	ssod.patch	1
stdlogd.patch	2	stdlogespmc.patch	1
tn-gw.patch	1	trans.patch	1
udp-pdk.patch	2	up242.patch	1
vscan.patch	1	vsrequest.patch	1
Checkspace.patch	2	Smtp.patch	1
Csmap.patch	2		

Authors: CSC Australia, AISEF

CC Version: Common Criteria for Information Technology Security Evaluation, Version 2.1

Assurance Level: EAL 4

General Status: Final

Keywords: Information flow control, Firewall, Packet filter, network security, Proxy server, application gateway

0.2 - References

[1] *Common Criteria for Information Technology Security Evaluation*, August 1999, Version 2.1, CCIMB-99-031

[2] *Gauntlet 6.0 (Solaris 8) Administrator's Guide*

0.3 - Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 2.1.4 of Part 2 of the CC. Except for the iteration operation, each of these is used in the Protection Profiles claimed in this Security Target.

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**.

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

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].

0.4 - Terminology

In Common Criteria many terms are defined in Section 2.3 of Part 1. The following are listed as an aide to understanding the Security Target.

Terms	Explanation
Authenticated data	Information used to verify the claimed identity of a user
Authorised Administrator	A role which human users maybe 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 not to compromise the security policy enforced by the TOE.
Authorised 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.
Bastion host	A host system on the internal network that is the main point of contact between end users and services on the internal network and the external network.
Dual or Multi-homed bastion host	A bastion host that is also a gateway between the internal network and the external networks. Separate physical communication links are used to connect to the networks.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE
Human User	Any person who interacts with the TOE
Identity	A representation (eg a string) uniquely identifying an authorised user, which can either by the full or abbreviated name of that user or a pseudonym
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
User	Any entity that has valid user account and passes information through the TOE. A user does not have privilege to log-on to the firewall configuration interface.

0.5 - Acronyms

Acronym	Explanation
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Programme
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile

Acronym	Explanation
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

0.6 - Document Organisation

Section 1 provides the introductory material for the Security Target.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively, that must be satisfied by the TOE.

Section 6 defines the IT security functions provided by the TOE to meet the security objectives defined in Section 4. Additionally this section provides a general mapping of assurance requirements to evidence that the developer provides appropriate assurance measures mitigating the specified requirements.

Section 7 provides a rationale to support conformance, additions and alterations to Protection Profiles.

0.7 - Security TOE Overview

Gauntlet 6.0 Firewall system is designed to provide secure access and internetwork communications between private, trusted networks and public, untrusted networks, such as the Internet, or between subnets within a private network.

The Gauntlet Firewall is a software application; application-level security services, IP screening facility, and the UNIX operating system management utilities.

The Gauntlet Firewall is an application-level proxy and traffic-filter based firewall that provides:

- Control over access to services,
- Prevention of the flow of IP packets for which no service in either direction is permitted,
- Mediation of IP packets corresponding to services for which proxies are provided, and

- Forwarding of just those IP packets corresponding to un-proxied services that have been authorised by Administrators for direct passage through the Firewall.

This Security Target limits itself to Internet Firewalls for the following reasons:

- Only TCP/IP protocols are addressed;

- It is assumed that the Firewall is being used :

    1. to protect a private network from a larger network not under the administrative control of the Firewall owner.

    2. To control communication between subnets that are under the same administrative control within a private network.

This can be expanded to include any Internet, including so-called Intranets.

All of the proxies are configurable. You can accept or reject requests to or from certain sites and networks, or set up other rules the proxies use when passing requests through the firewall. You can also enable or disable individual proxies and run only the ones you need. You can easily translate your security policies into configuration rules.

In addition, the Gauntlet Firewall also contains several programs that ease the job of administering the firewall. These include management tools for configuring the firewall, and scripts for reporting activity through the firewall and performing general administration.

The Graphical User Interface (GUI) Gauntlet Firewall Manager utility provides an easy-to-use interface to perform most standard configuration activities

The Gauntlet Firewall also includes shell scripts that assist in upgrading, creating backups, checking integrity, and other general administrative tasks.

0.8 - CC Conformance Claim

The TOE is conformant with Parts 2 and 3 of the CC Version 2.1.

1 - TOE Description

1.1 - Product Type

The Gauntlet Firewall is a software based application gateway & traffic-filter Firewall that supports only those services specifically configured by the Firewall Administrator, and only those that can be implemented securely. The Gauntlet Firewall offers application-level security services that regulate communications in both directions.

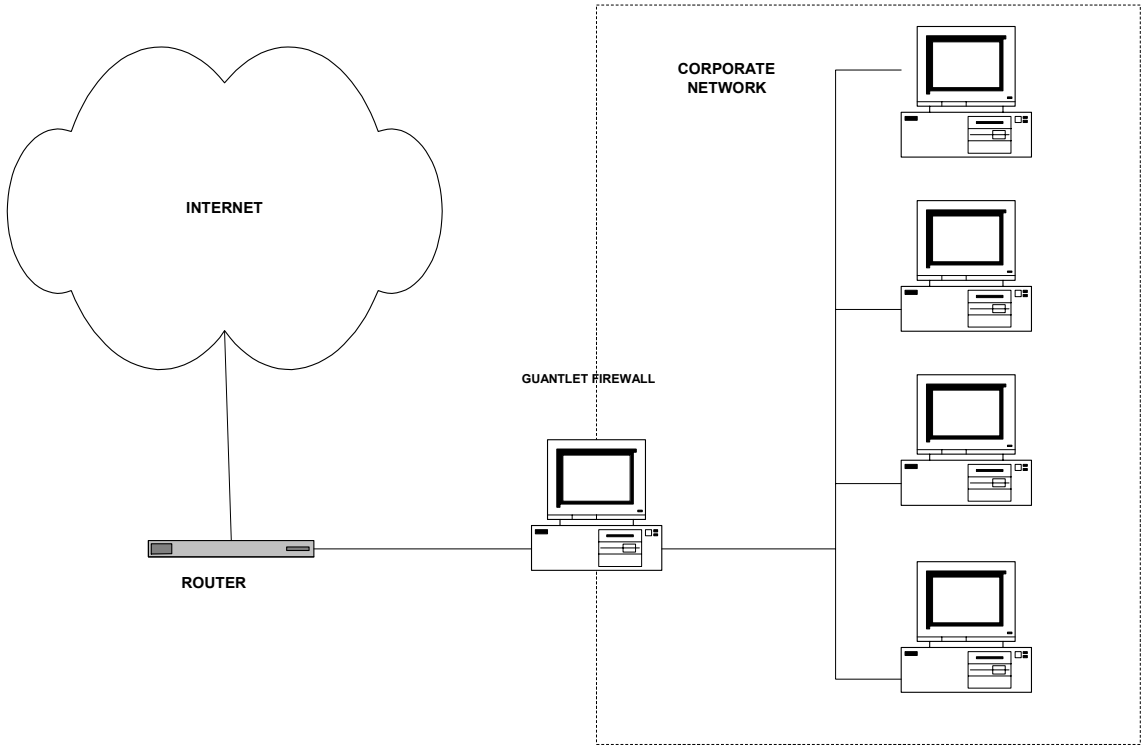
The Gauntlet Firewall provides secure access and internetwork communications between private, trusted networks (termed "internal" in this document) and public, untrusted networks such as the Internet (termed "external"), or between organisations within a private network.

In the evaluated configuration Gauntlet is installed as a dual or multi-homed bastion host between an internal and external network(s). This does not preclude its successful use in other Firewall configurations, but other configurations may involve the use of other components/products, which are outside the scope of the evaluated configuration.

1.2 - Physical Scope and Boundary

A Firewall may be used to limit the access that one network has to another. However, for this Security Target, the intended environment is assumed to comprise a private network on one side of the Firewall, and 'external' network(s) on the other as in Figure 2.1. The 'external' network(s) need not be malignant, but it is assumed that it may be. Certain assumptions are made about the internal network, ie. to the host systems on that network and to those systems' end users.

Figure 2.1 Physical Boundary



Gauntlet is an integrated product placed on an underlying operating system with product specific software but is submitted as a single product for evaluation.

Gauntlet will run on a number of variants of the UNIX operating system on various hardware platforms. This Security Target applies to:

- Gauntlet Version 6.0 (with the following proxies: Telnet, SMTP (smap/smapd), POP3, plug, http, Oracle SQL, Microsoft SQL, Sybase, FTP, SNMP and removal of Java, Active X from HTTP services);

- Solaris 8;

The table below defines the hardware and software requirements for the TOE. Increasing the values in the following table will generally have a positive impact on system performance. The firewall may operate below these values, but system performance may be significantly degraded.

Table 2.1 Minimum System Hardware Requirements

System	Sun (Solaris 8)
Type	Any Sun Platform capable of running the Solaris 8 Operating System
Memory	32-bit: 128MB Memory 64-bit: 512MB Memory
Disk Space	4 GB of disk (more is strongly recommended) configured with: • Root: 128 MB • Swap: a minimum of two times the size of the physical memory • /usr: 1GB • /var: remaining space (1GB minimum)
Other Hardware	• Access to CD-ROM drive supported by Solaris 8. • Also required are a minimum of two supported Ethernet adaptors (one for the trusted network and one or more for untrusted networks)
Other Software	Solaris software packages (required for installation): • Standalone System (do **not** select OS Server or Dataless Client); • Developer System Support (do **not** select End User System Support or Core System Support); and • Patches required by the Solaris 8 Security Target, Issue 1, 28 July 2000, to comply with the EAL 4 evaluation of Solaris 8.

There are no firmware dependencies.

1.3 - Logical Scope and Boundary

The software components of the Gauntlet Firewall include application-level security services, IP screening facility, and other management utilities.

- Operating System

The operating system is the evaluated version of UNIX (Solaris 8). The supporting protection mechanisms implemented in the hardware and relied upon by the operating system are, in summary, the following CPU features:

a) kernel mode and user mode execution;

b) segmentation and paging memory management;

c) exception and interrupt handling ;

- Application Level Security

The software on the Gauntlet Firewall includes security services on a per-application basis. All packets, and therefore all application requests, go to the firewall. On the firewall, proxy software relays information from one side of the firewall to the other. The proxy prevents unauthorised applications on external networks from talking directly with the applications on your internal network, and vice versa. No unauthorised IP packets pass from one side of the firewall to the other. All data is initially passed at the application level. Each application generally talks through a different proxy that understands the protocol for that application.

The proxies log all activities to and through the firewall. The logs can be used to gather usage statistics or to look for potential attacks. In addition, several proxies support strong user authentication systems. These one-time passwords systems provide additional security because users use a different password each time they access the network.

Currently, the Gauntlet Firewall includes proxies for the following types of services:

- Terminal services (TELNET)
- Electronic mail (SMTP (smap/smapd) and POP3)
- Plug gateway
- File transfer services (FTP)
- Web services (HTTP)
- SQL services (Oracle*SQL, Microsoft SQL and Sybase)
- SNMP (Simple Network Management Protocol)
- Removal of Java and Active X from HTTP services.

In addition, the Gauntlet Firewall includes two generic “plug” proxies, namely the “TCP Plug” and the “UDP Plug”. The TCP Plug proxy patches (plugs) TCP traffic from a particular port on one side of the firewall to a particular TCP port on another system on the other side of the firewall. As with the service-specific proxies, no unauthorised IP packets pass from one side of the firewall to the other. If you have not installed a proxy for a service, that type of traffic does not pass through the firewall. The TCP Plug is included in the scope of the evaluation. The UDP Plug is not in the scope of the evaluation.

The Gauntlet Firewall includes configured versions of the TCP plug proxy for:

- LDAP (certificate management);
- Usenet news (NNTP);
- Web services (SSL);
- AOL;
- Compuserve;
- Lotus Notes;
- NNTP;
- NetBIOS-tcp;
- NetMeeting; and
- X.500.

All of the proxies are configurable.

- IP Screening

The Gauntlet Firewall includes additional security software in the form of an IP screening facility. This feature checks IP packets based on several criteria (for example, address and protocol) and processes or rejects the packets. It detects spoofed packets claiming to be from one network that are actually from another network. The firewall does not support IP packet forwarding, source routed packets, or ICMP redirects. These services change the directions that packets flow, and could direct networks to circumvent the firewall. Services such as NFS, NIS, and RPCs cannot easily be made secure and so are disabled. Unsupported network services do not just report an error to the requesting site. The operating system logs these access attempts, providing information about probes of your system.

Using the IP screening utility, you can configure the firewall so that the firewall is transparent to your users for most activities. The IP screening facility provides a method for permitting high bandwidth or unsupported protocols in situations where the security requirements are not as stringent as with an Internet firewall.

Three services offer an "Adaptive Proxy" option that lets you define a configuration of the proxy that switches between an application proxy and IP filtering when circumstances warrant it. These services are FTP, HTTP, and the TCP plug proxy.

- Management

Management and administration of Gauntlet is performed by an Administrator who logs into the Firewall's underlying operating system via the Management Terminal. Remote Administration of the Gauntlet Firewall is outside the scope of the evaluation.

Gauntlet must be managed via the Management Terminal which is a dedicated physical port on which no other connections are permitted. (This may be any type of port provided no connections other than for management are permitted. It may therefore be for example, the PC's console or an RS232 port with a dumb terminal). For this Security Target, it is assumed that all users of the operating system are Administrators of Gauntlet.

In addition, the Gauntlet Firewall also contains several programs that ease the job of administering the firewall. These include management tools for configuring the firewall, and scripts for reporting activity through the firewall and performing general administration.

The graphical Gauntlet Firewall Manager utility provides an easy-to-use interface to perform most standard configuration activities. You do not need to modify system files or configuration files unless you want to customise your configuration.

The Gauntlet Firewall also includes shell scripts that assist in upgrading, creating backups, checking integrity, and other general administrative tasks.

1.4 - Security Features

The TOE provides the following security features:

Table 2.2 TOE Security Features

Feature	Description
Identification and Authentication	The Gauntlet Firewall requires users and administrators to identify themselves before they can perform any action.

Feature	Description
Security Audit	The Gauntlet Firewall detects the occurrence of selected events and stores information relating to those events in Administrator accessible log files. The Solaris operating system also detects the occurrence of certain events and records the related information.
Access Control	The Gauntlet Firewall restricts access between external and internal networks based on traffic filtering and application proxy rules.
Information Flow Control	The Gauntlet Firewall controls the flow of IP packets between any client and the application servers under its control.
System Security Management	The workstation console provides access to the Solaris operating system for security administration of the Gauntlet Firewall. The workstation console also provides access to the management functions relating to the auditing and audit report production.
System Architecture	The Solaris operating system maintains protection mechanisms for the Gauntlet security enforcing and other software components, that protects them from interference and tampering by untrusted subjects.

2 - TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any *assumptions* about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- Any known or assumed *threats* to the assets against which specific protection within the TOE or its environment is required.
- Any *organisational security policy* statements or rules with which the TOE must comply.

2.1 - Secure Usage Assumptions

Table 3.1 TOE Environmental Assumptions

Assumption ID	Description
A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerability's is considered low.
A.GENPUR	There are no general-purpose computing capabilities (eg the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorised 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.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (eg a console port) if the connection is part of the TOE.
A.NOREMO	Human users **including** authorised administrators can not access the TOE remotely from the internal or external networks.
A.TRAINING	Administrators are trained in Unix Administration and have a good knowledge of Internet protocols, including: HTTP, TCP/IP, FTP, Telnet and other proxies that they allow through their firewall.
A.USERS	Users are trusted not to deliberately bypass the firewall by installing rogue software, which may be used to open valid connections to transmit protected information.

2.2 - Threats to Security

Table 3.2 Threats addressed by the TOE

Threat ID	Description
T.NOAUTH	An unauthorised 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.REPEAT	An unauthorised person may repeatedly try to guess authentication data in order to use information to launch attacks on the TOE.
T.REPLAY	An unauthorised person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorised person may carry out spoofing in which information flow through the TOE into a connected network by using spoofed source address.
T.MEDIAT	An unauthorised person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
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 unauthorised person may read, modify or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorised person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions

Table 3.3 Threats to be addressed by operating environment

Threat ID	Description
T.TUSAGE	The TOE may be inadvertently configured, used and administered in a insecure manner by either authorised or unauthorised persons.

3 - Security Objectives

3.1 - Security Objectives for the TOE

Table 4.1 TOE IT Security Objectives

Objective ID	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.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information from users on a connected network to users on another network.
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 unauthorised 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 authorised administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorised administrator to use the TOE security functions, and must ensure that only authorised administrators are able to access such functionality.
O.LIMEXT	The TOE must provide the means for an authorised administrator to control and limit access to TOE security functions by an authorised external IT entity.

3.2 - Security Objectives for the Environment

Table 4.2 Security Objectives for the TOE Environment

Environmental Objective ID	Description
OE.PHYSEC	The TOE is physically secure.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerability's is considered low.
OE.GENPUR	There are no general-purpose computing capabilities (eg the ability to

	execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.PUBLIC	The TOE does not host public data.
OE.NOEVIL	Authorised administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (eg a console port) if the connection is part of the TOE.
OE.NOREMO	Human users including authorised administrators can not access the TOE remotely from the internal or external networks.
OE.GUIDAN	The TOE must be delivered, installed, administered and operated in a manner that maintains security.
OE.ADMTRA	Authorised administrators are trained in and responsible for: the establishment and maintenance of security policies and practices; user awareness; and operating system and internet protocol operation.
OE.OS	The Operating system will provide functions to the TOE to: provide time-stamping; assist in Audit entry recording and sorting and provide password-checking functionality.

3.3 - Security Objectives Rationale

The need to demonstrate that the correctness of mapping's and adequacy of objectives to threats and assumptions is satisfied as follows:

Table 4.3 demonstrates that each threat is met by at least one security objective and that all threats have been addressed.

The purpose of this rationale is to demonstrate that the stated security objectives are suitable and adequate to counter the identified threats to security.

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.

O.SINUSE This security objective is necessary to counter the threats: T.REPEAT and T.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.

O.MEDIAT This security objective is necessary to counter the threats T.ASPOOF and T.MEDIAT , which 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.

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

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and

T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

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.

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 authorised administrators are accountable for the use of security functions related to audit.

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

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

Table 4.3 All Threats to Security Addressed by Objectives

Threat	Short Description	Associated Security Objective
T.NOAUTH	Unauthorised attempt to bypass the security of the TOE.	O.IDAUTH O.SECSTA O.SECFUN O.LIMEXT OE.OS
T.REPEAT	Unauthorised attempt to repeatedly try to guess authentication data.	O.SINUSE
T.REPLAY	An unauthorised person may use valid identification and authentication data to access functions provided by the TOE.	O.SINUSE O.SECFUN
T.ASPOOF	An unauthorised person may carry out spoofing.	O.MEDIAT
T.MEDIAT	An unauthorised person may send impermissible information through the TOE thereby exploiting resources on the internal network.	O.MEDIAT
T.AUDACC	An attacker may escape detection as audit records have not been reviewed.	O.AUDREC O.ACCOUN OE.OS
T.SELPRO	An unauthorised person may read, modify or destroy security critical TOE configuration data.	O.SECSTA O.SELPRO
T.AUDFUL	Audit records can be lost when the audit storage capacity is exhausted.	O.SELPRO O.SECFUN
T.TUSAGE	The TOE may be inadvertently configured, used and administered in a insecure manner.	OE.GUIDAN OE.ADMTRA

3.4 - Security Objectives for the Environment Rationale

OE.PHYSEC The TOE is physically secure.

OE.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerability's is considered low.

OE.GENPUR There are no general-purpose computing capabilities (eg., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

OE.PUBLIC The TOE does not host public data.

OE.NOEVIL Authorised administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

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

OE.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (eg., a console port) if the connection is part of the TOE.

OE.NOREMO Human users including authorised administrators can not access the TOE remotely from the internal or external networks.

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

OE.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorised administrators receive the proper training.

OE.OS This non-IT security Objective is required to support the TOE in performing functions relevant to security. This objective is necessary to counter the Threats T.NOAUTH and T.AUDACC as supporting functionality provided by the environment is required for the TOE to counter these threats.

Since the rest of the security objectives for the environment are, in part, a re-statement of the security assumptions, those security objectives trace to all aspects of the assumptions.

Table 4.4 demonstrates that every assumption is met by at least one security objective and that all assumptions have been addressed.

Table 4.4 All Secure Usage Assumptions met by Objectives

Secure Usage Assumption	Short Description	Associated Security Objective
A.PHYSEC	The TOE is physically secure.	OE.PHYSEC
A.LOWEXP	Malicious attacks aimed at discovering exploitable vulnerability's is considered low.	OE.LOWEXP

Secure Usage Assumption	Short Description	Associated Security Objective
A.GENPUR	There are no general-purpose computing and storage repository capabilities on the TOE.	OE.GENPUR
A.PUBLIC	The TOE does not host public data.	OE.PUBLIC
A.NOEVIL	Authorised administrators are non hostile and follow all administrator guidance.	OE.NOEVIL OE.ADMTRA
A.TRAINING	Authorised administrators are trained in all relevant protocols and operating systems.	OE.ADMTRA
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.	OE.SINGEN
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection if the connection is part of the TOE.	OE.DIRECT
A.NOREMO	No one may access the TOE remotely from the internal or external networks.	OE.NOREMO
A.USERS	Users will not install software that may bypass the TOE.	OE.ADMTRA

4 - IT Security Requirements

4.1 - TOE Security Functional Requirements

Table 5.1 Security Functional Requirements

Functional Class	Functional Components
FMT_SMR.1	Security Roles
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.3	Static attribute initialisation
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.1	Timing of authentication
FIA_AFL.1	Authentication failure handling
FIA_UAU.4	Single use 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)
FPT_RVM.1	Non-bypassability of the TSP
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
FCS_COP.1	Cryptographic Operations
FTA_TSE.1	TOE session establishment

All Security Functional Requirements have been drawn from the CC Part 2.

4.1.1 -Security Management

FMT_MOF.1 Management of the security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***perform*** the functions:

a) [start-up and shutdown;

b) create, delete, modify and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify and view user attribute values defined in FIA_ATD.1;

d) enable and disable single-use authentication mechanisms in FIA_UAU.4;

e) modify and set the threshold for the number of permitted authentication attempt failures;

f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures;

g) enable and disable external IT entities from communicating with the TOE (if the TOE supports external IT entities);

h) not used;

i) archive, create, delete and empty the audit trail;

j) backup of user attribute values, information flow security policy rules and audit trail data, where the backup capability shall be supported by automated tools;

k) recover to the state following the last backup;

l) generate and verify checksums of the Firewall's current file system in the integrity database;]

to [an authorised administrator].

FMT_SMR.1 Security roles

FMT_SMR.1.1 - The TSF shall maintain the role [authorised administrator].

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

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 - The TSF shall enforce the [information flow control UNAUTHENTICATED SFP and AUTHENTICATED SFP,] to provide *restrictive* default values for **information flow** security attributes that are used to enforce the SFP.

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

4.1.2 -Identification and Authentication

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 - The TSF shall detect when [five attempts] unsuccessful authentication attempts occur related to [users not associated with the authorised administrator role attempting to authenticate from an internal or external network.]

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 authorised administrator takes some action to make authentication possible for the user in question.]

FIA_ATD.1 User Attribute Definition

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 authorised administrator role.]

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 - The TSF shall allow:

a) [information flow control decisions and subsequent passing or dropping of non-FTP and non-Telnet traffic;

b) identification as stated in FIA_UID.2]

on behalf of the authorised administrator or authorised external IT entity accessing the TOE to be performed before the authorised administrator or authorised external IT entity is authenticated.

FIA_UAU.1.2 - The TSF shall require **each authorised administrator or authorised external IT entity** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **authorised administrator or authorised IT entity**.

FIA_UAU.4 Single use authentication mechanisms

FIA_UAU.4.1 - The TSF shall prevent reuse of authentication data related to [authentication attempts from either an internal or external network by:

a) not used

b) authorised external IT entities;

c) human users attempting to access the following services through the TOE:

- File Transfer Protocol (FTP);
- Telnet]

FIA_UID.2 User identification before any action

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.

4.1.3 -User Data Protection

FDP_IFC.1 Subset information flow control (1)

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;

c) operation: pass information].

FDP_IFC.1 Subset information flow control (2)

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.4,

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

c) operation: initiate service and pass information].

FDP_IFF.1 Simple security attributes (1)[1]

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;

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;]

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 authorised 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

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

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

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

authorised 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.]

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 internal 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;

f) The TOE shall reject malformed service requests.]

FDP_IFF.1 Simple security attributes (2)[2]

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;

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;

---

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

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

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

- TOE interface on which traffic arrives and departs;
- Service (ie FTP and Telnet);
- Security relevant service command;]

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

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

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

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

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

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;

f) The TOE shall reject malformed service requests.]

4.1.4 -Protection of TOE Security Functions

FPT_RVM.1 Non-bypassability of the TSP

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.

4.1.5 -Security Audit

FAU_GEN.1 Audit data generation

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 **relevant** auditable events for the *minimal or basic* level of audit **specified in Table 5.2;** and

c) [the event in Table 5.2 listed at the "extended" level].

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, subjects identities, 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 ST, [information specified in column four of Table 5.2].

Table 5.2 Auditable Events

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Minimal	Modifications to the group of users that are part of **the authorised administrator** role.	The identity of the authorised administrator performing the modification and the user identity being associated with the authorised administrator role
FIA_UID.2	Basic	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.1	Basic	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_AFL.1	Minimal	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorised administrator of the users**	The identity of the offending user and the authorised administrator

		capability to authenticate.	
FDP_IFF.1	Basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Minimal	Changes to the time.	The identity of the authorised administrator performing the operation
FMT_MOF.1	Extended	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorised administrator performing the operation.

FAU_SAR.1 Audit review

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

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

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;

e) ranges of addresses].

FAU_STG.1 Protected audit trail storage

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

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

FAU_STG.4 Prevention of audit data loss

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

4.1.6 -TOE Session establishment

FTA_TSE.1 TOE session establishment

FTA_TSE.1 - The TSF shall be able to deny session establishment based on [times of day for defined end users, or sets of end users, for authenticated services.]

4.1.7 -Cryptographic Operations

FCS_COP.1 Cryptographic Operation

FSC_COP.1.1 – The TSF shall perform [one time password generation] in accordance with **the** specified cryptographic algorithm**s** [MD5 and S/Key5] and cryptographic key

sizes [none] that meet the following [RFC 1321].

4.2 - Security Requirements on the IT Environment

This section defines the requirements placed on the IT environment so that the TOE can function securely. Using Solaris 8 as the Operating System will satisfy these dependencies. Solaris 8 has been evaluated to EAL 4. These requirements are supportive of functions that the TOE provides.

The TOE provides audit viewing and filtering functions. However, to provide this functionality Gauntlet utilizes the functions grep, awk and tar from Solaris 8. In addition, Gauntlet does not keep time, utilizing instead the system time maintained by Solaris 8.

Gauntlet requires that only an administrator logged on to Solaris 8 as the root user can alter the configuration of Gauntlet.

All the requirements on the IT environment trace back to the Environmental Objective OE.OS. These requirements are the basis of the functions that will be relied on by Gauntlet, including Time-stamping, Audit storage and sorting functions and the initial log on for Administrators.

Based on the above rationale, the following functions are required to be provided by Solaris 8.

4.2.1 -Protection of TOE Security Functions

FPT_STM.1 Reliable time stamps

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

4.2.2 -Security Audit

FAU_SAR.1 Audit review

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

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

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

f) [user identity;

g) presumed subject address;

h) ranges of dates;

i) ranges of times;

j) ranges of addresses].

FAU_STG.1 Protected audit trail storage

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

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

4.2.3 -Identification and Authentication

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 - The TSF shall allow:

c) [information flow control decisions and subsequent passing or dropping of non-FTP and non-Telnet traffic;

d) identification as stated in FIA_UID.2]

on behalf of the authorised administrator or authorised external IT entity accessing the TOE to be performed before the authorised administrator or authorised external IT entity is authenticated.

FIA_UAU.1.2 - The TSF shall require **each authorised administrator or authorised external IT entity** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of **that authorised administrator or authorised IT entity**.

FIA_UID.2 User identification before any action

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.

4.3 - TOE Security Assurance Requirements

4.3.1 -Assurance Security Requirements Rationale

EAL4 was chosen to provide a moderate level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

The Security Assurance requirements relevant to this security target are drawn from CC Part 3 EAL4 assurance requirements. These assurance components are summarised in the following table.

Table 5-3 EAL4 Security Assurance Requirements

Assurance Class	Assurance Components	
Configuration Management (ACM)	ACM_AUT.1	Partial CM Automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation (ADO)	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development (ADV)	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high level design
	ADV_IMP.1	Subset of 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
Guidance Documents (AGD)	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support (ALC)	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests (ATE)	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: High level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

4.3.2 - Configuration Management (ACM)

Partial CM Automation (ACM_AUT.1)

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE

ACM_AUT.1.2D The developer shall provide a CM plan

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system

Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.1D The developer shall provide a reference for the TOE

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.1D The developer shall provide CM documentation.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

4.3.3 - Delivery and operation(ADO)

Detection of modification (ADO_DEL.2)

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the

user site.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

4.3.4 - Development (ADV)

Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

The developer shall provide a functional specification.

The functional specification shall be internally consistent.

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

The functional specification shall completely represent the TSF.

The functional specification shall include rationale that the TSF is completely represented.

Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.8C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Subset of the implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF

ADV_IMP.1.2C The implementation representation shall be internally consistent.

Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modelled.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modelled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

4.3.5 - Guidance documents(AGD)

Administrator guidance(AGD_ADM.1)

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

User guidance(AGD_USR.1)

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

4.3.6 - Life cycle support(ALC)

Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the

TOE.

Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Well-defined development tools(ALC_TAT.1)

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

4.3.7 - Tests(ATE)

Analysis of coverage (ATE_COV.2)

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation are complete.

Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Functional testing (ATE_FUN.1)

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and

describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Independent testing - sample (ATE_IND.2)

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

4.3.8 - Vulnerability assessment(AVA)

Validation of analysis (AVA_MSU.2)

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Independent vulnerability analysis (AVA_VLA.2)

AVA_VLA.2.1C The documentation shall show, for all identified vulnerability's, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.1D The developer shall perform and document an analysis of the TOE deliverable's searching for ways in which a user can violate the TSP.

AVA_VLA.2.2C The documentation shall justify that the TOE, with the identified vulnerability's,

is resistant to obvious penetration attacks.

AVA_VLA.2.2D The developer shall document the disposition of identified vulnerability's.

4.4 - Dependency Rationale

Table 5-4 demonstrates that the Functional / Assurance requirement dependencies are fully satisfied.

Table 5-4 Functional and Assurance Requirements Dependencies

Row	*Functional / Assurance Requirements*	*Dependencies*	*Satisfied by*
1	FMT_SMR.1	FIA_UID.1	FIA_UID.2 (Table 5.1)
2	FMT_MOF.1	FMT_SMR.1	Row 1
3	FMT_MSA.3	FMT_MSA.1	Row 2 Also see 5.4.1 Justification of unsupported dependencies.
4	FMT_MSA.3	FMT_SMR.1	Row 1
5	FIA_UAU.1	FIA_UID.1	FIA_UID.2 (Table 5.1)
6	FIA_AFL.1	FIA_UAU.1	Row 5
7	FDP_IFC.1(1)	FDP_IFF.1(1)	Row 9
8	FDP_IFC.1(2)	FDP_IFF.1(2)	Row 11
9	FDP_IFF.1(1)	FDP_IFC.1(1)	Row 7
10	FDP_IFF.1(1)	FMT_MSA.3	Row 3
11	FDP_IFF.1(2)	FDP_IFC.1(2)	Row 8
12	FDP_IFF.1(2)	FMT_MSA.3	Row 3
13	FAU_GEN.1	FPT_STM.1	FPT_STM.1 (Table 5.1)
14	FAU_SAR.1	FAU_GEN.1	Row 13
15	FAU_SAR.3	FAU_SAR.1	Row 14
16	FAU_STG.1	FAU_GEN.1	Row 13
17	FAU_STG.4	FAU_STG.1	Row 16
18	ACM_AUT.1	ACM_CAP.3	EAL4
19	ACM_CAP.4	ACM_SCP.1, ALC_DVS.1	EAL4
20	ACM_SCP.2	ACM_CAP.3	EAL4
21	ADO_DEL.2	ACM_CAP.3	EAL4
22	ADO_IGS.1	AGD_ADM.1	EAL4
23	ADV_FSP.2	ADV_RCR.1	EAL4
24	ADV_HLD.2	ADV_FSP.1, ADV_RCR.1	EAL4
25	ADV_IMP.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1	EAL4
26	ADV_LLD.1	ADV_HLD.2, ADV_RCR.1	EAL4
27	ADV_SPM.1	ADV_FSP.1	EAL4
28	AGD_ADM.1	ADV_FSP.1	EAL4
29	AGD_USR.1	ADV_FSP.1	EAL4
30	ALC_TAT.1	ADV_IMP.1	EAL4

Row	*Functional / Assurance Requirements*	*Dependencies*	*Satisfied by*
31	ATE_COV.2	ADV_FSP.1, ATE_FUN.1	EAL4
32	ATE_DPT.1	ADV_HLD.1, ATE_FUN.1	EAL4
33	ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	EAL4
34	AVA_MSU.2	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1	EAL4
35	AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	EAL4
36	AVA_VLA.2	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1	EAL4

4.4.1 - Justification of Unsupported Dependencies

The CC Part 2 states that FMT_MSA.3 depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. It should be noted that the SFR FMT_MSA.1 requires that the TOE restrict the ability to manipulate the security Attributes to authorised roles in accordance with the SFP. The function FMT_MOF.1 meets this requirement by ensuring that only an administrator can use the functions defined to change the Security attributes in the TOE. The SFR, as implemented by the TOE, provides protection for all security attributes, from User profiles and Authentication attributes to Information Flow definitions explicitly allowing or denying types of flows and permitted addresses. These attributes cover the attributes defined by FDP_IFC.1 as required by FMT_MSA.1. Therefore, FMT_MOF.1 adequately satisfies the concerns of leaving FMT_MSA.1 out of this Security Target.

The SFR FCS_COP.1.1 relies on the SFRs FDP_ITC.1, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2. These SFRs are all related to key generation, importing or destruction. The S/Key5 implementation of MD5 does not use keys when generating the one-time passwords. Therefore, key management is irrelevant to this TOE and the dependencies of FCS_COP are not required to be satisfied.

4.5 - Security Requirements Rationale

4.5.1 -Specific strength of TOE Security Functions

FIA_UAU.1 -For the generation of one time passwords and checksums the following algorithms are required:

:

a) MD5 – to generate one time passwords (see 5.1.4 -DX_AU_2)

b) S/Key5 - to control the use of one time passwords (see 5.1.2 FIA_UAU1.2and 6.1.4 DX_AU_2)

c) MD5 - to generate and verify checksums (see 5.1.1 FMT_MOF.1.1(l), 6.1.3 AC_5 and 6.1.3 AC_6)

MD5 is licensed by RSA Data Security, Inc.

The only functional requirements contained in the TOE that a permutational or probabilistic are listed above. No claim is made to the Strength of Function of the above requirements as these algorithms are cryptographic in nature.

As there are no functions or requirements that have a strength of function, this Security Target does not make a Claim of the Strength of function.

4.5.2 -Functional Security Requirements Rationale

Tables 5-5 and 5-6 demonstrate that each TOE Security Functional Requirement is mapped to at least one TOE Security Objective. All TOE objectives and TOE security functional Requirements have been covered in these tables. The following discussion provides the rationale for the suitability of the SFR's to meet the Security Objectives.

FMT_SMR.1 This component associates human users with the role of authorised administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 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.SINUSE.

FIA_UID.2 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_UAU.1 This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information (aside from FTP and Telnet information) before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorised administrator. If the authorised administrator was not always required to authenticate, there would be no means by which to audit any of their actions. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

FIA_AFL.1 This component ensures that human users who are not authorised administrators can not endlessly attempt to authenticate. After **five failed attempts**, the user becomes unable from that point on to authenticte. This goes on until an authorised administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_UAU.4 This component was chosen to ensure that some one-time authentication mechanism is used in all attempts to authenticate at the TOE from an internal or external network This component traces back to and aids in meeting the following objective: O.SINUSE.

FCS_COP.1 This component generates the onetime password used for authentication in the TOE. This component traces back to and aids in meeting the following objective: O.SINUSE.

FDP_IFC.1 (1) This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (ie., 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 (2) This component identifies the entities involved in the AUTHENTICATED information flow control SFP (ie., 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 (1) This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED 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 (2) This component identifies the attributes of the users sending and receiving the information in the AUTHENTICAED 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.3 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, O.SECSTA and O.SECFUN.

FPT_RVM.1 This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO.

FAU_GEN.1 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 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 This component ensures that a variety of searches and sorts can be performed on the audit trail. The requirements of FAU_SAR3.1 are met as follows:-

- User Identity: Extract using the Unix tools Grep and Awk.
- Presumed subject address: Gauntlet reporting scripts provide this facility.
- Ranges of dates: Extract using the Unix tools Grep and Awk.
- Ranges of times: Extract using the Unix tools Grep and Awk.
- Ranges of addresses: Extract using the Unix tools Grep and Awk.

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

FAU_STG.1 This component is chosen to ensure that the audit trail is protected from tampering. Only the authorised administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FAU_STG.4 This component ensures that the authorised 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 authorised 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 and O.SECFUN.

FMT_MOF.1 This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management / administration / security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

FTA_TSE.1 This SFR is used to restrict the times when people can send data through the firewall. This provides added assurance that the traffic passing through is authorised. This SFR traces back to and aids in meeting the following objective: IDAUTH.

Table 5-5 Functional Components to TOE Security Functions and Security Objective Mapping

Functional Component	***Functional Requirement***	***Security Objectives***
FMT_SMR.1	Security Roles	O.SECFUN
FMT_MOF.1	Management of security functions behaviour	O.SECSTA O.SECFUN O.LIMEXT
FMT_MSA.3	Static attribute initialisation	O.MEDIAT O.SECSTA O.SECFUN
FIA_ATD.1	User attribute definition	O.IDAUTH O.SINUSE
FIA_UID.2	User identification before any action	O.IDAUTH O.ACCOUN
FIA_UAU.1	Timing of authentication	O.IDAUTH O.SINUSE
FIA_AFL.1	Authentication failure handling	O.SELPRO
FIA_UAU.4	Single use authentication mechanisms	O.SINUSE
FDP_IFC.1(1)	Subset information flow control	O.MEDIAT
FDP_IFC.1(2)	Subset information flow control	O.MEDIAT
FDP_IFF.1(1)	Simple security attributes	O.MEDIAT

FDP_IFF.1(2)	Simple security attributes	O.MEDIAT
FPT_RVM.1	Non-bypassability	O.SELPRO
FAU_GEN.1	Audit data generation	O.AUDREC O.ACCOUN
FAU_SAR.1	Audit review	O.AUDREC
FAU_SAR.3	Selectable audit review	O.AUDREC
FAU_STG.1	Protected audit trail storage	O.SELPRO O.SECFUN
FAU_STG.4	Prevention of audit data loss	O.SELPRO O.SECFUN
FCS_COP.1	Generation of one-time passwords	O.SINUSE
FTA_TSE.1	Time based access	O.IDAUTH

Table 5-6 Mapping of Objectives to Functional Components

Security Objective	***Security Functional Components***
O.IDAUTH	FIA_ATD.1, FIA_UID.2, FIA_UAU.1, FTA_TSE.1
O.SINUSE	FIA_ATD.1, FIA-UAU.1, FIA_UAU.4, FCS_COP.1
O.MEDIAT	FMT.MSA.3, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2)
O.SECSTA	FMT_MOF.1, FMT.MSA.3,
O.SELPRO	FIA_AFL.1, FPT_RVM.1, FAU_STG.1, FAU_STG.4
O.AUDREC	FAU_GEN.1, FAU_SAR.1, FAU_SAR.3
O.ACCOUN	FIA_UID.2, FAU_GEN.1
O.SECFUN	FMT_SMR.1, FMT_MOF.1, FMT_MSA.3, FAU_STG.1, FAU_STG.4,
O.LIMEXT	FMT_MOF.1,

4.6 - Mutually Supportive Security Requirements

The purpose of this rationale is to show that the IT security requirements (and the SFRs in particular) are complete and internally consistent by demonstrating that they are mutually supportive and provide an 'integrated and effective whole'.

Dependency helps in showing mutual support because if SFR-A is dependent on SFR-B then by definition, SFR-B is supportive of SFR-A.

This ST is targeting a standard EAL 4 assurance package and so the dependency and mutual support of the assurance requirements is self-evident as the EAL is taken from the CC.

For those SFRs not directly related by dependency, mutual support is partly demonstrated by the fact that all IT security requirements have been mapped to the security objectives, and that the security objectives are consistent. Additionally, mutual support can be provided by SFRs which address the following:

4.6.1 - Help prevent bypassing of other SFRs

FIA_UID.1, FIA_UAU.1 and FMT_SMR.1 support the function FMT_MOF.1, which allows the management of the TOE, by restricting the actions the administrator can take before being authenticated.

FMT_MOF.1 supports all other SFRs by restricting the ability to manage firewall policies and firewall access to authorised administrators, ensuring unauthorised users cannot tamper with these SFRs.

FMT_MSA.3 limits the users authorised to change the values that define traffic policy, protecting the SFRs dependent on those values from being tampered.

FCS_COP.1 and FIA_UAU.4 support FIA_UAU.1 by providing one time passwords for authentication.

4.6.2 - Help prevent tampering of other SFRs

FIA_UID.1 and FIA_UAU.1 support the function FMT_MOF.1 which restricts the user access to the management functions by restricting the actions the user can take before being authenticated, reducing the ability of users to tamper with SFRs.

FMT_MOF.1 supports all other SFRs by restricting the ability to manage Firewall policy to authorised administrators, ensuring unauthorised users cannot tamper with these SFRs.

FMT_MSA.3 ensures that only authorised administrators can change the values that define traffic policy, protecting the SFRs dependent on those values from being tampered with.

FAU_GEN.1, FAU_SAR.1 and FAU_GEN.3 combine to allow administrator the ability to view actions of users and thus prevent any changes to management data by restricting the appropriate users access to the TOE.

FAU_STG.1 protects the audit trail and as such, prevents tampering of the functions FAU_GEN.1, FAU_SAR.1 and FAU_GEN.3

4.6.3 - Help prevent de-activation of other SFRs

FMT_MOF.1 supports all other SFRs by restricting the ability to change all management functions to authorised administrators, ensuring other users cannot de-activate these SFRs.

FMT_MSA.3 ensures that only authorised administrators can change the values that define traffic policy, protecting the SFRs dependent on those values from being de-activated.

5 - TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

5.1 - IT Security Functions

This section presents the security functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that it must satisfy.

5.1.1 - Security Audit TSFs

AU_1 The administrator can configure security alerts which are displayed at the management terminal for the following accounting events:

a) receipt of source-routed IP packets

b) receipt of ICMP redirects

c) receipt of IP packets that have no packet screening rule defined

d) receipt of IP packets that have no proxy configured

e) receipt of malformed IP packets

AU_2 Gauntlet records accounting events in a log file on the Firewall as identified in AU_3.

AU_3 The following events can be generated and recorded in the log file on the Firewall:

a) all service requests

b) all service terminations

c) any use of the authentication mechanisms

d) the events defined in AU_1 above

e) start-up and shutdown of the auditing system

f) the following configuration or system errors

- memory allocation failure
- failure to spawn child process
- missing Gauntlet database or configuration file
- missing parameter or missing syntax in the Netperm-table's security rules

AU_4 The log file contains the following information for the events defined in AU_3:

a) type of event

b) date - time of event

c) source IP address/host name (where appropriate)

d) destination IP address/host name (where appropriate)

e) proxy used (where appropriate)

f) success or failure of event

Depending on the type of event, the following information may also be recorded:

a) service connect and disconnect times (plug (plug_gw), Telnet (tn_gw), http (http_gw), SMTP (smap/smapd), POP3, Oracle*SQL (sql-gw), Microsoft SQL (mssql-qw), Sybase (syb-gw), FTP (ftp-gw), SNMP.

b) number of bytes transferred (plug_gw, tn_gw, http_gw, SMTP (smap/smapd), sql-gw, mssql-qw, syb-gw, ftp-gw and SNMP (snmp-gw))

c) username (as used in authenticated services) (tn_gw,)

d) individual commands and requests (e.g. URLs) (HTTP).

AU_5 Gauntlet utilises grep and awk provided by Solaris 8 to extract audit information on a regular basis from the log files based on the filtering rules specified in AC_3(f).

AU_6 Gauntlet allows Administrator to maintain the audit log files, i.e manage size and archiving capabilities, utilizing the Solaris 8 functions ‘mv’ and ‘compress’.

AU_7 Gauntlet will protect the audit log files from both unauthorized deletion and modification.

AU_8 Gauntlet will:

- Allow Administrators the ability to specify which auditable events, as identified in AU_3, to audit;
- Ensure that every auditable event specified by Administrators is recorded in a log file; and
- Take explicit actions to limit the loss of audit records in cases where the log files become full.

5.1.2 -Identification and Authentication TSFs

IA_1 An administrator is identified to the Gauntlet Firewall GUI by supplying their unique username.

IA_2 Not Used.

IA_3 An administrator cannot login to the Firewall remotely.

IA_4 An administrator must identify himself or herself to Solaris 8 before performing any administration functions.

IA_5 An administrator can only perform administration functions or commands following successful login locally to Solaris 8 as the root user.

IA_6 Only administrators can create or delete other administrator GUI accounts, or user accounts.

5.1.3 - Access Control TSFs

AC_1 All service interactions between internal and external networks must pass through the packet screening facility. The packet screening facility will operate in accordance with DX_AC_1.

AC_2 Not Used.

AC_3 The Firewall provides the administrator with the ability to display, initialise and modify the following functions:

a) the rules for screening packets

b) the proxy rules

c) the rules governing the time of day end users (or groups of end users) are permitted to use an authenticated service (applicable to tn-gw)

d) the rules governing whether JAVA applets or ActiveX modules in HTML pages are permitted through the Firewall

e) the rules which associate the permitted authentication mechanisms with specific end users (or groups of end users)

f) the filtering rules for the log files as recorded in the [2] Chapter 15.

g) define the Gauntlet related events that generate security alerts

h) rules to generate and verify the integrity of a Firewall

i) *unused*

j) *unused*

k) *unused*

l) define the events relating to network layer security that will generate log records

AC_4 Not used.

AC_5 Gauntlet provides the Administrator with a function to generate checksums of the Firewall's current files system, which are recorded in the integrity database. Moreover, the function is not available to any user who is not an Administrator.

AC_6 Gauntlet provides the Administrator with a function to verify the Firewall's current file system checksums against the checksums in the integrity database. Moreover, the function is not available to any user who is not an Administrator.

AC_7 Gauntlet provides the Administrator with a command to specify how the Firewall's backup function, which utilize Solaris 8 function "tar", will backup user attribute values, audit files, and policy rules. Moreover, the command is not available to any user who is not an Administrator.

AC_8 Gauntlet provides the Administrator with a restore function, which utilizes Solaris 8 function "tar", to recover user attribute values, audit files and policy rules from the latest backup. Moreover, the functions are not available to any user who is not an Administrator.

AC_9 Gauntlet provides the Administrator with the commands to start-up and shutdown Gauntlet. Moreover, the commands are not available to any user who is not an Administrator.

5.1.4 - Data Exchange TSFs

The Data Exchange TSFs are further divided into Data Exchange Access Control and Authentication TSFs.

Data Exchange - Access Control TSFs (DX_AC)

DX_AC_1 The administrator can configure the packet screening rules to allow the packet screening facility to perform the following on packets:

a) deny : which means the packet is blocked so that no service interaction is allowed in either direction.

b) absorb : which means that the packet is processed by a proxy.

c) permit : which means that the packet is passed through without further processing.

DX_AC_2 The administrator can configure the packet screening and proxy rules to allow the packet screening facility and proxies to perform the following on packets:

a) Discard ICMP redirect packets, IP packets which are source routed and IP packets for which no packet screening rule is defined.

b) Discard IP packets which purport to originate from host systems on the internal network but are received on the external network interface.

c) Discard IP packets for which there is no proxy or for which the proxy does not permit the service request.

d) Pass IP packets for which a proxy is defined to that proxy for onward transmission.

DX_AC_3 The plug_gw, http_gw, tn_gw, sql-gw, mssql-qw, syb-gw, ftp-gw and snmp-gw proxies/applications check attempted service requests between internal and external networks on the basis of:

a) source host system or set of host systems which is/are permitted or denied to request the service;

and

b) destination host system or set of host systems which is/are permitted or denied to respond to the service.

DX_AC_4 An administrator can configure the proxy rules to control how the plug_gw, http_gw, tn_gw sql-gw, mssql-qw, syb-gw, ftp-gw and snmp-gw proxies mediate services, in particular:

a) for each proxy, permitted and denied sources and destinations;

and/or

b) for individual requesting (source) host systems or sets of host systems, the permitted proxies and destinations.

DX_AC_5 *Unused*.

DX_AC_6 An administrator can configure the plug proxy rules to direct or redirect services and additionally any of the following:

a) to send to a specified TCP port at the destination

b) to send from a specified, possibly privileged TCP port (i.e. port number < 1024) at the Firewall

c) to use the source host system's identity to replace the source IP address in the redirected packets, rather than the Firewall's identity.

DX_AC_7 The csmap (smap/smapd) application can accept valid SMTP mail messages at the Firewall, for onward message distribution by a service provider also at the Firewall. The TOE will reject malformed SMTP messages.

DX_AC_8 Where a host system is specified or identified to Gauntlet by a DNS host name, Gauntlet uses DNS to determine the name to IP address relationship. Failure to obtain a mapping results in the host being regarded as unknown.

DX_AC_9 An administrator can configure the proxy rules for Telnet & FTP proxies to prevent the use of authenticated services at particular times of day for defined end users or sets of end users.

DX_AC_10 An administrator can configure the proxy rules so that the HTTP proxy will remove any detected JAVA applets being transferred through it.

Data Exchange - Authentication TSFs (DX_AU)

DX_AU_1 For the Telnet & FTP services from hosts that require authentication, Gauntlet identifies and authenticates an end user before permitting an onward session through the Firewall.

DX_AU_2 The end user authentication can be performed by supplying an S/Key5 passed one-time password.

DX_AU_3 The administrator will configure Gauntlet to require that the user be authenticated using an S/Key5 passed one-time password.

DX_AU_4 The Administrator can specify for Telnet & FTP requests, whether a source host or set of host systems require end user authentication.

DX_AU_5 Authentication credentials are not disclosed to the internal or external networks.

DX_AU_6 The Administrator can specify the number, five or less, of times a user can unsuccessfully attempt to log in before the TSF shall prevent the offending user from successfully authentication until an authorized Administrator has to take some action to make authentication possible for the user.

5.2 - Security Mechanisms and Techniques

The following algorithms are required:

a) MD5 – to generate one time passwords (see 5.1.4 -DX_AU_2)

b) S/Key5 - to control the use of one time passwords (see 5.1.2 FIA_UAU1.2, and 6.1.4 DX_AU_2)

c) MD5 - to generate and verify checksums (see 5.1.1 FMT_MOF.1.1(l), 6.1.3 AC_5 and 6.1.3 AC_6)

MD5 is licensed by RSA Data Security, Inc.

5.3 - TOE Summary Specification Rationale

This section presents the rationale demonstrating that the security functions performed by the TOE are suitable to meet the SFR's and are a complete representation of these functions. Table 6-1 (above) shows that every security functional requirement is covered by at least one TOE security function. Table 6-2 demonstrates that every TOE security function supports at least one security functional requirement.

AU_1 This TSF provides the authorised administrator to configure and display security alerts. This TSF component traces back to and aids in meeting the following SFR: FAU_GEN.1.

AU_2 This TSF allows Gauntlet to record events in a log file on the Firewall. This TSF component traces back to and aids in meeting the following SFR: FAU_GEN.1.

AU_3 This TSF specifies the events that are recorded through AU_2. This TSF component traces back to and aids in meeting the following SFR: FAU_GEN.1.

AU_4 This TSF specifies the information recorded through AU_3. This TSF component traces back to and aids in meeting the following SFR's: FAU_GEN.1.

AU_5 This TSF provides the ability to extract audit information from the Gauntlet log files. This TSF component traces back to and aids in meeting the following SFR's: FAU_GEN.1, FAU_SAR.1 and FAU_SAR.3.

AU_6 This TSF provides the authorised administrator with the ability to maintain the audit log files. This TSF component traces back to and aids in meeting the following SFR's: FMT_MOF.1 , FAU_GEN.1, FAU_SAR.1 and FAU_SAR.3.

AU_7 This TSF protects audit files from unauthorized deletion and modification. This TSF component traces back to and aids in meeting the following SFR: FAU_STG.1.

AU_8 This TSF provides the authorised administrator the ability to ensure that specified auditable events are audited and in cases when the audit files get full, limit the number of records lost. This TSF component traces back to and aids in

meeting the following SFR's: FAU_STG.4.

IA_1 Authorized administrators are identified to the GUI by their unique username by this TSF. This TSF component traces back to and aids in meeting the following SFR's: FMT_SMR.1.1and FIA_ATD.1.

IA_2 Not Used.

IA_3 This TSF ensures that remote administration is not possible. This TSF component traces back to and aids in meeting the following SFR: FMT_MOF.1.1.

IA_4 This TSF ensures that any administrative function is only possible following identification to Solaris 8. This TSF component traces back to and aids in meeting the following SFR's: FIA_UID.2 and FMT_MOF.1.

IA_5 This TSF ensures that administrators can perform administrations functions only following successful logon locally to Solaris 8. This TSF component traces back to and aids in meeting the following SFR's: FIA_UID.2, FIA_UAU.1.2, FMT_MOF.1

IA_6 This TSF ensures that only authorised administrators can create or delete user and administrator GUI accounts. This TSF component traces back to and aids in meeting the following SFR: FMT_MOF.1.

AC_1 This TSF ensures that interaction between internal and external networks must pass through the packet screening facility. This TSF component traces back to and aids in meeting the following SFR's: FMT_MSA.3, FDP_IFC.1 and FPT_RVM.1.

AC_2 Not Used.

AC_3 The firewall authorised administrator is able to display, initialise and modify Gauntlet security rules. This TSF component traces back to and aids in meeting the following SFR: FMT_MSA.3.

AC_5 The firewall authorised administrator is able to generate checksums of the firewalls current file system which are recorded in the integrity database. This TSF component traces back to and aids in meeting the following SFR'S: FMT_MOF.1.

AC_6 The firewall authorised administrator is able to verify checksums of the firewalls current file system against those recorded in the integrity database. This TSF component traces back to and aids in meeting the following SFR: FMT_MOF.1.

AC_7 The firewall authorised administrator is able to specify how the automated backup function should backup user attribute values, information flow security policy rules and audit records. This TSF component traces back to and aids in meeting the following SFR: FMT_MOF.1.

AC_8 The firewall authorised administrator is able to recover user attribute values, information flow security policy rules and audit records from the latest backup. This TSF component traces back to and aids in meeting the following SFR: FMT_MOF.1.

AC_9	Gauntlet provides the Administrator with the commands to start-up and shutdown Gauntlet. Moreover, the commands are not available to any user who is not an Administrator. This TSF component traces back to and aids in meeting the following SFR: FMT_MOF.1
DX_AC_1	The firewall authorised administrator is able to configure packet screening rules. This TSF component traces back to and aids in meeting the following SFR's: FMT_MOF.1, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1) and FDP_IFF.1(2).
DX_AC_2	The firewall authorised administrator is able to configure packet screening and proxy application rules. This TSF component traces back to and aids in meeting the following SFR's: FMT_MOF.1, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1) and FDP_IFF.1(2).
DX_AC_3	Proxied services are able to permit or deny service requests between internal & external networks based on source and destination hosts. This TSF component traces back to and aids in meeting the following SFR's: FDP_IFF.1(1) and FDP_IFF.1(2).
DX_AC_4	Proxied services are able to permit or deny service requests between internal & external networks based on source / destination hosts and source / destination addresses. This TSF component traces back to and aids in meeting the following SFR's: FDP_IFC.1, FDP_IFF.1(1) and FDP_IFF.1(2).
DX_AC_5	Unused.
DX_AC_6	The firewall authorised administrator is able to configure the service redirection's of the plug proxy. This TSF component traces back to and aids in meeting the following SFR's: FDP_IFC.1 and FDP_IFF.1
DX_AC_7	The csmap (smap/smapd) application can accept valid SMTP mail messages at the Firewall, for onward message distribution. Gauntlet will drop any malformed mail messages received on either the protected or external interface. This TSF component traces back to and aids in meeting the following SFR's: FDP_IFC.1 and FDP_IFF.1.
DX_AC_8	For a DNS host name, Gauntlet uses DNS to determine the name to IP address relationship. Failure to obtain a mapping results in the host being regarded as unknown. This TSF component traces back to and aids in meeting the following SFR's: FDP_IFC.1 and FDP_IFF.1.
DX_AC_9	The firewall authorised administrator is able to configure the Telnet proxy to prevent the use of authenticated services at particular times of day for defined users. This TSF component traces back to and aids in meeting the following SFR's: FDP_IFC.1, FDP_IFF.1 and FTA_TSE.1.
DX_AC_10	An authorised administrator can configure the proxy rules so that HTTP proxy will remove any detected JAVA applets being transferred through it. This TSF component traces back to and aids in meeting the following SFR: FDP_IFC.1.
DX_AU_1	For the Telnet and FTP services, Gauntlet can authenticate an end user before permitting an onward session through the Firewall. This TSF component traces back to and aids in meeting the following SFR: FDP_IFC.1(2) and FIA_UAU.1
DX_AU_2	End user authentication can be performed using one time passwords. This TSF component traces back to and aids in meeting the following SFR's: FCS_COP.1, FIA_UID.2, FIA_UAU.4 and FDP_IFC.1.

DX_AU_3 The authorised administrator can configure which authentication mechanisms are to be used by each end user, including one time passwords. This TSF component traces back to and aids in meeting the following SFR's: FCS_COP.1, FIA_UID.2 and FIA_UAU.4.

DX_AU_4 The Administrator can specify for Telnet requests, whether a source host or set of host systems require end user authentication. This TSF component traces back to and aids in meeting the following SFR's: FDP_IFC.1(2) and FDP_IFF.1(2).

DX_AU_5 Authentication credentials are not disclosed to the internal or external networks. This TSF component traces back to and aids in meeting the following SFR: FMT_MOF.1.

DX_AU_6 The authorised administrator can configure the number of unsuccessful logon attempts. In addition, the TSF will prevent the user in question from further logon attempts until an administrator takes some explict action. This TSF component traces back to and aids in meeting the following SFR's: FMT_MOF.1 and FIA_AFL.1.

Table 6-1 Complete Mapping of TSFs to SFRs

TOE Security Functions	*Security Functional Requirements*
AU_1	FAU_GEN.1
AU_2	FAU_GEN.1
AU_3	FAU_GEN.1
AU_4	FAU_GEN.1
AU_5	FAU_GEN1, FAU_SAR.1, FAU_SAR.3
AU_6	FMT_MOF.1, FAU_GEN.1, FAU_SAR.1, FAU_SAR.3
AU_7	FAU_STG.1
AU_8	FAU_STG.4
IA_1	FMT_SMR.1.1, FIA_ATD.1
IA_3	FMT_MOF.1
IA_4	FIA_UID.2.1, FMT_MOF.1
IA_5	FIA_UID.2, FIA_UAU.1.2, FMT_MOF.1
IA_6	FMT_MOF.1
AC_1	FMT_MSA.3, FDP_IFC.1, FPT_RVM.1
AC_3	FMT_MSA.3.2
AC_5	FMT_MOF.1
AC_6	FMT_MOF.1
AC_7	FMT_MOF.1
AC_8	FMT_MOF.1
AC_9	FMT_MOF.1
DX_AC_1	FMT_MOF.1, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2)
DX_AC_2	FMT_MOF.1, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2)

TOE Security Functions	*Security Functional Requirements*
DX_AC_3	FDP_IFF.1(1), FDP_IFF.1(2)
DX_AC_4	FDP_IFC.1, FDP_IFF.1(1), FDP_IFF.1(2)
DX_AC_6	FDP_IFC.1, FDP_IFF.1
DX_AC_7	FDP_IFC.1, FDP_IFF.1
DX_AC_8	FDP_IFC.1, FDP_IFF.1
DX_AC_9	FDP_IFC.1, FDP_IFF.1, FTA_TSE.1
DX_AC_10	FDP_IFC.1
DX_AU_1	FDP_IFC.1(2), FIA_UAU.1
DX_AU_2	FIS_UID.2, FIA_UAU.4, FDP_IFC.1, FCS_COP.1
DX_AU_3	FIA_UID.2, FIA_UAU.4, FCS_COP.1
DX_AU_4	FDP_IFC.1(2), FDP_IFF.1(2)
DX_AU_5	FMT_MOF.1
DX_AU_6	FMT_MOF.1, FIA_AFL.1

5.4 - Assurance Measures

Gauntlet 6.0 claims to satisfy the assurance requirements for Evaluation Assurance Level EAL4. This section identifies the Configuration Management, Delivery and Operation, System Development Procedures, Guidance Documents Life Cycle Support, Tests and Vulnerability Assessment measures applied to Gauntlet 6.0 to satisfy the CC EAL4 assurance requirements summarised in Table 6.3. Assurance Measures Rationale - shows that this evidence is sufficient to meet all of the EAL4 Assurance Requirements.

5.4.1 - Mapping of Assurance Measures to Assurance Requirements

Table 6-3 describes the mapping between the assurance measures of the TOE and the SARs as required by the assurance level (EAL-4).

Table 6-2 Mapping of Assurance Measures to Assurance Requirements

Security Assurance Measures	Security Assurance Requirements						
	Configuration Management (ACM)	Delivery and Operation (ADO)	Development (ADV)	Guidance Documents (AGD)	Life Cycle Support (ALC)	Tests (ATE)	Vulnerability Assessment (AVA)
Configuration Management Plan	Y						
Administrators Guide		Y		Y			
Getting Started Guide		Y					

Security Assurance Measures	Security Assurance Requirements						
	Configuration Management (ACM)	Delivery and Operation (ADO)	Development (ADV)	Guidance Documents (AGD)	Life Cycle Support (ALC)	Tests (ATE)	Vulnerability Assessment (AVA)
Installation Cover Letter		Y					
Netperm Table Reference Guide		Y					
High Level Design Documentation			Y			Y	
Functional Specification Documentation			Y			Y	
Addendum				Y	Y		
Implementation Representation			Y				
Low Level Design Documentation			Y				
Representation Correspondence			Y				
Security Policy Model			Y				
Development Security Documentation					Y		
Life Cycle Definition Documentation					Y		
Implementation-dependent options of the development tools					Y		
Test Documentation						Y	
Analysis of	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Security Assurance Measures	Security Assurance Requirements						
	Configuration Management (ACM)	Delivery and Operation (ADO)	Development (ADV)	Guidance Documents (AGD)	Life Cycle Support (ALC)	Tests (ATE)	Vulnerability Assessment (AVA)
Strength of TOE security functions							
Analysis of User and Admin Guide Documentation							Y
Vulnerability Analysis Documentation							Y

5.4.2 -Rationale of Assurance Measures to Assurance Requirements

This section presents the rationale demonstrating that the assurance measures indicated in table 6-3 are suitable to meet the Security Assurance Requirements of the Common Criteria. Table 6-3 (above) shows that every security assurance requirement is covered by at least one security assurance measure.

ACM — The Gauntlet Configuration Management Plan demonstrates the use of configuration management (CM) tools in the production and generation of the TOE. All areas required by the CC ACM_AUT.1, ACM_CAP.4 and ACM_SCP.2 are adequately met through the CM Plan.

ADO — The Gauntlet Administrators Guide assists in providing details necessary to maintain the integrity of the TOE and traces back to and aids in meeting the following ADO_DEL.2 and ADO_IGS.1. The Getting Started Guide, Users Guide, Installation Cover Letter and the Netperm Table Reference Guide provides additional coverage of the CC requirements and traces back to and aids in meeting the following ADO_DEL.2 and ADO_IGS.1, in particular the secure setup and configuration of the TOE.

ADV — The Functional Specification describes the user visible interfaces and behaviour of the TSF, the Representation Correspondence provides the correspondence between the various TSF representations both these trace back to and aids in meeting of ADV_FSP.2.

The High Level Design describes the TSF in terms of major structural units and relates these to the functions that they provide. This is a refinement of the Functional Specification. In combination with the Representation Correspondence these documents trace back to and aid in meeting of ADV_HLD.2 and ADV_LLD.1

The Implementation Representation, as a selection of source code, represents a subset of the TSF and traces back to the meeting of ADV_IMP.1

The Low Level Design documentation provides a description of the internal workings of the TSF giving assurance that the subsystems have been correctly and effectively refined and traces back to the meeting of ADV_LLD.1.

The TOE Security Policy Model provides assurance that the security functions in the Functional Specification enforce the policies of the TSP this traces back to the meeting of ADV_SPM.1.

ADG

The Gauntlet Administrators guidance describes the administrative functions and interfaces available to the administrator. It also gives sufficient information to allow the administration of the firewall in a secure manner. In association with the Functional Specification these documents trace back to and aid in meeting of ADG_ADM.1.

The Gauntlet User Guide describes the security functions provided by the TSF and provides instructions and guidelines including warnings, for its secure use and traces back to the meeting of ADG_USR.1

ALC

The Development Security describes all the physical, procedural, personnel and other security measures that protect the confidentiality and integrity of the TOE design and implementation in its development environment. This traces back to the meeting of ALC_DVS.1 The Life Cycle Definition documentation demonstrates the life cycle model used in the development and maintenance of theTOE and this traces back to the meeting of ALC_LCD.1

Through the Tools and Techniques documentation the development tools used in the production of the TOE are described. This includes any implementation dependent options being used. This traces back to the meeting of ALC_TAT.1

ATE

The Test Coverage documentation in combination with the Functional Specification will give an analysis and evidence of the correspondence between the tests and the TSF. This traces back to the meeting of ATE_COV.2

The testing documentation will include an analysis demonstrating that the tests identified in the Test Coverage documentation are sufficient to demonstrate that the TSF operates in accordance with the High Level Design. This traces back to the meeting of ATE_DPT.1.

The Functional Testing documentation contains the test plans, test procedure descriptions, expected and actual test results. This traces back to the meeting of ATE_FUN.1.

AVA

The Analysis of the guidance documentation demonstrates that guidance is provided for secure operation in all modes of operation of the TOE. This traces back to the meeting of AVA_MSU.2

The TOE does not contain any Functions or Requirements that require a strength of function Claim. No functions in the ST are based on Permutaional or Probablistic Mechanisms. Therefore, this Security Target does not make any Strength of functions claims and the Requirements for Strength of Function are Not Applicable to this TOE. As such, AVA_SOF.1 is not relevant to this evaluation.

The Vulnerability Analysis shows for all identified vulnerabilities, that the vulnerabilities cannot be exploited in the intended environment for the TOE. The analysis will justify that the TOE is resistant to obvious penetration attacks with the identified vulnerabilities and that the analysis has been systematic. This traces back to the meeting of AVA_VLA.2.