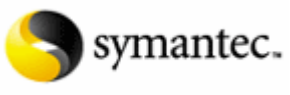

Security Target

for

Symantec Gateway Security (SGS) 5000 Series

Version 3.0

(Firewall Engine Only)

Reference: SGS3\ST

March 2006

Issue: 1.0a

Symantec Corporation
275 Second Avenue
Waltham, MA 02451
USA

Copyright notice

DOCUMENT AUTHORISATION

Document Title	Security Target for Symantec Gateway Security (SGS) 5000 Series Version 3.0 (Firewall Engine Only)

Issue	**Date**	**Description**
0.1	Oct 2005	Draft issued for TSM
0.2	Oct 2005	Correct details of 5640
0.3	Nov 2005	Address EOR1
0.4	Nov 2005	Correct conformance claim
0.5	Feb 2006	Address EOR 4
0.6	Feb 2006	Address EOR 6
1.0a	Mar 2006	Draft final issue

Contents

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004 (aligned with ISO 15408).

GLOSSARY AND TERMS

Authentication data	Information used to verify the claimed identity of a user.
Authorised User	Users, who may, in accordance with the TSP, perform an operation.
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.
CC	Common Criteria
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
FSB	Front Side Bus
FTP	File Transfer Protocol
Human User	Any person who interacts with the TOE
IP	Internet Protocol
IT	Information Technology
LCD	Liquid Crystal Display
Linux Operating System	The operating system used by the appliance.
MAC	Media Access Control
NAT	Network Address Translation
PP	Protection Profile
RFC	Request for Comments
SEF	Symantec Enterprise Firewall
SGS	Symantec Gateway Security
SFP	Security Function Policy

SOF	Strength of Function
SGMI	Security Gateway Management Interface
SGMI operating system	The operating system on the workstation used by the SGMI to access the TOE.
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSAP	Transport Service Application Protocol
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.
VPN	Virtual Private Network

1 Introduction to the Security Target

1.1 Security Target Identification

1 Title: Security Target for Symantec Gateway Security (SGS) 5000 Series Version 3.0 (Firewall Engine Only), issue 1.0a.

2 Assurance Level: EAL4, augmented with ALC_FLR.1.

1.2 Security Target Overview

3 The Symantec Gateway Security is a unique security solution that combines technologies from the Symantec Enterprise Firewall, Symantec Enterprise VPN, intrusion detection, content filtering and anti-virus scanning into one appliance. The Symantec Gateway Security maximizes network security without compromising performance.

4 The Symantec Gateway Security (SGS) 5000 Series Version 3.0 (Firewall Engine Only) is a Internet Protocol application and packet-filtering firewall. The application proxy provides connection services to the global Internet on behalf of hosts within a secured network; thus ensuring there is no direct connection between Internet and private networked hosts. The packet filtering allows the acceptance/refusal of data based on the attributes of the data packets. This assists the prevention of unauthorised services being accessed by Internet hosts.

5 The chapters of this Security Target are structured in accordance with the families in the [CC] ASE class, with the various rationales required by the ASE families collated in section 8.

1.3 CC Conformance Claim

6 This TOE has been developed using the functional components as defined in the Common Criteria version 2.2 [CC] Part 2 plus an additional functional component to interface to an external authentication server, with the assurance level of EAL4, augmented with ALC_FLR.1 as identified in Part 3 of [CC].

7 In CC terms the Security Target is Part 2 extended and Part 3 conformant.

2 TOE Description

2.1 Overview of the Symantec Gateway Security5000 Series Version 3.0 (Firewall Engine)

8 This section presents an overview of the Symantec Gateway Security (SGS) 5000 Series Version 3.0 and the firewall engine to assist potential users in determining whether it meets their needs.

9 The Symantec Gateway Security is an integrated gateway security appliance that incorporates five core security functions into a single solution. The solution combines firewall, anti-virus, intrusion detection, content filtering and VPN capabilities in a single appliance.

10 The Target of Evaluation (TOE) for this evaluation is the Symantec Gateway Security Version 3.0 (Firewall Engine Only) software running on a 5000 series appliance, the Security Gateway Management Interface (SGMI) and the Appliance Liquid Crystal Display (LCD) screen.

11 The Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) is an application level firewall (also referred to as the Symantec Gateway Security 5000 Series Version 3.0 appliance when including environment hardware and Symantec Gateway Security v3.0 when only considering software). The TOE uses a set of application-specific security proxies to validate each attempt to pass data in or out of the network it secures. This is substantially different from stateful packet filter firewalls that do not filter data at the application level.

12 The packets enter the TCP/IP stack of the Symantec Gateway Security 5000 Series Version 3.0 appliance. Various scanning techniques are then applied and completed via the TCP/IP protocol stack. After all tests are completed, if there are no problems, the packets are allowed to flow out of the Symantec Gateway Security 5000 Series Version 3.0 appliance to the next network segment.

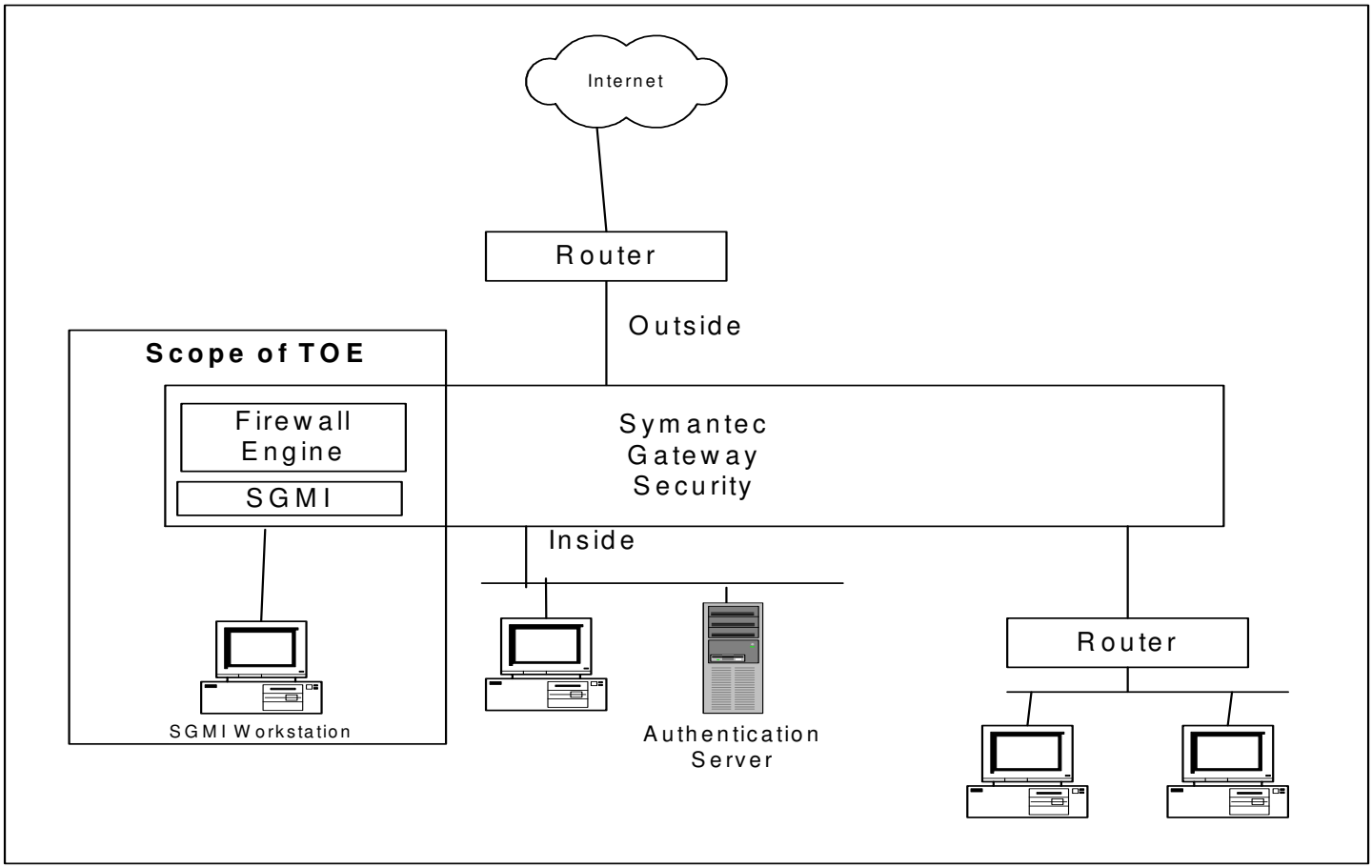

Diagram 2-1: Packet Flow through the Symantec Gateway Security 5000 Series Version 3.0

13 The Target of Evaluation (TOE) consists of three physical components, the firewall engine itself, and the Security Gateway Management Interface (SGMI) and the Appliance LCD screen that are used to manage the firewall.

14 The SGMI is a Java-based, standalone user interface that includes policy, location, system-monitoring, settings and reports. The SGMI is accessed by directing a web browser to the SGS and logging on with an Administrator's user name and password. There is no separate software to install.

15 The Appliance LCD screen displays the Symantec Gateway Security version number. LCD displays the following options:

- System startup self-tests;
- Performance monitoring;
- System Menu.

16 The LCD can be locked from the SGMI.

17 The TOE's security proxies perform the following functions:

- Examine the contents of packets
- Allow or deny connection based on IP address, user, time, type of service, and the interface the connection came in on.
- Control direction and type of operations for applications.
- Log all session data.

18 In addition the firewall engine provides the following functions:

- Syn flooding attack protection;
- Denial of Service protection;
- Port scanning detection.

19 The TOE can be configured not to disclose IP addresses and for users to be unable to identify listening services.

20 For the evaluation six network interface cards will be used with the TOE. It is possible to identify each network interface as either 'internal' or 'external'. If an interface is identified as external then the network to which it attaches is classed as being outside of the firewall. If an interface is identified as an internal interface then the network to which it attaches is classed as being inside (or behind) the firewall.

21 The workstation used to run SGMI will be connected directly to the appliance, using a physically secure connection such as a crossover cable. SGMI network traffic must not pass through shared network devices such as routers.

22 All traffic between each network attached to the TOE must flow through the firewall engine of the Symantec Gateway Security 5000 Series Version 3.0 to maintain security. The protocols that are within the scope of the evaluation are:

HTTP[i]	UDP	FTP	Ping	DNS
TELNET	SMTP	NTP	RTSP	IP
NNTP	POP3	RealAudio	TCP	

23 The application proxies through the TOE that are within the scope of the evaluation are:

HTTP	FTP	NNTP	RealAudio	DNS	NTP
TELNET	SMTP	POP3			

2.2 Scope and Boundaries of the Evaluated Configuration

24 The TOE configuration consists of:

- The firewall itself;
- The Security Gateway Management Interface (SGMI), which is used for local administration by the administrator;
- The Appliance Liquid Crystal Display (LCD), which is used for administration by the administrator;

2.2.1 Physical Scope

25 The physical scope of the TOE is identified in Table 2-1.

Software	**Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) with Security Gateway Management Interface** **Including SGS3.0-Bundle B-February 9th 2006.**

Table 2-1: TOE Component Identification

2.2.2 Hardware and Software for the Appliance

26 The required IT environment for the TOE is a 5000 Series appliance (e.g. 5420, 5440, 5460, 5620, 5640, 5660). Table 2-2 identifies the explicitly tested underlying hardware of the TOE, which forms part of the IT environment.

[i] HTTP proxy supports WebDAV (Web Distributed Authoring and Versioning)

Hardware	Symantec Gateway Security 5000 Series
Model	5640
Software	N/A
Operating System	Red Hat Linux 7.2 with a Linux 2.4.26 kernel.
Ethernet Network Interfaces	8 x Intel Pro10/100/1000 Base-T Ethernet network interfaces
User Interface	2 line x 16 character LCD
Processor	3.0 Ghz 800 P4
Disk	160 GB EIDE
Memory	2 GB

Table 2-2: Tested platform of the TOE

2.2.3 Hardware and Software Requirements for the SGMI

27 The SGMI is the administration interface accessible via a workstation required for local administration of the TOE. The SGMI is part of the software on the appliance, and is accessed by directing a workstation browser to the appliance. Table 2-3 identifies the explicitly tested IT environment for the SGMI.

Software	Internet Explorer 6.0 SP1 Java Plug-in Version 1.5 No TOE specific software has to be loaded onto the workstation in order for the workstation to run SGMI.
Operating System	Windows XP Service Pack 2

Table 2-3: IT Environment for the SGMI

28 If the Java Plug-in is not already installed in the browser, it can also be downloaded from the appliance. The SGMI Java WebStart application is automatically downloaded directly from the appliance when an administrator connects their browser to the appliance for the first time. No TOE specific software has to be loaded onto the workstation in order for the workstation to run SGMI, which runs in a Java runtime environment.

29 The hardware that is required for the SGMI will be located with the SGS and have a direct link. No other applications will be loaded onto the machine.

2.2.4 Hardware and Software for the Authentication Server

30 An authentication server is required for single-use authentication. A commercially available authentication server that is compatible with the Symantec Gateway Security Version 3.0 should be used.

2.2.5 Outside of the Scope

31 Software and hardware features outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- Virtual Private Networking (VPN) functionality;
- Symantec Enterprise VPN Client;
- Content filtering;
- High availability/load balancing;
- User Authentication by one-time password[ii];
- Setup Wizard;
- Anti-spam;
- H.323 Connections;
- Remote Administration;
- Forward Filtering;
- Secure Shell (SSH);
- Console Port Access;
- Tomcat Web server;
- Intrusion Detection and Prevention;
- Anti-virus;
- Live update support;
- Event Manager;
- Policy Configuration Manager.

[ii] One time password authentication for Telnet/Ftp connections is provided by a SecureID or RADIUS server as part of the environment of the TOE.

3 Security Environment

3.1 Introduction

32 This section provides the statement of the TOE security environment, which identifies and explains all:

1. known and presumed threats countered by either the TOE or by the security environment;

2. organisational security policies the TOE must comply with;

3. assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

33 Within the evaluation references are made to two operating systems, the appliance operating system and the operating system used by the SGMI. In order to distinguish between the two operating systems, the appliance operating system is referred to as the "Linux operating system", while the operating system on the workstation used by the SGMI is referred to as the "SGMI operating system".

3.2 Threats

34 This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

3.2.1 Threats countered by the TOE

35 The IT assets requiring protection are the services provided by, and data accessible via, hosts on the internal network (or networks if there are multiple network interfaces on the TOE configured as being behind the firewall).

36 The general threats to be countered are:

- attackers outside of the protection of the TOE who may gain unauthorised access to resources within the internal network;
- users on the internal network who may inappropriately expose data or resources to the external network.

37 If the TOE is configured to provide separation between different internal networks then the following general threats will also need to be countered:

- a user on one of the internal networks who may gain unauthorised access to resources on another of the internal networks;
- a user on one of the internal networks who may expose data or resources to users on other internal networks.

38 The threats that must be countered by the TOE are listed below.

T.NOAUTH	An unauthorised person may attempt to bypass the security of the TOE so as to access and use security function 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 this 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 on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g. spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorised person may send impermissible information through the TOE that results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorised person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An 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 attacker actions.
T.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

39 The following table identifies the threats that are partially met by the TOE.

Threats Partially met by the TOE	Reasons
T.NOAUTH	Part of the security of TOE is performed by the SGMI operating system, and the authentication server. This threat is partially met by the SGMI operating system and the authentication server.
T.SELPRO	The Linux operating system protects certain TOE sensitive data, for example the audit data. This threat is partially met by the Linux Operating System.
T.AUDFUL	The Linux operating system provides part of the auditing for TOE. This threat is partially met by the Linux Operating System.
T.AUDACC	The Linux operating system provides part of the auditing for TOE. This threat is partially met by the Linux Operating System.
T.REPEAT	This threat is partially met by the SGMI operating system and the authentication server, as authentication is performed by the SGMI operating system and the authentication server
T.REPLAY	This threat is partially met by the SGMI operating system and the authentication server, as authentication is performed by the SGMI operating system and the authentication server.
T.LOWEXP	As part of the security of TOE is performed by the Linux Operating System, the SGMI operating system and the authentication server this threat is partially met by the Linux Operating System, the SGMI operating system and the authentication server.

Table 3-1 Threats partially met by the TOE and IT Environment

3.2.2 Threats countered by the Operating Environment

40 The threats that must be countered by technical and/or non-technical measures in the IT environment, or must be accepted as potential security risks are listed below.

TE.USAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorised or unauthorised persons.

41 Table 3-1 identifies the threats that are partially met by the operating environment.

3.3 Organizational Security Policies

42 There are no organizational security policies or rules with which the TOE must comply.

3.4 Assumptions

43 The following assumptions are assumed to exist.

A.PHYSEC	The TOE, SGMI operating system and authentication server are physically protected to prevent unauthorised users. Only authorised administrators have physical access to the TOE, SGMI operating system and the authentication server.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	There are no general-purpose computing (e.g. the ability to execute arbitrary code or application) and storage repository capabilities on the TOE, SGMI operating system or authentication server.
A.PUBLIC	The TOE, SGMI operating system and authentication server do not host public data.
A.NOEVIL	Authorised administrators for the TOE, SGMI operating system and authentication server 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 (e.g. a console port) if the

	connection is part of the TOE.
A.NOREMO	Human users who are not authorised administrators can not access the TOE, the SGMI operating system or the authentication server remotely from the internal or external networks.
A.REMOS	The SGMI operating system and the authentication server are delivered to the user's site, installed and administered in a secure manner.
A.COMMS	The communication links between the TOE, the SGMI operating system and the authentication server are physically protected.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

44 The principal IT security objective of the TOE is to reduce the vulnerabilities of an internal network exposed to an external network (or another internal network should there be multiple internal networks) by limiting the hosts and services available. Additionally, the TOE has the objective of providing the ability to monitor established connections and attempted connections between networks.

45 The IT security objectives are listed below.

O.IDAUTH	The TOE must uniquely authenticate all users, before granting a user access to certain specified services (FTP / Telnet), to a connected network.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by 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.
O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.

46 The following table identifies the IT Security objectives listed that are partially met by the IT environment.

Partially met by IT Environment	**Reasons**
O.IDAUTH	Part of the security of the TOE is provided by the authentication server using a Single-use authentication mechanism.
O.SINUSE	Part of the security of the TOE is provided by the SGMI Operating System and the authentication server using a Single-use authentication mechanism.
O.SECSTA	Part of the security of the TOE is provided by the Linux Operating System, the SGMI Operating System and the authentication server using a Single-use authentication mechanism.
O.SELPRO	Part of the security of the TOE is provided by the Linux Operating System and the SGMI Operating System.
O.AUDREC	Part of the security of the TOE is provided by the Linux Operating System.
O.ACCOUN	Part of the security of the TOE is provided by the Linux Operating System.
O.SECFUN	Part of the security of the TOE is provided by the Linux Operating System, the SGMI Operating System and the authentication server.
O.LIMEXT	Part of the security of the TOE is provided by the Linux Operating System, the SGMI Operating System and the authentication server
O.EAL	Part of the security of the TOE is provided by the Linux Operating System, the SGMI Operating System and the authentication server.

Table 4-1 IT Security Objective partially met by IT Environment and TOE

4.2 Environment Security Objectives

4.2.1 IT Security Objectives

47 The following IT security objectives are met by the environment.

OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.GENPUR	There are no general-purpose computing capabilities (e.g. the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE, the SGMI operating system and the authentication server.
OE.PUBLIC	The TOE, the SGMI operating system and the authentication server do not host public data.
OE.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
OE.NOREMO	Human users who are not authorised administrators can not access the TOE, the SGMI operating system or the authentication server remotely from the internal or external networks.

48 Table 4-1 identifies the IT security objectives that are partially met by the IT environment.

4.2.2 Non-IT Security Objectives

49 The non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

OE.PHYSEC	The TOE, the SGMI operating system and the authentication server must be physically protected so only authorised administrators have access. (The TOE must only be administered locally).
OE.COMMS	The communication links between the TOE, the SGMI operating system and the authentication server must be physically protected.
OE.NOEVIL	Authorised administrators of the TOE, the SGMI

	operating system and the authentication server must be non-hostile and follow all administrator guidance; however, they may be capable of error.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g. a console port) if the connection is part of the TOE.
OE.GUIDAN	The TOE must be delivered to the user's site, installed, administered, and operated in a manner that maintains security
OE.ADMTRA	Authorised administrators must be trained as to establishment and maintenance of security policies and practices.
OE.REMOS	The SGMI operating system and the authentication server must be delivered to the user's site, installed and administered in a secure manner.

5 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

50 The TOE security functional requirements consist of components from Part 2 of the CC and one explicitly stated requirement (FIA_UAU_SERV.1). They are listed in the following table, along with an indication of the requirements that are either fully or partially met by the TOE.

Functional Components		Partially / Fully met by the TOE
FIA_UAU_SERV.1	Single-use authentication server	**Fully**
FDP_IFC.1	Subset Information Flow Control (1)	**Fully**
FDP_IFC.1	Subset Information Flow Control (2)	**Fully**
FDP_IFF.1	Simple Security Attributes (1)	**Fully**
FDP_IFF.1	Simple Security Attributes (2)	**Fully**
FMT_MSA.1	Management of security attributes (1)	**Fully**
FMT_MSA.1	Management of security attributes (2)	**Fully**
FMT_MSA.1	Management of security attributes (3)	**Fully**
FMT_MSA.1	Management of security attributes (4)	**Fully**
FMT_MSA.3	Static Attribute Initialisation	**Fully**
FMT_SMF.1	Specification of Management Functions (1)	**Fully**
FPT_RVM.1	Non-Bypassability of the TSP	**Fully**
FPT_SEP.1	TSF domain separation	**Partially**
FAU_GEN.1	Audit Data Generation	**Partially**

Functional Components		Partially / Fully met by the TOE
FAU_SAR.1	Audit review	**Fully**
FAU_SAR.3	Selectable audit review	**Fully**
FAU_STG.4	Prevention of audit data loss	**Fully**
FMT_MOF.1	Management of Security Functions Behaviour (1)	**Fully**
FMT_MOF.1	Management of Security Functions Behaviour (2)	**Fully**

Table 5-1: Functional Requirements

Identification and Authentication

51 This section addresses the requirements for functions to establish and verify a claimed user identity. This includes identification of any actions that the TOE may complete on the user's behalf prior to identification or authentication.

52 Only an authorised administrator is able to interact directly with the SGS 5000 series Version 3.0 (Firewall Engine Only) through the SGMI / LCD. The authorised administrator is the only user who can log onto the Firewall Engine via the SGMI / LCD and access TSF data. The SGS 5000 series Version 3.0 (Firewall Engine Only) provides a basic form of access control mechanisms for identification and authentication.

53 Unauthenticated users use services provided by the TOE but do not visibly interact with the TOE. In order to control service requests from unauthenticated users, basic identification of the request through source address of request identification is performed.

54 **FIA_UAU_SERV.1 Single-use authentication server**[iii]

FIA_UAU_SERV.1.1 The TSF shall invoke an authentication server to authenticate any user's claimed identity according to the [following single authentication mechanism rule:
a. single-use authentication mechanism shall be used for human users sending or receiving information through

[iii] FIA_UAU_SERV.1 is an explicitly stated requirement.

the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user].

User Data Protection

55 This section specifies requirements for the TOE security functions and TOE security function policies relating to protecting user data.

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

57 **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].

58 **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 via the mechanisms invoked by FIA_UAU_SERV.1;
b) information: FTP and Telnet traffic sent through the TOE from one subject to another;
c) operation: initiate service and pass information].

59 **FDP_IFF.1 Simple security attributes (1)**[iv]

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;
- Port

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;
- Time;
- Address Transformation;
- Service redirection;
- Viability of application data;
- URL blocking].

[iv] *The complete set of functional elements of a component must be selected for inclusion in a ST. However, since the following functional elements from the FDP_IFF.1 (1) component do not add anything significant to the ST, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1(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].

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 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; and

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

60 **FDP_IFF.1 Simple security attributes (2)**[v]

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;
- Port

[v] *The complete set of functional elements of a component must be selected for inclusion in a ST. However, since the following functional elements from the FDP_IFF.1 (2) component do not add anything significant to the ST, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1 (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].

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service (i.e., FTP and Telnet);
- security-relevant service command;
- Time;
- Address Transformation;
- Service redirection;
- Viability of application data;
- Extended authentication methods;
- URL blocking].

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 the mechanisms invoked by FIA_UAU_SERV.1;
- 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 the mechanisms invoked by FIA_UAU_SERV.1;
- 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; and

f) The TOE shall reject Telnet or FTP command requests that do not conform to generally accepted published protocol definitions (e.g. RFCs). This must be accompanied through protocol filtering proxies designed for that purpose.]

Security Management

61 This section defines requirements for the management of security attributes that are used to enforce the TSF.

62 **FMT_MOF.1 Management of security functions behavior (1)**

FMT_MOF.1.1 The TSF shall restrict the ability to *enable, disable,* the functions:

a) [operation of the TOE;
b) single use authentication functions described in FIA_UAU_SERV.1] to [an authorised administrator]

.

63 **FMT_MOF.1 Management of security functions behavior (2)**

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

a) [audit trail management ;
b) backup and restore for TSF data, information flow rules, and audit trail data; and
c) communication of authorised external IT entities with the TOE] to [an authorised administrator].

64 **FMT_MSA.1 Management of Security Attributes (1)**

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

65 **FMT_MSA.1 Management of Security Attributes (2)**

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

66 **FMT_MSA.1 Management of Security Attributes (3)**

FMT_MSA.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF1.1(1)] to [the authorised administrator].

67 **FMT_MSA.1 Management of Security Attributes (4)**

FMT_MSA.1.1 The TSF shall enforce the [AUTHENTICATED SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF1.1(2)] to [the authorised administrator].

68 **FMT_MSA.3 Static attribute initialization**

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

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.

69 **FMT_SMF.1 Specification of Management Functions (1)**

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [those for which FMT_MSA.1 (1),(2),(3),&(4) and FMT_MOF.1 (1) & (2) restrict use to the authorised administrator].

Protection of the TOE Security Functions

70 This section specifies functional requirements that relate to the integrity and management of the mechanisms providing the TSF and TSF data.

71 **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.

72 **FPT_SEP.1 TSF domain separation**

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

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

Security Audit

73 This section involves recognising, recording and storing information related to security relevant activities.

74 **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 auditable events for the *not specified* level of audit; and

c) [the events in Table 5.2].

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

a) Date and time of the event, type of event, subject identity, 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 three of Table 5.2].

Functional Component	Auditable Event	Additional Audit Record Contents
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorised administrator performing the operation
FMT_SMF.1	Use of the management functions.	The identity of the authorised administrator performing the operation
FIA_UAU_SERV.1	Any use of the authentication mechanism.	The user identities provided to the TOE

Table 5-2: Auditable Event

75 **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.

76 **FAU_SAR.3 Selectable audit review**

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

a) [user identity;
b) presumed subject address;
c) ranges of dates;
d) ranges of times;
e) ranges of addresses].

77 **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.

5.2 Security requirements for the IT Environment

78 This section details the IT security requirements that are met by the IT environment of the TOE. Table 5-3 lists the IT security requirements to be provided by the IT environment:

Functional Components		Partially / Fully met by the IT environment
FIA_UAU.2	User authentication before any action	**Fully**
FIA_UAU.4	Single-use authentication mechanisms	**Fully**
FIA_UID.2	User identification before any action	**Fully**
FPT_SEP.1	TSF domain separation	**Partially**
FPT_STM.1	Reliable Time Stamps	**Fully**
FAU_GEN.1	Audit Data Generation	**Partially**
FAU_STG.1	Protected audit trail storage	**Fully**
FMT_MOF.1	Management of security functions behavior (3)	**Fully**
FMT_SMF.1	Specification of Management Functions (2)	**Fully**

Table 5-3: IT Security Requirements of the Environment

79 **FIA_UAU.2 User authentication before any action**[vi]

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[vi] FIA_UAU.2 and FIA_UID.2 are fully met by the SGMI operating system.

80 **FIA_UAU.4 Single-use authentication mechanisms**[vii]

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user].

81 **FIA_UID.2 User identification before any action**[viii]

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.

82 **FPT_SEP.1 TSF domain separation**[ix]

FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC

83 **FPT_STM.1 Reliable time stamps**[x]

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

[vii] FIA_UAU.4 is fully met by the authentication server using a Single-use authentication mechanism.
[viii] FIA_UAU.2 and FIA_UID.2 are fully met by the SGMI operating system.
[ix] FPT_SEP.1 is partially met by the Linux operating system.
[x] FPT_STM.1 is fully met by the Linux operating system.

84 **FAU_GEN.1 Audit data generation**[xi][xii]

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

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

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

c) [the events in Table 5.4].

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

a) Date and time of the event, type of event, subject identity, 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 three of Table 5.4].

Functional Component	Auditable Event	Additional Audit Record Contents
FPT_STM.1	Changes to the time.	The identity of the authorised administrator performing the operation.

Table 5-4: Auditable Event

85 **FAU_STG.1 Protected audit trail storage**[xiii]

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* unauthorised modifications to the audit records in the audit trail.

[xi] FAU_GEN.1 is partially met by the Linux operating system.

[xii] The management of the audit trail is performed by the following TOE SFRs: FMT_MOF.1(2), FMT_SMF.1(1), FAU_SAR.1, FAU_SAR.3 and FAU_STG.4.

[xiii] FAU_STG.1 is fully met by the Linux operating system.

86 **FMT_MOF.1 Management of security functions behavior (3)**[xiv]

FMT_MOF.1.1 The TSF shall restrict the ability to *enable, disable* the functions:

a) [single use authentication functions described in FIA_UAU.4 on the authentication server] to [an authorised administrator].

87 **FMT_SMF.1 Specification of Management Functions (2)**[xv]

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [those for which FMT_MOF.1 (3) restrict use to the authorised administrator].

5.3 TOE Security Assurance Requirements

88 The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL4 level of assurance augmented with ALC_FLR.1. The assurance components are summarized in the following table.

Assurance Class	**Assurance Components**	
Configuration management	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_DEL.2	Detection of modification

[xiv] FMT_MOF.1(3) is fully met by the authentication server only allowing modification by authorized administrators.

[xv] FMT_SMF.1(2) is fully met by the authentication server using a Single-use authentication mechanism.

Assurance Class	Assurance Components	
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic Flaw Remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ATE_COV.2	Analysis of coverage

Assurance Class	Assurance Components	
Tests	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

Table 5-5: Assurance Requirements: EAL4 augmented with ALC_FLR.1

89 Further information on these assurance components can be found in [CC] Part 3.

5.4 Strength of Function Claim

90 A Strength of Function (SOF) claim of SOF-Medium is made for the TOE. No TOE Security functions contain a probabilistic or permutational mechanism.

91 For a justification of the Strength of Function claim see Section 8.3.7.

6 TOE Summary Specification

6.1 TOE Security Functions

92 This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in Section 5.1.

6.1.1 Identification and Authentication Function [IA]

93 Upon receipt of a request to send or receive Telnet / FTP through the TOE, a request for authentication must be issued to an external authentication server. The response from the external authentication server must be received prior to any further processing of the request. [IA1]

6.1.2 Management and Security Function [MT]

94 The authorised administrator can delete, modify, and add to a rule in the unauthenticated SFP. [MT1]

95 The authorised administrator can delete, modify, and add to a rule in the authenticated SFP. [MT2]

96 The authorised administrator can delete and create information flow rules in the unauthenticated SFP, as described by SFR FDP_IFF.1 (1). [MT3]

97 The authorised administrator can delete and create information flow rules in the authenticated SFP, as described by SFR FDP_IFF.1 (2). [MT4]

98 The TSF shall provide restrictive default values for the information flow security attributes for Unauthenticated and authenticated SFPs. [MT5]

99 The authorised administrator has the ability to enable and disable the following functions: [MT6]

a) Operation of the TOE. The operation refers to the ability to control all information flows;
b) Single use authentication's functions.

100 The authorised administrator has the ability to enable, disable, determine and modify the behavior of the following functions: [MT7]

a) Audit management;
b) Backup and restore for TSF data, information flow rules, and audit trail data; and
c) Communication of authorised external IT entities with the TOE.

101 The authorised administrator shall be able to specify initial values to override the default values for security attributes when an object or information is created. [MT8]

6.1.3 Audit Function [AU]

102 The accounting mechanisms cannot be disabled. The start-up and shutdown of audit functions is synonymous with the start-up and shutdown of the TOE. Start-up and shut-down of the TOE specific components can be configured to be recorded in the audit trail. [AU1]

103 It is possible to generate audit records for the following auditable events: [AU2]

- Start-up and shutdown of the audit functions;
- All level of challenge response (single use authentication);
- User identities for single use authentication and audit trail management;
- Every successful inbound and outbound connection;
- Every unsuccessful inbound and outbound connection;
- Creating, deleting, and modifying of rules and associated attributes;
- Creating, deleting, and emptying of the audit trail.

104 For each event the Audit Function will record the following: [AU3]

- Date and time of the event;
- User identity (for single use authentication and audit trail management);
- System name;
- Component name;
- Process id;
- Type of event or service;
- Success or failure of the event;
- Message number;
- Message description which includes:
  - Source and destination IP address (for connections only);
  - Prototype Port number.

105 The authorised administrator has read access only to all audit trail data through the controlled interface SGMI logfile window. [AU4]

106 The authorised administrator, via the SGMI, is able to perform searches of audit data based on: [AU5]

- Date and time ranges;
- Event Type
- System name;
- Component name;
- Process identification number;
- Message number;
- Pattern matching via regular expression implementation. The user identification, source address and a range of addresses can be searched using

this facility as required by the SFR FAU_SAR.3.

107 Archiving is a manual process that is performed on the log files. The files are retained as long as there is space available. The authorised administrator is informed when the space limit is nearly reached. Once the audit trail becomes full, the TSF drops all connections through the TOE. [AU6]

6.1.4 Protection of TOE security Functions [PT]

108 The TOE provides self-protection from external modification or interference of the TSF code or data structures by untrusted subjects via the vulture daemon. Untrusted subjects cannot bypass checks, which always must be invoked. [PT1]

109 The functions that enforce the TOE Security Policy (TSP) are always invoked and completed, before any function within the TSF Scope of Control (those interactions within the TOE that are subject to the rules of the TSP) is allowed to proceed. [PT2]

110 The TSF protects itself, by denying all processes unless a process is specifically stated by the TSF. [PT3]

6.1.5 User Data Protection Function [DP]

111 The Time range template function of the TOE provides the facility of allowing an administrator to specify the time that a specific user may have access. This function can only be accessed from the Rules icon within the Security Gateway Management Interface (SGMI). [DP1]

112 The TOE provides a flow control mechanism in the form of security policy rules for all connections through the TOE for either inbound traffic (external to internal) or outbound traffic (internal to external). [DP2]

113 The TSF permits or denies authenticated connections depending on the security policy rules created by the administrator. [DP3]

114 The TSF evaluates packets on a “best fit” method, to ensure that the most constructive and specific security policy rule for each connection attempt is applied. [DP4]

115 The security policy rules are non-order dependent. [DP5]

116 All Connections are denied unless a specific rule has been set-up to allow information to flow. [DP6]

117 The Service used can be one of the following protocols: [DP7]

HTTP	UDP	FTP	Ping	DNS
TELNET	SMTP	NTP	RTSP	IP

NNTP POP3 RealAudio TCP

118 The application proxies through the TOE that are within the scope of the evaluation are: [DP8]

HTTP RealAudio NNTP NTP DNS POP3
TELNET SMTP FTP

119 There are two main types of information flow that the TOE enforces: [DP9]

a) Unauthenticated – An external IT entity on an internal or external network sending information through the TOE to other external IT entities.

b) Authenticated – users on an internal or external network who must be authenticated at the TOE before using any protocol services.

Unauthenticated

120 The TSF shall enforce unauthenticated information flow based on the following attributes: [DP10]

a) Subject security attributes:
   - Presumed address,
   - Port.

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;
   - Time;
   - Address Transformation;
   - Service redirection;
   - Viability of application data;
   - URL blocking.

121 Unauthenticated information flow shall be permitted: [DP11]

- For unauthenticated external IT entities that send and receive information through the TOE to one another;
- For traffic sent through the TOE from one subject to another;
- To Pass information.

122 Rules in the Security policy are defined by the TOE authorised Administrator, and allow the parameters stated in paragraph 119 to be set for unauthenticated traffic flow. [DP12]

123 Traffic flows from the configured internal network to another connected network shall only be permitted if all the information security attribute values created by the authorised administrator are permitted. [DP13]

124 Traffic flows from the configured internal network to another connected network shall only be permitted if the presumed address of the source subject translates to an internal network address. [DP14]

125 Traffic flows from the configured internal network to another connected network shall only be permitted if the presumed address of the destination subject translates to an address on another connected network. [DP15]

126 Traffic flows from the external network to another connected network shall only be permitted if all the information security attribute values created by the administrator are permitted. [DP16]

127 Traffic flows from the external network to another connected network shall only be permitted if the presumed address of the source subject translates to an external network address. [DP17]

128 Traffic flows from the external network to another connected network shall only be permitted if the presumed address of the destination subject translates to an address on another connected network. [DP18]

129 Access or services requests shall be denied from an external TOE interface if the presumed address of the source for the traffic flow is an external IT entity on an internal network. [DP19]

130 Access or services requests shall be denied from an internal TOE interface if the presumed address of the source for the traffic flow is an external IT entity on an external network. [DP20]

131 Access or services requests shall be denied from an internal or external TOE interface with the presumed address of the source for the traffic flow is an external IT entity on a broadcast network. [DP21]

132 Access or services requests shall be denied from an internal or external TOE interface with the presumed address of the source for the traffic flow is an external IT entity on a loopback network. [DP22]

133 Traffic flows in which the subject specifies the route the information flow shall flow to its destination shall be denied. [DP23]

134 Protocol filtering proxies shall deny access or request services to protocols that do not conform to the associated published protocol specification. [DP24]

Authenticated

135 The TSF shall enforce authenticated information flow based on the following attributes: [DP25]

a) Subject security attributes:
- Presumed address;
- Port.

b) Information security attributes:
- User identity;
- Presumed address of source subject;
- Presumed address of destination subject;
- Transport layer protocol;
- TOE interface on which traffic arrives and departs;
- Service (i.e. FTP and Telnet);
- Security-relevant service command;
- Time;
- Address Transformation;
- Service redirection;
- Viability of application data;
- Extended authentication methods;
- URL blocking.

136 Authenticated information flow shall be permitted for human users and external IT entities that send or receive FTP and Telnet information through the Firewall, only after the human user initiating the information flow has been successfully authenticated using an authentication server. [DP26]

137 Rules in the Security policy are defined by the TOE authorised Administrator, and allow the parameters stated in paragraph 134 to be set for each authenticated traffic flow. [DP27]

138 Traffic flows from the configured internal network to the another connected network shall only be permitted if the human user initiating the traffic flow authenticates using authentication server for FTP and Telnet. [DP28]

139 Traffic flows from an internal network to another connected network shall only be permitted if all the information security attribute values created by the authorised administrator are permitted. [DP29]

140 Traffic flows from a controlled subject and another controlled subject via a controlled operation shall only be permitted if the presumed address of the source subject in the traffic flow, translates to an address on the internal network. [DP30]

141 Traffic flows from an internal network to another connected network shall only be permitted if the presumed address of the destination subject translates to an address on the other connected network. [DP31]

142 Traffic flows from an external network to the another connected network shall only be permitted if the human user initiating the traffic flow authenticates using an authentication server for FTP and Telnet. [DP32]

143 Traffic flows from an external network to another connected network shall only be permitted if all the information security attribute values created by the administrator are permitted. [DP33]

144 Traffic flows from the external network to another connected network shall only be permitted if the source address of the packet translate to an address on the external network. [DP34]

145 Traffic flows from the external network to another connected network shall only be permitted if the destination address of the packet translate to an address on the other connected network. [DP35]

146 Access or services requests shall be denied from an external TOE interface if the presumed address of the source for the traffic flow is an external IT entity on an internal network. [DP36]

147 Access or services requests shall be denied from an internal TOE interface if the presumed address of the source for the traffic flow is an external IT entity on an external network. [DP37]

148 Access or services requests shall be denied from an internal or external TOE interface if the presumed address of the source for the traffic flow is an external IT entity on a broadcast network. [DP38]

149 Access or services requests shall be denied from an internal or external TOE interface if the presumed address of the source for the traffic flow is an external IT entity on a loopback network. [DP39]

150 Traffic flows in which the subject specifies the route the information flow shall flow to its destination shall be denied. [DP40]

151 Protocol filtering proxies shall deny access or services to the following protocols that do not conform to the associated published protocol specification: FTP and Telnet. [DP41]

6.2 Identification and Strength of Function Claim for IT security Functions

152 This Security Target claims that the general strength of the security functions provided by the TOE is SOF-Medium.

153 No specific strength of function metric is defined.

6.3 Assurance Measures

154 Assurance measures will be produced to comply with the Common Criteria Assurance Requirements for EAL4 augmented with ALC_FLR.1. Table 8-6 maps the deliverables to the assurance requirements.

7 Protection Profiles Claims

No claims against a protection profile are made.

8 Rationale

8.1 Introduction

155 This section demonstrates that the TOE provides an effective set of IT security countermeasures within the security environment and that the TOE summary specification addresses the requirements.

8.2 Security Objectives for the TOE Rationale

156 Table 8-1 demonstrates how the IT security objectives and environment objectives of the TOE counter the IT threats and environment threats identified in Section 3.2.1 and 3.2.2.

Threats/ Assumptions / Objectives	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIATE	T.OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL	T.LOWEXP	TE.USAGE	A.PHYSEC	A.LOWEXP	A.GENPUR	A.PUBLIC	A.NOEVIL	A.SINGEN	A.DIRECT	A.NOREMO	A.REMOS	A.COMMS
O.IDAUTH	✓																				
O.SINUSE		✓	✓																		
O.MEDIAT				✓	✓	✓															
O.SECSTA	✓							✓													
O.SELPRO	✓							✓	✓												
O.AUDREC							✓														
O.ACCOUN							✓														
O.SECFUN	✓		✓						✓												
O.LIMEXT	✓																				
O.EAL										✓											
OE.PHYSEC												✓									
OE.LOWEXP													✓								
OE.GENPUR														✓							
OE.PUBLIC															✓						
OE.NOEVIL																✓					
OE.SINGEN																	✓				
OE.DIRECT																		✓			
OE.NOREMO																			✓		
OE.GUIDAN							✓				✓										
OE.ADMTRA							✓				✓										
OE.REMOS																				✓	
OE.COMMS																					✓

Table 8-1 Mapping of Objectives to Threats and Assumptions

157 The following are justifications for Objectives that are met by the TOE.

158 **O.MEDIAT**

159 This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF 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 and that no residual information is transmitted.

160 The following are justifications for Objectives that are partially met by the TOE and partially by the IT Environment

161 **O.IDAUTH**

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

163 The authentication server authenticates users using a single-use authentication mechanism.

164 **O.SINUSE**

165 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.

166 The authentication server authenticates users using a single-use authentication mechanism.

167 **O.SECSTA**

168 This security objective is necessary to counter the threats: T.NOAUTH and T.SELPRO because it requires that no information is compromised by the TOE upon start-up or recovery.

169 The Linux operating system performs part of the resistance to penetration attacks.

170 **O.SELPRO**

171 This security objective is necessary to counter the threats: T.SELPRO, T.AUDFUL and T.NOAUTH because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

172 The Linux operating system provides part of the protection for the TOE.

173 **O.AUDREC**

174 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.

175 The audit trail is stored on the Linux operating system.

176 **O.ACCOUN**

177 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.

178 The Linux operating system performs part of the audit functions.

179 **O.SECFUN**

180 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.

181 The configuration of the SGMI operating system, Linux operating system and the authentication server support this objective.

182 **O.LIMEXT**

183 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.

184 The configuration of the SGMI operating system, Linux operating system and the authentication server support this objective.

185 **O.EAL**

186 This security objective is necessary to counter the threat: T.LOWEXP because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing minimal attack potential.

187 The Linux operating system, the SGMI operating system and the authentication server perform part of the resistance to penetration attacks.

188 The following are justifications for Objectives that are met by the IT Environment.

189 **OE.PHYSEC**

190 This environmental security objective is necessary to support the assumption: A.PHYSEC because it requires that the TOE, the SGMI operating system and the authentication server are physically protected.

191 **OE.LOWEXP**

192 This environmental security objective is necessary to support the assumption: A.LOWEXP because it requires that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

193 **OE.GENPUR**

194 This environmental security objective is necessary to support the assumption: A.GENPUR because it requires that the TOE, the SGMI operating system and the authentication server do not provide general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) or storage repository capabilities.

195 **OE.PUBLIC**

196 This environmental security objective is necessary to support the assumption: A.PUBLIC because it requires that the TOE, the SGMI operating system and the authentication server do not host public data.

197 **OE.NOEVIL**

198 This environmental security objective is necessary to support the assumption: A.NOEVIL because it requires that Authorised administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

199 **OE.SINGEN**

200 This environmental security objective is necessary to support the assumption: A.SINGEN because it requires that information cannot flow among the internal and external networks unless it passes through the TOE.

201 **OE.DIRECT**

202 This environmental security objective is necessary to support the assumption: A.DIRECT because it requires that human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

203 **OE.NOREMO**

204 This environmental security objective is necessary to support the assumption: A.NOREMO because it requires that human users who are not authorised administrators can not access the TOE, the SGMI operating system or the authentication server remotely from the internal or external networks.

205 **OE.GUIDAN**

206 This environmental security objective is necessary to counter the threat: TE.USAGE and T.AUDACC because it requires that those responsible for the TOE ensure that it is delivered to the user's site, installed, administered, and operated in a secure manner.

207 **OE.ADMTRA**

208 This environmental security objective is necessary to counter the threat: TE.USAGE and T.AUDACC because it ensures that authorised administrators receive the proper training.

209 **OE.REMOS**

210 This environmental security objective is necessary to support the assumption: A.REMOS because it requires that the SGMI operating system and the authentication server are delivered to the user's site, installed and administered in a secure manner.

211 **OE.COMMS**

212 This environmental security objective is necessary to support the assumption: A.COMMS because it requires that the communication links between the TOE, SGMI operating system and the authentication server are physically protected.

213 The following are justifications for IT security threats that are partially met by the TOE and partially by the IT Environment.

214 **T.NOAUTH**

215 The TOE ensures all FTP and Telnet attempts from an internal or external network are authenticated using an authentication server. Only authenticated connections are allowed between the networks.

216 The SGMI operating system identifies and authenticates users before allowing access to the TOE.

217 **T.SELPRO**

218 Access to the internal data of the TOE is only possible through the machine that the TOE is installed on. The TOE relies on the physical environment to ensure that only the authorised user has physical access to the TOE.

219 The Linux operating system relies on the physical environment to ensure that only the authorised user has physical access to the Linux operating system.

220 **T.AUDFUL**

221 The TOE provides the administrator with Read Only access to the TOE audit data through the SGMI. The TOE informs the administrator when the space is reaching its limit. Once the audit trail is full, all connections to the TOE are dropped.

222 The Linux operating system informs the administrator when the audit storage space is reaching its limit.

223 The authorised user of the machine must ensure that the data is archived and that the storage space does not become exhausted.

224 **T.AUDACC**

225 The TOE through the SGMI provides the administrator with the means to configure the security-related functions and the information flows to be audited. The TOE will audit all attempts by hosts, connected through one network interface, to access hosts or services, connected on another interface, that are not explicitly allowed by the information flow policy. The administrator must ensure that the audit facilities are used and managed correctly including inspecting the logs on a regular basis.

226 The Linux operating system through the administrative tools allows the administrator to configure the security-related functions to be recorded in the audit trail. The administrator must ensure that the audit facilities are used and managed correctly including inspecting the logs on a regular basis.

227 **T.LOWEXP**

228 The TOE minimizes the threat of malicious attacks by setting the initial settings to deny. The authorised administrator is required to enable the required settings.

229 The Linux operating system, SGMI operating system and the authentication server provide part of the security to ensure that the threat of malicious attack is low, in particular no other applications should be loaded onto the Linux operating system, SGMI operating system and the authentication server.

230 **T.REPEAT**

231 The TOE invokes the authentication server for single use authentication. All attempts are audited.

232 The authentication server ensures that users using FTP or Telnet are authenticated by means of an authentication server that generates a one-time password.

233 The SGMI operating system authenticates authorised administrators prior to allowing an administrator access to TOE.

234 **T.REPLAY**

235 The TOE invokes the authentication server for single use authentication. All attempts are audited

236 The authentication server ensures that users using FTP or Telnet are authenticated by means of an authentication server that generates a one-time password.

237 The SGMI operating system authenticates authorised administrators prior to allowing an administrator access to TOE.

8.3 Security Requirements Rationale

8.3.1 Security Requirements are appropriate

238 Table 8-2 identifies which SFRs satisfy the Objectives as defined in Section 4.1.1.

Objective	Security Functional Requirement(s)
O.IDAUTH	FIA_UAU_SERV.1
O.SINUSE	FIA_UAU_SERV.1
O.MEDIAT	FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.3, FMT_SMF.1(1)
O.SECSTA	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.3, FPT_RVM.1, FPT_SEP.1, FAU_STG.4, FMT_MOF.1(1),

Objective	Security Functional Requirement(s)
	FMT_MOF.1(2), FMT_SMF.1(1)
O.SELPRO	FPT_RVM.1, FPT_SEP.1, FAU_STG.4
O.AUDREC	FAU_GEN.1, FAU_SAR.1, FAU_SAR.3
O.ACCOUN	FAU_GEN.1
O.SECFUN	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FAU_STG.4, FMT_MOF.1(1), FMT_MOF.1(2), FMT_SMF.1(1)
O.LIMEXT	FMT_MOF.1(1), FMT_MOF.1(2), FMT_SMF.1(1)
O.EAL	FIA_UAU_SERV.1, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.3, FPT_RVM.1, FPT_SEP.1, FAU_STG.4, FMT_MOF.1(1), FMT_MOF.1(2), FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FMT_SMF.1(1)

Table 8-2 Mapping of Objectives to SFRs

239 **O.EAL**

240 O.EAL is concerned with the TOE being resistant to obvious vulnerabilities. By default O.EAL maps to all the Security Function Requirements.

241 **FIA_UAU_SERV.1 Single-use authentication server**

242 This component ensures that an authentication server is appropriately used for Single-use authentication 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 objectives: O.SINUSE and O.IDAUTH.

243 **FDP_IFC.1 Subset information flow control (1)**

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

245 **FDP_IFC.1 Subset information flow control (2)**

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

247 **FDP_IFF.1 Simple security attributes (1)**

248 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.

249 **FDP_IFF.1 Simple security attributes (2)**

250 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.

251 **FMT_MSA.1 Management of security attributes (1)**

252 This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

253 **FMT_MSA.1 Management of security attributes (2)**

254 This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those specified security attributes that are listed in section FDP_IFF1.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

255 **FMT_MSA.1 Management of security attributes (3)**

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

257 **FMT_MSA.1 Management of security attributes (4)**

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

259 **FMT_MSA.3 Static attribute initialization**

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

261 **FMT_SMF.1 Specification of Management Functions (1)**

262 This component ensures that the TSF provide specific security functions. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, O.SECFUN and O.LIMEXT.

263 **FPT_RVM.1 Non-bypassability of the TSP**

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

265 **FPT_SEP.1 TSF domain separation**

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

267 **FAU_GEN.1 Audit data generation**

268 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.

269 **FAU_SAR.1 Audit review**

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

271 **FAU_SAR.3 Selectable audit review**

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

273 **FAU_STG.4 Prevention of audit data loss**

274 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, O.SECFUN and O.SECSTA.

275 **FMT_MOF.1 Management of security functions behavior (1)**

276 This component ensures that the TSF restricts the ability of the TOE start up and shut down operation and the single-use authentication function to the authorised administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

277 **FMT_MOF.1 Management of security functions behavior (2)**

278 This component ensures that the TSF restricts the ability to modify the behavior of functions such as audit trail management, back and restore for TSF data, and communication of authorised external IT entities with the TOE to an authorised administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

8.3.2 Environmental Security Requirements are appropriate

279 Table 8-3 identifies which environmental SFRs satisfy the Objectives as defined in Sections 4.1.1 and 4.2.1

Objective	Security Functional Requirement(s)
O.IDAUTH	FIA_UAU.4
O.SINUSE	FIA_UAU.4, FIA_UAU.2, FIA_UID.2
O.SECSTA	FPT_SEP.1, FAU_STG.1, FMT_MOF.1(3), FMT_SMF.1(2), FIA_UAU.2, FIA_UID.2
O.SELPRO	FPT_SEP.1, FAU_STG.1, FIA_UAU.2, FIA_UID.2
O.AUDREC	FAU_GEN.1, FPT_STM.1
O.ACCOUN	FAU_GEN.1, FPT_STM.1
O.SECFUN	FAU_STG.1, FMT_MOF.1(3), FMT_SMF.1(2),

Objective	Security Functional Requirement(s)
	FIA_UAU.2, FIA_UID.2
O.LIMEXT	FMT_MOF.1(3), FMT_SMF.1(2), FIA_UAU.2, FIA_UID.2
O.EAL	FPT_SEP.1, FAU_STG.1, FMT_MOF.1(3), FMT_SMF.1(2), FAU_GEN.1, FPT_STM.1, FIA_UAU.2, FIA_UID.2, FIA_UAU.4
OE.LOWEXP	FPT_SEP.1
OE.GENPUR	FPT_SEP.1
OE.PUBLIC	FPT_SEP.1
OE.SINGEN	FPT_SEP.1
OE.NOREMO	FPT_SEP.1

Table 8-3 Mapping of Objectives to environmental SFRs

280 **O.EAL**

281 O.EAL is concerned with the TOE being resistant to obvious vulnerabilities. By default O.EAL maps to all the Security Function Requirements.

282 **FIA_UAU.4 Single-use authentication mechanisms**

283 This component ensures that a Single-use authentication mechanism is used appropriately 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 objectives: O.SINUSE and O.IDAUTH.

284 **FPT_SEP.1 TSF domain separation**

285 This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorised users. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECSTA, OE.LOWEXP, OE.GENPUR, OE.PUBLIC, OE.SINGEN AND OE.NOREMO.

286 **FAU_GEN.1 Audit data generation**

287 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.

288 **FPT_STM.1 Reliable time stamps**

289 This component ensures that time stamping is enabled. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

290 **FAU_STG.1 Protected audit trail storage**

291 This component ensures that the audit records are protected from unauthorised deletion and modification to the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.

292 **FMT_MOF.1 Management of security functions behavior (3)**

293 This component ensures that the TSF restricts the ability of the single-use authentication function on the authentication server to the authorised administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

294 **FMT_SMF.1 Specification of Management Functions (2)**

295 This component ensures that that the TSF provides specific security functions. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN and O.LIMEXT.

296 **FIA_UAU.2 User authentication before any action**

297 This component ensures that before anything occurs on behalf of a user, the user is authenticated via the SGMI operating system to the TOE. This component traces back to and aids in meeting the following objectives: O.SINUSE, O.SECSTA, O.SELPRO, O.SECFUN and O.LIMEXT

298 **FIA_UID.2 User identification before any action**

299 This component ensures that before anything occurs on behalf of a user, the user's identity is identified via the SGMI operating system to the TOE. This component traces back to and aids in meeting the following objectives: O.SINUSE, O.SECSTA, O.SELPRO, O.SECFUN and O.LIMEXT.

8.3.3 Security Requirement dependencies are satisfied

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 See note below regarding FMT_SMR.1. FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 See note below regarding FMT_SMR.1. FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 See note below regarding FMT_SMR.1. FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 See note below regarding FMT_SMR.1. FMT_SMF.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 See note below regarding FMT_SMR.1.
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	See note below regarding FMT_SMR.1. FMT_SMF.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	See note below regarding FMT_SMR.1. FMT_SMF.1
FMT_SMF.1	NONE	NONE
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1[xvi]	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1, FMT_MSA.3
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1, FMT_MSA.3
FPT_RVM.1	None	None
FPT_SEP.1	None	None
FPT_STM.1[xvii]	None	None
FIA_UAU_SERV.1 [xviii]	FIA_UAU.4	FIA_UAU.4[xix]
FIA_UAU.4[xx]	None	None

Table 8-4 Mapping of TOE SFR Dependencies

300 The security functional requirements are hierarchical and may satisfy the dependency.

301 FMT_MSA.1, FMT_MSA.3, and FMT_MOF.1 have a dependency on FMT_SMR.1. For security management of the TOE, as stated in objective OE.PHYSEC and OE.NOREMO only an authorised administrator will have

[xvi] FAU_STG.1 is a security requirement for the IT environment.
[xvii] FPT_STM.1 is a security requirement for the IT environment.
[xviii] FIA_UAU_SERV.1 is an explicitly stated requirement.
[xix] FIA_UAU.4 is a security requirement for the IT environment.
[xx] FIA_UAU.4 is a security requirement for the IT environment.

physical access to the TOE, SGMI workstation and the authentication server. Human users, including authorised administrators can not access the TOE, SGMI workstation or the authentication server remotely from the internal or external networks. The dependency on FMT_SMR.1 is therefore regarded as satisfied.

8.3.4 IT security functions satisfy SFRs

302 Mapping of Section 6 IT functions to SFRs (Section 5.1 and 5.2).

IT Function	Security Functional Requirement(s)
Identification and Authentication	
IA1	FIA_UAU_SERV.1
Management and Security[xxi]	
MT1	FMT_MSA.1(1), FMT_SMF.1(1)
MT2	FMT_MSA.1(2) , FMT_SMF.1(1)
MT3	FMT_MSA.1(3) , FMT_SMF.1(1)
MT4	FMT_MSA.1(4) , FMT_SMF.1(1)
MT5	FMT_MSA.3
MT6	FMT_MOF.1(1) , FMT_SMF.1(1)
MT7	FMT_MOF.1 (2), FMT_SMF.1(1)
MT8	FMT_MSA.3
Audit	
AU1	FAU_GEN.1
AU2	FAU_GEN.1
AU3	FAU_GEN.1
AU4	FAU_SAR.1

[xxi] FAU_GEN.1 Table 5-2 is applicable to FMT_SMF.1, and FMT_MOF.1 (1), (2)

AU5	FAU_SAR.3, FAU_SAR.1
AU6	FAU_STG.4
Protection of TOE Security Functions	
PT1	FPT_SEP.1
PT2	FPT_RVM.1
PT3	FPT_RVM.1
User Data Protection[xxii]6	
DP1	FDP_IFF.1 (2)
DP2	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
DP3	FDP_IFC.1 (2), FDP_IFF.1 (1)
DP4	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
DP5	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
DP6	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
DP7	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
DP8	FDP_IFC.1 (1), FDP_IFC.1 (2)
DP9	FDP_IFF.1 (1) , FDP_IFF.1 (2)
DP10	FDP_IFF.1 (1)
DP11	FDP_IFC.1 (1)

[xxii] FAU_GEN.1 Table 5-2 is applicable to FDP_IFF.1

DP12	FDP_IFF.1 (1)
DP13	FDP_IFF.1 (1)
DP14	FDP_IFF.1 (1)
DP15	FDP_IFF.1 (1)
DP16	FDP_IFF.1 (1)
DP17	FDP_IFF.1 (1)
DP18	FDP_IFF.1 (1)
DP19	FDP_IFF.1 (1)
DP20	FDP_IFF.1 (1)
DP21	FDP_IFF.1 (1)
DP22	FDP_IFF.1 (1)
DP23	FDP_IFF.1 (1)
DP24	FDP_IFF.1 (1)
DP25	FDP_IFF.1 (2)
DP26	FDP_IFC.1 (2)
DP27	FDP_IFF.1 (2)
DP28	FDP_IFF.1 (2)
DP29	FDP_IFF.1 (2)
DP30	FDP_IFF.1 (2)
DP31	FDP_IFF.1 (2)
DP32	FDP_IFF.1 (2)
DP33	FDP_IFF.1 (2)
DP34	FDP_IFF.1 (2)
DP35	FDP_IFF.1 (2)

DP36	FDP_IFF.1 (2)
DP37	FDP_IFF.1 (2)
DP38	FDP_IFF.1 (2)
DP39	FDP_IFF.1 (2)
DP40	FDP_IFF.1 (2)
DP41	FDP_IFF.1 (2)

Table 8-5 Mapping of IT Functions to SFRs

303 To perform searches and sorts on the audit database the administrator will be able to use the Security Gateway Management Interface (SGMI) Logfile icon. This is to meet FAU_SAR.1. In the event of audit storage failure, exhaustion and / or attack the TOE will stop all connections through the TOE and so the amount of data to be lost is none. So that requirement FAU_STG.4 is met.

304 Once the audit trail becomes full, the TSF drops all connections through the TOE. Therefore the maximum amount of audit data to be lost is zero.

305 Table 8-5 demonstrates that the IT security functions map to TOE Security Functional Requirements provided by the TSS. Each of the IT Security Functions maps to at least one TOE security function, and all the TOE Security Function Requirements are covered. Therefore by implementing all the IT Security Functions, the TOE Functional Requirement is met.

8.3.5 IT security functions mutually supportive

306 The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 8.3.3), as each of the IT functions can be mapped to one or more SFRs, as demonstrated in Table 8-5.

8.3.6 Justification of Explicit Requirements

307 The explicit requirement FIA_UAU_SERV.1 has been specified to address the requirement for the TOE to invoke an authentication server to authenticate any human user's claimed identity when using FTP or Telnet prior to gaining access to the TOE. The single-use authentication mechanism is part of the IT environment.

8.3.7 Strength of Function claims are appropriate

308 The SOF claim made by the TOE is SOF-medium.

309 Products such as the SGS 5000 series Version 3.0 (Firewall Engine Only) are intended to be used in a variety of environments and used to connect networks with different levels of trust in the users. A number of deployments are possible. The Strength of Function of SOF-Medium for the TOE will be appropriate to a number of deployments, in both government and other organisations.

8.3.8 Justification of Assurance Requirements

310 EAL4 is defined in the CC as "methodically designed, tested and reviewed".

311 Products such as the SGS 5000 series Version 3.0 (Firewall Engine Only) are intended to be used in a variety of environments, and used to connect networks with different levels of trust in the users. A number of deployments are possible. The EAL4 assurance level will be appropriate to a number to a number of deployments, in both government and other organisations.

312 ALC_FLR.1 is appropriate to demonstrate the tracking and correction of flaws in products such as SGS that may have to be updated to address ever evolving methods of attack.

8.3.9 Assurance measures satisfy assurance requirements

313 Assurance measures in the form of deliverables will be produced to meet EAL4 assurance requirements, augmented with ALC_FLR.1.

314 Table 8-6, below, provides a tracing of the Assurance Measures to the assurance requirements that they meet. From the table it can be seen that all assurance requirements trace to at least one assurance measure.

315 The assurance requirements identified in the table are those required to meet the CC assurance level EAL4, augmented with ALC_FLR.1. As all assurance requirements are traced to at least one of the assurance measures, the identified assurance measures are sufficient to meet the assurance requirements. It is also asserted that the assurance measures have been produced with EAL4, augmented with ALC_FLR.1 in mind and as a consequence contains sufficient information to meet the assurance requirements of the TOE.

Assurance Measures	Assurance Requirements Met by Assurance Measure	
The implementation and documentation of procedures for the development of the TOE. Included in the procedures are: • The use of an automated configuration management system to support the secure development of the TOE, with user restrictions. • Procedures for authorising changes and implementing changes. • Procedures for tracking problems and rectification of problems.	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner.	ADO_DEL.2	Detection of modification

Assurance Measures	Assurance Requirements Met by Assurance Measure	
Documentation provided to the customers instructing the customer how to install and configure the TOE in a secure manner.	ADO_IGS.1	Installation, generation and start-up procedures
The implementation and documentation of procedures for the life-cycle model used to develop the TOE.	ALC_LCD.1	Developer defined life-cycle model
Functional Specification for the TOE describing the TSF and the TOE's external interfaces.	ADV_FSP.2	Fully defined external interfaces
System Design for the TOE providing descriptions of the TSF structure in the form of subsystems and the functionality of each subsystem.	ADV_HLD.2	Security enforcing high-level design
Various source code modules for the SGS 5000 series Version 3.0 (Firewall Engine Only)	ADV_IMP.1	Subset of the implementation of the TSF
System Design for the TOE providing descriptions of the TSF in the form of modules.	ADV_LLD.1	Descriptive low-level design
The documentation of the correspondence between all the TSF representations in specifically provided deliverables.	ADV_RCR.1	Informal correspondence demonstration
Documented Security Policy Model	ADV_SPM.1	Informal TOE security policy model

Assurance Measures	Assurance Requirements Met by Assurance Measure	
Documentation provided to the customers instructing the customer how to configure the TOE in a secure manner.	AGD_ADM.1	Administrator guidance
No specific user documentation is relevant as there are no non-administrative users.	AGD_USR.1	User guidance
The implementation and documentation of the physical security procedures to ensure the secure development of the TOE.	ALC_DVS.1	Identification of security measures
The implementation and documentation of procedures for tracking and rectifying flaws.	ALC_FLR.1	Basic Flaw Remediation
The implementation and documentation of the tools used to develop the TOE.	ALC_TAT.1	Well-defined development tools
Documented correspondence between the security functions and tests.	ATE_COV.2	Analysis of coverage
Documented correspondence between the High-level design subsystems and tests.	ATE_DPT.1	Testing: high-level design
The implementation and documentation of the test procedures including expected and actual results.	ATE_FUN.1	Functional testing
Independent Testing Resources	ATE_IND.2	Independent testing

Assurance Measures	Assurance Requirements Met by Assurance Measure	
Misuse Analysis is performed and documented to ensure that the guidance documents supplied are sufficient to ensure that the TOE can not be used in a insecure manner.	AVA_MSU.2	Validation of analysis
Strength of Function Assessment of the authentication mechanism is performed and documented to gain confidence in the security functionality of the TOE.	AVA_SOF.1	Strength of TOE security function evaluation
Vulnerability Assessment of the TOE and it's deliverables is performed documented to ensure that identified security flaws are countered.	AVA_VLA.2	Independent vulnerability analysis

Table 8-6 Mapping of Assurance Measures to Assurance Requirements

This page is intentionally blank.