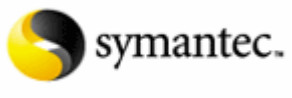

Security Target

for

Symantec Gateway Security

400 Series

version 2.1

(Firewall Engine Only)

Reference: T466\ST

May 2005

Issue: 2.0

Symantec Corporation
275 Second Avenue
Waltham, MA 02451
USA

Copyright notice

DOCUMENT AUTHORISATION

Document Title	Security Target for Symantec Gateway Security 400 Series version 2.1 (Firewall Engine Only)

Reference	**Issue**	**Date**	**Description**
T466/ST	0.1	May 2004	Draft
T466/ST	1.0	January 2005	Draft
T466/ST	2.0	May 2005	Final Issue

Contents

REFERENCES

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

GLOSSARY AND TERMS

Authorised Administrator	A person on the internal network allowed to administer the TOE.
CC	Common Criteria
DNS	Domain Name Server
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
FTP	File Transfer Protocol
Human User	Any person who interacts with the TOE
IP	Internet Protocol
IT	Information Technology
MAC	Media Access Control
MicroC/OS	SGS 400 operating system
NAT	Network Address Translation
NTP	Network Time Protocol
ROBO	Remote Office / Branch Office
SESA	Symantec Enterprise Security Architecture
SGS	Symantec Gateway Security
SGS 400 Series	Symantec Gateway Security 400-Series
SFP	Security Function Policy
SOF	Strength of Function
SGMI	Security Gateway Management Interface
SSMS	Symantec Security Management System
ST	Security Target
TCP	Transmission Control Protocol

TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
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
WAN	Wide Area Network

1 Introduction to the Security Target

1.1 Security Target Identification

1 Title: Security Target for Symantec Gateway Security 400 Series version 2.1 (Firewall Engine Only), issue 2.0.

2 Assurance Level: EAL2.

1.2 Security Target Overview

3 The Symantec Gateway Security 400-Series (SGS 400 Series) is Symantec's second-generation solution for the Remote Office / Branch Office (ROBO) and small office environments of medium and large enterprises. It combines a packet filtering Firewall, VPN, Intrusion Detection and Prevention, Content Filtering and Anti-Virus Policy Enforcement into one appliance.

4 The SGS 400 Series (Firewall engine only) is a packet filtering Firewall. It provides both packet inspection for all through traffic and firewall rule enforcement. It also provides network address translation to hide internal addresses. All firewall operations are applied to computer groups. A computer in the group is identified by its MAC address, or IP address, or its DNS name, or any combination of these.

1.3 CC Conformance Claim

5 This TOE has been developed using the functional components as defined in the Common Criteria version 2.2 [CC] part 2, with the assurance level of EAL2, as identified in part 3 of [CC].

6 The TOE conforms to [CC] Part 2 extended and [CC] Part 3 conformant with the assurance level of EAL2.

2 TOE Description

2.1 Overview of the Symantec Gateway Security 400 Series (Firewall Engine)

7 This section presents an overview of the Symantec Gateway Security 400 Series and the firewall engine to assist potential users in determining whether it meets their needs. Diagram 2-1 shows the configuration of Symantec Gateway Security 400 Series.

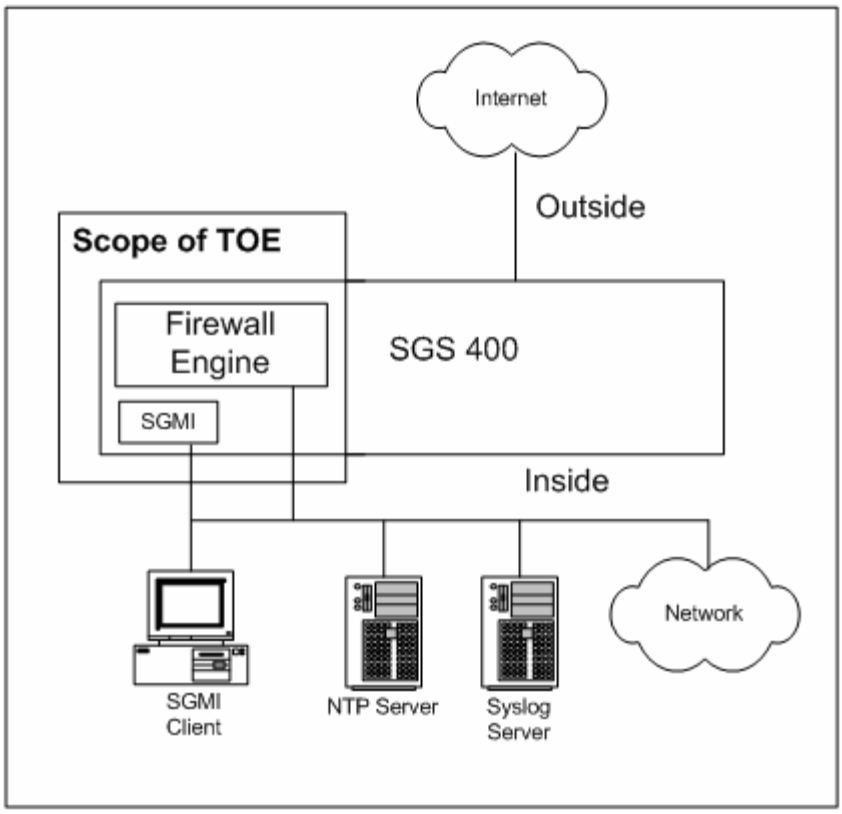

Diagram 2-1: Symantec Gateway Security 400 Series (Firewall Engine)

8 The Symantec Gateway Security 400 Series is an integrated gateway security appliance that incorporates five core security functions into a single solution. The solution combines firewall, anti-virus, intrusion detection and prevention, content filtering and VPN capabilities in a single appliance.

9 The Target of Evaluation (TOE) for this evaluation is the Symantec Gateway Security 400 Series (Firewall Engine Only), and the Security Gateway Management Interface (SGMI).

10 The Symantec Gateway Security 400 Series (Firewall Engine Only) is a packet filter firewall. It controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's administrator.

11 The Target of Evaluation (TOE) consists of the firewall itself, and the SGMI that is used to manage the firewall. See Diagram 2-1.

12 The SGMI component provides administrative services to the SGS 400 including policy, location, system-monitoring, settings and report generation. SGMI services can be accessed by supplying an administrator's user name and password via a HTML based web browser on the internal network. There is no separate software to install.

13 The SGS 400 has:

- one or two (depending on the model) built-in WAN ports serving as external connections (one WAN port will be used for the evaluated configuration);
- an Ethernet switch for up to 8 ports for internal networking;
- a serial port for potential dial-up connection to the outside (dial-up connections will not be used for the evaluated configuration).

14 The SGMI Client workstation used in the evaluated configuration to connect to the SGMI will be connected on the internal network. It is possible to connect to SGMI through the WAN port. But it is has to be enabled explicitly and an IP address from which the connection is made from has to be specified. For security reasons in the evaluated configuration the SGMI should not be connected from the outside network through the SGS 400's WAN port.

15 For the evaluated configuration a NTP server will be connected on the internal network to the SGS 400, in order to provide time stamping for the audit logs. Network Time Protocol (NTP) is an Internet standard protocol that ensures accurate synchronization to the millisecond of computer clock times in a network.

16 In order to retain audit logs, a Syslog server will also be connected on the internal network to the SGS 400. The Syslog server listens for log entries forwarded by the appliance and stores all log information for future analysis.

17 To maintain security, all traffic between each network attached to the SGS 400 must flow through the firewall. The protocols that are within the scope of the evaluation are:

DNS	FTP	HTTP	Telnet	UDP
POP3	SNMP	TFTP	TCP	SMTP

2.2 Scope and Boundaries of the Evaluated Configuration

18 The TOE configuration consists of:

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

2.2.1 Physical Scope

19 The TOE consists of facilities within firmware running on the SGS 400 hardware appliance, and the physical scope of the TOE is identified in Table 2-1.

Firmware	**Symantec Gateway Security 400 Series version 2.1 (Firewall Engine Only) with Security Gateway Management Interface**

Table 2-1: TOE Component Identification

2.2.2 Hardware and Firmware for the Appliance

20 The required IT environment for the TOE is the 400 Series (420, 440 and, 460). Table 2-2 identifies the explicitly tested underlying Firmware and hardware of the appliances that form part of the IT environment.

Firmware	Symantec Gateway Security version 2.1		
Build	703		
Hardware Model	420	440	460
Operating System	MicroC/OS-II 2.0	MicroC/OS-II 2.0	MicroC/OS-II 2.0
Network	• 10/100 Ethernet Auto-sensing WAN port (1) • 10/100 Ethernet Auto-sensing 4 LAN port switch • RS-232 Serial Port	• 10/100 Ethernet Auto-sensing WAN port (1) • 10/100 Ethernet Auto-sensing 4 LAN port switch • RS-232 Serial Port	• 10/100 Ethernet Auto-sensing WAN port (2) • 10/100 Ethernet Auto-sensing 8 LAN port switch • RS-232 Serial Port
User Interface	SGMI	SGMI	SGMI
CPU	• MIPS32 4Km Core Processor and encryption core • 2010 170 MHz • 32-bit bus @ 100 MHz • 16 KB data cache, and 16 KB instruction cache	• MIPS32 4Km Core Processor and encryption core • 2100 170 MHz • 32-bit bus @ 100 MHz • 16 KB data cache, and 16 KB instruction cache	• MIPS32 4Km Core Processor and encryption core • 2100 200 MHz • 32-bit bus @ 100 MHz • 16 KB data cache, and 16 KB instruction cache
Memory	• 8 MB Flash • 32 KB NVRAM • 64 MB DRAM	• 8 MB Flash • 32 KB NVRAM • 64 MB DRAM	• 8 MB Flash • 32 KB NVRAM • 64 MB DRAM

Table 2-2: Tested Underlying Firmware and Hardware of the Appliance

2.2.3 Hardware and Software Requirements for the SGMI

21 The SGMI is the administration interface to the SGS 400 and is part of the firmware on the SGS 400. It is accessible on the internal network via an SGMI client workstation running a web browser. Table 2-3 identifies the explicitly tested IT environment for the SGMI client.

Software	Internet Explorer 6.0 Service Pack 1
Operating System	Windows 2000 Service Pack 4

Table 2-3: IT Environment for the SGMI Client

22 No TOE specific software has to be loaded onto the workstation in order for the workstation to run SGMI.

23 Although the SGMI can be accessed from any machine connected to the internal network, in the evaluated configuration the authorized administrator is instructed to only access the SGMI from a dedicated client workstation.

2.2.4 Outside of the Scope

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

- Virtual Private Networking (VPN) functionality;
- Content filtering;
- High availability/load balancing/ bandwidth aggregation;
- Wizards;
- Remote Administration;
- Intrusion Detection and Prevention;
- Anti-virus policy enforcement;
- LiveUpdate support;
- Wireless networking;
- SESA (previously known as Symantec Security Management System);
- Event Manager;
- Advanced manager.

3 Security Environment

3.1 Introduction

25 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.

26 Within the evaluation references are made to the appliance operating system. The appliance operating system is referred to as the " MicroC/OS".

3.2 Threats

27 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 addressed by the TOE

28 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).

29 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 may inappropriately expose data or resources to the external network.

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

T.ASPOOF	An unauthorised person on an external network may attempt to pass information through the TOE into a connected network by using a spoofed address.
T.MEDIAT	An unauthorised person may send impermissible information through the TOE that results in the

	exploitation of resources on the internal network.
T.AUDACC	An attacker on an external network may escape detection because the audit logs are not reviewed.
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's actions.
T.CONFIG	An unauthorised person on the external network may exploit an insecure configuration of the TOE.

Table 3-1 Threats to be addressed by the TOE

31 The following table identifies the threats that are partially met by the TOE and partially met by the IT Environment.

Threats Partially met by the TOE & IT Environment	**Reasons**
T.SELPRO	The Syslog Server, NTP Server and MicroC/OS provide part of the protection against certain TOE sensitive data.
T.AUDFUL	The Syslog Server and NTP Server provide part of the auditing and time for the TOE.
T.AUDACC	The Syslog Server and NTP Server provide part of the auditing and time for the TOE.

Table 3-2 Threats partially met by the TOE and IT Environment

3.2.2 Threats countered solely by the IT Environment

32 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.

33 Table 3-2 identifies the threats that are partially met by the IT environment.

3.3 Organizational Security Policies

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

3.4 Assumptions

35 The following assumptions are assumed to exist.

A.TRUST	The users of the internal network from which administration of the TOE is performed are trusted not to attack the TOE, intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks.
A.PHYSEC	The TOE, NTP Server and Syslog Server are physically protected to prevent unauthorised use / user access. Only authorised administrators have physical access to the TOE, NTP Server and Syslog Server.
A.LOWEXP	The threat of malicious attacks from the external network aimed at discovering exploitable vulnerabilities is considered low.
A.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, NTP Server or the Syslog Server.
A.PUBLIC	The TOE, NTP Server and Syslog Server do not host public data.
A.NOEVIL	Authorised administrators for the TOE, NTP Server and Syslog Server are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information cannot flow between the internal network and the external network unless it passes through the TOE.
A.NOREMO	The TOE, Syslog Server and the NTP server cannot be accessed remotely from the external network.
A.REMOS	The Syslog Server and NTP Server are delivered to the user's site, installed and administered in a secure manner.
A.COMMS	The communication links between the TOE, NTP Server and the Syslog Server are physically protected.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

36 The principal IT security objective of the TOE is to reduce the vulnerabilities of an internal network exposed to an external network 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.

37 The IT security objectives are listed below.

O.MEDIAT	The TOE must mediate the flow of all information from users on a connected network to users on another connected network.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorised users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate times, and a means to sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide a record of all information flows through the TOE.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions.

38 The following table identifies the IT Security objectives listed that are partially met by the TOE and partially met by the IT Environment.

Partially met by IT Environment & TOE	Reasons
O.SECSTA	Part of the security of the TOE is provided by the MicroC/OS Operating System, Syslog server and the NTP Server.
O.SELPRO	Part of the security of the TOE is provided by the MicroC/OS Operating System, NTP Server and the Syslog server.
O.ACCOUN	Part of the security of the TOE is provided by the Syslog server and the NTP Server.
O.SECFUN	Part of the security of the TOE is provided by the Syslog server and the NTP Server.
O.AUDREC	Part of the security of the TOE is provided by the NTP Server and Syslog 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

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

OE.LOWEXP	The threat of malicious attacks from the external network 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, Syslog Server or NTP server.
OE.PUBLIC	The TOE, Syslog Server and NTP server do not host public data
OE.SINGEN	Information cannot flow between the internal network and the external network unless it passes through the TOE.
OE.NOREMO	The TOE, Syslog Server and NTP server cannot be accessed remotely from external networks.

OE.PARTSEP	The MicroC/OS Operating System must maintain a domain for its own execution that protects itself and its resources from external interference, or tampering.

4.2.2 Non-IT Security Objectives

40 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 firmware. Thus, they will be satisfied largely through application of procedural or administrative measures.

NOE.PHYSEC	The TOE, Syslog Server and NTP Server are physically secure.
NOE.NOEVIL	Authorized administrators of the TOE, Syslog server and NTP Server are non-hostile and follow all administrator guidance; however, they are capable of error.
NOE.GUIDAN	The TOE must be delivered to the user's site, installed, and administered in a secure manner.
NOE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
NOE.REMOS	The Syslog server and NTP server must be delivered to the user's site, installed and administered in a secure manner.
NOE.COMMS	The communication links between the TOE, the NTP server and the Syslog server must be physically protected.
NOE.TRUST	The network from which the TOE will be administered must be trusted.

5 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

41 The TOE security functional requirements consist of components from Part 2 of the CC, refined as indicated **in bold** and one explicitly stated requirement (FAU_GEN.1_EXP). They are listed in the following table.

Functional Components	
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_SMF.1	Specification of Management Functions
FPT_RVM.1	Non-Bypassability of the TSP
FAU_GEN.1_EXP	Audit Data Generation
FAU_SAR.1	Audit review (1)
FAU_STG.1	Protected audit trail storage (1)
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of Security Functions Behaviour
FPT_STM.1	Reliable time stamps (1)

Table 5-1: Functional Requirements

User Data Protection

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

43 Requirements Overview: *This Security Target consists of a single information flow control Security Function Policy (SFP). The information flow control SFP 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 information flowing between subjects in the policy 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.

44 **FDP_IFC.1 Subset information flow control**

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].

45 **FDP_IFF.1 Simple security attributes** [i]

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; • Physical interface: WAN, LAN]. b) information security attributes: • presumed address of source subject for outbound rules; • presumed address of destination subject for inbound rules; • TOE interface on which traffic arrives and departs; • service].
FDP_IFF.1.2	The TSF shall permit an information flow between a

[i] *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].

controlled subject and **another** controlled **subject** via a controlled operation if the
following rules hold:
[a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

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

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

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

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rule:
[Inbound and outbound traffic will be permitted to pass on specific ports, regardless of any other inbound or outbound rules, provided that these ports have been configured by the administrator and the request originates from a machine on the internal 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.]

Security Management

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

47 **FMT_MOF.1 Management of security functions behavior**

FMT_MOF.1.1 The TSF shall restrict the ability to ***perform*** the functions:
a) [start-up and shutdown;
b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;
c) enable NTP Server to set the time;
d) enable Syslog Server to log event;
e) archive and review the audit trail;
f) backup of configuration data file;
g) recover to the state following the last backup].
to [an authorized administrator].

48 **FMT_MSA.3 Static attribute initialization**

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

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

49 **FMT_SMF.1 Specification of Management Functions**

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

Protection of the TOE Security Functions

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

51 **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.

52 **FPT_STM.1 Reliable time stamps (1)**

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

Security Audit

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

54 **FAU_GEN.1_EXP Audit data generation**[ii]

FAU_GEN.1.1_EXP	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up of the audit functions; b) [the events listed in Table 5.2].
FAU_GEN.1.2_EXP	The TSF shall record within each audit record at least the following information: a) Time of the event, type of event, subject**s** identit**ies**, outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event

[ii] FAU_GEN.1_EXP is an explicit SFR, See Section 8.3.7 Rationale.

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.

Table 5-2: Auditable Event

55 **FAU_SAR.1 Audit review (1)**

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.

56 **FAU_STG.1 Protected audit trail storage (1)**

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

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorised modifications to the audit records in the audit trail**.**

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

FAU_STG.4.1 The TSF shall [*overwrite the oldest stored audit records*] if the audit trail is full.

5.2 Security requirements for the IT Environment

58 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	
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps (2)
FAU_GEN.1	Audit Data Generation
FAU_STG.1	Protected audit trail storage (2)
FAU_SAR.1	Audit review (2)
FAU_SAR.3	Selectable audit review

Table 5-3: IT Security Requirements of the Environment

Protection of the TOE Security Functions

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

60 **FPT_SEP.1 TSF domain separation** [iii]

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

61 *Application Note: The SGS 400 Series prevents the loading of additional capabilities to the TOE without physical access to the TOE being granted. Therefore preventing the remote uploading of malicious code (that which conflicts with the TSP). The SGS 400 Series uses a single domain of execution, it is only possible to execute TSF relevant processes, manipulating TSF data. There is no concept of user data in this instance.*

[iii] FPT_SEP.1 is met by MicrC/OS.

62 **FPT_STM.1 Reliable time stamps (2)**[iv]

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

Security Audit

63 This section involves recognizing, recording and storing information related to security relevant activities.

64 **FAU_GEN.1 Audit data generation**[v]

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 event listed 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**s** identit**ies**, 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**
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.

Table 5-4: Auditable Event

[iv] FPT_STM.1 is partially met by the MicroC/OS and the NTP Server.
[v] FAU_GEN.1 is fully met by the Syslog server.

65 **FAU_SAR.1 Audit review (2)**[vi]

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.

66 **FAU_SAR.3 Selectable audit review**[vii]

FAU_SAR.3.1	The TSF shall provide the ability to perform *searches and sorting* of audit data based on: a) [presumed subject address; b) ranges of dates; c) ranges of times; d) ranges of addresses].

67 **FAU_STG.1 Protected audit trail storage**[viii] **(2)**

FAU_STG.1.1	The TSF shall protect the stored audit records from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to *prevent* modifications to the audit records**.**

[vi] FAU_SAR.1 is partially met by the Syslog server.

[vii] FAU_SAR.3 is fully met by the Syslog server

[viii] FAU_STG.1 is partially met by the Syslog server.

5.3 TOE Security Assurance Requirements

68 The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL2 level of assurance. The assurance components are summarized in the following table.

Assurance Class	**Assurance Components**	
Configuration management	ACM_CAP.2	Configuration Items
Delivery and operation	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.1	Informal Functional Specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5-5: Assurance Requirements: EAL2

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

5.4 Strength of Function Claim

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

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

6 TOE Summary Specification

6.1 TOE Security Functions

72 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 Management and Security Function

73 **M.1 -** The authorised administrator has the ability to perform the following functions:

a) start-up and shutdown;
b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;
c) enable NTP Server to set the time;
d) enable Syslog Server to log event;
e) archive and review the audit trail;
f) backup of configuration data file;
g) recover to the state following the last backup.

74 **M.2 -** The NTP Server function of the TOE provides the facility of allowing an administrator to specify that time that is obtained from a NTP Server. This function can only be accessed from the Log Settings Tab within the Security Gateway Management Interface (SGMI).

75 **M.3 -** The TSF shall provide restrictive default values for inbound connections and permissive default values for outbound connections for the information flow security attributes for the Unauthenticated SFP.

76 **M.4 -** 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.

6.1.2 Audit Function

77 **A.1 -** 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.

78 **A.2 -** It is possible to generate audit records for the following auditable events:

- Start-up of the audit functions;
- Every successful inbound and outbound connection;
- Every unsuccessful inbound and outbound connection;

79 **A.3 -** The TOE includes its own facilities for recording and viewing all audit events, which are recorded in log files that can be viewed by way of the SGMI and archived manually by the authorised administrator by way of the syslog server.

80 **A.4 -** The following information is recorded for all audit log events:

- The time at which the event was logged, derived from MicroC/OS and the NTP server.
- Source and destination address.
- The text description of the message describing the event.

81 **A.5 -** The log messages written to NVRAM (non-volatile random access memory) are stored across reboots of the appliance. Once the maximum number of events in the queue is reached, the SGS 400 Series begins overwriting previous events using a circular queue algorithm. Through the SGMI, the administrator is able to enable a Syslog server to ensure that no records are lost. Events are then automatically written to the Syslog server.

82 **A.6 -** The authorised administrator has the ability to read and delete audit trail data through the controlled interface SGMI logfile window.

6.1.3 Protection of TOE security Functions

83 **P.1 -** 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.

84 **P.2 -** Time will be derived from MicroC/OS and the NTP server.

6.1.4 User Data Protection Function

85 **U.1 -** 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).

86 **U.2 -** The TSF permits or denies unauthenticated connections depending on the security policy rules created by the authorised administrator.

87 **U.3 -** The security policy rules are order dependent.

88 **U.4 -** All inbound connections are denied by default. All outbound connections are allowed by default.

89 **U.5 -** The Service used can be one of the following protocols:

DNS	FTP	HTTP	Telnet	UDP
POP3	SNMP	TFTP	TCP	SMTP

90 **U.6 –** The TOE enforces the following Unauthenticated information flow:

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

91 **U.7 -** The TSF shall enforce unauthenticated information flow based on the following attributes:

a) Subject security attributes:
   - Presumed address,
   - Physical interface (WAN, LAN),

b) Information security attributes:
   - Presumed address of source subject for outbound rules;
   - Presumed address of destination subject for inbound rules;
   - TOE interface on which traffic arrives and departs;
   - Service.

92 **U.8 -** Unauthenticated information flow shall be permitted:

- 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.

93 **U.9 -** Rules in the Security policy are defined by the TOE authorised Administrator, and allow the parameters stated in **U.7** to be set for unauthenticated traffic flow.

94 **U.10 -** 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.

95 **U.11 -** 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.

96 **U.12 -** Traffic flows from the external network to another connected network shall only be permitted if all the information security attribute values created by the authorised administrator are permitted.

97 **U.13 -** 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.

98 **U.14 -** 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.

99 **U.15 –** The TOE authorised administrator shall be able to configure certain ports as "special applications". Inbound and outbound traffic will be permitted to pass using these ports, regardless of any other inbound or outbound rules provided that the request originates from a machine on the internal network.

6.2 Identification and Strength of Function Claim for IT security Functions

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

101 No specific strength of function metric is defined.

6.3 Assurance Measures

102 Assurance measures will be produced to comply with the Common Criteria Assurance Requirements for EAL2. Table 8-6 maps the assurance measures to the assurance requirements.

7 Protection Profiles Claims

No claims against a protection profile are made.

8 Rationale

8.1 Introduction

103 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

104 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.ASPOOF	T.MEDIAT	T.AUDACC	T.SELPRO	T.AUDFUL	T.CONFIG	TE.USAGE	A.PHYSEC	A.LOWEXP	A.GENPUR	A.PUBLIC	A.NOEVIL	A.SINGEN	A.NOREMO	A.REMOS	A.COMMS	A.TRUST
O.MEDIAT	✔	✔				✔											
O.SECSTA				✔													
O.SELPRO				✔	✔	✔											
O.AUDREC			✔														
O.ACCOUN			✔														
O.SECFUN					✔												
OE.PARTSEP				✔	✔		✔										
OE.LOWEXP									✔								
OE.GENPUR										✔							
OE.PUBLIC											✔						
OE.SINGEN													✔				
OE.NOREMO														✔			
NOE.GUIDAN							✔										
NOE.ADMTRA			✔				✔										
NOE.PHYSEC								✔									
NOE.NOEVIL												✔					
NOE.REMOS															✔		
NOE.COMMS																✔	
NOE.TRUST																	✔

Table 8-1 Mapping of Objectives to Threats and Assumptions

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

106 **O.MEDIAT**

107 This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT, and T.CONFIG 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.

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

109 **O.SECSTA**

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

111 The MicroC/OS, Syslog Server and the NTP server perform part of the resistance to penetration attacks.

112 **O.SELPRO**

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

114 The MicroC/OS, NTP server and the Syslog Server provide part of the protection for the TOE.

115 **O.AUDREC**

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

117 The audit trail is stored on the Syslog server and in NVRAM. The MicroC/OS and the NTP server provides the time for the TOE.

118 **O.ACCOUN**

119 This security objective is necessary to counter the threat: T.AUDACC because it requires that information flows through the TOE are recorded.

120 The Syslog server performs part of the audit functions. The MicroC/OS and the NTP server provide the time for the TOE.

121 **O.SECFUN**

122 This security objective is necessary to counter the threat: T.AUDFUL by requiring that the TOE allows the authorised administrator access to the TOE security functions.

123 The configuration of the Syslog server, the MicroC/OS and the NTP server support this objective.

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

125 **OE.PARTSEP**

126 This security objective is necessary to counter the threats: T.SELPRO, T.AUDFUL, and TE.USAGE because it requires that the TOE protect itself and its resources from external interference, tampering or unauthorized disclosure of the TOE security functions.

127 The MicroC/OS provides the protection for the TOE.

128 **OE.LOWEXP**

129 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.

130 **OE.GENPUR**

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

132 **OE.PUBLIC**

133 This environmental security objective is necessary to support the assumption: A.PUBLIC because it requires that the TOE, Syslog server and the NTP server do not host public data.

134 **OE.SINGEN**

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

136 **OE.NOREMO**

137 This environmental security objective is necessary to support the assumption: A.NOREMO because it requires that the TOE, the Syslog server and the NTP server cannot be accessed remotely from the external network.

138 **NOE.GUIDAN**

139 This environmental security objective is necessary to counter the threat: TE.USAGE 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.

140 **NOE.NOEVIL**

141 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.

142 **NOE.PHYSEC**

143 This environmental security objective is necessary to support the assumption: A.PHYSEC because it requires that the TOE, the Syslog server and the NTP server are physically protected.

144 **NOE.ADMTRA**

145 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.

146 **NOE.REMOS**

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

148 **NOE.COMMS**

149 This environmental security objective is necessary to support the assumption: A.COMMS because it requires that the communication links between the TOE, the Syslog server and the NTP server are physically protected.

150 **NOE.TRUST**

151 This environmental security objective is necessary to support the assumption: A.TRUST because it requires that the internal network is trusted.

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

153 **T.SELPRO**

154 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.

155 **T.AUDFUL**

156 The TOE provides the administrator with Read Only access to the TOE audit data through the SGMI. Once the audit trail is full, the oldest audit record is overwritten.

157 Through the firewall configuration the administrator ensures that the audit logs are sent to the Syslog server.

158 The authorised administrator must ensure that the data is archived on the Syslog server and that the storage space does not become exhausted.

159 **T.AUDACC**

160 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.

161 The Syslog server 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.

8.3 Security Requirements Rationale

8.3.1 Security Requirements are appropriate

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

Objective	Security Functional Requirement(s)
O.MEDIAT	FDP_IFC.1, FDP_IFF.1, FMT_MSA.3, FMT_SMF.1
O.SECSTA	FMT_MOF.1, FMT_MSA.3
O.SELPRO	FPT_RVM.1, FAU_STG.4, FAU_STG.1 (1)
O.AUDREC	FAU_GEN.1_EXP, FAU_SAR.1 (1), FPT_STM.1(1)
O.ACCOUN	FAU_GEN.1_EXP, FAU_STG.1 (1), FPT_STM.1(1)
O.SECFUN	FAU_STG.4, FMT_MOF.1, FMT_SMF.1, FMT_MSA.3, FAU_STG.1 (1)

Table 8-2 Mapping of Objectives to SFRs

163 **FDP_IFC.1 Subset information flow control**

164 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.

165 **FDP_IFF.1 Simple security attributes**

166 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.

167 **FMT_MSA.3 Static attribute initialization**

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

169 **FMT_SMF.1 Specification of Management Functions**

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

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

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

173 **FAU_GEN.1_EXP Audit data generation**

174 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.

175 **FAU_SAR.1 Audit review (1)**

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

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

178 This component ensures that the audit trail is not lost by ensuring that the Syslog Server is enabled through the TOE. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

179 **FMT_MOF.1 Management of security functions behavior**

180 This component ensures that the TSF restricts the ability of the TOE start up and shut down, ability to create, delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1 to the authorised administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.SECSTA.

181 **FPT_STM.1 Reliable time stamps (1)**

182 This component ensures that auditable events are time stamped in the logs. Time will be derived from MicroC/OS and the NTP server. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

183 **FAU_STG.1 Protected audit trail storage (1)**

184 This component ensures that the audit trail is not modified by storing the logs in NVRAM. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.ACCOUN.

8.3.2 Environmental Security Requirements are appropriate

185 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.SECSTA	FPT_SEP.1, FAU_STG.1 (2)
O.SELPRO	FPT_SEP.1, FAU_STG.1 (2)
O.AUDREC	FAU_GEN.1, FPT_STM.1 (2), FAU_SAR.1 (2), FAU_SAR.3
O.ACCOUN	FAU_GEN.1, FPT_STM.1 (2)
O.SECFUN	FAU_STG.1 (2)
OE.PARTSEP	FPT_SEP.1
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

186 **FPT_SEP.1 TSF domain separation**

187 This component ensures that the TSF has 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: OE.PARTSEP, O.SELPRO, O.SECSTA, OE.LOWEXP, OE.GENPUR, OE.PUBLIC, OE.SINGEN and OE.NOREMO.

188 **FAU_GEN.1 Audit data generation**

189 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.

190 **FPT_STM.1 Reliable time stamps (2)**

191 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.

192 **FAU_STG.1 Protected audit trail storage (2)**

193 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.

194 **FAU_SAR.1 Audit review (2)**

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

196 **FAU_SAR.3 Selectable audit review**

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

8.3.3 Security Requirement dependencies are satisfied

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_ MOF.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_SMF.1	None	None
FAU_GEN.1_EXP	FPT_STM.1	FPT_STM.1 (1)
FAU_SAR.1 (1) FAU_STG.1 (1)	FAU_GEN.1 FAU_GEN.1	FAU_GEN.1_EXP FAU_GEN.1_EXP
FAU_STG.4	FAU_STG.1	FAU_STG.1 (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
FPT_RVM.1	None	None
FPT_STM.1 (1)	None	None

Table 8-4 Mapping of TOE SFR Dependencies

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

199 Functional component FMT_MSA.3 depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. Therefore FMT_MOF.1 more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Security Target.

200 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.NOREMO only an authorised administrator will have physical access to the

TOE, Syslog server and NTP server. Human users, including authorised administrators cannot access the TOE, Syslog server and NTP server remotely from the external networks. The assumption A.TRUST states that the users on the internal network are trusted users. The dependency on FMT_SMR.1 is therefore regarded as satisfied.

201 Functional components FAU_SAR.1 (1) and FAU_STG.1 (1) have a dependency on functional component FAU_GEN.1. FAU_GEN.1_EXP is the explicit requirement that has been included instead of FAU_GEN.1. Functional component FAU_GEN.1_EXP meets the dependencies of FAU_GEN.1.

8.3.4 IT security functions satisfy SFRs

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

IT Function	Security Functional Requirement(s)
Management and Security[ix]	
M.1	FMT_MOF.1, FMT_SMF.1
M.2	FMT_MOF.1, FMT_SMF.1
M.3	FMT_MSA.3
M.4	FMT_MSA.3
Audit	
A.1	FAU_GEN.1_EXP
A.2	FAU_GEN.1_EXP
A.3	FAU_GEN.1_EXP
A.4	FAU_GEN.1_EXP
A.5	FAU_STG.1 (1), FAU_STG.4
A.6	FAU_SAR.1 (1)

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

Protection of TOE Security Functions	
P.1	FPT_RVM.1
P.2	FPT_STM.1 (1)
User Data Protection[x]	
U.1	FDP_IFC.1, FDP_IFF.1
U.2	FDP_IFC.1, FDP_IFF.1
U.3	FDP_IFC.1, FDP_IFF.1
U.4	FDP_IFC.1, FDP_IFF.1
U.5	FDP_IFC.1, FDP_IFF.1
U.6	FDP_IFC.1, FDP_IFF.1
U.7	FDP_IFF.1
U.8	FDP_IFF.1
U.9	FDP_IFC.1
U.10	FDP_IFF.1
U.11	FDP_IFF.1
U.12	FDP_IFF.1
U.13	FDP_IFF.1
U.14	FDP_IFF.1
U.15	FDP_IFF.1

Table 8-5 Mapping of IT Functions to SFRs

203 To perform sorts on the audit database the administrator will be able to use the Security Gateway Management Interface (SGMI) Logfile icon. This is to meet

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

FAU_SAR.1 (1). In the event of audit storage failure, exhaustion the TOE will enable a Syslog server to log events, so that requirement FAU_STG.4 is met.

204 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 of the TOE security functional requirements, and all the TOE Security Function Requirements are covered. Therefore by implementing all of the IT Security Functions, all of the TOE Functional Requirements are met.

8.3.5 IT security functions mutually supportive

205 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 security functions can be mapped to one or more SFRs, as demonstrated in Table 8-5.

8.3.6 Strength of Function claims are appropriate

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

207 Products such as the Symantec Gateway Security 400 Series (Firewall Engine Only) are intended to provide security controls in order that SMEs can protect the resources on an internal network from an external network. The Strength of Function of SOF-Medium for the TOE will be appropriate to a number of deployments.

8.3.7 Explicit Requirements Rationale

208 The explicit requirement FAU_GEN.1_EXP has been added as the TOE does not record the shutdown of the TOE. Events are recorded in the log a fraction of a millisecond after they occur. It is therefore unlikely that records would be lost during shutdown. The only possible shutdown is a hard shutdown. The TOE does record the startup so an administrator would be able to calculate from the last event recorded to the startup event when a shutdown occurred.

209 The TOE log does not record the date of an event, however the syslog server records the date and time an event is logged. An event in the evaluated configuration is logged simultaneously in both the TOE log and the syslog.

210 FAU_GEN.1_EXP ensures that the auditing requirements performed by the TOE are captured.

8.3.8 Justification of Assurance Requirements

211 EAL2 is defined in the CC as "structurally tested".

212 Products such as the Symantec Gateway Security 400 Series (Firewall Engine Only) are intended to provide security controls in order that SMEs can protect the resources on an internal network from an external network.

8.3.9 Assurance measures satisfy assurance requirements

213 Assurance measures in the form of deliverables will be produced to meet EAL2 assurance requirements.

214 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.

215 The assurance requirements identified in the table are those required to meet the CC assurance level EAL2. 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 EAL2, 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. • List of configuration items.	ACM_CAP.2	Configuration items

Assurance Measures	Assurance Requirements Met by Assurance Measure	
The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner.	ADO_DEL.1	Delivery Procedures
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
Functional Specification for the TOE describing the TSF and the TOE's external interfaces.	ADV_FSP.1	Informal Functional Specification
System Design for the TOE providing descriptions of the TSF structure in the form of subsystems and the functionality of each subsystem.	ADV_HLD.1	Descriptive high-level design
The documentation of the correspondence between all the TSF representations in specifically provided deliverables.	ADV_RCR.1	Informal correspondence demonstration
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

Assurance Measures	Assurance Requirements Met by Assurance Measure	
Documented correspondence between the security functions and tests.	ATE_COV.1	Evidence of coverage
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
The documentation for the Strength of Function Assessment.	AVA_SOF.1	Strength of TOE security function evaluation
Vulnerability Assessment of the TOE and it's deliverables is performed and documented to ensure that identified security flaws are countered.	AVA_VLA.1	Developer vulnerability analysis

Table 8-6 Mapping of Assurance Measures to Assurance Requirements