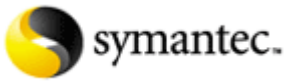

Security Target

for

Symantec Enterprise Firewall

Version 7.0.4

For Windows 2000 and Solaris

Reference: T426\ST

October 2003

Version: 2.3

Symantec Corporation
266 Second Avenue
Waltham, MA 02451
USA

Copyright notice

DOCUMENT AUTHORISATION

Document Title	Security Target for Symantec Enterprise Firewall Version 7.0.4 for Windows 2000 and Solaris

Reference	**Version**	**Date**	**Description**
ST	0.1	September 2002	Draft
ST	1.0	September 2002	Issued to evaluators
ST	1.1	May 2003	Version update
ST	1.2	June 2003	Issued to evaluators
ST	1.3	July 2003	Issued to evaluators
ST	1.4	July 2003	Issued to evaluators
ST	1.5	July 2003	Issued to evaluators
ST	1.6	July 2003	Issued to evaluators
ST	1.7	July 2003	Issued to evaluators
ST	1.8	August 2003	Issued to evaluators
ST	1.9	August 2003	Issued to evaluators
ST	2.0	September 2003	Not Issued
ST	2.1	September 2003	Issued to evaluators
ST	2.2	September 2003	Issued to evaluators
ST	2.3	October 2003	Issued to evaluators

Contents

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (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.
FTP	File Transfer Protocol
Human User	Any person who interacts with the TOE
IP	Internet Protocol
IT	Information Technology
MAC	Media Access Control
NAT	Network Address Translation
PP	Protection Profile
SEF	Symantec Enterprise Firewall
RCU	Raptor Console for Unix
SFP	Security Function Policy
SOF	Strength of Function
SRMC	Symantec Raptor Management Console
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
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.

1 Introduction to the Security Target

1.1 Security Target Identification

1 Title: Security Target for Symantec Enterprise Firewall Version 7.0.4 for Windows 2000 and Solaris issue 2.2.

2 Assurance Level: EAL4.

1.2 Security Target Overview

3 The Symantec Enterprise Firewall is an 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.

1.3 CC Conformance Claim

4 This TOE has been developed using the functional components as defined in the Common Criteria version 2.1 [CC] part 2, with the assurance level of EAL4.

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

2 TOE Description

2.1 Overview of the Symantec Enterprise Firewall

6 This section presents an overview of the Symantec Enterprise Firewall Version 7.0.4 to assist potential users in determining whether it meets their needs.

7 The Symantec Enterprise Firewall is an application level firewall. 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.

8 The packets enter the TCP/IP stack of the Symantec Enterprise Firewall. Various scanning techniques are then applied and completed via the seven layers of the OSI model. After all tests are completed, if there are no problems, the packets are allowed to flow out of the Symantec Enterprise Firewall to the next network segment.

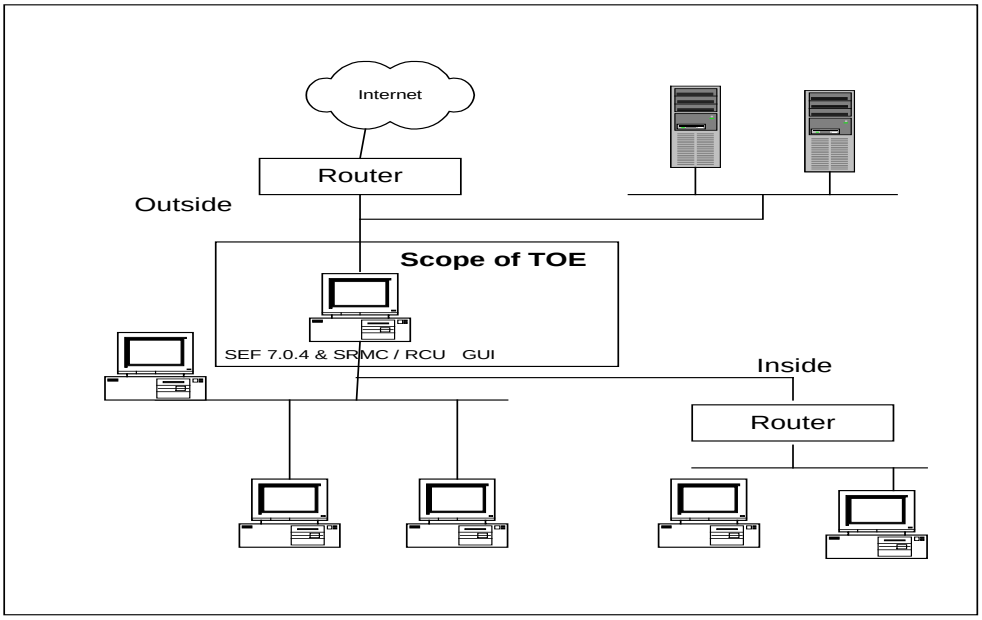

Diagram 2-1: Packet Flow through the Symantec Enterprise Firewall

9 The Target of Evaluation (TOE) consists of two physical components, the firewall itself and the Symantec Raptor Management Console (SRMC) / Raptor Console (RCU) for Unix (on the firewall server console), which is used to manage the firewall.

10 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.

11 In addition Symantec Enterprise firewall provides the following functions:

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

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

13 For the evaluation three 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.

14 All traffic between each network attached to the TOE must flow through the Symantec Enterprise Firewall 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
Gopher	NNTP	POP3	RealAudio	TCP

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

HTTP	Gopher	NNTP	RealAudio	DNS
TELNET	SMTP	FTP	NTP	

16 S/Key authentication for FTP / Telnet is within the scope of the TOE.

[i] Http proxy supports WebDAV (Web Distributed Authorising and Versioning)

2.2 Scope and Boundaries of the Evaluated Configuration

17 The TOE configuration consists of:

- The firewall itself;
- The Symantec Raptor Management Console (SRMC) for Windows 2000, which is used for administration by the administrator;
- The Raptor Console for Unix (RCU) for Solaris, which is used for administration by the administrator;
- Two Network Address Translation (NAT) options (static and dynamic address), to protect the identity of users and make addresses available as needed;

2.2.1 Physical Scope

18 The physical scope of the TOE is identified in Table 2-3.

Software	**Symantec Enterprise Firewall Version 7.0.4 with Symantec Raptor Management Console / Raptor Console for Unix.**

Table 2-3: TOE Component Identification

19 The required IT environment for the TOE is identified in Table 2-4.

Operating System	Microsoft Windows 2000 operating system with Service Pack 3.	Sun Solaris versions 7	Sun Solaris versions 8
Network Interface cards	A minimum of 2 Network Interface cards. For the evaluation 3 network interface cards will be used. Intel Pro/1000MT Desktop Adapter 3COM Etherlink 10/100 Mbps PCI with 3XP processor 3COM Etherlink XL 10/100 PCI 3C905C-TX	A minimum of 2 Network Interface cards For the evaluation the following network interface cards will be used. SUN Quad Ethernet (270 5406-06-Rev01) Motherboard Network card (4116914000-R4G)	A minimum of 2 Network Interface cards For the evaluation the following network interface cards will be used SUN Quad Ethernet (270 4366-04-Rev02) Motherboard Network card (4116959000-R2e-03)
CPU	Pentium III 1 Ghz	SUNW Ultrasparc III running on Sun Ultra 5 270 Mhz	SUNW Ultrasparc III running on Sun Ultra 5 270 Mhz
Memory	512 MB Memory of RAM	512 MB Memory of RAM	512 MB Memory of RAM
Disk space	20 GB Hard Disk	(minimum) 8gb	(minimum) 4.3 gb
Display	No specific display requirements are required for the SRMC.	256 color display 1024 x 768 to run RCU.	256 color display 1024 x 768 to run RCU.

Software	Microsoft Management Console 1.2 for the SRMC. Microsoft Internet Explorer 6.0 with Service Pack 1 for SRMC.	Not required for the RCU.	Not required for the RCU.

Table 2-4:IT Environment for the TOE

2.2.2 Outside of the Scope

20 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;
- High availability/load balancing;
- User Authentication by one-time password (excluding S/Key Authentication), and SecurID Authentication engine for mobile users to access services in the protected domain;
- Setup Wizard;
- H.323 Connections;
- Remote Administration;
- Forward Filtering;
- S/Key Password Generator;
- SQL*Net proxy.

3 Security Environment

3.1 Introduction

21 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.

3.2 Threats

22 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

23 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).

24 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.

25 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.

26 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.

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

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

Table 3-1 Threats partially met by the TOE

3.2.2 Threats countered by the Operating Environment

28 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.

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

3.3 Organizational Security Policies

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

3.4 Assumptions

31 The following assumptions are assumed to exist.

A.PHYSEC	The TOE will be physically protected to prevent unauthorised users. Only authorised administrators will have physical access to the TOE.
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.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorised administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (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 remotely from the internal or external networks.
A.REMOS	The operating system is assumed to be delivered to the user's site, installed and administered in a secure manner.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

32 The principal IT security objective of the Symantec Enterprise Firewall 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 Symantec Enterprise Firewall has the objective of providing the ability to monitor established connections and attempted connections between networks.

33 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.

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

Partially met by IT Environment	**Reasons**
O.SECSTA	Part of the security of the TOE is provided by the Operating System.
O.SELPRO	Part of the security of the TOE is provided by the Operating System.
O.AUDREC	Part of the security of the TOE is provided by the Operating System.
O.ACCOUN	Part of the security of the TOE is provided by the Operating System.
O.SECFUN	Part of the security of the TOE is provided by the Operating System.
O.LIMEXT	Part of the security of the TOE is provided by the Operating System.
O.EAL	Part of the security of the TOE is provided by the Operating System

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

4.2 Environment Security Objectives

4.2.1 IT Security Objectives

35 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.
OE.PUBLIC	The TOE does 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 remotely from the internal or external networks.

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

4.2.2 Non-IT Security Objectives

37 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 must be physically protected so only administrators have access. (The TOE must only be administered via the dedicated management port on the firewall.)
OE.NOEVIL	Authorised administrators are non-hostile and follow all administrator guidance; however, they are 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, installed, administrated, and operated in a manner that maintains security.
OE.ADMTRA	Authorised administrators are trained as to establishment and maintenance of security policies and practices.
OE.REMOS	The operating system will be delivered, installed and administered in a secure manner.

5 IT Security Requirements

5.1 TOE Security Requirements

38 This section provides functional requirements that are drawn from Part 2 of the CC.

5.1.1 TOE Security Functional Requirements

39 The functional security requirements for this Security Target consist of the components from Part 2 of the CC listed in the following table.

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

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

Table 5-1: Functional Requirements

Identification and Authentication

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

41 Only an authorised administrator is able to interact directly with the Symantec Enterprise Firewall through the SRMC / RCU. The authorised administrator is the only user who can log onto the Symantec Enterprise Firewall via the SRMC / RCU and access TSF data. The Symantec Enterprise Firewall provides a basic form of access control mechanisms for the identification and authentication.

42 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.

43 Component FIA_UAU.4 discusses when authentication mechanisms must be used. For the supported user authentication FIA_UAU.4, the SOF shall be demonstrated for the authentication mechanism.

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

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].

User Data Protection

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

46 *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.*

47 **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].

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

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

a) [subjects: a human user or external IT entity that sends and receives FTP and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.4,
b) information: FTP and Telnet traffic sent through

the TOE from one subject to another;

c) operation: initiate service and pass information].

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

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].

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

[2] *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].

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, and POP3), 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.]

50 **FDP_IFF.1 Simple security attributes (2)**[3]

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

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;

[3] *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].

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

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

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

connected network.]

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

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

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

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

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

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

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

52 **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.4] to [an authorised administrator].

53 **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].

54 **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].

55 **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].

56 **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].

57 **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].

58 **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.

59 **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_MSA.1(1),(2),(3)&(4) and FMT_MOF.1(1)&(2) restrict use to the authorised administrator].

Protection of the TOE Security Functions

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

61 **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.

62 **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

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

64 **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 event 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
FIA_UAU.4	Any use of the authentication mechanism.	The user identities provided to the TOE
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

Table 5-2: Auditable Event

65 **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.

66 **FAU_SAR.3 Selectable audit review**

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

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

67 **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

68 This section details the IT security requirements that are met by the IT environment of the TOE. Table 5-5 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_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_SAR.1	Audit review	**Partially**
FAU_SAR.3	Selectable audit review	**Partially**
FAU_STG.1	Protected audit trail storage	**Fully**
FAU_STG.4	Prevention of audit data loss	**Partially**
FMT_MOF.1	Management of security functions behavior (2)	**Partially**
FMT_SMF.1	Specification of management Functions	**Partially**

Table 5-3: IT Security Requirements of the Environment

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

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.

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

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

71 **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.

72 **FPT_STM.1 Reliable time stamps**

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

73 **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:

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

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

c) [the event 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.
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

Table 5-4: Auditable Event

74 **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.

75 **FAU_SAR.3 Selectable audit review**

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

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

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

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

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.

78 **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 and audit trail data] to [an authorised administrator].

79 **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(2) restricts use to the authorised administrator].

5.3 TOE Security Assurance Requirements

80 The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL4 level of assurance. 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
	ADO_IGS.1	Installation, generation and start-up procedures
	ADV_FSP.2	Fully defined external interfaces
Development	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

Assurance Class	Assurance Components	
	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_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
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

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

5.4 Strength of Function Claim

82 A Strength of Function (SOF) claim of SOF-Medium is made for the TOE. The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism. In the case of this Security Target, this minimum level shall be SOF-Medium.

83 For the supported user authentication FIA_UAU.4, the SOF shall be demonstrated for the authentication mechanism

84 For a justification of the Strength of Function claim see Section 8.3.6.

6 TOE Security Functions

85 This section describes the security functions provided by the TOE to meet the security functional requirements specified for the Symantec Enterprise Firewall in Section 5.1.

6.1.1 Identification and Authentication Function

86 Authorised human users sending or receiving information through the TOE, using FTP and Telnet must also be authenticated using S/Key authentication. S/Key authentication involves a challenge and response process, which generates one-time passwords. S/Key authentication password consists of 10 or more character length and 94 characters (alphanumeric characters and marks). The S/Key authentication has Strength of Claim for the mechanism, see Section 5.4.

87 All success or failure to authenticate using S/Key authentication will result in the generation of a record in the audit trail. In addition the user identities provided to the TOE will be recorded.

6.1.2 Management and Security Function

88 The authorised administrator can delete, modify, and add to a rule in the unauthenticated SFP.

89 The authorised administrator can delete, modify, and add to a rule in the authenticated SFP.

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

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

92 The TSF shall provide restrictive default values for the information flow security attributes for Unauthenticated and authenticated SFPs.

93 The authorised administrator has the ability to enable and disable the following functions:

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

94 The authorised administrator has the ability to enable, disable, determine and modify the behavior of the following functions:

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.

95 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.

6.1.3 Audit Function

96 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 audibly configured to be recorded in the audit trail.

97 It is possible to generate audit records for the following auditable events:

- Start-up and shutdown of the audit functions;
- All level of challenge response;
- Every successful inbound and outbound connection;
- Every unsuccessful inbound and outbound connection;
- Creating, deleting, and emptying of the audit trail.

98 For each event the Audit Function will record the following:

- Date and time of the event;
- 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.

99 The authorised administrator has read access only to all audit trail data through the controlled interface SRMC / RCU logfile window.

100 The authorised administrator via the SRMC / RCU is able through the use of filters to perform searches and sorting of audit data based on:

- 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 and sorted using this facility as required by the SFR FAU_SAR.3.

101 Archiving is a manual process that is performed on the text 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.

6.1.4 Protection of TOE security Functions

102 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.

103 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.

104 The TSF protects itself, by denying all processes unless a process is specifically stated by the TSF.

105 The Time range template function of the Symantec Enterprise Firewall 7.0.4 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 SRMC / RCU.

6.1.5 User Data Protection Function

106 The Symantec Enterprise Firewall provides a flow control mechanism in the form of security policy rules for all connections through the Symantec Enterprise Firewall for either inbound traffic (external to internal) or outbound traffic (internal to external).

107 The TSF permits or denies authenticated connections depending on the security policy rules created by the administrator.

108 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.

109 The security policy rules are non-order dependent.

110 All Connections are denied unless a specific rule has been set-up to allow information to flow.

111 The Service used can be one of the following protocols:

HTTP	UDP	FTP	Ping	DNS
TELNET	SMTP	NTP	RTSP	IP
Gopher	NNTP	POP3	RealAudio	TCP

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

HTTP	Gopher	NNTP	NTP	DNS
TELNET	SMTP	FTP	RealAudio	

113 There are two main types of information flow that the TOE enforces:

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

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

Unauthenticated

114 The TSF shall enforce unauthenticated information flow based on the following 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.

115 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.

116 Rules in the Security policy are defined by the Symantec Enterprise Firewall authorised Administrator, and allow the parameters stated in paragraph 112 to be set for unauthenticated traffic flow.

117 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.

118 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.

119 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.

120 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.

121 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.

122 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.

123 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.

124 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.

125 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.

126 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.

127 Traffic flows in which the subject specifies the route the information flow shall flow to its destination shall be denied.

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

Authenticated

129 The TSF shall enforce authenticated information flow based on the following attributes:

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.

130 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 S/key authentication.

131 Rules in the Security policy are defined by the Symantec Enterprise Firewall authorised Administrator, and allow the parameters stated in paragraph 127 to be set for each authenticated traffic flow.

132 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 S/Key authentication for FTP and Telnet.

133 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.

134 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

135 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.

136 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 S/Key authentication for FTP and Telnet.

137 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.

138 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.

139 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.

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

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

142 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.

143 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.

144 Traffic flows in which the subject specifies the route the information flow shall flow to its destination shall be denied.

145 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.

6.2 Identification and Strength of Function Claim for IT security Functions

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

147 A specific strength of function metric is defined for the following requirement: FIA_UAU.4. The Strength of function shall be demonstrated for the authentication mechanism. The single-use authentication mechanisms must demonstrate SOF-Medium, as defined in Part 1 of the CC.

6.3 Assurance Measures

148 Deliverables will be produced to comply with the Common Criteria Assurance Requirements for EAL4. 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

149 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

150 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
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																				✓

Table 8-1 Mapping of Objectives to Threats and Assumptions

151 **O.IDAUTH**

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

153 **O.SINUSE**

154 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.

155 **O.MEDIAT**

156 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.

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

158 **O.SECSTA**

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

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

161 **O.SELPRO**

162 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.

163 The operating system provides part of the protection for the TOE.

164 **O.AUDREC**

165 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.

166 The audit trail is stored on the operating system.

167 **O.ACCOUN**

168 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.

169 The operating system performs part of the audit functions.

170 **O.SECFUN**

171 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.

172 The operating system authenticates and identifies authorised administrators.

173 **O.LIMEXT**

174 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.

175 The operating system authenticates and identifies authorised administrators.

176 **O.EAL**

177 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.

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

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

180 **OE.PHYSEC**

181 This environmental security objective is necessary to counter the assumption: A.PHYSEC because it requires that the TOE is physically secure.

182 **OE.LOWEXP**

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

184 **OE.GENPUR**

185 This environmental security objective is necessary to counter the assumption: A.GENPUR because it requires that the TOE does not provide general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) or storage repository capabilities.

186 **OE.PUBLIC**

187 This environmental security objective is necessary to counter the assumption: A.PUBLIC because it requires that the TOE does not host public data.

188 **OE.NOEVIL**

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

190 **OE.SINGEN**

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

192 **OE.DIRECT**

193 This environmental security objective is necessary to counter 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.

194 **OE.NOREMO**

195 This environmental security objective is necessary to counter the assumption: A.NOREMO because it requires that human users who are not authorised administrators can not access the TOE remotely from the internal or external networks.

196 **OE.GUIDAN**

197 This non-IT 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, installed, administered, and operated in a secure manner.

198 **OE.ADMTRA**

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

OE.REMOS

200 This non-IT security objective is necessary to counter the assumption: A.REMOS because it requires that the operating system is delivered to the user's site, installed and administered in a secure manner.

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

202 **T.NOAUTH**

203 The TOE authenticates all FTP and Telnet attempts from an internal or external network. Only authenticated connections are allowed between the networks. A SOF metric for the authentication is described in Section 5.4.

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

205 **T.SELPRO**

206 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.

207 **T.AUDFUL**

208 The TOE provides the administrator with Read Only access to the audit data through the SRMC / RCU. 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. The authorised user of the machine must ensure that the data is archived and that the storage space does not become exhausted.

209 The operating system provides the administrator with Read Only access to the audit data through the event viewer. The authorised user of the machine must ensure that the data is archived and that the storage space does not become exhausted.

210 **T.AUDACC**

211 The TOE through the SRMC / RCU 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.

212 The 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.

213 **T.LOWEXP**

214 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.

215 The operating system provides part of the security to ensure that the threat of malicious attack is low, in particular no other applications should be loaded onto the operating system.

216 **T.REPLAY**

217 The TOE ensures that users using FTP or Telnet are authenticated by means of S/Key authentication that generates a one-time password. All attempts are audited.

218 Paragraph removed.

8.3 Security Requirements Rationale

8.3.1 Security Requirements are appropriate

219 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.4
O.SINUSE	FIA_UAU.4
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
O.SECSTA	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.3, FPT_RVM.1,

Objective	Security Functional Requirement(s)
	FPT_SEP.1, FAU_STG.4, FMT_MOF.1(1), FMT_MOF.1(2), FMT_SMF.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
O.LIMEXT	FMT_MOF.1(1), FMT_MOF.1(2), FMT_SMF.1
O.EAL	FIA_UAU.4, 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

Table 8-2 Mapping of Objectives to SFRs

220 **O.EAL**

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

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

223 This component was chosen to ensure that Single-use authentication mechanism is used appropriately in all attempts to authenticate at the TOE from an internal or external network. A SOF metric for this requirement is defined in section 5.4 to ensure that the mechanisms are of adequate probabilistic strength to protect against authentication data compromise. This component traces back to and aids in meeting the following objective: O.SINUSE and O.IDAUTH.

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

225 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.

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

227 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.

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

229 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.

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

231 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.

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

233 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.

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

235 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.

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

237 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.

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

239 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.

240 **FMT_MSA.3 Static attribute initialization**

241 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.

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

243 This component ensures that 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.

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

245 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.

246 **FPT_SEP.1 TSF domain separation**

247 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.

248 **FAU_GEN.1 Audit data generation**

249 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.

250 **FAU_SAR.1 Audit review**

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

252 **FAU_SAR.3 Selectable audit review**

253 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.

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

255 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.

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

257 This component ensures that the TSF restricts the ability of the TOE start up and shut down operation and multiple 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.

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

259 This component was to ensure 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

260 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, FAU_STG.4, FMT_MOF.1(2), FMT_SMF.1, FIA_UAU.2, FIA_UID.2
O.SELPRO	FPT_SEP.1, FAU_STG.4, FAU_STG.1, FIA_UAU.2, FIA_UID.2
O.AUDREC	FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FPT_STM.1
O.ACCOUN	FAU_GEN.1, FPT_STM.1
O.SECFUN	FAU_STG.1, FAU_STG.4, FMT_MOF.1(2),

Objective	Security Functional Requirement(s)
	FMT_SMF.1, FIA_UAU.2, FIA_UID.2
O.LIMEXT	FMT_MOF.1(2), FMT_SMF.1, FIA_UAU.2, FIA_UID.2
O.EAL	FPT_SEP.1, FAU_STG.1, FAU_STG.4, FMT_MOF.1(2), FAU_GEN.1, FPT_STM.1, FAU_SAR.1, FAU_SAR.3, FMT_SMF.1, FIA_UAU.2, FIA_UID.2
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

261 **O.EAL**

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

263 **FPT_SEP.1 TSF domain separation**

264 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, O.SECSTA, OE.LOWEXP, OE.GENPUR, OE.PUBLIC, OE.SINGEN AND OE.NOREMO.

265 **FAU_GEN.1 Audit data generation**

266 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.

267 **FAU_SAR.1 Audit review**

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

269 **FAU_SAR.3 Selectable audit review**

270 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.

271 **FPT_STM.1 Reliable time stamps**

272 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.

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

274 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.

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

276 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.

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

278 This component was to ensure 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.

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

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

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

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

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

284 This component ensures that before anything occurs on behalf of a user, the user's identity is identified via the operating system to the TOE. This component traces back to and aids in meeting the following objectives: 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**
FIA_UAU.4[ii]	None	None
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.

[ii] A SOF claim is made for FIA_UAU.4, see Section 5.4.

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
		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
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	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	None	None

Table 8-4 Mapping of SFR Dependencies

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

286 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.PHYSIC and OE.NOREMO only an authorised administrator will have physical access to the TOE. Human users, including authorised administrators can not access the TOE remotely from the internal or external networks. The dependency on FMT_SMR.1 is therefore regarded as satisfied.

287 A SOF claim is made for FIA_UAU.4, see Section 5.4.

8.3.4 IT security functions satisfy SFRs

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

IT Function	Security Functional Requirement(s)
Identification and Authentication	
86	FIA_UAU.4[iii]
87	FAU_GEN.1
Management and Security[iv]	
88	FMT_MSA.1(1), FMT_SMF.1
89	FMT_MSA.1(2) , FMT_SMF.1
90	FMT_MSA.1(3) , FMT_SMF.1
91	FMT_MSA.1(4) , FMT_SMF.1
92	FMT_MSA.3
93	FMT_MOF.1(1) , FMT_SMF.1
94	FMT_MOF.1 (2) FMT_SMF.1
95	FMT_MSA.3
Audit	
96	FAU_GEN.1
97	FAU_GEN.1
98	FAU_GEN.1

[iii] A SOF claim is made for FIA_UAU.4, see Section 5.4.

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

99	FAU_SAR.1
100	FAU_SAR.3, FAU_SAR.1
101	FAU_STG.4
Protection of TOE Security Functions	
102	FPT_SEP.1
103	FPT_RVM.1
104	FPT_RVM.1
105	FPT_SEP.1
User Data Protection[v]	
106	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
107	FDP_IFC.1 (2), FDP_IFF.1 (1)
108	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
109	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
110	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
111	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
112	FDP_IFC.1 (1), FDP_IFC.1 (2)
113	FDP_IFF.1 (1) , FDP_IFF.1 (2)
114	FDP_IFF.1 (1)

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

115	FDP_IFC.1 (1)
116	FDP_IFF.1 (1)
117	FDP_IFF.1 (1)
118	FDP_IFF.1 (1)
119	FDP_IFF.1 (1)
120	FDP_IFF.1 (1)
121	FDP_IFF.1 (1)
122	FDP_IFF.1 (1)
123	FDP_IFF.1 (1)
124	FDP_IFF.1 (1)
125	FDP_IFF.1 (1)
126	FDP_IFF.1 (1)
127	FDP_IFF.1 (1)
128	FDP_IFF.1 (1)
129	FDP_IFF.1 (2)
130	FDP_IFC.1 (2)
131	FDP_IFF.1 (2)
132	FDP_IFF.1 (2)
133	FDP_IFF.1 (2)
134	FDP_IFF.1 (2)
135	FDP_IFF.1 (2)
136	FDP_IFF.1 (2)
137	FDP_IFF.1 (2)
138	FDP_IFF.1 (2)

139	FDP_IFF.1 (2)
140	FDP_IFF.1 (2)
141	FDP_IFF.1 (2)
142	FDP_IFF.1 (2)
143	FDP_IFF.1 (2)
144	FDP_IFF.1 (2)
145	FDP_IFF.1 (2)

Table 8-5 Mapping of IT Functions to SFRs

289 A SOF claim is made for FIA_UAU.4, see Section 5.4.

290 To perform searches and sorts on the audit database the administrator will be able to use the SRMC / RCU 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 amount of data to be lost is none. So that requirement FAU_STG.4 is met.

291 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.

292 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

293 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 Strength of Function claims are appropriate

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

295 Products such as the Symantec Enterprise Firewall 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's probabilistics and premutational mechanisms will be appropriate to a number of deployments, in both government and other organisations.

8.3.7 Justification of Assurance Requirements

296 EAL4 is defined in the CC as “methodically designed, tested and reviewed”.

297 Products such as Symantec Enterprise Firewall 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.

8.3.8 Assurance measures satisfy assurance requirements

298 Assurance measures in the form of deliverables will be produced to meet EAL4 assurance requirements.

299 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.

300 The assurance requirements identified in the table are those required to meet the CC assurance level EAL4. 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 EAL 4 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
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

Assurance Measures	Assurance Requirements Met by Assurance Measure	
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 Symantec Enterprise Firewall 7.0.4	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
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	
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 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
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

Assurance Measures	Assurance Requirements Met by Assurance Measure	
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.