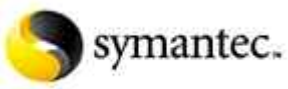

Security Target

for

Symantec Enterprise Firewall

Version 7.0

For Windows NT

Reference: T349\ST

May 2002

Version: 2.0

Europe:
Symantec (UK) Ltd
Apex House
4A-10 West Street
Epsom
Surrey KT18 7RG
United Kingdom

USA:
Symantec Corporation
266 Second Avenue
Waltham, MA 02451
USA

Copyright notice

DOCUMENT AUTHORISATION

Document Title	Security Target for Symantec Enterprise Firewall Version 7.0 for Windows NT

Reference	**Version**	**Date**	**Description**
ST	1.0	December 2000	Initial Issue
ST	2.0	May 2002	Final Issue

Contents

1 INTRODUCTION TO THE SECURITY TARGET 9

1.1 SECURITY TARGET IDENTIFICATION 9
1.2 SECURITY TARGET OVERVIEW 9
1.3 CC CONFORMANCE CLAIM 9

2 TOE DESCRIPTION 10

2.1 OVERVIEW OF THE SYMANTEC ENTERPRISE FIREWALL 10
2.2 SCOPE AND BOUNDARIES OF THE EVALUATED CONFIGURATION 12
2.2.1 [PP] EAL 2 Scope 12
2.2.2 EAL 4 Scope 12
2.2.3 Physical Scope 13
2.2.4 Outside of the Scope 14

3 SECURITY ENVIRONMENT 15

3.1 INTRODUCTION 15
3.2 THREATS 15
3.2.1 Threats countered by the TOE 15
3.2.2 Threats countered by the Operating Environment 17
3.3 ORGANIZATIONAL SECURITY POLICIES 18
3.4 ASSUMPTIONS 18

4 SECURITY OBJECTIVES 19

4.1 TOE SECURITY OBJECTIVES 19
4.1.1 IT Security Objectives 19
4.2 ENVIRONMENT SECURITY OBJECTIVES 21
4.2.1 IT Security Objectives 21
4.2.2 Non-IT Security Objectives 21

5 IT SECURITY REQUIREMENTS 22

5.1 EAL2 TOE SECURITY REQUIREMENTS 22
5.1.1 TOE Security Functional Requirements 22
5.2 EAL2 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 38
5.3 EAL 4 TOE SECURITY REQUIREMENTS 38
5.3.1 TOE Security Functional Requirements 38
5.4 EAL4 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 49
5.5 TOE SECURITY ASSURANCE REQUIREMENTS 55
5.6 STRENGTH OF FUNCTION CLAIM 57

6 TOE SECURITY FUNCTIONS 58

6.1.1 Identification and Authentication Function 58
6.1.2 Management and Security Function 58
6.1.3 Audit Function 59
6.1.4 Protection of TOE security Functions 60
6.1.5 User Data Protection Function 60
6.1.6 [PP] EAL2 Functions 65
6.2 IDENTIFICATION AND STRENGTH OF FUNCTION CLAIM FOR IT SECURITY FUNCTIONS 67
6.3 ASSURANCE MEASURES 67

7 PROTECTION PROFILES CLAIMS 68

7.1 PP TOE CONFIGURATION 68
7.2 PP ORGANIZATIONAL SECURITY POLICIES 69
7.3 PP THREATS OUTSIDE THE SCOPE OF THE TOE 69
7.4 PP SECURITY OBJECTIVES OUTSIDE THE SCOPE OF THE TOE 69
7.5 PP NON-IT SECURITY OBJECTIVES OUTSIDE THE SCOPE OF THE TOE 69
7.6 PP SFRS OUTSIDE THE SCOPE OF THE EVALUATION 69
7.7 PP SFR REFINEMENTS 71
7.8 PP TOE SECURITY FUNCTIONS 71
7.9 [PP] SPECIFIC IT SECURITY FUNCTIONS SATISFY SFRS 73

8 RATIONALE 75

8.1 INTRODUCTION 75
8.2 SECURITY OBJECTIVES FOR THE TOE RATIONALE 75
8.2.1 EAL2 Security Objectives for the TOE Rationale 75
8.2.2 EAL4 Security Objectives for the TOE Rationale 75
8.3 SECURITY REQUIREMENTS RATIONALE 78
8.3.1 Requirements are appropriate 78
8.3.2 EAL4 Security Requirements are appropriate 78
8.3.3 Security Requirement dependencies are satisfied 83
8.3.4 IT security functions satisfy SFRs 85
8.3.5 IT security functions mutually supportive 89
8.3.6 Strength of Function claims are appropriate 89
8.3.7 Justification of Assurance Requirements 89
8.3.8 Assurance measures satisfy assurance requirements 90

REFERENCES

[CC]	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (aligned with ISO 15408).
[PP]	U.S. Department of Defence Application-Level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, 22 June 2000
[FIPS-PUB 46]	Federal Information Processing Standard Publication (FIPS-PUB) 46-2, Data Encryption Standard (DES), December 1993
[FIPS-PUB 81]	Federal Information Processing Standard Publication (FIPS-PUB) 81, DES Modes of Operation, December 1980
[FIPS-PUB 140]	Federal Information Processing Standard Publication (FIPS-PUB) 140-1, Security Requirements for Cryptographic Modules, dated, January 11, 1994

GLOSSARY AND TERMS

Authentication data	Information used to verify the claimed identity of a user.
Authorised User	A user 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.
FIPS	Federal Information Processing Standard
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
Raptor	Symantec Enterprise Firewall
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 for Windows NT, issue 1.9.

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 unauthorized 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. The TOE meets the requirements of the U.S. Department of Defense Application-Level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, 22 June 2000 [PP].

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 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 TCP/IP protocol stack. 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.

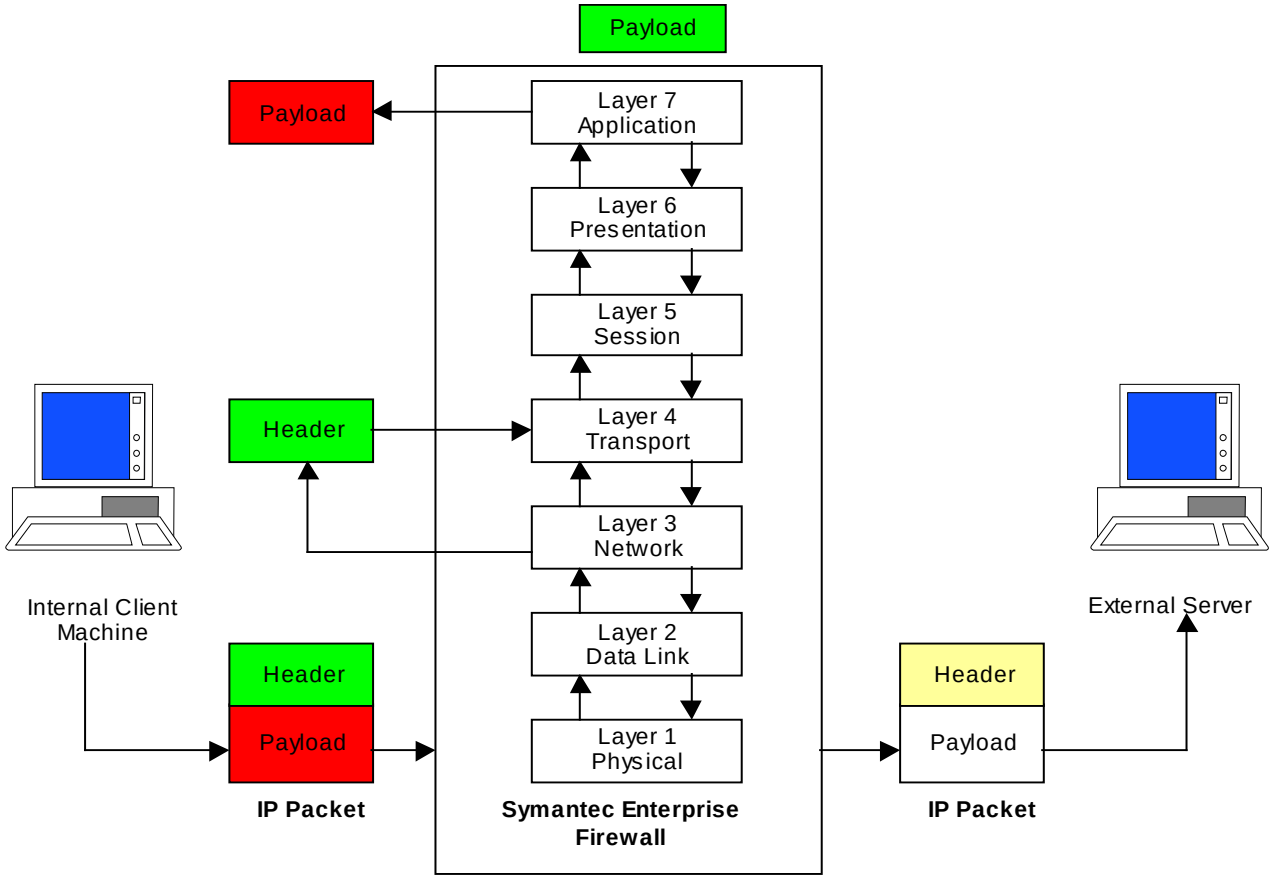

Diagram 2-1: Packet Flow through the Symantec Enterprise Firewall

9 The Target of Evaluation (TOE) consists of two physical components, the firewall itself and the Symantec Raptor Management Console (SRMC), 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 3 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	SQL*Net V2	POP Mail	IP
Gopher	NNTP	POP3	RealAudio	TCP
RTSP	NTP			

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

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

HTTP	Gopher	NNTP	SQL*Net V2	DNS	NTP
TELNET	SMTP	FTP	Ping	RealAudio	

2.2 Scope and Boundaries of the Evaluated Configuration

16 Within this Security Target there are two scopes for the TOE. One is in relation to the [PP] EAL2 and the other is for EAL4.

2.2.1 [PP] EAL 2 Scope

17 The TOE configuration consists of:

- The firewall itself;
- The Symantec Raptor Management Console (SRMC), 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;
- **Windows NT 4.0 Operating system with Service Pack 6a**. The functions that are included are:
  - Utilities and Authentication functions to provide authorized users with user ids and passwords and to associate the authorized users with the administrator group. The authentication function ensures that only authorized users have access to the TOE.
  - Protection of processes by ensuring all process are allocated separate memory locations within RAM and flushing the sensitive memory prior to re-allocation.
  - Auditing logs the authentication attempts, including the authentication failure, and access to the user management function (mentioned above). The logs are viewed through the event viewer. The NT Access Control Subsystem protects the logs.
  - NT System Time is used for the NT audit functions, as well as the TOE audit function.

2.2.2 EAL 4 Scope

18 For EAL4 the TOE configuration excludes Windows NT 4.0 Operating system with Service Pack 6a.

19 Windows NT Operating system with Service Pack 6a for EAL4 is part of the IT environment.

2.2.3 Physical Scope

2.2.3.1 EAL2

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

Software	**Symantec Enterprise Firewall Version 7.0 with Symantec Raptor Management Console.**
Operating System	**Microsoft Windows NT 4.0 operating system with Service Pack 6a.** **The functions are:** • **Utilities and Authentication** • **User Management** • **Protection of processes** • **Auditing logs** • **NT System Time**

Table 2-1: EAL2 TOE Component Identification

21 The required IT environment for the EAL2 TOE is identified in Table 2-2.

Software	Microsoft Internet Explorer 6.0 for SRMC
Hardware	Pentium III 1 GHz, 256 MB, 20 GigaBytes A minimum of 2 Network Interface card from the Symantec approved list. For the evaluation 3 network interface cards will be used.

Table 2-2: IT Environment for the EAL2 TOE

2.2.3.2 EAL4

22 The physical scope of the EAL4 TOE is identified in Table 2-3.

Software	**Symantec Enterprise Firewall Version 7.0 with Symantec Raptor Management Console.**

Table 2-3: EAL 4TOE Component Identification

23 The required IT environment for the EAL4 TOE is identified in Table 2-4.

Operating System	Microsoft Windows NT 4.0 operating system with Service Pack 6a.
Software	Microsoft Internet Explorer 6.0 for SRMC
Hardware	Pentium III 1 GHz, 256 MB, 20 GigaBytes A minimum of 2 Network Interface card from the Symantec approved list. For the evaluation 3 network interface cards will be used.

Table 2-4: EAL 4 IT Environment for the TOE

2.2.4 Outside of the Scope

24 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;
- Remote Administration;
- User Authentication by one-time password, and SecurID Authentication engine for mobile users to access services in the protected domain;
- Setup Wizard;
- H.323 Connections;
- Forward Filtering.

3 Security Environment

3.1 Introduction

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

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

2. organisational security policies the TOE must comply with;

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

3.2 Threats

26 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

27 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).

28 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.

29 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.

[PP] EAL2 Certification

30 The threats that must be countered by the EAL2 TOE are listed in the [PP] Section 3.2.1.

31 **The threat T.PROCOM is not applicable, as Remote Administration is outside the scope of the TOE**.

EAL4 Certification

32 The threats that must be countered by the EAL4 TOE are listed in the [PP] Section 3.2.1. **The threat T.PROCOM is not applicable, as Remote Administration is outside the scope of the TOE**.

33 The following table identifies the threats listed in [PP] Section 3.2.1 that are partially met by the TOE at EAL4.

[PP] Threats Partially met by the TOE at EAL4	**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.REPEAT	This is partially met by the Operating System, as authentication is performed by the Operating System. However, the TOE performs S/Key authentication.
T.REPLAY	This is partially met by the Operating System, as authentication is performed by the Operating System.
T.LOWEXP	As the part of the security of TOE is performed by the

	operating system. This threat is partially met by the Operating System.

Table 3-1 [PP] Threats partially met by the TOE at EAL4

3.2.2 Threats countered by the Operating Environment

[PP] EAL2 Certification

34 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 at EAL2 are listed in the [PP] Section 3.2.2.

EAL4 Certification

35 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 at EAL4 are listed in the [PP] Section 3.2.2.

36 The following table identifies the threats listed in [PP] Section 3.2.1 that are partially met by the operating environment at EAL4.

[PP] Threats Partially met by Operating Environment at EAL4	**Reasons**
T.NOAUTH	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.REPEAT	This is partially met by the Operating System, as authentication is performed by the Operating System. However, the TOE performs S/Key authentication.
T.REPLAY	This is partially met by the Operating System, as authentication is performed by the Operating System.
T.LOWEXP	As the part of the security of TOE is performed by the operating system. This threat is partially met by the Operating System.

Table 3-2 [PP] Threats partially met by Operating Environment at EAL4

3.3 Organizational Security Policies

37 US Federal agencies are required to protect sensitive but unclassified information with cryptography. Products and systems compliant with the [PP] are expected to utilize cryptographic modules for remote administration compliant with FIPS PUB 140-1 (level 1).

P.CRYPTO Triple DES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1) [5].

38 **This Organizational Security Policy is not applicable for EAL2 and EAL4, as Remote Administration is outside the scope of the TOE**.

3.4 Assumptions

39 The conditions, which are assumed to exist in the operational environment for EAL2 and EAL4, are listed in the [PP] Section 3.1. The Assumption A.REMACC is not applicable for EAL2 and EAL4, as Remote Administration is outside the scope of the TOE. The following additional assumption is listed below.

A.WINNT	The Windows NT 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

40 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.

[PP] EAL2 Certification

41 The IT security objectives are listed in [PP] Section 4.1. **The security objective O.ENCRYP is not applicable, as Remote Administration is outside the scope of the TOE.**

EAL4 Certification

42 The IT security objectives are listed in [PP] Section 4.1. The following table identifies the IT Security objectives listed in [PP] Section 4.1 that are partially met by the IT environment at EAL4. **The security objective O.ENCRYP is not applicable, as Remote Administration is outside the scope of the TOE.**

Partially met by IT Environment at EAL4	Reasons
O.IDAUTH	At EAL4 authentication of users is provided by the Operating System.
O.SINUSE	At EAL4 authentication of users is provided by the Operating System.
O.SECSTA	At EAL4, part of the security of the TOE is provided by the Operating System.
O.SELPRO	At EAL4, part of the security of the TOE is provided by the Operating System.
O.AUDREC	The Operating System audits some of the information at EAL4 and therefore provides a

	means to read that information.
O.ACCOUN	The Operating System audits some of the information at EAL4.
O.SECFUN	At EAL4, part of the security of the TOE is provided by the Operating System.
O.LIMEXT	At EAL4 authentication of users is provided by the Operating System.
O.EAL	At EAL4, part of the security of the TOE is provided by the Operating System.

Table 4-1 [PP] IT Security Objective partially met by IT Environment at EAL4

4.2 Environment Security Objectives

4.2.1 IT Security Objectives

43 For the [PP] EAL2, there are no IT security objectives for the environment.

44 [ST] Table 4-1 identifies the IT security objectives that are partially met by the IT environment at EAL4.

4.2.2 Non-IT Security Objectives

45 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. These are listed in [PP] Section 4.2. The following additional objective is listed below.

O.WINNT	The Windows NT operating system will be delivered, installed and administered in a secure manner.

46 **The Non-IT security objective O.REMAC is not applicable, as Remote Administration is outside the scope of the TOE.**

5 IT Security Requirements

5.1 EAL2 TOE Security Requirements

47 This section provides functional requirements that must be satisfied by a Protection Profile-compliant TOE. These requirements consist of functional components drawn from Part 2 of the CC.

5.1.1 TOE Security Functional Requirements

48 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	
FMT_SMR.1	Security Roles
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_AFL.1	Authentication failure handling
FIA_UAU.2[ii]	User Authentication before any action
FIA_UAU.5	Multiple 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)

[ii] FIA_UAU.2 has been included in this ST as FIA_AFL.1 in the PP has a dependency on FIA_UAU.1.

Functional Components	
FMT_MSA.1	Management of security attributes (4)
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of TSF data (1)
FMT_MTD.1	Management of TSF data (2)
FMT_MTD.2	Management of limits on TSF data
FDP_RIP.1	Subset Residual Information Protection
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable Time Stamps
FAU_GEN.1	Audit Data Generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of Security Functions Behaviour (1)
FMT_MOF.1	Management of Security Functions Behaviour (2)

Table 5-1: Functional Requirements

49 [PP] SFR FCS_COP.1 has been excluded from the above list, as remote administration is outside the scope of the TOE. FIA_UAU.5.2 parts a), b) and d) are also not applicable as remote administration is outside the scope of the evaluation.

50 The following paragraphs are intended to clarify why the functional components in this Security Target are presented in the order outlined in Table 5.1. FMT_SMR.1

is the first component because it defines the authorized administrator role, which appears in a number of the components that follow.

51 The class FIA components are listed after FMT_SMR.1. They describe the identification and authentication policy that all users, both human users and external IT entities, must abide by before being able to use other TOE functions.

52 The order of the class FIA components was chosen on the following basis. Since users are already defined in the Terminology section on [PP] page VI, the Security Target reader is introduced in component FIA_ATD.1 to their security attributes. The next component, FIA_UID.2, forces users to identify themselves to the TOE using the user security attributes of component FIA_ATD.1 before further actions take place. Then, component FIA_AFL.1 describes what results if the user fails to authenticate after some settable number of attempts. Lastly, component FIA_UAU.5 discusses when authentication mechanisms must be used. For the supported user authentication FIA_UAU.5, the SOF shall be demonstrated for the password mechanism such that the probability that authentication data can be guessed is no greater than one in two to the fortieth (2^40).

53 There are two information flow control SFPs, and they are defined after the class FIA components in FDP_IFC.1. Then the policy rules, which must be enforced, as well as the attributes of the entities defined in FDP_IFC.1 are written in FDP_IFF.1. Next, management of the attributes in FDP_IFF.1 are specified in FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3) and FMT_MSA.1(4). Component FMT_MSA.3, which FDP_IFF.1 depends on, follows. As part of the installation and start-up of the TOE, FMT_MSA.3 mandates a default deny policy, which permits no information to flow through the TOE. FMT_MTD.1(1), FMT_MTD.1(2), and FMT_MTD.2 define the management of TSF data. FDP_RIP.1 is listed next, ensuring that resources are cleared before being allocated to hold packets of information at the TOE.

54 Components dealing with the protection of trusted security functions come next. These include components FPT_RVM.1 and FPT_SEP.1.

55 Since FAU_GEN.1 requires recording the time and date when audit events occur, it follows the FPT_STM.1 component that alerts developers that an accurate time and date must be maintained on the TOE. The class FAU requirements follow to define the audit security functions, which must be supported by the TOE. FAU_GEN.1 is the first audit component listed because it depicts all the events that must be audited, including all the information which must be recorded in audit records. The remainder of the class FAU components ensure that the audit records can be read (component FAU_SAR.1), searched and sorted (component FAU_SAR.3), and protected from modification (FAU_STG.1). Lastly,

FAU_STG.4 ensures that the TOE is capable of preventing auditable actions, not taken by an authorized administrator, from occurring in the event that the audit trail becomes full.

56 The last component in the profile is FMT_MOF.1. It appears last because it lists all the functions to be provided by the TOE for use only by the authorized administrator. Almost all of these functions are based on components, which precede it. Thus it is listed last.

57 **FMT_SMR.1 Security roles**

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

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

58 **FIA_ATD.1 User attribute definition**

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;

b) association of a human user with the authorized administrator role;

c) ***Authorised Access Console***].

59 **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.

60 **FIA_AFL.1 Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [a non-zero number determined by the authorised administrator] **of** unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorised TOE IT entity access].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent

the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question.]

61 **FIA_UAU.2 User authentication before any action**[iii]

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.

62 **FIA_UAU.5 Multiple authentication mechanisms**[iv] [v]

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

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:
c) single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user].

63 *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*

[iii] FIA_UAU.2 has been included in this ST as FIA_AFL.1 in the PP has a dependency on FIA_UAU.1.

[iv] FIA_UAU.5.2 point a), b) and d) as described in the [PP] are not applicable as the TOE does not include remote administration. See Paragraph 44 of the [PP]. However, FIA_UAU.5.1 as stated above is correct from a [CC] perspective.

[v] A SOF claim is made for FIA_UAU.5, see Section 5.6.

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.

64 **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].

65 **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.5,
b) information: FTP and Telnet traffic sent through the TOE from one subject to another;
c) operation: initiate service and pass information].

66 **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

[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 PP, 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].

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

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

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the

values of the information flow security attributes, created by the authorized administrator;
• the presumed address of the source subject, in the information, translates to an external network address;
• and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

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.]

67 **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;
- 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.5;

[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 PP, 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].

• all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

• the presumed address of the source subject, in the information, translates to an internal network address;

• and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

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

• the human user initiating the information flow authenticates according to FIA_UAU.5;

• all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

• the presumed address of the source subject, in the information, translates to an external network address; and

• the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

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.]

68 **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 authorized administrator].

69 **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 authorized administrator].

70 **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)] to [the authorized administrator].

71 **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(2)] to [the authorized administrator].

72 **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 [the authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

73 **FMT_MTD.1 Management of TSF data (1)**

FMT_MTD.1.1 The TSF shall restrict the ability to *query*, *modify*, *delete* [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

74 **FMT_MTD.1 Management of TSF data (2)**

FMT_MTD.1.1 The TSF shall restrict the ability to [set] the [the time and date used to form the timestamps in FPT_STM.1.1] to [the

authorized administrator].

75 **FMT_MTD.2 Management of limits of TSF data**

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

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

76 **FDP_RIP.1 Subset residual information protection**

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* [all objects].

77 **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.

78 **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

79 **FPT_STM.1 Reliable time stamps**

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

80 **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 PP/ST, [information specified in column three of Table 5.2].

Functional Component	**Auditable Event**	**Additional Audit Record Contents**
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.5[vi]	Any use of the authentication	The user identities provided to the TOE

[vi] FIA_UAU.5.2 points a), b) and d) are outside the scope of the evaluation.

	mechanism.	
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorized administrator of the users capability to authenticate.**	The identity of the offending user and the authorized administrator
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FCS_COP.1[vii]	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation

Table 5-2: Auditable Event

81 **FAU_SAR.1 Audit review**

FAU_SAR.1.1 The TSF shall provide [an authorized 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.

82 **FAU_SAR.3 Selectable audit review**

[vii] FCS_COP.1 is outside the scope of the evaluation

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].

83 **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.

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

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

85 **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) multiple use authentication functions described in FIA_UAU.5] to [an authorized administrator].

86 **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 authorized administrator].

5.2 EAL2 Security requirements for the IT Environment

87 To meet the requirements for the [PP] and EAL2 assurance level there are no security requirements for the TOE's IT Environment

5.3 EAL 4 TOE Security Requirements

88 The functional security requirements are drawn from [CC] Part 2.

5.3.1 TOE Security Functional Requirements

89 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.5	Multiple 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	
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 5-3: Functional Requirements

FIA_UAU.5 Multiple authentication mechanisms[viiiix]

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

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:
c) single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user.

90 *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*

[viii] FIA_UAU.5.2 point a), b) and d) are not applicable as the TOE does not include remote administration.

[ix] A specific SOF claim is made for FIA_UAU.5 password mechanism, see Section 5.6.

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.

91 **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].

92 **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.5,
b) information: FTP and Telnet traffic sent through the TOE from one subject to another;
c) operation: initiate service and pass information].

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

[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)*

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 security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the

---

component do not add anything significant to the PP, 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].

information, translates to an internal network address;

• and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

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

• all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

• the presumed address of the source subject, in the information, translates to an external network address;

• and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

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.]

94 **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;
- service (i.e., FTP and Telnet);
- security-relevant service command;
- ***Time;***

[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 PP, 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].

- ***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.5;
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

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

- the human user initiating the information flow authenticates according to FIA_UAU.5;
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

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.]

95 **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 authorized administrator].

96 **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 authorized administrator].

97 **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 authorized administrator].

98 **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 authorized administrator].

99 **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 authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

100 **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.

101 **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

102 **FAU_GEN.1 Audit data generation**[x]

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 5.4].

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 PP/ST, [information specified in column three of Table 5.4].

[x] At EAL4 FAU_GEN.1 is partially met by the IT Environment.

Functional Component	Auditable Event	Additional Audit Record Contents
FIA_UAU.5[xi]	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.
FCS_COP.1[xii]	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FMT_MOF.1[xiii]	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation

Table 5-4: Auditable Event

103 **FAU_SAR.1 Audit review[xiv]**

FAU_SAR.1.1 The TSF shall provide [an authorized 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.

104 **FAU_SAR.3 Selectable audit review[xv]**

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

a) [user identity;

[xi] FIA_UAU.5.2 points a), b) and d) are outside the scope of the evaluation.
[xii] FCS_COP.1 is outside the scope of the evaluation
[xiii] FMT_MOF.1 is partially met by the environment.
[xiv] FAU_SAR.1 is partially met by the environment.

[xv] FAU_SAR.3 is partially met by the environment.

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

105 **FAU_STG.4 Prevention of audit data loss[xvi]**

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

106 **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) multiple use authentication functions described in FIA_UAU.5] to [an authorized administrator].

107 **FMT_MOF.1 Management of security functions behavior (2)[xvii]**

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 authorized administrator].

5.4 EAL4 Security requirements for the IT Environment

108 For the assurance level EAL4, this section details the IT security requirements that are either partially or fully met by the IT environment of the TOE. Table 5-5 lists the IT security requirements to be provided by the IT environment:

[xvi] FAU_STG.4 is partially met by the environment
[xvii] FMT_MOF.1 (2) is partially met by the environment

Functional Components		Partially / Fully met by the IT environment
FMT_SMR.1	Security Roles	**Fully**
FIA_ATD.1	User attribute definition	**Fully**
FIA_UAU.2	User Authentication before any action[xviii]	**Fully**
FIA_UID.2	User identification before any action	**Fully**
FIA_AFL.1	Authentication Failure Handling	**Fully**
FMT_MTD.1	Management of TSF data (1)	**Fully**
FMT_MTD.1	Management of TSF data (2)	**Fully**
FMT_MTD.2	Management of limits of TSF data	**Fully**
FDP_RIP.1	Subset Residual Information Protection	**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 behaviour (2)	**Partially**

[xviii] FIA_UAU.2 has been included in this ST as FIA_AFL.1 in the PP has a dependency on FIA_UAU.1.

Functional Components		Partially / Fully met by the IT environment
	behavior (2)	

Table 5-5: IT Security Requirements of the Environment

109 **FMT_SMR.1 Security roles**

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

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

110 **FIA_ATD.1 User attribute definition**

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;

b) association of a human user with the authorized administrator role;

c) ***Authorised Access Console***].

111 **FIA_UAU.2 User authentication before any action**[xix]

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.

112 **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.

[xix] FIA_UAU.2 has been included in this ST as FIA_AFL.1 in the PP has a dependency on FIA_UAU.1.

113 **FIA_AFL.1 Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [a non-zero number determined by the authorised administrator] **of** unsuccessful authentication attempts occur related to [authorised TOE administrator access or authorised TOE IT entity access].

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

114 **FMT_MTD.1 Management of TSF data (1)**

FMT_MTD.1.1 The TSF shall restrict the ability to *query*, *modify*, *delete* [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

115 **FMT_MTD.1 Management of TSF data (2)**

FMT_MTD.1.1 The TSF shall restrict the ability to [set] the [the time and date used to form the timestamps in FPT_STM.1.1] to [the authorised administrator].

116 **FMT_MTD.2 Management of limits of TSF data**

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

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

117 **FDP_RIP.1 Subset residual information protection**

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* [all objects].

118 **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

119 **FPT_STM.1 Reliable time stamps**

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

120 **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 5.6].

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 5.6].

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

Table 5-6 Auditable Events

121 **FAU_SAR.1 Audit review**

FAU_SAR.1.1 The TSF shall provide [an authorized 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.

122 **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) ranges of dates;
c) ranges of times].

123 **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.

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

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

125 **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 authorized administrator].

5.5 TOE Security Assurance Requirements

126 The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL4 level of assurance, and the U.S. Department of Defense Application-Level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, 22 June 2000 [PP]. 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

Assurance Class	Assurance Components	
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_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

Assurance Class	Assurance Components	
	AVA_VLA.2	Independent vulnerability analysis

Table 5-7: Assurance Requirements: EAL4

127 Further information on these assurance components can be found in [PP] section 5.1.2 and in [CC] Part 3.

5.6 Strength of Function Claim

128 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.

129 For the supported user authentication FIA_UAU.5, the SOF shall be demonstrated for the password mechanism such that the probability that authentication data can be guessed is no greater than one in two to the fortieth (2^40).

130 For a rationale for this selected level, see [PP] section 6.3 of the rationale. For a justification of the Strength of Function claim see [ST] 8.3.6.

6 TOE Security Functions

131 This section describes the security functions provided by the TOE (both for the [PP] EAL2 and EAL4 scopes) to meet the security functional requirements specified for the Symantec Enterprise Firewall in Section 5.1. Sections 6.1.1 – 6.1.5 are specifically on the Symantec Enterprise Firewall and are for EAL2 and EAL4, while Section 6.1.6 is concerned with the Windows NT and are specifically for EAL2 only.

6.1.1 Identification and Authentication Function

132 Authorized 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 [ST] Section 5.6.

133 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

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

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

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

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

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

139 The authorized 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) Multiple use authentication’s functions.

140 The authorized 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.

141 The authorized 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

142 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.

143 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.

144 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.

145 The authorized administrator has read access only to all audit trail data through the controlled interface SRMC logfile window.

146 The authorized administrator via the SRMC 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.

147 Archiving is a manual process that is performed on monthly basis to text files. The files are retained as long as there is space available. The authorized 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

148 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.

149 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.

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

151 The Time range template function of the Symantec Enterprise Firewall 7.0 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 Symantec Raptor Management Console (SRMC).

6.1.5 User Data Protection Function

152 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).

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

154 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.

155 The security policy rules are non-order dependent.

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

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

HTTP	UDP	FTP	Ping	DNS
TELNET	SMTP	SQL*Net V2	POP Mail	IP
Gopher	NNTP	POP3	RealAudio	TCP
RTSP	NTP			

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

HTTP	Gopher	NNTP	Ping	DNS	NTP
TELNET	SMTP	FTP	SQL*Net V2	RealAudio	

159 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

160 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.

161 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.

162 Rules in the Security policy are defined by the Symantec Enterprise Firewall authorized Administrator, and allow the parameters stated in paragraph 159 to be set for unauthenticated traffic flow.

163 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 authorized administrator are permitted.

164 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.

165 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.

166 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.

167 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.

168 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.

169 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.

170 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.

171 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.

172 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.

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

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

Authenticated

175 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.

176 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.

177 Rules in the Security policy are defined by the Symantec Enterprise Firewall authorized Administrator, and allow the parameters stated in paragraph 174 to be set for each authenticated traffic flow.

178 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.

179 Traffic flows from an internal network to another connected network shall only be permitted if all the information security attribute values created by the authorized administrator are permitted.

180 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

181 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.

182 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.

183 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.

184 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.

185 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.

186 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.

187 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.

188 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.

189 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.

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

191 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.

6.1.6 [PP] EAL2 Functions

192 The following functions are specific to the [PP] and are performed by the NT operating system.

Authentication

193 Windows NT authenticates and identifies human users as authorized administrators. Windows NT associates authorized administrators by user identification, password and administrator users group. An authorized administrator may set the authentication attempts for the user accounts. An authorized administrator gains access to TOE only after successful authentication and identification through Windows NT as an authorized administrator.

194 The authorized administrator has the ability to query, modify, delete and assign user attributes.

195 An authorized administrator has the ability to configure the number of authentication failures. After a configurable number of unsuccessful authentication attempts human users are locked out. An authorized administrator in Windows NT using the built in Windows NT Administrator account is able to unlock the account of a human associated to the administrator group.

Management

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

a) Audit management; and

b) Backup and restore for TSF data, and audit trail data.

Protection of TOE Security Functions

197 Within the Windows NT environment all processes are allocated separate memory locations within the RAM. Whenever sensitive memory is re-allocated it is flushed of data prior to re-allocation. These processes are routinely terminated to ensure clean memory

Audit

198 Windows NT is able to generate an audit record for the start-up and shutdown of the audit functions and the following auditable events.

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

Table 6-1 Auditable Events

199 The Window NT logs are viewed searched and sorted through the Windows NT Management module. Windows NT shall record the following for these events:

- Date and time of event;
- Type of event;
- Subject identity,
- Success or failure of the event;
- Column three of additional audit record contents

200 Modifications to the content of the audit trail are not permitted. The authorized administrator has the ability read and delete all audit trail data through the controlled interface Event viewer window.

201 Archiving is a manual process that is performed on the text files. The authorized administrator has the ability to set the Event Log settings not to overwrite events and for the log to be manually cleared.

Time

202 The time used by the audit function is taken from the Window NT system time. The authorized administrator has the ability to set the time and date.

6.2 Identification and Strength of Function Claim for IT security Functions

203 This Security Target claims that the general strength of the security functions provided by the TOE is SOF-Medium. The mechanisms to which this claim relates are defined in [PP] 5.1.1 paragraph 25 -27.

6.3 Assurance Measures

204 Deliverables will be produced to comply with the Common Criteria Assurance Requirements for EAL4. Table 8-5 maps the deliverables to the assurance requirements.

7 Protection Profiles Claims

205 The Symantec Enterprise Firewall claims compliance with the US Application Level Firewall Protection Profile for Basic Robustness Environments [PP].

206 The Symantec Enterprise Firewall claims to meet Assurance requirements EAL4, while the US Application Firewall Protection Profile for Basic Robustness Environments is for Assurance requirement EAL2. The evaluation is for Assurance Level EAL4 with the inclusion of additional Security Functional Requirements to ensure completeness of the EAL2 [PP].

7.1 PP TOE Configuration

207 The TOE configuration consists of:

- The firewall itself;
- The Symantec Raptor Management Console (SRMC), which is used to manage and administer the firewall 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;
- Denial of Service attacks protection;
- Automatic port blocking.
- **Windows NT 4.0 Operating system with Service Pack 6a**. The functions that are included are:
  - Utilities and Authentication functions to provide authorized users with user ids and passwords and to associate the authorized users with the administrator group. The authentication function ensures that only authorized users have access to the TOE.
  - User Management allows an authorized user to set the authentication policy for all users.
  - Protection of processes by ensuring all process are allocated separate memory locations within RAM and flushing the sensitive memory prior to re-allocation.
  - Auditing logs the authentication attempts, including the authentication failure. Access to the user management function. The logs are viewed through the event viewer. The NT Access Control Subsystem protects the logs.

– NT System Time is used for the NT audit functions, as well as the TOE audit function.

7.2 PP Organizational Security Policies

208 P.CRYPTO Triple DES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1) [5].

209 P.CRYPTO is not applicable, as Remote Administration is outside the scope of the evaluation.

7.3 PP Threats Outside the scope of the TOE

210 The threat T.PROCOM is not applicable, as Remote Administration is outside the scope of the TOE.

7.4 PP Security Objectives outside the scope of the TOE

211 The security objective O.ENCRYP is not applicable, as Remote Administration is outside the scope of the TOE.

7.5 PP Non-IT Security Objectives Outside the Scope of the TOE

212 The Non-IT security objective O.REMAC is not applicable, as Remote Administration is outside the scope of the TOE.

7.6 PP SFRs Outside the Scope of the Evaluation

213 The following SFRs are not applicable, as remote administration has been excluded from the evaluation:

FIA_UAU.5.2 a), b) and d)	Multiple Authentication Mechanisms
FCS_COP.1	Cryptographic Operation

214 **FIA_UAU.5 Multiple authentication mechanisms**

215 The following parts of FIA_UAU.5 are not applicable as the sections relate to remote administration:

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

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

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

c) reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator].

216 *Application Note: TOEs that do not provide capabilities for authorized administrators to access the TOE remotely from either an internal or external network (i.e., for remote administration), or for authorized external IT entities do not have to make such functionality available in order to satisfy this requirement. The intent of this requirement is not to require developers to provide all such capabilities and their associated single-use authentication mechanisms. The requirement applies to those developers that do incorporate such functionality and intend for it to be evaluated.*

217 **FCS_COP.1 Cryptographic operation**

218 Component FCS_COP.1 is a conditional requirement. If the developer allows administration from a remote location outside the physically protected TOE, then evaluation against the Security Target shall require the TOE to meet this component. FCS_COP.1 defines a cryptographic algorithm as well as the key size that must be used. The cryptographic module must be FIPS PUB 140-1 compliant for the reasons stated in Section 3.

219 *Application Note: This requirement is applicable only if the TOE includes the capability for the authorized administrator to perform security functions remotely from a connected network. In this case, Triple DES encryption must protect the communications between the authorized administrator and the TOE, and the*

associated cryptographic module(s) must comply at a minimum with FIPS PUB 140-1 Level 1. The intent of this requirement is not for the evaluator to perform a FIPS PUB 140-1 evaluation: rather, the evaluator will check for a certificate, verifying that the module did complete a FIPS PUB 140-1 evaluation.

7.7 PP SFR refinements

220 The following SFRs were refined further for this Security Target:

FIA_ATD.1	User attribute definition
FDP_IFF.1	Simple Security Attributes (1)
FDP_IFF.1	Simple Security Attributes (2)

7.8 PP TOE Security Functions

221 The following TOE Security Functions are specific to the [PP] EAL2. These are:

Authentication

222 Windows NT authenticates and identifies human users as authorized administrators. Windows NT associates authorized administrators by user identification, password and administrator users group. An authorized administrator may set the authentication attempts for the user accounts. An authorized administrator gains access to TOE only after successful authentication and identification through Windows NT as an authorized administrator.

223 The administrator has the ability to query, modify, delete and assign user attributes.

224 An authorized administrator has the ability to configure the number of authentication failures. After a configurable number of unsuccessful authentication attempts human users are locked out An authorized administrator in Windows NT using the built in Windows NT Administrator account is able to unlock the account of a human associated to the administrator group.

Management

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

a) Audit management; and

b) Backup and restore for TSF data, and audit trail data.

Protection of TOE Security Functions

226 Within the Windows NT environment all processes are allocated separate memory locations within the RAM. Whenever sensitive memory is re-allocated it is flushed of data prior to re-allocation. These processes are routinely terminated to ensure clean memory

Audit

227 Windows NT is able to generate an audit record for the start-up and shutdown of the audit functions and the following auditable events.

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

Table 7-1 Auditable Events

228 The Window NT logs are viewed, searched and sorted through the Windows NT Management module. Windows NT shall record the following for these events:

- Date and time of event;

- Type of event;
- Subject identity,
- Success or failure of the event;
- Column three of additional audit record contents

229 Modifications to the content of the audit trail are not permitted. The authorized administrator has the ability read and delete all audit trail data through the controlled interface Event viewer window.

230 Archiving is a manual process that is performed on the text files. The authorized administrator has the ability to set the Event Log settings not to overwrite events and for the log to be manually cleared.

Time

231 The time used by the audit function is taken from the Window NT system time. The authorized administrator has the ability to set the time and date.

7.9 [PP] specific IT security functions satisfy SFRs

232 Mapping of [PP] EAL2 Functions to [PP] EAL2 SFRs (Section 5.1 and 5.2).

IT Function	Security Functional Requirement(s)
[PP] EAL2 Functions	
193	FMT_SMR.1, FMT_MTD.2, FIA_UID.2, FIA_ATD.1, FIA_UAU.2
194	FMT_MTD.1(1)
195	FMT_MTD.2, FIA_AFL.1
196	FMT_MOF.1 (2)
197	FPT_RIP.1, FPT_SEP.1
198	FAU_GEN.1
199	FAU_GEN.1, FAU_SAR.3
200	FAU_STG.1, FAU_SAR.1

201	FAU_STG.4
202	FMT_MTD.1(2), FPT_STM.1

8 Rationale

8.1 Introduction

233 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

8.2.1 EAL2 Security Objectives for the TOE Rationale

234 [PP] Section 6.1 and 6.2 demonstrates how the EAL2 IT security objectives and environment objectives of the TOE counter the EAL2 IT threats and environment threats identified in [ST] Section 3.2.

235 The following additonal objective is met by the following assumption.

Threats/ Assumptions / **Objectives**	A.WINNT
O.WINNT	✓

236 The following IT Security objectives, environment objectives, IT threats and security policy are not applicable as remote administration is outside the scope of the evaluation:

- T.PROCOM
- P.CRYPTO
- O.ENCRYP
- O.REMACC
- A.REMACC

8.2.2 EAL4 Security Objectives for the TOE Rationale

237 Table 8-1 demonstrates how the EAL4 IT security objectives and environment objectives of the TOE counter the EAL4 IT threats and environment threats identified in [ST] 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	T.USAGE	A.PHYSEC	A.LOWEXP	A.GENPUR	A.PUBLIC	A.NOEVIL	A.SINGEN	A.DIRECT	A.NOREMO	A.WINNT
O.IDAUTH	✓																			
O.SINUSE		✓	✓																	
O.MEDIAT				✓	✓	✓														
O.SECSTA	✓							✓												
O.SELPRO	✓							✓	✓											
O.AUDREC							✓													
O.ACCOUN							✓													
O.SECFUN	✓		✓						✓											
O.LIMEXT	✓																			
O.EAL										✓										
O.PHYSEC												✓								
O.LOWEXP													✓							
O.GENPUR														✓						
O.PUBLIC															✓					
O.NOEVIL																✓				
O.SINGEN																	✓			
O.DIRECT																		✓		
O.NOREMO																			✓	
O.GUIDAN							✓				✓									
O.ADMTRA							✓				✓									
O.WINNT																				✓

Table 8-1 Mapping of EAL4 Objectives to EAL4 Threats and Assumptions

238 [PP] Section 6.1and 6.2 provides a justification for the mapping of IT security objectives to the EAL4 TOE. The following are justifications IT security objectives that are partially met by the TOE and partially by the IT Environment.

239 **T.NOAUTH**

240 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 [ST] Section 5.6.

241 The operating system identifies and authenticates users before allowing access to the TOE. The operating system assigns users to roles and only administrators have access to the TOE security functions.

242 **T.SELPRO**

243 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 authorized user has physical access to the TOE.

244 **T.AUDFUL**

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

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

247 **T.AUDACC**

248 The TOE through the SRMC 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.

249 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.

250 **T.REPEAT**

251 The TOE ensures that users using FTP or Telnet are authenticated S/Key authentication that generates a one-time password.

252 The administrator through the administrative tools of the operating system is responsible for ensuring that the number of user authentication attempts is set.

253 **T.REPLAY**

254 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.

255 The administrator through the administrative tools of the operating system is responsible for ensuring that the number of user authentication attempts is set. All attempts are audited

8.3 Security Requirements Rationale

8.3.1 Requirements are appropriate

256 [PP] section 6.3 which SFRs satisfy the Objectives as defined in [ST] Section 4.1.1

257 The following SFRs are not applicable and therefore considered satisfied, as remote administration is outside the scope of the evaluation:

- FCS_COP.1
- FIA_UAU.5.2 parts a), b) and d)

8.3.2 EAL4 Security Requirements are appropriate

258 Table 8-2 identifies which EAL4 SFRs satisfy the Objectives as defined in [ST] Section 4.1.1

Objective	Security Functional Requirement(s)
O.IDAUTH	FIA_UAU.5

Objective	Security Functional Requirement(s)
O.SINUSE	FIA_UAU.5
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
O.SECSTA	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.3, FPT_RVM.1, FPT_SEP.1, FAU_STG.4, FMT_MOF.1(1), FMT_MOF.1(2)
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)
O.LIMEXT	FMT_MOF.1(1), FMT_MOF.1(2)
O.EAL	FIA_UAU.5, 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

Table 8-2 Mapping of Objectives to EAL4 SFRs

259 **O.EAL**

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

261 **FIA_UAU.5 Multiple authentication mechanisms**[xx]

[xx] A SOF claim is made for FIA_UAU.5, see [ST] Section 5.6.

262 This component was chosen to ensure that multiple 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 [ST] section 5.6 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.

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

264 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.

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

266 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.

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

268 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.

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

270 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.

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

272 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.

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

274 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.

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

276 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.

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

278 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.

279 **FMT_MSA.3 Static attribute initialization**

280 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.

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

282 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.

283 **FPT_SEP.1 TSF domain separation**

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

285 **FAU_GEN.1 Audit data generation**

286 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.

287 **FAU_SAR.1 Audit review**

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

289 **FAU_SAR.3 Selectable audit review**

290 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.

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

292 This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.

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

294 This component was to ensure the TSF restricts the ability of the TOE start up and shut down operation and multiple authentication function to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

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

296 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 authorized external IT entities with the TOE to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

8.3.3 Security Requirement dependencies are satisfied

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FIA_ATD.1	None	None
FIA_UID.2	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5[xxi]	None	None
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1	FDP_IFC.1, FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1	FDP_IFC.1, FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1	FDP_IFC.1, FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1	FDP_IFC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1

[xxi] A SOF claim is made for FIA_UAU.5, see [ST] Section 5.6.

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	FMT_MTD.1, FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
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
FDP_RIP.1	None	None
FPT_RVM.1	None	None
FPT_SEP.1	None	None
FPT_STM.1	None	None

Table 8-3 Mapping of SFR Dependencies

297 The security functional requirements are hierarchical and may satisfy the dependency. Therefor the FMT_SMR.1 and FIA_UAU.1 dependency of FIA_UID.1 is met by FIA_UID.2. The FIA_UID.1 dependency on FIA_UAU.1 is met by FIA_UAU.2. A SOF claim is made for FIA_UAU.5, see [ST] Section 5.6.

298 [PP] Section 6.5 provides the rationale for not satisfying all Dependencies. All dependencies are contained in this [ST].

8.3.4 IT security functions satisfy SFRs

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

IT Function	Security Functional Requirement(s)
Identification and Authentication	
132	FIA_UAU.5[xxii]
133	FAU_GEN.1
Management and Security	
134	FMT_MSA.1(1)
135	FMT_MSA.1(2)
136	FMT_MSA.1(3)
137	FMT_MSA.1(4)
138	FMT_MSA.3
139	FMT_MOF.1
140	FMT_MOF.1
141	FMT_MSA.3
Audit	
142	FAU_GEN.1
143	FAU_GEN.1
144	FAU_GEN.1

[xxii] A SOF claim is made for FIA_UAU.5, see [ST] Section 5.6.

145	FAU_SAR.1
146	FAU_SAR.3
147	FAU_STG.4
Protection of TOE Security Functions	
148	FPT_SEP.1
149	FPT_RVM.1
150	FPT_RVM.1
151	FPT_SEP.1
User Data Protection	
152	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
153	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
154	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
155	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
156	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
157	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2)
158	FDP_IFC.1 (1), FDP_IFC.1 (2)
159	FDP_IFF.1 (1)
160	FDP_IFF.1 (1)
161	FDP_IFC.1 (1)

162	FDP_IFF.1 (1)
163	FDP_IFF.1 (1)
164	FDP_IFF.1 (1)
165	FDP_IFF.1 (1)
166	FDP_IFF.1 (1)
167	FDP_IFF.1 (1)
168	FDP_IFF.1 (1)
169	FDP_IFF.1 (1)
170	FDP_IFF.1 (1)
171	FDP_IFF.1 (1)
172	FDP_IFF.1 (1)
173	FDP_IFF.1 (1)
174	FDP_IFF.1 (1)
175	FDP_IFF.1 (2)
176	FDP_IFC.1 (2)
177	FDP_IFF.1 (2)
178	FDP_IFF.1 (2)
179	FDP_IFF.1 (2)
180	FDP_IFF.1 (2)
181	FDP_IFF.1 (2)
182	FDP_IFF.1 (2)
183	FDP_IFF.1 (2)
184	FDP_IFF.1 (2)

185	FDP_IFF.1 (2)
186	FDP_IFF.1 (2)
187	FDP_IFF.1 (2)
188	FDP_IFF.1 (2)
189	FDP_IFF.1 (2)
190	FDP_IFF.1 (2)
191	FDP_IFF.1 (2)
[PP] EAL2 Function	
193	FMT_SMR.1, FMT_MTD.2, FIA_UID.2, FIA_ATD.1, FIA_UAU.2
194	FMT_MTD.1(1)
195	FMT_MTD.2, FIA_AFL.1
196	FMT_MOF.1 (2)
197	FPT_RIP.1
198	FAU_GEN.1
199	FAU_GEN.1, FAU_SAR.3
200	FAU_STG.1, FAU_SAR.1
201	FAU_STG.4
202	FMT_MTD.1(2), FPT_STM.1

Table 8-4 Mapping of IT Functions to SFRs

300 The following parts of FIA_UAU.5 are not applicable as the sections relate to remote administration. FIA_UAU.5.2 a), b) and d), which is outside the scope of the evaluation. A SOF claim is made for FIA_UAU.5, see [ST] Section 5.6. FCS_COP.1 also relates to remote administration, which is outside the scope of the evaluation.

301 To perform searches and sorts on the audit database the administrator will be able to use the Symantec Raptor Management Console Logfile icon (SRMC). 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.

302 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.

303 Table 8-4 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.

304 [PP] EAL2 Functions identify the SFRs that are either partially or fully met by the Windows NT operating system at EAL2.

8.3.5 IT security functions mutually supportive

305 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 8-4.

8.3.6 Strength of Function claims are appropriate

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

307 [PP] paragraph 182 identifies a threat involving minimal attack potential. The [PP] goes on to confirm that SOF-Basic is appropriate to meet this threat and therefore SOF-Medium exceeds this protection and is therefor also appropriate.

8.3.7 Justification of Assurance Requirements

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

309 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. The Symantec Enterprise Firewall is intended to be suitable for use in UK Government departments, which require an ITSEC E3 equivalent level of assurance, for which EAL4 assurance is suitable.

8.3.8 Assurance measures satisfy assurance requirements

310 Table 8-5, 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.

311 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 (Symantec documentation)	Assurance Requirements Met by Assurance Measure	
Configuration Management Delivery Procedures for Symantec Enterprise Firewall Version 7.0, Issue 1.7	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
	ADO_DEL.2	Detection of modification

Assurance Measures (Symantec documentation)	Assurance Requirements Met by Assurance Measure	
Symantec Enterprise Firewall and Symantec Enterprise VPN 7.0 Reference Guide, Part Number: 16-30-00035 Symantec Enterprise Firewall & Symantec Enterprise VPN 7.0 Installation Guide for NT / Windows 2000, Part Number: 16-30-00033 Symantec Enterprise Firewall & Symantec Enterprise VPN 7.0 Configuration Guide for NT / Windows 2000, Part Number: 16-30-00034 Symantec Enterprise Firewall & Symantec Enterprise VPN for NT / Windows 2000 version 7.0 Release Notes, Part Number: 16-30-00036 Certified Symantec Enterprise Firewall 7.0 Release Notes, version 1.0 Configuration Management Delivery Procedures for Symantec Enterprise Firewall Version 7.0, Issue 1.7	ADO_IGS.1	Installation, generation and start-up procedures
Configuration Management Delivery Procedures for Symantec Enterprise Firewall Version 7.0, Issue 1.7	ALC_LCD.1	Developer defined life-cycle model

Assurance Measures (Symantec documentation)	Assurance Requirements Met by Assurance Measure	
Functional Specification for Symantec Enterprise Firewall Version 7.0, Issue 1.9 Guide to Windows NT Security - A practical Guide to Securing Windows NT Servers and Workstations, ISBN 0-07-057833-8	ADV_FSP.2	Fully defined external interfaces
System Design for Symantec Enterprise Firewall Version 7.0, Issue 1.4	ADV_HLD.2	Security enforcing high-level design
Various source code modules for Symantec Enterprise Firewall 7.0	ADV_IMP.1	Subset of the implementation of the TSF
System Design for Symantec Enterprise Firewall Version 7.0, Issue 1.4 Raptor Firewall Software Architecture, version 5 Software Development Kit (SDK) Programming Guide, version 5 Logging Interface from VPN Driver, version 7	ADV_LLD.1	Descriptive low-level design
Correspondence Demonstration for Symantec Enterprise Firewall Version 7.0, Issue 1.4 System design for Symantec Enterprise Firewall Version 7.0, Issue 1.4	ADV_RCR.1	Informal correspondence demonstration

Assurance Measures (Symantec documentation)	Assurance Requirements Met by Assurance Measure	
Security Policy Model for Symantec Enterprise Firewall Version 7.0, Issue 1.2	ADV_SPM.1	Informal TOE security policy model
Symantec Enterprise Firewall and Symantec Enterprise VPN 7.0 Reference Guide, Part Number: 16-30-00035 Symantec Enterprise Firewall & Symantec Enterprise VPN 7.0 Installation Guide for NT / Windows 2000, Part Number: 16-30-00033 Symantec Enterprise Firewall & Symantec Enterprise VPN 7.0 Configuration Guide for NT / Windows 2000, Part Number: 16-30-00034 Symantec Enterprise Firewall & Symantec Enterprise VPN for NT / Windows 2000 version 7.0 Release Notes, Part Number: 16-30-00036 Certified Symantec Enterprise Firewall 7.0 Release Notes, version 1.0	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 (Symantec documentation)	Assurance Requirements Met by Assurance Measure	
Development Security for Symantec Enterprise Firewall Version 7.0, Issue 1.4	ALC_DVS.1	Identification of security measures
Development Tools Configuration Management Delivery Procedures for Symantec Enterprise Firewall Version 7.0, Issue 1.7	ALC_TAT.1	Well-defined development tools
Test Coverage and Depth for Symantec Enterprise Firewall Version 7.0, Issue 1.3	ATE_COV.2	Analysis of coverage
Test Coverage and Depth for Symantec Enterprise Firewall Version 7.0, Issue 1.3	ATE_DPT.1	Testing: high-level design
Test Plan for Symantec Enterprise Firewall Version 7.0	ATE_FUN.1	Functional testing
Independent Testing Resources	ATE_IND.2	Independent testing

Assurance Measures (Symantec documentation)	Assurance Requirements Met by Assurance Measure	
Validation of Analysis for Symantec Enterprise Firewall Version 7.0, Issue 1.2 Symantec Enterprise Firewall and Symantec Enterprise VPN 7.0 Reference Guide, Part Number: 16-30-00035 Symantec Enterprise Firewall & Symantec Enterprise VPN 7.0 Installation Guide for NT / Windows 2000, Part Number: 16-30-00033 Symantec Enterprise Firewall & Symantec Enterprise VPN 7.0 Configuration Guide for NT / Windows 2000, Part Number: 16-30-00034 Symantec Enterprise Firewall & Symantec Enterprise VPN for NT / Windows 2000 version 7.0 Release Notes, Part Number: 16-30-00036 Certified Symantec Enterprise Firewall 7.0 Release Notes, version 1.0	AVA_MSU.2	Validation of analysis
Strength of Function Assessment for Symantec Enterprise Firewall Version 7.0, Issue 1.1	AVA_SOF.1	Strength of TOE security function evaluation

Assurance Measures (Symantec documentation)	Assurance Requirements Met by Assurance Measure	
Vulnerability Assessment for Symantec Enterprise Firewall Version 7.0, Issue 1.4	AVA_VLA.2	Independent vulnerability analysis

Table 8-5 Mapping of Assurance Measures to Assurance Requirements

This page is intentionally blank.