UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P171

Symantec Enterprise Firewall

Version 7.0

running on Windows NT 4.0 SP6a

Issue 2.0

November 2003

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Trademarks:

The following trademarks are acknowledged:

Microsoft and Windows NT are registered trademarks of Microsoft Corporation.

Intel and Pentium are registered trademarks of the Intel Corporation.

Ethernet is a registered trademark of Xerox Corporation.

CERTIFICATION STATEMENT

The Symantec Enterprise Firewall is an Application-level firewall running on Windows NT. A set of application-specific security proxies can be configured to validate each attempt to pass data in or out of the network it secures.

Symantec Enterprise Firewall Version 7.0 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 conformant functionality in the specified environment when running on the platforms specified in Annex A.

The firewall, with the addition of certain aspects of the operating system functionality, has also met the requirements of the Application-level Firewall Protection Profile for Basic Robustness Environments at the EAL2 Evaluation Assurance Level when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body, UK IT Security Evaluation and Certification Scheme
Date authorised	17 November 2003

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
DMZ	De-militarised Zone
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIC	Network Interface Card
OSI	Open Systems Interconnection
OSP	Organisational Security Policy
PDF	Portable Document Format
SFR	Security Functional Requirement
SOF	Strength of Function
SRMC	Symantec Raptor Management Console
TCP/IP	Transmission Control Protocol / Internet Protocol
TOE	Target of Evaluation
TSFI	TOE Security Functions Interface
UKSP	United Kingdom Scheme Publication
VPN	Virtual Private Network
WAN	Wide Area Network

(This page is intentionally left blank)

REFERENCES

a. Security Target for Symantec Enterprise Firewall Version 7.0,
Symantec Corporation,
T349/ST, Version 2.0, May 2002.

b. Application-level Firewall Protection Profile for Basic Robustness Environments,
U.S. Department of Defense,
Version 1.0, June 22 2000.

c. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

d. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

e. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

f. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

g. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.

h. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

i. LFS/T349 Evaluation Technical Report,
Syntegra CLEF,
LFS/T349/ETR, Issue 1.0, May 2002.

j. Additional Evaluation Evidence,
Syntegra CLEF,
Response to CB/8052/LFS/T349, Version 3.0, May 2002.

k. Certified Symantec Enterprise Firewall 7.0 Release Notes,
Symantec Corporation,
Version 1.0, 28 May 2002.

l. Configuration Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000,
Symantec Corporation,
Part Number: 16-30-00034.

m. Reference Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000,
Symantec Corporation,
Part Number 16-30-00035.

n. Installation Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000,
Symantec Corporation,
Part Number: 16-30-00033.

o. Symantec Enterprise Firewall and Symantec Enterprise VPN for Windows 2000/NT,
Version 7.0 Release Notes,
Symantec Corporation,
Part Number: 16-30-00036.

p. Common Criteria Certification Report No. P171:
Symantec Enterprise Firewall Version 7.0,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, June 2002.

q. Letter from the evaluators to the Certifier,
Syntegra CLEF,
LFS/T423/lett04, 23 October 2003.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Symantec Enterprise Firewall Version 7.0 to the Sponsor, Symantec Corporation, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

   Version 7.0 of the Symantec Enterprise Firewall, running on a Windows NT Version 4.0 (Workstation or Server) SP6a platform.

   The Developer was Symantec Corporation.

4. The Symantec Enterprise Firewall is an Internet Protocol application and packet-filtering firewall. The application proxies provide connection services on behalf of hosts within a secured network. The packet filtering allows the acceptance or refusal of data on the attributes of the data packets.

5. This product was evaluated to the predefined Evaluation Assurance Level EAL4. It is also described in this report as the Target of Evaluation (TOE).

6. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

7. An overview of the TOE's security architecture can be found in Annex B.

8. The TOE, with the addition of the Windows NT4.0 SP6a operating system functionality listed below under 'TOE Scope' was also evaluated against the EAL2 requirements of the Application-level Firewall Protection Profile for Basic Robustness Environments [b].

TOE Scope

9. The scope for the EAL4 evaluation of the TOE consists of Version 7.0 of the Symantec Enterprise Firewall running on a Windows NT Version 4.0 (Workstation or Server) SP6a platform. The TOE configuration consists of:

   a. Version 7.0 of the Symantec Enterprise Firewall; and

   b. The Symantec Raptor Management Console (SRMC), which is used for administration.

10. The TOE with the addition of the following Windows NT4.0 SP6a operating system functionality was also evaluated against the requirements of the Protection Profile (PP) [b]:

a. User Administration functionality;

b. Logon Process;

c. Date/Time Application;

d. Network Configuration;

e. Event Logs and Archiving;

f. Event Viewer Application; and

g. Functionality relating to the protection of processes.

11. The following software and hardware features were not evaluated:

a. Virtual Private Networking (VPN) functionality;

b. Symantec Enterprise VPN Client;

c. High Availability / Load Balancing;

d. Remote Administration;

e. User Authentication by one-time password, and SecurID Authentication engine for mobile users to access services in the protected domain;

f. Setup Wizard;

g. H.323 Connections; and

h. Forward Filtering.

12. Note that this evaluation did not address use of the TOE on operating systems other than Windows NT4.0 SP6a. In particular, whilst a number of the supporting guidance documents [l-o] also address operation on Windows 2000, this was not addressed by this evaluation.

Protection Profile Conformance

13. The Security Target [a] claimed conformance to the Application-level Firewall Protection Profile for Basic Robustness Environments [b]. This applies to the evaluation of the TOE, with the addition of the Windows NT4.0 SP6a operating system functionality listed above under 'TOE Scope', at the EAL2 assurance level.

14. The Protection Profile's [b] cryptographic protection and authentication claims associated with a remote administration capability (objectives O.ENCRYP and O.REMAC, and Security Functional Requirements (SFRs) FSC_COP and FIA_UAU.5.2 a), b) and d)) were excluded

from the Security Target [a], in accordance with the option permitted by the Protection Profile, as the remote administration capability was excluded from the TOE.

15. The Security Target [a] also includes the objective O.WINNT, which is discussed below under 'Installation and Guidance Documentation'.

Assurance

16. The Security Target [a] specified the EAL4 assurance requirement for the TOE. Common Criteria Part 3 [e] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [c].

17. The TOE, with the addition of the Windows NT4.0 SP6a operating system functionality listed above under 'TOE Scope', was also evaluated against the EAL2 requirements of the Protection Profile [b].

Strength of Function Claims

18. The publicly known Bellcore S/Key authentication mechanism is used to meet the Security Target's [a] and Protection Profile's [b] authenticated information flow security policy claim for FTP and Telnet transfers. The firewall includes an S/Key challenge mechanism, incorporating an MD4 hashing algorithm to check one time passwords expected from a user password, a seed value and a decrementing counter. A user attempting a firewall-authenticated transfer must have a local S/Key mechanism to generate the expected response, and must first arrange to use a user password expected by the firewall.

19. The minimum Strength of Function (SOF) claimed for the TOE was SOF-Medium. This was claimed for the user password supplied as an input to the S/Key mechanism. A specific metric, the probability that the password can be guessed is no greater than one in two to the fortieth, was also claimed for this password.

20. The MD4 algorithm is publicly known and as such it is the policy of the UK national authority for cryptographic mechanisms, the Communications-Electronics Security Group (CESG), not to specifically relate this to the SOF claim. Consumers should note however that it is public knowledge that MD4 is relatively weak. The sponsor is accordingly considering further evaluation of the next version (7.0.4) of the product, to address the functionality used to invoke the use of an external authentication mechanism.

21. Furthermore the SOF claims did not cover either the administrative login to the firewall or the operating system login. As the TOE is assumed to operate in a physically secure environment no strength in these mechanisms was considered necessary.

Security Policy

22. Two forms of information flow security policy are claimed by the Security Target [a]:

a. Unauthenticated : for information flow between IT entities on connected networks.

b. Authenticated: for information flow initiated by a user on a connected network who is authenticated by the firewall, as discussed above under 'Strength of Function Claims'.

23. There are no Organizational Security Policies (OSPs) with which the TOE must comply. The Protection Profile [b] specifies one OSP, but this is related to remote administration, and is therefore outside the scope of the evaluation.

Security Claims

24. The Security Target [a] fully specifies the TOE's security objectives, the threats which these objectives counter and SFRs and security functions to elaborate the objectives. All of the SFRs are taken from CC Part 2 [d]; use of this standard facilitates comparison with other evaluated products.

25. Claims are primarily made for security functionality in the following areas:

- Information Flow Control
- Identification & Authentication
- Security Management
- Audit
- Protection of Security Functions

Evaluation Conduct

26. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [g, h]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

27. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE, and the Windows NT 4.0 SP6a functionality listed above under 'TOE Scope', were then evaluated against this baseline. All parts of the evaluation were performed in accordance with CC Part 3 [e] and the Common Evaluation Methodology (CEM) [f].

28. The Certification Body monitored the evaluation which was carried out by the Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the final Evaluation Technical Report (ETR) [i] to the Certification Body in May 2002. Following a number of clarifications [j], the CLEF drafted Issue 1.0 of the Certification Report [p] which was then agreed and released by the Certification Body. Following further

evaluation work to clarify the implementation of the S/Key mechanism (see [q]), the Certification Body then produced this Issue 2.0 of the Certification Report.

General Points

29. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

30. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Issue 2.0 of the Certification Report reflects the Certification Body's view at the time of Issue 1.0. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since Issue 1.0 and, if appropriate, should check with the Developer to see if any patches exist for the products and whether such patches have been evaluated and certified.

31. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

32. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [i] under the CC Part 3 [e] headings. The following sections note considerations that are of particular relevance to consumers.

Delivery

33. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

34. All TOE software and documentation components identified in Annex A are delivered to the consumer with the product, with the exception of the Certified Symantec Enterprise Firewall 7.0 Release Notes [k]. This document is available on Symantec's website at www.symantec.com/techsupp/enterprise/products/sym_ent_firewall/sym_ent_firewall_7_nt/manuals.html

35. The following measures provide security for delivery of the product and guidance documentation packaged with it:

a. The product is delivered by registered delivery using a reputable delivery firm.

b. The product is delivered in a sealed box.

c. To install the product the consumer must obtain a license key. This is obtained from Symantec's web-site, quoting the serial number of the product and the volume serial number of the hard disk the product is to be installed on.

36. The primary considerations governing the security of web-based delivery are as follows:

a. Standard procedures associated with a well managed web interface should be followed; and

b. The Certified Symantec Enterprise Firewall 7.0 Release Notes [k] are downloaded as a Portable Document Format (PDF) file.

37. Symantec are not responsible for secure delivery of the operating system. However the following measures provide appropriate security:

a. The Certified Release Notes [k] recommend that the operating system is obtained from a reputable source.

b. Secure configuration and operation of the operating system for use with the firewall is addressed by firewall guidance documentation, primarily the Certified Release Notes [k].

c. When the firewall is installed it runs a number of automated configuration checks on the operating system, and this gives further confidence in the authenticity of the operating system.

Installation and Guidance Documentation

38. The Certified Symantec Enterprise Firewall 7.0 Release Notes [k] describe the procedures that have to be followed to install the product and operate it securely. This document also includes procedures that need to be followed regarding configuration of the operating system. It is thus recommended that this document be read first.

39. Further administrative guidance is provided by the following documentation:

a. Configuration Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000 [l];

b. Reference Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000 [m];

c. Installation Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000 [n]; and

d. Symantec Enterprise Firewall and Symantec Enterprise VPN for Windows 2000/NT, Version 7.0 Release Notes [o].

40. Symantec do not provide guidance relating to installation and operation of a 'vanilla' Windows NT base; assumption A.WINNT and objective O.WINNT are included in the Security Target [a] regarding the installation and operation of NT in a generally secure manner. However the firewall guidance documentation addresses secure configuration and operation of the operating system for use with the firewall as noted above under 'Delivery'.

41. The guidance documentation is aimed at the firewall administrator. However, as noted below under 'Strength of Function', administrators are required to ensure that users are aware of the correct method of operating the S/Key mechanism where authenticated FTP and Telnet transfers are required.

Strength of Function

42. The SOF claims for the password element of the S/Key authentication mechanism were as given above under 'Strength of Function Claims'. Confirmation of these claims was based on the requirement, specified in the guidance documentation [k], that the password chosen must be at least 10 characters long.

43. The Evaluators confirmed the TOE's correct implementation of the S/Key mechanism, including the MD4 hashing algorithm, by testing.

44. A potential weakness in use of the S/Key mechanism, if the counter is not decremented correctly, is addressed by the guidance documentation [k, m] which requires the administrator to ensure that users are aware of the correct method of operating the mechanism.

Vulnerability Analysis

45. The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE and operating system given by the evaluation process.

Testing

46. The TOE was tested against the TOE Security Functions Interface (TSFI) provided by the various components of the interface categories listed under 'TSF Interfaces' in Annex B.

47. The Developer performed tests using all aspects of the TSFI. These tests also exercised:

a. All related security functions specified in the Security Target [a]; and

b. All high level design subsystems identified in Annex B.

48. The Developer also performed some tests relating to the operating system.

49. The Developer's testing was performed manually following test scripts. The scripts contained all procedures necessary to repeat the tests, and where appropriate provided a description of any external stimulus required.

50. The Evaluators performed the following independent testing:

a. A sample of the Developer's tests was repeated to validate the Developer's testing. The sample was at least 20% of the total Developer security testing, included tests from all functional areas and tests performed by different Developer test engineers.

b. A test for each section of the firewall TSFI, different from those performed by the Developer, was devised wherever possible. Independent tests were thus performed for the majority of the security functions.

c. Testing of operating system functionality within the scope of the evaluation was completed.

51. The Evaluators also devised and performed penetration tests, wherever needed, to confirm the non-exploitability of potential vulnerabilities which had been noted in the course of the evaluation.

52. Developer and Evaluator tests were performed on both a Windows NT Server and a Windows NT Workstation platform.

53. The testing performed was equally relevant to mediation of traffic between internal networks and between internal and external networks.

54. Firewall functionality addressed in the course of testing included the following:

a. All communications protocols and application proxies listed in the Security Target [a];

b. Syn flooding attack and denial of service protection;

c. Port scanning detection; and

d. Both static and dynamic Network Address Translation options.

Platform Issues

55. The firewall was evaluated on the hardware platforms specified in Annex A. Strictly therefore the certified configuration excludes other hardware options, e.g. other Network Interface Cards (NICs) from the Symantec-approved list. However the Evaluators noted that:

a. During the performance of the various evaluation activities no evidence was found to indicate that the results of the evaluation would be different on a firewall installed on a hardware platform with a different specification.

b. Whilst there may be a low risk in using a different hardware platform, this risk is mitigated by the fact that the firewall only interacts with the hardware through the operating system, and thus any machine which successfully runs the operating system should also run the firewall.

56. It is possible to configure the firewall to notify the administrator when certain security-relevant events occur. A possible method of notification requires the use of a sound card in order to play a sound file in response to an event generated by the firewall. The Administrative guidance [l, m] describes how to set up and manage notifications, and details that, should audio notification be required, a properly installed and configured sound card is required.

57. A CD drive is required to support installation of the TOE, which is delivered on CD. Removable read/write media are also required to support archiving of configuration and audit data.

III. EVALUATION OUTCOME

Certification Result

58. After due consideration of the ETR [i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that the Symantec Enterprise Firewall Version 7.0 running on Windows NT 4.0 SP6a meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 conformant functionality in the specified environment, when running on the platforms specified in Annex A.

59. Furthermore the Symantec Enterprise Firewall Version 7.0, with the addition of the Windows NT4.0 SP6a operating system functionality listed above under 'TOE Scope', meets the EAL2 requirements of the Application-level Firewall Protection Profile for Basic Robustness Environments [b] in the specified environment, when running on the platforms specified in Annex A.

60. The user password of the S/Key authentication mechanism meets the minimum Strength of Function of SOF-Medium and the specific metric given above under 'Strength of Function Claims'.

Recommendations

61. Prospective consumers of Symantec Enterprise Firewall Version 7.0 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

62. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under 'TOE Scope' and 'Evaluation Findings'.

63. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

64. The above 'Evaluation Findings' include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE, which has been evaluated to EAL4 consists of:

   a. Version 7.0 of the Symantec Enterprise Firewall;

   b. The Symantec Raptor Management Console (SRMC), which is used for administration.

2. The TOE is provided on a single CD, part no. 16-26-00029, and must be installed on either Windows NT Server 4.0 SP6a or Windows NT Workstation 4.0 SP6a.

3. In addition, in order to claim compliance to the Protection Profile [b], the TOE, with the addition of the Windows NT4.0 SP6a operating system functionality listed above under 'TOE Scope', was evaluated against the EAL2 Protection Profile requirements.

TOE Documentation

4. The supporting guidance documents evaluated were:

   a. Certified Symantec Enterprise Firewall 7.0 Release Notes [k];

   b. Configuration Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000, Part Number: 16-30-0034 [l];

   c. Reference Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000, Part Number: 16-30-0035 [m];

   d. Installation Guide for Symantec Enterprise Firewall 7.0 for Windows NT/2000, Part Number: 16-30-0033 [n]; and

   e. Symantec Enterprise Firewall and Symantec Enterprise VPN for Windows 2000/NT, Version 7.0 Release Notes, Part Number: 16-30-0036 [o].

5. Further discussion of the supporting guidance material is given above under 'Installation and Guidance Documentation'.

TOE Configuration

6. The following configuration was used for testing:

   a. TOE installed on a machine running Microsoft Internet Explorer 6.0 (which is used by the SRMC) and Windows NT Server 4.0 SP6a; and

   b. TOE installed on a machine running Microsoft Internet Explorer 6.0 and Windows NT Workstation 4.0 SP6a.

Environmental Configuration

7. The two hardware platforms used for the testing of the TOE were as follows:

- **Firewall running on Windows NT Server:**

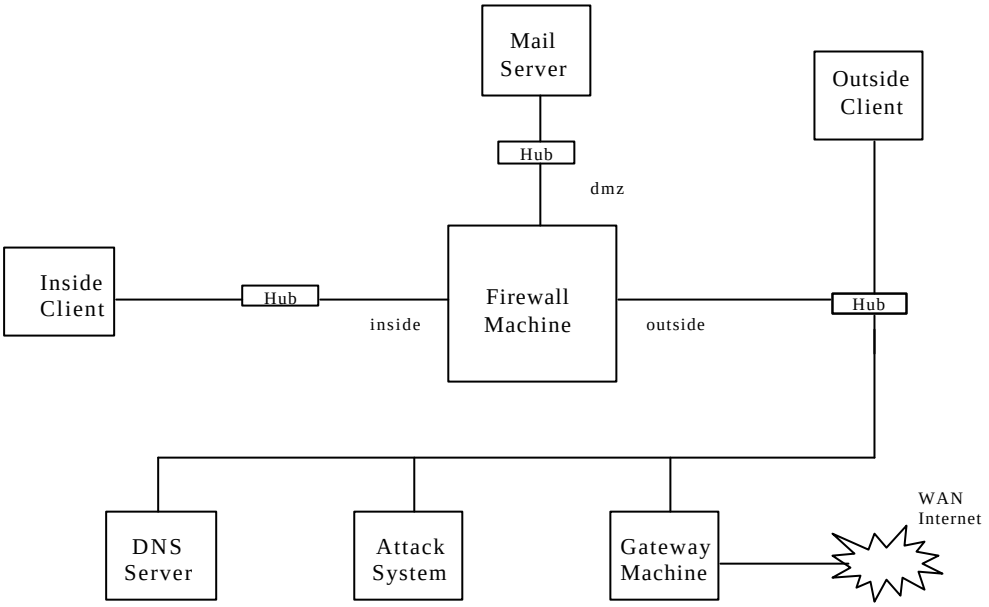
CPU: Pentium III – 1GHZ	
RAM: 256MB	
Hard Drive: 20Gb	
Software: Windows NT Server Version 4.0 (Service Pack 6a)	
	Microsoft Internet Explorer 6.0
	Symantec Enterprise Firewall Version 7.0 with Symantec Raptor Management Console
NICs:	Intel Pro/100S Desktop Adapter, Netgear FA312 Fast Ethernet PCI, 3COM Etherlink 10/100 PCI

- **Firewall running on Windows NT Workstation**

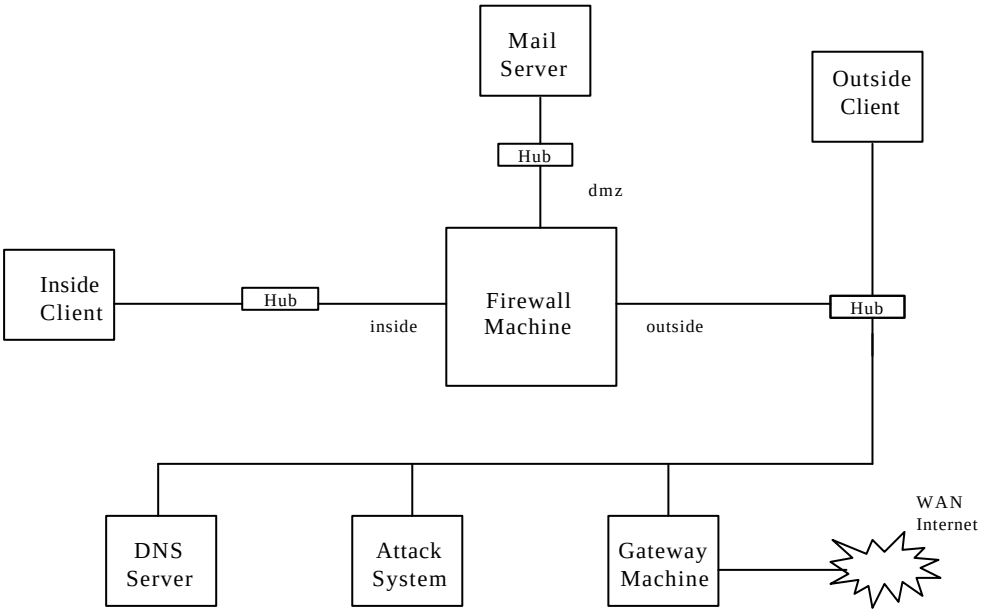
CPU: Pentium III – 1GHZ	
RAM: 256MB	
Hard Drive : 20Gb	
Software: Windows NT Workstation Version 4.0 (Service Pack 6a)	
	Microsoft Internet Explorer 6.0
	Symantec Enterprise Firewall Version 7.0 with Symantec Raptor Management Console
NICs:	Intel Pro/100S Desktop Adapter, Netgear FA312 Fast Ethernet PCI, 3COM Etherlink 10/100 PCI

8. The machines hosting the firewall were connected via Ethernet using 10BaseT network connections (RJ45 interface). They were connected in the following network configurations:

- Network Configuration – NT Server:



- Network Configuration – NT Workstation:



(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

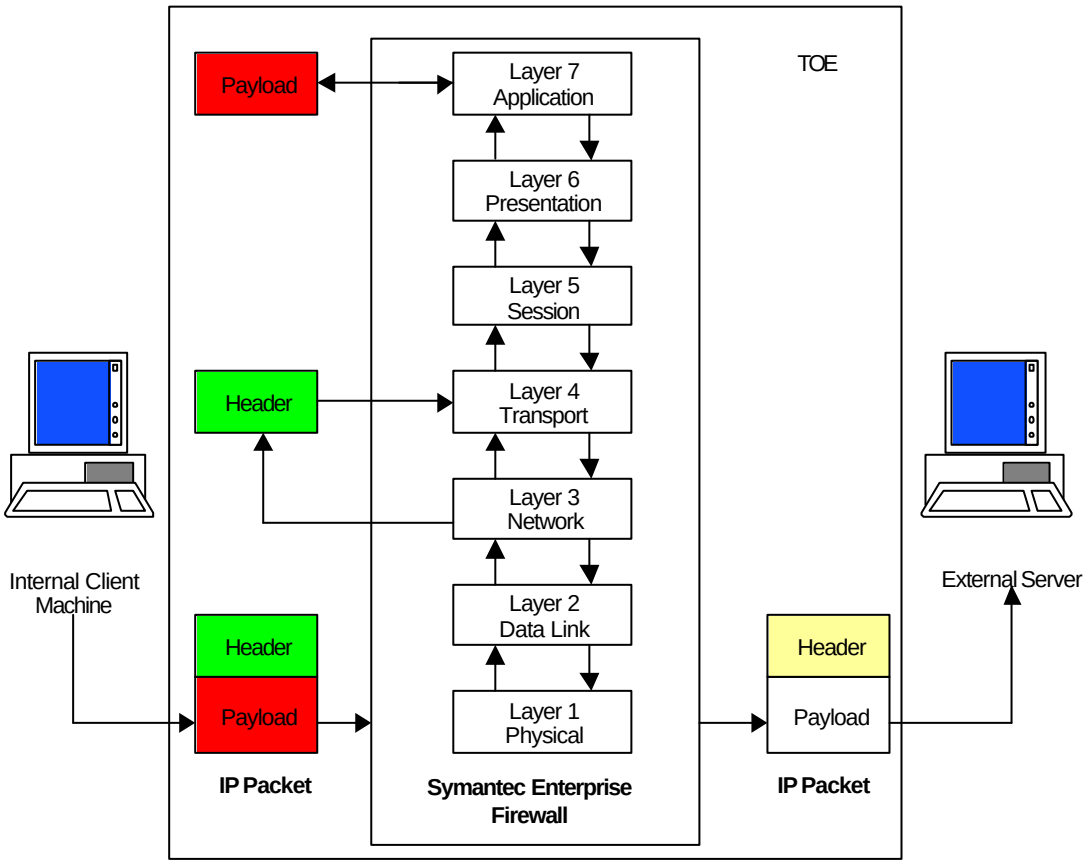
1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Further specification of the scope of evaluation is given in various sections above.

Architectural Features

2. The TOE is an Application-level firewall running on Windows NT. A set of application-specific security proxies can be configured to validate each attempt to pass data in or out of the network it secures.

3. The packets enter the TCP/IP stack of the 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 firewall to the next network segment.

4. Most of the proxies operate at the Application Layer of the OSI 7-layer model. This is shown in the diagram below which details the passage of a packet through the firewall.



5. The Ping proxy is an exception in that, although referred to as an 'application proxy', it does not actually operate at the Application Layer. When the firewall passes Ping traffic destined for an address other than the firewall itself, the Ping proxy constructs a new echo request with a new sequence number and does not send the original. If the firewall is the target of the ping then the Ping proxy responds to the client normally.

6. The firewall has only one class of user who is the administrator. The administrator is trusted to manage the firewall, either locally or remotely, but remote management is outside the scope of the evaluation. Users of the network service connections through the firewall cannot log on to the firewall.

7. The firewall offers a number of failsafe features, including the following:

   a. Network connections are denied unless an information flow rule has been set up to explicitly allow them (i.e. if the 'best fit' feature is unable to identify an appropriate rule);

   b. Network connections are dropped if the audit log becomes full; and

   c. Internal processes exist to restart any key processes which go down and to terminate any unauthorised processes.

TSF Interfaces

8. The external interfaces that comprise the TSFI are as follows:

   a. The administrator's interface via the SRMC; and

   b. The interface between the firewall and the operating system (which also gives indirect interfaces to network connections and disk backup of configuration and audit files).

9. The following interfaces are relevant for the consideration against the Protection Profile:

   a. The administrator's interface via the SRMC;

   b. The interface to the network connections from the operating system;

   c. The administrator's interface to the operating system; and

   d. The disk backup of configuration files and audit files.

10. The administrator's interface via the SRMC provides the method by which the administrator can configure and control all subsystems of the firewall. The exception is the Operating System Functions subsystem which is administered and controlled through its own interface.

Design Subsystems

11. The Symantec Enterprise Firewall product consists of three main subsystems

    a. Management Functions;

    b. Firewall Functions; and

    c. Audit Functions.

12. In addition the operating system is considered as another subsystem for the purposes meeting the Protection Profile [b] requirements.

13. All subsystems are security enforcing. The purpose of each is identified in the table below:

Subsystem	Purpose
Management Functions	The Management Functions subsystem enables the administrator to define the packet filters, proxies and authorisation rules. This subsystem also allows the administrator to configure the TOE authentication and audit functions.
Firewall Functions	The Firewall Functions subsystem controls the mediation of network data and provides controls to protect the security of data and services on the product
Audit Functions	The Audit Functions subsystem records all audit events relevant to the firewall. It also provides event viewing and filtering facilities.
Operating System Functions	The Operating System Functions subsystem defines the security attributes, rights and privileges of all administrators. This subsystem also controls the operating system auditing functionality, and controls the system time.

Hardware and Firmware Dependencies

14. In order to support the firewall, the following security functions are required to be provided by the underlying hardware:

a. Interrupts;

b. Processor Execution Levels;

c. Memory Allocation; and

d. System Clock.