UK IT SECURITY EVALUATION AND
CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P198

Symantec Enterprise Firewall

Version 7.0.4

running on Windows 2000 SP3 and on Solaris 7 & 8

Issue 1.0

November 2003

© Crown Copyright 2003

Reproduction is authorised provided the report
is copied in its entirety

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:

All product and company names are used for identification purposes only and may be trademarks of their owners.

CERTIFICATION STATEMENT

Symantec Enterprise Firewall Version 7.0.4 is an application-level firewall running on Windows 2000 (with Service Pack 3), Solaris 7 and Solaris 8. A set of application-specific security proxies can be configured to validate each attempt to pass data in or out of the network that the firewall secures.

Symantec Enterprise Firewall Version 7.0.4 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.

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	Demilitarised Zone
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IP	Internet Protocol
MD4	Message Digest 4
NIC	Network Interface Card
OSI	Open Systems Interconnection
RCU	Raptor Console for Unix
SFR	Security Functional Requirement
SOF	Strength of Function
SP	Service Pack
SRMC	Symantec Raptor Management Console
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
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 7.0.4 for Windows 2000 and Solaris,
Symantec Corporation,
T426/ST, Version 2.3, October 2003.

b. Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Common Criteria Interpretation Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements,
Common Criteria Interpretation Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
Common Criteria Interpretation Management Board,
CCIMB-99-033, Version 2.1, August 1999.

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

f. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

g. CLEF Requirements: Part I – Startup and Operation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02 Part I, Issue 4.0, April 2003.

h. CLEF Requirements: Part II – Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02 Part II, Issue 1.0, April 2003.

i. LFS/T426 Evaluation Technical Report,
Syntegra CLEF,
LFS/T426/ETR, Issue 1.0, August 2003.

j. Common Criteria Certification Report No. P171:
Symantec Enterprise Firewall Version 7.0 running on Windows NT 4.0 SP6a,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, June 2002.

k. Symantec Enterprise Firewall, Version 7.0.4 - Certified Common Criteria Release Notes for Windows 2000,
Symantec Corporation,
Version 1.1, 3 October 2003.

l. Symantec Enterprise Firewall, Version 7.0.4 - Certified Common Criteria Release Notes for Solaris 7 & 8,
Symantec Corporation,
Version 1.1, 3 October 2003.

m. Symantec Enterprise Firewall and Symantec Enterprise VPN, Version 7.0.4 - Release Notes for Windows *(for Windows NT4.0 & 2000)*,
Symantec Corporation,
Part Numbers 10053984 *(US edition)* and 10060059-IN *(international edition).*

n. Symantec Enterprise Firewall and Symantec Enterprise VPN, Version 7.0.4 - Release Notes for Solaris *(for Solaris 7, 8 & 9)*,
Symantec Corporation,
Part Numbers 10050680 *(US edition)* and 10059305-IN *(international edition).*

o. Symantec Enterprise Firewall and Symantec Enterprise VPN, Version 7.0 - Configuration Guide *(for Windows NT4.0 & 2000, Solaris 7 & 8 and Linux (VelociRaptor))*,
Symantec Corporation,
Part Number 16-30-00034.

p. Symantec Enterprise Firewall, Symantec Enterprise VPN and VelociRaptor Firewall Appliance, Version 7.0 - Reference Guide *(for Windows NT4.0 & 2000, Solaris 7 & 8 and VelociRaptor Firewall Appliance)*,
Symantec Corporation,
Part Number 16-30-00035.

q. Symantec Enterprise Firewall and Symantec Enterprise VPN, Version 7.0 - Installation Guide for Windows *(for Windows NT4.0 & 2000)*,
Symantec Corporation,
Part Number 16-30-00033.

r. Symantec Enterprise Firewall and Symantec Enterprise VPN, Version 7.0 - Installation Guide for Solaris *(for Solaris 7 & 8)*,
Symantec Corporation,
Part Number 16-30-00050.

s. 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 (CC) security evaluation of Symantec Enterprise Firewall Version 7.0.4 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:

Symantec Enterprise Firewall Version 7.0.4, running on Microsoft Windows 2000 Service Pack (SP) 3 and on Sun Microsystems Solaris Versions 7 and 8.

4. The product is described in this report as the Target of Evaluation (TOE). The Developer was Symantec Corporation.

5. The product is an Internet Protocol (IP) 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.

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

7. An overview of the TOE's security architecture is provided in Annex B.

TOE Scope

8. The TOE consists of two physical components:

a. The firewall itself.

b. Depending on the operating system: either the 'Symantec Raptor Management Console' (SRMC) for Windows 2000 or the 'Raptor Console for Unix' (RCU) for Solaris. The SRMC/RCU provides a Graphical User Interface (GUI) for administration of the firewall via the firewall server console.

9. The scope of this certification applies to the TOE running on the following operating system platforms:

a. Microsoft Windows 2000 with SP3 (identified in this report as 'Windows 2000');

b. Sun Microsystems Solaris Version 7 (identified in this report as 'Solaris 7');

c. Sun Microsystems Solaris Version 8 (identified in this report as 'Solaris 8').

10. Those operating systems are in the TOE's IT environment and are therefore outside the scope of this certification.

11. This certification does not address any use of the TOE on operating systems other than those listed in paragraph 9 above. In particular, whilst some of the supporting guidance documents [k - r] also address operation on Windows NT, Solaris 9 and Linux, that use is not addressed by this certification.

12. The following software and hardware features are also outside the scope of this certification:

- Virtual Private Networking (VPN) functionality
- Symantec Enterprise VPN Client
- High Availability / Load Balancing
- User Authentication by one-time password (excluding S/Key Authentication), and SecurID Authentication engine for mobile users to access services in the protected domain
- Setup Wizard
- H.323 Connections
- Remote Administration
- Forward Filtering
- S/Key Password Generator
- SQL*Net Proxy

Protection Profile Conformance

13. The Security Target [a] makes no claims regarding Protection Profile conformance.

Assurance

14. The Security Target [a] specifies the assurance requirement for the TOE as CC predefined Evaluation Assurance Level EAL4.

15. CC Part 1 [b] provides an overview of the CC. CC Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7.

Strength of Function Claims

16. The publicly known Bellcore S/Key authentication mechanism is used to meet the Security Target's [a] 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.

17. 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.

18. The MD4 algorithm is publicly known and as such it is the policy of the UK national authority for cryptographic mechanisms, 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 product, to address the functionality used to invoke the use of an external authentication mechanism.

19. The SOF claim did not cover administrative login to the firewall. As the TOE is assumed to operate in a physically secure environment, no strength in this mechanism was considered necessary.

Security Policy

20. 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’.

21. There are no Organisational Security Policies with which the TOE must comply.

Security Claims

22. The Security Target [a] fully specifies the TOE’s security objectives, the threats that the objectives counter, and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives.

23. All of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

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

- Information Flow Control
- Identification and Authentication
- Security Management
- Audit
- Protection of TOE Security Functions (TSF)

Evaluation Conduct

25. 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 (UKSP) 01 [f] and 02 Parts I and II [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 that Arrangement.

26. 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 was then evaluated against that baseline.

27. The evaluation was performed in accordance with the following requirements:

- the EAL4 requirements specified in CC Part 3 [d]
- the Common Evaluation Methodology (CEM) [e]
- the appropriate CC interpretations

28. Some results were reused from the previous EAL4 evaluation of the firewall's Version 7.0 for Windows NT 4.0 SP6a (see Certification Report P171 [j]), where such results were still valid for the TOE.

29. 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) [h] to the Certification Body in August 2003. The Certification Body requested further details and, following the CLEF's satisfactory responses [s], the Certification Body produced this Certification Report.

General Points

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

31. 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 Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the products and whether such patches have been evaluated and certified.

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

II. EVALUATION FINDINGS

Introduction

33. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [h] under the CC Part 3 [d] headings.

34. The following sections note considerations of particular relevance to consumers.

Delivery

35. On receipt of the TOE, the consumer should check that the evaluated version has been supplied and should check that the security of the TOE has not been compromised during delivery.

36. All of the TOE software and documentation identified in Annex A is delivered to the consumer with the product, except for the Certified Release Notes [k - l]. Consumers should download those Notes from Symantec's websites at:

a. (for Windows 2000):
http://www.symantec.com/techsupp/enterprise/products/sym_ent_firewall/sym_ent_firewall_704_nt/manuals.html

b. (for Solaris 7 and 8):
http://www.symantec.com/techsupp/enterprise/products/sym_ent_firewall/sym_ent_firewall_704_solaris/manuals.html

37. The TOE documentation delivered with the product is either in hard copy or in Portable Document Format (PDF) files on the CDs. Some of those documents reference the previously evaluated version of the product (i.e. Version 7.0); this is intentional, as those Version 7.0 documents are also applicable to Version 7.0.4.

38. The CDs and the software (when installed) identify the product as Version 7.0.4.

39. The following measures provide security for delivery of the product (including the guidance documentation packaged with it):

a. The product is delivered in a sealed box, by registered delivery, using a reputable delivery firm.

b. A Value Licence Certificate is delivered separately from the product, using a reputable delivery firm. It is usually dispatched after the product, so as to arrive after the product.

c. To install the product, the consumer must activate it by entering a valid Licence Key. The Licence Key is obtained from Symantec's website, by inputting the consumer's details and quoting the valid activation number provided on the Value Licence Certificate.

40. 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.

b. The Certified Release Notes [k, l] are downloaded as PDF files.

Installation and Guidance Documentation

41. The Certified Release Notes [k, l] describe the procedures that must be followed to install the product and operate it securely, and include warnings to identify unevaluated functionality. Those notes also include procedures that must be followed to configure the operating system. Hence it is recommended that the appropriate notes, for Windows [k] or Solaris [l], are read first.

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

- Release Notes for Windows [m]
- Release Notes for Solaris [n]
- Configuration Guide [o]
- Reference Guide [p]
- Installation Guide for Windows [q]
- Installation Guide for Solaris [r]

43. 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

44. 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, l], that the password chosen must be at least 10 characters long.

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

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

Vulnerability Analysis

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

Testing

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

49. 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];

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

50. 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.

51. 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 Developer's total security testing, and included tests from all functional areas and tests performed by the Developer's different 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.

52. 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.

53. The Developer's tests and the Evaluators' tests were performed on Windows 2000, Solaris 7 and Solaris 8.

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

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

    - all communications protocols and application proxies listed in the Security Target [a]
    - Syn flooding attack protection
    - denial of service protection
    - port scanning detection
    - both static and dynamic NAT options
    - IP address spoof checking

Platform Issues

56. 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).

57. 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, to play a sound file in response to an event generated by the firewall. The administrative guidance [k, l, p] describes how to set up and manage notifications; it also notes that, if audio notification is required, a properly installed and configured sound card is needed.

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

III. EVALUATION OUTCOME

Certification Result

59. After due consideration of the ETR [h], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Symantec Enterprise Firewall Version 7.0.4, running on Microsoft Windows 2000 SP3 and on Sun Microsystems Solaris 7 and 8, meets the CC Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified CC Part 2 conformant functionality in the specified environment, when running on the platforms specified in Annex A.

60. The Certification Body has also determined that the TOE meets the minimum Strength of Function of SOF-Medium claimed above under "Strength of Function Claims".

Recommendations

61. Prospective consumers of the TOE should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a].

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 its evaluated configuration. The TOE should also be used in accordance with a number of environmental considerations as specified in the Security Target [a].

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

65. The product provides some features that were not within the scope of the certification, as identified above under 'TOE Scope'. Those features should therefore not be used if the TOE is to comply with its evaluated configuration.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The evaluated configuration of the TOE comprises:

   a. Symantec Enterprise Firewall Version 7.0.4 for Windows 2000 and Solaris;

   b. (for Windows 2000): SRMC, used for administration of the firewall via the firewall server console;

   c. (for Solaris 7 and 8): RCU, used for administration of the firewall via the firewall server console.

2. The TOE is provided on two CDs, as follows:

   a. For the US edition, the two CDs are together in one jewel case (which is imprinted with Part Number 10053980):

      i) one CD is labelled as Symantec Enterprise Firewall Version 7.0.4 for Windows 2000; and

      ii) one CD is labelled as Symantec Enterprise Firewall Version 7.0.4 for Solaris 7 and 8.

   b. For the international edition, the two CDs are in separate jewel boxes:

      i) one CD is labelled as Symantec Enterprise Firewall Version 7.0.4 for Windows 2000 (Part Number 10059316-IN); and

      ii) one CD is labelled as Symantec Enterprise Firewall Version 7.0.4 for Solaris 7 and 8 (Part Number 10059315-IN).

3. The consumer installs the version of the TOE for which they have purchased a Licence Key, i.e. on either Windows 2000 or Solaris 7 or Solaris 8, using the appropriate CD above.

TOE Documentation

4. The supporting guidance documents evaluated were:

   - Certified Release Notes for Windows [k]
   - Certified Release Notes for Solaris [l]
   - Release Notes for Windows [m]
   - Release Notes for Solaris [n]
   - Configuration Guide [o]
   - Reference Guide [p]
   - Installation Guide for Windows [q]
   - Installation Guide for Solaris [r]

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

TOE Configuration

6. The following configuration of the TOE was used for testing:

a. The TOE with SRMC, installed on a machine running Windows 2000 (as detailed in paragraph 7.a below);

b. The TOE with RCU, installed on a machine running Solaris 7 (as detailed in paragraph 7.b below);

c. The TOE with RCU, installed on a machine running Solaris 8 (as detailed in paragraph 7.c below).

Environmental Configuration

7. The three platforms used by the Evaluators to test the TOE were equivalent to those used by the Developer to test the TOE, and were as follows:

a. Firewall running on Windows 2000:

Hardware:

CPU: Intel Pentium III (1 GHz)

512 Mb RAM

20 Gb Hard Disk

CD-ROM

3.5 inch Floppy Disk Drive

Monitor and Keyboard

NICs: a) Intel Pro/1000MT Desktop Adapter
b) 3COM EtherLink 10/100 Mbps PCI NIC with 3XP processor
c) 3COM EtherLink XL 10/100 PCI NIC (3C905C-TX)

Software:

a) Windows 2000 SP3 (with no subsequent hotfixes)
b) Microsoft Internet Explorer 6.0 SP1 (with no subsequent hotfixes), which is used by the SRMC
c) Microsoft Management Console 1.2, for the SRMC

b. Firewall running on Solaris 7:

Hardware:

CPU: SUNW UltraSPARC III running on SUN Ultra 5_10 (270 MHz)

512 Mb RAM

8 Gb Hard Disk

CD-ROM

3.5 inch Floppy Disk Drive

Monitor and Keyboard

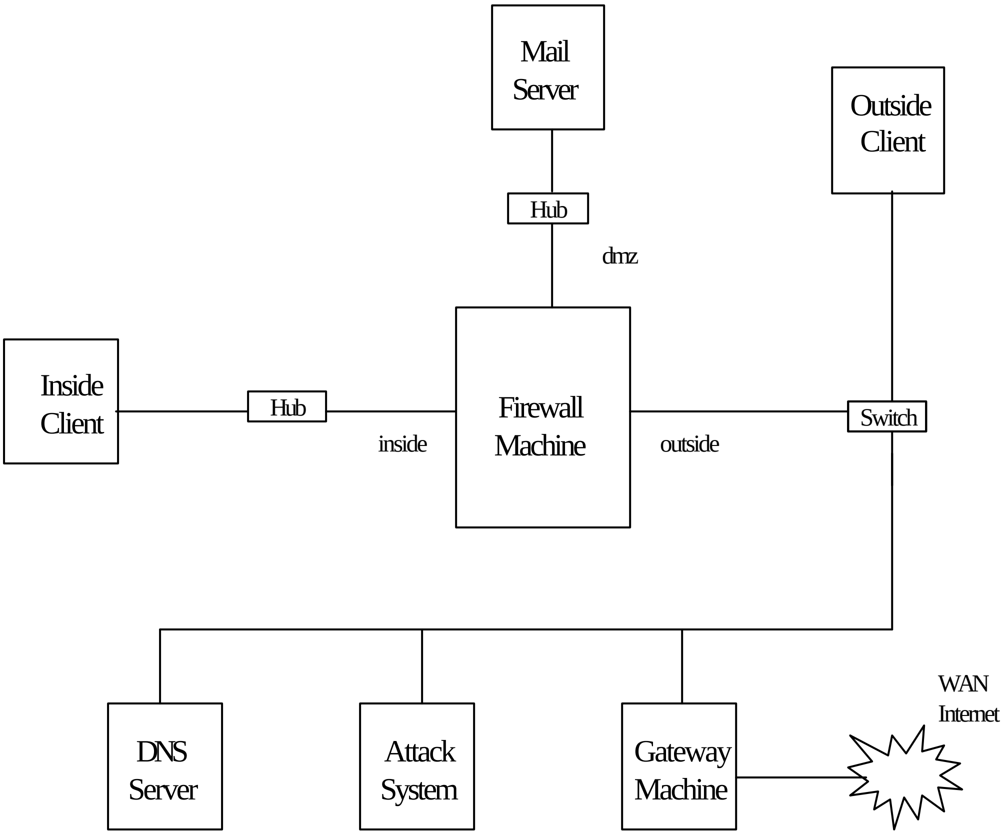
NICs: a) SUN Quad Ethernet NIC (270 5406-06-Rev01) – 2 adaptors used
b) NIC on Motherboard (4116914000-R4G)

Software: Solaris 7 (with all patches installed up to and including 17 July 2003)

c. Firewall running on Solaris 8:

Hardware:
CPU: SUNW UltraSPARC III running on SUN Ultra 5_10 (270 MHz)
512 Mb RAM
4.3 Gb Hard Disk
CD-ROM
3.5 inch Floppy Disk Drive
Monitor and Keyboard
NICs: a) SUN Quad Ethernet NIC (270 4366-04-Rev02) – 2 adaptors used
b) NIC on Motherboard (4116959000-R2e-03)
Software: Solaris 8 (with all patches installed up to and including 17 July 2003)

8. For each of the above three machines hosting the firewall, the machine was connected in the following network configuration:



(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

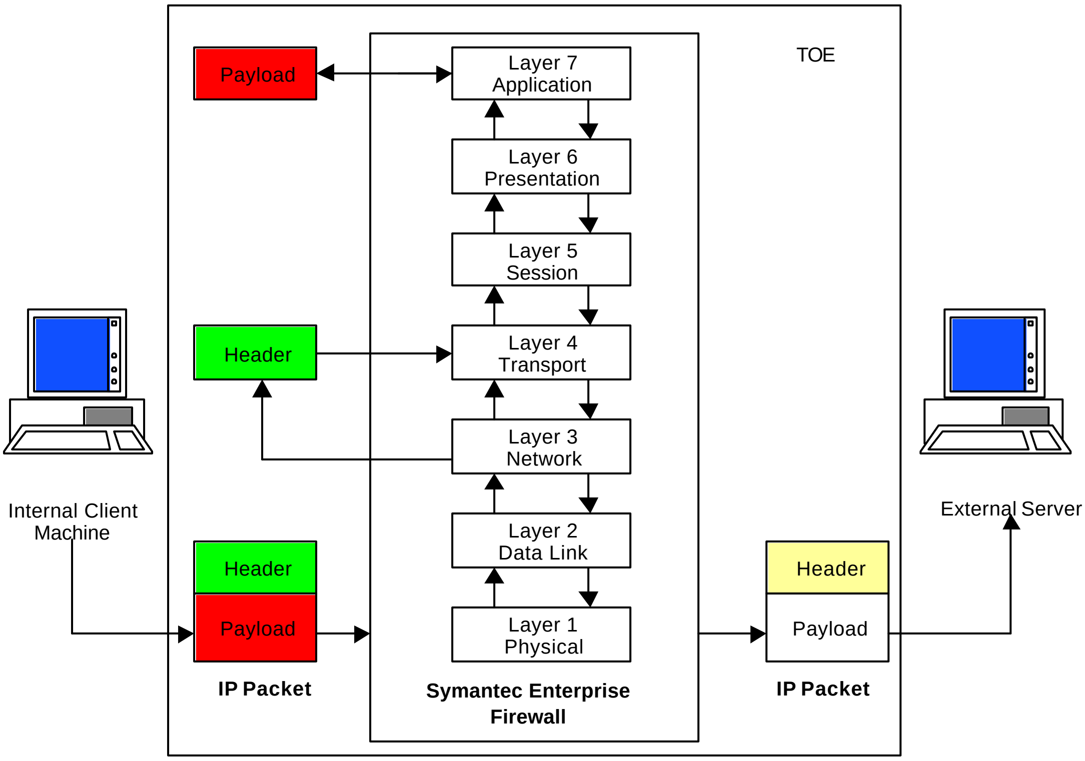
1. This annex gives an overview of the main architectural features of the product that are relevant to the security of the TOE. Further specification of the scope of the evaluation is given in various sections above.

Architectural Features

2. The product is an application-level firewall running on Windows 2000, Solaris 7 or Solaris 8. It uses a set of application-specific security proxies 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 Open Systems Interconnection (OSI) 7-layer model. 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.

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

TSF Interface

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

a. The administrator's interface via the SRMC/RCU.

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 administrator's interface via the SRMC/RCU provides the means by which the administrator can configure and control all subsystems of the firewall.

Design Subsystems

10. The product consists of three main subsystems, which are all security-enforcing:

a. Management Functions. This subsystem enables the administrator to define the packet filters, proxies and authorisation rules. It also allows the administrator to configure the product's audit functions.

b. Firewall Functions. This subsystem controls the mediation of network data and provides controls to protect the security of data and services on the product.

c. Audit Functions. This subsystem records all audit events relevant to the firewall. It also provides event viewing and filtering facilities.

Operating System Dependencies

11. The operating system (i.e. Windows 2000, Solaris 7 or Solaris 8) defines the administrators' security attributes, rights and privileges. It also controls the operating system auditing functionality and controls the system time.

Hardware and Firmware Dependencies

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

- Interrupts and Exceptions
- Processor Execution Levels
- Memory Allocation
- System Clock

(This page is intentionally left blank)