UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UKAS PRODUCT CERTIFICATION

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P205

Symantec Enterprise Firewall

Version 8.0

running on specified platforms

Issue 1.0

July 2004

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham GL51 0EX
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:

CERTIFICATION STATEMENT

Symantec Enterprise Firewall, Version 8.0, is an application-level firewall. A set of application-specific security proxies can be configured to validate each attempt to pass data in or out of the network that is secured by the firewall.

Symantec Enterprise Firewall, Version 8.0, 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, augmented with ALC_FLR.1, for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Head of the Certification Body, UK IT Security Evaluation and Certification Scheme
Date authorised	22 July 2004

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

BGE	Broadcom Gigabit Ethernet
CC	Common Criteria
CD-ROM	Compact Disc – Read-only Memory
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
DMZ	De-militarised Zone
DNS	Domain Name Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
MD5	Message Digest 5
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
NNTP	Network News Transfer Protocol
OSI	Open System Interconnection
PDF	Portable Document Format
POP3	Post Office Protocol version 3
RTSP	Real-time Streaming Protocol
SESA	Symantec Enterprise Security Architecture
SFR	Security Functional Requirement
SGMI	Security Gateway Management Interface
SMTP	Simple Mail Transfer Protocol
SoF	Strength of Function
SP	Service Pack
SRL	Secure Remote Login
SYN	SYNchronise
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UDP	User Datagram Protocol
UKSP	United Kingdom Scheme Publication
VPN	Virtual Private Networking

(This page is intentionally left blank)

REFERENCES

a. Security Target for Symantec Enterprise Firewall Version 8.0,
Symantec Corporation,
T462\ST, Issue 1.0, 8 July 2004.

b. Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Common Criteria Interpretation Management Board,
CCIMB-2004-01-001, Version 2.2 Revision 256, January 2004.

c. Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements,
Common Criteria Interpretation Management Board,
CCIMB-2004-01-002, Version 22, January 2004.

d. Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
Common Criteria Interpretation Management Board,
CCIMB-2004-01-003, Version 2.2 Revision 256, January 2004.

e. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Interpretation Management Board,
CCIMB-2004-01-004, Version 2.2 Revision 256, January 2004.

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 1.1, October 2003.

i. Evaluation Technical Report: Common Criteria EAL4 Evaluation of
Symantec Enterprise Firewall Version 8.0,
BT Syntegra CLEF,
LFS/T462/ETR, Issue 1.0, May 2004.

j. Common Criteria Certification Report: Symantec Gateway Security, Version 2.0,
5400 Series (Firewall Engine only),
UK IT Security Evaluation and Certification Scheme,
P203, Issue 2.0, April 2004.

k. Common Criteria Certification Report: Symantec Enterprise Firewall, Version 7.0.4,
UK IT Security Evaluation and Certification Scheme,
P198, Issue 1.0, November 2003.

l. Common Criteria Certification Report: Symantec Enterprise Firewall, Version 7.0,
UK IT Security Evaluation and Certification Scheme,
P171, Issue 2.0, November 2003.

m. Release Notes: The Certified Symantec Enterprise Firewall Version 8.0,
Symantec Corporation,
Issue 1.8, 22 July 2004.

n. Symantec Enterprise Firewall Installation Guide,
Symantec Corporation,
Documentation Version 8.0, 10 March 2004,
US edition: Part Number 10202273; International edition: Part Number 10234812-IN.

o. Symantec Enterprise Firewall Administrator's Guide,
Symantec Corporation,
Documentation Version 8.0, 10 March 2004.

p. Symantec Security Gateways Reference Guide,
Symantec Corporation,
Documentation Version 8.0.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of the Symantec Enterprise Firewall, Version 8.0, 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:

Symantec Enterprise Firewall, Version 8.0.

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

4. The product is an Internet Protocol (IP) application proxy and packet-filtering firewall. The application proxy provides connection services on behalf of hosts within a secured network. The packet filtering allows acceptance and refusal of data, based on the attributes of the data packets.

5. All traffic between each network attached to the TOE must flow through the firewall. Packets enter the Transmission Control Protocol (TCP) / IP stack of the firewall. Various scanning techniques are applied and completed via 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.

6. The product's security proxies perform the following functions:

a. examine the contents of packets;

b. allow or deny connection based on IP address, user, time, type of service and interface used;

c. control the direction and type of operations for applications;

d. log all session data.

7. The product also provides the following functions:

a. protection against SYN Flood attacks;

b. protection against Denial of Service attacks;

c. protection against port scanning.

8. Details of the evaluated configuration of the TOE, including its guidance documents, are provided in Annex A.

9. An overview of the product security architecture is provided in Annex B.

TOE Scope

10. The scope of the TOE is Symantec Enterprise Firewall, Version 8.0.

11. The TOE consists of the following software:

a. The firewall itself.

b. The Security Gateway Management Interface (SGMI). This is supplied as part of the above firewall software; it is accessed via an SGMI client workstation, by inputting an administrator's user name and password. It is used by the administrator for local administration of the TOE, e.g. policy, location, system monitoring, settings and reports.

12. Part of the security of the TOE is supported by security functionality provided by the firewall operating system, the SGMI client operating system and the authentication server (as outlined in paragraphs 13, 14 and 15 respectively below). Those are all part of the environment of the TOE, so they are all outside the scope of the evaluation.

13. The firewall runs on one of the following operating systems:

a. Microsoft Windows 2000 Advanced Server with Service Pack (SP) 4 (hereinafter referred to as 'Windows 2000');

b. Microsoft Windows Server 2003 Standard Edition (hereinafter referred to as 'Windows 2003');

c. Sun Microsystems Solaris Version 8 (64 bit) with all patches installed up to and including 3 September 2003 (hereinafter referred to as 'Solaris 8');

d. Sun Microsystems Solaris Version 9 (64 bit) with all patches installed up to and including 3 September 2003 (hereinafter referred to as 'Solaris 9').

14. The SGMI client workstation runs on either Windows 2000 or Windows 2003, using Internet Explorer 6.0 SP1 with Java Plug-in version 1.4.2_02. (The choice of operating system for the SGMI client workstation is independent of the choice of operating system for the firewall in paragraph 13 above.) No other application or TOE-specific software is loaded onto the SGMI client workstation for it to run the SGMI; the SGMI applet simply downloads automatically from the firewall when an administrator connects the browser to the firewall for the first time. If the Java plug-in is not already installed in the browser, it can also be downloaded from the firewall. The SGMI client hardware must be connected to a dedicated Network Interface Card (NIC) on the machine hosting the firewall, via a physically secure connection from a specific IP address, and the SGMI client hardware must be physically contained in the same room as that machine.

15. One-time password authentication for Telnet connections and File Transfer Protocol (FTP) connections is provided by a commercially-available, external authentication server on an internal network (e.g. a De-militarised Zone (DMZ) - see Annex A, paragraph 15). That server is required to be compatible with the TOE; currently two such servers are available:

a. RSA Secure Dynamics 'SecurID' authentication server for one-time passwords;

b. PassGo Technologies 'Defender' token generator of a one-time password based on a seed value.

16. Local administration of the firewall via the SGMI is within the scope of the evaluation. Remote administration of the firewall is outside the scope of the evaluation.

17. The following protocols are within the scope of the evaluation:

- Hypertext Transfer Protocol (HTTP);
- User Datagram Protocol (UDP);
- File Transfer Protocol (FTP);
- Ping;
- Domain Name Service (DNS);
- Telnet;
- Simple Mail Transfer Protocol (SMTP);
- Network Time Protocol (NTP);
- Real-time Streaming Protoc ol (RTSP);
- Internet Protocol (IP);
- Network News Transfer Protocol (NNTP);
- Post Office Protocol version 3 (POP3);
- RealAudio;
- Transmission Control Protocol (TCP).

18. The following application proxies through the TOE are within the scope of the evaluation:

- HTTP;
- FTP;
- DNS;
- Telnet;
- SMTP;
- NTP;
- NNTP;
- RealAudio.

19. This certification does not address any use of the firewall on operating systems other than those listed in paragraph 13 above. In particular, whilst some of the guidance documents [n-p] also address operation of the firewall on Windows 2000 Server and Sun Solaris Version 8 (32 bit), that use is not addressed by this certification.

20. The following software and hardware features of the product are also outside the scope of the evaluation:

- Virtual Private Networking (VPN) functionality;
- Symantec Enterprise VPN client;
- high availability / load balancing;
- user authentication by one-time password [1];
- wizards;
- H.323 connections;
- remote administration;
- forward filtering;
- Secure Remote Login (SRL);
- Apache Tomcat web server;
- anti-virus;
- anti-spam;
- content filtering;
- live update support;
- event manager;
- policy configuration manager;
- Symantec Enterprise Security Architecture (SESA);
- global Internet Key Exchange (IKE) policy.

Protection Profile Conformance

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

Assurance

22. The Security Target [a] specifies the assurance requirement for the TOE as Common Criteria predefined Evaluation Assurance Level EAL4, augmented with ALC_FLR.1 flaw remediation.

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

Strength of Function Claims

24. The minimum Strength of Function (SoF) claimed for the TOE was SoF-Medium. There are no probabilistic or permutational mechanisms within the TOE; hence no mechanisms have a SoF claim associated with them.

25. 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.

[1] One-time password authentication for Telnet connections and FTP connections is provided by SecurID or Defender, as part of the environment of the TOE, as noted in paragraph 15 above.

Security Policy

26. 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 using the external authentication server, as discussed above under 'TOE Scope' (see paragraph 15).

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

Security Claims

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

29. All of the SFRs, except for FIA_UAU_SERV.1, are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

30. SFR FIA_UAU.4 requires the TOE's environment to provide a single-use authentication mechanism for FTP and Telnet traffic. That mechanism is provided by a commercially-available, external authentication server and is outside the scope of the TOE. SFR FIA_UAU_SERV.1, which is within the scope of the TOE, merely ensures that use of the single-use authentication server is invoked.

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

- information flow control;
- identification and authentication;
- security management;
- protection of the TOE Security Functions (TSF);
- security audit.

Evaluation Conduct

32. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme, as described in UKSP 01 [f] and UKSP 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.

33. 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 Common Criteria evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline.

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

- the EAL4 requirements, augmented with ALC_FLR.1, specified in CC Part 3 [d];
- the Common Evaluation Methodology (CEM) [e].

No subsequent interpretations for CC [b-d] or CEM [e] were applicable to the evaluation.

35. Some results were reused from the following previous evaluations, where such results were still valid for the TOE:

a. the EAL4 (augmented with ALC_FLR.1) evaluation of Symantec Gateway Security, Version 2.0, 5400 Series (Firewall Engine only) (see Certification Report P203 [j]);

b. the EAL4 evaluation of Symantec Enterprise Firewall, Version 7.0.4 (see Certification Report P198 [k]); and

c. the EAL4 evaluation of Symantec Enterprise Firewall, Version 7.0 (see Certification Report P171 [l]).

36. The Certification Body monitored the evaluation, which was carried out by the BT Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [i] to the Certification Body in May 2004. The Certification Body requested further details and, following the CLEF's satisfactory responses, the Certification Body then produced this Certification Report.

General Points

37. 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.

38. 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 product and whether such patches have been evaluated and certified.

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

II. EVALUATION FINDINGS

Introduction

40. 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 [d] headings.

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

Delivery

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

43. The following measures provide security for delivery of the product, including its guidance documents:

a. Symantec or its agent loads the product onto CD-ROMs.

b. The product is then delivered, in a sealed inner box inside a sealed outer box, to the consumer by registered delivery using a reputable delivery firm. Attached to the outside of the outer box is a sealed envelope containing a commercial invoice that provides information about the product. Attached to the outside of the inner box is a bar-coded sticker that identifies the product and its version number.

c. A certificate is despatched separately to the consumer.

d. The consumer should download the Certified Release Notes [m] for the TOE, from Symantec's website at www.symantec.com. (Note: There are also other release notes for the product on that website so, for the evaluated configuration of the TOE, the consumer should take care to download the Certified Release Notes.)

e. The remaining guidance documents are delivered with the product, in the sealed inner box to the consumer, as follows:

i) Installation Guide [n]: in soft-copy (as a Portable Document Format (PDF) file on the product CD-ROMs) and in hard copy;

ii) Administrator's Guide [o] and Reference Guide [p]: in soft-copy (as PDF files on the product CD-ROMs) only, owing to those documents' size.

f. To use the product, the consumer obtains a Licence File from Symantec's website. To obtain that file, the consumer inputs two separate (but matching) items of information:

i) the 'software serial number', as provided on the certificate at c. above; and

ii) the 'software Symantec id', which is a number (unique to each instantiation of the product) obtained via the SGMI by accessing the *System folder > System information* tab.

g. If a Licence File is obtained successfully, this provides assurance to the consumer that the delivered product is a genuine Symantec product that has not been tampered with.

h. Using the guidance in the Certified Release Notes [m], the consumer should verify that the product identifies itself as Symantec Enterprise Firewall, Version 8.0.

44. The primary considerations governing the security of web-based delivery of the Certified Release Notes [m] are as follows:

a. standard procedures associated with a well-managed web interface must be followed;

b. the document is downloaded as a PDF file.

Installation and Guidance Documentation

45. The Certified Release Notes [m] describe the procedures that must be followed to install and configure the TOE, and operate it securely, and include warnings that identify unevaluated functionality. Those notes also include procedures that must be followed to configure the environment. Hence it is recommended that those notes are read first.

46. Further guidance is provided in the Installation Guide [n], the Administrator's Guide [o] and the Reference Guide [p].

47. The intended audience of the installation and guidance documents is the firewall administrator.

Flaw Remediation

48. Symantec's flaw remediation procedures for the product include providing flaw information, corrections and guidance to consumers.

49. Hotfixes are available to consumers from the *'downloads: product updates'* portal for the product on Symantec's website at www.symantec.com. An MD5 checksum can be used to check a downloaded hotfix. For each hotfix, the following details are provided via that portal:

- prerequisites;
- included modules;
- fix descriptions;
- installation instructions;
- uninstallation instructions.

50. Each consumer who reports a flaw is informed of the outcome by Symantec. In some cases, the flaw is only relevant to that particular consumer. If a flaw results in corrective action being necessary for all consumers (e.g. by means of a hotfix), then consumers must obtain the hotfix from Symantec's website as outlined above.

51. The Installation Guide [n] and the Administrator's Guide [o] advise consumers to visit Symantec's website for the latest information regarding product updates and upgrades. Such information is provided on that website on:

- the *'downloads: product updates'* portal for the product (as outlined above);
- the *'technical support: security advisories'* portal;
- the *'technical support: knowledge base'* portal for the product.

52. Also, all consumers with a maintenance contract for the product are informed by their Symantec Customer Support Engineer when a hotfix is available for the product on that website.

Strength of Function

53. The SoF claim for the TOE was as given above under 'Strength of Function Claims'. The Evaluators confirmed that there are no mechanisms for which a SoF claim is appropriate.

Vulnerability Analysis

54. The Evaluators' vulnerability analysis was based on public domain sources and on the visibility of the following given by the evaluation process:

- the TOE;
- the firewall operating system;
- the SGMI client operating system;
- the authentication server.

Testing

55. The TOE was tested against the set of external interfaces that comprise the TOE Security Functions Interface (TSFI), as listed under 'TSF Interface' in Annex B.

56. The Developer performed tests using all aspects of the TSFI. Those tests also exercised:

- all related security functions specified in the Security Target [a];
- all high level design subsystems identified in Annex B.

57. 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.

58. 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. For each interface of the TSFI, a test that was different from those performed by the Developer was devised wherever possible.

Independent tests were thus performed for the majority of security functions.

59. The Evaluators also devised and performed penetration tests, wherever needed, to confirm the non-exploitability of potential vulnerabilities that had been noted during the evaluation.

60. The Evaluators used the following tools during testing:

- Port Flooding Tool version 1.062 from 7th Sphere;
- Ethersniff – July 2003;
- Nmap version 3.30;
- Ethereal version 0.9.13;
- TcpReplay version 1.3.1;
- IPX_Ping version 2.0 from Magma Concepts.

No other specific evaluation tools were used during the evaluation.

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

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

- all communications protocols and application proxies listed in the Security Target [a];
- protection against SYN Flood attacks;
- protection against Denial of Service attacks (including use of badly formatted IP packets);
- protection against port scanning attacks;
- both static and dynamic Network Address Translation (NAT) options;
- IP address spoof checking.

Platform Issues

63. The TOE was evaluated on each of the platforms specified in Annex A. Strictly therefore the certified configuration excludes other hardware options, e.g. other NICs.

64. 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 appropriate guidance documents [n-p] describe how to set up and manage notifications; they also note that, if audio notification is required, a properly installed and configured sound card is needed.

65. The TOE's mechanisms and interfaces regarding authentication were tested using an external authentication server: the Developer's tests used SecurID and Defender, the Evaluators' tests used SecurID. The Evaluators are aware of no issues regarding the authentication servers that would suggest that the TOE would behave differently on either SecurID or Defender.

66. A CD-ROM drive is required to support installation of the TOE, which is delivered on CD-ROM. Removable read/write media are also required, but only to support the archiving of configuration and audit data. The TOE software does not require use of removable read/write media; hence they are not part of the hardware platform on which the TOE was evaluated.

III. EVALUATION OUTCOME

Certification Result

67. 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 Symantec Enterprise Firewall, Version 8.0, meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4, augmented with ALC_FLR.1, for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the platforms specified in Annex A.

Recommendations

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

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

70. The TOE should be used in accordance with the guidance documents included in its evaluated configuration [m-p]. The TOE should also be used in accordance with a number of environmental considerations as specified in its Security Target [a].

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

72. The product provides some features that were not within the scope of the evaluation, as identified above in paragraph 20 under 'TOE Scope'. Those features should therefore not be used if the TOE is to comply with its evaluated configuration.

(This page is inte ntionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is the Symantec Enterprise Firewall, Version 8.0. It consists of the following software:

- the firewall itself;
- the SGMI.

2. The product is delivered on two CD-ROMs to the consumer, as follows:

   a. one CD-ROM labelled 'Symantec Enterprise Firewall Version 8.0 Windows 2000/2003 (Part Number 10202265)';

   b. one CD-ROM labelled 'Symantec Enterprise Firewall Version 8.0 Solaris 8 & 9 (Part Number 10202264)'.

Note: There is no difference between the US edition of those CD-ROMs and the international edition of those CD-ROMs. Hence, in each of those editions, the CD-ROMs have the above part numbers.

3. The consumer installs and configures the version of the TOE for their firewall operating system (i.e. for Windows 2000 or Windows 2003, or for Solaris 8 or Solaris 9), using the appropriate CD-ROM above.

TOE Documentation

4. The guidance documents evaluated were:

- Certified Release Notes [m];
- Installation Guide [n];
- Administrator's Guide [o];
- Reference Guide [p].

5. The Certified Release Notes [m] are downloaded as a PDF file from Symantec's website. The other guidance documents are delivered with the product as follows:

- Installation Guide [n]: in soft-copy (PDF file on the CD-ROMs) and in hard-copy;
- Administrator's Guide [o]: in soft-copy (PDF file on the CD-ROMs) only;
- Reference Guide [p]: in soft-copy (PDF file on the CD-ROMs) only.

6. For the TOE, the Certified Release Notes [m] take precedence over the remaining guidance documents [n-p].

7. The set of guidance documents [m-p] applies equally to Windows and Solaris, as the firewall operating system.

8. Further discussion of the guidance documents [m-p] is given above under 'Delivery', 'Installation and Guidance Documentation' and 'Flaw Remediation'.

TOE Configuration

9. The following configurations of the TOE were used for testing:

a. The TOE installed on a machine running Windows 2000, with the SGMI client workstation running Windows 2000 (as detailed in paragraph 11.a below);

b. The TOE installed on a machine running Windows 2003, with the SGMI client workstation running Windows 2003 (as detailed in paragraph 11.b below);

c. The TOE installed on a machine running Solaris 8, with the SGMI client workstation running Windows 2000 (as detailed in paragraph 11.c below); and

d. The TOE installed on a machine running Solaris 9, with the SGMI client workstation running Windows 2003 (as detailed in paragraph 11.d below).

Environmental Configuration

10. Part of the security of the TOE is supported by security functionality provided by the firewall operating system, the SGMI client operating system and the authentication server. Those are all part of the environment of the TOE, so they are outside the scope of the evaluation.

11. The four platforms used by the Evaluators to test the TOE, as follows, were equivalent to those used by the Developer to test the TOE:

a. for the Firewall running on Windows 2000:

For the Firewall: Hardware: CPU: Intel Pentium 4 (3.066 GHz). 512 Mb RAM. 30 Gb Hard Disk (ST340014A). Monitor (Panasync E70), Keyboard (ALPS PC concept) and Mouse (AOpen). NICs: 4 x Intel Pro/1000MT Dual Port Server Adaptor. Software: Windows 2000 Advanced Server SP4 (with no subsequent hotfixes).
For the SGMI Client: Hardware: CPU: Intel Pentium 4 (2.4 GHz). 512 Mb RAM. NIC: Broadcom NetXtreme Gigabit Ethernet. Software: a) Windows 2000 Advanced Server SP4 (with no subsequent hotfixes). b) Microsoft Internet Explorer 6.0 SP1 (with no subsequent hotfixes). c) Java Plug-in version 1.4.2_02.

b. for the Firewall running on Windows 2003:

For the Firewall:
Hardware:
CPU: Intel Pentium 4 (3.066 GHz).
512 Mb RAM.
30 Gb Hard Disk (ST340014A).
Monitor (Panasync E70), Keyboard (ALPS PC concept) and Mouse (AOpen).
NICs: 4 x Intel Pro/1000MT Dual Port Server Adaptor.
Software:
Windows Server 2003 Standard Edition (with no subsequent SPs or hotfixes).

For the SGMI Client:
Hardware:
CPU: Intel Pentium 4 (2.4 GHz).
512 Mb RAM.
NIC: Broadcom NetXtreme Gigabit Ethernet.
Software:
a) Windows Server 2003 Standard Edition (with no subsequent SPs or hotfixes).
b) Microsoft Internet Explorer 6.0 SP1 (with no subsequent hotfixes).
c) Java Plug-in version 1.4.2_02.

c. for the Firewall running on Solaris 8:

For the Firewall:
Hardware:
CPU: 4 x SunW UltraSPARC III+ (1 GHz).
8 Gb RAM.
72 Gb Hard Disk (Sun).
Monitor (Sun), Keyboard (Sun) and Mouse (Sun).
NICs: 4 port Sun 10/100 Peripheral Component Interconnect (PCI) (qfe0, qfe1, qfe2 and qfe3).
Software:
Sun Solaris 8 (with all patches installed up to and including 3rd September 2003.

For the SGMI Client:
Hardware:
CPU: Intel Pentium 4 (2.4 GHz).
512 Mb RAM .
NIC: Broadcom NetXtreme Gigabit Ethernet.
Software:
a) Windows 2000 Advanced Server SP4 (with no subsequent hotfixes).
b) Microsoft Internet Explorer 6.0 SP1 (with no subsequent hotfixes).
c) Java Plug-in version 1.4.2_02.

d. for the Firewall running on Solaris 9:

For the Firewall:

Hardware:

CPU: SunW UltraSPARC IIIi (1 GHz).

1 Gb RAM.

36 Gb Hard Disk (Sun).

Monitor (Sun), Keyboard (Sun) and Mouse (Sun).

NICs: 4 x Broadcom Gigabit Ethernet (BGE) card on Motherboard.

Software:

Sun Solaris 9 with all patches installed up to and including 3rd September 2003.

For the SGMI Client:

Hardware:

CPU: Intel Pentium 4 (2.4 GHz).

512 Mb RAM.

NIC: Broadcom NetXtreme Gigabit Ethernet.

Software:

a) Windows Server 2003 Standard Edition (with no subsequent SPs or hotfixes).

b) Microsoft Internet Explorer 6.0 SP1 (with no subsequent hotfixes).

c) Java Plug-in version 1.4.2_02.

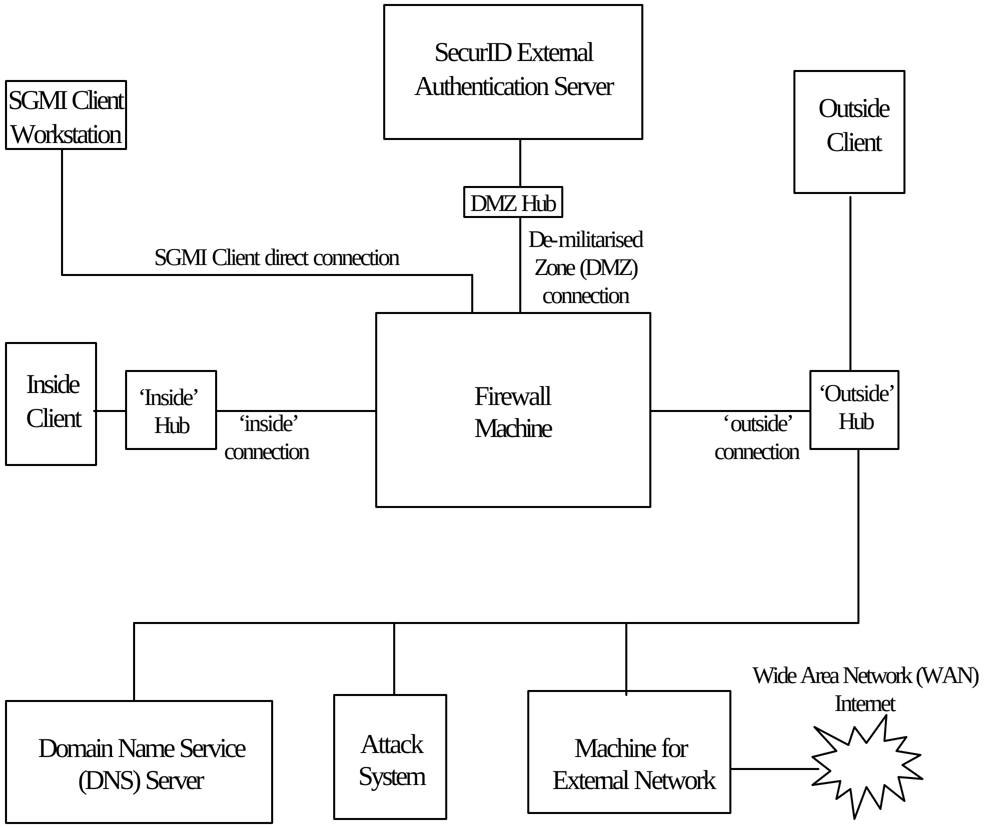
12. The evaluators performed all of their tests on all four of the above platforms, except for those tests that were dependent on the specific operating system hosting the firewall (e.g. Windows-only tests, Solaris-only tests).

13. In each of the above four platforms, the SGMI client workstation was co-located with the machine hosting the firewall and attached to it via a physically secure, direct HTTP connection from a specific IP address. The SGMI was part of the software on the firewall. No TOE-specific software needed to be loaded onto the SGMI client for it to run the SGMI. No other applications were loaded onto the SGMI client. The SGMI applet downloaded automatically from the firewall when an administrator connected the browser to the firewall for the first time.

14. For one-time passwords, the Evaluators tested the TOE using a SecurID authentication server, as follows. As the authentication server is not within the scope of the TOE, the purpose of this test was to test the TOE's mechanisms and interfaces regarding external authentication. Those interfaces and mechanisms were assessed by the Evaluators in other aspects of the evaluation and shown to work in a consistent manner for different types of external authentication. Therefore the Evaluators have no reason to believe that the TOE would behave differently using a Defender authentication server.

For the SecurID Authentication Server:	
Hardware:	ACE Server.
Operating System:	Windows 2000.
Other Software:	RSA ACE/Server 5.1 for Windows.
NIC:	Intel Pro/1000 MT Desktop Adaptor.
Processor:	AMD (1.526 GHz).
Memory:	256 Mb.

15. For each of the four machines hosting the firewall, the machine was connected in the following network configuration:


SecurID External Authentication Server
SGMI Client Workstation
Outside Client
DMZ Hub
De-militarised Zone (DMZ) connection
SGMI Client direct connection
Inside Client
'Inside' Hub
'inside' connection
Firewall Machine
'outside' connection
'Outside' Hub
Wide Area Network (WAN) Internet
Domain Name Service (DNS) Server
Attack System
Machine for External Network

16. The connectivity in that configuration was provided by the following hubs:

- 'inside' hub: Netgear Model GS108 8-port 10/100/1000 Mbps Gigabit switch;
- 'outside' hub: Netgear Model GS108 8-port 10/100/1000 Mbps Gigabit switch;
- DMZ hub: Dell Powerconnect 2508.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

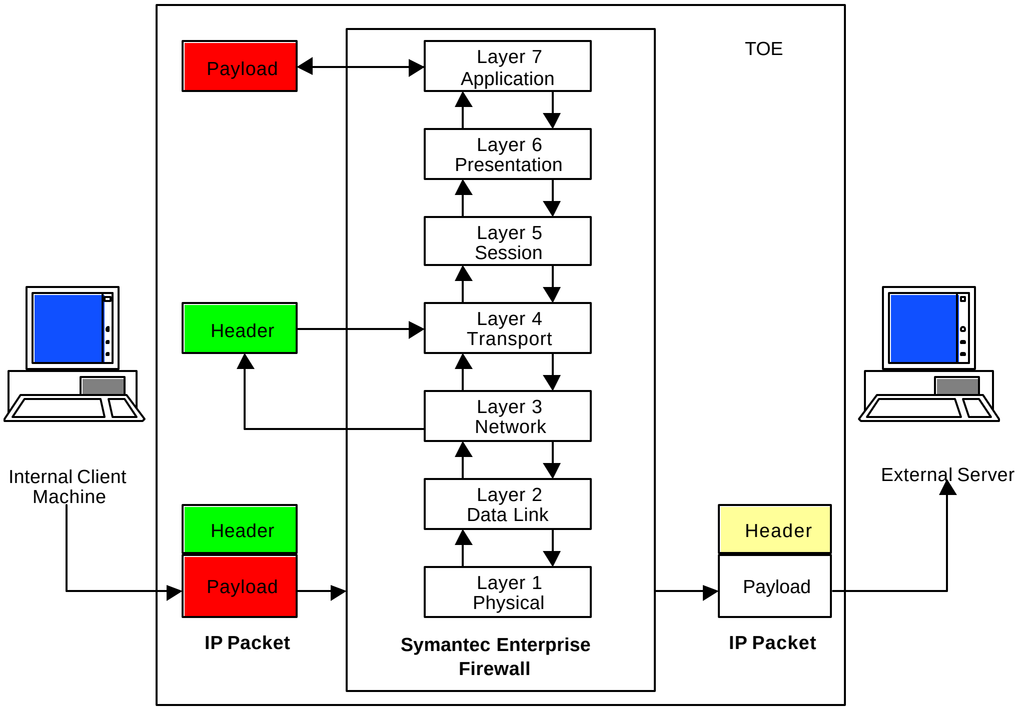
1. This annex gives an overview of the main architectural features of the product that are relevant to the security of the TOE. Further specification of the scope of the evaluation is given in various sections above.

Architectural Features

2. The product is an application-level firewall. 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 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 Open System Interconnection (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 clie nt normally.

6. The product has only one class of user (i.e. the administrator). The administrator is trusted to manage the product, 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 product offers a number of failsafe features, including:

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. if the audit log becomes full, all network connections through the TOE are dropped;

c. internal processes exist to restart any key processes that go down and to terminate any unauthorised processes.

TSF Interface

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

a. The administrator's interface via the SGMI. This enables the administrator to configure and control all subsystems of the product.

b. The interface between the firewall and the firewall operating system. This also gives indirect interfaces to network connections (including the connection for the external authentication server) and to disc backup of configuration and audit files.

Design Subsystems

9. 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 product. It also provides event viewing and filtering facilities.

Operating System Dependencies

10. The firewall operating system defines the administrator's security attributes, rights and privileges. It also controls the operating system auditing functionality and controls the system time.

Hardware and Firmware Dependencies

11. In order to support the product, 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)