UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P203

Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only)

Issue 2.0

April 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. *

* Whilst the Arrangement has not yet been extended to address ALC_FLR.1, a working agreement exists amongst Parties to the Arrangement to recognise the Common Evaluation Methodology ALC_FLR supplement (reference [f] in this report) and the resultant inclusion of ALC_FLR.1 elements in certificates issued by a Qualified Certification Body.

Trademarks:

CERTIFICATION STATEMENT

Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only) is an application-level firewall on an appliance. 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 Gateway Security Version 2.0 5400 Series (Firewall Engine only) has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL4 (i.e. augmented with ALC_FLR.1) for the specified Common Criteria Part 2 extended functionality in the specified environment.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body, UK IT Security Evaluation and Certification Scheme
Date authorised	27 April 2004

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

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
EIDE	Enhanced Integrated Drive Electronics
ETR	Evaluation Technical Report
FSB	Front Side Bus
FTP	File Transfer Protocol
GigE	Gigabit Ethernet
GUI	Graphical User Interface
IP	Internet Protocol
LCD	Liquid Crystal Display
NAT	Network Address Translation
NIC	Network Interface Card
OSI	Open System Interconnection
PDF	Portable Document Format
SFR	Security Functional Requirement
SGMI	Security Gateway Management Interface
SOF	Strength of Function
SP	Service Pack
SRL	Secure Remote Login
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 Gateway Security Version 2.0 5400 Series
(Firewall Engine only),
Symantec Corporation,
T423\ST, Issue 3.3, 26 April 2004.

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. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation,
Common Evaluation Methodology Editorial Board,
CEM-2001/0015R, Version 1.1, February 2002.

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

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

i. CLEF Requirements: Part II – Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02 Part II, Issue 1.1, October 2003.

j. Evaluation Technical Report: Common Criteria Evaluation of
Symantec Enterprise Firewall on Symantec Gateway Security Version 2.0,
BT Syntegra CLEF,
LFS/T423/ETR, Issue 1.0, January 2004.

k. Supplement 1 to Evaluation Technical Report (LFS/T423/ETR, 23 January 2004),
BT Syntegra CLEF,
LFS/T423/Supp1, Issue 1.0, 16 April 2004.

l. Common Criteria Certification Report: Symantec Enterprise Firewall Version 7.0 running on Windows NT 4.0 SP6a,
UK IT Security Evaluation and Certification Scheme,
P171, Issue 2.0, November 2003.

m. Common Criteria Certification Report: Symantec Enterprise Firewall Version 7.0.4 running on Windows 2000 SP3 and on Solaris 7 & 8,
UK IT Security Evaluation and Certification Scheme,
P198, Issue 1.0, November 2003.

n. Common Criteria Certification Report: Symantec Enterprise Firewall on Symantec Gateway Security Version 2.0,
UK IT Security Evaluation and Certification Scheme,
P203, Issue 1.0, March 2004.

o. Release Notes: The Certified Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only),
Symantec Corporation,
Issue 2.5, 27 April 2004.

p. Symantec Gateway Security 5400 Series - Installation Guide
(Supported Appliance models: 5420, 5440, 5441, 5460 and 5461),
Symantec Corporation,
US edition: Part Number 10097551, Issue 2.0, 20 August 2003;
International edition: Part Number 10139289-IN, Issue 2.0, 1 September 2003.

q. Symantec Gateway Security 5400 Series - Administrator's Guide
(Supported Appliance models: 5420, 5440, 5441, 5460 and 5461),
Symantec Corporation,
Issue 2.0, 27 August 2003.

r. Symantec Gateway Security 5400 Series - Reference Guide
(Supported Appliance models: 5420, 5440, 5441, 5460 and 5461),
Symantec Corporation,
Issue 2.0, 27 August 2003.

s. Symantec Gateway Security 5400 Series – Quick Start:
Installing and Setting up Model 5420,
Symantec Corporation,
US edition: Part Number 10097565; International edition: Part Number 10148825-IN.

t. Symantec Gateway Security 5400 Series – Quick Start:
Installing and Setting up Models 5440, 5441, 5460 and 5461,
Symantec Corporation,
US edition: Part Number 10097566; International edition: Part Number 10139296-IN.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of the Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only) 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:

the Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only) with Hotfix HB8000-20031023-00 - December 2003 patch.

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

5. The product is an Internet Protocol (IP) application proxy and packet-filtering firewall. The application proxies provide 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.

6. All traffic between each network attached to the TOE must flow through the firewall. Packets enter the 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.

7. 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.

8. The product also provides the following functions:

a. protection against Syn flooding attacks;

b. protection against Denial of Service attacks;

c. protection against port scanning.

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

10. An overview of the TOE security architecture is provided in Annex B.

TOE Scope

11. The Symantec Gateway Security integrates several network security applications in one appliance, including:

- firewall;
- intrusion detection and prevention;
- anti-virus;
- anti-spam;
- content filtering;
- Virtual Private Network (VPN).

12. The TOE is the firewall application only (other applications such as intrusion detection and prevention, anti-virus, anti-spam, content filtering and VPN are outside the scope of the evaluation). Hence the scope of the TOE is the Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only) with Hotfix HB8000-20031023-00 - December 2003 patch.

13. The product runs on dedicated appliance hardware. The TOE consists of the product's following software:

a. the firewall itself;

b. the Security Gateway Management Interface (SGMI), which is a Graphical User Interface (GUI) used for local administration by the administrator;

c. the 'device driver' for the appliance Liquid Crystal Display (LCD), which is a small screen used to display local administration summary information to the administrator.

14. The SGMI is a Java-based, standalone GUI that includes policy, system-monitoring, settings and reports. The SGMI is accessed from an SGMI workstation running Windows 2000 Service Pack (SP) 4, making use of Internet Explorer 6.0 (with Java Plug-in Version 1.3.1_04). The SGMI workstation must be connected to one of the appliance's network interfaces via a physically secure connection, from a specific IP address. The SGMI software is included in the appliance. No other software needs to be loaded onto the SGMI workstation for it to run the SGMI. The SGMI applet downloads automatically from the appliance when an administrator connects their browser to the appliance for the first time.

15. The LCD displays the Symantec Gateway Security version number and the options for startup self-tests, performance monitoring and the system menu. The LCD can be locked from the SGMI.

16. One-time password authentication for Telnet/File Transfer Protocol (FTP) connections is provided by a commercially-available, external authentication server on the internal network. 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.

17. Local administration of the firewall (i.e. via the SGMI and the LCD) is within the scope of the evaluation. Remote administration is outside the scope of the evaluation.

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

- HTTP;
- UDP;
- FTP;
- Ping;
- DNS;
- Telnet;
- SMTP;
- NTP;
- RTSP;
- IP;
- NNTP;
- POP3;
- RealAudio;
- TCP.

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

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

20. Part of the security of the TOE is supported by security functionality provided by the appliance’s operating system, the SGMI’s 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.

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

- VPN functionality;
- Symantec Enterprise VPN client;
- high availability / load balancing;
- user authentication by one-time password [1];
- setup wizard;

[1] One-time password authentication for Telnet/FTP connections is provided by SecurID or Defender as part of the environment of the TOE.

- H.323 connections;
- remote administration;
- forward filtering;
- Secure Remote Login (SRL);
- console port access;
- Apache Tomcat web server;
- intrusion detection and prevention;
- anti-virus;
- anti-spam;
- content filtering;
- live update support;
- event manager;
- policy configuration manager.

Protection Profile Conformance

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

Assurance

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

24. 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

25. 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.

26. 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

27. 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’.

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

Security Claims

29. 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.

30. 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.

31. 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.

32. 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

33. 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 [g] and UKSP 02 Parts I and II [h-i]. 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.

34. 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.

35. 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 CEM supplement on Flaw Remediation [f];
- the appropriate CC and CEM interpretations.

36. Some results were reused from the previous EAL4 evaluation of Symantec Enterprise Firewall Version 7.0 on Windows NT 4.0 SP6a, and the previous EAL4 evaluation of Symantec Enterprise Firewall Version 7.0.4 on Windows 2000 SP3 and on Solaris 7 and 8, where such results were still valid for the TOE. (See Certification Reports P171 [l] and P198 [m].)

37. 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) [j] to the Certification Body in January 2004. The Certification Body requested further details and, following the CLEF's satisfactory responses, the Certification Body then produced Issue 1.0 of this Certification Report [n].

38. The Developer subsequently proposed two changes:

a. to change the name of the TOE (from 'Symantec Enterprise Firewall on Symantec Gateway Security Version 2.0') to 'Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only)';

b. to upgrade the assurance requirement for the TOE (from EAL4) to EAL4 augmented with ALC_FLR.1 flaw remediation.

39. Following further evaluation work to assess those changes, the CLEF submitted an ETR Supplement [k] to the Certification Body in April 2004. The Certification Body requested further details and, following the CLEF's satisfactory responses, the Certification Body then produced this Issue 2.0 of the Certification Report.

General Points

40. 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.

41. 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.

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

II. EVALUATION FINDINGS

Introduction

43. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [j] and ETR Supplement [k], under the CC Part 3 [d] headings.

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

Delivery

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

46. The following measures provide security for delivery of the TOE, including its guidance documentation:

a. Symantec or its agent pre-loads the TOE (except for Hotfix HB8000-20031023-00 - December 2003 patch), onto the appliance for delivery to the consumer.

b. The appliance is then delivered in a sealed box to the consumer, by registered delivery, using a reputable delivery firm. A Licence Certificate (including a valid activation number, specific to the appliance's serial number) is despatched separately to the consumer, by email, to arrive after the product has been delivered.

c. The consumer should download the Certified Release Notes [o] in Portable Document Format (PDF) 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.)

d. The remaining guidance documents [p-t] are delivered, with the appliance in the sealed box, to the consumer in both:

- soft-copy (as PDF files on a CD-ROM); and
- hard-copy (except for the Administrator's Guide [q] and Reference Guide [r], owing to their size).

e. To activate the product, the consumer must enter a valid Licence Key. That key is obtained from Symantec's website, by inputting the consumer's details, the appliance serial number and quoting the valid activation number provided on the Licence Certificate.

f. Using the guidance in the Certified Release Notes [o], the consumer should verify that the appliance identifies the pre-loaded software as Symantec Gateway Security Version 2.0 (with no patches).

47. The following measures provide security for web-based delivery of the evaluated Hotfix:

a. Hotfixes for the product are available only from Symantec's website at www.symantec.com.

b. Using the guidance in the Certified Release Notes [o], consumers should download and install Hotfix HB8000-20031023-00 - December 2003 patch from that website.

c. Using an MD5 checksum utility, the consumer can generate an MD5 checksum for the downloaded patch and compare it with the MD5 hash value published for that patch on Symantec's website, to confirm the integrity of the patch. (For reference, the MD5 hash value published on Symantec's website for Hotfix HB8000-20031023-00 - December 2003 patch is 3C8CA2C3EA9A2B544EC29656C6CBB781.) Symantec's website provides a link to obtain an MD5 checksum utility but, to guard against spoofing, the consumer could instead obtain an MD5 checksum utility from an independent source.

d. Using the guidance in the Certified Release Notes [o], the consumer should verify that the appliance identifies that the specified patch has been installed.

48. The primary considerations governing the security of web-based delivery of the Certified Release Notes [o] and Hotfix HB8000-20031023-00 - December 2003 patch are as follows:

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

b. the Certified Release Notes are downloaded as a PDF file;

c. an MD5 checksum can be used to check the authenticity of the downloaded patch.

Installation and Guidance Documentation

49. The Certified Release Notes [o] 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.

50. Further guidance is provided in the following documents:

- Installation Guide [p];
- Administrator's Guide [q];
- Reference Guide [r];
- Quick Start - Model 5420 [s];
- Quick Start - Models 5440, 5441, 5460 and 5461 [t].

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

Flaw Remediation

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

53. 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.

54. 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 above.

55. The product's installation and guidance documents (e.g. the Installation Guide [p] and the Administrator's Guide [q]) advise consumers to visit Symantec's website for the latest information regarding product updates and upgrades. Such information is provided on Symantec's website on:

a. the 'downloads: product updates' portal for the product (as noted above);

b. the 'technical support: security advisories' portal;

c. the 'technical support: knowledge base' portal for the product.

56. 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

57. 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

58. The Evaluators' vulnerability analysis was based on public domain sources and on the visibility of the TOE, and the appliance's operating system, given by the evaluation process.

Testing

59. 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.

60. 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.

61. 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.

62. 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.

63. 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.

64. 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.

No other specific evaluation tools were used during the evaluation.

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

66. 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 flooding attacks;
- protection against Denial of Service attacks;
- protection against port scanning;
- both static and dynamic NAT options;
- IP address spoof checking.

Platform Issues

67. The TOE was evaluated on the appliance specified in Annex A.

68. There are five models of the appliance. The differences are their memory, processor, hard disc size and NICs installed (however their NICs all use the same type of network device driver).

69. Each model runs the same version of the TOE (including the Hotfix) on the same version of the appliance's operating system.

70. The Developer tests on the five models showed no differences in operation between them. The Evaluators' tests were performed using the 5440 model. The Evaluators are aware of no issues regarding the above differences (including NICs) between models that would suggest that the TOE would behave differently on any of the five models of the appliance.

71. The TOE's mechanisms and interfaces regarding authentication were tested using an external authentication server. The Developer 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.

72. 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

73. After due consideration of the ETR [j] and ETR Supplement [k], produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only) with Hotfix HB8000-20031023-00 - December 2003 patch meets the CC Part 3 augmented requirements of Evaluation Assurance Level EAL4 (i.e. augmented with ALC_FLR.1) for the specified CC Part 2 extended functionality in the specified environment.

Recommendations

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

75. 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’ and ‘Evaluation Findings’.

76. The TOE should be used in accordance with the guidance documentation included in its evaluated configuration [o-t]. The TOE should also be used in accordance with a number of environmental considerations as specified in its Security Target [a].

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

78. The product provides some features that were not within the scope of the evaluation, 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 TOE is the Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine only) with Hotfix HB8000-20031023-00 - December 2003 patch. That consists of the following software:

- the firewall;
- the SGMI;
- the LCD device driver.

TOE Documentation

2. The guidance documents evaluated were:

- Certified Release Notes [o];
- Installation Guide [p];
- Administrator’s Guide [q];
- Reference Guide [r];
- Quick Start - Model 5420 [s];
- Quick Start - Models 5440, 5441, 5460 and 5461 [t].

3. The Certified Release Notes [o] are downloaded as a PDF file from Symantec’s website.

4. The other guidance documents are delivered with the appliance as follows:

- documents [p, s, t]: as soft-copy (PDF files on a CD-ROM) and hard copy;
- documents [q, r]: as soft copy (PDF files on a CD-ROM) only.

5. The US edition of the CD-ROM has Part Number 10139303; the international edition of the CD-ROM has Part Number 10139303-IN. There is no significant difference between the US edition and the international edition of the CD-ROM; similarly there is no significant difference between the US edition and the international edition of the guidance documents thereon.

6. Further discussion of the guidance documents is given above under ‘Delivery’, ‘Installation and Guidance Documentation’ and ‘Flaw Remediation’.

TOE Configuration

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

a. TOE, as part of Symantec Gateway Security Version 2.0, on a Model 5440 appliance;

b. SGMI accessed from an SGMI workstation running Windows 2000 SP4, using Internet Explorer 6.0 (with Java Plug-in Version 1.3.1_04).

Environmental Configuration

8. The required hardware environment for the TOE is one of the 5400 series of appliances (i.e. Models 5420, 5440, 5441, 5460 and 5461).

9. Each of those five models runs the same version of the TOE (including the Hotfix) on the same version of the appliance's operating system. The differences between those five models are their memory, processor, hard disc size and NICs installed (however their NICs all use the same type of network device driver software, namely the Intel E1000 driver).

10. The Developer tested the TOE on all five models (i.e. 5420, 5440, 5441, 5460 and 5461). Those tests included various Syn Flood attacks, other Denial Of Service tests (including use of badly formatted IP packets) and tests to check that the TOE can detect port scanning attacks. The Evaluators tested the TOE on Model 5440.

11. Confidence was gained that the TOE behaves in exactly the same manner on all five models, as their underlying operating system is exactly the same version, and the tests showed no differences in their operation. Therefore the Evaluators are aware of no issues regarding the differences between the five models (including NICs) that would suggest that the TOE would behave differently on any of the five appliances in the 5400 series (i.e. Models 5420, 5440, 5441, 5460 and 5461).

12. Part of the security of the TOE is supported by security functionality provided by the appliance's operating system, the SGMI's 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.

13. The environmental configuration used by the Evaluators to test the TOE was equivalent to that used by the Developer to test the TOE, as follows:

a. Appliance (including LCD):

Hardware:	Symantec Gateway Security Version 2.0 – Model 5440
Operating System:	Red Hat Linux 7.2 with a Linux 2.4.18 kernel.
Other Software:	None.
Network Interface Cards (NICs):	Total of 6 Gigabit Ethernet (GigE) ports, comprising:
Ethernet on motherboard:	2 x 10/100/1000 Base-T Ethernet network interfaces;
Ethernet network interfaces:	2 x Intel Pro/1000 MT Dual port server adapters.
User (Administrator) Interface:	2 line x 16 character Appliance LCD screen.
Processor:	Intel 2.4 GHz 533 FSB Xeon.
Hard Disk:	80 Gb EIDE.
Memory:	1 Gb.

b. SGMI workstation:

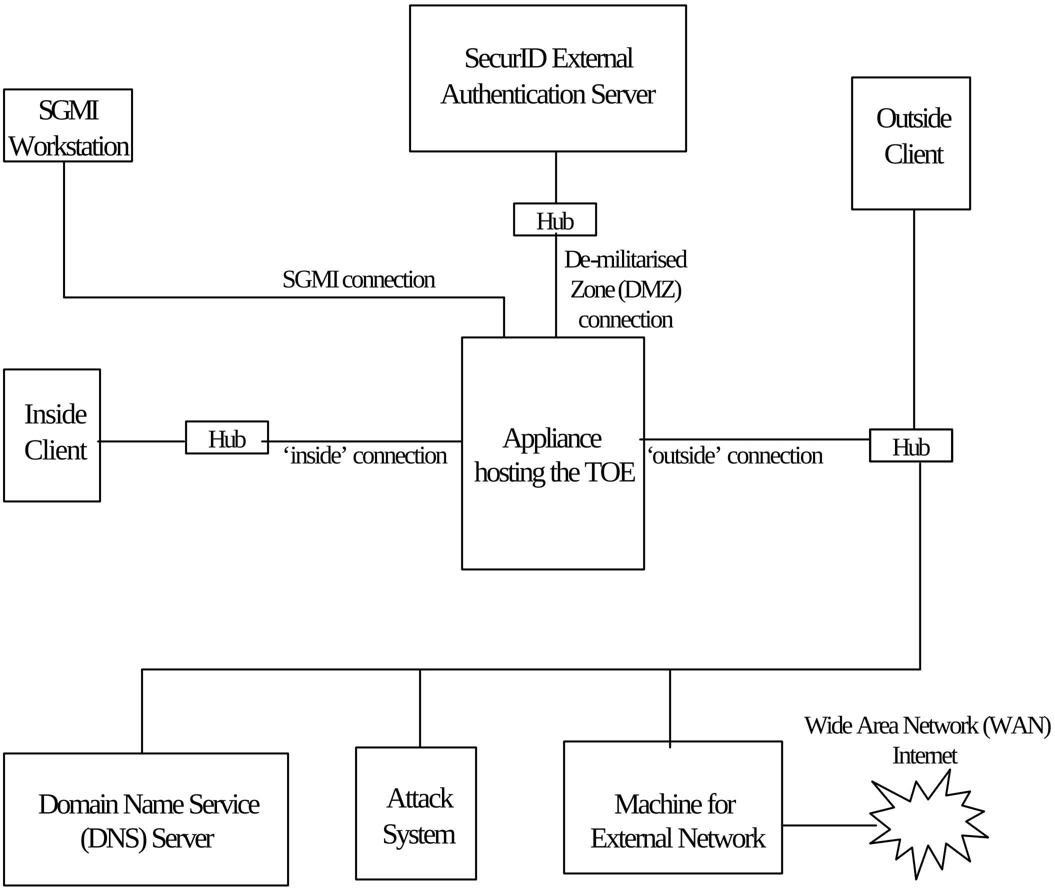
Hardware:	The SGMI workstation was co-located with the above Appliance hardware and attached to it via a physically secure, direct HTTP connection, from a specific IP address.
Operating System:	Windows 2000 SP4.
Other Software:	Internet Explorer 6.0; Java Plug-in Version 1.3.1_04. No other applications were loaded onto the SGMI workstation. No TOE specific software needs to be loaded onto the SGMI workstation, for the workstation to run the SGMI.
NIC	3com EtherLink XL 10/100 PCI.
Processor:	Intel Pentium 4 (1816 MHz).
Memory:	512 Mb.

c. External Authentication Server:

For one-time passwords, the Evaluators tested the TOE using a SecurID authentication server, as follows. As the external authentication server is not within the scope of the TOE, the purpose of this test was to test the mechanisms and interfaces of the TOE relating to 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.

Hardware:	ACE Server.
Operating System:	Windows 2000.
Other Software:	RSA ACE/Server 5.1 for Windows.
NIC	Intel PRO/1000 MT Desktop Adapter.
Processor:	AMD (1526 MHz).
Memory:	256 Mb.

14. The appliance hosting the TOE was connected in the following network configuration:


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

The connectivity in that configuration was provided by three Dell Powerconnect 2508 hubs.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

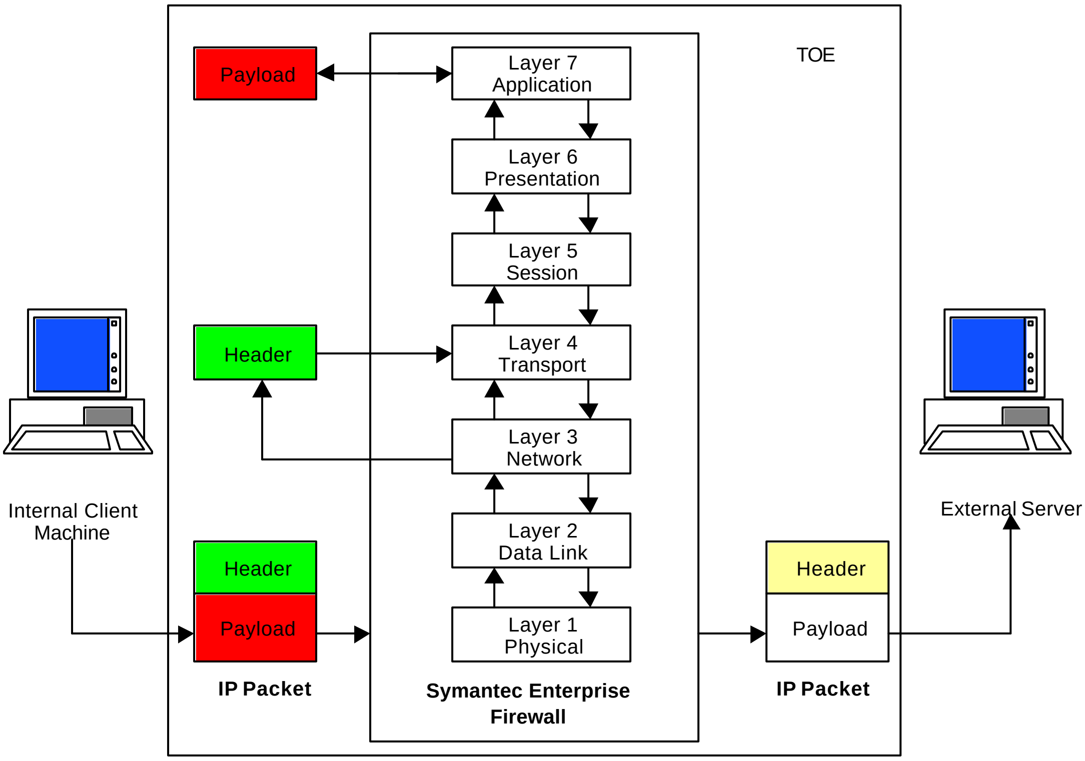
1. This annex gives an overview of the main architectural features of the product that are relevant to the security of the TOE. Further specification of the scope of the evaluation is given in various sections above.

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 client normally.

Annex B

6. The product has only one class of user: 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 administrator's interface via the LCD device driver.

c. The interface between the firewall and the appliance's 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 appliance's operating system controls that operating system's 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)