UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P226

Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only)

Issue 1.0

April 2006

UK 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.

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	**Symantec Corporation**
Product and Version	**Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only)**
Description	Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) is an application level firewall on a Symantec 5000 series appliance.
CC Part 2	**Extended**
CC Part 3	**Conformant**
EAL	**EAL4** augmented by ALC_FLR.1
CLEF	**BT CLEF**
Certifier	**CESG**
Date authorised	7 April 2006

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 ([a] - [c]). The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [d], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was itself first evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [g], the Common Evaluation Methodology (CEM) [h], and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Symantec Gateway Security 5000 Series Version 3.0 (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 [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The version of the product evaluated was:

Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) with Hotfix SGS3.0-bundleB – February 2006 Maintenance Update (SGS3.0-20060201-00)

4. 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. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration'.

7. The scope of the evaluation is limited to the Firewall Engine and the graphical user interfaces, the Security Gateway Management Interface (SGMI) and the Liquid Crystal Display (LCD). The evaluation includes the TOE running on the 5420, 5440, 5460, 5620, 5640 and 5660 appliances in the 5000 range.

8. An overview of the product and its security architecture can be found in Chapter IV 'Product Security Architecture'.

Security Claims

9. The Security Target [d] fully specifies the TOE's security objectives, the threats which these objectives counter and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives. With the exception of FIA_UAU_SERV.1 (see Security Target [d]) all of the SFRs are taken from CC Part 2 [f]; use of this standard facilitates comparison with other evaluated products.

10. The TOE security policies are detailed in the Security Target [d].

Strength of Function Claims

11. 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.

12. 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 is considered necessary.

Evaluation Conduct

13. The evaluation has specifically taken into account UK CC interpretations UK/2.2/007 [n], UK/2.2/012 [o] and UK/2.2/013 [p].

14. The TOE Security Functions and security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine Only), which had previously been certified by the UK IT Security Evaluation and Certification Scheme to the CC EAL4 augmented with ALC_FLR.1 assurance level [i]. For the evaluation of Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) the evaluators addressed every CEM [h] EAL4 and ALC_FLR.1 work unit, but made some use of Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine Only) evaluation results where these were valid for both Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) and the CEM requirements.

15. The Certification Body monitored the evaluation which was carried out by the BT Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [d]. The results of this work, completed in March 2006, were reported in the ETR [j].

Conclusions and Recommendations

16. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

17. Prospective consumers of Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) should understand the specific scope of the certification by reading this report in conjunction with the Security Target [d].The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

18. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III ‘Evaluated Configuration’.

19. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II 'Product Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

20. **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 these patches have further assurance . The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product.

II. PRODUCT SECURITY GUIDANCE

Introduction

21. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

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

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

a. For the 5600 models Symantec or its agent pre-loads the TOE (except for Hotfix SGS3.0-bundleB), onto the appliance for delivery to the consumer.

b. For the 5400 models Symantec provide a CD containing the TOE (except for Hotfix SGS3.0-bundleB) to the consumer.

c. The appliance is delivered in a sealed box to the consumer, by registered delivery, using a reputable delivery firm. A License Certificate (including a valid activation number) is dispatched separately to the consumer, by email.

d. The consumer should download the Certified Release Note [k] in Portable Document Form (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 Note [k]).

e. The remaining guidance documents Administration Guide [l] and Installation Guide [m] are delivered with the appliance or CDROM upgrade in softcopy form on a CD.

f. If upgrading a 5400 model the consumer should follow the guidance in the Installation Guide [m] in order to install the TOE (except for Hotfix SGS3.0-bundleB) onto the hardware.

g. To activate the product (both the preinstalled TOE and the upgrade), the consumer must enter a valid License Key. That key is obtained from Symantec's website by inputting the consumer's details, the appliance serial number, the system ID number (obtained through the SGMI) and the activation number from the License Certificate.

h. Using the guidance in the Certified Release Note [k], the consumer should verify that the appliance identifies the pre-loaded (or installed by the consumer in the case of 5400 models) software as Symantec Gateway Security 3.0 (with no patches).

24. 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 Installation Guide [m], consumers should download and install Hotfix SGS3.0-bundleB from that website.

c. Using an MD5 checksum utility, the consumer can generate an MD5 checksum for the downloaded hotfix and compare it with the MD5 hash value published for that hotfix on Symantec's website, to confirm the integrity of the hotfix. For reference, the MD5 hash value published on Symantec's website for Hotfix SGS3.0-bundleB is 55BD1968AF8921DFE67EDA7CDDFBA27E. 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 Note [k], the consumer should verify that the appliance identifies that the specified hotfix has been installed.

25. The primary considerations governing the security of web-based delivery of the Certified Release Note [k] and Hotfix SGS3.0-bundleB are as follows:

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

b. the Certified Release Note is downloaded as a PDF file;

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

Installation and Guidance Documentation

26. The Certified Release Note [k] describes the procedures that must be followed to install and configure the TOE, and operate it securely, and include warnings that identify unevaluated functionality. These notes also include procedures that must be followed to configure the environment. Hence it is recommended that this note is read first.

27. Further guidance is provided in the following documents:

- Installation Guide [m]

- Administrator's Guide [l]

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

Flaw Remediation

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

30. 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 validate a downloaded hotfix. For each hotfix, the following details are provided via that portal:

- prerequisites;
- special notes;
- included modules with fix descriptions;
- installation instructions;
- uninstallation instructions;
- special instructions.

31. 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.

32. The product's installation and guidance documents (e.g. the Installation Guide [m] and the Administrator's Guide [l]) 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.

33. 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.

III. EVALUATED CONFIGURATION

TOE Identification

34. The TOE is the Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) with Hotfix SGS3.0-bundleB. It consists of the following software:

- the firewall engine;
- the SGMI, which is used for local administration;
- the LCD, which is also used for local administration.

TOE Documentation

35. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'.

36. The guidance documentation (with the exception of the Certified Release Note [k]) is provided on a CD delivered to the consumer along with the appliance. This CD has a part number 10440186-IN.

TOE Scope

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

- Firewall;
- Virtual Private Networking (VPN);
- High-availability;
- Anti-spam;
- Intrusion detection and prevention;
- Anti-virus.

38. **The TOE is the firewall application only**, other applications are outside the scope of the evaluation. Hence the scope of the TOE is the Symantec Gateway Security 5000 Series Version 3.0 (Firewall Engine Only) with Hotfix SGS3.0-bundleB.

39. The product runs on dedicated appliance hardware. The TOE consists of the following product software:

a. The firewall itself;

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

c. The software for the appliance Liquid Crystal Display (LCD), which is a small screen and push buttons used also for local administration.

40. The SGMI is a Java-based GUI that includes policy, system-monitoring, settings and reporting functionality. The SGMI is accessed by directing a workstation browser to the appliance network address. The workstation must be running the Java Run-time Environment (JRE) version 1.5 which is downloaded from the appliance if not already present on the workstation. 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 and no other software needs to be loaded onto the SGMI workstation for it to run the SGMI. The SGMI Java WebStart application, which essentially provides a program shortcut to connect the SGMI Workstation to the appliance, is automatically downloaded from the appliance when an administrator connects their browser to the appliance for the first time.

41. The LCD displays various information relating to the CPU status and throughput and can be used to reboot and shutdown the appliance. The LCD can be locked from the SGMI.

42. One-time password authentication for Telnet/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;

b. RADIUS Server.

43. 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.

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

- HTTP;
- UDP;
- FTP;
- Ping;
- DNS;
- Telnet;

- SMTP;
- NTP;
- RTSP;
- IP;
- NNTP;
- POP3;
- RealAudio;
- TCP.

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

- HTTP;
- FTP;
- NNTP;
- RealAudio;
- DNS;
- NTP;
- TELNET;
- SMTP;
- POP3.

46. Part of the security of the TOE is supported by security functionality provided by the appliance's operating system, the SGMI Workstation's operating system and the authentication server. These are all part of the environment of the TOE, so they are outside the scope of the evaluation.

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

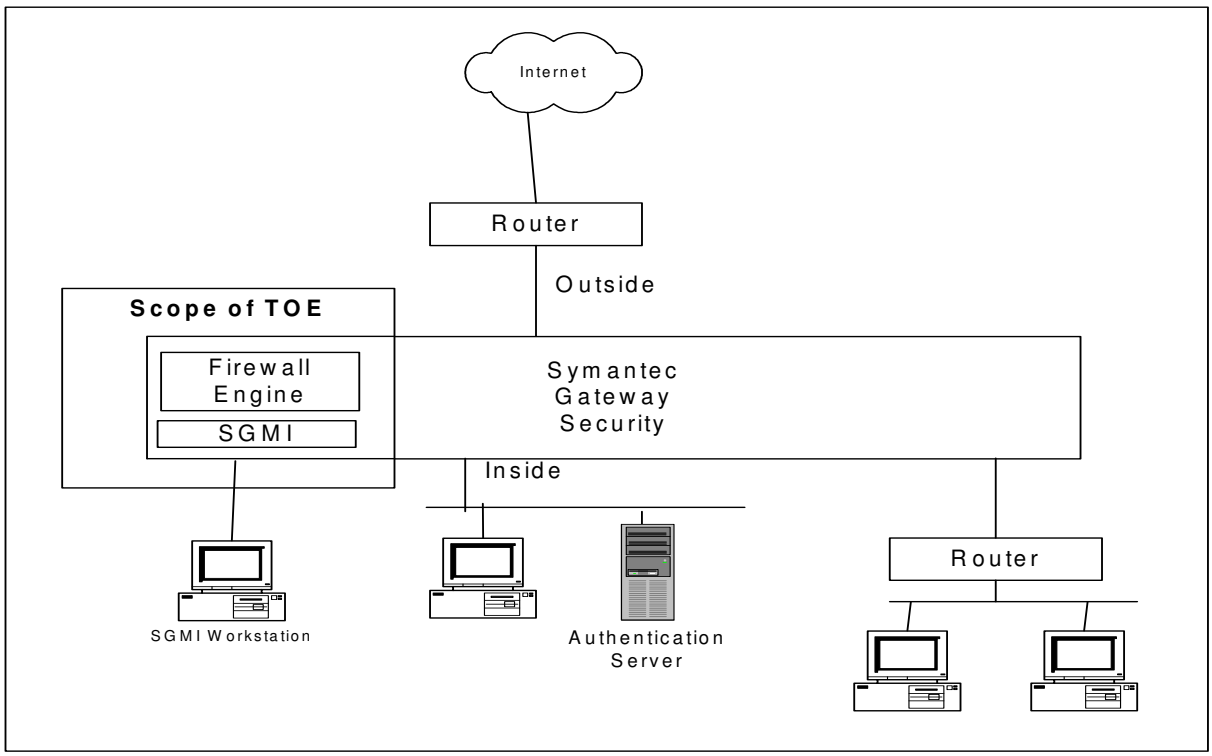
- VPN functionality;
- Symantec Enterprise VPN client;

- content filtering;
- high-availability / load balancing;
- user authentication by one-time password[1];
- setup wizard;
- anti-spam;
- H.323 connection;
- remote administration;
- forward filtering;
- secure shell (SSH);
- console port access;
- tomcat web server;
- intrusion detection and prevention;
- anti-virus;
- live update support;
- event manager;
- policy configuration manager.

TOE Configuration

48. The evaluated TOE configuration consists of the Firewall Engine, SGMI and LCD software on an SGS 5000 Series appliance running the SGS Version 3.0 software as represented in the diagram below.

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



Environmental Requirements

49. The general threats that are countered by the TOE are:

- Attackers on one network who may gain unauthorised access to resources within another network;

- Users on one network who may inappropriately expose data or resources to another network.

50. There are a number of assumptions relating to the environment. These are detailed in the Security Target [d]. Specifically the following must be provided in the evaluated configuration:

a. The TOE, SGMI Workstation operating system and authentication server including their communication links are physically protected to prevent unauthorized access.

51. The environmental configuration is as follows.

52. The required IT environment for the TOE is any one of the following 5000 series appliances:

- 5660 (excluding use of the 'Small Form Factor Plugable Slots')[2];
- 5640;
- 5620;
- 5460;
- 5440;
- 5420.

53. In addition an SGMI Workstation running Windows is required which is capable of running JRE version 1.5. If version 1.5 of the JRE is not already installed on the SGMI Workstation it is downloaded from the appliance.

54. An authentication server is required for single-use authentication. A commercially available authentication server (either an RSA Secure Dynamics 'SecurID' Server or a RADIUS Server) should be used.

Test Configuration

55. The following configuration was used by the developer for testing:

a. TOE, as part of Symantec Gateway Security Version 3.0, on a model 5640 appliance;

b. SGMI accessed from an SGMI Workstation running Windows XP SP2, using Internet Explorer 6.0 SP1.

56. The evaluators used the same test configuration in order to repeat a sample of the developer's tests and also to perform independent functional and penetration testing. In addition the evaluators also performed some tests relating to flooding attacks on all other appliances within the scope of the evaluation (see paragraph 52 above).

57. 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:

[2] The Small Form Factor Pluggable Slots can be used to provide additional network ports. They are excluded from the evaluated configuration.

a. Appliances tested (including LCD) – note that the developer tests were only performed on an SGS5640 model. All evaluator tests were performed on an SGS5640 model and some (relating to flooding attacks) were also performed on the other 5 models:

Hardware Model O/S NICs Processor Disk Memory	SGS version 3.0 5660 Redhat Linux 7.2 with Linux 2.4.26 kernel 6 Gigabit Ethernet Ports 3.6 GHz 800 FSB XEON 160GB EIDE 4GB	Hardware Model O/S NICs Processor Disk Memory	SGS version 3.0 5640 Redhat Linux 7.2 with Linux 2.4.26 kernel 8 Gigabit Ethernet Ports 3.0 GHz 800 P4 160GB EIDE 2GB
Hardware Model O/S NICs Processor Disk Memory	SGS version 3.0 5620 Redhat Linux 7.2 with Linux 2.4.26 kernel 6 Gigabit Ethernet Ports 2.8 GHz Celeron 80GB EIDE 1GB	Hardware Model O/S NICs Processor Disk Memory	SGS version 3.0 5460 Redhat Linux 7.2 with Linux 2.4.26 kernel 8 Gigabit Ethernet Ports 2.8 GHz 533 FSB XEON P4 80GB EIDE 1GB
Hardware Model O/S NICs Processor Disk Memory	SGS version 3.0 5440 Redhat Linux 7.2 with Linux 2.4.26 kernel 6 Gigabit Ethernet Ports 2.4 GHz 533 FSB XEON 80GB EIDE 1GB	Hardware Model O/S NICs Processor Disk Memory	SGS version 3.0 5420 Redhat Linux 7.2 with Linux 2.4.26 kernel 6 Fast Ethernet Ports 2.0 GHz Celeron 40GB EIDE 512MB

b. SGMI Workstation

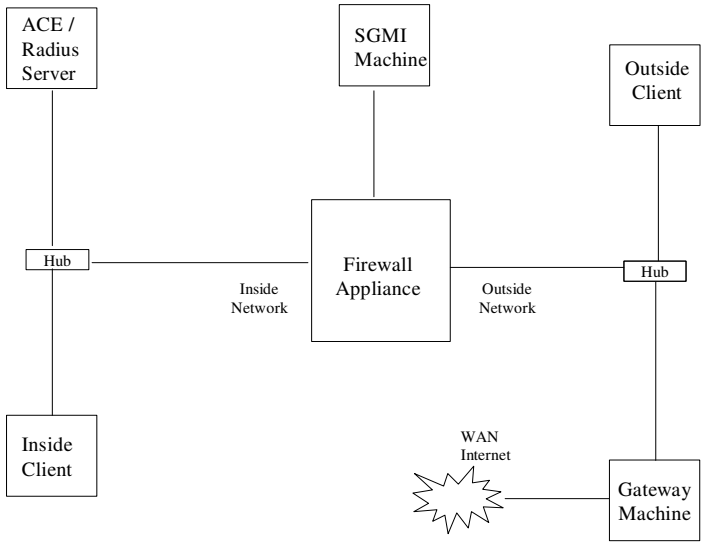
Hardware:	The SGMI Workstation was co-located with the above Appliance hardware and attached to it via a crossover cable
Operating System:	Windows XP SP2
Other Software:	Internet Explorer 6.0 SP1 JRE Version 1.5 No other applications were loaded onto the

	SGMI workstation. No TOE specific software needs to be loaded onto the SGMI workstation to run the SGMI.
Network Interface Cards (NICs):	Intel PRO/1000 MT Desktop Adapter
Processor:	Intel Pentium 4 2.4Ghz
Memory:	512 Mb

c. External Authentication Server:

Hardware:	ACE Server and RADIUS Server
Operating System:	Windows Server 2003
Other Software:	RSA ACE/Server 5.2 for Windows Steel-Belted Radius Version 4.0.248
Network Interface Cards (NICs):	Intel PRO/1000 MT Desktop Adapter
Processor:	AMD (1800Mhz)
Memory:	256 Mb

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


ACE / Radius Server
SGMI Machine
Outside Client
Hub
Inside Network
Firewall Appliance
Outside Network
Hub
Inside Client
WAN Internet
Gateway Machine

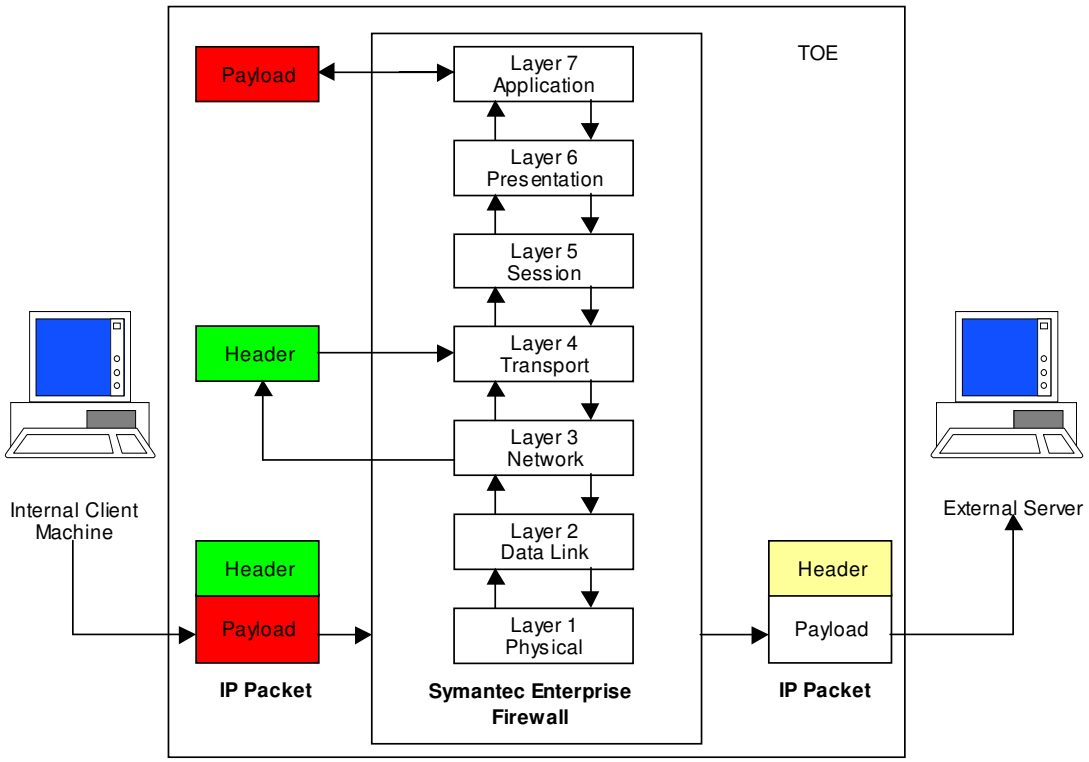
IV. PRODUCT SECURITY ARCHITECTURE

59. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

60. 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.

61. 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.



62. 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.

63. 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.

Design Subsystems

64. 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.

Hardware and Firmware Dependencies

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

a. interrupts and exceptions;

b. processor execution levels;

c. memory allocation;

d. system clock.

Product Interfaces

66. 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.

V. PRODUCT TESTING

IT Product Testing

67. The TOE was tested against the set of external interfaces that comprise the TOE Security Functions Interface (TSFI), as listed under 'Product Interfaces in Chapter IV.

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

69. all related security functions specified in the Security Target [d];

70. all high level design subsystems identified in Chapter IV.

71. 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.

72. All testing by the developer was performed using SGS 5000 Series Version 3.0 with Hotfix RC8A on an SGS5640 appliance.

73. The Evaluators performed the following independent testing using SGS 5000 Series Version 3.0 with Hotfix SGS3.0-bundleB on an SGS5640 appliance:

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.

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

75. 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.

76. The evaluators used the following tools during testing:

- Port Flooding Tool version 1.062 from 7th Sphere;
- Nmap version 3.81;
- Ethereal version 0.10.11;
- Bandwidth Controller Manager version 1.00.

77. No other specific evaluation tools were used during the evaluation.

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

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

- all communications protocols and application proxies listed in the Security Target [d];
- 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.

Vulnerability Analysis

80. The evaluators' vulnerability analysis, which preceded penetration testing, was based on both public domain sources and the visibility of the TOE given by the evaluation process.

Platform Issues

81. The following appliances are within the scope of the evaluation:

- 5660 (excluding use of the 'Small Form Factor Plugable Slots');
- 5640;
- 5620;
- 5460;
- 5440;
- 5420.

82. Each of the models runs exactly the same version of the TOE (including the hotfix) on the same version of the appliances operating system. The difference between the models are their memory, processor, hard disk size and NICs installed (however their NICs all use the same type of network device driver software, namely the Intel E1000 driver).

83. Both the developer and evaluator performed all tests on the 5640 model. In addition the evaluator repeated 3 tests (relating to flooding attacks) on the other 5 models. The results obtained were exactly the same in all cases.

84. Confidence was gained that the TOE behaves in exactly the same manner on all 6 models, as their underlying operating system is exactly the same version, and the tests performed showed no differences in their operation. Therefore the evaluators are aware of no issues regarding the differences between the models that would suggest that the TOE would behave differently on any of the 6 models listed above.

VI. REFERENCES

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

[b] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.0, October 2003.

[d] Security Target for Symantec Gateway Security (SGS) 5000 Series Version 3.0 (Firewall Engine Only)
Symantec Corporation
SGS3\ST, Issue 1.0, March 2006

[e] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-001, Version 2.2, January 2004.

[f] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-002, Version 2.2, January 2004.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-003, Version 2.2, January 2004.

[h] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2004-01-004, Version 2.2, January 2004.

[i] 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.

[j] Evaluation Technical Report: Common Criteria EAL4 Evaluation of Symantec Gateway Security Version 3.0 (Firewall Engine Only)
BT CLEF
LFS/T506/ETR, Issue 1.0, April 2006.

[k] Certified Symantec Gateway Security 5000 Series v3.0 Release Notes
Symantec Corporation
Issue 1.2, March 2006.

[l] Symantec Gateway Security 5000 Series v3.0 Administration Guide
Symantec Corporation
Issue 8.0, January 2006

[m] Symantec Gateway Security 5000 Series v3.0 Installation Guide
Symantec Corporation
Version 1.0, October 2005

[n] UK CC Interpretation – UK/2.2/007 (Verdict justifications in CC compliant evaluations), 24 March 2005

[o] UK CC Interpretation – UK/2.2/012 (Multi-platform TOEs), 29 October 2004

[p] UK CC Interpretation – UK/2.2/013 (Secure electronic delivery), 19 April 2005.

VII. ABBREVIATIONS

85. This list does not include well known IT terms such as LAN, GUI, PC or standard Common Criteria abbreviations such as TOE, TSF (see Common Criteria Part 1 [e], Section 2.3)

DNS	Domain Name Service
EIDE	Enhanced Integrated Drive Electronics
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
JRE	Java Run-time Environment
LCD	Liquid Crystal Display
NAT	Network Address Translation
NIC	Network Interface Card
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
POP	Post Office Protocol
RTSP	Real Time Streaming Protocol
SGS	Symantec Gateway Security
SGMI	Security Gateway Management Interface
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
SSH	Secure Shell
UDP	User Datagram Protocol
VPN	Virtual Private Networking