UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P216

Symantec Gateway Security 400 Series Version 2.1 (Firewall Engine only)

Issue 1.0

May 2005

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.

CERTIFICATION STATEMENT

Symantec Gateway Security 400 Series Version 2.1 (Firewall Engine only) is a packet filtering firewall on an appliance.

Symantec Gateway Security 400 Series Version 2.1 (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 conformant requirements of Evaluation Assurance Level EAL2 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	5 May 2005

(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
DNS	Domain Name Service
DRAM	Dynamic Random Access Memory
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
NVRAM	Non Volatile Random Access Memory
PDF	Portable Document Format
RAM	Random Access Memory
ROBO	Remote Office / Branch Office
SESA	Symantec Enterprise Security Architecture
SFR	Security Functional Requirement
SGMI	Security Gateway Management Interface
SGS	Symantec Gateway Security
SOF	Strength of Function
SP	Service Pack
SSMS	Symantec Security Management System
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 400 Series Version 2.1 (Firewall Engine only),
Symantec Corporation,
T466\ST, Issue 2.0, May 2005.

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, 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 2.2, 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, January 2004.

e. Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Interpretation Management Board,
CCIMB-2004-01-004, Version 2.2, 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 EAL2 Evaluation of Symantec Gateway Security 400 Series Version 2.1 (Firewall Engine only),
BT CLEF,
LFS/T466/ETR, Issue 1.0, 31 March 2005.

j. Release Notes: The Certified Symantec Gateway Security 400 Series Version 2.1 (Firewall Engine only),
Symantec Corporation,
Issue 1.5, May 2005.

k. Symantec Gateway Security 400 Series - Installation Guide (Supported Models: Models 420, 440, 460, and 460R), Symantec Corporation, Issue 2.1, 23 June 2004.

l. Symantec Gateway Security 400 Series - Administrator's Guide (Supported Models: Models 420, 440, 460, and 460R), Symantec Corporation, Issue 2.1, 23 June 2004.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of the Symantec Gateway Security (SGS) 400 Series Version 2.1 (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:

   Symantec Gateway Security 400 Series Version 2.1 (Firewall Engine only).

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

5. The SGS 400 Series is intended for Remote Office / Branch Office (ROBO) and small office environments of medium and large enterprises. It combines several network security applications into one appliance. The TOE is one of those applications, namely the firewall engine only, which is a packet filtering firewall.

6. The TOE is intended to act as a security gateway to ensure that resources on an internal network are protected from an external network (which could be the Internet). To maintain security, all traffic between each network attached to the appliance must flow through the TOE.

7. The TOE provides packet inspection for all through traffic and provides firewall rule enforcement. It controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's administrator. This allows acceptance and refusal of data, based on attributes of the data packets.

8. The TOE also provides Network Address Translation (NAT) to hide internal addresses. All of the firewall operations are applied to computer groups (i.e. a computer in the group is identified by its Media Access Control (MAC) address, or its Internet Protocol (IP) address, or its Domain Name Service (DNS) name, or any combination of these).

9. The TOE also provides protection against:

   - Syn flooding attacks;
   - port scanning attacks;
   - IP address spoofing attacks.

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

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

TOE Scope

12. The SGS 400 Series integrates several network security applications in one appliance, including:

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

13. The TOE is the firewall application only (i.e. the other applications above are outside the scope of the evaluation). Hence the scope of the TOE is the Symantec Gateway Security 400 Series Version 2.1 (Firewall Engine only).

14. The TOE is firmware only, installed on SGS 400 Series appliance hardware. The TOE consists of the following firmware components:

a. the firewall itself;

b. the Security Gateway Management Interface (SGMI), which is used for local administration by the administrator.

15. The SGMI is a Graphical User Interface (GUI) that provides administrative services to the SGS 400, including policy, system-monitoring, settings and reports. The SGMI is accessed on the internal network via an SGMI client workstation running Windows 2000 Service Pack (SP) 4, using Internet Explorer 6.0 SP1. No separate software needs to be installed for the workstation to run SGMI. (Although the SGMI can be accessed from any machine connected to the internal network, in the evaluated configuration the authorised administrator is instructed to only access the SGMI from a dedicated client workstation.) In the evaluated configuration, the SGMI must not be connected from the outside network through the SGS 400's WAN port.

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

17. In addition, for the evaluated configuration, the following were connected on the internal network to the SGS 400 Series appliance:

a. A Network Time Protocol (NTP) server, to provide time stamping for the audit logs. NTP is an Internet standard protocol that ensures accurate synchronization to the millisecond of computer clock times in a network.

b. A Syslog server, to retain audit logs. This server listens for log entries forwarded by the appliance and stores all log information for future analysis.

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

- HTTP;
- UDP;
- FTP;
- DNS;
- Telnet;
- SMTP;
- POP3;
- TCP;
- SNMP
- TFTP.

19. Part of the security of the TOE is supported by security functionality provided by the appliance's operating system (i.e. Micrium's MicroC/OS-II 2.0), the Syslog Server and the NTP Server. Those are all part of the environment of the TOE, so they are outside the scope of the evaluation.

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

- VPN functionality;
- high availability / load balancing / bandwidth aggregation;
- wizards;
- remote administration;
- intrusion detection and prevention;
- anti-virus policy enforcement;
- content filtering;
- LiveUpdate support;
- event manager;
- advanced manager;
- Symantec Enterprise Security Architecture (SESA), previously known as Symantec Security Management System (SSMS);
- wireless networking.

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 CC predefined Evaluation Assurance Level EAL2.

23. 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

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.

Security Policy

26. One form of information flow security policy is claimed by the Security Target [a]:

    Unauthenticated: for information flow between external IT entities, on an internal or external connected network, sending information to other external IT entities.

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 the objectives counter, and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives.

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

30. FAU_GEN.1_EXP is an explicit requirement, which has been added because:

    a. The TOE does not record the shutdown of the TOE. (However the only possible shutdown is a hard shutdown and, as events are recorded in the audit log a fraction of a millisecond after they occur, it is unlikely that records would be lost during shutdown. Also, as the TOE does record start-up, an administrator can calculate (from the last event recorded to the start-up event) when a shutdown occurred.)

    b. The TOE log does not record the date of an event. (However the Syslog Server records the date and time that an event is logged. Hence an event in the evaluated configuration is logged simultaneously in both the TOE log and the syslog.)

FAU_GEN.1_EXP thus ensures that the auditing actions performed by the TOE are captured.

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

- information flow control – these functions manage data flowing through the TOE;
- security management – these functions allow an authorised administrator to configure and manage the TOE;
- protection of the TOE Security Functions (TSF) – these functions ensure the internal protection of the TOE;
- security audit – these functions allow auditable events to be recorded and reviewed by an authorised administrator.

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 United Kingdom Scheme Publication (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 CC 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 EAL2 requirements specified in CC Part 3 [d];
- the Common Evaluation Methodology (CEM) [e];
- the appropriate CC and CEM interpretations.

35. The Certification Body monitored the evaluation, which was carried out by the BT Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [i] to the Certification Body in April 2005. The Certification Body requested further details and, following the CLEF's satisfactory responses, the Certification Body then produced this Certification Report.

General Points

36. 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.

37. 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.

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

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

39. 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.

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

Delivery

41. Symantec ships each SGS 400 Series appliance (including its CD-ROMs, documentation, cables, etc) in a sealed box to a Symantec authorised reseller. Consumers are required to order the appliance from a reputable supplier (i.e. a Symantec authorised reseller), who then ships the sealed box to the consumer by registered delivery, using a reputable delivery firm.

42. On receipt of the appliance, consumers should check that the ordered model has been supplied and that the security of the appliance has not been compromised during delivery.

43. When consumers receive an appliance, they are required to follow the following process as detailed in the Certified Release Notes [j]:

a. Download the file containing SGS 400 Series Version 2.1, Build 703 (i.e. the evaluated configuration), from the following Symantec website:

http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sgs_2_400/files.html

b. Verify the supplied MD5 checksum, as described in the Certified Release Notes.

c. Apply the build to update the firmware on the SGS 400 Series appliance. Then check that the firmware update took place correctly (i.e. the evaluated TOE is installed).

44. The following measures provide security for delivery of the appliance and the TOE's guidance documentation:

a. The box is sealed with a tamper-evident, clear label.

b. The appliance is wrapped in a polythene bag, sealed with a tamper proof seal. A statement on the seal advises that, by opening the seal, the consumer accepts the licence agreement.

c. On the base of the appliance is a tamper-evident 'Symantec' label, which states:

- appliance model (e.g. SGS 440);
- appliance version (e.g. Revision 1.3);
- appliance serial number (e.g. 040703560623);
- appliance MAC address (e.g. 00A065CD6C8);
- appliance country of manufacture.

d. The consumer should download the Certified Release Notes [j] 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.)

e. The remaining guidance documents [k-l] are delivered, with the appliance in the sealed box, in soft-copy (i.e. as PDF files on the CD-ROM). The US edition of that CD-ROM has Part Number 10278209; the international edition has Part Number 10279661-ML. There is no significant difference between those editions, or of the guidance documents thereon.

45. The following measures provide security for web-based delivery of the TOE:

a. The TOE is available only from Symantec's website, stated in Paragraph 43a above.

b. Using the guidance in the Certified Release Notes [j], consumers should download and install the TOE from that website.

c. Using an MD5 checksum utility, the consumer can generate an MD5 checksum for the downloaded TOE and compare it with the MD5 hash value published for the TOE in the Certified Release Notes, to confirm the integrity of the TOE. (For reference, the Certified Release Notes specify that the MD5 hash value for the TOE is 580A939B83AC93FC2765BB7A1C1D32B2.) Symantec's website (stated in Paragraph 43a above) 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, the consumer should verify that the appliance identifies that the TOE (i.e. Symantec Gateway Security 400 Series, Version 2.1, Build 703) has been installed.

46. The primary considerations governing the security of web-based delivery of the Certified Release Notes [j] and the TOE are as follows:

- standard procedures associated with a well-managed web interface must be followed;
- the Certified Release Notes are downloaded as a PDF file;
- an MD5 checksum can be used to check the authenticity of the downloaded TOE.

Installation and Guidance Documentation

47. The Certified Release Notes [j] 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.

48. Further guidance is provided in the following documents:

- Installation Guide [k];
- Administrator's Guide [l].

49. The Installation Guide [k] provides general details concerning installation, such as connecting LAN and WAN cables. The Certified Release Notes [j] provide instructions to the administrator on how to download and apply Build 703 of the firmware (i.e. the TOE) to the appliance, as described above under 'Delivery'. The Certified Release Notes then detail how to configure the appliance in the evaluated configuration.

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

Strength of Function

51. 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

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

Testing

53. 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.

54. 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.

55. 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.

56. 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, tests on all of the hardware models 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.

57. 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.

58. The Evaluators used the following tools during testing:

- Ethersniff - produced by Michael Komm in 2003;
- Portf**k - from 7th Sphere;
- Nmap - Version 3.81;
- Ethereal - Version 0.10.9;
- Misoskian's Packet Builder – Version 0.6 Beta.

No other specific evaluation tools were used during the evaluation.

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

- all communications protocols listed in the Security Target [a];
- protection against Syn flooding attacks;
- protection against port scanning attacks;
- protection against IP address spoofing attacks.

Platform Issues

60. There are four models in the SGS 400 appliance series (i.e. SGS 420, SGS 440, SGS 460 and SGS 460R).

61. The TOE was evaluated on three of those models (i.e. SGS 420, SGS 440 and SGS 460), as specified in Annex A. The differences are their processor type and clock speed, and number of LAN and WAN ports. Each of those models runs the same version of the TOE, on the same version of the appliance's operating system.

62. The Developer's tests on the three models showed no difference in operation between them. The Evaluators' tests were also performed using the three models. The Evaluators are aware of no issues regarding the above differences between models that would suggest that the TOE would behave differently on any of those three models.

63. Different versions of a given model exhibit minor variations in hardware. The evaluators were satisfied that the minor nature of those variations should not cause the TOE to behave differently.

III. EVALUATION OUTCOME

Certification Result

64. 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 Gateway Security 400 Series Version 2.1 (Firewall Engine only) meets the CC Part 3 conformant requirements of Evaluation Assurance Level EAL2 for the specified CC Part 2 extended functionality in the specified environment.

Recommendations

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

66. 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'.

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

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

69. 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 400 Series Version 2.1 (Firewall Engine only), identified as Firmware Version 2.1.0 Build 703. That consists of the following firmware:

- the firewall;
- the SGMI.

TOE Documentation

2. The guidance documents evaluated were:

- Certified Release Notes [j];
- Installation Guide [k];
- Administrator's Guide [l].

3. Further discussion of the guidance documents is given above under 'Delivery' and 'Installation and Guidance Documentation'.

TOE Configuration

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

a. the firewall, as part of Symantec Gateway Security 400 Series Version 2.1, on a Model 420 appliance, a Model 440 appliance and a Model 460 appliance;

b. the SGMI, accessed from an SGMI client workstation running Windows 2000 SP4, using Internet Explorer 6.0 SP1.

Environmental Configuration

5. The required hardware environment for the TOE is one of the SGS 400 series of appliances, specifically Models 420, 440 and 460. (This excludes the 460R model, which was outside the scope of the evaluation.)

6. Each of those three models runs the same version of the TOE on the same version of the appliance's operating system. The differences between those three models are their processor type and clock speed, and number of LAN and WAN ports.

7. The Developer tested the TOE on all three models (i.e. 420, 440 and 460).

8. All of the Evaluators' tests were performed on the 440 model, and 50% of those tests were also performed on the other two models (i.e. 420 and 460). As the firmware (the TOE) is exactly the same on all three models and the hardware differences relate only to processor type and clock speed, and number of LAN and WAN ports, this approach was sufficient to gain confidence in all three platforms and to allow the results to be applicable across the 420, 440 and 460 models.

9. Part of the security of the TOE is supported by security functionality provided by the appliance's operating system (MicroC/OS-II 2.0), the Syslog Server and the NTP Server. (In the evaluated configuration, the Syslog Server and the NTP Server were on the internal network). Those are all part of the environment of the TOE, so they are outside the scope of the evaluation.

10. During their on-site testing, the evaluators used the guidance in [k] and [j] in order to install, generate a secure configuration and start-up the TOE. The evaluators performed those activities on the 420, 440 and 460 models.

11. 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:

Firmware & Build	Symantec Security Gateway Version 2.1.0, Build 703		
Operating System:	MicroC/OS-II 2.0		
Hardware Model:	420	440	460
Hardware Build:	Revision 1.3	Revision 1.4	Revision 1.4
Processor:	2010 (170 MHz)	2100 (170 MHz)	2100 (200 MHz)
	MIPS32 4Km Core Processor and encryption core		
	32-bit bus @ 100MHz		
	16KB data cache and 16KB instruction cache		
Network Interfaces:	10/100 Ethernet auto-sensing WAN port (x1)		10/100 Ethernet auto-sensing WAN port (x2)
	10/100 Ethernet auto-sensing 4 LAN port switch		10/100 Ethernet auto-sensing 8 LAN port switch
	RS-232 serial port		RS-232 serial port
User (Administrator) Interface:	SGMI		
Hard Disk:	None		
Memory:	8 MB Flash, 32 KB NVRAM and 64 MB DRAM		

Although the SGS 460 appliance has two physical WAN ports, in the evaluated configuration only one is used and the other is disabled.

b. SGMI client workstation:

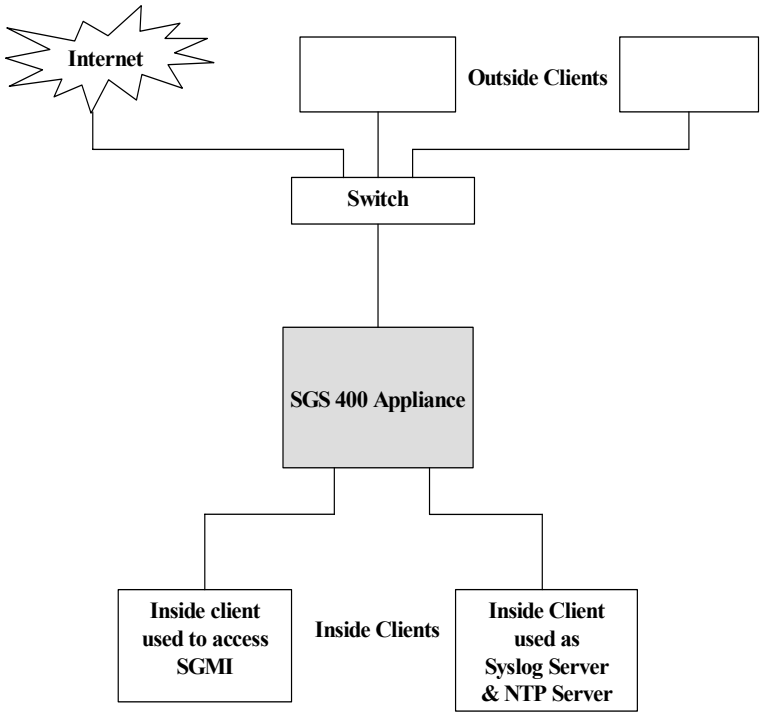
Hardware:	HIQ PC
Operating System:	Windows 2000 Advanced Server (SP4)
Other Software:	Internet Explorer 6.0 (SP1). No TOE specific software needs to be loaded onto the SGMI workstation, for the workstation to run the SGMI.
NIC	Intel PRO/1000 MT Desktop Adapter
Processor:	Intel Pentium 4 (1.8 GHz)
Memory:	1 GB RAM

c. Syslog Server and NTP Server:

The Evaluators tested the TOE using a Syslog Server and an NTP Server, as follows. (As the Syslog Server and the NTP Server are not within the scope of the TOE, the purpose of this testing was to test the mechanisms and interfaces of the TOE relating respectively to storage of audit logs and time stamping of audit logs.)

Hardware:	HIQ PC
Operating System:	Windows 2000 Advanced Server (SP4)
Other Software:	Internet Explorer 6.0 (SP1)
NIC	Intel PRO/1000 MT Desktop Adapter
Processor:	Intel Pentium 4 (1.8GHz)
Memory:	512 MB

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



The switch in that configuration was a Hawking Technology H-GS8T 8 port 10/100/1000M GigaSwitch.

(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 TOE is firmware only, installed on dedicated appliance hardware (i.e. SGS 400 series appliances). In addition to the TOE, the product's firmware also consists of a proprietary operating system (i.e. Micrium's MicroC/OS-II 2.0), as required by the TSF, which runs on the appliance hardware.

3. The TOE is intended to act as a security gateway between an internal network and an external network (which could be the Internet). It allows inbound rules to be set, whereby connections can be permitted from external clients to specific servers on the internal network. It is also possible to configure outbound rules, limiting external connections to specific clients on the internal network.

4. The TOE controls the flow of IP traffic, by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's administrator.

5. As well as the firewall engine (i.e. the TOE), the SGS 400 series also provides a number of additional security features, such as VPN functionality and anti-virus support. Those additional features are disabled in the evaluated configuration and do not form part of the TOE.

6. Figure 2-1 of the Security Target [a] shows the TOE within a typical network, consisting of a number of inside clients and a number of outside clients. The inside clients are attached to either a 4-port LAN switch on the SGS 420 and SGS 440 models, or to an 8-port LAN switch on the SGS 460 model, and the outside clients are attached to the WAN port of the appliance.

7. The TOE provides a GUI for system configuration and management by way of a firmware component called the SGMI. The SGMI is accessible from a machine on the internal network, from which the administrator accesses the SGMI by directing a web browser to the appliance.

8. 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.

9. The product offers a number of failsafe features, e.g. inbound connections are denied unless an information flow rule has been set up to explicitly allow them.

TSF Interface

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

    a. The interface between the administrator and the SGMI. This menu-driven GUI enables the administrator to configure the firewall and review the audit logs. The administrator's input data and selections are checked by the TOE upon entry.

b. The interface between the TOE and the operating system (i.e. MicroC/OS-II 2.0). This also includes the following interfaces, via the network interfaces of the appliance:

- the interface with the network traffic (both on the WAN and LAN ports);
- the interface with the NTP Server on the internal network;
- the interface with the Syslog server on the internal network;

Design Subsystems

11. The TOE consists of the following main subsystems, which are all security-enforcing:

a. SGMI. This subsystem enables the administrator to access the TOE via an HTTP connection between a client machine (on the internal network) and the TOE. The SGMI runs on the TOE and accepts requests from the machine acting as the SGMI client. The SGMI is used by the administrator to manage the TOE, e.g. by means of configuration settings for logging/monitoring, administration, firewall functions, connections and protections. The administrator can use the SGMI to perform the following security enforcing actions;

- start up and shutdown;
- create, delete, modify and view information flow security policy rules that permit or deny information flows;
- enable an NTP Server to set the time;
- enable a Syslog Server to log events;
- review the audit trail;
- backup of configuration data file;
- recover to the state following the last backup.

a. Syslog Service. This subsystem enables the administrator to log audit events to an external Syslog Server. This subsystem receives audit events from the Logging Subsystem, which are then passed to an external Syslog Server which ensures that a permanent record of all events is maintained. (In the evaluated configuration, the external Syslog Server is located on the internal network.)

b. NTP Service. This subsystem enables the TOE to obtain real time from an external remote time service using the network time protocol (NTP), from an external NTP Server. The administrator uses the SGMI to configure the NTP Server. The timestamp is then added to every audit event recorded by the TOE. (In the evaluated configuration, the external NTP Server is located on the internal network.)

c. Logging. This subsystem generates audit events and writes them to non-volatile memory (NVRAM) (which maintains a record of the last 100 events) and simultaneously sends them via the Syslog Service subsystem to the Syslog Server (which provides a permanent audit record). The TOE overwrites the log messages when the maximum number of log messages in the queue is reached, by using a circular queue algorithm; the oldest records are replaced by the new messages.

d. Firewall Functional Group. This subsystem mediates the traffic flow between the internal and external networks and protects the security, integrity and privacy of services and data on the internal network. The major element of the Firewall Functional Group relates to firewall rule enforcement.

Operating System Dependencies

12. The appliance's operating system (MicroC/OS-II 2.0) controls the system time, controls network links, and provides TSF domain separation.

Hardware and Firmware Dependencies

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

a. non-volatile RAM (NVRAM) - to store configuration and audit data;

b. device interrupts to the CPU;

c. exceptions (i.e. unexpected events, such as divide by zero);

d. processor execution levels;

e. memory allocation;

f. system clock. (The system clock provided by the underlying hardware is used as part of the calculation of timestamps for the audit trail. The SGS 460 model runs at 200 MHz, while the SGS 420 and 440 models run at 170 MHz. The operating system uses this clock speed to generate an operating system 'tick count', which is always 20 ticks per second.)

(This page is intentionally left blank)