UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

CERTIFICATION REPORT No. P139

Safegate

Version 2.0.2

running on Solaris Version 2.6 with patch 105580-01

Issue 1.0

March 2000

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

ARRANGEMENT ON THE
MUTUAL 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 Arrangement 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

Fujitsu Limited' s Safegate is a firewall that provides an Internet Protocol packet filtering function, an application gateway function and an audit function.

Safegate Version 2.0.2 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria Part 3 requirements for Evaluation Assurance Level EAL3 for the specified Common Criteria Part 2 conformant functionality in the specified environment when running on Solaris Version 2.6 with patch 105580-01 as specified in Annex A.

Originator	**CESG** Certifier
Approval	**CESG** Technical Manager of the Certification Body
Authorisation	**CESG** Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	02 March 2000

(This page is intentionally left blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT iii

TABLE OF CONTENTS v

ABBREVIATIONS vii

REFERENCES ix

I. EXECUTIVE SUMMARY 1
Introduction 1
Evaluated Product 1
TOE Scope 2
Protection Profile Conformance 2
Assurance Level 2
Strength of Function 2
Security Claims 3
Threats Countered 3
Threats Countered by the TOE' s Environment 3
Threats and Attacks not Countered 4
Environmental Assumptions and Dependencies 4
IT Security Objectives 5
Non-IT Security Objectives 5
Security Functional Requirements 6
Security Function Policy 6
Evaluation Conduct 7
Certification Result 7
General Points 8

II. EVALUATION FINDINGS 9
Delivery and Installation 10
User Guidance 10
Misuse 10
Developer' s Tests 11
Evaluators' Tests 12

III. EVALUATION OUTCOME 15
Certification Result 15
Recommendations 15

ANNEX A: EVALUATED CONFIGURATION 17

ANNEX B: PRODUCT SECURITY ARCHITECTURE 19

(This page is intentionally left blank)

ABBREVIATIONS

ARP	Address Resolution Protocol
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
NNTP	Network News Transfer Protocol
RIP	Routing Information Protocol
SFR	Security Functional Requirements
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SoF	Strength of Function
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	Universal Datagram Protocol
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 3.0, 2 December 1996.

b. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

c. Safegate Security Target,
Fujitsu Limited,
Version 1.2e, 22 February 2000.

d. Common Criteria Part 1,
Common Criteria Implementation Board,
CCIB-98-026, Version 2.0, May 1998.

e. Common Criteria Part 2,
Common Criteria Implementation Board,
CCIB-98-027, Version 2.0, May 1998.

f. Common Criteria Part 3,
Common Criteria Implementation Board,
CCIB-97-028, Version 2.0, May 1998.

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
Version 1.0, CEM-99/045, August 1999.

h. Evaluation Technical Report for LFL/T119,
Logica UK Limited,
CLEF.24839/7.2/1, Version 1.0, 20 December 1999.

i. Evaluation Technical Report for LFL/T119 Phase 3 - Rework,
Logica UK Limited,
CLEF.24839/7.2/2, Version 1.0, 11 February 2000.

j. Safegate Description Manual,
Fujitsu Limited,
SX01, Version 3.0, February 2000.

k. Installation Guide,
Fujitsu Limited,
SX03., Version1.0, 22 August 1999.

l. S Family Software Description,
Fujitsu Limited,
SX02,Version 4.0, 15 February 2000.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the IT security evaluation of Safegate Version 2.0.2 to the Sponsor, Fujitsu Limited, and is intended to assist potential consumers when judging the suitability of the product for their particular requirements.

2. The prospective consumer is advised to read the report in conjunction with the Security Target [Reference c], which specified the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

Safegate Version 2.0.2.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Fujitsu Limited. Details of the evaluated configuration, including the product's supporting guidance documentation, are given in Annex A.

4. Safegate is a firewall that provides an Internet Protocol (IP) packet filtering function, an application gateway function (transparent and non-transparent) and a security management function containing all the audit functions. The TOE works as a firewall that serves as a single point connecting a private network to the Internet or hostile network.

5. The IP packet filtering function permits or denies the transmission of IP packets through the TOE between the hostile network and the private network in accordance with the filtering rules defined by the authorised administrator.

6. The application gateway operates in transparent mode and non-transparent mode. Transparent mode provides direct connection between the client on the private network and the target host on the Internet and establishes a session between the networks. Transparent mode provides Transmission Control Protocol (TCP), Universal Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) proxy services for File Transfer Protocol (FTP), Telnet, mail (excluding Simple Mail Transfer Protocol, SMTP), news (excluding Network News Transfer Protocol, NNTP), HyperText Transfer Protocol (HTTP), Wais, Gopher and RealAudio, VDO Live and Stream Work multimedia services. In non-transparent mode the TOE mediates between the client on the private network and the Internet host by establishing simultaneous sessions with the client and host. Non-transparent mode only applies to the FTP and Telnet services. No extra authentication for these services is provided by the TOE.

7. The auditing function is used to log information on IP packet filtering and the application gateway, to provide an alert function if an invalid packet is detected, a monitoring function and an audit filtering function.

8. The security management function is used to configure and operate the TOE.

9. The TOE consists of 39 subsystems which are all TOE Security Policy (TSP)-enforcing. These systems provide the IP packet filtering, application gateway, audit and security management functions.

10. Details of the TOE' s architecture can be found in Annex B to this report.

TOE Scope

11. The scope of the Certification applies to the TOE running on the Solaris Version 2.6 operating system with patch 105580-01 and on a SUN 4 machine with a 248 MHZ processor and 128MB of RAM. The TOE must be used in an Ethernet Local Area Network (LAN, 10M and 100M) based on STREAMS of SVR4 on which IP and ICMP function correctly with all TCP/IP network protocols available. The TOE can have a maximum of 8 LAN interface cards with IEEE802.3 Ethernet.

12. The subsystems within the scope of the evaluation are detailed in Annex B to this report. The services within the scope of the evaluation are detailed in paragraph 6 above.

13. The evaluation of Safegate Version 2.0.2 **excludes** the following functionality:

- Authentication function
- original encryption function
- IP security encryption function
- Load balancing function

Protection Profile Conformance

14. The Security Target [c] did not claim conformance to any protection profiles.

Assurance Level

15. The Security Target [c] specifies the assurance requirements for the resultant evaluation. Predefined evaluation assurance level EAL3 was used. Common Criteria Part 3 [f] describes the scale of assurance given by predefined evaluation assurance levels EAL1 to EAL7. EAL0 represents no assurance.

Strength of Function

16. The TOE did not contain any cryptographic, permutational or probabilistic security mechanisms and therefore no Strength of Function (SoF) was applicable to the TOE.

17. The minimum SoF for the search for vulnerabilities conducted by the Evaluators was SOF-medium to provide adequate protection against intruders with a moderate attack potential.

Security Claims

18. The Security Target [c] fully specifies the TOE' s security objectives, and threats which these objectives counter, and functional requirements and security functions to elaborate the objectives. The Security Target does not mandate compliance with any Organisational Security Policies. All of the functional requirements were taken from Common Criteria (CC) Part 2 [e]; use of this standard facilitates comparison with other evaluated products. An overview of CC is given in CC Part 1 [d].

Threats Countered

19. The threats that the TOE is to counter are as follows:

a. Attackers on the external network may gain inappropriate access to the private network.

b. Users on the private network may inappropriately expose data or resources to the hostile network.

c. Attackers on a hostile network posing as private network users may modify, destroy or disclose resources on the private network.

d. Attackers on a hostile or private network may intrude into the TOE to make changes to the filtering rules and the environment definition file, and as a result unauthorised packets and services pass through the TOE.

e. Attackers on a hostile or private network may intrude into the TOE to make changes to the logging information, and as a result obscure evidence of their entry.

f. Private network users accessing hostile networks may inadvertently expose the addresses and physical configuration of the private network to hostile users.

g. Information on the private network system may be exposed to hostile network users by using ICMP attacks on the target system that includes the TOE and the private network.

h. As a result of incorrect definition of packet filtering rules, the TOE security functions may permit services that violate the security policy.

Threats Countered by the TOE' s Environment

20. The threats that are countered by the TOE' s environment are as follows:

a. Attackers on a hostile network may exploit new, previously unknown, attack method.

b. Attackers on a hostile network may attack unsecured configurations of hosts on the private network.

c. Attackers on a hostile network may attack the TOE and machines on the private network by taking advantage of security relevant defects in existing services.

d. Attackers may attack to modify the TOE itself and pass unauthorised packets through the TOE.

Threats and Attacks not Countered

21. The threats that are not countered by the TOE or by the TOE' s environment are as follows:

a. Attackers on a hostile network may successfully hijack an open session with a host on the private network.

b. Viruses within incoming traffic are not scanned.

c. Malicious active content, such as Java and ActiveX, is not blocked separately from HTTP.

d. The private network may be exposed to attack by routing packets through routers peripheral to the private network using Routing Information Protocol (RIP).

e. Attackers on a hostile network attack the TOE and the private network by issuing source routing packets with unauthorised routing information.

Environmental Assumptions and Dependencies

22. The TOE' s environment must also satisfy the following assumptions:

a. The TOE must be protected so that only the administrator can access it.

b. The TOE is assumed to be a host connected to 2 or more networks.

c. Only one connection point must exist on the TOE between the private and hostile networks.

d. There shall be no violations of the network security policy as a result of inaction or irresponsible action by careless, willfully negligent or unethical system administrators.

e. The configuration of the TOE should be reviewed on a regular basis to ensure that the configuration continues to meet the organisation' s security objectives when the TOE' s configuration, security objectives, threat environment or available private hosts change and services change.

f. The TOE administrator shall follow the administrative procedures, shall ensure that users are trained and shall check the audit trail on a regular basis to for unauthorised operations.

23. The TOE has no hardware or firmware dependencies, but it relies on the Solaris Version 2.6 operating system software for file access and use of root privilege.

IT Security Objectives

24. The IT security objectives in the Security Target [c] are as follows:

a. The TOE must be capable of identifying a single host or group of hosts before the TOE allows a connection to be established.

b. The TOE must limit the valid range of addresses expected on each of the private and hostile networks.

c. The TOE must limit the hosts and service ports on the private network that can be accessed from the hostile network.

d. The TOE must limit the hosts and service ports on the hostile network that can be accessed from the private network.

e. The TOE must have the ability to conceal the IP addresses of clients on the private network from a hostile network.

f. The TOE must provide a single focus of administrative control of the TOE, ensuring that only the authorised administrator can exercise control.

g. The TOE must provide a facility for monitoring successful and unsuccessful attempts at connections between the private and the hostile network.

h. The TOE must provide measures for recording, searching and retrieving an audit trail in a format that enables recognition of security related events and that includes accurate date and time records.

Non-IT Security Objectives

25. The non-IT security objectives in the Security Target [c] are met by procedural or administrative measures in the TOE' s environment and are as follows:

a. Those responsible for the TOE must ensure that it is delivered, installed and managed in a manner that maintains the security policy.

b. The TOE must be established in an environment where only administrators can enter and the TOE itself must be protected from unauthorised modification by the operating system' s function.

c. Those responsible for the TOE must train administrators to establish and maintain sound security policies and practices.

d. Administrators of the firewall must ensure that the audit facilities are used and managed effectively. In particular, appropriate action must be taken to ensure that sufficient free space to allow continued audit logging is available. Furthermore, audit logs should be inspected on a regular basis and appropriate archive action must be taken upon detecting security breaches or events that are likely to lead to a future security breach.

e. Safegate is designed and configured to act solely as a firewall on a host and does not provide any user services that are not related to the TOE' s execution.

f. The firewall must be configured as the only network connection between the internal networks and external networks.

Security Functional Requirements

26. The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- Subset information flow policy (FDP_IFC.1)
- Information flow functions based on simple security attributes (FDP_IFF.1)
- Security alarms (FAU_ARP.1)
- Security audit data generation (FAU_GEN.1)
- Security audit analysis (FAU_SAA.1)
- Security audit review (FAU_SAR.1)
- Selectable audit review (FAU_SAR.3)
- Selective audit (FAU_SEL.1)
- Prevention of audit data loss (FAU_STG.4)
- Management of security functions' behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Management of TOE Security Functions' (TSF) data (FMT_MTD.1)

27. The underlying operating system is required to satisfy the following SFRs:

- Restricted audit review (FAU_SAR.2)
- Protected audit trail storage (FAU_STG.1)
- Non-bypassibility of the TSP (FPT_RVM.1)
- TSF domain separation (FPT_SEP.1)
- Reliable time stamps (FPT_STM.1)
- Security roles (FMT_SMR.1)

Security Function Policy

28. The TOE has an explicit information flow policy defined in the FDP_IFC.1 and FDP_IFF SFRs.

29. Packet filtering is performed on the basis of a filtering condition based on the Organisational Security Policy and can be used to restrict information flow based on packet direction, network interface, packet processing type (acceptance or rejection of filtered packets) and protocol header information. The TOE' s default is to block all packets on which a filtering condition is not defined.

30. The application gateway provides address translation for addresses on the private network to the TOE' s global IP address for outgoing traffic and translation in the reverse direction for incoming traffic.

Evaluation Conduct

31. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UKSP 01 and UKSP 02 [a, b]. The Scheme has established a Certification Body which is jointly managed by the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry on behalf of Her Majesty' s Government.

32. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [c]. To ensure that the Security Target gave an appropriate baseline for a Common Criteria evaluation, it was first itself evaluated, as outlined in CC Part 3 [f].

33. The evaluation was performed against the EAL3 assurance package defined in CC Part 3 [f]. The Common Evaluation Methodology (CEM) [g] was used as the methodology for the evaluation.

34. The Evaluators conducted sampling during the evaluation as required for the relevant work-units for EAL3. Guidance provided in the CEM [g], Annex B, Section B.2, was followed in all cases. The Evaluators also confirmed the sample size and approach with the Certifier in all cases. For the testing the Evaluators repeated a sample of 5% of the Developer' s tests and checked that the sample covered all the security functions and sub-functions of the TOE. Where the sampling related to gaining evidence that a process such as configuration control was being followed, the Evaluators sampled sufficient information to gain reasonable confidence that this was the case.

35. The Evaluators did not use any software tools during independent testing.

36. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The interim Evaluation Technical Report (ETR) for the first two phases [h] was submitted to the Certification Body in December 1999. The evaluation was completed in February 2000 when the CLEF submitted the final ETR [i] to the Certification Body which, in turn, produced this Certification Report.

Certification Result

37. For the evaluation result see the "Evaluation Outcome" section.

General Points

38. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) 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. Consumers are reminded of the security dangers inherent in downloading ' hot-fixes' where these are available, and that the UK Certification Body provides no assurance whatsoever for patches obtained in this manner. More up to date information on known security vulnerabilities within individual certified products and systems can be found on the IT Security Evaluation and Certification Scheme web site www.itsec.gov.uk.

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

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

II. EVALUATION FINDINGS

41. The Evaluators examined the following assurance classes and components taken from CC Part 3 [f]. These classes comprise the EAL3 assurance package.

Assurance class	Assurance components
Configuration management	Authorisation Controls (ACM_CAP.3)
	TOE Configuration Management coverage (ACM_SCP.1)
Delivery and operation	Delivery procedures (ADO_DEL.1)
	Installation, generation and startup procedures (ADO_IGS.1)
Development	Informal functional specification (ADV_FSP.1)
	Security enforcing high-level design (ADV_HLD.2)
	Informal correspondence demonstration (ADV_RCR.1)
Guidance documents	Administrator guidance (AGD_ADM.1)
	User guidance (AGD_USR.1)
Life cycle support	Identification of security measures (ALC_DVS.1)
Security Target	TOE description (ASE_DES)
	Security Environment (ASE_ENV)
	Security Target introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	Protection Profile claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)
Tests	Analysis of coverage (ATE_COV.2)
	Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability Assessment	Misuse: examination of guidance (AVA_MSU.1)
	Strength of TOE security function evaluation (AVA_SOF.1)
	Developer vulnerability analysis (AVA_VLA.1)

42. All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

43. The Evaluators made a number of recommendations which are recorded in the "Recommendations" section below.

44. There are a number of aspects of the evaluation that are relevant to consumers. These are summarised in the sections that follow.

Delivery and Installation

45. The consumer receives the TOE as a shrink wrapped package clearly labelled as Safegate Version 2.0.2. This will ensure that interference with the TOE will be detectable. It is sent by a courier to the consumer. A licence application form is sent to the consumer with the TOE software package. The consumer completes the licence application form which is faxed to the Developer, who checks the application and faxes back a licence password to use the product. This ensures that a third party could not masquerade as the Developer and supply potential malicious software.

46. Consumers should be aware that the installation guidance is contained in the S Family Software Description [l] rather than in the Installation Guide [k]. The Installation Guide is concerned with licensing during installation.

47. The TOE contains 2 patches (910101-01 and 910160-02) which are installed on top of the base product (Safegate Version 2.0). Installation guidance for these patches is contained in the S Family Software Description [l].

48. The TOE has a number of configuration options which the consumer must perform in order to use the TOE. These options are described in the S Family Software Description [l]. The Evaluators were satisfied that the recommended configuration options described in the S Family Software Description [l] lead to a secure installation of the TOE.

User Guidance

49. The Evaluators found that all TOE security is invisible to non-administrative users. The evaluation of user documentation (AGD_USR.1) was not relevant, and the assurance class was trivially satisfied.

50. The administrator can configure the TOE to start and stop services, stop and start IP filtering, to set conditions for a remote X terminal when used as a visual display, to set conditions for Simple Network Management Protocol (SNMP) linkage used for alert notification, to control licensing and to allow monitoring, logging and alerts. In order to maintain security, the administrator should use IP filtering, the application gateway function, monitoring, logging and alerts. In particular, switching off logging would greatly reduce the security of the TOE. It is therefore recommended that logging is used at all times unless there is a good reason for switching it off.

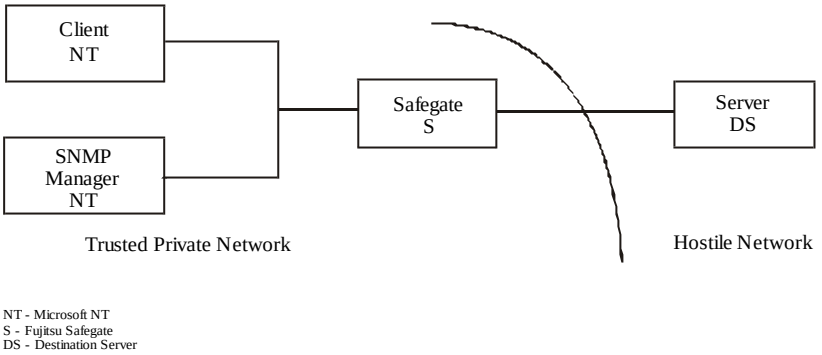
Misuse

51. Administrators should follow the guidance in the administration guidance documentation [j] in order to ensure that the TOE operates in a secure manner. The guidance document adequately described all possible error codes and subsequent administrator action.

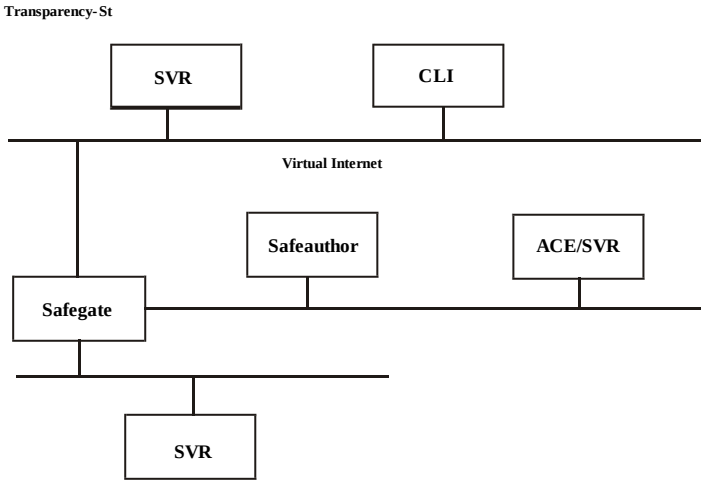
Developer's Tests

52. Two forms of developer testing were performed: component testing and system testing. The Developer performed component testing to ensure that all of the security functionality provided by the TOE operated correctly.

53. 2 test environments were used by the Developer for component testing:



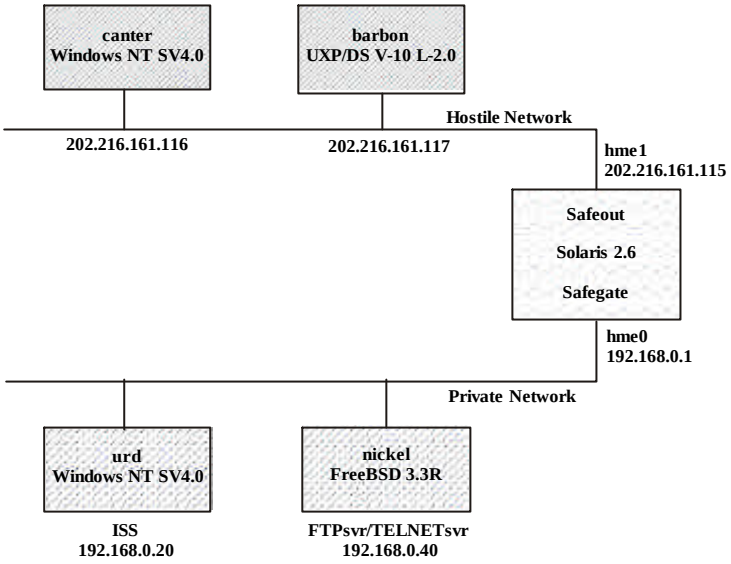
Test Environment 1 for Component Testing



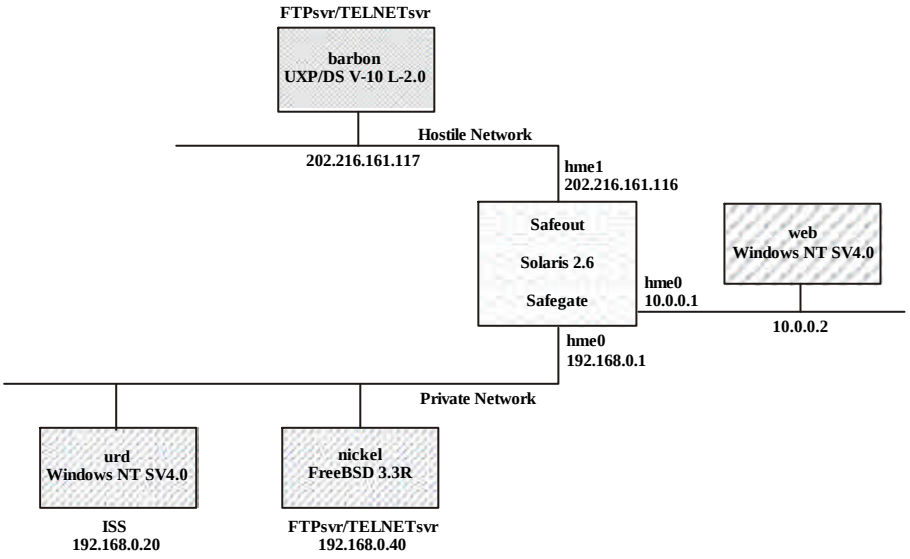
Test Environment 2 for Component Testing

Evaluators' Tests

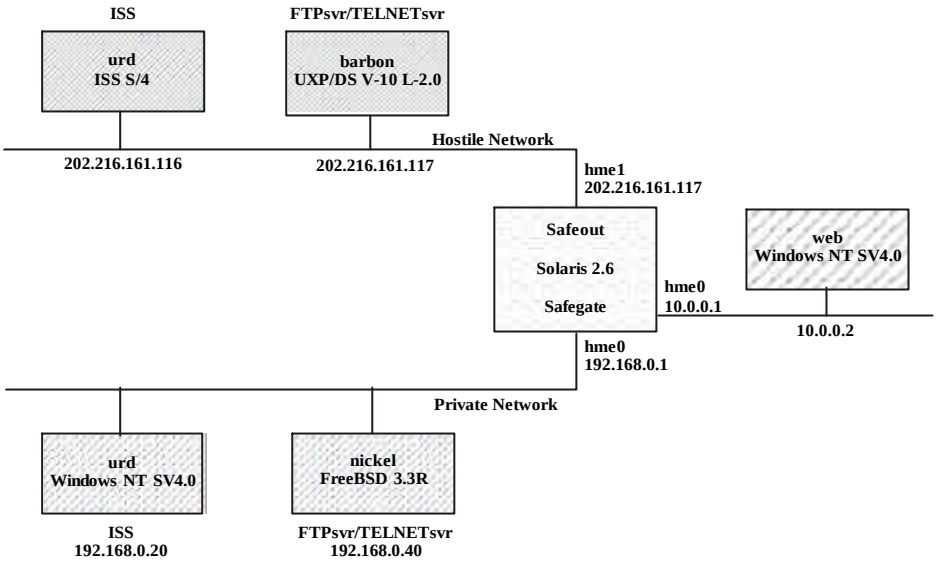
54. Evaluator testing covered the following three environments:



Evaluators' Test Environment 1



Evaluators' Test Environment 2



Evaluators' Test Environment 3

55. Evaluator testing confirmed the following:

a. The TOE separates a private network from a hostile network and that there is only one connection between private and hostile networks, mediated by Safegate.

b. External interfaces behaved as expected for TCP, ICMP, RIP, ARP and UDP.

c. The TOE withstands IP spoofing and fragment attacks.

d. Access mediation, access display, access control, event auditing and alarm mechanisms worked as specified.

e. Limit and range of buffer boundaries, protocol settings and alert thresholds operate adequately.

III. EVALUATION OUTCOME

Certification Result

56. After due consideration of the ETRs [h, i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Safegate Version 2.0.2, running on Solaris Version 2.6 with patch 105580-01 in the environment specified in Annex A, meets the CC Part 3 specified CC Part 3 [f] augmented requirements of Evaluation Assurance Level EAL3 for the specified CC Part 2 [e] conformant functionality in the specified environment. No minimum SoF claim was applicable as the TOE did not contain any cryptographic, permutational or probabilistic security mechanisms.

Recommendations

57. Prospective consumers of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [c].

58. The TOE provides some features that were not within the scope of the evaluation as identified in the "TOE Scope" section above. The secure use of these features has thus not been considered by the evaluation. It is recommended that these features should not be used if the TOE is to comply with the evaluated configuration.

59. Only the evaluated product configuration, specified in Annex A, should be installed. The product should be used in accordance with its guidance documentation.

60. The product should only be used in accordance with the environmental considerations outlined in the Security Target [c].

61. Consumers should consider the threats not countered by the TOE when devising their Organisational Security Policy and may need to consider additional products to provide content checking and virus checking functionality not provided by the TOE.

62. It is recommended that the output logging function is active at all times unless there is a good reason for switching it off.

63. It is extremely important that the administrator follows the correct procedures and understands the consequences of every action in using the environmental setting commands.

64. It is important that all FTP and Telnet user names and passwords, including the TOE administrator user name and password, are kept confidential because it is necessary to log on to the TOE if FTP or Telnet are used. It is therefore also recommended that the administrator password is set to a large number of characters which are chosen in such a way as to make it extremely unlikely that the administrator password could be guessed.

65. It is recommended that the TOE' s guidance documentation specifies that the TOE cannot be used with a multicast router (as used for the transmission of high bandwidth applications such as video and audio conferencing) and so cannot filter IP-in-IP tunnelled packets.

66. The Certification Body recommends that the Developer implements the following suggestions made by the Evaluators for improving the development environment:

a. a configuration management tool could be used to manage all configuration items;

b. an overall configuration controller and a deputy could be appointed;

c. a paper copy of the PowerDM configuration tool password could be securely stored for use in emergencies;

d. measures to protect backup tapes could be introduced;

e. a disaster recovery procedure including off-site storage of backups could be introduced;

f. project related waste could be locked away before incineration; and

g. a clear desk policy could be introduced.

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

   Safegate Version 2.0.2

2. The supporting guidance documents evaluated were:

   - Safegate Description Manual [j]
   - Installation Guide [k]
   - S Family Software Description [l]

TOE Configuration

3. The TOE had the following configuration options at installation:

   - Order of the TOE' s individual packages - The numeric values representing the packages required must be entered in the specified order.
   - network connectivity - Installation allows the TOE to be connected to the hostile network. It is recommended that this is not allowed.
   - IP forwarding - This may be enabled or disabled.
   - Use of the inetd command - When Package Number 4 (FSUNfwip) is installed, it is recommended that this command is used to disable all available services.

4. There are 7 packages available for installation are as follows:

   - Safegate Application Gateway
   - Safegate IP filter
   - Flexible Licence Manager
   - Authentication function
   - Original encryption function
   - IP security encryption function
   - load balancing function

5. Of these 7 packages, all were installed during Developer' s and Evaluators' testing but only the following 3 packages were within the scope of the evaluation:

   - Safegate Application Gateway
   - Safegate IP filter
   - Flexible Licence Manager

6. The TOE contains 2 patches (910101-01 and 910160-02) which are installed on top of the base product (Safegate Version 2.0). Guidance on the order of installing packages and patches and on secure initial configuration is provided in the S Family Software Description [l].

Environmental Configuration

7. The TOE runs on Solaris Version 2.6 with patch 105580-01. This patch was developed by Fujitsu Limited.

8. The specific configuration of the machine used during the Evaluators' tests for the TOE was a SUN 4 with 248 MHZ processor, 128 MHZ RAM and 4.2 GB hard disk.

9. The minimum recommended memory specification for the TOE is as follows:

- 32MB + (0.5 MB*number of connections) RAM for the transparent gateway
- 6 MB + (0.5 MB*number of connections) swap size for the transparent gateway

10. To install the TOE a hard disk with at least 47.7 MB available space is required. This should be as follows:

- /root directory 1.0 MB
- /usr directory 0.7 MB
- /var directory 16.0 MB
- /opt directory 30.0 MB

11. The TOE must be used in an Ethernet Local Area Network (LAN, 10M and 100M) based on STREAMS of SVR4 on which IP and ICMP function correctly with all TCP/IP network protocols available. The TOE can have a maximum of 8 LAN interface cards with IEEE802.3 Ethernet.

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. The main high level design components of Safegate comprise:

   a. IP packet filtering, which is composed of the following subsystems:

      i. IP packet filtering control. This controls the IP packet filtering at the kernel level by allowing filtering conditions to be set, activated and deactivated.

      ii. IP packet filtering. This filters IP packets according to the conditions defined above.

      iii. Re-configuration of the IP packets. This reassembles the fragments of IP packets.

   b. Transparent gateway, which is composed of the following subsystems:

      i. Start-up. This starts up the transparent gateway.

      ii. Termination. This terminates the transparent gateway.

      iii. Timeout monitoring. This monitors the timeout in relay processing by the transparent gateway.

      iv. TCP relay. This relays packets through the TCP connection.

      v. FTP relay. This relays packets through the FTP connection, supported by the TCP connection.

      vi. Waiting for TCP connection. Once an address translation has changed the destination address to the host address, there is a request for a TCP connection.

      vii. Address translation. This translates the source IP address and destination IP address of an IP packet.

   c. Non-transparent gateway, consisting of the following subsystems:

      i. TELNET daemon. This is the Telnet proxy which relays the Telnet server facilities and the Telnet connection with the destination system.

      ii. FTP daemon. This is the FTP proxy which relays the FTP server facilities and the FTP connection.

   d. Security management, comprising the following subsystems:

i. Start-up of the filter logging daemon. This allows the user to start up the filter logging daemon.

ii. Termination of the filter logging daemon. This allows the user to terminate the filter logging daemon.

iii. Filter logging daemon. This collects, analyses and outputs the log information from the IP packet filtering function. Any alerts are notified.

iv. Filter logging viewer. This displays the information output by the filter logging daemon.

v. Filter logging monitor. This displays in real time the information the filter logging daemon has found.

vi. Transparent gateway logging daemon. This collects, analyses and outputs the information from the transparent gateway.

vii. Transparent gateway logging viewer. This displays the information output by the transparent gateway logging daemon.

viii. Transparent gateway logging output. This outputs the information output by the transparent gateway logging daemon.

ix. Transparent gateway logging monitor. This displays in real time the information the transparent gateway logging daemon has found.

x. Non-transparent gateway logging daemon. This collects, analyses and outputs the information from the non-transparent gateway.

xi. Non-transparent gateway logging viewer. This displays information about the logging files output by the non-transparent gateway.

xii. Non-transparent gateway logging output. This displays the information output by the non-transparent gateway logging daemon.

xiii. Environment set-up Graphical User Interface (GUI). This is the TOE environment set-up for setting the TOE operating environment.

xiv. Network configuration diagram. This allows the user to set-up the network configuration.

xv. Interface settings. This allows the network interface information to be set.

xvi. Host settings. This allows the user to set-up host information.

xvii. Host group settings. This allows the user to set-up information about grouping of multiple hosts.

xviii. Network settings. This allows the user to set-up grouping information for multiple hosts.

xix. Protocol settings. This allows the user to set the IP protocol that will be used for the IP packet filtering.

xx. Service settings. This allows the user to set the port number to be used for the IP packet filtering.

xxi. Service group settings. This allows the user to set the information about grouping services.

xxii. Filtering conditions. This allows the user to set the filtering conditions for the IP packet filtering.

xxiii. Transparent mode gateway settings. These allow the user to set the operating environment for the transparent mode gateway.

xxiv. Non-transparent mode gateway settings. These allow the user to set the operating environment for the non-transparent mode gateway.

xxv. Logging operating environment. These allow the user to set the operating environment for the different types of logging facilities.

xxvi. Alert operating environment. This allows the user to set-up the operating environment for the alert facilities.

2. Security Management breaks down into 8 trusted functions. They map to subsystems as follows:

Security Function	Subsystem
Logging	Start-up of the filter logging daemon Termination of the filter logging daemon Filter logging daemon Transparent Gateway logging daemon Non-transparent Gateway logging daemon.
Alert	Alert notification
Monitoring	Filter logging monitor Transparent Gateway logging monitor
Log output	Filter logging output

Security Function	Subsystem
Log viewer	Filter logging viewer Transparent Gateway logging viewer Non-transparent Gateway logging viewer
Environment setting	Environment set-up GUI Network configuration diagram Interface settings Host settings Network settings Protocol settings Service settings Service group settings Filtering conditions Transparent mode Gateway settings Non-transparent Gateway settings Logging settings Alert settings

3. The following diagram shows the subsystems described in the high level design and relationships between them: