UK IT SECURITY EVALUATION AND
CERTIFICATION SCHEME

UKAS
PRODUCT
CERTIFICATION
122-B

COMMON CRITERIA CERTIFICATION REPORT No. P184

CS Bastion II

running on Trusted Solaris 8 4/01 and specified Sun Workstations

Issue 1.0

June 2003

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

Clearswift (CS) Bastion II is an application-level messaging firewall designed for use between incompatible or mutually mistrusting subscriber networks. Its primary goal is to provide assured separation between 2 subscriber networks, while permitting limited authorised message transfer.

CS Bastion II has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality in the specified environment when running on Trusted Solaris 8 4/01 and the Sun Workstations specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body, UK IT Security Evaluation and Certification Scheme
Date authorised	12 June 2003

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CC	Common Criteria
CD-ROM	Compact Disk – Read Only Memory
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
CMW	Compartmented Mode Workstation
CS	Clearswift
DISP	Directory Information Shadowing Protocol
DMZ	De-Militarised Zone
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
I/O	Input/Output
ITSEC	Information Technology Security Evaluation Criteria
ROSE	Remote Operations Service Element
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SoF	Strength of Function
TMS	Trusted Messaging Subsystem
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. CS Bastion II Security Target (EAL4),
Clearswift,
DN11272/5, Issue 5.0, 29 May 2003.

b. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

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

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

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

h. Certification Report No. P170, Sun Microsystems, Inc, Trusted Solaris Version 8 4/01,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, June 2002.

i. Certification Report No. P144, MailGuard Bastion Release 1.0.0, including Trusted Solaris 2.5.1, running on Sun Ultra SPARC-1/170 Workstation,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, June 2000.

j. Bastion Version 2 Evaluation Technical Report,
CMG CLEF, CMG (UK) Ltd,
114254/T15/1, Issue 1.0, April 2003.

k. Supplement to T169 Evaluation Technical Report,
CMG CLEF, CMG (UK) Ltd,
114254/T3.2/3, 29 May 2003.

l. Clearswift Bastion 2 Installation Guide,
Clearswift,
DN11326/2, Issue 2.0, 13 February 2003.

m. Clearswift Bastion 2 Release Notice,
Clearswift,
DN11327/3-RN, Issue 3.0, 10 February 2003.

n. Clearswift Bastion 2 Administration Guide,
Clearswift,
DN11333/4, Issue 4.0, 21 May 2003.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Clearswift (CS) Bastion II to the Sponsor, Clearswift, 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:

CS Bastion Version 2.0.0.

This product is also described in this report as the Target of Evaluation (TOE). The product is marketed and hereafter referenced in this report as CS Bastion II. The Developer was Clearswift.

4. CS Bastion II is an application-level messaging firewall designed for use between incompatible or mutually-mistrusting subscriber networks where one or both networks may require complete accountability of all traffic passing through the firewall. Its primary goal is to provide assured separation between 2 subscriber networks, while permitting limited authorised message transfer.

5. CS Bastion II provides a protected De-Militarised Zone (DMZ) into which additional software modules can be installed to police the traffic flow in each direction. A separate channel is provided in each traffic flow direction to permit message checks by different vetting (or DMZ) functions. Each channel supports up to 5 independent DMZ functions, each in its own protected environment (a compartment defined by the underlying UNIX-based operating system, Trusted Solaris 8 4/01). A channel is defined by the number and order of proxy and DMZ compartments that each message is forced to pass through by the messaging system. The first DMZ compartment in each channel is reserved for a message-archiving function, which, if employed, will take a copy of all data passing between the networks to a protected partition on disk.

6. CS Bastion II provides a framework into which a variety of proxy and DMZ functions can be pre-configured at install time, creating a range of different firewall services. Currently there is a choice of X.400, SMTP or ROSE (for DISP) proxies, and each has an optional DMZ function for verifying conformance to the protocol. However the architecture will also support many other store-and-forward style protocols, such as FTP or any other ROSE-based protocol, along with any number of specialized DMZ functions to meet specific customer requirements. The DMZ functions can be used to apply import/export sanctions, or to enforce additional elements of network security policy such as (but not limited to) virus scanning, content filtering, filtering based on sensitivity labels or digital signature verification. It is also possible to give

individual DMZ functions (with the exception of the message-archiving function) access to their own private network to create one or more "extended DMZs" and to meet a much wider range of applications.

7. Each CS Bastion II will support just one pair of proxies, so multiple copies of CS Bastion II are required to support multiple protocols between subscriber networks. In configurations composed of multiple copies of CS Bastion II, each CS Bastion II instantiation is maintained and supported independently by Trusted Solaris 8 4/01.

8. Annex A provides details of the evaluated configuration of the TOE.

9. Annex B provides an overview of the TOE's security architecture.

TOE Scope

10. The TOE is preinstalled and preconfigured and runs on the Trusted Solaris 8 4/01 operating system and specified Sun Workstations. (See paragraph 14 below.) The operating system provides Administrator identification and authentication, together with system auditing, and has been previously certified to CC Evaluation Assurance Level EAL4 [h]. The environmental configuration used for evaluation excludes any subsequent patches to the previously-certified Trusted Solaris 8 4/01 [h] (as no Trusted Solaris 8 4/01 patches available at the time of the CS Bastion II certification were considered relevant to the security of the TOE) and any uncertified Trusted Solaris 8 4/01 functionality except that which supports the specified hardware platforms.

11. With the exception of the message-archiving program, the software running in all DMZ and proxy compartments is not implementing any TOE Security Function and it may therefore be considered security irrelevant (i.e. neither security critical nor security supporting) with respect to the TOE, subject to the constraints listed under the heading "Rationale for Security-Irrelevant Subsystems". However, depending on the criticality of the vetting software to the specific application, the consumer may need to seek independent assurance in the correct operation of such software.

12. The evaluated DMZ functions include only the message-archiving function. Although the X.400 and SMTP proxies and associated protocol conformance verification functions are not included in the Security Functions, it should be noted that their correct operation was checked during the Developer tests. No other proxy or vetting functions were checked for correct operation during the Developer tests.

13. The environmental configuration of CS Bastion II includes 2 subscriber network interfaces and between zero and 8 private network interfaces, the latter allowing each DMZ compartment (except the message-archiving compartments) to have the option of an extended DMZ.

14. The TOE will execute on any single Sun SPARC Workstation running Sun Trusted Solaris 8 4/01 as detailed in Annex A. The TOE was evaluated on Sun Blade 100, Sun Fire 280R and Sun Ultra 5/10 test platforms as detailed in Annex C. The rationale for the inclusion of other platforms in the evaluated configuration is discussed under "Platform Issues" below.

15. Network interface cards are part of the platform and are those supported by Trusted Solaris 8 4/01. Note that only those network interface cards detailed in Annex C have been tested. A rationale for extension of the test results to other network interface cards is provided under the heading "Platform Issues". However, only those cards that have been tested and acknowledged by Sun Microsystems to be free of potential vulnerabilities should be used. Only the latter type of cards will be included in the pre-configured systems delivered by Clearswift. (See further discussion under the heading "Recommendations".)

16. The Security Target [a] assumes that if one or both of the mediated subscriber networks is considered hostile then the use of a perimeter network and packet-level filters is required to protect CS Bastion II from low-level attacks such as denial-of-service. Such additional protection measures are excluded from the scope of the evaluation.

17. Configurations composed of multiple copies of CS Bastion II were not tested during the evaluation.

Protection Profile Conformance

18. The Security Target [a] did not claim conformance to any protection profile.

Assurance

19. The Security Target [a] specified the assurance requirements for the evaluation. The predefined Evaluation Assurance Level EAL4 was used.

20. CC Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

21. A minimum Strength of Function (SoF) claim of SoF-Medium was made for the TOE. This was commensurate with the Administrator password authentication function, which was provided by the previously-certified Trusted Solaris 8 4/01 [h].

Security Policy

22. The TOE Security Policy, i.e. the Bastion Message Flow Control Policy, is expressed implicitly within the SFRs detailed in Section 5.1 of the Security Target [a].

23. There are no Organizational Security Policies with which the TOE must comply.

Security Claims

24. The Security Target [a] 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.

25. With the exception of FAU_GEN.3, FAU_GEN.4 and FMT_SMR.4, all of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated

products. FAU_GEN.3, FAU_GEN.4 and FMT_SMR.4 are fully defined in Section 5.1 of the Security Target [a]. If pre-configured, FAU_GEN.3 ensures that all messages entering the DMZ are archived. FAU_GEN.4 ensures that all changes in state of CS Bastion II software, and all security-critical Trusted Solaris 8 4/01 events, are recorded in a Trusted Solaris 8 4/01 audit trail. FMT_SMR.4 ensures that CS Bastion II roles are configured in Trusted Solaris 8 4/01.

26. Security functionality claims are made for the following 7 categories of IT Security Functions:

- Domain Separation
- Network Separation
- Assured Message Handling
- Assured Message Channels
- Message Archives
- System Auditing
- Administration Access Control

Evaluation Conduct

27. 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 and UKSP 02 [e, f]. The Scheme has established a Certification Body which is managed by the Communications-Electronics Security Group on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the CC Mutual Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

28. 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.

29. To ensure that the Security Target gave an appropriate baseline for the CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [d], the Common Evaluation Methodology (CEM) [g] and relevant interpretations.

30. The Security Functions and security environment, together with the supporting evaluation deliverables, have undergone some revision and re-organisation compared with that of the previous TOE Release, i.e. MailGuard Bastion Release 1.0.0, which had previously been certified by the UK IT Security Evaluation and Certification Scheme to ITSEC E3 [i]. For the evaluation of CS Bastion II, the Evaluators thus enhanced the previous test scripts as appropriate, but otherwise made no re-use of the MailGuard Bastion evaluation results and addressed every CEM [g] EAL4 work unit.

31. The Certification Body monitored the evaluation which was carried out by the CMG Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the final Evaluation Technical Report (ETR) [j] to the Certification Body in April 2003. Following the CLEF response [k] to a request for clarification, the Certification Body then produced this Certification Report.

General Points

32. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. 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.

33. 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 penetration testing (January 2003). 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 such patches have been evaluated and certified.

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

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

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

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

Delivery

37. Secure delivery of the TOE is described in the delivery procedures, detailed in Section 3 of the Installation Guide [l], which describes the process of releasing the TOE to consumers. Some password advice related to the **csbuser** account and EEPROM password is also included in the Release Notice [m]. (Secure delivery of Trusted Solaris 8 4/01 is summarised in Certification Report No. P170 [h].)

38. Secure delivery is triggered by the completion of a Clearswift Customer Order Form, which provides details of the consumer's network infrastructure and the required TOE configuration, in particular the composition of the proxy and DMZ compartments.

39. Following confirmation of the order, copies of the TOE (either 2 CD-ROMs or a CD-ROM with a floppy disk, in protective Clearswift-branded packaging), together with the installation and guidance documentation and 2 Trusted Solaris 8 4/01 CD-ROMs, are packed in Clearswift-branded packages with a tamper-resistant seal in the Developer's distribution facility to form an installation kit. The TOE with delivery note is hand-delivered to the consumer as an installation kit for use by the Clearswift or Clearswift-trained consumer installation team at the consumer site and optionally as a pre-installed, pre-configured system that includes the required hardware. The method of hand delivery by a trusted person (a member of the Clearswift or consumer installation team) ensures that the TOE is not susceptible to tampering during delivery.

40. On receipt of the TOE, the consumer is recommended to check that the installation kit includes the required components. (See Annex A for details of the TOE media and related labelling.) The contents of the delivery should be checked against the delivery note sent with the delivery, which for a pre-installed system would also include a copy of the Sun-produced delivery note.

41. Once the delivery has been checked and, if appropriate, the on-site installation performed (see below), the installation team must contact the distribution site either to obtain the Clearswift-supplied master password required by the startup procedures as detailed in the Release Notice [m] or to request a reshipment if installation has been unsuccessful. The consumer is then recommended to follow the startup procedures detailed in the Release Notice to check that all network connections are operational, that all compartments and network interfaces match the configuration specified on the Customer Order Form, and that all compartment subsystems are present with the correct operational status. The startup procedures enable the consumer to check that the TOE configuration includes the csblaunch software version detailed in Annex A paragraph 3. (The csbarchtidy software version should be checked when managing the message archives.)

42. If the TOE installation is to be performed at the consumer's site, then prior to installation, the consumer should check the TOE media in the installation kit against the evaluated configuration as recommended in paragraph 40. (If such an installation is to be performed by Clearswift, the installer will have their own identical copy of the TOE media that will normally be returned to Clearswift after the installation is complete. This copy of the TOE media should also be checked against the evaluated configuration.) The installer will complete the installation using the information provided on the Customer Order Form.

43. If the TOE installation is to be performed at the distribution site, then the installation will be performed using one of the Clearswift distribution copies of the TOE media and the information provided on the Customer Order Form. The system, which includes Trusted Solaris 8 4/01 and all required hardware, is then re-packaged in the original packaging and accompanied to the consumer site by a member of the Clearswift or consumer installation team.

Installation and Guidance Documentation

44. Secure installation, generation and startup of the TOE are described in the Installation Guide [l] and Release Notice [m].

45. The installation procedures must be carried out by Clearswift-trained members of the installation team prior to handover (ie delivery) to the consumer. Installation and configuration may be performed either on the consumer site, or off-site (for pre-configured systems) at a central installation and distribution site. The installation procedures are semi-automated and:

- Ensure all network cards are correctly installed, with interfaces marked for each network.
- Ensure Trusted Solaris 8 4/01 is correctly and fully installed, in its evaluated configuration, using the 2 Trusted Solaris 8 4/01 CD-ROMs.
- Configure one or 2 channels in accordance with customer requirements.
- Ensure the core CS Bastion II software is correctly and fully installed, in its evaluated configuration.
- Install/configure each PROXY subsystem in accordance with customer requirements.
- Install/configure each DMZ subsystem in accordance with customer requirements.
- Password protect all means of direct access to the system using a Trusted Solaris 8 4/01 generated, Clearswift-supplied master password.
- Securely define and configure all network families (IP-address groups tied to a compartment).

46. The startup procedures are described in the Release Notice [m] and must be followed to complete the CS Bastion II installation into its target environment. These procedures explain how to:

- Switch on and perform the initial boot of the TOE.

- Use Trusted Solaris 8 4/01 to generate a new consumer password for each administration account.

- Physically attach the networks to the CS Bastion II and verify the connections are correct.

- Complete a phased startup of all TOE software and verify each TOE component is functioning correctly.

47. The system operation and administration procedures are described in the Administration Guide [n] and must be followed during normal day-to-day operation. With respect to the TOE, these procedures explain how to:

- Disable/enable message flow through a channel
- Disable/enable the software running in a DMZ compartment, whilst maintaining message flow in the channel.
- Stop/start the TOE during normal operation.

48. The Administration Guide [n] procedures also describe the use of Trusted Solaris 8 4/01 in the context of the TOE and explain how to:

- Reconfigure an administrator account (in the event that one has to be reassigned).
- Reconfigure a network family entry (in the event that IP addresses change).
- Disable/enable network access to those compartments that require it.
- Back-up the system audits.
- If message archiving is configured, back-up the message archives.
- Use the system audits or message archives to detect a breach of security.
- Recover the system after abnormal failure.

49. There are no non-privileged users or direct users of the TOE. All human interaction with the TOE is by authorised administrators. User guidance is therefore not applicable to the TOE.

50. Note that all channels for a particular TOE installation are pre-configured into the product (and verified) prior to handover (delivery). Channels may only be re-configured by Clearswift-trained installation staff.

Strength of Function

51. The SoF claim for the TOE is identified above under the heading "Strength of Function Claims".

52. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE.

Vulnerability Analysis

53. The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. No known vulnerabilities were identified in the construction of the TOE or from the public domain sources, with the exception of one potential vulnerability relating to Ethernet network interface cards which is discussed below under "Platform Issues"

Platform Issues

54. To demonstrate that the TOE would execute on any single Sun SPARC Workstation supported by Trusted Solaris 8 4/01, the Sponsor supplied a Multi-Platform Rationale that examined the impact of platform variations by:

- Identifying the variations in the currently-supported platforms for Trusted Solaris 8 4/01 (eg processor type, processor speed, number of processors & amount of memory)
- Analysing the security and assurance impact on the TOE of the platform variations (in particular, by relating the platform variations to the testing performed)

55. The evaluators assessed this Multi-Platform Rationale and performed equivalent analysis in respect of their additional evaluation activities.

56. CS Bastion II runs on Trusted Solaris 8 4/01 and the TOE development representations were found to exhibit no variations in respect of the underlying hardware platform options. The Developer and Evaluators did not have the extent of visibility of the Sun-proprietary information that would be available for an EAL4 evaluation of Trusted Solaris 8 4/01. However, the CS Bastion II analysis drew upon publicly available Trusted Solaris 8 4/01 information, including the Sun website http://wwws.sun.com/software/solaris/trustedsolaris/index.html, the Certification Report [h] and the Security Target, together with the Trusted Solaris 8 4/01 guidance documentation. Factors considered included the following:

- All CS Bastion II communication with the hardware platform is via Trusted Solaris 8 4/01 programming interfaces;
- Trusted Solaris 8 4/01 security functions are implemented in distinct (kernel or privileged user space) processes from any low level platform-dependent code;
- The platform processor types (listed in Annex A) implement the same processor architecture and instruction set;
- Memory and I/O addressing schemes are independent of memory size.

57. It should be noted that the CS Bastion II test configuration did not incorporate a full suite of resource-intensive vetting software. However, in line with the recommendations of the Trusted Solaris 8 4/01 Certification Report [h], it is recommended that the TOE be run on hardware with the recommended minimum memory sizes specified in Annex B.

58. Product testing, including details of the test configurations, is summarised in Annex C. The full set of Developer's tests produced identical results on each of 3 different hardware platforms. The Evaluators repeated a subset of these tests on a differently configured hardware platform and produced identical results to those of the Developer. The Developer and Evaluators tests therefore supported the Multi-Platform Rationale summarised above.

59. Subsequent to penetration testing, a potential vulnerability was identified relating to network interface cards. This takes effect where the method of padding Ethernet frames results in leakage of sensitive data (e.g. if frame buffer data from a message to one subscriber is re-used to pad a message to another subscriber). The significance of such a vulnerability is dependent on the method of use of the TOE and the threat environment in which it is deployed, which may in turn relate to the vetting software loaded into its compartments. Consumers who have such concerns are advised to contact the CERT Coordination Center website (http://www.kb.cert.org/vuls/id/JPLA-5BGNYP) to confirm that a particular Sun network interface card and driver does not exhibit this vulnerability. At the time of certification of CS Bastion II, those network interface cards and drivers investigated and acknowledged by Sun Microsystems to be free of this vulnerability are listed in the table below.

Network Interface Card	Network Interface Card
ce(7D) - Cassini Gigabit-Ethernet	iprb(7D) - Intel 82557, 82558, 82559-controlled Ethernet
dmfe(7D) - Davicom Fast Ethernet	pcelx(7D) - 3COM EtherLink III PCMCIA Ethernet
eri(7D) - eri Fast-Ethernet	qfe(7D) - Quad Fast-Ethernet
ge(7D) - GEM Gigabit-Ethernet	

Sun Network Interface Cards Confirmed by Sun to be Free of Potential Vulnerability

Rationale for Security-Irrelevant Subsystems

60. The Evaluators confirmed that the vetting and proxy subsystems were identified as security irrelevant (i.e. neither security critical nor security supporting) for the TOE since they did not contribute towards any Security Function and did not support any component that implements a Security Function. (The rationale is dependent on subsystem separation, which is discussed further under the heading "Design Subsystems" in Annex B.)

61. The following requirements detail how an alternative vetting and proxy subsystem can be installed and run on the TOE without affecting any Security Functions and thus maintain their non-security supporting status. The information is provided to potential consumers who wish to ensure that the certification of the TOE is not invalidated by the use of such an alternative subsystem.

62. The key requirements that must be met by any vetting and proxy subsystem to maintain its non-security supporting status are as follows:

a. The subsystem must be packaged such that all the software can be installed and configured pre-delivery, by Clearswift or equivalently trained staff, using standard SYSGEN mechanisms and procedures, as documented in the Installation Guide [l].

b. It must be possible to install and run the subsystem without alteration to the evaluated TMS, ARCHIVE and RUNCTL subsystems of the TOE.

c. The subsystem must run with no Trusted Solaris 8 4/01 privileges other than `net_privaddr` (if required) to allow access to one of the reserved network ports.

d. The procedures covered in any subsystem-specific guidance documentation do not compromise or contradict any of the procedures defined in the TOE Administration Guide [n], covering the administration of the security critical modules of the TOE.

e. The procedures covered in any subsystem-specific guidance documentation do not compromise or contradict any of the TOE Environmental Assumptions described in the Security Target [a].

III. EVALUATION OUTCOME

Certification Result

63. After due consideration of the ETR [j, k], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that CS Bastion II meets the CC Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified CC Part 2 extended functionality, in the specified environment, when running on Trusted Solaris 8 4/01 and the Sun Workstations specified in Annex A.

Recommendations

64. Prospective consumers of CS Bastion II should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a].

65. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target [a].

66. The TOE should be delivered, installed, configured and used in accordance with the guidance documentation [l - n] included in the evaluated configuration.

67. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under “TOE Scope” and “Evaluation Findings”.

68. The Certification Body recommends that any evaluated or assurance-maintained security patches to Trusted Solaris 8 4/01 are applied to future versions of the TOE if they are relevant to the TOE’s security functionality or counter vulnerabilities relevant to the TOE’s configuration.

69. Further recommendations, relating to the secure receipt, installation, configuration and operation of the TOE, are provided above under the headings of “TOE Scope” and “Evaluation Findings”.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

CS Bastion Version 2.0.0, otherwise known as CS Bastion II.

2. The TOE is available on CD-ROM or floppy disk labelled as “Clearswift Bastion II Master” containing the TOE software, together with a CD-ROM labelled “Clearswift Bastion II Packages” containing the requested untrusted optional proxy and DMZ software packages. Currently, there are 3 optional Clearswift Bastion II Packages CD-ROMs, one for each of the SMTP, X.400 and DISP proxies. These are additionally labelled “SMTP”, “X.400” and “Directory Bastion” respectively. If requested, the TOE is also supplied pre-installed and pre-packaged.

3. The TOE includes the following software:

- csblaunch Version 1.02.01
- csbarchtidy Version 1.02.00

TOE Documentation

4. The guidance documents evaluated were:

- Clearswift Bastion 2 Installation Guide [l]
- Clearswift Bastion 2 Release Notice [m]
- Clearswift Bastion 2 Administration Guide [n]

5. The documentation is included on the CS Bastion II CD-ROMs. Further discussion of the guidance documents is provided above under the heading “Installation and Guidance Documentation”.

TOE Configuration

6. The TOE should be configured in accordance with the guidance documents identified in paragraph 4 above.

Environmental Configuration

7. The TOE’s operational environment includes:

- Sun Trusted Solaris 8 4/01, in its evaluated configuration (except in respect of the hardware platforms as specified in [l, m])
- Any single Sun SPARC Workstation that runs Sun Trusted Solaris 8 4/01
- Interfaces to the 2 subscriber networks mediated by CS Bastion II
- Interfaces to between zero and 8 extended DMZ networks (up to 4 per channel)
- Specific Sun-tested network interface cards (see paragraph 59)

8. The table below provides details of the specific Sun SPARC Workstations that form part of the evaluated configuration of CS Bastion II. The rationale for these additional platforms is summarised under the heading “Platform Issues”.

9. Annex C provides details of the 3 hardware platforms used for the Developer tests and the single platform used for the Evaluator tests, together with the specific network interface cards tested. Annex C also provides details of the test configurations used by the Developer and Evaluators.

10. Further details of the hardware requirements are provided in Annex B under the heading “Hardware and Firmware Dependencies”.

Sun Workstation	**Sun Workstation**	**Sun Workstation**	**Sun Workstation**
SPARCclassic	SPARCstation LX	SPARCstation 4	SPARCstation 5
SPARCstation 5 Model 170	SPARCstation 10	SPARCstation 10SX	SPARCstation 20
SPARCstation 20 Model HS11, HS12, HS14, HS21, HS22, 151 and 152	Ultra 1 Model 140, 170	Ultra 1 Creator Model 140E, 170E, 200E	Ultra 1 Creator3D Model 140E, 170E, 200E
Sun Enterprise 1 Model 140, 170, 170E	Ultra 2 Creator Model 1170, 2170, 1200, 2200, 1300, 2300	Ultra 2 Creator3D Model 1170, 2170, 1200, 2200	Ultra 5
Ultra 10	Ultra 30	Ultra 60	Ultra 80
Ultra 450	Sun Enterprise 2 Model 1170, 2170, 1200, 2200, 1300, 2300	Sun Enterprise 150	Sun Enterprise 220R
Sun Enterprise 250	Sun Enterprise 420R	Sun Enterprise 450	Sun Enterprise 3000
Sun Enterprise 4000	Sun Enterprise 5000	Sun Enterprise 6000	Sun Enterprise 3500
Sun Enterprise 4500	Sun Enterprise 5500	Sun Enterprise 6500	Sun Enterprise 10000
SPARCserver 1000 and 1000E	SPARCcenter 2000 and 2000E	Sun Blade 100	Sun Blade 1000
Sun Fire 280R	Sun Fire 880	Sun Fire 6800	Sun Fire 4810
Sun Fire 4800	Sun Fire 3800		

Sun SPARC Workstations Supported by Trusted Solaris 8 4/01 and CS Bastion II

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the product's main architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

2. CS Bastion II, running on the Trusted Solaris 8 4/01 UNIX-based operating system and any single Sun SPARC Workstation with 2 subscriber network interfaces, provides an application-level messaging firewall for use between 2 incompatible or mutually-mistrusting subscriber networks.

3. CS Bastion II provides an architectural framework into which a variety of proxy and DMZ functions can be pre-configured to create a range of different firewall services. Trusted Solaris 8 4/01 provides a Compartmented Mode Workstation (CMW) environment that is used by CS Bastion II to provide the assured separation between the subscriber networks and between the specified independent DMZ vetting functions.

4. The architectural framework is thus a set of compartments that protect each specified proxy and DMZ function from potential interference. The design permits security-irrelevant proxy and DMZ subsystems to be managed/re-configured without compromising CS Bastion II Security Functions. (See associated subsystem requirements under the heading "Rationale for Security-Irrelevant Subsystems".)

5. CS Bastion II configures and uses many Trusted Solaris 8 4/01 features, including the Trusted Solaris 8 4/01 authentication and auditing functions to provide detailed accountability of system activity.

6. The security features associated with each CS Bastion II Security Function are summarised below.

Domain Separation

7. The TOE is able to configure 2 PROXY compartments, between zero and 10 inclusive DMZ compartments, each disjoint with respect to each other, and one Trusted Messaging Subsystem (TMS) compartment which strictly dominates all other CS Bastion II compartments.

8. A subsystem in a PROXY or DMZ compartment therefore executes in a domain protected from interference by any software running in any other PROXY or DMZ compartment.

9. The TMS executes in a domain, the TMS compartment, protected from interference by any software running in any other compartment.

Network Separation

10. Each of the networks that are physically attached to the TOE is connected to a compartment that is not connected to any other network. Each subscriber network is connected to a different PROXY compartment.

Assured Message Handling

11. The transfer of messages between compartments, and thus across the TOE, is managed by the TMS. This subsystem is the only additional product component, over and above Trusted Solaris 8 4/01, that has sufficient privileges to move data between compartments.

12. Subsystems executing in other compartments are configured to have their sensitivity label set equal to that of the compartment in which they are executing.

13. The sensitivity label of a message is initially set to that of the PROXY compartment in which the message is first received, and relabeled by the TMS when moved between compartments, to that of the compartment to which it is moved.

Assured Message Channels

14. The TMS (including its configuration files) guarantees that there shall be no more than one channel for **successful** message flow through the DMZ (and thus across the TOE) in each direction.

15. A channel is defined by the number and order of PROXY and DMZ compartments that each message will be forced to pass through by the TMS. The TOE may be configured to block all **successful** message flow in one direction.

16. The TMS gives each vetting compartment in an assured message channel the opportunity to check and/or reject every message. The TMS moves messages from a queue of type OUT in one compartment to a queue of type IN in the next compartment. TMS moves messages from a queue of type RETURN to the PROXY compartment in the same channel from which they originated. Only the subsystem executing in a PROXY or DMZ compartment is enabled to move messages from the compartment's IN queue to the compartment's OUT, RETURN or REJECT queue.

Message Archives

17. If configured during installation, all messages entering the DMZ of the TOE shall be archived. A copy of every message shall be saved to an archiving spool directory.

System Auditing

18. The TOE records in the Trusted Solaris 8 4/01 audit trail the TOE-specific events detailed in the Security Target [a]. The TOE, via the SYSGEN Subsystem, also preconfigures the Trusted Solaris 8 4/01 audit system to record the Trusted Solaris 8 4/01-specific events detailed in the TOE's Security Target.

Administration Access Control

19. Two TOE-specific administration roles are configured and used, one for administering the trusted and untrusted components of the TOE (**tms**) and one for the untrusted proxy and vetting software only (**cots**). At least one Trusted Solaris 8 4/01 administration user account is configured, with access to both **tms** and **cots** roles. It is required that these roles are not modified and that all administrative accounts are managed in strict accordance with the procedures specified in the TOE documentation, as detailed in Annex A.

20. Access to all TOE administration accounts, and thus the product, is protected by passwords generated by the Trusted Solaris 8 4/01 password generator.

Design Subsystems

21. The TOE consists of the following security critical and security supporting subsystems:

- TMS
- RUNCTRL
- ARCHIVE
- SYSGEN

22. The TMS controls the flow of all data between TOE compartments.

23. The RUNCTRL Subsystem ensures that all TOE subsystems run correctly within the bounds of their compartment. It executes the csblaunch command which ensures that the csbrun script in each compartment runs at the correct sensitivity label and checks the compartment status. The csblaunch command is used by the administrator to co-ordinate the launch of all subsystems within TOE compartments. It is used to start and stop all TOE subsystems and to check their runtime status.

24. The ARCHIVE Subsystem, if configured, is protected in its own CMW compartment and takes a copy of all data entering a channel to a separate partition of disk.

25. The SYSGEN Subsystem supports the TOE Security Functions (TSF) by ensuring the correct configuration of CS Bastion II and Trusted Solaris 8 4/01 at TOE installation time as part of a semi-automatic procedure. (See “Installation and Guidance Documentation”.) SYSGEN installs Trusted Solaris 8 4/01 using a jumpstart mechanism that includes specific security hardening of the operating system. It also sets up the auditing and label encoding files.

26. Security-irrelevant subsystems are separated from the security-critical and security-supporting subsystems (ie TMS, RUNCTRL, ARCHIVE and SYSGEN) by the use of Trusted Solaris 8 4/01 domain separation. Trusted Solaris 8 4/01 domain separation depends on the correct configuration of Trusted Solaris 8 4/01 itself and correct installation of all software. It is thus supported by the SYSGEN Subsystem that guarantees the freshly installed state of the TOE is a secure state (with sensitivity labels and privileges correctly applied where required).

Hardware and Firmware Dependencies

27. CS Bastion II requires a single Sun SPARC Workstation supported by Trusted Solaris 8 4/01. The supported workstations are detailed in Annex A under the heading "Environmental Configuration" and are characterised by the processor attributes detailed in the table below.

Processor Attribute	Range
Type	UltraSPARC II, UltraSPARC IIe, UltraSPARC IIi 440, UltraSPARC IIi 650, UltraSPARC III
Speed	360MHz to 1050MHz

Processor Requirements

28. The specification of platforms capable of supporting the TOE is further constrained by the following minimum system requirements: 20GB disk space, 256MB memory, 17-inch monitor, mouse, keyboard, integral CD-ROM drive and 2 Ethernet interfaces (provided by either Sun Quad or Sun single-port Ethernet cards). The TOE also permits platforms with optional floppy and SCSI tape drives, together with up to 8 extended DMZ interfaces.

29. The hardware was relied upon to provide general supporting protection mechanisms, including processor states and memory management, and the system real time clock. The Evaluator's results confirmed that these mechanisms, which were controlled by Trusted Solaris 8 4/01 software components, operated correctly in both single and dual processor configurations.

30. The TOE has no firmware components, although the firmware in the TOE platform is protected by an EEPROM password to reduce the risk of tampering during delivery and operation. There were no other firmware dependencies that affected the evaluation.

31. Further discussion of the supported platforms is provided under the heading "Platform Issues" in the "Evaluation Findings" chapter.

TSF Interface

32. The following external TSF Interface (TSFI) is identified for the TOE:

- IF_CDE
- IF_SUSER
- IF_NETSUB
- IF_NETDMZ
- IF_TSOL

33. The IF_CDE interface is an administrator interface. It gives access to the **tms** and **cots** roles and thus provides administrative control over the TOE.

34. The IF_SUSER interface is an administrator interface. It is used during the TOE installation process.

35. The IF_NETSUB interface is a network interface. It provides a PROXY subsystem with access to a subscriber network for the acceptance and delivery of subscriber data (e.g. email).

36. The IF_NETDMZ interface is a network interface. It provides a DMZ subsystem access to its own private, protected DMZ network, to gain access to additional resources or to extend functionality.

37. The IF_TSOL interface is an operating system interface. It is used by the TOE to gain access to Trusted Solaris 8 4/01 provided services such as Mandatory Access Control, process management, privilege management, file management and Trusted Solaris 8 4/01 auditing.

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The Developer's Test Plan included 69 tests covering all SFRs, all TOE subsystems and the TSFI (as detailed in Annex B). It included tests to check the installation and configuration of the TOE, the administrative functions, the interfaces between subsystems and modules, 2 types of proxy (SMTP and X.400) and the platform variations, including network interface card types.

2. The Developer's testing used 3 different Sun SPARC Workstations specifically configured to address the platform variations, as indicated in the table below. The full set of tests was run twice on each platform, once with the TOE configured with the SMTP proxies and once with the TOE configured with the X.400 proxies. The tests covered 8 different channel configurations, including zero and 5 DMZ (message-archiving or vetting) compartments per channel and the disablement options. Identical results were obtained on each platform and satisfactorily demonstrated the correct operation of the TOE in all platform variation conditions.

Platform	Processor	Memory	Disc Size	Network Interface Card
Sun Blade 100 OpenBoot Version 4.3	UltraSPARC IIe Single 500MHz	256MB	18GB	One X1034A Sun Quad FastEthernet PCI Adapter card
Sun Ultra 5/10 UPA/PCI OpenBoot Version 3.25	UltraSPARC IIi Single 400MHz	128MB	18GB	Two X1033A Sun FastEthernet PCI Adapter cards
Sun Fire 280R OpenBoot Version 4.2	UltraSPARC III Dual 750MHz	4096MB	2 x 32GB	One X1034A Sun Quad FastEthernet PCI Adapter card

3. The Evaluator's testing used a Sun SPARC workstation configured as indicated in the table below. The Evaluators witnessed the installation and configuration of the TOE and confirmed that the test configuration was consistent with that specified in the Security Target [a]. The Evaluators repeated a sample of 19 developer tests, which included at least one developer test for each SFR, giving a 28% sample. The tests included a TOE configuration with 5 DMZ compartments in one traffic flow direction and no DMZ compartments in the other. The results were identical to those produced by the Developer.

Platform	Processor	Memory	Disc Size	Network Interface Card
Sun Blade 100 OpenBoot Version 4.3	UltraSPARC IIe Single 500MHz	512MB	18GB and 20GB	X1034A Sun Quad FastEthernet PCI Adapter and X1032A SunSwift 10/100BaseT Fast/Wide UltraSCSI PCI Adapter

4. The Evaluators devised a further set of 7 independent functional tests and test data to independently test each of the Security Functions. No anomalies were found. The Evaluators also devised a set of 17 penetration tests to address potential vulnerabilities considered during the course of the evaluation. No vulnerabilities were detected.

5. Penetration tests that scanned for vulnerabilities used the following tools:

- Nessus 1.2.0
- Internet Security Systems Internet Scanner, Release 6.21.2001.320

6. Further evidence of the correct operation of the TOE's platform (ie Trusted Solaris 8 4/01 on specified Sun SPARC Workstations) is reported in [h].

Test Configurations

7. Details of the Sun SPARC Workstations used in the developer and evaluator tests are provided above under the heading "IT Product Testing".

8. The Developer's test configuration was a standalone system that included the TOE platform (one of 3 examples, interchanged as required, with both proxies enabled in turn) situated between 2 representative subscriber networks. Each subscriber network included one host computer handling test messages and test tools. Each host computer could therefore examine incoming and outgoing test messages in either traffic flow direction. This test configuration facilitated the testing of not only the TOE, but also the correct operation of the SMTP and X.400 proxies (which were not included in the Security Functions). The test configuration with 10 DMZ compartments was modified to test network connectivity and separation by connecting a shared network to 2 proxy and 2 vetting compartments. The tests were repeated with different pairs of compartments to check all extended DMZ connections.

9. The Evaluators used 3 test configurations. The first test configuration used a host computer connected to the TOE but with proxies disabled. The host computer could be connected directly to each of the 2 proxy and 8 DMZ vetting compartments (using a crossover cable). Test messages were generated on the host computer and could be injected directly from the host to any compartment of the TOE. The test configuration allowed a TOE with all 10 DMZ compartments to be tested.

10. The second test configuration was equivalent to the developer's test configuration and enabled a host computer connected to each subscriber network to send and receive test messages across the TOE platform.

11. The third test configuration enabled a host computer on a private network to be connected to a DMZ vetting compartment (ie an extended DMZ network), to perform vulnerability tests against the TOE. This facilitated checks for potential weaknesses in the installation and configuration of a DMZ private network.

12. The Evaluator's host computer in each test configuration was a laptop that included the vulnerability test tools detailed at paragraph 5 above.

The test configurations excluded the ROSE (for DISP) proxy and its associated protocol conformance verification function, the extended DMZ option (other than DMZ network interface separation) and any platform with more than dual processor options. The test configurations also excluded configurations that were composed of multiple copies of CS Bastion II.