CS Bastion II V2.2
Security Target (EAL4)

Author:	Andrea Gilbert (owner)
Approved By:	See Document Registry
Status:	Approved
Issue:	DN11272/7
Date:	13/9/06

Table of Contents

1. Introduction

1.1 ST Identification

Title: CS Bastion II V2.2 Security Target (EAL4).

TOE Version: CS Bastion Version 2.2.0 (marketed as *CS Bastion II V2.2* or *Bastion 2.2*; also referred to in this Security Target as *Clearswift Bastion V2.2* (CSB2.2)).

Keywords: Firewall, proxy firewall, application-level firewall, bastion, X.400, SMTP, ROSE, DISP, FTP, Trusted Solaris, TSOL, Compartmented Mode Workstation (CMW), MAC.

This document is the security target for the Common Criteria [CC] EAL4 evaluation of the Clearswift Bastion V2.2 product and is conformant with the CC.

1.2 ST Overview

This Security Target (ST) specifies the environment, security objectives, security requirements and security functions for the CC EAL4 evaluation of the Clearswift Bastion V2.2 product.

Clearswift Bastion V2.2 (CSB2.2) is an application-level firewall designed for use between incompatible or mutually mistrusting networks. Its primary goal is to provide assured network separation, while permitting limited authorized message transfer. That is, an assurance that network traffic cannot be accidentally or deliberately leaked between (subscriber) networks via CSB2.2 outside of the pre-defined and tightly controlled message channels provided by the CSB2.2 software.

CSB2.2 also offers a protected DMZ into which additional software modules can be installed to police the traffic flow between networks. One DMZ module is the CSB2.2 archive utility, which will take a backup copy of all data passing through the firewall to a protected section of disc.

CSB2.2 currently supports X.400 and SMTP protocols by making use of commercial-of-the-shelf networking proxies, adapted to suit the bastion architecture, it also offers a variety of optional software modules to police and manage message flow within the DMZ. The CSB2.2 architecture allows for alternative networking proxies and DMZ modules to be developed and introduced at a later date without compromising product security.

CSB2.2 runs on Trusted Solaris 8 4/01, 12/02, 7/03 or 2/04 (TSOL) and makes use of many TSOL security features.

For more information see the TOE description in section 2.

1.3 CC Conformance

This Security Target is CC Part 2 extended, Part 3 conformant, with a claimed evaluation assurance level of EAL4. It is extended because it contains explicitly stated security functional requirement components.

No conformance with any Protection Profile is claimed.

1.4 Re-Evaluation

A previous version of Bastion was evaluated to ITSEC E3. This Security Target has been produced for a re-evaluation to Common Criteria EAL4. As such it has re-used the wording of the ITSEC assumptions, threats etc. but has given them acronyms rather than simple numbering.

The Certification report for the previous evaluation also made some comments about the ITSEC SEF5. In order to address these comments the wording of this SEF has been incorporated with ITSEC SEF 4 into AMC.

The change of evaluation criteria between ITSEC and Common Criteria means that the difference between the TOE and the TOE environment must be more clearly defined. This has resulted in some parts of the ITSEC SEFs being mapped into the TOE environment.

The following table provides a mapping between assumptions, threats, SEFs, etc. used in the ITSEC Security Target and those used in this Security Target.

ITSEC	Common Criteria
MOU ASSUMPTION 1	A.CSB_DELIVERY
MOU ASSUMPTION 2	A.CSB_INSTALLATION
MOU ASSUMPTION 3	A.CSB_ADMIN
E1	A.CSB_PROTECTION
E2	A.CSB_PHYSICAL_ACCESS
E3	Become part of A.CSB_SOFTWARE
E4	A.CSB_ADMIN_ACCESS
E5	A.CSB_SOFTWARE
E6	A.CSB_ROLES
T1	T.CSB_OSBYPASS
T2	T.CSB_OVERRUN
T3	T.CSB_DMZBYPASS
T4	T.CSB_LEARN
T5	T.CSB_ABUSE
T6	T.CSB_DIRECT
T7	T.CSB_SPOOF
SEF1	DOM_SEP Reworded)
SEF2	NET_SEP (Reworded)
SEF3	AMH (Reworded)
SEF4	AMC (Reworded)
SEF5	Has become part of AMC
SEF6	ARCH
SEF7	AUD (Reworded)
SEF8	AC (Reworded)

1.5 Definitions

This section contains definitions of the technical terms that will be used within this document.

The definition of the following terms can be found in the [TSOL] and are not repeated here: Trusted Process, Mandatory Access Control (MAC), Sensitivity Label, Privilege, Authorisation, Role.

ARCHIVE compartment A type of DMZ compartment that contains the CSB2.2 trusted archive function.

Bastion Proxy: General term for any bastion subsystem responsible for handling data traffic to/from a subscriber network. MTA and Sendmail are example Bastion Proxies.

Channel *A sequence of CSB2.2 compartments comprising, in strict order, the incoming PROXY compartment, zero or one ARCHIVE compartment, between zero and four (inclusive) VET compartments and the outgoing PROXY compartment. Two channels will usually be defined, one for each direction of flow of messages through CSB2.2, with the incoming PROXY compartment for one channel being the outgoing PROXY compartment for the other channel.*

Compartment: A distinct area of information in a system, implemented by use of sensitivity labels.

Compartmented Mode Workstation (CMW):
A trusted workstation that contains enough built-in security to be able to function as a trusted computer. A CMW is trusted to keep data of different security levels and categories in separate compartments.

cots role A CSB2.2 configured, TSOL managed, untrusted role which can reconfigure or administer only CSB2.2 ‘untrusted’ subsystems in PROXY and VET compartments.

CSB2.2 compartment: A CMW disjoint compartment used by the CSB2.2.

CSB2.2 operation The execution of an instance of CSB2.2 (see Section 2.4). The tms role may enable and disable the operation of CSB2.2 by starting CSB2.2, starting CSB2.2 such that it automatically restarts when TSOL is rebooted (auto-restart) and stopping CSB2.2 such that auto-restart is switched off.

Disjoint Compartments: Two compartments that are incomparable in terms of their sensitivity labels (neither compartment dominates the other). Access to one compartment does not imply any access to the other.

DISP: Directory Information Shadowing Protocol defined in ITU-T Recommendation X.525 (2001) | ISO/IEC 9594-9: 2001, *Information technology – Open Systems Interconnection – The Directory: Replication.*

DMZ: De-militarised Zone.

DMZ compartment: A protected CSB2.2 compartment reserved for running the CSB2.2 trusted archive function or additional software to police (eg. sanction or filter) data flow between subscriber networks.

DMZ network: A private, protected network, connected to a DMZ compartment to support DMZ services.

Extended DMZ: A DMZ compartment with network access to a DMZ network.

Firewall: Firewalls are security components used in conjunction with other security hardware and software to provide actively managed channels between networks with differing security policies. Communications are allowed only through specific pre-configured channels. This communication is generally audited and tightly controlled.

Message: Unit of subscriber data flow within Bastion. Typically refers to an X.400 or SMTP email message, but may also refer to any unit of data produced or consumed by a Bastion Proxy.

Message Transfer Agent (MTA):
A process that collects and delivers messages for mail users, mail-enabled applications and gateways. Usually used in reference to X.400 (P1) messages, for which the term was originally defined.

PROXY compartment A CSB2.2 compartment, which is connected to one of the subscriber networks.

ROSE: ITU-T Recommendation X.881 (1994) | ISO/IEC 13712-2:1995, *Information technology – Remote Operations: OSI realizations – Remote Operations Service Element (ROSE) service definition*.

Sendmail: A commonly used SMTP-based MTA.

Simple Mail Transfer Protocol (SMTP): An Internet standard for delivering text based messages across the Internet.

Subscriber network: A network connected to one CSB2.2 PROXY compartment, which sends or receives subscriber messages to/from CSB2.2 such that the messages transverse and are checked by the CSB2.2 software before receipt, or after sending, by the other subscriber network connected to the other CSB2.2 PROXY compartment.

System All of the hardware and software that comprises CSB2.2 running on TSOL on a supported platform.

The CSB2.2 DMZ: The group of all CSB2.2 DMZ compartments and their networks.

TMS Trusted Messaging Subsystem; the trusted software executing in the TMS compartment that is responsible for managing the flow of messages between a pair of CSB2.2 compartments within a channel.

TMS compartment The trusted CSB2.2 compartment that strictly dominates all other CSB2.2 compartments.

tms role A CSB2.2 configured, TSOL managed, trusted role that provides for authorised access to TMS to permit start/stop of CSB2.2 operation, enabling/disabling message flow through a channel and enabling/disabling software in a DMZ compartment.

TSOL: Trusted Solaris 8 4/01, 12/02, 7/03 or 2/04 in its evaluated configuration (as specified in [IG] and [RN]).

VET compartment A type of DMZ compartment that contains additional software to police (eg. sanction or filter) data flow between subscriber networks.

X.400: The messaging protocol defined by ISO (International Organisation for Standardisation) and ITU-T as part of the OSI model (Open Systems Interconnection).

1.6 References

[CC] Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, Version 2.1, August 1999:

Part 1 Introduction and general model, CCIMB-99-031
Part 2 Security functional requirements, CCIMB-99-032
Part 3 Security assurance requirements, CCIMB-99-033

[AG] Clearswift Bastion II Version 2.2 Administration Guide, DN11527/1

[IG] Clearswift Bastion II Version 2.2 Installation Guide, DN11526/1

[RN] Clearswift Bastion II Release 2.2.0 Release Notice, DN11528/1

[TSOL] Trusted Solaris 8 4/01 Security Target, LogicaCMG, TS8_101, Issue 3.1, 12 November 2003.

[TSOL2/04] Trusted Solaris 8 2/04 Security Target, LogicaCMG, TS8_101, Issue 1.1, 20 February 2006.

2. TOE Description

2.1 Overview

Clearswift Bastion V2.2 (CSB2.2) is an application-level firewall designed for use between incompatible or mutually mistrusting subscriber networks. Its primary goal is to provide assured network separation, while permitting limited authorized message transfer. That is, an assurance that network traffic cannot be accidentally or deliberately leaked between networks via CSB2.2 outside of the pre-defined and tightly controlled message channels provided by the CSB2.2 software.

In addition to network separation, CSB2.2 provides a DMZ into which additional software can be installed to police traffic flow in each direction. The DMZ is protected from both networks, so that data can be processed securely and safely ‘in the clear’ if required. Separate DMZ channels are provided in each direction so that different checks can be performed in each direction, and if necessary blocked completely in one direction. Each DMZ channel supports up to five independent DMZ functions, each in its own protected environment (compartment). CSB2.2 guarantees that no DMZ compartment will be bypassed.

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 networks to a protected partition on disk.

CSB2.2 is effectively 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 or SMTP or ROSE (for DISP) proxies, and each has an optional DMZ module for verifying protocol conformance within the DMZ. However the architecture will also support many other store-and-forward style protocols, such as FTP or any protocol based on ROSE, like DISP, along with any number of specialized DMZ functions to meet specific customer requirements. Also with CSB2.2 it is now possible to give individual DMZ functions access to their own private network to create one or more ‘extended DMZs’ and meet a much wider range of applications.

The strength of CSB2.2 design, introduced in 2.2 below, is that the proxy and DMZ subsystems can be interchanged or upgraded without compromising CSB2.2 security functions.

Each CSB2.2 will support just one pair of proxies, so separate CSB2.2s are required to support multiple protocols between subscriber networks.

CSB2.2 runs on TSOL[1] and makes use of many TSOL security features, notably it uses TSOL authentication and auditing functions to provide detailed accountability of all system activity.

CSB2.2 is aimed primarily at connecting incompatible networks rather than hostile networks. If one or both of the networks is considered hostile then the use of a perimeter network and packet level filters is recommended to protect CSB2.2 from low level attacks such as denial-of-service.

2.2 Design Rationale

A CSB2.2 consists of several large and co-operating software sub-systems, and like most networking applications the networking sub-system represents a particularly large and complex component of the product which, due to its size, complexity and exposure to the network is particularly vulnerable to attack. Networking products are thus particularly difficult to assure at a security level. The CSB2.2 acknowledges this difficulty and assumes that the networking sub-system (proxy) is inherently untrustworthy. The primary aim of the design is thus to isolate the proxy sufficiently such that the correct operation of the proxy does not impact or threaten the security objectives. This separation also applies to DMZ subsystems, which means both DMZ and proxy subsystems can be classified as security irrelevant within the scope of

[1] Versions 4/01, 12/02, 7/03 or 2/04, as defined by Security Targets [TSOL] and [TSOL2/04]. Note all references to [TSOL] in this document apply equally to [TSOL2/04] since the relevant content is identical in both [TSOL] and [TSOL2/04].

the evaluation of CSB2.2 and can be interchanged, upgraded or enhanced with relative ease, and without compromising the security objectives. It is however noted that DMZ (and possibly proxy) subsystems may be separately assured outside of the context of the current evaluation of CSB2.2.

2.3 Summary of Security Features

The primary security features of the CSB2.2 can be summarized as follows:

- A non-bypassable application level firewall between two subscriber networks connected to, and separated by, the CSB2.2.
- Archiving of all traffic passing through the CSB2.2 (configurable)
- A protected DMZ for running additional software checks on all traffic flow.
- Separate channels to manage message flow in each direction.
- Administrator identification and authentication, along with system-auditing, provided by TSOL (evaluated to EAL4).

The TOE does not include TSOL which has been evaluated separately.

2.4 Evaluated Configuration

The target of the evaluation (TOE) is the CSB2.2 that consists of a pre-installed bundle of CSB2.2 specific software and configuration files executing on the following items of software and hardware, which form part of the TOE environment:

- Any single SUN SPARC Workstation that is supported by SUN Trusted Solaris 8 4/01, 12/02, 7/03 or 2/04
- Interfaces to the two subscriber networks mediated by CS Bastion II V2.2
- Interfaces to all required extended DMZ networks (up to 8 total, 4 in each direction of traffic flow)
- SUN Trusted Solaris 8 4/01, 12/02, 7/03 or 2/04, in its evaluated configuration (as specified in [IG] and [RN])
- Specific SUN-tested NICs.

The TOE includes several optional components that must be configured into the product during the initial installation phase to create up to two channels (one in each direction of message flow). Effectively this configuration process results in a number of different instances of the product which, as a group, form the TOE.

The TOE (with all options configured) comprises:

- two PROXY compartments - one either end of each channel (each shared by both channels)
- one ARCHIVE compartment and subsystem in each channel, next to the first PROXY compartment in the direction of subscriber message flow
- four VET compartments in each channel
- the Trusted Messaging Subsystem (TMS) running in the TMS compartment, which controls the flow of subscriber messages through the channels
- subsystem software running in the PROXY and VET compartments.

The configurable components that form an instance of the TOE are:

- the number of channels – one or two

- the VET compartments - zero to four in each channel
- the ARCHIVE compartments and subsystems - present or not present in each channel
- the type and configuration of subsystem software running in the PROXY and configured VET compartments.

It should be noted that the subsystem software running in all VET and PROXY compartments will be shown to be security-irrelevant in the context of this evaluation and will not require evaluation.

3 TOE Security Environment

3.1 Secure Usage Assumptions

A.CSB_DELIVERY:

The installation procedures (described in the [IG]) must be carried out by trained staff to install and configure the product prior to handover (delivery) to the customer. Installation may be performed either on customer site, or off-site at a central installation and distribution site. These procedures will be semi-automated and will:

- Ensure all network cards are correctly installed, with interfaces marked for each network.
- Ensure TSOL is correctly and fully installed, in its evaluated configuration (as specified in [IG] and [RN]).
- Configure one or two channels in accordance with customer requirements.
- Ensure the core CSB2.2 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 TSOL generated passwords.
- Securely define and configure all network families (IP-address groups tied to a compartment).

[Note 1] These procedures will take input from a CSB2.2 customer order form (completed by the Customer with help from Sales/Support at or around the point of order).

[Note 2] If CSB2.2 is not installed on site then physical delivery of CSB2.2 to customer site must be accompanied by a trusted person, either a member the installation team, or by the customer. This is to ensure CSB2.2 does not get tampered with during delivery.

A.CSB_INSTALLATION:

The start-up procedures (described in [RN]) must be followed to complete the CSB2.2 installation into its target environment. These procedures will explain how to:

- Switch on and perform initial boot of product.
- Use TSOL to generate new passwords for each administration account.
- Physically attach the networks to the CSB2.2 and verify the connections are correct.
- Complete a phased start-up of all software and verify each component is functioning correctly.

A.CSB_ADMIN:

The system operation and administration procedures (described in the [AG]) must be followed during normal day-to-day operation. These procedures will 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 changes)
- disable/enable the software running in one of the DMZ compartments (if this need arises)
- 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
- stop/start the system during normal operation
- recover the system after abnormal failure.

3.2 Assumptions concerning the TOE Environment

This section indicates the remaining personnel, physical and procedural measures required to maintain the security of the CSB2.2 product. Note that the TSOL environmental assumptions, except A.PROTECT, A.BRIDGES&ROUTERS and A.NIS_DOMAINS, (as listed in [TSOL] Section 3.4) also apply and are not repeated here.

A.CSB_PROTECTION The system running the CSB2.2 must be kept in a physically secure environment that meets or exceeds the environmental security requirements of all attached networks.

A.CSB_PHYSICAL_ACCESS Physical access to the system should be restricted to the nominated personnel who require access for core administration purposes.

A.CSB_ADMIN_ACCESS Administrator access to the system will be restricted to direct local access or, if applicable, remote access from within the DMZ network.

A.CSB_SOFTWARE All non-essential software packages will be removed from the system. No 'firewall-irrelevant' applications will be installed or run on the CSB2.2.

A.CSB_ROLES The CSB2.2 administration roles defined during installation will not be added to or modified in any way and all administration accounts will be managed in strict accordance with the procedures laid down in the CSB2.2 documentation.

A.CSB_NON_HOSTILE CSB2.2 is primarily aimed at non-hostile subscriber networks. If one or both of the subscriber networks is considered hostile then the use of a perimeter network and packet level filters is required to protect CSB2.2 from low level attacks such as denial-of-service.

3.3 Threats

The assumed threats for the Clearswift Bastion V2.2 are as follows. Note that the TSOL threats, except T.TRANSIT, (as listed in [TSOL] Section 3.2) also apply, to the TOE environment only, and are not repeated here. The applicable TSOL threats are a complete refinement of CSB2.2 threat T.CSB_ABUSE.

T.CSB_OSBYPASS: A network-based attacker attempts to establish an independent network connection at the hardware or OS level that bypasses the CSB2.2 software.

T.CSB_OVERRUN: A network-based attacker overruns one or both of the bastion proxies and then attempts direct communication between proxies thus bypassing the entire DMZ.

T.CSB_DMZBYPASS: A local or network-based attacker attempts to modify or overrun the CSB2.2 mechanisms that control a DMZ channel, thus allowing one or more DMZ functions to be bypassed.

T.CSB_LEARN: Local or network-based attack attempts go undetected allowing an attacker to slowly learn the weaknesses of the product and, through a trial-and-error process, eventually defeat the security objectives.

T.CSB_ABUSE: A locally based attack by an unauthorised user to the system, or abuse of trust/privilege by an authorised user.

T.CSB_DIRECT: A deliberate or accidental attempt by a network user to send data in the wrong direction across the CSB2.2 when the CSB2.2 is configured to support message flow in one direction only.

T.CSB_SPOOF: An IP ‘spoofing’ attack, where a network user on one network attempts to make a connection to the proxy running in the wrong (i.e. opposing) networking compartment by using a source IP address of a host based on the opposing network.

4 Security Objectives

4.1 Security objectives for the TOE

The CSB2.2 security objectives are as follows:

O.CSB_NO_BYPASS The TOE must provide a gateway between two networks that guarantees that no network traffic flowing between the two networks (via the CSB2.2) can bypass the CSB2.2 software.

O.CSB_CHECKS The TOE must provide a means of applying additional security checks on all messages moving between the two networks.

O.CSB_BLOCK If configured to block message flow in one direction, the TOE must guarantee that traffic cannot flow in the direction being blocked.

O.CSB_ARCHIVE If configured, the TOE must provide a means of archiving all messages moved between the two networks.

O.CSB_AUDIT The TOE must record changes in state of CSB2.2 software and ensure that a minimum set of security-critical TSOL events is recorded.

O.CSB_ROLE The TOE must provide separate roles to administer the trusted core components and the CSB2.2 ‘untrusted’ subsystems.

4.2 Security Objectives for the environment

The security objectives for the environment include:

- those that are specific to CSB2.2, required to cover the CSB2.2 secure usage and environment assumptions defined in Sections 3.1 and 3.2
- those that are TSOL TOE objectives, required to partially counter CSB2.2 threats
- those that are TSOL objectives for the environment, required to partially counter CSB2.2 threats.

Applicable TSOL objectives are listed in this section, but not described. Please refer to [TSOL] Sections 4.1 and 4.2 for their description.

The following security objectives for the environment are specific to CSB2.2, required to cover the CSB2.2 secure usage and environment assumptions defined in Sections 3.1 and 3.2:

O.CSB_DELIVERY

The installation procedures (described in [IG]) must be carried out by trained staff to install and configure a basic CSB2.2 product prior to handover (delivery) to the customer. Installation may be performed either on customer site, or off-site at a central installation and distribution site. These procedures will be semi-automated and will:

- Ensure all network cards are correctly installed, with interfaces marked for each network.
- Ensure TSOL is correctly and fully installed, in its evaluated configuration (as specified in [IG] and [RN]).
- Configure one or two channels in accordance with customer requirements.
- Ensure the core CSB2.2 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 TSOL generated passwords.
- Securely define and configure all network families (IP-address groups tied to a compartment).

[Note 1] These procedures will take input from a CSB2.2 customer order form (completed by the Customer with help from Sales/Support at or around the point of order).

[Note 2] If CSB2.2 is not installed on site then physical delivery of CSB2.2 to customer site must be accompanied by a trusted person, either a member the installation team, or by the customer. This is to ensure CSB2.2 does not get tampered with during delivery.

O.CSB_INSTALLATION

The start-up procedures (described in [RN]) must be followed to complete the CSB2.2 installation into its target environment. These procedures will explain how to:

- Switch on and perform initial boot of product.
- Use TSOL to generate new passwords for each administration account.
- Physically attach the networks to the CSB2.2 and verify the connections are correct.
- Complete a phased start-up of all software and verify each component is functioning correctly.

O.CSB_ADMIN

The system operation and administration procedures (described in [AG]) must be followed during normal day-to-day operation. These procedures will 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 changes)
- disable/enable the software running in one of the DMZ compartments (if this need arises)
- disable/enable network access to those compartments that require it
- back-up the system audits and message archives (if configured)
- use the system audits or message archives to detect a breach of security
- stop/start the system during normal operation
- recover the system after abnormal failure.

O.CSB_PROTECTION CSB2.2 must be kept in a physically secure environment which meets or exceeds the environmental security requirements of all attached networks.

O.CSB_PHYSICAL_ACCESS Only nominated personnel who require access for core administration purposes shall be able to directly access CSB2.2.

O.CSB_ADMIN_ACCESS Administrator access to the CSB2.2 shall be restricted to direct local access or, if applicable, remote access from within a DMZ network.

O.CSB_SOFTWARE All non-essential software packages shall be removed from the system. No ‘firewall-irrelevant’ applications will be installed or run on the CSB2.2.

O.CSB_ROLES The CSB2.2 administration roles defined during installation shall not be added to or modified in any way and all administration accounts shall be managed in strict accordance with the procedures laid down in the CSB2.2 documentation.

O.CSB_NON_HOSTILE CSB2.2 is primarily aimed at non-hostile subscriber networks. If one or both of the subscriber networks is considered hostile then use shall be made of a perimeter network and packet level filters to protect CSB2.2 from low level attacks such as denial-of-service.

Applicable TSOL TOE objectives are:

- O.AUTHORISATION
- O.DAC
- O.MAC
- O.AUDIT
- O.RESIDUAL_INFO
- O.MANAGE
- O.ENFORCEMENT
- O.DUTY
- O.HIERARCHICAL
- O.ROLE.

Applicable TSOL objectives for the environment are:

- O.ADMIN
- O.ACCOUNTABLE
- O.AUDITDATA
- O.AUTHDATA
- O.BOOT
- O.CLEARANCE
- O.CONNECT
- O.INSTALL
- O.INFO_PROTECT
- O.LABELS
- O.MAINTENANCE
- O.RECOVER
- O.SOFTWARE_IN
- O.SENSITIVITY.

5 IT Security Requirements

5.1 TOE Security Requirements

All CSB2.2 configuration options that have an impact on the TOE security functions are included in the SFRs specified in this section. Options are configured before and/or after handover of CSB2.2 to the customer, as clarified in footnotes. Specification of the tms role covers only those options that may be configured after handover to the customer.

TOE Security Functional Requirements

Message archiving (FAU_GEN.3)

The TOE Security Functions (TSF) shall, if configured[2], archive a copy of all messages entering the DMZ. FAU_GEN.3.1

Hierarchical to: No other components.

Dependencies: No dependencies.

<u>Note:</u> This component is explicitly stated, i.e. it is not taken from [CC] Part 2.

Audit data generation (FAU_GEN.4)

The TSF shall generate an audit record for changes in state of CSB2.2 software. FAU_GEN.4.1

The TSF shall configure[3] TSOL to generate an audit record of the following auditable events: FAU_GEN.4.2

- all authentication and identification events
- all failed attempts to access an object
- all failed attempts to create a subject (i.e. process)
- all changes to the configuration of user accounts
- all failed attempts to change a security attribute (i.e. message sensitivity label)
- all events affecting the operation of system auditing
- all system shutdown/start-up events.

For each audit record generated by the TSF, the TSF shall record within each audit record at least the following information: FAU_GEN.4.3

- date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps.

<u>Note:</u> This component is explicitly stated, i.e. it is not taken from [CC] Part 2.

Subset information flow control (FDP_IFC.1)

[2] The trusted archive function is installed in each ARCHIVE compartment and, if requested on the Customer Order Form, enabled during installation before handover to the customer. The tms role may subsequently disable/enable the archive function.

[3] TSOL audit events are configured once during installation before handover to the customer.

The TSF shall enforce the Bastion Message Flow Control Policy on: FDP_IFC.1.1

- Subjects: TMS
- Information: a message being passed from one subscriber network to the other subscriber network through a channel, or being returned to the originating subscriber network
- Operations: the transfer of a message from a PROXY or DMZ compartment in a channel to the next such compartment in the sequence configured for that channel, or to the originating PROXY compartment.

Simple security attributes (FDP_IFF.1)

The TSF shall enforce the Bastion Message Flow Control Policy based on the following types of subject and information security attributes: FDP_IFF.1.1

- Subject security attributes:
    - the TMS sensitivity label and privileges
    - the configuration of the channel
- Information security attributes:
    - the sensitivity labels of the message before and after it is moved by TMS
    - the message queue type from which and to which TMS moves the message.

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: FDP_IFF.1.2

- TMS shall be permitted to move a message from a message queue of type OUT in any PROXY or DMZ compartment of a given channel to a message queue of type IN in the next compartment of the same channel
- TMS shall be permitted to move a message from a message queue of type RETURN in a VET compartment of a given channel to a message queue of type RETURN in the originating PROXY compartment of the same channel.

The TSF shall enforce no additional information flow control rules. FDP_IFF.1.3

The TSF shall provide[4] the following: FDP_IFF.1.4

- two PROXY compartments and between zero and two inclusive ARCHIVE compartments and between zero and eight inclusive VET compartments, each disjoint with respect to each other, and one TMS compartment which strictly dominates all other CSB2.2 compartments
- assignment of each of the two subscriber network interfaces to a separate PROXY compartment
- for one or each direction of message flow between the two subscriber networks, a single channel, configured in accordance with a strict ordering of compartments in the direction of message flow, from the incoming PROXY compartment through zero or one ARCHIVE compartment and between zero and four (inclusive) VET compartments to the outgoing PROXY compartment

[4] The CSB2.2 compartments, assignment of each subscriber network interface to a separate PROXY compartment and sequence of compartments in the channels are defined once, as requested on the Customer Order Form, during installation before handover to the customer. After delivery to the customer, the tms role may block message flow in one channel. The tms role may also disable the archive function in an ARCHIVE compartment and/or software running in a VET compartment, whilst maintaining message flow through the channel.

- when moving a message, TMS shall change the sensitivity label of the message to that of the compartment to which it is moved.

The TSF shall explicitly authorise an information flow based on the following rules: none. FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: FDP_IFF.1.6

- TMS shall not move a message through a channel for which message flow has been blocked.

Management of security functions behaviour (FMT_MOF.1)

The TSF shall restrict the ability to enable and disable the functions listed below to tms role: FMT_MOF.1.1

- operation of CSB2.2
- operation of the archive function in an ARCHIVE compartment
- operation of the software in a VET compartment
- message flow in a channel.

Security roles (FMT_SMR.4)

The TSF shall configure[5] the roles: FMT_SMR.4.1

- tms, a CSB2.2 configured, TSOL managed, trusted role that provides for authorised access to TMS to permit start/stop of CSB2.2 operation, enabling/disabling message flow through a channel and enabling/disabling software in a DMZ compartment
- cots, a CSB2.2 configured, TSOL managed, untrusted role which can reconfigure or administer only CSB2.2 'untrusted' subsystems in PROXY and VET compartments.

The TSF shall be able to configure an association between users and roles. FMT_SMR.4.2

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

Note: **This component is explicitly stated, i.e. it is not taken from [CC] Part 2.**

Strength of Function

The minimum strength of function claimed for CSB2.2 is *SOF-medium*.

TOE Security Assurance Requirements

The TOE shall meet the assurance requirements of [CC] Part 3 EAL4 with no augmentation or extension.

5.2 Security Requirements for the IT environment

In order to operate in a secure manner CSB2.2 relies on TSOL to provide some protection. This section identifies the TSOL SFRs upon which CSB2.2 depends.

CSB2.2 depends on all of the TSOL SFRs identified in [TSOL] Section 5.1.

[5] The two CSB2.2 specific roles, tms and cots, are configured to give appropriate access to CSB2.2 compartments before handover to the customer. A single CSB2.2 user, csbuser, is configured with access to CSB2.2 specific roles and groups. After handover to the customer, additional CSB2.2 users can be defined. CSB2.2 roles and their association with CSB2.2 users are maintained by TSOL.

6 TOE Summary Specification

6.1 TOE Security Functions

DOM_SEP: Domain Separation

The CSB2.2 product shall configure two PROXY compartments and between one and ten inclusive DMZ compartments, each disjoint with respect to each other, and one TMS compartment which strictly dominates all other CSB2.2 compartments.

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.

The Trusted Messaging Subsystem (TMS) executes in a domain, the TMS compartment, protected from interference by any software running in any other compartment.

Note: The protection from interference between different compartments is enforced by the security objective for the environment, O.MAC.

NET_SEP: Network Separation

Each of the networks that are physically attached to the CSB2.2 shall be connected to a compartment that is not connected to any other network. Each subscriber network shall be connected to a different PROXY compartment.

To illustrate, imagine two networks (INNERNET and OUTERNET) and two compartments (INSIDE and OUTSIDE). All call attempts from remote hosts on INNERNET shall be associated with and handled by compartment INSIDE. All call attempts from remote hosts on OUTERNET shall be associated with and handled by compartment OUTSIDE.

Note: The protection from interference between different compartments, and hence between connected networks, is enforced by the security objective for the environment, O.MAC.

AMH: Assured message handling

The transfer of messages between compartments, and thus across the CSB2.2, shall be managed by TMS executing in the TMS compartment. This sub-system shall be the only additional product component, over and above TSOL, that has sufficient privileges to move data between compartments.

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

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 it is moved to.

AMC: Assured message channels

The TMS (including its configuration files) that controls the movement of messages between compartments shall guarantee that there shall be no more than one channel for **successful** message flow through the DMZ (and thus across the CSB2.2) in each direction.

A channel is defined by the number and order of PROXY and DMZ compartments that each message will be forced to pass through by TMS. All channels for a particular CSB2.2 installation shall be pre-configured into the product (and verified) prior to handover (delivery). The CSB2.2 product may be configured after delivery to the customer to block all **successful** message flow in one direction.

TMS, that controls the movement of messages between compartments, shall give each VET compartment in an assured message channel the opportunity to check and/or reject every message. TMS moves messages from a queue of type OUT in one compartment to a queue of type IN in the next compartment. Only the subsystem executing in a DMZ compartment is enabled to move messages from the compartment's IN queue to the compartment's OUT, RETURN or REJECT queue. Messages moved into the OUT queue are enabled to continue through the channel. Messages moved into the RETURN queue are returned to the initial PROXY compartment in the channel (i.e. the PROXY compartment they originated from). Messages moved into the REJECT queue are terminated in the compartment. Messages moved into a RETURN or REJECT queue result in **unsuccessful** message flow.

ARCH: Message archives

If configured during installation, all messages entering the DMZ of the CSB2.2 shall be archived. A copy of every message shall be saved to an archiving spool directory.

AUD: System Auditing

The CSB2.2 product shall record in the TSOL system audit trail at least the date, time, type of event, subject identity, and the outcome (success or failure) for the following CSB2.2 specific events:

- start-up of CSB2.2 software
- shutdown of CSB2.2 software
- change of CSB2.2 software state to UP
- change of CSB2.2 software state to DOWN
- change of CSB2.2 software state to UPALWAYS.

The CSB2.2 product shall configure the TSOL audit system to always record the following TSOL events (defined in TSOL documents referenced in [AG]):

- audit administration
- administrative
- other administration
- system-wide administration
- login or logout
- change system state
- CSB2.2 events
- file creation (failure only)
- file deletion (failure only)
- file attribute modification (failure only)
- network access (failure only)
- process modification (failure only)
- non-attributable events (not attributable to a user).

AC: Administration Access Control

Two CSB2.2 administration roles shall be configured and used, one for administering the trusted and untrusted components of the CSB2.2 (tms) and one for the untrusted components only (cots). At least one CSB2.2 administration user account shall be configured, with access to both tms and cots roles.

The tms role shall be able to perform the following actions, described in [AG] under 'Administering Clearswift Bastion V2.2':

- change the run state of CSB2.2 (i.e. start, start and switch on auto-start, stop and switch off auto-start)
- disable/enable the software running in a VET compartment
- disable/enable the archive function
- disable/enable message flow in one direction.

Note: Identification and authentication of users is enforced by the security objective for the environment, O.AUTHORISATION. The capability to define roles and role attributes is enforced by the security objectives for the environment, O.DUTY and O.ROLE. The limitation of roles to access and manage subsystems in specific compartments is enforced by the security objectives for the environment, O.DAC and O.MAC.

Note: Access to all CSB2.2 administration accounts, and thus the product, shall be protected by a password which is generated by the TSOL password generator.

6.2 Assurance Measures

This section describes how the assurance requirements will be met.

- **Measures Used to Meet Component: ACM_AUT.1**

  This requirement will be met by documentation describing the Configuration Management system used during the development of the TOE.

- **Measures Used to Meet Component: ACM_CAP.4**

  This requirement will be met by documentation describing the Configuration Management system used during the development of the TOE.

- **Measures Used to Meet Component: ACM_SCP.2**

  This requirement will be met by documentation describing the Configuration Management system used during the development of the TOE.

- **Measures Used to Meet Component: ADO_DEL.2**

  This requirement will be met by documentation describing the Trusted delivery of the TOE.

- **Measures Used to Meet Component: ADO_IGS.1**

  This requirement will be met by documentation describing the Installation, Generation and Start-up of the TOE.

- **Measures Used to Meet Component: ADV_FSP.2**

  This requirement will be met by the Functional Specification for the TOE supported by the Security Target and Administration documentation.

- **Measures Used to Meet Component: ADV_HLD.2**

  This requirement will be met by the high level design for the TOE supported by the Security Target and Functional Specification.

- **Measures Used to Meet Component: ADV_IMP.1**

  This requirement will be met by the low-level design for the TOE supported by the Security Target and the source code.

- **Measures Used to Meet Component: ADV_LLD.1**

  This requirement will be met by the high and low level designs for the TOE supported by the Security Target and the functional specification.

- **Measures Used to Meet Component: ADV_RCR.1**

  This requirement will be met by the high and low level designs for the TOE supported by the Security Target, the functional specification and the correspondence between the levels of design representation.

- **Measures Used to Meet Component: ADV_SPM.1**

  This requirement will be met by the TOE Security Policy Model, which is implied by the SFRs specified in the Security Target, as permitted by Common Criteria Final Interpretation No. 069.

- **Measures Used to Meet Component: AGD_ADM.1**

  This requirement will be met by the Administration documentation supported by the Security Target, Functional Specification, high-level design, installation, guidance and start-up documentation, and the life-cycle definition documents.

- **Measures Used to Meet Component: AGD_USR.1**

  This assurance component will not be applicable to this evaluation as there are no direct users of the TOE but is included for completeness of the EAL4 assurance requirements.

- **Measures Used to Meet Component: ALC_DVS.1**

  This assurance requirement will be met by the Developer Security documentation.

- **Measures Used to Meet Component: ALC_LCD.1**

  This assurance requirement will be met by the lifecycle documentation.

- **Measures Used to Meet Component: ALC_TAT.1**

  This assurance requirement will be met by the development tools documentation and the source code.

- **Measures Used to Meet Component: ATE_COV.2**

  This assurance requirement will be met by the Security Target, Functional Specification, test documentation and test coverage analysis.

- **Measures Used to Meet Component: ATE_DPT.1**

  This assurance requirement will be met by the Security Target, Functional Specification, high-level design, test documentation and depth of testing analysis.

- **Measures Used to Meet Component: ATE_FUN.1**

  This assurance requirement will be met by the Security Target, Functional Specification, test documentation and procedures.

- **Measures Used to Meet Component: ATE_IND.2**

  This assurance requirement will be met by all the evaluation deliverables and a TOE suitable for testing.

- **Measures Used to Meet Component: AVA_MSU.2**

  This assurance requirement will be met by the Misuse Analysis supported by the other evaluation deliverables.

- **Measures Used to Meet Component: AVA_SOF.1**

  This assurance requirement will be met by Strength of Function Analysis and the other evaluation deliverables.

- **Measures Used to Meet Component: AVA_VLA.2**

  This assurance requirement will be met by Vulnerability Analysis, the other evaluation deliverables and a copy of the TOE suitable for testing.

7 Rationale

7.1 Security objectives rationale

This section provides a mapping between the security objectives and the threats and assumptions. It demonstrates that all the security objectives are required in order to cover the assumptions and counterthreats.

Assumption/Threat	**Security Objective**
A.CSB_DELIVERY	O CSB_DELIVERY
A.CSB_INSTALLATION	O.CSB_INSTALLATION
A.CSB_ADMIN	O.CSB_ADMIN
A.CSB_PROTECTION	O.CSB_PROTECTION
A.CSB_PHYSICAL_ACCESS	O.CSB_PHYSICAL_ACCESS
A.CSB_ADMIN_ACCESS	O.CSB_ADMIN_ACCESS
A.CSB_SOFTWARE	O.CSB_SOFTWARE
A.CSB_ROLES	O.CSB_ROLES
A.CSB_NON_HOSTILE	O.CSB_NON_HOSTILE
T.CSB_OSBYPASS	O.CSB_NO_BYPASS O.MAC O.ENFORCEMENT O.INFO_PROTECT
T.CSB_OVERRUN	O.CSB_NO_BYPASS O.MAC O.ENFORCEMENT O.INFO_PROTECT
T.CSB_DMZBYPASS	O.CSB_NO_BYPASS O.CSB_CHECKS O.CSB_ROLE O.AUTHORISATION O.DAC O.MAC O.ENFORCEMENT O.DUTY O.ROLE O.ADMIN O.ACCOUNTABLE O.INFO_PROTECT
T.CSB_LEARN	O.CSB_ARCHIVE O.CSB_AUDIT O.AUTHORISATION O.AUDIT O.MANAGE O.ENFORCEMENT O.ADMIN O.ACCOUNTABLE O.AUDITDATA
T.CSB_ABUSE	O.CSB_ROLE All TSOL TOE objectives listed in 4.2 All TSOL objectives for the environment listed in 4.2, except O.MAINTENANCE

Assumption/Threat	Security Objective
T.CSB_DIRECT	O.CSB_NO_BYPASS O.CSB_BLOCK O.MAC O.ENFORCEMENT O.INFO_PROTECT
T.CSB_SPOOF	O.CSB_NO_BYPASS O.MAC O.ENFORCEMENT O.INFO_PROTECT

The following demonstrates that all of the security objectives are required and suitable to cover the assumptions:

The coverage of A.CSB_DELIVERY by O.CSB_DELIVERY is self evident.

The coverage of A.CSB_INSTALLATION by O.CSB_INSTALLATION is self evident.

The coverage of A.CSB_ADMIN by O.CSB_ADMIN is self evident.

The coverage of A.CSB_PROTECTION by O.CSB_PROTECTION is self evident.

The coverage of A.CSB_PHYSICAL ACCESS by O.CSB_PHYSICAL ACCESS is self evident.

The coverage of A.CSB_ADMIN_ACCESS by O.CSB_ADMIN_ACCESS is self evident.

The coverage of A.CSB_SOFTWARE by O.CSB_SOFTWARE is self evident.

The coverage of A.CSB_ROLES by O.CSB_ROLES is self evident.

The coverage of A.CSB_NON_HOSTILE by O.CSB_ NON_HOSTILE is self evident.

Note that the TSOL environmental assumptions, (as listed in [TSOL] Section 3.4) also apply, except for A.PROTECT, A.BRIDGES&ROUTERS and A.NIS_DOMAINS. [TSOL] Section 7.2.3 demonstrates the suitability of TSOL security objectives for the environment to cover TSOL assumptions, which is not repeated here (note that O.MAINTENANCE is required to cover TSOL assumption A.ADMIN).

The following demonstrates that all of the security objectives are required and suitable to counter the threats:

T.CSB_OSBYPASS: A network based attacker attempts to establish an independent network connection at the hardware or OS level that bypasses the CSB2.2 software.

Security objective O.CSB_NO_BYPASS directly counters this threat by ensuring that the TOE is configured with a number of protected domains (compartments) which separate the networks and the CSB2.2 subsystems executing in each DMZ compartment. O.CSB_NO_BYPASS depends directly on security objective O.MAC provided by TSOL, which enforces separation between compartments. O.MAC is supported by security objectives O.ENFORCEMENT, which protects the integrity of TSOL, and O.INFO_PROTECT, which ensures that the correct settings for security attributes of security critical files required to implement O.CSB_NO_BYPASS are maintained.

T.CSB_OVERRUN: A network based attacker overruns one or both of the bastion proxies and then attempts direct communication between proxies thus bypassing the entire DMZ.

Security objective O.CSB_NO_BYPASS directly counters this threat by ensuring that the TOE is configured with a number of protected domains (compartments) which separate the networks and the CSB2.2 subsystems executing in each DMZ compartment. O.CSB_NO_BYPASS depends directly on security objective O.MAC provided by TSOL, which enforces separation between compartments. O.MAC is supported by security objectives O.ENFORCEMENT, which protects the integrity of TSOL, and

O.INFO_PROTECT, which ensures that the correct settings for security attributes of security critical files required to implement O.CSB_NO_BYPASS are maintained.

T.CSB_DMZBYPASS: A local or network-based attacker attempts to modify or overrun the CSB2.2 mechanisms that control a DMZ channel, thus allowing one or more DMZ functions to be bypassed.

Security objective O.CSB_CHECKS directly counters this threat by maintaining the correct configuration of compartments and message queues to ensure that there is only one channel in each direction of flow through CSB2.2 for successful message flow and that messages can only flow if action is taken by the CSB2.2 software enabled in each DMZ compartment.

Security objective O.CSB_NO_BYPASS also directly counters this threat by ensuring that the TOE is configured with a number of protected domains (compartments) which separate the networks and the CSB2.2 subsystems executing in each DMZ compartment. O.CSB_NO_BYPASS depends directly on security objective O.MAC provided by TSOL, which enforces separation between compartments. O.MAC is supported by security objective O.INFO_PROTECT, which ensures that the correct settings for security attributes of security critical files required to implement O.CSB_NO_BYPASS are maintained.

Security objective O.CSB_ROLE also directly counters this threat by ensuring that users who administer ‘untrusted’ subsystems in the DMZ are assigned to a role which cannot modify the configuration of compartments and message queues maintained by the trusted core components of CSB2.2. O.CSB_ROLE depends directly on O.DUTY and O.ROLE, which provide the capability to define roles and role attributes. The enforcement of separation between roles is provided by O.DAC and O.MAC, given appropriate settings of role attributes. O.CSB_ROLE also depends on O.AUTHORISATION, which enforces the identification and authentication of users. O.AUTHORISATION is supported by O.ACCOUNTABLE, which ensures CSB2.2 users are uniquely authorized, and by O.ADMIN, which ensures that user accounts and roles are appropriately managed.

All of the above are supported by O.ENFORCEMENT, which protects the integrity of TSOL.

T.CSB_LEARN: Local or network-based attack attempts go undetected allowing an attacker to slowly learn the weaknesses of the product and, through a trial-and-error process, eventually defeat the security objectives.

Security objective O.CSB_ARCHIVE directly counters the threat from network-based attackers by ensuring that, if configured, all messages entering the DMZ are archived.

Security objective O.CSB_AUDIT directly counters the threat by ensuring that changes in state of CSB2.2 software, and security-critical TSOL events, are always recorded in an audit trail.

Security objective O.AUDIT, provided by TSOL, directly counters this threat by ensuring security relevant events are recorded in an audit trail. The relevance of the other security objectives listed against this threat is demonstrated in [TSOL] Section 7.2.2 under P.ACCOUNTABLE.

T.CSB_ABUSE: A locally based attack by an unauthorised user to the system, or abuse of trust/privilege by an authorised user.

Security objective O.CSB_ROLE directly counters this threat by limiting the access of ‘untrusted’ subsystem administrators.

Note that the TSOL threats, except T.TRANSIT, (as listed in [TSOL] Section 3.2) also apply, to the TOE environment only. The applicable TSOL threats are a complete refinement of CSB2.2 threat T.CSB_ABUSE, hence all of the TSOL security objectives which counter these TSOL threats are required to counter T.CSB_ABUSE. The suitability of these TSOL security objectives is demonstrated in [TSOL] Section 7.2.1 and is not repeated here.

T.CSB_DIRECT: A deliberate or accidental attempt by a network user to send data in the wrong direction across the CSB2.2 when the CSB2.2 is configured to support message flow in one direction only.

Security objective O.CSB_BLOCK directly counters this threat by ensuring that compartments and message queues are configured such that successful message flow cannot occur in the direction of flow through CSB2.2 that is to be blocked.

Security objective O.CSB_NO_BYPASS also directly counters this threat by ensuring that the TOE is configured with a number of protected domains (compartments) which separate the networks and the CSB2.2 subsystems executing in each DMZ compartment. O.CSB_NO_BYPASS depends directly on security objective O.MAC provided by TSOL, which enforces separation between compartments. O.MAC is supported by security objectives O.ENFORCEMENT, which protects the integrity of TSOL, and O.INFO_PROTECT, which ensures that the correct settings for security attributes of security critical files required to implement O.CSB_NO_BYPASS are maintained.

T.CSB_SPOOF: An IP ‘spoofing’ attack, where a network user on one network attempts to make a connection to the proxy running in the wrong (i.e. opposing) networking compartment by using a source IP address of a host based on the opposing network.

Security objective O.CSB_NO_BYPASS directly counters this threat by ensuring that the TOE is configured with a number of protected domains (compartments) which separate the networks and the CSB2.2 subsystems executing in each DMZ compartment. O.CSB_NO_BYPASS depends directly on security objective O.MAC provided by TSOL, which enforces separation between compartments. O.MAC is supported by security objectives O.ENFORCEMENT, which protects the integrity of TSOL, and O.INFO_PROTECT, which ensures that the correct settings for security attributes of security critical files required to implement O.CSB_NO_BYPASS are maintained.

7.2 Security Requirements rationale

The table below provides a mapping between security objectives for the TOE and TOE security functional requirements (SFRs).

TOE Security Objective	**TOE SFR**
O.CSB_NO_BYPASS	FDP_IFC.1 FDP_IFF.1
O.CSB_CHECKS	FDP_IFC.1 FDP_IFF.1 FMT_MOF.1
O.CSB_BLOCK	FDP_IFC.1 FDP_IFF.1 FMT_MOF.1
O.CSB_ARCHIVE	FAU_GEN.3 FMT_MOF.1
O.CSB_AUDIT	FAU_GEN.4
O.CSB_ROLE	FMT_SMR.4 FMT_MOF.1

The following demonstrates that all of the SFRs are required and suitable to meet the security objectives:

O.CSB_NO_BYPASS The TOE must provide a gateway between two networks that guarantees that no network traffic flowing between the two networks (via the CSB2.2) can bypass the CSB2.2 software.

SFRs FDP_IFC.1 and FDP_IFF.1 defines an information flow control policy, attributes and rules which meet security objective O.CSB_NO_BYPASS by ensuring that all messages received from a network traverse CSB2.2 through pre-defined channels which guarantee attention by the subsystem software in the configured DMZ compartments.

O.CSB_CHECKS The TOE must provide a means of applying additional security checks on all messages moving between the two networks.

SFRs FDP_IFC.1 and FDP_IFF.1 ensure that all messages moving through the pre-defined channels between networks are guaranteed attention by the CSB2.2 software, by implicitly requiring the DMZ subsystem software to move messages from the DMZ IN queue to the same DMZ OUT queue, thus ensuring the DMZ subsystem software can apply any required security checks. SFR FMT_MOF.1 permits the trusted tms role to disable or enable the software running in a specific DMZ (VET) compartment.

O.CSB_BLOCK If configured to block message flow in one direction, the TOE must guarantee that traffic cannot flow in the direction being blocked.

SFRs FDP_IFC.1 and FDP_IFF.1 include a rule which, if configured, blocks all successful message flow in the specified direction between networks. SFR FMT_MOF.1 permits the trusted tms role to disable or enable message flow in one direction.

O.CSB_ARCHIVE If configured, the TOE must provide a means of archiving all messages moved between the two networks.

SFR FAU_GEN.3 ensures that, if configured, all messages entering the DMZ are archived. SFR FMT_MOF.1 permits the trusted tms role to disable or enable the trusted archive function in a specific DMZ (ARCHIVE) compartment.

O.CSB_AUDIT The TOE must record changes in state of CSB2.2 software and ensure that a minimum set of security-critical TSOL events is recorded.

SFR FAU_GEN.4 ensures that all changes in state of CSB2.2 software, and all security-critical TSOL events, are recorded in an audit trail.

O.CSB_ROLE The TOE must provide separate roles to administer the trusted core components and the CSB2.2 ‘untrusted’ subsystems.

SFR FMT_SMR.4 provides the trusted administrator role, tms, and the ‘untrusted’ subsystems role, cots. These are assigned to authorized users as required during initial configuration of CSB2.2 and by the TSOL secadmin role during operation. SFR FMT_MOF.1 permits the trusted tms role to disable or enable the operation of CSB2.2 (i.e. starting CSB2.2, starting CSB2.2 such that it automatically restarts when TSOL is rebooted (auto-restart) and stopping CSB2.2 such that auto-restart is switched off).

Note that the security objectives for the IT environment are all TSOL TOE objectives, as listed in Section 4.2. Hence, the SFRs for the IT environment are not included in this document. Please refer to [TSOL] for a full specification of TSOL SFRs and justification that they are required and suitable to meet the TSOL TOE objectives.

The dependency of SFR FAU_GEN.4 on FPT_STM.1 is met by the TSOL TOE.

The dependency of FDP_IFF.1 on FMT_MSA.3 is unnecessary, since it is not possible to change the default or initial values of the Bastion Message Flow Control Policy security attributes after installation.

The dependency of SFR FMT_SMR.4 on SFR FIA_UID.1 is met by the TSOL TOE.

The SFR FAU_GEN.3 component is explicitly stated. It is an additional function that falls naturally within the [CC] Part 2 security audit class, security audit data generation family. It is necessary to explicitly state this component since, although it defines audit data generation in a similar way to FAU_GEN.1, there is no requirement for the TOE to generate audit data for start-up or shutdown of the audit functions, nor to record the specific information required by FAU_GEN.1 in an audit record. The requirement is, if configured, to archive all messages entering the DMZ. The audit requirements of FAU_GEN.1 are met by the TSOL TOE. FAU_GEN.3 is a simple, stand-alone, function that archives messages. It is hierarchical to no other component and has no dependencies. The EAL4 assurance requirements are fully applicable to FAU_GEN.3.

The SFR FAU_GEN.4 component is explicitly stated. It is an additional function that falls naturally within the [CC] Part 2 security audit class, security audit data generation family. It is necessary to explicitly state this component since, although it defines audit data generation in a similar way to FAU_GEN.1, there is no requirement for the TOE to generate audit data for start-up or shutdown of the audit functions, and some of the audit data generation defined is configured by the TOE, but generated by the IT environment (TSOL). The audit requirements of FAU_GEN.1 are met by the TSOL TOE. FAU_GEN.3 covers generation of CSB2.2 specific audit records and configuration of TSOL to always audit a minimum set of security-critical TSOL events. It is hierarchical to no other component and has one dependency (met by TSOL). The EAL4 assurance requirements are fully applicable to FAU_GEN.4.

The SFR FMT_SMR.4 component is explicitly stated. It is identical to the [CC] Part 2 SFR FMT_SMR.1, except that the required roles and association with users are configured, rather than maintained, by the TOE. The CSB2.2 roles and users are configured using the TSOL role and user capabilities and thereafter maintained by TSOL.

Apart from SFRs FAU_GEN.3 and FAU_GEN.4, the TOE SFRs comply with [CC] Part 2, with all required operations of assignment and selection performed to make the requirements TOE specific. The assignment and selection operations were performed using consistent computer security and TOE specific terminology. Hence the SFRs are internally consistent.

Where relevant, the TOE SFRs are mutually supportive, in accordance with their dependencies. SFR functional element FMT_SMR.4.1 defines the tms role, which provides for administration of the trusted core components of CSB2.2 in accordance with FMT_MOF.1, including appropriate reconfiguration – again, O.ADMIN applies, and it is required that any reconfiguration performed does not violate the security objectives of the TOE.

The claimed evaluation assurance level of EAL4 is justified by market requirements, and is appropriate for the type of threats, security objectives and environment claimed.

The claimed strength of function of SOF-Medium is also appropriate for the type of threats, security objectives and environment claimed.

7.3 TOE Summary specification rationale

The table below provides a mapping between TOE SFRs and the TOE Security Functions. This section shows that all the SFRs are met and that each SFR is required.

TOE Security Requirement	TOE Security Function
FAU_GEN.3	ARCH
FAU_GEN.4	AUD
FDP_IFC.1	DOM_SEP NET_SEP AMH AMC
FDP_IFF.1	DOM_SEP NET_SEP AMH AMC
FMT_MOF.1	AC
FMT_SMR.4	AC

FAU_GEN.3 requires that, if configured, a copy of all messages entering the DMZ is taken. ARCH ensures that this occurs.

FAU_GEN.4 requires that all changes in state of CSB2.2 software, and all security-critical TSOL events, are recorded in an audit trail. AUD ensures that this occurs.

FDP_IFC.1 requires that information flows through the TOE in accordance with the Bastion Message Flow Policy. DOM_SEP configures up to one channel in each direction of message flow through CSB2.2, comprising the appropriate number and order of PROXY and DMZ disjoint compartments, and a trusted TMS compartment to manage message flow. NET_SEP ensures that networks are connected to different compartments. AMH ensures that only the trusted messaging subsystem executing in the TMS compartment can move messages between compartments. AMC ensures that messages can only move through CSB2.2 via the defined channels, that messages must be actioned by software executing in each configured DMZ compartment, and that, if configured, successful message flow is blocked in the specified direction.

FDP_IFF.1 requires that information flows through the TOE in accordance with the Bastion Message Flow Policy security attributes and rules. DOM_SEP configures up to one channel in each direction of message flow through CSB2.2, comprising the appropriate number and order of PROXY and DMZ disjoint compartments, and a trusted TMS compartment to manage message flow. NET_SEP ensures that networks are connected to different compartments. AMH ensures that only the trusted messaging subsystem executing in the TMS compartment can move messages between compartments. AMC ensures that messages can only move through CSB2.2 via the defined channels, that messages must be actioned by software executing in each configured DMZ compartment, and that, if configured, successful message flow is blocked in the specified direction.

FMT_MOF.1 requires that the trusted tms role is permitted to enable and disable the operation of CSB2.2, the archive function, operation of software in a VET compartment and block message flow in one direction. AC defines the functions that the tms administrator role can perform.

FMT_SMR.4 requires tms and cots roles to be configured and associated with users. AC defines the allowable roles for the TOE, tms and cots, accessible by at least one user. Roles and users are maintained by TSOL.

The compliance of assurance measures with assurance requirements is demonstrated in Section 6.2.