Security Target for BorderWare Firewall Server 6.5

Reference: ST

January 2002

Version : 2.4

North America:
50 Burnhamthorpe Rd. W.
Suite 502
Mississauga
Ontario
Canada L5B 3C2

Europe:
1 The Harlequin Centre
Southall Lane
Southall
Middlesex
UB2 5NH U.K.

DOCUMENT AUTHORISATION

DOCUMENT TITLE	Security Target for BorderWare Firewall Server 6.5

Version	Date	Description
1.0	October 2000	Issue for evaluation.
1.1 Draft	February 2001	Update to change version number from V6.2. to V6.5
1.2 Draft	March 2001	Update to reflect naming of additional interfaces
1.3Draft	March 2001	Updated to remove Office Gateway option
1.3	March 2001	Released for Evaluation
1.4	April 2001	Address EORs 7 and 8 (removal of WWW as authenticated service, as Web Caching Proxy not included in this release)
1.5	April 2001	Updates to address Certifier comments
1.6	April 2001	Constrain proxies to support NetMeeting
1.7	June 2001	Include the assurance component AVA_VLA.3
1.8	August 2001	Remove the reference to Web Caching Proxy server.
1.9	August 2001	Modify references to Ping services.
2.0	October 2001	Explicitly identify that Proxy caching and SNMP servers are put of scope.
2.1	November 2001	Updated to add HTTP filters to scope.
2.2	November 2001	Minor format changes for HTTP filters text.
2.3	December 2001	Identify augmentation of AVA_VLA.3 in all instances.
2.4	January 2002	Correct function requirement headings.

Contents

1 INTRODUCTION TO THE SECURITY TARGET 7

1.1 Security Target Identification 7

1.2 Security Target Overview 7

1.3 CC Conformance Claim 7

2 TOE DESCRIPTION 8

2.1 Features 8

2.2 TOE Hardware Requirements 9

2.3 Scope of evaluation 11

2.4 Hardware and Software Requirements for Admin GUI 12

3 SECURITY ENVIRONMENT 13

3.1 Introduction 13

3.2 Threats 13

3.2.1 Threats countered by the TOE 13

3.2.2 Threats countered by the Operating Environment 14

3.3 Organisational Security Policies 14

3.4 Assumptions 14

4 SECURITY OBJECTIVES 15

4.1 TOE Security Objectives 15

4.1.1 IT Security Objectives 15

4.1.2 Non-IT Security Objectives 16

4.2 Environment Security Objectives 16

4.2.1 IT Security Objectives 16

4.2.2 Non-IT Security Objectives 16

5 IT SECURITY REQUIREMENTS 18

5.1 TOE Security Functional Requirements 18

5.1.1 Identification and Authentication 19

5.1.2 Security Management 20

5.1.3 Security Audit 21

5.1.4 Protection of the Trusted Security Functions 23

5.1.5 User Data Protection 24

5.2 TOE Security Assurance Requirements 28

5.3 Security Requirements for the IT Environment 30

5.4 Strength of Function Claim 30

6 TOE SUMMARY SPECIFICATION 31

6.1 TOE Security Functions 31

6.1.1 Identification and Authentication 31

6.1.2 Management and Security Attributes 31

6.1.3 Audit 32

6.1.4 Protection of TOE Security Functions 33
6.1.5 User Data Protection 34

6.2 Assurance Measures 38

6.3 Permutational IT Security Functions 38

7 PROTECTION PROFILES CLAIMS 39

8 RATIONALE 40

8.1 Introduction 40

8.2 Security Objectives for the TOE and Environment Rationale 40
8.2.1 T.EXT_CONN 41
8.2.2 T.INT_CONN 41
8.2.3 T.SOURCE 41
8.2.4 T.CONFIG 41
8.2.5 T.UNAUTH 41
8.2.6 T.OS_FAC 41
8.2.7 TE.VIOLATE 42
8.2.8 A.PHYSICAL 42
8.2.9 A.LIMIT 42

8.3 Security Requirements Rationale 42
8.3.1 Requirements are appropriate 42
8.3.2 Security Requirement dependencies are satisfied 46
8.3.3 Security Requirements are mutually supportive 47
8.3.4 ST complies with the referenced PPs 47
8.3.5 IT security functions satisfy SFRs 47
8.3.6 IT security functions mutually supportive 50
8.3.7 Strength of Function claims are appropriate 50
8.3.8 Assurance measures satisfy assurance requirements 50

FIGURE 2-1- OVERVIEW OF BFS 10

TABLE 2-1 HARDWARE REQUIREMENTS OF THE TOE 11
TABLE 6-1 - UNIDENTIFIED SERVICES PROVIDED BY PROXIES 36
TABLE 6-2 - UNIDENTIFIED SERVICES PROVIDED BY SERVERS 37
TABLE 6-3 – UNIDENTIFIED SERVICES PROVIDED BY CLIENTS 37
TABLE 6-4 – AUTHENTICATED SERVICES PROVIDED BY SERVERS 38
TABLE 8-1 OBJECTIVES RATIONALE 41
TABLE 8-2 MAPPING OF OBJECTIVES TO SFRS 43
TABLE 8-3 MAPPING OF SFR DEPENDENCIES 46
TABLE 8-4 MAPPING OF IT FUNCTIONS TO SFRS 49

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (aligned with ISO 15408)

GLOSSARY AND TERMS

AUX	Auxiliary/SSN Interface
DMZ	De-militarised Zone
DNS	Domain Name Server
FTP	File Transfer Protocol
GUI	Graphical User Interface
IP	Internet Protocol
IT	Information Technology
POP	Post Office Protocol
PP	Protection Profile
SFP	Security Function Policy
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSN	Secure Servers Network (see also AUX)
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
UDP	User Datagram Protocol
WWW	World Wide Web

1 Introduction to the Security Target

1.1 Security Target Identification

Title: Security Target for BorderWare Firewall Server 6.5

Assurance Level: EAL4, augmented with ALC_FLR.1 and AVA_VLA.3.

1.2 Security Target Overview

The BorderWare Firewall Server (BFS) is designed to combine robust security with the complete set of ancillary services necessary to implement an Internet connection or to provide secure Intranet connections. The Firewall Server is built on the S-CORE operating system. S-CORE is a hardened operating system that has been specifically designed by BorderWare Technologies Inc and is derived from BSD 4.4 Unix. S-CORE has all non essential functions removed and is further optimised for security and through-put.

The purpose-designed operating system provides a separate domain of execution for each critical subsystem and implements kernel-level packet filtering to compliment the application proxies and application servers. The proxies manage connections for all well-known TCP/IP applications, which the servers provide facilities such as DNS and mail relay. BFS provides dual Domain Name Servers, which together with Network Address Translation ensure complete separation between Internal and external networks. The mail relay service ensures protects e-mail servers by allowing mail dispatch and delivery without ever permitting a connection between the server and the untrusted network.

1.3 CC Conformance Claim

This TOE has been developed to conform to the functional components as defined in the Common Criteria version 2.1 [CC] part 2, with the assurance level of EAL4, augmented with ALC_FLR.1 and AVA_VLA.3 as identified in part 3 of [CC].

2 TOE Description

2.1 Features

The BFS is an application-level firewall. It mediates information flows between clients and servers located on internal and external networks governed by the BFS. The BFS employs proxies to screen information flows. Proxy servers on the BFS, for services such as FTP and Proxy Server HTTP requests (optional), require authentication at the BFS by client users before requests for such services can be authorised. Thus, only valid requests are relayed by the proxy server to the actual server on the internal network.

The BFS delivers three security layers:

- packet filtering;
- circuit level gateways; and
- application level gateways.

The packet filtering controls are performed at the operating system kernel level. By default, these security policy rules deny all inbound information flows. Only an authorised BFS administrator has the authority to change the security policy rules.

The BFS's underlying operating system does not permit any operating system user logins. All direct interaction with the BFS to perform configuration and administration tasks is performed on the firewall server console or using the Admin GUI on a client connected to the internal, protected network. The BFS administrator is the only user who is able to directly interact with the BFS. Interaction with the BFS is transparent to all other users.

The BFS administrator is able to perform basic configuration and administration of the BFS using the firewall server console, via the "Admin menu". Access to the console is to be physically protected and logically controlled through password protection. Full administration services are only provided through use of the Admin GUI at a client workstation. Use of the Admin GUI is protected by use of a password. A challenge/response Crypto Card authentication token (56 bit DES encryption) may be used, but this is beyond the scope of the evaluation.

The BFS supports up to six network cards, each of which is connected to a different network segment. Each network segment must be physically separate for the other segments. The minimal configuration is two network cards, in this configuration one network card is assigned the role of "internal" interface and will be connected to the internal network. The second card will be assigned the role of "external" interface and will be connected to the external network. In the majority of cases the internal network will be a corporate LAN and the external network will be the Internet, but other uses are possible.

If more that two network cards are used then additional cards will be assigned the role of SSN or Auxiliary (AUX) interfaces. The term SSN is used to describe the 3rd network card, any additional cards are described as AUX. Any number of additional cards up to a maximum of six cards in total is supported. The SSN and AUX interfaces are identical, they provide the functions of a de-militarised zone (DMZ). The different names are assigned for historical reasons. Prior versions of the BFS supported a maximum of three network interfaces; the 3rd interface way termed the SSN. This name has been retained for interface 3 for reasons of backwards compatibility; interfaces 4, 5 and 6 (if present) are named AUX1, AUX2 and AUX3. This document refers collectively to the SSN and AUX interfaces as SSN/AUX.

A connection from the network connected to the Internal interface to a network connected to the external interface or to any of the SSN/AUX interfaces is considered an outbound connection (connection from one network to a another network with a lower level of trust). Assuming the appropriate information flow is permitted, outbound connections provide a transparent service to the user on the originating network.

Connections in the reverse direction, from the external to any SSN/AUX interface , from the external to the internal interface or from any SSN/AUX to the internal interface are considered inbound connections. Inbound connections are generally outside the scope of this security target. Where permitted these connections are *not* transparent. Permitted connections must be mapped to pre-defined network address on the destination network. For connections from External to any SSN/AUX interface or to the internal interface, multiple destinations may be defined. This facility, know as Multiple Address Translation (MAT) requires that additional network addresses (aliases) are assigned to the external interface.

Connections between any two SSN/AUX interfaces are not permitted. Transparent address translation is performed for all outbound traffic. Requests for connections from a client on the internal network to a server on the external network or any SSN/AUX network are directed by the client to the server's actual IP address. If the BFS is configured correctly, as the only connection between the internal and external or SSN/AUX networks, then the appropriate proxy for the requested service will be activated by the BFS (subject to successfully passing any appropriate identification, authentication or access controls) to handle that request. The proxy will ensure that the apparent source address of that connection is set to that of the BFS's external or SSN/AUX interface before any IP datagrams are transmitted on the external network. Inbound address translation is not transparent. An external entity must direct all traffic to an address assigned to the BFS's external or SSN/AUX interface. Subject to successful identification and authentication this traffic can be relayed to an entity on the internal network. The address translation is augmented by the separate Domain Name Servers who ensure that internal addresses are never disclosed to an external entity by domain name lookup.

2.2 TOE Hardware Requirements

The TOE requires at least two network interfaces to function correctly and can support a maximum of six network interface cards, as shown in Figure 2-1. If the

TOE is running on a hardware platform with two network cards these are assigned the function of *internal* and *external* network interfaces. If optional additional network cards are installed, these cards are assigned the function of the SSN/AUX network interface (i.e. up to 4 SSN/AUX interfaces may be present). Information flows are *not* permitted between multiple SSN/AUX interfaces, but information flows may be established between each SSN/AUX interface and the internal and external interfaces. (see section6)

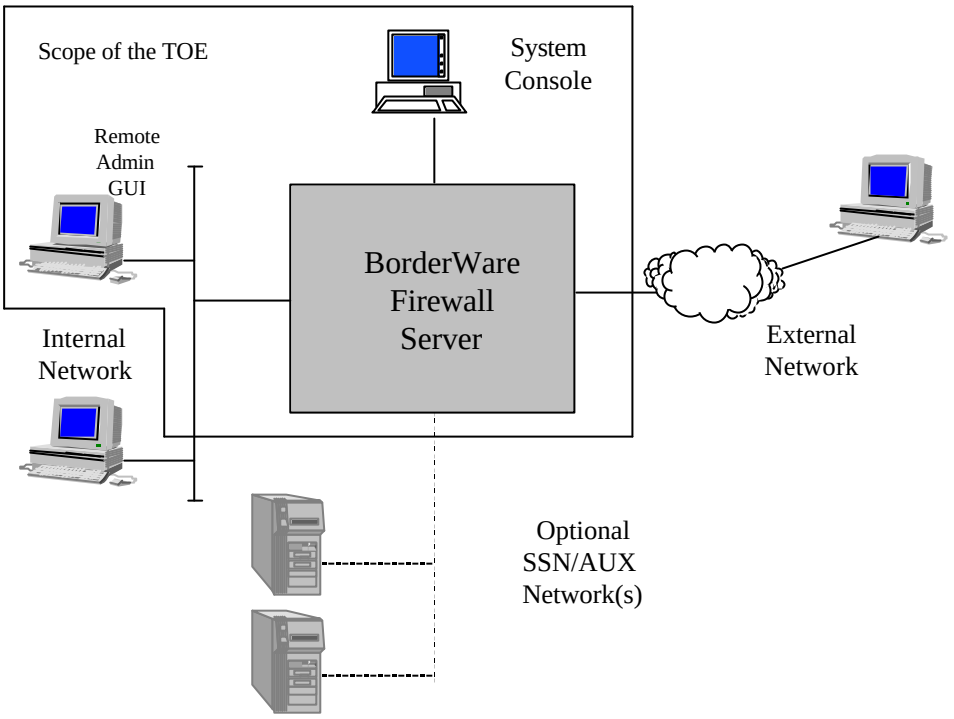

Figure 2-1- Overview of BFS

The following table identifies the hardware requirements for an installation of the BorderWare firewall server. For the purposes of this evaluation, equipment within the range of specifications stated in the following table were tested on Compaq, Dell, Intel and BorderWare (badged BSDi) hardware.

Hardware	CPU	Ram	Network Cards	Hard Disk(s)
Compaq Deskpro	400 MHz Celeron	64 Mbytes Memory	2 Ethernet Interfaces	6 Gbyte IDE Disk
Compaq Proliant	600 MHz PIII	128 Mbytes Memory	3 Ethernet Interfaces	9 Gbyte SCSI Disk
Dell Dimension	466 MHz Celeron	64 Mbytes Memory	3 Ethernet Interfaces	6 Gbyte IDE disk
Dell PowerEdge	500 MHz PIII	256 Mbytes Memory	6 Ethernet Interfaces	9 Gbyte SCSI Disk

Intel ISP 1100	600 MHz PIII	128 Mbytes Memory	2 Ethernet Interfaces	2 8 Gbyte IDE Disks
BorderWare R-2000 Security Server	700 MHz PIII	256 Mbytes RAM	3 Ethernet Interfaces	2 20 Gbyte IDE Disks

Table 2-1 Hardware Requirements of the TOE

With the exception of the Intel ISP 1100, each of the above hardware platforms include:

- CD-ROM drive;
- 3.5" diskette drive;
- monitor;
- keyboard.

The Intel ISP 1100 lacked a VGA card or attached monitor. To support hardware of this type (typically rack-mount systems) the TOE is able to divert the system console to the serial port. An attached laptop running a VT100 compatible terminal emulator was used for the system console on all testing on this hardware platform.

2.3 Scope of evaluation

The proxies included within the scope of evaluation of this product are identified in Section 6.1.5.

When recorded, the audit trail data is stamped with the date and time information. Audit events include:

- Every successful inbound and outbound connection;
- Every unsuccessful connection;
- Every successful and unsuccessful administrator authentication attempt.

If the audit trail becomes filled, then the trail will be archived and a new audit trail initialised. If the limit of archived audit trails is reached, the oldest archive will be deleted to allow the current audit trail to be archived. This mechanism ensures that partition on the TOE's disc reserved for audit information never becomes full, an event which could lead to loss of audit information.

The BorderWare product also provides the following functionality that is not within the scope of this evaluation:

- 3rd Party Authentication (e.g. Crypto Card for administration authentication at remote Admin GUI or Secure inbound FTP and Telnet proxies);
- Virtual Private Network (VPN);
- User Defined Proxies;
- URL Filtering (SmartFilter);
- Secure administration of the BFS from the external (unprotected) network;
- Web caching proxy;
- Point-to-point Tunnelling Protocol;
- SNMP Agent.

2.4 Hardware and Software Requirements for Admin GUI

The Admin GUI required for remote administration of the TOE is supplied as an application called BWClient. BWClient runs on any Win32 operating system (Windows NT, Windows 95, Windows 98 and Windows 2000). BWClient is a user level program and has no special hardware or software requirements, except that Win32 system must be equipped with a network connection and must have TCP/IP networking installed and configured. Certain early versions of windows were lacking certain network DLLs which are supplied as part of the Internet Explorer package and are required by BWClient. BWClient includes a "minimal impact" set of these DLLs and will install them (after prompting for confirmation) if it detects that these DLLs are not present. In addition it is recommended (but not mandatory) that NT systems should be patched to at least Service pack 3.

A copy of BWClient is included on the TOE distribution CD ROM. It is packaged as a standard Windows installation package and should be installed on any Win32 system meeting the requirements outlined above.

3 Security Environment

3.1 Introduction

This section provides the statement of the TOE security environment, which identifies and explains all:

- known and presumed threats countered by either the TOE or by the security environment;
- organisational security policies the TOE must comply with;
- assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

3.2 Threats

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

3.2.1 Threats countered by the TOE

The IT assets requiring protection are the services provided by, and data accessible via, hosts on the internal network.

The general threats to be countered are:

- attackers on the external network may gain inappropriate access to resources and data on the internal network;
- users on the internal network may inappropriately expose data or resources to the external network.

The following specific threats are countered:

T.EXT_CONN	An attacker on the external network may try to connect to services other than those expressly intended to be available in accordance with the security policy (e.g. an external user attempts to use unauthenticated FTP).
T.INT_CONN	An attacker on the internal network may try to connect to services other than those expressly intended to be available.
T.SOURCE	An attacker on the internal/external network may attempt to initiate a service from an unauthorised source.

T.CONFIG	An attacker on the internal/external network may exploit an insecure configuration (i.e. not in accordance with the chosen network security policy) of the firewall.
T.UNAUTH	Unauthorised changes to the configuration may be completed without being identified.
T.OS_FAC	An attacker on the internal/external network may attempt to use operating system facilities on the firewall server.

3.2.2 Threats countered by the Operating Environment

The following is a list of threats that must be countered by technical and/or non-technical measures in the IT environment, or must be accepted as potential security risks.

TE.VIOLATE	Violation of network security policy as a result of inaction, or action taken, by careless, wilfully negligent, or external system administrators.

3.3 Organisational Security Policies

There are no organisational security policies or rules with which the TOE must comply.

3.4 Assumptions

The following assumptions describe security aspects of the environment in which the TOE will be used or is intended to be used. This includes information about the intended usage of the TOE and the environment of use of the TOE.

A.PHYSICAL	The firewall will be physically protected to prevent hostile individuals engaging in theft, implantation of devices, or unauthorised alteration of the physical configuration of the firewall (e.g. bypassing the firewall altogether by connecting the internal and external networks together).
A.LIMIT	The firewall will limit the access to resources and data between an internal and external network.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

The principal IT security objective of this firewall is to reduce the vulnerabilities of an internal network exposed to an external network by limiting the hosts and services available. Additionally, the firewall has the objective of providing the ability to monitor established connections and attempted connections between the two networks.

The specific IT security objectives are as follows:

O.VALID	The firewall must limit the valid range of addresses expected on each of the internal and external networks (i.e. an external host cannot spoof an internal host).
O.HOSTILE	The firewall must limit the hosts and service ports that can be accessed from the external network.
O.PRIVATE	The firewall must limit the hosts and service ports that can be accessed from the internal network.
O.AUTH	The firewall must provide authentication of the end-user prior to establishing a through connection, in accordance with the security policy enforced on the BFS. (The policy is to ensure no services are allowed for inbound connections.)
O.ATTEMPT	The firewall must provide a facility for monitoring successful and unsuccessful attempts at connections between the networks.
O.ADMIN	The firewall must provide a secure method of administrative control of the firewall, ensuring that the authorised administrator, and only the authorised administrator, can exercise such control
O.SECPROC	The firewall must provide separate areas in which to process security functions and service requests. The processing of a security function must be completed prior to invocation of subsequent security functions.
O.CONFIG	The firewall is designed or configured solely to act as a firewall and does not provide any operating system user services (e.g. login shell) to any network users; only administrators have direct access. (The firewall does, however, provide application proxy authentication.)

4.1.2 Non-IT Security Objectives

There are no non-IT security objectives to be satisfied by the TOE.

4.2 Environment Security Objectives

4.2.1 IT Security Objectives

There are no IT environment security objectives to be provided by software outside the scope of the TOE.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

NOE.DELIV	Those responsible for the firewall must ensure that it is delivered, installed, managed and operated in a manner that maintains the security policy.
NOE.TRAIN	Those responsible for the firewall must train administrators to establish and maintain sound security policies and practices.
NOE.AUDIT	Administrators of the firewall must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Furthermore, appropriate archive action must be taken to ensure security logs archived by the firewall are no overwritten before they are inspected
NOE.NETWORK	The firewall must be configured as the only network connection between the internal network and the external network.
NOE.MANAGE	A firewall administrator is assigned with responsibility for day to day management and configuration of the firewall. Including the management of the audit trail.
NOE.PHYSICAL	The firewall must be physically protected so that only administrators have access. (The firewall must only be administered via the dedicated management port on the firewall or using the administration GUI on the internal network.)

NOE.REVIEW	The configuration of the firewall will be reviewed on a regular basis to ensure that the configuration continues to meet the organisation's security objectives in the face of: - changes to the firewall configuration; - changes in the security objectives; - changes in the threats presented by the external network; - changes in the hosts and services made available to the external network by the internal network.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

The functional security requirements for this Security Target are discussed in detail below. The following table summarises those security requirements.

Functional Components	
FIA_UID.1	Timing of Identification
FIA_UAU.1	Timing of Authentication
FIA_AFL.1	Authentication Failure Handling
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_SMR.1	Security Roles
FMT_MTD.1	Management of the TSF Data
FAU_GEN.1	Audit Data Generation
FAU_ARP.1	Security Alarms
FAU_SAA.1	Security Audit Analysis
FAU_SAR.1	Audit Review
FAU_STG.1	Protected Audit Trail Storage
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes

Table 5-1: Functional Requirements

5.1.1 Identification and Authentication

This section addresses the requirements for functions to establish and verify a claimed user identify. This includes identification of any actions that the TOE may complete on the user's behalf prior to identification or authentication.

The only type of user who can interact directly with the BFS interface (System Console or remote Admin GUI) is a BFS administrator. Therefore, BFS administrators are the only users who can log into the BFS interface (identify and authenticate themselves) and access the TSF data. As BFS administrators are able to access all TSF data, the identification and authentication mechanisms to the BFS interface provide a basic form of access control.

Unprivileged operators, use services provided by the TOE but do not visibly interact with the TOE. For the TOE to control requests for services by these unprivileged users the TOE performs basic identification of the request in the form of checking the source address of the request. However, this is dealt with by the rules in the UNIDENTIFIED and AUTHENTICATED information flow policies. The TOE requires the user to authenticate prior to interaction with some servers provided by BFS, these are specified in the AUTHENICATED information flow control policy.

A privileged operator, the FTP administrator user (FTP account "admin"), is able to access additional areas (e.g. where system accounting logs are stored) on the FTP server than an unprivileged FTP user, and has privileges to create, delete and modify directories on the server which are not available to an unprivileged FTP user. This account is referred to as "FTP Admin". These privileges are controlled by the BFS operating system. This account can only be accessed from a request generated on the internal network. It is assumed (as stated in the non-IT environment objective NOE.MANAGE) that this account is used by those performing the administration of the BFS, including the management of the audit trail.

FIA_UID.1	**Timing of identification**
FIA_UID.1.1	The TSF shall allow [information flows, compliant with the UNIDENTIFIED information flow FSP] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1 **Timing of authentication**

FIA_UAU.1.1 The TSF shall allow:

a) [information flows, compliant with the UNIDENTIFIED information flow FSP (information flow control decisions based on the information flow control outbound and inbound proxies, and service request policies to allow or deny traffic);

b) identification mechanisms defined in FIA_UID.1;

c) audit of failed authentication attempts,]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The "user" referred to in the SFRs above relates to both a BFS administrative user (administrator at the BFS console or using the Admin GUI on an internal client) and a service requested by an indirect user (including FTP Admin), which is associated with an individual IP address on the internal or external network.

FIA_AFL.1 **Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [1] unsuccessful authentication attempts occur related to [an authentication attempt originating from an individual IP address on the internal network or a BFS administrator].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [log the unsuccessful authentication attempt].

5.1.2 Security Management

This section defines requirements for the management of security attributes that are used to enforce the SFP.

FMT_SMR.1 **Security Roles**

FMT_SMR.1.1 The TSF shall maintain the roles [BFS administrator, FTP Admin].

FMT_SMR.1.2 The TSF shall be able to associate users with the roles.

FMT_MSA.1	**Management of security attributes**
FMT_MSA.1.1	The TSF shall enforce the [BFS Access Control SFP] to restrict the ability to : • [change_default, query, modify and delete] the security attributes [the rules (permissions) to permit or deny traffic flow]; • [query, modify, delete and [create]] the security attributes [BFS administrator accounts[1] and Proxy Server user accounts]; • [modify] the security attributes [the FTP admin password]; • [change_default, query, modify] the security attributes [FTP server, Web server, Proxy Server]; • [change_default, query, modify] the security attributes [events to be accounted and alarm parameters] to the [BFS administrator role].
FMT_MSA.3	**Static attribute initialisation**
FMT_MSA.3.1	The TSF shall enforce the [Information flow control SFP and Access Control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [BFS administrator] to specify alternative initial values to override the default values when an object or information is created.
FMT_MTD.1	**Management of TSF data**
FMT_MTD.1.1a	The TSF shall restrict the ability to: • [query] the [audit logs]; • [query and modify] the [time]; to [BFS administrator].
FMT_MTD.1.1b	The TSF shall restrict the ability to [query, copy and delete] the [audit logs] to [FTP administrator].

5.1.3 Security Audit

This section involves recognising, recording and storing information related to security relevant activities.

[1] An element of the BFS Administrator account is the BFS administrator password.

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [Every successful inbound and outbound connection[2];

Every unsuccessful connection;

Every successful and unsuccessful administrator authentication attempt].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [required destination address, and TCP/UDP port for network connections].

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take [the following actions:

a) log a record of the event in the security trail;

b) e-mail the BFS administrator with details of the actual/potential security violation]

upon detection of a potential security violation.

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation in the TSP.

[2] With the exception of NTP requests made to the BFS NTP server.

FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) accumulation or combination of [a configurable number of attempts to make a connection to a service which does not have a server or proxy enabled] known to indicate a potential security violation; b) [no other rules].

FAU_SAR.1	**Audit review**
FAU_SAR.1.1	The TSF shall provide [BFS administrators] with the capability to read [all audit information] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1	**Protected audit trail storage**
FAU_STG.1.1	The TSF shall protect the stored audit records from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [prevent] modifications to the audit records.

5.1.4 Protection of the Trusted Security Functions

This section specifies functional requirements that relate to the integrity and management of the mechanisms providing the TSF and the TSF data.

FPT_RVM.1	**Non-Bypassability of the TSP**
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1	**TSF domain separation**
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1	**Reliable Time Stamps**
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.

5.1.5 User Data Protection

This section specifies requirements for TOE security functions and TOE security function policies relating to protecting user data. These are used to ensure a secure channel for administration and the control of user traffic through the firewall. The policies selected for the control of user traffic will depend on the number of interfaces configured in the TOE.

Access to the BFS internal data is controlled by the identification and authentication of a BFS administrator at the BFS console. Once this has been completed, according to the requirements specified by the FIA class of components, an administrative user is able to access all TSF data.

Access to data stored in the FTP server is controlled according to the FTP account the user has successfully provided the necessary authentication information. An "anonymous" or "ftp" FTP user can only access a subset of the information that the FTP Admin user is able to access.

FDP_ACC.1	**Subset access control**
FDP_ACC.1.1a	The TSF shall enforce the [BFS Access Control SFP] on 1. [manipulation of TSF data and security attributes (as specified in FMT_MSA.1) by the BFS administrator; 2. no access to TSF data by any other user].
FDP_ACC.1.1b	The TSF shall enforce the [FTP Access Control SFP] on [FTP server data].
FDP_ACF.1	**Security attribute based access control**
FDP_ACF.1.1a	The TSF shall enforce the [BFS Access Control SFP] to objects based on [the user being an authenticated BFS administrator].
FDP_ACF.1.1b	The TSF shall enforce the [FTP Access Control SFP] to objects based on [the user being an authenticated FTP Admin user].
FDP_ACF.1.2a	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the subject invoking an operation on the object is a BFS administrator].

FDP_ACF.1.2b	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. [creation, modification or deletion of objects on the FTP server may only be performed by authenticated FTP admin users; 2. access to the admin area on the FTP server may only be granted to authenticated FTP admin users; 3. anonymous FTP users are granted read and copy access to the public area only on the FTP server].
FDP_ACF.1.3	The TSF has explicitly authorised access of subjects to objects based on the following additional rules [none].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [subject not being a BFS administrator or an FTP Admin user].

There are two types of information flow:

a) AUTHENTICATED – traffic from the internal network to the TOE, providing access to the BFS for a remote BFS Administrator on the internal network, which requires the source subject to be identified and authenticated as a BFS administrator. Also, Web access, if authentication requirements are configured.

b) UNIDENTIFIED – outbound traffic from the internal network and inbound traffic from the external to the SSN/AUX[3], serviced by proxies. Also, traffic directed at the specified servers provided by the BFS.

Note: In the specification of the SFR FDP_IFF.1.2 below, the subsections of the requirement listed as 'a.)', 'b.)', 'c.)', etc. are to be read as "or" operators and the bullets within these subsections are to be read as "and" operators.

FDP_IFC.1	**Subset information flow control**
FDP_IFC.1.1	The TSF shall enforce the [AUTHENTICATED and UNIDENTIFIED information flow control SFPs] on: a) [external IT entities to send and receive information through the TOE; b) internal IT entities to initiate a service and to send and receive information through the TOE].

[3] Only applicable if 3[r] or more network card are configured in the TOE.

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [AUTHENTICATED and UNIDENTIFIED information flow control SFPs] based on the following types of subject and information security attributes:

a) [the interface on which the request arrives;

b) the following information attributes:

- presumed address of the source subject, as appropriate;
- presumed address of the destination subject, as appropriate;
- transport layer protocol;
- requested service.]

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

a) [subjects on the internal network can cause information to flow through the TOE to either the SSN/AUX or the external network if:

- all information security attribute values are expressly permitted by the information flow SFP rules;
- the request arrives on the internal interface;
- the presumed address of the destination subject translates to an address on either the SSN/AUX or an address that is reachable via the external network.

b) subjects on the external network can cause information to flow through the TOE to the internal network if:

- all information security attribute values are expressly permitted by the information flow SFP rules;
- the presumed address of the source subject translates to an external network address;
- the presumed address of the destination subject translates to an address assigned to the external interface of the TOE.

c) [4]subjects on the external network can cause information to flow through the TOE to the SSN/AUX if:

- all information security attribute values are expressly permitted by the information flow SFP rules;

[4] Only applicable if 3 or more network card are configured in the TOE.

- the presumed address of the source subject translates to an external network address;
- the presumed address of the destination subject translates to an address assigned to the external interface of the TOE.

d) [5]subjects on the SSN/AUX can cause information to flow through the TOE to the external network if:

- all information security attribute values are expressly permitted by the information flow SFP rules;
- the presumed address of the source subject translates to an SSN/AUX address;
- the presumed address of the destination subject translates to an address on the external network.

e) [6]subjects on the SSN/AUX can cause information to flow through the TOE to the internal network if:

- all information security attribute values are expressly permitted by the information flow SFP rules ;
- the presumed address of the source subject translates to an SSN/AUX address;
- the presumed address of the destination subject translates to an address assigned to an SSN/AUX interface on the firewall.]

FDP_IFF.1.3 The TSF shall enforce the [additional SFP rules:

a) restrict by time].

[5] Only applicable if 3 or more network card are configured in the TOE.

[6] Only applicable if 3 or more network card are configured in the TOE.

FDP_IFF.1.4	The TSF shall provide the following [notification to the user (BFS administrator) if the attributes of the permitted information flow specified are considered to be insecure, in the following instances: a) defining a non-authenticated inbound proxy; b) enabling any external to internal proxy; c) creating a user defined external to internal proxy; d) enabling any external to SSN/AUX proxy[7]; e) creating a user defined external to SSN/AUX proxy[8]; f) enabling any SSN/AUX to internal proxy[9]; g) creating a user defined SSN/AUX to internal proxy[10].]
FDP_IFF.1.5	The TSF shall explicitly authorise an information flow based on the following rules [no additional rules to authorise information flow]
FDP_IFF.1.6	The TSF shall explicitly deny an information flow based on the following rules: a) [there is no rule which explicitly allows it; b) if any of the attributes identified in FDP_IFF.1.1 do not match].

5.2 TOE Security Assurance Requirements

The assurance requirements for this Security Target, taken from Part 3 of the CC, compose the EAL4 level of assurance, augmented with the Flaw Remediation assurance component ALC_FLR.1 and the Vulnerability Analysis component AVA_VLA.3, both identified in Part 3. The assurance components are summarised in the following table.

[7] Only applicable if 3 or more network card are configured in the TOE.

[8] Only applicable if 3 or more network card are configured in the TOE.

[9] Only applicable if 3 or more network card are configured in the TOE.

[10] Only applicable if 3 or more network card are configured in the TOE.

Assurance Class	**Assurance Components**	
Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

Assurance Class	Assurance Components	
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately Resistant

Table 5-2: Assurance Requirements

Further information on these assurance components can be found in [CC] Part 3.

5.3 Security Requirements for the IT Environment

There are no security requirements on the IT environment of the TOE.

5.4 Strength of Function Claim

A Strength of Function (SoF) claim of SOF-MEDIUM is made for the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the BorderWare firewall server in Section 5.1.

6.1.1 Identification and Authentication

1. The BFS administrator must be authenticated with the TOE before any administration functions can be completed. Interaction with the administrator interface at the system console requires physical access to the console and the password, or interaction with the administrator interface at the admin GUI requires identification and the corresponding password.

2. The only flows of information that can take place before identification of the source of the request are those that conform to the UNIDENTIFIED information flow policy.

3. The only flows of information that can take place before authentication of an identified source are those that conform to the UNIDENTIFIED information flow policy.

4. Any failure of an administrator (BFS administrator or FTP Admin) to authenticate with the TOE must result in the generation of a record in the audit trail.

6.1.2 Management and Security Attributes

1. The rules, which specify the permissible flows of information, can be modified by an BFS administrator of the TOE. The BFS administrator may provide alternative initial values to be applied when an information flow rule is created.

2. The TOE shall default to deny all flows of information through the TOE, all proxies and servers are initially disabled. (Interaction with the BFS administration functions using the BFS console by an authenticated BFS administrator is permitted at this stage). After the installation, the BFS administrator must go through each service and enable the ones necessary for their network. The result is a completely controlled environment in which specified services are allowed and all others are denied.

3. Access to the TSF data and security attributes stored on the TOE (data required for the TOE to operate in a secure manner) is controlled by authentication of an authorised (access to the BFS console is permitted or identification if remote) BFS administrator.

4. Access to the data stored on the FTP server will be permitted according to the FTP account for which the FTP user has successfully provided identification and authentication information. An anonymous FTP user (identified as “anonymous”)

may access only the data in the "public" directory of the FTP server. An FTP admin (identified as "admin" and authenticated) user may access all data on the FTP server (including the TSF audit data stored in the Admin area of the FTP server).

5. The only type of direct user of the TOE is a BFS administrator. The FTP admin user is only able to access the data provided on the FTP server supported by the BFS.

6. In the following instances, where the attributes of the permitted information flow specified are considered to be insecure, the TOE shall provide the BFS administrator with a warning:

    a) defining a non-authenticated inbound proxy;

    b) enabling any external to internal proxy;

    c) creating a user defined external to internal proxy;

    d) an option of "none" is selected as the authentication option for remote administration;

    The following are also applicable if three or more network cards are installed in the TOE:

    e) enabling any external to SSN/AUX proxy;

    f) creating a user defined external to SSN/AUX proxy;

    g) enabling any SSN/AUX to internal proxy;

    h) creating a user defined SSN/AUX to internal proxy.

7. The BFS administrator can query, create, delete and modify BFS administrator accounts and reset a BFS administrator's password. The BFS administrator can query, create, delete and modify Proxy Server user accounts and reset an FTP Admin's password.

8. The BFS administrator can configure and modify the FTP server for the storage of audit trails, the Web server for remote access.

6.1.3 Audit

1. The accounting mechanisms cannot be disabled. The start-up and shutdown of audit functions is synonymous with the start-up and shutdown of the TOE. Start-up and shut-down of the TOE must be recorded in the audit trail.

2. It shall be possible to generate an accounting record of the following events:

    - Every successful inbound and outbound connection;

- Every unsuccessful inbound and outbound connection;
- Every successful and unsuccessful administrator (BFS administrator and FTP Admin) authentication attempt.

3. The following data is to be recorded for each event:
   - Date and Time of the event;
   - type of event;
   - subject identity (source address);
   - outcome of the event;
   - required destination address;
   - TCP/UDP port for network connections.
4. Modifications to the content of the audit trail are not permitted. Read access only is permitted to the BFS administrator through a controlled interface.
5. An FTP admin user is permitted read, copy or delete access only to an archived audit log. An FTP admin user is not permitted modify access to an audit trail while it is stored in the admin area of the FTP server. Deletion of the audit trail from the FTP server can only be performed by an FTP admin user.
6. A record will be generated in the security trail and an e-mail sent to the BFS administrator in the event of an attempt to make a connection to a service that does not have a server or proxy enabled.

6.1.4 Protection of TOE Security Functions

1. The TOE will provide self-protection from external modification or interference of the TSF code or data structures by untrusted subjects. Untrusted subjects cannot bypass checks, they will always be invoked.

   The functions that enforce the TOE Security Policy (TSP) will always be invoked and completed, before any function within the TSF Scope of Control (those interactions within the TOE that are subject to the rules of the TSP) is allowed to proceed.

   The TSF will protect itself, ensuring that all other processes are executed within other domains to those of the TSF processes and thereby are unable to modify or damage the TSF.

2. The TOE shall provide reliable time stamps for use in determining whether an information flow is permissible and for stamping entries in the audit trail.

6.1.5 User Data Protection

1. There are two types of information flow that the TOE enforces:

   a) AUTHENTICATED – traffic from the internal network to the TOE, providing access to the BFS for a remote BFS administrator on the internal network, which requires the source subject to be identified and authenticated as a BFS administrator. Also, Web access, if authentication requirements are configured.

   b) UNIDENTIFIED – outbound traffic from the internal network and inbound traffic from the external to an SSN/AUX network[11], serviced by proxies. Also, traffic directed at the specified servers provided by the BFS.

2. The information flow control security functional policy mediates traffic between the network interface cards of the BFS host and the BFS itself. This policy ensures that when a request for a connection arrives, the BFS takes the following action:

   a) Checks the port and destination address to see if they are consistent with an enabled server or proxy;

   b) If they are, then the number of current sessions are checked against the maximum set for that service. If a number of sessions is at the maximum, then the connection is denied. Otherwise, access rules are checked (as in 'c.)' below);

   c) For each access rule assigned to the service, the following conditions must be met for the particular connection request:

      - The access rule session limit has not been reached;
      - The current time is within any configured time slot;
      - The source or destination address is allowed.

   d) The firewall decides the following:

      - If any rule is applicable that denies the connection, then the connection is denied;
      - If no access rules are applicable or assigned to the service, then the connection is denied[12];

[11] Only applicable if three or more network cards are configured in the TOE.

[12] If no access rules are assigned to a service, then no access rules will ever be applicable, and so access will always be denied

- Otherwise, the connection is allowed[13].

3. The requested services are permitted according to the UNIDENTIFIED information flow policy (based purely on the direction (source and destination) of the request and the service type requested), as indicated in the following tables (Table 6-1, Table 6-2 and Table 6-3). These services can be configured on the BFS (within the scope of this Security Target) to be provided by either Proxies, Servers or Clients provided by the BFS.

I-E	**I-SSN/AUX[14]**	**E-SSN/AUX[15]**	**SSN/AUX-E[16]**
America On-Line	Finger	Anonymous FTP	BookWhere (Z39.50)
BookWhere (Z39.50)	FTP	Finger	DNS Relay
DNS Relay	Gopher	Ident	Finger
Finger	ICMP Ping/Timestamp	NNTP	FTP
FTP	Ident	Oracle SQL*Net	Gopher
Gopher	IMAP	SMTP Mail	ICMP Ping/Timestamp
ICMP Ping/Timestamp	Lotus Notes	WWW	Ident
Ident	Magistrate (Snare)		IMAP
IMAP	MS SQL		Lotus Notes
Lotus Notes	NetShow		Magistrate (Snare)

[13] Response packets will be checked against the packet filter rules but not the access rules, which are used only to establish a connection.

[14] Only applicable if 3 or more networks card are configured in the TOE.

[15] Only applicable if 3 or more network cards are configured in the TOE.

[16] Only applicable if 3 or more network cards are configured in the TOE.

I-E	I-SSN/AUX[14]	E-SSN/AUX[15]	SSN/AUX-E[16]
Magistrate (Snare)	NNTP		MS SQL
MS SQL	Oracle SQL*Net		NetShow
NetShow	POP Mail		NNTP
NNTP	RealAudio		Oracle SQL*Net
Oracle SQL*Net	SMTP Mail		POP Mail
NetMeeting[17]	SSH		Real Audio
POP Mail	Telnet		SMTP Mail
Real Audio	WWW		SSH
SMTP Relay			Telnet
SSH			WWW
Telnet			
Whois			
WWW			

Table 6-1 - UNIDENTIFIED Services provided by Proxies

The Internal to External and External to SSN/AUX WWW proxy identified in Table 6-1 above includes a data content filtering module which may optionally be enabled. The data content filtering module is designed to detect abnormal content in HTTP headers. The primary purpose of the filtering module is to protect web servers connected to one of the SSN/AUX interfaces from known vulnerabilities exploited via malformed HTTP headers (for example Trojan Horses and Worms such as Code Red).

[17] Only the H.323 and LDAP proxy connections are permissible to support the provision of the NetMeeting service within the scope of this evaluation.

Internal	External	SSN/AUX[18]
DNS	Anonymous FTP	Anonymous FTP
Finger	DNS	DNS
FTP	Finger	Finger
ICMP Ping/Timestamp	ICMP Ping/Timestamp	ICMP Ping/Timestamp
Ident	Ident	Ident
LDAP[19]	NTP	NTP
NTP	SMTP Mail	POP Mail
POP Mail	Traceroute Response	SMTP Mail
SMTP Mail	WWW	Traceroute Response
Traceroute Response		WWW
WWW		

Table 6-2 - UNIDENTIFIED Services provided by Servers

Internal	External	SSN/AUX[20]
NTP	DHCP	NTP
	NTP	

Table 6-3 – UNIDENTIFIED Services provided by Clients

4. The requested services are permitted according to the AUTHNETICATED information flow policy (based purely on the direction (source and destination) of the request and the service type requested), as indicated in Table 6-4. These services can be configured on the BFS (within the scope of this Security Target) to

[18] Only applicable if 3 or more network cards are configured in the TOE.

[19] LDAP server on Internal interface is provided to work with the NetMeeting proxy to support Microsoft's Conferencing application.

[20] Only applicable if 3 or more network cards are configured in the TOE.

be provided by Servers (there are no services provided by Proxies or Clients on the BFS that conform to the AUTHENTICATED information flow policy).

Internal	External	SSN/AUX[21]
FTP		
GUI Config		

Table 6-4 – AUTHENTICATED Services provided by Servers

6.2 Assurance Measures

Deliverables will be produced to comply with the Common Criteria Assurance Requirements for EAL4, augmented with ALC_FLR.1 and AVA_VLA.3.

6.3 Permutational IT Security Functions

The only permutational IT security functions that are realised in the TOE are the administrator passwords at the system console and the administration GUI, and the ftp-admin password. The Strength of function claim for these mechanisms is SOF-MEDIUM.

[21] Only applicable if 3 or more network cards are configured in the TOE.

7 Protection Profiles Claims

There are no Protection Profile Claims.

8 Rationale

8.1 Introduction

This section identifies the rationale for the adequacy of the security functional requirements and the security assurance requirements in addressing the threats and meeting the objectives of the TOE.

8.2 Security Objectives for the TOE and Environment Rationale

The following table demonstrates how the objectives of the TOE and the TOE environment counter the threats, policies and assumptions identified in Section 3.2.1.

Threats / **Objectives/ Assumptions**	**T.EXT_CONN**	**T.INT_CONN**	**T.SOURCE**	**T.CONFIG**	**T.UNAUTH**	**T.OS_FAC**	**TE.VIOLATE**	**A.PHYSICAL**	**A.LIMIT**
O.VALID	✓	✓	✓						✓
O.HOSTILE	✓		✓	✓					✓
O.PRIVATE		✓	✓	✓					✓
O.AUTH	✓								✓
O.ATTEMPT			✓		✓				✓
O.ADMIN					✓				
O.SECPROC				✓		✓			
O.CONFIG						✓			
NOE.DELIV							✓		
NOE.TRAIN							✓		
NOE.AUDIT							✓		
NOE.NETWORK	✓	✓						✓	✓
NOE.MANAGE							✓		
NOE.PHYSICAL								✓	
NOE.REVIEW				✓	✓				

Table 8-1 Objectives Rationale

As can be seen from the table above, all threats and assumptions met by at least one objective, either TOE or environment, as applicable. The coverage of the threats and assumptions countered by the TOE is discussed in the subsections below.

8.2.1 T.EXT_CONN

As the only point of connection between the networks, the BFS controls the information flow between the internal and external networks. BFS limits the hosts, address ranges (i.e., it will reject a packet received at the external network interface with an address within the internal network address range) and service ports available from the external network. No inbound services are permitted connection.

8.2.2 T.INT_CONN

As the only point of connection between the networks, the BFS controls the information flow between the internal and external networks. BFS limits the hosts, address ranges (i.e., it will reject a packet received at the internal network interface with an address within the external network address range) and service ports available from the internal network.

8.2.3 T.SOURCE

BFS limits the hosts and service ports available from the internal and external network, in order to prevent exploitation of vulnerabilities in Internet services. BFS will monitor attempts to initiate connections between the networks (internal and external, and SSN/AUX if 3 or more network cards are configured in the TOE).

8.2.4 T.CONFIG

BFS limits the range of addresses expected on the internal and external networks. BFS will process security functions and service requests in separate domains to ensure the security functions are not affected by indirect user traffic. Each process will complete before another process requiring the same data structures/processes is invoked.

8.2.5 T.UNAUTH

BFS ensures only the BFS administrator can amend the configuration. BFS will monitor attempts to initiate connections between the networks (internal and external, and SSN/AUX if 3 or more network cards are configured in the TOE), including attempts to initiate a remote administration session.

8.2.6 T.OS_FAC

BFS does not provide any operating system services to any user of the BFS. (There is no command line access provided). BFS will process security functions and service requests in separate domains to ensure the security functions are not affected by indirect user traffic.

8.2.7 TE.VIOLATE

The administrators of the BFS are trusted to install, manage and operate (including using and managing the audit facilities) the BFS in a manner consistent with the security policy. The BFS administrators should be provided with the appropriate training in order to complete this.

8.2.8 A.PHYSICAL

The BFS must be the only (physical and logical) connection between the internal and external networks, and the SSN/AUX network if 3 or more network cards are configured in the TOE. Access to the system console must be controlled.

8.2.9 A.LIMIT

BFS limits the hosts and service ports available from the internal and external network, to prevent exploitation of vulnerabilities in Internet services . BFS will monitor attempts to initiate connections between the networks (internal and external, and SSN/AUX if 3 or more network cards are configured in the TOE). BFS limits the address ranges (i.e., it will reject a packet received at the internal network interface with an address within the external network address range, and vice versa) available from the internal and external network. Service requests will be subject to authentication checks, in accordance with the security policy enforced on the BFS.

8.3 Security Requirements Rationale

8.3.1 Requirements are appropriate

The following table identifies which SFRs satisfy the Objectives defined in Section 4.1.1

Objective	Security Functional Requirement(s)
O.VALID	FDP_IFC.1, FDP_IFF.1[22]
O.HOSTILE	FDP_IFC.1, FDP_IFF.1[23], FMT_MSA.3, FIA_UID.1, FIA_UAU.1, FPT_STM.1
O.PRIVATE	FDP_IFC.1, FDP_IFF.1[24], FMT_MSA.3, FIA_UID.1, FIA_UAU.1, FPT_STM.1

[22] The valid range of addresses expected on internal and external interfaces are limited by the checks of the interface on which the request arrives and the presumed source address of the request whether there are 2 or more network cards configured in the TOE.

[23] The host and services ports that can be accessed from the external network are limited by the following completions of the assignment in FDP_IFF.1.2: b) if there are 2 network cards configured in the TOE, and b) and c) if there are 3 or more network cards configured in the TOE.

Objective	Security Functional Requirement(s)
O.AUTH	FIA_UID.1, FIA_UAU.1, FDP_IFC.1, FDP_IFF.1[25]
O.ATTEMPT	FAU_GEN.1, FAU_ARP.1, FAU_SAA.1, FAU_SAR.1, FAU_STG.1, FIA_AFL.1, FIA_UID.1, FIA_UAU.1, FPT_STM.1
O.ADMIN	FMT_SMR.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FIA_UID.1, FIA_UAU.1, FDP_ACC.1, FDP_ACF.1
O.SECPROC	FPT_RVM.1, FPT_SEP.1
O.CONFIG	FDP_IFF.1, FPT_RVM.1, FPT_SEP.1

Table 8-2 Mapping of Objectives to SFRs

O.VALID

The range of addresses expected on the internal and external network are limited by the control of information flow through the BFS. Information flow control is based on a number of attributes of the request, including the source address of the request. This address is linked to the interface on which the request was received to ensure it is an address expected on that interface (FDP_IFC.1, FDP_IFF.1[26])

O.HOSTILE

The BFS must limit the internal hosts and service ports that can be accessed from the external network. The BFS achieves this by controlling information flows with respect to external to internal network and internal to external network. The BFS controls information flow by allowing or denying traffic through based on (FDP_IFC.1, FDP_IFF.1[27], FPT_STM.1):

---

[24] The hosts and service ports that can be accessed from the internal network are limited by completion a) of the assignment in FDP_IFF.1.2 whether there are 2 or more network cards configured in the TOE.

[25] The authentication of an end user will be provided according to the following completions of the assignment in FDP_IFF.1.2: a) and b) if there are 2 network cards configured in the TOE, and a), b), c) d) and e) if there are 3 or more network cards configured in the TOE.

[26] The valid range of addresses expected on internal and external interfaces are limited by the checks of the interface on which the request arrives and the presumed source address of the request whether there are 2 or more network cards configured in the TOE.

[27] The hosts and service ports that can be accessed from the internal network are limited by completion a) of the assignment in FDP_IFF.1.2 whether there are 2 or more network cards

- Source address;
- Destination address;
- Service used;
- The time the activity is performed is permitted.

The BFS will also deny any information flows for which no rule is defined and defaults to deny all information flows through the TOE (FMT_MSA.3) except interaction with the administration functions by an authenticated BFS administrator (FIA_UID.1, FIA_UAU.1).

O.PRIVATE

The BFS must limit the internal hosts and service ports that can be accessed from the external network. The BFS achieves this by controlling information flows with respect to external to internal network and internal to external network. The BFS controls information flow by allowing or denying traffic through based on (FDP_IFC.1, FDP_IFF.1[28], FPT_STM.1):

- Source address;
- Destination address;
- Service used;
- The time the activity is performed is permitted.

The BFS will also deny any information flows for which no rule is defined and defaults to deny all information flows through the TOE (FMT_MSA.3) except interaction with the administration functions by an authenticated BFS administrator (FIA_UID.1, FIA_UAU.1).

O.AUTH

The BFS controls information flow by allowing or denying traffic through based on the configured rules (FDP_IFC.1, FDP_IFF.1[29]). These rules implement the UNIDENTIFIED and AUTHENTICATED information flow policies. Any rule implementing the AUTHENTICATED information flow policy requires the user to identify and authenticate themselves with the BFS server prior to processing the requested service (FIA_UID.1, FIA_UAU.1).

---

configured in the TOE.

[28] The hosts and service ports that can be accessed from the internal network are limited by completion a) of the assignment in FDP_IFF.1.2 whether there are 2 or more network cards configured in the TOE.

[29] The hosts and service ports that can be accessed from the internal network are limited by completion a) of the assignment in FDP_IFF.1.2 whether there are 2 or more network cards configured in the TOE.

O.ATTEMPT

The BFS provides an accounting mechanism that cannot be disabled. The start-up and shutdown of the audit function is synonymous with the start-up and shutdown of the firewall. Start-up and shutdown of the TOE is recorded in the audit log. The following events can be recorded with their associated data (FAU_GEN.1, FPT_STM.1, FIA_AFL.1, FIA_UID.1, FIA_UAU.1):

- All inbound and outbound connection attempts;
- Every successful and unsuccessful administrator authentication;
- Change of administrator password;

The BFS provides the facility for the BFS administrator to view the audit trail (read-only access) and for the FTP Admin to read, copy and delete the audit trail archived to the admin area of the FTP server (FAU_SAR.1, FAU_STG.1).

The BFS also provides alerting facilities. When the TOE encounters an event for which alerts are defined, it will record the event in the audit log and send e-mail to the administrator (FAU_ARP.1, FAU_SAA.1).

O.ADMIN

BFS only maintains two types of user (FMT_SMR.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1):

- BFS Administrator – able to manipulate the configuration of the firewall and view the audit trail data;
- FTP Admin – able to view, copy and delete the audit trail data.

Identification and authentication of the requesting user provides an access control mechanism to the management functions of the BFS (FIA_UID.1, FIA_UAU.1, FDP_ACC.1, FDP_ACF.1).

O.SECPROC

Control of security functions processes is provided by the separation of areas in which to security functions and service requests are processed (FDP_SEP.1), and through ensuring the completion of security function processing prior to invocation of subsequent security functions (FDP_RVM.1).

O.CONFIG

The BFS is designed to provide no operating system user services by ensuring the information flows do not access the operating system (FDP_IFF.1) and that separate domains are provided in which to process security functions (FDP_SEP.1) and controlling the invocation of subsequent functions (FDP_RVM.1).

As it can be seen in Table 8-2 and the descriptions above, all objectives are satisfied by at least one SFR and all SFRs are required to meet at least one objective.

Therefore, as demonstrated in Table 8-1 and Table 8-2, all SFRs specified for the TOE are appropriate to counter the threats and meet the objectives of the TOE.

8.3.2 Security Requirement dependencies are satisfied

( ) indicates an indirect dependency

[ ] indicates an optional dependency

Functional Component	Dependencies
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FIA_UID.1	none
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1
FAU_GEN.1	FPT_STM.1
FAU_ARP.1	FAU_SAA.1
FAU_SAA.1	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1
FPT_RVM.1	none
FPT_SEP.1	none
FPT_STM.1	none
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3

Table 8-3 Mapping of SFR Dependencies

As demonstrated in the table above, each of the SFRs identified as dependencies have been stated as Functional Components of the TOE. Therefore, all dependencies have been satisfied.

8.3.3 Security Requirements are mutually supportive

The only interactions between the security requirements specified for the BFS are those which are identified in the CC Part 2 as dependencies between the SFRs. These dependencies are documented and demonstrated to be satisfied in Section 8.3.2. These interactions are specified in the CC Part 2, and are therefore mutually supportive

8.3.4 ST complies with the referenced PPs

This Security Target does not claim compliance with a Protection Profile.

8.3.5 IT security functions satisfy SFRs

Mapping of Section 6 IT functions to SFRs (Section 5.1).

IT Function	Security Functional Requirement(s)	Coverage of SFR(s) by IT Function
6.1.1/1	FIA_UAU.1.2	Complete
6.1.1/2	FIA_UID.1.1	Complete
6.1.1/3	FIA_UID.1.2 FIA_UAU.1.1	Complete Parts a and b
6.1.1/4	FIA_AFL.1.1 FIA_AFL.1.2 FIA_UAU.1.1	Complete Complete Part c
6.1.2/1	FMT_MSA.1.1 FMT_MSA.3.2	Point 1 Complete
6.1.2/2	FMT_MSA.3.1 FDP_ACF.1.4	Complete Partial – BFS administrator
6.1.2/3	FMT_MSA.1.1 FDP_ACC.1.1a FDP_ACF.1.1a	Complete Complete Complete

	FDP_ACF.1.2a FDP_ACF.1.4	Complete Partial – BFS administrator
6.1.2/4	FDP_ACC.1.1b FDP_ACF.1.1b FDP_ACF.1.2b FDP_ACF.1.4	Complete Complete Complete Partial – FTP
6.1.2/5	FMT_SMR.1.1 FMT_SMR.1.2	Complete Complete
6.1.2/6	FDP_IFF.1.4	Complete
6.1.2/7	FMT_MSA.1.1	Points 2, 3, 4 and 5
6.1.2/8	FMT_MSA.1.1	Point 6
6.1.3/1	FAU_GEN.1.1	Part a
6.1.3/2	FAU_GEN.1.1	Part c
6.1.3/3	FAU_GEN.1.2	Complete
6.1.3/4	FAU_STG.1.1 FAU_STG.1.2 FAU_SAR.1.1 FAU_SAR.1.2	Complete Complete Complete Complete
6.1.3/5	FAU_STG.1.1 FAU_STG.1.2 FMT_MTD.1.1a FMT_MTD.1.1b	Complete Complete Complete Complete
6.1.3/6	FAU_ARP.1.1 FAU_SAA.1.1 FAU_SAA.1.2	Complete Complete Complete

6.1.4/1	FPT_RVM.1.1	Complete
	FPT_SEP.1.1	Complete
	FPT_SEP.1.2	Complete
6.1.4/2	FPT_STM.1.1	Complete
6.1.5/1	FDP_IFC.1.1	Partial
	FDP_IFF.1.2	Partial
6.1.5/2	FDP_IFC.1.1	Partial
	FDP_IFF.1.1	Partial
	FDP_IFF.1.2	Partial
	FDP_IFF.1.3	Complete
	FDP_IFF.1.6	Complete
6.1.5/3	FDP_IFF.1.1	Partial
	FDP_IFF.1.2	Partial
6.1.5/4	FDP_IFF.1.1	Partial
	FDP_IFF.1.2	Partial

Table 8-4 Mapping of IT Functions to SFRs

SFR FAU_GEN1.1 part b requires no IT Functions.

SFRs FDP_ACF.1.3 and FDP_IFF.1.5 have not been translated into IT security functions, as they specify that no rules are required in addition to those specified in other elements of the respective components.

The combination of the IT Functions specified in 6.1.5/1, 6.1.5/2 , 6.1.5/3 and 6.1.5/4 fully provide the requirements of SFRs FDP_IFC.1.1, FDP_IFF.1.1 and FDP_IFF.1.2.

Therefore, as demonstrated all Security Functional Requirements of the TOE are fully provided by the IT security functions specified in the TOE Summary Specification.

Also demonstrated in Table 8-4, all IT Security Functions identified for the TOE in the TOE Summary Specification are required to meet the TOE Security Functional Requirements.

8.3.6 IT security functions mutually supportive

The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 8.3.3), as each of the IT functions can be mapped to one or more SFRs, as demonstrated on Table 8-4.

8.3.7 Strength of Function claims are appropriate

The SoF claim made by the TOE is SOF-MEDIUM, which is defined in the CC Part 1 as “resistance to attackers possessing a moderate attack potential”.

This product is to be used in environments such as government departments to protect internal networks when connecting them to external networks. The guidance for such interconnections is to use Firewall products with ITSEC E3 or equivalent (CC EAL4) assurance, for which a strength of SOF-MEDIUM is generally felt to be acceptable.

Therefore, the claim of SOF-MEDIUM made by BFS is viewed to be appropriate for this use.

8.3.8 Assurance measures satisfy assurance requirements

EAL4 is defined in the CC as “methodically designed, tested and reviewed”.

Products such as BFS are intended to be used in a variety of environments, and used to connect networks with different levels of trust in the users. The BFS is intended to be suitable for use in UK HMG, which requires an ITSEC E3 equivalent level of assurance, for which EAL4 assurance is suitable.

In the Internet area of IT new exploits are continually being discovered and published, which the BFS will be expected to protect the internal network against. It is therefore considered to be appropriate to augment the EAL4 assurance requirements for the BFS with the ALC_FLR.1 and AVA_VLA.3 assurance components. This will provide additional assurance that new vulnerabilities identified and reported in the services the product supports, or in the product itself, are addressed in a controlled and suitable manner and that the TOE has been analysed and tested to demonstrate that it is "moderately resistant" to attack.