Common Criteria Security Target

Author	Deniz Kucukreisoglu
Reporting to	Bhavin Desai
Valid on	05 February 2003
Status	Definitive
Deliverability	EXTERNAL
File number	CLEF.EC25402.40.1
Issue Number	3.0
Page count	60

Copyright ©2003 by CyberGuard Corporation. All rights reserved. This publication or any part thereof is intended for use with CyberGuard Corporation products by CyberGuard Corporation personnel, customers, and end users. It may not be reproduced in any form without the written permission of the publisher.

TABLE OF CONTENTS

REFERENCES

Standards & Criteria

CC
Common Criteria for Information Technology Security Evaluation
(Comprising Parts 1-3, [CC1], [CC2], [CC3])

CC1
Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and General Model
CCIMB-99-031, Version 2.1, August 1999

CC2
Common Criteria for Information Technology Security Evaluation
Part 2: Security Functional Requirements
CCIMB-99-032, Version 2.1, August 1999

CC3
Common Criteria for Information Technology Security Evaluation
Part 3: Security Assurance Requirements
CCIMB-99-033, Version 2.1, August 1999

ITSEC
Information Technology Security Evaluation Criteria,
Version 1.2, CEC, 28 June 1991

CGFM
CyberGuard Firewall Manual
Part Number FW001-050
CyberGuard Corporation
June 2000

MANUAL M
CESG COMPUSEC Manual M
Protecting Government Connections
To the Internet – Firewall Architectures
Issue 1.0 – September 1996

Plat_Comp
CyberGuard Firewall Platform Compliance
and Certification
Version 2.0
CyberGuard Corporation
April 1998

1. INTRODUCTION

1.1 Purpose

This document is the security target for the CC evaluation of the CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) product. The developers of the TOE are CyberGuard Corporation.

The role of the security target within the development and evaluation process is described in the CC: the Common Criteria for Information Technology Security Evaluation [CC].

1.2 ST overview

CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) safeguards information held on internal networks, by controlling the access of external users and protecting the integrity, availability, authentication data and anonymity of the internal network. Configuration and Reporting is performed with a local Graphical User Interface (GUI). Additional network interfaces (up to 32) provide DMZ or further internal/ external network connections.

The firewall runs on UnixWare 2.1.3 either as a single or multi-processor, on the Intel family of processors[1] including:

- Pentium
- Pentium Pro
- Pentium II
- Pentium III
- Pentium III Xeon

Security features within the scope of this ST include:

- Connection level Access Control for IP packets e.g. permit/deny source & destination addresses or ports, divert IP packets to a proxy process (FTP, HTTP, SMTP, NNTP, TELNET).
- Accounting, auditing and statistics of firewall traffic and security related events.
- Alerts (e.g. log-file, e-mail, SNMP traps) for security events.
- Network address translation facility for networks and hosts.
- Split Domain Name Server (SDNS).

[1] These are members of the IA-32 family of processors that use the same (4-ring) protection architecture specified in the Intel Architecture Software Developer's Manual Vol 1 (Basic architecture), which is built on by the UnixWare operating system.

The firewall relies on unevaluated functionality provided by the UnixWare operating system to perform identification and authorisation of the FTP and TELNET proxies. The auditing performed by the firewall is an extension of the UnixWare® auditing subsystem.

1.3 CC Conformance

This ST is CC Part 2 [CC2] conformant and CC Part 3 [CC3] conformant for EAL4.

This ST does not claim conformance with any Protection Profile. There are no explicitly stated IT security requirements that are not in [CC2].

1.4 Scope

The structure of this document is as defined by [CC] Part 1 Annex C.

- Section 2 is the TOE Description, which concentrates on the evaluated configurations of the CyberGuard 4.3 Firewall for UnixWare and a summary of the security features of the TOE.
- Section 3 provides the statement of TOE security environment, in particular the Environmental and Method of Use assumptions, the assumed threats and the Organisational Security Policies that collectively define the 'security problem' to be addressed by the TOE.
- Section 4 provides the statement of security objectives to be met by the TOE and its environment.
- Section 5 provides the statement of IT security requirements, detailed by the TOE Security Functional Requirements, the claimed Strength of the TOE Security Functions, the TOE Security Assurance Requirements and the Security Requirements for the IT Environment.
- Section 6 provides the TOE summary specification; this is broken down into the IT Security Functions, the Required Security Mechanisms, and Assurances measures.
- Annex A provides the ST Rationale, comprising the rationales for the security objectives, security requirements and TOE summary specification.

1.5 Terminology

This section contains technical definitions of terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise. The following are selected terms used within the firewall arena and are included by way of general relevance to this Security Target. They are based on the definitions provided by [MANUAL M].

Air-Gap: A physical separation between two networks. Data can only be transferred across an air-gap using removable computer media. There is no such thing as a logical air gap.

Access Router: An Access Router is an IP Router that has been configured to prevent the Internal Masquerade variant of IP Source-Address Spoofing attacks. Typically, an Access Router has two physical connections (ports), one to the external network (Internet) and one to the internal network. Such a device is configured so that IP packets that have source addresses purporting to be from the internal network will not be allowed through if they arrive on the external port. Likewise, IP packets that have source addresses purporting to be from the external network (Internet) will not be allowed through if they arrive on the internal port. It would also deny access to any IP datagram with the Loose Source-Router flag set. No device can prevent the External Masquerade variant of Source-Address Spoofing attacks.

Acknowledgement (or ACK) Flag:

Within the TCP protocol, an acknowledgement system is used within each conversation. When a conversation is first started, a flag within the TCP packet is cleared (the Acknowledgement (or ACK) Flag), on all subsequent parts of the conversation the Acknowledgement (or ACK) Flag is set. i.e. When the Acknowledgement (or ACK) Flag is set in a TCP packet, the packet is part of an already established conversation. (Note it may be possible for an attacker to tamper with the ACK flag.)

Anonymity: The process of preventing an external process (whether automated or manned) from determining the source of a piece of information, or the identity of an individual or an organisation. i.e. the outside(rs) cannot determine the identity of the inside(rs).

Application Level Gateway:

See Firewall.

Bastion Host: The Bastion Host provides the primary line of defence against outside attack, and must be suitably strengthened. It may provide anonymity to the users of the internal network, and to the topology of the internal network itself. It must have a minimal configuration, and must have a minimum number of users (e.g. perhaps only the administrator account). A Bastion Host can operate as an Application Level Gateway or Circuit Level Gateway, or both. Some Bastion Hosts appear to act as strengthened Screening Routers (though they don't route packets), whilst others provide transparent or non-transparent Proxy Services. The latest generation of Bastion Hosts provide both of these services simultaneously.

See Firewall.

Blocking Router: An IP Router configured to prevent the Internal variant of IP Source-Address Spoofing Attacks, and all connection requests - i.e. it only supports acknowledgement packets from the external network. They can be viewed as a similar functionality as a Guard, but do not solve any data separation or confidentiality issues. See Access Router.

Circuit level gateway: See Firewall.

De-Militarized Zone (DMZ): Same as No-Mans-Network (q.v.).

Domain Name Service (DNS):

A system that allows users or applications to match user-friendly domain names (such as www.itsec.gov.uk) to numeric IP Addresses (such as 123.123.123.123), and vice-versa. The DNS database can hold information about hardware types, operating system version numbers, and system administrators' names, and much more. DNS has to be supported by a site wishing to connect to the Internet, though it is sometimes provided by the service provider.

Drop safe logging:

The practice of protecting audit logs from modification by an attacker. Example means of achieving this include dumping audit logs to a dedicated PC via a serial line from the firewall machine, or using protected media such as Write Once Read Many (WORM) discs.

Encryption: (a) In-line IP encryption employs an in-line hardware device, that encrypts the payload (data portion plus transport and application headers) of each IP packet. The IP headers are left in clear so that packets can still be routed.

(b) Off-line encryption uses a software utility to encrypt a message at the users workstation before it is sent. Only the data is encrypted, so all headers are in clear.

File Transfer Protocol (FTP):

The File Transfer Protocol allows the transfer of files to and from remote hosts on the Internet. It uses two simultaneous TCP sessions - one for the data and one for management.

Firewall: A Firewall is a collection of Hardware and Software components that collectively provide an actively managed channel between networks with differing security policies. Legitimate communication may only be made through this channel, and when such communication takes place, it is tightly controlled and heavily audited. Attempts at unauthorised communication will be detected, though not necessarily prevented. A Firewall can be anything from a suitably configured Screening Router, through to a fully-fledged Bastion Host, to a combination of measures. This definition is intentionally broad to reflect the vast array of differing products described as a Firewall. In fact, firewalls can be one of four distinct types:

(a) Packet level firewalls use filter rules to mediate access at the IP level, and are typically specially modified routers. Hence, access control decisions are based upon IP addresses. They can also base the decision on packet attributes such as TCP/UDP port number or ACK flag status. An example of a packet filtering gateway is a Screening Router.

Advantages

- fast
- inexpensive
- applicable to all protocols and services
- transparent to user and applications

Disadvantages

- generally no logging or alarms
- filter rules are complex and have limited granularity
- they rely on trustworthiness of servers running on end system ports since the application data is not visible to the router filtering rules

- direct connection to outside
- stateless, so have difficulty with fragmented IP packets and with connectionless protocols such as UDP
- no network address translation (NAT)
- no authentication services can be provided

(b) Circuit level gateways, unlike packet filters, use proxying so that there is no direct connection between the external network and your internal network. The circuit level gateway checks the legitimacy of the connection, and if it is legitimate, then relays packets between the two networks. Circuit level gateways typically do not have any knowledge of the application protocol, and exhibit weaker authentication than an application level gateway. In contrast to application gateways, a circuit level gateway is totally transparent to the user, on the condition that he uses a specially modified client. They are therefore most suitable for controlling out-bound traffic. One popular means of creating a circuit level gateway is to use the public domain SOCKS package, with the software residing on a Bastion Host.

(c) Application level gateways are proxying firewalls which mediate access at the level of TCP/IP applications (e.g. FTP, SMTP), and are thus able to exert a much finer granularity of control than either packet filters or circuit level gateways. Therefore, a different proxy must be developed for each application, and that proxy may always be transparent to the user (e.g. he may have to connect to the firewall itself, then request an onward connection to the destination host). An application level gateway is typically implemented on a Bastion Host.

Advantages

- simple proxy, which is more verifiable than whole application
- finer granularity of filtering
- network address translation (NAT)
- logging and alarm capability
- stateful
- strong authentication of clients

Disadvantages

- applications limited by proxy availability
- proxy may not be transparent to user or application
- administrative burden
- may be running on a complex operating system, prone to bugs

d) Screens filter packets but operate at the data link layer, thus have no IP address and are not visible to attackers. How much of incoming packets are examined depends upon the product.

For maximum security and flexibility, a combination of such devices is usually required. For example, initial checks on incoming traffic can be handled by a packet filtering router, and a bastion host can provide application level checks of particular protocols and services. Outgoing traffic can be mediated using a circuit level gateway. However, most modern firewall products now combine many of the services traditionally provided by packet, circuit and application level gateways in one box. Such hybrid devices may either implement a mixture of packet filtering and proxying functionality (filtering on all open ports but providing proxies for specific applications), or may implement an extended form of packet filtering where application data is examined as well as address and port number.

Note: the CyberGuard Firewall is a combination of a packet level firewall and application level gateway (router).

See Bastion Host, Proxy Service, Screening Router.

Gateway: See Firewall. Note: In the United States a Router is referred to as a Gateway.

Guard: A Guard is a device that controls information flow between networks operating at differing protective marking levels. Some Guards only allow information to flow one way, from the network with a low or no protective marking to a network with a higher marking. Others act on security labels attached to each piece of information, and allow certain pieces of information to flow from the highly marked network to the lowly marked network in a controlled manner - i.e. the highly marked network is treated as a multi-level network.

A guard can be viewed as a particularly specialised type of firewall. Also see Mail Guard.

Internet Protocol (IP):

The Internet Protocol is designed for use in systems of packet-switched computer networks. IP transmits blocks of data called datagrams from sources to destinations, where both the sources and destinations are identified by fixed length addresses. IP also provides fragmentation and reassembly facilities for datagrams that are too long to be passed through networks that can only process smaller packet sizes. Datagrams are passed, by use of the Internet (IP) Address, from one router to another until they reach their destination.

IP contains no mechanisms to improve end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. IP treats each Datagram as independent from any other Datagram. There are no connections or logical circuits (virtual or otherwise).

IP Router: An IP Router is a standalone hardware device, or host, whose sole function is to route IP packets according to its internal configuration ("filtering") rules. By configuring an IP router appropriately, the Internal Masquerade variant of IP Source-Address Spoofing attacks can be prevented. Note: In the United States a router is referred to as a gateway.

IP Source-Address Spoofing Attacks:

IP Source-Address Spoofing is a method of attacking a network's trust relationships. To launch the attack, IP packets are created by hand with incorrect source addresses. The source addresses inserted into the packets are based on the addresses used in the trust relationships on the network being attacked. The aim of the attack is for a host on the network to believe the source address and to act on the contents of the packets. Such packets often change routing tables, or request information about the internal structure of the network. There are two types of IP Source Address Spoofing attacks, as described below.

(a) Internal Masquerade Variant:

In an Internal Masquerade attack, an attacker forges IP packets to claim that they are from a host on the network being attacked. A suitably configured router can prevent such attacks. This attack is often combined with a TCP Sequence Number Prediction Attack to hijack an established TCP connection, and the Loose-Source Routing option of IP.

(b) External Masquerade Variant:

In an External Masquerade attack, an attacker forges IP packets to claim that they are from another host on the Internet. i.e. The Time Server that your site uses, or an Internet DNS Server. This type of attack cannot be prevented without cryptographic mechanisms providing strong authentication and connection integrity between your site and the hosts you wish to communicate with, and these mechanisms are not supported between standard Internet hosts.

IP Tunnelling (Defensive):
IP Tunnelling is a method of passing a particular protocol through a Bastion Host without the Bastion Host providing a Proxy-Service. When a connection request arrives at the Bastion Host it is redirected to another host to be actioned.

IP Tunnelling (Offensive):
IP Tunnelling is a method that an attacker may use to pass information through a firewall. If an attacker can find a suitable internal host, such as one running the Mbone protocol, it can pass messages to it, to try and persuade the host to run the enclosed information.

Mail Guard
The main purpose of a mail guard is to ensure only authorised information is exported from a system. The mail guard will work in conjunction with the mail application, which will provide security information for each message. The security information provided by the mail application will include security labelling, and the digital signature of the originating user, who will have signed using their secret authentication key. This information will be used by the mail guard to authenticate the user, and check that the information has been authorised, by the user, for release.

Multimedia Internet Mail Extensions (MIME):
An extension to SMTP that allows binary files (containing, for example, executable files, images) to be transported across the Internet.

Network News Transfer Protocol (NNTP):
The Network News Transfer Protocol is a text-based TCP protocol which is used to transfer Usenet news around the Internet. This is essentially a global bulletin board system.

Network Time Protocol (NTP):
NTP is used to synchronise time and co-ordinate time-distribution across the Internet, and is based on the provision of a distributed network of time servers operating in a self-organising hierarchy.

No-Man's Network: A Network which contains no users, but acts as an intermediate buffer area between two networks with different trust levels that have real users.

Post Office Protocol (POP):
The Post Office Protocol provides the SMTP equivalent of the P7 protocol in X.400 Messaging - i.e. it allows a user to access a message stored on a remote host.

Packet filtering gateway: See Firewall.

Proxy-Service: A service provided by a Firewall (usually on the Bastion Host) on behalf of a user on an internal network. For example, a user may wish to use the FTP protocol to transfer files from an external system on the Internet to their local host. The user would request an FTP connection to the external host via the proxy server, and as far as the external system is concerned the request originates at the proxy server - this allows an organisation to hide their internal network structure behind a proxy serving host. The FTP protocol-dialogue would then take place between the proxy-server and the external system. The proxy server would "vet" the incoming data before passing it on to the internal system.

Proxy servers can be used to provide an application level gateway, which unlike a circuit level gateway, does not require the use of modified clients. However, this means that the proxy server may not be fully transparent to the user.

See Firewall.

Screening Router: An IP Router which has been configured to prevent the Internal Masquerade variant of IP Source-Address Spoofing Attacks, and to allow communication between specific sets of hosts. Example, any internal user would be allowed to connect to a Bastion Host, but the Bastion Host would not be able to connect to anything within an internal network. See Firewall, Access Router.

Simple Message Transfer Protocol (SMTP):
The simple message transfer protocol is a text-based TCP protocol which is used for transferring text-only electronic mail messages around the Internet. This protocol is defined in RFC 822.

Simple Network Management Protocol (SNMP):
The simple network management protocol is used to remotely configure and manage network components such as routers, hosts and bridges. Firewall components should not support this protocol.

Transmission Control Protocol (TCP):

TCP is the TCP/IP standard transport level protocol that provides the reliable connection-oriented service on which most applications protocols depend. TCP allows an application program on one machine to establish a virtual connection across the network to an application program on another. TCP includes a protocol port number, to distinguish between multiple application programs on a given remote machine (a particular connection is uniquely identified by the combination of source and destination port numbers, and source and destination addresses). Before transmitting data, participants must establish a connection with each other. All data travels in TCP segments (or packets) that travel across the Internet on IP datagrams. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two fundamental protocols.

TCP Sequence Number Prediction Attacks:

This attack involves the attacker predicting the (supposedly) random sequence number placed on the first TCP packet of a given connection. A good Firewall would have a good random initial sequence number. A typical UNIX operating system increases this number by a fixed amount, making it fully deterministic. These attacks have been seen in use on the Internet.

TCP Session Hijacking Attack:

An attack that allows an attacker to take over an already established TCP session. To the valid user it just appears that the session is lost. These attacks are normally aimed at terminal log in sessions, after the user is authenticated.

User Datagram Protocol (UDP):

UDP is the TCP/IP standard protocol that allows an application program on one machine to send a datagram to an application on another. It uses IP to deliver the datagrams. Like TCP, UDP includes a protocol port number, to distinguish between multiple application programs on a given remote machine. UDP optionally includes a checksum over the data being sent.

UDP delivery is termed "best-effort basis". That is, it does not provide error correction, re-transmission or detection of lost, duplicated or re-ordered packets. However, its overheads are much lower than TCP.

Virtual Circuit: Path established through a network over which a connection is established. In some systems it is possible to have no IP addresses assigned, thereby making the circuit "invisible" to network sniffers (e.g. high-speed collapsed backbone systems). Bastion Hosts and Guards usually use virtual circuits internally to pass information from one network to another.

Virtual Private Network (VPN): Private network, which partly makes use of public network connections (e.g. the Internet). Tunnelling encrypted communications over the untrusted links ensures privacy over the public segments of the network. From the user's perspective, it appears that the entire private network belongs to the organisation.

1.6 Document Layout

IT security functions are assigned a unique reference identifier of the form Name_x to enable ease of reference, where x relates to a sequence in ascending order of that particular category of Security Function. For example, DAC_1, IA_5 and AUD_2.

2. TOE DESCRIPTION

2.1 Introduction

This part of the ST describes the TOE as an aid to the understanding of its security requirements. The scope and boundaries of the TOE are described in general terms both in a physical way (hardware and/or software components/modules) and a logical way (IT and security features offered by the TOE).

2.2 Intended Use

The CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) Firewall is intended for use in organisations that need to safeguard information held on their internal network, by controlling the access that external network users have to that network. The firewall is intended to protect the integrity, availability, authentication data and anonymity of the internal network. The access that internal users have to the external network can also be controlled by CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3).

CyberGuard Firewall provides mediation of network traffic (IP packets). It is able to enforce a number of controls on the traffic (such as denying access, or directing users to an additional identification and authentication process). The controls that are applied are configurable and should be used in accordance with a defined network security policy.

The network security policy should cover all aspects of CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3)’s operation. Specifically, it should cover physical and procedural measures (e.g. location of the firewall hardware in a physically secure area, and rules on which events are to be logged or configured as alerts) in addition to electronic aspects (e.g. guidelines on which internal services are to be accessible from the external network).

It must be emphasised that the definition of the network security policy is likely to be the most important stage in the implementation of the firewall security system. Note also that the network security policy should be defined in accordance with section 2.3 “Evaluated Configurations”, which describes the product set-up and features that may be used within the scope of the evaluation.

There are a number of possible connection topologies for firewalls. A firewall can be multi-homed (multiple network interfaces) or single-homed – which dictates whether all network traffic must pass through the firewall system. Firewalls enforce their security policy using techniques such as IP packet filtering, circuit-level (SOCKS) controls, or application-level proxies – which dictates the granularity of security control that can be imposed upon the network communications.

The CyberGuard Firewall evaluated in this evaluation is a multi-homed configuration providing both IP packet filtering and application-level proxies. CyberGuard Firewall for UnixWare also provides circuit-level (SOCKS) controls, however, this feature of the product is not being evaluated.

In a multi-homed gateway scheme the firewall is connected to two or more networks and is assigned a network address on each. This is illustrated in Figure 1, below, which shows a typical scenario in which CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) is used to protect an organisation's internal network from the Internet.

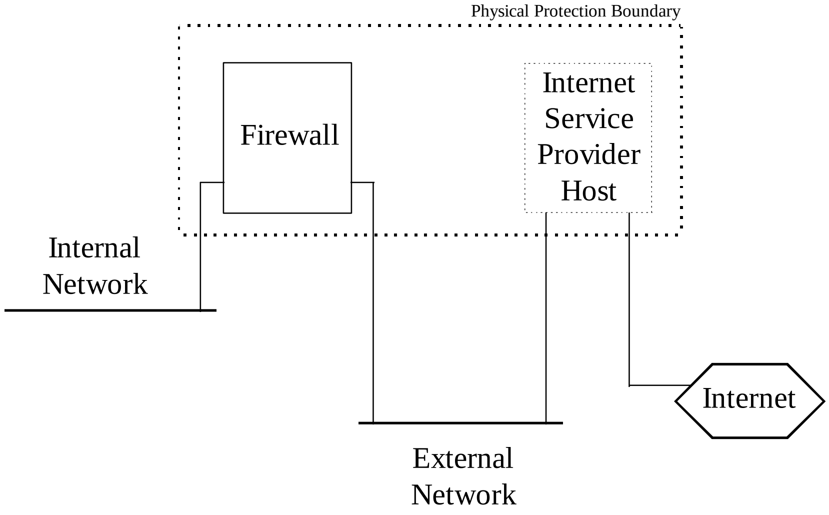

Figure 1 - Typical Internet Firewall Connection

However, this does not demonstrate the full versatility of the product. The internal and external networks can be any networks, which use IP protocol and therefore CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) is equally suited to the implementation of security between departmental networks in a single organisation, or a combination of internal security and protection from the Internet. An example of CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) used between networks in a small systems environment is illustrated in Figure 2 overleaf.

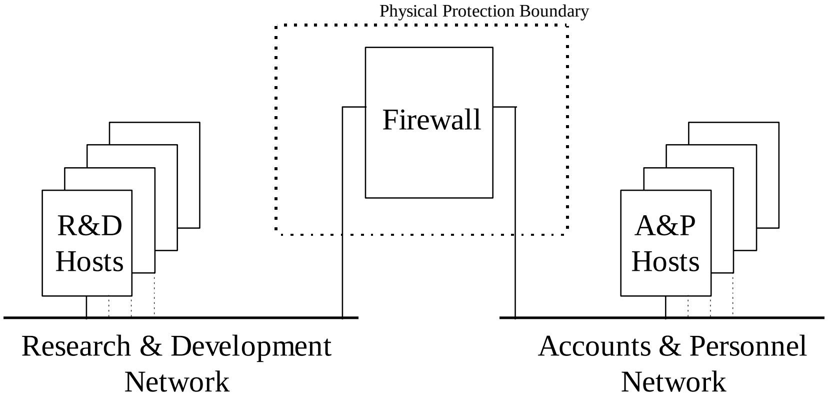
Physical Protection Boundary
Firewall
R&D Hosts
A&P Hosts
Research & Development Network
Accounts & Personnel Network

Figure 2 - Typical Departmental Firewall Connection

The firewall acts as an IP packet filtering gateway, determining the source and destination of every IP packet which attempts to flow across the gateway. It then uses a Rule Set to determine whether any given requested connection should be permitted or denied. This is illustrated in Figure 3. CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) also implements state based logic so that control of the traffic can be performed on a higher 'connection level', hence giving more intelligent mediation than simple IP packet filtering.

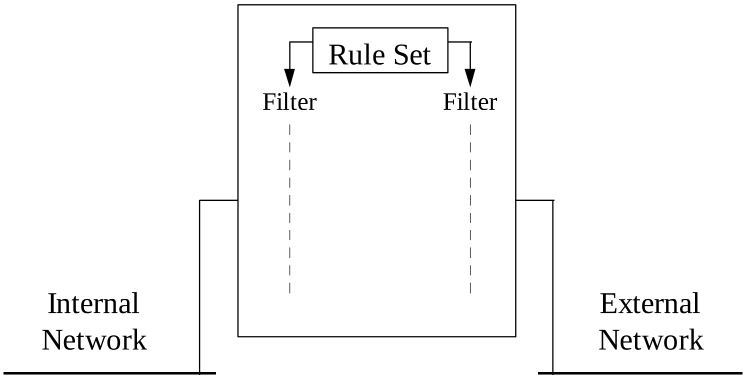

Figure 3 - IP Packet Filtering Gateway

CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) supports TCP/IP, ICMP and UDP protocols, and recognises many standard services such as SMTP, FTP, and Telnet. The Rule Set can permit or deny IP packets from flowing through the gateway, or direct them to a proxy server.

Where proxy access is configured, the firewall will invoke an application on the firewall to mediate the connection. The proxy will usually provide a secondary login facility, and then indirect (but transparent) access to the requested service. Proxy configuration can be unidirectional, so that for example incoming FTP connections to a specific internal host are always handled by a proxy server, but outgoing FTP connections from that host are permitted directly.

The following application proxies are provided by CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) and are part of the TOE: Telnet, FTP (file transfer services), SMTP (e-mail), HTTP (World Wide Web) and NNTP (electronic news). CyberGuard Firewall for UnixWare also provides a proxy for the circuit-level gateway known as SOCKS which can provide additional security to services for which no application proxy is available. SOCKS is not part of the evaluation.

According to specific needs, and the chosen network security policy a major optional feature of CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) may be employed which is having an additional network adapter available. Controls can then be applied at the interface level, giving a finer granularity than simply the distinction between the one internal network and one external network.

2.3 Evaluated Configurations

2.3.1 Hardware and Software

The Target of Evaluation (TOE) is the CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) running on SCO UnixWare version 2.1.3. The evaluated configuration will be the Intel platform (min speed 133MHz) running SCO UnixWare version 2.1.3 and CyberGuard Firewall for UnixWare Release 4.3[2]. This includes the CyberGuard Firewall Appliance Product line, which consists of a series of Intel based platforms running SCO UnixWare 2.1.3 and CyberGuard Firewall Release 4.3. The CyberGuard Firewall Appliance Product line consists of the following products:

FireSTAR is available as a compact 1U size unit and is designed for use in mid-size, growing network environments.

KnightSTAR is available as a 2U or 5U size unit and is designed to provide powerful protection for enterprises, data centres and service providers.

STARLord is available as a 4U size unit and is designed to provide comprehensive security for high-bandwidth data centres, web hosting and ISP/ASP markets.

The system will be connected to an Internet Provider (acting as an external network) and an internal network. Additional hardware includes multiple Ethernet interfaces, a disk storage device, memory, a CD player, and a tape drive. Before CyberGuard acknowledges a platform as being capable for using the CyberGuard Firewall, the platform must pass platform verification. This verification is performed according to CyberGuard's platform compliance and certification process. This is described in [Plat_Comp].

[2] A description of Security Hardening measures can be found in [UWSecHarden].

Although the operating system clearly is a part of the definition of the Target of Evaluation, the security features of the CyberGuard Firewall are being implemented without using known UnixWare specific security measures. We are providing the network security measures independent of the operating system. For the packet filtering process and network address translation, add-ons to the kernel are compiled into the kernel. The UnixWare kernel is changed to call two modules, one for packet filtering and one for address translation. We provide modules for packet filtering and address translation. For the proxies, redirection of IP-packets is performed in our packet filtering modules. All other security measures are applications running independent of the operating system. Issues that play a role obviously are file system controls, user identification and authentication, and network reliability. We make no claims about the security of these modules. Also, the version of UnixWare is not the evaluated version. It is UnixWare version 2.1.3. Our security claims will be only about the CyberGuard Firewall and its modules.

2.3.2 Network Security Policy

In the evaluated configuration the standard supplied hardware and software products must be configured in accordance with a defined network security policy. Services other than those explicitly allowed by the network security policy must not be enabled, so that traffic permitted to flow through the firewall is restricted to that which is authorised.

In defining a network security policy, it is necessary to follow the guidelines provided in [MANUAL M]. In particular that the firewall will be configured so that no direct connections to the firewall are allowed (this refers to connections such as Telnet and FTP sessions, rather than proxy or other services which result from use of the firewall as a Bastion Host).

The recommendations outlined in the CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) Firewall Manual [CGFM] must be followed in addition to the advice given here. These recommendations cover administrative actions ensuring that administration users have passwords assigned, that the passwords are not disclosed, that the system is implemented and tested in incremental stages, and that the audit trail is configured to record invalid IP packets rather than all IP packets.

2.3.3 IP Packet Filtering Rules

The Rule Set must be written as “permit” instructions with the default rule being “deny”. This is the default rule for CyberGuard Firewall. However for administration purposes, the last line in the Rule Set should be “deny ALL EVERYONE EVERYONE”, which specifies that all connections must be denied unless they are expressly permitted. This rule will be present when the firewall is supplied, thereby ensuring that the firewall will behave like an Air Gap until “permit” rules are added.

CyberGuard packet filtering can be configured to disable interface checking by using the NO_IF_CHECK option. This feature should not be used in the evaluated configuration.

2.3.4 Network Address Translation

Network Address Translation (NAT) should be enabled for the external interface only[3]. This ensures that the source address is translated for packets travelling through the firewall from the internal networks.

2.3.5 Auditing

If auditing is on and the audit trail becomes full, then no further auditable actions will be allowed by the TOE. The reason behind this action is to avoid writing over existing records when the audit trail becomes full. This is a configurable option that is specified in the default audit configuration file, **audit**. There are three settings that can be configured when audit trail becomes full. DISABLE (disable auditing), SHUTDOWN (stop network traffic and disable auditing), or EXECUTE (issue a specified command). The default setting is SHUTDOWN, which shuts down network traffic and disables auditing and therefore does not allow any additional auditable actions to take place.

Auditing can be turned off by the administrator using a privileged command, auditoff. This command is not used in the evaluated configuration.

2.3.6 Split Domain Name Server

The [CGFM] provides guidance on how to configure this server. In the evaluated configuration this is enabled with the external server attending to requests from the external network and the internal server attending to requests from the internal network.

2.3.7 Proxies

Proxies are a significant aid to network topology hiding and therefore the use of proxies is recommended if the chosen network security policy defines address hiding to be desirable. A proxy authentication database may also reside on the systems.

Specifically, the following proxies are being used in the evaluation:

- Telnet proxy
- FTP proxy
- SMTP proxy

[3] Network Address Translation can be enabled for both internal and external addresses at the same time. However, doing this causes no packets to travel through the firewall.

- HTTP proxy
- NNTP proxy

The [CGFM] provides guidance on how to configure these proxies. For a minimum security state all five proxies should be enabled and configured to proxy inbound traffic to the firewall and outbound traffic through the firewall[4]. Keep in mind that some of the proxies have features which permit less than secure operation. For instance, some can be configured to allow the client address to be passed (the Pass Client Address option) from an internal network to an external network. Features such as these are not consistent with the evaluated configuration and should not be part of a minimum security state.

2.3.8 Year 2000 Compliance Testing

The evaluated configuration has passed Y2K tests.

2.4 Summary of Security Features

The primary security features of the product are:

- Connection level Access Control for IP packets flowing to or through the firewall. The following controls can be applied: permit/deny source and destination addresses or ports, validate source address against network interface, permit/deny service, time-outs, suppress/allow replies, divert IP packets to a proxy process for additional processing, suppress/allow IP packet forwarding.
- Accounting and auditing of firewall traffic and security related events, plus display of IP packet filtering statistics.
- Alerts (console messages, e-mail, logging, SNMP traps or custom program execution) for significant security related events.
- Address translation facility for internal networks and hosts, hiding the network topology from external users.
- Split domain name server facility, which provides different responses to DNS requests depending on which port the requests are received on.

These features are described briefly in sections 2.4.1. to 2.4.5. In addition to these security features, a range of administration facilities exists for configuring the product.

[4] If Network Address Translation is turned on, the ftp proxy needs to be configured to proxy inbound traffic at the firewall in order to function properly.

2.4.1 Connection Level Access Control

CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) can perform packet filtering based on the source and destination addresses of packets received on the network interfaces. The addresses are determined by extracting the 32-bit IP addresses directly from the “self identifying” headers of IP packets. Controls can be applied in terms of hosts, networks or subnets.

Of greater benefit, the product implements more advanced controls at the connection level. This is facilitated by the maintenance of a list of temporary ‘dynamic rules’, which are updated when connections are established or closed. The dynamic rule base also acts as a rule caching facility, improving firewall performance.

Controls which can be applied to connections are: permit, deny, or redirect to proxy server. In the case of SMTP connections, the provided proxy server re-writes mail headers to hide the internal network topology - this is one of three facilities which can be configured to work together to hide the internal network (see 2.4.4. below). NNTP proxy provides address hiding for news, and HTTP proxy ensures that the appropriate information is displayed for World Wide Web services.

2.4.2 Accounting and Auditing

An audit trail is implemented by CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) for firewall traffic and security related events, in addition to the facilities provided by the operating system. This ensures that a record of all security relevant actions is, or can be, maintained. Individual hosts, networks and events can be selected for review and analysis by the system administrator. Audit output for each auditable event can be sent to any of a number of possible destinations.

2.4.3 Alerts

For significant security related events that should be brought to the attention of an administrator as quickly as possible, CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) may be configured to perform a number of special actions. It can produce an alert message on the system console, send e-mail to an administrator, add a message to a log file, respond to SNMP traps, or execute a custom program.

2.4.4 Address Translation

This facility supports anonymity for internal network hosts. It will re-write IP packet headers so that the real IP addresses of the hosts never appear on the external network. The address translator will instead substitute the address of the firewall, record the state of the connection, and similarly re-route the response IP packet to the originating internal network host.

In this way the translation is transparent. It hides the internal network topology from external examination of the information included in IP packet headers. When used together with proxies (see 2.4.1.) and the Split Domain Name Server facility (see 2.4.5.), the internal network topology will be fully hidden.

2.4.5 Split Domain Name Server

This facility is also used to provide anonymity for internal network hosts. It allows the firewall to respond to host look-up requests differently for each interface defined within the system. For example, returning correct network topology information when DNS requests originate from the internal network, but giving the appearance that all hosts are at a single IP address when requests originate from the external network.

It is therefore able to hide the internal network topology from external users' requests via DNS. When used together with proxies (see 2.4.1.) and the Address Translation facility (see 2.4.4.), the internal network topology will be fully hidden.

2.4.6 Management Interface

CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) should only be managed via a directly connected management console. This interface is a Motif based Windows in GUI front end to the configuration files that are used by the underlying constructs of the CyberGuard firewall, described above. The evaluation covers this interface.

3. TOE SECURITY ENVIRONMENT

3.1 Introduction

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

To this end, the statement of TOE security environment identifies and lists the assumptions made on the operational environment (including physical and procedural measures), states the intended method of use of the product, defines the threats that the product is designed to counter, and identifies the organisational security policies with which the product is designed to comply.

3.2 Environmental and Method of Use Assumptions

3.2.1 Physical

A.PHYSICAL It is assumed that only Firewall Administrators have physical access to the firewall hardware. *(Formerly Assertion_2)*

3.2.2 Personnel

A.TRAIN Firewall Administrators are assumed to be suitably qualified. *(Formerly Assertion_6)*

3.3 Sources of Threats and Methods of Attack

3.3.1 Introduction

The IT assets to be protected comprise the information and resources residing within the internal network. In particular, the integrity, availability, authentication data and anonymity of the internal network is to be protected.

The table below shows the relationship between threat agents (perpetrators), their possible levels of expertise, resources and corresponding levels of motivation to instigate a breach of security for the own purposes.

Table 3.3.1, Potential sources of threats

Threat Agents	*Expertise level*	*Level of Available Resources*	*Motivation level*
Casual browser	Low	None, Ordinary Internet browser (e.g.) Netscape Navigator	None to Low, Non-malicious user, (e.g.) ‘accidental’ hacks
Knowledgeable user	Medium	Medium, Network Knowledge and (e.g.) packet sniffing tools	Low, for ‘fun’ or ‘prestige’
Professional hacker	High	High, Specialist training and (e.g.) Stealth tools	High, Paid for results (e.g.) data harvested

Attacks could potentially be mounted by sources with different levels of opportunity to breach a security policy. Insiders, Outsiders or 3Rd Parties (such as contractors). The Insider would probably be able to mount an attack more easily than an outsider, however it is likely that person would also be easier to detect. Conversely an outside attacker may not be have easy access to a data asset but may be much harder (or perhaps practically impossible) to locate. 3rd Parties would fall somewhere in between with perhaps limited windows of opportunity to do damage.

The table below illustrates attack types correlating them with what event occurs how and the possible consequences of such attacks.

Table 3.3.2, Attack methods, mechanisms and consequences of attacks

Attack Type	*What can happen*	*How it can happen*	*Consequences*
Disclosure of Information	Eavesdropping	A service provider could be breached, or could be run/managed by unprofessional or dishonest people. A disgruntled employee could ‘listen’ to communications on the network.	Proprietary information (e.g. customer information, product specifications, industry pricing model) may end up in the hands of a competitor.
	Password sniffing	A programme which ‘collects’ passwords is installed on a service provider’s computer without	Employees’, managers’, or administrators’ passwords are disclosed, possibly leading to unauthorised

Attack Type	*What can happen*	*How it can happen*	*Consequences*
		their knowledge.	access to systems.
	Accidental disclosure	An employee inadvertently sends a highly confidential electronic mail message to a wide distribution over the Internet (e.g. a newsgroup, or an electronic mailing list).	Proprietary information is disclosed to the public, leading to a loss of competitive advantage and/or reputation.
Unauthorised access to systems and applications	Internal systems are breached	A hole in gateway software could be exploited (e.g. WWW server, electronic mail gateway). User passwords can be stolen or guessed.	Systems could be brought down. All data and applications could be modified or erased. Information can be stored on the system by the 'hacker'. Systems could be modified to foil recovery attempts.
	Spoofing	A third party can impersonate trusted user and act with that user's privileges in order to gain access to a system.	As above. Communications could be diverted to a third party, e.g. a competitor or the press. 'Viruses' or 'Trojan Horses' could be planted in the system to restrict the ability of the organisation to 'see' or investigate the attacker.
	Attack on other systems launched	Attacks on other organisations are launched from an internal system, by either an intruder or an unscrupulous insider.	Legal and financial liability. Loss of public confidence. Damage to reputation.
Loss of information	Modification of data in transit	Message contents are 'eavesdropped', altered, and	Diversion of funds.

Attack Type	*What can happen*	*How it can happen*	*Consequences*
integrity		retransmitted.	Modification of contracts or transactions. Misrepresentation of an organisation.
	Modification of data on a system	Unauthorised access as a privileged user. Introduction of viruses.	False information given to partners/clients. Damage or destruction of data. Alteration of file contents on a system.
Denial of service	Packet storms	A large quantity of data is sent to a computer which must process it. The computer can not do anything else during this time. A network is deliberately flooded with extraneous information. Due to its limited capacity, it cannot transmit valuable information.	Inability to conduct business. Possibility for unauthorised access via ‘spoofing’.
	Network outage	Unauthorised access to a service provider brings down a network.	As above.

3.3.2 Examples of specific technical attack methods

This may include (but is not limited to) the following:

- TFTP daemon attacks: Remote users on the Internet may access world-readable files on an internal network using an unrestricted TFTP service. Thus sensitive files could be retrieved by an adversary on the external side of the firewall.

- IP Spoofing attacks: Firewalls are vulnerable to IP spoofing attacks, including TCP SYN Flooding attacks. Firewalls should have a mechanism to handle SYN Flooding attacks. Firewalls should be capable of preventing traffic from entering the protected local network when packets claim to originate from local network, broadcast network, reserved network, or loopback network addresses.

- UDP attacks: Tools exist to flood UDP ports with packets causing degradation in system performance and increased network congestion. Firewalls must be capable of being configured to filter all UDP services.

3.3.3 Examples of specific exploitable vulnerabilities

- This may include (but is not limited to) the following:

- FTP daemon vulnerabilities: In certain versions of the FTP daemon, a vulnerability exists allowing local and remote users to gain root privileges. This is accomplished through different means for distinct version such as through the signal handling routine increasing process privileges or through exploiting the SITE EXEC command.

- rlogin with TERM environment variable vulnerability: If, during a rlogin attempt on certain vulnerable systems, the buffer containing the value of the TERM environment variable is overflowed, arbitrary code can be executed as root.

  - Telnet Environment Option vulnerability: If the system to which the Telnet connection attempt is directed is running Telnet daemons that are RFC 1408 or RFC 1572 compliant and the system supports shared object libraries then the system may be vulnerable. Both users with and without accounts on the system could become root by transferring environment variables that influence the login program called by the Telnet daemon.

  - ICMP (ping) vulnerability: Large ICMP datagrams may cause systems to crash, freeze, or reboot, resulting in a denial of service.

  - IP loose source route option vulnerability: Firewalls should be capable of rejecting packets that use the IP loose source route option. A TCP connection where the loose source route option is enabled allows an attacker to explicitly route packets through the network to a destination without following the usual routing process. A malicious attacker can pose as a host that is on the return path for this type of TCP traffic since, according to RFC 1122, the traffic must follow the reverse order of the route which it followed from source to destination.

- DNS vulnerabilities: A flood of DNS responses injected into the network could cause a denial of service since the DNS server may become confused. A DNS resolver may check several different levels before checking the correct one. If a host, FOO.BAR.COM, attempts to connect to ONE.TWO, the check will be made first to ONE.TWO.BAR.COM and then to ONE.TWO.COM and finally to ONE.TWO. Thus a malicious host can impersonate a domain that the resolver would encounter before encountering the appropriate level. If an attacker can contaminate a target's DNS responses cache before the call is made, the target can be fooled into believing that the cross-check it performs is legitimate. As a result, the attacker gains access.

3.4 Assumed Threats

In the previous section examples of threat agents and assets were shown. This section formalises the threats into a more focused and concise form.

The assumed threats are listed below.

T1 A connection being established across the firewall between hosts, networks or subnets which can be exploited by an attacker to compromise the assets

T2 A remote connection to the firewall being established which could be exploited by an attacker to compromise the assets. This may range from a single user attempting a simple Telnet session, to a determined attacker using a tool such as SATAN.

T3 An attacker (whether using an authorised path through the firewall or not) makes repeated attempts to compromise the assets, and eventually succeeds without being detected.

T4 An attacker compromises the assets by exploiting the use of tools which contain known security faults (such as e-mail, news and FTP applications).

T5 An unauthorised user gaining access to a system on an opposing side of the firewall, by sending an IP packet with a fake source address.

It is envisaged that the attacker may use the IP protocol Source Routing option to ensure that other systems in the Internet route the IP packet according to the attacker’s wishes, but this is not assumed by this threat.

T6 A host on the internal network being configured insecurely, or being vulnerable to exploitation of faults in the protocol stacks of the services which it provides.

3.5 Organisational Security Policies

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

4. SECURITY OBJECTIVES

4.1 Security Objectives to be met by the TOE

The CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) product is intended to satisfy a number of security objectives. The following security objectives relate to the firewall software and the IP traffic processed by the firewall. These objectives will form the basis for the evaluation:

O.CONTROL The firewall must ensure that services which are available on either the internal or external network are accessible to users on the opposite side of the firewall if and only if the firewall has been configured to allow the access.

O.PROXY The firewall must invoke a proxy to mediate all access to the services that are configured on the firewall to be accessible via proxy, and must provide where appropriate (in conjunction with the environment) the means to identify and authenticate users before access is permitted.

O.NETHIDE The firewall must provide the means to hide the internal network topology from external attackers.

O.AUDIT The firewall, in conjunction with the underlying operating system, must provide a means of recording information about the IP packets flowing through the firewall.

4.2 Security Objectives to be met by the TOE Environment

O.ADMIN The underlying operating system shall ensure administration facilities for the configuration of the host and rule databases are only available to Firewall Administrative Users.

O.AUDIT The firewall, in conjunction with the underlying operating system, must provide a means of recording information about the IP packets flowing through the firewall.

This security objective is repeated for the environment in accordance with [CC1, C.2.5].

O.AUDITMAN Procedures shall exist to ensure that the audit trails are regularly analysed and archived. *(Formerly Assertion_3)*

O.EXTMASQ Those responsible for the TOE shall accept the risk posed by External Masquerade attacks.

This type of attack cannot be prevented without cryptographic mechanisms providing strong authentication and connection integrity between the internal network and hosts on the external network with which communicate is required. Such mechanisms are not supported between standard Internet hosts.

O.IMU The firewall will be configured in accordance with the Evaluated Configuration section of the Security Target, and with the chosen network security policy. No optional features shall be enabled unless recommended in the Evaluated Configuration.

O.NSP Those responsible for the TOE shall define a network security policy prior to any attempted installation or implementation of the firewall. The network security policy shall cover physical and procedural measures in addition to electronic issues. The network security policy shall be reviewed and revised according to the perceived needs.

O.PHYSICAL Those responsible for the TOE shall establish appropriate measures and procedures to ensure that only Firewall Administrative Users have physical access to the firewall hardware. *(Formerly Assertion_2)*

O.REMOTE Firewall Administrators should NOT use a privileged account for remote proxy authentication.

This eliminates the possibility of the privileged passwords being detected using network sniffers.

O.TRAIN Firewall Administrators should have received training, taken a course in firewall administration, or something equivalent. *(Formerly Assertion_6)*

5. SECURITY REQUIREMENTS

5.1 TOE Security Functional Requirements

In the specification of SFRs within this section the following notation is used:

- *italicised text* is used to denote the completion of an assignment or selection operation on a functional component

- **emboldened text** is used to denote the refinement of a functional component.

5.1.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the *Firewall Information Flow Control Policy* on:

a) subjects: external IT entities that send and receive information through the firewall to one another

b) information: traffic sent through the TOE from one subject to another

c) operation: pass information.

5.1.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the *Firewall Information Flow Control Policy* based on at least the following types of subject and information security attributes:

a) subject security attributes:

- *presumed address;*

b) information security attributes:

- *user identity;*
- *presumed address of source subject;*
- *presumed address of destination subject;*
- *transport layer protocol;*
- *TOE interface on which traffic arrives and departs;*
- *service; i.e. FTP, Telnet, SMTP, DNS, NNTP, HTTP*
- *security-relevant service command.*

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

a) *subjects can cause information to flow through the firewall to another connected network only if the rules specified by the authorised administrator unambiguously permit such information flow, based on the information security attributes; and*

b) *the connection is via a proxy service, if this is required by the administrator-specified rules.*

FDP_IFF.1.3 The TSF shall enforce the following *additional information flow control rules*:

a) *if an FTP service is permitted via proxy, then users of the service will be subject to the access rights configured in the FTP Proxy Database;*

b) *it shall be possible to range restrict the service port to be the same as that of the destination port;*

c) *it shall be possible to enable the reply path for a limited period for specified rules.*

FDP_IFF.1.4 The TSF shall provide the following *additional capabilitie*s *to ensure addresses and names of internal hosts are hidden*:

a) *If optionally enabled, the external name server processes requests to and from the external network.*

b) *If optionally enabled, the internal name server processes requests to and from only the internal network and can make requests to the external name server, subject to Rule c)**.***

c) *When configured for address translation the TOE will re-write the headers of IP packets flowing from the internal network to the external network, so that the real addresses of internal hosts are hidden.*

d) *When the SMTP proxy is enabled the TOE will re-write the headers of mail messages flowing through it, so that the real addresses of internal hosts are hidden.*

e) *The TOE will correctly re-route incoming mail (arriving on the external interface) for hosts which are hidden (connected to the internal TOE interface).*

f) *If the NNTP proxy is enabled the TOE will re-write the headers of news messages flowing through it.*

g) *The TOE will ensure that appropriate information is displayed for internal World Wide Web type documents.*

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

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

a) *The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network.*

b) *The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network.*

Application Note: The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a "presumed address" is used to identify source and destination addresses. A "service", listed in FDP_IFF.1.1(b), could be identified, for example, by a source port number and/or destination port number.

5.1.3 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing use of any **Telnet or FTP functions** on behalf of that user.

Application Note: This component has been refined to replace 'other TSF-mediated functions' with 'Telnet or FTP functions'.

5.1.4 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing use of any **Telnet or FTP functions** on behalf of that user.

Application Note: This component has been refined to replace 'other TSF-mediated functions' with 'Telnet or FTP functions'.

5.1.5 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.

5.1.6 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 as listed below:*

- *network access attempts that were denied*
- *interface spoofing attempts*
- *network access attempts that failed to match an IP packet filter rule*
- *network access attempts that were permitted due to a network configuration rule*
- *traffic flow in terms of IP address, port, bytes sent/received*

c) *All auditable events as listed below:*

- *attempts to forward IP packets through the firewall when configured as a Bastion Host*
- *attempts of external systems to scan the firewall ports.*

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.

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, other audit relevant information *as specified below:*

- *For the events listed in FAU_GEN.1.1b): Identification of the physical port on which the IP packet was received or transmitted; source IP address of the IP packet; destination IP address of the IP packet; protocol name; source port; and destination port.*

Application Note: The outcome (success or failure) of an event is to be recorded explicitly only where applicable to the event.

5.1.7 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide the *Firewall Administrator* with the capability to read *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.

5.2 Strength of Function

The claimed SoF rating for this TOE is *SOF-Medium*.

5.3 TOE Security Assurance Requirements

The target evaluation assurance level for the product is EAL4 [CC]. The evaluation assurance level has been augmented by addition of the CC class ALC_FLR. This requires definition of procedures and mechanisms employed by CyberGuard to address any security flaws, vulnerability reports or functional problems with the product.

5.4 Security Requirements for the IT Environment

The IT environment (i.e. the underlying operating system) is required to provide:

- protected permanent storage of the audit trails generated by the firewall, and also provide reliable timestamps in support of auditing (O.AUDIT);
- identification and authentication in support of FTP and Telnet authentication (O.PROXY);
- the means to ensure that only Firewall Administrators are able to access facilities for the configuration of the host and rule databases (O.ADMIN).

As a minimum, therefore, the following security functional requirements are to be satisfied by the IT environment.

Table 5.4: SFRs on the IT Environment

SFR	***SFR Description***
FAU_STG.1	Protected audit trail storage
FPT_STM.1	Reliable time stamps
FMT_MSA.3	Static attribute initialisation
FMT_MSA.1	Management of security attributes
FMT_SMR.1	Security roles
FIA_UID.2	Timing of identification
FIA_UAU.2	Timing of authentication

6. TOE SUMMARY SPECIFICATION

6.1 IT Security Functions

Listed below are the IT Security Functions (SFs) provided by the TOE. The are grouped in under the three categories of:

- Identification and Authentication,

- Discretionary Access Control and

- Accountability and Audit.

6.1.1 Identification And Authentication

IA_1: CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) will, by default configuration, discard all IP packets which are received on a network interface other than that which is implied by their source address.

IA_2: CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) proxy servers for Telnet and FTP provide user identification and authentication through interfaces to the underlying operating system. This IT security function assumes that the interfaces are correctly implemented by the underlying operating system.

IA_3: When configured for address translation, CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) will re-write the headers of IP packets flowing from the internal network to the external network, so that the real addresses of internal hosts are hidden.

IA_4: When the Split Domain Name Server facility is enabled, CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) will respond to DNS requests differently for each defined network interface. The External name server processes requests to and from the external network. The Internal name server processes requests from only the internal network. The Internal name server can make requests to the external name server.

N.B. IA_3 provides hiding of addresses and names of the internal network.

IA_5: If the SMTP proxy is enabled, CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) will re-write the headers of mail messages flowing through the firewall, so that the real addresses of internal hosts are hidden. CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) will correctly re-route incoming mail for hosts which are hidden.

If the NNTP proxy is enabled, it will perform similar header re-writing on news messages flowing through the firewall. If the HTTP proxy is enabled, it will ensure appropriate information is displayed as defined in the **httpd-proxy.conf** file for internal World Wide Web documents.

6.1.2 Discretionary Access Control [5]

DAC_1: The product shall be able to correctly determine which rule from the Rule Set should be applied to all IP packets. For every IP packet the rule applied shall be the first found in the dynamic rule base or the Rule Set which matches the source, destination, service, and protocol characteristics of a given IP packet.

DAC_2: The IP packet sources and destinations which can be specified for each rule in the Rule Set (and enforced by the product) may be any pair-wise combination of the following:

a) an individual user-defined host, network or subnet (can be an internet address in dotted quad notation, a host from the Host Database, or a network/subnet mask pair).

b) membership of a group identified by the keywords INTERNAL_INTERFACES (all traffic via internal network interface), EXTERNAL_INTERFACES (all traffic via external network interface), ALL_EXTERNAL, ALL_INTERNAL, or EVERYONE (all hosts);

c) the firewall, referred to using the identifier FIREWALL or LOCAL_HOST *(maintained for backward compatibility)*

d) all traffic via a specific port, specified by an identifier of the form interface_NETWORK, or using the keyword interface_IPADDRESS to refer to the IP address of a specific interface.

DAC_3: The IP packet services and protocols which can be specified for each rule in the Rule Set (and enforced by the product) may be any one of the following:

[5] More optional keywords are available than are covered by the Security Functions. Those which are not covered are not under evaluation. They are not included in the CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) Evaluated Configuration.

a) a specific recognised service or service/protocol pair defined in the Service Database. If the service is ambiguous, because it is defined for more than one protocol, then the protocol must be specified explicitly;

b) membership of a group identified by the keyword ALL (all services), or the combination ALL/protocol (which specifies any service that uses a given protocol). The protocol may be numeric or one from the Protocol Database;

c) an identifier of the form icmp_type/ICMP, denoting internet control messages.

DAC_4: The IP packet controls which can be specified for each rule in the Rule Set (and enforced by the product) may be any one of the following:

a) the identifier ‘permit’, which shall allow the specified connection to take place. If applied to a TCP/IP protocol then the reply path will also be enabled;

b) the identifier ‘deny’, which shall prevent the specified connection from taking place;

c) the identifier ‘proxy’, which shall allow the specified connection to take place only via a proxy service provided by the firewall;

DAC_5: If an FTP service is permitted via proxy, then users of the service will be subject to the access rights[6] configured in the FTP Proxy Database.

DAC_6: If the symbol ‘=’ appears before the service component in any rule then the service port shall be range restricted to be the same as that of the destination port.

DAC_7: If the identifier ‘enable_reply’ appears after any rule then the operation of a rule shall be modified such that the reply path is enabled (for a limited time). Note that:

a) the time-out period will be determined by the status of the connection.

b) if attached to a deny rule, then the firewall will generate a return IP packet which indicates that the destination is unreachable.

[6] FTP proxy access rights are enforced at the granularity of a single user. The enforceable rights are denoted by identifiers such as DELE, STOR, and CWD. The full list of rights is listed on the ftpd-proxy(1M) manual page.

6.1.3 Accountability and Audit

AUD_1: The product shall contain an accountability component which is able to log security relevant events relating to IP traffic to or through the firewall. This SF assumes that the underlying operating system interfaces that are utilized are correctly implemented by the underlying operating system. The following logs will be maintained by the product:

ForwardD Lists attempts to forward IP packets through the firewall when configured as a Bastion Host.

NetguardD Lists the network access attempts that were denied.

NetguardI Lists interface spoofing attempts.

NetguardM Lists network access attempts that failed to match an IP packet filter rule.

NetguardP Lists network access attempts that were permitted due to a network configuration rule.

NetguardS Summary of the following logs: ForwardD, NetguardD, NetguardI, NetguardM and NetguardP; i.e. all IP Events.

NetguardT Lists traffic in terms of IP address, port, bytes sent/received, and number of IP packets.

Portscan Lists attempts of external systems to scan the firewall ports.

AUD_2: The following data, when CyberGuard Firewall is configured to not overwrite audit files, is always recorded in each audit log listed in SF AUD_1:

Date; time; record type (records success or failure of the attempts, or other special conditions).

The network logs contain the following information:

Identification of the physical port on which the IP packet was received or transmitted; source IP address of the IP packet; destination IP address of the IP packet; protocol name; source port; and destination port.

AUD_3: There exists documented tools to maintain the accountability files and examine the files for the purposes of audit.

AUD_4: It is possible to configure the Rule Set such that the operation of a rule is modified by the following optional identifier: dont_audit. This overrides AUD_1, preventing an IP Event from being recorded in the audit log.

6.2 Required Security Mechanisms

No specific security mechanisms are mandated by this security target.

6.3 Assurance Measures

The assurance requirements for EAL4 and their corresponding assurance measures which satisfy them are tabulated below.

Table 6.3: Assurance measures:

Assurance class	*Assurance components*	*How satisfied*
Configuration Management	**ACM_AUT.1** Partial CM automation	Configuration Management Plan and Procedures will be provided.
Configuration Management	**ACM_CAP.4** Generation support and acceptance procedures	Configuration Management Plan and Procedures will be provided.
Configuration Management	**ACM_SCP.2** Problem tracking CM coverage	Configuration Management Plan and Procedures will be provided.
Delivery and Operation	**ADO_DEL.2** Detection of modification	Delivery Procedures will be provided.
Delivery and Operation	**ADO_IGS.1** Installation, generation, and start-up procedures	CyberGuard Firewall Administrators Manual will be provided.
Development	**ADV_FSP.2** Fully defined external interfaces	CyberGuard Firewall Functional Specification will be provided.
Development	**ADV_HLD.2** Security enforcing high-level design	High Level Design will be provided.
Development	**ADV_IMP.1** Subset of the implementation of the TSF	Source code will be provided.

Assurance class	*Assurance components*	*How satisfied*
Development	**ADV_LLD.1** Descriptive low-level design	Low Level Design will be provided.
Development	**ADV_RCR.1** Informal correspondence demonstration	This will be provided within the design documentation.
Development	**ADV_SPM.1** Informal TOE security policy model	This will be satisfied by the CC Security Target
Guidance documents	**AGD_ADM.1** Administrator guidance	CyberGuard Firewall Manual will be provided.
Guidance documents	**AGD_USR.1** User guidance	CyberGuard Firewall Manual will be provided.
Life cycle support	**ALC_DVS.1** Identification of security measures	Developer Security Procedures will be provided.
Life cycle support	**ALC_LCD.1** Developer defined life-cycle model	Definition of Life-cycle model will be provided.
Life cycle support	**ALC_TAT.1** Well defined development tools	List of development tools and Languages will be provided.
Tests	**ATE_COV.2** Analysis of coverage	Developer’s Tests will be provided.
Tests	**ATE_DPT.1** Testing: low-level design	Test Coverage Analysis will be provided.
Tests	**ATE_FUN.1** Functional testing	Developer’s Tests will be provided.
Tests	**ATE_IND.2** Independent testing - sample	TOE will be provided for testing
Vulnerability assessment	**AVA_MSU.2** Validation of analysis	Misuse Analysis will be provided.
Vulnerability assessment	**AVA_SOF.1** Strength of TOE security function evaluation	Strength of Function Analysis will be provided.

Assurance class	*Assurance components*	*How satisfied*
Vulnerability assessment	**AVA_VLA.2** Independent vulnerability analysis	Operational and Construction Vulnerability Analysis will be provided.
Flaw Remediation	**ALC_FLR** Flaw Remediation Procedures	Flaw Remediation Procedures will be provided.

A SECURITY TARGET RATIONALE

This annex provides the ST rationale which is divided into the following sections:

- security objectives rationale
- security requirements rationale
- TOE summary specification rationale.

A.1 Security Objectives Rationale

This annex presents the security objectives rationale, showing how each of the threats enumerated in section 3.3 are countered by the security objectives (in sections 4.1 and 4.2), and also how each of the assumptions enumerated in section 3.2 are upheld by the security objectives.

The approach taken is first to show the correlation of the security objectives to threats and assumptions in tabular form. This is then followed by a justification of why the security objectives are suitable to counter the threats and uphold the assumptions.

Table A.1.a: Threats' correlation with Security objectives:

Threats		TOE Objectives	Environment Objectives
T1	A connection being established across the firewall between hosts, networks or subnets which can be exploited by an attacker to compromise the assets.	O.CONTROL O.PROXY O.NETHIDE	O.EXTMASQ
T2	A remote connection to the firewall being established which could be exploited by an attacker to compromise the assets.	O.CONTROL O.PROXY	O.EXTMASQ O.REMOTE
T3	An attacker (whether using an authorised path through the firewall or not) makes repeated attempts to compromise the assets, and eventually succeeds without being detected.	O.PROXY O.NETHIDE O.AUDIT	O.AUDITMAN O.REMOTE
T4	An attacker compromises the assets by exploiting the use of tools which contain known security faults (such as e-mail, news and FTP applications).	O.CONTROL O.PROXY O.NETHIDE	
T5	An unauthorised user gaining access to a system on an opposing side of the firewall, by sending an IP packet with a fake source address.	O.CONTROL O.PROXY O.NETHIDE	O.EXTMASQ
T6	A host on the internal network being configured insecurely, or being vulnerable to exploitation of faults in the protocol stacks of the services which it provides.	O.CONTROL O.PROXY	O.EXTMASQ

In addition to the specific correlation given in the above table, O.ADMIN, O.IMU, O.NSP, O.PHYSICAL and O.TRAIN are of global importance. They are required to counter all threats, because they relate to the integrity of the firewall, CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3)'s system files, and the correct configuration of the product in accordance with the chosen network security policy. In order to avoid clutter, these assertions are not explicitly listed against the threats unless they specifically relate to an aspect of the threat.

The justification of the suitability of the security objectives to counter the threats is as follows.

T1 A connection being established across the firewall between hosts, networks or subnets which can be exploited by an attacker to compromise the assets.

This threat is countered by the security objective O.CONTROL which imposes controls on permitted connections to or through the firewall. All requested connections are received in the form of IP packets, and therefore the controls operate by examining the IP packets and denying connections if necessary.

O.CONTROL states that the appropriate rule from the Rule Set will always be applied. If no matching rule is found then access will be denied due to the inclusion of the last rule "deny ALL EVERYONE EVERYONE" as required by the evaluated configuration (O.IMU).

If proxy controlled access is configured, then O.PROXY will ensure that the user is identified and authenticated before access is permitted.

O.NSP provides essential support by ensuring that a network security policy is defined which will identify which connections can be permitted without placing assets on the internal network at risk.

These measures therefore ensure that the network security policy for connections is enforced, provided that the IP packets correctly identify their source and destination. Unfortunately, no method for preventing IP packets from containing fake addresses is currently employed in standard IP protocols, and therefore this residual risk has to be accepted in accordance with O.EXTMASQ. See T5, below, for further discussion of this deficiency in the IP protocol.

T2 A remote connection to the firewall being established which could be exploited by an attacker to compromise the assets.

This threat is similar to T1, but involves an attack on the firewall itself. It is countered by the same security objectives as T1, i.e. O.CONTROL and O.PROXY together with acceptance of the residual risk from External Masquerade attacks (O.EXTMASQ).

O.NSP provides essential support by ensuring that a network security policy is defined which will identify which connections can be permitted without placing assets on the internal network at risk.

The TOE objectives address all aspects other than access to the firewall through the Administration Port. This aspect of T2 is controlled by physical measures as directed by O.PHYSICAL.

T3 An attacker (whether using an authorised path through the firewall or not) makes repeated attempts to compromise the assets, and eventually succeeds without being detected.

This threat is countered by O.AUDIT which provides the capability to audit the attacker's attempts at defeating the security objectives. This objective is provided by the TOE in conjunction with its IT environment. Supporting O.AUDIT is O.AUDITMAN which states the requirement for an administrator to check the audit log. The attack is therefore both recorded and brought to the attention of an administrator, and therefore the threat is countered.

O.REMOTE reduces the risk of successful undetected attack based on the detection of privileged passwords using network sniffers.

T4 An attacker compromises the assets by exploiting the use of tools which contain known security faults (such as e-mail, news and FTP applications).

This threat is countered by O.PROXY which provide for the introduction of proxies. Proxies provide an additional layer of security and/or authentication. They run on the firewall, forming a first contact with an external user. The proxy will determine whether the user is to be allowed access to an internal service and then connect and mediate access to the service.

The proxy therefore handles identification, authentication and other security controls irrespective of any known faults of the internal services, preventing the internal service faults from being exploited.

Note that the use of proxies for these services is optional - this threat therefore will not be countered unless the chosen network security policy indicates that the firewall should be configured for proxy access to all internal network services (O.NSP).

T5 An unauthorised user gaining access to a system on an opposing side of the firewall, by sending an IP packet with a fake source address.

The threat of IP source-address spoofing is countered by O.CONTROL which ensures that IP network interface spoofing attempts are countered, by discarding all traffic which is received on one network interface, but claims (in its IP source address) to have come from another. This is a common form of attack which is effectively countered by refusing to process any such traffic.

It is accepted, however, that whilst this case is fully countered by O.CONTROL, the definition of the IP protocol does not allow for the detection of IP source-address spoofing in the case that a host issues IP packets claiming to be from another host on the same network interface. This case cannot be countered by any firewall, because there is no known defence. Therefore, it is necessary to accept this residual risk as described in O.EXTMASQ.

T6 A host on the internal network being configured insecurely, or being vulnerable to exploitation of faults in the protocol stacks of the services which it provides.

This threat describes the need for a migration of the responsibility for network security from the hosts on an internal network to the firewall. It encapsulates both the convenience of a single point at which the network security policy can be implemented (O.NSP), as well as the hiding of vulnerabilities that individual hosts may otherwise exhibit (due to faults in applications or errors in configuration).

To achieve this, CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) implements the IP protocol and proxy controls in accordance with O.IMU and O.PROXY. The residual risk posed by External Masquerade attacks has to be accepted as described by O.EXTMASQ.

In addition, O.NETHIDE provides defence against attackers by hiding the internal network topology from external users. This prevents an attacker from gaining vital information about the network and very much reduces the chance of any form of attack on an internal host being successful. This objective covers all of the methods that an attacker can use to discover the information, so long as internal network services are made available by proxy only, in accordance with O.IMU.

The justification of the suitability of the security objectives to satisfy the assumptions is as follows:

Table A.1.b: Showing the correlation of Assumptions with Objectives:

Assumptions	*Objectives*
A.PHYSICAL	***O.PHYSICAL***
A.TRAIN	***O.TRAIN***

The mapping between assumptions and objectives is straightforward, and it is clear from the definition of the objectives that they directly uphold the relevant assumption.

A.2 Security Requirements Rationale

A.2.1 Security Functional Requirements Suitable to Achieve the Security Objectives

This section provides the correlation and justification of suitability between the objectives and the Security Functional Requirements. The approach taken is first to show the correlation of the SFRs to the security objectives. This is then followed by a justification of why the SFRs are suitable to achieve the security objectives.

Table A.2.1: Correlation of Security Objectives with SFRs.

Security Objective for the TOE		SFR
O.CONTROL	The firewall must ensure that services which are available on either the internal or external network are accessible to users on the opposite side of the firewall if and only if the firewall has been configured to allow the access.	FDP_IFC.1 FDP_IFF.1 FIA_UID.2 FIA_UAU.2 FPT_RVM.1
O.PROXY	The firewall must invoke a proxy to mediate all access to the services that are configured on the firewall to be accessible via proxy, and must provide where appropriate (in conjunction with the environment) the means to identify and authenticate users before access is permitted	FDP_IFC.1 FDP_IFF.1 FIA_UID.2 FIA_UAU.2 FPT_RVM.1
O.NETHIDE	The firewall must provide the means to hide the internal network topology from external attackers.	FDP_IFF.1
O.AUDIT	The firewall, in conjunction with the underlying operating system, must provide a means of recording information about the IP packets flowing through the firewall.	FAU_GEN.1 FAU_SAR.1

The justification of the suitability of the SFRs to achieve the security objectives by the TOE is as follows.

O.CONTROL	The firewall must ensure that services which are available on either the internal or external network are accessible to users on the opposite side of the firewall if and only if the firewall has been configured to allow the access.

FDP_IFF.1 describes the general behaviour of CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3), stating that the appropriate rule from the Rule Set will always be applied.

FDP_IFF.1.1 describes the different IP packet sources and destinations for which connections can be controlled, and also describes the different protocols and services for which connections can be controlled.

FDP_IFF.1.2 describes the controls that can be applied. Connections can be denied if required by the chosen network security policy. Connections can be permitted where allowed by the chosen network security policy.

FDP_IFF.1.3 will also ensure that the connections are also restricted to a specific port, if so required by the network security policy.

FDP_IFC.1 describes the general way in which the TOE will behave with respect to the information flow control policy.

FDP_IFC.1.1 identifies what attributes (subjects, information & operation) the TOE uses to make decisions to apply the information flow control policy.

FIA_UID.2 describes TOE actions with respect to identification of users.

FIA_UID.2.1 specifically identifies that the Telnet and FTP functions require users to be identified before they are able to use those functions.

FIA_UAU.2 describes TOE actions with respect to authentication of users.

FIA_UAU.2.1 specifically identifies that the Telnet and FTP functions require users to be authenticated before they are able to use those functions.

FPT_RVM.1 describes the non-bypassability of the TOE functionality.

FPT_RVM.1.1specifically ensures that the TSP enforcement functions are operating as required and terminate legally and gracefully before other functions within the TSC can proceed.

O.PROXY	The firewall must invoke a proxy to mediate all access to the services that are configured on the firewall to be accessible via proxy, and must provide where appropriate (in conjunction with the environment) the means to identify and authenticate users before access is permitted.

Proxies provide an additional layer of security and/or authentication. They run on the firewall (invoked automatically if the Rule Set indicates “proxy”), forming a first contact with an external user. The proxy will determine whether the user is to be allowed access to an internal service and then connect and mediate access to the service.

The proxy therefore handles identification, authentication and other security controls irrespective of any known faults of the internal services, preventing the internal service faults from being exploited.

FDP_IFF.1 describes the general behaviour of CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3), stating that the appropriate rule from the Rule Set will always be applied.

FDP_IFF.1.1 describes the different protocols and services for which connections can be controlled.

FDP_IFF.1.2 describes the controls that can be applied. Connections are controlled by proxies if required by the chosen network security policy.

If proxy controlled access is configured, then FIA_UID.2 and FIA_UAU.2 will ensure that the user is identified and authenticated before access is permitted.

In addition, FDP_IFF.1 which relates to the SMTP, NNTP and HTTP proxies, helps achieve this objective by avoiding sendmail faults and re-writing information within IP packets. It similarly relates to the FTP proxy, providing additional FTP security in addition to enforcing an additional set of access rights.

FDP_IFC.1 describes the general way in which the TOE will behave with respect to the information flow control policy.

FDP_IFC.1.1 identifies what attributes (subjects, information & operation) the TOE uses to make decisions to apply the proxy mediation rules.

FPT_RVM.1 describes the non-bypassability of the TOE functionality.

FPT_RVM.1.1specifically ensures that the TSP enforcement functions are operating as required and terminate legally and gracefully before proxy functions can proceed.

O.NETHIDE	The firewall must provide the means to hide the internal network topology from external attackers.

CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) is able to defend against attackers by hiding the internal network topology from external users. This prevents an attacker from gaining vital information about the network and very much reduces the chance of any form of attack on an internal host being successful.

The measures implemented to hide the network cover: hiding of e-mail and host addresses by the SMTP and NNTP proxies, hiding of addresses via DNS requests, and the hiding of addresses in IP packet headers. FDP_IFF.1 implements all of this.

FDP_IFF.1 allows CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) to respond to bogus messages with appropriate error messages, in accordance with good network etiquette. This can be used if permitted by the chosen network security policy.

O.AUDIT The firewall, in conjunction with the underlying operating system, must provide a means of recording information about the IP packets flowing through the firewall.

This security objective is satisfied by auditing the attacker’s attempts at defeating the security objectives as described in FAU_GEN.1. This records information such as login attempts, attempts to access security related files using FTP, and network interface spoofing attempts. Since any breach of security objectives will include either at least one received IP packet (remote attack), or at least one console login attempt (local attack), then FAU_GEN.1 will potentially (i.e. according to configuration) ensure that the attempts are logged.

FAU_GEN.1 lists the details that are recorded for each auditable event. No minimum amount of information is required to counter the threat, and therefore the threat is countered by any configuration which satisfies the network security policy. FAU_SAR.1 states that a tool exists to examine the audit logs. This enables an administrator to detect the attacker once FAU_GEN.1 has recorded the attack.

FAU_GEN.1 allows certain events to be excluded from auditing if permitted by the chosen network security policy.

Table A.2.2

Security Objective for the IT Environment		SFR
O.ADMIN	The underlying operating system shall ensure administration facilities for the configuration of the host and rule databases are only available to Firewall Administrative Users.	FMT_MSA.1 FMT_MSA.3 FMT_SMR.1
O.AUDIT	The firewall, in conjunction with the underlying operating system, must provide a means of recording information about the IP packets flowing through the firewall.	FAU_STG.1 FPT_STM.1
O.AUDITMAN	Procedures shall exist to ensure that the audit trails are regularly analysed and archived. *(Formerly Assertion_3)*	Procedural
O.EXTMASQ	Those responsible for the TOE shall accept the risk posed by External Masquerade attacks.	Procedural
O.IMU	The firewall will be configured in accordance with the Evaluated Configuration section of the Security Target, and with the chosen network security policy. No optional features shall be enabled unless recommended in the Evaluated Configuration.	Procedural
O.NSP	Those responsible for the TOE shall define a network security policy prior to any attempted installation or implementation of the firewall. The network security policy shall cover physical and procedural measures in addition to electronic issues. The network security policy shall be reviewed and revised according to the perceived needs.	Procedural
O.PHYSICAL	Those responsible for the TOE shall establish appropriate measures and procedures to ensure that only Firewall Administrative Users have physical access to the firewall hardware. *(Formerly Assertion_2)*	Procedural
O.REMOTE	Firewall Administrators should NOT use a privileged account for remote proxy authentication.	Procedural
O.TRAIN	Firewall Administrators should have received training, taken a course in firewall administration, or something equivalent. *(Formerly Assertion_6)*	Procedural

The justification of the suitability of the SFRs to achieve the security objectives to be met by the TOE environment is as follows.

O.ADMIN	The underlying operating system shall ensure administration facilities for the configuration of the host and rule databases are only available to Firewall Administrative Users.

CyberGuard Firewall Version 4.3 (for UnixWare 2.1.3) is able to achieve this security objective since logins to such facilities are available from the console to which administrators must login. In addition the underlying operating system is a multi-level system (MLS) which compartments processes running at different levels.

FMT_MSA.1 ensures that the security attributes identifying and authenticating administrators match their assigned profiles (e.g. if there is more than one administrator or firewall security officer) so that only the appropriate database(s) are accessible.

FMT_MSA.3 ensures that the appropriate initial security attributes are created that match their assigned profiles and can only be given alternative initial values that match the their profile.

FMT_SMR.1 ensures that users, administrators and (if configured) different administrators with specific profiles are distinguished and recognised by the TOE.

O.AUDIT	The firewall, in conjunction with the underlying operating system, must provide a means of recording information about the IP packets flowing through the firewall.

The TOE can be configured to audit various events and functions such as information related to IP packets and their flow through the TOE in the audit log(s).

FAU_STG.1 ensures that the audit trail is appropriately protected and only available to those authorised to access it.

FPT_STM.1 ensures that a reliable timestamp is provided to the auditing function to append to the events recorded in the audit logs by the TOE.

A.2.2 Security Assurance Requirements Appropriate

An assurance level of EAL4 was chosen since it is roughly equal to the ITSEC E3 level of assurance that was established in previous versions of the TOE. This represents the maximum level of assurance attainable by a product that has not been specifically designed with the assurance criteria in mind. The addition of flaw remediation (ALC_FLR) procedures augments the EAL4 assurance with a view to giving confidence in the ongoing support of the product.

Particular aspects of EAL4 that were considered appropriate for a firewall are:

- confidence in the correct implementation of the security functions at the source code level (pointing to ADV_IMP.1 and components on which this depends);
- secure configuration is a particular concern with firewalls (pointing to the need for a misuse analysis, i.e. AVA_MSU.2).

A.2.3 Strength of Function Claims Appropriate

A level of *SOF-Medium* was chosen as being commensurate with an assurance level of EAL4. Note that in the TOE Summary Specification, there are no security functions that have an associated SOF claim.

A.2.4 Dependencies Satisfied

The following tables demonstrate that all dependencies of CC Part 2 functional components are satisfied within this ST, giving rise to requirements on either the TOE or its IT environment (i.e. underlying operating system). All dependencies between CC Part 3 assurance components are satisfied since the assurance requirement is defined purely in terms of a self-contained assurance package, i.e. EAL4.

Note: in the following table, '[E]' denotes a requirement on the IT environment.

Table A.2.4: SFR Dependencies

SFR	*Dependencies satisfied by*
FAU_STG.1 [E]	No dependencies
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1
FIA_UID.2	No dependencies
FIA_UAU.2	FIA_UID.2 (hierarchical to FIA_UID.1)
FIA_UAU.2 [E]	FIA_UID.2 [E]
FMT_MSA.1 [E]	FDP_IFC.1 FMT_SMR.1 [E]
FMT_MSA.3 [E]	FMT_MSA.1 [E]
FMT_SMR.1 [E]	FIA_UID.2 [E] (hierarchical to FIA_UID.1)
FPT_RVM.1	No dependencies
FPT_STM.1 [E]	No dependencies
FAU_GEN.1	FPT_STM.1 [E]
FAU_SAR.1	FAU_GEN.1

A.2.5 Security Requirements Mutually Supportive

It can be taken that since the above table shows dependencies, this also implicitly shows support between the SFRs since it is merely a different perspective of the same relationship. Therefore, the preceding section shows that the SFRs are mutually supportive since all dependencies between CC Part 2 functional components are satisfied.

Additional instances of support between SFRs are as follows:

- FAU_GEN.1 supports FDP_IFF.1 and FDP_IFC.1 by providing the means to detect security relevant events that might undermine the firewall information flow control policy, and FAU_SAR.1 provides the means to review and interpret this information.

- FPT_RVM.1 ensures that the firewall information flow control policy cannot be bypassed.

- FIA_UID.2 and FIA_UAU.2 provide identification and authentication of FTP and Telnet users, in support of the firewall information flow control policy.

- A.PHYSICAL ensures that only Firewall Administrators have physical access to the firewall hardware so as to prevent tampering for example.

- A.TRAIN ensures that Firewall Administrators are assumed to be suitably qualified and that they are competent enough not as to accidentally deactivate any security functionality through lack of knowledge.

A.3 TOE Summary Specification Rationale

A.3.1 Suitability of IT Security Functions

This section demonstrates the suitability of the IT Security Functions to address the Security Functional Requirements.

Table A.3.1: SFR to SF correlation:

SFR	*Security Function*
FDP_IFC.1	
FDP_IFC.1.1	IA_1, IA_2, IA_3, IA_4, IA_5 DAC_1, DAC_2, DAC_3, DAC_4
FDP_IFF.1	
FDP_IFF.1.1	IA_1, IA_2, IA_3, IA_4, IA_5 DAC_1, DAC_2, DAC_3, DAC_4
FDP_IFF.1.2	DAC_1, DAC_2, DAC_3, DAC_4
FDP_IFF.1.3	DAC_5, DAC_6, DAC_7
FDP_IFF.1.4	IA_3, IA_4, IA_5
FDP_IFF.1.5	Not Applicable - Null Requirement
FDP_IFF.1.6	IA_1 DAC_1
FIA_UID.2	
FIA_UID.2.1	IA_2
FIA_UAU.2	
FIA_UAU.2.1	IA_2
FPT_RVM.1	
FPT_RVM.1.1	IA_1, IA_2, IA_3, IA_4, IA_5 DAC_1, DAC_2, DAC_3, DAC_4
FAU_GEN.1	
FAU_GEN.1.1	AUD_1, AUD_4
FAU_GEN.1.2	AUD_1, AUD_2
FAU_SAR.1	
FAU_SAR.1.1	AUD_3

SFR	*Security Function*
FAU_SAR.1.2	AUD_3

The majority of the TOE capability is provided by FDP_IFF.1 to which all of the DAC SFs and most of the IA SFs correlate. FIA_UID.2 and FIA_UAU.2 are for the express purpose of the standard identification and Authentication capability to which IA_2 maps. The FAU_GEN.1 covers the auditing capability of the TOE and AUD_1, AUD_2 and AUD_4 provide for this. The last remaining SF is AUD_3 which maps directly onto FAU_SAR.1 which concerns the reading and interpretation of raw audit data.

A.3.2 Suitability of Assurance Measures

Section 6.3 provides a table which maps assurance measures to each of the EAL4 and ALC_FLR assurance requirements, demonstrating that these will be sufficient to ensure the assurance requirements are met.

A.4 Protection Profile Conformance

This ST makes no claims of conformance with any PP.