CyberGuard Corporation

CyberGuard Firewall/VPN Version 6.2.1

Security Target

EAL4 Augmented

CyberGuard Firewall/VPN Version 6.2.1 Security Target
September 30, 2005

Document No. FCC101-002
Revision No. 1.3

DOCUMENT INTRODUCTION

Prepared By:	**Prepared For**:
CyberGuard Corporation 350 SW 12th Avenue Deerfield Beach, Florida, 33442	Common Criteria EAL4+ Certification

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the CyberGuard Firewall/VPN Version 6.2.1. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Document Number	Revision	Effective Date
FCC101-000	1.0	July 1, 2005
FCC101-001	1.1	July 1, 2005
FCC101-002	1.2	August 31, 2005
FCC101-003	1.3	September 30, 2005

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Table 1 - Acronym List

AP-MRPP	**Final U.S. Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000**
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-2004-01-001, Version 2.2, January 2004, Revision 256**
CC2	**Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-2004-01-002, Version 2.2, January 2004**
CC3	**Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements CCIMB-2004-01-003, Version 2.2, January 2004, Revision 256**
CGIA	**CyberGuard Firewall Identification and Authentication**
CLI	**Command-Line Interface**
DMZ	**Demilitarized Zone**
EAL4	**Evaluation Assurance Level 4**
GUI	**Graphical User Interface**
HTTP	**Hyper Text Transfer Protocol**
IT	**Information Technology**
LAN	**Local Area Network**
NAT	**NetWork Address Translation**
NIAP	**National Information Assurance Partnership**
PP	**Protection Profile**
RSBAC	**Rule Set Based Access Control**
SAR	**Security Assurance Requirements**
SF	**Security Function**
SFP	**Security Function Policy**
SMTP	**Simple Mail Transfer Protocol**
SOF	**Strength Of Function**

ST	**Security Target**
TF-MRPP	**Final U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000**
TOE	**Target of Evaluation**
TSC	**TSF Scope of Control**
TSF	**TOE Security Functions**
TSFI	**TSF Interface**
TSP	**TOE Security Policy**
VPN	**Virtual Private Network**

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) identifies the Target Of Evaluation (TOE), TOE Common Criteria (CC) and Protection Profile (PP) conformance claims and describes the objectives, requirements and rationale for the TOE, which is CyberGuard Firewall/VPN Version 6.2.1. This Security Target conforms to Common Criteria for Information Technology Security Evaluation, Version 2.2.

1.1 Security Target Reference

This section provides identifying information for the CyberGuard Firewall/VPN Version 6.2.1 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

CyberGuard Firewall/VPN Version 6.2.1 Security Target, Revision 1.3, September 30, 2005

1.1.2 TOE Reference

CyberGuard Firewall/VPN Version 6.2.1.

1.1.3 Security Target Evaluation Status

This ST is currently under evaluation for Common Criteria EAL4 assurance level augmented by flaw remediation.

1.1.4 Security Target Author

CyberGuard Corporation.

1.1.5 Evaluation Assurance Level

Assurance claims conform to EAL4 (Evaluation Assurance Level 4) from the *Common Criteria for Information Technology Security Evaluation, Version 2.2*. EAL4 is augmented by ALC_FLR.3, Systematic Flaw Remediation.

1.1.6 Keywords

Traffic-filter, Application-Layer firewall, Application Proxy, Packet filter

1.2 TOE Overview

This Security Target defines the requirements for the CyberGuard Firewall/VPN Version 6.2.1. The evaluated configuration of the TOE shall consist of the following:

1. CyberGuard Firewall/VPN version 6.2.1 software
2. CG Linux Version 3.1 Kernel Extensions
3. CG compliance tested hardware
4. Authentication Server
5. Management Station

1.2.1 CyberGuard Firewall/VPN version 6.2.1

The CyberGuard Firewall/VPN version 6.2.1 sits as a barrier between an organization's network and external networks. It provides controlled and audited access to services, both from inside and outside an organization's network, by inspecting and allowing, denying and/or redirecting the flow of data (IP packets) that pass through the barrier. The Sub-Systems of the CG Firewall/VPN version 6.2.1 software that shall be part of the evaluated TOE are:

- Packet Filter
- FTP Proxy
- Telnet Proxy
- HTTP Proxy
- SMTP Proxy
- NAT
- CyberGuard Identification and Authentication (CGIA) for single-use and multi-use authentication.
- Rule Set Based Access Control (RSBAC) (access control component)
- Audit Subsystem (accountability component)
- Administration (Graphical user interface for configuration of the TOE)

1.2.2 CG Linux Version 6.2.1 Kernel Extensions

CGLinux Version 3.1 operating system contains enhancements to provide protection against bypassibility. The components of the CG Linux version 6.2.1 operating system, referred to as the 'Kernel Extensions Subsystem' that shall be part of the evaluated TOE are the enhancements that help the operating system achieve the following:

- Kernel residual data protection
- Non-bypassibility
- Process Control

1.2.3 CG Compliance Tested Hardware[1]

The 'CyberGuard Firewall/VPN version 6.2.1' software and the 'CGLinux Version 3.1' operating system are installed and delivered on an intel processor based CG Compliance Tested Hardware. Currently the following configurations of the CG Compliance Tested Hardware, also referred to as the 'CyberGuard Firewall/VPN Appliance' through out this document, are available:

1000 Series	is available as a compact 1U size unit and is designed for use in mid-size, growing network environments.
3000 Series	is available as a 1U, 2U, and 5U size unit and is designed to provide powerful protection for enterprises, data centres and service providers.
5000 Series	is available as a 5U size unit and is designed to provide comprehensive security for high-bandwidth data centres, web hosting and ISP/ASP markets.
7000 Series	is available as a 3U size unit and is designed to provide comprehensive security for high-bandwidth data centres, web hosting and ISP/ASP markets.
Where: 'U'	is the form factor depicting the unit slots occupied on the 'Rack Mount'. For e.g., Form Factor=1U indicates that the 'CG Firewall 'CyberGuard Firewall/VPN Appliance' occupies 1 slot on the rack mount; Form Factor=5U indicates that the 'CyberGuard Firewall/VPN Appliance' occupies 5 slots on the rack mount

Detals of the various configurations of the 'CG Compliance Tested Hardware' are depicted in Table 2 - Table 3 - below :

[1] The terms 'CG Compliance Tested Hardware' and 'CyberGuard Firewall/VPN Appliance[s]' are interchangeably used throughout this document.

Table 2 - CG Compliance Tested Hardware Models

Model	On-Board NIC Card	Network Interface Cards (NIC)	Maximum Interfaces	Expansion Slots	CPU	Memory	RAID	Power Supply
1150	Yes	See Table 3 - below	3	None	1 x Intel P4 2.4 GHz.	128 MB	N	1
1250	Yes	See Table 3 - below	6	None	1 x Intel P4 2.8 GHz.	256 MB	N	1
3100	Yes	See Table 3 - below	8	None	1 x Intel P4 Xeon 2.4 GHz.	512 MB	N	1
3400	Yes	See Table 3 - below	20	4	1 x Intel P4 Xeon 3.06 GHz.	512 MB	N	1 Standard; 2nd Optional
3600	Yes	See Table 3 - below	22	3	1 x Intel P4 Xeon 3.06 GHz.	1 GB	Y	2 Standard; 3rd Optional
5100	Yes	See Table 3 - below	22	1	2 x Intel P4 Xeon 3.06 GHz.	2GB	Y	2 Standard; 3rd Optional
7100	Yes	See Table Below	38	3	4 x AMD Opteron 2.2 GHz	4 GB	Y	Redundant Power Supply

Table 3 - Supported Network Interface Cards

		CG COMPLIANCE TESTED HARDWARE MODELS							NIC CHIPSET
		1150	1250	3100	3400	3600	5100	7100	
NETWORK INTERFACE CARDS (NIC)	Silicon 6-Port Copper Silicom	Option	Standard	Standard	Standard	Standard	Standard	Standard	Intel 882546
	4-Port Fiber Intel	No	No	Option	Option	Option	Option	Option	Intel 882546
	PRO 1000MT Dual Copper	Option	Option	Standard	Option	Option	Option	Option	Intel 882546
	Intel PRO 1000MF Dual Fiber	Option	Option	Option	Option	Option	Standard	Option	Intel 882546
	Intel PRO100M Single 10/100	Standard	Option	Option	Option	Option	Option	No	Intel 82551
	Interphase 554	Option	Option	Option	Option	Option	Option	No	Intel 21143

The CyberGuard Firewall/VPN Appliance, as depicted in Table 2 - Table 3 - above, come in various models. All the models share a very similar hardware architecture, use Intel CPUs as their main processor and have a similar packet flow. All the models run the CGLinux 3.1 operating system and the CyberGuard Firewall/VPN 6.2.1 with the same core features and therefore perform the same security functions and implement the same interfaces in the same way. The onboard NIC cards that are available on all the models are used to connect the appliance to an authentication server, the management station and/or the Internal Interfaces. These onboard NIC cards are functionally equivalent to the NIC cards available on the 'CG Compliance tested Hardware Models' mentioned in Table 2 - Table 3 - above, and have either Intel 82551 or Intel 882546 chipsets. The on-board NIC card on the 7100 uses a Broadcom BCM570x chipset[2]. The CyberGuard compliance tested hardware also has the provision for external NIC cards (mounted on the standard PCI slots in the appliance). All the NIC cards as depicted in Table 3 - above, have same/similar chipset and can be interchangeably[3] mounted/installed on any model of the appliance. As such, any of the above mentioned 6 NIC cards, installed on anyone of the above mentioned CG compliance tested hardware models, can be used towards meeting the security function requirements associated with the INTERCEPT security function defined in the TOE Summary Section (section 6.) of this document.

All the other hardware components (i.e., with the exception of the 'Network Interface Cards') listed in the tables above are not security relevant as they do not provide any internal/external interfaces that could be exploited by individuals with hostile or malicious intent.

1.2.4 Authentication Server

The single use Authentication Server is the 'RSA Authentication Manager Version 6.0' that interacts with the 'CyberGuard Firewall/VPN version 6.2.1 ' via the RADIUS authenticator plug-in module. The RADIUS authenticator plug-in is a dynamically linked library that extends the capabilities of the authentication subsystem by authenticating users via the external 'RSA Authentication Manager Version 6.0'. In the evaluated version of the TOE the 'Authentication Server' shall be dedicated for single use authentication of users and shall not be connected/interfaced to any other network or product.

1.2.5 Management Station

A dedicated 'Management Station' running 'Microsoft Internet Explorer' version 6.0 or above shall allow an 'authorized administrator' to manage/configure the 'CyberGuard Firewall/VPN version 6.2.1'. The 'Management Station' interacts/interfaces with the

---

[2] The Broadcom BCM570x chipset is functionally same/similar to the Intel 82551 and Intel 882546 chipsets.

[3] The 4-Prot Fiber Intel NIC card cannot be mounted on the 1150 and 1250 because of mechanical limitations.

'Management Software', a part of the 'CyberGuard Firewall/VPN version 6.2.1' residing on the CG Compliance tested hardware, while allowing only an 'authorized administrator' to manage/configure the TOE.

1.2.6 Security Target Organisation

Chapter 1. of this ST provides introductory and identifying information for the TOE.

Chapter 2. describes the TOE and provides some guidance on its use.

Chapter 3. provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4. identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5. provides the TOE security functional requirements, as well as requirements on the IT environment.

Chapter 6. is the TOE Summary Specification, a description of the functions provided by the CyberGuard Firewall/VPN Version 6.2.1 to satisfy the security functional and assurance requirements.

Chapter 7. identifies claims of conformance to registered Protection Profiles (PP).

Chapter 8. provides a rationale for the security objectives, requirements, and TOE summary specification and PP claims.

1.2.7 Common Criteria Conformance

The CyberGuard Firewall/VPN Version 6.2.1 is conformant with the Common Criteria (CC) Version 2.2, functional requirements (Part 2) and assurance requirements (Part 3) conformant for EAL4 augmented by ALC_FLR.3, Systematic Flaw Remediation.

1.2.8 Protection Profile Conformance

The CyberGuard Firewall/VPN Version 6.2.1 has been modeled[4] on the following two Protection Profiles:

A. *Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000*

B. *Application-Level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000*

[4] Albeit the CyberGuard Firewall/VPN version 6.2.1 has been modeled on the TF-MRPP & AP-MRPP it does not claim conformance to either.

1.3 Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in version 2.2 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Security Target user. The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Some or all of these operations have been used in this Security Target.

- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text. For example, **refinement**.

- The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*. For example, *allocation of the resource* to all objects.

- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value]. For an example, [8 characters].

- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number). For example, see FDP_IFC in this Security Target.

Differences in the text used to describe the functional components within the two PPs this security target claims conformance to have been described in the *'Protection Profile Claims'* chapter.

This Security Target also utilizes bolding and underlining to mark the chapter and section headings and captions. Regular italics have been used to identify unique references in the ST, such as the reference to the Protection Profiles to which the TOE conforms.

1.4 Terminology and Acronyms

For a list of Acronyms, see Table 1 - Acronyms List.

This section contains the terminology that has been used throughout the ST. Additional definitions are available in the following protection profiles that were used as a model for the construction of this ST.

A. *Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000*

B. *Application-Level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000*

Firewall: The many forms of a bastion host (one that does not automatically allow traffic to flow through it) which generally protect the boundary of the network, working as a gatekeeper, and have built in features to either perform packet filtering or application proxy or a combination of both on the network traffic.

Network Address Translation (NAT): This is a method by which real internal (protected) network address are translated to fake internal addresses in and out of a network in order to hide the internal network topology.

NAT: **Network Address Translation**: An Internet standard that is used where two networks with incompatible addressing schemes meet. It allows a Local Area Network (LAN) to use one set of IP addresses for 'Internal Traffic' and a second set of addresses for 'External Traffic thereby facilitating internal IP address hiding and reuse of IP addresses by internal networks.

Virtual Private Network (VPN): This is a method of encapsulating data in a tunnel using cryptographic algorithms in order to protect data from discovery while en route to and from its source and destination.

Packet Filtering (also called Stateful Inspection) This is a general form of various schemes of inspection of each and every packet to and from a protected network to check its integrity and making decisions on whether to permit or deny that packet from traversing the protected network.

FTP: File Transfer Protocol: A network application protocol that facilitates transfer of files between two connected computers.

Telnet: A network application protocol that facilitates remote connection to and accessing remote computers.

HTTP: Hyper Text Transfer Protocol: A network application protocol that facilitates transfer of hypertext documents and related resources across the Internet from servers to clients.

SMTP: Simple Mail Transfer Protocol: A store-and-forward protocol used by mail transfer agents to transfer electronic mail messages.

Application Proxy: These are security hardened versions of corresponding network application services such as HTTP, SMTP, FTP, and Telnet that work as agents on a firewall and mediate the connection between a client and a server on the protected side, thereby protecting the server from direct access and attack by clients on the unprotected side of the network.

Demilitarized Zone (DMZ): This is a protected segment of the internal network in which the access to the unprotected side is allowed, however, the ability to connect to the internal network is disabled or limited and controlled. The purpose of a DMZ is to allow access to unprotected network, without compromising the integrity of the protected side. Example, when hosting an external web site for an organization, a DMZ segment of the network allows free access to the web site by clients on the external network, yet eliminates possibility of those clients gaining access to internal (protected segments) of the organization's network.

Single-use Authentication Mechanism: This is a method of authentication in which a random and one time token is generated for the user to authenticate itself. The one-time use of the token for authentication purposes eliminates the possibility of reuse of the authentication data if intercepted and captured.

Multi-use Authentication Mechanism: This is a method of authentication in which a static password is assigned to the user to authenticate with each time authentication is required.

CHAPTER 2

2. Introduction

This section provides the context for the TOE evaluation by identifying the product, its type and features, defining the scope of the TOE and TOE boundaries, both physical and logical, and describing the evaluated configuration.

2.1 Product Description

CyberGuard Firewall/VPN Product represents integrated firewall appliances that utilize hybrid firewall architecture, consisting of packet filtering and application proxy techniques to inspect, control and protect the flow of network traffic in and out of an organization's network and to protect the integrity of organizations' internal networks. CyberGuard Firewall/VPN Product further combines this functionality with Virtual Private Network capability in order to protect network traffic that goes in and out of an organizations' network while en route to and from its source and destination.

CyberGuard Firewall/VPN Product also provides Network Address Translation (NAT) facilities in order to hide the internal network addresses of an organization. The product also has a provision for various network service application proxies that break the direct connection between clients and servers in order to protect an organization's servers and where applicable identify and authenticate users before allowing requested services to be provided to them.

Split DNS capability of the CyberGuard Firewall/VPN Product allows the organizations' domain name servers to be split between servicing internal and external requests for name/IP translations and is aimed at controlling communication between external and internal nameservers under strict rules so as to avoid allowing direct access to internal nameservers and thereby exposing internal network addresses or allowing the internal nameservers to be directly contacted or exploited.

Passport capabilities of the product allows known remote users access to an organization's internal network resources by identifying and authenticating those users and providing a fine grained level of control over the time and method of access and resources to be accessed by such users.

In identifying and authenticating users, CyberGuard Firewall/VPN Product utilizes a multi-faceted central authentication mechanism that allows various methods of authentication such as password or single-use token authentication to be assigned to administrators and network users.

A User Graphical Interface (GUI), also referred as the 'Management Software' throughout this document, is used to manage the 'CyberGuard Firewall/VPN Product'. The firewall may be managed locally or remotely. The product has full auditing and alerting capabilities with additional tools designed for filtering, reviewing, and inspecting specific audit records, as well as full backup and restore capabilities and audit data relocation to secondary storage devices in a secure manner.

The packet-filtering engine inspects and filters network traffic based on a configured security policy and corresponding rule set. The packet filtering engine contains a VPN component that inspects VPN protected traffic on arrival and before handing it off to the packet filter for access control and further processing and applies VPN protection to the inspected and permitted traffic after packet filter has completed its processing and before handing it off to the network interface.

The NAT facility translates all internal addresses on out-bound traffic based on a configured rule set to fake addresses before traffic leaves the firewall and translates in-bound traffic to their corresponding real addresses on arrival.

The application proxies protect internal servers from exploitation by breaking the direct connection between clients and servers and mediating the traffic between them, and where applicable:

- hide the internal addresses of real servers by rewriting the headers of messages on out-bound traffic and removing references to internal addresses;
- identify and authenticate users of network services before providing requested service to them;
- Perform protocol filtering to ensure adherence to established protocol standards.

The Rule Set Based Access Control component of the CyberGuard Firewall/VPN Product is an internal access control mechanism that protects the various Sub-Systems of the firewall against unauthorized access and provides domain separation for the firewall's internal processes, based on a configured rule set.

The CyberGuard Firewall/VPN Product is available in High Availability (HA) configurations and further contains features that cover version tracking and change control features.

The CG Linux Version 6.2.1 has been enhanced to allow residual data protection in memory utilized for packet processing. This is done by zeroizing the memory bits before reuse of the memory for additional packets and also by allowing the 'CyberGuard Firewall/VPN Product' kernel modules (Packet Filter, NAT driver, and VPNguard) to break into and bind to the network layer and control flow of traffic at the lowest possible layer of the OSI model.

The CyberGuard Firewall Product can also have up to a maximum of thirty eight (38) physical interface (network) connections.

2.2 TOE Description

The TOE is a subset of full functionality that the 'CyberGuard Product' (described above, under 'Section 2.1 Product Description ') provides. The TOE claims conformance to the *TF-MRPP* and *AP-MRPP* protection profiles as it contains Sub-Systems that are directly involved in enforcing the security functional requirements mandated by the two protection profiles

A brief TOE description is provided above, under 'Section 1.2 - TOE Overview'. It consists of CyberGuard Firewall/VPN version 6.2.1 software, CGLinux Version 3.1

kernel enhancements, Authentication Server, Management Station and the CG compliance tested hardware (CyberGuard Firewall/VPN Appliances). Together these components implement the requirements of the 'Final U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments (*TF-MRPP*)' and 'Final U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness environments (*AP-MRPP*)' upon which the CyberGuard Firewall/VPN version 6.2.1 is modeled.

The '*CyberGuard Firewall/VPN version 6.2.1'* sits as a barrier between an organization's network and external networks. It provides controlled and audited access to services, both from inside and outside an organization's network, by inspecting and allowing, denying and/or redirecting the flow of data (IP packets) that pass through the barrier. The Sub-Systems of the CG Firewall/VPN version 6.2.1 software that are part of the evaluated TOE are the Packet Filter engine, NAT, FTP Proxy, Telnet Proxy, HTTP Proxy, SMTP Proxy, CGIA (used for single-use and multi-use authentication), Rule Set Based Access Control (RSBAC) (access control component), Audit subsystem (accountability component), and the Administration (Graphical user interface for configuration of the TOE).

The *'CGLinux Version 3.1'* operating system contains enhancements to provide protection against bypassibility. These enhancements also referred to as as the 'Kernel Extension' subsystem are part of the evaluated TOE that help the operating system achieve kernel residual data protection, Non-bypassibility, and Process Control.

The single use *'Authentication Server'* is the 'RSA Authentication Manager version 6.0' that interacts with the 'CyberGuard Firewall/VPN version 6.2.1' via the RADIUS authenticator plug-in module. The RADIUS authenticator plug-in is a dynamically linked library that extends the capabilities of the authentication subsystem by authenticating users via the external 'RSA Authentication Manager Version 6.0'. In the evaluated version of the TOE the 'Authentication Server' shall be dedicated for single use authentication of users and shall not be connected/interfaced to any other network or product.

A dedicated *'Management Station'* running 'Microsoft Internet Explorer' version 6.0 or above shall allow an 'authorized administrator' to manage/configure the 'CyberGuard Firewall/VPN version 6.2.1'. The 'Management Station' interacts/interfaces with the 'Management Software', a part of the 'CyberGuard Firewall/VPN version 6.2.1' residing on the CG Compliance tested hardware, while allowing only an 'authorized administrator' to manage/configure the TOE.

The evaluated *'CyberGuard Firewall/VPN Appliances (CG compliance tested hardware)'* have the *'CyberGuard Firewall/VPN version 6.2.1'* software and the *'CGLinux Version 3.1'* operating system installed and delivered on them and are based on commodity 'Intel IA-32 Architecture'. The '*CyberGuard Firewall/VPN Appliances'* consist of any of the configurations mentioned in 'Section 1.2.3 - CG Compliance Tested Hardware', with a minimum processor speed of 133 MHz. These appliances run on the following single or multi, Intel family processors:

A) Pentium III

B) Pentium III Xeon

C) Pentium 4

D) Pentium 4 Xeon

A '*Management Station*', running Microsoft Internet Explorer, version 6.0 or above, is directly (or via an isolated or protected network) attached to the '*CyberGuard Firewall/VPN Appliances'*. In addition, in the evaluated configuration, the single-use 'Authentication Server' is also either directly or through an isolated network connected to the '*CyberGuard Firewall/VPN Appliance'*.

The TOE safeguards information held on internal networks, by controlling the access of external users and protecting the integrity, availability, and authentication data of the internal network. Additional network interfaces (up to 38) provide further internal/ external network connections.

Security features within the scope of the TOE include:

A) Connection level Access Control for IP packets (e.g. permit/deny source & destination addresses or ports; divert IP packets to a proxy process [FTP, TELNET, HTTP, SMTP]).

B) Network Address Translation [NAT] for hiding the internal network addresses of an organization.

C) Single-use and multi-use authentication mechanisms.

D) Rule Set Based Access Control facility for role enforcement and domain separation.

E) Accounting, auditing and statistics of firewall traffic and security related events.

F) Enhancements for and extensions to the CGLinux operating system modules to ensure that TOE security functions are non-bypassable and resistant to modification.

VPN, Remote Administration capabilities, Passport facility, SDNS, other proxies, version tracking features, and High Availability (HA) configurations, have not been included in the TOE, as their functionality does not have any bearing on claims of conformance to the PPs.

2.3 Physical Boundary

The TOE as shown in Figure 1 - below, includes a management station (where its administrative interface is installed), an authentication server (where its single-use authentication server is installed), the CG Compliance Tested Hardware, CGLinux version 3.1 kernel enhancements (Kernel Extensions) and CyberGuard Firewall/VPN version 6.2.1 software. The management station, along with the single-use authentication server, must both be located in a physically secure location and be directly connected to the CG Compliance Tested Hardware or alternatively, installed on a protected subnet,

such as a DMZ network configuration. The CGLinux version 3.1 and CyberGuard Firewall/VPN version 6.2.1 software are installed on the CG Compliance Tested Hardware.

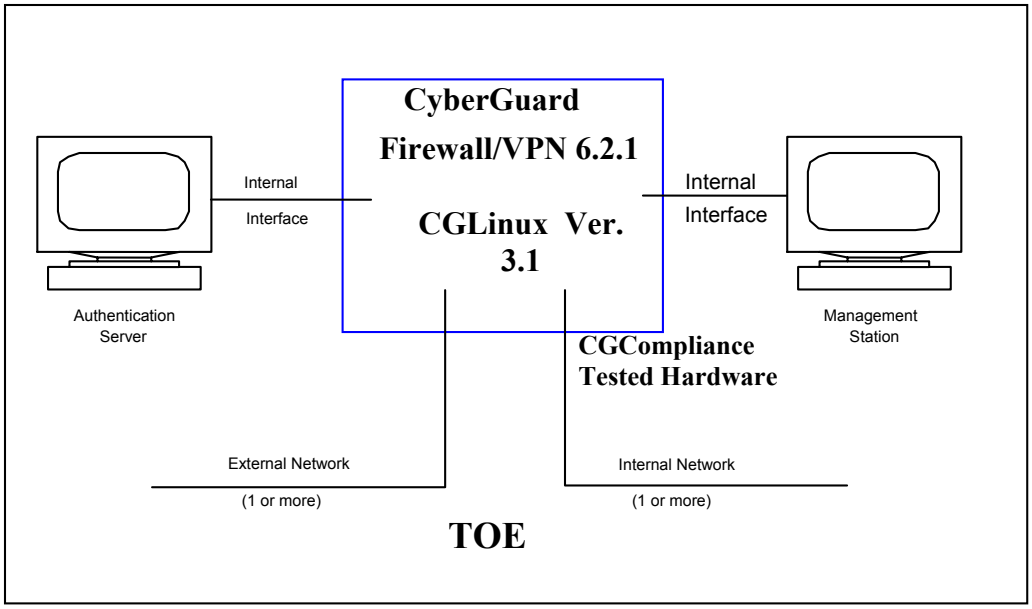


Figure 1 - TOE Physical Configuration

The TOE's physical boundary therefore, consists of the CG Compliance Tested Hardware on which the CGLinux version 3.1 and the CyberGuard Firewall/VPN version 6.2.1 software are installed, the management station where its administrative interface is installed and an authentication server where its single-use authentication server is installed . Within its physical boundary the TOE contains the following software sub-systems:

A) Administration: The Administration subsystem has user interfaces for configuring the security policy, for controlling the security functions, and for processing audit information. These interfaces consist of the graphical user interfaces (GUI).

B) NAT: The 'Network Address Translation' component translates all internal addresses on out-bound traffic based on a configured rule set to fake addresses before traffic leaves the firewall and translates in-bound traffic to their corresponding real addresses on arrival. This facilities in hiding the internal network addresses of an organization

C) Packet Filter: The packet Filter component filters packets according to the network security policy. Depending on addresses and rules present a packet can be rejected (dropped), passed through, or passed to an appropriate application proxy.

D) RSBAC: The RSBAC component provides access control mechanisms for the TOE in terms of role enforcement and to create a separate domain of execution for the TOE and TOE security functions.

E) Proxies (FTP Proxy, Telnet Proxy, HTTP, SMTP): The TOE provides proxies for FTP, TELNET, HTTP and SMTP proxies that enforce correctness of the protocols, limitations on access, and user identification and authentication for the protocols.

F) Audit: The Audit component provides for secure storage and review of audit records generated by all of the Sub-Systems of the TOE. Audit records can be viewed, searched, sorted, dumped, and deleted. Audit record are time stamped based on time that is calculated and maintained by the TOE, using an initial time obtained from the hardware platform's battery backed up clock.

G) Kernel Extensions: The TOE includes enhancements for several kernel functions to meet the requirements of the Protection Profiles. Functions modified are the IP packet input and output handling functions to allow the packet filter to bind to network interfaces, and the memory release functions to guard against residual data in memory utilized for processing packets. These enhancements ensure that the Packet Filter engine processes all packets, that the TOE security mechanisms are not bypassable and that all memory is cleared upon release to the system. Extensions to the kernel include RSBAC, which controls access control routines by restricting all access to security enforcing functions of the TOE to authorized administrators only and providing internal access control and domain separation for the TOE.

H) CyberGuard Firewall Identification and Authentication (CGIA): CGIA provides the authentication functions that are used by the TOE to allow access to proxies, and to administration using either a password mechanism or a single-use, token based method of authentication.

I) Single use Authentication Server[5]

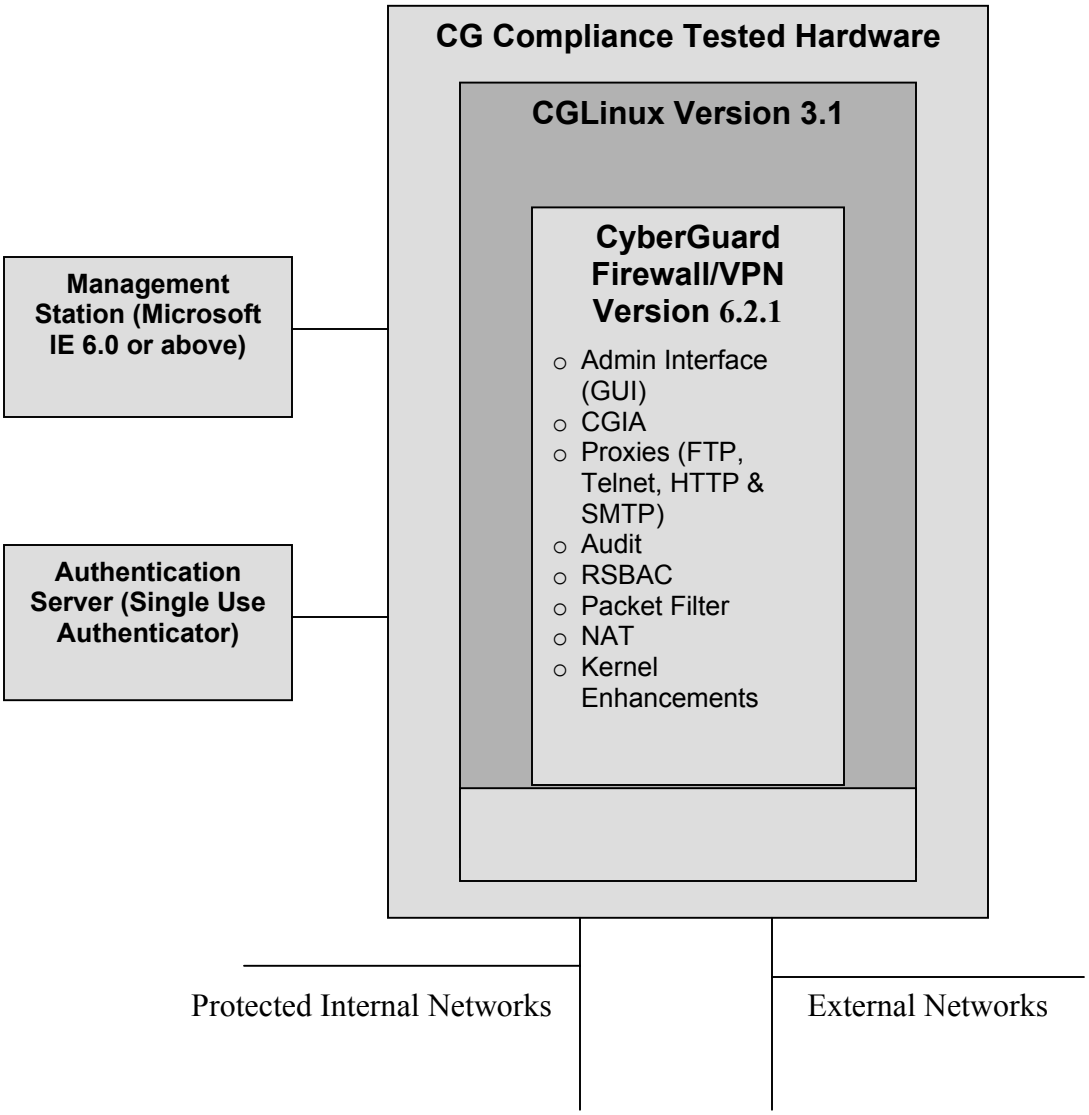
J) Management Station[6] with the Microsoft Internet Explorer version 6.0 or above

The physical boundary of the TOE's software Sub-Systems is outlined in Figure 2 - below:

[5] The 'RSA Authentication Manager 6.0' is the 'Single use Authentication Server'. The terms 'Single use Authentication Server', 'Authentication Server' and 'RSA Authentication Manager 6.0' have been interchangeably used throughout this document.

[6] No other software, besides the Internet Explorer 6.0 or above, runs on the Management station. The sole purpose of the Management Station is to provide a browser (i.e., Internet Explorer 6.0 or above) for the GUI to run.

Figure 2 - TOE Physical Boundary



2.4 Logical Boundary

As shown below in Figure 3 -, part of the TOE is tightly coupled with the CGLinux operating system upon which it is installed. In general, the TOE is the application software, however portions of the TOE are hooked into or modify portions of the CGLinux kernel, to ensure that all network traffic is passed through the TOE Sub-Systems and all Protection Profile requirements are met. The TOE also includes the CG Compliance tested hardware, the management station and the authenticator server.

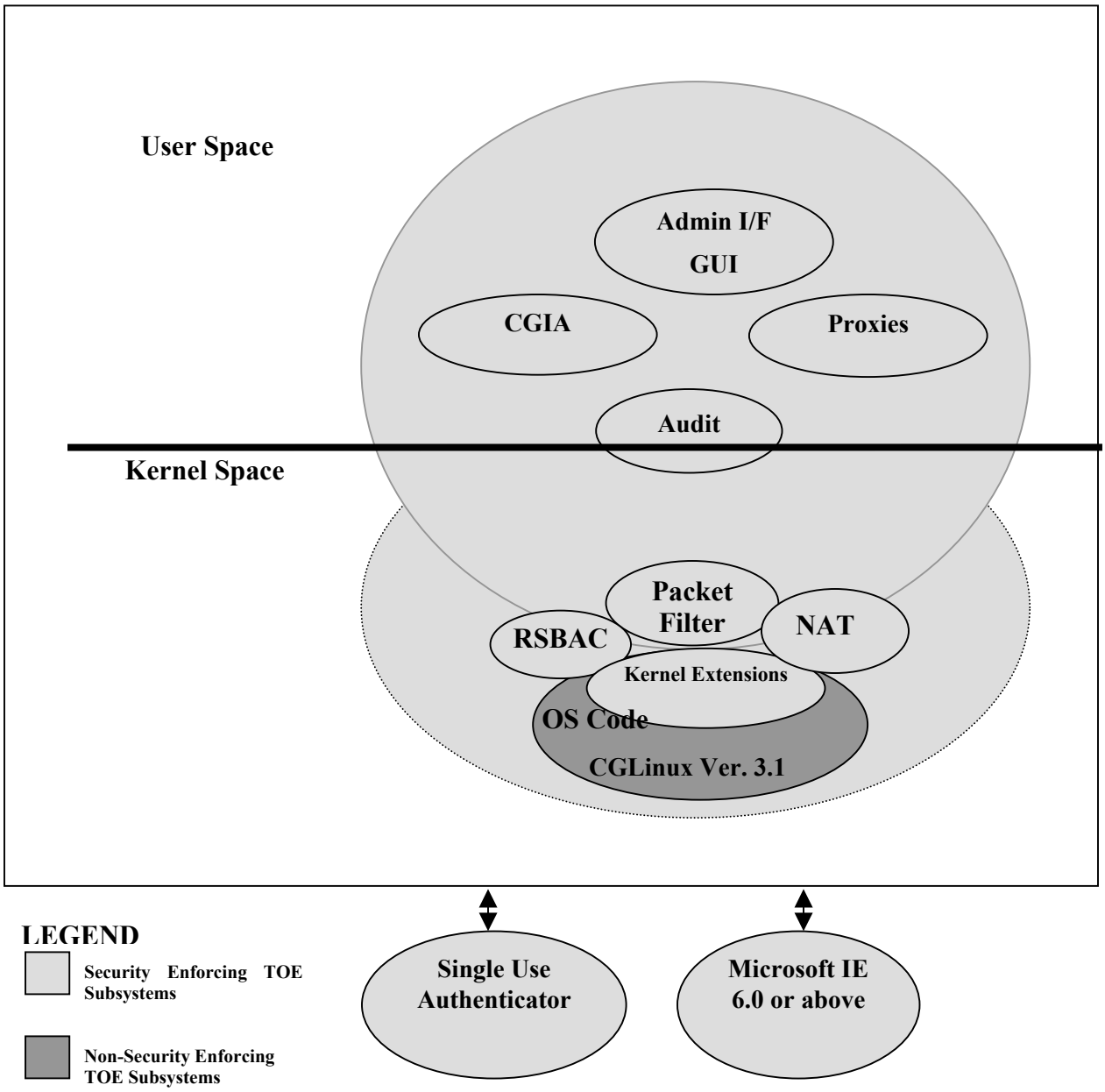


Figure 3 - Logical Boundaries of the TOE

The Administrative Interfaces, Proxies, CGIA, and Audit subsystems are application software. The Packet Filter subsyetm hooks into the CGLinux IP packet handling functions to ensure that all packets are filtered and translated through the TOE. RSBAC subsystem is a kernel extension that provides access control, role enforcement, security, and domain separation for the TOE. The TOE also modifies the CGLinux kernel routines for releasing memory to provide protection for residual information in that memory.

The *'Management Station GUI'* utilizes Microsoft Internet Explorer (IE) revision 6.0 or above as a front-end to display the configurable features of the TOE so that the site security policy can be implemented. The GUI features a modular design and although it

presents many default secure options, it also enables the administrator to define objects and utilize those objects in defining the rule set that will represent the security policy for the TOE.

This makes the management software and its configuration options more flexible to allow all sorts of configuration options to be implemented and configured. These features provide the administrator with finer grain of control and details in defining security policy of the site. The GUI allows only the authorized administrator to log on and to configure the security features of the TOE. There is no concept of users on the TOE, other than the administrator user.

The *'CyberGuard Identification and Authentication (CGIA)'* subsystem is a central set of libraries and associated interfaces that are utilized by all Sub-Systems of the product that require identification and authentication services. The CGIA facilitates Multiple Authentication Mechanisms for various applications/proxies.

Using the multiple methods of authentication, the administrator can assign single use authentication method to users of network services (such as Telnet and FTP) in order to identify and authenticate such users. The single use authenticator server that is part of the TOE is the 'RSA Authentication Manager 6.0'.

The configured method is enforced per user. Safeguards have also been put into place so that if a user is unsuccessful in completing both the identification and authentication phases within a configurable number of attempts, and within a configurable length of time, for the TOE to take action by blacklisting such users until the administrator can review and access the reason for the failures and restore the user. This guards against attempts at guessing valid user Ids or passwords.

The *'Network Address Translation (NAT)'* subsystem is used to hide internal network addresses from external hosts, while allowing network services to be routed through the firewall. Local IP addresses are translated to one of the firewall's registered external IP interface addresses so that, from outside, all traffic appears to be originating from or terminating at the firewall. This is accomplished by rewriting the packet headers flowing through the firewall.

The '*Packet Filter*' subsystem is responsible for inspecting each and every packet that reaches the organization's network and using its knowledge of organizational security policy, translated to its rule set makes critical decisions on whether to allow the traffic to go through, deny the traffic or if configured for proxy service to hand off the packet to an appropriate proxy service on the TOE for further processing of the request.

The packet filter has a variety of security checks on packets before making any decisions on the status of the packet. These include defenses for variety of mal formed or invalid packets. If the rule set explicitly mandates dropping a specific type of traffic, it will be likewise dropped. If the rule set permits a certain type of traffic to enter the internal network, the packet filter engine will allow the traffic. When a packet arrives that is destined for a network service and such services has been configured for proxy services, the packet filter will pass the packet to the appropriate proxy to validate the users and further process the packet and return the appropriate responses in a secure manner.

The *FTP, Telnet, HTTP and SMTP* proxies are security-hardened versions of the corresponding network services that operate on the TOE. On one hand, the proxy communicates with the packet filter to receive requests for specific services for which it is responsible and on the other, the proxy service establishes connections between the client and the real server on the protected side of the network, and intercepts all requests from the client, delivers such request to the real server and in turn retrieves responses from the server and delivers them back to the client. This processing takes place in a seamless fashion, in which the client is unaware of the proxy service breaking its direct connection to the real server. The purpose of the proxy is to identify valid users, protect the servers from exploitation, and hide their real addresses in order to protect them from direct attack by the rogue clients.

The *'Audit'* subsystem is a central auditing mechanism in which all Sub-Systems of the TOE collect security relevant information and drop them into a funnel that feeds to the audit subsystem, which will process and then post them to the audit trail file with real-time time stamps to signify when the event occurred. The audit subsystem is configurable and is equipped with accompanying tools for filtering, reviewing, searching and sorting through the audit records based on a variety of criteria, including IP address ranges, date and time ranges, and specific event types.

The audit trail is designed to provide accountability of actions taken when configuring the security policy and to aid the administrator in recognizing suspicious activities and setting alert conditions to be delivered in a variety of ways. The audit subsystem has been configured to shut down network traffic in the event the audit space is exhausted, in order to eliminate the possibility of suspicious activities taking place on the system while no accountability exist. Once the administrator accesses the situation and frees up space by moving the existing audit data to an appropriate medium, network traffic and auditing will once again resume.

The *'Kernel Extensions'* subsystem includes enhancements for several kernel functions that help meet the requirements of the Protection Profiles. Functions modified are the IP packet input and output handling functions to allow the packet filter to bind to network interfaces, and the memory release functions to guard against residual data in memory utilized for processing packets. These enhancements ensure that the Packet Filter engine processes all packets, that the TOE security mechanisms are not bypassable and that all memory is cleared upon release to the system.

The '*RSBAC*' subsystem is used to provide internal access control to the various Sub-Systems and resources of the TOE. The RSBAC has a variety of functionality such as mandatory and discretionary access control and role enforcement that essentially work to separate administrative access to the TOE resources from non-administrative access. RSBAC checks multiple credentials for users that attempt to access the internal Sub-Systems or resources of the TOE and only when all the related credentials are in place and match its rule set it will allow access to the resource to be made. The RSBAC database of users is aware of every user's assigned role in addition to the set of commands associated with the role that a user can execute. In this fashion, if and when a user (non administrative user such as a network FTP or Telnet user for example) attempt to access the TOE's internal resources or objects, such access will not be granted.

2.5 Evaluated Configuration

The evaluated configuration of the CyberGuard Firewall/VPN Version 6.2.1 software is supplied on CG Compliance Tested Hardware (please refer to Section 1.2.3 above) that has passed a verification performed according to CyberGuard's platform compliance and certification process. It consists of the Intel platform (min speed 133 MHz) running CyberGuard CGLinux Version 3.1 and CyberGuard Firewall/VPN Version 6.2.1, equipped with both on-board[7] and PCI Network Interface Cards (NIC), a disk storage device, memory, and a CDRom device. The evaluated configuration shall also consist of the Management Station containing the Microsoft Internet Explorer 6.0 or above and the 'RSA Authentication Manager 6.0' for single use authentication.

The evaluated configuration requires configuration of some specific values of features, which have been outlined below. More details on these security considerations can be found in the product's guidance documentation:

- The prospective customer must define, document, and follow a network security policy that is appropriate for their site. However, the following security considerations must also be implemented to be complaint with the evaluated configuration of TOE:
- The TOE must be secured so that only authorized personnel have physical access to the TOE.
- The minimum password length for users must be set at eight and the password must consist of a combination of alphanumeric and special characters. These combinations will place the password name space well beyond the range that might make the passwords guessable within a reasonable amount of time.
- It is recommended that configuration and management of the TOE be designated to one administrator who has all administrative roles assigned to them.
- The TOE must not be configured to allow remote administration, since remote administration is not included in the scope of this evaluation.
- Direct connections to the TOE from an unprotected network (example FTP connections) must not be allowed in the site security policy.
- The TOE's interfaces must be configured to protect against IP Spoofing attempts in which a packet arrives on an interface other than that identified by its source address.
- It is not recommended to change the default setting of the "audit full condition" for the TOE to any other settings, since the TOE by default is set to shut down the network traffic if the audit space becomes full in order not to allow any traffic to pass where the audit of such traffic is not taking place.
- The TOE must be configured to proxy all Telnet network traffic.
- The TOE must be configured to proxy all FTP network traffic.

[7] In the evaluated configuration, the onbard NIC cards shall not be used for the means of providing external network interface(s).

- The TOE must be configured to proxy all HTTP network traffic.
- The TOE must be configured to proxy all SMTP network traffic.
- Users of network services Telnet and FTP must be set up with a single-use token-based method of authentication, not reusable password mechanism.
- User blacklisting feature must be enabled (it is not enabled by default).
- The "Set Blacklist Duration (minutes)" checkbox must also be enabled (not enabled by default). This field, when checked specifies the duration of time a user remains blacklisted. It is recommended that a large value to be set for this field (maximum number 2,147,483,647), in order to keep a user blacklisted until the administrator reviews and releases such users (as per requirements of the [PP]).
- The "Number of Failed Logon Attempts" field for repeated unsuccessful login attempt is set to three by default. Although the site security policy may dictate a different value for this field, it is not recommended to set this allowable number of attempts to a very large value.
- A value of 60 seconds has been configured by default for "Time Duration (seconds)" field of the user-blacklisting page. This is the duration of time in which the users are allowed to attempt to authenticate. Although the site security policy may dictate a different value for this field, but it is not recommend setting this value to a very high values.
- Both the authentication server and the management station must be configured using either as a direct connection to the TOE or from an internal protected network, or afforded the same physical protection and access control as required for the TOE.

2.5.1 Network Security Policy

In the evaluated configuration, the standard supplied hardware and software that constitute the TOE 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 authorized.

In defining a network security policy, it is necessary that the firewall be configured so that no direct connections to the firewall are allowed and remote administration capabilities are not configured. This implies that no connections such as the Telnet or the FTP application sessions shall be allowed into the firewall. The firewall as a bastion host shall however provide proxy services such as Telnet, FTP, HTTP and SMTP.

The recommendations outlined in the CyberGuard Firewall/VPN Version 6.2.1 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 shut down on audit failures in order to create an air gap and to record invalid IP packets rather than all IP packets.

2.5.2 IP Packet Interface Checking

The evaluated configuration has IP-Forwarding capabilities disabled and interface checking capabilities enabled, to detect packets that arrive on interfaces inconsistent with their addressing. This mechanism enables the TOE to counter common forms of IP spoofing attempts in which when a packet arrives on an interface other than that identified by its source address it will be rejected (dropped).

2.5.3 Auditing

The evaluated configuration for auditing is to shutdown traffic when audit trail becomes full. The [CGFM] provides guidance on how to configure other reactions to a full audit trail.

2.5.4 NAT

The evaluated configuration has NAT enabled to hide internal network addresses from external hosts, while allowing network services to be routed through the firewall. Local IP addresses are translated to one of the firewall's registered external IP interface addresses so that, from outside, all traffic appears to be originating from or terminating at the firewall.

2.5.5 Proxies

The evaluated configuration has the following proxies enabled. The method of authentication, wherever applicable, for users of these proxies must be set as single-use authentication mechanism, using the RSA Authentication Manager 6.0:

A) Telnet proxy

B) FTP proxy

C) HTTP

D) SMTP

The [CGFM] provides guidance on how to configure these proxies.

2.5.6 Administrative Interfaces

The evaluated configuration covers local administration of the TOE using the Management Software (Graphical User Interface). The Management Software station must be configured using either a direct connection to the firewall, or across a protected subnet such as a DMZ, and be located along with the firewall in a physically secure location that allows authorized access to the TOE only. In addition, it is recommended that one administrator role with all administrative capabilities be created and used to manage the firewall. [CGFM] provides guidance on how to configure the firewall to accept only local administration.

2.6 Security Policy Model (SPM)

The Security Policy Model requirement (ADV_SPM.1) is met by this Security Target.

CHAPTER 3

3. Security Environment

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) IT related threats to the organisation countered by the TOE.

C) Environmental threats requiring controls to provide sufficient protection.

D) Organizational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies assumptions (A), threats (T) and organisational security policies (P). For assumptions, threats or policies that apply to the environment, the initial character is followed by a period and then an 'E'. For example, T.E.PHYSICAL is a security environmental threat of unauthorised physical access.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

3.1.1 Connectivity Assumptions

A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
A.REMACC[8]	Authorized administrators may only access the TOE locally.

3.1.2 Personnel Assumptions

A.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

[8] The TOE does not claim conformance to the optional remote administration. Hence authorized administrator are allowed to access the TOE only locally.

A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.TRAIN	Firewall Administrators are assumed to be suitably qualified.

3.1.3 Physical Assumptions

A.PHYSEC	The TOE is physically secure.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.

3.2 Threats

The following threats are addressed either by the TOE or the environment..

3.2.1 Threats Addressed by the TOE

T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address. An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

T.PROCOM[9]	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
T.MODEXP	A skilled attacker with moderate attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.

3.2.2 Threats to be Addressed by Operational Environment

T.E.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

3.3 Organizational Security Policies

P.CRYPTO	Triple DES encryption, as specified in FIPS 46-3 (3) must be used to protect remote administration functions, as the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level1)[10]Environments.

[9] This threat is not applicable to this ST, since both the protection profiles (i.e., TF-MRPP & AP-MRPP) that require this threat to be addressed by the ST writer make Remote Administration an optional component. Since the TOE does not claim remote administration, this threat is therefore outside the scope of the TOE.

[10] This organizational security policy is not applicable to this ST, since both the protection profiles (i.e., TF-MRPP & AP-MRPP) that require this policy also make Remote Administration an optional component. Since the TOE does not claim remote administration, this policy is therefore outside the scope of the TOE and as such, it is not implemented.

CHAPTER 4

4. Security Objectives

4.1 Security Objectives for the TOE

All of the objectives listed in this section ensure that all of the security threats listed in Chapter 3 have been countered, and all of the policies have been implemented. The security objectives (O) for CyberGuard Firewall/VPN Version 6.2.1 are:

O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols and ensuring that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.

4.2 Security Objectives for the IT Environment

O.E.PHYSEC	The TOE is physically secure.
O.E.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
O.E.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
O.E.PUBLIC	The TOE does not host public data.
O.E.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
O.E.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
O.E.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
O.E.NOREMO	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
O.E.REMACC[11]	Authorized administrators may only access the TOE locally.
O.E.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
O.E.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.

[11] The TOE does not claim conformance to the optional remote administration. Hence authorized administrator are allowed to access the TOE only locally.

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

5.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.2*.

The following table (Table 4 - below) has been utilized to indicate all the functional components the TOE claims conformance with. It also indicates the Protection Profiles that mandates each one of the mentioned functional components including those that are common to both the PPs.

Table 4 - Functional Components of the TOE

	AP-MRPP	TF-MRPP	CC FUNCTIONAL COMPONENT DESCRIPTION
CC FUNCTIONAL COMPONENTS	FMT_SMR.1	FMT_SMR.1	Security roles
	FIA_ATD.1	FIA_ATD.1	User attribute definition
	FIA_UID.2	FIA_UID.2	User identification before any action
	FIA_AFL.1	FIA_AFL.1	Authentication failure handling
	FIA_UAU.5	FIA_UAU.5	Multiple authentication mechanisms
	FDP_IFC.1 (1)	FDP_IFC.1	Subset information flow control (1)
	FDP_IFC.1 (2)		Subset information flow control (2)
	FDP_IFF.1 (1)	FDP_IFF.1	Simple security attributes (1)
	FDP_IFF.1 (2)		Simple security attributes (2)
	FMT_MSA.1 (1)	FMT_MSA.1 (1)	Management of security attributes (1)
	FMT_MSA.1 (2)	FMT_MSA.1 (2)	Management of security attributes (2)
	FMT_MSA.1 (3)		Management of security attributes (3)

	AP-MRPP	TF-MRPP	CC FUNCTIONAL COMPONENT DESCRIPTION
	FMT_MSA.1 (4)		Management of security attributes (4)
	FMT_MSA.3	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1 (1)	FMT_MTD.1 (1)	Management of TSF data (1)
	FMT_MTD.1 (2)	FMT_MTD.1 (2)	Management of TSF data (2)
	FMT_MTD.2	FMT_MTD.2	Management of limits on TSF data
	FDP_RIP.1	FDP_RIP.1	Subset residual information protection
	FCS_COP.1	FCS_COP.1	Cryptographic operation
	FPT_RVM.1	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	FPT_SEP.1	TSF domain separation
	FPT_STM.1	FPT_STM.1	Reliable time stamps
	FAU_GEN.1	FAU_GEN.1	Audit data generation
	FAU_SAR.1	FAU_SAR.1	Audit review
	FAU_SAR.3	FAU_SAR.3	Selectable audit review
	FAU_STG.1	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	FAU_STG.4	Prevention of audit data loss
	FMT_MOF.1 (1)	FMT_MOF.1 (1)	Management of security functions behavior (1)
	FMT_MOF.1 (2)	FMT_MOF.1 (2)	Management of security functions behavior (2)

In general, the Strength of Function for this TOE is SOF-Medium. Specific strength of function metrics are provided for FIA_UAU.5 - Strength of Function is in compliance with the "Statistical random number generator tests" found in section 4.11.1 of FIPS PUB 140-1 and the "Continuous random number generator test" found in section 4.11.2 of FIPS PUB 140-1 [4]. Strength of function for the password authentication mechanism is that the probability that authentication data can be guessed is no greater than one in two to the fortieth (2^40). The single-use and password authentication mechanisms must demonstrate SOF-medium, as defined in Part 1 of the CC.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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

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

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

c) [the events in Table 5].

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, outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 5].

Dependencies: FPT_STM.1 Reliable Time Stamps.

Table 5 - Auditable Events (Table 5.2 in TF-MRPP & AP-MRPP)

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role. Unsuccessful attempts to authenticate the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role. The user identity and the role.
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.
FIA_UAU.5	The final decision on authentication.	The user identity and the success or failure of the authentication.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorized administrator of the users capability to authenticate.**	The identity of the offending user and the authorized administrator.
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation.

Note: The requirement to audit contents of functional component FCS_COP.1 is not applicable to this ST as both the protection profiles (i.e., TF-MRPP & AP-MRPP) used to instantiate this ST make Remote Administration an optional component. Since the TOE does not claim remote administration, and hence compliance to the FCS_COP.1, this requirement is therefore outside the scope of the TOE and as such is not implemented or included here.

5.1.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1 - The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] 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.

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.3 FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

FAU_SAR.3.1 - The TSF shall provide the ability to perform *searches and sorting* of audit data based on:

a) [user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times;

e) ranges of addresses].

Application Note: Searching and Sorting is provided by a query tool builtin the TOE.

Dependencies: FAU_SAR.1 Audit Review.

5.1.1.4 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

FAU_STG.1.1 - The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 - The TSF shall be able to *prevent* **unauthorized** modifications to the audit records **in the audit trail**.

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.1.5 FAU_STG.4 Prevention of Audit Data Loss

Hierarchical to: FAU_STG.3 Action in Case of Possible Audit Data Loss.

FAU_STG.4.1 - The TSF shall *prevent auditable events, except those taken by the authorized **administrator*** and [shall limit the number of audit records lost] if the audit trail is full.

Application Note: The 'Security Requirements Rationale' section provides an analysis of the maximum amount of audit data that might be lost in the event of audit storage failure, exhaustion and/or attack.

Dependencies: FAU_STG.1 Protected Audit Trail Storage.

5.1.2 User Data Protection (FDP)

Requirements Overview: This Security Target consists of multiple information flow control Security Function Policies (SFPs). The CC allows multiple policies to exist, each having a unique name. This is accomplished by iterating FDP_IFC.1 for each of the two named information flow control policies. The first policy identified is called the UNAUTHENTICATED SFP. The subjects under control of this policy are external IT entities on an internal or external network sending information through the TOE to other external IT entities. The second policy identified is called the AUTHENTICATED SFP. The subjects under control of this policy are human users on an internal or external network who must be authenticated at the TOE before using the services in FIA_UAU.5. The information flowing between subjects in both policies is traffic with attributes, defined in FDP_IFF.1.1, including source and destination addresses. The rules that define each information flow-control SFP are found in FDP_IFF.1.2. Component FDP_IFF.1 is iterated twice to correspond to each of the two iterations of FDP_IFC.1.

5.1.2.1 FDP_IFC.1 Subset Information Flow Control (1)

Hierarchical to: No other components.

FDP_IFC.1.1 - The TSF shall enforce the [UNAUTHENTICATED SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

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

c) operation: pass information **with Network Address Translation**].

Dependencies: FDP_IFF.1 Simple Security Attributes (1).

5.1.2.2 FDP_IFC.1 Subset Information Flow Control (2)

Hierarchical to: No other components.

FDP_IFC.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] on:

a. [subjects: a human user or external IT entity that sends and receives FTP and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.5,

b. information: FTP and Telnet traffic sent through the TOE from one subject to another;

c. operation: initiate service and pass information **with Network Address Translation**].

Dependencies: FDP_IFF.1 Simple Security Attributes (2).

5.1.2.3 FDP_IFF.1 Simple Security Attributes (1)

Hierarchical to: No other components.

FDP_IFF.1.1 - The TSF shall enforce the [UNAUTHENTICATED SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address;
- **and no additional subject security attributes**

b) information security attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service;
- **and no additional information security attributes**].

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 on an internal network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3 - The TSF shall enforce the **following information flow control rules:** [**no additional information control SFP rules**].[12]

FDP_IFF.1.4 - The TSF shall provide the following [**no additional SFP capabilities**].[12]

FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based upon the following rules: [**no explicit authorization rules**].[12]

FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based upon 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;

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

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

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) For application protocols HTTP and SMTP supported by the TOE, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC). This shall be accomplished through protocol filtering proxies that are designed for that purpose.]

Application Note: The generalized wording of FDP_IFF.1.6f (1) has been modified from the PP to highlight that only HTTP and SMTP proxies are included in the TOE. The DNS & POP3 application level proxies are not included in the TOE and hence are not applicabple.

Dependencies: FDP_IFC.1 Subset Information Flow Control (1),

FMT_MSA.3 Static Attribute Initialization.

5.1.2.4 FDP_IFF.1 Simple Security Attributes (2)

Hierarchical to: No other components.

FDP_IFF.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] based on **at least** the following types of subject and information security attributes

a) [subject security attributes:

[12] This change has been made to conform to U.S. Interpretation I-0407.

- presumed address;
- **no additional subject security attributes**;

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 and Telnet);
- security-relevant service command; and
- **no additional information security attributes**].

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 on an internal network can cause information to flow through the TOE to another connected network if:

- the human user initiating the information flow authenticates according FIA_UAU.5;[13]
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

[13] There is a typographical error in the AP-MRPP with respect to FDP_IFF.1(1) and FDP_IFF.1(2). The PP authors have included the phrase, "the human user initiating the information flow authenticates according to FIA_UAU.5," in FDP_IFF.1.2(1) UNAUTHENTICATED SFPs and it is absent in FDP_IFF.1.2(2) AUTHENTICATED SFPs, where it really belongs. This has been rectified in this ST. For details please refer to the 'Precedent Database' at http://niap.nist.gov/cc-scheme/PD/0026.html.

- the human user initiating the information flow authenticates according FIA_UAU.5[13]
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3 - The TSF shall enforce the **following information flow control rules:** [**no additional information control SFP rules**].[14]

FDP_IFF.1.4 - The TSF shall provide the following [**no additional SFP capabilities**].[14]

FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based upon the following rules: [**no explicit authorization rules**].[14]

FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based upon 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;

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

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

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) The TOE shall reject Telnet or FTP command requests that do not conform to generally accepted published protocol definitions (e.g., RFCs). This must be accomplished through protocol filtering proxies designed for that purpose.]

[14] This change has been made to conform to U.S. Interpretation I-0407.

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. A "service command", also mentioned FDP_IFF.1.1(b), could be identified, for example, in the case of the File Transport protocol (FTP) service as an FTP STOR or FTP RETR.

Dependencies: FDP_IFC.1 Subset Information Flow Control (2),

FMT_MSA.3 Static Attribute Initialization

5.1.2.5 FDP_RIP.1 Subset Residual Information Protection

Hierarchical to: No other components.

FDP_RIP.1.1 - The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* [all objects].

Application Note: This requirement is met by zeroing all de-allocated and newly allocated memory pages.

Dependencies: No dependencies.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1 Authentication Failure Handling[15]

Hierarchical to: No other components.

FIA_AFL.1.1 - The TSF shall detect when [**an administrator configurable positive integer within a range of 1-3**] **of** unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access].

FIA_AFL.1.2 - When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question.]

Dependencies: FIA_UAU.1 Timing of Authentication.

5.1.3.2 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.

[15] The TOE does not claim the optional remote administration functionality and hence the SFR, FIA_AFL.1, as mentioned in the TF-MRPP and AP-MRPP is not applicable to the TOE. It has however been included in this ST to handle authentication failure handling of the remote proxy (telnet, ftp) users and local administrator as required by the AP-MRPP and TF-MRPP.

FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;

b) association of a human user with the authorized administrator role;

c) **and no additional security attributes**].

Dependencies: No dependencies.

5.1.3.3 FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 - The TSF shall provide [password and single-use authentication mechanisms] to support user authentication.

FIA_UAU.5.2 - The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:

a) single-use authentication mechanism shall be used for authorized administrators to ace ss the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.[16]

b) Single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity[16];

c) single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user;

d) reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator].

Application Note: Rules a and b are not applicable because the TOE does not claim conformance to the optional remote administrator access or for authorized external IT entities.

Dependencies: No dependencies.

[16] The TOE does not claim conformance to the optional remote administration. As a result, single use authentication required by administrators for remote access or by authorized external IT entities is not applicable to this TOE. This functional requirement has only been duplicated here for completeness.

5.1.3.4 FIA_UID.2 User Identification Before any Action

Hierarchical to: No other components.

FIA_UID.2.1 - The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of Security Functions Behavior (1)

Hierarchical to: No other components.

FMT_MOF.1.1(1) - The TSF shall restrict the ability to *enable, disable* the functions

a) [operation of the TOE;

b) multiple use authentication functions described in FIA_UAU.5]

to [an authorized administrator].

Application Note: By "Operation of the TOE" in a) above, we mean having the TOE start up (enable operation) and shut down (disable operation). By "multiple use" in b) above, we mean the management of password and single-use authentication mechanisms.

Dependencies: FMT_SMR.1 Security Roles.

FMT_SMF.1 Specification of Management Function[17]

5.1.4.2 FMT_MOF.1 Management of Security Functions Behavior (2)

Hierarchical to: No other components.

FMT_MOF.1.1(2) - The TSF shall restrict the ability to *enable, disable, determine and modify the behavior* of the functions

a) [audit trail management;

b) backup and restore for TSF data, information flow rules, and audit trail data; and

c) communication of authorized external IT entities with the TOE] to [an authorized administrator].

[17] The SFRs FMT_MOF.1 (1-2), FMT_MSA.1 (1-4) and FMT_MTD.1 (1-2) have a dependency on the SFR FMT_SMF.1 (which is a new addition to the CC Part 2 version 2.2). Albeit the two protection profiles used to instantiate this ST did not include the mentioned dependency, as they were evaluated against CC Part 2 version 2.1, this ST has included the mentioned dependency for each one of the specified SFRs. Please refer to [CC2] document to view the SFR FMT_SMF.1.

Application Note: Determine and modify the behavior of element c (communication of authorized external IT entities with the TOE) is intended to cover functionality such as providing a range of addresses from which the authorized external entity can connect.

Dependencies: FMT_SMR.1 Security Roles.

FMT_SMF.1 Specification of Management Function[17]

5.1.4.3 FMT_MSA.1 Management of Security Attributes (1)

Hierarchical to: No other components.

FMT_MSA.1.1 (1) - The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, and add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(1)] to [the authorized administrator].

Dependencies: FDP_IFC.1 Subset Information Flow Control(1), FMT_SMR.1 Security Roles, FMT_SMF.1 Specification of Management Function[17].

5.1.4.4 FMT_MSA.1 Management of Security Attributes (2)

Hierarchical to: No other components.

FMT_MSA.1.1 (2) - The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF.1(2)] to [the authorized administrator].

Dependencies: FDP_IFC.1 Subset Information Flow Control(2), FMT_SMR.1 Security Roles, FMT_SMF.1 Specification of Management Function[17].

5.1.4.5 FMT_MSA.1 Management of Security Attributes (3)

Hierarchical to: No other components.

FMT_MSA.1.1 (3) - The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the authorized administrator].

Dependencies: FDP_IFC.1 Subset Information Flow Control(1), FMT_SMR.1 Security Roles, FMT_SMF.1 Specification of Management Function[17].

5.1.4.6 FMT_MSA.1 Management of Security Attributes (4)

Hierarchical to: No other components.

FMT_MSA.1.1(4) - The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF.1(2)] to [the authorized administrator].

Dependencies: FDP_IFC.1 Subset Information Flow Control(2), FMT_SMR.1 Security Roles, FMT_SMF.1 Specification of Management Function[17].

5.1.4.7 FMT_MSA.3 Static Attribute Initialization

Hierarchical to: No other components.

FMT_MSA.3.1 - The TSF shall enforce the [UNAUTHENTICATED_SFP and AUTHENTICATED_SFP] to provide *restrictive* default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2 - The TSF shall allow the [the authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

Application Note: Following TOE installation, the default configuration is to allow no traffic through the firewall. The default values for the information flow control security attributes appearing in FDP_IFF.1 (1) and FDP_IFF.1 (2) are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

Dependencies: FMT_MSA.1 Management of Security Attributes (1-4),

FMT_SMR.1 Security Roles.

5.1.4.8 FMT_MTD.1 Management of TSF Data (1)

Hierarchical to: No other components.

FMT_MTD.1.1 (1) - The TSF shall restrict the ability to *query, modify, delete,* [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

Dependencies: FMT_SMR.1 Security Roles, FMT_SMF.1 Specification of Management Function[17].

5.1.4.9 FMT_MTD.1 Management of TSF Data (2)

Hierarchical to: No other components.

FMT_MTD.1.1 (2) - The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

Dependencies: FMT_SMR.1 Security Roles, FMT_SMF.1 Specification of Management Function[17].

5.1.4.10 FMT_MTD.2 Management of Limits on TSF Data

Hierarchical to: No other components.

FMT_MTD.2.1 - The TSF shall restrict the specification of the limits for [the number of authentication failures] to [the authorized administrator].

FMT_MTD.2.2 - The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions specified in FIA_AFL.1.2].

Dependencies: FMT_MTD.1 Management of TSF Data (1-2),
FMT_SMR.1 Security Roles.

5.1.4.11 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 - The TSF shall maintain the role [authorized administrator].

FMT_SMR.1.2 - The TSF shall be able to associate **human** users with **the authorized administrator** role**.**

Dependencies: No dependencies.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

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.

Dependencies: No dependencies.

5.1.5.2 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

FPT_SEP.1.1 - The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 - The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.1.5.3 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time-stamps for its own use.

Application Note: The word “reliable” in the above requirement means that the order of the occurrence of auditable events is preserved

Dependencies: No dependencies.

5.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL4 augmented[18] which are summarized in Table 6 - below.

Table 6 - Assurance Requirements of the TOE: EAL4 Augmented

Assurance Class	Component ID	Component Title
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.2	Fully Defined External Interfaces
	ADV_HLD.2	Security Enforcing High-Level Design
	ADV_IMP.1	Subset of the Implementation of the TSF
	ADV_LLD.1	Descriptive Low-Level design
	ADV_RCR.1	Informal Correspondence Demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model

[18] The 'Assurance Requirements' mentioned in **Error! Reference source not found.** (EAL4 Augmented) are as per the 'Assurance Requirements' mentioned in 'Common Criteria for Information Technology Security Evaluation Part 3 (CC3)'.

Assurance Class	Component ID	Component Title
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.3	Systematic Flaw Remediation.
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE Security Function Evaluation
	AVA_VLA.2	Independent Vulnerability Analysis

5.2.1 Additional Security Assurance Requirements

EAL4 was chosen for a moderate to high level of independently assured security in line with strong commercial development practices. This section describes the maintenance assurance requirements from the CC Part 3 that the TOE must satisfy in **addition** to the previously listed EAL 4 SARs.

The ALC_FLR.3, Systematic Flaw Remediation was added to augment the EAL4 level of evaluation . This augmentation, which is in line with the robust 'Software Development Life Cycle (SDLC)' model already being followed by the TOE developer, was included due to the strong consumer demand that the developer be able to systematically receive security flaw reports, fix security flaws and dispatch corrective fixes to the TOE users in a systematic, secure and a timely manner. ALC_FLR.3 is not included in any EAL. This additional SAR is restated verbatim from the CC.

5.3 Security Requirements for the IT Environment

There are no explicit security requirements on the IT Security Environment.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

The security functions implemented by the TOE are:

TIME — The TIME function maintains a reliable timestamp based on an initial time obtained from the hardware platform. The TIME function then maintains a software clock within the control of the TOE for stamping audit records and synchronizes the software and hardware clocks so that consistent time is maintained during operation of the TOE and at each boot up. The TIME function provides the timestamp to the functions that generate audit records, and to the audit reviewing functions thereby contributing in the audit trail generation mechanism.

INTERCEPT — The INTERCEPT function intercepts packets with the help of the external NIC card. The NIC card performs basic address recognition checks on all packets and filters out any that have a destination address different from that of the NIC card itself. It subsequently transfers all accepted packets to the other TOE security functions for filtering. CyberGuard Firewall CGLinux kernel includes enhancements to the IP packet handling software that ensure that all packets are forwarded to, and processed through the filtering functions and that the filtering functions are not bypassable.

REAPER — The REAPER function clears a released memory resource before it can be re-used. CyberGuard Firewall CGLinux kernel contains enhancements to the routines that free memory upon release/de-allocation. These enhancements ensure that the routines that free memory upon release/de-allocation also clear the contents of the freed memory before its reuse. This memory content clearing mechanism results in residual information protection.

NAT — When configured for address translation, the TOE re-writes the headers of IP packets flowing from the internal network to the external network, so that the real addresses of internal hosts are hidden.

IAC — The IAC function provides internal access control. It is an extension to the CGLinux kernel and controls the kernel's access routines and enforces roles and credentials to provide separation of processes and data on the CyberGuard Firewall to ensure that errors in non-trusted portions of the firewall cannot propagate to the TOE security functions and non-authorized entities can not modify its trusted security enforcing functions.

AUD_PROC — The AUD_PROC function allows an authorized administrator to review and clear audit records. The AUD_PROC function provides a mechanism to allow itself and other Sub-Systems to submit significant event information for storage and reporting. It collects the audit records

submitted by the various functions of the TOE. The AUD_PROC function provides an interface with the MGM function that allows these records to be searched, sorted, displayed, and evaluated in compliance with the protection profile search/sort parameters. Before allowing access to the audit records, the AUD_PROC function uses the AUTH function to authenticate the authorized administrator. All successful and unsuccessful attempts by an authorized administrator to access/manage the audit subsystem (in compliance with the 'management of security functions behavior' stated in the CC requirements) are also audited.

The AUD_PROC function allows the authorized administrator to review the audit records based on user identity, network addresses, ranges of dates and times, and ranges of addresses. If the audit trail is full i.e. maximum allowed disk utilization percentage is reached, the AUD_PROC function initiates a controlled shut down of the TOE and all traffic flowing through it. The controlled shutdown process is audited and results in the complete switching-off (power-off) of the TOE and all traffic flowing through it. Since the TOE is switched-off in a controlled manner when the audit trail reaches the maximum allowed disk space, there is no loss of audit trail data.

PF

The PF function filters packets received from the INTERCEPT function depending on rules selected by the PF_Rule_Select function.

The PF function discards any IP packets that are received on either an internal or an external network interface in compliance with the common criteria requirements for information control policy/functions mentioned in the Protection Profiles used to instantiate this security target.

If these steps have not discarded the packet, the PF function interfaces with the PF_Rule_Select function to find the packet filter rule to apply to the packet. If no packet filter rule is found, the PF function discards the packet. If a packet filter rule is found, the PF function applies the rule found to the packet.

Depending upon the result of how the packet filter rules are applied to corresponding packets, the PF decides if packets are dropped, passed through, or passed to a proxy. If the packet is dropped, a destination unreachable message will be sent only if indicated by the rule. The PF function also participates in audit data generation by passing audit records to the AUD_PROC function containing the results of all decisions regarding information flow, and the presumed addresses of the source and destination of the packets. The PF function passes packets to the FTP_Proxy and Telnet_Proxy functions if the rule found indicates that the packet should be passed to a proxy. An additional criterion that may be specified in the packet filter rule is the list of senders and recipients to whom the rule applies. The PF function interrogates the packet filter rules to determine the senders and recipients to whom the rule applies and

subsequently prompts the applicable proxy to identify a user via the AUTH function.

PF_Rule_Select The PF_Rule_Select function 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 that matches the source, destination, service, and protocol characteristics of a given IP packet.

The rule set is established by the MGM function, and passed to the PF_Rule_Select function. Source and destination addresses, service and protocol, potential results and modifiers specify the rules. Source and Destination addresses are specified by pairwise combinations of individual hosts, subnets, or networks, the firewall itself, or all traffic via a specific port. Service and protocol are specified by service/protocol pair, all protocols, or ICMP. Potential results are one of permit, deny and proxy. Modifiers include restrictions on port ranges, and enabling replies, which allows a back-channel if attached to a permit result, and sends a destination-unreachable if attached to a deny rule.

Telnet_Proxy The telnet service is an application that is typically used to allow a user to log into a remote machine. This is done by allowing a user on a client system to interactively start a login session on a remote system. Once the login session is established the client process passes the input to the server process, which performs the required tasks on the remote system, and transmits the output back to the client. To protect against intruders, 'CyberGuard Firewall/VPN version 6.2.1' uses the Telnet_Proxy as a more secure channel. When a connection is requested, the Telnet-Proxy responds instead of the actual telnet service and since each connection request is forwarded to the Telnet_Proxy running on the TOE it is not possible for external hosts to access IP addresses of internal networks. The AUTH function performs authentication and passes audit records to the AUD_PROC function containing among other parameters the applicable user identity, session ID and the sensor value[19]. These parameters that are used in the overall composition of the 'Telnet Proxy' related audit trail records are made available to the AUTH and the AUD_PROC functions by the Telnet_Proxy function. The Telnet_Proxy function also ensures that the telnet protocol in use meets the generally accepted published protocol definitions.

FTP_Proxy The FTP service is an application that is typically used to allow a user to log into a remote machine. This is done by allowing a user on a client system to interactively start a login session on a remote system. Once the login session is established the client process passes the input to the server process, which performs the required tasks on the remote system, and transmits the output back to the client. To protect against intruders,

[19] Sensor value contains the name of the sub-system that has generated the audit record.

'CyberGuard Firewall/VPN version 6.2.1' uses an FTP_Proxy as a more secure channel. When a connection is requested, the FTP_Proxy responds instead of the actual ftp service and since each connection request is forwarded to the FTP_Proxy running on the TOE it is not possible for external hosts to access IP addresses of internal networks. The FTP_Proxy function passes information through the TOE after requiring the user to undergo Identification & Authentication using the AUTH function. The AUTH function performs authentication and passes audit records to the AUD_PROC function containing among other parameters the applicable user identity, session ID and the sensor[19] value. These parameters that are used in the overall composition of the 'FTP Proxy' related audit trail records are made available to the AUTH and the AUD_PROC functions by the FTP_Proxy. The FTP_Proxy function also ensures that the FTP protocol in use meets the generally accepted published protocol definitions.

HTTP_Proxy Hypertext Transfer Protocol (HTTP) is the primary network protocol that is used to transfer hypertext documents and related resources across the Internet from servers to clients. The 'CyberGuard Firewall/VPN version 6.2.1' uses the HTTP_Proxy to secure an enterprise's HTTP traffic by impersonating a server when communicating with a client and optionally impersonating a client when communicating with a server. It does this by intercepting HTTP packets going through the firewall and applying redirection and filtering services to the packets. Redirection service allows the HTTP_Proxy to allocate the identity of the actual server. Filtering service allows the HTTP_Proxy to examine the contents of the HTTP packets and secure the HTTP traffic flowing into and out of the networks.

The HTTP_Proxy can operate as a transparent or nontransparent proxy. If operating as a transparent proxy, the HTTP_Proxy intercepts HTTP traffic without the knowledge of HTTP clients (e.g., Web browsers). If operating as a nontransparent proxy, the client is aware of the existence of the proxy and connects directly to it or a virtual address handled by the proxy. The HTTP_Proxy redirects the session to an actual server address. In this mode, the HTTP_Proxy provides the additional capabilities of client authentication.

The HTTP_Proxy function also ensures that the HTTP protocol in use meets the generally accepted published protocol definitions and audits all related information flow requests via the AUD_PROC function. These audit records contain the presumed addresss of both the source and the destination subjects.

SMTP_Proxy Simple Mail Transfer Protocol (SMTP) is a store-and-forward protocol used by mail transfer agents[20] to transfer electronic mail messages. The

[20] A Mail Transfer Agent (MTA) is a service that examines an electronic mail message to determine who the recipients are and how to forward the mail message to those recipients.

'CyberGuard Firewall/VPN version 6.2.1' uses the SMTP_Proxy to secure an enterprise's SMTP traffic by impersonating a server when communicating with a client and optionally impersonating a client when communicating with a server. It does this by intercepting SMTP packets going through the firewall and applying redirection and filtering mechanisms to the packets.

Via redirection the SMTP_Proxy allocates the identity of the actual server at configuration time.

Via the filtering mechanism the SMTP_Proxy examines the contents of the SMTP packets that flow between the client and server, it. This allows the SMTP proxy to secure the SMTP traffic flowing into and out of the networks at both a low level (i.e., mail connections and commands) and a high level (i.e., mail headers, messages, and attachments). It allows the SMTP_proxy to hide information about the internal networks by deleting message headers and changing the mailboxes found in the message headers.

The SMTP_Proxy function also ensures that the SMTP protocol in use meets the generally accepted published protocol definitions and audits all related information flow requests via the AUD_PROC function. These audit records contain the presumed addresss of both the source and the destination subjects.

AUTH

The AUTH function provides the challenge and response for user authentication. It supports username/password authentication as well as the single-use authentication mechanism via the RSA Authentication Manager 6.0. The function that requires authentication passes the identity of the user to the AUTH function, which selects the appropriate type of authentication for the user and application.

The TOE Authentication policy determines how the AUTH function will authenticate the client of a network session. It is expressed with an ordered list of authentication rules which are configured via the MGM function. Each rule associates an authenticator (Radius, 'single use' Authenticator or Internal, 'multiple use' Authenticator) with the conditions under which to invoke that authenticator. These conditions include the rule's service, source, destination, and application condition categories.

A network session matches a rule only if it matches the rule's service, source, destination, and application condition categories. A network session matches a category if it matches any of the objects in the category. The way in which a network session matches an object in a category varies with the type of object. Generally, if an object specifies several criteria, a network session must match all of those criteria

The AUTH function identifies the rule that a network session matches and the authenticator associated with that rule. It then invokes the authenticator. When an authenticator is invoked, it will succeed or fail

authentication. Network sessions related to the he 'FTP_Proxy' and the 'Telnet_Proxy' are assigned 'Authentication Rules' that have the 'Radius Authenticator' (for single-use authentication) associated with them.

If a network session does not match any of the authentication rules, the firewall invokes a special **Deny** authenticator that conducts an authentication dialog but fails all authentication requests.

The AUTH function performs the authentication as described above and returns the results to the calling function. The AUTH function locks the user if there are excessive user authentication failures. The AUTH function as mentioned above supports authentication requests from the FTP_Proxy, Telnet_Proxy, and MGM functions.

The AUTH function interfaces with the MGM function to receive the lists of users, authentication mechanisms and applications, the setting for how many failures to allow, and to reset locked accounts. The AUTH function passes audit records to the AUD_PROC function containing the user identity, session GroupId, sensor value, authenticator type, and the results of the attempt (i.e., either successful and unsuccessful) thereby forming the source of authentication related audit trails to the AUD_PROC function.

The single use authentication mechanism is in compliance with the "Statistical random number generator tests" found in section 4.11.1 of FIPS PUB 140-1 and the "Continuous random number generator test" found in section 4.11.2 of FIPS PUB 140-1. The password authentication mechanism requires a minimum of 8 character passwords. Each one of the 8 characters in the password is allowed any one of the following 95 ASCII values:

32	sp	33	!	34	"	35	#	36	$	37	%	38	&	39	'
40	(	41	)	42	*	43	+	44	,	45	-	46	.	47	/
48	0	49	1	50	2	51	3	52	4	53	5	54	6	55	7
56	8	57	9	58	:	59	;	60	<	61	=	62	>	63	?
64	@	65	A	66	B	67	C	68	D	69	E	70	F	71	G
72	H	73	I	74	J	75	K	76	L	77	M	78	N	79	O
80	P	81	Q	82	R	83	S	84	T	85	U	86	V	87	W
88	X	89	Y	90	Z	91	[	92	\	93	]	94	^	95	_
96	`	97	a	98	b	99	c	100	d	101	e	102	f	103	g
104	h	105	i	106	j	107	k	108	l	109	m	110	n	111	o
112	p	113	q	114	r	115	s	116	t	117	u	118	v	119	w
120	x	121	y	122	z	123	{	124	|	125	}	126	~		

Thus, there are 95^8 = 6,634,204,312,890,625 potential password combinations implying that the probability that the authentication data can be guessed is no greater than one in ninety five to the power eight (95 ^ 8). This demonstrates that for password authentication the probability that the authentication data can be guessed is even lower than the common

criteria requirements of one in two to the power forty (2^40 = 1,099,511,627,776) as specified in the Protection Profiles used to instantiate this security target. The Strength of Function for the AUTH function hence complies with SOF-medium.

MGM

The MGM function provides the authorized administrator the ability to manage the TOE. The MGM function via the GUI interface allows the authorized administrator to configure, manage and review the TOE. It also provides the authorized administrator the ability to setup queries to view the audit trails stored in the audit sub-system via the GUI. The MGM will force the user to authenticate by calling the AUTH function before taking any action. The below mentioned items are managed through the MGM function which also generates audit events for all management control functions (which for example include, login, logout, system startup and shutdown, user un-blacklisting etc.) and sends them to the AUD_PROC function thereby contributing in the generation of corresponding audit trail records.

A) Rules selected by the PF_Rule_Select function.

B) Time reported by the TIME function

C) User identities and assignment of those identities to the authorized administrator roles.

D) Authentication mechanisms to be used by the AUTH function.

E) Thresholds for reactions to authentication failure, used by the AUTH function.

F) Unlocking accounts locked by the AUTH function.

G) Privileged and protected items for use by the IAC function.

H) Maximum allowed disk utilization percentage for audit trails.

I) Controlled/Scheduled system startup and shutdown.

J) Audit Trail display and view.

Audit trails for all other functions are generated and stored via the AUD_PROC function by their respective security functions.

Note:

The strength of function requirement applies to password authentication mechanism. The related IT security function is AUTH. The Strength of Function claim for the password authentication mechanism is SOF Medium. Overall SOF requirement for the TSF, aside from the specific Strength of Function claimed for the authentication function, is SOF-Medium. All TOE security functions are implemented in accordance with a strength of SOF-Medium [CC1].

6.2 TOE Security Function Rationale

Table 7 - demonstrates the correspondence between the security functional requirements (from both PPs) identified in Sections 5.1 and the TOE security functions identified in Section 6.1.

Table 7 - Mappings Between TOE SFRs and TOE Security Functions

	TIME	INTERCEPT	REAPER	IAC	AUD_PROC	NAT	PF	PF_RULE_SELECT	TELNET_PROXY	FTP_PROXY	HTTP_Proxy	SMTP_Proxy	AUTH	MGM
FAU_GEN.1	X				X		X						X	X
FAU_SAR.1					X									X
FAU_SAR.3					X									X
FAU_STG.1				X										
FAU_STG.4				X	X									X
FDP_IFC.1(1)						X	X	X			X	X		
FDP_IFC.1(2)						X	X	X	X	X				
FDP_IFF.1(1)						X	X	X			X	X		
FDP_IFF.1(2)						X	X	X	X	X				
FDP_RIP.1			X											
FIA_AFL.1													X	X
FIA_ATD.1														X
FIA_UAU.5									X	X			X	X
FIA_UID.2							X	X	X	X				X
FMT_MOF.1(1)				X									X	X
FMT_MOF.1(2)				X									X	X
FMT_MSA.1(1)				X									X	X
FMT_MSA.1(2)				X									X	X
FMT_MSA.1(3)				X									X	X
FMT_MSA.1(4)				X									X	X
FMT_MSA.3				X									X	X

	TIME	INTERCEPT	REAPER	IAC	AUD_PROC	NAT	PF	PF_RULE_SELECT	TELNET_PROXY	FTP_PROXY	HTTP_Proxy	SMTP_Proxy	AUTH	MGM
FMT_MTD.1(1)				X									X	X
FMT_MTD.1(2)				X									X	X
FMT_MTD.2				X									X	X
FMT_SMR.1														X
FPT_RVM.1		X												X
FPT_SEP.1				X										
FPT_STM.1	X													

6.2.1 FAU_GEN.1

In order to meet FAU_GEN.1 the TSF must generate an audit record of a listed set of auditable events, with additional information as required to meet the SFR. The TOE Security function that processes the auditable event generates the audit record, and sends it to the AUD_PROC function for processing. All audit records include identity of the subject that caused the event, the outcome of the event, and the date and time of the event, as reported by the TIME function. The following table lists the events required and the TSF that is the source of the event, and the additional information in the audit record. This additional information meets the requirements for the additional audit record contents in Table 5 - above.

Table 8 - TSF Sources of Audit Data

Functional Component	Auditable Event	TSF Source	Additional Audit Record Contents
FDP_IFF.1	All decisions on requests for information flow.	PF	The presumed addresses of the source and destination subject.
FMT_SMR.1	Modifications to the group of users that are part of the authorized administrator role. Unsuccessful attempts to authenticate the authorized	MGM	The identity of the authorized administrator performing the modification and the user identity being associated with the

Functional Component	Auditable Event	TSF Source	Additional Audit Record Contents
	administrator role.		authorized administrator role.
FIA_UID.2	All use of the user identification mechanism.	AUTH	The user identities provided to the TOE.
FIA_UAU.5	The final decision on authentication.	AUTH	The user identitiy and the success or failure of the authentication.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the user's capability to authenticate.	AUTH and MGM	The identity of the offending user and the authorized administrator.
FMT_STM.1	Changes to the time.	MGM	The identity of the authorized administrator performing the operation.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	AUD_PROC	The identity of the authorized administrator performing the operation.

6.2.2 FAU_SAR.1

In order to meet FAU_SAR.1, the TSF must provide the authorized administrator the ability to review the audit data. The AUD_PROC function provides this ability via the graphical user interfaces of the MGM function.

6.2.3 FAU_SAR.3

In order to meet FAU_SAR.3, the TSF must provide the ability to perform searches and sorting of audit data based on user identity, presumed addresses, ranges of dates, times and addresses. This function is provided through the AUD_PROC function, and is accessible via the graphical user interfaces of the MGM function.

6.2.4 FAU_STG.1

In order to meet FAU_STG.1, the TSF must protect audit records from unauthorized deletion or any modification. The IAC function protects the records from unauthorized deletion or any modification.

6.2.5 FAU_STG.4

When the audit trail is full, the AUD_PROC function contacts the MGM function, which shuts down the TOE to prevent future auditable events. This addresses the requirement to prevent loss of audit data, which is FAU_STG.4. If the audit trail is full i.e. maximum allowed disk utilization percentage is reached, the AUD_PROC function *initiates* a controlled shut down of the TOE and all traffic flowing through it. The controlled shutdown process is audited and results in the complete switching-off (power-off) of the TOE and all traffic flowing through it. Since the TOE is switched-off in a controlled manner when the audit trail reaches the maximum allowed disk space, there is no loss of audit trail data. The IAC function, which enforces roles and credentials to provide separation of data and processes, is responsible for ensuring that only the AUD_PROC function can *initiate* the shutdown of the TOE in the event the audit trail reaches the maximum allowed disk space.

6.2.6 FDP_IFC.1(1)[21]

In order to meet FDP_IFC.1 (1), the TSF must enforce the UNAUTHENTICATED_SFP that covers the exchange of information between unauthenticated external IT entities through the TOE. The NAT and PF functions in conjunction with the 'SMTP_Proxy' and the 'HTTP_Proxy' addresses this requirement by enforcing the rules provided by the PF_Rule_Select function on IP packets passed through the TOE.

6.2.7 FDP_IFC.1(2)[22]

In order to meet FDP_IFC.1 (2), the TSF must enforce the AUTHENTICATED_SFP that covers the exchange of information between authenticated external IT entities through the TOE. The NAT & PF functions in conjunction with the 'Telnet_Proxy' and the 'FTP_Proxy' addresses this requirement by enforcing the rules provided by the PF_Rule_Select function on IP packets passed through the TOE.

---

[21] The unauthenticated information flow control policy (UNAUTHENTICATED _SFP) is collectively enforced by the FDP_IFC.1 (1) & FDP_IFF.1 (1) functional components. While, the FDP_IFC.1 (1) functional component at a high level lists the entities [namely: 'subjects', 'information flow control' and 'operation'] on which the SFP applies, the corresponding FDP_IFF.1 (1) functional component defines the attributes for these entities. Hence all security functions that satisfy the FDP_IFC.1 (1) must also satisfy FDP_IFF.1 (1).

[22] The authenticated information flow control policy (AUTHENTICATED _SFP) is collectively enforced by the FDP_IFC.1 (2) & FDP_IFF.1 (2) functional components. While, the FDP_IFC.1 (2) functional component at a high level lists the entities [namely: 'subjects', 'information flow control' and 'operation'] on which the SFP applies, the corresponding FDP_IFF.1 (2) functional component defines the attributes for these entities. Hence all security functions that satisfy the FDP_IFC.1 (2) must also satisfy FDP_IFF.1 (2).

6.2.8 FDP_IFF.1 (1)[21]

In order to meet FDP_IFF.1 (1) the TSF must enforce a set of rules over the information flows. The rules cover cases where information flow is always denied, and allow for the administrator to set rules that accept information flows. The PF function denies information flow by discarding packets. The element FPD_IFF.1.6 requires the TSF to prevent information flow if the addressing makes it unlikely that the packet would have been routed to the TOE. These cases are handled by the PF, HTTP_Proxy & SMTP_Proxy security functions. The rules that explicitly allow information flows, described in FDP_IFF.1.2, are implemented by the PF_Rules_Select function, which implements the rules that allow information flow.

The element FDP_IFF.1.2 also requires the TSF to:

- Permit subjects on an internal network to cause information flow through the TOE to another connected network if the presumed address of the source subject translates to an internal address.
- Permit subjects on external network to cause information flow through the TOE to another connected network: if the presumed address of the source subject, in the information, translates to an external network address and the the presumed address of the destination subject, in the information, translates to an address on the other connected network.

These cases are handled by the NAT security function.

6.2.9 FDP_IFF.1 (2)[22]

In order to meet FDP_IFF.1 (2) the TSF must enforce a set of rules over the information flows. The rules cover cases where information flow is always denied, and allow for the administrator to set rules that accept information flows. The PF function denies information flow by discarding packets. The element FPD_IFF.1.6 requires the TSF to prevent information flow if the addressing makes it unlikely that the packet would have been routed to the TOE. These cases are handled by the PF, FTP_Proxy and Telnet_Proxy functions. The rules that explicitly allow information flows, described in FDP_IFF.1.2, are implemented by:

- The PF_Rule_Select function, which implements the rules that allow information flow.
- The FTP_Proxy and Telnet_Proxy functions that ensure that human users initiating information flow through the TOE are authenticated according to FIA_UAU.5.

The element FDP_IFF.1.2 also requires the TSF to:

- Permit subjects on an internal network to cause information flow through the TOE to another connected network if the presumed address of the source subject translates to an internal address.
- Permit subjects on external network to cause information flow through the TOE to another connected network: if the presumed address of the source subject, in the information, translates to an external network address and the the presumed address of

the destination subject, in the information, translates to an address on the other connected network.

These cases are handled by the NAT security function.

6.2.10 FDP_RIP.1

In order to meet FDP_RIP.1, the TSF must ensure that information content of resources used by the TOE is made unavailable upon the allocation of the resources. The REAPER function implements this requirement by clearing all information from all memory resources upon release of the resource. Since the resource is cleared before release, it remains clear when the resource needs to be allocated again.

6.2.11 FIA_AFL.1

In order to meet FIA_AFL.1, the TSF must detect when a configured number of unsuccessful authentication attempts have been made by a user, and then lock that user out until the authorized administrator takes action. The limit on the number of failed events, and the actions to allow a user access again are implemented by the MGM function. The AUTH function counts the number of failures and locks the user out if the number exceeds that established by the MGM function.

6.2.12 FIA_ATD.1

In order to meet FIA_ATD.1, the TSF must maintain an association between users and the security attributes of identity, authorized administrator role, and proxy user. This list is established and maintained by the MGM function

6.2.13 FIA_UAU.5

In order to meet FIA_UAU.5

- The TSF must successfully authenticate a user before allowing that user administrative or proxy access. This requirement is met in each function that requires authentication: Telnet_Proxy, FTP_Proxy, and MGM, by calling the AUTH function before allowing any action by the users.
- The TSF must also provide password and single-use authentication mechanisms, and use single-use authentication for FTP and Telnet authentication. The AUTH function implements the password and single-use authentication mechanisms, and maintains a list of which authentication mechanisms are appropriate for each types of access. Note that the TOE does not include remote administration, or remote access by authorized IT entities and hence does not claim single use authentication of authorized administrator and IT entities .

6.2.13.1 FIA_UAU.5 Strength of Function

In order to meet the strength of function requirements for FIA_UAU.5 single-use authentication mechanisms must be in compliance with the “Statistical random number

generator tests" found in section 4.11.1 of FIPS PUB 140-1 and the "Continuous random number generator test" found in section 4.11.2 of FIPS PUB 140-1. Strength of function shall be demonstrated for the password authentication mechanism such that the probability that authentication data can be guessed is no greater than one in two to the fortieth (2^40).

Strength of function for single-use authentication mechanisms can be demonstrated by the effective bit strength of the packet. For single use authentication the TOE includes the 'RSA Authentication Manager version 6.0'. The effective bit strength of the packet is as follows:
8 character (Alpha/Numeric) PIN = 41.3 bits
6 digit token = 19.8 bits
Total bit strength = 61.1 bits or 1 in 2,471,341,346,050,066,508

Strength of function for the password authentication mechanisms can be demonstrated by the following calculation: Passwords are required to be a minimum of 8 characters, which can be each by one of 95 values (any upper case or lower case letter, any digit, and all punctuation marks). The chance of guessing a password is therefore 1 in ninety-five to the power eight (95^8), which is even less than the recommended one in two to the fortieth (2^40). The Strength of Function for the AUTH function hence complies with SOF-medium.

6.2.14 FIA_UID.2

In order to meet FIA_UID.2, the TSF must require each user to identify itself before allowing any other TSF-mediated access. For services that require authentication, MGM, Telnet_Proxy, and FTP_Proxy, the function prompts for identity before calling the AUTH function, which occurs before any actions by that function. For normal packet transfer, the presumed identity of the external IT entity is carried in the source and destination addresses of the packet.

6.2.15 FMT_MOF.1 (1)

In order to meet FMT_MOF.1(1), the TSF must restrict the ability to enable or disable the TOE and the single-use authentication functions to the authorized administrator. The MGM function enforces this restriction by requiring the user to successfully authenticate as an authorized administrator, via the AUTH function, before accessing any administrative functions. The IAC function protects modification of these functions by any function except for the MGM function acting on behalf of an authorized administrator.

6.2.16 FMT_MOF.1 (2)

In order to meet FMT_MOF.1(2), the TSF must restrict the ability to enable, disable, or modify the behavior of audit trail management, and backup and restore for TSF data to the authorized administrator. The MGM function enforces this restriction by requiring the user to successfully authenticate as an authorized administrator, via the AUTH function, before accessing any administrative functions. The IAC function protects

modification of these functions by any function except for the MGM function acting on behalf of an authorized administrator.

6.2.17 FMT_MSA.1(1)

In order to meet FMT_MSA.1(1) the TSF must restrict the ability to add, modify, or delete attributes in the unauthenticated SFP information flow control rules to the authorized administrator. The IAC function ensures that only the MGM function can add, delete, or modify the attributes, and the MGM function accesses the AUTH function to ensure that only authorized administrator are allowed to perform any administration.

6.2.18 FMT_MSA.1(2)

In order to meet FMT_MSA.1(2) the TSF must restrict the ability to add, modify, or delete attributes in the authenticated SFP information flow control rules to the authorized administrator. The IAC function ensures that only the MGM function can add, delete, or modify the attributes, and the MGM function accesses the AUTH function to ensure that only authorized administrator are allowed to perform any administration.

6.2.19 FMT_MSA.1(3)

In order to meet FMT_MSA.1(1) the TSF must restrict the ability to create or delete unauthenticated SFP information flow control rules to the authorized administrator. The IAC function ensures that only the MGM function can create or delete rules, and the MGM function accesses the AUTH function to ensure that only authorized administrator are allowed to perform any administration.

6.2.20 FMT_MSA.1(4)

In order to meet FMT_MSA.3(2) the TSF must restrict the ability to create or delete authenticated SFP information flow control rules to the authorized administrator. The IAC function ensures that only the MGM function can create or delete the rules, and the MGM function accesses the AUTH function to ensure that only authorized administrator are allowed to perform any administration.

6.2.21 FMT_MSA.3

In order to meet FMT_MSA.3, the TSF must provide restrictive default values for information flow control security attributes, and allow the authorized administrator to set different default values. The PF function implements a default of deny for any packets for which PF_Rule_Select cannot find a rule. An authorized administrator can override this by using MGM to create a rule for PF_Rule_Select that refers to all addresses. The MGM function accesses the AUTH function to ensure that only authorized administrator are allowed to perform any administration.

6.2.22 FMT_MTD.1 (1)

In order to meet FMT_MTD.1(1), the TSF must restrict the ability to query, modify, or delete the association of users to authorized administrator roles to the authorized administrators. The IAC function ensures that only the MGM function can query, modify, or delete the association between users and authorized administrators. The MGM function accesses the AUTH function to ensure that only authorized administrators are allowed to perform any administration.

6.2.23 FMT_MTD.1 (2)

In order to meet FMT_MTD.1(2), the TSF must restrict the ability to set the date and time used to form timestamps to the authorized administrators. The IAC function ensures that only the MGM function can set the date and time used to form timestamps. The MGM function accesses the AUTH function to ensure that only authorized administrators are allowed to perform any administration.

6.2.24 FMT_MTD.2

In order to meet FMT_MTD.2, the TSF must restrict the ability to specify limits on failed authentication attempts to the authorized administrator, and lock users who exceed those limits. The AUTH function enforces limits on failed authentication attempts passed to it by the MGM function. The IAC function ensures that only the MGM function can change those limits. The MGM function accesses the AUTH function to ensure that only users that authenticate as authorized administrator can perform any administration.

6.2.25 FMT_SMR.1

In order to meet FMT_SMR.1, the TSF must maintain the role of authorized administrator and associate human users with that role. The MGM function maintains the role of authorized administrator, and associates users with that role.

6.2.26 FPT_RVM.1

In order to meet FPT_RVM.1, the TSF must ensure that enforcement functions are invoked and succeed before allowing data to pass. The INTERCEPT function forces all packets to be passed through to be evaluated by the enforcement functions, specifically the PF function, before allowing the packet to pass. Also, the MGM function ensures that the TOE configuration is successfully applied by the system administrator before any data traffic is allowed to be passed.

6.2.27 FPT_SEP.1

In order to meet FPT_SEP.1, the TSF must maintain a domain for its execution that protects it from interference by non-TSF functions, must enforce separation between the security domains of subject in the TSC. The IAC function provides separation between the security domains in the system. Separate domain are maintained for each TSF, for

subjects acting on behalf of authorized administrator, and other subjects that may be present on the TOE, or it's CGLinux host.

6.2.28 FPT_STM.1

In order to meet FPT_STM.1, the TSF must be able to provide reliable timestamps for its own use. The TIME function maintains the reliable timestamps that are used by the TOE internally, such as to stamp the audit records.

6.3 Assurance Measures

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed, and independent analysis and testing.

The general level of assurance for the TOE is:

A) Consistent with current best practice for IT development and provides a product that is competitive against other evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL4 from part 3 of the Common Criteria.

Table 9 - demonstrates the correspondence between the security assurance requirements listed in Sections 5.2 to the developer evidence.

Table 9 - Assurance Correspondence

Assurance Class	Component ID	Documentation
Configuration Management	ACM_AUT.1 (Partial CM automation)	The CM documentation describes the processes and procedure that are followed and automated tools that are utilized in the tracking and monitoring the changes to the
	ACM_CAP.4 (Generation support and acceptance procedures)	

Assurance Class	Component ID	Documentation
	ACM_SCP.2 (Problem tracking CM coverage)	CM items and the generation of the TOE. The configuration management measures applied by CyberGuard ensure that configuration items are uniquely identified. CyberGuard ensures that changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. CyberGuard performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation.
Delivery and Operation	ADO_DEL.2 (Detection of modification)	CyberGuard provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. CyberGuard's delivery procedures describe the procedures to be used for the secure installation, generation, and start-up of the TOE.
	ADO_IGS.1 (Installation, Generation, and Start-Up Procedures)	
Development	ADV_FSP.2 (Fully Defined External Interfaces)	CyberGuard provides design documentation that identifies and describes the external interfaces and the decomposition of the TOE into subsystems.
	ADV_HLD.2 (Security Enforcing High-Level Design)	The CyberGuard High Level Design, and its references, group the TOE into subsystems and describe how the subsystems behave and interact with each other.
	ADV_IMP.1 (Subset of the Implementation of the TSF)	The Cyberguard FSP, HLD and TAT documents collectively satisy this requirement.

Assurance Class	Component ID	Documentation
	ADV_LLD.1 (Descriptive Low-Level design)	TheCyberGuard Low-level Design Specification satisfies the requirement to decompose each subsystem into modules and fully describes each module.
	ADV_RCR.1 (Informal Correspondence Demonstration)	This informal correspondence demonstration is done by mapping Security Functions, SFRs, TOE SubSystems & Modules and appropriate Test cases in the CyberGuard FSP document.
	ADV_SPM.1 (Informal TOE security policy model)	The SPM environment is met by configuring the product as per the documentation provided in this ST.
Guidance Documents	AGD_ADM.1 (Administrator Guidance)	CyberGuard provides administrator guidance on how to utilize the TOE security functions and warnings to authorized administrators about actions that can compromise the security of the TOE. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install CyberGuard appliances in accordance with the evaluated configuration. This is done via the administrator and user guidance documents
	AGD_USR.1 (User Guidance)	
Life Cycle Support	ALC_DVS.1 (Identification of security measures)	CyberGuard ensures the adequacy of the procedures used during the development and maintenance of the
	ALC_LCD.1 (Developer defined life-cycle model)	

Assurance Class	Component ID	Documentation
	ALC_TAT.1 (Well-defined development tools)	TOE through the use of a comprehensive life-cycle management plan. CyberGuard includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. CyberGuard achieves this through the use of a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results. CyberGuard has procedures for accepting and addressing identified operational flaws as well as security flaws, including tracking of all identified flaws, describing, correcting, and taking other remedial actions such as producing guidance related to such flaws.
Tests	ATE_COV.2 (Analysis of Coverage) ATE_DPT.1 (Testing: high-level design) ATE_FUN.1 (Functional Testing) ATE_IND.2 (Independent Testing - Sample)	CyberGuard provides test documentation that describes how each of the TOE security functions is tested, as well as the actual results of applying the tests. The documentation shall contain the following: o The test case descriptions o Test Plan
Vulnerability Assessment	AVA_MSU.2 (Validation of analysis) AVA_SOF.1 (Strength of TOE Security Function Evaluation) AVA_VLA.2 (Independent Vulnerability Analysis)	CyberGuard has a documented process of tracking and remedying all vulnerabilities that are reported via various sources to maintain TOE in a secure state.
Flaw Remediation*	ALC_FLR.3 (Systematic Flaw Remediation)	CyberGuard comprehensively documents the method and procedures it has in place to track all flaws. These flaws are assigned a priority based on several criteria (For example whether or not the flaw is security relevant). Based on a priority level assigned to a flaw

Assurance Class	Component ID	Documentation
		they are rectified/remedied in a timely fashion.

NOTE:

The ALC_FLR.3, Systematic Flaw Remediation was added to augment the EAL4 level of evaluation .This augmentation, which is in line with the robust 'Software Development Life Cycle (SDLC)' model already being followed by the TOE developer, was included due to the strong consumer demand that the developer be able to systematically receive security flaw reports, fix security flaws and dispatch corrective fixes to the TOE users in a systematic, secure and a timely manner.

CHAPTER 7

7. Protection Profile Claims

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].

7.1 Protection Profile Reference

The CyberGuard Firewall/VPN Version 6.2.1 has been modeled[23] on the following two Protection Profiles:

Final U.S. Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000

Final U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000

[23] Albeit the CyberGuard Firewall/VPN version 6.2.1 has been modeled on the TF-MRPP & AP-MRPP it does not claim conformance to either.

CHAPTER 8

8. Rationale

The set of IT security requirements together forms a mutually supportive whole. For each active security function, the requirements that support and protect that function are also present in the profile.

The IT security functions work together to satisfy the TOE security functional requirements. Each security function contributes to satisfying the SFRs.

8.1 Security Objectives Rationale

Table 10 - demonstrates the correspondence between the security objectives listed in Sections 4.1 and 4.2 to the assumptions, threats and policies identified in Sections 3.2, 3.3 and 3.4.

Table 10 - Environmental Security Objectives, Assumptions/Threats Mappings

	T.E.TUSAGE	A.SINGEN	A.DIRECT	A.NOREMO	A.REMACC	A.MODEXP	A.NOEVIL	A.TRAIN	A.PHYSEC	A.GENPUR	A.PUBLIC
O.E.SINGEN		X									
O.E.DIRECT			X								
O.E.NOREMO				X							
O.E.REMACC					X						
O.E.MODEXP						X					
O.E.ADMTRA	X							X			
O.E.PHYSEC									X		
O.E.GENPUR										X	
O.E.GUIDAN	X										
O.E.NOEVIL							X				
O.E.PUBLIC											X

Table 11 - Mappings Between IT Security Objectives, and Threats

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL	T.MODEXP
O.IDAUTH	X									
O.SINUSE		X	X							
O.MEDIAT				X	X	X				
O.SECSTA	X							X		
O.SELPRO	X							X	X	
O.AUDREC							X			
O.ACCOUN							X			
O.SECFUN	X		X						X	
O.LIMEXT	X									
O.EAL										X

8.1.1 Rationale for TOE Security Objectives

8.1.1.1 T.NOAUTH

T.NOAUTH is the threat that an unauthorized person may attempt to bypass the security of the TOE so as to access and use security function and/or non-security functions provided by the TOE. This threat is addressed by O.IDAUTH, O.SECSTA, O.SELPRO, O.SECFUN and O.LIMEXT. Collectively these security objectives counter the threat (T.NOAUTH) by ensuring that the TOE does the following:

- Uniquely identify and authenticate the claimed identity of all users, before granting a user access to the TOE functions or, for certain specified services to a connected network.
- Ensure that upon initial start-up of the TOE or recovery from an interruption in the TOE service, the TOE must not compromise its resources or those of any connected network.
- Ensure that the TOE protects itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
- Guarantee that it (the TOE) provides functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only the authorized administrators are able to access such functionality.

- Guarantee that it (the TOE) provides the means for an authorized administrator to control and limit access to the TOE security functions by an authorized external IT entity.

8.1.1.2 T.REPEAT[24]

T.REPEAT is the threat that an unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE. This threat (T.REPEAT) is countered by the O.SINUSE security objective, which ensures that the TOE does the following:

- Guarantee that it (the TOE) prevents the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.

8.1.1.3 T.REPLAY[25]

T.REPLAY is the threat that an unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE. This threat is addressed by O.SINUSE, O.SECFUN. These TOE security objectives counter the threat (T.REPLAY).

The TOE security objectives, O.SINUSE and O.SECFUN, ensure that the TOE does the following:

- Guarantee that it (the TOE) prevents the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
- Guarantee that it (the TOE) provides functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only the authorized administrators are able to access such functionality.

8.1.1.4 T.ASPOOF

T.SPOOF is the threat that an unauthorized person on an external network may attempt to bypass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network. This threat (T.ASPOOF) is countered by the O.MEDIAT security objective, which ensures that the TOE does the following:

- Ensure that it (the TOE) mediates the flow of all information between clients and servers located on internal and external networks governed by the TOE or from users on a connected network to users on another connected network. It (The TOE) also ensures that residual information from a previous information flow is not transmitted in any way.

8.1.1.5 T.MEDIAT

T.MEDIAT is the threat that an unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network. This

[24] Since the TOE does not claim remote administration T.REPEAT is not applicable to the TOE for authenticating a remote administrator. However, this threat is mitigated via single use authentication of proxy users.

[25] Since the TOE does not claim remote administration T.REPLAY is not applicable to the TOE for authenticating a remote administrator. However, this threat is mitigated via single use authentication of proxy users.

threat (T.MEDIAT) is countered by O.MEDIAT security objective, which ensures that the TOE does the following:

- Ensure that it (the TOE) mediates the flow of all information between clients and servers located on internal and external networks governed by the TOE or from users on a connected network to users on another connected network. It (The TOE) also ensures that residual information from a previous information flow is not transmitted in any way.

8.1.1.6 T.OLDINF

T.OLDINF is the threat that, because of a flaw in the TOE functioning, may allow an unauthorized person to gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE. This threat (T.OLDINF) is countered by O.MEDIAT security objective, which ensures that the TOE does the following:

- Ensure that it (the TOE) mediates the flow of all information between clients and servers located on internal and external networks governed by the TOE or from users on a connected network to users on another connected network. It (The TOE) also ensures that residual information from a previous information flow is not transmitted in any way.

8.1.1.7 T.AUDACC

T.AUDACC is the threat that allows persons not to be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape. This threat (T.AUDACC) is addressed by O.AUDREC and O.ACCOUN. Collectively these security objectives counter the threat (T.AUDACC) by ensuring that the TOE does the following:

- Ensure that it (the TOE) provides a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
- Ensure that it (the TOE) provides user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

8.1.1.8 T.SELPRO

T.SELPRO is the threat that allows an unauthorized person read, modify, or destroy security critical TOE configuration data. This threat (T.SELPRO) is addressed by O.SECSTA and O.SELPRO. Collectively these security objectives counter the threat (T.SELPRO) by ensuring that the TOE does the following:

- Ensure that upon initial start-up of the TOE or recovery from an interruption in the TOE service, the TOE must not compromise its resources or those of any connected network.
- Ensure that the TOE protects itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

8.1.1.9 T.AUDFUL

T.AUDFUL is the threat that allows an unauthorized person to cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions. This threat (T.AUDFUL) is addressed by O.SELPRO and O.SECFUN. Collectively these security objectives counter the threat (T.AUDFUL) by ensuring that the TOE does the following:

- Ensure that the TOE protects itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
- Guarantee that it (the TOE) provides functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only the authorized administrators are able to access such functionality.

8.1.1.10 T.MODEXP

T.MODEXP is the threat of malicious attacks aimed at discovering exploitable vulnerabilities and is considered medium. This threat (T.MODEXP) is countered by the O.EAL[26] security objective, which ensures that the TOE does the following:

- Guarantee that it (the TOE) be structurally tested and shown to be resistant to obvious vulnerabilities.

[26] The security objective O.EAL is not met by any SFRs in the ST, however this objective is met by the EAL 4 Security Assurance Requirements mentioned in the 'TOE Security Assurance Requirements' section of the ST.

8.1.2 Rationale for IT Environment Security Objectives

8.1.2.1 T.E.TUSAGE

T.E.TUSAGE is the threat that the TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons. This threat is addressed by O.E.GUIDAN, which ensures that the TOE is to be delivered, installed, administered, and operated in a manner that maintains security, and O.E.ADMTRA which ensures that administrators that proper training to ensure that correct operation continues.

8.1.2.2 A.SINGEN

If O.E.SINGEN is achieved, then information cannot flow between the internal and external networks without passing though the TOE, which is A.SINGEN.

8.1.2.3 A.DIRECT

If O.E.DIRECT is achieved, then human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE, which is A.DIRECT.

8.1.2.4 A.NOREMO

If O.E.NOREMO is achieved, then human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks, which is A.NOREMO.

8.1.2.5 A.REMACC

If O.E.REMACC is achieved, then authorized administrators may only access the TOE locally, which is A.REMACC.

8.1.2.6 A.MODEXP

If O.E.MODEXP is achieved, then the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered medium, which is A.MODEXP.

8.1.2.7 A.NOEVIL

If O.E.NOEVIL is achieved, then authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error, which is A.NOEVIL.

8.1.2.8 A.TRAIN

If O.E.ADMTRA is achieved, then Firewall Administrators are trained as to the establishment of security policies and practices, which ensures that they are familiar with the various Sub-Systems

of the TOE's Management Software and are able to implement the site's security policy, which is A.TRAIN.

8.1.2.9 A.PHYSEC

If O.E.PHYSEC is achieved, then the TOE is physically secure, which is A.PHYSEC.

8.1.2.10 A.GENPUR

If O.E.GENPUR is achieved, then there are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE, which is A.GENPUR.

8.1.2.11 A.PUBLIC

If O.E.PUBLIC is achieved, then the TOE does not host public data, which is A.PUBLIC.

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements Rationale for the TOE

Table 12 - demonstrates the correspondence between the security objectives listed in Sections 4.1 to the security functional requirements (from both PPs) identified in Sections 5.1.

Table 12 - Mappings Between TOE Security Objectives and TOE SFRs

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FAU_GEN.1						X	X		
FAU_SAR.1						X			
FAU_SAR.3						X			
FAU_STG.1				X	X			X	
FAU_STG.4				X	X			X	
FDP_IFC.1 (1)			X						
FDP_IFC.1 (2)			X						
FDP_IFF.1 (1)			X						
FDP_IFF.1 (2)			X						
FDP_RIP.1			X						
FIA_ATD.1	X							X	
FIA_AFL.1					X				
FIA_UAU.5	X	X							
FIA_UID.2	X						X		
FMT_MOF.1 (1)				X				X	X
FMT_MOF.1 (2)				X				X	X
FMT_MSA.1 (1)			X	X				X	
FMT_MSA.1 (2)			X	X				X	
FMT_MSA.1 (3)			X	X				X	
FMT_MSA.1 (4)			X	X				X	
FMT_MSA.3			X	X				X	

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FMT_MTD.1 (1)								X	
FMT_MTD.1 (2)								X	
FMT_MTD.2								X	
FMT_SMR.1								X	
FPT_RVM.1				X	X				
FPT_SEP.1					X				
FPT_STM.1						X			

8.2.1.1 O.IDAUTH

In order to implement O.IDAUTH, the TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network. This is implemented by requiring user identification before any action (FIA_UID.2), allowing limited actions before authentication, authentication mechanisms (FIA_UAU.5), and binding the user identity to security attributes (FIA_ATD.1). Together these SFRs combine to address the objective to uniquely identify and authenticate users, which is O.IDAUTH.

8.2.1.2 O.SINUSE[27]

In order to implement O.SINUSE, the TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network. Also the TOE must prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack. The TOE implements this requirement by specifying single-use authentication mechanisms in FIA_UAU.5 and user attribute definition FIA_ATD.1. Note

[27] As explicitly stated elsewhere in this document, this Security Target has been instantiated from two Protection Profiles (*TF-MRPP, AP-MRPP).* Albeit, FIA_ATD.1 SFR is present in both the protection profiles, it has been mapped to O.IDAUTH and O.SECFUN objectives in Table 6.3 of the *AP-MRPP* and to O.IDAUTH & O.SINUSE objectives in Table 6.3 of the *TF-MRPP*. This ST has retained the mapping between the mentioned SFR and the objectives as per Table 6.3 of the AP-MRPP. This is because the maintenance of security attributes (like the identity and association of human user with authorized administrator role) by the TSF for individual users has no bearing on the ability of the TOE to prevent reuse of authentication data (as per O.SINUSE). Hence in this ST the mapping of FIA_ATD.1 is more appropriate with O.IDAUTH and O.SECFUN as opposed to O.IDAUTH & O.SINUSE.

that since the TOE does not support remote access or administration, the only use of single-use authentication mechanisms is for the Telnet and FTP proxies[28].

8.2.1.3 O.MEDIAT[27]

In order to implement O.MEDIAT, the TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols and ensuring that residual information from a previous information flow is not transmitted in any way. Both the authenticated and the unauthenticated information flow control policies [FDP_IFC.1(1), FDP_IFC.1(2)] and functions [(FDP_IFF.1(1), FDP_IFF.1(2)] combine to actively mediate the information flows to satisfy the objective. Residual information protection (FDP_RIP.1) is used to ensure that residual information from a previous flow is not transmitted. The components FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), Management of the security attributes and FMT_MSA.3, Static attribute initialization, ensure the integrity of the information flow rules by allowing only the authorized administrators to perform the above operations. . Together, the above SFRs help satisfy the objective O.MEDIAT.

8.2.1.4 O.SECSTA

In order to implement O.SECSTA, upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network. FMT_MOF.1(1) restricts the ability to startup the TOE to only authorized administrators so that it cannot be compromised during this stage. Only the administrator, again, is allowed to restore old values for TSF data (FMT_MOF.1(2)). Proper setting of restrictive default security attributes (FMT_MSA.3) complements management of security attributes (FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4)), and reference mediation (FPT_RVM.1) to ensure that start-up or recover states in the TOE have a restrictive default state that prevents compromise, as required by the objective. FAU_STG.1 protects the audit trails from unauthorized deletion/modification and FAU_STG.4[29] prevents loss of audit data when the audit trail is full by preventing auditable events.

---

[28] O.SINUSE is included both in TF-MRPP and AP-MRPP. Albeit the TOE does not claim remote administration (and hence single use authentication for the remote administrator) it however, does claim single use authentication for proxy users. For the purpose of this ST, the O.SINUSE objective is aimed to mitigate the T.REPEAT and T.REPLAY threats only while authenticating proxy (telnet, ftp) users and not remote administrators.

[29] **FAU_STG.4 requires the TSF to limit the number of audit records lost if the Audit Trail is Full. The TOE by default is configured to automatically shut itself down in a normal manner when the disk that holds the audit files reaches a threshold or maximum disk utilization capacity caused by an event of exhaustion or an attack that effects audit data exhaustion. Hence, when this threshold capacity (depicted as a percentage of the total disk space) is reached, the TOE initiates an audited shutdown of itself and in the process stops new audit events long before the remaining disk space is filled. This prevents any audit data loss. Based on this detailed analysis of the TOE it can be concluded that the TOE is expected to lose no data when the audit trail gets full. In the event of any storage failure, the loss of audit data is also limited by the automatic capabilities of the TOE to archive data on a scheduled basis. In this case, the worst-case lose of data is limited to the amount of time since the last regularly scheduled archive, typically 24 hours or less.**

8.2.1.5 O.SELPRO

In order to implement O.SELPRO, the TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. The component FPT_RVM.1 protects against bypass by requiring that all accesses be mediated. The component FPT_SEP.1 protects against attempts to tamper or deactivate security functions by providing a separate domain of execution for the functions. Any brute force attempts made by an attacker are countered by FIA_AFL.1, which bounds the number of invalid attempts and requires intervention by an authorized administrator thereafter. The component FAU_STG.1 protects the audit related TOE security functions and hence the stored audit trails from unauthorized deletion/modification, and the component FAU_STG.4[29] ensures that no audit data is lost when the audit trail is full.

8.2.1.6 O.AUDREC

In order to implement O.AUDREC, the TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes. The SFRs from the audit family are included to ensure the TOE collects audit records (FAU_GEN.1 and FPT_STM.1), and allows them to be reviewed (FAU_SAR.1) with searching and sorting capability (FAU_SAR.3).

8.2.1.7 O.ACCOUN

In order to implement O.ACCOUN, the TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit. Accountability in the TOE is implemented by requiring that each user to be successfully authenticated to the TOE before performing any operation on it (FIA_UID.2), and by requiring collection of audit (FAU_GEN.1).

8.2.1.8 O.SECFUN

In order to implement O.SECFUN, the TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality. The management components FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2) & FMT_MTD.2 and the audit components FAU_STG.1 & FAU_STG.4[29] ensure that only authorized administrators are allowed to manage their respective behavior. Similarly, user association with roles is provided by FIA.ATD.1.

8.2.1.9 O.LIMEXT

In order to implement O.LIMEXT, the TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity. FMT_MOF.1(1) and FMT_MOF.1(2) ensure that only an authorized administrator can communicate with the TOE and manage its security functions.

8.2.2 Security Functional Requirements Rationale for the IT Environment

There are no SFRs for the IT Environment.

8.2.3 Security Assurance Requirements Rationale

The rationale for the Security Assurance Requirements is defined in Chapter 6 Section 6.3.

8.3 TOE Summary Specification Rationale

The rationale for the TOE Summary Specification is defined in Chapter 6, Section 6.2.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.

8.5 Strength of Functions (SOF) Rationale

8.5.1 SOF for Password Mechanism

The rationale for the chosen level is based on the low attack potential of the threat agents identified in the ST. This security target includes a probabilistic or permutational function. The list of relevant security functions and security functional requirements includes:

- Identification and Authentication
    - FIA_UAU.1 - Timing of authentication
    - FIA_UAU.5 – Multiple Authentication Mechanisms

    The password used at administrator login from a locally connected console is the only probabilistic or permutational function on which the strength of the authentication mechanism depends.

The TOE places the following restrictions on the passwords selected by the user:

- The password must be at least eight long;

Furthermore, the user is advised not to use consecutive sequences, or easily guessable passwords

The password space is calculated as follows:

Patterns of human usage are important considerations that can influence the approach to searching apassword space, and thus affect SOF. Assuming the worst case scenario and the user chooses a number comprising only eight characters, the number of password permutations is:

Each one of the 8 characters in the password is allowed any one of the following 95 ASCII values:

32	sp	33	!	34	"	35	#	36	$	37	%	38	&	39	'
40	(	41	)	42	*	43	+	44	,	45	-	46	.	47	/
48	0	49	1	50	2	51	3	52	4	53	5	54	6	55	7
56	8	57	9	58	:	59	;	60	<	61	=	62	>	63	?

64	@	65	A	66	B	67	C	68	D	69	E	70	F	71	G
72	H	73	I	74	J	75	K	76	L	77	M	78	N	79	O
80	P	81	Q	82	R	83	S	84	T	85	U	86	V	87	W
88	X	89	Y	90	Z	91	[	92	\	93	]	94	^	95	_
96	`	97	a	98	b	99	c	100	d	101	e	102	f	103	g
104	h	105	i	106	j	107	k	108	l	109	m	110	n	111	o
112	p	113	q	114	r	115	s	116	t	117	u	118	v	119	w
120	x	121	y	122	z	123	{	124	|	125	}	126	~		

Thus, there are 95^8 = 6,634,204,312,890,625 potential password combinations implying that the probability that the authentication data can be guessed is no greater than one in ninety five to the power eight (95 ^ 8).

The amount of time it takes to manually type a password, given that authentcaion can only occur based upon manual input, is 7 seconds.

An attacker can at best attempt (60/7= 8.6 password entries every minute, or 514 password entries every hour. On average, an attacker would have to enter (6,634,204,312,890,625/ 2 =) 3,317,102,156,445,310 passwords, over (3,317,102,156,445,310 / 514) = 6,453,506,140,944 hours, before entering the correct password. The average successful attack would, as a result, occur in slightly less than:
6,453,506,140,944 /24/365 = 736,701,614 years

In accordance with annex B.8 in the CEM, the elapse time of attack is not practical and thus results in a high strength of function rating which exceeds SOF-Medium**.**

8.5.2 SOF for Single Use Authentication Mechanism

Strength of function rating of SOF-medium was designated for this TOE to exceed the U.S. Government Application-Level Firewall Protection Profile for Medium Robustness Environments upon which the TOE is modeled. The rationale for the chosen level is based on the low attack potential of the threat agents identified in the ST.

The list of relevant security functions and security functional requirements includes:

- FIA_UAU.5 – Multiple Authentication Mechanisms

An analysis for the ‘Strength of Function’ for single-use authentication mechanism is provided below:

1. For single use authentication the TOE includes the ‘RSA Authentication Manager version 6.0’ that validates the passcode corresponding to a user at any given time. This is done by matching the actual passcode presented by the user at a given time to the computed passcode calculated by the by the ‘Authentication Manager’ for the same user at the same given time. If the two passcodes match the user is successfully authenticated else a failure corresponding to the user is registered.
2. The14 character passcode that is used to authenticate a user at any given time comprises of the following two contiguous parts:
   - 8 character (Alpha Nummeric) PIN Code that changes only on demand.

- o 6 digit (numeric) random token that changes every minute. The RSA authentication Manager uses the 'AES hashing of 128 bit seed'[30] algorithm to generate the random tokens that change every minute.

3. Assuming a worst case scenario where the entropy assigned to the 8 character PIN number is zero (because it changes only on demand), the passcode contains only the 6 digit token that is truly unique, independent and random. This implies that at any given minute the effective bit strength of the Passcode would be equal to the effective bit strength of the 6 digit token.
   Passcode Bit Strength = 2 ^ 19.93 = 1,000,000 [i.e., one in 1,000,000]
4. The TOE also deploys the following functionality:
   - o Blacklisting of users on the 'CyberGuard Firewall/VPN 6.2.1' after 3 consecutive invalid identification and authentication attempts.
   - o Disabling of tokens on the 'RSA Authentication Manager version 6.0' after 3 consecutive invalid passcodes corresponding to a user are entered.

   NOTE:
   If a user is blacklisted and his token is disabled he is deemed to fail all subsequent authentication attempts even if he were to enter the correct passcode. For the user to be able to authenticate successfully again, an authorized system administrator must physically re-activate his token and remove him from the user blacklist database. Hence theses TOE features/environment measures prevent even an expert attacker's use of equipment.

5. Based on assertions 3 & 4 above a user with malicious intent shall have only 3 chances in 3 minutes to guess the random passcode that changes every minute. Each time the probability of a user guessing the passcode would be:
   1 / 1,000,000 = .000001

In accordance with annex B.8 in the CEM, the 'Access to the TOE' is:
- o For a very limited time period and for a very limited number of times.
- o Easily and automatically detectable.

[30] A separate document from RSA shall be provided as evidence that RSA uses the CCEVS accepted 'AES hashing of 128 bit seed' algorithm while generating random tokens.

It is hence not practical for an attacker to try and access the TOE illegally without being detected. This therefore results in a high strength of function rating which exceeds SOF-Medium.					

Strength of function rating of SOF-medium was designated for this TOE to exceed the U.S. Government 'Traffic-Filter Firewall Protection Profile for Medium-Robustness Environments' and 'Application-Level Firewall Protection Profile for Medium Robustness Environments' upon which the TOE is modeled.