Lucent Technologies
Lucent VPN Firewall
Version 7.0 (Patch 531)
Security Target

Version: 1.3

Release Date: October 27, 2003

Prepared for:
Lucent Technologies
480 Red Hill Road
Room 2B241
Middletown, NJ 07748

Prepared by:
Corsec Security, Inc.
10340 Democracy Lane
Suite 208
Fairfax, VA 22030

Table of Contents

Figures and Tables

1 Security Target Introduction

This introductory section presents *security target* (ST) identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., target of evaluation (TOE)). An ST principally defines:

- A set of assumptions about the security aspects of the environment, a list of threats which that product is intended to counter, and any known rules with which the product must comply.

- A set of security objectives and a set of security requirements to address that problem.

The ST for a TOE is a basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation. Because the audience for an ST may include not only evaluators but also developers and, “those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE” this ST minimizes terms of art from the *Common Criteria for Information Technology Security Evaluations* (CC).

An ST, like a Protection Profile (PP), contains sections which address Security Environment, Security Objectives, and IT Security Requirements, as well as Security Objectives Rationale and Security Requirements Rationale sections. Under certain conditions, the contents of these sections of the ST may be identical with those of the PP, namely, when the ST:

- Claims compliance with the PP.

- Performs no additional operations on the PP security functional requirements.

- Does not extend the PP by adding security objectives and/or security requirements.

Under these conditions, the CC states that, “reference to the PP is sufficient to define and justify the TOE objectives and requirements. Restatement of the PP contents is unnecessary”.

The methodology used to develop and present this ST includes the following steps:

- Those PP security objectives and requirements with which the ST claims compliance and for which no additional operations are to be performed are restated within the ST verbatim.

- If the ST will perform additional operations on PP requirements, the ST restates the requirements, performs the operations, and identifies the change by convention.

- If the ST extends the PP by adding security objectives and/or security requirements, the ST states the objectives and/or requirements, makes any needed additions to the Security Environment section, and documents suitable Rationale sections.

1.1 ST and TOE Identification

This section will provide information necessary to identify and control the Security Target and the TOE.

ST Title:	Lucent Technologies Lucent VPN Firewall Version 7.0 (Patch 531) Security Target Version: 1.3
TOE Identification:	Lucent VPN Firewall (LVF) Version 7.0 (Patch 531)
CC Identification:	Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999 **(aligned with ISO/IEC 15408: 1999)** including interpretations as of October 24, 2002.
PP Identification:	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Final, Version 1.1 April 1999 (referred to as TFFPP)
Assurance Level:	Evaluation Assurance Level 2
Keywords:	Information flow control, firewall, packet filter, network security, traffic filter, security target
ST Author	Corsec Security Inc.

1.2 Organization of Security Target Overview

The LVF v7.0 ST contains the following sections:

Security Target Introduction: Presents the Security Target (ST) identification and an overview of the ST structure.

TOE Description: Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE Security.

TOE Security Environment: Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.

Security Objectives: Identifies the security objectives that are satisfied by the TOE and the TOE environment.

IT Security Requirements: Presents the Security Functional Requirements (SFRs) met by the TOE.

TOE Summary Specification: Describes the security functions provided by the TOE to satisfy the security requirements and objectives.

Protection Profile Claims: Presents the rationale concerning compliance of the ST with the TFFPP.

Rational: Presents the rational for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

1.2.1 Common Criteria Conformance Claims

This ST claims conformance to CC Version 2.1, August 1999 Part 2 and Part 3; specifically CC Part2 Conformant and CC Part 3 conformant including interpretations as of October 24, 2002. Additionally, the TOE claims conformance to the Evaluation Assurance Level 2 package.

1.2.2 Protection Profile Conformance Claims

The TOE claims conformance to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.

1.2.3 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

- The CC allows several operations to be performed on functional requirements; assignment, iteration, refinement, and selection are defined in paragraph 2.1.4 of Part 2 of the CC.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].

- 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**.

- The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by <u>*underlined italicized text*</u>.

- Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

- The National and International Interpretations issued are reflected in this ST as **(Bold Text in parenthesis).**

1.2.3 Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Human user – Any person who interacts with the TOE.

External IT entity – Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Role – A predefined set of rules establishing the allowed interactions between a user and the TOE.

Identity – A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Authentication data – Information used to verify the claimed identity of a user.

In addition to the above general definitions, this Security Target provides the following specialized definitions:

Authorized Administrator – A role human users may be associated with in which to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized external IT entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Datagrams – Internet Protocol (IP) traffic

1.2.4 Acronyms

The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level

FA	Firewall Appliance
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
PP	Protection Profile
SFP	Security Function Policy
LSMS	Security Management Server
ST	Security Target
TCP	Transmission Control Protocol
TFFPP	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol

1.3 Security Target Overview

The LVF architecture consists of two physically distinct components:

- The VPN/Firewall Brick (Brick), which controls the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces; and

- The Lucent Security Management Server (LSMS) software, by means of which administrators manage the security of one or more VPN Firewall Brick.

The firewall code runs on Inferno™, a small Bell Labs developed operating system. The separate Lucent Security Management Server software, implemented by Java Code, runs either on Windows NT/2000/XP or Sun Solaris operating systems.

The Brick controls the flow of IP datagrams based on security policy rules. As with other traffic filter firewalls, the Brick controls the flow of datagrams based upon the interface of arrival, interface or egress, source and destination addresses, higher protocol and ports, and action to be taken (pass or drop).

Policy rules are defined by authorized administrators using the LSMS. The LSMS also supports the management of the other LVF security features, notably, or audit (for example, event selection, reports, and routing of selected audit event information to console, email, syslog, or beeper) and of administrator accounts.

The administrative interface to the LSMS is via a LSMS Navigator implemented by Java code.

In the secure configuration for evaluation the protected network is connected to one Brick interface, the isolated LSMS network to a second Brick Interface, and the external network (via a router) to a third Brick Interface.

1.4 TOE Common Criteria Conformance Claims

This TOE claims conformance to CC Version 2.1, August 1999 Part 2 and Part 3; specifically CC Part 2 - Conformant and CC Part 3 - Conformant including interpretations as of October 25, 2002. Additionally, the TOE claims conformance to the Evaluation Assurance Level 2 package.

1.5 Evaluation Traceability

The LMF v4.0 has been successfully evaluated against the Security Target, v1.0, for the Lucent Managed Firewall (LMF), v4.0, January 17, 2000 at the EAL2 level of assurance.

The LMF v3.0 has been successfully evaluated against the Security Target, v1.1, for the Lucent Managed Firewall (LMF), v3.0, December 8, 1998 at the EAL2 level of assurance.

2 TOE Description

This section provides a general overview of the TOE, in order to provide an understanding of how this TOE functions and to aid customers in determining whether this product meets their needs.

2.1 Application Context

The LVF can be used either by an enterprise, where the firewall is located on enterprise premises, or by an Internet Service Provider (ISP), where the firewall is located in the ISP's network. Whether employed by enterprise or ISP, the LVF is useful in a variety of scenarios. For example:

a) A Brick can be placed at the perimeter of an enterprise's intranet to protect it from the Internet. The protected network is connected to one interface, the isolated LSMS network to a second, and the external network (via a router) to a third as shown in the figure below. **Evaluation of the TOE is based on this configuration.**

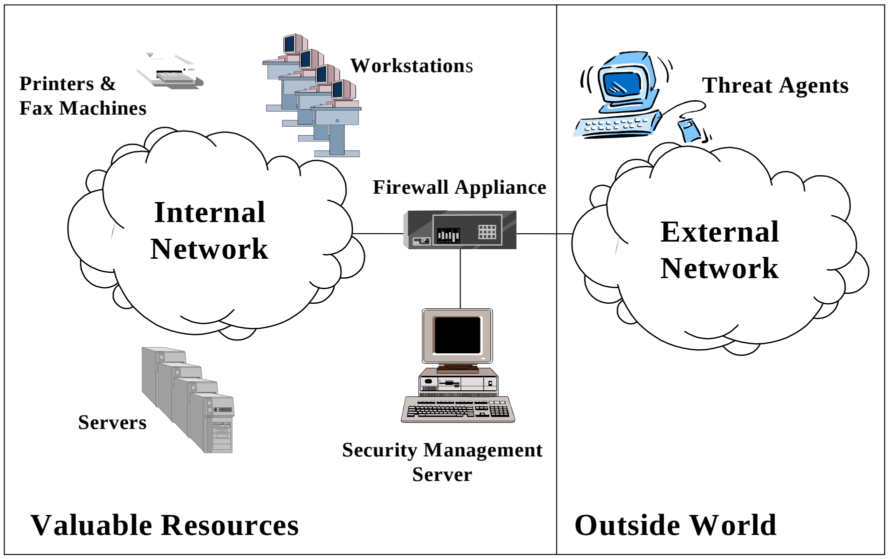

Figure 1 : Secure Configuration

Note: In the above figure only the Firewall Appliance and Security Management server in the "Valuable Resources" is in the scope of evaluation

b) Building upon the previous configuration, one can add a “demilitarized zone” (DMZ), in which to place the enterprise’s publicly available Web servers, for example

c) Multiple Brick’s can be placed to control several security zones within the enterprise intranet.

d) An ISP can manage multiple Brick’s with a single LSMS, and, using the LVF security zone feature, can allow different customers to control their own security policies. This configuration is shown in the figure below.

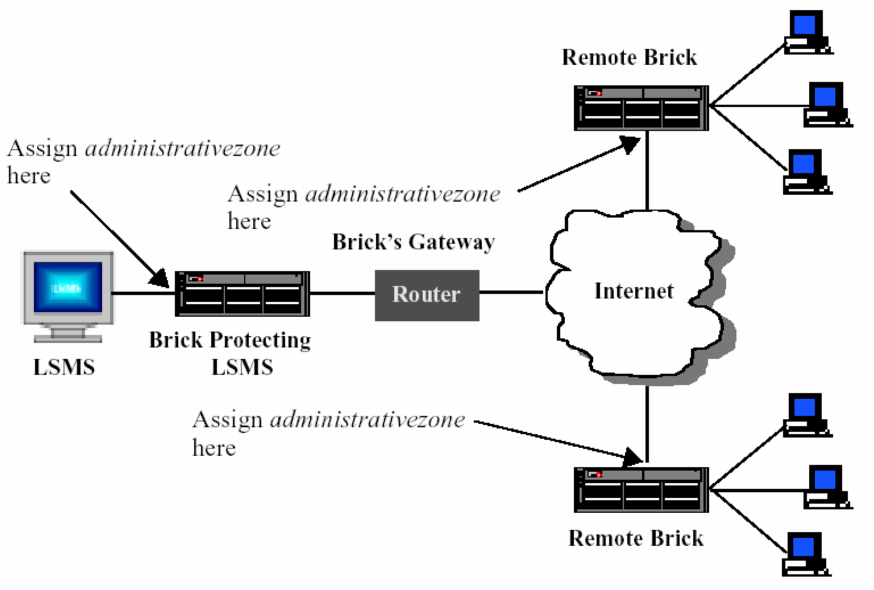
Remote Brick
Assign *administrativezone* here
Assign *administrativezone* here
Brick’s Gateway
Router
Internet
LSMS
Brick Protecting LSMS
Assign *administrativezone* here
Remote Brick

Figure 2 : Administering Multiple Bricks

2.2 Product Type

This section identifies the LVF’s product type.

The LVF is a traffic-filter firewall. A traffic-filter firewall controls the flow of Internet Protocol (IP) datagrams by matching information contained in IP and higher layer headers against a set of rules specified by the firewall’s administrator. This header information includes source and destination host IP addresses, source and destination port numbers, and upper level protocol identifier (for transmission control protocol (TCP) or user datagram protocol (UDP), e.g.). Depending upon the rule and the results of the match, the firewall either passes or drops the packet. In addition to protocol header information, traffic-filter firewalls use other information, such as the direction (incoming or outgoing) of the packet on a given firewall interface. The LVF provides the following features. Note that all these features may not be specifically validated in this Common Criteria validation effort. See the functional claims in Section 5 for the complete list of functionality that has been validated in the Common Criteria evaluation.

The following features of the LVF is validated in the common criteria evaluation.

a) Stateful Packet filtering: Every packet processed by the brick is considered part of a "session", regardless of IP type or higher-layer protocol instead of processing each and every packet individually.
b) Logging: All logging is done in real-time from the brick to its management server (LSMS).Apart from the logging events on the bricks the LSMS also logs administrative events and user authentication events.
c) Policy objects: LSMS resources are divided into groups where each group contains sets of resources. Enterprises can use a single group or multiple LSMS Groups.
d) Reporting: The LSMS has the ability to generate HTML-based reports and serve them via its own internal secure (HTTP or HTTPS). The internal web server is a Lucent-developed web server that only communicates with the LSMS and provides no external TOE interfaces.

The following are the features that the LSMS provides which are not required to be present for TFFPP compliancy and hence are not validated in the common criteria evaluation.

e) Network Address Translation: Network Address Translation and Source Address Translation are performed on policy rule level.
f) Denial of Service: The brick offers a variety of denial of service mechanisms tailored to both existing attacks as well as newly-emerging attacks not yet seen.
g) Dynamic Address Support: The brick has the ability to exist in a dynamic address environment .The brick can register its public address with its management server when used behind a many to one NAT device.
h) Alarms: The LSMS has the ability to create alarm triggers and associate them with appropriate actions to facilitate monitoring systems events.

i) QoS: The TOE provides Quality of Services features, specifically Bandwidth management functionality.

j) VPN: The TOE provides confidentiality and integrity of an enterprise's messages by means of Virtual Private Networks (VPNs) between the enterprise's VPN Firewall Bricks, using IP Security Protocol (IPSEC) encryption and cryptographic checksums.

k) Remote administration of the LVF.

l) Application Filters: The brick has the ability to perform inspection at the application layer of packet-based traffic passing through it using its unique Application filter architecture. Application filter protocols [and their associated functions] currently supported by the brick are as follows:

   - HTTP (HyperText Transfer Protocol) [URL logging, URI pattern match blocking, root directory traversal blocking]
   - H.323 [full v2 support, dynamic channel opening, address translation, FastStart, H.245 tunneling]
   - H.323 RAS [address translation]
   - H.323 is used to deliver multimedia (voice/video) services over Internet Protocol (IP) networks. It is used to provide Voice Over IP (VoIP) in telephone networks.
   - DHCP Relay (allows DHCP messages to be translated and sent to a preconfigured known DHCP server, on an arbitrary IP network)
   - FTP (File Transfer Protocol) [Command logging, dynamic channel opening, address translation, attack protection]
   - TFTP (Trivial File Transfer Protocol) [dynamic channel opening, address translation]
   - Oracle SQL*Net [dynamic channel opening]
   - Microsoft NetBIOS [address translation]

2.3 Physical Scope and Boundary

The Lucent VPN Firewall architecture consists of two physically distinct components:

- The VPN/Firewall Brick[1], which controls the flow of IP datagrams between network interfaces; and

- The LSMS software, by means of which administrators manage the security of multiple Brick's.

The evaluated LVF configuration consists of one LSMS and one Brick. At minimum, the LVF physical boundary includes just these two components. The secure configuration for evaluation is the basic network configuration as described in the_Figure 1 : Secure Configuration. The protected network is connected to one Brick interface, the isolated LSMS network to a second, and the external network (via a router) to a third.

Physical scope of the LVF includes hardware and software components identified in the table below.

LVF Element	Hardware/Software Components
VPN Firewall Brick	VPN Firewall Brick Model 20 VPN Firewall Brick Model 80 VPN Firewall Brick Model 201 VPN Firewall Brick Model 300 VPN Firewall Brick Model 500 VPN Firewall Brick Model 1000 Inferno Operating System (proprietary) Version 1.1
Lucent Security Management Server	400 MHz Pentium processor 512 MB of RAM Swap space at least as large as the amount of RAM 4 GB hard drive CD-ROM drive 3.5 inch floppy drive Ethernet interface card Video card capable of 1024 x 768 resolution (65,535 colors).
	Microsoft Windows NT with service pack 6a or Microsoft Windows 2000 with service pack 3, Adobe Acrobat Reader version 4.5 Netscape Navigator 4.7 or Internet Explorer 5.5 Java JRE, Version 1.3.1 and 1.1.7 Cloudscape, Version 3.6

LVF Element	Hardware/Software Components

Table 1 : Hardware/Software Components[1]

The LSMS utilizes the Cloudscape, version 3.6 database for storage of policies and audit information. The internal database itself is installed as part of the LSMS product and has no separate management interfaces. Cloudscape communicates only with the LSMS directly. The Java JRE (Java Runtime Environment) is installed as part of the LSMS and has no separate management interface.

The LSMS Software is designed and architected to be platform independent by implementing a Java Execution environment for the LSMS GUI. This GUI is the same whether running on Windows 2000 or Windows NT. The VPN Firewall brick models listed in the table above differ only in throughput and network interface capacity rather than functionality. They all run the same version of the Lucent Inferno operating system as pushed down by the LSMS console The LSMS GUI is the same whichever model is used,

Following table provides a detailed description of the Brick models.

VPN Firewall Brick Model number	Processor	Memory	Ethernet ports	Fiber Gigabit interfaces	Capacity Clear text / sessions	Encryption Accelerator
20	X86 compatible @120 mhz	64MB RAM	3 10/100 RJ45	N/A	140MBPS / 3000	N/A
80	AMD K6-2 350mhz	64MB RAM	4 10/100 RJ45	N/A	190MBPS / 30,000	N/A
201	Pentium II 400 MHZ	64MB RAM	4 10/100 RJ45	N/A	380MBPS / 100,000	O
300	Pentium III 1.26 Ghz	128MB RAM	8 10/100 RJ45	N/A	650MBPS / 400,000	O
500	Pentium III 1.26 Ghz	256MB RAM	14 10/100 RJ45	1	975MBPS / 600,000	O
1000 9/2	Pentium III 1 Ghz	1GB RAM	9 10/100 RJ45	2	1.5GBPS / 3 million	n/a
1000 7/2	Pentium III 1 Ghz	1GB RAM	7 10/100 RJ45	2	1.5GBPS / 3 million	I
1000 5/4	Pentium III 1 Ghz	1GB RAM	5 10/100 RJ45	4	1.5GBPS / 3 million	n/a
1000 3/4	Pentium III 1 Ghz	1GB RAM	3 10/100 RJ45	4	1.5GBPS / 3 million	I

2.4 Logical Scope and Boundary

The security functional requirements implemented by the LVF are usefully grouped under the following classes or families:

User Data Protection: The Brick controls the flow of incoming and outgoing IP datagrams. The firewall software that runs on the FA is based on the Inferno™ operating system, a small Bell Labs-developed operating system. The Security policy which controls the information flow through the brick is embedded within the Inferno™ operating system kernel. The Brick extracts information from the IP packet header and applies rules from a security policy. Information within an IP packet that is used to make access control decisions includes source and destination address, TCP or UDP port number, and packet type. Unless an authorized administrator explicitly configured the brick to accept requests based on specific security attributes, the LVF will successfully reject any and all requests. The primary components of the LVF that implement the user data protection are the inferno operating system and the Brick.

Security Audit: The Brick detects the occurrence of selected events, gathers information concerning them, and sends that information to the LSMS. The LSMS collects this information time stamps it and stores it in log files on the Windows NT/2000 operating system file system The LSMS also detects the occurrence of selected events (e.g., security administrator actions), gathers information concerning them, and records it. Audit reporting features are also provided by the LSMS. Included among the reporting features is the routing of selected audit event information to console, email, syslog, or beeper, as selected by an authorized administrator. The LSMS software, implemented by Java Code, using a JVM, runs either on Windows NT or Windows 2000 operating systems.
Audit can be done by LSMS reports generated by an LSMS webserver, LSMS log viewer and Windows NT/2000 event viewer. The primary components of the LVF that implement the Security Audit are LSMS logger subsystem, LSMS webserver, LSMS Log viewer, Windows Event Viewer and Brick.

Identification and Authentication (I&A): The LSMS software provides the tools to manage the security policies of the security zones that are applied to the Brick. The software runs at the application layer using Java™ on Windows NT™ / Windows 2000. The LSMS implements and enforces an administrator privilege model.

Two categories of administrators can be created: LSMS administrators and Group administrators. There can be multiple LSMS Administrators and Group Administrators. A group is a collection of objects that are managed as a whole. Every administrator must have a valid administrator account in the LSMS and underlying windows NT/2000 operating system. Administrators have to successfully log into the operating system before an LSMS login. The LSMS requires administrators to identify and authenticate themselves before they can perform any other LSMS actions. The Brick has no user (including administrator) accounts. The primary components of the LVF that implement the Identification and Authentication are Windows NT/2000 Logon GUI, LSMS login GUI and the LSMS subsystems.

Security Management: The LSMS provides all LVF security management capabilities. By means of it, administrators manage the security policy rules enforced by the Brick, configuration parameters and administrator accounts. All edits to the policy and user account information of the LSMS is stored in the cloudscape database which is a part of the LSMS. The primary components of the LVF that implement the Security Management are LSMS Navigator, cloudscape database, Windows NT/2000 file system.

Protection of TOE Security Functions: The Brick security functions which implement the LVF access control policy are physically separated from the unauthenticated external IT entities which send and receive IP datagrams through the Brick; and the design of these functions is such that they cannot be bypassed by those external IT entities. The primary components of the LVF that implement Protection of TOE Security Functions are LSMS, Windows NT/2000, the inferno operating system and the Brick.

The LVF logical boundary includes the Brick and the LSMS. The logical scope of the LVF extends to the five classes or families of security functional requirements just mentioned.

3 TOE Security Environment

This section aims to clarify the nature of the security problem that the LVF v7.0 is intended to solve. It does so by describing:

- Any assumptions about the security aspects of the environment and/or of the manner in which the LVF v7.0 is intended to be used.
- Any known or assumed threats to the assets against which specific protection within the LVF v7.0 or its environment is required.
- Any organizational security statements or rules with which the LVF v7.0 must comply

The LVF v7.0 is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

3.1 Assumptions

This section helps define the scope of the security problem by identifying assumptions about the security aspects of the environment and/or of the manner in which the LVF v7.0 is intended to be used.

3.1.1 Assumptions from the TFFPP

The TOE claims all the assumptions delineated below within the TFFPP. Those assumptions that are claimed are stated verbatim below.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

3.1.2 Modified Assumptions from the TFFPP

Four additional security environment assumptions described in the TFFPP have been modified in this ST. These modified assumptions are stated below. The refined assumptions are applicable to the architecture of this specific TOE.

A.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.

A.DIRECT The TOE is available to authorized administrators only.

A.PHYSEC The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.

3.1.3 Additional Assumptions not described in the TFFPP

A.SECFUN With the exception of identification and authentication, there are no security functions on the TOE accessible to human users who are not authorized administrators.

3.1.4 Other Additional Assumptions not described in the TFFPP

In addition to the above assumptions, the following assumptions about the TOE and the TOE environment are also made:

- The secure configuration for evaluation will be the basic network configuration as described in the Section 2.3 “Physical Scope and boundary”.
- The protected network is connected to one Brick interface, the isolated LSMS network to a second, and the external network (via a router) to a third.
- The evaluated secure configuration must contain the same physical and logical isolation.

3.2 Threats

This section helps define the nature and scope of the security problem by identifying assets which require protection as well as threats to those assets.

Threats may be addressed either by the LVF v7.0 or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.2.1 Threats to be Addressed by the LVF v7.0

The TOE addresses all threats delineated below from the TFFPP. These threats are restated verbatim from the TFFPP.

T.NOAUTH An unauthorized user may attempt to bypass the security of the TOE so as to assess and use security functions and/or non-security 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.

T.MEDIAT An unauthorized person may send impermissible information through the TOE those 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 for 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 user 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 form being recorded by taking actions to exhaust storage capacity, thus masking an attackers actions.

T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

This threat has been mapped to the objective O.SINUSE which states that the TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network. Authentication to the TOE from a connected network is a remote administration. Remote administration is not part of the evaluated TOE.

T.PROCOM 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.
Remote administration of the TOE is not part of the current evaluation and this threat can be ignored.

T.REPLAY An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
Remote administration of the TOE is not part of the current evaluation and this threat can be ignored.

3.2.2 Threats To Be Addressed by the Operating Environment

The TOE Operating Environment addresses the same TFFPP, Section 3.2.2 Threat To Be Addressed by Operating Environment. This threat has been adapted for the LVF because the physical and logical isolation dictated by the evaluated secure configuration.

T.TUSAGE The TOE may be used and administered in an insecure manner.

T.OEAUDAC 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.

4. Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives of the TOE, and
- Security objectives for the Operating Environment.

4.1 Security Objectives for the TOE

The TOE accomplishes a subset of the security objectives delineated within the TFFPP. For clarity, these security objectives are restated below.

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.

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.

4.2 Modified Security Objectives for the TOE from the TFFPP

Two additional security objectives described in the TFFPP have been modified in this ST. These modified objectives are stated below. The refined objectives are applicable to the architecture of this specific TOE.

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.MEDIAT The TOE must mediate the flow of all information between users on an internal network connected to the TOE and users on an external network connected to the TOE, and must ensure that residual information from previous information flow is not transmitted in any way.

4.3 Security Objectives for the Environment

Ten security objectives for the TOE environment are those specified below and are derived form the assumptions stated in the TFFPP.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

A.REMACC Because of the physical and logical isolation, the A.REMACC secure usage assumption is not included. Remote administration will not be part of evaluated secure configuration functionality.

O.GUIDAN Those responsible for the TOE must ensure that the TOE is delivered, installed, administered, and operated in a manner that maintains security.

O.ADMTRA Authorized administrators are trained as to establishment and maintenance of sound security policies and practices.

4.4 Modified Security Objectives for the Environment from the TFPP

A.PHYSEC The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.

A.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.

A.DIRECT The TOE and associated direct-attached console are available to authorized administrators only.

5. IT Security Requirements

IT security requirements include:

- TOE security requirements and (optionally)
- Security requirements for the TOE's IT environments (that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends).

These requirements are discussed separately below.

5.1 TOE Security Requirements

The CC divides security requirements into two categories:

- Security functional requirements (SFRs), that is, requirements for security functions such as information flow control, audit, identification and authentication.
- Security assurance requirements (SARs) provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment).

The section presents the security functional and assurance requirements for the TOE.

5.1.1 TOE Security Functional Requirements

This section presents the SFRs for the TOE. In accordance with the methodology described in Section 1.4, Security Target Preparation Methodology, this section has the following five subsections:

1) Restated PP SFRs: those PP security functional requirements with which the ST claims compliance and for which no additional operations are to be performed. These PP SFRs are included in the ST verbatim.

2) Omitted PP SFRs: those PP security functional requirements that have been omitted from this ST because the evaluated configuration of LVF v7.0 does not support Remote Administration of the TOE.

3) Tailored PP SFRs: those PP security functional requirements with which the ST claims compliance but for which additional operations are to be performed.

4) Additions to PP SFRs (optional): any security functional requirements additional to those of the PP.

5) SFRs With Strength of Function (SOF) Declarations: any security functional requirement that requires a SOF declaration.

5.1.1.1 Restated PP SFRs

The TOE shall satisfy the SFRs stated in the table below which lists the CC names of the SFR components contained in the TFFPP. Following the table, the individual functional requirements are restated form the TFFPP.

Functional Component ID	Functional Component Name
FAU_SAR.1	Audit review
FAU_STG.4	Prevention of audit data loss
FDP_IFC.1	Subset information flow control
FDP_RIP.1	Subset residual information protection
FIA_UAU.1	Timing of authentication
FIA_UID.2	User identification before any action
FMT_SMR.1	Security roles
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps

Table 2 : Restated Security Functional Requirements

- The National and International Interpretations issued are reflected in this ST as **(Bold Text in parenthesis).**

FAU_SAR.1 Audit review

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.

FAU_STG.4 Prevention of 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.

FDP_IFC.1 Subset information flow control

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;

c) operation: pass information.]

FDP_RIP.1 Subset residual information protection

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* the following objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the authorized administrator or authorized external IT entity accessing the TOE to be performed before the authorized administrator or authorized external IT entity is authenticated.

FIA_UAU.1.2 The TSF shall require each authorized administrator or authorized external IT entity to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator or authorized IT entity.

FIA_UID.2 User identification before any action

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.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [LSMS administrator and Group Administrator].

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

FPT_RVM.1 Non-bypassability of the TSP

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

FPT_SEP.1 TSF domain separation

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

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

FPT_STM.1 Reliable time stamps

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

5.1.1.2 Omitted PP SFRs

The TFFPP specifies that some functional requirements are optional and may be omitted from compliant TOEs. The SFRs in the table below have been omitted from this ST because the evaluated configuration of the LVF v7.0 does not support Remote Administration of the TOE.

Reference	**Description**
FCS_COP.1	Cryptographic operation
FIA_AFL.1	Authentication failure handling
FIA_UAU.4	Single-use authentication mechanisms

Table 3: Functional Components Omitted from the TOE

5.1.1.3 Tailored PP SFRs

The TFFPP identifies several SFRs that contain operations to be completed in PP-compliant security targets. This section identifies those TFFPP requirements and performs the required operations. The TOE shall satisfy the resultant requirements.

The table below names the SFRs for which the ST is required to perform operations. The table also identifies the operations (assignment, iteration, refinement, and selection) performed on them in this ST. Following the table, the individual functional requirements are restated form the TFFPP, and the operations completed.

Functional Component ID	**Functional Component Name**	**Operation**
FAU_GEN.1	Audit data generation	Refinement Selection
FAU_SAR.3(1)	Selectable audit review (1)	Iteration
FAU_SAR.3(2)	Selectable audit review (2)	Assignment Iteration
FAU_STG.1	Protected audit trail storage	Refinement
FDP_IFF.1	Simple security attributes	Assignment
FIA_ATD.1	User attribute definition	Assignment
FMT_MSA.3	Static attribute initialization	Assignment Refinement Selection
FMT_MOF.1	Management of security functions behavior	Refinement

Table 4: Tailored TFFPP SFRs

FAU_GEN.1 Audit data generation

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

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

b) All **relevant** auditable events for the *minimal or basic* level of audit **specified in Table 5**; and

c) [the event in **the table below** listed at the “extended” level.]

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**s** identit**ies**, and the outcome (success or failure) of the event; and

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

Functional Component	**Level**	**Auditable**	**Additional Audit Record Contents**
FMT_SMR.1	Minimal	Modifications to the group of users that are part of the authorized administrator role	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
FIA_UID.2	Basic	All use of the user identification mechanism	The user identities provided to the TOE.
FIA_UAU.1	Basic	Any use of the authentication mechanism	The user identities provided to the TOE
FDP_IFF.1	Basic	All decisions on requests for information flow	The presumed addresses of the source and destination subject
FPT_STM.1	Minimal	Changes to the time	The identity of the authorized administrator performing the operation
FMT_MOF.1	Extended	Use of the functions listed in this requirement pertaining to audit	The identity of the authorized administrator performing the operation

Table 5: Auditable Events

FAU_SAR.3 Selectable audit review (1)

FAU_SAR.3.1 The TSF shall provide the ability to perform <u>*searches*</u> of audit data based on

a) [user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times;

e) ranges of addresses.]

FAU_SAR.3 Selectable audit review (2)

FAU_SAR.3.1 The TSF shall proved the ability to perform *sorting* of audit data based on

a) [the chronological order of audit event occurrence.]

FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.2 The TSF shall be able to prevent (**unauthorized**) modifications to the audit records in the audit trail**. (International Interpretation 141)**

FDP_IFF.1 Simple security attributes

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 attributes:

1) presumed address;

2) {no other subject attributes}.

b) INFORMATION attributes:

1) presumed address of source subject;

2) presumed address of destination subject;

3) transport layer protocol;

4) TOE interface on which traffic arrives and departs;

5) service;

6) {no other 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:

1) 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;

2) the presumed address of the source subject, in the information translates to an internal network address;

3) 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:

1) 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;

2) the presumed address of the source subject, in the information translates to an external network address;

3) and the presumed address of the destination subject, in the information, translates to an address on the other connected network.].

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

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

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

c) The TOE shall reject requests for access or services where that information arrives on either an internal or external TOE interface, and the presumed address of the source subjects 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**;]

FIA_ATD.1 User attribute definition

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) {no other user security attributes.}]

FMT_MSA.3 Static attributes initialization

FMT_MSA.3.1 The TSF shall enforce the [information flow control **UNAUTHENTICATED** 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 an [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***perform*** the functions

a) [start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

h) modify and set the time and date;

i) archive, create, delete, empty, and review the audit trail;

j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;

k) recover to the state following the last backup

l) {no other services}

to an authorized administrator.

5.1.1.4 Additions to PP SFRs

The ST has no additional requirements beyond those already stated in the TFFPP.

5.1.1.5 SFRs With SOF Declarations

FIA_UAU.1 The FIA_UAU.1 SFR requires that the TOE have an authentication mechanism that has a probability of authentication data being guessed will be less than one in a million.

The overall Strength of function claim for the TOE is SOF-basic.

5.1.2 TOE Security Assurance Requirements

The table below identifies the security assurance components drawn from CC Part 3: Security Assurance Requirements, EAL2. The assurance requirements are stated verbatim from TFFPP section 5.1.2, TOE Security Assurance Requirements.

Assurance Component ID	Assurance Component Name
ACM_CAP.2	Configuration Items

ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	In depending testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

Table 6: EAL 2 TFFPP SARs

5.1.2.1 ACM_CAP.2 Configuration items

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version on the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list. (**The configuration list shall unique identify all configuration items that comprise the TOE. Interpretation 003)**

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.2 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.3 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The (**installation, generation and startup)** documentation shall describe (**all)** the steps necessary for secure installation, generation, and start-up of the TOE. **(Interpretation 051)**

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.1.2.4 ADV_FSP.1 Informal functional specification-

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.1.2.5 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.1.2.6 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements”

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.7 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.8 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.9 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.10 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.11 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.1.2.12 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform strength of TOE security function analysis for each mechanism identified in the ST as having strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.1.2.13 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform **(a vulnerability analysis. Interpretation 051)**

AVA_VLA.1.2D The developer shall (**provide vulnerability analysis documentation**. **Interpretation 051)**

Content and presentation of evidence elements:

AVA_VLA.1.1C **(The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious way in which a user can violate the TSP.**

The Vulnerability analysis documentation shall describe the disposition of the obvious vulnerabilities.

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. Interpretation 051)

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.2 Security Requirements for the IT Environment

The TOE has no security requirements allocated to its IT environment.

6 TOE Summary Specification

This section presents a functional overview of the TOE; the security functions implemented by the TOE; and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

This section presents a functional overview of the TOE; the security functions implemented by the TOE; and the Assurance Measures applied to ensure their correct implementation. The following paragraphs briefly summarize which security functions implement specific functional requirements specified in TOE Security Functional Requirements section:

Component **FAU_GEN.1**, audit data generation, is implemented by the VPN/Firewall Brick and the Lucent System Management Server (LSMS). The LSMS makes a non-volatile record (audit) of all security audit events of LVF. The resident operating system auditing functionality provides auditing of all security events provided by the operating system.

Component **FAU_SAR.1**, audit review, is accomplished via the LSMS. The LSMS provides the administrator reports wizards and log viewer to filter and sort audit data. The resident operating system provides the administrator an event viewer to view the log files that are generated by the operating system.

Component **FAU_SAR.3 (1) and (2)**, selectable audit review, is implemented via the LSMS. The LSMS report wizards and LSMS log viewer allow for sorting and filtering of all attributes identified. The procedures for filtering and sorting the log files are provided in the administrative guidance documents. The operating system generated logs can be filtered and sorted using the capabilities provided by the operating system event viewer.

Component **FAU_STG.1**, protected audit trail storage, is implemented by the LSMS and resident operating system. The log files are stored on the resident operating system and the assumed secure basic configuration requires physical and logical separation to permit access to only authorized administrators. The TOE configuration assumes only authorized administrators of the resident operating system will have access to TOE environment containing the LSMS and its resident operating system. Hence only authorized administrators have access to log files generated by both the LSMS and the resident operating system.

Component **FAU_STG.4**, prevention of audit data loss, is implemented by the LSMS.When the Session logs generated by the LSMS are full, the brick stops allowing traffic. Only authorized administrators who have successfully performed the operating system I & functionality can access these session log files that reside on the resident operating system file system and perform necessary actions to allow traffic through the brick.

Component **FDP_IFC.1**, The UNAUTHENTICATED subset information flow control, is implemented by the VPN/Firewall Brick. The VPN/Firewall Brick controls the flow of incoming and outgoing IP packets. The default is **DROP**, which means the brick will discard the packet and not allow it through. Unless an authorized administrator explicitly configured the brick to accept requests based on specific security attributes, the LVF will successfully reject any and all requests.

Component **FDP_IFF.1**, The UNAUTHENTICATED simple security attributes is implemented by the VPN/Firewall Brick. Security attributes include security policy specified rules, host groups, service groups, dependency masks, and VPN information generated by the LSMS on behalf of the Administrators. In addition, time-of-day, day-of-week, direction of access, physical Ethernet port, and existing session information can be used to determine whether or not a packet is allowed to pass in either direction.

Component **FDP_RIP.1**, subset residual information protection, is implemented by the VPN/Firewall Brick. Pointers are used by the operating system to identify the beginning and ending of each packet in memory. The correct operation of these pointers ensures that data previously stored in memory is not inadvertently included in a packet.

Component **FIA_ATD.1**, user attribute definition associated with the authorized administrators is managed by the LSMS. The LSMS is responsible for maintaining administrator account information and providing administrator privilege information for enforcement. It provides the Administrator with the capability to create or update Administrator accounts. Account creation and management includes specifying privileges. The resident operating system also provides I & functionality. The resident operating sytem maintains the administrator information which includes his human user identity.

Component **FIA_UAU.1**, timing of authentication for the administrators will be provided by the LSMS. An authorized administrator has to successfully perform the I & A functionality provided by the resident operating system to access the LSMS and TOE environment. To access the security functions provided by the TOE the administrator then has to successfully perform the I & A functionality provided by the LSMS.

Component **FIA_UID.2**, user identification before any action for the administrators is provided by the LSMS and underlying operating system. An authorized administrator has to successfully perform I & A functionality provided by the resident operating system and this functionality is further refined by the I & A functionality provided by the LSMS. An authorized administrator perform any TSF-mediated actions only after successfully performing both resident operating system I & A and LSMS I&A.

Component **FMT_MOF.1**, management of security functions behavior has several security functions associated with this SFR. Both the resident operating system and LSMS combine to provide this functionality.

Component **FMT_MSA.3** static attribute initialization functionality is provided by the TOE. Specific instructions are provided by the LSMS and VPN/Firewall Brick. Specific rules mentioned in the wrapper document have to be applied to Zones rulesets of the VPN/Firewall Brick.

Component **FMT_SMR.1**, security roles, is provided by the LSMS.

Component **FPT_RVM.1**, non-bypassability of the TSP of the TOE is provided by a combination of the secure configuration (LSMS directly connected to the brick) and enforcement of the security policy rules.

Component **FPT_SEP.1**, TSF domain separation is implemented by the TOE. The VPN/Firewall Brick, the LSMS, and resident operating system combine to perform this security functionality.

Component **FPT_STM.1**, Reliable time stamps is implemented by the resident operating system, the VPN/Firewall Brick, and the LSMS. The LVF preserves the sequence of events in the log files by timestamping. The VPN/Firewall Brick preserves the order of the packet and sends the information to the LSMS. The LSMS respects the ordering of the VPN/Firewall Brick and provides a timestamp using the clock setting on the resident operating system.

6.1.1 Security Management

The Lucent Security Management Server (LSMS) provides all LVF security management capabilities. Only an authorized administrator working through the LSMS on an NT/2000 Server can perform security management functions to include creating and editing security policy, creating administrator accounts and modifying and setting thresholds for auditable events .The LVF TOE configuration assumes only authorized administrators will have access to LVF environment containing the LSMS and its resident operating system. Any administrative actions conducted by the resident operating system are restricted to authorized administrators.

The LSMS provides backup and recovery of Configuration data, policy and device data. This data is stored in both database and configuration files in the lmf directory on the operating system file system. The Operating system provides the back-up of LSMS log files located in the lmf directory, operating system log files and operating system configuration data (user account information).

These actions are logged by the resident operating system and include:

- Creation of administrators and changes to privileges of administrators on operating system
- Administrator login attempts (successful and unsuccessful)
- Modification of the time and date of operating system
- Deleting of the log files generated by the resident operating system.
- Start-up and Shutdown of the LSMS
- Backup and recovery of operating system's audit logs; LSMS audit Logs and operating system configuration files.

There are two types of Administrators that manage the LSMS; Group administrators and LSMS administrators. LSMS Administrators have full privileges over all groups, which means they can access all folders in all groups and make any additions, modifications, or deletions they deem necessary. Group Administrators, on the other hand, can only access the specific groups to which they are assigned. In addition, Group Administrators can be given three levels of privilege over the folders in their groups: None, View and Full.

Start-up and shut-down of the LSMS is done from the resident operating system and is restricted to authorized administrators. LSMS provides a timestamp using the clock setting on the resident operating system. The changes to date and time setting in the operating system are restricted to authorized administrators.

The audit trail created by the LSMS is stored on the resident operating system file system. The access to these audit files is restricted to authorized administrators. The administrators have to successfully perform the I & A functionality to review the audit trail.

Chapter 2 of the Lucent Security Management Server v7.0 Administration Guide provides information on securely accessing the LSMS. The administrative guidance provides information on accessing the LSMS using the LSMS Navigator and Remote Navigator. Accessing the LSMS using the remote navigator is not in the scope of the evaluation.

The LSMS:

a) generates zone security policies in accordance with a corporate security policy on behalf of the Administrators. This responsibility includes taking the Administrator zone security policy specified rules, host groups, service groups, dependency masks, and VPN information and encoding it (policy compilation) into a file format suitable for local storage and/or downloading to a Brick Subsystem.

b) manages administrator accounts by performing LSMS and Group administrator account management, and privilege preservation.

c) maintains the Administrator account information. The LSMS maintains for each administrator their UserID, User name, password, domain, role, and privileges.

d) preserves the LSMS and Group administrator's privilege information and provides it for enforcement.

e) logs the administrator out if unrecognized data is received from the administrator interface or un-handled exceptions occur within LSMS.

f) receives administrator edits to policy information in accordance with a corporate security policy.

g) receives administrator edits to account information.

h) receives administrator edits to alarm configuration information.

i) receives administrator edits to zone information.

j) receives administrator edits to firewall information.

The LSMS allows Zone policy rules to be set to allow information flow through the Firewall. By default the zone policy rules drop a packet and hence restrictive default values are used during the creation of a policy. The LSMS and Group administrators can then alter these values to allow creation of Zone policy rulesets for appropriate information flow.

The VPN/Firewall Brick (Brick) permits the security policies to be loaded into the Brick from the LSMS. The administration applications of the LSMS also provide system status information.

Loading a Brick loads the Zone Assignment Table on the Brick. The Zone Assignment Table identifies the zones that are assigned to each of the Brick's interfaces.

Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.3, and FMT_SMR.1

6.1.2 Identification and Authentication

Every administrator has an operating system login account and an LSMS login account. The administrator's operating system account has to be created before the creation of an LSMS account. During the creation of operating system administrator accounts the attributes of the user (i.e. his identity and his association of his name with the administrator role) is collected and stored by the operating system. Similarly during the creation of other administrator accounts the attributes of the user is collected and stored by the LSMS.

The assumed secure basic configuration is physically and logically isolated and only authorized administrators will have physical access to the LSMS server. The LSMS software will be the only software on the server in addition to the resident operating system software. The Brick has no user (including administrator) accounts.

At least one Operating system administrator account and one LSMS Administrator are required to administer an installation of the LSMS. The first LSMS Administrator login is created automatically during the software installation process. This administrator can then create other administrator accounts (LSMS and Group).

Authorized administrators have to successfully perform the I & A functionality provided by the resident operating system before accessing the LSMS or the TOE environment. The only action that an authorized administrator can perform before successful I & A are accessing the operating system login id and password screen.

Once administrators successfully are logged in they can access the following :

- Lucent Security Management Server menu items from the file menu

- LSMS command line interface
- LSMS and operating system log files
- Configuration file from the lmf file directory

The LSMS requires administrators to identify and authenticate themselves before they can perform any other LSMS action. The administrator establishes communication with the LSMS by bringing up the LSMS Navigator login screen from the windows start menu folder or through the LSMS command line interface.

The only action that the administrator can perform on the LSMS Navigator before authentication is accessing the LSMS Navigator login window. The LSMS Navigator then establishes a connection with the LSMS and displays the LSMS Login Screen to the user.

The administrator provides his userID and password within the LSMS Navigator login window. After identifying and authenticating the System Administrator, a Java based GUI is downloaded to the System Administrator's desktop to provide the Primary User Interface and to secure the communications between the Java GUI and the LSMS. The LSMS manages the administrator's interface. This includes interacting with the administrator management screens presented within the GUI JVE to provide the appropriate Java GUI in response to administrator's input. Such interactions include – based on type of administrator (LSMS or Group) administrator input, presenting the System Administrator interface the appropriate Java GUI for management of System Administrator accounts, alarms, logging, and zone management.

The LSMS uses the administrator account information to make authentication decisions based upon the userID and password provided to it.

This security function requires strength of function rating for the following:

- Authentication mechanism of the operating system to authenticate an administrator
- Authentication mechanism of the LSMS to authenticate an administrator.

The SOF claim for these mechanisms is SOF-basic and the probability of authentication data being guessed will be less than one in a million.

Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, and FIA_UID.2

6.1.3 User Data Protection

The Brick controls the flow of incoming and outgoing IP packets. The BRICK extracts information from the IP packet header and applies rules from a security policy. The default is **DROP**, which means the brick will discard the packet and not allow it through unless an authorized administrator explicitly configured the brick to accept requests based on specific security attributes, the LVF will successfully reject any and all requests.

Security rules in the security policy perform this filtering function based on the following pieces of information (security attributes) in each packet to see if they match the same information in the rule. The following rule properties are applied to the attributes of an IP packet

a) The direction of the packet.

b) The source host (the presumed address)

- Single host if source is a single machine, this field will contain its IP address.
- Host group if the source is a group of machines, this field will contain the host group name. (A host group is a collection of IP addresses. It can consist of one or more single addresses, or ranges of addresses. Host groups are created by the administrator prior to creating the rule.)

c) The destination host (the presumed address)

- Single host if destination is a single machine, this field will contain its IP address.
- Host group if the destination is a group of machines, this field will contain the host group name. A host group is a collection of IP addresses. It can consist of one or more single addresses, or ranges of addresses. Host groups are created by the administrator prior to creating the rule.)

d) The service or protocol: Every security rule must specify an Internet service. Services are application-level protocols that are identified by their destination address, TCP or UDP port numbers. There are four ways to enter this information.

- Protocol name or number
- Protocol number/destination port
- Protocol number/destination port/source port
- For ICMP messages, the format is protocol/type/code.

In addition to the above mentioned security attributes there exists a field in the policy rule that defines the action that the Brick will take when it encounters a packet that matches all the information in the above four fields. The default is "DROP", which means the brick will discard the packet and not allow it through. To allow a packet matching the above four fields through the brick, the field must be set to "PASS".

In addition to security policy specified rules, host groups, service groups, and dependency masks generated by the LSMS on behalf of the Administrators, security attributes include time-of-day, day-of-week, direction of access and existing session.

When packets arrive on a brick interface they are written into memory for processing. The packet overwrites information previously stored in that memory location. Pointers are used by the operating system to identify the beginning and ending of each packet in memory. The correct operation of these pointers ensures that data previously stored in memory is not inadvertently included in a packet.

<u>Functional Requirements Satisfied</u>: FDP_IFC.1, FDP_IFF.1, and FDP_RIP.1

6.1.4 Protection of TOE Security Functions

Non-bypassability of the TOE is provided by a combination of the basic configuration and enforcement of the security policy rules. The assumed secure basic configuration maintaining physical and logical isolation supports the Protection of Security Functions (PSF). The functions that enforce the TOE Security Policy (TSP) will always be invoked, before any function within the TSF Scope of Control is allowed to proceed. The points where the TOE is accessible to an external subject is through the Brick network interfaces. The packet filtering mechanism of the Brick allows only explicitly stated information flows through the Brick. The security policy rules enforced by the Brick are applied to every packet and no packets can bypass this packet filtering mechanism.

The LSMS is directly connected to the Brick and no user information flow is allowed to the LSMS from the Brick. The LSMS passes management information to the Brick through a direct Ethernet crossover cable that is connected to one of the network ports of the Brick. Apart from this port that is used for management of the Brick, two other Ethernet ports (one for external network and one for internal network) which allow information flow to pass through them. The LSMS and the residing operating system runs only processes that are need for its proper execution and does not run any other user processes. The Brick does not contain a hard drive, file system or user accounts and can be deployed without a monitor and keyboard. It runs only the policy rulesets embedded in its kernel and doesn't provide a provision to run any other executables. This implementation provides the required TSF domain separation.

Functional Requirements Satisfied: FPT_RVM.1, FPT_SEP.1

6.1.5 Security Audit

The Brick detects the occurrence of selected events, gathers information concerning them, and sends that information to the LSMS, where it is stored. The LSMS also detects the occurrence of selected events (e.g., security administrator actions), gathers information concerning them, and records it. Audit reporting and alarm features are also provided by the LSMS. The reporting feature of the LVF allows Administrators to view and analyze internal and system information of the LVF. Using Report Wizards, audit event items can be extracted and presented in a legible and coherent format.

The types of audit events recorded in AdminEvents Log, the Sessions Log, the user authentication log, and the proactive monitoring log are contained in a Lucent Security Management Server v7.0 Reports, Alarms and Logs manual. They include but are not limited to the following:

- Modifications to group of authorized administrator
- Use of user identification mechanism
- Any use of the authentication mechanism
- All decisions on requests for information flow
- The identity of the user performing the following :

- archive, create, delete, empty, and review the audit trail;
- backup and recovery of user attribute values, information flow security policy rules, and audit trail data
- start-up and shutdown of the above mentioned functions.

The User Authentication Log contains log messages that record successful or unsuccessful authentication requests firewall users. The user authentication log records a minimum of the following fields:

- Date and type
- Group
- User Authentication Details (User id)
- Source Host
- Destination Host
- Protocol
- Destination Port
- Result of the action (success/failure)

The Administrative Events Log contains log messages about administrative events (e.g., brick zone ruleset was loaded), brick events (e.g., brick was lost), error messages, and alarms that were triggered and delivered.

The Admin event log records a minimum of the following fields:

- Date and Time
- Event Log Details (Source and Description of the event)

The session log contains a minimum of the following fields:

- Zone
- Source Port
- Destination Port
- Source Host
- Destination Host
- Protocol
- Action/Result (Pass or Fail)
- Rule Number (The policy number responsible of the action)

The Proactive Monitoring Log contains a minimum of the following fields:

- Source Type
- Source Identifier

- LSMS timestamp
- Proactive monitoring Subtype

The information contained in the audit logs can be retrieved through filtering and sorting options provided in the Reporting subsystem. Reports are based on records of an audit log. Each line in an audit log is a record. A record consists of fields and each field contains a value. Some fields can be filtered to look for specific user-defined values. Logical “AND” and “OR” functions can be performed across filterable fields. A report ‘wizard’ enables the user to specify values for filterable fields to hone in on field criteria values. The ‘wizard’ permits selection of fields on which to sort and allows selection of sorting direction (ascending or descending). When generating an Admin Events or Sessions Log report, the ability to search the raw log file by entering a text string is also provided.

In addition to the logs generated by the LSMS, the resident operating system (Windows NT/2000) Security Log also generates log files which have the following fields:

- Type
- Date
- Time
- Event
- Type
- User (administrator who performed the action)

6.1.5.1 Audit Generation

The Brick records the start and end of a session. It extracts information from the session cache to uniquely identify each session, and it records:

a) Start and stop times

b) Action taken

c) Statistics, such as number of bytes and packets passed

The Brick bundles this information into an audit message and sends it to an awaiting audit server, located on the LSMS.

The LSMS logs session info sent to it by Brick, and logs operational information from all LSMS Subsystems (including Brick Subsystems). The LSMS reformats the log events it receives, applies a time stamp, and writes the event to the appropriate log file. The LSMS uses the clock setting on the resident operating system to generate timestamps for audit records.

In addition to the above mentioned audit data generated by the LSMS the underlying operating system logs (Windows NT/2000 Security Log) the following events.

a) Administrator account actions (operating system login, operating system logout, operating system account configuration changes)
b) Changes to date/time on the operating system
c) Start-up and Shutdown on the LSMS
d) Backup and Recovery of LSMS log files, operating system log files and operating system administration files.
e) Changes / Deletion of the LSMS or operating system log files

The auditable events mentioned in table 5 are audited in the above mentioned logs.

Functional Component	**Log**	**Auditable**	**Additional Audit Record Contents**
FMT_SMR.1	Admin Event Log	Modifications to the group of users that are part of the authorized administrator roles provided by the LSMS	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
	Windows NT/2000 Security Log	Modifications to the group of users that are part of the authorized administrator roles provided by Windows NT/2000	
FIA_UID.2	User Authentication	All use of the user identification mechanism provided by the LSMS	The user identities provided to the TOE.

Functional Component	**Log**	**Auditable**	**Additional Audit Record Contents**
	Windows NT/2000 Security Log	All use of the user identification mechanism provided by Windows NT/2000	
FIA_UAU.1	User Authentication. Log	Any use of the authentication mechanism provided by LSMS	The user identities provided to the TOE
	Windows NT/2000 Security Log	Any use of authentication mechanism provided by Windows NT/2000	
FDP_IFF.1	Sessions Log	All decisions on requests for information flow	The presumed addresses of the source and destination subject
FPT_STM.1	Windows NT/2000 Security Log	Changes to the time made on Windows NT/2000	The identity of the authorized administrator performing the operation
FMT_MOF.1	Admin Events Log	Use of the functions listed in this requirement pertaining to audit	The identity of the authorized administrator performing the operation
	Windows NT/2000 Security Log	changes to time, Changes to user account attribute values, start-up and shutdown of the LSMS, access to LSMS and operating system log files, backup and recovery of operating system user account configuration information,	

Functional Component	Log	Auditable	Additional Audit Record Contents
		operating system log files and LSMS log files.	

Table 7 : Auditable Events Logged

Functional Requirements Satisfied: FAU_GEN.1, FPT_STM.1

6.1.5.2 Audit Review

The LSMS makes a non-volatile record (audit) of all security audit events, management, or maintenance of the LVF, and it enables an Administrator to view critical user and system information (e.g., Brick up/down status and logged on users, etc). It also enables Administrators to monitor the configuration of and access to the Bricks deployed throughout the network.

The LSMS provides a Log viewer which provides the administrator the capability read the audit trail from user authentication logs, session logs, administrative event logs and proactive monitoring logs. These logs can be viewed real-time or historically. The log viewer enables creation of filters to filter the audit data based on log filter parameters and the type of log that has to be processed. The LSMS also provides authorized administrators with the ability to perform searches on the audit data based on user identity, presumed subject address, range of dates and perform sorting based on the chronological order of audit event occurrence.

Reports are generated using logged administrative events and Brick session log data. LSMS Administrators can run reports for any group. Group Administrators can only run reports for groups for which they have at least View privileges. Reports cannot display real time information, as logs can, they do allow access to the same information as contained in the historical logs from any location. The report “wizards” are displayed to enable Administrators to filter and sort data. Through this interface, the administrator has the capability to generate “Memorized Reports” (i.e., report templates) and to generate Closed Session, Session; and Administrative Events reports.

The LSMS provides the Administrator with an automated tool that reviews audit logs for configurable alarming events, and when found, to notify the administrator.

The resident operating system provides an event viewer to view the logs generated by the operating system. The log records can be filtered using filters and also sorted based on date, time and administrator who generated the log records.

Functional Requirements Satisfied: FAU_SAR.1 and FAU_SAR.3 (1) and (2)

6.1.5.3 Audit Storage

The operating system generated log files (security log files) are stored on the operating system file system. The log files are separated into four different directories: sessions, admin events, user authentication, and proactive monitoring.

a) One for “sessions” data: The Session Log contains Brick session records, which describe network activity through one or many bricks. Session transactions through all Brick ports are recorded here.

b) One for “admin events”: The Administrative Events Log contains log messages about administrative events (e.g., Brick zone ruleset was loaded), Brick events (e.g., brick was lost), error messages, and alarms that were triggered and delivered.

C) One for “User Authentication Logs”: The User Authentication Log contains log messages that record successful or unsuccessful authentication requests for firewall users. Login and logout messages for LSMS Administrators and Group Administrators are recorded in the Administrative Events Log.

d) The Proactive Monitoring Log (often referred to as the Promon log), contains log messages about monitored events for bricks and LSMS

In each directory, the filenames are assigned in an ordered way. The purpose of the assignment algorithm is to assure that a lexical sort by filename also provides a chronological sort of the data in the files. This improves performance in reading log files for reports and alarms. The log files are stored in the native operating system file system on which the LSMS runs. Only authorized users are allowed access to these log files.

The LSMS provides the authorized administrator with the capability to configure the log file maximum size and the amount of disk space to allocate for all logs together in a directory. When an audit file reaches the configured log file size or a new day is started, the LSMS closes the current log file and starts a new audit file. This goes on until the log file directory is full. The LSMS must be configured to not lose audit data and halt the traffic through the Brick if any of the log directories reach the maximum allotted size. When the contents of the log directory reaches the configured maximum size, the LSMS provides the authorized administrator with the ability to reclaim disk space by clearing the log files to create space to allow traffic through the Brick.

This capability can be separately configured for each of the logs (admin, sessions, user authentication and promon). To assist in managing this capability, LVF version 7.0 has an error messages that can tell you that the logs have filled and traffic has been halted. The LSMS enables Administrators to monitor the configuration and traffic mediation of the firewalls deployed throughout the network.

The LSMS provides preconfigured alarm triggers to notify administrators when a brick has been lost and when unauthorized LSMS login attempts are made. You can also create your own alarm triggers and associate them with appropriate actions to facilitate monitoring system events of interest to you.

Alarm triggers and actions are configured on a per-Administrator basis and are not shared among Administrators. Therefore, when an LSMS Administrator or Group Administrator logs onto the LSMS, they can only view the alarm triggers and actions that they have configured themselves. Any alarms created by an LSMS Administrator or Group Administrator will apply to all groups that the administrator has rights to.

The operating system generated log files are set to a default maximum size of 10 MB. An administrator’s intervention is required to clear them when log file size has reached the maximum limit. The operating system log events can be cleared using the event viewer provided by the operating system.

The assumed TOE configuration assumes only authorized administrators of the resident operating system will have access to TOE environment containing the LSMS and its resident operating system. Hence only authorized administrators have access to log files generated by both the LSMS and the resident operating system.

Functional Requirements Satisfied: FAU_STG.1 and FAU_STG.4

6.2 TOE Security Assurance Requirements

The LVF was developed with the following security assurance measures in place, which constitutes a Common Criteria EAL 2 level of assurance.

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documents
- Tests
- Vulnerability Assessment

This section of the ST provides a mapping demonstrating that the Assurance Measures listed meet the Assurance Requirements necessary to achieve an EAL 2. In this case the specification of assurance measures is done by referencing the appropriate documentation. Analysis of the referenced documentation ensures that the documentation listed meets the Assurance requirements of the "US Government Traffic Filter Firewall Protection Profile for Low-Risk Environments version 1.1". This protection profile requires of the Assurance Requirements from part 3 of CC at EAL 2.

CC Assurance Requirements	**LVF Assurance Measures**
ACM_CAP.2	Lucent VPN Firewall Version 7.0 (Patch 531), Configuration Management v0.5
ADO_DEL.1	Lucent VPN Firewall Version 7.0 (Patch 531), Secure Delivery v0.5
ADO_IGS.1	Lucent Security Management Server Version 7.0, Installation Guide Lucent Security Management Server Version 7.0, Administration Guide Lucent Security Management Server Version 7.0 (Patch 531) TOE README FILE v1.0
ADV_FSP.1	Lucent VPN Firewall, Version 7.0 (Patch 531), Functional Specification v1.4
ADV_HLD.1	Lucent VPN Firewall, Version 7.0 (Patch 531), High Level Design v1.0
ADV_RCR.1	Lucent VPN Firewall, Version 7.0 (Patch 531), Correspondence Document v0.6
AGD_ADM.1	Lucent Security Management Server, Version 7.0 , Administration Guide, Lucent Security Management Server, Version 7.0, Reports, Alarms and Logs

	Lucent Security Management Server, Version 7.0, Tools and Trouble Shooting Guide
AGD_USR.1	Lucent Security Management Server, Version 7.0, Administraton Guide Lucent Security Management Server Version 7.0, Policy Guide
ATE_COV.1	Lucent VPN Firewall, Version 7.0 (Patch 531), Evidence of Coverage v0.9
ATE_FUN.1	Lucent VPN Firewall, Version 7.0 (Patch 531), Firewall Appliance Filtering Test Cases v0.7 Lucent VPN Firewall, Version 7.0 (Patch 531), User Model and Authentication Test cases v0.8 Lucent VPN Firewall ,Version 7.0 (Patch 531) LSMS FA-Test Results
ATE_IND.2	Lucent VPN Firewall, Version 7.0 (Patch 531)
AVA_SOF.1	Lucent VPN Firewall, Version 7.0 (Patch 531), Strength of Function Claims v0.8
AVA_VLA.1	Lucent VPN Firewall, Version 7.0 (Patch 531) , Vulnerability Analysis v0.5

Table 8: TOE Security Assurance Measures

7 Protection Profile Claims

This section provides the PP conformance claims statements.

7.1. PP Reference

The TOE conforms to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, and April 1999.

7.2. PP Refinements

The following PP requirements were further refined for this Security Target:

a) FAU_GEN.1 Audit data generation

b) FDP_IFF.1 Simple security attributes

c) FIA_ATD.1User attribute definition

d) FAU_SAR.3 (1) Selectable Audit Review

e) FAU_SAR.3 (2) Selectable Audit Review

f) FAU_STG.1 Protected audit trail storage

g) FMT_MSA.3 Static attribute initialization

h) FMT_MOF.1 Management of security functions behavior

In the case of FAU_SAR.3, the refinement interprets the TFFPP SFR to require that LVF be capable of searching the audit data for user identity, presumed subject address, ranges of dates, ranges of time, and ranges of IP address and sorting audit data based on chronological order of occurrence. LVF satisfies this SFR. .

7.3 Additional Assumptions not described in the TFFPP

- A.SECFUN which states that with the exception of I & A there are no other security functions that are accessible to the human user on the TOE other than the authorized administrators.
- The secure configuration for evaluation will be the basic network configuration as described in the Section 2.3 "Physical Scope and boundary".
- The protected network is connected to one Brick interface, the isolated LSMS network to a second, and the external network (via a router) to a third.
- The evaluated secure configuration must contain the same physical and logical isolation.
- Because of the physical and logical isolation, the A.REMACC secure usage assumption is not included. Remote administration will not be part of evaluated secure configuration functionality.

7.4 PP Objectives Not Applicable to the TOE

The following objectives that are present in the PP are not applicable to the TOE.

- O.LIMEXT
- O.SINUSE
- A.REMACC
- O.ENCRYPT

7.5 Rationale for Modified PP objectives

The following objectives (Security Objectives for TOE and Environment) that are present in the PP are modified in this ST. These refined objectives are applicable to the architecture of this specific TOE.

- O.IDAUTH
- O.MEDIAT
- A.PHYSEC
- A.GENPUR
- A.DIRECT

7.6 Rationale for not implementing all PP security objectives

The ST does not include the following TOE and environment security objectives: O.ENCRYP, O.LIMEXT, O.SINUSE and A.REMACC. These security objectives are relevant to secure remote administration of the TOE. These objectives are beyond the scope of this evaluation.

8. Rationale

8.1 Rationale For excluding A.REMACC Assumption

Because of the physical and logical isolation, the A.REMACC secure usage assumption is not included. Remote administration will not be part of evaluated secure configuration functionality.

8.2 Rationale for T.OEAUDAC in the Operating Environment

T.OEAUDAC is also encountered in the threats for the Operating Environment since the Operating Environment Administrators also have control over the LSMS.

8.3 Rationale For Modified PP Assumptions

A.GENPUR The assumption A.GENPUR from the PP is modified to be more specific to the TOE since the TOE actually stores its TSF data.

A.DIRECT The assumption A.DIRECT is modified to state that the TOE is available to only authorized administrators since there are no direct connections to the TOE

A.PHYSEC The assumption PHYSEC is modified to suit the architecture of the TOE that the Brick which is part of the TOE will be located physically secure location that might mitigate unauthorized access.

8.4 Rationale For IT Security Objectives

O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF, which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

O.SECSTA This security objective ensures that no information is comprised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

	T.NOAUTH	T.ASPOOF	T.MEDIAT	T.OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL
O.IDAUTH	X						
O.MEDIAT		X	X	X			
O.SECSTA	X					X	
O.SELPRO						X	X
O.AUDREC					X		
O.ACCOUN					X		
O.SECFUN	X						X

Table 9: Mapping of Threats To Security Objectives

8.5 Rationale For Security Objectives For The Environment

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

A.SECFUN With the exception of identification and authentication, there are no security functions on the TOE accessible to human users who are not authorized administrators.

A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

A.PHYSEC The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.

A.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.

A.DIRECT The TOE is available to authorized administrators only.

O.GUIDAN This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

O.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorized administrators receive the proper training. O.ADMTRA also counters the threat T.OEAUDAC by helping ensure the audit logs are reviewed.

A.REMACC Because of the physical and logical isolation, the A.REMACC secure usage from internal and external networks objective is not included. Remote administration will not be part of evaluated secure configuration functionality.

	T.TUSAGE	T.OEAUDAC	A.LOWEXP	A.PUBLIC	A.NOEVIL	A.SINGEN	A.NOREMO	A.PHYSEC	A.GENPUR	A.DIRECT
O.GUIDAN	X									
O.ADMTRA	X	X								
A.LOWEXP			X							
A.PUBLIC				X						
A.NOEVIL					X					
A.SINGEN						X				

A.NOREMO							X			
A.PHYSEC								X		
A.GENPUR									X	
A.DIRECT										X

Table 10: Mappings Between Threats/Assumptions and Security Objectives for the Environment

8.6 Rationale For Modified PP Objectives

O.IDAUTH This objective is modified to take into consideration the information flow through the TOE to the internal network along with granting access to TOE functions.

O.MEDIAT This objective is modified to be more specific to the architecture of the the TOE where connected networks are further classified to internal network and external network.

A.PHYSEC This objective is modified to suit the architecture of the TOE that the Brick is protected physically from unauthorized physical access.

A.GENPUR This objective is modified to be more specific to the TOE to state that the TOE stores its TSF data for its functioning.

A.DIRECT This objective is modified to suit the architecture of the TOE to state that there is no console port available to unauthorized users.

O.ADMTRA This objective is modified to lay more emphasis on the security policies.

8.7 Rationale for Threats to Objectives mapping

Assumptions and Threats	**Objectives for TOE and Environment**
Assumptions	
A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	A.LOWEXP covers this assumption by ensuring that the possibility of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

Assumptions and Threats	Objectives for TOE and Environment
A.PUBLIC The TOE does not host public data.	A.PUBLIC covers this assumption by the objective that the TOE does not host public data.
A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	A.NOEVIL covers this assumption by ensuring that the Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.	A.SINGEN covers this assumption by ensuring that Information can not flow among the internal and external networks unless it passes through the TOE.
A.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.	A.GENPUR covers this assumption by ensuring that the TOE only stores and executes security-relevant applications and only stores data required for its secure operation
A.DIRECT The TOE is available to authorized administrators only.	A.DIRECT covers this assumption by ensuring that The TOE is available to authorized administrators only.
A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.	A.NOREMO covers this assumption by ensuring that human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.PHYSEC The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.	A.PHYSEC covers this assumption by ensuring that The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access
THREATS	
T.NOAUTH An unauthorized user may attempt to bypass the security of the TOE so as to assess and use security functions	O.IDAUTH covers this threat by ***making*** sure that before any access is granted to the TSF functions or any services inside the

Assumptions and Threats	Objectives for TOE and Environment
and/or non-security functions provided by the TOE.	protected network successful authentication is performed. O.SECSTA covers this threat by ensuring that the TOE up-on startup or recovery from an interruption in the TOE service doesn't compromise any of its resources or doesn't allow any free flow of information through it to the connected network. O.SECFUN covers this functionality by ensuring that only authorized users can access the TOE security functions.
T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records form being recorded by taking actions to exhaust storage capacity, thus masking an attackers actions.	O.SELPRO covers this threat by ***ensuring*** that unauthorized users are restricted from ***bypassing, deactivating*** or tamper with TOE security ***functions***. O.SECFUN covers this threat by ensuring authorized users posses the functionality to use the TOE security functions and further by ensuring that such functionality is available to only authorized administrators.
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.	O.MEDIAT covers this threat by ensuring that the residual information from a previous information flow is not transmitted in any way.
T.MEDIAT An unauthorized person may send impermissible information through the TOE that results in the exploitation of resources on the internal network.	O.MEDIAT covers this threat by ensuring that TOE mediate the flow of all information from users on a connected network to users on another connected 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	O.MEDIAT covers this threat by ensuring that the TOE will never allow residual information of a previous information flow to be transmitted in subsequent information flows through the TOE.

Assumptions and Threats	Objectives for TOE and Environment
information flows for 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.	O.AUDREC covers this threat by ensuring that the TOE provide a means to record events with accurate dates and times and also provide capabilities to do search and sort of the audit trail ***based*** on relevant attributes. O.ACCOUN covers this threat by ensuring that only authorized administrators have control over the audit trail and no unauthorized tampering of the audit trail.
T.SELPRO An unauthorized user may read, modify, or destroy security critical TOE configuration data.	O.SECSTA covers this threat by ensuring that no information is comprised by the TOE upon start-up or recovery. O.SELPRO covers this threat by ensuring that the TOE has the capability to protect itself against attempts by unauthorized users to bypass, deactivate or tamper with TOE security functions.
T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.	This threat has been mapped to the objective O.SINUSE which states that the TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network. Authentication to the TOE from a connected network is a remote administration. Remote administration is not part of the evaluated TOE.
T.PROCOM 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.	Remote administration of the TOE is not part of the current evaluation and this threat can be ignored
T.REPLAY An unauthorized person may use valid identification and authentication data obtained to access	Remote administration of the TOE is not part of the current evaluation and this threat can be ignored.

Assumptions and Threats	**Objectives for TOE and Environment**
functions provided by the TOE.	
T.TUSAGE The TOE may be used and administered in an insecure manner.	O.GUIDAN covers this threat by ensuring that the TOE is delivered, installed, administered and operated in a manner that maintains security. O.ADMTRA covers this threat by ensuring that authorized administrators are trained as to establishment and maintenance of security policies and practices.

8.8 Rationale For Security Requirements

The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified in this security target. Those security objectives imply probabilistic or permutational security mechanism and that the metrics defined are the minimal “industry” accepted (for the passwords) and government required (for the encryption) metrics they should be good enough for SOF-Basic.

FMT_SMR.1 Security roles

Each of the CC class FMT components in this Security Target depend on this component. It requires the ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the user’s identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_UAU.1 Timing of authentication

This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this requirement is defined in section 5.1.1.5 to ensure that the authentication mechanism chosen cannot be easily bypassed. This component traces back to and aids in meeting the following objectives: O.IDAUTH.

FDP_IFC.1 Subset information flow control

This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes

This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FMT_MSA.3 Static attribute initialization

This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FDP_RIP.1 Subset residual information protection

This component ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_SEP.1 TSF domain separation

This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_GEN.1 Audit data generation

This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3(1) Selectable audit review

This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

The TOE provides a Log Viewer tool where filters can be created based on the presumed subject address and range of addresses. When the filter is applied against the log data the relevant data matching against the filter is fetched and displayed. Before the filter is applied the range of dates for which the filtered audit data is requested can be mentioned in one of the screens of the Tool. The data is displayed in manner suitable for sorting by clicking on the heading section tab of each column.

FAU_SAR.3(2) Selectable audit review

This component ensures that sorting of the audit data could be done based on the chronological order of audit event occurrence. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status.

The maximum number of audit records that could be lost is 656..

This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FMT_MOF.1 Management of security functions behavior

This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, and O.SECSTA

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN
FMT_SMR.1							X
FIA_ATD.1	X						
FIA_UID.2	X					X	
FIA_UAU.1	X						
FDP_IFC.1		X					
FDP_IFF.1		X					
FMT_MSA.3		X	X				X
FDP_RIP.1		X					
FPT_RVM.1				X			

FPT_SEP.1				X			
FPT_STM.1					X		
FAU_GEN.1					X	X	
FAU_SAR.1					X		
FAU_SAR.3(1)					X		
FAU_SAR.3(2)					X		
FAU_STG.1				X			X
FAU_STG.4				X			X
FMT_MOF.1			X				X

Table 11: Mappings Between TOE Security Functions and IT Security Objectives

8.9 Rationale for Security Objectives to Security Requirements mapping

Security Objective		IT Security Requirement
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.	FIA_ATD.1 satisfies this objective by ensuring that the TOE maintain the identity and association of the human user/user name with the authorized administrator role. FIA_UID.2 satisfies this objective by ensuring that the TOE grants access to users only after they have been successfully authenticated FIA_UAU.1 satisfies this objective by ensuring that authorized administrators or unauthorized external IT entity is authorized prior to performing any TSF mediated actions.
O.MEDIAT	The TOE must mediate the flow of all information between users on an internal network connected to the TOE and users on an external network connected to the TOE, and must ensure that residual information from previous information flow is not transmitted in any way.	FDP_IFC.1 satisfies this objective by enforcing the policies on the flow of information through the TOE from one subject to another. FDP_IFF.1 satisfies this objective by enforcing the Security Function Policy on the information flow through the TOE. Further policies can be made to allow information flow through simple security attributes. These policies can be applied to appropriate information flows to allow/deny flow to/from a connected

Security Objective		IT Security Requirement
		network to an external network through the TOE. FMT_MSA.3 satisfies this objective by having restrictive default values to control the information flow through the TOE. Also, these default values can be altered to control the information flow. FDP_RIP.1 satisfies this objective by ensuring that any previous information content of a resource or a prior information flow is made unavailable to the subsequent information flows.
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_MSA.3 satisfies this objective by having restrictive default values to control the information flow through the TOE. Also, these default values can be altered to control the information flow. FMT_MOF.1 satisfies this objective by ensuring that only authorized administrators have control of specifying the restrictive default values, start-up and shut-down of the TOE and creation of policy rules to permit information flow.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	FPT_RVM.1 satisfies this objective by enforcing the TSP before each function within the TSC are allowed to proceed. FPT_SEP.1 satisfies this objective by ensuring that the TOE is protected from interference and tampering by untrusted subjects FAU_STG.1 satisfies this objective by ensuring that the audit data trail is not lost and that no unauthorized modifications of the audit trail can be done. FAU_STG.4 satisfies this objective by ensuring that the audit data trail is safe and if full the information flow through the

Security Objective		IT Security Requirement
		TOE is stopped until an authorized administration takes action.
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.	FPT_STM.1 satisfies this objective by providing reliable timestamps for its own use FAU_GEN.1 satisfies this objective by collecting all necessary audit events which include the date and time when the event occurred along with all relevant parameters of the event. FAU_SAR.1 satisfies this objective by allowing the administrator with the capability to read all the audit trail data from the audit records. FAU_SAR.3(1) satisfies this requirement by providing the TSF to peruse the audit data by convenient searching of audit data based on vital parameters of the type of events.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions.	FIA_UID.2 satisfies the objective by ensuring that each user is identified before performing any TSF-mediated actions on behalf of the user. FAU_GEN.1 satisfies this objective by ensuring that all requests for information flows through the TOE are audited. Also all attempts to log into the TOE are audited.
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.	FMT_SMR.1 satisfies this objective by maintaining administrative roles and by associating each administrator in a particular role with his human identity. FMT_MSA.3 satisfies this requirement by ensuring that only authorized administrators be granted privileges to change the restrictive default values governing the creation of objects FAU_STG.1 satisfies this objective by

Security Objective	IT Security Requirement
	ensuring that only authorized administrator's access audit records. FAU_STG.4 satisfies this objective by ensuring that audit records are not lost if audit trail is full. FMT_MOF.1 satisfies this objective by restricting the TSF-mediated functions to authorized administrators only.
O.SINUSE	This security objective is relevant to secure remote administration of the TOE. This objective is beyond the scope of this evaluation because remote administration of the TOE is not permitted in the evaluated configuration.
O.ENCRYP	This security objective is relevant to secure remote administration of the TOE. This objective is beyond the scope of this evaluation because remote administration of the TOE is not permitted in the evaluated configuration.
O.LIMEXT	This security objective is relevant to secure remote administration of the TOE. This objective is beyond the scope of this evaluation because remote administration of the TOE is not permitted in the evaluated configuration.

8.10 Rationale for Omitted PP SFRs

Omitted SFR	Rationale
FCS_COP.1	FCS_COP.1 is a conditional requirement that needs to be satisfied if the TOE supports remote administration. Remote Administration of the TOE is not in the scope of the current evaluation.
FIA_AFL.1	FIA_AFL.1 requires that number of unsuccessful authentication attempts from an entity internal to the network or external to the network have to be controlled. TOE under evaluation does not support remote administration and hence does not

	allow authentication to it either from internal network or external network.
FIA_UAU.4	FIA_UAU.4 is a conditional requirement that needs to be satisfied if the TOE supports remote administration. Remote administration of the TOE is not in the scope of current evaluation.

8.11 Rationale For TOE Summary Specifications

Mapping of Security Functions to Security Functional Requirements

TOE Security Functions (6.1)	Security Functional Requirements	Rationale
TOE Security Management	**FMT_MOF.1** **FMT_MSA.3** **FMT_SMR.1**	The TOE provides ability to start-up and shutdown, change policy, user authentication data, configure a number of permitted authentication attempt failures and restoring the authentication capability to users, modifying date and time, view and modify audit trail, manage backup activities.(*FMT_MOF.1*) The TSF provide default values for security attributes (*FMT_MSA.3*), which can be overridden by an initial value and managed by users in certain roles. The TOE can implements managing the group of roles that can interact with the security attributes and the initial values of security attributes for the access control SFP (*FMT_SMR.1*).
Identification and Authentication	**FIA_UAU.1** **FIA_ATD.1** **FIA_UID.2**	To gain access to the TOE data and functionality the authorized users must successfully authenticate and identify themselves (*FIA_UAU.1*) and the perform authentication .The TOE shall maintain the identity of the user. The TOE uses the System Administrator account information to make authentication decisions based upon the userID and password provided to it. (*FIA_ATD.1, FIA_UID.2)*
User Data Protection	**FDP_IFC.1** **FDP_IFF.1** **FDP_RIP.1**	The TOE controls the incoming and outgoing packets and imposes security policy to filter them. *(FDP_IFC.1)* The TOE filters packets based on direction of the packet,

		source address, destination address, direction of flow and service. Packets are allowed to pass through the TOE only if the imposed rules are met and all other packets are either dropped or appropriate actions are taken. *(FDP_IFF.1)* The TOE ensures that the residual information is unavailable to other resources.*(FDP_RIP.1)*
Protection of TOE Security Functions	**FPT_RVM.1** **FPT_SEP.1**	The secure configuration providing the physical and logical isolation of the TOE supports the Protection of TOE Security Functions. Further the to ensure that the security functions on the VPN Firewall Brick can not be tampered or bypassed, the security functions are embedded in the inferno operating system. The secure LVF configuration assumes only authorized administrators will have access to the LVF environment containing the LSMS and its resident operating system. *(FPT_RVM.1)* All packets should pass through the VPN Firewall Brick and the VPN Firewall Brick has no user accounts or passwords. This implementation provides the required TSF domain separation.*(FPT_SEP.1)*
Security Audit	**FAU_GEN.1** **FPT_STM.1** **FAU_SAR.1** **FAU_SAR.3** **FAU_STG.1** **FAU_STG.4**	The TOE collects audit records from all of its subsystems and timestamps it with the native operating system clock and logs it.*(FAU_GEN.1 and FPT_STM.1)* The TOE allows authorized administrators to view configure the security policy and audit data. The TOE also allows authorized administrators to view audit data in a convenient manner. It also enables authorized administrators to monitor the configuration of and access to the VPN Firewall Brick deployed. *(FAU_SAR.1 and FAU_SAR.3)* The TOE protects the audit data from unauthorized deletion The TOE provides authorized administrators with the capability to configure the log file maximum and the amount of disk space to allocate or all logs.*(FAU_STG.1)* The audit storage management architecture ensures that storage for audit data will never be exhausted and cause the VPN Firewall Brick to stop passing traffic or the LSMS from performing properly.*(FAU_STG.4)*

Table 12: Mappings Between TOE Security Functions to Security Functional Requirements

8.12 Rationale For Assurance Requirements

EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. As such, minimal additional tasks are imposed upon the vendor to the extent that if the vendor applies reasonable standards of care to the development, evaluation may be feasible without vendor involvement other than support for functional testing and vulnerability testing verification. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

8.13 Rationale For Not Satisfying All Dependencies

Functional component FMT_MSA.3 depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. Therefore FMT_MOF.1 more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Protection Profile.

8.14 Consistency and Mutually Supportive Rationale

The set of security requirements provided in this LVF ST form a mutually supportive and internally consistent whole as evidenced by the following:

a) The choice of security requirements is justified as shown in Sections 8.8, Section 8.9 and 8.10. The choice of SFR and SARs were made based on the assumptions about, the objectives for, and the threats to the TOE and the security environment. This ST provides evidence the security objectives counter threats to the TOE, and also, the assumptions and objectives counter threats to the TOE environment.

b) The security functions of LVF satisfy the SFRs. All SFR dependencies have been satisfied with the exception of those noted in Section 8.13.

c) The SOF claims are valid and are satisfied. The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified in this security target. The identified metrics and SOF claim is commensurate with the EAL2 level of assurance.

d) The SARs are appropriate for the assurance level of EAL2 and are satisfied by LVF v7.0 and are satisfied. EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor.