Lucent Technologies
Lucent VPN Firewall
Version 7.2
(Patch 292)
EAL4
Security Target

Version: 2.1

December 13, 2005

Lucent Technologies
600 Mountain Ave.
Murray Hill, NJ 07974-0636

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 contains sections which address Security Environment, Security Objectives, and IT Security Requirements, as well as Security Objectives Rationale and Security Requirements 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 VPN Firewall (LVF) V7.2 EAL4 Security Target, Version 2.1
TOE Identification:	Lucent VPN Firewall (LVF) v7.2 with Patch 292[1]
CC Identification:	Common Criteria for Information Technology Security Evaluation (CC),

[1] For the purposes of Common Criteria, the TOE is composed of the group of products under evaluation, the Guidance Manuals associated with those products, and all the Common Criteria specific documentation created for the purpose of evaluation. This complete set of items is collectively referred to as the TOE.

	Version 2.1, August 1999 (**aligned with ISO/IEC 15408: 1999)** including interpretations as of October 06, 2003.
PP Identification:	None
Assurance Level:	Evaluation Assurance Level 4
Keywords:	Information flow control, firewall, packet filter, network security, traffic filter, security target
ST Author	Corsec Security Inc.

1.2 Organization of Security Target

The LVF v7.2 ST contains the following sections:

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

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

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

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

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

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

7) **Protection Profile Claims**: States there is no Protection Profile conformance claims

8) **Rationale**: 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 Part 2 Conformant and CC Part 3 conformant including interpretations as of October 06, 2003. Additionally, the TOE claims conformance to the Evaluation Assurance Level 4 package.

1.2.2 Protection Profile Conformance Claims

None

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 *underlined italicized text*.

- The iteration operation is used to repeat or reuse a CC requirement multiple times in the same document with different operations used to complete the requirement for each occurrence. Iterations are denoted by an increasing number inside parenthesis following the requirements short name. Example: FCS_COP.1 (1).

- 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).**

1.2.4 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. In addition to these general definitions, this Security Target also provides the more specialized definitions. They are listed here to aid the user of the Security Target:

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

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. An Authorized administrator also is an authorized operating system administrator.

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.

Data Encryption Standard (DES) – A method for encrypting information. DES was approved as a federal standard in November 1976, and published on 15 January 1977 as FIPS PUB 46, authorized for use on all unclassified data. It was subsequently reaffirmed as the standard in 1983, 1988 (revised as FIPS-46-1), 1993 (FIPS-46-2), and again in 1998 (FIPS-46-3), the latter prescribing "Triple DES" (see below).

Encrypted Socket Connection – This term is used to refer to the encrypted socket connection between the LSMS and other TOE components. If encrypted socket is mentioned without a reference to the TLS protocol then it means that Lucent-developed protocol which is similar to Secure Socket Layer (SSL) v3.0 is used. It uses Triple DES (Data Encryption Standard) for encryption and keyed SHA-1 (Secure Hash Algorithm) for integrity and authentication. When LSMS and FA are communicating mutual-authenticated takes place. All cryptographic operations are FIPS 140-2 validated.

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

FA – The abbreviation used to refer to the Lucent Firewall Appliance which also known as the Brick.
Human user – Any person who interacts with 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.

LSMS Host - The machine running the LSMS software package.

LSMS Remote Navigator Host – The machine running the LSMS Remote Navigator.

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

SHA-1 – This standard specifies a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file. The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify.

Transport Layer Security (TLS) – TLS is a cryptographic protocol which provide secure communications on networks. TLS provides endpoint authentication and communications privacy.

Triple DES (3DES) – One solution to overcome the short-key limitation is to run the Data Encryption Standard (DES) algorithm a multiple number of times.

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

1.2.5 Acronyms

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

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level

FA	Firewall Appliance
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
LSMS	Security Management Server
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TLS	Transport Layer Security
UDP	User Datagram Protocol

1.3 Security Target Overview

The Lucent VPN/Firewall (LVF) architecture consists of three physically distinct components:

- The Lucent VPN/Firewall Appliance (FA), which controls the flow of Internet Protocol (IP) traffic between network interfaces. The FA is also referred to as the Brick;

- The Lucent Security Management Server (LSMS) software package, enabling administrators to manage the security of one or more Firewall Appliances (FA). The LSMS software package running on the host are jointly called the LSMS as a general term for the both components together as a workstation.

- The Lucent Security Management Server (LSMS) Remote Navigator is a Graphical User Interface client, enabling administrators to manage the security of one or more Firewall Appliances by remotely accessing the primary LSMS software package.

The firewall application code runs on Inferno™, a Bell Labs developed operating system. The separate Lucent Security Management Server software package runs on either Windows or Solaris host environments as described in the TOE Environment. An Administrator can log into the LSMS software package remotely using the LSMS Remote Navigator client, which is installed on Window host environment.

The Firewall Appliance (FA) controls the flow of IP packets based on security policy rules. As with other traffic filter firewalls, the FA controls the flow of packets based upon the interface of arrival, interface of egress, source and destination addresses, upper level protocol and ports, and action to be taken (pass or drop). The FA consists of the Lucent firewall application running on the Inferno operating system.

Policy rules are defined by authorized administrators using the LSMS software package. The LSMS software package also supports the management of the other LVF security features notably, auditing features (reports, alarms[2] and logs), secure communications and administrator accounts,

The LSMS software package includes the LSMS Application, the LSMS Navigator, and the LSMS Command Line Interface. The administrative interface to the LSMS software package is provided by the following interfaces:

1. LSMS Navigator
2. LSMS Command Line Interface and
3. LSMS Remote Navigator
4. Log Viewer
5. Configuration Assistant

1.4 Common Criteria Conformance Claims

The TOE and hence this ST claims to be

[2] The alarms feature is not a part of the evaluated configuration of the TOE

Common Criteria for Information Technology Security Evaluation, Version 2.1, Part 2 – August 1999 including interpretations as of October 06, 2003.

CC Version 2.1 Part 2 – conformant

CC Version 2.1 Part 3 – conformant

Additionally, the TOE claims conformance to the Evaluation Assurance Level 4 package.

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 General TOE Functionality and Product Type

This section identifies the LVF's product type.

The LVF is a traffic-filter firewall with management software. A traffic-filter firewall controls the flow of Internet Protocol (IP) packets by matching information contained in IP and upper 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 features the LVF offers are listed below. 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 this Common Criteria evaluation.

The following features of the LVF are validated in the Common Criteria evaluation:

a) Stateful Packet filtering: Every packet processed by the FA is considered part of a "session", regardless of IP type or upper-layer protocol instead of processing each and every packet individually.
b) Logging: All logging is done in real-time from the FA to its management server (LSMS application). Apart from the logging events on the FAs the LSMS application 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 application has the ability to generate HTML-based reports and serve them via its own internal secure web server (HTTPS)

e) Remote administration: An LSMS application can manage multiple FAs that are located remotely in a secure manner. An LSMS Remote Navigator can manage an LSMS application remotely in a secure manner.

The following are the features that the LVF provides which are **not** in the scope of current Common Criteria evaluation.

f) Dynamic Address Support: The FA has the ability to exist in a dynamic address environment. The FA can register its public address with its management server when used behind a many to one NAT device.
g) Application Filters: The FA has the ability to perform inspection at the application layer of packet-based traffic passing through it using its unique Application filter architecture.
h) Denial of Service: The FA offers a variety of denial of service mechanisms tailored to both existing attacks as well as newly-emerging attacks not yet seen.
i) Alarms: The LSMS application has the ability to create alarm triggers and associate them with appropriate actions to facilitate monitoring systems events.
j) QoS: The TOE provides Quality of Services features, specifically Bandwidth management functionality.
k) VPN: The TOE provides confidentiality and integrity of an enterprise's messages by means of Virtual Private Networks (VPNs) between the enterprise's Firewall Appliances (LAN-LAN VPN as well as Client-to-LAN VPN, using the IPSec protocol), using IP Security Protocol (IPSec) encryption and cryptographic checksums.
l) The FA 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 FA 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]
- RPCs
- DNS
- GTP

2.2 Application Context

The LVF is used to connect networks where information flows to and from the networks must be controlled based on security policies. The LVF which consists of an LSMS software package, an LVF FA, and an LSMS Remote Navigator application can be deployed in various ways as shown in the figure below.

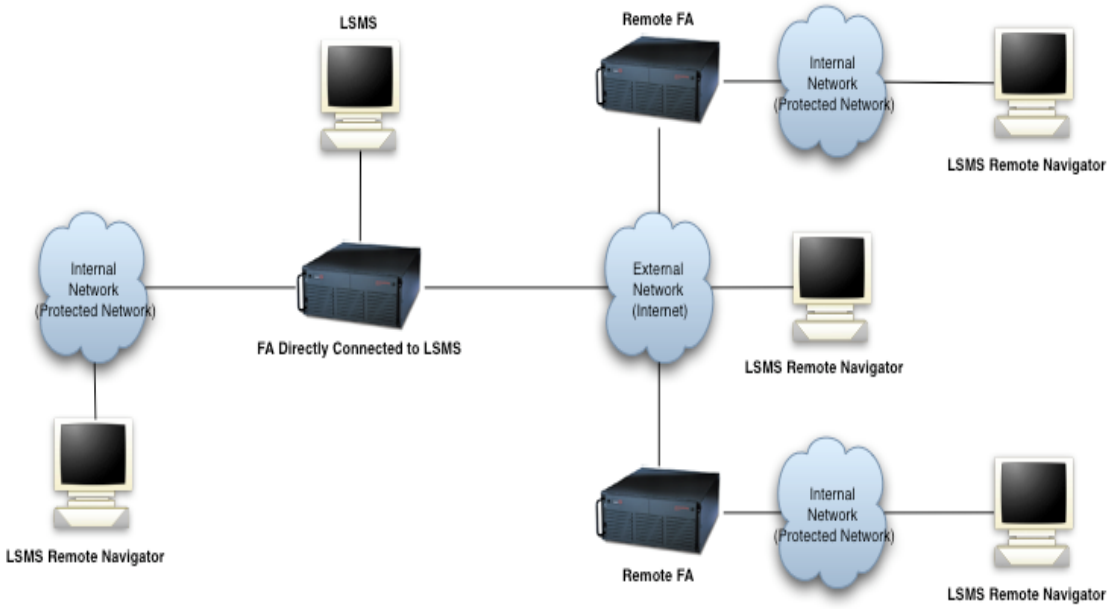

Figure 1: Possible Deployment Configuration

The LSMS host is directly connected to a FA. An LSMS Remote Navigator host can be present in any Internal Network, a network protected by an FA. Additionally, an LSMS Remote Navigator host can be located on an External Network, such as the Internet.

2.3 Physical Scope and Boundary

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

- The Firewall Appliance, which controls the flow of IP packets between network interfaces; and
- The LSMS software package, which enables administrators to manage the security of multiple FA's.
- The Lucent Security Management Server (LSMS) Remote Navigator software, enabling administrators to manage the security of one or more FA's by remotely accessing LSMS application.

This evaluation involves two TOE configurations as described in the **Figure 2: TOE Configuration #1** and **Figure 3: TOE Configuration #2.** The TOE Configuration #1 represents the set of the TOE components to provide the full set of functionality described in this ST. The TOE Configuration #2 is a superset of TOE Configuration #1 and shows how additional FA's and LSMS Remote Navigators can be added to the deployment. A requirement for the TOE to be deployed in the evaluated configuration is one Firewall Appliance, one LSMS software package whose host machine is directly connected to the FA and one LSMS Remote Navigator. This configuration is represented in TOE Configuration #1.

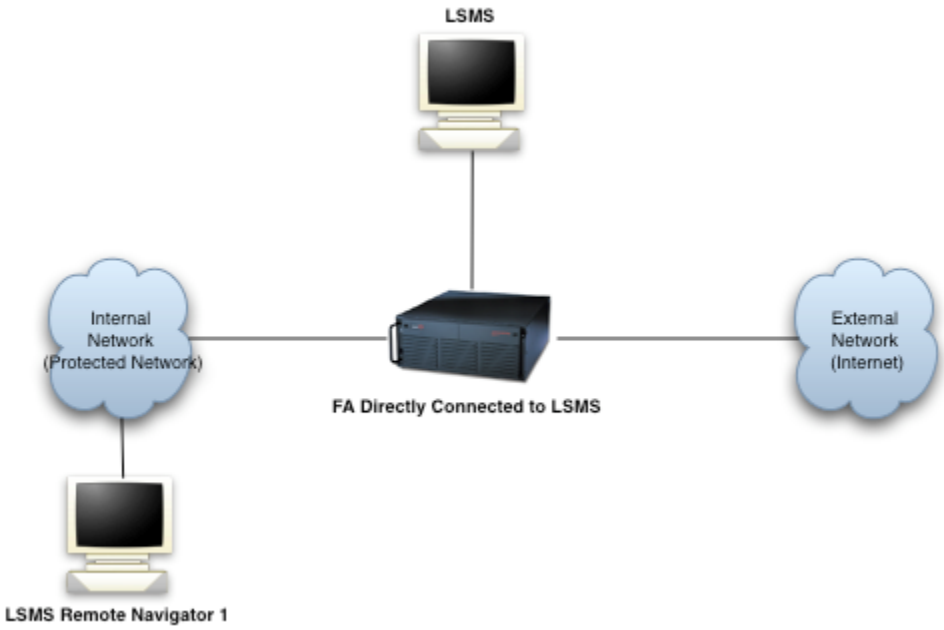

Figure 2 - TOE Configuration[3] #1

[3] It is recommended to secure host running LSMS Remote Navigator and further guidance is provided the TOE ReadMe section 2.2

There are two secure communication paths that are established through the connections depicted in Figure 2.

- The LSMS application negotiates and establishes a encrypted socket connection from the LSMS application to the FA.
- The LSMS application negotiates and establishes an encrypted socket connection from the LSMS application to the LSMS Remote Navigator. The initial request to establish an encrypted socket connection is made by the LSMS Remote Navigator.

The larger TOE deployment configuration evaluated, named TOE Configuration #2, includes: two Firewall Appliances, two LSMS Remote Navigators, and one LSMS software package. The interconnection between these components is depicted in the configuration shown in Figure 3 below.

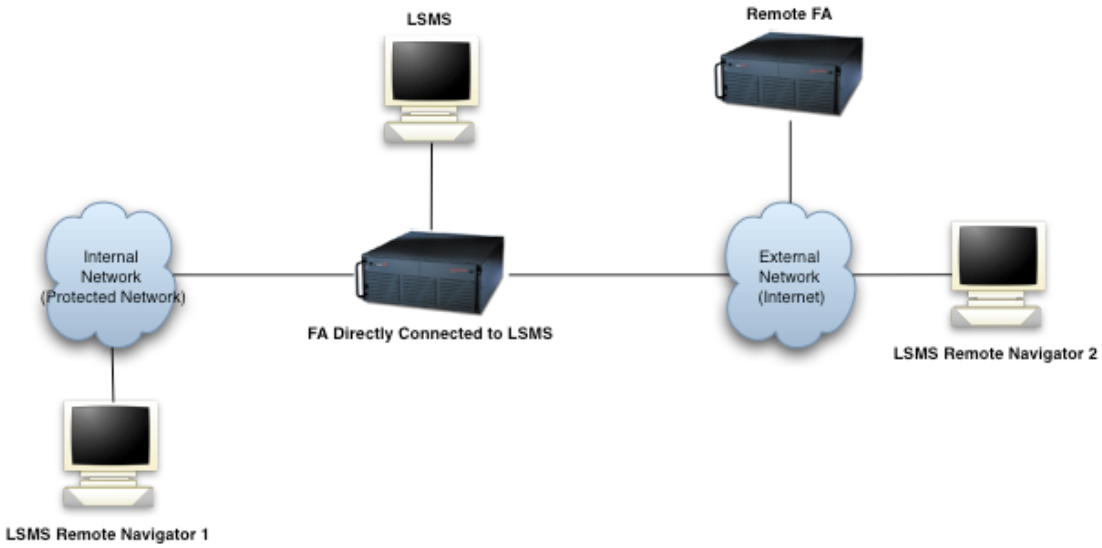

Figure 3 - TOE Configuration #2

There are two secure communication paths that are established through the connections depicted in Figure 3.

- The LSMS application negotiates and establishes an encrypted socket connection from the LSMS application to any FA whether it is locally connected or remotely located.
- The LSMS application negotiates and establishes a secure communication from the LSMS to any LSMS Remote Navigator, whether is it on an internal or external network. The initial request to establish an encrypted socket connection is made by the LSMS Remote Navigator.

Each model of the firewall appliance has multiple network interfaces as described in Section 2.3: Physical Scope and Boundary, Table 1: Firewall Appliance Hardware. Three network interfaces are used in the evaluated configurations; one for connecting to the External Network, one for connecting to the Internal Network, and one for connecting directly to the LSMS host. The FA is used to control information flow between the internal and external networks. For the TOE configurations at least one FA must be directly connected to the LSMS host. The second FA can be installed anywhere geographically but must be on an interconnected network with the LSMS.

The LSMS Remote Navigator host could be located on either an internal network (protected network) or an external interconnected network (i.e. the internet).

The scope of the evaluated configuration allows an administrator to administer multiple FAs from a single LSMS application. Additionally an administrator can connect to the LSMS application to perform FA administration from an LSMS Remote Navigator. The communications between the LSMS application and the FA, and the communications between the LSMS Remote Navigator and LSMS application are all through an encrypted socket connection, which provides confidentiality and integrity. The cryptographic software modules on the LSMS Remote Navigator, LSMS application and the FA that provide secure communications for the TOE are all either FIPS 140-2 validated cryptographic modules or FIPS 140-2 compliant cryptographic modules (See Secure Communications: *FIPS 140-2 Approved Cryptographic Support*).

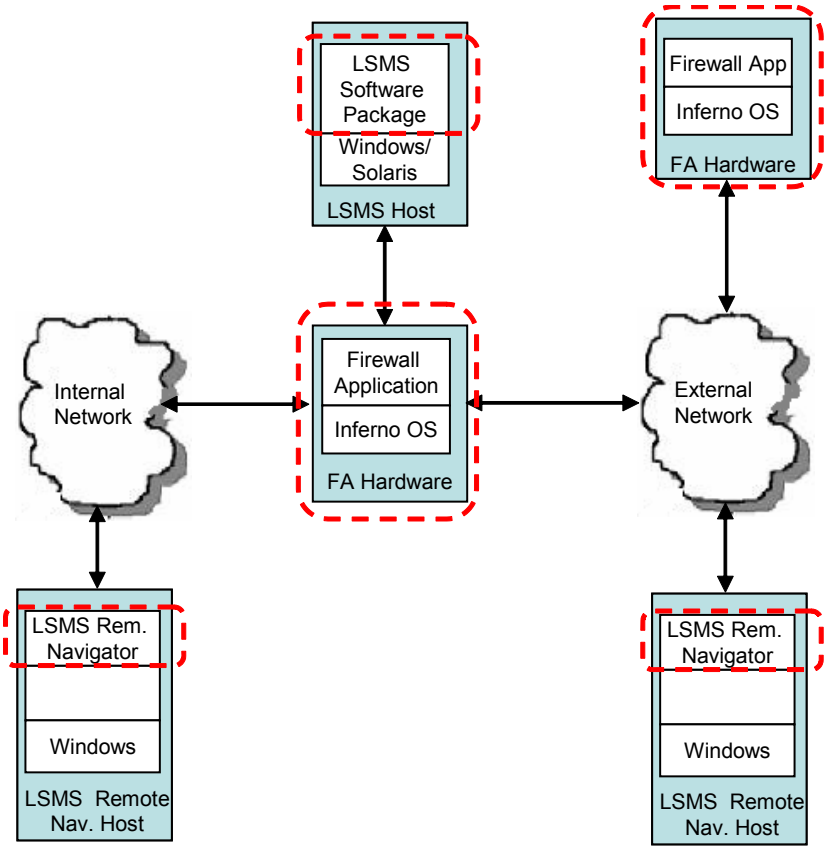

Figure 4: TOE Boundary and Environment

The physical scope of the TOE includes the component circled in red dashed lines in Figure 4. The figure presents the TOE Configuration #2; however, as this a superset of TOE Configuration #1, it includes all parts that will make up the TOE Configuration #1.

The physical TOE components include:

- The LSMS software package consists of the LSMS Software Application, LSMS Command Line Interface and the LSMS Navigator.
- One or two Firewall Appliances along with the FA operating system, the three NICs, and the firewall application software that runs on the FA hardware, and
- One or two LSMS Remote Navigators.

The TOE Environment is required to include the following components, which are not part of the TOE:

- The host machines and the operating systems for the LSMS Remote Navigator and LSMS software package;
- The NICs on the LSMS host and LSMS Remote Navigator hosts;

The simplest TOE configuration consists of one LSMS directly connected to an FA and an LSMS Remote Navigator installed anywhere on an interconnected network. The LSMS application can manage one to many FAs and can support remote management from one to many LSMS Remote Navigators. Management of a single FA is the same as managing multiple FAs. All the same security features, including secure communication, exist for each additional FA installed in the configuration. Further, the LSMS application handles one LSMS Remote Navigator connection in the same fashion as multiple LSMS Remote Navigators connecting to perform management. All of the same security features, including secure communication, exist for each additional LSMS Remote Navigator installed in the configuration. Therefore, installing one LSMS application and any number of Bricks and LSMS Remote Navigators will still allow the deployment to remain EAL 4 compliant because the TOE components will continue to operate in the same fashion and will provide the same set of security functionality. The additional LSMS Remote Navigators will operate with the LSMS Software Package in the same fashion as the single LSMS Remote Navigator and they will provide the same security functionality and services as the single LSMS Remote Navigator. Likewise, the additional Bricks will operate with the LSMS Software Package and provide the same security functionality as the single Brick in TOE Configuration #1. Figure 1, above demonstrates a possible deployment configuration.

The Lucent firewall application and the Inferno Operating System can be run on several hardware models, which are called Firewall Appliances (FA) or Bricks or VPN Firewall Brick Models. The different Brick models provide different scalable solutions and are all included in this evaluation:

- Lucent VPN Firewall Brick Model 300 (FIPS Compliant based on vendor assertion)
- Lucent VPN Firewall Brick Model 350 (FIPS Validated)
- Lucent VPN Firewall Brick Model 500 (FIPS Compliant based on vendor assertion)
- Lucent VPN Firewall Brick Model 1000 (FIPS Validated)
- Lucent VPN Firewall Brick Model 1100 (FIPS Validated)

The Lucent VPN Firewall Brick models listed in 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 application.

The following table provides the detailed specifications of the Lucent VPN Firewall Brick Models or FA or Brick hardware models.

VPN	Processor	Memory	Ethernet	Fiber	Capacity	Encryption

Firewall Brick Model Number			ports	Gigabit interfaces	Clear text / sessions	Accelerator
300 (FIPS Compliant based on vendor assertion)	Pentium III 1.26 Ghz	128MB RAM	8 10/100 RJ45	N/A	650MBPS / 400,000	O
350 (FIPS Validated)	2.4GHz Xeon	512MB	7 10/100	1	TBD	1
500 (FIPS Compliant based on vendor assertion)	Pentium III 1.26 Ghz	256MB RAM	14 10/100 RJ45	1	975MBPS / 600,000	O
1000 9/2 (FIPS Validated)	Pentium III 1 Ghz	1GB RAM	9 10/100 RJ45	2	1.5GBPS / 3 million	n/a
1000 7/2 (FIPS Validated)	Pentium III 1 Ghz	1GB RAM	7 10/100 RJ45	2	1.5GBPS / 3 million	I
1000 5/4 (FIPS Validated)	Pentium III 1 Ghz	1GB RAM	5 10/100 RJ45	4	1.5GBPS / 3 million	n/a
1000 ¾ (FIPS Validated)	Pentium III 1 Ghz	1GB RAM	3 10/100 RJ45	4	1.5GBPS / 3 million	I
1100 (FIPS Validated)	2.4 GHz Xeon	2 GB RAM	7 10/100	0,4,6 (three configurations)	3.0, 2.6, 3.0 / 4 million respectively for three configurations.	2, 3, 2 respectively for three configurations.

Table 1: Firewall Appliance Hardware

The FAs vary in hardware configurations as shown in the above table (i.e. memory size, number of Ethernet ports). The software image that implements the security enforcing functionality is the same on all FAs. Hence all the FA models are considered identical. They are identical because one can take any software binary image (tvpc or tvpc.z file) from any FA and run it on any other FA. This can be verified simply by doing a "make floppy" operation for each FA and then comparing the image files on the floppy for each FA.

The same software binary image ("tvpc.Z") runs on all modules, so all features are available on all module platforms. The binary images are identical across all platforms, regardless of the FA's model number or configuration setup.

However, since the OS image provides a superset of all drivers that can interface with the module, each module only needs to use a subset of the drivers installed. When the administrator creates the floppy bootable OS image from the Lucent Security Management Server, one of the selectable options (via a drop down box) in the LSMS application is to reference the specific driver configurations of the FA model. This selection of the FA model specifies which subset of drivers is needed and places this configuration data within a separate configuration file ("inferno.ini"), which is created alongside the OS image. The purpose of the configuration file is to distinguish which drivers are applicable to the module it is installed on, while the binary image file ("tvpc.z") serves as the same identical executable applicable to all FA models.

2.4 Logical Scope and Boundary

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

User Data Protection: The firewall software that runs on the FA is based on the Inferno™ operating system, a Bell Labs-developed operating system. The firewall code is imbedded within the Inferno™ operating system kernel. The operating system itself has no user accounts. The entire firewall software resident on the FA fits on a single 3.5-inch floppy diskette. The FA communicates with its Security Management Server using IP.

The FA must be assigned a logical IP address. To preserve network invisibility, the FA protecting the LSMS host can be configured to communicate only with the LSMS's over a private network address, where the administrative policies only allow administrative traffic while dropping all other communication attempts.

All communications between each FA and the Lucent Security Management Server (LSMS application) are encrypted and authenticated using an encrypted socket connection.

The FA (local or remote) must be visible to the Lucent Security Management Server's IP address on at least one physical interface, but can be invisible at the network layer to network elements on the other physical interface ports. The firewall software in the FA consists of modules, proxies, and applications. The FA boot diskette contains the FA operating system, firewall application (the operating system and firewall application are a single executable), FA assigns IP address and subnet address for each FA interface, Certificate Authority key, the IP address of the LSMS host responsible for managing the FA, and the default firewall policy along with any additional policies that may be required.

The FA initially boots from a floppy diskette that is created by the LSMS application. Boot images after the initial boot can be loaded from FLASH RAM in about 30 seconds. The FA operating system can be pushed to each FA from the LSMS application when the FA is capable of communicating with the LSMS application, without physically interacting with the device. However, if the FA is being setup and installed for the first time in a remote location from the LSMS application, a boot floppy will need to be delivered to that location and the FA will needed to be administered accordingly.

The FA controls the flow of incoming and outgoing IP packets. The security policy rulesets are created by authorized administrators using the LSMS Navigator or LSMS Remote Navigator. The LSMS Navigator is the GUI component of the LSMS software package. The Lucent Security Management Server (LSMS) is the means by which administrators manage the security of one or more FAs. The policy rulesets are then pushed from the LSMS application to the operating system (Inferno) on the FA. The security policy which controls the information flow through the FA is embedded within the Inferno™ operating system kernel. The FA extracts information from the IP packet header and applies rules from a security policy. The 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 FA 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 is the Firewall Appliance.

Security Audit: The FA detects the occurrence of selected events, gathers information concerning them, and sends that information to the LSMS application. The LSMS software package collects this information; time stamps it and stores it in log files on the LSMS host operating system in the TOE Environment. The LSMS application also detects the occurrence of selected events (e.g., security administrator actions), gathers information concerning them, and records it. Audit review is accomplished by LSMS reports generated by an LSMS web server and LSMS log viewer which are components of the LSMS. The primary components of the LVF that implement the Security Audit are LSMS software package and the FA.

Identification and Authentication (I&A): The LSMS software provides the tools to manage the security policies of the Groups that are applied to the FA. The software runs at the application layer using Java™ on the resident operating system. The LSMS application implements and enforces an administrator privilege model.

The TOE allows only a small number of services to be accessed by an unauthenticated entity before the entity is identified and authenticated as an administrator to the TOE. These services include: the presentation of the LSMS Navigator Login window, presentation of LSMS Logviewer window, presentation of LSMS Remote Navigator Window, Start Services, Stop Services, Restart Services, Utilities menu access. This is only on the LSMS host machine and cannot be done from the RN but for the login window.

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 application. Administrators have to successfully log into the operating system before an LSMS login. The LSMS application requires administrators to identify and authenticate themselves before they can perform any other LSMS actions. The FA has no user (including administrator) accounts. The primary components of the LVF that implement the I&A are the LSMS software package and the LSMS Remote Navigator.

Security Management: The LSMS provides all LVF security management capabilities. Administrators manage the security policy rules enforced by the FA and configuration parameters and administrator accounts using the LSMS. All edits to the policy and user account information of the LSMS is stored in the relational database which is a part of the TOE Environment. The primary components of the TOE that implement the Security Management are the LSMS software package and the LSMS Remote Navigator.

Protection of TOE Security Functions: The security functions which implement the LVF access control policy are physically separated from the unauthenticated external IT entities which send and receive IP packets through the FA; 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 the LSMS software package and the FA.

Secure Communications: The communications between the LSMS application and the FA and the communication between LSMS application Remote Navigator and LSMS are all through an encrypted socket connection which provides confidentiality and integrity.

The LSMS application also has a simple Web server (part of the RAP subsystem) which is used to deliver reports and help files. This Web server is configured for HTTPS for the purposes of this TOE. Once an

administrator is logged in and connected to the RAP, the web server is used to display reports and online documentation (including help files). FIPS 140-2 approved TLS mode is required since reports may contain sensitive information.

The primary components of the TOE that implement this are the LSMS Remote Navigator, the LSMS software package, and the FA.

The LVF logical boundary includes the FA (FA Hardware, Inferno Operating System, and Firewall Application), the LSMS Software Package and LSMS Remote Navigator. The logical scope of the LVF extends to the six 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 v7.2 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 v7.2 is intended to be used.
- Any known or assumed threats to the assets against which specific protection within the LVF v7.2 or its environment is required.
- Any organizational security statements or rules with which the LVF v7.2 must comply.

Lucent recommends the following minimal system configurations for the LSMS host:

Hardware (windows operating systems):

- 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 resolutions (65,535 colors)

Software:

- Windows 2000 Professional and Service Pack 2 or higher, Windows 2000 Server and Service Pack 2 or higher, Windows XP Professional and Service Pack 1, or Windows Server 2003
- Adobe Acrobat Reader version 4.5,
- Netscape Navigator 4.7 or Internet Explorer 5.5
- Java Run Time Environment (Included in TOE installation CD)
- Relational Database (Included in TOE installation CD)

Hardware (Solaris operating system):

- A Sun Ultra Sparc 5 (330 Mhz processor)
- 500 MB free disk space
- 50 MB of free space in root partition
- 512 MB of RAM
- Swap space at least as large as the amount of RAM

- CD-ROM drive
- 3.5 inch floppy drive
- Ethernet Card

Software:

- Solaris 2.9
- Netscape Navigator 4.7
- Adobe 4.0
- Java Run Time Environment (Included in TOE installation CD)
- Relational Database (Included in TOE installation CD)

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 v7.2 is intended to be used.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance.

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

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

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

A.REMACC The authorized administrators will provide all the necessary security features installed and properly configured all LSMS Remote Navigator hosts.

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 v7.2 or by its intended environment (for example, using personnel, physical, or administrative safeguards).

The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the LSMS host or the Firewall Appliance.
- TOE users: They have knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are however assumed not to be willfully hostile to the TOE)

Both are assumed to have a moderate level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network.

3.2.1 Threats to be Addressed by the TOE

The TOE addresses all threats mentioned below.

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.MEDIAT A user on a network may attempt to access unauthorized services or connect to unauthorized hosts on another network

T.ASPOOF An unauthorized entity may carry out spoofing in which information flows through the TOE into a connected network by using a spoofed source address.

T.OLDINF Persons 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, thus allowing an attacker to escape detection.

T.SELPRO An unauthorized user may read, modify, or destroy security critical TOE configuration data stored on the TOE.

T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from 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 used for performing I & A functionality in order to use this information to launch attacks on the 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 remotely located parts of the TOE.

3.2.2 Threats to be addressed by the Operating Environment

The TOE Operating Environment addresses all threats mentioned below.

TE.AUDACC Persons may not be accountable for the actions that they conduct in the TOE Environment, thus allowing an attacker to escape detection due to lack of reliable timestamps or by tampering the TSF data stored in the TOE Environment.

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

3.3 Organizational Security Policies

There are no organizational Security Policies specified.

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

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

O.DEFALT Upon initial start-up of the TOE service, the TOE must not compromise its resources or those of any connected network.

O.DOMSEP 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 Firewall Appliance and for authorized administrator use of TOE 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.

O.CRYPTO The TOE should ensure the confidentiality and integrity of the communications between different components of the TOE separated physically by a network.

O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

4.2 Security Objectives for the Environment

The following are the non-IT security objectives, which, in addition to assumptions mentioned in section 3.1, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software.

OE.PHYSEC The TOE components that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.

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

OE.GENPUR The TOE operating environment that hosts the TOE software only stores and executes security-relevant applications and only stores data required for its secure operation.

OE.PUBLIC The TOE does not host public data.

OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance.

OE.SINGEN Information can not flow among the internal and external networks unless it passes through the Firewall Appliance.

OE.DIRECT The components of the TOE and the associated direct-attached console are available to authorized administrators only.

OE.GUIDAN Those responsible for the TOE must ensure that the TOE is delivered, installed, administered, operated in a manner that maintains security and the TOE Environment is setup in a secure way such that it supports the TSF.

OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of sound security policies and practices for both the TOE and required TOE Environment components. They do not tamper the TOE Environment image, configuration files and log files from the file system of the operating system on which the TOE resides. Administrators review the environment audit logs to ensure security.

OE.TMSTMP The TOE operating environment shall be able to generate reliable timestamps for the TOE's use.

OE.REMACC The TOE operating environment shall provide all the necessary security features installed and properly configured by authorized administrators on the LSMS Remote Navigator host to protect the LSMS Remote Navigator and host operating system from attacks aimed at compromising the LSMS Remote Navigator.

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, I&A.
- 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. The TOE shall satisfy the SFRs stated in the table below which lists the CC names of the SFR components. Following the table, the individual functional requirements are restated with any necessary operations completed.

The SFRs for the TOE are taken from the CC Version 2.1, August 1999 Part 2 including interpretations as of October 06, 2003.

Functional Component ID	Functional Component Name
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3(1)	Selectable audit review (1)
FAU_SAR.3(2)	Selectable audit review (2)

FAU_STG.4	Prevention of audit data loss
FCS_COP.1 (1)	Cryptographic Operation (1)
FCS_COP.1 (2)	Cryptographic Operation (2)
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	User identification
FMT_MOF.1	Management of security functions behavior
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMR.1	Security roles
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation

Table 2 : Security Functional Requirements

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 *not specified* level of audit **specified in** Table 3; and

c) [(**None)**] **(International Interpretation 202).**

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

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

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

Functional Component	**Level**	**Auditable**	**Additional Audit Record Contents**
FMT_SMR.1	Not Specified	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_UAU.1	Not Specified	Any use of the authentication mechanism	The user identities provided to the TOE
FDP_IFF.1	Not Specified	All decisions on requests for information flow	The presumed addresses of the source and destination subject
FMT_MOF.1	Not Specified	Use of the functions listed in this requirement pertaining to audit	The identity of the authorized administrator performing the operation
FCS_COP.1 (1-2)	Not Specified	Success and failure of operation	Type of cryptographic operation performed
FIA_AFL.1	Admin Events Log	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration	The identity of the administrator attempt to make the authentication attempts and the authorized administrator who unlocks the user account.

Table 3: Auditable Events

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 including real time audit 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_SAR.3 (1)	Selectable audit review
FAU_SAR.3.1 (1)	The TSF shall provide the ability to perform *searches* 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 (2)	Selectable audit review
FAU_SAR.3.1 (2)	The TSF shall provide the ability to perform *sorting* of audit data based on a) [the chronological order of audit event occurrence.]
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.
FCS_CKM.1	Cryptographic key generation
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [pseudo-random

number generation] and specified cryptographic key sizes [56-168 bits] that meet the following: [FIPS 140-2].

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization of all cryptographic keys within the FA, LSMS and LSMS Remote Navigator] that meets the following: [FIPS 140-2].

FCS_COP.1 (1) Cryptographic Operation

FCS_COP.1.1 (1) The TSF shall perform [encryption] in accordance with a specific cryptographic algorithm [3DES] and the key size [168 bits] that meet the following [FIPS 46-3] **using a FIPS 140-2 compliant module**.

FCS_COP.1 (2) Cryptographic Operation

FCS_COP.1.1 (2) The TSF shall perform [message hashing] in accordance with a specific cryptographic algorithm [SHA-1] and the key size [160 bits] that meet the following [FIPS 180-1] **using a FIPS 140-2 compliant module**.

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_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:

[SUBJECT attributes:

1) presumed address;

2) {no other subject attributes}.

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) time of day;

7) {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.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall provide the following [none].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow **of administrative traffic** based on the following rules: [Network Address Translation (NAT)].
Application Note: *Some policies that allow only administrative traffic to flow to the LSMS host must be Network Address Translation (NAT) enabled for remote FA session logging and remote administration capability to function properly. The modifications are done through the LSMS Navigator/CLI to these administrative policies to enable NAT. These policies are then loaded by the FA protecting the LSMS application and then applied. NAT helps redirect administrative traffic from the external public IP of the LSMS application to its internally protected private IP.*

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:
a) [if there is no rule in the policy ruleset which explicitly allows the information flow ;
b) if any of the attributes identified in FDP_IFF.1.1 do not match].

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

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1	The TSF shall detect when [Administrator configured number (0 – 25)] unsuccessful authentication attempts occur related to [an authentication attempt by an administrator].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lock the administrator account].
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.}]
FIA_UAU.1	Timing of authentication
FIA_UAU.1.1	The TSF shall allow [identification as stated in FIA_UID.1] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UID.1	User identification before any action
FIA_UID.1.1	The TSF shall allow [Presentation of the LSMS Navigator Login window, Presentation of LSMS Log Viewer window, Presentation of LSMS Remote Navigator Window, Start Services, Stop Services, Restart Services, Utilities menu access] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
FMT_MOF.1	Management of security functions behavior
FMT_MOF.1.1	The TSF shall restrict the ability to ***perform*** the functions

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

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

c) review the audit trail

d) backup of user attribute values, information flow security policy rules

e) unlock locked administrators

f) Add, Remove, Reboot FAs

g) {no other services}] to an authorized administrator.

FMT_MSA.2	Secure security attributes
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for 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_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 from interference and tampering by untrusted subjects.

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

5.1.2 TOE Security Assurance Requirements

The table below identifies the security assurance requirements for the TOE drawn from CC Part 3: Security Assurance Requirements, EAL4. Necessary SARs have been modified to include National and International Interpretations till October 06, 2003.

Assurance Component ID	Assurance Component Name
ACM_AUT.1	CM Automation
ACM_CAP.4	Configuration Items
ACM_SCP.2	CM Scope
ADO_DEL.2	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Informal functional specification
ADV_HLD.2	Descriptive high-level design
ADV_IMP.1	Implementation Representation
ADV_LLD.1	Low Level Design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Security Policy Modeling
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Development Security
ALC_LCD.1	Life Cycle Definition
ALC_TAT.1	Tools and Techniques
ATE_COV.2	Evidence of Coverage
ATE_DPT.1	Evidence of Depth
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing

AVA_MSU.2	Misuse
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Developer vulnerability analysis

Table 4: Security Assurance Requirements for EAL4

5.2 Security Requirements for the IT Environment

This section presents the SFRs for the IT Environment. The IT Environment shall satisfy the SFRs stated in the table below which lists the CC names of the SFR components. These requirements do not levy any additional requirements on the TOE itself, but rather on the TOE Environment.

The SFRs for the TOE Environment are taken from the CC Version 2.1, August 1999 Part 2 including interpretations as of October 06, 2003.

Functional Component ID	Functional Component Name
FMT_MTD.1	Management of TSF Data
FPT_STM.1	Reliable Time Stamps
FAU_STG.1	Protected Audit Trail Storage

Table 5: Security Requirements for IT Environment

FMT_MTD.1. Management of TSF data

FMT_MTD.1.1 The **IT Environment hosting the TOE** shall restrict the ability to *delete, clear, view and modify* the [All TSF data on the residing operating system] to [an authorized administrator].

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The **IT Environment hosting the TOE** shall provide reliable time stamps for **the TOE's** use.

FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The **IT Environment hosting the TOE** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The **IT Environment hosting the TOE** shall be able to *detect* modifications to the audit records.

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 the security functions performed by the TOE.

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 Navigator or LSMS Remote Navigator can perform security management functions to include creating and editing security policy, creating administrator accounts, backing up FA and user these data, modifying and setting thresholds for auditable events. The LVF TOE configuration assumes only authorized administrators will have access to LVF environment containing the LSMS.

Before an authorized administrator is identified, the TSF shall allow the presentation of the LSMS Navigator Login window, presentation of LSMS Logviewer window, presentation of LSMS Remote Navigator Window, Start Services, Stop Services, Restart Services, and Utilities menu access on behalf of the administrator to be performed before he/she is identified and authenticated.

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.

Chapter 2 of the Lucent Security Management Server v7.2 Administration Guide provides information on securely accessing the LSMS. The administrative guidance provides information on accessing the LSMS using the LSMS Navigator and LSMS Remote Navigator.

The LSMS:

a) generates Group 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 FA Subsystem. The dependency mask is a tool that allows an Administrator to set up a dependency between a particular rule in a brick zone ruleset and a specific session in the session cache. This means that even if a packet matches the rule, and the rule is a pass rule, that packet will still not be permitted to pass through the brick until the brick verifies that a certain session, identified in the dependency mask, already exists in the session cache.

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 policy information

j) allows unlocking of locked user accounts by authorized administrators

k) allows addition, removal and rebooting of FAs

l) database backup, which by default runs every day at 2:00 A.M

m) The LSMS uses the administrator account to create new accounts and uses user associated account information to make authentication decisions that are based upon the userID and password provided to it. If the administrator makes a configurable number of unsuccessful authentication attempts then the user account is locked until it is unlocked by another authorized administrator.
The LSMS allows policy rules to be set to allow information flow through the FA. By default the 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 Firewall Appliance permits the security policies to be loaded into the FA from the LSMS. The administration applications of the LSMS also provide system status information.

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

6.1.2 Identification and Authentication

During the creation of LSMS and Group administrator accounts the attributes of the user is collected by the LSMS. The assumed secure configuration is physically and logically isolated and only authorized administrators will have physical access to the LSMS host. The LSMS software will be the only software on the server in addition to the resident operating system software. The FA has no user (including administrator) accounts.

The first LSMS Administrator login is created automatically during the software installation process. This administrator can then create other administrator accounts (LSMS and Group).

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

- Lucent Security Management Server menu items from the file menu
- LSMS command line interface
- LSMS log files

- Other LSMS Configuration files from the lmf 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 or LSMS Remote Navigator screen from the windows start menu folder or through the LSMS command line interface. The LSMS administrator uses user associated account information to make authentication decisions that are based upon the userID and password provided to it. If the administrator makes a configurable number of unsuccessful authentication attempts then the user account is locked until it is unlocked by another authorized administrator.

The only actions that the administrator can perform on the LSMS before authentication is accessing the LSMS Navigator Login window, LSMS Logviewer window, LSMS Remote Navigator Window, Start Services, Stop Services, Restart Services and the Utilities menu. The LSMS Navigator then establishes a connection with the LSMS application and displays a login screen to the user.

The administrator provides his userID and password within the LSMS Navigator or LSMS Remote Navigator login window. A Java based GUI is installed on 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 (Java Virtual Environment) 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, logging, and group management.

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

- 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_UAU.1, FIA_AFL.1 and FIA_UID.1

6.1.3 Secure Communications

The LSMS can be configured to manage one to many FAs across an exposed network such as the internet. The LSMS communications with the FA involve security relevant information such as configurations settings and policy settings as well user's authentication information. The LSMS and the FA communicate through a protected communication channel. All policy and configuration information from the LSMS to the FA are sent through a communication channel that provides confidentially and integrity. Similarly, an administrator sitting on a remote machine can make security relevant policy changes to a remote FA via an LSMS using the LSMS Remote Navigator. All communications between the LSMS Remote Navigator and the LSMS are sent through a communication channel that is secure and confidential.

All communications between the LSMS and the FA are done using a Lucent developed protocol that is similar to Secure Socket Layer (SSL) v3.0. When the LSMS is first installed, a root certificate is created which includes a public/private DSA key pair. A certificate is also created for the LSMS itself which is signed using the root public/private key pair. When an FA is created, yet another certificate is created, also signed with the root public/private key pair. All of these certificates include a common set of Diffie-Hellman parameters (alpha, p, etc).

When the LSMS and FA want to talk to each other(securely), they exchange the public parts of their certificates and verify that the owner of the certificate is what they expect and that the certificate is signed using the same public/ private key pair (i.e., they were both created on the same LSMS). There is also a Diffie-Hellman key exchange performed at this time. The shared secret resulting from that process is used as the triple-DES key as well as the input to the SHA digest algorithm.

Each new session from the LSMS to the FA uses Diffie-Hellman for key agreement between the LSMS and FA. The LSMS and FA use a 3DES implementation, which is FIPS 46-3 validated, for the encryption of the messages between each other. The SHA-1 hashing, which is FIPS 180-1 validated, is used for a message integrity check. All messages are and the resulting hash is encrypted to be sent across the exposed network. Initially the LSMS Remote Navigator and the LSMS will exchange keys to set up a 3DES tunnel (3DES for confidentiality and SHA-1 for integrity). Once the tunnel is in place, the LSMS will authenticate the administrator ID and password. If the ID and password are indeed valid, another 3 DES tunnel is enabled to maintain maximum security throughout the session.

The keys that are used for encryption and hashing are based on parts of the key negotiated during Diffie-Hellman key agreement. A FIPS 140-2

approved Pseudo Random Number Generator (PRNG) is used to generate keys that are used during the cryptographic communication process. The usage of the PRNG ensures that non-trivial keys are generated. All keys that are stored are destroyed by overwriting the old keys with new keys. All ephemeral keys are destroyed when cryptographic modules of the TOE reboot. All key destruction mechanisms used are FIPS 140-2 validated/compliant.

A simple Web server is used to deliver reports and help files. This Web server when configured for HTTPS uses a TLS connection between the LSMS Navigator/LSMS Remote Navigator and the Web server. Once an administrator is logged in and connected to the RAP subsystem, the Web server is used to display reports and online documentation (including help files). Web server is required to use FIPS 140-2 approved TLS mode of operation since reports may contain sensitive information. When HTTPS is used, Reports and Help files are retrieved via an established TLS connection. A web browser (Netscape or IE) is used to display reports.

Functional Requirements Satisfied: FCS_COP.1 (1) FCS_COP.1 (2), FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2

6.1.3.1 Secure Communications: *FIPS 140-2 Approved Cryptographic Support*

All the cryptographic operations within the TOE are performed by one of two FIPS 140-2 validated/compliant[4] cryptographic modules. These modules have been tested by the FIPS 140-2 validation program, which has confirmed that the FIPS-approved algorithms (3DES & SHA-1) have been implemented correctly and that the modules enforce FIPS-approved key management techniques. Confidence in the cryptographic mechanism discussed is gained from the FIPS 140-2 certificates that have been awarded to the **Lucent "VPN Firewall Brick" Models and an additional validated cryptographic module.**

The VPN Brick Models themselves (listed below) are FIPS approved cryptographic modules.

The VPN Brick Models are :

- Lucent VPN Firewall Brick Model 350[5] **(FIPS Certificate # 460 and # 461)**
- Lucent VPN Firewall Brick Model 1000[6] **(FIPS Certificate # 460 and #461)**

[4] See discussion of vendor assertion and rationale for FIPS conformance claims below in this section.
[5] Note: The marketed product naming for the product has changed overtime; however, the Lucent VPN Firewall Brick is the same product as the Lucent Firewall Appliance
[6] ibid

- Lucent VPN Firewall Brick Model 1100[7] **(FIPS Certificate #461)**

Two of the VPN Firewall Brick Models that are part of the evaluated configuration of the TOE are not FIPS validated, however, the Model 300 and Model 500 run identical software as the three FIPS validated models; Model 350, 1000 and 1100 respectively.

The VPN Firewall Brick Models vary in hardware configurations as shown in the Table 1: Firewall Appliance Hardware (i.e. memory size, number of Ethernet ports). The software image that implements the security enforcing functionality is the same on all VPN Firewall Brick Models. Hence all the VPN Firewall Brick models are considered identical. They are identical because one can take any software binary image (tvpc or tvpc.z file) from any VPN Firewall Brick and run it on any other VPN Firewall Brick. This can be verified simply by doing a "make floppy" operation for each VPN Firewall Brick and then comparing the image files on the floppy for each VPN Firewall Brick.

The same software binary image ("tvpc.Z") runs on all modules, so all features are available on all module platforms. The binary images are identical across all platforms, regardless of the VPN Firewall Brick's model number or configuration setup.

However, since the OS image provides a superset of all drivers that can interface with the module, each module only needs to use a subset of the drivers installed. When the administrator creates the floppy bootable OS image from the Lucent Security Management Server, one of the selectable options (via a drop down box) in the LSMS application is to reference the specific driver configurations of the VPN Firewall Brick model. This selection of the VPN Firewall Brick model specifies which subset of drivers is needed and places this configuration data within a separate configuration file ("inferno.ini"), which is created alongside the OS image. The purpose of the configuration file is to distinguish which drivers are applicable to the module it is installed on, while the binary image file ("tvpc.z") serves as the same identical executable applicable to all VPN Firewall Brick models. Thus, it is vendor asserted that during the operation of the VPN Firewall Brick Models the same FIPS certified cryptographic algorithms and logic is being used by all the VPN Firewall Brick Models that are a part of this evaluation. Therefore, for the VPN Firewall Brick models that have not been through the FIPS validation process are hereby compliant to the FIPS standards based on vendor assertion. The compliant VPN Firewall Brick Models are listed below:

- Lucent VPN Firewall Brick Model 300

[7] ibid

- Lucent VPN Firewall Brick Model 500

The VPN Firewall Brick Models uses the FIPS validated/compliant cryptographic module to establish an encrypted socket connection between the LSMS application and itself during transmission of audit data and during reception of policies from the LSMS application. The encrypted socket uses **SHA-1 (FIPS algorithm certificate #65 and #225)** for message (or packet) integrity checking and **3DES (FIPS algorithm certificate #75 and #245)** to encrypt the message/package/packet for confidentiality. When connections are established all the key material is generated by the FIPS 140-2 validated module following FIPS-evaluated techniques. Likewise, when the connection is terminated the key material is destroyed by the FIPS 140-2 validated module using FIPS-evaluated techniques.

The LSMS software package and the LSMS Remote Navigator both include the FIPS 140-2 validated cryptographic module**.** The LSMS software package and the LSMS Remote Navigator use this module for all cryptographic functionality required to negotiate and maintain the encrypted socket connections between:

- The LSMS Navigator/LSMS Remote Navigator/LSMS CLI/LSMS Log Viewer and the LSMS host.
- The FIPS enabled TLS connection between the LSMS Web server and a web browser (located in the TOE environment)
- The LSMS host and the FA during policy push to an FA and during reception of log data from a FA.

The encrypted socket uses **SHA-1 (FIPS algorithm certificate #138)** for message (or packet) integrity checking and **3DES (FIPS algorithm certificate #148)** to encrypt the message/package/packet for confidentiality. When connections are established all the key material is generated by the FIPS 140-2 validated module following FIPS-evaluated techniques. Likewise, when the connection is terminated the key material is destroyed by the FIPS 140-2 validated module using FIPS-evaluated techniques.

The Lucent VPN Firewall Brick Models have received **FIPS 140-2 certificate #460 and #461** and the additional validated cryptographic module has received a FIPS 140-2 certificate**.** The certificates and the Non-Proprietary Security Policies are available on the Cryptographic module Validation Program website:

http://csrc.nist.gov/cryptval/140-1/1401val.htm.

6.1.4 User Data Protection

The security policy rulesets are created by authorized administrators using the LSMS Navigator or LSMS Remote Navigator or Command Line Interface. The LSMS Navigator and the LSMS Remote Navigator is the GUI component of the LSMS software package, and the CLI is a window for issuing typed commands from the keyboard. The Lucent Security Management Server (LSMS) is the means by which administrators manage the security of one or more FAs. The policy rulesets are then pushed from the LSMS to the operating system (Inferno) on the FA.

The FA controls the flow of incoming and outgoing IP packets. The FA extracts information from the IP packet header and applies rules from a security policy. The default is **DROP**, which means the FA will discard the packet and not allow it through unless an authorized administrator explicitly configured the FA 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 FA will take when it encounters a packet that matches all the information in the above four fields. The default is "DROP", which means the FA will discard the packet and not allow it through. To allow a packet matching the above four fields through the FA, 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 FA 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.

Functional Requirements Satisfied: FDP_IFC.1, FDP_IFF.1, and FDP_RIP.1

6.1.5 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. LSMS can be accessed through LSMS Navigator, the LSMS Remote Navigator

or LSMS Command Line Interface. The LSMS Navigator is the GUI component of the LSMS which provides the human user an interface to interact with the LSMS.

The LSMS Remote Navigator host, that can be located on any interconnected network, has to access the LSMS and successfully authenticates itself to perform any security management or policy changes to the FA. The packet filtering mechanism of the FA allows only explicitly stated information flows through the FA. The security policy rules enforced by the FA are applied to every packet and no packets can bypass this packet filtering mechanism.

The LSMS is directly connected to the FA and no user information flow is allowed to the LSMS from the FA. The only communications that the LSMS receives are from the FA that it monitors and the LSMS Remote Navigator hosts. The LSMS passes management information to the FA which is protecting it through a direct Ethernet crossover cable that is connected to one of the network ports of the FA. The LSMS passes the management information to the remote FA through an encrypted socket connection, which ensures the confidentiality and integrity of the data transfer by cryptographic mechanisms. Apart from this port that is used for management of the FA, two other Ethernet ports (one for external network and one for internal network) which allow information flow to pass through them. The LSMS host runs only processes that are needed for its proper execution and does not run any other user processes. The FA does not contain a hard drive 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,

6.1.6 Audit

The FA detects the occurrence of selected events, gathers information concerning them, and sends that information to the LSMS. 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 v7.2 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;
    - start-up and shutdown of the above mentioned functions.

The User Authentication Log contains log messages that record successful or unsuccessful authentication requests LVF 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., FA zone ruleset was loaded), FA events (e.g., FA was lost) and error messages 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.

The log files are separated into four different directories on the resident operating system which is part of the TOE Environment: sessions, admin events, user authentication, and proactive monitoring.

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

b) One for "admin events": The Administrative Events Log contains log messages about administrative events (e.g., FA zone ruleset was loaded), FA events (e.g., FA was lost) and error messages 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 LVF 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 FAs and LSMS

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 FA if any of the log directories reach the maximum allotted size. When the contents of the log directory reach the configured maximum size, disk space has to be reclaimed by an administrator of the residing operating system by clearing the log files to create space to allow traffic through the FA.

This capability can be separately configured for each of the logs (admin, sessions, user authentication and promon).

6.1.6.1 Audit Generation

The FA 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 FA 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 FA, and logs operational information from all LSMS Subsystems (including FA 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 (TOE Environment) to generate timestamps for audit records.

The auditable events mentioned in Table 6 are audited in the above mentioned logs (sessions, admin events, user authentication, and proactive monitoring).

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.
FIA_UAU.1	User Authentication. Log	Any use of the authentication mechanism provided by LSMS	The user identities provided to the TOE
FDP_IFF.1	Sessions Log	All decisions on requests for information flow	The presumed addresses of the source and destination subject
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
FCS_COP.1 (1) FCS_COP.1 (2)	Not Specified	Success and failure of operation	Type of cryptographic operation performed
FIA_AFL.1	Admin Events Log	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration	The identity of the administrator attempt to make the authentication attempts and the authorized administrator who unlocks the user account.

Table 6: Auditable Events Logged

Functional Requirements Satisfied: FAU_GEN.1, FAU_STG.4

6.1.6.2 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., FA up/down status and logged on users, etc). It also enables Administrators to monitor the configuration of and access to the FA 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 FA 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.

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

6.2 TOE Assurance Measures

The LVF was developed with the following security assurance measures in place, which constitutes a Common Criteria EAL 4 level of assurance.

- Configuration Management
- Delivery and Operation
- Development

- Life Cycle
- 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 4. In this case the specification of assurance measures is done by referencing the appropriate documentation.

CC Assurance Requirements	LVF Assurance Measures
ACM_AUT.1	Lucent Security Management Server Version 7.2, Configuration Management Guide
ACM_CAP.4	Lucent Security Management Server Version 7.2, Configuration Management Guide
ACM_SCP.2	Lucent Security Management Server Version 7.2, Configuration Management Guide
ADO_DEL.2	Lucent Security Management Server Version 7.2, Secure Delivery Procedures
ADO_IGS.1	Lucent Security Management Server Version 7.2, Installation Guide Lucent Security Management Server Version 7.2, Administrator Guide
ADV_FSP.2	Lucent VPN Firewall, Version 7.2, Functional Specification
ADV_HLD.2	Lucent VPN Firewall, Version 7.2, High Level Design
ADV_IMP.1	Lucent VPN Firewall, Version 7.2, Source Code Files (LVF source. zip)
ADV_LLD.1	Lucent VPN Firewall, Version 7.2, Low Level Design
ADV_RCR.1	Lucent VPN Firewall, Version 7.2, Correspondence Analysis
AGD_ADM.1	Lucent Security Management Server, Version 7.2 , Administration Guide, Lucent Security Management Server, Version 7.2, Reports, Alarms and Logs Lucent Security Management Server,

	Version 7.2, Tools and Trouble Shooting Guide
AGD_USR.1	There are no "Users" for the Lucent product, only different levels of administrators. This requirement is not applicable and therefore vacuously satisfied.
ALC_DVS.1	Lucent VPN Firewall, Version 7.2, Life Cycle Document
ALC_LCD.1	Lucent VPN Firewall, Version 7.2, Life Cycle Document
ALC_TAT.1	Lucent VPN Firewall, Version 7.2, Life Cycle Document
ATE_COV.2	Lucent VPN Firewall, Version 7.2, Testing Depth and Coverage Analysis
ATE_DPT.1	Lucent VPN Firewall, Version 7.2, Testing Depth and Coverage Analysis
ATE_FUN.1	Lucent VPN Firewall, Version 7.2 (Patch 292), Firewall Appliance Filtering Test Cases Lucent VPN Firewall, Version 7.2 (Patch 292), User Model and Authentication Test cases Lucent VPN Firewall ,Version 7.2 (Patch 292) LSMS FA-Test Results
ATE_IND.2	Lucent VPN Firewall, Version 7.2 (Patch 292)
AVA_MSU.2	Lucent Security Management Server, Version 7.2, Administrator Guide Lucent Security Management Server Version 7.2, Policy Guide
AVA_SOF.1	Lucent Security Management Server, Version 7.2, Strength of Function Analysis
AVA_VLA.2	Lucent Security Management Server, Version 7.2, Vulnerability Analysis

Table 7: TOE Security Assurance Measures

7 Protection Profile Claims

The Security Target doesn't claim conformance to any PP.

8 Rationale

8.1 Rationale for TOE Security Objectives

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

O.INSPEC 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.DEFALT 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.DOMSEP This security objective is necessary to counter the threats: T.SELPRO 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.

O.CRYPTO This security objective is necessary to counter the Threats: T.PROCOM by requiring the TOE to provide functionality that ensure confidentiality

and integrity for the communication between physically separated parts of the TOE.

O.SINUSE This security objective is necessary to counter the threat: T.REPEAT by requiring the TOE to provide functionality that ensures repeated guessing of the authentication information is prevented.

	T.NOAUTH	T.ASPOOF	T.MEDIAT	T.OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL	T.REPEAT	T.PROCOM
O.IDANDA	X								
O.INSPEC		X	X	X					
O.DEFALT	X					X			
O.DOMSEP						X			
O.AUDREC					X				
O.ACCOUN					X				
O.SECFUN	X						X		
O.CRYPTO									X
O.SINUSE								X	

Table 8: Mapping of Threats to Security Objectives

8.2 Rationale for Security Objectives for the Environment

OE.PHYSEC This objective is necessary to satisfy the assumption A.PHYSEC by ensuring that the TOE environment will be set up to provide controlled access facilities that mitigate unauthorized, physical access to the LSMS host and the Firewall.

OE.MODEXP This objective is necessary to satisfy the assumption A.MODEXP by ensuring that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is moderate.

OE.GENPUR This objective is necessary to satisfy the assumption A.GENPUR by ensuring that the only security relevant applications are stored and execute in addition to storing data for its secure operation.

OE.PUBLIC This objective is necessary to satisfy the assumption A.PUBLIC ensuring that the MS Host and the Firewall Appliance do not host public data.

OE.NOEVIL This objective is necessary to satisfy the assumption A.NOEVIL ensuring that authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

OE.SINGEN This objective is necessary to satisfy the assumption A.SINGEN ensuring that information can not flow among the internal and external networks unless it passes through the Firewall Appliance.

OE.DIRECT This objective is necessary to satisfy the assumption A.DIRECT by ensuring that only authorized administrators have access to the TOE and the associated direct attached console.

OE.GUIDAN This non-IT security objective is necessary to counter the threat: TE.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, operated in a secure manner and the TOE Environment is setup so that it supports the TSF by following the corresponding guidance documentation.

OE.ADMTRA This non-IT security objective is necessary to counter the threat: TE.TUSAGE because it ensures that authorized administrators receive the proper training and follow the corresponding guidance for TOE operation and for operating required components in the TOE environment. OE.ADMTRA also counters the threat TE.AUDACC by helping ensure the audit logs are reviewed on a regular basis.

OE.TMSTMP This objective is necessary to provide reliable timestamp for the TOE for its use. The OE.TMSTMP objective assists the TOE objectives in countering the threat TE.AUDACC by providing reliable timestamps for the log records.

OE.REMACC The TOE operating environment shall provide all the necessary security features installed and properly configured by authorized administrators on the LSMS Remote Navigator host to protect the LSMS Remote Navigator and host operating system from attacks aimed at compromising the LSMS Remote Navigator.

	TE.TUSAGE	TE.AUDACC	A.PUBLIC	A.NOEVIL	A.SINGEN	A.PHYSEC	A.GENPUR	A.MODEXP	A.REMACC	A.DIRECT
OE.GUIDAN	X									
OE.ADMTRA	X	X								
OE.PUBLIC			X							
OE.NOEVIL				X						

OE.SINGEN					X					
OE.PHYSEC						X				
OE.MODEXP								X		
OE.REMACC									X	
OE.GENPUR							X			
OE.DIRECT										X
OE.TMSTMP		X								

Table 9: Mappings between Threats/Assumptions and Security Objectives for the Environment

8.3 Rationale for Threats to Objectives mapping

Assumptions and Threats	Objectives for TOE and Environment
Assumptions	
A.PUBLIC The TOE does not host public data.	OE.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.	OE.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 Firewall Appliance.	OE.SINGEN covers this assumption by ensuring that Information can not flow among the internal and external networks unless it passes through the Firewall Appliance.
A.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.	OE.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.	OE.DIRECT covers this assumption by ensuring that The TOE components are available to authorized administrators only.

Assumptions and Threats	Objectives for TOE and Environment
A.PHYSEC The TOE components that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.	OE.PHYSEC covers this assumption by ensuring that the TOE Environment will be set up to provide controlled access facilities that mitigate unauthorized, physical access to the TOE.
A.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.	OE.MODEXP covers this assumption by ensuring that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is moderate.
A.REMACC The authorized administrators will properly install and configure necessary security features on all the LSMS Remote Navigator hosts.	OE.REMACC covers this assumption by ensuring the TOE operating environment shall provide all the necessary security features installed and properly configured by authorized administrators on the LSMS Remote Navigator host to protect the LSMS Remote Navigator and host operating system from attacks aimed at compromising the LSMS Remote Navigator.
Threats	
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.	O.IDANDA covers this threat by ***making*** sure that before any access is granted to the TSF functions or any services inside the protected network successful authentication is performed. O.DEFALT 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 from being recorded by taking actions to exhaust	O.SECFUN covers this threat by ensuring authorized users posses the functionality to use the TOE security functions and further

Assumptions and Threats	Objectives for TOE and Environment
storage capacity, thus masking an attackers actions.	by ensuring that such functionality is available to only authorized administrators.
T.ASPOOF An unauthorized entity may carry out spoofing in which information flows through the TOE into a connected network by using a spoofed source address.	O.INSPEC covers this threat by ensuring that the Firewall Appliance mediates the flow of all information between users on an internal network connected to the FA and users on an external network connected to the FA. The traffic flows includes traffic within a tunnel and inter TOE component secure communications.
T.MEDIAT An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.	O.INSPEC covers this threat by ensuring that Firewall Appliance mediates the flow of all information from users on a connected network to users on another connected network. The traffic flows include traffic within a tunnel and inter TOE component secure communications.
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.	O.INSPEC covers this threat by ensuring that the Firewall Appliance will never allow residual information of a previous information flow to be transmitted in subsequent information flows through the Firewall Appliance. The traffic flows include traffic within a tunnel and inter TOE component secure communications.
T.AUDACC Persons may not be accountable for the actions that they conduct , 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.DEFALT covers this threat by ensuring that upon initial start-up of the TOE service, the TOE must not compromise its resources or those of any connected network. O.DOMSEP covers this threat by ensuring that the TOE has the capability to protect

Assumptions and Threats	Objectives for TOE and Environment
	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 guessing of authentication data from a connected network.
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 remotely located parts of the TOE.	This threat has been mapped to the objective O.CRYPTO which states the TOE should ensure the confidentiality and integrity of the communications between different components of the TOE separated physically by a network. The cryptography implemented for O.CRYPTO will make it infeasible for an attacker to view, modify or delete security relevant information in transit from physically separated parts of the TOE.
TE.AUDACC Persons may not be accountable for the actions that they conduct in the TOE Environment, thus allowing an attacker to escape detection due to lack of reliable timestamps or by tampering the TSF data stored in the TOE Environment.	OE.TMSTMP covers this threat by ensuring that the TOE is provided with a reliable timestamp for its use. OE.ADMTRA covers this threat by ensuring that the operating system administrators do not tamper with the audit logs that are stored on the file system of the underlying operating system and they review the environment audit logs to ensure security.
TE.TUSAGE The TOE may be used and administered in an insecure manner	OE.ADMTRA covers this threat by ensuring that the operating system administrators are trained as to establishment and maintenance of sound security policies and practices for both the TOE and required TOE Environment components. This would include the setup, secure physical access practices, and access control configuration practices for the TOE environment items like the host operating systems and the Lucent IPSec Client personal firewall. Administrators are trained to follow secure

Assumptions and Threats	Objectives for TOE and Environment
	practices and OE.GUIDAN covers this threat by ensuring that the TOE is delivered, installed, administered, operated in a manner that maintains security and the TOE Environment is setup so that it supports the TSF..

Table 10 : Threats to Objectives Mapping

8.4 TOE Security Requirements Rationale

The rationale for the chosen level of SOF-basic is based on the moderate 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.IDANDA and O.SINUSE.

FIA_AFL.1 Authentication Failure Handling

This component exists to minimize guessing the authentication information of authentic users by brute force method. A user account is locked until further actions are taken by an authorized administrator when a predefined number of consecutive unsuccessful login attempts are reached. This component traces back to and aids in meeting the following objectives: O.IDANDA, O.ACCOUN and O.SINUSE.

FIA_UID.1 User identification

This component ensures that before anything other than those mentioned in the requirement 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.IDANDA 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. This component traces back to and aids in meeting the following objectives: O.IDANDA and O.SINUSE.

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.INSPEC.

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.INSPEC.

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.INSPEC.

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.DOMSEP.

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.DOMSEP.

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.

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. Further it ensures that if the space allocated for all audit records exceeds, the FA will halt all traffic

through itself with the exception of Administrator traffic. This halting to a secure state to protect the internal network ensures that the TOE's primary security function, to protect the network is never compromised. 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. Once the audit trail is restored to a non full status the FA will no longer halt traffic and resume its regular operation. The maximum number of audit records that could be lost is 656 (assuming that the average message size is 100 bytes and the queue is 65,536 bytes (64K)). This component traces back to and aids in meeting the following objectives: O.ACCOUN 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.DEFALT

FMT_MSA.2 Secure Security Attributes

This component was chosen to provide secure and non-trivial security attributes during the cryptographic operations performed by the TOE. This component ensures that the keys used for the cryptographic operations are secure and are non-trivial. This component traces back to and aids in meeting the following objectives: O.CRYPTO.

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.INSPEC, O.DEFALT, and O.SECFUN.

FCS_CKM.1 Cryptographic Key Generation

This component was chosen to provide secure communications between the LSMS application and the FAs. This component ensures that the keys used for the cryptographic operations are generated using a FIPS 140-2 approved method. This component traces back to and aids in meeting the following objectives: O.CRYPTO.

FCS_CKM.4 Cryptographic Key Destruction

This component was chosen to provide secure communications between the LSMS application and the FAs. This component ensures that the keys used for the cryptographic operations are destroyed using a FIPS 140-2 approved method. This component traces back to and aids in meeting the following objectives: O.CRYPTO.

FCS_COP.1 (1),
FCS_COP.1 (2) Cryptographic Operation

These components were chosen to provide secure communications between the LSMS application, FAs, Web server and the GUI (LSMS Navigator, LSMS Remote Navigator). This component traces back to and aids in meeting the following objective: O.CRYPTO.

	O.IDANDA	O.INSPEC	O.DEFALT	O.DOMSEP	O.AUDREC	O.ACCOUN	O.SECFUN	O.SINUSE	O.CRYPTO
FMT_SMR.1							X		
FIA_ATD.1	X							X	
FIA_AFL.1	X					X		X	
FIA_UID.1	X					X			
FIA_UAU.1	X							X	
FDP_IFC.1		X							
FDP_IFF.1		X							
FMT_MSA.2									X
FMT_MSA.3		X	X				X		
FDP_RIP.1		X							
FPT_RVM.1				X					
FPT_SEP.1				X					
FAU_GEN.1					X	X			
FAU_SAR.1					X				
FAU_SAR.3(1)					X				
FAU_SAR.3(2)					X				
FAU_STG.4						X	X		
FMT_MOF.1			X				X		
FCS_COP.1 (1)									X
FCS_COP.1 (2)									X
FCS_CKM.1									X
FCS_CKM.4									X

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

8.5 Rationale for IT Security Requirements for the Environment

FMT_MTD.1 Management of TSF data

This component ensures that only authorized administrators of resident operating system apart from TOE administrators will be able to access the LSMS application, resident operating system clock and TSF data. This component also ensures that the TOE configuration files, policy files, log files and other TSF data that resides on the file system of the underlying operating system is protected from tampering. This component traces back to and aids in meeting the following objectives: OE.ADMTRA and OE.TMSTMP.

FPT_STM.1 Reliable Time Stamps

This component ensures that the operating system provides reliable time stamps that can be used by the TOE. This component traces back to and aids in meeting the following objectives: OE.TMSTMP.

FAU_STG.1 Protected Audit Trail Storage

This component ensures that the operating system provides reliable storage of Audit data that is generated by the TOE. Any modifications to the audit trail are detected. This component traces back to and aids in meeting the following objectives: OE.ADMTRA

	OE.ADMTRA	OE.TMSTMP
FMT_MTD.1	X	X
FPT_STM.1		X
FAU_STG.1	X	

Table 12: Mappings between IT Security Functions and Security Objectives of the Environment

8.6 Rationale for Security Objectives to Security Requirements mapping

Security Objective		IT Security Requirement
O.IDANDA	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 maintains the identity and association of the human user/user name with the authorized administrator role. FIA_AFL.1 satisfies this objective by minimizing a brute force attack to guess the authentication information. FIA_UID.1 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.INSPEC	The Firewall Appliance must mediate the flow of all information between users on an internal network connected to the FA and users on an external network connected to the FA, 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 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.

Security Objective		IT Security Requirement
		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.DEFALT	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.DOMSEP	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
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.	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) and FAU_SAR.3 (2) satisfies this requirement by providing the TSF to peruse the audit data by convenient

Security Objective		IT Security Requirement
		searching and sorting 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 Firewall Appliance and for authorized administrator use of TOE security functions.	FIA_UID.1 satisfies the objective by ensuring that each user is identified before performing any TSF-mediated actions on behalf of the user other than those mentioned in the requirement. FIA_AFL.1 satisfies this objective by minimizing a brute force attack to guess the authentication information and logging each and every unsuccessful authentication attempt. 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. FAU_STG.4 satisfies this objective by ensuring that the audit data trail is safe and if full, the information flow through the TOE is stopped until an authorized administration takes action.
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.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

Security Objective		IT Security Requirement
		authorized administrators only.
O.CRYPTO	The TOE should ensure the confidentiality and integrity of the communications between different components of the TOE separated physically by a network.	FCS_COP.1 (1) and FCS_COP.1 (2) satisfies this objective by specifying the encryption and hashing functionality required for the confidentiality and integrity checking. Further, the cryptography for encryption and integrity checking is performed in a FIPS 140-2 validated/compliant cryptographic module. FCS_CKM.1 and FCS_CKM.4 satisfies this objective by specifying that the keys used for cryptographic operations are generated and destructed in a FIPS 140-2 approved way. FMT_MSA.2 satisfies this objective by the usage of a FIPS 140-2 approved Pseudo Random Number Generator (PRNG) to generate keys that are used during the cryptographic communication process. The usage of the PRNG ensures that non-trivial keys are generated
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.	FIA_AFL.1 satisfies this objective by minimizing a brute force attack to guess the authentication information and logging each and every unsuccessful authentication FIA_ATD.1 satisfies this objective by ensuring that the TOE maintains the identity and association of the human user/user name with the authorized administrator role. 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

Table 13 : Security Objectives - SFRs Mapping

8.7 TOE Summary Specification Rationale

Mapping of Security Functions to Security Functional Requirements

TOE Security Functions	Security Functional Requirements	Rationale
TOE Security Management	**FMT_MOF.1** **FMT_MSA.3** **FMT_SMR.1** **FIA_ATD.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.(*FMT_MOF.1*) The TOE uses the System Administrator accounts to create other accounts. (*FIA_ATD.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_AFL.1** **FIA_UID.1**	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 locks an administrator if a predefined number of consecutive unsuccessful login attempts are made before a successful login attempt. *(FIA_AFL.1)* The TOE uses the System Administrator accounts to uses the associated account information to make authentication decisions that are based upon the userID and password provided to it. (*FIA_UID.1)*

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 FA 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 application and its resident operating system. *(FPT_RVM.1)* All packets should pass through the Firewall Appliance and the FA has no user accounts or passwords. This implementation provides the required TSF domain separation.*(FPT_SEP.1)*
Security Audit	**FAU_GEN.1** **FAU_SAR.1** **FAU_SAR.3 (1)** **FAU_SAR.3 (2)** **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)* 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 FA deployed. *(FAU_SAR.1 and FAU_SAR.3)* The audit storage management architecture ensures that incase the Audit data storage exhaustion takes place, the Firewall appliance stops passing traffic. An authorized administrator configures the LSMS APPLICATION in such a way not to loose any audit data and halt the FA if any of the log directories reach the maximum allocated size. When log directories size reaches the configured limit, disk space needs to be reclaimed by an administrator of the resident operating system, by clearing the log directories to create space and allow

		traffic through the FA. This mechanism ensures that audit records are not lost if audit trail is full. *(FAU_STG.4)*
Secure Communications	**FCS_COP.1 (1)** **FCS_COP.1 (2)** **FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	The TOE provides a means for its components (LSMS application, FA, Web server and GUI (LSMS Navigator, LSMS Remote Navigator) separated by a physical network to communicate through an encrypted socket connection which provides confidentiality and integrity to the flow of information through the channel. (FCS_COP.1 (1), FCS_COP .1 (2)) The TOE generates cryptographic keys that are used for communications between the LSMS Remote Navigator, LSMS application and the FA, in a FIPS 140-2 approved way. (FCS_CKM.1) The TOE destroys cryptographic keys that are used for communications between the LSMS Remote Navigator, LSMS application and the FA in a FIPS 140-2 approved way. (FCS_CKM.4) The TOE uses secure and non-trivial security attributes while performing the various cryptographic operations i.e. the TSF shall ensure that only secure values are accepted for security attributes (FMT_MSA.2).

Table 14: Mappings Between TOE Security Functions to Security Functional Requirements

8.8 Rationale for Assurance Requirements

EAL4 was chosen to provide a moderate to high level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment. EAL4 was chosen to provide a moderate to high level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. Additionally, the product vendor has specific customer requests for the evaluation of the TOE at this assurance level. These potential customers of the product vendor have determined for their own networks that an EAL4 evaluation of the product will provide satisfactory assurance.

Configuration Management Documents – The Configuration Management documentation provides the description of the Configuration Management (CM) System and the CM plan of the LVF. It should describe how the CM system provides automated means to support the generation of the TOE and how the automated tools are used in the CM system. A description of tools used to control the configuration items and how they are used at Lucent should be there. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Partial CM Automation
- Capabilities - Generation Support and Acceptance Procedures
- Scope – Problem Tracking CM Coverage

Secure Delivery and Operation Documents – The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Lucent to protect against TOE modification during product delivery. The Installation Documentation provided by Lucent details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

Development Documents – The LVF design documentation consist of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design

identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.

- The Low-Level Design describes each security supporting module in terns of its purpose and interaction with other modules. It describes the TSF in terms of modules, designating each module as either security-enforcing or security-supporting. It provides an algorithmic description for each security-enforcing module detailed enough to represent the TSF implementation.
- The Implementation Representation unambiguously defines the TSF to a level of detail such that the TSF can be generated without further design decisions. It also describes the relationships between all portions of the implementation.
- The Security Policy Model provides an informal TSP model and it demonstrates correspondence between the functional specification and the TSP model by showing that all of the security functions in the functional specification are consistent and complete with respect to the TSP model. The TSP model describes the rules and characteristics of all policies of the TSP that can be modeled. The model should include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Functional Specification with Complete Summary
- Security-enforcing High-Level Design
- Security-enforcing Low-Level Design
- Implementation of the TSF
- Informal TOE Security Policy Model
- Informal Correspondence Demonstration

Guidance Documents – The Guidance documentation provides administrator guidance on how to securely operate the TOE. The administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. Lucent provides a set of administrator guidance documents which address the administrator guidance requirements. The product does not provide a "user" or non-administrator role. The user guidance assurance requirements are not applicable and therefore vacuously satisfied..

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance - Not applicable

Life Cycle Support Documents – The Life Cycle Support documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. It provides evidence that these security measures are followed during the development and maintenance of the TOE. It provides evidence that these security measures are followed during the development and maintenance of the TOE. The flaw remediation procedures addressed to the TOE developers are provided and so are the established procedures for accepting and acting upon all reports of security flaws and requests for corrections of those flaws. The flaw remediation guidance addressed to TOE users is provided. The description also contains the procedures used by the Lucent to track all reported security flaws in each release of the LVF. The established life-cycle model to be used in the development and maintenance of the LVF is documented and explanation on why the model is used is also documented. The selected implementation-dependent options of the development tools are described.

Corresponding CC Assurance Components:

- Identification of Security Measures
- Flaw Reporting Procedures
- Developer defined life-cycle model
- Well-defined development tools and techniques.

Testing Documents – There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. The depth analysis demonstrates that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design. LVF Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided. The Independent Testing documentation provides an equivalent set of resources to those that were used in the developer's functional testing.

Corresponding CC Assurance Components:

- Analysis of Coverage

- Low–level Design
- Functional Testing
- Independent Testing

8.9 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 Security Target.

Functional Component FMT_MOF.1 depends on functional component FMT_SMF.1 Specification of Management Functions. All the management functions that could be specified in the FMT_SMF.1 are specified in the functional requirement FMT_MOF.1. Further FMT_MOF.1 provides more information on restricting these management functions. Restricting the functions implicitly requires that they be provided which is what the intension of FMT_SMF.1 is and hence FMT_SMF.1 is not included in the security Target.

Functional Component FMT_MTD.1 depends on functional component FMT_SMF.1.Since FMT_MTD.1 is an Environment SFR its dependency FMT_SMF.1 needn't be met.

Functional Component FMT_MTD,1 depends on functional component FMT_SMR.1 on the IT Environment.. Since FMT_MTD.1 is an IT Environment SFT its dependency on FMT_SMR.1 on the IT Environment needn't be met.

8.10 Strength of Function Claims Rationale

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL 4 assurance requirements. The rationale for the chosen level is based on the moderate attack potential of the threat agents identified in this ST. The list of relevant security functions and security functional requirements which have probabilistic or permutational functions are:

FIA_UAU.1 - Timing of authentication
FIA_AFL.1 - Authentication Failure Handling

The password used by the administrator login is the only probabilistic or permutational function on which the strength of the authentication mechanism depends.

Authorized administrators of the TOE choose their own passwords numbers when initially authorized to use the system; the system places the following restrictions on the passwords selected by the user:

- The password must be at least six characters long;
- No Dictionary words are allowed.

A proof that the TOE meets its SOF-Claims can be found in "Lucent VPN Firewall v7.2 Strength of Function Claims" document,

8.10 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 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 as shown in Table 14. All SFR dependencies have been satisfied with the exception of those noted in above Sections.

c) The SARs are appropriate for the assurance level of EAL4 and are satisfied by LVF v7.2. EAL4 was chosen to provide a moderate to high level of independently assured security in the absence of ready availability of the complete development record from the vendor.