

Security Target, v1.3, for the Lucent Managed Firewall (LMF), v3.0

December 22, 1998

Prepared For:

Lucent Technologies
Bell Labs Innovations



Lucent Technologies
480 Red Hill road
Room 2B241
Middletown, NJ 07748

Prepared by:



Computer Sciences Corporation
7471 Candlewood Road
Hanover, MD 21076

Table of Contents

1 INTRODUCTION TO THE SECURITY TARGET (ST)..... 1

1.1 ST OVERVIEW 1

1.2 ST AND TOE IDENTIFICATION..... 2

1.3 OVERVIEW OF THE LUCENT MANAGED FIREWALL..... 2

1.4 CC CONFORMANCE CLAIM 3

2 DESCRIPTION OF THE LUCENT MANAGED FIREWALL 4

2.1 APPLICATION CONTEXT 4

2.2 EVALUATION APPLICATION CONTEXT 5

2.3 PRODUCT TYPE..... 5

2.4 LMF SCOPE AND BOUNDARIES 6

 2.4.1 *Physical Scope and Boundary*..... 6

 2.4.2 *Logical Scope and Boundary* 7

3 SECURITY ENVIRONMENT 9

3.1 ASSUMPTIONS..... 9

3.2 THREATS 10

 3.2.1 *Threats To Be Addressed by the LMF*..... 10

 3.2.2 *Threats To Be Addressed by the LMF Environment* 11

3.3 ORGANIZATIONAL SECURITY POLICIES 11

4 SECURITY OBJECTIVES..... 12

4.1 SECURITY OBJECTIVES FOR THE LMF 12

4.2 SECURITY OBJECTIVES FOR THE LMF ENVIRONMENT 13

5 IT SECURITY REQUIREMENTS 14

5.1 LMF SECURITY FUNCTIONAL REQUIREMENTS (SFRs) 14

 5.1.1 *Access Control* 15

 5.1.2 *Audit* 18

 5.1.3 *Identification and Authentication* 20

 5.1.4 *Security Management* 21

 5.1.5 *Protection of Security Functions* 22

5.2 TOE SECURITY ASSURANCE REQUIREMENTS..... 23

5.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 23

6 LMF TOE SUMMARY SPECIFICATION..... 24

6.1 DESCRIPTION OF LMF SECURITY FUNCTIONS 24

 6.1.1 *Security Management [LMF_SMAN]*..... 24

 6.1.2 *Identification and Authentication [LMF_INA]*..... 26

 6.1.3 *Access Control [LMF_ACCESS]*..... 27

 6.1.4 *Audit [LMF_AUDIT]*..... 29

 6.1.5 *Protection of Security Functions [LMF_PSF]*..... 32

6.2 SFR CORRESPONDENCE 33

6.3 ASSURANCE MEASURES 34

 6.3.1 *Configuration Management* 34

 6.3.2 *Delivery and Operation* 34

 6.3.3 *Architecture*..... 34

 6.3.4 *Guidance*..... 34

 6.3.5 *Test*..... 35

 6.3.6 *Vulnerability Assessment* 35

7 PROTECTION PROFILE (PP) CLAIMS..... 36

7.1 PP REFERENCE 36

8	ANNEX A RATIONALE	37
8.1	RATIONALE FOR IT SECURITY OBJECTIVES.....	37
8.2	RATIONALE FOR NON-IT SECURITY OBJECTIVES	38
8.3	RATIONALE FOR FUNCTIONAL REQUIREMENTS	39
8.4	RATIONALE FOR ASSURANCE REQUIREMENTS	43
8.5	RATIONALE FOR NOT SATISFYING ALL DEPENDENCIES.....	43
8.6	TOE SUMMARY SPECIFICATION RATIONALE.....	43

Table of Tables

TABLE 1:	LMF ELEMENTS AND THEIR HARDWARE/SOFTWARE COMPONENTS.....	6
TABLE 2:	SFR COMPONENTS.....	14
TABLE 3:	AUDITABLE EVENTS	18
TABLE 4:	EAL2 ASSURANCE COMPONENTS	23
TABLE 5:	ADMINISTRATOR ACCOUNT INFORMATION.....	26
TABLE 6:	CORRESPONDENCE OF SFRs TO SECURITY FUNCTIONS	33
TABLE 7:	MAPPINGS BETWEEN THREATS AND IT SECURITY OBJECTIVES	38
TABLE 8:	MAPPING BETWEEN ASSUMPTIONS AND NON-IT SECURITY OBJECTIVES	39
TABLE 9:	MAPPING OF SECURITY FUNCTIONAL REQUIREMENTS TO IT SECURITY OBJECTIVES	42

1 INTRODUCTION TO THE SECURITY TARGET (ST)

1 This introductory section presents ST identification information and an overview of the identified TOE as well as of the ST structure. A brief discussion of the methodology employed to develop this ST is also included.

1.1 ST Overview

2 A *security target (ST)* is a document that provides the basis for the evaluation of a specific *target of evaluation (TOE)* (that is, an information technology [IT] product or system).¹ An ST principally defines:

- ◆ A security problem (in Section 3, Security Environment)
- ◆ A set of security objectives and a set of security requirements to address that problem (in Sections 4 and 5, Security Objectives and IT Security Requirements, respectively)
- ◆ The IT security functions provided by the TOE that meet that set of requirements (in Section 6, LMF Summary Specification)

3 A concluding Annex presents "Rationale," which provides evidence of traceability among aspects of the security environment, the security objectives, the security requirements, and the security functions.

4 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,"² this ST minimizes the use of terms of art from the *Common Criteria for Information Technology Security Evaluation (CC)*.

5 The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex C, and in Part 3, Chapter 5.

¹ In this ST, *italicized text* is used for document titles, to highlight key terms, and to give emphasis.

² *Common Criteria for Information Technology Security Evaluation (CC)*, Part 1, C.1, par. 2.

1.2 ST and TOE Identification

- 6 This section provides information needed to identify and control this ST and its TOE, the Lucent Managed Firewall, Version 3.0. This ST targets an evaluation Assurance Level (EAL) 2 level of assurance.

ST Title: Security Target, v1.3, for the Lucent Managed Firewall (LMF), v3.0, December 22, 1998.

TOE Identification: Lucent Managed Firewall, v3.0 (Build 150).

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998.

PP Identification: None.

ST Evaluation: U.S. Government Department of Defense.

Keywords: information flow control, firewall, packet filter, network security, traffic filter, security target

1.3 Overview of the Lucent Managed Firewall

- 7 This section presents a general overview of the Lucent Managed Firewall (LMF). Not all security functions described are included in the evaluation. The secure configuration for this evaluation is described in Section 2.2.

- 8 The Lucent Managed Firewall architecture consists of two physically distinct components:

- ◆ The Firewall Appliance, which controls the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces.
- ◆ The Security Management Server (SMS) software, by means of which administrators manage the security of one or more Firewall Appliances.

- 9 The firewall code runs on Inferno™, a small Bell Labs-developed operating system. The separate Security Management Server software, implemented as Inferno daemons and Java applets, runs on Hosted Inferno and Netscape Enterprise Server, v3.0, respectively; the latter runs either on Windows NT™ or Sun Solaris™ operating systems.

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

- 11 Policy rules are defined by authorized administrators using the SMS. The SMS also supports the management of the other LMF security features, notably, of audit (for example, event selection, reports, and routing of selected audit event information to console, email, syslog, or beeper) and of administrator accounts.
- 12 The administrative interface to the SMS is via a Netscape Communicator browser; the interface is implemented by Java applets. In the evaluated configuration, the browser runs on the same platform as the SMS.
- 13 All communications between a Firewall Appliance and the SMS are encrypted and authenticated using native Inferno™ encryption and authentication mechanisms, such as Diffie Hellman for key exchange, ElGamal for digital signatures and signature verification, and DES for session encryption.

1.4 CC Conformance Claim

- 14 The TOE conforms to parts 2 and 3 of the Common Criteria. This is described as follows:
 - a) ***Part 2 conformant*** – the security functional requirements are based on those identified in Part 2 of the Common Criteria, and
 - b) ***Part 3 conformant*** – the security assurance requirements are in the form of an EAL or assurance package that is based upon assurance components in Part 3 of the Common Criteria.

2 DESCRIPTION OF THE LUCENT MANAGED FIREWALL

15 This section provides context for the LMF evaluation, by identifying the product type of the LMF and by describing in general terms the physical and logical scope and boundaries of the LMF.

2.1 Application Context

16 When, as in this case, the product to be evaluated is one "whose primary function is security, this section may be used to describe the wider application context into which such a TOE will fit."³

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

- ◆ A Firewall Appliance can be placed at the perimeter of an enterprise's intranet to protect it from the Internet.
- ◆ Building upon the previous configuration, one can add a "demilitarized zone" (DMZ), in which to place the enterprise's publicly available Web servers, for example.
- ◆ Multiple Firewall Appliances can be placed to control several security zones within the enterprise intranet.
- ◆ An ISP can manage multiple Firewall Appliances with a single SMS and, using the LMF security zone feature, can allow different customers to control their own security policies.

³ CC, Part 1, C.2.3, par.2.

2.2 Evaluation Application Context

- 18 This section identifies the evaluated configuration. For the TOE to be ST compliant, the TOE configuration must conform to the following specifications:
- ◆ The secure configuration of the LMF must be configured in accordance with the directives contained in the *Lucent Managed Firewall Delivery, Installation, Generation, and Start-up Procedures*.
 - ◆ The configured SMS must be physically isolated from user networks.
 - ◆ The configured LMF must be physically protected as a single collocated entity.
 - ◆ The LMF must be configured to have only an SMS and one FA.
 - ◆ The configured LMF must be isolated from communication (e.g., through rules enforced by the FA) with any other connected network.
 - ◆ The configured LMF must be used only for the administration of Firewall Appliances. (The SMS must not use the Netscape Server to host web pages or provide word processing applications, etc.)

2.3 Product Type

- 19 This section identifies the LMF's product type.
- 20 The LMF is a traffic-filter firewall. A traffic-filter firewall controls the flow of individual IP datagrams by matching information contained in IP and higher layer headers against a set of rules specified by the firewall's administrator. This header information includes source and destination host (IP) addresses, source and destination port numbers, and upper level protocol identifier (for TCP or UDP, for example). 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.

2.4 LMF Scope and Boundaries

21 This section provides a general description of the physical and logical scope and boundaries of the LMF.

2.4.1 Physical Scope and Boundary

22 As stated in Section 1.3 above, the Lucent Managed Firewall architecture consists of two physically distinct components:

- ◆ The Firewall Appliance, which controls the flow of IP datagrams between network interfaces.
- ◆ The Security Management Server (SMS) software, by means of which administrators manage the security of multiple Firewall Appliances.

23 The evaluated LMF configuration consists of one SMS and one Firewall Appliance. At minimum, the LMF physical boundary includes just these two components. The secure configuration for evaluation is described in the *Lucent Managed Firewall Installation, Start-up and Configuration* document.

24 The physical scope of the LMF includes the hardware and software components identified in Table 1.

Table 1: LMF Elements and Their Hardware/Software Components

LMF Element	Hardware/Software Components
	Intel x86 processor 4MB flash disk four 10/100BaseT Ethernet interface cards high-speed IPSEC encryption card RS-232 port for failover floppy disk
	Inferno™ operating system
Security Management Server	200 MHz Pentium-pro processor 96 MB system memory 2GB hard disk CD-ROM drive Ethernet interface card backup device (e.g., tape or zip drive)
	Microsoft Windows NT Workstation 4.0 with Service Pack 3.0 Netscape Enterprise Server 3.0 Netscape Communicator 4.03

25 The LMF has 11 major subsystems. For an account of them, see the *LMF Functional Specification and High-Level Design Document*.

2.4.2 Logical Scope and Boundary

- 26 The security functional requirements implemented by the LMF are usefully grouped under the following classes or families:
- ◆ *Access Control*:⁴ the Firewall Appliance controls the flow of incoming and outgoing IP datagrams.
 - ◆ *Audit*: the Firewall Appliance detects the occurrence of selected events, gathers information concerning them, and sends that information to the Security Management Server (SMS), where it is stored. The SMS also detects the occurrence of selected events (e.g., security administrator actions), gathers information concerning them, and records it. Audit reporting features are also provided by the SMS, to include reporting features such as the routing of selected audit event information to console, email, syslog, or beeper, as selected by an authorized administrator.
 - ◆ *Identification and Authentication (I&A)*: the Firewall Appliance has no user (including administrator) accounts. The SMS requires administrators to identify and authenticate themselves before they can perform any other SMS actions.
 - ◆ *Security Management*: the SMS provides all LMF security management capabilities. By means of it, administrators manage the security policy rules enforced by associated Firewall Appliances, audit mechanism configuration parameters, and administrator accounts.
 - ◆ *Protection of Security Functions*: the Firewall Appliance security functions, which implement the LMF access control policy⁵, are physically separated from the unauthenticated external IT entities that send and receive IP datagrams through the Appliance; and the design of these functions is such that they cannot be bypassed by those external IT entities.
- 27 The LMF logical boundary includes the Firewall Appliance(s) and the SMS. The evaluated secure configuration must contain the same physical and logical isolation. The logical scope of the LMF extends to the five classes or families of security functional requirements mentioned above.

⁴ Books on firewalls typically identify "access control" as a firewall's central security mechanism. The *Common Criteria* (CC) distinguishes "access control" from "information flow control"; Here, the term "access control" is used in the broader sense known to the firewall community, in order to facilitate the understanding of firewall developers, marketers, and others unfamiliar with the *Common Criteria's* terms of art.

⁵ More precisely, they implement the information flow control policy named "UNAUTHENTICATED SFP" (Security Function Policy).

28 The LMF also provides the following capabilities, but they fall outside the scope of this evaluation:

- ◆ Remapping source and destination host addresses to other internal addresses, using Network Address Translation (NAT).
- ◆ Protecting the confidentiality and integrity of an enterprise's messages by means of Virtual Private Networks (VPNs) between the enterprise's Firewall Appliances, using IP Security Protocol (IPSEC) encryption and cryptographic checksums.
- ◆ Dividing administrative responsibilities between the LMF system administrator role and one or more LMF zone administrators, each of which manages the security of a subset of the Firewall Appliances associated with an SMS.
- ◆ Remote administration of the LMF is another capability that falls outside the scope of this evaluation. The LMF does not itself provide the capability for authorized administrators to remotely administer the SMS. Users who wish to remotely administer the SMS are advised to obtain a digital ID from Verisign in order to establish Secure Sockets Layer (SSL) sessions between the Netscape Enterprise Server and the Netscape Communicator browser on the remote platform.

3 SECURITY ENVIRONMENT

- 29 This section aims to clarify the nature of the security problem that the Lucent Managed Firewall is intended to solve, by describing the following:
- ◆ Any *assumptions* about the security aspects of the environment and/or of the manner in which the LMF is intended to be used
 - ◆ Any known or assumed *threats* to the assets against which specific protection within the LMF or its environment is required
 - ◆ Any *organizational security policy* statements or rules with which the LMF must comply
- 30 The TOE is intended to be used in environments where either, at most, sensitive but unclassified information is processed or the sensitivity level of information in both the internal and external networks is equivalent.

3.1 Assumptions

- 31 The following conditions are assumed to exist in the operational environment.
- A.GUIDAN The LMF is delivered, installed, administered, and operated in a manner that maintains security.
 - A.ADMTRA Authorized administrators are trained in the establishment and maintenance of sound security policies and practices.
 - A.PHYSEC The LMF is physically secure.
 - A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
 - A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the LMF.
 - A.PUBLIC The LMF does not host public data.
 - A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
 - A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.
 - A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., console port) if the connection is part of the TOE.
 - A.NOREM The LMF is administered by an unauthorized administrator through a dedicated administration network connection.

32 It is assumed that the secure configuration for evaluation will be the basic network configuration as described in Section 3 of the *LMF System Administrator Reference Manual*, Version 3.0. The protected network is connected to one interface, the isolated SMS network to a second, and the external network (via a router) to a third. The evaluated secure configuration must contain the same physical and logical isolation.

3.2 Threats

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

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

3.2.1 Threats To Be Addressed by the LMF

35 The threats discussed below are addressed by the LMF. The threat agents are either human users or external IT entities not authorized to use the LMF. The assets that are subject to attack are the IT resources residing on the LMF.

- T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use the security functions and/or non-security functions provided by the TOE.
- T.ASPOOF An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
- T.MEDIAT An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
- T.OLDINF Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
- T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
- T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.

3.2.2 Threats To Be Addressed by the LMF Environment

36 There are not threats identified for the LMF Environment.

3.3 Organizational Security Policies

37 No organizational security policies are specified.

4 SECURITY OBJECTIVES

38 "The security objectives are a concise statement of the intended response to the security problem."⁶ These objectives indicate, at a high level, how the security problem, as characterized in the "Security Environment" section of the ST, is to be addressed.

39 Just as some threats are to be addressed by the LMF and others by its intended environment, so some security objectives are for the LMF and others are for its environment. These two classes of security objectives are discussed separately.

4.1 Security Objectives for the LMF

40 The following are those IT security objectives for the LMF:

- O.IDAUTH The LMF must uniquely identify and authenticate the claimed identity of all users, before granting a user access to LMF functions.
- O.MEDIAT The LMF must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.
- O.SECSTA Upon initial start-up of the LMF or recovery from an interruption in LMF service, the LMF must not compromise its resources or those of any connected network.
- O.SELPRO The LMF must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with LMF security functions.
- O.AUDREC The LMF 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 LMF must provide user accountability for information flows through the LMF and for authorized administrator use of security functions related to audit.
- O.SECFUN The LMF must provide functionality that enables an authorized administrator to use the LMF security functions, and must ensure that only authorized administrators are able to access such functionality.

⁶ CC, Part 3, par. 5.4.

4.2 Security Objectives for the LMF Environment

- 41 The following are the non-IT security objectives that are to be satisfied without imposing technical requirements on the LMF. That is, they will not require the implementation of functions in the LMF hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.
- O.GUIDAN The LMF must be delivered, installed, administered, and operated in a manner that maintains security.
 - O.ADMTRA Authorized administrators must be trained in the establishment and maintenance of sound security policies and practices.
 - O.PHYSEC The LMF must be physically secure.
 - O.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities must be considered low.
 - O.GENPUR There must be no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the LMF.
 - O.PUBLIC The LMF must not host public data.
 - O.NOEVIL Authorized administrators must be non-hostile and must follow all administrator guidance.
 - O.SINGEN Information must not flow among the internal and external networks unless it passes through the TOE.
 - O.NOREM The LMF must be administered by an unauthorized administrator through a dedicated administration network connection.

5 IT SECURITY REQUIREMENTS

42 As seen above, security objectives provide a general, highly abstract answer to the question of how the security problem is to be addressed. IT security requirements are a refinement of the objectives and provide a more specific, less abstract answer to that same question.

43 IT security requirements include:

- ◆ Security functional requirements (SFRs), that is, requirements for such security functions as access control, audit, identification, and authentication.
- ◆ Security assurance requirements, which give grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, vulnerability assessment).
- ◆ Security requirements for the TOE's IT environment (that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends).

44 This section presents the security functional and assurance requirements for the Lucent Managed Firewall along with a discussion of the TOE's IT environment.

5.1 LMF Security Functional Requirements (SFRs)

45 The LMF shall satisfy the SFRs identified in Table 2. For the reader's convenience, the components are grouped by well-known security requirement type (i.e., what is variously called security service, security mechanism, class or family of security requirement, etc.). The types are named in the shaded rows (beginning with "Access Control").

Table 2: SFR Components.

Functional Components for the TOE	
<i>Access Control [User Data Protection / Information Flow Control]</i>	
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FMT_MSA.3	Static attribute initialization
FDP_RIP.2	Full residual information protection
<i>Audit</i>	
FAU_GEN.1	Audit data generation
FPT_STM.1	Reliable time stamps
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
<i>Identification and Authentication (I&A)</i>	
FIA_UID.2	User identification before any action
FIA_UAU.1	Timing of authentication

Functional Components for the TOE	
FIA_ATD.1	User attribute definition
<i>Security Management</i>	
FMT_SMR.1	Security roles
FMT_MOF.1	Management of security functions behavior
<i>Protection of Security Functions</i>	
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation

46 The secure configuration for evaluation will be the basic network configuration as described in Section 3 of the *LMF System Administrator Reference Manual*, Version 3.0. The evaluated secure configuration must be physically and logically isolated. Because of the physical and logical isolation, remote administration will not be part of evaluated secure configuration functionality.

47 The overall Strength of Function rating for the LMF is *SOF-basic*.

48 This ST states specific strength of function metrics for the FIA_UAU.1, Timing of Authentication SFR. The metric specified for the FIA_UAU.1 SFR is as follows:

FIA_UAU.1: "the probability that authentication data can be guessed is no greater than one in one million"

5.1.1 Access Control

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:

- a) [subject security attributes:
 - presumed address
- b) information security attributes:
 - presumed address of source subject
 - presumed address of destination subject

- transport layer protocol
- TOE interface on which traffic arrives and departs
- Service]

FDP_IFF.1.2

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

- a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:
 - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
 - the presumed address of the source subject, in the information, translates to an internal network address;
 - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.
- b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
 - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
 - the presumed address of the source subject, in the information, translates to an external network address;
 - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

- FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:
- a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
 - b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;
 - c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;
 - d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.]

FMT_MSA.3 Static attribute initialization

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

FDP_RIP.2 Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to all objects*.

5.1.2 Audit

FAU_GEN.1 Audit data generation

- FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
- a) Start-up and shutdown of the audit functions;
 - b) All **relevant** auditable events for the *minimal or basic* level of audit **specified in Table 3**; and
 - c) [the event in Table 3 listed at the "extended" level].
- FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
- a) Date and time of the event, type of event, subjects identities, 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 Table 3: Auditable events].

Table 3: Auditable events

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

FPT_STM.1 Reliable time stamps

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

FAU_SAR.1 Audit review

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

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

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

- a) [presumed subject address;
- b) ranges of dates;
- c) ranges of times;
- d) ranges of addresses].

5.1.3 Identification and Authentication

FIA_UID.2 User identification before any action

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

FIA_UAU.1 Timing of authentication

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

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

FIA_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.]

5.1.4 Security Management

FMT_SMR.1 Security roles

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

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

FMT_MOF.1 Management of security functions behavior

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

- a) start-up and shutdown
- b) create, delete, modify, and view information flow security policy rules that permit or deny information flows
- c) create, delete, modify, and view user attribute values defined in FIA_ATD.1
- d) enable and disable single-use authentication mechanisms in FIA_UAU.4
- e) modify and set the time and date
- f) archive, create, delete, and empty the audit trail
- g) back up user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools
- h) recover to the state following the last backup
- i) apply information flow security policy rules that permit or deny information flows
- j) create, update, save, delete, and view a security zone, assign it to a Firewall Appliance interface, and load the assignment information onto the Firewall Appliance
- k) create, update, delete, and view Host Groups
- l) create, update, delete, and view Service Groups

to [the authorized administrator role].

5.1.5 Protection of Security Functions

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.

5.2 TOE Security Assurance Requirements

- 49 The Lucent Managed Firewall shall satisfy the security assurance requirements for Evaluation Assurance Level Two (EAL2), as defined in Part 3 of the CC.
- 50 This ST does not augment EAL2 with other security assurance requirements from Part 3 of the CC; nor does it extend EAL2 by explicitly stating additional security assurance requirements not taken from Part 3 of the CC.
- 51 Table 4 identifies the security assurance requirements components included in EAL2.

Table 4: EAL2 Assurance Components

Assurance Components for the TOE	
ACM_CAP. 2	Configuration items
ADO_DEL. 1	Delivery procedures
ADO_IGS. 1	Installation, generation, and start-up procedures
ADV_FSP. 1	Informal functional specification
ADV_HLD. 1	Descriptive high-level design
ADV_RCR. 1	Informal correspondence demonstration
AGD_ADM. 1	Administrator guidance
AGD_USR. 1	User guidance (The TOE does not support unprivileged users)
ATE_COV. 1	Evidence of coverage
ATE_FUN. 1	Functional testing
ATE_IND. 2	Independent testing – sample
AVA_SOF. 1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.3 Security Requirements for the IT Environment

- 52 This section specifies security requirements for the TOE's IT environment (that is, for hardware, software, or firmware that is external to the TOE and upon which satisfaction of the TOE's security objectives depends).
- 53 The Lucent Managed Firewall has no security requirements allocated to its IT environment.

6 LMF TOE SUMMARY SPECIFICATION

54 This section presents the security functions of the Lucent Managed Firewall, which are being evaluated, and the assurance measures applied to ensure their correct implementation.

6.1 Description of LMF Security Functions

55 The following subsections present the security functions that will be performed by the TOE and provide a mapping between the identified security functions and the Security Functional Requirements that the TOE must satisfy.

56 The SFRs identified in Section 5.1.1.1 above are grouped into the following security functional areas:

- ◆ Access Control⁷
- ◆ Audit
- ◆ Identification and Authentication (I&A)
- ◆ Security Management
- ◆ Protection of Security

6.1.1 Security Management [LMF_SMAN]

57 The SMS provides all LMF security management capabilities. By means of it, administrators manage the security policy rules enforced by associated FAs and audit mechanism configuration parameters and administrator accounts. Only an authorized administrator working through the SMS can perform security management functions to include creating and editing security policy; creating administrator accounts and modifying and setting thresholds for auditable events; and creating, modifying, deleting, and viewing rules regarding routing of information.

58 The secure LMF configuration assumes that only authorized administrators will have access to LMF environment containing the SMS and its resident operating system. These actions are logged by the resident operating system and include:

- ◆ Modification of the time and date on the SMS (FA does not have timestamp)
- ◆ Backup and recovery

⁷ Books on firewalls typically identify "access control" as a firewall's central security mechanism. The *Common Criteria* (CC) distinguishes "access control" from "information flow control"; Here, the term "access control" is used in the broader sense known to the firewall community, in order to facilitate the understanding of firewall developers, marketers, and others unfamiliar with the *Common Criteria's* terms of art.

59 The SMS performs the following security functions:

- ◆ Generating zone security policies on behalf of the Administrators. This responsibility includes taking the Administrator zone security policy specified rules, host groups, service groups, dependency masks, and VPN information and encoding it (policy compilation) into a file format suitable for local storage and/or downloading to a Brick Subsystem.
- ◆ Managing administrator accounts by maintaining the Certificate of Authority (CA) public key, performing system and administrator account management, and privilege preservation.
- ◆ Maintaining the Administrator account information. The SMS maintains for each System Administrator their UserID, password, domain, role, and privileges.
- ◆ Preserving the System Administrator's privilege information and provides it for enforcement.
- ◆ Enforcing System Administrator privileges. Privilege enforcement is based upon a privilege vector that is returned to it in response to a System Administrator login attempt. The privilege vector identifies the role (administrator or zone administrator) and identifies the System Administrator's access permissions representing r/w/x for {access, audit, accounts, and system}.
- ◆ Logging the System Administrator out if unrecognized data is received from the System Administrator interface or unhandled exceptions occur within SMS Subsystems.
- ◆ Receiving System Administrator edits to policy information and writes the information to policy files within the domain directory.
- ◆ Receiving System Administrator edits to account information and passes the information for incorporation into files within the admin directory for system retention.
- ◆ Receiving System Administrator edits to alarm configuration information and writes the information to action, trigger, alarmConfig files within the load directory for system retention.
- ◆ Receiving System Administrator edits to zone information and writes the information to zone files within the file system for system retention.
- ◆ Receiving System Administrator edits to firewall information and writes the information to the firewall's directory.

- 60 The Firewall Appliance (FA) permits the security policies to be loaded into the FA from the SMS over an authenticated and encrypted session. Each security policy’s digital signature is verified before the policy is loaded (the policies are digitally signed by the SMS using the firewall administrator’s certificate when created or edited). The administration applications also provide system status information.

- 61 Loading an FA loads the Zone Assignment Table on the FA. The Zone assignment Table identifies the zones that are assigned to each of the FA’s interfaces.

- 62 The Media Access Control table contains the IP addresses of all local machines. The session cache identifies all active sessions traversing an FA. The FA applies the zone security policy to the first session packet it detects and not to subsequent packets within the same session.

6.1.2 Identification and Authentication [LMF_INA]

- 63 At least one System Administrator is required to administer an installation of the SMS. A System Administrator is defined as a person who logs into the SMS as a System Administrator and has System Administrator privileges. The first System Administrator login is created automatically during the software installation process. This administrator can then create other administrator accounts. The assumed secure basic configuration is physically and logically isolated, and only authorized administrators will have physical access to the SMS server. The SMS software will be the only software on the server in addition to the benign resident operating system software. The FA has no user (including administrator) accounts. The SMS requires administrators to identify and authenticate themselves before they can perform any other SMS actions as illustrated in Table 5.

Table 5: Administrator Account Information

Field	Description
AdminID	The administrator’s login.
Full Name	The administrator’s name
Role	System or Zone Administrator
Zone	The zones this administrator will be permitted to access
Password	The password required to validate the login
Verify Password	The password entered exactly as above
Phone Number	The administrator’s office telephone number
Email Number	The administrator’s email address
Pager Info	The PIN of the administrator’s paging service
Expiration Date	The date the account expires

- 64 The System Administrator establishes communication with the SMS by launching the Netscape Communicator 4.03 browser and specifying the Universal Resource Locator (URL) for the SMS's Login Screen. The browser then establishes a HyperText Transport Protocol (HTTP) Secure Session Layer (SSL) connection with the SMS and displays the SMS Login Screen to the System Administrator. The Client/GUI Subsystem is now communicating with the Netscape Subsystem. The evaluated configuration requires that the Netscape browser is located on the same host as the SMS software.
- 65 The System Administrator provides his userID and password within the browser window. A login servlet is launched by the Netscape subsystem when the System Administrator provides his userID and password. The servlet passes this information to a Remote Access Daemon (RAD) through a file interface and abides by its access control decision. After identifying and authenticating the System Administrator, an applet is downloaded to the System Administrator's desktop to provide the Primary User Interface and to secure the communications between the applet and the administration application.
- 66 The SMS manages the System Administrator's interface. This includes interacting with the System Administrator management screens presented within the GUI JVE to provide the appropriate Java™ Applet in response to System Administrator's input. Such interactions include, based on System Administrator input, presenting the System Administrator interface the appropriate applet for management of System Administrator accounts, alarms, logging, and zone management.
- 67 The SMS uses the System Administrator account information to make authentication decisions based upon the userID and password provided to it by the Netscape Subsystem (servlet) via its file interface with the servlet.

6.1.3 Access Control [LMF_ACCESS]

- 68 The FA controls the flow of incoming and outgoing IP packets. The default is **DROP**, which means that the brick will discard the packet and not allow it through. Unless an authorized administrator explicitly configured the brick to accept requests based on specific security attributes, the LMF will successfully reject any and all requests.
- 69 The FA works with data at the IP packet level. Security rules in the security policy perform this filtering function by looking at five basic pieces of information (security attributes) in each packet to see if they match the same information in the rule.
- ◆ *The direction of the packet*
 - ◆ *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 system administrator prior to creating the rule. A host group can be used to define broadcast or loopback addresses to permit filtering.)
- ◆ *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 system administrator prior to creating the rule.)
- ◆ *The service or protocol* - Every security rule must specify an Internet service. Services are application-level protocols that are identified by their destination TCP or UDP port numbers. There are three ways to enter this information, as follows:
 - ◆ Protocol name or number
 - ◆ Protocol number/destination port
 - ◆ Protocol number/destination port/source port
 - ◆ For ICMP messages, the format is protocol/type/code.
- ◆ *The action taken by the rule* - This field defines the action that the brick will take when it encounters a packet that matches all the information in the above four fields. The default is DROP, which means that the brick will discard the packet and not allow it through. To allow a packet matching the above four fields through the brick, the field must be set to PASS.

70 The FA extracts information from the IP packet header and applies rules from a security policy. Information within an IP packet that is used to make access control decisions includes source and destination TCP or UDP port number, and packet type.

71 The LMF allows the System Administrator to set both service groups and host groups to apply the security policy to the FA device. A host group identifies a range of IP addresses and the service group identifies several UDP or TCP services. Both of these groups can be applied to policy rules that are used to enforce the security policy. To meet some of the SFRs the *Lucent Managed Firewall Delivery, Installation, Generation, and Start-up*

Procedures document describes the host groups, service groups, and rule set that must be created to install the LMF in an evaluated configuration.

- 72 Security attributes include security policy specified rules, host groups, service groups, dependency masks, and VPN information generated by the SMS on behalf of the Administrators. In addition, time-of-day, day-of-week, direction of access, physical Ethernet port, and existing session information can be used to determine whether or not a packet is allowed to pass in either direction.
- 73 The FA relies on internal pointers at the beginning and end of the packet to ensure full residual information protection.

6.1.4 Audit [LMF_AUDIT]

- 74 The FA detects the occurrence of selected events, gathers information concerning them, and sends that information to the SMS, where it is stored. The SMS 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 SMS. The reporting feature of the LMF allows Administrators to view and analyze internal and system information of the LMF. Using Report Wizards, audit event items can be extracted and presented in a legible and coherent format.
- 75 The types of audit events recorded in AdminEvents Log and the Sessions Log are contained in Appendix B of *LMF System Administrators Manual, Version 3.0* and 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
- ◆ Reaching the unsuccessful authentication attempt threshold

(Note: Due to the assumptions about the IT environment and only trusted users, i.e., administrators, accessing the system, authentication privileges are not revoked and subject to restoration.)

- 76 The audit log will record at a minimum the following information:
- ◆ Type of message (audit event)
 - ◆ Source type (b for messages originating from the brick; I for messages originating from the SMS)
 - ◆ Source (firewall name or an SMS subsystem)
 - ◆ Timestamp

◆ Subtype

77 Additional audit log fields can be defined to include source IP and results. 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’ permits specifying value for filterable fields to hone in on field criteria values. The ‘wizard’ permits selection of fields on which to sort as well as sorting direction (ascending or descending). When generating an Admin Event or Sessions Log report, the ability to search the raw log file by entering a text string is also provided. Details regarding the report Wizard capabilities can be found in the *LMF Systems Administrator Reference Manual*, Version 3.0.

6.1.4.1 Audit Generation

78 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 the following:

- Start and stop times
- Action taken
- Statistics, such as number of bytes and packets passed

79 The FA bundles this information into an audit message and sends it to an awaiting audit server, located on the SMS.

80 The SMS logs session info sent to it by FA and logs operational information from all SMS Subsystems (including FA Subsystems). The SMS reformats the log events it receives, applies a time stamp, and writes the event to the appropriate log file. The SMS uses the NT or Solaris clock on the motherboard to generate timestamps for audit records.

6.1.4.2 Reliable Time Stamps

81 The LMF preserves the sequence of events in the log files by time stamping. The FA preserves the order of the packet and sends the information to the SMS. The SMS respects the ordering of the FA and provides a timestamp using the clock setting on the resident operating system. The logs are ASCII files containing newline-delimited records, i.e., each record is a line of the file. All records have the same four fields at their beginning:

- ◆ The record type, an integer.
- ◆ Did the record come from a firewall or an SMS subsystem?
- ◆ The name of the firewall or subsystem.

- ◆ A timestamp, consisting of six decimal digits, and reading to the second. The date is not necessary, since the file is strictly rolled over at midnight. Thus records in a single file are all from the same day; that day is a property of the file, not the record.

82 Beyond the fixed first four fields, the format of the record depends on what type it is. The “type” number explicitly drives the parse. The fields themselves are delimited by colons, except for the arguments in error records. It was impossible to pick a single character that might not occur in an error record. (For example, such records could contain colons as part of a Windows filename, any character that could appear in an internet address or URL, etc.) So error arguments are delimited “out of band”, using numerical descriptors of their length.

6.1.4.3 Audit Review

83 The log files are separated into two different directories: sessions and admin events.

- ◆ “sessions” data, containing information about traffic through the brick
- ◆ “admin events”: logins and actions of administrators, errors, contacting and losing bricks, and pretty much everything else except information about brick traffic

The log file directories are stored on the resident operating system. The assumed secure basic configuration requires physical and logical separation to permitting access to only authorized administrators.

84 In each directory, the filenames are assigned in the same way. The purpose of the assignment algorithm is to ensure that a lexical sort by filename also provides a chronological sort of the data in the files. This improves performance in reading log files for reports and alarms.

85 Even at full-rated load, the seconds digits are seldom needed; logs roll over every minute at most. If either the Sessions or Admin Events log grows to the maximum size allowed, then a new log is created and subsequent network data is recorded in the new log.

86 Logs roll over:

- ◆ At midnight, so there are never records from two different days in the same log file.
- ◆ When a configurable file size is reached (default = 10MB for sessions, 1MB for events).

87 The SMS enables Administrators to monitor the configuration and traffic mediation of the firewalls deployed throughout the network. The report “wizards” are displayed to enable Administrators to filter and sort data. Through this interface, the System

Administrator has the capability to generate “Memorized Reports” (i.e., report templates) and to generate Closed Session, Session, and Administrative Events reports.

88 The SMS enables an Administrator to view critical System Administrator and system information to view:

- ◆ the identities of all logged in system users
- ◆ their session duration
- ◆ IP address of the host they logged in from
- ◆ The status of the communication link between each brick and the SMS

89 The SMS provides the LMF System with a real-time alarming capability. In a manner similar to the creation of management reports, alarms can be specified using a wizard to define an alarm. The alarm feature of the LMF allows Administrators to configure alarmable events and the action(s) taken when and if these events occur in the system.

6.1.5 Protection of Security Functions [LMF_PSF]

90 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 PSF. To further ensure that security functions on the FA cannot be tampered with or bypassed, the security functions are embedded in the Inferno™ operating system kernel. The FA has no user (including administrator) accounts. This implementation provides the required TSF domain separation. SMS security functions, implemented as Inferno daemons and Java™ applets, are protected by Hosted Inferno and by the Netscape Java™ Virtual Machine (JVM). The security policy rules enforced by the FA are applied to every packet.

91 The FA is equipped with four auto-sensing 10/100Base-T Ethernet interface cards and can be positioned between any type of Ethernet-based network elements (e.g., routers, hubs, switches, servers, PCs).

92 The FA does not contain a hard drive and can be deployed without a monitor and keyboard. Other than a floppy disk drive for initial software boot, it has few moving parts, which are an on/off switch and a power supply fan.

93 Tools used to backup and restore the configuration files are the tools provided by the native operating system (NT or Solaris). The configuration files are distributed across the file system that belongs to the server’s native operating system. The secure LMF configuration assumes only authorized administrators will have access to LMF environment containing the SMS and its resident operating system.

94 The subject separation is provided by the SMS. The SMS enforces System Administrator privileges. Privilege enforcement is based upon a privilege vector that is returned to it in response to a System Administrator login attempt. The privilege vector identifies the role

(administrator or zone administrator) and identifies the System Administrator’s access permissions representing r/w/x for {access, audit, accounts, and system}. (Note: Due to the assumptions about the IT environment and only trusted users, i.e., administrators, accessing the system, authentication privileges are not revoked and subject to restoration.) SMS logs the System Administrator out if unrecognized data is received from the System Administrator interface or unhandled exceptions occur within SMS Subsystems.

6.2 SFR Correspondence

95 Table 6 provides the required correspondence between the functional specification and the SFRs stated in the LMF Security Target.

Table 6: Correspondence of SFRs to Security Functions

	FDP_IFC.1	FDP_IFF.1	FMT_MSA.3	FDP_RIP.2	FAU_GEN.1	FPT_STM.1	FAU_SAR.1	FAU_SAR.3	FIA_UID.2	FIA_UAU.1	FIA_ATD.1	FMT_SMR.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
LMF_ACCESS	X	X	X	X											
LMF_AUDIT					X	X	X	X							
LMF_INA									X	X	X				
LMF_SMAN												X	X		
LMF_PSF														X	X

6.3 Assurance Measures

96 The LMF assurance measure compliance to the assurance requirements is described in the following subsections.

6.3.1 Configuration Management

97 The Configuration Management measures applied by Lucent include assigning a unique product identifier for each release of the TOE. Associated with this Product Identified is a list of Hardware and Software configuration items that compose a single instance of the TOE. These configuration management measures are documented within the following Lucent Documents:

- Sablime User Guide
- Sablime Administrator Guide
- Sablime User Reference Manual
- Configuration Guide for the Lucent Managed Firewall v3.0

6.3.2 Delivery and Operation

98 Lucent provides Delivery and Operation documentation that describes what components are delivered with the LMF, guidance for initially installing it, and warnings about the importance of properly unpacking, installing, and configuring the TOE. These deliver and operation measures are documented within the following Lucent documents:

- Delivery, Installation, Generation, and Start-Up Procedures (Version 8.0)
- Lucent Managed Firewall Security Management Server Version 3.0 Installation Guide

6.3.3 Architecture

99 The Lucent architecture documents satisfy the functional specification and high-level design information requirements, as well as provide a correspondence between that information and this ST. These architecture measures are documented within the following Lucent documents:

- Functional Specification for the Lucent Managed Firewall, v3.0
- High Level Design for the Lucent Managed Firewall, v3.0

6.3.4 Guidance

100 The Guidance Documents provided by Lucent include both the Installation and Configuration manuals, which guide administrators through the process of unpacking, installing, and configuring the LMF. These guidance measures are documented within the following Lucent documents:

- Configuration Guide for the Lucent Managed Firewall v3.0

- Delivery, Installation, Generation, and Start-Up Procedures (Version 8.0)
- Lucent Managed Firewall Security Management Server Version 3.0 Installation Guide
- Lucent Managed Firewall Security Management Server Version 3.0 System Administrator Reference Manual
- Lucent Managed Firewall Security Management Server Version 3.0 System Administrator Task Manual
- Lucent Managed Firewall Security Management Server Version 3.0 Zone Administrator Reference Manual
- Lucent Managed Firewall Security Management Server Version 3.0 Zone Administrator Task Manual

6.3.5 Test

- 101 Lucent performs functional testing to ensure that the LMF meets its design goals. Lucent testing documentation consists primarily of Excel Spreadsheets, which enumerate the test cases performed by testers, and record the "pass/fail/not run" status of each test case. These test cases exercise all of the Security Functions described earlier in this document.

6.3.6 Vulnerability Assessment

- 102 As part of the design and testing process, Lucent conducted Vulnerability Analysis of the LMF. The goal of this analysis was to identify any obvious weaknesses that could be exploited by an attack. In addition to the testing conducted by CSC, ISS Real Secure also conducted preliminary vulnerability analysis. The vulnerability analysis is document within the following Lucent documents:

- Lucent Managed Firewall Vulnerability Assessment, June 18, 1998, A Technical Report Prepared For Lucent Technologies By The Security Professionals At Internet Security Systems
- Lucent Managed Firewall Vulnerability Assessment, November 30, 1998.

- 103 A Strength of Function Analysis performed on Timing of Authentication. This analysis is documented in the Lucent IGS document. It indicates that the probability that authentication data can be guessed is no greater than one in one million.

7 PROTECTION PROFILE (PP) CLAIMS

104 This section provides the PP conformance claim statements.

7.1 PP Reference

105 The Lucent Managed Firewall does not conform to any protection profiles.

8 ANNEX A RATIONALE

106 This Annex presents the "Rationale" for the LMF ST. The first three subsections of the Annex provide evidence of traceability among aspects of the security environment, the security objectives, the security requirements, and the security functions.

8.1 Rationale For IT Security Objectives

- O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH, because it requires that users be uniquely identified before accessing the TOE.
- O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF, which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
- O.SECSTA This security objective ensures that no information is comprised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.
- O.SELPRO This security objective is necessary to counter the threat: 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 administrator are accountable for the use of security functions related to audit.
- O.SECFUN This security objective is necessary to counter the threat: T.NOAUTH by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

Table 7: Mappings between threats and IT security objectives

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

8.2 Rationale For Non-IT Security Objectives

- O.GUIDAN** This objective is necessary to enforce the environmental assumption A.GUIDAN, and requires that the TOE is delivered, installed, administered, and operated in a manner that maintains security.
- O.ADMTRA** This objective is necessary to enforce the environmental assumption A.ADMTRA, and requires that an authorized administrators be trained in the establishment and maintenance of sound security policies and practices.
- O.PHYSEC** This objective is necessary to enforce the environmental assumption A.PHYSEC, and requires that the TOE be physically secure.
- O.LOWEXP** This objective is necessary to enforce the environmental assumption A.LOWEXP, and requires that the TOE be installed in an environment where the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- O.GENPUR** This objective is necessary to enforce the environmental assumption A.GENPUR, and requires that there be no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- O.PUBLIC** This objective is necessary to enforce the environmental assumption A.PUBLIC, and requires that the TOE does not host public data.
- O.NOEVIL** This objective is necessary to enforce the environmental assumption A.NOEVIL, and requires that the TOE operates in an environment where the authorized administrators is non-hostile and follows all administrator guidance.
- O.SINGEN** This objective is necessary to enforce the environmental assumption A.SINGEN, and requires that information does not flow among the internal and external networks unless it passes through the TOE.

- O.NOREM This objective is necessary to enforce the environmental assumption A.NOREM, and requires that the TOE be administered by an unauthorized administrator through a dedicated administration network connection.

Table 8: Mapping between assumptions and non-IT security objectives

	A.GUIDAN	A.ADMTRA	A.PHYSEC	A.LOWEXP	A.GENPER	A.PUBLIC	A.NOEVIL	A.SINGEN	A.NOREM
O.GUIDAN	X								
O.ADMTRA		X							
O.PHYSEC			X						
O.LOWEXP				X					
O.GENPER					X				
O.PUBLIC						X			
O.NOEVIL							X		
O.SINGEN								X	
O.NOREM									X

8.3 Rationale For Functional Requirements

- 107 The TOE has a primary security function of enforcing an information flow control security policy. The FDP_IFF and FDP_IFC components state the requirements for this security policy. The remaining security functions are used to support that function and ensure that the TOE provides a set of mutually supportive security functions that form a consistent whole.
- 108 The security function of identification and authentication ensures that the configuration and management of the TOE and its security functions are restricted to the authorized administrator. This security function also provides a requirement for a strength of function analysis to be performed for the mechanism used to authenticate the administrator. This is due to this mechanism being instantiated by a quantitative mechanism and that it could be defeated by a brute force attack. The mechanism used to implement this security function ensures that the probability of determining a password during its lifetime is less than one in a million (0.000001, or 1×10^{-6}).
- 109 The auditing security function supports the security policy by requiring that all flow control decisions are captured for analysis. This security function is supported by the SFRs that require the TOE to provide tools for searching and sorting the audit records.
- 110 The TOE also provides security management functions to support the secure administration and configuration of the TOE. The TOE is required to have a restrictive default configuration to ensure that the administrator can implement a secure information flow control policy that reflects the needs of the organization.
- 111 The TOE also provides security functions that require the TOE to be self-protecting. In addition, there is requirement to ensure that the security policy cannot be bypassed. These

requirements also support the information flow control security policy enforced by the TOE.

- 112 The set of SFRs selected for this TOE includes all dependencies defined in the *Common Criteria Part 2*. The security functions selected describe a mutually supportive and consistent set of requirements.

FMT_SMR.1 Security roles

- 113 Each of the CC class FMT components in this document depend on this component. This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

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

FIA_UID.2 User identification before any action

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

FIA_UAU.1 Timing of authentication

- 116 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 objective: O.IDAUTH.

FDP_IFC.1 Subset information flow control

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

FDP_IFF.1 Simple security attributes

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

FMT_MSA.3 Static attribute initialization

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

FDP_RIP.2 Full residual information protection

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

FPT_RVM.1 Non-bypassability of the TSP

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

FPT_SEP.1 TSF domain separation

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

FPT_STM.1 Reliable time stamps

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

FAU_GEN.1 Audit data generation

124 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

125 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 Selectable audit review

126 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.

FMT_MOF.1 Management of security functions behavior

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

Table 9: Mapping of security functional requirements to IT security objectives

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

8.4 Rationale For Assurance Requirements

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

8.5 Rationale For Not Satisfying All Dependencies

129 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 document.

8.6 TOE Summary Specification Rationale

130 The Correspondence of SFRs to Security Functions is demonstrated in Table 6 maps the security functions defined by this ST and implemented by the Lucent Managed Firewall to the required SFRs. The combined correspondence and the assurance measures provided to ensure their correct implementation as described Section 6 demonstrate that the implemented LMF security functions satisfy the TOE security functional requirements.

131 The demonstration of the combination of LMF security functions is contained in Section 6 in the following formats:

132 Section 6.1 provides a functional overview of the LMF to include the description of the secure basic configuration, the relationship between the LMF components, and the required physical and logical isolation of the configuration.

133 Section 6.2 identifies the LMF security functions and how the IT security functions will be realized by the LMF security mechanisms (subsystems). The security functions are categorized under six functional security areas. The LMF security functions are described in terms of these six security areas.

134 Section 6.3 presents the six LMF security functions corresponding to the SFRs identified in this ST.

135 Section 6.4.7 identifies the SOF for SFR SOF requirements named in Section 5.1.1.1.

136 Section 6.4 presents the LMF assurance measure compliance.