

Lucent Security Management Server Security, VPN, and QoS Management Solution



Lucent Security Management Server (LSMS) software brings you the most advanced carrier-grade IP services management solution at today's lowest ownership costs. Teaming with Lucent's award-winning VPN Firewall Brick™ family, LSMS lets you rapidly provision and manage high-return services for thousands of users in a single console. It integrates firewall, VPN, QoS, VLAN and virtual firewall policy management; provides industry-leading scalability and availability; delivers robust monitoring, logs and reports; and gives you flexible deployment options—all without the costly additional modules or recurring license fees that competitive products require.

Applications

- Advanced security services
- Site-to-site and remote access VPN services
- Bandwidth management (QoS) services
- Secure data center web/application hosting
- Mobile data services

Features

- Fully integrates firewall, VPN, QoS, VLAN, and virtual firewall management
- Comprehensive remote management capabilities with role-based administration
- Flexible management model: controls policies at global, customer, device, interface, VLAN and IP address range levels
- Unmatched scalability: supports 1,000 VPN Firewall Bricks™, and 10,000 Lucent IPSec Client users from one LSMS console
- Carrier-grade reliability: distributable across multiple network operations centers (NOCs) for active/active network redundancy with no single point of failure
- Real-time monitoring, robust logging, and customized reporting
- Multiple IP services deployment options: premises-based, network-based, tiered, and data-center architectures

Benefits

- **One-and-done management solution**—single platform provides centralized, comprehensive management of all IP services
- **Low operating costs**—totally secure remote management eliminates need for network reconfigurations, truck-rolls, on-site support; VLAN, virtual firewall, and QoS support included at no extra charge; management efficiencies cut staffing and administrative expenses
- **Simple, economical licensing model**—no ongoing license fees or add-ons required for complete security management
- **Cost-saving growth**—easily migrate from basic to advanced security, VPN, and QoS services
- **Assured business continuity**—native high availability, carrier-grade reliability, no advisories or reported vulnerabilities
- **Proven carrier-class performance**—mature product with over 5 years of service in the world's largest networks



LSMS Technical Specifications

1. Mode of Operation

Centralizes firewall, virtual firewall, VLAN, VPN and QoS policy management
Proactively monitors all VPN Firewall Bricks™ and IPSec Client users
Provides real-time monitoring, log collection, reporting and alarm generation
Supports network-based and premises-based deployments

2. Performance and Capacity

Supports 1,000 customer groups each with hundreds of unique policies
Manages 1,000 VPN Firewall Bricks™ and 10,000 IPSec Client users
Centrally collects up to 15,000 log records per second
Supports 100 simultaneous administrators

3. Policy Management

Uses a group-based model to manage a collection of devices, security policies, VPN tunnels, and user authentication components as a single entity
Controls policies at the global, customer, device, interface, VLAN and IP address range level
Includes preconfigured typical security and VPN policy templates that can be tailored to suit unique requirements
Uses user-definable Host Groups, Service Groups, Application Filters and User Groups
Supports global and nested policy objects

4. Role-based Administration

Uses two administrative classes:
LSMS Administrators – full privileges over all groups, devices, policies and users
Group Administrators – restricted privileges and access only to assigned group(s)
Supports shared administration with customers
Local and remote administration via LSMS Remote Navigator utility (included); provides secure access to all LSMS utilities
Allows concurrent administrators to exchange messages via a real-time messenger service

5. Secure 3-Tier Architecture

LSMS to VPN Firewall Brick™ communications secured with Diffie-Helman and 3DES encryption, SHA-1 authentication and integrity, and digital certificates for VPN Firewall Brick™ to LSMS authentication
LSMS Remote Navigator to LSMS communications secured with 3DES encryption and SHA-1 authentication and integrity, and either local password or external database authentication with SecurID or RADIUS servers
Transfers logs in real-time over reliable and secured connections

6. Authentication

Built-in internal database – 10,000 users
Browser-based authentication allows authentication of any user protocol
Local passwords, RADIUS, SecurID, X.509 digital certificates with Entrust CA PKI
PKI Certificate requests (PKCS 12)
Automatic LDAP certificate retrieval
User assignable RADIUS attributes

7. Remote Access VPN Tunnel Management

Fully integrates remote access VPN support, including Lucent IPSec Client software distribution and updates
Centralizes management of all IPSec Client configurations, including personal firewall settings
Allows any combination of authentication methods; configurable per user, user group or application
Supports virtual addresses for tunnel end points
Allows administrator to terminate specific tunnels when necessary, or terminate all tunnels in a single action

8. Site-to-Site VPN Tunnel Management

Provides SLA probes for real-time round trip delay statistics and tunnel status indicators to verify tunnel availability in real-time; configurable with alarm notifications
Supports virtual addresses for tunnel end points
Configurable tunnel default settings
Includes preconfigured VPN policy templates
Fully integrated with firewall policy

9. High Availability/Redundancy

Supports active/active management with geographically distributed servers and real-time database replication
Internal database automatically backs up to a local and remote disk daily; additional backups can be scheduled at any time
Backup file contains ALL policy, configuration, and security information for ALL configured devices and policies

10. Central Staging with Secure Upgrades

Securely pushes the VPN Firewall Brick™ operating system to each device with no truck-rolls or on-site hardware support; maintains ALL sessions during an OS upgrade with a failover pair of VPN Firewall Bricks™

11. Application Programming Interfaces (APIs)

Scriptable command line interface
Parsable ASCII log files (for per-customer reporting)
Supports SNMP GET v2c (read-only) and SNMP traps v1 and v2c

12. Audit Log Management

Four categories of audit logs created daily:
Firewall Session Logs
Administrative Event Logs
User Authentication Logs
Proactive Monitoring Statistic Logs
Real time logs viewable with Log Viewer; historical logs viewable with Log Viewer or Reporting System (see below).
Log viewing and manipulation follows administrative permissions model
Configurable log file disk management
Automated log scheduling and forwarding for post-processing

13. Real-time Log Viewer

Displays log records as received from all VPN Firewall Bricks™; messages can be filtered, sorted and highlighted
Includes historical record search capabilities with specified time parameters

14. Reporting System

Generates HTML-based reports with full filtering, sorting and scheduling capabilities; configurable per administrator

Reports include sessions over time, policy snapshots, administrator events and configuration changes

Includes preconfigured reports for fast initial deployment

15. Customer Specific Report Generation and Delivery

Integrates with the WebTrends Firewall Reporting Suite from NetIQ Corporation; uses the WebTrends Enhanced Log Format (WELF)

Fully automates generation and delivery of customer-specific, traffic statistic graphic reports to customers via FTP, e-mail or http server

16. Policy Change Control

Records all administrative activity to audit logs

Captures all policy and configuration changes in detailed, user-configurable history files that are secured from tampering/modification and support policy roll-back

17. Alarms

Generates alarms based on VPN Firewall Brick™ log messages and locally generated log messages from LSMS subsystems; configurable per-administrator

Includes preconfigured alarms for fast initial deployment

Configurable alarm triggers include:

LSMS Error

VPN Firewall Brick™ Error

VPN Firewall Brick™ Lost/Found

VPN Firewall Brick™ Interface Up/Down

Proactive Monitoring Threshold Crossing

VPN Firewall Brick™ Redundancy Alarms

LSMS Redundancy Alarms

ISS RealSecure Alarms

Configurable notification methods:

Console Alarm (via the LSMS Remote Navigator)

Email

Out-of-band modem-dialed alphanumeric message sent to pager (via the TAP protocol)

SNMP Trap

SYSLOG Message (with configurable SYSLOG level)

Alarm triggers can be mapped to any combination of notification methods

18. Real-Time Status Monitors

Support real-time and historical dynamically-updating text and graphical monitoring

VPN Firewall Brick™ monitor - provides windows for each device and aggregate collection of devices; monitors statistics for each physical port, packet, byte, and session; includes Quality-of-Service graphs to monitor throughput and performance relative to configured guarantees and limits

VPN Tunnel monitor - provides status of each VPN tunnel; monitors Service-Level Agreements (SLAs) for VPN tunnel round-trip delay

Administrator and LSMS monitor – views all logged-in administrators and connection statistics; reports connection status of each LSMS in real-time

19. Command Line Interface

Allows administrators to script the configuration of many LSMS components and policy objects using a text file-based interface

20. SNMP Agent

Accesses limited configuration and statistic information regarding the system and associated VPN Firewall Bricks™ in a Read-Only fashion via the LSMS. Absolutely NO information may be configured via SNMP. VPN Firewall Bricks™ do NOT respond to SNMP or any variation thereof. Available in SNMP v2c format.

21. VPN Firewall Brick™ Remote Console

Provides a secure remote console to any VPN Firewall Brick™ and executes debugging/troubleshooting commands

No policy modifications can be made from this Remote Console or any VPN Firewall Brick™ console interface

LSMS Hardware Requirements

Microsoft Windows NT 4.0 (Server or Workstation), Windows 2000 (Professional or Server)

500 MHz Pentium Pro processor (minimum)

512MB system memory or higher recommended

128 MB system swap space (minimum)

4-GB hard drive

CD-ROM drive

3.5 inch floppy drive

1 Ethernet card

Video card capable of 1024 X 768 resolution with 65,535 colors

Sun Solaris 7, or 8

333 MHz processor (minimum)

512MB system memory or higher recommended

500 MB free disk space in the partition in which the server software is installed

Swap space as large as the amount of RAM (minimum)

CD-ROM drive

3.5-inch floppy drive

1 Ethernet card

Ordering Information

LSMS Basic (includes license to manage up to 5 VPN Firewall Brick™ 20, 80, 201, 300 and 500, unlimited LAN-to-LAN VPN tunnels and 5 simultaneous IPSec Client tunnels)	Part Number 300532629
LSMS Premium (includes license to manage all models of up to 5 VPN Firewall Bricks™, unlimited LAN-to-LAN VPN tunnels, 105 simultaneous IPSec Client tunnels and Lucent IPSec Client Custom Branding Package)	Part Number 300531761
LSMS Basic Redundancy Package (for High Availability applications)	Part Number 300532637
LSMS Premium Redundancy Package (for High Availability applications)	Part Number 300532603
Additional 5 VPN Firewall Brick™ management license	Part Number 300532918
Additional 25 VPN Firewall Brick™ management license	Part Number 300532934
Additional 50 VPN Firewall Brick™ management license	Part Number 300532967
Additional 100 VPN Firewall Brick™ management license	Part Number 300533023
Upgrade LSMS Basic to LSMS Premium	Part Number 300532611
Lucent Proxy Agent	Included in LSMS software
Lucent IPSec Client	See Lucent IPSec Client data sheet for ordering details

To learn more, please contact your Lucent Technologies Sales Representative or Lucent BusinessPartner. Or visit our web site at www.lucent.com.

This document is provided for planning purposes only and is not intended to modify or supplement any Lucent Technologies specifications or warranties relating to the products or services described herein.

Specifications are subject to change without notice.

VPN Firewall Brick is a trademark of Lucent Technologies Inc.

Copyright © 2002
Lucent Technologies Inc.
All rights reserved

LSMS v1 07/02

Lucent Technologies
Bell Labs Innovations

