Alcatel-Lucent Security Management Server

SECURITY, VPN, AND QoS MANAGEMENT SOLUTION

The Alcatel-Lucent Security Management Server software brings you advanced carrier-grade IP services management at a low total cost of ownership (TCO). Teamed with Alcatel-Lucent award-winning VPN Firewall Brick™ security appliance portfolio and the Alcatel-Lucent IPSec Client, the Alcatel-Lucent Security Management Server lets you rapidly provision and manage high-return services for thousands of users in a single console. It integrates firewall, VPN, QoS, VLAN, VoIP and virtual firewall policy management; provides industry-leading scalability and availability; delivers robust monitoring, logs and reports; and provides flexible deployment options — all without the costly additional modules or recurring license fees that competitive products require.

Applications

- Advanced security services
- VPN services for site-to-site and remote access
- Bandwidth management capabilities
- VoIP security
- Secure data center Web and application hosting
- Storage network security solution
- Mobile data security
- Packet data gateway and packet data interworking functions for fixed mobile convergence/Wi-Fi VPN and VoIP/data security
- Managed security services
- Unlicensed mobile access (UMA) and IP multimedia subsystem (IMS) security

FEATURES	BENEFITS
• One management solution including remote management	• Single platform provides centralized, comprehensive management of all IP services with real-time monitoring, robust logging and customized reporting
• Low operating costs	• Secure remote management reduces need for network reconfigurations, truck rolls, or on-site support; VLAN, virtual firewall, and QoS support included at no extra charge • Management efficiencies cut staffing and administrative expenses
• Cost-saving growth	• Easily migrate from basic to advanced security, VPN, and QoS services
• Simple, economical licensing model	• No ongoing license fees or add-ons required for complete security management
• Native high availability and carrier class reliability	• Assures business continuity through native high availability with carrier-class reliability, and virtually impenetrable to hacker attacks

FEATURES	BENEFITS
• Proven carrier-class performance	• Mature product with over ten years of service in the world's largest networks • Distributable across up to four network operations centers (NOCs) for active/active network redundancy with no single point of failure
• Integrated security	• Network is kept secure through integrated firewall, VPN, QoS, VLAN and virtual firewall management
• Flexible management model	• Provides a wide range of controls policies at global, customer, device, interface, VLAN and IP address range levels
• Multiple IP services deployment options	• Addresses specific needs with premises-based, network-based, tiered, and data-center architecture deployment options
• High scalability	• Supports 20,000 Alcatel-Lucent VPN Firewall Brick security appliances and up to 500,000 simultaneously connected Alcatel-Lucent IPSec Client (or third party) VPN users

Complete, cost-effective solutions for network security, VPN, VoIP, service-quality assurance and more

The Alcatel-Lucent VPN Firewall Brick portfolio offers a broad range of enterprise and carrier-class security solutions to protect corporate and service provider networks delivering mission-critical IP applications to headquarter employees, branch offices, trading partners, road warriors and customers. Alcatel-Lucent VPN Firewall Brick solutions help stretch IT budgets with superb price / performance and low total cost of ownership. Leading edge technology with timesaving, work-saving features help maximize IT staff resources. Plus ample flexibility, availability and scalability simplify deployment and management of diverse applications including:

- Advanced security services
- VPN services for site-to-site and remote access
- Bandwidth management capabilities
- Secure data center Web and application hosting
- Storage network secure solution
- Mobile data security
- Packet data gateway and packet data inter working functions for dual-mode wireless/Wi-Fi VPN and VoIP/data security

The Alcatel-Lucent VPN Firewall Brick portfolio forms a unique three tier security architecture and includes:

- *VPN Firewall Brick security appliances* – Security appliances that integrate application layer inspection, firewall functionality with advanced VPN capabilities for small office through data-center requirements
- *Alcatel-Lucent Security Management Server* – Software for robust, tightly synchronized firewall, VPN, service quality, VLAN and virtual firewall policy management.
- *Alcatel-Lucent IPSec Client* – Software that provides secure remote access VPN services for mobile workforce and telecommuters

Deploy robust security safeguards network-wide

The VPN Firewall Brick security appliances are built as security-specific devices. In contrast to traditional router-based systems, they operate as intrinsically secure Ethernet layer bridges that are virtually invisible to hackers scanning your network. Completely segregated from the routing process, these security appliances are not vulnerable to dynamic routing protocol attacks. In many instances, they are undetectable by any device not on the same network segment, protecting enterprises with a high level of stealth security.

Reinforcing this depth of defense is the security appliances' innovative, operating system, a compact real-time kernel designed exclusively for security. Far less easily compromised than general purpose operating systems running on server platforms, this exceptionally thin system virtually eliminates all points of vulnerability.

As a result, the VPN Firewall Brick security appliances have no security-threatening back doors (no telnet, ftp, HTTP or other insecure access method can be used to compromise the configuration of these security devices) and can only be accessed by a secure, encrypted management channel from the Alcatel-Lucent Security Management Server software. The software adds exposure-limiting safeguards including strong IP-specific denial-of-service attack protection, premium firewall and VPN authentication services, application layer defense and content-level security including command blocking, URL blocking and a unique rules-based routing capability that seamlessly integrates the VPN Firewall Brick portfolio with any third party security appliance (for example: content filtering or virus scanning systems).

Implement large-scale VPN support with high-performance packet processing

The VPN Firewall Brick security appliances deliver the performance needed to provide vital security and VPN services for thousands of enterprise users. High capacity packet processing capabilities help maximize user efficiency and productivity. Systems in the portfolio can provide up to 1.7 Gbps VPN throughput and a full 4.75 Gbps firewall throughput. Portfolio-wide scalability helps protect expanding user populations cost effectively.

A single VPN Firewall Brick unit can support up to 3 million simultaneous sessions and over 20,000 simultaneous VPN tunnels. Its highly efficient operating system contributes to these outstanding processing capabilities by freeing memory for session and policy management.

Streamline firewall deployment, configuration and management

The VPN Firewall Brick security appliances can be installed and working at any network location. These flexible bridging firewalls work as quickly as a physical connection can be made. There's no need to re-segment the network, worry about downtime during network conversion to the new topology or wait as hosts are directed to a new gateway. Alcatel-Lucent Security Management Server software delivers:

- Sophisticated IP services management capabilities with low operating costs to manage security, not individual devices — easy security deployment, management and maintenance with centrally controlled VPN Firewall Brick clients
- Scalability to rapidly provision and manage up to 20,000 VPN Firewall Brick security appliances and 500,000 Alcatel-Lucent IPSec Clients (or third party IPSec Client) users from one console — fewer devices to maintain and fewer people to maintain them
- Seamless integration of firewall, VPN, bandwidth management, virtual LAN (VLAN) and virtual firewall policy management — centralized real-time monitoring, robust logging and customized reporting capabilities
- Integrated Denial of Service protection, intrusion detection / prevention facilities and intelligent cache management capabilities maximizes uptime and mitigates impacts of network attacks

Leverage high-availability bandwidth management for consistent service quality

The VPN Firewall Brick security appliances can increase both network security and quality of service through uniquely granular bandwidth management. They incorporate — at no extra charge — robust implementation of class-based queuing (CBQ) technology for committed-rate bandwidth control and traffic prioritization. Bandwidth limits to help defend against flood attacks, and bandwidth guarantees to enhance end-user experiences, are enforced at the server and user levels. Traffic can be classified by physical interface, virtual firewall, policy rule and session, enabling simplified yet precisely targeted security implementations.

Sustain business continuity with carrier-class reliability and availability

A high-availability architecture is built into every component of the Alcatel-Lucent Brick portfolio. There is no single point of failure solution-wide. All VPN Firewall Brick models support native sub-second failover to a standby unit. In an outage, services continue uninterrupted. Out-of-band management capabilities ensure continued service even if communications are lost due to a network outage. For added reliability, Alcatel-Lucent Security Management Server software can be distributed across multiple geographically dispersed operations centers for active/active network redundancy. This enables immediate disaster recovery in the event of a catastrophe at the primary management location.

Keep your total ownership costs low

Solutions based on the VPN Firewall Brick portfolio efficiently address the need to contain operations outlays, make efficient use of in-house technical expertise and protect network investments. All solution components are built to inter operate smoothly with existing infrastructure elements. Introducing them requires no costly network retrofits.

The VPN Firewall Brick portfolio helps cut IT staff hours and shorten time-to-service with its full-featured bridging support. And because it doesn't run on a general purpose operating system, it eliminates the high costs and time-intensive efforts associated with OS upgrades and patches.

The performance-proven Alcatel-Lucent Security Management Server security management solution offers one simple, economical licensing structure — without costly additional modules or recurring license fees. Its high-capacity processing and high device count management capabilities help minimize additional capital-equipment purchases.

And its comprehensive security safeguards dramatically reduce network vulnerabilities that consume IT staff time and budget.

Alcatel-Lucent VPN Firewall Brick portfolio

- *Simplified management* – Unique client/server design; centralized staging, real-time monitoring and no-touch management of all VPN, security and service-quality assurance capabilities via scalable, proven Alcatel-Lucent Security Management Server
- *Full-featured bridging* – Enables stealthy, depth of defense security that conventional router-based firewalls cannot match

- *Advanced security safeguards* – Denial-of-service attack protection; high-speed content security; premium authentication services; with no occurrences of reported advisories or vulnerabilities and no backdoors
- *Uniquely granular bandwidth management* – Maximize service quality via flexible class-based queuing (CBQ) technology, server-level and user-level limits and guarantees
- *Carrier-grade reliability* – Native high-availability architecture with no single point of failure
- *Rules-based routing* – Routes all packets matching the rule to a proxy server, router or other device using third-party software to perform content filtering functions such as command blocking, URL filtering and virus scanning. It allows transparent interaction with any third-party equipment
- *High performance packet processing* – Range of systems available to support up to three million simultaneous sessions, 1,100 virtual firewalls and 20,000 VPN tunnels
- *Ultra-thin, highly secure operating system* – Virtually impenetrable to hacker attacks; frees memory for packet processing, policy management
- *Virtual firewall and VLAN support* – Easily assign and enforce security policies for diverse user groups
- *Plug-and-play deployment* – Implement secure mission critical applications without costly, time-intensive network reconfiguration
- *Low ownership costs* – No ongoing feature-licensing expenses; easy installation, management and upgrades save IT staff time and effort; high performance, high capacity features reduce the need to purchase additional equipment

Technical specifications

Mode of operation

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

Performance and capacity

- Supports 1,000 customer groups each with hundreds of unique policies
- Centrally collects up to 30,000 log records per Alcatel-Lucent Security Management Server or Compute Server for a maximum of 300,000 log records per second
- Central management of up to 20,000 Brick devices and 500,000 simultaneously connected IPSec-based VPN users from a single management cluster
  - ¬ Hierarchical solution consisting of redundant Security Management Server and Compute Servers
  - ¬ Each Alcatel-Lucent Security Management Server can manage up to 1,000 VPN Firewalls Brick and 100,000 IPSec based Remote Access VPN Users
  - ¬ Up to four Security Management Server systems can be configured in a load sharing (co-located or geo-diverse) configuration
  - ¬ Each Security Management Server System can support up to five Alcatel-Lucent Security Management Server Compute Servers for logging and management offloading

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

Role-based administration

- Uses two administrative classes:
  - ¬ *Alcatel-Lucent Security Management Server 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 Alcatel-Lucent Security Management Server Remote Navigator utility (included); provides secure access to all Alcatel-Lucent Security Management Server utilities
- Allows concurrent administrators to exchange messages via a real-time messenger service

Secure 3-tier architecture

- Alcatel-Lucent Security Management Server to VPN Firewall Brick security appliance communications secured with Diffie-Helman and 3DES encryption, SHA-1 authentication and integrity, and digital certificates for VPN Firewall Brick Security Management Server authentication
- Alcatel-Lucent Security Management Server Remote Navigator to Security Management Server 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, secured, AES-encrypted connections

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
- PKI Certificate requests (PKCS 12)
- User assignable RADIUS attributes
- DoD PKI

Remote access VPN tunnel management

- Supports IKEv1 and IKEv2 remote access VPN Clients, including the Alcatel-Lucent IPSec Client, third party IPSec VPN clients and IKEv2 clients embedded in next-generation mobile products. Provides support for EAP-SIM, EAP-AKA, EAP-TLS and EAP-MD5
- Centralizes management of the Alcatel-Lucent IPSec Clients, including software distribution, software updates, client VPN configurations and client 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

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
- Supports IKEv1 and IKEv2 site-to-site tunnels

High availability/redundancy

- Supports active/active management with up to four geographically distributed servers and realtime 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

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 operating system upgrade with a failover pair of VPN Firewall Brick units

Application programming interfaces (APIs)

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

Audit log management

- Six categories of audit logs created daily:
  - ¬ VPN log
  - ¬ Firewall session logs
  - ¬ Administrative event logs
  - ¬ User authentication logs
  - ¬ Proactive monitoring statistic logs
  - ¬ SOX audit log
- 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

Real-time log viewer

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

Reporting system

- Automatically merges data from geographically distributed log servers
- 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

Customer specific report generation and delivery

- Integrates with the WebTrends Firewall Reporting Suite; 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

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

Alarms

- Generates alarms based on VPN Firewall Brick log messages and locally generated log messages from Alcatel-Lucent Security Management Server subsystems; configurable per-administrator
- Includes preconfigured alarms for fast initial deployment
- Configurable alarm triggers include:
  - ¬ Security Management Server 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
  - ¬ Security Management Server Redundancy Alarms
- Configurable notification methods:
  - ¬ Console Alarm (via the Alcatel-Lucent Security Management Server Remote Navigator)
  - ¬ E-mail
  - ¬ 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

Real-time status monitors

- Support real-time and historical dynamically-updating text and graphical monitoring
- VPN Firewall Brick security appliance 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 Alcatel-Lucent Security Management Server monitor – views all logged-in administrators and connection statistics; reports connection status of each Security Management Server or Compute Server in real-time

Command line interface

- Allows administrators to script the configuration of many Alcatel-Lucent Security Management Server components and policy objects using a text file-based interface

SNMP agent

- Access-limited configuration and statistic information regarding the system and associated VPN Firewall Brick security appliances in a read only manner via the Alcatel-Lucent Security Management Server. Access limited configuration and statistic information regarding the "VPN Firewall" Brick security appliances is available from either the Alcatel-Lucent Security Management Server or from the VPN Firewall Brick Security appliance in SNMP v2c format.

VPN Firewall Brick remote console

- Provides a secure remote console to any VPN Firewall Brick security appliance and executes debugging/troubleshooting commands
- No policy modifications can be made from this Remote Console or any VPN Firewall Brick console interface

Rules-based routing

- Provides capability to configure a rule for HTTP, FTP, or SMTP protocol traffic. Routes all packets matching the rule to a proxy server, router or other device utilizing third party software to perform content filtering functions such as command blocking, URL filtering, and virus scanning. Allows transparent interaction with any third party equipment

Alcatel-Lucent Security Management Server and Compute Server

Software requirements:

- Sun Solaris™ 2.9 or 2.10 on SPARC processors
- Red Hat Linux version RHEL4 and RHEL5 support on x86 processors
- Windows XP Professional, Windows Server 2003, or Windows Vista Business

Hardware requirements:
Sun® Workstation or server for Sun Solaris Operating System:

- Solaris Sparc:
  - ¬ 600 MHz UltraSPARC or better
  - ¬ 512 MB of memory or more
- Linux RHEL4/5:
  - ¬ 700 MHz Pentium III or better
  - ¬ 1 GB of memory or more
- Windows XP/2003:
  - ¬ 700 MHz Pentium III or better
  - ¬ 512 MB of memory or more
- Vista:
  - ¬ 700 MHz Pentium III or better
  - ¬ 1 GB of memory or more
- Common:
  - ¬ Swap space at least as large as system memory
  - ¬ 4GB free disk space in file system partition where software is to be installed
  - ¬ 50MB free disk space in root partition
  - ¬ One 10/100 Ethernet interface
  - ¬ CD-ROM drive
  - ¬ 3.5" floppy drive, USB port and serial port (Floppy is only required for older model Bricks. Brick50,150,700,1200 Models do not require the Floppy)
  - ¬ Video card capable of supporting minimum resolution of 1024x768 (65,535 colors)

Ordering Information

PART NUMBER	DESCRIPTION
301033320	Alcatel-Lucent Security Management Server v9.4 Base Package (includes license to manage up to five VPN Firewall Brick products, and 100 simultaneous client tunnels (including IPSec client and third party IPSec VPN clients)
301033338	Alcatel-Lucent Security Management Server v9.4 Redundancy Package (for high availability applications – up to three supported per Security Management Server v9.4 base package)
301033346	Alcatel-Lucent Security Management Server v9.4 Compute Server Package (for offloading logging and management functions – up to five supported per Security Management Server (either Base or Redundancy package)
301033411	Management license to manage five additional VPN Firewall Brick devices
301033429	Management license to manage 25 additional VPN Firewall Brick devices
301033437	Management license to manage 50 additional VPN Firewall Brick devices
301033445	Management license to manage 100 additional VPN Firewall Brick devices
301033452	Management license to manage 250 additional VPN Firewall Brick devices
301033460	Management license to manage 500 additional VPN Firewall Brick devices
301033387	V9.4 upgrade Alcatel-Lucent Security Management Server v9.4 Base package to v9.4 base
301033478	SMS 9.4 Radius Accounting License – enables the use of Radius Accounting for dual mode services
301033395	9.4 Redundant upgrade package
301033403	9.4 Compute server upgrade package
301033379	9.4 Lawful Intercept License
301033353	9.4 Radius Accounting License

Alcatel·Lucent