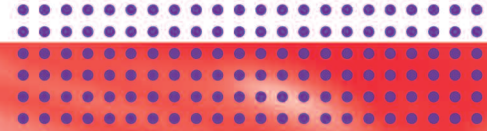Alcatel·Lucent

Alcatel-Lucent VPN Firewall Brick 50 Security Appliance

VPN FIREWALL, VoIP, AND QoS SECURITY GATEWAY

Deliver service level-assured advanced security, IP VPN, and bandwidth management services to small office and home office locations. The carrier-class, VPN Firewall Brick® 50 security appliance stretches investment dollars and lowers total ownership costs by offering a low price/high-performance solution with service-enhancing, revenue-building features.

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 WiFi VPN and VoIP/Data Security

Managed Security Services

Unlicensed Mobile Access (UMA) and IP Multimedia Subsystem (IMS) Security

FEATURES

- **Integrated security security appliance** — Provides high-speed firewall, VPN, QoS, VLAN and virtual firewall capabilities in one configuration

- **High Performance system** — Delivers 195 Mbps firewall performance, 75 Mbps 3DES VPN and 60 Mbps AES VPN performance using integrated hardware-assisted encryption accelerator.

- **Innovative security services** — Includes advanced distributed denial of service attack protection, latest IKEv2 standards, strong authentication and real-time monitoring, logging and reporting

- **High capacity** — Supports up to 1,000 simultaneous VPN tunnels, 4,094 VLANs, 50 virtual firewalls, and 135,000 simultaneous sessions

- **Intrinsically secure, transparent Layer-2 bridge** — Outperforms firewalls running on routers, general purpose operating systems or PC servers

BENEFITS

- **Higher performance** — Deliver an enhanced user experience with 195 Mbps cleartext, 75 Mbps 3DES and 60 Mbps AES IPSec VPN throughput, combined with best-in-class bandwidth management — with customer-level, user-level and server-level QoS control

- **Low price/performance** — Get outstanding security and throughput for less than the per-Mbps price of major competitors

- **Low cost of ownership** — One configuration supports multiple IP services with no additional or recurring licensing fees

- **Flexible deployment** — Options include premises- or network-based services with shared or dedicated hardware environments

- **Economical growth path** — Seamless migration to advanced, VoIP, QoS and VPN security services with no added infrastructure investments

- **Plug-and-Play interoperability** — there's no need for costly network reconfigurations or on-site support

FEATURES

- **Central staging and secure remote management** — Provides integrated control over thousands of VPN Firewall Brick appliances and IPSec VPN Client users including the Alcatel-Lucent IPSec Client, from one console, using the Alcatel-Lucent Brick Security Management Server (SMS) software

- **High-availability architecture** — Eliminates any single point of failure

- **Proven secure** — Virtually impenetrable hardened security operating system coupled with secure management infrastructure.

BENEFITS

- **Cost-effective business continuity** — Take advantage of low priced encryption performance and maintain carrier-class reliability for today's data-heavy business applications

- **Assured business continuity** — native high availability with carrier-class reliability

- **Centralized, Scalable, carrier-class management** — Centrally manage up to 20,000 VPN Firewall Brick units and 500,000 Alcatel-Lucent IPSec Client (or 3rd party IPSec client) users with Alcatel-Lucent Brick Security Management Server v9.0 or later.

TECHNICAL SPECIFICATIONS

Processor/Memory

- 466MHz AMD Geode Processor with 64 MB of RAM

LAN Interfaces

- (3) 10/100 Base-TX Ethernet Ports

Other Ports

- DB9 serial, USB (1)

Performance

- Concurrent sessions – 135,000

- New sessions/second – 1,600

- Rules – 10,000 (shared among all virtual firewalls)

- Maximum clear text throughput – 195 Mbps (1514 byte UDP packets) 88,000 pps (78 byte UDP packets)

- Maximum 3DES throughput with hardware encryption acceleration – 75 Mbps (1460 byte UDP packets without LZS compression) 9,200 pps (78 byte, UDP packets)

- Maximum AES 256 throughput with hardware encryption acceleration – 60 Mbps (1024 byte UDP packets without LZS compression) 9,200 pps (78 byte UDP packets without LZS compression)

- Hardware Assisted Encryption – on-board encryption accelerator module

Virtualization

- Maximum number of virtual firewalls – 50

- Number of VLANs supported – 4,094

- VLAN domains – up to 16 per VLAN trunk

- VPN Firewall Brick partitions – allows for virtualization of customer IP address range, including support for overlapping IP addresses

Modes of Operation

- Bridging and/or routing on all interfaces

- All features supported with bridging

- IP routing with static routes

- 802.1Q VLAN tagging supported inbound and outbound on any combination of ports

- Layer-2 VLAN bridging

- Network Address Translation (NAT)

- Port Address Translation (PAT)

- Policy-based NAT and PAT (per rule)

- Supports virtual IP addresses for both address translation and VPN tunnel endpoints

- PPPoE and DHCP-assignable interface/VLAN addresses

- Redundant DHCP Relay capabilities

- Dynamic registration of mobile VPN Firewall Brick addresses for centralized remote management

- Nested zone rulesets for common firewall policies for all Bricks in zone.

- Link Aggregation

- Mobile Brick using integrated DHCP Client.

Services Supported

- Bootp, http, irc, netstat, pop3, SNMP, tftp, pptp, dns, https, kerberos, nntp, rip, ssh, who, RADIUS, eigrp, ident, ldap, ntp, rip2, syslog, shell, X11, exec, gmp, login, OSPF, rlogin, telnet, talk, H.323, ftp, imap, mbone, ping, rsh, traceroute, lotus notes, VoIP/SIP, Gopher, IPSec, netbios, pointcast, SMTP, sql*net

- Any IP protocol (user definable)

- Any IP protocol + layer 4 ports (user definable)

- Support for non-IP protocols as defined by DSAP/Ethertype

Layer-7 Application Support

- Application Filter architecture supports Layer-7 protocol inspection (deep packet inspection) for command and protocol validation, protocol anomaly detection, dynamic channel pinholes and application layer address translation. Application filters include http, ftp, RPC, tftp, H.323/H.323 RAS, SMTP, Oracle SQL*Net, NetBIOS, ESP, DHCP Relay, DNS, GTP, and SIP

Firewall Attack Detection and Protection

- Generalized day 0 anomaly-based flood protection extensible to new flood attacks as discovered with patent-pending Intelligent Cache Management

- SYN flood protection to specifically protect inbound servers, e.g. Web servers, from inbound TCP SYN floods

- Strict TCP validation to ensure TCP session state enforcement, validation of sequence and acknowledgement numbers, rejection of bad TCP flag combinations

- Rejection of bad TCP flag combinations

- Initial Sequence Number (ISN) rewriting for weak TCP stack implementations

- Fragment flood protection with Robust Fragment Reassembly, ensures no partial or overlapping fragments are transmitted

- Generalized IP Packet Validation including detection of malformed packets

- DoS mitigations for over 190 DoS attacks, including ping of death, land attack, tear drop attack, etc.

- Drops bad IP options as well as source route options

- Connection rate limits to minimize effects of new attacks.

QoS/Bandwidth Management

- Classified by Physical Port, Virtual Firewall, Firewall Rule, Session Bandwidth Guarantees – Into and out of Virtual Firewall, allocated in bits/second

- Bandwidth Limits - Into and out of Virtual Firewall, allocated in bits/second, packets/session, sessions/second

- ToS/DiffServ marking and matching

- Integrated with Application Layer Filters

Content Security

- HTTP Filter Keyword support integrated with HTTP Application Filter

- Basic content filtering with configurable whitelist/blacklist and content keyword matching.

- URL redirection for blacklist sites

- Rules-based routing feature for HTTP, SMTP and FTP features (Security Management Server v9.1 or later)

  - ¬ Interoperates with all 3rd party Anti-virus, Anti-Spam, and Content Filtering systems

  - ¬ Redirects only protocol-specific packets to 3rd party systems performing Anti-virus, Anti-spam, and content filtering services.

- Application-layer protocol command recognition and filtering

- Application-layer command line length enforcement

- Unknown protocol command handling

- Extensive session-oriented logging for application-layer commands and replies

- Hostile mobile code blocking (Java®, ActiveX™)

Firewall User Authentication

- Browser-based authentication allows authentication of any user protocol

- Built-in internal database – user limit 10,000

- Local passwords, RADIUS, SecurID

- User assignable RADIUS attributes

VPN

- Maximum number of dedicated VPN tunnels – 1000

- Manual Key, IKEv1, IKEv2, DoD PKI, X.509

- 3DES (168-bit), DES (56-bit)

- AES (128, 192, 256-bit)

- SHA-1 and MD5 authentication/integrity

- Replay attack protection

- Remote access VPN

- Site-to-site VPN

- IPSec NAT Traversal/UDP encapsulated IPSec

- IKEv2 IPSec NAT Traversal and Dead Peer Detection

- LZS compression

- Spliced and nested tunneling

- Fully meshed or Hub and Spoke Site-to-Site VPN

VPN Authentication

- Local passwords, RADIUS, SecurID, X.509 digital certificates

- PKI Certificate requests (PKCS 12)

- Automatic LDAP certificate retrieval

- DoD PKI

High Availability

- Brick security appliance to Brick security appliance active/passive failover with full synchronization

- 400 millisecond device failure detection and activation

- Session protection for firewall, VoIP and VPN

- Link failure detection

- Alarm notification on failover

- Encryption and authentication of session synchronization traffic

- Self-healing synchronization links

- Pre-emption and IP tracking for improved health state checking

- Seamless system upgrade with no downtime for redundant deployments

TECHNICAL SPECIFICATIONS

Diagnostic Tools

- Out of band debugging and analysis via serial port/modem/terminal server

- Centralized, secure remote console to any VPN Firewall Brick

- Brick security appliance supports Ping, Traceroute, and packet trace with filters

- Remote VPN Firewall Brick bootstrapping

- Real-time log viewer analysis tool

- Java-based Navigator for remote access to management system

3-Tier Management Architecture

- Centralized, carrier-class, active/active management architecture with Alcatel-Lucent Brick Security Management Server (SMS) software

- Secure VPN Firewall Brick to SMS communications with Diffie-Helman and 3DES encryption, SHA-1 authentication and integrity and digital certificates for VPN Firewall Brick security appliance/ Alcatel-Lucent Brick Security Management

- Server authentication

- Up to 100 simultaneous administrators securely managing all aspects of up to 20000 VPN Firewall Brick units in a hierarchical management cluster.

- Secure, reliable, redundant real-time alarms, logs, reports

Certifications

- ICSA V4.1 Firewall Certified

- ICSA V1.0D IPSec Certified, v1.2 in process

- FIPS 140-2 Certification in process

- EAL-4 Certification in process

Mean Time Between Failure

- 409,688 Hrs

- Telecordia SR-332 at Standard Reference Conditions.

Dimensions (W x L x H)

- 8.5" (W) x 5.9" (D) x 1.1" (H) (1U)

- 21.6 cm x 15 cm x 2.8 cm (1U)

- Wall, or Table Mountable

- Weight: 2 lbs., 3 oz. (1.0 Kg)

- Shipping Weight: 4 lbs., 12 oz. (2.2 Kg)

Cooling

- Passive cooling

Operating Altitude

- Up to 13,123 feet (4,000 m.)

Environmental

OPERATING

- Temperature: 0 to 50 C.

- Shock: 2.5g. at 15 – 20 ms on any axis

- Relative Humidity: 5 – 95% at 40 C. (non-condensing)

- Vibration: 5g. at 2 – 200 Hz on any axis

NON-OPERATING

- Temperature: -40 to 70 C.

- Shock: 35g. at 15 – 20 ms on any axis

- Relative Humidity: 5 – 95% at 40 C. (non-condensing)

- Vibration: 5g at 2 – 200 Hz on any axis

Power

- External AC to DC Power Supply: Rated 25W max.

- Input: CV mode, 100 – 254 VAC, 47 to 63 Hz, 64 watts

- Typical Consumption: 1.2A max. @ 115V, 0.6A @ max. 230V

Alcatel-Lucent Security Management Server

Software Requirements

- Sun Solaris™ 2.8, 2.9 or 2.10 on SPARC processors

- Microsoft Windows® 2000 Professional, Windows® 2000 Server, Windows XP Professional, Windows Server 2003 or Windows Vista Business.

Hardware Requirements

SUN® WORKSTATION OR SERVER FOR SUNSOLARIS OPERATING SYSTEM:

- Sun UltraSPARC5 (600 MHz processor or better) or better

- 512MB of system memory (minimum)

- Swap space at least as large as system memory

- 2 GB free disk space in file system partition where software is to be installed

- 50MB free disk space in root partition

- 1 10/100 Ethernet interface

- CD-ROM drive

- 3.5" floppy drive, USB port and serial port.

- Video card capable of supporting 1024x768 resolution (65,535 colors)

INTEL®-BASED COMPUTER (FOR MICROSOFT WINDOWS® 2000 PROFESSIONAL, WINDOWS 2000 SERVER, WINDOWS XP PROFESSIONAL, WINDOWS SERVER 2003)

- 700 MHz Pentium III processor (minimum)

- 512 MB system memory (minimum), higher recommended

- CD-ROM drive

- Swap space at least as large as install system memory

- 2 GB free space on an NTFS partition

- 3.5" floppy, USB port and serial port.

- 1 Ethernet 10/100 card

- Video card capable of supporting 1024x768 resolution

INTEL®-BASED COMPUTER (FOR MICROSOFT VISTA® BUSINESS)

- 2.0 GHz processor (minimum)

- 1GB system memory (minimum), 2GB recommended

- CD-ROM drive

- Swap space at least as large as install system memory

- 80 GB harddisk with 40GB free space on a NTFS partition

- 3.5" floppy, USB port and serial port.

- 1 Ethernet 10/100 card

- Video card capable of supporting 1024x768 resolution

Ordering Information	North and South America	Europe	Asia, Pacific
Product Safety Approvals	CSA Certified to UL® 60950-1, 1st Edition	CE	CB Scheme to EN/IEC 60950-1
	CAN/CSA 22.2 No. 60950-1-03	CB Scheme to EN/IEC 60950-1	AS/NZS 3260 1993 with amendments 1,2,3 and 4
			ACA TS 001 1997
EMC Approval	FCC Part 15, Class B	CE	VCCI Class B
	ICES-003, Class B	EN55024	AS/NZS – CISPR PUB 22, Class B
		EN55022, Class B	
Network Attachment Approvals	Not Applicable	Not Applicable	Not Applicable

ORDERING INFORMATION

PART NUMBER	DESCRIPTION
300819075	VPN Firewall Alcatel-Lucent Brick 50 Security Appliance
Contact your Alcatel-Lucent Representative or authorized reseller for details.	Alcatel-Lucent Security Management Server Brick 50 requires v9.0 (patch level 232) or later version. Available in several configurations to meet your networking requirements.
Contact your Alcatel-Lucent Representative or authorized reseller for details.	Alcatel-Lucent IPSec Client Available in several configurations to meet your networking requirements.

To learn more, contact your dedicated Alcatel-Lucent representative, authorized reseller, or sales agent. You can also visit our Web site at www.alcatel-lucent.com.

www.alcatel-lucent.com

Alcatel·Lucent