. . . connecting your business

LANCOM 9100+ VPN (CC)

Central-site VPN gateway for highly secure connectivity of up to 1,000 sites

- Certified IT security "Made in Germany" – CC EAL 4+ compliant
- Ideal for highly secure site connectivity and the protection of critical sub-areas
- Incl. 200 VPN channels, upgradable to 1,000 per device
- Advanced Routing & Forwarding with 256 IP contexts
- 4 x Gigabit Ethernet

LANCOM
Systems

The LANCOM 9100+ VPN (CC) is a central site VPN gateway for connecting 200 sites by default, with the LANCOM VPN Option up to 1,000. It is ideal for public authorities, institutions, and commercial organizations that need a high level of security in their data communications: The LANCOM 9100+ VPN (CC) is intended for high-security operations based on CC EAL 4+. The certification by the German Federal Office for Information Security (BSI) guarantees that the evaluation of the LANCOM products meets worldwide highest standards. The evaluation level CC EAL 4+ is the highest level of certification a commercial network product can achieve. On top of that, the LANCOM 9100+ VPN (CC) comes with a field-proven scope of functionalities and interfaces. Comprehensive VPN functions enable remote sites to access the company network securely. A practical display permanently illustrates all relevant device information, such as temperature, CPU load, and active VPN tunnels.

More data security.

Certified IT security: Made in Germany. The LANCOM 9100+ VPN (CC) is ideal for public authorities, institutions, and commercial organizations that require the security level "CC EAL 4+" (Common Criteria for Information Technology Security Evaluation, Evaluation Assurance Level 4+) as specified by the German Federal Office for Information Security (BSI). This internationally recognized seal of approval guarantees the security and confidentiality of the LANCOM 9100+ VPN (CC), which an independent body has methodically examined and tested to level 4. Hence, the LANCOM 9100+ VPN (CC) provides certified protection against cyber attacks to cross-site networks with pronounced security requirements and to critical infrastructures.

More performance.

The LANCOM 9100+ VPN (CC) offers a high-performance hardware platform, meeting high demands for network virtualization, security, and VPN connectivity. At the same time, memory capacity and high-speed interfaces guarantee high performance of networks, even at times of heavy data traffic.

More virtualization.

The LANCOM 9100+ VPN (CC) helps you to use your IT resources more efficiently and to save costs. The device simultaneously supports multiple independent networks. This is made possible by the powerful technology Advanced Routing and Forwarding (ARF). The ARF function on the LANCOM 9100+ VPN (CC) provides up to sixteen virtual networks, each with its own settings for routing and firewall.

The LANCOM security pledge.

LANCOM Systems GmbH is a German enterprise, with German management board, which is not subject to legal regulations or the influence of other states, requiring the implementation of backdoors or allow the sniffing of unencrypted data. The LANCOM portfolio for high-security site connectivity provides networks of enterprises and public authorities a comprehensive, guaranteed backdoor-free, and BSI-certified protection (CC EAL 4+) against cyber attacks.

LANCOM 9100+ VPN (CC)

Features as of: LCOS 8.70 CC

Firewall	
Packet filter	Check based on the header information of an IP packet (IP or MAC source/destination addresses; source/destination ports, DiffServ attribute); remote-site dependant and direction dependant
Extended port forwarding	Network Address Translation (NAT) based on protocol and WAN address, i.e. to make internal webservers accessible from WAN
N:N IP address mapping	N:N IP address mapping for translation of IP addresses or entire networks
Tagging	The firewall marks packets with routing tags, e.g. for policy-based routing
Actions	Forward, drop, reject, block sender address, close destination port, disconnect
Notification	SYSLOG (internally)
Security	
Intrusion Prevention	Monitoring and blocking of login attempts and port scans
IP spoofing	Source IP address check on all interfaces: only IP addresses belonging to the defined IP networks are allowed
Access control lists	Filtering of IP or MAC addresses and preset protocols for configuration access
Denial of Service protection	Protection from fragmentation errors and SYN flooding
General	Detailed settings for handling reassembly, PING, stealth mode and AUTH port
Password protection	Password-protected configuration access can be set for each interface
Alerts	Alerts via SYSLOG (internally)
Authentication mechanisms	PAP, CHAP, MS-CHAP and MS-CHAPv2 as PPP authentication mechanism
Adjustable reset button	Adjustable reset button for 'ignore', 'boot-only' and 'reset-or-boot'
High availability / redundancy	
FirmSafe	For completely safe software upgrades thanks to two stored firmware versions, incl. test mode for firmware updates
VPN redundancy	Backup of VPN connections across different hierarchy levels, e.g. in case of failure of a central VPN concentrator and re-routing to multiple distributed remote sites. Any number of VPN remote sites can be defined (the tunnel limit applies only to active connections). Up to 32 alternative remote stations, each with its own routing tag, can be defined per VPN connection. Automatic selection may be sequential, or dependant on the last connection, or random (VPN load balancing)
Line monitoring	Line monitoring with LCP echo monitoring, dead-peer detection and up to 4 addresses for end-to-end monitoring with ICMP polling
VPN	
Number of VPN tunnels	Max. number of active IPSec tunnels: 200 (500 / 1000 with VPN-500 / VPN-1000 Option). Unlimited configurable connections. Configuration of all remote sites via one configuration entry when using the RAS user template or Proadaptive VPN.
Hardware accelerator	Integrated hardware acceleration for ESP encryption and decryption (data path)
Realtime clock	Integrated, buffered realtime clock to save the date and time during power failure. Assures timely validation of certificates in any case
Random number generator	Generates high-quality randomized numbers in software
IKE	IPSec key exchange with Preshared Key or certificate (in software)
Certificates	X.509 digital self signed certificate support, compatible with OpenSSL, upload of PKCS#12 files via SCP. Secure Key Storage protects a private key (PKCS#12) from theft
RAS user template	Configuration of all VPN client connections in IKE ConfigMode via a single configuration entry
Proadaptive VPN	Automated configuration and dynamic creation of all necessary VPN and routing entries based on a default entry for site-to-site connections. Propagation of routes via RIPv2 if required
Algorithms	AES (128, 192 or 256 bit) and HMAC with SHA-1 / SHA-256 hashes
NAT-Traversal	NAT-Traversal (NAT-T) support for VPN over routes without VPN passthrough
VPN throughput (max., AES)	
1418-byte frame size UDP	576 Mbps
Firewall throughput (max.)	
1518-byte frame size UDP	986 Mbps
Routing functions	
Router	IP-Router

LANCOM 9100+ VPN (CC)

Features as of: LCOS 8.70 CC

Routing functions	
Advanced Routing and Forwarding	Separate processing of 256 contexts due to virtualization of the routers. Mapping to VLANs and complete independent management and configuration of IP networks in the device. Automatic learning of routing tags for ARF contexts from the routing table
Policy-based routing	Policy-based routing based on routing tags. Based on firewall rules, certain data types are marked for specific routing, e.g. to particular remote sites or lines
Dynamic routing	Propagating routes; separate settings for LAN and WAN. Extended RIPv2 including HopCount, Poisoned Reverse, Triggered Update for LAN (acc. to RFC 2453) and WAN (acc. to RFC 2091) as well as filter options for propagation of routes. Definition of RIP sources with wildcards
Layer 2 functions	
VLAN	VLAN ID definable per interface and routing context (4,094 IDs) IEEE 802.1Q
ARP lookup	Packets sent in response to LCOS service requests (SSH) via Ethernet can be routed directly to the requesting station (default) or to a target determined by ARP lookup
LAN protocols	
IP	ARP, Proxy ARP, IP, ICMP, PPPoE (Server), RIP-2 (Propagation), TCP, UDP
WAN protocols	
Ethernet	PPPoE, Multi-PPPoE, ML-PPP, IPoE, VLAN, IP
xDSL (ext. modem)	ADSL1, ADSL2 or ADSL2+ with external ADSL2+ modem
Interfaces	
Ethernet ports	4 individual 10/100/1000 Mbps Ethernet ports; up to 3 ports can be switched as additional WAN ports with load balancing. Ethernet ports can be electrically disabled within LCOS configuration
Port configuration	Each Ethernet port can be freely configured (LAN, DMZ, WAN, monitor port, off). Additionally, external DSL modems or termination routers can be operated as a WAN port with load balancing and policy-based routing.
Serial interface	Serial configuration interface / COM port (8 pin Mini-DIN): 9,600 - 115,000 baud
Management	
Device Syslog	Syslog buffer in the RAM (size depending on device memory) to store events for diagnosis. Default set of rules for the event protocol in Syslog. The rules can be modified by the administrator. Display and saving of internal Syslog buffer (events) from LANCOM devices.
Remote maintenance	Remote configuration with SSH in software
SSH & Telnet client	SSH-client function (in software) compatible to Open SSH under Linux and Unix operating systems for accessing third-party components from a LANCOM router. Also usable when working with SSH to login to the LANCOM device. Support for certificate- and password-based authentication. SSH client functions are restricted to administrators with appropriate rights.
Security	Access rights (read/write) over WAN or LAN can be set up separately (SSH), access control list
Scripting	Scripting function for batch-programming of all command-line parameters and for transferring (partial) configurations, irrespective of software versions and device types, incl. test mode for parameter changes. Utilization of timed control (CRON) or connection establishment and termination to run scripts for automation.
Timed control	Scheduled control of parameters and actions with CRON service
Diagnosis	Extensive LOG and TRACE options, PING and TRACEROUTE for checking connections, internal logging buffer for firewall events, monitor mode for Ethernet ports
Statistics	
Statistics	Extensive Ethernet and IP statistics
Accounting	Connection time, online time, transfer volumes per station. Snapshot function for regular read-out of values at the end of a billing period. Timed (CRON) command to reset all counters at once
Hardware	
Power supply	Internal power supply unit (110–230 V, 50-60 Hz)
Environment	Temperature range 5–40° C; humidity 0–95%; non-condensing
Housing	Robust metal housing, 19' 1 HU, 435 x 45 x 207 mm, with removable mounting brackets, network connectors on the front
Fans	1
Power consumption (max)	30 Watt
Declarations of conformity	
CE	EN 60950-1, EN 55022, EN 55024

LANCOM 9100+ VPN (CC)

Features as of: LCOS 8.70 CC

Declarations of conformity	
CC certification	LCOS Certifcation based on Common Criteria for Information Technology Security Evaluation (CC EAL 4+) with test number "BSI-DSZ-CC-0815" at the German Federal Office for Information Security
Package content	
Manual	Printed User Manual (DE, EN) and Installation Guide (DE/EN/FR/ES/IT/PT/NL)
Reference manual	Printed LCOS reference manual
CD/DVD	Data medium with firmware, management software (LANconfig, LANmonitor, LANCAPI) and documentation
Cable	Serial configuration cable, 1.5m
Cable	2 Ethernet cables, 3m
Cable	IEC power cord
Support	
Warranty	4 years
Options	
VPN	LANCOM VPN-500 Option (500 channels), item no. 61402
VPN	LANCOM VPN-1000 Option (1000 channels), item no. 61403
Item numbers	
LANCOM 9100+ VPN (EU, CC)	62608