



. . . c o n n e c t i n g   y o u r   b u s i n e s s

## LANCOM 7100 VPN (CC)

Central site VPN gateway for networking up to 200 sites

- Provides 100 VPN channels, upgradable to 200 remote sites
- 4 x Gigabit Ethernet + ISDN BRI
- load balancing
- Advanced Routing & Forwarding with 128 VLAN / IP contexts
- Status and error display

The LANCOM 7100 VPN is a central-site VPN gateway which provides VPN connections for up to 100 sites as standard, upgrading to 200 sites with the LANCOM VPN Option. Quality-of-Service, dynamic bandwidth management and the four Gigabit-Ethernet ports ensure that data is correctly prioritized in the network and that speeds are maximized. Integrated VPN accelerator hardware massively increases the encryption performance of this powerful platform. Practical: Various information on the device is permanently displayed, including temperature, CPU load, and active VPNs. The fan's function is permanently displayed by LED and, additionally, an acoustic signal is emitted should the CPU overheat.

#### **More security.**

The integrated firewall with the latest security functions such as stateful inspection, intrusion detection and denial-of-service protection is supplemented by dynamic bandwidth management and comprehensive backup, high-availability and redundancy functions over ISDN and VRRP. VPN that uses the IPSec standard provides optimal security for connecting branches and home offices thanks to the high-security 3-DES or AES encryption, integrated hardware acceleration and support of digital certificates.

#### **More management.**

LCMS, the LANCOM Management System, is a free software package for the Microsoft Windows operating system for the configuration, remote maintenance and real-time monitoring of all LANCOM routers, central-site gateways, access points, WLAN controllers and managed switches. LANconfig is an application for remote configuration via HTTP, HTTPS, TFTP or ISDN dial-up. It offers easy-to-use wizards that cater for everything from the basic setup to the configuration of VPN connections, but it can also handle the fine-tuning of individual device parameters. A single LCMS installation can handle the monitoring and maintenance of any of the various LANCOM devices. LANmonitor offers detailed, real-time monitoring of parameters, it provides access to log files and statistics, and it can carry out a detailed trace-protocol analysis. Along with convenient functions such as the firewall GUI for object-orientated firewall programming, a range of professional functions help with the administration of projects, including the automatic configuration backup, saving and uploading scripts, a folder-based organization, and a dynamic search filter. Service providers benefit from the broad range of scripting methods and professional access with individual access rights for administrators via SSH, HTTPS, TFTP, telnet and ISDN dial-in. Rollouts and operations are assisted by the automatic upload of configurations and firmware from USB data media and the option of storing project-specific boot configurations in place of the standard factory settings—all of which offers big potential savings on expensive manual maintenance.

#### **More benefits.**

The versatile functions for address translation and routing allow completely different networks to be connected over common infrastructure. Thanks to the LANCOM Advanced and Routing concept, professional network virtualization is easy: Existing networks at partner companies, home-office workstations or subsidiaries can be integrated into the VPN without problem.

#### **More virtualization.**

Advanced Routing and Forwarding (ARF) from LANCOM is a unique technology for network virtualization. It enables different logical networks, each with their own settings for DHCP, DNS, routing and firewall, to operate on a single device and share the same physical infrastructure. For example, networks in the LAN can be assigned to different VLANs, tagged in the WAN or assigned to different RAS connections. The innovative Tunnel-in-Tunnel technology for VPN allows different networks between LANCOM routers to be completely isolated even over a shared IPSec-VPN connection—even with overlapping IP-address ranges. ARF is suitable for the cross-site separation of logical networks, for example where different applications or service providers work on shared infrastructure. Conflicts can be completely avoided. Incursions from one logical network to another, either intentionally or by accident, are effectively prevented by ARF. In particular for companies located at multiple sites, ARF enables the switch to a purely IP-based infrastructure, so offering considerable potential savings in operations.

**More reliability for the future.**

From the very start, LANCOM products are designed for a product life of several years. They are equipped with hardware dimensioned for the future. Even reaching back to older product generations, updates to the LANCOM Operating System—LCOS—are available several times a year, free of charge and offering major features. LANCOM offers unbeatable protection of your investment!

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 webserver 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; Source routing tags for the creation of independent firewall rules for different ARF contexts
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: 100. 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 certificates (no CA 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
Routing functions	
Router	IP-Router
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

Routing functions	
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
WAN operating mode	
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 operated 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 Watts
Declarations of conformity*	
CE	EN 60950-1, EN 55022, EN 55024
CC certification	LCOS Certification based on Common Criteria for Information Technology Security Evaluation (CC EAL 4+) with certificate number "BSI-DSZ-CC-0815" at the German Federal Office for Information Security

Declarations of conformity*	
*) Note	You will find all declarations of conformity in the products section of our website at <a href="http://www.lancom-systems.de/en">www.lancom-systems.de/en</a>
Scope of delivery	
Manual	Printed User Manual (DE, EN) and Installation Guide (DE/EN/FR/ES/IT/PT/NL)
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	3 years
Options	
VPN	LANCOM VPN-200 Option (200 channels), item no. 61404
Warranty Extension	LANCOM Warranty Basic Option L, item no. 10712
Warranty Extension & Advanced Replacement	LANCOM Warranty Advanced Option L, item no. 10717
Accessories	
LANCOM CC Start-up Kit	All-in-one package for the certified start-up and highly secure configuration of LANCOM CC products based on CC EAL 4+, item no. 62910
Item number(s)	
LANCOM 7100 VPN (EU, CC)	62605