



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

LANCOM 8011 VPN

Central-Site-VPN-Gateway für Vernetzung von bis zu 1.000 Standorten

- Dynamic VPN Gateway für bis zu 200 Gegenstellen
- Aufrüstbar auf bis zu 500/1000 simultane VPN-Kanäle
- Display zur Statusanzeige
- 5 frei konfigurierbare 10/100 Mbit/s Ports für LAN, WAN, DMZ
- Quality of Service mit dynamischem Bandbreitenmanagement und Traffic Shaping
- Load Balancing mit bis zu 4 Breitbandanschlüssen
- ISDN für Dynamic VPN, Remote Access, Fernwartung und LANcapi
- Hochverfügbarkeit via Dynamic VPN Endpoint, RIP, ISDN, Modem und VRRP
- VPN-Hardware-Beschleunigung für die 3-DES/AES-Ver- und Entschlüsselung

LANCOM 8011 VPN ist das Topmodell der hochintegrierten LANCOM-VPN-Vernetzungskomponenten und dient als Central Site VPN-Gateway für mittlere und größere Standorte.

Mit dem VPN-Hardwarebeschleuniger, professionellem Quality of Service und Load Balancing für bis zu vier WAN-Anschlüsse bietet der hochleistungsfähige VPN-Router genügend Kapazität für breitbandige Standortkopplung und mobile VPN-Einwahlzugänge. Werksseitig bereits mit 200 VPN-Kanälen ausgestattet, kann LANCOM 8011VPN auf die Unterstützung von bis zu 500 bzw. 1000 Gegenstellen aufgerüstet werden.

Einen besonderen Vorteil bietet die IPSec-Erweiterung LANCOM Dynamic VPN, die jederzeit einen aktiven Verbindungsaufbau zu Außenstellen mit dynamischer IP-Adresse ermöglicht – selbst dann, wenn die Gegenstelle nicht "always on" ist.

Mehr Sicherheit.

Die integrierte Firewall mit aktuellsten Sicherheitsfunktionen wie Stateful-Inspection, Intrusion-Prevention und Denial-of-Service-Protection wird durch dynamisches Bandbreitenmanagement sowie umfangreiche Backup-, High-Availability- und Redundanzfunktionen über ISDN und VRRP ergänzt. Die VPN-Unterstützung nach IPSec-Standard mit hochsicherer 3-DES- oder AES-Verschlüsselung, integrierter Hardwarebeschleunigung und der Unterstützung digitaler Zertifikate sorgt für optimale Sicherheit bei der Anbindung von Filialen und Teleworkern.

Mehr Management.

Die mitgelieferten Managementsysteme LANconfig und LANmonitor bieten neben kostengünstiger Fernwartung ganzer Installationen und besonders komfortablen Setup-Assistenten auch eine vollständige Echtzeitüberwachung und -Protokollierung. Darüber hinaus stehen für Service-Provider umfangreiche Scripting-Methoden sowie professionelle Managementzugänge mit individuellen Zugriffsrechten über SSH, HTTPS, TFTP und ISDN-Einwahl zur Verfügung.

Mehr Nutzen.

Dank vielseitiger Adressumsetzungs- und Routingfunktionen können unterschiedlichste Netze problemlos über ein und dieselbe Infrastruktur angebunden werden. Bestehende Netzwerke von Partnerunternehmen, Heimarbeitsplätzen oder Filialen werden so problemlos in ein VPN integriert. Durch die Möglichkeit der Port-Separierung und einen separaten Adresskreis können auch eigene Web-Server sicher vom LAN getrennt betrieben werden.

Die integrierte ISDN-Schnittstelle bietet Ferninbetriebnahme, Einwahlzugänge und CAPI-Komfortfunktionen wie z.B. Fax-Dienste für alle angeschlossenen PCs.

Mehr Zukunftssicherheit.

LANCOM-Produkte sind grundsätzlich auf eine langjährige Nutzung ausgelegt und verfügen daher über eine zukunftssichere Hardware-Dimensionierung. Selbst über Produktgenerationen hinweg sind Updates des LANCOM Operating Systems – LCOS – mehrmals pro Jahr kostenfrei erhältlich, inklusive "Major Features". LANCOM bietet so einen unvergleichlichen Investitionsschutz!

| | |
|--------------------------------------|--|
| Firewall | |
| Stateful Inspection Firewall | Richtungsabhängige Prüfung anhand von Verbindungsinformationen |
| Paketfilter | Prüfung anhand der Header-Informationen eines Pakets (IP oder MAC Quell-/Zieladressen; Quell-/Zielports, DiffServ-Attribut); gegenstellenabhängig, richtungsabhängig, bandbreitenabhängig |
| Erweitertes Port-Forwarding | Network Address Translation (NAT), optional auch abhängig von Protokolltyp und WAN-Adresse, um z.B. Webserver im LAN von außen verfügbar zu machen |
| N:N IP-Adressumsetzung | N:N-Mapping zum Umsetzen oder Verstecken von IP-Adressen oder ganzen Netzwerken |
| Tagging | Markierung von Paketen in der Firewall mit Routing-Tags, z.B. für Policy-based Routing |
| Aktionen | Weiterleiten, Verwerfen, Zurückweisen, Absenderadresse sperren, Zielport schließen, Verbindung trennen |
| Benachrichtigungen | Via Email, SYSLOG oder SNMP-Trap |
| Quality of Service | |
| Traffic Shaping | Dynamisches Bandbreitenmanagement mit IP Traffic-Shaping |
| Bandbreitenreservierung | Dynamische Reservierung von Mindest- und Maximalbandbreiten, absolut oder verbindungsbezogen, für Sende- und Empfangsrichtung getrennt einstellbar |
| DiffServ/TOS | Priority-Queueing der Pakete anhand des DiffServ/TOS-Felds |
| Paketgrößensteuerung | Automatische Steuerung der Paketgrößen über Fragmentierung oder Path Maximum Transmission Unit (PMTU) Anpassung |
| Layer 2/Layer 3-Tagging | Automatisches oder festes Umsetzen von Layer-2-Prioritätsinformationen (802.1p markierte Ethernet-Frames) auf Layer-3-DiffServ-Attribute im Routing-Betrieb. Umsetzen von Layer 3 auf Layer 2 mit automatischer Erkennung der 802.1p-Unterstützung des Zielgerätes |
| Sicherheit | |
| Intrusion Prevention | Überwachung und Sperrung von Login-Versuchen und Portscans |
| IP-Spoofing | Überprüfung der Quell-IP-Adresse auf allen Interfaces: nur die IP-Adressen des zuvor definierten IP-Netzes werden akzeptiert |
| Access-Control Listen | Filterung anhand von IP- oder MAC-Adresse sowie zuvor definierten Protokollen für den Konfigurationszugang und LANCAPI |
| Denial-of-Service Protection | Schutz vor Fragmentierungsfehlern und SYN-Flooding |
| Allgemein | Detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung |
| URL-Blocker | Filtern von unerwünschten URLs anhand von DNS-Hitlisten sowie Wildcard-Filtern |
| Passwortschutz | Passwortgeschützter Konfigurationszugang für jedes Interface einstellbar |
| Alarmierung | Alarmierung durch Email, SNMP-Traps und SYSLOG |
| Authentifizierungsmechanismen | PAP, CHAP und MS-CHAP als PPP-Authentifizierungsmechanismen |
| Diebstahlschutz | Diebstahlschutz durch ISDN-Standortverifikation über den B- oder D-Kanal (Selbstanruf und ggf. Sperrung) |
| Progammierbarer Reset-Taster | Einstellbarer Reset-Taster für "ignore", "boot-only" und "reset-or-boot" |
| Hochverfügbarkeit / Redundanz | |
| VRRP | VRRP (Virtual Router Redundancy Protocol) zur herstellerübergreifenden Absicherung gegen Geräte- oder Gegenstellenausfall. Ermöglicht passive Standby-Gruppen oder wechselseitige Ausfallsicherung mehrerer aktiver Geräte inkl. Lastverteilung sowie frei einstellbare Backup-Prioritäten |
| FirmSafe | Für absolut sichere Software-Upgrades durch zwei speicherbare Firmware-Versionen, inkl. Testmodus bei Firmware-Updates |
| ISDN-Backup | Bei Ausfall der Hauptverbindung kann eine Backup-Verbindung über ISDN aufgebaut werden; automatische Rückkehr zur Hauptverbindung |
| Analog/GSM-Modem-Backup | Optionaler Analog/GSM-Modem-Betrieb an der seriellen Schnittstelle |
| Load-Balancing | Statische und dynamische Lastverteilung auf bis zu 4 WAN-Strecken; Kanalbündlung durch Multilink-PPP (sofern vom Netzbetreiber unterstützt) |
| VPN-Redundanz | Ansteuerung von bis zu 16 redundanten VPN-Gateways für Hochverfügbarkeit oder Lastverteilung |
| Leitungsüberwachung | Leitungsüberwachung mit LCP Echo Monitoring, Dead Peer Detection und bis zu 4 Adressen für Ende-zu-Ende-Überwachung mit ICMP-Polling |
| VPN | |
| 1-Click-VPN Client Assistent | Erstellung von VPN-Client-Zugängen mit gleichzeitiger Erzeugung von Profilen für den LANCOM Advanced VPN Client mit einem Click aus LANconfig heraus |
| 1-Click-VPN Site-to-Site | Erzeugen von VPN-Verbindungen zwischen LANCOM-Routern per "Drag and Drop" mit einem Click in LANconfig |
| Anzahl der VPN-Tunnel | 200 IPSec Verbindungen gleichzeitig aktiv (500 in Verbindung mit der VPN-500 Option, bzw. 1000 in Verbindung mit der VPN-1000 Option), 500 konfigurierbare Gegenstellen (800 in Verbindung mit der VPN-500 Option, bzw. 1500 in Verbindung mit der VPN-1000 Option). Konfiguration aller Gegenstellen über einen einzigen Eintrag möglich bei Nutzung RAS User Template oder Proadaptive VPN |
| Hardware-Beschleuniger | Integrierter Hardwarebeschleuniger für die 3-DES/AES Ver- und Entschlüsselung |
| IKE | IPSec Schlüsselaustausch über Preshared Key oder Zertifikate |

| | |
|------------------------------------|--|
| VPN | |
| Zertifikate | Unterstützung von X.509 digitalen mehrstufigen Zertifikaten, kompatibel z.B. zu Microsoft Server / Enterprise Server und OpenSSL, Upload von PKCS#12-Dateien über HTTPS-Interface und LANconfig |
| Zertifikatsrollout | Automatisierte Erzeugung sowie Rollout und Verlängerung von Zertifikaten mit SCEP (Simple Certificate Enrollment Protocol) |
| Certificate Revocation Lists (CRL) | Abruf von CRLs mittels HTTP |
| RAS User Template | Konfiguration aller VPN-Client-Verbindungen im IKE-Config-Mode über einen einzigen Konfigurationseintrag |
| Proadaptive VPN | Automatisierte Konfiguration und dynamisches Anlegen aller notwendigen VPN- und Routing-Einträge anhand eines Default-Eintrags bei Site-to-Site Verbindungen. Propagieren der dynamisch gelernten Routen kann auf Wunsch per RIPv2 erfolgen. |
| Algorithmen | 3-DES (168 Bit), AES (128, 192 und 256 Bit), DES, Blowfish (128-448 Bit) und CAST (128 Bit); MD-5 oder SHA-1 Hashes |
| NAT-Traversal | Unterstützung von NAT-Traversal (NAT-T) für den VPN-Einsatz auf Strecken, die kein VPN-Passthrough unterstützen |
| IPCOMP | VPN-Datenkompression für höhere IPSec-Durchsatzraten mittels LZS- oder Deflate-Komprimierung |
| LANCOM Dynamic VPN | Ermöglicht den VPN-Verbindungsaufbau von oder zu dynamischen IP-Adressen. IP-Adresse wird über ISDN B- oder D-Kanal übermittelt bzw. verschlüsselt mittels ICMP- oder UDP-Protokoll übertragen. Dynamische Einwahl von Gegenstellen mittels Verbindungs-Template |
| Dynamic DNS | Ermöglicht die Registrierung der IP-Adresse bei einem Dynamic DNS-Provider, falls keine feste IP-Adresse für den VPN-Verbindungsaufbau verwendet wird |
| Spezifisches DNS-Forwarding | DNS-Forwarding einstellbar pro DNS-Domäne, z.B. zur Auflösung interner Namen durch eigenen DNS-Server im VPN und Auflösung externer Namen durch Internet-DNS-Server. Eintrag für Backup-DNS pro DNS-Weiterleitung |
| VPN-Durchsatz (max.)* | |
| 1364 Byte Paketgröße | 61 Mbit/s |
| 265 Byte Paketgröße | 12 Mbit/s |
| *) Hinweis | alle VPN-Zahlen bei AES-Verschlüsselung |
| Firewall-Durchsatz (max.) | |
| 1470 Byte Paketgröße | 93 Mbit/s |
| 256 Byte Paketgröße | 23 Mbit/s |
| Routingfunktionen | |
| Router | IP-, IPX- und NetBIOS/IP-Multiprotokoll-Router |
| VLAN | VLAN-ID einstellbar pro Schnittstelle und Routing-Kontext (4094 IDs) |
| Q-in-Q Tagging | Unterstützung von geschachtelten 802.1q VLANs |
| Advanced Routing and Forwarding | Separates Verarbeiten von 64 Kontexten durch Virtualisierung des Routers. Abbildung in VLANs und vollkommen unabhängige Verwaltung und Konfiguration von IP-Netzen im Gerät möglich, d.h. individuelle Einstellung von DHCP, DNS, Firewalling, QoS, VLAN, Routing usw. |
| HTTP | HTTP- und HTTPS-Server für die Konfiguration per Webinterface |
| DNS | DNS-Client, DNS-Server, DNS-Relay, DNS-Proxy und Dynamic DNS-Client |
| DHCP | DHCP-Client, DHCP-Relay und DHCP-Server mit Autodetection |
| NetBIOS | NetBIOS/IP-Proxy |
| NTP | NTP-Client und SNTP-Server, automatische Sommerzeit-Anpassung |
| Policy-based Routing | Policy-based Routing auf Basis von Routing Tags. Anhand von Firewall-Regeln können bestimmte Daten so markiert werden, dass diese dann anhand ihrer Markierung gezielt vom Router z.B. nur auf bestimmte Gegenstellen oder Leitungen geroutet werden. |
| Dynamisches Routing | Dynamisches Routing mit RIPv2. Lernen und Propagieren von Routen, getrennt einstellbar für LAN und WAN. Extended RIPv2 mit HopCount, Poisoned Reverse, Triggered Update für LAN (nach RFC 2453) und WAN (nach RFC 2091) sowie Filtereinstellungen zum Propagieren von Routen |
| LAN-Protokolle | |
| IP | ARP, Proxy ARP, BOOTP, LANCAPI, DHCP, DNS, HTTP, HTTPS, IP, ICMP, NTP/SNTP, NetBIOS, PPPoE (Server), RADIUS, RIP-1, RIP-2, RTP, SIP, SNMP, TCP, TFTP, UDP, VRRP |
| IPX | RIP, SAP, IPX- und SPX-Watchdogs, NetBIOS Watchdogs |
| WAN-Protokolle | |
| Ethernet | PPPoE, Multi-PPPoE, ML-PPP, PPTP (PAC oder PNS) und Plain Ethernet (mit oder ohne DHCP), RIP-1, RIP-2, VLAN |
| ISDN | 1TR6, DSS1 (Euro-ISDN), PPP, X75, HDLC, ML-PPP, V.110/GSM/HSCSD, CAPI 2.0 über LANCAPI, Stac-Datenkompression |

| Schnittstellen | |
|-------------------------|---|
| WAN: Ethernet | 10/100 Mbit/s Fast Ethernet |
| Ethernet Ports | 4 individuelle Ports, 10/100 Mbit/s Ethernet, bis zu 3 Ports können als zusätzliche WAN-Ports inkl. Load-Balancing geschaltet werden |
| Port-Konfiguration | Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus). LAN Ports können als Switch oder isoliert betrieben werden. Als WAN-Port können zusätzliche externe DSL-Modems oder Netzabschlussrouter inkl. Load-Balancing und Policy-based Routing betrieben werden. DMZ-Ports können mit einem eigenen IP-Adresskreis ohne NAT versorgt werden |
| ISDN | ISDN-S0-Bus |
| Serielle Schnittstelle | Serielle Konfigurationsschnittstelle / COM-Port (8-pol. Mini-DIN): 9.600-115.000 Baud, optional zum Anschluss eines Analog-/GPRS-Modems geeignet |
| Management | |
| LANconfig | Konfigurationsprogramm für Microsoft Windows, inkl. komfortabler Setup-Assistenten. Möglichkeit zur Gruppenkonfiguration, gleichzeitige Fernkonfiguration und Management mehrerer Geräte via ISDN-Einwahl oder IP-Verbindung (HTTPS, HTTP, TFTP). Projekt- oder benutzerbezogene Einstellung des Konfigurationsprogramms |
| LANmonitor | Monitoring-Applikation für Microsoft Windows zur (Fern-)Überwachung und Protokollierung von Geräte- und Verbindungsstatus von LANCOM-Geräten, inkl. PING-Diagnose und TRACE mit Filtern und Speichern der Ergebnisse in eine Datei |
| Webconfig | Integrierter Webserver zur Konfiguration der LANCOM-Geräte über Internetbrowser mittels HTTPS oder HTTP |
| Zugriffsrechte | Individuelle Zugriffs- und Funktionsrechte für bis zu 16 Administratoren |
| Benutzerverwaltung | RADIUS-Benutzerverwaltung für Einwahlzugänge (PPP/PPTP und ISDN CLIP). Unterstützung von RADSEC (Secure RADIUS) zur sicheren Anbindung an RADIUS-Server |
| Fernwartung | Fernkonfiguration über Telnet/SSL, SSH (mit Passwort oder öffentlichem Schlüssel), Browser (HTTP/HTTPS), TFTP oder SNMP; Firmware-Upload über HTTP/HTTPS oder TFTP. Zum Fernzugriff auf Komponenten hinter dem LANCOM können nach Authentifizierung beliebige TCP-basierte Protokolle getunnelt werden (z.B. für einen HTTP(S)-Zugriff auf VoIP-Telefone oder Drucker im LAN) |
| ISDN Fernwartung | Fernwartung über ISDN-Einwahl mit Rufnummernüberprüfung |
| Sicherheit | Zugriff über WAN oder (W)LAN, Zugangsrechte (lesen/schreiben) separat einstellbar (VPN only, Telnet/SSL, SSH, SNMP, HTTPS/HTTP), Access Control List |
| Scripting | Scripting-Funktion zur Batch-Programmierung von allen Kommandozeilenparametern und zur Übertragung von (Teil-)Konfigurationen über unterschiedliche Softwarestände und Gerätetypen, inkl. Testmodus für Parameteränderungen |
| SNMP | SNMP-Management via SNMP V2, private MIB per WEBconfig exportierbar, MIB II |
| Zeitsteuerung | Zeitliche Steuerung aller Parameter und Aktionen durch CRON-Dienst. Aktionen können "unscharf", d.h. mit zufälliger Zeitvarianz ausgeführt werden. |
| TFTP | TFTP-Client und -Server mit variablen Dateinamen (Name, MAC-/IP-Adresse, Seriennummer) |
| Diagnose | Sehr umfangreiche LOG- und TRACE-Möglichkeiten, PING und TRACEROUTE zur Verbindungsüberprüfung, LANmonitor Zustandsanzeige, interne Loggingbuffer für SYSLOG und Firewall-Events, Monitor-Modus für Ethernet-Ports |
| Statistiken | |
| Statistiken | Umfangreiche Ethernet-, IP- und DNS-Statistiken; SYSLOG-Fehlerzähler |
| Accounting | Verbindungs- und Onlinezeit sowie Übertragungsvolumen pro Station. Snapshot-Funktion zum regelmäßigen Auslesen der Werte am Ende einer Abrechnungsperiode. |
| Export | Accounting-Information exportierbar via LANmonitor und SYSLOG |
| Hardware | |
| Spannungsversorgung | Internes Netzteil (110–230 V, 50-60 Hz) |
| Umgebung | Temperaturbereich 5–40°C; Luftfeuchtigkeit 0–95%; nicht kondensierend |
| Gehäuse | Robustes Metallgehäuse, 19" 1 HE mit abschraubbaren Montagewinkeln, Netzwerkanschlüsse auf der Frontseite |
| Anzahl Lüfter | Keine; lüfterloses Design ohne rotierende Teile, mit hoher MTBF |
| Konformitätserklärungen | |
| CE | EN 55022, EN 55024, EN 60950 |
| Lieferumfang | |
| Handbuch | Gedrucktes Benutzerhandbuch (DE, EN) und Quick Installation Guide (DE/EN/FR/ES/IT/PT/NL) |
| Referenzhandbuch | Gedrucktes LCOS Referenzhandbuch |
| CD | CD mit Firmware, Management-Software (LANconfig, LANmonitor, LANCAPI) und Dokumentation |
| Kabel | Seriell Konfigurationskabel, 1,5 m |
| Kabel | 2 Ethernet-Kabel, 3m |
| Kabel | ISDN-Kabel, 3m |
| Kabel | Kaltgeräte-Netzkabel |

| Support | |
|------------------------|---|
| Garantie | 3 Jahre Support über Hotline und Internet KnowledgeBase |
| Software-Updates | Regelmäßige kostenfreie Updates (LCOS Betriebssystem und Management-Tools) via Internet |
| Optionen | |
| VPN | LANCOM VPN-500 Option (500 Kanäle), Art.-Nr. 61402 |
| VPN | LANCOM VPN-1000 Option (1000 Kanäle), Art.-Nr. 61403 |
| Service | LANCOM Service Option (24h-Vorabaustausch innerhalb Deutschlands, 4 Jahre Garantie, nicht für PoE Power Injector), Art.-Nr. 61401 |
| Zubehör | |
| Backup-Modem-Anschluss | LANCOM Modem-Adapter-Kit, Art.-Nr. 61500 |
| VPN-Client-Software | LANCOM Advanced VPN Client für Windows® 2000, Windows® XP, Windows Vista™, 1er Lizenz, Art.-Nr. 61600 |
| VPN-Client-Software | LANCOM Advanced VPN Client für Windows® 2000, Windows® XP, Windows Vista™, 10er Lizenz, Art.-Nr. 61601 |
| VPN-Client-Software | LANCOM Advanced VPN Client für Windows® 2000, Windows® XP, Windows Vista™, 25er Lizenz, Art.-Nr. 61602 |
| Artikelnummern | |
| LANCOM 8011 VPN | 61053 |
| LANCOM 8011 VPN UK | 61054 |

LANCOM, LANCOM Systems und LCOS sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Änderungen vorbehalten. Keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen. 07/08