

...connecting your business



## **LANCOM** DYNAMIC VPN SOLUTIONS

Kostengünstige Standortvernetzung mit System –  
Gesicherte Daten- und Sprachübertragung (VoIP)

- ▶ Anbindung von nationalen und internationalen Standorten
- ▶ Anbindung von Home- oder Mobile Offices
- ▶ Anbindung von Partnerunternehmen, Kunden oder Lieferanten

**LANCOM**  
Systems

# LANCOM SYSTEMS – DYNAMIC VPN SOLUTION GUIDE



---

## VIRTUELLE PRIVATE NETZWERKE

### Innovative Lösungen, die sich rechnen

Unternehmensweite Kommunikation ist zu einem wichtigen Faktor für den geschäftlichen Erfolg geworden. Informationen, Datenbanken oder Arbeitsunterlagen sollen für alle Mitarbeiter schnell erreichbar sein, ohne dass Betriebsfremde darauf zugreifen können. Je weiter sich ein Unternehmensnetzwerk spannt und je höher die Anforderungen einzelner Anwendungen an die Übertragungsqualität sind, desto wichtiger wird eine innovative und kundenspezifische Lösung.

Ein Virtuelles Privates Netzwerk (VPN) bietet hierzu weitreichende Möglichkeiten. Ein VPN ist ein geschlossenes logisches Netz, welches die einzelnen Punkte einer bestimmten Benutzergruppe über ein vorhandenes Netz wie z.B. das Internet miteinander verbindet. Mit der Nutzung des Internet durch IPSec-basierte VPN-Lösungen als Unternehmensbackbone ergeben sich vielfältige Vorteile. Die große Wirtschaftlichkeit ist eines der stärksten Argumente für innovative Standortvernetzung. Dies ist auch interessant für kleine und mittlere Unternehmen, die bisher aus Kostengründen auf eine unternehmensweite Netzinfrastruktur verzichtet haben.

### Jederzeit und überall verbunden

Viele Unternehmen nutzen bereits sichere Kommunikationslösungen, um die Flexibilität der Mitarbeiter zu erhöhen. Jederzeit und überall können Mitarbeiter auf Informationen zugreifen und Prozesse steuern. Durch den Einsatz eines VPN ist es möglich, dass sich z.B. ein Dienstreisender oder auch ein Mitarbeiter im Home Office unter Nutzung des Internets in das Firmennetzwerk einwählt. Die Mobilität wird deutlich erhöht: Mit jeder beliebigen Zugangstechnologie wie z.B. einem einfachen Internetzugang ist die Einwahl in das Unternehmensnetzwerk möglich. Außerdem eignet sich ein VPN für die Vernetzung regionaler und überregionaler, nationaler und internationaler Standorte oder zur kontrollierten Anbindung an bzw. von Partnerunternehmen, Kunden oder Lieferanten.

### Wirtschaftlichkeit

Realer Nutzen Virtueller Privater Netzwerke ist zweifels- ohne die Wirtschaftlichkeit: VPN-Lösungen sind nicht nur

bezahlbar, sondern nutzen gemeinsame Netzressourcen und fortschrittliche Technologie. Sie integrieren Daten, Sprache und Multimedia, ermöglichen universelle Zugangsschnittstellen und bieten ein Maximum an Flexibilität und Skalierbarkeit, was beispielsweise Ausdehnung und Anschlussverfahren betrifft. Und sie sind zukunftssicher, da sie auf den verbreiteten IP- und Internet-Standards basieren.

Beispiel: Eine Handelsgesellschaft mit rund 21 Standorten in sechs europäischen Ländern möchte die Netzinfrastruktur optimieren, um die Erreichbarkeit für die Kunden zu steigern und die Kosten zu senken. Für eine kundenorientierte, minutenaktuelle Auftragsbearbeitung ist die überregionale Einbindung aller Standorte notwendig. Der Ausbau der bestehenden Netzinfrastruktur erfolgt durch ein überregionales IP-VPN mit LANCOM-Technologie. Die Sprach- und Datenkommunikation der Standorte mit der Firmenzentrale kann im IP-VPN erheblich verbessert werden:

- ▶ Durch den Verzicht auf teure Standleitungen (ca. 1600 Euro/Monat) und den Abschluss einer DSL-Flatrate (ab 30 Euro/Monat) können die Netzkosten maßgeblich gesenkt werden
- ▶ Optimale Datenintegration wie z.B. Warenwirtschaftssystem und Unified Messaging Server
- ▶ Sprachvermittlung über das Internet als absolut günstige Möglichkeit national und europaweit zu telefonieren

### Sicherheit

Auch für Unternehmen mit weit verstreuten Standorten und komplexen Kommunikationsbeziehungen zeigt ein VPN seine volle Leistungsstärke: Mitarbeiter können geschützt miteinander kommunizieren und über verteilte Standorte hinweg eng zusammenarbeiten. Abhörsichere Authentifizierungsverfahren und extrem starke Verschlüsselungen (IPSec) sichern die Vertraulichkeit und Integrität der unternehmensinternen Daten trotz Übertragung durch das Internet. Mit IPSec existiert ein Standard, der skalierbare Sicherheit in VPNs durch unterschiedliche Dienste und Verschlüsselungs- und Authentisierungsverfahren (Zertifikate) bietet. Dieser Standard ist im Behörden- und Bankenumfeld anerkannt.

# LANCOM SYSTEMS

---

...connecting your business



---

## Sicherheit

Alle LANCOM VPN Produkte und Lösungen basieren auf dem IPSec-Standard und bieten die höchste Sicherheitsstufe. Die Authentifizierung erfolgt über Passworte oder digitale Zertifikate. Umfangreiche Firewall-Features wie Stateful-Inspection, Intrusion-Detection und Schutz vor Denial-of-Service Angriffen sind Bestandteil des zum LANCOM-Sicherheitsstandards dazu.

## Qualität

LANCOM VPN-Produkte und Lösungen basieren auf dem von LANCOM entwickelten Dynamic-VPN Verfahren. VPN-Gateways von LANCOM stehen seit über 10 Jahren für zuverlässige, hochwertige Qualität und innovative, marktgerechte Produkte. LANCOM gewährt bis zu 4 Jahren Garantie auf alle LANCOM Access Points, Router und Gateways.

## LCOS

LANCOM VPN-Gateways basieren auf High-Speed RISC-Prozessoren und laufen unter LCOS (LANCOM Operating System). LCOS bietet einen einheitlichen Funktionsumfang aller LANCOM-Produkte und eine komfortable Konfiguration über die Windows-Tools LANconfig und LANmonitor sowie plattformunabhängig per Browser (WEBconfig).

## Netzwerkmanagement mit den LANtools

Die LANtools (bestehend aus LANconfig und LANmonitor) eignen sich hervorragend zum Konfigurieren und Überwachen von LANCOM-Geräten in komplexen Anwendungsszenarien. Mehrere Router bzw. Gateways in einem Netzwerk können dabei genauso von einer zentralen Stelle aus administriert werden wie Geräte in verteilten Netzwerken, z.B. bei den Kunden eines Dienstleisters.

## Diagnose mit dem LANmonitor

Mit dem Überwachungstool LANmonitor lassen sich unter Windows-Betriebssystemen die wichtigsten Informationen über den Status der Gateways auf dem Bildschirm anzeigen. Und zwar den Status aller LANCOM-Geräte im Netz. So ist beispielsweise der Datenverkehr auf den verschiedenen Schnittstellen der Gateways ablesbar und gibt wichtige Hinweise darüber, mit welchen Einstellungen der Datenverkehr optimiert werden kann.

## Quality-of-Service

Quality-of-Service gewährleistet, dass bestimmte Datenpakete entweder besonders sicher oder möglichst sofort übertragen werden. Bei der Übertragung von Daten steht die Sicherheit und Vollständigkeit im Vordergrund. Bei der Übertragung von Sprache bei z.B. der Telefonie über das Internet ist es viel wichtiger, dass die Sprachpakete mit möglichst geringer zeitlicher Verzögerung beim Empfänger eintreffen.

## Hochverfügbarkeit

LANCOM bietet ein redundantes Hochverfügbarkeitskonzept: höhere Bandbreiten und mehr Geschwindigkeit. Load Balancing und High Availability Lösungen überwachen den Datenverkehr in Unternehmensnetzen sowie im Internet und verteilen Informationen gleichmäßig je nach Verfügbarkeit der Router.

## Backup Möglichkeiten

Mit LANCOM VPN-Gateways steht zusätzlich zu ISDN oder DSL auch der Mobilfunk (GPRS/UMTS) oder das analoge Modem als Backup-Möglichkeit bereit. Sollte die Hauptleitung des Netzwerkes ausfallen, weicht das Gateway alternativ auf eine ISDN-, DSL-, GPRS- oder Analog-Verbindung aus. Die Umschaltung auf Backup-Betrieb und wieder zurück erfolgt völlig automatisch.

## Investitionssicherheit

Investition in LANCOM Produkte und Lösungen bedeutet langfristige Produktivitätssteigerung. Durch kostenlos verfügbare Software-Updates ist jederzeit ein Update auf neue Standards und Features möglich. LANCOM Produkte sind auf eine langjährige Nutzung ausgelegt und verfügen über zukunftssichere Dimensionierung von Rechenleistung und Speicher.

## Service

Alle Software-Updates für LANCOM VPN-Gateways (über Produktgenerationen hinweg) werden mehrmals pro Jahr kostenfrei im Internet zur Verfügung gestellt. Technischen Support bekommen Kunden und Partner direkt von LANCOM per Telefon-Hotline, per E-Mail oder per Internet.

# LANCOM SYSTEMS – VIRTUELLE PRIVATE NETZWERKE

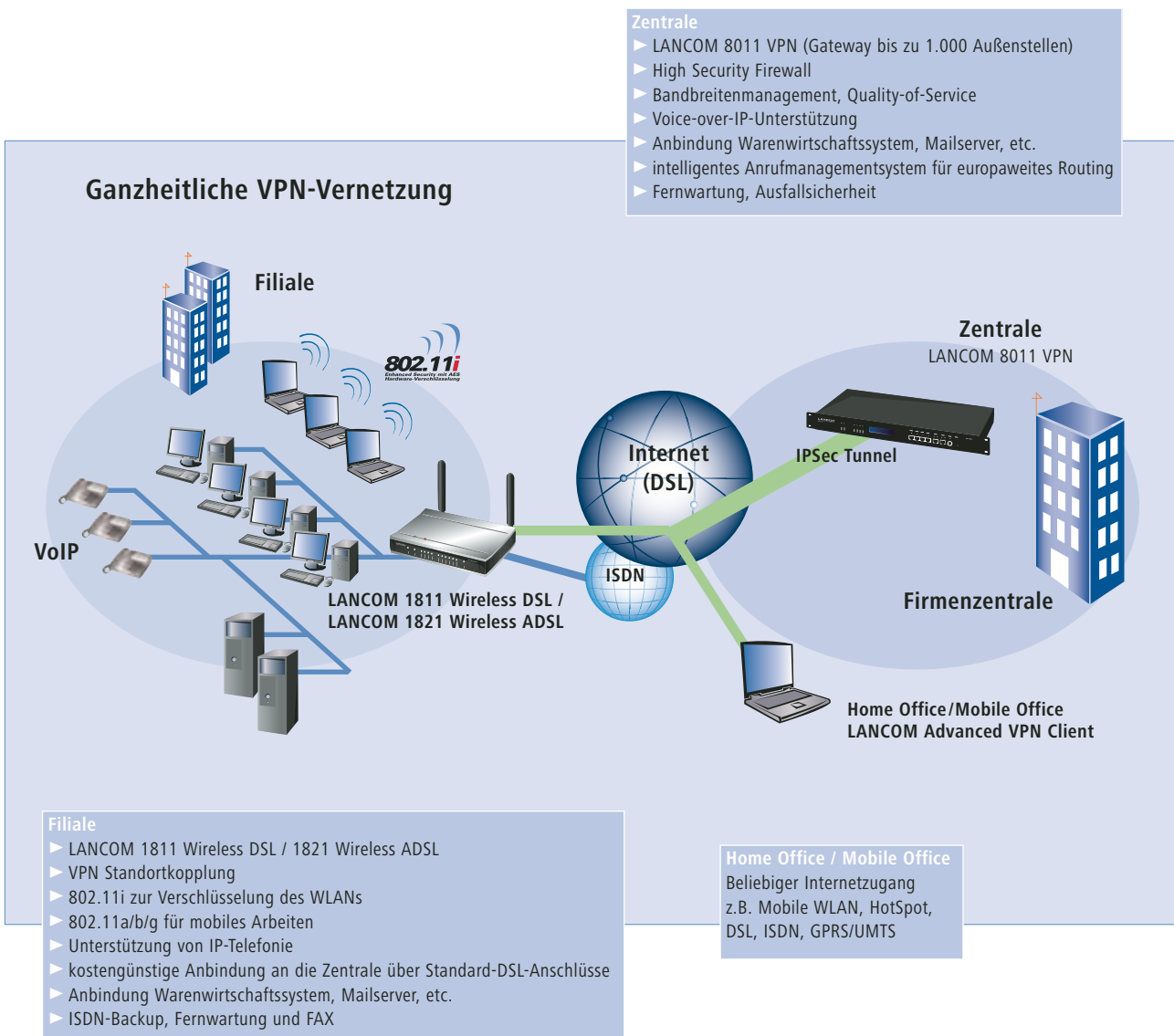
## VPN – Einsatzgebiete

Es gibt verschiedene Gründe, warum ein Unternehmen VPN als Alternative zu konventionellen Netzwerkstrukturen einsetzen sollte. Neben dem Wunsch IT- und TK-Kosten zu senken, sind Faktoren wie der Aufbau einer flexiblen Arbeitsplatzstruktur (z.B. Home Offices) oder der Umzug bzw. Neueinzug in ein Gebäude wichtig. Auslösend können jedoch auch die Kapazitätsgrenzen des bestehenden Netzwerkes sein.

Die Umstellung auf ein VPN erfolgt in der Regel sukzessive. Basierend auf der vorhandenen IT-Infrastruktur wird ein Migrationsplan erarbeitet, um die bereits getätigten und neuen Investitionen zu sichern. Bestehende Netzwerke können mit LANCOM-Produkten und -Lösungen problemlos mit-

tels der integrierten N:N-Adressumsetzung migriert werden. Die technische Ausstattung in der Unternehmenszentrale wird maßgeblich reduziert.

Ein VPN sorgt für eine vereinfachte, allgegenwärtige Kommunikation zwischen allen Teilnehmern eines Netzwerkes. Anstatt auf ein dediziertes Netzwerk von z.B. teuer gemieteten Standleitungen zu vertrauen, nutzt ein VPN die günstige Infrastruktur des Internets. So können die Büros und die Mitarbeiter der unterschiedlichen Unternehmensstandorte kostengünstig miteinander kommunizieren, während sie neue webbasierte Applikationen einsetzen, um effektiv und wirtschaftlich zusammenzuarbeiten.



Der Einsatz von VPNs empfiehlt sich für alle Unternehmen – ob kleinere, mittlere oder große Unternehmen – auch bei sehr hohen Sicherheits- und Qualitätsanforderungen.

Zum Beispiel zur Anbindung

- ▶ der Standorte von Kanzleien, Praxen und Büros der freien Berufe (Anwälte, Ärzte, Architekten etc.)
- ▶ der Außenstellen eines Dienstleistungsunternehmens oder einer Versicherung
- ▶ der Standorte im Bereich Groß- und Einzelhandel, Industrie, Chemie und Pharma, Automobil, Logistik und Verkehr oder im Gesundheitswesen
- ▶ der Home oder Mobile Offices von Mitarbeitern

### Voice-over-IP: Die Herausforderung für Quality-of-Service

Die Sprachvermittlung über IP-Netze gibt VoIP ihren Namen. Die Sprache wird im Netz wie eine Sonderform der Daten behandelt. VoIP-Lösungen sind durch die verwendeten Sprachkompressions-Algorithmen in der Lage, Sprache bei gleicher Qualität mit wesentlich geringeren Bitraten als traditionelle Systeme über normale Datenleitungen wie z.B. DSL zu übertragen.

Die Herausforderungen für die Übertragung von Sprachdaten über IP-Netze werden von Quality-of-Service-Mechanismen

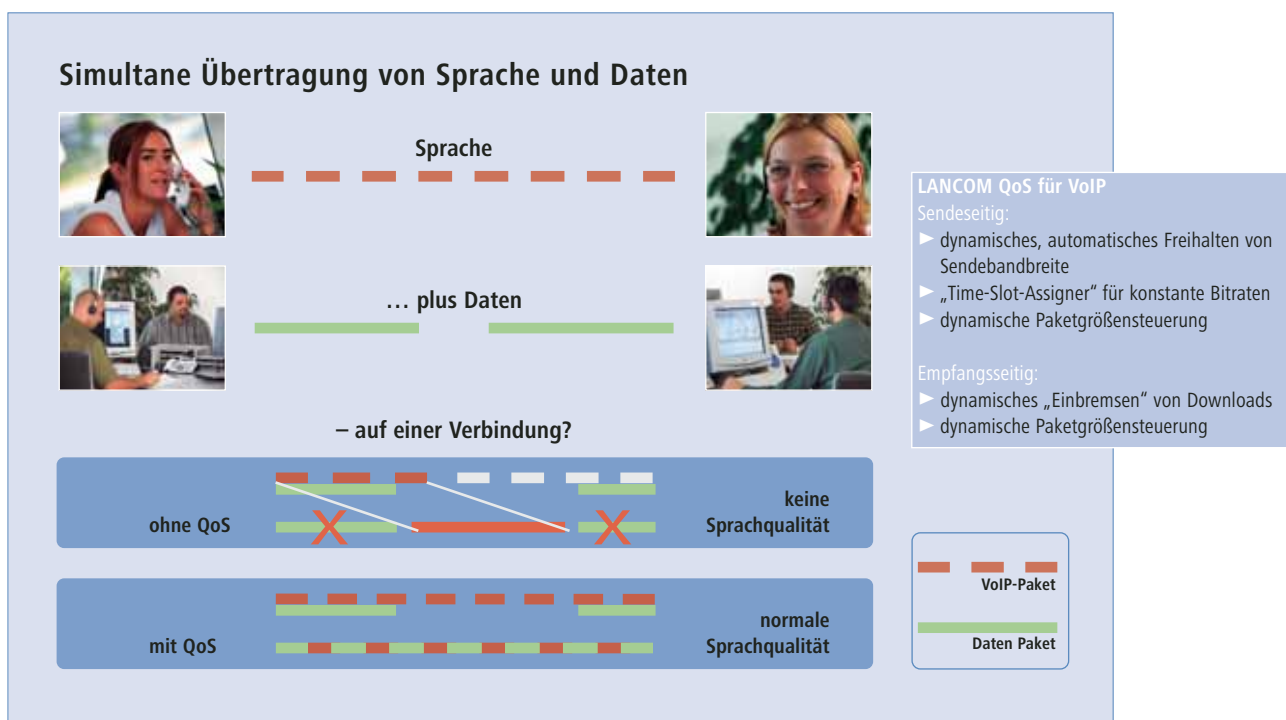
▶ an bzw. von Partnerunternehmen, Kunden oder Lieferanten im Rahmen von eBusiness oder zur

- ▶ Campusvernetzung in Forschung und Lehre
- ▶ Behördenvernetzung im öffentlichen Sektor

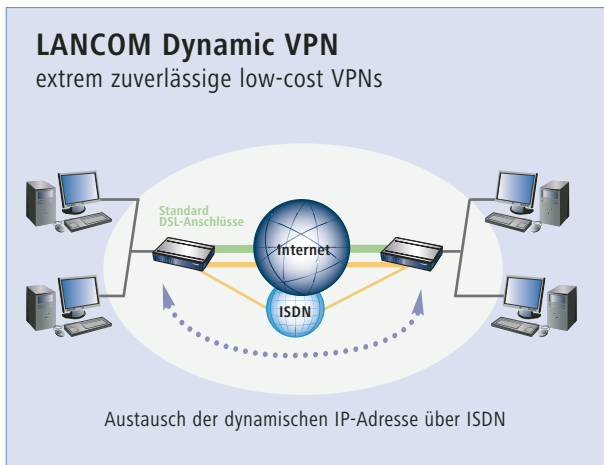
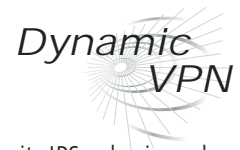
Anders als bei SSL-basierten Diensten, die jeweils nur genau eine Applikation (z. B. HTTPS-Browser) unterstützen, stehen bei IPsec-basierten VPNs alle Dienste zur Verfügung: Email, FTP, Zugriff auf Server usw., Windows-Netzwerke (Zugriff auf Dateien, Verzeichnisse und Drucker), Novell IPX-Netzwerke oder Voice-over-IP-Telefonie (Einbindung in die bestehende TK-Anlage).

angenommen. Diese Funktionen sorgen dafür, dass bei der Vermittlung die Sprachdaten bevorzugt werden. Dank der priorisierten Sendereihenfolge gilt: Sprache vor Daten!

Mit Hilfe intelligenter, dynamischer Algorithmen werden zu große Datenpakete zerkleinert und beugen so einem Blockieren der Leitung vor. Durch die simultane Übertragung von Sprache und Daten ergeben sich neben vielen neuen Möglichkeiten der Unternehmenskommunikation erhebliche Einsparungen bei den Telefonie- und Netzwerkkosten.



# LANCOM SYSTEMS – DYNAMIC VPN

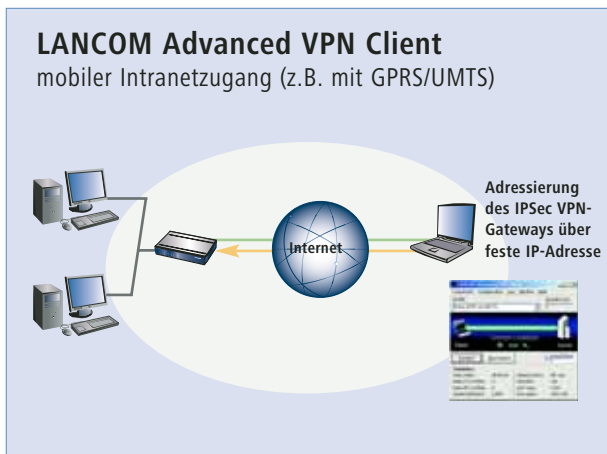


## LANCOM Dynamic VPN

Die geschützte Datenübertragung mit IPSec-basierenden VPNs benötigt normalerweise feste IP-Adressen, zwischen denen ein VPN-Tunnel aufgebaut wird. Mit dem Dynamic-VPN-Verfahren bietet LANCOM Systems erstmalig die Möglichkeit, VPNs auch an ganz normalen, kostengünstigen Standard-Internetzugängen mit dynamischer IP Adresse zu betreiben. Kernpunkt des patentierten Verfahrens ist die Vorab-Übermittlung der aktuellen IP-Adresse der IPSec-Gateways über ISDN. Der Wegfall der teuren statischen IP-Adresse bringt immense Kostenvorteile.

## LANCOM Dynamic VPN Endpoint

Neben den vielfältigen Leitungs-Backupmöglichkeiten unterstützen LANCOM VPN Router und Gateways über die Dynamic VPN Endpoint Funktion bis zu 8 redundante VPN Einwahlgateways. Stellt die integrierte Leitungsüberwachung über "Dead Peer Detection" oder Polling fest, dass ein Einwahlknoten nicht erreichbar ist, so wird automatisch der nächste verfügbare VPN-Einwahlknoten ausgewählt. Durch eine zufällige Wahl des Einwahlknotens kann die Last auf die zur Verfügung stehen Gateways gleichmäßig verteilt werden. Die zentralseitigen VPN Gateways aktualisieren die jeweils aktuelle Verbindung zur Gegenstelle über dynamisches Routing (RIPv2).



## LANCOM Advanced VPN Client

Der LANCOM Advanced VPN Client ermöglicht die Einwahl in ein Unternehmens-Intranet von beliebigen Standorten aus. Einzige Voraussetzung ist ein Internet-Zugang, z. B. mittels Notebook im Hotel oder sogar per Wireless LAN in einem öffentlichen HotSpot, z. B. an Flughäfen. Der LANCOM Advanced VPN Client bietet dabei gegenüber vielen anderen Implementationen die Besonderheit, dass dem User eine private Adresse aus dem angebundnen Intranet zugeteilt wird. Somit stehen alle Dienste und Server des jeweiligen Intranets auch mobilen Nutzern zur Verfügung.

Der LANCOM Advanced VPN Client ist kostenlos ohne Funktionseinschränkung als 30-Tage-Testversion auf der LANCOM Webseite oder der LANCOM-Produkt CD erhältlich.

[www.lancom.de/download/](http://www.lancom.de/download/)

- ▶ Sicherer, verschlüsselter Firmenzugang unterwegs
- ▶ IPSec Verschlüsselung mit AES oder 3-DES, IPCOMP Datenkompression, Unterstützung digitaler Zertifikate und Hardware-Tokens
- ▶ Integrierte Stateful Inspection Firewall
- ▶ Application-Level Firewall
- ▶ "Friendly Net"-Erkennung für situationsangepasste Sicherheitslevel
- ▶ Unterstützt Windows XP, 2000, NT, ME, 98SE und auf Anfrage Windows CE
- ▶ Profile für LAN/WLAN, Analog/DSL Modem, ISDN und GPRS/UMTS
- ▶ Einfache und schnelle VPN-Integration durch Installations-Assistenten

## IPSec Standards

Das Tunnelprotokoll IPSec wird für die meisten öffentlichen Internet-basierten IP-VPNs eingesetzt. Dieses Protokoll bietet eine umfassende Sicherheit für die Authentifizierung und Verschlüsselung. Über den sogenannten Authentifizierungs-Header prüft IPSec, ob das empfangene Datenpaket vom richtigen Absender stammt und ob das Paket nicht verändert wurde (Integrität).

IPsec unterstützt unter anderem folgende Verschlüsselungsstandards und Verfahren:

- ▶ Diffie-Hellmann (Austausch von Schlüsseln)
- ▶ Verschlüsselungs-Algorithmen wie AES und Triple DES (Sicherung des eigentlichen Datenaustausches)
- ▶ Hash-Algorithmen (Authentifizierung der einzelnen Datenpakete)
- ▶ Digitale Signaturen (= digitale Ausweise) oder Pre-Shared-Key

## Digitale Zertifikate

Digitale Zertifikate sind von einem anerkannten Trustcenter – Zertifizierungsstelle (CA) – geprüfte und beglaubigte digitale Dokumente. Hierin finden sich Angaben wie Inhaber, Zweck und Gültigkeitsdauer des Zertifikats, ein oder mehrere öffentliche Schlüssel und die Internet-Adresse, unter der der aktuelle Gültigkeitsstand dieses Zertifikates geprüft werden kann. Das Prinzip ist die Ausgabe einer digitalen Signatur unter Verwendung asymmetrischer Verschlüsselung. Die Zertifikate werden auf der Basis von X.509 (PKCS#12) und dem "public key"-Verfahren nach RSA erstellt.

Digitale Zertifikate dienen immer als Ausweis, zur Identifikation und Authentifizierung und bieten ein Höchstmaß an Sicherheit.

<b>IPSec Protokolle</b>	ESP – Tunnel/Transport, AH – Tunnel/Transport, IPCOMP Datenkompression*
<b>Symmetrische Verschlüsselungsverfahren</b>	DES 56 Bit, 3DES 168 Bit, CAST 128 Bit, Blowfish 128 Bit, AES 128 bis AES 256 Bit*
<b>Hash Algorithmus</b>	HMAC-MD5-96 / 128 Bits, HMAC-SHA-1-96 / 160 Bits
<b>Schlüsselmanagement</b>	IKE / ISAKMP, Lifetimes Time / KByte
<b>IKE</b>	Pre-Shared-Key pro User, Digitale Zertifikate (X.509)*, IKE Mode (Main & Agressive)
<b>Schlüsselaustausch</b>	Oakley, Diffie Hellmann, Algorithmus mit Schlüssellängen von 768, 1025, 1536 (in Gruppen 1,2,5)

\* ab LCOS 5.0

# LANCOM SYSTEMS – MANAGEMENT TOOLS

Eine ganzheitliche VPN-Vernetzung erfordert leistungsfähige und einfache Möglichkeiten der Überwachung und Steuerung. Mit LCOS und den LANtools bietet LANCOM Systems hierfür hervorragende Management Tools – selbst in komplexen Anwendungsszenarien.

- ▶ Skripting
- ▶ Einspielen von neuen Firmware-Versionen
- ▶ Freischalten zusätzlicher Software-Optionen
- ▶ Überwachung des Gerätestatus
- ▶ Überwachung der Verbindungen (inklusive VPN)
- ▶ Überwachung der Firewallaktionen

Das Netzwerk-Management mit den LANtools ermöglicht u.a. folgende Funktionen:

- ▶ Konfiguration der Geräte
- ▶ Konfigurationsverwaltung – Sichern und Wiederherstellen der Einstellungen

The screenshot shows the LANconfig application window. The main area displays a table of devices with their names, addresses, and firmware update status. A progress bar and percentage are shown for each device. Below the main table is a log window showing the date, time, name, address, and message for each device's firmware update.

Name	Adresse	Gerätestatus	Verlauf
DRESDEN	10.1.202.192	Firmw. hochladen ...	53% (68968 Bytes/s)
GERA	10.1.202.193	Firmw. hochladen ...	58% (69240 Bytes/s)
GOETTINGEN	10.1.202.194	Firmw. hochladen ...	58% (55022 Bytes/s)
ERFURT	10.1.202.198	Firmw. hochladen ...	57% (43670 Bytes/s)
GOERLITZ	10.1.202.199	Firmw. hochladen ...	53% (68675 Bytes/s)
NUERNBERG	10.1.202.210	Firmw. hochladen ...	59% (70285 Bytes/s)
HOYERSWERDA	10.1.202.211	Firmw. hochladen ...	53% (52147 Bytes/s)
MAGDEBURG	10.1.202.213	Firmw. hochladen ...	58% (53007 Bytes/s)
KOETHEN	10.1.202.217	Firmw. hochladen ...	56% (52525 Bytes/s)
LEIPZIG	10.1.202.218	Firmw. hochladen ...	32% (21644 Bytes/s)
TEMPELHOF	10.1.202.219	Firmw. hochladen ...	46% (53706 Bytes/s)
MERSEBURG	10.1.202.220	Firmw. hochladen ...	58% (50486 Bytes/s)
WITTENBERG	10.1.205.137	Firmw. hochladen ...	42% (66901 Bytes/s)
ANGERMUENDE	10.1.206.211	Firmw. hochladen ...	54% (62541 Bytes/s)
CHEMNITZ	10.1.206.212	Firmw. hochladen ...	53% (70732 Bytes/s)
ADLERSHOF	10.1.206.213	Firmw. hochladen ...	57% (55326 Bytes/s)
DESSAU	10.1.206.214	Firmw. hochladen ...	53% (65047 Bytes/s)

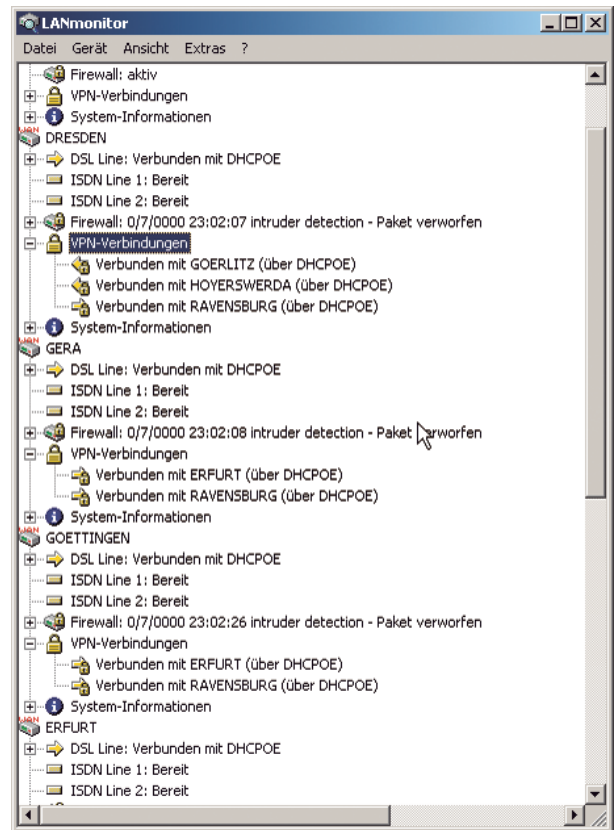
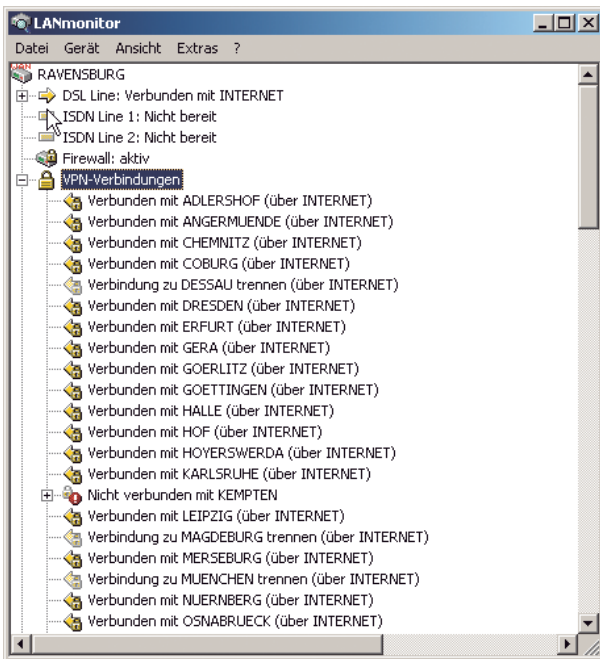
  

Datum	Zeit	Name	Adresse	Meldung
27.01.2004	10:38:00	LEIPZIG	10.1.202.218	Firmware hochladen gestartet
27.01.2004	10:38:00	TEMPELHOF	10.1.202.219	Firmware hochladen gestartet
27.01.2004	10:38:00	MERSEBURG	10.1.202.220	Firmware hochladen gestartet
27.01.2004	10:38:00	WITTENBERG	10.1.205.137	Firmware hochladen gestartet
27.01.2004	10:38:00	ANGERMUENDE	10.1.206.211	Firmware hochladen gestartet
27.01.2004	10:38:00	CHEMNITZ	10.1.206.212	Firmware hochladen gestartet
27.01.2004	10:38:00	ADLERSHOF	10.1.206.213	Firmware hochladen gestartet
27.01.2004	10:38:00	DESSAU	10.1.206.214	Firmware hochladen gestartet

17 Geräte ausgewählt

LANconfig hilft bei der Grundeinstellung des Gerätes und vereinfacht das Einrichten des Netzwerkes wesentlich. LANconfig listet alle im Netzwerk befindlichen LANCOM-Geräte auf. Der Setup-Assistent leitet durch die wichtigsten Installationsschritte.

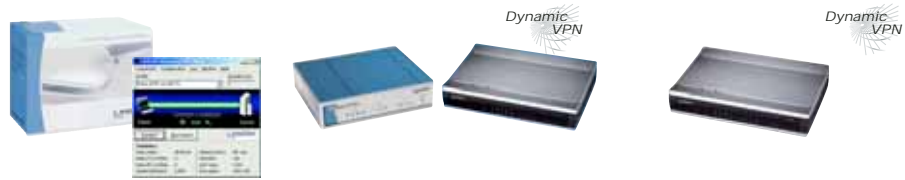
Name	Status	Letzter Fehler	Maßezeit	Verbindung	Gateway	Verschlüsselungs-Algo...	Hmac-Algorithmus	Hash-Algorithmus
VPN_AMAY	Nicht Verbunden	Leistungsüberwa...	0 Sekunden	INTERNET	217.228.41.56	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)
VPN_CBUIERSCH	Verbunden		0 Sekunden	INTERNET	80.142.186.239	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)
VPN_CSCHALLE	Verbunden		0 Sekunden	INTERNET	80.146.98.22	AES (128 Bk)	(none) (0 Bk)	HMAC_MD5 (128 Bk)
VPN_DEICH	Verbunden		0 Sekunden	INTERNET	80.142.139.67	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)
VPN_ETRABER	Verbunden		0 Sekunden	INTERNET	212.202.73.28	BLOWFISH (128 Bk)	SHA (160 Bk)	HMAC_SHA (160 Bk)
VPN_FJANSSEN	Verbunden		0 Sekunden	INTERNET	82.82.232.129	BLOWFISH (128 Bk)	SHA (160 Bk)	HMAC_SHA (160 Bk)
VPN_FTHEINEN	Verbunden		0 Sekunden	INTERNET	80.146.66.20	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)
VPN_HBATTI	Verbunden		0 Sekunden	INTERNET	80.146.114.101	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)
VPN_MBAIGSIK	Verbunden		0 Sekunden	INTERNET	213.23.254.236	AES (128 Bk)	(none) (0 Bk)	HMAC_MD5 (128 Bk)
VPN_MORIX	Verbunden		0 Sekunden	INTERNET	213.54.77.150	AES (128 Bk)	(none) (0 Bk)	HMAC_MD5 (128 Bk)
VPN_MPLUM	Verbunden		0 Sekunden	INTERNET	80.146.89.25	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)
VPN_OSCHLPE	Verbunden		0 Sekunden	INTERNET	80.72.51.100	AES (128 Bk)	(none) (0 Bk)	HMAC_MD5 (128 Bk)
VPN_THEO	Verbunden		0 Sekunden	INTERNET	217.82.205.102	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)
VPN_WOHN	Verbunden		0 Sekunden	INTERNET	217.136.170.119	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)
VPN_WTTW	Verbunden		0 Sekunden	INTERNET	217.80.153.52	BLOWFISH (128 Bk)	(none) (0 Bk)	HMAC_SHA (160 Bk)



Mit dem Überwachungstool LANmonitor lassen sich Netzwerke bequem und strukturiert überwachen. Sämtliche VPN-Verbindungen können überwacht werden. So ist beispielweise der Datenverkehr auf den verschiedenen Schnittstellen der Gateways ablesbar. Mit Hilfe der Diagnose ist sichtbar, mit welchen Einstellungen der Datenverkehr optimiert werden kann. Im Falle eines Fehlers kann sofort reagiert werden. Dank Skripting wird das Automatisieren von Konfigurationseinstellungen erheblich vereinfacht: bestimmte Parameter wie z.B. Firewall-Einstellungen werden mit Hilfe einer Skript-Datei auf komplette Installationen übertragen.

Die Management Tools bieten ferner die Möglichkeit sicherheitsrelevante Daten und Accounting-Informationen abzurufen. Damit existiert ein Steuerungsinstrument z.B. zur Kostenkontrolle und Kostenzuordnung.

# PRODUKTÜBERSICHT VPN Router und Gateways



	LANCOM Advanced VPN Client	LANCOM DSL/I-1611 Office LANCOM 1621 ADSL/ISDN	LANCOM 1711 VPN
<b>Einsatz</b>	<ul style="list-style-type: none"> <li>• Client-to-WAN</li> </ul>	<ul style="list-style-type: none"> <li>• VPN-Gateway</li> <li>• ADSL-Router (1621)</li> <li>• Breitband-Router (1611)</li> <li>• ISDN-Router</li> <li>• Firewall</li> </ul>	<ul style="list-style-type: none"> <li>• VPN-Gateway</li> <li>• Breitband-Router</li> <li>• ISDN-Router</li> <li>• Dual-Band WLAN Access Point</li> <li>• Firewall</li> </ul>
<b>Empfehlung</b>	<ul style="list-style-type: none"> <li>• VPN-Software-Client für den mobilen Nutzer</li> </ul>	<ul style="list-style-type: none"> <li>• Filialrouter für ADSL-Anschlüsse (1621)</li> <li>• Filialrouter für ADSL, SDSL- oder andere Breitbandanschlüsse (1611)</li> </ul>	<ul style="list-style-type: none"> <li>• Filialrouter für DSL, SDSL- oder andere Breitbandanschlüsse</li> </ul>
<b>Vorteile</b>	<ul style="list-style-type: none"> <li>• Sicherer, verschlüsselter Firmenzugang unterwegs</li> <li>• Unterstützt Windows XP, 2000, NT, ME, 98SE und Windows CE***</li> <li>• Profile für LAN/WLAN, Analog/DSL Modem, ISDN und GPRS/UMTS</li> <li>• Integrierte Stateful-Inspection Firewall</li> <li>• Application-Level- Firewall mit "Friendly Net"-Erkennung</li> </ul>	<ul style="list-style-type: none"> <li>• Anbindung von bis zu 25 Außenstellen oder VPN-RAS-Usern</li> <li>• Load Balancing (2-fach) (1621)**</li> <li>• High Security Firewall</li> <li>• digitale Zertifikate**</li> <li>• Dial Backup (ISDN, 2. DSL, GPRS oder Analog Backup)</li> <li>• ISDN-Schnittstelle für Office-Kommunikation und Remote Management</li> <li>• Dynamic VPN Endpoint</li> </ul>	<ul style="list-style-type: none"> <li>• Anbindung von bis zu 25 Außenstellen oder VPN-RAS-Usern</li> <li>• Load Balancing (4-fach)**</li> <li>• High Security Firewall</li> <li>• digitale Zertifikate**</li> <li>• Höchste Sicherheit und Performance durch VPN Hardwarebeschleuniger</li> <li>• hochintegriert</li> <li>• Dial Backup (ISDN, 2. DSL, GPRS oder Analog Backup)</li> <li>• Dynamic VPN Endpoint</li> </ul>
<b>Technische Daten</b>			
<b>Integriertes WLAN</b>	–	–	–
<b>ISDN</b>	–	✓	✓
<b>4-Port-Switch integriert, Ports separierbar</b>	–	✓ (1621)	✓
<b>ADSL-Modem integriert</b>	–	✓ (1621)	–
<b>VPN-Hardwarebeschleuniger</b>	–	–	✓ in Verbindung mit VPN 25 Option
<b>DMZ-Port (via Port-Separierung)</b>	–	✓ (1621)	✓
<b>Max. VPN-Tunnel - gleichzeitig aktiv - mit Erweiterungsoption</b>	1/beliebig –	5 25	5 25
<b>Max. VPN-Durchsatz-Rate (Mbit/s) - AES 128 bit - 3-DES 168 bit - Blowfish 128 bit</b>	–	> 2.3 > 1.2 > 3.2	> 16* > 16* > 10
<b>ISDN Festverbindungsoption (D-64; D64SY)</b>	–	✓	✓
<b>Artikel-Nr:</b>	61600 1er-Lizenz 61601 10er-Lizenz 61602 25er-Lizenz	60302 (EU); 60303 (UK) 60682 (Annex B; EU); 60681 (Annex A; EU) 61013 (Annex A; UK)	61125 (EU) 61126 (UK)

\*\*\* auf Anfrage

Der LANCOM Advanced VPN Client ist kostenlos ohne Funktionseinschränkung als 30-Tage-Testversion auf der LANCOM Webseite oder der LANCOM-Produkt CD erhältlich: [www.lancom.de/download/](http://www.lancom.de/download/)



LANCOM 1811 Wireless DSL LANCOM 1821 Wireless ADSL	LANCOM 3550 Wireless	LANCOM 7111 VPN	LANCOM 8011 VPN
<ul style="list-style-type: none"> <li>• VPN-Gateway</li> <li>• Breitband-Router (1811)</li> <li>• ADSL-Router (1821)</li> <li>• ISDN-Router</li> <li>• Dual-Band WLAN Access Point</li> <li>• Firewall</li> </ul>	<ul style="list-style-type: none"> <li>• VPN-Gateway</li> <li>• Breitband-Router</li> <li>• Dual-Band WLAN Access Point</li> <li>• Firewall</li> </ul>	<ul style="list-style-type: none"> <li>• VPN-Gateway</li> <li>• Firewall</li> </ul>	<ul style="list-style-type: none"> <li>• VPN-Gateway</li> <li>• Firewall</li> </ul>
<ul style="list-style-type: none"> <li>• Filialrouter für ADSL-Anschlüsse mit integriertem ADSL-Modem (1821)</li> <li>• Filialrouter für DSL, SDSL- oder andere Breitbandanschlüsse (1811)</li> </ul>	<ul style="list-style-type: none"> <li>• High Security WLAN Access Point</li> </ul>	<ul style="list-style-type: none"> <li>• zentrales VPN-Gateway für mittelgroße Standorte</li> </ul>	<ul style="list-style-type: none"> <li>• zentrales VPN-Gateway für große Standorte</li> </ul>
<ul style="list-style-type: none"> <li>• Anbindung von bis zu 25 Außenstellen oder VPN-RAS-Usern</li> <li>• Load Balancing (4-fach)**</li> <li>• High Security Firewall</li> <li>• digitale Zertifikate**</li> <li>• optional VPN Hardwarebeschleuniger</li> <li>• Dial Backup (ISDN, 2. DSL, GPRS oder Analog Backup)</li> <li>• ISDN-Schnittstelle</li> <li>• WLAN Verschlüsselung nach 802.11i</li> <li>• WLAN 108 Mbit/s Turbo-Modus</li> <li>• Dynamic VPN Endpoint</li> </ul>	<ul style="list-style-type: none"> <li>• Externer Cardbus-Slot für 2. WLAN Funkkarte oder UMTS-Datenkarte</li> <li>• WLAN Verschlüsselung nach 802.11i</li> <li>• WLAN 108 Mbit/s Turbo-Modus</li> <li>• optional VPN mit IPSec over WLAN</li> <li>• Dynamic VPN Endpoint</li> </ul>	<ul style="list-style-type: none"> <li>• breitbandige Standortkopplung</li> <li>• bis zu 100 Gegenstellen</li> <li>• 19"-Gehäuse</li> <li>• ISDN-Schnittstelle für Office-Kommunikation und Remote Management</li> <li>• integriertes Netzteil</li> <li>• Load Balancing (4-fach)**</li> <li>• digitale Zertifikate**</li> <li>• Dynamic VPN Endpoint</li> </ul>	<ul style="list-style-type: none"> <li>• VPN-Hardwarebeschleuniger</li> <li>• Für 200, 500, 1000 Gegenstellen</li> <li>• 19"-Gehäuse</li> <li>• ISDN-Schnittstelle für Office-Kommunikation und Remote Management</li> <li>• integriertes Netzteil</li> <li>• Load Balancing (4-fach)**</li> <li>• digitale Zertifikate**</li> <li>• Dynamic VPN Endpoint</li> </ul>
✓ (802.11 a,b,g)	✓ (802.11 a,b,g)	–	–
✓	–	✓	✓
✓	–	✓	✓
✓ (1821)	–	–	–
✓ in Verbindung mit VPN 25 Option	–	–	✓
✓	–	✓	✓
5 25	- 5 oder 25	100 –	200 500 oder 1000
> 16* > 16* > 10	> 5 > 3 > 7	> 20 > 20 > 15	> 25 > 25 > 15
✓	–	integriert	integriert
61116 (EU); 61117 (UK) 61118 (Annex B; EU); 61124 (Annex A; EU) 61119 (Annex A; UK)	61112 (EU) 61113 (UK)	61055 (EU) 61056 (UK)	61053 (EU) 61054 (UK)

\*Nur in Verbindung mit Hardwarebeschleuniger  
\*\* ab LCOS 5.0

## ...connecting your business

- ▶ LANCOM VPN-Technologie für ein gemeinsames Netzwerk aller Standorte und Telearbeitsplätze
- ▶ Vertraulicher Datenaustausch und optimale Sicherheit durch IPSec und LANCOM Dynamic VPN
- ▶ Keine Investition in teure Hardware – bedarfsgerechte Ausbaufähigkeit
- ▶ Reduktion von Wartungs- und Supportaufwand
- ▶ Multiserviceanwendungen (z.B. IP-Contact/Call Center) erhöhen die Wettbewerbsfähigkeit
- ▶ Professionelle Firewall- und Security-Funktion gegen potentielle Angriffe
- ▶ Konvergenz der Technologien: Daten- und Sprachübermittlung (Voice-over-IP)
- ▶ Immense Einsparungen bei Telefonie- und Netzwerkkosten
- ▶ Schneller Return On Investment durch innovative LANCOM VPN-Technologie



#### **Kundenbetreuung via Home Office:**

Eine Rechnung die aufgeht.

Die OEG in Lienen ist eine der ersten Adressen für Handwerksbetriebe und Hersteller rund um das Thema Heizungszubehör. OEG wandte sich an T-Com, um die Kundenbetreuung zu optimieren und das komplette Sortiment flächendeckend anbieten zu können. Zusammen mit LANCOM Systems und T-Com entstand eine bahnbrechende VPN-Lösung: Alle Kunden werden vom Home Office aus betreut und bestellen – europaweit zum Nulltarif – telefonisch, per Fax oder online. Kompromissloser Service und kurze Wege für die Kunden als Grundpfeiler der OEG-Philosophie konnten durch die Sprach- und Datenübertragung mittels der LANCOM VPN-Technologie realisiert werden: beste Ergebnisse und geringste Kosten – eine Rechnung die aufgeht.



#### **Deutsche Post In Haus Service GmbH:**

O Outsourcing der hausinternen Poststellen.

Die Deutsche Post, Erfahrung und Kompetenz rund um die Logistik der Kommunikation, bietet mit In Haus Service erfolgreich Lösungen für die interne Postbearbeitung. Über 140 Kunden-Poststellen betreibt die In Haus Service für Ihre Kunden. Mit der LANCOM VPN-Technologie ist es gelungen, die Poststellen z.B. von Großkunden sicher und problemlos zu vernetzen. Das Ergebnis der Verbindung von Kernkompetenzen der Deutschen Post mit der innovativen Technologie von LANCOM Systems: Erhöhte Wirtschaftlichkeit, gesteigerte Effizienz und enorme Einsparpotenziale.

### **Zentrale**

LANCOM Systems GmbH

Adenauerstr. 20/B2  
52146 Würselen  
Deutschland

### **Vertriebsbüros**

München

### **Vertriebsregionen**

Australien  
Belgien  
Deutschland  
Frankreich  
Italien  
Luxemburg  
Niederlande  
Osteuropa  
Schweiz  
United Kingdom  
Österreich

### Telefon

+49 (0)2405 49936-0

### Fax

+49 (0)2405 49936-99

### E-Mail

[info@lancom.de](mailto:info@lancom.de)

### Internet

[www.lancom.de](http://www.lancom.de)

LANCOM, LANCOM Systems, LCOS und LANvantage 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.

110195/0205

**LANCOM**  

---

**Systems**