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

LANCOM Advanced VPN Client Version 2.22 (Windows) Version 1.00 (Mac OS X)

- **Handbuch**
- **Manual**

LANCOM
Systems

LANCOM Advanced VPN Client

Version 2.22 (Windows)
Version 1.00 (Mac OS X)

LANCOM Systems

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Juni 2010

DE

Inhalt

DE

DE

1 Produktbeschreibung

1.1 LANCOM Advanced VPN Client - universeller IPSec Client

Der LANCOM Advanced VPN Client kann in beliebigen VPN-Umgebungen eingesetzt werden. Er kommuniziert auf der Basis des IPSec-Standards mit den Gateways verschiedenster Hersteller. Die Client Software emuliert einen Ethernet LAN-Adapter. Der LANCOM Advanced VPN Client verfügt dazu über zusätzliche Leistungsmerkmale, die dem Anwender den Einstieg in eine ganzheitliche Remote Access VPN-Lösung ermöglichen.

Der LANCOM Advanced VPN Client bietet:

- Unterstützung aller gängigen Windows-Betriebssysteme
- Einwahl über alle Übertragungsnetze (auch LANCOM LANCAPI) (nur Windows-Version)
- Kompatibilität mit den VPN Gateways unterschiedlichster Hersteller
- Integrierte Personal Firewall für mehr Sicherheit
- Dialer-Schutz (keine Bedrohung durch 0190er- und 0900er-Dialer) (nur Windows-Version)
- Höhere Geschwindigkeit im ISDN (Kanalbündelung) (nur Windows-Version)
- Gebührenersparnis (Kosten- und Verbindungskontrolle)
- „Friendly-Net"-Erkennung für situationsabhängige Firewallregeln
- Automatische Hot-Spot-Erkennung (nur Windows-Version)
- Bedienungskomfort (grafische Oberfläche)
- VPN Path Finder

1.2 Leistungsumfang

Der LANCOM Advanced VPN Client unterstützt alle gängigen Betriebssysteme (Windows 2000, Windows 2003 Server, XP, Vista, CE (auf Anfrage); Mac OS X 10.5 Leopard (nur Intel), Mac OS X 10.6 Snow Leopard). Die Einwahl in das Firmennetz erfolgt unabhängig vom Mediatyp, d.h. neben ISDN, PSTN (analoges Fernsprechnetz), GSM, GPRS, UMTS und xDSL wird auch LAN-Technik wie kabelgebundenes LAN und Funknetzwerk (WLAN) unterstützt. Auf diese Weise kann mit ein und demselben Endgerät von unterschiedlichen Lokationen auf das Firmennetz zugegriffen werden:

- in der Filiale über WLAN (nur Windows-Version)
- in der Zentrale über LAN
- unterwegs an Hotspots und beim Kunden über WLAN bzw. GPRS/UMTS (nur Windows-Version)
- im Home Office über xDSL oder ISDN (nur Windows-Version)

DE

Alle Ausführungen und Abbildungen in dieser Dokumentation beziehen sich auf die Windows-Version. Alle Unterschiede bezüglich der Mac-Version sind entsprechend gekennzeichnet.

1.3 Wichtige Hinweise

① Dieses Handbuch beschreibt den Funktionsumfang des LANCOM Advanced VPN Clients auf Basis der Software-Release 2.22.

② Sofern der verwendete Rechner noch nicht z.B. über einen lokalen Netzwerkzugang (LAN, WLAN oder LANCAPI) mit dem Internet verbunden ist, muss zuerst ein geeigneter Internetzugang hergestellt werden (z.B. durch Einbuchen an einem WLAN Hotspot). Ferner kann der Client selbständig die Interneteinwahl mit folgenden Geräten steuern: Analog-Modems, DSL-Modems (PPPoE), ISDN-, GPRS- oder UMTS-Karten. Anders als bei Verbindungen über das Internet, bei denen der Client darauf basierende VPN-Verbindungen aufbauen kann, brauchen direkte Wählverbindungen (z.B. ISDN-Karte oder LANCAPI, Analog-Modem, HSCSD-Mobiltelefon) i.d.R. nicht verschlüsselt zu werden.

③ Beim LANCOM Advanced VPN Client handelt es sich um eine kostenpflichtige Software. Unter www.lancom.de/download sowie auf der LANCOM-CD finden Sie eine 30-Tage-Demoversion des LANCOM Advanced VPN Clients. Diese Demoversion können Sie nach Ablauf der 30 Tage mit einer entsprechenden Lizenz zu einer Vollversion freischalten. Der Vertrieb der Lizenzen für die Vollversion erfolgt ausschließlich über LANCOM Distributions-, Fachhandels- und Systemhauspartner. Sie können die Lizenzen dort unter folgenden Artikelnummern für Windows (XP, 2000, Me und 98SE) zu bestellen:

- 61600 LANCOM Advanced VPN Client (1er Lizenz)
- 61601 LANCOM Advanced VPN Client (10er Lizenz)
- 61602 LANCOM Advanced VPN Client (25er Lizenz)

Die gleichzeitige Nutzung einer Lizenz auf verschiedenen Systemen ist lizenzrechtlich nicht erlaubt.

④ Die gleichzeitige Einwahl von VPN-Clients, die nicht über die erforderliche Lizenzfreischaltung verfügen (Demo-Mode), ist auf drei begrenzt. Die im VPN eingebuchten LANCOM Advanced VPN Clients werden im LANCOM LANmonitor angezeigt.

⑤ Wenn die VPN-LAN-Schnittstelle (LANCOM Advanced VPN Client) über das Netzwerkmanagement (Gerätemanager) manuell deaktiviert wird, muss das System danach gebootet werden. Eine erneute manuelle Reaktivierung erfordert wiederum einen manuellen Neustart des Betriebssystems.

1.4 Client Monitor - Grafische Benutzeroberfläche

Die grafische Oberfläche des LANCOM Advanced VPN Client schafft Transparenz während des Einwahlvorganges und Datentransfers. Sie informiert u.a. auch über den aktuellen Datendurchsatz.

Der Anwender ist zu jeder Zeit darüber informiert, ob sein PC online ist und wo letztlich die Gebühren anfallen.

1.5 Dialer

Nur für Windows-Version verfügbar.

Ein eigener Dialer ersetzt den sonst üblichen Microsoft DFÜ-Dialer. Daraus ergeben sich Vorteile gleich in mehrfacher Hinsicht:

- intelligentes Line Management (Short Hold Mode) in Wählnetzen
- Steuerung der Bandbreite (Kanalbündelung) im ISDN
- integrierte Personal Firewall-Mechanismen
- Schutz vor "automatischen Dialern"

1.6 Line Management

Um die Übertragungsgebühren möglichst gering zu halten, können aktive Verbindungen automatisch unterbrochen werden, wenn keine Daten fließen. Liegen erneut Daten für die Übertragung vor, wird die ruhende Verbindung ohne Einwirkung des Benutzers reaktiviert. Gebühren fallen immer nur dann an, wenn Daten übertragen werden. Bei der Interneteinwahl via ISDN können

beide Nutzkanäle gebündelt werden (dynamische Linkzuschaltung), falls für den Transfer größerer Datenmengen eine hohe Übertragsrate benötigt wird.

Ein weiteres Instrument zur Kostenkontrolle ist die intelligente Verbindungssteuerung. Hier werden Online-Sessions nach Zeit, nach Anzahl der Verbindungsaufbauten oder Gebühreneinheiten angezeigt und bei Bedarf überwacht.

1.7 Personal Firewall

Der LANCOM Advanced VPN Client verfügt über alle erforderlichen Personal Firewall Funktionalitäten, um den PC-Arbeitsplatz umfassend gegenüber Angriffen aus dem Internet und anderer LAN-Teilnehmer (WLAN oder LAN) zu schützen. Weiter besteht keine Möglichkeit, dass der Dialer von automatischen 0190er- und 0900er-Dialern für ungewollte Verbindungen missbraucht wird. Die wesentlichen Security-Mechanismen sind IP-NAT und Protokollfilter. NAT (Network Address Translation) ist ein Security-Standard zum Verbergen der individuellen IP-Adressen gegenüber dem Internet. NAT bewirkt eine Übersetzung der von außen sichtbaren Adresse in entsprechende Client-Adressen und umgekehrt. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filtermechanismus nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.

Zudem verfügt der LANCOM Adavanced VPN Client über eine Application-Layer Firewall und über Friendly-Net-Erkennung. Mit der Application-Layer Firewall können Filterregeln mit bestimmten Anwendungen verknüpft werden. Mit der Friendly-Net-Erkennung können können situationsabhängig Filterregeln aktiviert bzw. deaktiviert werden. So können z.B. strikte Regeln für die Einwahl an einem öffentlichen Hot-Spot definiert werden, die bei der Einwahl an einem vertrauenswürdigen Netzknoten gelockert werden (nur für Windows verfügbar).

1.8 PKI-Unterstützung

Die Zugangssicherheit zum Firmennetz kann durch den Einsatz digitaler Zertifikate in Form von Software (PKCS#12) oder Smart Cards (PKCS#11, CT-API, PC/SC) erhöht werden. Der LANCOM Advanced VPN Client unterstützt hierfür die Einbindung in eine PKI (Public Key Infrastruktur). LANCOM Router unter-

stützen das Pre-Shared-Key Verfahren und ab LCOS-Version 5.0 digitale Zertifikate.

1.8.1 Public Key Infrastruktur

Public-Key-Infrastrukturen (PKI) beschreiben ein weltweit genutztes Verfahren, um zwischen beliebigen Kommunikationspartnern auf elektronischem Wege Schlüssel sicher auszutauschen. Die PKI bedient sich dabei sogenannter Schlüsselpärchen aus jeweils einem öffentlichen und einem privaten Schlüssel. In der Welt des elektronischen, globalen Informationsaustausches wird so eine Vertrauensbasis aufgebaut, wie wir sie in der traditionellen Geschäftswelt auf Papierbasis kennen. Die digitale Signatur in Verbindung mit Datenverschlüsselung ist das elektronische Äquivalent zur händisch geleisteten Unterschrift und belegt Ursprung sowie die Authentizität von Daten und Teilnehmer.

Eine PKI basiert auf digitalen Zertifikaten, die - von einer öffentlichen Zertifizierungsstelle (Trust Center) ausgestellt - als persönliche "elektronische Ausweise" fungieren und idealerweise auf einer Smart Card abgespeichert sind. Sicherheitsexperten und der IETF (Internet Engineering Task Force) sind sich darüber einig, dass ein nachhaltiger Schutz vor Man-In-The-Middle-Attacken nur durch den Einsatz von Smart Cards mit Zertifikaten erreicht werden kann.

1.8.2 Smart Card

Smart Cards sind die ideale Ergänzung für hochsichere Remote Access-Lösungen. Sie bieten doppelte Sicherheit beim Login-Vorgang, nämlich Wissen über PIN (Persönliche Identifikations Nummer) und Besitz der Smart Card. Der Anwender identifiziert sich mit der Eingabe der PIN eindeutig als rechtmäßiger Besitzer (Strong Authentication). Die PIN ersetzt das Passwort und die Eingabe der User-ID (Basistechnologie für Single Sign On). Der Anwender weist sich nur noch gegenüber der Smart Card aus. Der Check gegenüber dem Netz erfolgt zwischen Smart Card und Security-System. Alle sicherheitsrelevanten Operationen laufen vollständig im Inneren der Karte - also außerhalb des PCs - ab. Das System ist neben individuellen Anpassungen an Schutzmechanismen offen für multifunktionalen Einsatz (z. B. als Company Card). Auch biometrische Verfahren lassen sich integrieren.

DE

1.9 VPN Path Finder

In manchen Umgebungen ist es nicht möglich, über eine vorhandene Internetverbindung eine geschützte VPN-Verbindung aufzubauen, weil in den Einstellungen einer vorgeschalteten Firewall die von IPSec genutzten Ports gesperrt sind. Um auch in einer solchen Situation eine IPSec-geschützte VPN-Verbindung aufbauen zu können, unterstützt der LANCOM Advanced VPN Client die VPN Path Finder-Technologie.

Dabei wird zunächst eine Datenübertragung über Standard-IPSec versucht. Kommt diese Verbindung nicht zustande (z.B. weil der IKE Port 500 in einem Mobilfunknetz gesperrt ist), so wird automatisch ein Verbindungsaufbau versucht, bei dem das IPSec VPN mit einem zusätzlichen SSL-Header (Port 443, wie bei https) gekapselt wird.

DE

2 Installation

Die Installation der Secure Software für Windows- und Mac-Systeme erfolgt komfortabel über Setup. Der Installationsablauf ist für alle Versionen des LANCOM Advanced VPN Clients identisch. Im folgenden ist die Installation für Windows 2000/XP und Vista beschrieben.

Bevor Sie die Software installieren, müssen zur vollen Funktionsfähigkeit die Installationsvoraussetzungen, wie im folgenden Kapitel beschrieben, erfüllt sein.

2.1 Installationsvoraussetzungen

2.1.1 Betriebssystem

Die Software kann auf Computern mit den Betriebssystemen Microsoft Windows 2000, Microsoft Windows 2003 Server, Microsoft XP oder Microsoft Vista, sowie Mac OS X 10.5 Leopard (nur Intel) und Max OS X 10.6 Snow Leopard installiert werden.

Halten Sie für die Dauer der Installation unbedingt die Datenträger (CD oder DVD) für das jeweils im Einsatz befindliche Betriebssystem bereit, um Daten für die Treiberdatenbank des Betriebssystems nachladen zu können!

2.1.2 Zielsystem

Das Zielsystem muss eine der folgenden Verbindungsarten unterstützen: ISDN, PSTN (analoges Modem), GPRS, UMTS, LAN over IP, WLAN, PPP over Ethernet oder PPP over CAPI.

2.1.3 Lokales System

Eines der folgenden Kommunikationsgeräte muss installiert sein.

ISDN-Adapter (ISDN)

Nur für Windows-Version vefügbar.

Der ISDN-Adapter muss die ISDN CAPI 2.0 unterstützen. Wenn Sie PPP Multilink nutzen, kann die Software bis zu 8 ISDN B-Kanäle (je nach Kanalanzahl des Adapters) bündeln. Prinzipiell kann jeder ISDN-Adapter, der die ISDN-Schnittstelle CAPI 2.0 unterstützt, eingesetzt werden. (Für gewöhnlich wird die CAPI bei der Installation eines ISDN-Adapters automatisch eingerichtet.)

DE

Modem oder Datenkarte

Nur für Windows-Version verfügbar.

Für die Kommunikation über Modem muss das Modem korrekt installiert sein, sowie Modem Init. String und COM-Port Definition zugewiesen sein. Das Modem muss den Hayes-Befehlssatz unterstützen.

Ebenso können Mobiltelefone für die Datenkommunikation genutzt werden, nachdem die zugehörige Software installiert wurde, die sich für den Client genauso darstellt wie ein analoges Modem. Als Schnittstelle zwischen Handy und PC kann die serielle Schnittstelle, die IR-Schnittstelle (Infrarot, nur für Windows) oder Bluetooth genutzt werden. Je nach Übertragungsart (GSM, V.110, GPRS, UMTS oder HSCSD) muss die Gegenstelle über die entsprechende Einwahlplattform verfügen. Der in die Modemkonfiguration des LANCOM Advanced VPN Clients einzutragende Initialisierungs-String ist vom ISP oder dem Hersteller des Mobiltelefons zu beziehen.

Direkte Unterstützung von UMTS/HSDPA- oder GPRS-Datenkarten

Nur für Windows-Version verfügbar.

Der LANCOM Advanced VPN Client unterstützt die direkte Verwendung von Datenkarten für Notebooks, wie sie von vielen Mobilfunkbetreibern angeboten werden. Die Parameter für die Einwahl können direkt in die Profileinstellungen eingetragen werden.

Weitere Hinweise zur Konfiguration eines mobilen Onlinezugang über UMTS oder GPRS finden Sie unter 'UMTS- oder GRPS-Profil einrichten' →Seite 125.

DE

LAN-Adapter (LAN over IP)

Um die Client-Software mit der Verbindungsart "LAN" in einem Local Area Network betreiben zu können, muss zusätzlich zum bereits installierten LAN-Adapter (Ethernet oder Token Ring) kein weiterer Adapter installiert werden. Die Verbindung der LAN-Clients ins WAN stellt ein beliebiger Access Router her. Einzige Vorausetzung: IP-Verbindung zum Zielsystem muss möglich sein. Die VPN-Funktionalität liefert die Client Software. Adapter für ein Wireless LAN (WLAN-Adapter) werden genauso behandelt wie normale LAN-Adapter. Für WLAN-Verbindungen wird als Verbindungsart "IPSec over WLAN" gewählt.

LANCOM LANCAPI

Nur für Windows-Version verfügbar.

Wenn Sie zum Herstellen Ihrer Internetverbindung die LANCOM LANCAPI verwenden, beachten Sie bitte folgendes:

- Bei gleichzeitiger Verwendung der Statefull Inspection Firewall muss die Einstellung "Ausschließlich Kommunikation im Tunnel zulassen" ausgeschaltet bleiben, da sonst der LANCAPI Server im lokalen Netzwerk nicht mehr erreicht werden kann.
- Bei ausgeschalteter Statefull Inspection Firewall funktioniert die Internet- und VPN- Kommunikation ohne weitere Einstellungen.

xDSL-Modem (PPPoE/PPTP)

Nur für Windows-Version verfügbar.

Die Verbindungsart PPP over Ethernet setzt voraus, dass eine Ethernet-Karte installiert und darüber ein xDSL-Modem mit Splitter korrekt angeschlossen ist. Wichtig (wenn Sie ADSL in der Anschlussvariante ausführen, die nach Verbindungsdauer berechnet wird): Nachdem die Client-Software installiert wurde, beachten Sie bitte unbedingt den Abschnitt "Adapter und Protokoll für PPPoE".

WLAN-Adapter (WLAN)

Nur für Windows-Version verfügbar.

Der WLAN-Adapter wird mit der Verbindungsart "WLAN" betrieben. Im Monitormenü erscheint eigens der Menüpunkt "WLAN-Einstellungen", worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können. Wird diese "WLAN-Konfiguration aktiviert", so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool

DE

der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Wird die Verbindungsart WLAN für ein Zielsystem in den Profileinstellungen eingestellt, so wird unter dem grafischen Feld des Client-Monitors eine weitere Fläche eingeblendet, auf der die Feldstärke und das WLAN-Netz dargestellt werden.

Bitte beachten Sie zur Konfiguration der WLAN-Einstellungen die Beschreibung zum Parameter 'Verbindungsmedium (nur für Windows-Version verfügbar)' →Seite 92.

Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsarten genutzt, so erkennt der Client automatisch, welche Verbindungsarten aktuell zur Verfügung stehen und wählt davon die schnellste aus.

Auf Grundlage eines vorkonfigurierten Zielsystems wird automatisch die Verbindungsart erkannt und eingesetzt, die für den Client-PC aktuell zur Verfügung steht, wobei bei mehreren alternativen Übertragungswegen automatisch der schnellste gewählt wird. In einer Suchroutine ist die Priorisierung der Verbindungsarten in folgender Reihenfolge festgelegt:

1. LAN
2. WLAN (nur Windows-Version)
3. DSL (nur Windows-Version)
4. UMTS/GPRS (nur Windows-Version)
5. ISDN (nur Windows-Version)
6. MODEM (nur Windows-Version)

Die Konfiguration erfolgt mit der Verbindungsart "automatische Medienerkennung" in den Profileinstellungen unter "Zielsystem". Alle für diesen Client-PC vorkonfigurierten Zielsysteme zum VPN Gateway des Firmennetzes können dieser automatischen Medienerkennung – sofern gewünscht – zugeordnet werden (über das Parameterfeld "Zielsystem" in den Profileinstellungen). Damit erübrigt sich die manuelle Auswahl eines Mediums (WLAN, UMTS, Netzwerk, DSL, ISDN, Modem) aus den Profileinträgen. Die Eingangsdaten für die Verbindung zum ISP werden für den Anwender transparent aus den vorhandenen Profileinträgen übernommen.

Beachten Sie dazu die Beschreibung zu 'Verbindungstyp' →Seite 92.

DE

2.1.4 Voraussetzungen für den Einsatz von Zertifikaten

Um mit der Security Software die Zertifizierung (X.509) nutzen, zu können, müssen folgende Voraussetzungen erfüllt sein:

Chipkartenleser (PC/SC-konform)

Wenn Sie die "Erweiterte Authentisierung" (Strong Authentication) mit Smart Cards nutzen wollen, muss ein Chipkartenleser an Ihr System angeschlossen sein. Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Diese Chipkartenleser werden nur in der Liste der Chipkartenleser aufgenommen, nachdem der Leser angeschlossen und die zugehörige Treiber-Software installiert wurde. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden. Dazu stellen Sie nach dem ersten Start des Monitors den Chipkartenleser ein unter "Verbindung →Zertifikate →Konfiguration". Beachten Sie dazu die Beschreibung unter "Client Monitor".

Chipkartenleser (CT-API-konform)

Wenn Sie einen CT-API-konformen Chipkartenleser nutzen, beachten Sie bitte folgendes:

Mit der aktuellen Software werden Treiber für die Modelle Kobil B0/B1, Kobil KAAN, SCM Swapsmart und SCM 1x0 (PIN Pad Reader) mitgeliefert. Diese Chipkartenleser können im Monitor unter "Verbindung →Zertifikate →Konfiguration" eingestellt werden. Sollte der Chipkartenleser mit den mitgelieferten Treibern nicht funktionieren oder ein anderer Chipkartenleser installiert sein, wenden Sie sich unbedingt an den Hersteller des Chipkartenlesers, bzw. konsultieren Sie die entsprechende Website bezüglich aktueller Hardware-Treiber, um den aktuellsten CT-API-Treiber zu erhalten und zu installieren. Nehmen Sie außerdem folgende Einstellung in der Client Software vor:

- Editieren Sie die Datei NCPPKI.CONF, befindlich im Windows\System-Verzeichnis (unter Windows 95/98) oder System32-Verzeichnis (unter Windows NT/2000) mit einem ASCII-Editor, indem Sie als "Modulname" den Namen des angeschlossenen Chipkartenlesers (xyz) eintragen und als DLLWIN95 bzw. DLLWINNT den Namen des installierten Treibers eintragen. (Der Standardname für CT-API-konforme Treiber ist CT32.DLL).

  Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit "visible = 1" auf sichtbar gesetzt wurden!

  Modulname= SCM Swapsmart (CT-API)→xyz

DE

DLLWIN95= scm20098.dll→ct32.dll

DLLWINNT= scm200nt.dll→ct32.dll

Nach einem Boot-Vorgang erscheint der von Ihnen eingetragene "Modulname" im Monitor-Menü unter "Verbindung →Zertifikate →Konfiguration → Chipkartenleser". Selektieren Sie nun diesen Chipkartenleser.

Chipkarten

Folgende Chipkarten werden unterstützt:

- Signtrust
- NetKey 2000
- TC Trust (CardOS M4)

Soft-Zertifikate (PKCS#12)

Statt einer Smart Card können auch Soft-Zertifikate genutzt werden.

Chipkarten oder Token (PKCS#11)

Mit der Software für die Smart Card oder den Token werden Treiber in Form einer PKCS#11-Bibliothek (DLL) mitgeliefert. Diese Treiber-Software muss zunächst installiert werden. Anschließend muss die Datei NCPPKI.CONF editiert werden.

- Editieren Sie die Datei NCPPKI.CONF, befindlich im Windows\System-Verzeichnis (unter Windows 95/98) oder System32-Verzeichnis (unter Windows NT/2000) mit einem ASCII-Editor, indem Sie als "Modulname" den Namen des angeschlossenen Lesers oder Tokens (xyz) eintragen. Als PKCS#11-DLL muss der Name der DLL eingegeben werden. Der zugehörige "Slotindex" ist herstellerabhängig (Standard = 0).

  Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit "visible = 1" auf sichtbar gesetzt wurden!

  Modulname= xyz

  PKCS#11-DLL= Name der DLL

  Slotindex=

Nach einem Boot-Vorgang erscheint der von Ihnen eingetragene "Modulname" im Monitor-Menü unter "Verbindung →Zertifikate →Konfiguration → Chipkartenleser". Selektieren Sie nun diesen Chipkartenleser oder Token.

TCP/IP

Das Netzwerk-Protokoll TCP/IP muss auf dem Rechner installiert sein.

2.2 LANCOM Advanced VPN Client installieren und aktivieren

Zur Installation des LANCOM Advanced VPN Clients legen Sie bitte die mitgelieferte CD in Ihr CD-ROM-Laufwerk. Sollte das Setup-Programm nach einigen Sekunden nicht automatisch starten, öffnen Sie bitte die Datei „autostart.exe" aus dem Stammverzeichnis der CD. Der folgende Assistent leitet Sie durch die weiteren Schritte der Installation. Wählen Sie dabei die 'Standard-Installation' aus.

- Beginnen Sie die Installation mit dem Punkt **LANCOM Software**.
- Fahren Sie mit der Option **LANCOM Advanced VPN Client installieren** fort.

Sollte bereits eine frühere Version des Clients vorhanden sein, so wird diese automatisch erkannt und es wird ein Update durchgeführt.

Zur vollständigen Installation ist ein Neustart erforderlich.

DE

Aktivierung

Nach dem Neustart ist der LANCOM Advanced VPN Client bereits vollständig installiert. Sie können den LANCOM Advanced VPN Client vor der Aktivierung 30 Tage lang testen. Nach dem Start des Clients erscheint das Hauptfenster.

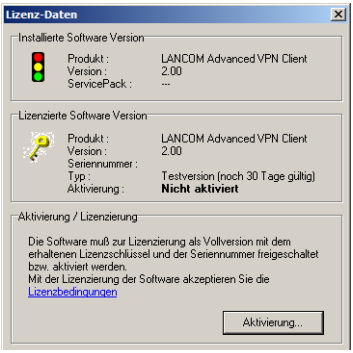
Um nach der 30 Tage Testphase den vollen Funktionsumfang nutzen zu können ist eine Produktaktivierung notwendig. Hierfür stehen drei mögliche Szenarien zur Verfügung:

- Es handelt sich um eine Erstinstallation mit Erwerb einer vollen Lizenz.
- Ein Software- und Lizenz-Upgrade von einer früheren Version mit Erwerb einer neuen Lizenz. Hier können alle neuen Funktionen der neuen Version benutzt werden.
- Ein Software-Update als reines Buxfixing. Sie behalten Ihre bisherige Lizenz bei. Hierbei wird zwar die neue Client-Version installiert, jedoch steht dem Anwender nur die Funktionalität der bisherigen Version zur Verfügung.

In jedem Fall sind folgende Schritte abzuarbeiten:

DE

1. Klicken Sie im Hauptfenster auf **Aktivierung**. Im folgenden erscheint ein Dialog, der ihre aktuelle Versionsnummer und die verwendete Lizenz anzeigt.



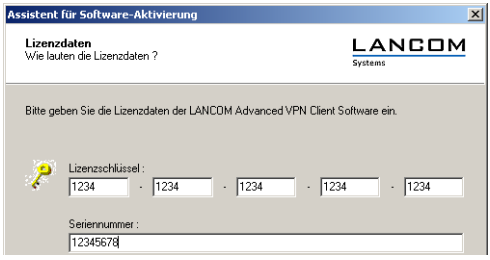
Dieser Dialog kann alternativ im Hauptfenster über den Menüpunkt **Hilfe ▶ Lizenzinfo und Aktivierung** aufgerufen werden.

2. Klicken sie hier erneut auf **Aktivierung**. Sie können die Aktivierung online oder offline vornehmen.

Auch für die „Offline-Aktivierung“ wird ein Zugang zum Internet benötigt.

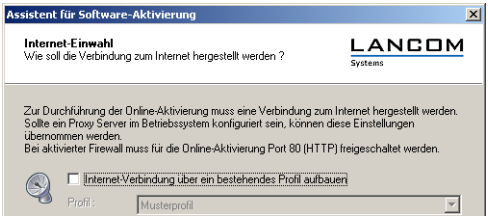
Online-Aktivierung

1. Falls sie die Online-Aktivierung wählen, geben sie in folgendem Dialog ihre Lizenzdaten ein. Diese haben sie mit dem Erwerb des LANCOM Advanced VPN Client erhalten.



DE

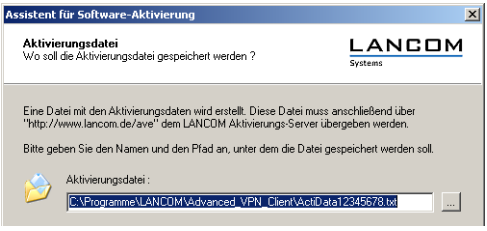
2. Nun muss der Client eine Verbindung zum LANCOM-Server herstellen.



Falls sie bereits eine ältere Version des LANCOM Advanced VPN Client benutzen, können sie ein bereits eingerichtetes VPN-Profil zur Verbindung mit dem Internet verwenden. Sobald der Computer über eine Verbindung mit dem Internet verfügt, verbindet er sich automatisch mit dem LANCOM-Server. Die Aktivierung erfolgt nun ohne weiteres Zutun und der Vorgang schließt selbstständig ab.

Offline-Aktivierung

1. Falls Sie die Offline-Aktivierung gewählt haben, müssen sie wie bei der Aktivierung zunächst ihre Lizenzdaten und die Seriennummer eingeben. Diese werden dann überprüft und in einer Datei auf Festplatte gespeichert. Den Dateinamen können sie frei wählen, es muß sich allerdings um eine Textdatei (.txt) handeln.

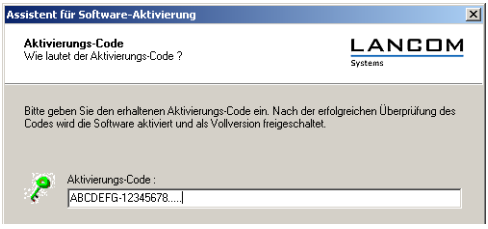


2. In dieser Aktivierungsdatei sind ihre Lizenzdaten enthalten. Zur Aktivierung muß diese Datei dem LANCOM-Server übergeben werden. Starten

sie dazu ihren Browser und öffnen Sie die Site www.lancom.de/avc/activation.

3. Klicken sie auf **Durchsuchen** und wählen Sie die eben erstellte Aktivierungsdatei aus. Im Anschluß daran klicken Sie auf **Absenden**. Die Aktivierungsdatei wird nun vom LANCOM-Server bearbeitet. Sie werden nun auf eine Website weitergeleitet, der Sie ihren Aktivierungs-Code entnehmen können. Drucken Sie diese Seite aus oder notieren Sie sich den angegebenen Code.

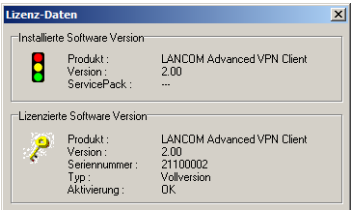
4. Wechseln sie wieder zum LANCOM Advanced VPN Client und klicken sie im Hauptfenster auf **Aktivierung**. Geben sie im folgenden Dialog den Code ein, den Sie ausgedruckt oder notiert haben.



DE

5 Mit der Eingabe des Aktivierungs-Codes ist die Produktaktivierung abgeschlossen und sie können den LANCOM Advanced VPN Client im Umfang ihrer Lizenz benutzen.

Abhängig von der von Ihnen erworbenen Lizenz wird nun die Lizenz- und Versions-Nummer angezeigt.



2.3 Vor der Inbetriebnahme

Nach der Installation zeigt sich der Client Monitor wie in untenstehender Abbildung.

Um den Secure Entry Client nutzen zu können, muss zunächst in den Profil-Einstellungen ein Eintrag erzeugt werden, d.h. ein Zielsystem definiert werden, zu dem eine IPSec-Verbindung hergestellt werden kann.

Beachten Sie zur Konfiguration eines Zielsystems vor allem die Beschreibungen unter "3. Client Monitor":

- Konfiguration / Profil-Einstellungen (Die Einträge der Profil-Einstellungen)
- Konfiguration / IPSec (Die Einträge der IPSec-Konfiguration)

und zur weiteren Parametrisierung:

- Profil-Einstellungen (Die Parameterfelder zur Konfiguration der Verbindung)

- IPSec (Die Parameterfelder zur Konfiguration der Richtlinien)

Erst nach der Einrichtung eines Zielsystems in den Profil-Einstellungen kann eine Verbindung dorthin hergestellt werden:

- Eine Verbindung herstellen

DE

3 Client Monitor

Wenn die Software installiert wurde, kann der Monitor über das **Start > Programme > LANCOM > LANCOM Advanced VPN Client** aktiviert werden. Damit öffnet sich das Fenster des Monitors auf dem Bildschirm.

Hinweis: Wenn der Monitor geladen wurde, erscheint er entweder auf dem Bildschirm oder, wenn er dort nicht dargestellt wird, in der Taskleiste.

Der Monitor hat vier wichtige Funktionen:

- den aktuellen Status der Kommunikation wiederzugeben
- den Verbindungsmodus einzustellen
- die Limits der Verbindungssteuerung bestimmen
- die Definition und Konfiguration der Profile zur Anwahl an ein Zielsystem

3.1 Monitor-Bedienung

Die Hauptmenüpunkte in der Menüleiste von links nach rechts sind:

- Verbindung [Menü]
- Konfiguration [Menü]
- Log [Menü]
- Fenster [Menü]
- Hilfe

3.1.1 Verbindung [Menü]

Das Pulldown-Menü hat folgende Menüpunkte:

- Verbinden
- Trennen
- HotSpot-Anmeldung (nur Windows-Version)
- Multifunktionskarte
- Verbindungs-Informationen
- Verfügbare Verbindungsmedien (nur Windows-Version)
- Zertifikate [Ansicht]
- PIN eingeben
- PIN zurücksetzen
- PIN ändern
- Sperre aufheben
- Beenden

Verbinden

Eine Verbindung wird aufgebaut. Eine Verbindung kann nur aufgebaut werden, wenn ein Profil aus der Liste der Profil-Einstellungen selektiert ist. Das selektierte Profil wird in der Monitoroberfläche unter der Menüleiste angezeigt.

Wenn Sie die Funktion **Verbinden** wählen, wird die Anwahl an das Ziel über das ausgewählte Profil manuell durchgeführt.

Wenn Sie, je nach Profil, die Verbindung manuell oder automatisch herstellen wollen, so können Sie dies in den Profil-Einstellungen mit dem Parameter Verbindungsaufbau im Feld "Timeout (Sek)" definieren (siehe **Konfiguration > Profil-Einstellungen > Konfigurieren > Line Management**).

DE

Trennen

Eine Verbindung kann manuell abgebaut werden mit der Funktion "Trennen" im Pull-down-Menü oder nach Klick auf die rechte Maustaste.

Wenn die Verbindung abgebaut wurde, wechseln die Signallampen des Monitors für die gesamte Offline-Dauer von grün zu rot.

HotSpot-Anmeldung

Nur für Windows-Version verfügbar.

Voraussetzungen: Der Rechner muss sich mit aktivierter WLAN-Karte im Empfangsbereich eines HotSpots befinden. Die Verbindung zum HotSpot muss hergestellt und eine IP-Adresse für den Wireless-Adapter muss zugewiesen sein. (Unter Windows XP steht eine entsprechende Konfiguration für den Zugriff auf WLANs zur Verfügung.)

Die Firewall des LANCOM Advanced VPN Client sorgt dafür, dass lediglich die IP-Adresszuweisung per DHCP erfolgen darf, weitere Zugriffe ins WLAN bzw. vom WLAN werden unterbunden. Die Firewall gibt dynamisch die Ports für http bzw. https für die Anmeldung bzw. Abmeldung am HotSpot frei. Dabei ist nur Datenverkehr mit dem HotSpot Server des Betreibers möglich. Ein öffentliches WLAN wird auf diese Weise ausschließlich für die VPN-Verbindung zum zentralen Datennetz genutzt. Direkter Internet-Zugriff ist ausgeschlossen. Damit die Anmeldeseite des HotSpots im Browser geöffnet werden kann, muss eine eventuelle Proxy-Konfiguration deaktiviert werden.

Derzeit unterstützt die HotSpot-Anmeldung des Clients ausschließlich HotSpots, die mit einer Umleitung (Redirect) einer Anfrage mit einem Browser auf die Anmeldeseite des öffentlichen WLAN-Betreibers arbeiten (z. B. T-Mobile oder Eurospot).

Sind obige Voraussetzungen erfüllt, so öffnet ein Klick auf den Menüpunkt "HotSpot-Anmeldung" die Website zur Anmeldung im Standard-Browser. Nach Eingabe der Zugangsdaten kann die VPN-Verbindung z. B. zur Firmenzentrale aufgebaut und sicher kommuniziert werden.

Die HotSpot-Anmeldung erfolgt über das Monitor-Menü "Verbindung / HotSpot-Anmeldung". Nachdem dieser Menüpunkt angeklickt wurde, können verschiedene Verbindungsmeldungen am Bildschirm erscheinen:

- Wenn sich der Benutzer bereits im Internet befindet, wird er mit der Startseite http://www.lancom.de verbunden. Es erscheint ein Fenster mit folgender Meldung:

  Dieser Text kann vom Administrator ausgetauscht werden, indem die Adresse einer anderen HTML-Startseite in der Form angegeben wird

  http://www.mycompany.de/error.html

  und der Text von error.html entsprechend geändert wird.

- Ist der Benutzer noch nicht angemeldet, erscheint ein Fenster mit der Aufforderung Benutzername und Passwort für die Anmeldung am HotSpot-Betreiber einzugeben.
- Wenn der Benutzer keine Website erreicht, erscheint die Microsoft-Fehlermeldung "... not found".

Multifunktionskarte

Nur für Windows-Version verfügbar.

Nachdem eine Multifunktionskarte installiert wurde (siehe dazu auch den Anhang dieses Handbuchs), wird dieser Menüpunkt dargestellt. Außerdem wird das Feld mit der Anzeige für UMTS / GPRS im Monitor eingeblendet und das WLAN-Panel ausgeblendet (siehe oben "Symbole des Monitors").

- **Netzsuche**

Die installierte Multifunktionskarte sucht nach dem Start des Monitors automatisch nach einem Funknetz und zeigt es mit der entsprechenden Feldstärke an, sobald es gefunden wurde (T-Online im Bild unten). Durch Anwahl des Menüpunkts oder des Buttons für "Netzsuche" kann eine erneute Netzsuche ausgelöst werden.

Bei zu geringer Feldstärke schaltet die Karte automatisch von der Datenübertragungstechnik UMTS auf GPRS, wobei die Verbindung bestehen bleibt.

Erhöht sich die Feldstärke wieder, schaltet die Karte automatisch wieder zurück.

Wurde eine Netzsuche durchgeführt, wird das Fenster zur Netzauswahl eingeblendet. Das gewünschte Netz kann aus einer Liste ausgewählt werden. Wird die erneute Netzsuche nach jedem Aufruf des Monitors nicht gewünscht, so muss die standardmäßig aktive Funktion über den Check-Button ausgeschaltet werden.

- **GPRS / UMTS aktivieren**

Die Datenübertragungstechnik kann auch manuell gewechselt werden. Dazu wird mit der Maus der Text mit der gewünschten Übertragungstechnik angeklickt oder dieser Menüpunkt gewählt. Bei einem manuellen Wechsel des Mediums wird die Verbindung zunächst abgebaut. Die Verbindung wird dann wieder automatisch aufgebaut, wenn "automatischer Verbindungsaufbau" im Telefonbuch konfiguriert wurde.

- **SIM PIN eingeben**

Der Dialog zur Eingabe der SIM PIN erscheint automatisch bei einem Verbindungsaufbau. Über diesen Menüpunkt kann die SIM PIN auch vor einem Verbindungsaufbau eingegeben werden.

- **SIM PIN ändern**

Die Änderung der SIM PIN kann nur vorgenommen werden, wenn die bisherige SIM PIN korrekt eingegeben wurde.

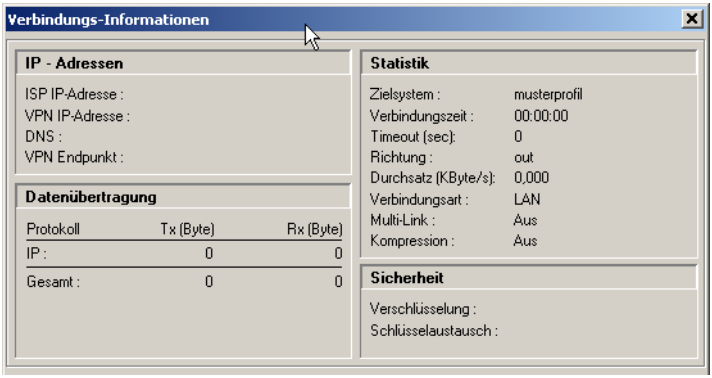
- **PUK Eingabe**

Nach dreimaliger Falscheingabe der SIM PIN erscheint das Fenster zur Eingabe des PUK (Personal Unblocking Key), welcher der SIM-Karte beiliegt. Nach korrekter Eingabe des PUK kann eine neue SIM PIN eingegeben werden.

Verbindungs-Informationen

Wenn Sie den Menüpunkt "Verbindungs-Informationen" anklicken, werden statistische Werte gezeigt. Darüber hinaus aber auch welche Security-Schlüs-

sel (SSL mit Zertifikat, Blowfish ...) verwendet werden und welche IP-Adressen über PPP-Verhandlung zwischen Client und Server ausgetauscht werden.

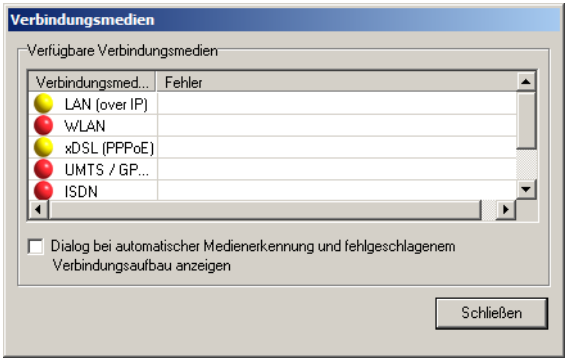


Der Monitor mit den Verbindungs-Informationen hat keinerlei Einfluss auf die Funktionen der Client-Software.

Verfügbare Verbindungsmedien

Nur für Windows-Version verfügbar.

Dieses Fenster dient ausschließlich der Benutzerinformation über die zur Verfügung stehenden Verbindungsmedien und das aktuell genutzte Medium. Werden wechselweise unterschiedliche Verbindungsarten genutzt, so erkennt der Client automatisch, welche Medien aktuell zur Verfügung stehen und wählt davon das schnellste aus.



Die zur Verfügung stehenden Verbindungsarten werden mit gelber Signallampe dargestellt, die ausgewählte Verbindungsart mit einer grünen.

Mit der Checkbox kann eingestellt werden, dass dieses Fenster bei automatischer Medienerkennung selbständig aufgeblendet wird, wenn der Verbindungsaufbau fehlgeschlagen ist. Das Fenster wird auch dann am Bildschirm eingeblendet, wenn der Client-Monitor minimiert ist. Hinter der genutzten Medienart wird der Fehler bezeichnet.

Zur Konfiguration der automatischen Medienerkennung beachten Sie in den Profil-Einstellungen das Parameterfeld "Grundeinstellungen".

Zertifikate [Ansicht]

Im Pulldown-Menü "Verbindung" finden Sie den Menüpunkt "Zertifikate" mit den Menüabzweigungen "Konfiguration", "Aussteller-Zertifikat anzeigen", "Eingehendes Zertifikat anzeigen" und "CA-Zertifikate anzeigen".

Zertifikate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt und auf eine Smart Card (Chipkarte) gebrannt. Diese Smart Card enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen.

Aussteller-Zertifikat anzeigen

Wenn Sie sich das Aussteller-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z.B. die eindeutige E-Mail-Adresse.

Aussteller (CA): Benutzer und Aussteller eines Aussteller-Zertifikates sind für gewöhnlich identisch (selfsigned certificate). Der Aussteller des Aussteller-Zertifikats muss mit dem Aussteller des Benutzer-Zertifikats identisch sein (siehe -> Benutzer-Zertifikat anzeigen).

Seriennummer: Nach der Seriennummer werden die Zertifikate mit den in der Revocation List der Certification Authority gehaltenen verglichen.

Gültigkeitsdauer: Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit dem Erlöschen der Gültigkeit des Aussteller-Zertifikats erlischt automatisch die Gültigkeit eines vom gleichen Aussteller ausgestellten Benutzer-Zertifikates.

Fingerprint: = Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

Benutzer-Zertifikat anzeigen

Wenn Sie sich Ihr Benutzer-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z.B. die eindeutige E-Mail-Adresse.

Austeller (CA): Der Aussteller Ihres Benutzer-Zertifikates muss mit dem Aussteller des Aussteller-Zertifikates identisch sein. (siehe -> Aussteller-Zertifikat anzeigen).

Seriennummer: Nach der Seriennummer werden die Zertifikate mit den in der Revokation List der Certification Authority gehaltenen verglichen.

Gültigkeitsdauer: Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit Erlöschen der Gültigkeit geht auch die Funktion des Zertifikats verloren.

Fingerprint: = Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

- **Eingehendes Zertifikat anzeigen**

Anzeige des Zertifikats, das bei der SSL-Verhandlung von der Gegenstelle (VPN Gateway) übermittelt wird. Sie können z.B. sehen, ob Sie den hier gezeigten Aussteller in der Liste Ihrer CA-Zertifikate (siehe unten) aufgenommen haben.

Ist das eingehende Benutzer-Zertifikat einer der CAs aus der Liste "CA-Zertifikate anzeigen" nicht bekannt, kommt die Verbindung nicht zustande.

Sind keine CA-Zertifikate im Windows-Verzeichnis CaCerts\ gespeichert, so findet keine Überprüfung statt.

Allgemein

In der allgemeinen Anzeige finden Sie die Angaben zu Benutzer und Aussteller der Zertifikats (die bei einem Aussteller-Zertifikat identisch sind), sowie die Seriennummer, die Angaben zur Gültigkeitsdauer und den Fingerprint.

Erweiterungen

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den LANCOM Advanced VPN Client und das VPN Gateway sind drei Erweiterungen von Bedeutung:

- extendedKeyUsage

- subjectKeyIdentifier
- authorityKeyIdentifier

extendedKeyUsage:

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der LANCOM Advanced VPN Client, ob der definierte erweiterte Verwendungszweck die "SSL-Server-Authentisierung" ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss

subjectKeyIdentifier / authorityKeyIdentifier:

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades. Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.

- **CA-Zertifikate anzeigen**

Mit der Client Software werden mehrere Aussteller-Zertifikate unterstützt (Multi CA-Unterstützung). Dazu müssen die Aussteller-Zertifikate im Windows-Verzeichnis CaCerts\ gesammelt werden. Im Monitor des Clients wird die Liste der eingespielten CA-Zertifikate angezeigt unter dem Menüpunkt **Verbindung > Zertifikate > CA-Zertifikate**.

Wird das Aussteller-Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat,

zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis CaCerts\.

Ist das Aussteller-Zertifikat nicht bekannt, kommt die Verbindung nicht zustande (No Root Certificate found).

Sind keine CA-Zertifikate im Windows-Verzeichnis CaCerts\ vorhanden, so wird keine Verbindung unter Einsatz von Zertifikaten zugelassen.

Allgemein

In der allgemeinen Anzeige finden Sie die Angaben zu Benutzer und Aussteller der Zertifikats (die bei einem Aussteller-Zertifikat identisch sind), sowie die Seriennummer, die Angaben zur Gültigkeitsdauer und den Fingerprint.

Erweiterungen

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den LANCOM Advanced VPN Client und das VPN Gateway sind drei Erweiterungen von Bedeutung:

- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier

extendedKeyUsage:

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der LANCOM Advanced VPN Client, ob der definierte erweiterte Verwendungszweck "SSL-Server-Authentisierung" enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss

subjectKeyIdentifier / authorityKeyIdentifier:

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades. Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.

PIN eingeben

Die PIN-Eingabe kann bereits vor einem Verbindungsaufbau erfolgen, nachdem der Monitor gestartet wurde. Wird zu einem späteren Zeitpunkt eine Verbindung aufgebaut, die ein Zertifikat erfordert, so kann dann die PIN-Eingabe unterbleiben - es sei denn, die Konfiguration zum Zertifikat verlangt es (siehe -> Konfiguration, Zertifikat).

Haben Sie den Menüpunkt "Verbindung - PIN eingeben" gewählt, kann in das geöffnete Eingabefeld die PIN (mindestens 6-stellig) eingegeben werden und mit **OK** bestätigt werden. Die Ziffern der PIN werden als Sterne "*" am Bildschirm dargestellt.

Sofern die PIN noch nicht vor einem Verbindungsaufbau eingegeben wurde, erscheint der Dialog zur PIN-Eingabe spätestens wenn die erste Verbindung zu einem Ziel hergestellt werden soll, das die Verwendung eines Zertifikats erfordert. Nachfolgend kann bei einem wiederholten manuellen Verbindungsaufbau die PIN-Eingabe unterbleiben, wenn dies so konfiguriert wurde (siehe -> Konfiguration, Zertifikate).

Wenn Sie den LANCOM Advanced VPN Client zur Verwendung einer Smart Card oder eines PKCS#11-Moduls konfiguriert haben (siehe -> Konfiguration, Zertifikate), erscheint im Statusfeld ein hellblaues Symbol für die Smart Card. Wenn Sie Ihre Smart Card in das Lesegerät gesteckt haben, ändert sich die Farbe des Symbols von hellblau zu grün.

DE

Wurde der LANCOM Advanced VPN Client zur Verwendung eines Soft-Zertifikats konfiguriert (siehe -> Konfiguration, Zertifikate), erscheint im Statusfeld kein eigenes Symbol.

Wurde die PIN korrekt eingegeben, so wird dies in der Monitoroberfläche mit einem grünen Haken hinter "PIN" dargestellt.

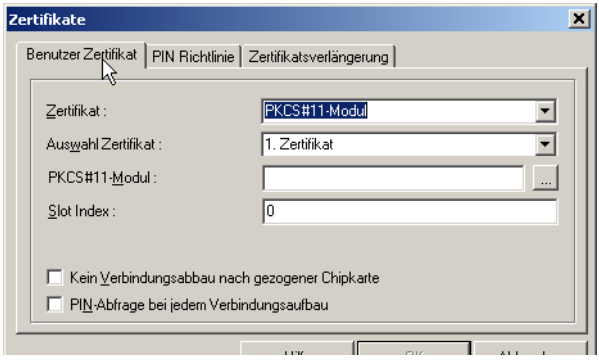
Fehlerhafte Eingaben und falsche PINs werden nach ca. 3 Sekunden mit einer Fehlermeldung "Falsche PIN!" quittiert. Ein Verbindungsaufbau ist dann nicht möglich.

Bitte beachten Sie, dass bei mehrmaliger falscher PIN-Eingabe eine Smart Card oder ein Token gesperrt werden kann. Wenden Sie sich in diesem Fall an Ihren Administrator.

Erst nach korrekter PIN-Eingabe kann der Verbindungsaufbau erfolgen.

Wird eine Smart Card oder ein Token während des laufenden Betriebs entfernt, findet standardmäßig ein Verbindungsabbau statt.

Der Verbindungsabbau muss jedoch nicht bei gezogener Chipkarte erfolgen! Ob "Kein Verbindungsabbau bei gezogener Chipkarte" erfolgt, wird über das Hauptmenü des Monitors unter dem Menüpunkt **Konfiguration > Zertifikate** eingestellt.



Die Richtlinien zur PIN-Eingabe können im Hauptmenü unter **Konfiguration > Zertifikate** festgelegt werden (siehe -> Konfiguration, Zertifikate, PIN-Richtlinie). Diese Richtlinien müssen auch befolgt werden, wenn die PIN geändert wird (siehe -> Verbindung, PIN ändern).

Bitte beachten Sie: Unter dem Menüpunkt "PIN ändern" kann die PIN für eine Smart Card oder ein Soft-Zertifikat geändert werden, wenn

vorher die richtige PIN eingegeben wurde. Ohne die vorherige Eingabe einer gültigen PIN wird dieser Menüpunkt nicht aktiviert.

PIN zurücksetzen

Dieser Menüpunkt ist nur aktiv, wenn die PIN bereits richtig eingegeben wurde, d. h. das Zertifikat für die aufzubauende Verbindung genutzt werden soll. Wird die PIN zurückgesetzt, kann dieses Zertifikat für einen Verbindungsaufbau nicht mehr genutzt werden, bis die dazugehörige PIN wieder richtig eingegeben wurde.

PIN ändern

Unter diesem Menüpunkt kann die PIN für eine Smart Card oder ein Soft-Zertifikat geändert werden, wenn vorher die richtige PIN eingegeben wurde (siehe -> PIN eingeben). Ohne die vorherige Eingabe einer gültigen PIN wird dieser Menüpunkt nicht aktiviert.

Aus Sicherheitsgründen, um die PIN-Änderung nur für den authorisierten Benutzer zuzulassen, muss nach Öffnen dieses Dialogs die noch gültige PIN ein zweites Mal eingegeben werden. Die Ziffern der PIN werden in diesem und den nächsten Eingabefeldern als Sterne "*" dargestellt.

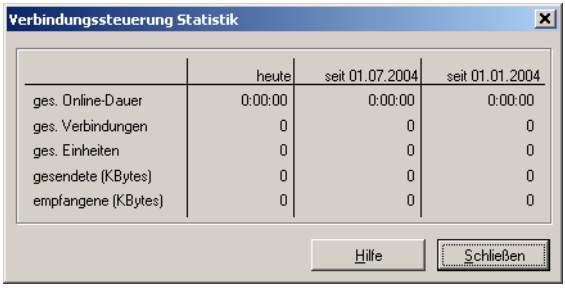
Anschließend geben Sie Ihre neue PIN ein und bestätigen diese durch Wiederholung im letzten Eingabefeld. Mit Klick auf **OK** haben Sie Ihre PIN geändert.

Die einzuhaltenden PIN-Richtlinien werden unter den Eingabefeldern eingeblendet. Sie können im Hauptmenü unter **Konfiguration > Zertifikate > PIN-Richtlinien** eingestellt werden.

Verbindungssteuerung Statistik

Die Statistik gibt Ihnen Auskunft über Ihre Datenkommunikation. In ihr werden sowohl gesondert als auch aufaddiert die gesamten Online-Zeiten, die gesamte Anzahl der Verbindungen und die gesamten Einheiten, sowie emp-

fangene und gesendete KBytes für den aktuellen Tag, den laufenden Monat und das laufende Jahr angezeigt.



Sperre aufheben

Je nachdem, wie die Verbindungssteuerung eingestellt ist, erhalten Sie bei Überschreiten eines Limits Meldungen auf dem Bildschirm.

Wird ein Limit überschritten und die Verbindung automatisch abgebaut, wird eine Sperre aktiv, die jeden weiteren Verbindungsaufbau unterbindet (-> siehe "Verbindung"-Menü im Monitor).

Eine Verbindung kann erst dann wieder neu aufgebaut werden, wenn Sie die Sperre aufheben.

Beenden

Beenden (des Monitors): Wurde die Verbindung bereits getrennt, beendet ein Klick auf diesen Menüpunkt oder der Schließen-Button den Monitor. Besteht noch eine Verbindung, kann nach Klick auf diesen Menüpunkt oder den Schließen-Button der Monitor ebenfalls beendet werden. Beachten Sie jedoch unbedingt, dass die Verbindung dabei nicht automatisch getrennt wird. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung von der Software verlangt.

Klicken Sie in diesem Bestätigungsfenster auf "Nein", so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um eine bestehende Verbindung korrekt zu beenden!

DE

3.1.2 Konfiguration [Menü]

Das Pulldown-Menü hat folgende Menüpunkte:

- Profil-Einstellungen [Menü]
- Erweiterte Firewall-Einstellungen [Menü]
- WLAN-Einstellungen (nur Windows-Version)
- Amtsholung (nur Windows-Version)
- Zertifikate [Einstellungen]
- Verbindungssteuerung [Einstellungen]
- EAP-Optionen [Einstellungen] (nur Windows-Version)
- Logon Optionen
- Konfigurations-Sperren
- Profile importieren
- HotSpot (nur Windows-Version)
- Profil-Sicherung

Sobald die Software installiert und ein Profil korrekt konfiguriert wurde, kann die Anwahl über dieses Profil an ein Zielsystem stattfinden. Dabei ist es nicht nötig, die Anwahl manuell durchzuführen, um eine Verbindung herzustellen.

Lediglich die gewünschte Applikations-Software (Email, Internet Browser, Terminal Emulation, etc.) muss gestartet werden. Die Verbindung wird dann, entsprechend den Parametern des Profils, automatisch aufgebaut und gehalten.

Daneben ist es auch möglich manuell eine Verbindung herzustellen, indem Sie im Monitor den Hauptmenüpunkt "Verbindung" anklicken und "Verbinden" wählen. Alternativ kann auch der Button "Verbinden" am Monitor angeklickt werden.

Profil-Einstellungen [Menü]

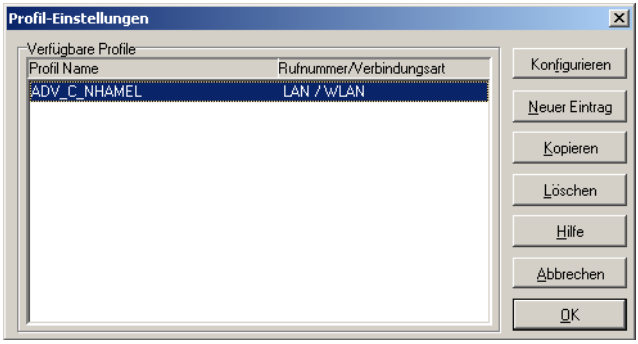
Die Einträge der Profil-Einstellungen

Bei einer Erstinstallation der LANCOM Advanced VPN Client Software ist noch kein Profil vorhanden. In diesem Fall wird automatisch ein Konfigurations-Assistent eingeblendet, der Ihnen hilft, Konfigurationen anzulegen. Damit wird zugleich das erste Profil der LANCOM Advanced VPN Client Software angelegt.

Mit den Profil-Einstellungen kann die Parametrisierung für die Zielsysteme (Profil) durchgeführt und die Übertragungsart, den Benutzeranforderungen entsprechend, bis ins Detail konfiguriert werden.

Nachdem Sie auf **Konfiguration > Profil-Einstellungen** in der Menüleiste des Monitors geklickt haben, öffnet sich das Menü und zeigt in einer Liste der bereits verfügbaren Profile deren Namen und die Rufnummern der zugehörigen Zielsysteme.

Auf der rechten Seite der Profil-Einstellungen sind Buttons angebracht zu folgenden Funktionen: **Konfigurieren**, **Neuer Eintrag**, **Kopieren**, **Löschen**, **OK**, **Hilfe** und **Abbrechen**.



Neuer Eintrag - Profil

Um ein neues Profil zu definieren, klicken Sie in der Menüleiste auf "Profil-Einstellungen". Das Fenster des Menüs öffnet sich nun und zeigt die bereits definierten Profile. Klicken Sie jetzt auf "Neuer Eintrag". Jetzt legt der "Assistent für ein neues Profil" mit Ihrer Hilfe ein neues Profil an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder des Profils werden Standardwerte eingetragen, die Sie unter dem Menüpunkt "Konfigurieren" (siehe -> Konfigurieren - Profil) auch ändern können.

Das neue Profil erscheint nun in der Liste der Profile mit dem von Ihnen vergebenen Namen. Wenn keine weiteren Parameter-Einstellungen nötig sind, können Sie die Liste mit OK schließen. Das neue Profil ist im Monitor sofort verfügbar. Es kann im Monitor ausgewählt werden und über das Menü "Verbindung -> Verbinden" kann das zugehörige Ziel sofort angewählt werden.

DE

Konfigurieren - Profil

Um die (Standard-)Werte eines Profils zu editieren, wählen Sie mit der Maus das Profil, dessen Werte Sie ändern möchten, und klicken anschließend auf "Konfigurieren". Die Profil-Einstellungen zeigen nun in ihrem linken Fenster eine Liste von Begriffen, denen jeweils ein Parameterfeld zugeordnet ist:

Grundeinstellungen Netzeinwahl Modem Line Management IPSec-Einstellungen Identität IP-Adressen-Zuweisung VPN IP-Netze Zertifikats-Überprüfung Firewall-Einstellungen

Ok - Profil

Die Konfiguration eines Profils ist abgeschlossen, wenn Sie das Konfigurationsfenster mit **OK** schließen. Das neue oder geänderte Profil ist im Monitor sofort verfügbar. Es kann im Monitor ausgewählt werden und über das Menü "Verbindung -> Verbinden" sofort zur Anwahl an das Zielsystem verwendet werden.

Kopieren - Profil

Um die Parameter-Einstellungen eines bereits definierten Profils zu kopieren, markieren sie das zu kopierende Profil in der Liste und klicken Sie auf den Kopieren-Button. Daraufhin wird das Grundeinstellungen-Parameterfeld geöffnet. Ändern Sie nun den Eintrag in "Profil-Name" und klicken Sie anschließend Ok. Nur wenn Sie den Namen des Profils ändern, kann es auch als neuer Eintrag in der Liste der Profile vermerkt werden.

Ein kopiertes Profil muss einen neuen, noch nicht vergebenen, Namen erhalten. Nur so kann es in der Liste der Profile abgelegt werden.

Löschen - Profil

Um ein Profil zu löschen, wählen Sie es aus und klicken den Löschen-Button.

Firewall-Einstellungen

Alle Firewall-Mechanismen sind optimiert für Remote Access-Anwendungen und werden bereits beim Start des Rechners aktiviert. D.h. im Gegensatz zu VPN-Lösungen mit eigenständiger Firewall ist der Telearbeitsplatz bereits vor der eigentlichen VPN-Nutzung gegen Angriffe geschützt.

Die Firewall bietet auch im Fall einer Deaktivierung der Client-Software vollen Schutz des Endgerätes.

Bitte beachten Sie, dass die Firewall-Einstellungen global gültig sind, d.h. für alle in den Profilen gespeicherten Zielsysteme.

Dagegen ist die Einstellung der Link Firewall, die im Profil vorgenommen werden kann, nur für das dazu gehörenden Zielsystem und die Verbindung zu diesem Zielsystem wirksam.

Eigenschaften der Firewall

Die Firewall arbeitet nach dem Prinzip der Paketfilterung in Verbindung mit Stateful Packet Inspection (SPI). Die Firewall prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis des konfigurierten Regelwerks, ob ein Datenpaket weitergeleitet oder verworfen wird.

Sicherheit wird in zweierlei Hinsicht gewährleistet:

- Zum einen wird der unbefugte Zugriff auf Daten und Ressourcen im zentralen Datennetz verhindert.
- Zum anderen wird mittels Stateful Inspection der jeweilige Status bestehender Verbindungen überwacht.

Die Firewall kann darüber hinaus erkennen, ob eine Verbindung „Tochterverbindungen" geöffnet hat – wie beispielsweise bei FTP – deren Pakete ebenfalls weitergeleitet werden müssen. Wird eine Regel für eine ausgehende Verbindung definiert, die einen Zugriff erlaubt, so gilt die Regel automatisch für entsprechende Antwortpakete. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf.

Stateful Inspection Firewall erkennt automatisch „Tochterverbindungen"

Die Stateful Inspection Firewall ist in der Lage, automatisch alle Tochterverbindungen folgender Protokolle zu erkennen:

- TCP, UDP
- FTP (active und passive Mode)
- ICMP

Wenn Applikationen zusätzlich zur Hauptverbindung dynamisch weitere Ports benötigen, so können diese über anwendungsspezifische Firewall-Regeln bereitgestellt werden (z.B. für bestimmte Multimedia-Anwendungen auf Basis H.323).

Die Firewall-Regeln können dynamisch konfiguriert werden, d.h. ein Anhalten der Software oder ein Neustart des Systems ist nicht nötig.

Die Firewall-Einstellungen im Konfigurationsmenü des Client-Monitors gestatten eine genaue Spezifikation von Firewall-Filterregeln. Sie wirken global. D.h. unabhängig vom aktuell gewählten Zielsystem werden immer zuerst die Regeln der erweiterten Firewall-Einstellungen abgearbeitet, bevor die Regeln der Firewall aus den einzelnen Profilen angewendet werden.

Eine Kombination der globalen und link-bezogenen Firewall kann in bestimmten Szenarien durchaus sinnvoll sein. Im Allgemeinen sollten jedoch nahezu alle Anforderungen über die globalen Einstellungsmöglichkeiten abzudecken sein.

Bitte beachten Sie, dass die link-bezogenen Firewall-Einstellungen bei Aktivierung Vorrang vor den globalen haben. Ist z.B. die Link-Firewall auf 'immer' und 'Ausschließlich Kommunikation im Tunnel zulassen' eingestellt, kann trotz evtl. anders lautender Regeln der globalen Konfiguration nur ein Tunnel aufgebaut und darüber kommuniziert werden. Jeglicher anderer Datenverkehr wird von der Link-Firewall verworfen.

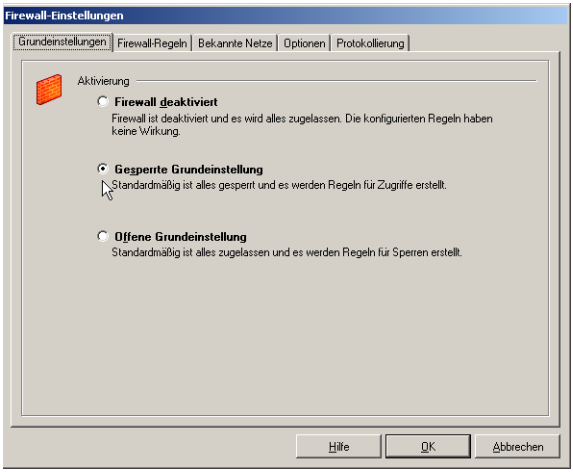
Konfiguration der Firewall-Einstellungen

Die Filterregeln der Firewall können sowohl anwendungsbezogen als auch (zusätzlich) adressorientiert, bezüglich bekannter/unbekannter Netze, definiert werden.

Bitte beachten Sie, dass der gleichzeitige Betrieb von zwei Firewalls auf einem Rechner zu unvorhersehbaren Ereignissen führen kann. Prüfen Sie daher vor dem Einsatz der Firewall im LANCOM Advanced VPN Client, ob ggf. eine andere Personal Firewall auf dem Rechner aktiv ist (z. B. Internetverbindungsfirewall von Windows XP).

Grundeinstellungen

Auf der Registerkarte 'Grundeinstellungen' wird die grundlegende Sicherheits-Policy der Firewall festgelegt:



- Firewall deaktiviert: Wird die erweiterte Firewall deaktiviert, so wird nur die in den Profilen konfigurierte Firewall genutzt. Dies bedeutet, dass alle Datenpakete nur über die Sicherheitsmechanismen dieser verbindungsorientierten Firewall abgearbeitet werden, sofern diese konfiguriert ist.
- Gesperrte Grundeinstellung: In diesem Zustand ist die Firewall aktiv und **sperrt** zunächst vollständig den Datenaustausch zwischen dem Rechner mit LANCOM Advanced VPN Client und allen anderen Rechnern oder Netzwerken. Dieses Verhalten entspricht einer „Deny-All"-Strategie. Um gezielt den Datenverkehr für bestimmte Rechner, Netzwerke oder Anwendungen freizugeben, müssen geeignete Firewall-Regeln den Datenaustausch erlauben.

Im Modus der gesperrten Grundeinstellung kann auf komfortable Weise eine L2Sec/IPSec-Tunnelkommunikation freigeschaltet werden. Dazu kann im Konfigurationsfeld 'Optionen' der Datenverkehr über VPN-Protokolle (L2Sec, IPSec) global zugelassen werden.

Mit der Freischaltung von L2Sec oder IPSec wird automatisch auch das DHCP-Protokoll freigeschaltet. Die über die Firewall geschützten Rechner können also auch in der gesperrten Grundeinstellung mit

aktiviertem VPN-Protokoll eine IP-Adresse und andere Adress-Informationen von einem erreichbaren DHCP-Server beziehen.

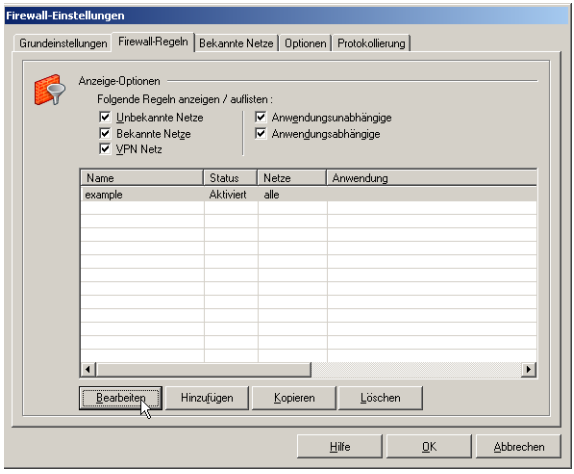
- Offene Grundeinstellung: In diesem Zustand ist die Firewall aktiv und **erlaubt** zunächst vollständig den Datenaustausch zwischen dem Rechner mit LANCOM Advanced VPN Client und allen anderen Rechnern oder Netzwerken. Dieses Verhalten entspricht einer „Allow-All"-Strategie. Um gezielt den Datenverkehr für bestimmte Rechner, Netzwerke oder Anwendungen zu blockieren, müssen geeignete Firewall-Regeln den Datenaustausch sperren.

LANCOM Systems empfiehlt dringend die Verwendung der gesperrten Grundeinstellung. Nur in dieser Einstellung kann der unkontrollierte Zugriff auf den Rechner mit LANCOM Advanced VPN Client verhindert werden.

Beim Nachträglichen Umschalten der Grundeinstellung von 'gesperrt' auf 'offen' oder umgekehrt werden alle bis dahin definierten Firewall-Regeln „umgedreht": Eine Allow-Regel in gesperrter Grundeinstellung wird in offener Grundeinstellung zu einer Deny-Regel und umgekehrt.

Firewall-Regeln

Auf der Registerkarte 'Firewall-Regeln' werden die vorhandenen Regeln der Firewall aufgelistet. Hier können neue Regeln angelegt sowie vorhandene Regeln bearbeitet, kopiert oder gelöscht werden.



Anzeige-Optionen

In den Anzeige-Optionen wird festgelegt, welche Firewall-Regeln in der Liste angezeigt werden. Zur Auswahl stehen:

- Unbekannte Netze: Es werden alle Regeln angezeigt, die auf unbekannte Netze angewendet werden.
- Bekannte Netze: Es werden alle Regeln angezeigt, die auf bekannte Netze angewendet werden.
- VPN Netze: Es werden alle Regeln angezeigt, die auf VPN Netze angewendet werden. Hierunter fallen auch verschlüsselte Direkteinwahlverbindungen z.B. über ISDN.
- Anwendungsunabhängige: Es werden alle Regeln angezeigt, die **nicht** nur für bestimmte Anwendungen gültig sind.
- Anwendungsabhängige: Es werden alle Regeln angezeigt, die **nur** für bestimmte Anwendungen gültig sind.

Diese Auswahlfelder für das Anzeigen der Regeln dienen nur der Übersichtlichkeit und haben keine Auswirkung auf die Anwendung einer Filterregel. Für jede definierte Regel werden die wichtigsten Eigenschaften gezeigt:

- Name
- Status
- Netz
- Anwendung

Durch Klick auf einen Überschrifts-Button werden die eingeblendeten Regeln entsprechend sortiert.

Die Anzeige-Optionen zum Netzbezug und zum Anwendungsbezug sind untereinander so verbunden, dass eine Regel nur dann angezeigt wird, wenn sowohl der Netzbezug als auch der Anwendungsbezug erfüllt sind. Eine Regel für 'Bekannte Netze' und 'VPN Netze' mit Bezug zur Anwendung 'outlook.exe' wird also nur dann in der Liste angezeigt, wenn sowohl die Anzeige-Optionen 'Anwendungsabhängige' als auch 'Bekannte Netze' oder 'VPN Netze' markiert sind.

Firewall-Regeln erstellen, ändern und löschen

Mit den Schaltflächen **Bearbeiten**, **Hinzufügen**, **Kopieren** und **Löschen** Bearbeiten Sie die Liste der Firewall-Regeln.

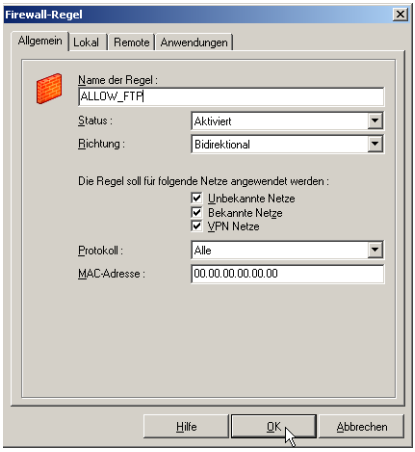
Die Firewall-Regeln werden immer nur dann auf ein Datenpaket angewendet, wenn alle in der Regel definierten Kriterien zutreffen. Nur wenn dieses „Matching“ erfolgreich ist, wird das Datenpaket je nach Grundeinstellung entweder zugelassen („Allow-Regel“) oder verworfen („Deny-Regel“).

Bitte beachten Sie, dass es sich bei den Firewall-Regeln je nach Grundeinstellung der Firewall ('gesperrt' oder 'offen') um „Allow“-Regeln oder um „Deny“-Regeln handelt (‘Grundeinstellungen’ →Seite 47).

DE

Allgemein

Auf der Registerkarte 'Allgemein' tragen Sie einen frei definierbaren Namen der Firewall-Regel ein. Außerdem stellen Sie die folgenden Optionen ein:



- Name der Regel: Unter diesem Namen erscheint die Regel in der Anzeigeliste.
- Status: Hier kann jede einzelne Regel ein- oder ausgeschaltet werden (aktiviert oder deaktiviert).
- Richtung: Gilt die Regel nur für eingehende, nur für ausgehende Datenpakete oder für beide Richtungen (bidirektional)?

Wird die Richtung auf 'ausgehend' gesetzt, wird nach dem Prinzip von Stateful Inspection gearbeitet (siehe 'Eigenschaften der Firewall'). Stateful Inspection wird jedoch nur für die Protokolle UDP, TCP, FTP (active und passive Mode) und ICMP angewendet.

Auf 'eingehend' kann z.B. dann geschaltet werden, wenn von Remote-Seite eine Verbindung aufgebaut werden soll (z.B. für 'eingehende Rufe' oder Administrator-Zugriffe).

Die Einstellung 'bidirektional' ist nur sinnvoll, wenn Stateful Inspection nicht zur Verfügung steht. Die Firewall verhält sich dann wie eine klassische Paket-Filter-Firewall. In diesen Fällen empfiehlt sich eher die Steuerung der Firewall über anwendungsspezifische Filterregeln, z. B. bei Netmeeting oder VoIP auf Basis von H.323.

DE

- Netze: Beim Neuanlegen einer Regel ist diese zunächst keinem Netz zugeordnet. Eine Regel kann erst dann gespeichert werden, wenn die gewünschte Zuordnung erfolgt ist und ein Name vorgegeben wurde.
  - Unbekannte Netze sind alle Netze, die nicht in der Liste der bekannten Netze eingetragen und die nicht in einer VPN-Verbindung als Ziel definiert sind. Darunter fallen z.B. Verbindungen über das DFÜ-Netzwerk von Microsoft oder auch direkte und unverschlüsselte Verbindungen mit dem integrierten Dialer des Clients, wie auch HotSpot WLAN-Verbindungen.
  - Bekannte Netze sind alle Netze, die in der Liste der bekannten Netze eingetragen sind.
  - VPN Netze sind alle Netze, die in einer VPN-Verbindung als Ziel definiert sind, also alle L2Sec- oder IPSec-Verbindungen in aufgebautem Zustand. Darüber hinaus fallen unter diese Gruppe auch alle verschlüsselten Direkteinwahlverbindungen über den integrierten Dialer des Clients.

Eine Firewall-Regel kann nur dann angelegt werden, wenn mindestens eine Gruppe von Netzen aktiviert ist.

- Protokoll: Wenn Sie hier optional ein Protokoll ausgewählt haben, dann wird die Regel nur auf Datenpakete angewendet, die das gewählte Protokoll verwenden.
- MAC-Adresse: Die MAC-Adresse ist weltweit eindeutig und lässt bei eingehenden Verbindungen nur Datenpakete zu, die von dem Gateway mit dieser MAC-Adresse stammen. Bei einer ausgehenden Verbindung wird unter Angabe der MAC-Adresse des Ziel-Gateways sichergestellt, dass der Client nur eine Verbindung zu diesem Ziel-Gateway aufbauen kann. Nach Aufbau einer VPN-Verbindung über dieses Gateway hat der Client Zugriff auf das Firmennetz je nach konfiguriertem Link-Profil. Dies ist eine sehr restriktive Regel, die sich nur in ganz speziellen Situationen sinnvoll anwenden lässt.

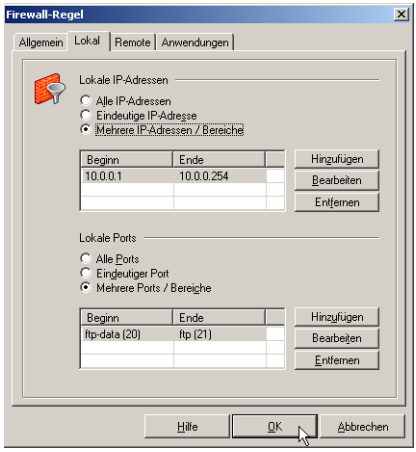
Lokal

Auf dieser Registerkarte werden die Filter für die lokalen IP-Adressen und IP-Ports eingestellt.

Je nachdem, ob die gerade zu definierende Regel 'ausgehenden', 'eingehenden' oder 'bidirektionalen' Datenverkehr betrifft (siehe

Registerkarte 'Allgemein'), haben die Begriff 'Lokale IP-Adressen' und 'Lokale Ports' unterschiedliche Bedeutung:

- Bei **ausgehenden** Regeln sind mit 'lokal' die Quell-IP-Adressen und Quell-IP-Ports gemeint und mit 'remote' die Ziel-IP-Adressen und Ziel-IP-Ports der Pakete.
- Bei **eingehenden** Regeln sind mit 'lokal' die Ziel-IP-Adressen und Ziel-IP-Ports gemeint und mit 'remote' die Quell-IP-Adressen und Quell-IP-Ports der Pakete.



- Lokale IP-Adressen: Wählen Sie hier aus, ob die Firewall-Regel für alle IP-Adressen, nur für eine bestimmte IP-Adresse oder für mehrere IP-Adressen bzw. Bereiche von IP-Adressen gelten soll.

  Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall-Regel zugelassen, deren IP-Adressen in diesem Bereich definiert sind. Dabei verhält sich die Firewall unterschiedlich je nach Einstellung der Verbindungsrichtung:

  - Bei einer Firewall-Regel für **ausgehenden** Datenverkehr werden ausgehende Datenpakete durchgelassen, deren **Quell**adresse im IP-Paket mit den unter 'Lokale IP-Adressen' definierten Adressen übereinstimmt.

    Bei Einsatz der Stateful Inspection – bei den Protokollen UDP, TCP, FTP (active und passive Mode) und ICMP – werden **zusätzlich** eingehende Datenpakete dann durchgelassen, wenn die **Ziel**adresse im IP-Paket mit den unter 'Lokale IP-Adressen' definierten Adressen übereinstimmt **und** die Datenverbindung vorher von einem lokalen Rech-

ner her aufgebaut wurde, die Verbindung also in der Stateful-Inspection-Verbindungsliste eingetragen ist. Versucht ein Angreifer ein Datenpaket in den geschützten Netzbereich abzusetzen, dessen **Ziel**adresse im IP-Paket zwar mit den unter 'Lokale IP-Adressen' definierten Adressen übereinstimmt, für den aber kein gültiger Eintrag in der Verbindungsliste vorhanden ist, so wird das Datenpaket verworfen.

- Bei einer Firewall-Regel für **eingehenden** Datenverkehr wird keine Stateful Inspection durchgeführt. Es werden alle eingehenden Datenpakete in den geschützten Bereich hereingelassen, deren **Ziel**adresse im IP-Paket mit den unter 'Lokale IP-Adressen' definierten Adressen übereinstimmt.
- Auch bei einer **bidirektionalen** Firewall-Regel wird keine Stateful Inspection durchgeführt. Es werden also alle **ausgehenden** Datenpakete durchgelassen, deren **Quell**adresse im IP-Paket mit den unter 'Lokale IP-Adressen' definierten Adressen übereinstimmt und alle **eingehenden** Datenpakete, deren **Ziel**adresse im IP-Paket mit den unter 'Lokale IP-Adressen' definierten Adressen übereinstimmt.

Folgende Möglichkeiten zur Definition der lokalen IP-Adressen können genutzt werden:

- Alle IP-Adressen: Umfasst alle Quell-IP-Adressen abgehender bzw. Ziel-IP-Adressen eingehender Pakete, unabhängig vom lokalen Netzwerkadapter.
- Eindeutige IP-Adresse: Ist die für den lokalen Netzwerkadapter definierte IP-Adresse. Sie kann je nach Verbindung z.B. der Adresse der Ethernet-Karte, der WLAN-Karte oder auch dem VPN-Adapter zugeordnet sein.
- Mehrere IP-Adressen: Bezeichnet einen Adressbereich oder Pool. Z.B. kann dies der IP-Adress-Pool sein, aus dem die vom DHCP Server an den Client zugewiesene Adresse stammt.

- Lokale Ports: Wählen Sie hier aus, ob die Firewall-Regel für alle Ports, nur für einen bestimmten Port oder für mehrere Ports bzw. Bereiche von Ports gelten soll.

  Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall-Regel zugelassen, deren Ports in diesem Bereich definiert sind. Dabei verhält sich die Firewall unterschiedlich je nach Einstellung der Verbindungsrichtung:

- Bei einer Firewall-Regel für **ausgehenden** Datenverkehr werden alle Datenpakete nach außen durchgelassen, deren Quell-Port im IP-Paket mit den unter 'Lokale IP-Ports' definierten Ports übereinstimmt.

  Bei Einsatz der Stateful Inspection – bei den Protokollen UDP, TCP, FTP (active und passive Mode) und ICMP – werden **zusätzlich** eingehende Datenpakete dann durchgelassen, wenn die **Ziel**-Ports im IP-Paket mit den zulässigen Ports übereinstimmt **und** die Datenverbindung vorher von einem lokalen Rechner her aufgebaut wurde.

  Zulässig sind alle Ports, die unter 'Lokale IP-Ports' definiert sind sowie die von der Stateful Inspection ggf. automatisch geöffneten Ports für bestimmte „Tocherverbindungen". Versucht ein Angreifer ein Datenpaket in den geschützten Netzbereich abzusetzen, dessen **Ziel**-Port im IP-Paket zwar mit den zulässigen Ports übereinstimmt, für den aber kein gültiger Eintrag in der Verbindungsliste vorhanden ist, so wird das Datenpaket verworfen.

- Bei einer Firewall-Regel für **eingehenden** Datenverkehr wird keine Stateful Inspection durchgeführt. Es werden alle eingehenden Datenpakete in den geschützten Bereich hereingelassen, deren **Ziel**-Port im IP-Paket mit den unter 'Lokale IP-Ports' definierten Ports übereinstimmt.
- Auch bei einer **bidirektionalen** Firewall-Regel wird keine Stateful Inspection durchgeführt. Es werden also alle **ausgehenden** Datenpakete durchgelassen, deren **Quell**-Port im IP-Paket mit den unter 'Lokale IP-Ports' definierten Ports übereinstimmt und alle **eingehenden** Datenpakete, deren **Ziel**-Port im IP-Paket mit den unter 'Lokale IP-Ports' definierten Ports übereinstimmt.

Folgende Möglichkeiten zur Definition der lokalen IP-Ports können genutzt werden:

- Alle Ports: Erlaubt Kommunikation über alle Quellports bei ausgehenden und alle Ziel-Ports bei eingehenden Paketen.
- Eindeutiger Port: Diese Einstellung sollte nur dann verwendet werden, wenn dieses System einen Server-Dienst zur Verfügung stellt (z.B. Remote Desktop auf Port 3389).
- Mehrere Ports: Diese Einstellung sollte nur dann verwendet werden, wenn sich die lokalen Ports zu einem Bereich zusammenfassen lassen, die von einem Dienst benötigt werden, der auf diesem System zur Verfügung gestellt wird (z.B. FTP Ports 20/21).

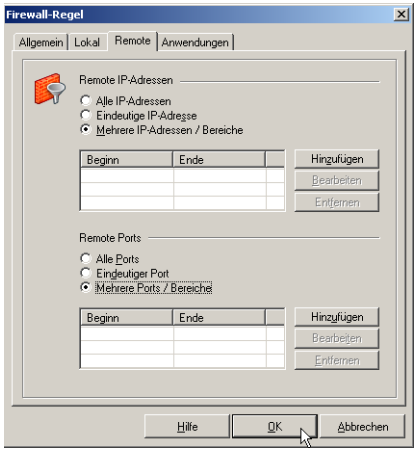
DE

Remote

Auf dieser Registerkarte werden die Filter für die lokalen IP-Adressen und IP-Ports eingestellt. Die Bedeutung der Einträge verläuft analog zu den lokalen IP-Adressen und Ports.

Je nachdem, ob die gerade zu definierende Regel 'ausgehenden', 'eingehenden' oder 'bidirektionalen' Datenverkehr betrifft (siehe Registerkarte 'Allgemein'), haben die Begriff 'Remote IP-Adressen' und 'Remote Ports' unterschiedliche Bedeutung:

- Bei **ausgehenden** Regeln sind mit 'remote' die Ziel-IP-Adressen und Ziel-IP-Ports gemeint und mit 'lokal' die Quell-IP-Adressen und Quell-IP-Ports der Pakete.
- Bei **eingehenden** Regeln sind mit 'remote' die Quell-IP-Adressen und Quell-IP-Ports gemeint und mit 'lokal' die Ziel-IP-Adressen und Ziel-IP-Ports der Pakete.



- Remote IP-Adressen: Wählen Sie hier aus, ob die Firewall-Regel für alle IP-Adressen, nur für eine bestimmte IP-Adresse oder für mehrere IP-Adressen bzw. Bereiche von IP-Adressen gelten soll.

  Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall-Regel zugelassen, deren IP-Adressen in diesem Bereich definiert sind. Dabei verhält sich die Firewall unterschiedlich je nach Einstellung der Verbindungsrichtung:

  - Bei einer Firewall-Regel für **ausgehenden** Datenverkehr werden ausgehende Datenpakete durchgelassen, deren **Ziel**adresse im IP-Paket

mit den unter 'Remote IP-Adressen' definierten Adressen übereinstimmt.

Bei Einsatz der Stateful Inspection – bei den Protokollen UDP, TCP, FTP (active und passive Mode) und ICMP – werden **zusätzlich** eingehende Datenpakete dann durchgelassen, wenn die **Quell**adresse im IP-Paket mit den unter 'Remote IP-Adressen' definierten Adressen übereinstimmt **und** die Datenverbindung vorher von einem lokalen Rechner her aufgebaut wurde, die Verbindung also in der Stateful-Inspection-Verbindungsliste eingetragen ist. Versucht ein Angreifer ein Datenpaket in den geschützten Netzbereich abzusetzen, dessen **Quell**adresse im IP-Paket zwar mit den unter 'Remote IP-Adressen' definierten Adressen übereinstimmt, für den aber kein gültiger Eintrag in der Verbindungsliste vorhanden ist, so wird das Datenpaket verworfen.

- Bei einer Firewall-Regel für **eingehenden** Datenverkehr wird keine Stateful Inspection durchgeführt. Es werden alle eingehenden Datenpakete in den geschützten Bereich hereingelassen, deren **Quell**adresse im IP-Paket mit den unter 'Remote IP-Adressen' definierten Adressen übereinstimmt.
- Auch bei einer **bidirektionalen** Firewall-Regel wird keine Stateful Inspection durchgeführt. Es werden also alle **ausgehenden** Datenpakete durchgelassen, deren **Ziel**adresse im IP-Paket mit den unter 'Remote IP-Adressen' definierten Adressen übereinstimmt und alle **eingehenden** Datenpakete, deren **Quell**adresse im IP-Paket mit den unter 'Remote IP-Adressen' definierten Adressen übereinstimmt.

Folgende Möglichkeiten zur Definition der remoten IP-Adressen können genutzt werden:

- Alle IP-Adressen: Erlaubt die Kommunikation mit beliebeigen IP-Adressen auf der Gegenseite (ohne Einschränkung).
- Eindeutige IP-Adresse: Läßt nur die Kommunikation mit der hier angegebenen IP-Adresse auf der Gegenseite zu.
- Mehrere IP-Adressen: Gestattet die Kommunikation mit verschiedenen IP-Adressen auf der Gegenseite entsprechend der hier vorgenommenen Einträge.

- Remote Ports: Wählen Sie hier aus, ob die Firewall-Regel für alle Ports, nur für einen bestimmten Port oder für mehrere Ports bzw. Bereiche von Ports gelten soll.

Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall-Regel zugelassen, deren Ports in diesem Bereich definiert sind. Dabei verhält sich die Firewall unterschiedlich je nach Einstellung der Verbindungsrichtung:

- Bei einer Firewall-Regel für **ausgehenden** Datenverkehr werden alle Datenpakete nach außen durchgelassen, deren Ziel-Port im IP-Paket mit den unter 'Remote IP-Ports' definierten Ports übereinstimmt.

  Bei Einsatz der Stateful Inspection – bei den Protokollen UDP, TCP, FTP (active und passive Mode) und ICMP – werden **zusätzlich** eingehende Datenpakete dann durchgelassen, wenn die **Quell**-Ports im IP-Paket mit den zulässigen Ports übereinstimmt **und** die Datenverbindung vorher von einem lokalen Rechner her aufgebaut wurde.

  Zulässig sind alle Ports, die unter 'Remote IP-Ports' definiert sind sowie die von der Stateful Inspection ggf. automatisch geöffneten Ports für bestimmte „Tocherverbindungen". Versucht ein Angreifer ein Datenpaket in den geschützten Netzbereich abzusetzen, dessen **Quell**-Port im IP-Paket zwar mit den zulässigen Ports übereinstimmt, für den aber kein gültiger Eintrag in der Verbindungsliste vorhanden ist, so wird das Datenpaket verworfen.

- Bei einer Firewall-Regel für **eingehenden** Datenverkehr wird keine Stateful Inspection durchgeführt. Es werden alle eingehenden Datenpakete in den geschützten Bereich hereingelassen, deren **Quell**-Port im IP-Paket mit den unter 'Remote IP-Ports' definierten Ports übereinstimmt.
- Auch bei einer **bidirektionalen** Firewall-Regel wird keine Stateful Inspection durchgeführt. Es werden also alle **ausgehenden** Datenpakete durchgelassen, deren **Ziel**-Port im IP-Paket mit den unter 'Remote IP-Ports' definierten Ports übereinstimmt und alle **eingehenden** Datenpakete, deren **Quell**-Port im IP-Paket mit den unter 'Remote IP-Ports' definierten Ports übereinstimmt.

Folgende Möglichkeiten zur Definition der lokalen IP-Ports können genutzt werden:

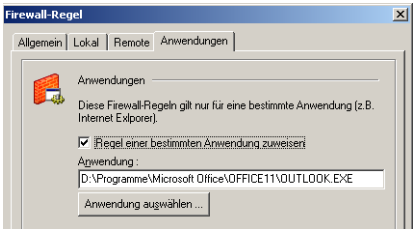
- Alle Ports: Erlaubt Kommunikation über alle Ziel-Ports bei ausgehenden und alle Quell-Ports bei eingehenden Paketen.
- Eindeutiger Port: Läßt nur eine Kommunikation über den angegebenen Port zu, wenn dieser als Ziel-Port bei ausgehenden bzw. als Quell-Port bei eingehenenden IP-Paketen verwendet wird. Soll z.B. eine

Firewall-Regel nur Telnet zu einem anderen System zulassen, so ist hier der Port '23' einzutragen.

- Mehrere Ports: Diese Einstellung sollte nur dann verwendet werden, wenn sich die remote Ports zu einem Bereich zusammenfassen lassen, die von einem Dienst benötigt werden, der auf diesem System zur Verfügung gestellt wird (z.B. FTP-Ports 20/21).

Anwendungen

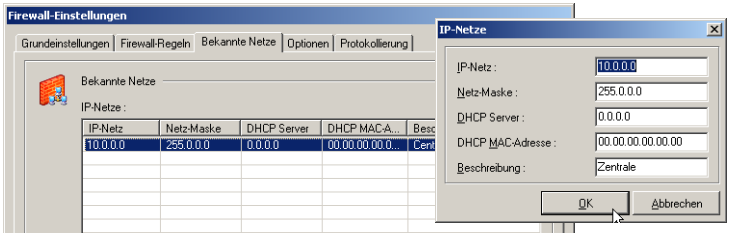
Auf dieser Registerkarte können Sie der Regel eine bestimmte Anwendung zuweisen. Bei gesperrter Grundeinstellung der Firewall ist dann eine Kommunikation über die ausgewählte Anwendung möglich.



Bitte beachten Sie, dass die zur Anwendung benötigten Protokolle ebenfalls freigeschaltet werden müssen.

Bekannte Netze

In der Liste der bekannten Netze können Sie die Erkennungsmerkmale von vertrauenswürdigen Netzwerken eintragen. Die Firewall-Regeln können bei der Konfiguration von der Erkennung eines vertrauenswürdigen Netzes abhängig gemacht werden.



Der LANCOM Advanced VPN Client befindet sich dann in einem bekannten Netz, wenn:

- Die IP-Adresse des LANCOM Advanced VPN Client aus dem angegebenen Netzbereich stammt. Ist z.B. das IP-Netz 192.168.254.0 mit der Maske 255.255.255.0 angegeben, so würde die Adresse 192.168.254.10 auf

DE

dem LANCOM Advanced VPN Client eine Zuordnung zum bekannten Netz bewirken.

UND

- IP-Adresse des LANCOM Advanced VPN Client von dem DHCP Server zugewiesen wurde, der die hier angegebene IP-Adresse besitzt.

  UND

- Wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt. Diese Option kann nur dann verwendet werden, wenn sich der DHCP Server im selben IP-Subnet befindet wie der DHCP-Client (also der LANCOM Advanced VPN Client).

Sind diese Bedingungen erfüllt, so handelt es sich ein vertrautes Netz. Die Zuordnung eines Adapters zu unbekannten oder bekannten Netzen wird automatisch protokolliert im Log-Fenster des Client-Monitors und in der Log-Datei der Firewall (siehe 'Protokollierung').

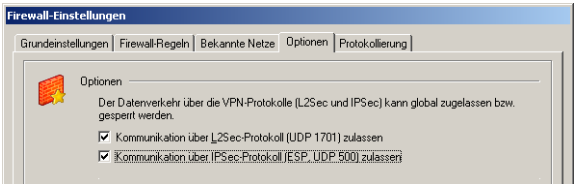
Optionen

Datenverkehr über die VPN-Protokolle

Bei den Optionen der Firewall kann der Datenverkehr über die VPN-Protokolle IPSec und L2Sec bei gesperrter Grundeinstellung der Firewall erlaubt oder gesperrt werden.

Es werden die folgenden für den Tunnelaufbau benötigten Protokolle und Ports per automatisch generierter Filter freigegeben:

- Für L2Sec: UDP 1701 (L2TP), UDP 67 (DHCPS), UDP 68 (DHCPC)
- Für IPSec: UDP 500 (IKE ISAKMP), IP-Protokoll 50 (ESP), UDP 4500 (NAT-T), UDP 67 (DHCPS), UDP 68 (DHCPC)



Mit der Freischaltung von L2Sec oder IPSec wird automatisch auch das DHCP-Protokoll freigeschaltet. Die über die Firewall geschützten Rechner können also auch in der gesperrten Grundeinstellung mit aktiviertem VPN-Protokoll eine IP-Adresse und andere Adress-Informationen von einem erreichbaren DHCP-Server beziehen.

Bitte beachten Sie, dass mit der Freischaltung von L2Sec oder IPSec lediglich der Tunnelaufbau ermöglicht wird. Existieren keine weiteren Regeln für VPN-Netze, die eine Kommunikation im Tunnel zulassen, kann über die VPN-Verbindung kein Datenaustausch erfolgen.

Die Einstellungen für die VPN-Protokolle können nur geändert werden, wenn sie die Firewall in der Betriebsart 'Gesperrte Grundeinstellung' befindet.

Firewall bei gestopptem Client weiterhin aktivieren

Die Firewall kann auch bei gestopptem Client aktiv sein, wenn diese Funktion selektiert ist. Damit wird verhindert, dass ein Anwender durch einfaches Ausschalten des LANCOM Advanced VPN Client den Schutz der Firewall umgeht.

- Ist diese Funktion aktiviert, wird bei Deaktivierung des LANCOM Advanced VPN Client **jede** ein- und ausgehende Kommunikation unterbunden. Es ist keinerlei Datenverkehr möglich, solange der LANCOM Advanced VPN Client deaktiviert ist.
- Ist diese Funktion deaktiviert, so wird mit dem stoppen des LANCOM Advanced VPN Client auch die Firewall deaktiviert.

Die Einstellung für die 'Aktivierung der Firewall bei gestopptem Client' kann durch geeignete Konfigurations-Sperren geschützt werden.

Der LANCOM Advanced VPN Client wird nicht schon durch das Schliessen des Client-Fensters gestoppt. Der Dienst läuft inklusive Firewall intern weiter. Der Client ist erst dann gestoppt, wenn man den Dienst z. B. mit dem Kommando „rwscmd /stop“ in der Eingabeaufforderung beendet.

UDP Pre-Filtering

In der Standardeinstellung werden bei gestartetem Client (unabhängig von der Firewall) UDP-Pakete ausgefiltert, so dass eine Verbindung von außen zum Client PC nicht möglich ist. Ist auf dem Client PC eine Anwendung mit Server-Funktion gestartet, die auf UDP-Datentransfer basiert (wie z. B. Terminalanwendungen oder NTP), kann sich diese Standardeinstellung störend auf die Datenkommunikation auswirken. Daher kann diese Standardeinstellung ausgeschaltet oder auf die UDP-Pakete unbekannter Netze beschränkt werden.

- immer: Standardeinstellung. In dieser Schalterstellung gelangen bei gestartetem Client keine UDP-Pakete auf den Client PC.

- nur bei unbekannten Netzen: In dieser Schalterstellung wirkt der UDP-Filter nur auf Pakete, die über Adapter unbekannter Netze eintreffen.
- aus: Wird der Filter ausgeschaltet, gelangen alle UDP-Pakete auf den Client PC. Diese Einstellung sollte nur verwendet werden, wenn Probleme mit einer Anwendung auftreten.

HotSpot-Anmeldung für externe Dialer zulassen

Wenn diese Funktion aktiviert ist, kann über einen externen Dialer eine HotSpot-Anmeldung erfolgen. Dazu wird die Kommandozeilen-schnittstelle rwscmd.exe aufgerufen. Mit dem Befehl

```
rwscmd /logonhotspot [Timeout]
```

wird die Firewall für die Ports 80 (HTTP) und 443 (HTTPS) freigeschaltet. Damit wird eine dynamische Regel erzeugt, die den Datenverkehr zulässt, bis der übergebene Timeout (in Sekunden) abgelaufen ist.

Protokollierung

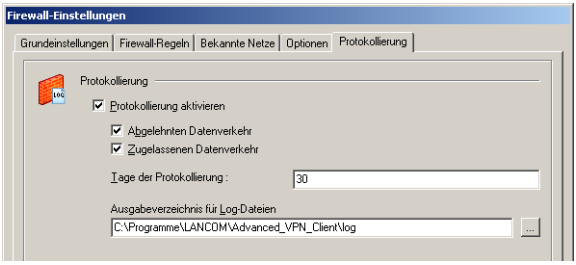
Die Aktivitäten der Firewall werden je nach Einstellung in eine Log-Datei geschrieben. Das "Ausgabeverzeichnis für Log-Dateien" befindet sich standardmäßig im Installationsverzeichnis z.B. unter:

```
C:\Programme\LANCOM\Advanced_VPN_Client\log
```

Die Log-Dateien für die Firewall sind im reinen Textformat geschrieben und benannt als `Firewallyymmdd.log`. Sie beinhalten eine Beschreibung vom "abgelehnten Datenverkehr" und/oder "zugelassenen Datenverkehr". Wurde keine dieser Optionen selektiert, so werden nur Statusinformationen zur Firewall hinterlegt.

Die Log-Dateien werden bei jedem Start der Firewall geschrieben. Maximal werden davon so viele im Log-Verzeichnis gehalten, wie als Anzahl der "Tage der Protokollierung" eingegeben wurde.

Die Log-Dateien werden bei jedem Start der Firewall geschrieben. Maximal werden davon so viele im Log-Verzeichnis gehalten, wie als Anzahl der 'Tage der Protokollierung' eingegeben wurde.

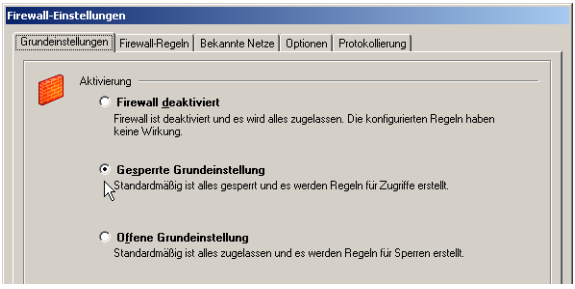


Je nach Art und Umfang der eingestellten Protokollierung können sehr große Datenmengen entstehen. Für eine optimale Performance sollte entweder auf eine Protokollierung verzichtet werden oder die Protokollierung auf bestimmte Fälle begrenzt werden.

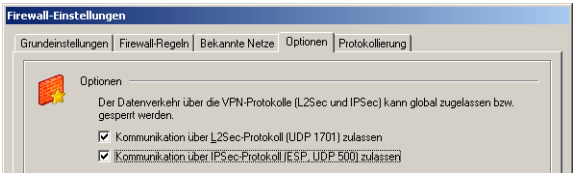
Basiskonfiguration der Firewall

Um einen sicheren Datenverkehr zu gewährleisten, können Sie die Firewall mit wenigen Einstellungen gegen den Zugriff von außen abschotten.

① Aktivieren Sie die 'Gesperrte Grundeinstellung' auf der Registerkarte 'Grundeinstellungen'.



② Für den Aufbau von VPN-Verbindungen aktivieren Sie global die VPN-Protokolle L2Sec und IPSec auf der Registerkarte 'Optionen'

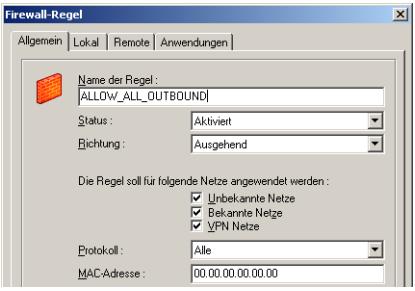


DE

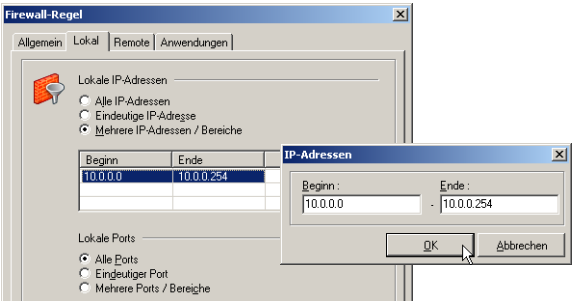
Mit der Freischaltung von L2Sec oder IPSec wird automatisch auch das DHCP-Protokoll freigeschaltet. Die über die Firewall geschützten Rechner können also auch in der gesperrten Grundeinstellung mit aktiviertem VPN-Protokoll eine IP-Adresse und andere Adress-Informationen von einem erreichbaren DHCP-Server beziehen.

③ Erstellen Sie dann eine Firewall-Regel, die den gesamten ausgehenden Datenverkehr erlaubt. Damit werden alle Verbindungen zugelassen, die von den Rechnern und Anwendungen aus dem eigenen lokalen Netz heraus geöffnet werden.

Die Stateful Inspection überwacht diese Verbindungen und lässt automatisch auch die Antworten von externen Rechnern zu. Mit der Stateful Inspection werden dabei Verbindungen über UDP, TCP, FTP (active und passive Mode) und ICMP überwacht.

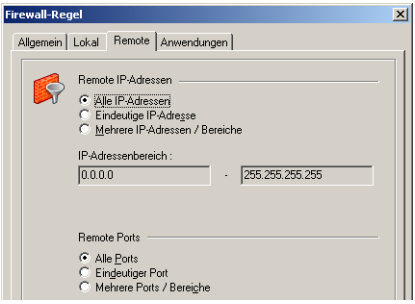


Aktivieren Sie auf der Registerkarte 'Lokal' als 'Lokale IP-Adressen' die Option 'Mehrere IP-Adressen/Bereiche' und tragen Sie die IP-Adressen ein, die in Ihrem lokalen Netz verwendet werden. Gilt diese Firewall nur für einen einzelnen Rechner, können Sie auch die Option 'Eindeutige IP-Adresse' wählen und die entsprechende lokale IP-Adresse eintragen.

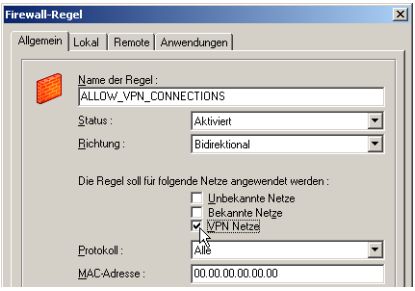


Als lokale IP-Adressen werden hier die IP-Adressen der Netzwerkadapter in den Rechnern eingetragen, die durch die Firewall geschützt werden. In einem LAN sind das üblicherweise die IP-Adressen, die vom DHCP-Server zugewiesen worden sind. Bei einem einzelnen Rechner mit einem direkten Internet-Anschluss (nicht über einen Router) ist das meistens die IP-Adresse, die vom Provider dynamisch zugewiesen worden ist.

Aktivieren Sie auf der Registerkarte 'Remote' als 'Remote IP-Adressen' die Option 'Alle IP-Adressen' und als 'Remote Ports' die Option 'Alle Ports'. Damit können die Rechner im lokalen Netz oder ein Einzelplatzrechner Datenverbindungen zu allen Gegenstellen über alle Ports aufbauen.

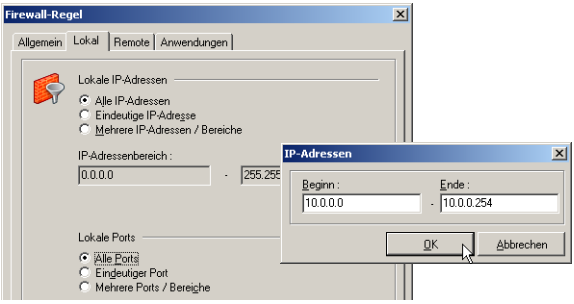


④ Erstellen Sie alternativ oder zusätzlich eine Firewall-Regel, die den gesamten ein- und ausgehenden Datenverkehr im VPN-Tunnel erlaubt, wenn Sie sich mit dem LANCOM Advanced VPN Client in das Netzwerk der Zentrale einwählen. Wählen Sie als Richtung für diese Regel 'Bidirektional' aus und schränken Sie die Regel auf die Anwendung nur für 'VPN-Netze' ein.

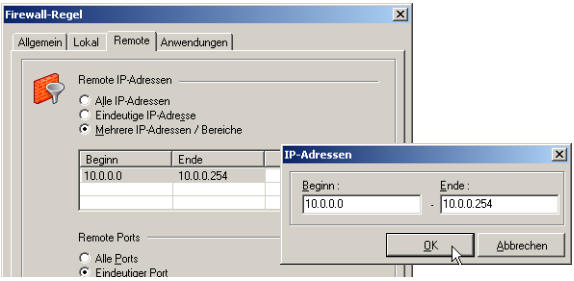


DE

Aktivieren Sie auf der Registerkarte 'Lokal' als 'Lokale IP-Adressen' die Option 'Alle IP-Adressen', da die IP-Adressen des virtuellen Netzwerkadapters der VPN-Verbindung möglicherweise wechseln können.



Aktivieren Sie auf der Registerkarte 'Remote' als 'Remote IP-Adressen' die Option 'Mehrere IP-Adressen/Bereiche' und tragen Sie die IP-Adressen des Netzwerks in der Zentrale ein.



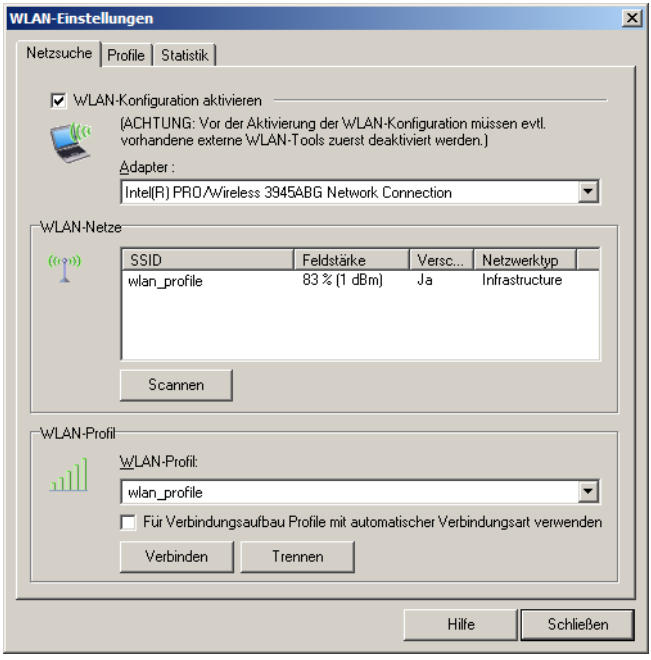
⑤ Je nach Anwendungszweck können Sie die Funktion der Firewall durch weitere Regeln zu bestimmten IP-Adressen, Protokollen, Ports oder Anwendungen erweitern.

DE

WLAN-Einstellungen

Nur für Windows-Version verfügbar.

Der WLAN-Adapter kann mit der Verbindungsart "WLAN" betrieben werden. Im Monitormenü "Konfiguration / WLAN-Einstellungen" können die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden.



WLAN-Automatik

Unter "WLAN-Profil" wird das Profil selektiert, über das eine Verbindung zum Access Point hergestellt werden soll. Außer diesem Profil können automatisch noch weitere Profile zur Anwahl an den Access Point verwendet werden, wenn diese mit Verbindungsart "automatisch" konfiguriert wurden und in den "WLAN-Einstellungen" die Funktion "Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden" aktiviert wird.

D. h. wurden mehrere Profile mit der Verbindungsart "automatisch" angelegt und wird die Funktion "Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden" genutzt, so wird zunächst das zuletzt selektierte Profil für einen möglichen Verbindungsaufbau herangezogen. Ist die SSID nicht passend, sodass mit diesem Profil keine Verbindung zum Access Point hergestellt werden kann, so werden anschließend die als "automatisch" konfigu-

rierten Profile für den Verbindungsaufbau herangezogen und das mit der passenden SSID verwendet.

Netzsuche

Wird diese "WLAN-Konfiguration aktiviert", so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Adapter

Sofern ein WLAN-Adapter installiert ist, wird dieser angezeigt.

WLAN-Netze

Nach einem automatischen Scan-Vorgang von wenigen Sekunden, der manuell auch mit dem Button "Scannen" ausgelöst werden kann, werden die derzeit verfügbaren Netze mit den Daten zu SSID, Feldstärke, Verschlüsselung und Netzwerktyp angezeigt. In einem zugehörigen Profil müssen diese Werte entsprechend konfiguriert werden:

SSID / Feldstärke / Verschlüsselung / Netzwerktyp

Der Name für die SSID (Standard Security) wird vom Netzbetreiber vergeben und unter dem grafischen Feld des Monitors ebenso angezeigt wie die Feldstärke (Bild unten). Die SSID wird nach einem Doppelklick auf das zu wählende Netz automatisch in ein WLAN-Profil für diesen Adapter übernommen wenn zu diesem Netz noch kein Profil erstellt wurde (siehe unten -> WLAN-Profile / Allgemein.)

WLAN-Profil

Ein bereits erstelltes WLAN-Profil kann hier für das gewünschte (bzw. gescannte) Netz ausgewählt werden. Mit Klick auf den Verbinden-Button wird der Verbindungsaufbau initialisiert.

WLAN-Profile

Bereits erstellte Profile zum oben selektierten Adapter werden in einer Liste dargestellt. Netzwerktyp, Verschlüsselung und SSID müssen mit den obigen Netzwerkparametern übereinstimmen.Ein neues Profil wird erzeugt, indem der Button "Neu" gedrückt wird oder im vorigen Fenster auf das zugehörige

Netz ein Doppelklick ausgeübt oder die rechte Maustaste geklickt wird. Über die Buttons können Profile auch bearbeitet oder gelöscht werden.

Allgemeine Profil-Einstellungen

Der Name kann frei vergeben werden und ist bei einer neuen Profilerzeugung nach Doppelklick auf das gescannte Netz zunächst identisch mit der SSID dieses Netzes. Ebenso verhält es sich mit dem Netzwerktyp, der identisch sein muss mit dem im Broadcast des Funknetzes gesendeten.

Der Netzwerktyp muss dann manuell auf "Ad-Hoc" umgestellt werden, wenn ein Profil für eine Direktverbindung von PC zu PC hergestellt werden soll. Sofern der WLAN-Adapter dies gestattet, kann der Energie Mode für ihn ausgewählt werden.

Wird die Verbindungsart für ein selektiertes Profil auf automatisch gestellt, so kann dieses Profil für die WLAN-Automatik verwendet werden.

Verschlüsselung

Der Verschlüsselungsmechanismus wird vom Access Point (WLAN Router) vorgegeben und über den Administrator mitgeteilt.

Wird WPA mit EAP (TLS) genutzt, so müssen die EAP-Optionen im Konfigurations-Menü des Monitors aktiviert werden und ein Zertifikat konfiguriert sein (im Monitor-Menü unter "Konfiguration / Zertifikate").

Der Netzwerktyp muss dann manuell auf "Ad-Hoc" umgestellt werden, wenn ein Profil für eine Direktverbindung von PC zu PC hergestellt werden soll. Sofern der WLAN-Adapter dies gestattet, kann der Energie Mode für ihn ausgewählt werden.

IP-Adressen

In diesem Fenster wird die IP-Adress-Konfiguration der WLAN-Karte vorgenommen.

Die hier gemachten Einstellungen werden dann wirksam, wenn die WLAN-Konfiguration wie oben beschrieben aktiviert wurde. In diesem Fall wird die hier eingetragene Konfiguration in die Microsoft-Einstellungen der Netzwerkverbindungen übernommen. (Siehe dort -> Netzwerkverbindungen / Eigenschaften von Internetprotokoll (TCP/IP)).

Authentisierung

In diesem Fenster müssen die Zugangsdaten für den HotSpot eingetragen werden. Diese Benutzerdaten werden nur für dieses WLAN-Profil verwendet.

Die Authentisierung kann durch Eintragen von Benutzername und Passwort erfolgen oder über Script. Das Script automatisiert die Anmeldung beim HotSpot-Betreiber.

Beachten Sie dabei, dass die Verbindung über einen HotSpot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des HotSpot-Betreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

- **Statisik**

Das Statistik-Fenster der WLAN-Einstellungen zeigt im Klartext den Status der Verbindung zum Access Point.

Amtsholung

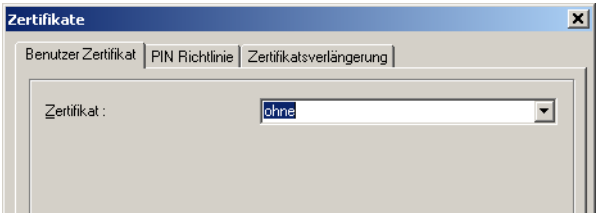
Nur für Windows-Version verfügbar.

Eine Amtsholung ist dann nötig, wenn der LANCOM Advanced VPN Client an einer Nebenstellenanlage betrieben wird. Damit die definierten Profile des LANCOM Advanced VPN Clients auch im mobilen Einsatz verwendbar bleiben, ohne Rufnummern umkonfigurieren zu müssen, kann, sofern an einem Anschluss eine Amtsholung nötig wird, diese hier eingetragen werden. Die Nummer für die Amtsholung wird dann für alle Zielrufnummern der Profile automatisch mitgewählt.

Zertifikate [Einstellungen]

Klicken Sie auf die Menüabzweigung **Konfiguration > Zertifikate**, so können Sie zunächst bestimmen, ob Sie die Zertifikate und damit die "Erweiterte Authentisierung" nutzen wollen, und wo Sie die Benutzer-Zertifikate hinterlegen wollen.

In weiteren Konfigurationsfeldern werden die Richtlinien zur PIN-Eingabe festgelegt und das Zeitintervall eingestellt innerhalb dessen das Zertifikat abläuft bzw. eine Zertifikatsverlängerung beantragt werden muss.



- **Benutzer-Zertifikat**

Zertifikat: Klicken Sie auf die Menüabzweigung **Konfiguration > Zertifikate**, so können Sie zunächst bestimmen, ob Sie die Zertifikate und damit die

"Erweiterte Authentisierung" nutzen wollen, und wo Sie die Zertifikate hinterlegen wollen.

ohne: Wählen Sie in der Listbox "Zertifikat" die Einstellung "ohne", so wird kein Zertifikat ausgewertet und die "Erweiterte Authentisierung" findet nicht statt.

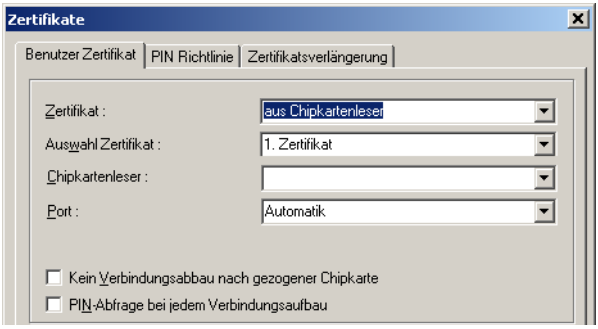
aus PKCS#12 Datei: Wählen Sie "aus PKCS#12 Datei" aus der Listbox, so werden bei der "Erweiterten Authentisierung" die relevanten Zertifikate aus einer Datei auf der Festplatte Ihres Rechners gelesen.

aus Chipkartenleser: Wählen Sie "aus Chipkartenleser" in der Listbox, so werden bei der "Erweiterten Authentisierung" die relevanten Zertifikate von der Smart Card in ihrem Chipkartenleser ausgelesen.

PKCS#11-Modul: Wählen Sie "PKCS#11-Modul" in der Listbox, so werden bei der "Erweiterten Authentisierung" die relevanten Zertifikate von der Smart Card in einem Chipkartenleser oder von einem Token gelesen.

- **Chipkartenleser:**

Wenn Sie die Zertifikate von der Smart Card mit Ihrem Lesegerät nutzen wollen, wählen Sie Ihren Chipkartenleser aus der Listbox. (Siehe auch -> PIN eingeben)



Chipkartenleser (PC/SC-konform)

Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden.

Chipkartenleser (CT-API-konform)

Mit der aktuellen Software werden Treiber für die Modelle SCM Swapsmart und SCM 1x0 (PIN Pad Reader) mitgeliefert. Sollte der Chipkartenleser mit den

DE

mitgelieferten Treibern nicht funktionieren oder ein anderer Chipkartenleser installiert sein, wenden Sie sich unbedingt an den Hersteller. Nehmen Sie außerdem folgende Einstellung in der Client Software vor: Editieren Sie die Datei NCPPKI.CONF, befindlich im Windows\System-Verzeichnis (unter Windows 95/98) oder System32-Verzeichnis (unter Windows NT/2000) mit einem ASCII-Editor, indem Sie als "ReaderName" den Namen des angeschlossenen Chipkartenlesers (xyz) eintragen und als DLLWIN95 bzw. DLLWINNT den Namen des installierten Treibers eintragen. (Der Standardname für CT-API-konforme Treiber ist CT32.DLL).

Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit "visible = 1" auf sichtbar gesetzt wurden!

ReaderName	= SCM Swapsmart (CT-API)	-> xyz
DLLWIN95	= scm20098.dll	-> ct32.dll
DLLWINNT	= scm200nt.dll	-> ct32.dll

Nach einem Boot-Vorgang erscheint der "ReaderName" im Monitor-Menü.

Port:

Der Port wird bei korrekter Installation des Lesegeräts automatisch bestimmt. Bei Unstimmigkeiten können die COM Ports 1-4 gezielt angesteuert werden.

Auswahl Zertifikat:

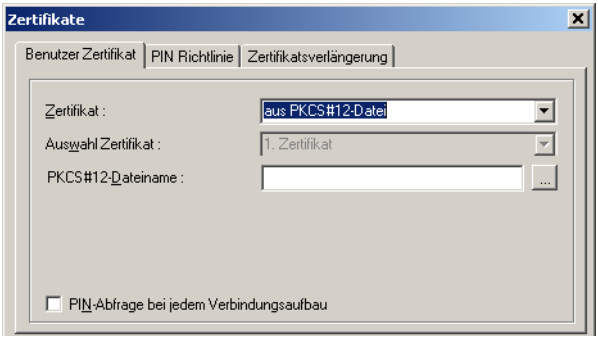
1. Zertifikat ... 3.: (Standard = 1) Aus der Listbox kann aus bis zu drei verschiedenen Zertifikaten gewählt werden, die sich auf der Chipkarte befinden. Die Anzahl der Zertifikate auf der Chipkarte ist abhängig von der Registration Authority, die diese Karte brennt. Wenden Sie sich zu weiteren Fragen bitte an Ihren Systemadministrator. Auf den Chipkarten von Signtrust und NetKey 2000 befinden sich drei Zertifikate:

6. zum Siginieren
7. zum Ver- und Entschlüsseln
8. zum Authentisieren (optional bei NetKey 2000)

PKCS#12-Dateiname:

Nutzen Sie das PKCS#12-Format, so erhalten Sie von Ihrem Systemadministrator eine Datei, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname der PKCS#12 Datei eingegeben, bzw. nach einem Klick auf den [...]-Button (Auswahl-Button) die Datei

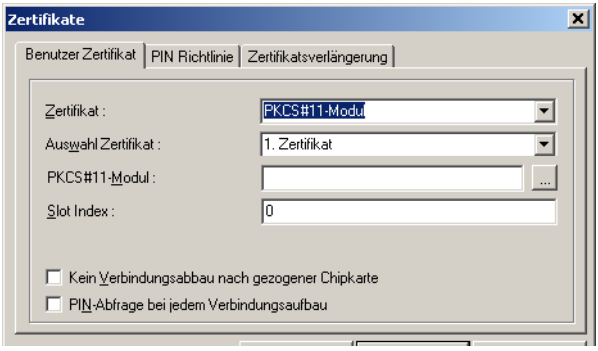
ausgewählt werden. Statt den Verzeichnisnamen komplett einzugeben, kann der Name dynamisch zusammengesetzt werden. z.B. %SYSTEMROOT%\ncple\user1.p12 %SYSTEMDRIVE%\winxxx\ncple\user1.p12



Wichtig: Die Strings für den Dateinamen können mit Variablen eingegeben werden. Dies erleichtert insbesondere das Handling der Konfigurationsdateien mit dem Client Manager, da nun für alle Benutzer die gleichen Strings mit Umgebungsvariablen eingegeben werden können.

PKCS#11-Modul:

Nutzen Sie das PKCS#11-Format, so erhalten Sie eine DLL vom Hersteller des Chipkartenlesers oder des Tokens, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname des Treibers eingegeben werden. Statt den Verzeichnisnamen für die PKCS#11.DLL komplett einzugeben, kann der Name dynamisch zusammengesetzt werden. z.B. %SYSTEMROOT%\ncple\pkcs#11.dll %SYSTEMDRIVE%\winxxx\ncple\ pkcs#11.dll



Wichtig: Die Strings für das Modul können mit Variablen eingegeben werden. Dies erleichtert insbesondere das Handling der Konfigurationsdateien mit dem Client Manager, da nun für alle Benutzer die gleichen Strings mit Umgebungsvariablen eingegeben werden können.

Kein Verbindungsabbau bei gezogener Chipkarte

Beim Ziehen der Chipkarte wird nicht unbedingt die Verbindung abgebaut. Damit "Kein Verbindungsabbau bei gezogener Chipkarte" erfolgt, muss diese Funktion aktiviert werden.

PIN-Abfrage bei jedem Verbindungsaufbau

Standardeinstellung: Wird diese Funktion nicht genutzt, so wird die PIN nur einmalig beim ersten Verbindungsaufbau des LANCOM Advanced VPN Clients abgefragt.

Wird diese Funktion aktiviert, so wird bei jedem Verbindungsaufbau die PIN erneut abgefragt.

Wichtig: Ist der Monitor nicht gestartet, kann kein PIN-Dialog erfolgen. In diesem Fall wird bei einem automatischen Verbindungsaufbau die Verbindung ohne erneute PIN-Eingabe hergestellt!

PIN-Richtlinie

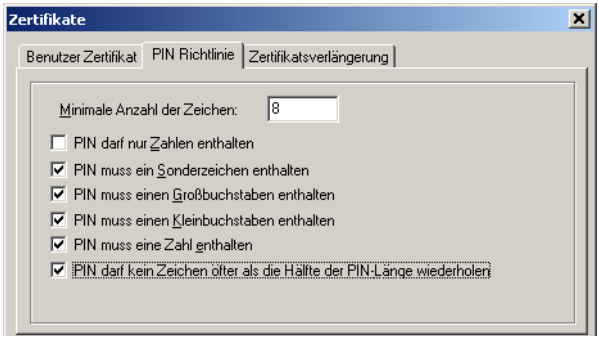
Minimale Anzahl der Zeichen

Standard ist eine 6-stellige PIN. Aus Sicherheitsgründen werden 8 Stellen empfohlen.

DE

Weitere Richtlinien

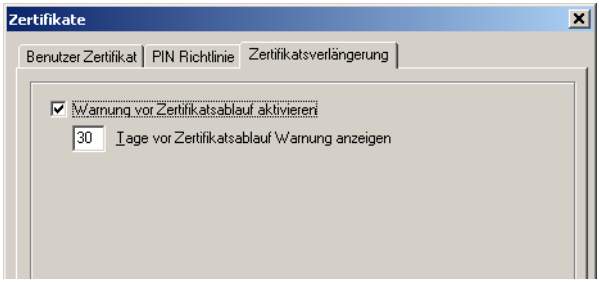
Es wird empfohlen alle PIN-Richtlinien einzusetzen, außer der, dass nur Zahlen enthalten sein dürfen. Zudem sollte die PIN nicht mit einer Zahl beginnen.



Die vorgegebenen Richtlinien werden eingeblendet, wenn die PIN geändert wird und die Richtlinien, die bei der Eingabe erfüllt werden, werden grün markiert (siehe -> PIN ändern).

Zertifikatsverlängerung

In diesem Konfigurationsfeld kann eingestellt werden, ob und wie viele Tage vor Ablauf der Gültigkeit des Zertifikats eine Meldung ausgegeben werden soll, die vor dem Ablauf der Gültigkeit warnt. Sobald die eingestellte Zeitspanne vor Ablauf in Kraft tritt, wird bei jeder Zertifikatsverwendung eine Meldung aufgeblendet, die auf das Ablaufdatum des Zertifikats hinweist.



Hardware-Zertifikat

Mit einem Hardware-Zertifikat authentisiert sich der Rechner gegenüber dem Gateway. Wird es zusätzlich zu einem Benutzer-Zertifikat eingesetzt, so kann sichergestellt werden, dass sich der Benutzer immer vom gleichen Rechner aus einwählt.

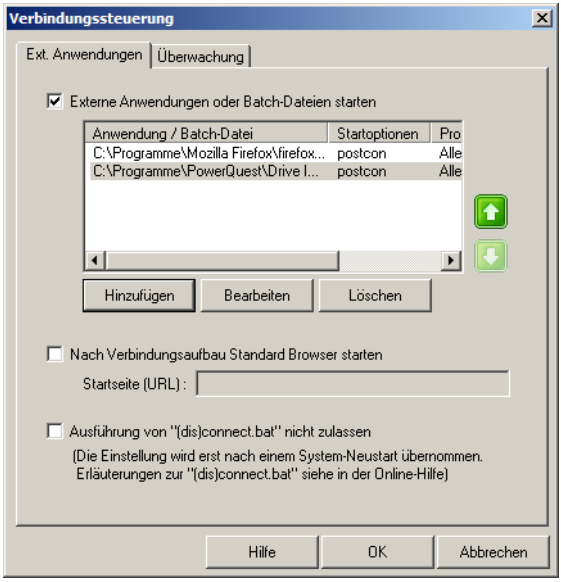
DE

Ein Hardware-Zertifikat kann als PKCS#12-Datei eingespielt werden. Der entsprechende Dateiname ist anzugeben. Bei einem Hardware-Zertifikat entfällt die Eingabe einer PIN.

Verbindungssteuerung [Konfiguration]

Über dieses Konfigurationsfeld können in Abhängigkeit vom Client Monitor Anwendungen oder Batch-Dateien gestartet werden. Die externen Anwendungen werden wie unten beschrieben eingefügt. Die Reihenfolge ihres Aufrufs von oben nach unten kann mit den grünen Pfeiltasten verändert werden.

Wollen Sie nach dem Verbindungsaufbau den Standard-Browser starten, so aktivieren Sie diese Funktion und tragen Verzeichnis und Dateinamen des Browsers ein.

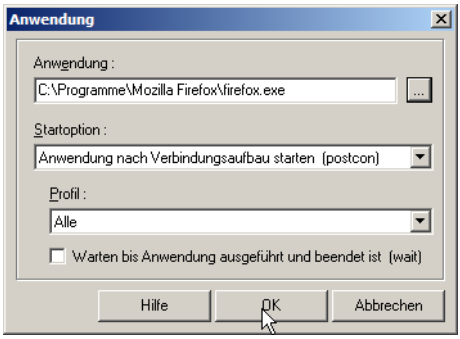


Nachdem Sie die Funktion "Externe Anwendungen oder Batch-Dateien starten" selektiert haben, können Sie über den Button mit "Hinzufügen" eine Anwendung oder Batch-Datei vom Rechner selektieren, die je nach Startoption geladen wird:

- vor Verbindungsaufbau starten (precon)
- nach Verbindungsaufbau starten (postcon)
- nach Verbindungsabbau starten (discon)

Zusätzlich können diese auszuführenden Anwendungen auch an ein bestimmtes Profil gebunden werden.

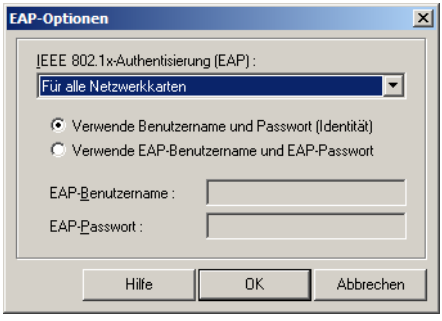
Die Wait-Funktion "Warten bis Anwendung ausgeführt und beendet ist" kann dann von Bedeutung sein, wenn eine Reihe von Batch-Dateien nacheinander ausgeführt werden soll.



EAP-Optionen [Einstellungen]

In den "EAP-Optionen" kann angegeben werden, ob die EAP-Authentisierung nur über WLAN-, LAN- oder alle Netzwerkkarten erfolgen soll. Die hier gemachte Einstellung gilt global für alle Einträge des Telefonbuchs. In der Aktivierungsbox kann die EAP-Authentisierung wie folgt eingestellt werden:

- Deaktiviert
- Für alle Netzwerkkarten
- Nur für WLAN-Karten
- Nur für LAN-Karten



Das Extensible Authentication Protocols Message Digest5 (EAP MD5) kann dann zum Einsatz kommen, wenn für den Zugang zum LAN ein Switch oder

DE

für das Wireless LAN ein Access Point verwendet werden, die 802.1x-fähig sind und eine entsprechende Authentisierung unterstützen.

Mit dem Extensible Authentication Protocol (EAP MD5) kann verhindert werden, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Zur Authentisierung kann wahlweise "VPN-Benutzername" mit "VPN-Passwort" verwendet werden oder ein eigener "EAP-Benutzername" mit einem "EAP-Passwort".

Zertifikatsinhalte können dergestalt automatisch übernommen werden, indem im Telefonbuch unter "Tunnel-Parameter" VPN-Benutzername und VPN-Passwort vom Zertifikat übernommen werden und in den EAP-Optionen "Verwende VPN-Benutzername und VPN-Passwort" aktiviert wird.

Bei EAP-TLS (mit Zertifikat) kann der EAP-Benutzername direkt aus der Zertifikats-Konfiguration bezogen werden. Folgende Inhalte des konfigurierten Zertifikats können genutzt werden, indem in die EAP-Konfiguration die entsprechenden Platzhalter eingegeben werden:

```
Commonname : %CERT_CN%
```

```
E-Mail : %CERT_EMAIL%
```

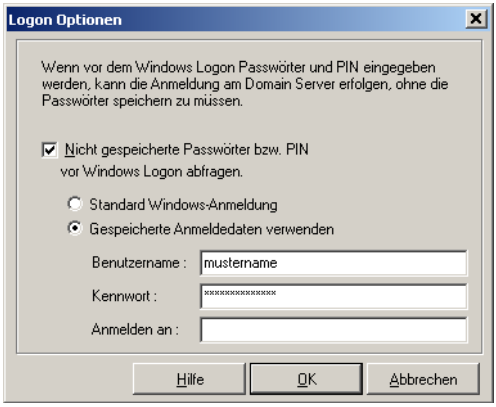
Nach Konfiguration des EAP erscheint eine Statusanzeige im grafischen Feld des Monitors. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt automatisch eine erneute EAP-Verhandlung.

Logon Optionen

Nur für Windows-Versionen verfügbar.

Wenn Sie diesen Menüpunkt unter **Konfiguration > Logon Optionen** wählen, können Sie im folgenden Fenster entscheiden, ob vor dem Windows-Logon an einer remote Domain die Verbindung von der Client-Software zum Network Access Server aufgebaut werden soll. Dies bedeutet, dass die Client-Software beim nächsten Booten die Verbindung aufbaut. Für diesen Verbindungsaufbau müssen Sie gegebenenfalls die PIN für Ihr Zertifikat und das (nicht gespeicherte) Passwort für die Client-Software eingeben.

Nachdem die Verbindung zum Network Access Server von der Client-Software hergestellt wurde, können Sie sich an der remote Domain anmelden. Diese Anmeldung erfolgt dann bereits verschlüsselt.



Nach jeder Änderung der "Logon Optionen" muss der Rechner gebootet werden.

Konfigurations-Sperren

Über **Konfiguration > Konfigurations-Sperren** kann das Konfigurations-Hauptmenü im Monitor so modifiziert werden, dass der Benutzer die voreingestellten Konfigurationen nicht mehr abändern kann, bzw. ausgewählte Parameterfelder für den Benutzer nicht sichtbar sind.

Die Konfigurations-Sperren werden in der definierten Form erst wirksam, wenn die Einstellungen mit **OK** übernommen werden. Wird der **Abbrechen** Button gedrückt, wird auf die Standard-Einstellung zurückgesetzt.

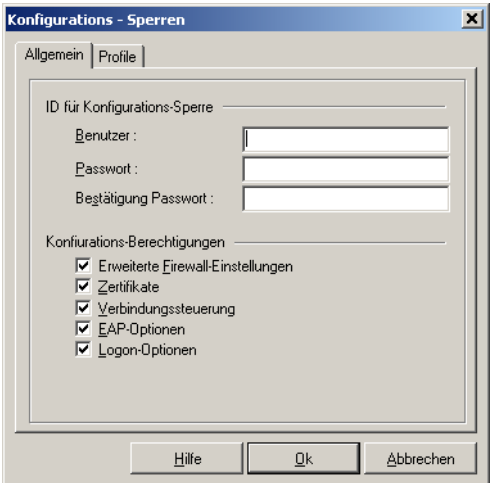
Allgemein [Konfigurations-Sperren]

Um die Konfigurations-Sperren wirksam festlegen zu können, muss eine ID eingegeben werden, die sich aus "Benutzer" und "Passwort" zusammensetzt. Das Passwort muss anschließend bestätigt werden.

Bitte beachten Sie, dass die ID für die Konfigurations-Sperre unbedingt nötig ist, die Sperren wirksam werden zu lassen oder die Konfigurations-Sperren auch wieder aufzuheben. Wird die ID vergessen, besteht keine Möglichkeit mehr, die Sperren wieder aufzuheben!

Anschließend kann die Berechtigung, die Menüpunkte unter dem Hauptmenüpunkt Konfiguration zu öffnen, für den Benutzer eingeschränkt werden.

Standardmäßig kann der Benutzer alle Menüpunkte öffnen und die Konfigurationen bearbeiten. Wird zu einem Menüpunkt der zugehörige Haken mit einem Mausklick entfernt, so kann der Benutzer diesen Menüpunkt nicht mehr öffnen.

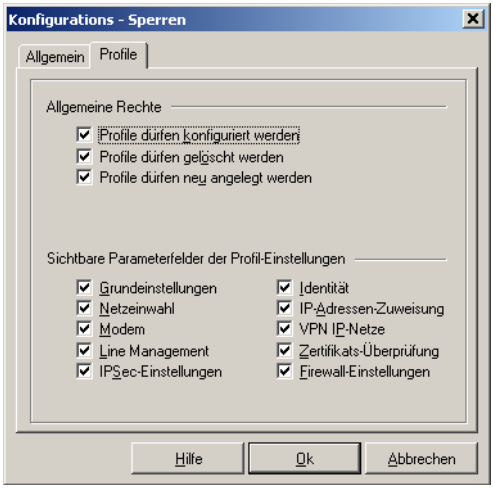


- **Profile [Konfigurations-Sperren]**

Die Bearbeitungsrechte für die Parameter in den Profil-Einstellungen sind in zwei Sparten unterteilt:

- Allgemeine Rechte

- Sichtbare Parameterfelder der Profile



Allgemeine Rechte

Die allgemeinen Rechte beziehen sich nur auf die (Konfiguration der) Profile. Wird festgelegt "Profile dürfen neu angelegt werden", "Profile dürfen konfiguriert werden" bleibt jedoch ausgeschlossen, so können zwar mit dem Assistenten neue Profile definiert werden, eine nachfolgende Änderung einzelner Parameter ist dann jedoch nicht mehr möglich.

Sichtbare Parameterfelder der Profile

Die Parameterfelder der Profil-Einstellungen können für den Benutzer ausgeblendet werden.

Beachten Sie, dass Parameter eines nicht sichtbaren Feldes auch nicht konfiguriert werden können.

Profile importieren

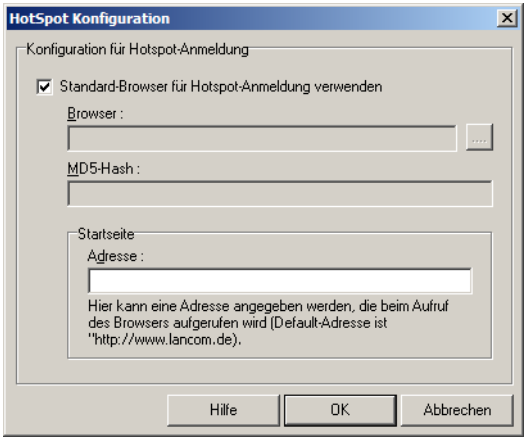
Über diese Funktion können Profil-Einstellungen vom Client eingelesen werden. Diese Profil-Einstellungen können in Form einer INI-Datei vom Zielsystem erstellt oder manuell editiert werden. Im Installationsverzeichnis befinden sich dazu die Beispieldateien IMPORT_D.TXT und IMPORT_E.TXT. In den Beispieldateien sind auch Syntax und Parameterwerte beschrieben.

DE

HotSpot

Nur für Windows-Version verfügbar.

Unter diesem Menüpunkt erfolgt die Konfiguration zur HotSpot-Anmeldung. Folgende Einstellungen sind möglich:



"Standard-Browser für HotSpot-Anmeldung verwenden" ist die Standardeinstellung. Wird der Haken in der Checkbox entfernt, kann ein anderer Browser angegeben werden in der Form:

`%PROGDIR%\Mozilla\Firefox\firefox.exe.`

Der alternative Browser kann speziell für die Anforderungen am HotSpot konfiguriert werden. D. h. es wird kein Proxy Server konfiguriert und alle aktiven Elemente (Java, Javascript, ActiveX) werden deaktiviert. (Der alternative Browser ist nicht Bestandteil der Client Software!) Darüber hinaus kann der MD5-Hash-Wert der Browser-Exe-Datei ermittelt und in das Feld "MD5-Hash" eingetragen werden. Auf diese Weise wird sichergestellt, dass nur mit diesem Browser eine HotSpot-Verbindung zustande kommt.

Unter "Startseite / Adresse" wird die oben beschriebene Startseite eingegeben in der Form:

`http://www.mycompany.de/start.html.`

Profil-Sicherung

Existiert noch kein gesichertes Profil, zum Beispiel bei einer Erstinstallation, so wird automatisch ein erstes angelegt.

- **Erstellen**

Nach jedem Klick auf den Menüpunkt "Erstellen" wird nach einer Sicherheitsabfrage eine Profil-Sicherung angelegt, die die Konfiguration zu diesem Zeitpunkt enthält.

- **Wiederherstellen**

Nach jedem Klick auf "Wiederherstellen" wird die letzte Profil-Sicherung eingelesen. Änderungen in der Konfiguration, die seit der letzten Profil-Sicherung vorgenommen wurden, gehen damit verloren.

3.1.3 Log

Mit der Log-Funktion werden die Kommunikationsereignisse der LANCOM Advanced VPN Client Software mitprotokolliert. Wählen Sie die Log-Funktion an, öffnet sich das Fenster des "Logbuches". Die hier abgebildeten Daten werden bis zum nächsten Reboot im Speicher gehalten.

Eine zusätzliche Log-Datei speichert die Aktionen des Clients selbständig für die letzten sieben Tage. Log-Ausgaben, die älter als sieben Betriebstage sind, werden automatisch gelöscht. Die Datei steht unter LOG\ und heißt NCPyymmdd.LOG. Sie wird mit Datumsangabe (yymmdd) immer bei Beenden des Monitors geschrieben. Die Datei kann mit einem Texteditor geöffnet und analysiert werden.

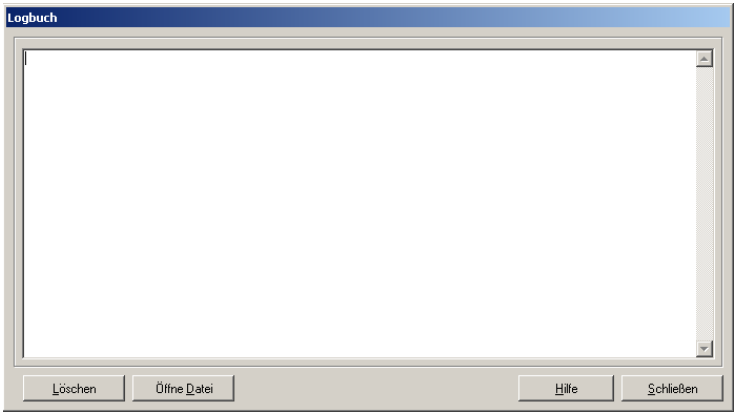
Logbuch

Die Buttons des Logbuchfensters haben folgende Funktionen:

- Öffne Datei
- Schließe Datei
- Löschen
- Fensterinhalt
- Schließen

DE

- Log-Fenster



- **Öffne Datei**

Wenn Sie auf diesen Button klicken, erhalten Sie in einem weiteren Fenster die Möglichkeit Name und Pfad einer Datei einzugeben, in die der Inhalt des Log-Fensters geschrieben wird. Alle Transaktionen mit der LANCOM Advanced VPN Client Software, wie Anwahl und Empfang, einschließlich der Rufnummern, werden automatisch mitprotokolliert und in diese Datei geschrieben, bis Sie auf den Button mit **Schließe Datei** klicken. Wenn Sie eine Log-Datei anlegen, können Sie die Transaktionen mit dem LANCOM Advanced VPN Client über einen längeren Zeitraum verfolgen.

- **Schließe Datei**

Wenn Sie auf diesen Button klicken, wird die Datei geschlossen, die Sie mit **Öffne Datei** angelegt haben. Die geschlossene Log-Datei kann zur Analyse der Transaktionen mit dem LANCOM Advanced VPN Client oder zur Fehlersuche verwendet werden.

- **Löschen - Fensterinhalt**

Wenn Sie auf diesen Button drücken wird der Inhalt des Log-Fensters gelöscht.

- **Schließen - Log-Fenster**

Wenn Sie auf "Schließen" klicken, schließen Sie das Fenster des "Logbuches" und kehren zum Monitor zurück.

3.1.4 Fenster [Menü]

Unter dem Menüpunkt **Fenster** können Sie die Bedienoberfläche des Monitors variieren und die Sprache für die Monitoroberfläche festlegen. Folgende Einstellungen stehen zur Auswahl:

- Profilauswahl anzeigen
- Buttonleiste anzeigen
- Statistik anzeigen
- WLAN-Status anzeigen
- Immer im Vordergrund
- Autostart
- Beim Schließen minimieren
- Nach Verbindungsaufbau minimieren
- Sprache

Profilauswahl anzeigen

Wenn Sie auf "Profilauswahl anzeigen" klicken, kann aus der Liste der konfigurierten Profile das gewünschte ausgewählt werden.

Buttonleiste anzeigen

Wenn Sie auf "Buttonleiste anzeigen" klicken, werden Buttons für die Menüpunkte "Verbinden" und "Trennen" aus dem Hauptmenü "Verbindung" eingeblendet.

Statistik anzeigen

Wenn Sie auf "Statistik anzeigen" klicken, werden Informationen zu Datenmenge, Verbindungszeit, Timeout etc. angezeigt. Die Monitor-Oberfläche ist dann entsprechend größer.

WLAN-Status anzeigen

Unabhängig vom Verbindungsmedium des aktuell selektierten Linkprofils kann das Feld zur grafischen Anzeige des WLAN-Status geöffnet bzw. geschlossen werden, wenn im Monitormenü "Konfiguration" unter "WLAN-Einstellungen" eine WLAN-Konfiguration aktiviert wurde. Wurde eine Multifunktionskarte konfiguriert, ist der Menüpunkt "WLAN-Status anzeigen" nicht aktiv.

DE

Immer im Vordergrund

Wenn Sie "Immer im Vordergrund" geklickt haben, wird der Monitor immer im Bildschirmvordergrund angezeigt, unabhängig von der jeweils aktiven Anwendung.

Autostart

Mit diesem Menüpunkt wird der Monitor so eingestellt, dass er nach dem Booten selbständig startet. "Autostart" ersetzt den Menüpunkt "Fenster - Nach booten starten". Über den neuen Menüpunkt können folgende Optionen eingestellt werden:

- kein Autostart: nach dem Booten nicht automatisch starten
- minimiert starten: nach dem Booten den Monitor starten und minimiert darstellen
- maximiert starten: nach dem Booten den Monitor starten und in normaler Größe darstellen

Wenn Sie oft mit der LANCOM Advanced VPN Client Software arbeiten und die Informationen des Monitors benötigen, so sollten Sie die Einstellung "maximiert starten" wählen. Prinzipiell ist es für die Kommunikation mit dem Zielsystem nicht nötig, den Monitor zu starten.

Beim Schließen minimieren

Wird der Monitor bei einer bestehenden Verbindung über den Schließen-Button [x] rechts in der Kopfzeile oder das Systemmenü links in der Kopfzeile geschlossen [Alt + F4], so informiert ein Meldungsfenster darüber, dass kein Ampelsymbol (Tray Icon) mehr in der Task-Leiste erscheint, worüber der Status dieser Verbindung kontrolliert werden könnte, d.h. der Benutzer kann dann auf der Oberfläche seines Desktops nicht erkennen, ob und wie lange noch Verbindungsgebühren anfallen, oder ob die Verbindung bereits beendet wurde. (Um in diesem Fall den Status der Verbindung zu erfahren und sie gegebenenfalls korrekt zu beenden, muss der Monitor erneut gestartet werden.)

Ist dieser Menüpunkt aktiviert, so wird der Monitor beim Schließen über den Button [x] rechts in der Kopfzeile oder über [Alt + F4] nur minimiert und erscheint als Ampelsymbol in der Task-Leiste, worüber der Status der Verbindung abgelesen werden kann. Der Klick auf den Schließen-Button [x] der Kopfzeile hat in dieser Einstellung die gleiche Wirkung wie der Klick auf den Minimieren-Button [-] der Kopfzeile.

(In der Darstellung des Ampelsymbols in der Task-Leiste kann nach einem rechten Mausklick auf das Symbol das mögliche Zielsystem abgelesen und die Verbindung aufgebaut oder getrennt werden, bzw. bei abgebauter Verbindung der Monitor auch beendet werden.)

Das Beenden des Monitors ist nur noch über das Hauptmenü "Verbindung - Beenden" möglich.

Nach Verbindungsaufbau minimieren

Ist dieser Menüpunkt aktiviert, so wird der Monitor nach erfolgreichem Verbindungsaufbau automatisch minimiert.

Sprache

Die LANCOM Advanced VPN Client Software ist mehrsprachig angelegt. Die Standardsprache bei Auslieferung ist Deutsch. Um eine andere Sprache zu wählen, klicken Sie "Language / Sprache" im Pulldown-Menü Fenster und wählen die gewünschte Sprache (für Mac-Version verfügbar in Englisch und Deutsch).

3.1.5 Hilfe

Die "Hilfe" zeigt Ihnen den kompletten Hilfetext mit Inhaltsverzeichnis und Index.

Unter dem Menüpunkt Hilfe finden Sie mit Klick auf "Info" die Versionsnummer Ihrer eingesetzten Software und Treiber.

3.2 Das Firewall-Konzept

3.2.1 Globale Firewall und Link-Firewall

Das Firewall-Konzept des LANCOM Advanced VPN Client basiert auf zwei Komponenten:

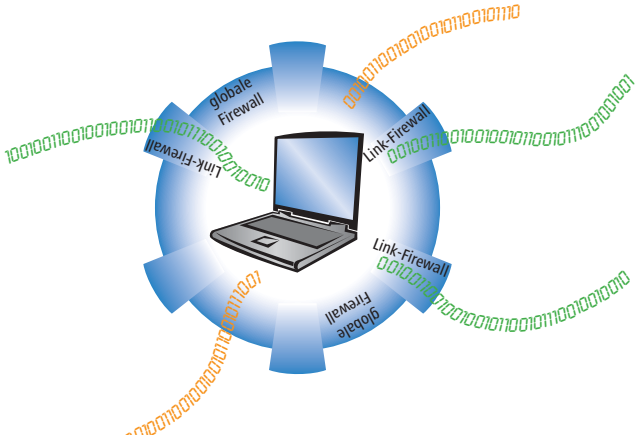
- Globale Firewall mit allen relevanten Funktionen einer „Personal Firewall"
- Link-Firewall zur besonderen Behandlung des Datenverkehrs auf bestimmten Verbindungen

Die globale Firewall schützt Ihren Rechner beim Datenaustausch mit anderen Computern oder Netzwerken. Die hier definierten Regeln gelten auch dann, wenn der LANCOM Advanced VPN Client keine Verbindung aufgebaut hat. Die globale Firewall ist auch dann aktiv, wenn der Client Monitor – also die Bedienoberfläche des LANCOM Advanced VPN Client – geschlossen ist. Je

DE

nach Einstellung kann die globale Firewall sogar dann den Datenaustausch verhindern, wenn der entsprechende Dienst im Betriebssystem beendet wurde.

Die Einstellungen der Link-Firewall gelten nur für die entsprechenden Verbindungsprofile, bei denen sie konfiguriert sind. Die Link-Firewall wird auch nur dann aktiv, wenn die zugehörige Verbindung aufgebaut ist. Mit der Link-Firewall kann die Funktion der globalen Firewall weiter eingeschränkt werden.



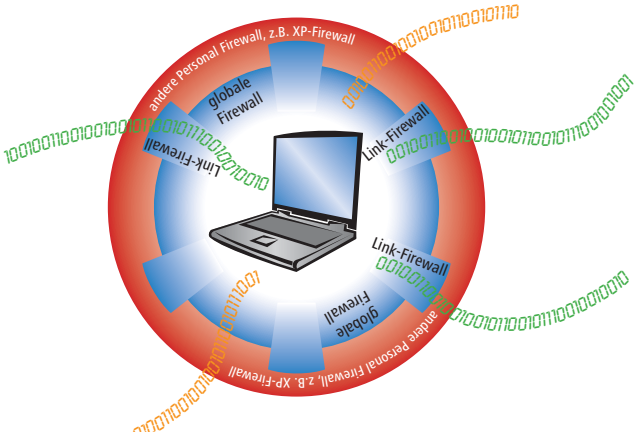
Im vorstehenden Bild werden die orange-farbenen Datenströme nur von der globalen Firewall geprüft. Für die grünen Datenströme, die über eine bestimmte Verbindung des LANCOM Advanced VPN Client verlaufen, gelten zusätzlich die Bestimmungen der Link-Firewall.

Im Allgemeinen können alle Anforderungen an eine Firewall mit den Einstellungen der globalen Firewall erfüllt werden. Konfigureiren Sie daher die globale Firewall nach Möglichkeit so, dass keine weiteren Einstellungen der Link-Firewall notwendig sind. Aktivieren Sie die Link-Firewall nur gezielt für die Verbindungen, deren Sicherheitsanforderungen sich nicht mit dem globalen Firewall-Konzept verbinden lassen.

3.2.2 Zusammenspiel mit anderen Firewalls

Auf vielen Rechnern ist neben der Firewall im LANCOM Advanced VPN Client eine weitere Personal Firewall installiert. Bitte beachten Sie, dass die beiden

Firewalls nacheinander auf den Datenverkehr wirken, sofern sie gleichzeitig aktiv sind.



Der Datenverkehr kann die verschiedenen Firewalls nur dann passieren, wenn alle Komponenten das Versenden bzw. das Empfangen der Datenpakete erlauben: Sowohl gobale Firewall und Link-Firewall im LANCOM Advanced VPN Client als auch die zusätzliche Personal Firewall müssen den Datenaustausch zulassen. Wenn nur eine der Firewall-Komponenten die Übertragung sperrt, wird der Datenverkehr verhindert.

Wie auch beim Zusammenwirken von globaler Firewall und Link-Firewall im LANCOM Advanced VPN Client empfiehlt es sich auch bei der Verwendung einer weiteren Personal Firewall, möglichst viele Sicherheits-Funktionen auf eine Stelle zu konzentrieren. Legen Sie bei der Planung des Sicherungskonzeptes eine Firewall als Haupt-Firewall fest und aktivieren Sie die restlichen Firewall-Komponenten nur dann, wenn die gewählte Firewall nicht alle gewünschten Sicherungs-Funktionen ermöglicht bzw. bestimmte Verbindungen besondere Sicherungsvorkehrungen erfordern.

DE

4 Profil-Einstellungen [Parameter]

Im folgenden sind alle Parameterbeschreibungen aufgeführt, und sie sind so angeordnet, wie sie auf der Oberfläche des Client Monitors erscheinen.

Nachdem Sie **Profil-Einstellungen** im Menü des Monitors angeklickt haben, öffnet sich das Menü und zeigt eine Übersicht über die bereits definierten Profile und die Rufnummern (nur Windows-Version) der zugehörigen Ziele.

Seitlich finden Sie Buttons, über die Sie die Einträge des Telefonbuchs (Zielsysteme) modifizieren können.

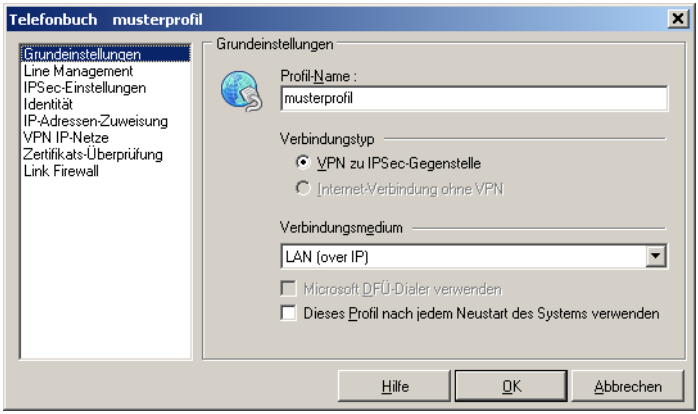
Die Parameter, die die jeweilige Verbindung über das Profil zu den Zielen spezifizieren, sind in verschiedenen Parameterfeldern gesammelt. In der Kopfzeile steht der Name des Profils (siehe auch -> Profil-Einstellungen, Konfigurieren). Seitlich sind die Titel der Parameterfelder angeordnet:

- Grundeinstellungen
- Netzeinwahl (nur für Windows-Version verfügbar)
- Modem (nur für Windows-Version verfügbar)
- Line Management (nur für Windows-Version verfügbar)
- IPSec-Einstellungen
- Erweiterte IPSec-Optionen
- Identität
- IP-Adressen-Zuweisung
- VPN-IP-Netze
- Zertifikats-Überprüfung
- Firewall-Einstellungen

DE

4.1 Grundeinstellungen

Im Parameterfeld "Grundeinstellungen" wird der Profil-Name und die Verbindungsart zu einem Profil eingegeben.



-> siehe auch die Parameter:

- Profil-Name
- Verbindungsart
- Microsoft DFÜ-Dialer (nur Windows-Version)
- Diesen Telefonbucheintrag nach jedem Neustart des Systems verwenden

Die LANCOM Advanced VPN Client Software gestattet die Einrichtung individueller Profile für entsprechende Zielsysteme, die nach den Benutzeranforderungen konfiguriert werden können.

Um ein neues Profil zu definieren, klicken Sie in der Menüleiste des Monitors auf **Profil-Einstellungen**. Das Menü öffnet sich nun und zeigt die bereits definierten Profile. Klicken Sie jetzt auf **Neuer Eintrag**. Jetzt legt der "Assistent für ein neues Profil" mit Ihrer Hilfe ein neues an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder werden Standardwerte eingetragen.

Um diese Standardwerte zu editieren, d.h. weitere Parameter so einzustellen, wie es den Verbindungsanforderungen zum zugehörigen Zielsystem entspricht, wählen Sie mit der Maus das Profil aus, dessen Werte Sie ändern möchten und klicken anschließend auf **Konfigurieren** (siehe -> Profil-Einstellungen - Konfigurieren).

Um die Definitionen eines bereits definierten Profils zu kopieren, klicken Sie **Kopieren**.

Um ein Profil zu löschen, wählen Sie es aus und klicken **Löschen**.

4.1.1 Profil-Name

Wenn Sie ein neues Profil definieren, sollten Sie zunächst einen unverwechselbaren Namen für dieses System eintragen (z.B. IBM London). Der Name des Profils darf jeden gewünschten Buchstaben wie auch Ziffern beinhalten und darf, Leerzeichen mitgezählt, bis zu 39 Zeichen lang sein.

4.1.2 Verbindungstyp

Alternativ stehen mit dem LANCOM Advanced VPN Client zwei Verbindungstypen zur Wahl:

- VPN zu IPSec-Gegenstelle: In diesem Fall wählen Sie sich mit dem LANCOM Advanced VPN Client in das Firmennetz ein (bzw. an das VPN Gateway an). Dazu wird ein VPN-Tunnel aufgebaut.
- Internet-Verbindung ohne VPN (nur für Windows-Version verfügbar): In diesem Fall nutzen Sie den LANCOM Advanced VPN Client nur zur Einwahl in das Internet. Dabei wird Network Address Translation (IPNAT) weiterhin im Hintergrund genutzt, sodass nur Datenpakete akzeptiert werden, die angefordert wurden.

4.1.3 Verbindungsmedium (nur für Windows-Version verfügbar)

Die Verbindungsart kann für jedes Profil eigens eingestellt werden, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem (Windows-)System installiert.

ISDN:

Angeschlossene Hardware: ISDN-Hardware mit Capi 2.0-Unterstützung;

Netze: ISDN-Festnetz

Gegenstellen: ISDN-Hardware

Modem:

Angeschlossene Hardware: Asynchrone Modems (PCMCIA-Modem, GSM-Karte) mit Com Port-Unterstützung;

Netze: Analoges Fernsprechnetz (PSTN) (auch GSM)

Gegenstellen: Modem oder ISDN-Karte mit digitalem Modem

LAN (over IP):

Angeschlossene Hardware: LAN-Adapter oder UMTS/GPRS-Adapter mit Software des Herstellers/Providers (siehe 'UMTS- oder GRPS-Profil einrichten' →Seite 125);

Netze: Local Area Network mit Ethernet oder Token Ring

Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im LAN

WLAN (over IPSec):

Angeschlossene Hardware: WLAN-Adapter

Netze: Wireless Local Area Network

Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im WLAN;

Das Verbindungsmedium WLAN kann nur unter Windows 2000/XP/Vista genutzt werden. Unter Windows 98/NT wird der Adapter für ein wireless LAN (WLAN-Adapter) genauso behandelt wie normale LAN-Adapter. D.h. auch für WLAN wird als Verbindungsmedium "LAN (over IP)" gewählt. Dazu wird das Tool der WLAN-Karte oder das von Windows zur Konfiguration der Funknetzverbindung genutzt.

Unter Windows 2000/XP/Vista kann der WLAN-Adapter mit dem Verbindungsmedium "WLAN" betrieben werden. Im Monitormenü erscheint eigens der Menüpunkt "WLAN-Einstellungen", worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können. Wird diese "WLAN-Konfiguration aktiviert", so muss das Management-Tool der WLAN-Karte deaktiviert werden. Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.

Wird das Verbindungsmedium WLAN für ein Zielsystem im Telefonbuch eingestellt, so wird unter dem grafischen Feld des Client-Monitors eine weitere Fläche eingeblendet, auf der die Feldstärke und das WLAN-Netz dargestellt werden.

xDSL (PPPoE):

Angeschlossene Hardware: Ethernet-Adapter, xDSL-Modem

Netze: xDSL

Gegenstellen: Access-Router im xDSL

GPRS (UMTS)

Dieses Einwahlmedium wählen Sie, wenn die Einwahl über das Mobilfunknetz (GPRS/UMTS) erfolgen soll (als Alternative zur Verwendung der bei den UMTS/GPRS-Karten mitgelieferten Software des Herstellers/Providers). Beachten Sie dazu den Hinweis unter den Installationsvoraussetzungen zu 'Modem oder Datenkarte' →Seite 16 und die Konfigurationshinweise unter 'UMTS- oder GRPS-Profil einrichten' →Seite 125.

PPTP Microsoft Point-to-Point Tunnel Protocol;

Angeschlossene Hardware: Ethernet-Adapter, xDSL-Modem

Netze: xDSL

Gegenstellen: Access-Router im xDSL

Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsarten genutzt, wie zum Beispiel Modem und ISDN, so kann die manuelle Auswahl des Zielsystems mit dem jeweils zur Verfügung stehenden Verbindungsmedium entfallen. Alternativ kann die "Automatische Medienerkennung" konfiguriert werden.

Dabei ist zu beachten, dass das Zielsystem mit automatischer Medienerkennung mit allen für die Verbindung zum VPN Gateway nötigen Parametern (insbesondere der IP-Adresse des VPN Gateways) konfiguriert wird. Zusätzlich werden die Zielsysteme mit den alternativen Verbindungsmedien so konfiguriert, dass das jeweils gewünschte Verbindungsmedium (evtl. auch die Modemparameter) eingestellt ist und die Funktion "Eintrag für automatische Medienerkennung verwenden" aktiviert ist.

Außerdem müssen für das jeweilige Verbindungsmedium die Eingangsdaten zum ISP im Parameterfeld "Netzeinwahl" gesetzt sein.

Bei einem Verbindungsaufbau erkennt der Client automatisch, welche Verbindungsarten aktuell zur Verfügung stehen und wählt davon die schnellste aus. In einer Suchroutine ist die Priorisierung der Verbindungsarten in folgender Reihenfolge festgelegt:

1. LAN
2. WLAN
3. DSL
4. UMTS/GPRS
5. ISDN

6 MODEM

Die Eingangsdaten für die Verbindung zum ISP werden aus den Telefonbucheinträgen übernommen, die für die automatische Medienerkennung konfiguriert wurden.

4.1.4 Microsoft DFÜ-Dialer

Nur für Windows-Version verfügbar.

Zur Einwahl am ISP (Internet Service Provider) kann der Microsoft DFÜ-Dialer genutzt werden. Dies ist immer dann nötig, wenn der Einwahlpunkt ein Einwahl-Script benötigt. Der DFÜ-Dialer unterstützt dieses Script. Im Parameterfenster "Netzeinwahl" wird anschließend die Script-Datei unter Eingabe von Pfad und Namen zur eingespielten Script-Datei eingetragen (siehe -> Script-Datei).

4.1.5 Dieses Profil nach jedem Neustart des Systems verwenden

Normalerweise wird der Client-Monitor nach einem Neustart mit dem zuletzt genutzten Profil geöffnet. Wird diese Funktion aktiviert, wird nach einem Neustart des Systems immer das hierzu gehörige Profil geladen, unabhängig davon, welches Profil zuletzt genutzt wurde.

4.2 Netzeinwahl

Nur für Windows-Version verfügbar.

Dieses Parameterfeld beinhaltet den Benutzernamen und das Passwort, die bei der Anwahl an das Zielsystem zur Identifizierung benötigt werden. Diese beiden Größen werden auch für die PPP-Verhandlung zum ISP (Internet Service Provider) benötigt.

Das Parameterfeld erscheint überhaupt nicht, wenn der LANCOM Advanced VPN Client in der Verbindungsart "LAN over IP" betrieben wird.

-> siehe auch die Parameter:

- Benutzername [Netzeinwahl]
- Passwort [Netzeinwahl]
- Rufnummer (Ziel)
- Passwort speichern
- Script-Datei

DE

4.2.1 Benutzername [Netzeinwahl]

Mit dem "Benutzernamen" weisen Sie sich gegenüber dem Network Access Server (NAS) aus, wenn Sie eine Verbindung zum Zielsystem aufbauen wollen. Bei Kommunikation über das Internet benötigen Sie den Benutzernamen zur Identifikation am ISP (Internet Service Provider). Der Name für den Benutzer kann bis zu 256 Zeichen lang sein. Für gewöhnlich wird Ihnen ein "Benutzername" vom Zielsystem zugewiesen, da Sie vom Zielsystem (auch Radius- oder LDAP-Server) erkannt werden müssen. Sie erhalten ihn von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

4.2.2 Passwort [Netzeinwahl]

Das Passwort benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 256 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Hinweis: Für den Fall, dass Sie den Parameter "Passwort speichern" nicht aktiviert haben, gilt: Auch wenn Sie für den Verbindungsmodus "automatisch" gewählt haben, müssen Sie die Verbindung beim ersten Mal manuell aufbauen. Dabei werden Sie nach dem Passwort gefragt. Für jeden weiteren automatischen Verbindungsaufbau wird dieses Passwort selbständig übernehmen, bis Sie den PC erneut booten oder Sie das Profil wechseln.

4.2.3 Rufnummer (Ziel)

Für jedes Ziel muss eine Rufnummer definiert sein, da der LANCOM Advanced VPN Client ansonsten keine Verbindung herstellen kann. Diese Rufnummer muss genauso eingetragen werden, als würden Sie diese Telefonnummer per Hand wählen. D.h. Sie müssen alle notwendigen Vorwahlziffern berücksichtigen: Landesvorwahl, Ortsvorwahl, Durchwahlziffern, etc. etc.

Tragen Sie jedoch nicht die Amtsholung ein, auch wenn Sie an einer Nebenstellenanlage angeschlossen sind! Die Amtsholung wird unter

dem Monitor-Menüpunkt "Verbindung" eingetragen und hat auf diese Weise Gültigkeit für alle Rufe (siehe -> Amtsholung).

Beispiel: Sie wollen eine Verbindung von Deutschland nach England herstellen:

00 (für die internationale Verbindung, wenn Sie von Deutschland aus wählen)

44 (dies ist die landesspezifische Vorwahl für England)

171 (Vorwahl für London)

1234567 (die Nummer, die Sie zu erreichen wünschen)

Insgesamt wird nach diesem Beispiel folgende Nummer im Telefonbuch gespeichert und für die Anwahl verwendet: 00441711234567

Die Rufnummer des Ziels kann bis zu 30 Ziffern beinhalten.

Alternative Rufnummern:

Möglicherweise ist das Zielsystem ein Network Access Server (NAS), der mit mehreren S0-Anschlüssen für verschiedene Rufnummern ausgestattet ist. In diesen Fall empfiehlt es sich, alternative Rufnummern einzugeben - falls zum Beispiel die erste Nummer besetzt ist. Die alternativen Rufnummern werden der ersten Nummer angehängt, nur mit einem Doppelpunkt (:) oder einem Semikolon (;) getrennt.

Maximal werden 8 alternative Rufnummern unterstützt.

Beispiel : 00044171123456 7:00044171123456 8

Die erste Nummer ist die Standard-Rufnummer und wird immer zuerst gewählt. Kann keine Verbindung hergestellt werden, weil besetzt ist, wird die zweite Nummer gewählt, usw.

Wichtig: Bitte beachten Sie, dass der Verbindungsaufbau nur funktionieren kann, wenn die Protokoll-Eigenschaften für die Anschlüsse der alternativen Rufnummern die gleichen sind.

4.2.4 Passwort speichern

Dieser Parameter muss aktiviert (angeklickt) werden, wenn gewünscht wird, dass das Passwort und das Passwort Ziel (sofern es eingegeben ist) gespeichert wird. Andernfalls werden die Passwörter gelöscht, sobald der PC gebootet wird oder ein Zielsystem gewechselt wird. Standard ist die aktivierte Funktion.

Wichtig: Bitte beachten Sie, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann - auch wenn er die Passwörter nicht kennt.

4.2.5 Script-Datei

Wenn Sie den Microsoft DFÜ-Dialer benutzen, tragen Sie hier die Script-Datei unter Eingabe von Pfad und Namen ein.

4.3 Modem

Nur für Windows-Version verfügbar.

Dieses Parameterfeld erscheint ausschließlich, wenn Sie als "Verbindungsart" "Modem" gewählt haben. Alle nötigen Parameter zu dieser Verbindungsart sind hier gesammelt.

-> siehe auch die Parameter:

- Modem
- Anschluss
- Baudrate
- Com Port freigeben
- Modem Init. String
- Dial Prefix
- APN
- GPRS/UMTS
- PIN

4.3.1 Modem

Dieses Parameterfeld zeigt die auf dem PC installierten Modems. Wählen Sie aus der Liste das gewünschte Modem aus.

Je nachdem, welches Modem Sie wählen, werden die zugehörigen Parameter "Com Port" und "Modem Init. String" automatisch in die Konfigurationsfelder des Telefonbuchs aus der Treiberdatenbank des Systems übernommen.

(Weitere Parameter für dieses Kommunikationsmedium können auch über die Systemsteuerung des PCs konfiguriert werden.)

Hinweis: Bitte beachten Sie, dass Sie das Modem vor der Konfiguration der Verbindung im Telefonbuch installiert haben müssen, um es korrekt für Kommunikationsverbindungen nutzen zu können.

4.3.2 Anschluss

An dieser Stelle bestimmen Sie, welcher Com Port von Ihrem Modem genutzt werden soll. Wenn Sie bereits Modems unter Windows installiert haben, wird der während dieser Installation festgesetzte Com Port automatisch übernommen, sobald Sie das entsprechende Gerät unter "Modem" auswählen.

Hinweis: Wenn Sie ein bereits unter Ihrem System installiertes Modem nutzen möchten, so wählen Sie vor der Einstellung des Com Ports zuerst das gewünschte Gerät unter "Modem" aus - der entsprechend konfigurierte Com Port wird dann automatisch gesetzt.

4.3.3 Baudrate

Die Baudrate beschreibt die Übertragungsgeschwindigkeit zwischen Com Port und Modem. Wenn Ihr Modem z.b. mit 14.4 Kbits übertragen kann, sollten sie die nächsthöhere Baudrate 19200 wählen.

Folgende Baudraten können gewählt werden:

1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200

4.3.4 Com Port freigeben

Wenn Sie für Ihre Workstation ein analoges Modem verwenden, kann es wünschenswert sein, dass der Com Port nach Beendigung der Kommunikation für andere Applikationen freigegeben wird (z.B. Fax). In diesem Fall stellen Sie den Parameter auf "Ein". Solange der Parameter in der Standardstellung auf "Aus" bleibt, wird der Com Port ausschließlich von der LANCOM Advanced VPN Client Software genutzt.

4.3.5 Modem Init. String

Je nach eingesetzem Handy oder Modem und der jeweiligen Verbindungsart können AT-Kommandos nötig sein. In diesem Fall müssen die jeweiligen Kommandos dem zugehörigen Benutzerhandbuch oder den Mitteilungen der Telefongesellschaft bzw. des Providers entnommen werden. Jedes der in diesem Fall einzutragenden Kommandos muss mit einem <cr> (Carriage Return) abgeschlossen werden.

4.3.6 Dial Prefix

Dieses Feld ist optional. Ist das Modem korrekt installiert und steht der Software als Standardtreiber zur Verfügung, so muss hier kein Eintrag vorgenom-

men werden. Der Dial Prefix ist nur in seltenen Ausnahmefällen nötig. Ziehen Sie dazu das Modem-Handbuch zu Rate.

Im folgenden einige Beispiele für Dial Prefix:

- ATDT
- ATDP
- ATDI
- ATDX

4.3.7 APN

Der APN (Access Point Name) wird für die GPRS oder UMTS-Einwahl benötigt. Sie erhalten ihn von Ihrem Provider. Der APN wird insbesondere zu administrativen Zwecken genutzt.

4.3.8 GPRS/UMTS PIN

Benutzen Sie eine SIM-Einsteckkarte für GPRS (auch UMTS), so geben Sie hier die PIN für diese Karte ein. Benutzen Sie ein Handy, so muss diese PIN am Mobiltelefon eingegeben werden.

4.4 HTTP-Anmeldung

Nur für Windows-Version verfügbar.

Mit den Einstellungen in diesem Parameterfeld kann die automatische script-gesteuerte HTTP-Anmeldung vorgenommen werden. Zentral erstellte Anmelde-Scripts und die hinterlegten Anmeldedaten können vom Access Point (HotSpot) übernommen werden, ohne dass ein Browserfenster geöffnet wird.

Bitte beachten Sie, dass die Verbindung über einen HotSpot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des HotSpot-Betreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

Wenn der Access Point einen HTTP-Redirect ausführt, kann die Eingabe von Benutzername und Passwort in einem Browser-Fenster entfallen. Statt dessen erfolgt die Authentisierung mit den hier eingegebenen Daten automatisch im Hintergrund.

Für die script-gesteuerte Anmeldung kann ein Script aus dem Installationsverzeichnis

\scripts\samples

für weitere HotSpots entsprechend angepasst werden.

Bei der Verbindungsart WLAN werden die Authentisierungsdaten für den Hotspot aus den WLAN-Einstellungen übernommen.

4.4.1 Benutzername [HTTP-Anmeldung]

Dies ist der Benutzername, den Sie von Ihrem HotSpot-Betreiber erhalten haben.

4.4.2 Passwort [HTTP-Anmeldung]

Dies ist das Passwort, das Sie von Ihrem HotSpot-Betreiber erhalten haben. Das Passwort wird in verdeckter Schreibweise (mit *) eingegeben.

4.4.3 Passwort speichern [HTTP-Anmeldung]

Nachdem das Passwort eingegeben wurde, kann es gespeichert werden.

4.4.4 HTTP Authentisierungs-Script [HTTP-Anmeldung]

Hier kann nach Klick auf den Suchen-Button [...] das hinterlegte Anmelde-Script selektiert werden.

Um eingehende Zertifikate bei der HTTP-Authentisierung überprüfen zu können, muss im Script die Variable CACERTDIR gesetzt worden sein. Desweiteren können auch Inhalte des WEB Server-Zertifikats überprüft werden. Hierzu stehen weitere Variablen zur Verfügung:

`CACERTVERIFY_SUBJECT`

überprüft den Inhalt des Subjects (z.B. cn=WEB Server 1),

`CACERTVERIFY_ISSUER`

Überprüft den Inhalt der Issuers,

`CACERTVERIFY_FINGERPRINT`

überprüft den MD5 Fingerprint des Aussteller-Zertifiats.

Stimmt der Inhalt der Variable mit dem eingegebenen Zertifikat nicht überein, wird die SSL-Verbindung nicht hergestellt und eine Log-Meldung im Monitor ausgegeben.

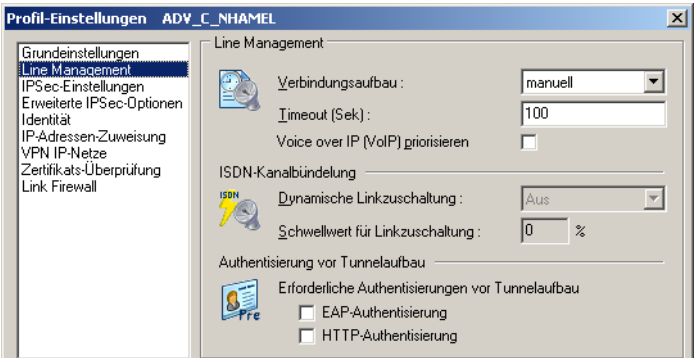
DE

4.5 Line Management

Nur für Windows-Version verfügbar.

In diesem Parameterfeld bestimmen Sie, wie der "Verbindungsaufbau" erfolgen soll und stellen die Timeout-Werte ein.

Wenn Sie die Workstation in der Verbindungsart ISDN betreiben, können Sie in diesem Parameterfeld auch eine Kanalbündelung aktivieren. Bitte beachten Sie dabei, dass die Kanalbündelung nur funktionieren kann, wenn sowohl der LANCOM Advanced VPN Client als auch der NAS für eine Verbindung über gleich viele mögliche Kanäle verfügen.



-> siehe auch die Parameter:

- Verbindungsaufbau
- Timeout
- Dynamische Linkzuschaltung (nur bei Verbindungsart ISDN möglich)
- Schwellwert für Linkzuschaltung (nur bei Verbindungsart ISDN möglich)
- EAP-Authentisierung
- HTTP-Authentisierung
- Voice over IP (VoIP) priorisieren

4.5.1 Verbindungsaufbau

Hier definieren Sie, wie die Verbindung über ein Profil zum eingetragenen Zielsystem aufgebaut werden soll. Drei Modi stehen zur Wahl:

manuell = In diesem Fall müssen Sie die Verbindung zum Zielsystem manuell herstellen. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout. Ist der Timeout auf Null (0) gesetzt, d.h. kein Timeout eingestellt, müssen Sie in jedem Fall die Verbindung manuell trennen.

automatisch (default) = Dies bedeutet, dass die LANCOM Advanced VPN Client Software die Verbindung zum Zielsystem automatisch herstellt. Das Trennen der Verbindung erfolgt je nach Protokoll Ihres Systems, entsprechend den Anforderungen der Anwendung und den Einstellungen im Telefonbuch.

wechselnd = Wird dieser Modus gewählt, muss zunächst die Verbindung "manuell" aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau:

- Wird die Verbindung nun mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung "automatisch" hergestellt,
- wird die Verbindung manuell abgebaut, muss sie auch wieder manuell aufgebaut werden.

Wichtig: Sollten Sie den Verbindungsaufbau auf "manuell" setzen, so sollten Sie den Timeout aktivieren, um den Verbindungsabbau zu automatisieren. Andernfalls könnten unnötige Verbindungskosten für Sie entstehen.

4.5.2 Timeout

Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 0 und 65535 angegeben. Der Standardwert ist "40".

Wenn Ihr Anschluss (ISDN oder analog) einen Gebührenimpuls erhält, verwendet die LANCOM Advanced VPN Client Software das Impulsintervall, um den optimalen Zeitpunkt des Verbindungsabbaus bezüglich dem von Ihnen gesetzten Wert zu ermitteln. Der nach Gebührentakt optimierte Timeout läuft im Hintergrund und hilft die Verbindungskosten zu reduzieren.

Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65356 einzutragen. Mit dem Wert "0" wird der automatische Timeout (Verbindungsabbau) nicht ausgeführt. Der Wert "0" bedeutet, dass das Trennen der Verbindung manuell durchgeführt werden muss. Ziehen Sie bei diesem Parameter bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

Wichtig: Der Timer für das gewählte Zeitintervall läuft erst dann an, wenn keine Datenbewegung oder Handshaking mehr auf der Leitung stattfindet.

DE

4.5.3 Voice over IP (VoIP) priorisieren

Wird dieser Client für Kommunikation mit Voice over IP genutzt, so sollte diese Funktion aktiviert werden, um die Sprachdaten verzögerungs- und verzerrungsfrei senden und empfangen zu können.

Für die VoIP-Priorisierung werden definierte Ports auf eingehende bzw. ausgehende Verbindungen überwacht. Sollte eine solche Verbindung entstehen, so wird die Bandbreite für das FTP- und SMB-Protokoll reduziert. Nach dem Abbau dieser Verbindung wird die Bandbreite wieder freigegeben.

4.5.4 Dynamische Linkzuschaltung

Nur für ISDN.

Mit dynamischer Linkzuschaltung (für ISDN) kann die LANCOM Advanced VPN Client Software bis zu 8 ISDN B-Kanäle bündeln. Um diese Funktion in vollem Umfang nutzen zu können, muss allerdings Ihr PC wie auch das Zielsystem mit der nötigen Anzahl von So-Schnittstellen (4) ausgestattet sein.

Die dynamische Linkzuschaltung funktioniert nur, wenn sie auch vom Network Access Server des Zielsystems unterstützt wird. Mit dynamischer Linkzuschaltung erhöhen sich zwar die Kosten für jeden zugeschalteten B-Kanal, gleichzeitig verringern sie sich jedoch in gleichem Maße, weil sich die Übertragungsdauer entsprechend verkürzt!

Mit diesem Parameter bestimmen Sie, wie die Linkzuschaltung erfolgen soll. Drei Möglichkeiten stehen zur Auswahl:

- Aus = (standard)
- Tx = Links werden zugeschaltet, entsprechend der vom Sender geforderten Bitrate
- Rx = Links werden zugeschaltet, entsprechend der vom Empfänger geforderten Bitrate
- TxRx= Links werden sowohl nach der vom Sender als auch der vom Empfänger geforderten Bitrate zugeschaltet

4.5.5 Schwellwert für Linkzuschaltung

Nur für ISDN

Der Wert dieses Parameters teilt der LANCOM Advanced VPN Client Software die Bitrate mit, ab der ein weiterer Link (Kanal) zugeschaltet werden soll. Der Wert entspricht Prozenten der maximalen Bitrate. Mögliche Werte sind von 1 bis 100 (Prozent). Standardwert ist "20". Diese Einstellung gilt für Sender und Empfänger.

Ein Wert kann hier nur eingetragen werden, wenn dynamische Linkzuschaltung aktiviert wurde.

Wichtig: Diese Einstellung kommt nur zum Tragen, wenn die Gegenstelle dynamische Linkzuschaltung unterstützt.

4.5.6 EAP-Authentisierung

Muss sich der Client mit EAP (Extensible Authentication Protocol) authentisieren, so muss diese Funktion aktiviert werden. Sie bewirkt, dass für dieses Zielsystem die EAP-Konfiguration im Monitor-Menü unter "EAP-Optionen" zum Einsatz kommt.

Bitte beachten Sie, dass die EAP-Konfiguration im Monitor-Menü für alle Zielsysteme gültig ist und aktiv geschaltet sein muss, wenn diese linkspezifische Einstellung wirksam sein soll.

EAP wird dann eingesetzt, wenn für das wireless LAN ein Access Point verwendet wird, der 802.1x-fähig ist und eine entsprechende Authentisierung verlangt. EAP kann aber auch dann eingesetzt werden, wenn der Client über einen Router auf ein anderes Netzsegment des Firmennetzes zugreifen möchte. Generell wird mit EAP verhindert, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Nach Konfiguration des EAP muss eine Statusanzeige im grafischen Feld des Monitors erscheinen. Ist dies nicht der Fall, so muss die EAP-Konfiguration im Monitor-Menü aktiv geschaltet werden. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt die EAP-Verhandlung erneut.

4.5.7 HTTP-Authentisierung

Für die automatische HTTP-Authentisierung am Access Point (HotSpot) muss diese Funktion aktiviert werden.

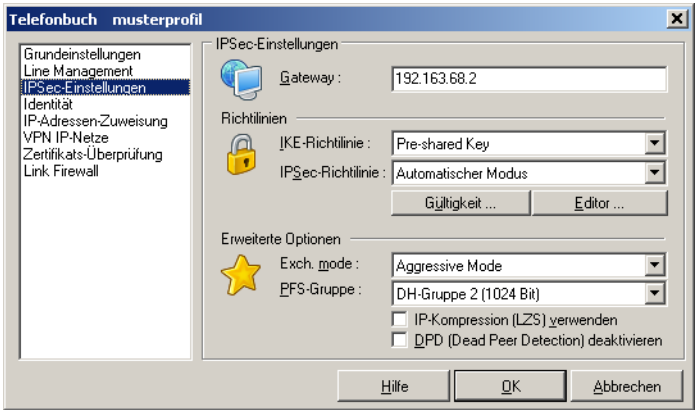
Damit wird ein weiteres Parameterfeld "HTTP-Anmeldung" im Telefonbuch zugeschaltet, in welches im folgenden die Authentisierungsdaten eingegeben werden können (siehe -> HTTP-Anmeldung).

DE

Bei einem Link mit dem Verbindungsmedium WLAN wird die HTTP-Anmeldung im Telefonbuch nicht zugeschaltet! Statt dessen wird mit der Aktivierung dieser Funktion bewirkt, dass für dieses Zielsystem die Authentisierungsdaten aus den WLAN-Einstellungen im Monitor-Menü zum Einsatz kommen.

Bitte beachten Sie, dass die Verbindung über einen HotSpot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des HotSpotbetreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

4.6 IPSec-Einstellungen



4.6.1 Gateway

Dies ist die IP-Adresse des VPN Gateways, auch Tunnel-Endpunkt. Sie erhalten die Adresse von Ihrem Administrator entweder als Hex-Adresse, wenn das VPN Gateway über eine feste offizielle IP-Adresse verfügt - oder als Namens-String, wenn das VPN Gateway eine wechselnde IP-Adresse von einem Internet Service Provider erhält.

Hex-Adresse: Die Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen.

Namens-String: Sie tragen den Namen ein, den Sie von Ihrem Administrator erhalten haben. Es handelt sich dabei um den DNS-Namen des Gateways, der beim DynDNS Service Provider hinterlegt wurde.

4.6.2 IKE-Richtlinie

Die IKE-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IKE-Richtlinien aufgeführt, die Sie im Konfigurationsbaum unter der Verzweigung **IPSec > IKE-Richtlinie** angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Von Gegenstelle bestimmt: In diesem Fall kann die Konfiguration der IKE-Richtlinie im IPSec-Menü entfallen.

Pre-shared Key: Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden. Beidseitig wird der gleiche "Statische Schlüssel" verwendet (siehe oben -> Statischer Schlüssel).

RSA-Signatur: Diese vorkonfigurierte Richtlinie kann nur mit PKI-Unterstützung eingesetzt werden. Als zusätzliche, verstärkte Authentisierung ist der Einsatz der RSA-Signatur nur sinnvoll unter Verwendung einer Smart Card oder eines Soft-Zertifikats.

4.6.3 IPSec-Richtlinie

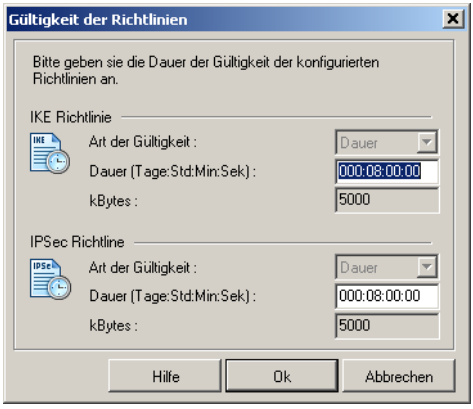
Die IPSec-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IPSec-Richtlinien aufgeführt, die Sie unter **Konfiguration > IPSec > IPSec-Richtlinie** angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Von Gegenstelle bestimmt: In diesem Fall kann die Konfiguration der IKE-Richtlinie im IPSec-Menü entfallen.

DE

4.6.4 Richtlinien-Gültigkeit



Die hier definierte Dauer der Gültigkeit gilt für alle Richtlinien gleichermaßen.

Art der Gültigkeit

Bestimmt nach welchen Kriterien die Art der Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach beiden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

- **Dauer [IKE-Richtlinie]**

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

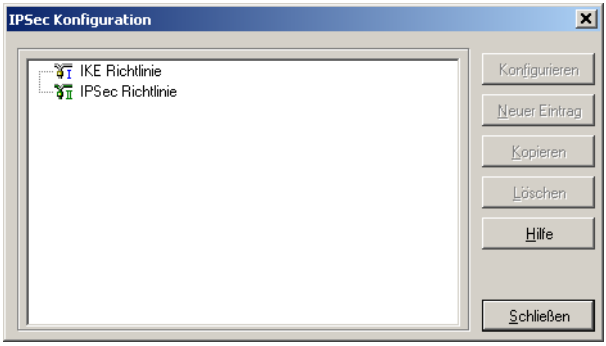
- **kBytes [IKE-Richtlinie]**

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

4.6.5 Richtlinien-Editor

Zur Konfiguration der Richtlinien und gegebenenfalls einer statischen Secure Policy Database wird dieser Menüpunkt angeklickt. Damit öffnet sich ein Konfigurationsfenster mit der Verzweigung der Richtlinien und Secure Policy Database zu IPSec, sowie Buttons zur Bedienung auf der rechten Seite des Konfigurationsfensters.

Um die (Standard-)Werte der Richtlinien zu editieren, d.h. Parameter so einzustellen oder abzuändern, wie es den Verbindungsanforderungen zum definierten Zielsystem entspricht, wählen Sie mit der Maus die Richtlinie, deren Werte Sie ändern möchten - die Buttons zur Bedienung werden dann aktiv.



Konfigurieren

Um eine Richtlinie oder eine SPD abzuändern, wählen Sie mit der Maus den Namen, der Gruppe deren Werte Sie ändern möchten und klicken auf **Konfigurieren**. Dann öffnet sich das entsprechende Parameterfeld mit den IPSec-Parametern.

Neuer Eintrag

Wenn Sie eine neue Richtlinie oder SPD anlegen möchten, selektieren Sie eine der Richtlinien oder die SPD und klicken auf **Neuer Eintrag**. Die neue Richtlinie oder SPD wird erzeugt. Alle Parameter sind auf Standardwerte gesetzt, bis auf den Namen. Kopieren

Um die Parameter-Einstellungen eines bereits definierten Richtlinie oder SPD zu kopieren, markieren sie die zu kopierende Richtlinie oder SPD und klicken auf **Kopieren**. Daraufhin wird das Parameterfeld geöffnet. Ändern Sie nun den Namen und klicken Sie anschließend Ok. Die neue Richtlinie oder SPD ist nun angelegt. Die Parameterwerte sind zu denen der kopierten identisch, bis auf den Namen.

Löschen

Wenn Sie eine Richtlinie oder SPD aus dem Konfigurationsbaum löschen wollen, selektieren Sie sie und klicken auf **Löschen**. Die Richtlinie oder SPD ist damit auf Dauer aus der IPSec-Konfiguration gelöscht.

DE

Schließen

Wenn Sie das IPSec-Feld schließen, kehren Sie zum Monitor zurück. Die Daten werden so wie sie konfiguriert wurden behalten.

- **IKE-Richtlinie**

Die Parameter in diesem Feld beziehen sich auf die Phase 1 des Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird. Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in dem Parameterfeld "IPSec-Einstellungen" im Telefonbuch.

Die IKE-Richtlinien, die Sie hier konfigurieren, werden zur Auswahl gelistet.

Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf, d.h. eine Richtlinie kann aus mehreren Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons **Hinzufügen** und **Entfernen** erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Parameter:

- Name [IKE-Richtlinie]
- Authentisierunng [IKE-Richtlinie]
- Verschlüsselung [IKE-Richtlinie]
- Hash [IKE-Richtlinie]
- DH-Gruppe [IKE-Richtlinie]

Name [IKE-Richtlinie]

Geben Sie dieser Richtlinie einen Namen, über den sie später einer SPD zugeordnet werden kann.

Authentisierung [IKE-Richtlinie]

Bevor der Kontrollkanal für die Phase 1-Verhandlung (IKE Security Association) aufgebaut werden kann, muss beidseitig eine Authentisierung stattgefunden haben.

Zur gegenseitigen Authentisierung wird der allen gemeinsame pre-shared Key (statischer Schlüssel) verwendet. Diesen Schlüssel definieren Sie im Parameterfeld "Identität".

Verschlüsselung [IKE-Richtlinie]

Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal, sofern der Main Mode (Identity Protection Mode) gefahren wird. Zur Wahl stehen: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

Hash [IKE-Richtlinie]

Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird. Zur Wahl stehen: MD5 (Message Digest, Version 5) und SHA (Secure Hash Alogrithm), SHA 256, SHA 384 und SHA 512.

DH-Gruppe [IKE-Richtlinie]

Mit der Wahl einer der angebotenen Diffie-Hellmann-Gruppen wird festgelegt, wie sicher der Key Exchange im Kontrollkanal erfolgen soll, nach dem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH Group desto sicherer ist der Key Exchange.

- **IPSec-Richtlinie [IPSec]**

Die IPSec-Richtlinien (Phase-2-Parameter), die Sie hier konfigurieren, werden zur Auswahl für die SPD gelistet.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons **Hinzufügen** und **Entfernen** erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Parameter:

- Name [IPSec-Richtlinie]
- Protokoll [IPSec-Richtlinie]
- Transformation [IPSec-Richtlinie]
- Authentisierung (nur ESP) [IPSec-Richtlinie]

Name [IPSec-Richtlinie]

Geben Sie dieser Richtlinie einen Namen, über den Sie sie später einer SPD zuordnen können.

Protokoll [IPSec-Richtlinie]

Die IPSec-Richtlinien sind im Wesentlichen nach den beiden Sicherheitsprotokollen unterschieden, AH oder ESP, die sich im Tunnelmodus gegenseitig ausschließen. Die fest eingestellte Standardwert ist ESP.

Transformation [IPSec-Richtlinie]

Wenn das Sicherheitsprotokoll ESP eingestellt wurde, kann hier definiert werden wie mit ESP verschlüsselt werden soll. Zur Wahl stehen die gleichen Verschlüsselungsalgorithmen wie für Layer 2: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

Authentisierung [IPSec-Richtlinie]

Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung eigens eingestellt werden. Zur Wahl stehen: MD5 und SHA.

4.6.6 Exch. mode

Der Exchange Mode (Austausch-Modus) bestimmt wie der Internet Key Exchange vonstatten gehen soll. Zwei unterschiedliche Modi stehen zur Verfügung, der Main Mode, auch Identity Protection Mode und der Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch deren Verschlüsselung.

- **Main Mode:**

Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden - daher auch Identity Protection Mode.

- **Aggressive Mode:**

Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

4.6.7 PFS-Gruppe

Mit Auswahl einer der angebotenen Diffie-Hellmann-Gruppen wird festgelegt, ob ein kompletter Diffie-Hellmann-Schlüsselaustausch (PFS, Perfect Forward Secrecy) in Phase 2 zusätzlich zur SA-Verhandlung stattfinden soll. Standard ist “keine”.

4.7 Erweiterte IPSec-Optionen

Benutze IP-Kompression (LZS)

Die Datenübertragung mit IPSec kann ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache.

Deaktiviere DPD (Dead Peer Detection)

DPD (Dead Peer Detection) und NAT-T (NAT Traversal) werden automatisch im Hintergrund ausgeführt, sofern dies das Ziel-Gateway unterstützt. Der IPSec Client nutzt DPD, um in regelmäßigen Intervallen zu prüfen, ob die Gegenstelle noch aktiv ist. Ist dies nicht der Fall, erfolgt ein automatischer Verbindungsabbau.

Mit dieser Funktion kann DPD ausgeschaltet werden.

UDP-Encapsulation verwenden

Mit UDP-Encapsulation muss an der externen Firewall nur der Port 4500 freigeschaltet werden (anders bei NAT Traversal oder UDP 500 mit ESP). Das NCP Gateway erkennt die UDP-Encapsulation automatisch.

Wird die UDP-Encapsulation verwendet, so kann der Port frei gewählt werden. Standard für IPSec mit UDP ist der Port 4500, für IPSec ohne UDP der Port 500.

VPN Path Finder

Mit dem VPN Path Finder können IPsec-Datenverbindungen auch hinter Firewalls aufgebaut werden, selbst wenn deren Port Einstellungen dies grundsätzlich verhindern (z.B. in Hotels oder Hotspots). So kann die IPsec-basierte Datenübertragung vollständig gewährleistet werden.

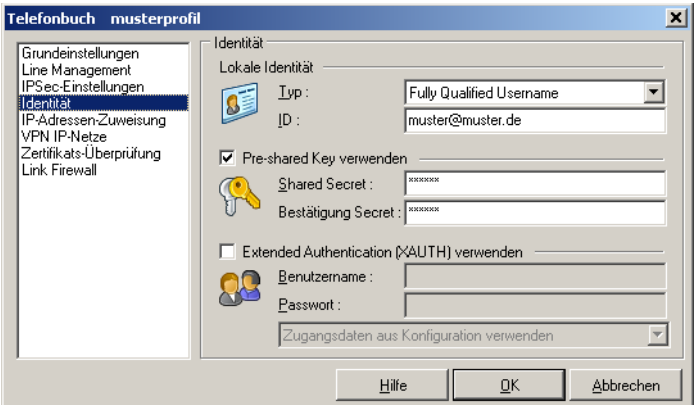
Der VPN Path Finder schaltet automatisch auf das alternative Verbindungsprotokoll TCP Encapsulation mit SSL Header (Port 443) um, sobald der Standart IPsec über Port 500 bzw. UDP Encapsulation über einen frei konfigurierbaren Port nicht möglich ist.Dies ist dann von Bedeutung, wenn für den Client nur der HTTPS Port 443 zur Verfügung steht und eine reine IPsec-Verbindung nicht möglich ist. Ebenso ist es möglich einen Proxy Server voran zu schalten, wenn dies für die Verbindung notwendig ist.

Der VPN Path Finder setzt als Gegenstelle einen LANCOM VPN-Router mit LCOS Version 8.0 oder höher vorraus.

DE

4.8 Identität

Entsprechend des Sicherheitsmodus IPSec kann noch detailliertere Sicherheitseinstellungen vorgenommen werden.



4.8.1 Typ [Identität]

Bei IPSec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Folgende ID-Typen stehen zur Auswahl:

- IP Address
- Fully Qualified Domain Name
- Fully Qualified Username
- IP Subnet Address
- ASN1 Distinguished Name
- ASN1 Group Name
- Free String used to identify Groups

4.8.2 ID [Identität]

Bei IPSec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Entsprechend dem ID-Typ muss die zugehörige ID als String eingetragen werden.

4.8.3 Pre-shared Key

Der Pre-shared Key wird zur Verschlüsselung verwendet und ist ein String beliebiger Zeichen in einer maximalen Länge von 255 Zeichen. Alle alphanumerischen Zeichen können verwendet werden. Wenn die Gegenstelle einen pre-shared Key während der IKE-Verhandlung erwartet, dann muss dieser Schlüssel in das Feld "Shared Secret" eingetragen werden.

Bestätigen Sie das "Shared Secret" im darunter liegenden Feld. Der gleiche pre-shared Key muss auf beiden Seiten verwendet werden.

Wird der Pre-shared Key nicht verwendet, so wird zur Verschlüsselung der Private Key eines zu konfigurierenden Zertifikats genutzt.

4.8.4 Benutze erweiterte Authentisierung (XAUTH)

Wird "IPSec-Tunneling" genutzt, so kann die Authentisierung über Extended Authentication (XAUTH Protokoll, Draft 6) erfolgen. Wird XAUTH eingesetzt und vom VPN Gateway untersützt, so aktivieren Sie "Benutze erweiterte Authentisierung (XAUTH)". Zusätzlich zum pre-shared Key können dann noch folgende Parameter gesetzt werden:

- Benutzername = Benutzername des IPSec-Benutzers
- Passwort = Kennwort des IPSec-Benutzers

4.8.5 Benutze Zugangsdaten aus Konfiguration

Als Zugangsdaten für das VPN können folgende Einträge ausgelesen und verwendet werden:

- Benutze Zugangsdaten aus Konfiguration: Dies bedeutet, dass die in diesem Parameterfeld unter "Benutzername" und "Passwort" gemachten Angaben zur erweiterten Authentisierung verwendet werden.
- Benutze Zugangsdaten aus Zertifikat (E-Mail): Dies bedeutet, dass statt "Benutzername" und "Passwort" der E-Mail-Eintrag des Zertifikats verwendet wird.
- Benutze Zugangsdaten aus Zertifikat (Common Name): Dies bedeutet, dass statt "Benutzername" und "Passwort" der Benutzer-Eintrag des Zertifikats verwendet wird.

- Benutze Zugangsdaten aus Zertifikat (Seriennummer): Dies bedeutet, dass statt "Benutzername" und "Passwort" die Seriennummer des Zertifikats verwendet wird.

4.8.6 Benutzername [Identität]

Den Benutzernamen für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

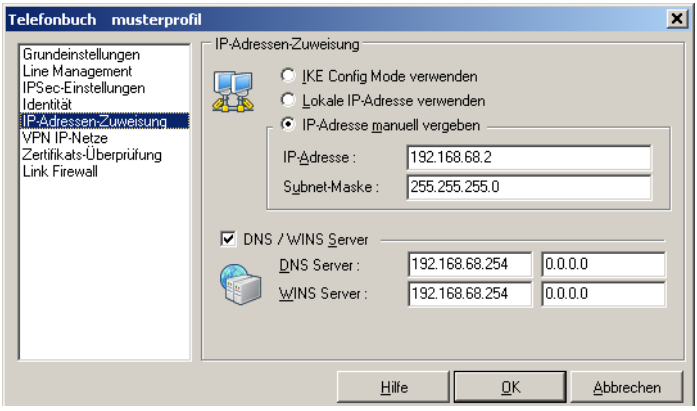
Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das VPN Gateway auf der remote Seite zu bekommen.

4.8.7 Passwort [Identität]

Das Passwort für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das VPN Gateway auf der remote Seite zu bekommen.

4.9 IP-Adressen-Zuweisung



4.9.1 Zuweisung der privaten IP-Adresse

In diesem Parameterfeld kann angegeben werden, wie die IP-Adresse zugewiesen werden soll.

Benutze IKE Config Mode

Mit IKE Config Mode (Draft 2) werden dynamische IP des Clients, des DNS- und WINS-Servers sowie der Domain Name zugewiesen. Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

Bei "IPSec-Tunneling" wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Der Einsatz von NAT Traversal erfolgt beim Client automatisch und ist immer nötig, wenn auf Seiten des Zielsystems ein Gerät mit Network Address Translation zum Einsatz kommt.

Benutze lokale IP-Adresse

In diesem Fall wird die aktuell in den Netzwerkeinstellungen des PCs konfigurierte IP-Adresse (auch DHCP) für den LANCOM Advanced VPN Client genutzt. (Dies ist die Standard-Einstellung).

Benutze manuelle IP-Adresse

Dies ist die IP-Adresse und die Subnet-Maske, die hier frei eingegeben werden können. In diesem Fall wird die hier eingetragene Adresse genutzt, unabhängig von der Konfiguration in den Netzwerkeinstellungen.

DHCP über IPSec

Alternativ zur Verwendung des IKE Config Modes kann auch ein DHCP Server des Gateways genutzt werden. Dabei wird über den VPN-Tunnel dem Client in einer DHCP-Verhandlung die IP-Adrsse zugeweisen.

4.9.2 DNS/WINS

Wird die Funktion IKE Config Mode aktiviert, kann alternativ zu dem DNS/WINS-Server, der automatisch während der PPP-Verhandlung zum NAS/ISP zugewiesen wird, ein anderer DNS/WINS Server bestimmt werden.

4.9.3 DNS-Server

Der zuerst eingetragene DNS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt.

DE

4.9.4 WINS-Server

Der zuerst eingetragene WINS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt.

4.9.5 Domain Name

Dies ist der Domain Name der sonst per DHCP dem System in den Netzwerkeinstellungen übergeben wird.

4.10 VPN IP-Netze

Hier können genau die IP-Netze definiert werden, über die der Client via VPN-Tunnel komunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so wird die Verbindung immer zum Tunnel-Endpunkt des VPN Gateways aufgebaut. Soll alternativ ein Tunneling zur Zentrale erfolgen, so müssen hier die IP-Netze eingetragen werden, die vom Client erreicht werden sollen.

Hinweis: Dies wird auch als “Split Tunneling” bezeichnet.

4.10.1 Netzwerk-Adressen [VPN IP-Netze]

In diesem Parameterfenster definieren Sie, in welchem IP-Netz oder welchen IP-Netzen der Client über VPN-Tunneling kommunizieren kann. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie ferner darauf, daß die IP-Adresse des VPN Gateways nicht im Bereich der Netz-Adresse liegt.

4.10.2 Subnet-Masken

Hier tragen Sie die zugehörige Netzmaske des IP-Netzes ein. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie darauf, daß die IP-Adresse des VPN Gateways nicht im Bereich der Netz-Adresse liegt.

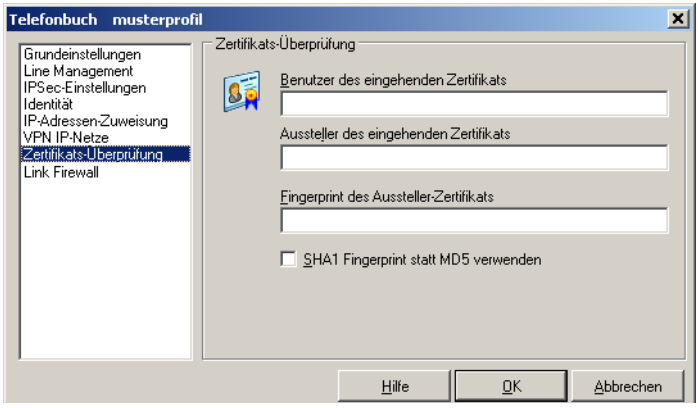
4.10.3 Auch lokale Netze im Tunnel weiterleiten

Wenn der Datenverkehr des lokalen Netzes über VPN-Tunneling weitergeleitet werden soll, so muss diese Funktion aktiviert werden.

4.11 Zertifikats-Überprüfung

Überprüfung der Zertifikatsinhalte

Im Parameterfeld "Zertifikats-Überprüfung" kann pro Zielsystem des LANCOM Advanced VPN Clients vorgegeben werden, welche Einträge in einem Zertifikat der Gegenstelle (VPN Gateway) vorhanden sein müssen (siehe -> Eingehendes Zertifikat anzeigen, Allgemein).



-> siehe auch:

Benutzer des eingehenden Zertifikats Aussteller des eingehenden Zertifikats Fingerprint des Aussteller-Zertifikats Benutze SHA1 Fingerprint statt MD5 Weitere Zertifikats-Überprüfungen

DE

4.11.1 Benutzer des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Benutzers, soweit bekannt - auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu, welche Einträge bei "eingehendes Zertifikat anzeigen" unter Benutzer aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

- cn = Common Name / Name
- s = Surname / Nachname
- g = Givenname / Vorname
- t = Title / Titel
- o = Organisation / Firma
- ou = Organization Unit / Abteilung
- c = Country / Land
- st = State / Bundesland, Provinz
- l = Location / Stadt, Ort

email = E-mail

Beispiel: cn=VPNGW*, o=ABC, c=de Der Common Name des Security Servers wird hier nur bis zur Wildcard "*" überprüft. Alle nachfolgenden Stellen können beliebig sein, etwa 1 - 5 als Numerierung. Die Organzation Unit muss in diesem Fall immer ABC sein und das Land Deutschland.

4.11.2 Aussteller des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Ausstellers, soweit bekannt - auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu welche Einträge bei "eingehendes Zertifikat anzeigen" unter Aussteller aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

- cn = Common Name / Name
- s = Surname / Nachname
- g = Givenname / Vorname
- t = Title / Titel
- o = Organisation / Firma
- ou = Organization Unit / Abteilung

- c = Country / Land
- st = State / Bundesland, Provinz
- l = Location / Stadt, Ort email = E-mail

Beispiel: cn=ABC GmbH Hier wird nur der Common Name des Ausstellers überprüft.

4.11.3 Fingerprint des Aussteller-Zertifikats

Um zu verhindern, dass ein Unberechtigter, der die vertrauenswürdige CA imitiert, ein gefälschtes Aussteller-Zertifikat verwenden kann, kann zusätzlich der Fingerprint des Ausstellers, soweit bekannt, eingegeben werden.

4.11.4 Benutze SHA1 Fingerprint statt MD5

Der Algorithmus zur Erzeugung des Fingerprints kann MD5 (Message Digit 5) oder SHA1 (Secure Hash Algorithm 1) sein.

4.11.5 Weitere Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am LANCOM Advanced VPN Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Windows-Verzeichnis \CaCerts\ gespielt. Das Einspielen kann bei einer Software-Distribution mit Disketten automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software im Root-Verzeichnis der ersten Diskette befinden. Nachträglich können Aussteller-Zertifikate automatisch über den Secure Update Server verteilt werden (siehe -> Handbuch zum Update Server), oder - sofern der Benutzer über die notwendigen Schreibrechte in genanntem Verzeichnis verfügt - von diesem selbst eingestellt werden (siehe -> CA-Zertifikate anzeigen).

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt **Verbindung > Zertifikate > CA-Zertifikate anzeigen** eingesehen werden.

Wird am LANCOM Advanced VPN Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend

im Verzeichnis CaCerts\. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande.

Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den LANCOM Advanced VPN Client und das VPN Gateway sind drei Erweiterungen von Bedeutung:

- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier

extendedKeyUsage:

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der LANCOM Advanced VPN Client, ob der definierte erweiterte Verwendungszweck "SSL-Server-Authentisierung" enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

Ausnahme: Bei einem Rückruf des Servers an den Client nach einer Direkteinwahl ohne VPN aber mit PKI prüft der Server das Zertifikat des Clients auf die Erweiterung extendedKeyUsage. Ist diese vorhanden, muss der Verwendungszweck "SSL-Server-Authentisierung"

beinhaltet sein, sonst wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

subjectKeyIdentifier / authorityKeyIdentifier:

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades.

(Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem LANCOM Advanced VPN Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Windows-Verzeichnis \crls\ gespielt. Ist eine CRL vorhanden, so überprüft der LANCOM Advanced VPN Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Windows-Verzeichnis \arls\ gespielt werden muss.

Sind eingehende Zertifikate in den Listen von CRL oder ARL enthalten, wird die Verbindung nicht zugelassen.

Sind CRLs oder ARLs nicht vorhanden findet keine diesbezügliche Überprüfung statt.

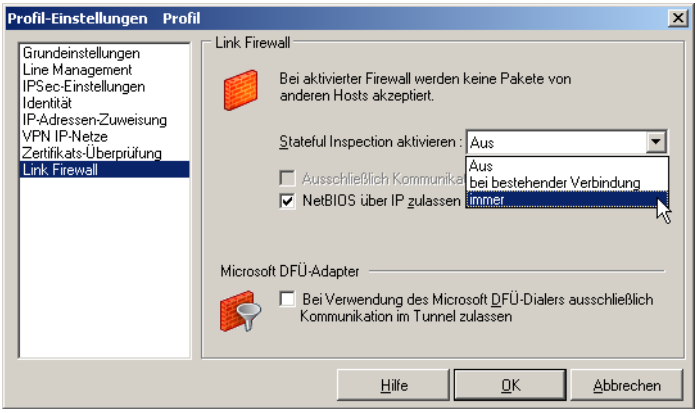
4.12 Link-Firewall

Die Link-Firewall für alle Netzwerkadapter wie auch für RAS-Verbindungen genutzt werden. Die aktivierte Firewall wird in der grafischen Oberfläche des Clients als Symbol (Mauer mit Pfeil) dargestellt.

Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und

DE

entscheidet auf der Basis vorher festgelegter Konfigurationen, ob ein Datenpaket durchgelassen wird oder nicht. Die hier zu aktivierende Firewall arbeitet nach dem Prinzip der Stateful Inspection. Stateful Inspection ist eine neue Firewall-Technologie und bietet den derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung „Tochterverbindungen" geöffnet hat – bei den Protokollen UDP, TCP, FTP (active und passive Mode) und ICMP – deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf (siehe -> Handbuch, Beispiele und Erklärungen).



4.12.1 Aktiviere Stateful Inspection

aus: Die Sicherheitsmechanismen der Firewall werden nicht in Anspruch genommen.

immer: Die Sicherheitsmechanismen der Firewall werden immer in Anspruch genommen, d.h. auch wenn keine Verbindung aufgebaut ist, ist der PC vor unberechtigten Zugriffen geschützt.

bei bestehender Verbindung: Der PC ist dann nicht angreifbar, wenn eine Verbindung besteht.

4.12.2 Ausschließlich Kommunikation im Tunnel zulassen

Ausschließlich Kommunikation im Tunnel zulassen: Bei aktivierter Firewall kann diese Funktion zusätzlich eingeschaltet werden, um in ein- und ausgehender Richtung ausschließlich VPN-Verbindungen zuzulassen.

Beachten Sie bitte, dass bei gleichzeitiger Benutzung der LANCOM LANCAPI diese Einstellung ausgeschaltet bleiben muss, da sonst der LANCAPI Server im lokalen Netzwerk nicht mehr erreicht werden kann.

4.12.3 Erlaube NetBios over IP

Mit diesem Parameter wird ein Filter aufgehoben, der Microsoft NetBios Frames unterdrückt. Diesen Filter aufzuheben, um den Verkehr von NetBios Frames zu gestatten, ist immer dann zweckmäßig, wenn Sie zum Beispiel Microsoft Networking über den LANCOM Advanced VPN Client nutzen.

In der Standardeinstellung ist dieser Filter gesetzt, das heißt der Checkbutton nicht mit einem Haken markiert, so dass Microsoft NetBios Frames unterdrückt werden, damit sie den Datenverkehr nicht unnötig belasten. Markieren Sie den Checkbutton mit einem Haken, werden NetBios Frames over IP erlaubt.

4.12.4 Bei Verwendung des Microsoft DFÜ-Dialers ausschließlich Kommunikation im Tunnel zulassen

Nur für Windows-Version verfügbar.

Bei Verwendung des Client-Monitors wird bei Aktivierung dieser Funktion verhindert, dass eine Kommunikation über den DFÜ-Dialer zum Internet stattfinden kann.

4.13 UMTS- oder GRPS-Profil einrichten

Nur für Windows-Version verfügbar.

Mit dem LANCOM Advanced VPN Client können Sie auch von unterwegs mit dem Notebook gesicherte Verbindungen zum eigenen Netzwerk oder zum Netzwerk der Zentrale herstellen und auf alle verfügbaren Dienste und Server zugreifen. Eine sehr komfortable Möglichkeit bietet sich durch die Nutzung einer speziellen Datenkarte mit Datenübertragung nach dem UMTS- oder GPRS-Standard, wie sie von fast allen Mobilfunkgesellschaften angeboten werden.

DE

4.13.1 Alternative Wege für die UMTS- oder GPRS-Verbindung

Für die Nutzung einer solchen Datenkarte als Verbindungsmedium für den LANCOM Advanced VPN Client ergeben sich zwei verschiedene Konfigurationsmöglichkeiten:

- Die Datenkarte wird über die mitgelieferte Software des Mobilfunkbetreibers verwendet. Mit Hilfe dieser Software wird zunächst eine Verbindung zum Internet aufgebaut. Das Profil im LANCOM Advanced VPN Client nutzt diese Internetverbindung dann als „LAN-Verbindung".

  Das Profil wird auch dementsprechend mit dem Verbindungsmedium 'LAN (over IP)' und den benötigten VPN-Parametern eingerichtet, es sind keine weiteren Angaben zum Verbindungsaufbau notwendig.

  Die Vorteile dieser Variante:

  - Einfache Konfiguration des Profils im LANCOM Advanced VPN Client
  - Umfangreiche Statusinformationen des Software des Mobilfunkbetriebers stehen zur Verfügung (ausgewähltes Netz, Signalstärke, Übertragungsvolumen, Statistiken etc.)

  Nachteilig wirkt sich in diesem Szenario degegen der manuelle Verbindungsauf- und abbau aus.

- Die Datenkarte kann alternativ auch direkt über den LANCOM Advanced VPN Client angesteuert werden. Dabei werden neben den VPN-Angaben alle notwendigen Parameter für den Verbindungsaufbau über die Datenkarte in das Verbindungsprofil eingetragen.

  Der besondere Vorteil dieser Variante: Nach dem Einrichten des Profils im LANCOM Advanced VPN Client können Sie die UMTS- oder GPRS-Verbindung automatisch mit dem Starten der VPN-Verbindung aufbauen. Allerdings bleibt dabei der aktuelle Netzwerkzustand der Datenkarte unsichtbar.

Bei der direkten Ansteuerung der Datenkarte wird der Modemtreiber für das jeweilige Modell benötigt. Dieser Treiber wird bei der Installation der Betriebssoftware des Mobilfunkbetreibers eingerichtet.

4.13.2 Verbindung über Betriebssoftware des Mobilfunkanbieters einrichten

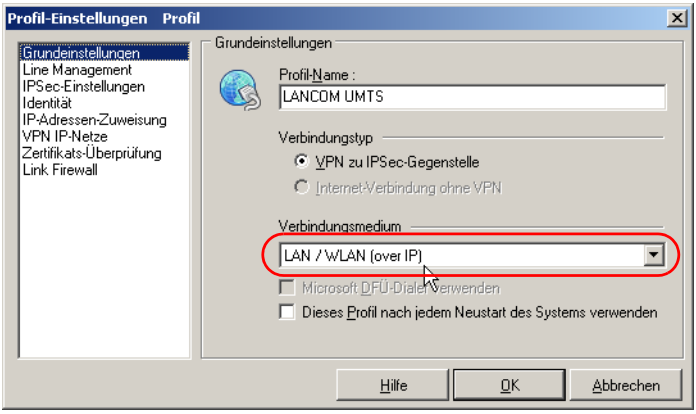
So richten Sie ein neues Profil für eine UMTS- oder GPRS-Verbindung über die Betriebssoftware des Mobilfunkanbieters ein:

DE

① Installieren Sie die Datenkarte nach der Anleitung des Mobilfunkanbieters auf Ihrem Rechner und testen Sie den korrekten Verbindungsaufbau.

② Erstellen Sie im LANCOM Advanced VPN Client ein neues Profil mit allen benötigten Parametern für den Aufbau der gewünschten VPN-Verbindung.

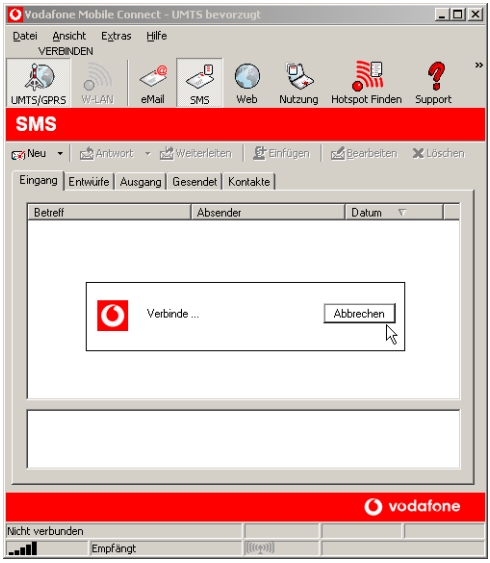
③ Wählen Sie dabei als Verbindungsmedium die Option 'LAN / WLAN (over IP)' aus. Eine bestehende Verbindung auf einer UMTS- oder GPRS-Datenkarte stellt sich für den LANCOM Advanced VPN Client wie eine LAN-Verbindung dar, die für den Aufbau eines VPN-Tunnels genutzt werden kann.



④ Testen Sie die Funktionsfähigkeit des Profils und den korrekten Aufbau des VPN-Tunnels nach Möglichkeit über eine „echte" LAN- bzw. WAN-Verbindung (z.B. Ethernetverbindung ins Internet o.ä.).

DE

⑤ Trennen Sie dann alle Verbindungen ins Internet (über Ethernet, ISDN o.ä.) und starten Sie erneut die UMTS- oder GPRS-Verbindung über die Betriebssoftware des Mobilfunkanbieters (Beispiel im Bild: Vodafone).



⑥ Sobald die Verbindung ins Internet über die UMTS- oder GPRS-Datenkarte hergestellt ist, starten Sie die Verbindung über den LANCOM Advanced VPN Client.

4.13.3 Direkte Verbindung über LANCOM Advanced VPN Client einrichten

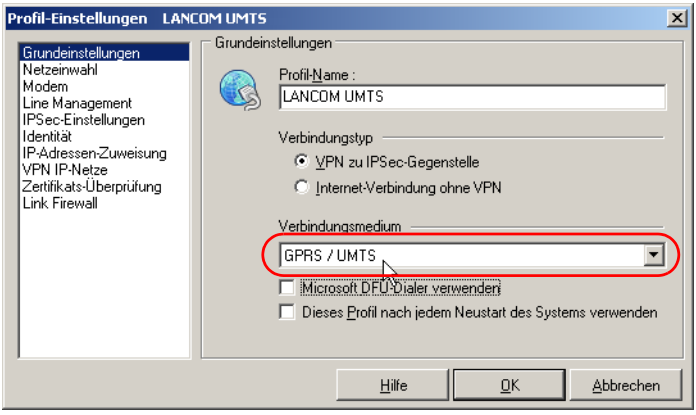
So richten Sie ein neues Profil für die direkte Ansteuerung einer UMTS- oder GPRS-Datenkarte ein:

① Installieren Sie die Datenkarte nach der Anleitung des Mobilfunkanbieters auf Ihrem Rechner und testen Sie den korrekten Verbindungsaufbau.

② Erstellen Sie im LANCOM Advanced VPN Client ein neues Profil mit allen benötigten Parametern für den Aufbau der gewünschten VPN-Verbindung.

Belassen Sie die UMTS- oder GPRS-Datenkarte während der weiteren Einrichtung des Verbindungs-Profils im PCMCIA- oder PC-Card-Schacht, damit das installierte Modem bei der Konfiguration ausgewählt werden kann.

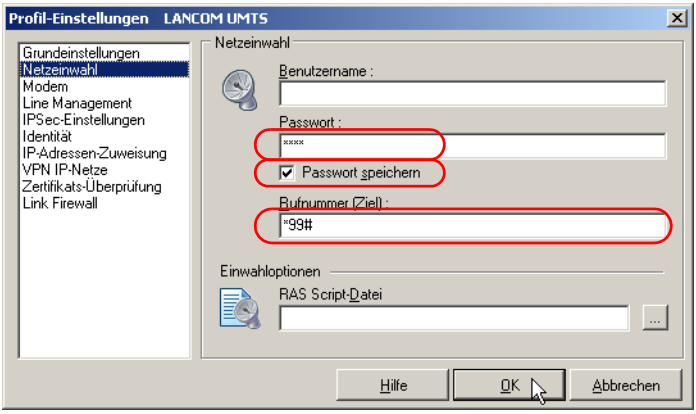
③ Wählen Sie als Verbindungsmedium die Option 'GPRS / UMTS' aus. Die UMTS- oder GPRS-Datenkarte stellt sich für den LANCOM Advanced VPN Client wie ein Modem dar, das für den direkten Aufbau eines VPN-Tunnels über die Modemverbindung genutzt werden kann.



④ Tragen Sie im Bereich 'Netzeinwahl' die Informationen ein, die für die Einwahl in den Server beim Mobilfunkbetrieber benötigt werden (siehe 'Einwahlinformationen für verschiedenen Mobilfunkbetreiber' →Seite 132).

Dabei müssen Sie auf jeden Fall die Rufnummer eintragen. Das Passwort (die PIN der SIM-Karte in der UMTS- oder GPRS-Datenkarte) kann optio-

nal als 'Passwort' eingetragen werden. Wenn dieses Passwort im Profil gespeichert wird, wird es beim Verbindungsaufbau nicht mehr abgefragt.

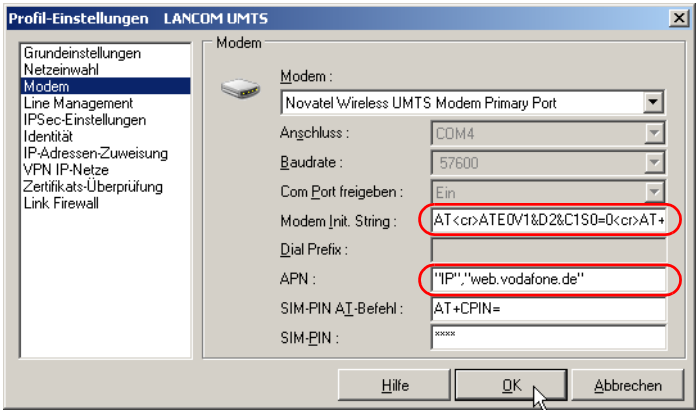


⑤ Wählen Sie im Bereich 'Modem' den Modemtreiber aus, der mit Ihrer UMTS- oder GPRS-Datenkarte installiert wurde. Tragen Sie dazu den benötigten Modem-Init-String ein. In der Regel besteht dieser Init-String aus folgenden Teilen:

- `AT+F<cr>` (setzt die Firmware des Modems auf Defaultwerte)
- `AT+CGDCONT=1, "IP",` (Beginn der APN-Eingabe des Mobilfunkbetriebers)
- `web.vodafone.de` (APN des Mobilfunkbetriebers)

Für den Init-String können je nach Modell der Datenkarte weitere Informationen erforderlich sein. Erkundigen Sie sich ggf. in der Dokumentation zu Ihrer Datenkarte oder bei Ihrem Mobilfunkbetrieber nach dem erforderlichen Init-String.

APN und SIM können in den weiteren Feldern eingetragen werden,



Weitere APNs von verschiedenen Mobilfunkanbietern finden Sie unter 'Einwahlinformationen für verschiedenen Mobilfunkbetreiber' →Seite 132.

⑥ Wenn das Profil so vollständig mit VPN-Parametern und UMTS- bzw. GPRS-Informationen eingerichtet ist, genügt ein Klick auf die Schaltfläche **Verbinden** im LANCOM Advanced VPN Client. Der Client baut dann zunächst die Verbindung über die UMTS- oder GPRS-Datenkarte auf und danach automatisch den VPN-Tunnel zum ausgewählten VPN-Gateway.

DE

4.13.4 Einwahlinformationen für verschiedenen Mobilfunkbetreiber

Mobilfunk-betrieber	T-Mobile	Vodafone	E-Plus	O2 Genion
Rufnummer	*99#	*99#	*99#	*99#
Benutzername	(beliebig)	(beliebig)	eplus	(beliebig)
Kennwort	(beliebig)	(beliebig)	(beliebig)	(beliebig)
DNS-Server	193.254.160.1	139.7.30.125	212.23.97.2	195.182.96.28
Alternativer DNS-Server	0.0.0.0	139.7.30.126	212.23.97.3	195.182.96.61
Modembefehl (Init-String)	+cgdcont=1, "IP", "internet.t-d1.de"	+cgdcont=1, "IP", "web.vodafone.de"	+cgdcont=1, "IP", "internet.eplus.de"	+cgdcont=1, "IP", "internet" ("internet.interkom.de" für Prepaid O2 Loop)

DE

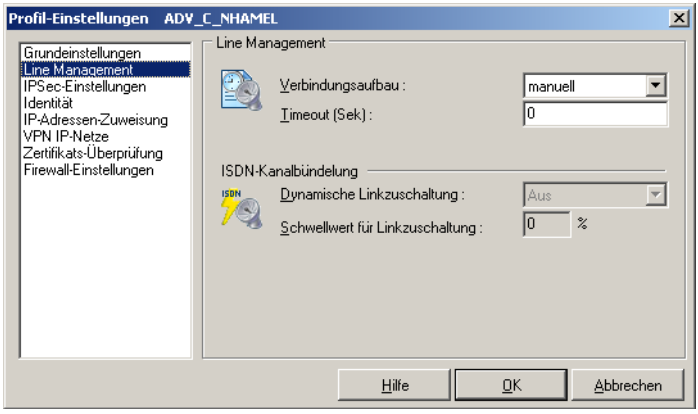
5 Eine Verbindung herstellen

5.1 Verbindungsaufbau zum Zielsystem

Die Client Software gestattet die Definition verschiedenster Zielsysteme, die je nach Anforderung benannt und konfiguriert werden können.

Um ein Zielsystem zu definieren, klicken Sie in der Menüleiste auf **Konfiguration > Profil-Einstellungen**. Das Fenster der Profileinstellungen öffnet sich nun und zeigt die bereits definierten Ziele.

Sobald die Software installiert und die Zielparameter korrekt konfiguriert wurden, kann die Anwahl an das Zielsystem stattfinden. Dabei ist auch die Art der Anwahl Bestandteil der Konfiguration eines Zielsystems. Sie können aus drei Anwahl-Modi für den Verbindungsaufbeu wählen: automatisch, manuell und wechselnd. Sie definieren den Modus des Verbindungsaufbaus für ein Zielsystem unter **Konfiguration > Profil-Einstellungen > Konfigurieren > Line-Management**.



5.1.1 Automatischer Verbindungsaufbau

Im Unterschied zu Microsoft RAS, bei dem jedes Ziel manuell angewählt werden muss, arbeitet die Client Software nach dem Prinzip der LAN-Emulation. Dabei ist es lediglich erforderlich, die entsprechende Applikations-Software zu starten (Email, Internet Browser, Terminal Emulation, etc.). Die Verbindung wird dann, entsprechend den Parametern des Zielsystems, automatisch aufgebaut und gehalten.

5.1.2 Manueller Verbindungsaufbau

Daneben ist es auch möglich manuell die Verbindung zu einem ausgewählten Ziel herzustellen, indem Sie im Monitor **Verbindung** anklicken und **Verbinden** wählen.

5.1.3 Wechselnder Verbindungsaufbau

Wird dieser Modus gewählt, muss zunächst die Verbindung "manuell" aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau wie folgt:

- Wird die Verbindung mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung "automatisch" hergestellt,
- wird die Verbindung "manuell" abgebaut, muss sie auch wieder "manuell" aufgebaut werden.

5.2 Verbinden

Gleich wie die Verbindung aufgebaut wird, der Monitor, sofern er im Vordergrund sichtbar ist, zeigt immer den Status des Verbindungsaufbaus wie in folgendem Beispiel an:

Danach wird die Verbindung hergestellt – hier manuell über das Menü, das nach dem rechten Mausklick erscheint.

Wurde die Verwendung eines (Soft-)Zertifikats konfiguriert – wie bei der Testverbindung mit SSL – so muss zunächst die PIN eingegeben werden.

5.2.1 Einwahl beim Internetprovider

Findet eine Einwahl zu einem Network Access Server bzw. Internet-Dienste-Anbieter (ISP) ins Internet statt, so wird die Einwahlverbindung mit einer dünnen gelben Linie symbolisiert. Die Einwahl ist abgeschlossen und die Verbindung zum ISP erfolgreich hergestellt, wenn die dünne Verbindungslinie die Farbe Grün annimmt. Gleichzeitig mit dem Start des Verbindungsaufbaus ändern sich auch die Farben der Symbole für die NAS-Einwahl.

Die Einwahl am ISP ist mit einem Globus dargestellt, die Authentisierung am ISP mit einem Händeschütteln. Ihre Farben wechseln während des Verbindungsaufbaus von grau zu blau, blinken dann grün, um schließlich bei erfolgreichem Verbindungsaufbau grün stehen zu bleiben.

Die Parameter für die NAS-Einwahl befinden sich in den Profil-Einstellungen unter "Netzeinwahl". Soll das Profil für die "automatische Medienerkennung" (siehe Profil-Einstellungen / Grundeinstellungen) verwendet werden, so muss unter "Netzeinwahl" unbedingt ein Benutzername und ein Passwort eingegeben sein.

Beachten Sie, dass grüne Ampellampen eine stehende Verbindung und ggf. anfallende Gebühren signalisieren!

5.2.2 Symbole der VPN-Einwahl

Nach abgeschlossener NAS-Einwahl kann die VPN-Einwahl zum Firmen-Gateway stattfinden. Dabei wird die Einwahlverbindung mit einer dicken gelben Linie symbolisiert. Die Einwahl ist abgeschlossen und die Verbindung zum

VPN Gateway erfolgreich hergestellt, wenn die dicke Verbindungslinie die Farbe Grün annimmt.

Gleichzeitig mit dem Start des Verbindungsaufbaus zum Gateway ändern sich auch die Farben der Symbole für die VPN-Einwahl. Die Einwahl und die Authentisierung am VPN Gateway ist genauso wie bei der NAS-Einwahl dargestellt. Hinzu kommen noch die Symbole für die Schlüsselverhandlung (Schlüssel) und die Kompression (Zange), sofern deren Konfiguration von Seiten des Gateways vorgeschrieben ist.

Die Farben der Symbole der VPN-Einwahl wechseln von grau zu blau, blinken dann grün, um schließlich bei erfolgreichem Verbindungsaufbau grün stehen zu bleiben. Dabei muss der Vorgang der Einwahl und Authentisierung am VPN Gateway immer durchlaufen werden, Verschlüsselung und Kompression sind optional. Die Symbole der VPN-Einwahl sind von links nach rechts:

- Einwahl am VPN Gateway:

  Die Zieladresse des VPN-Gateways wird in den Profil-Einstellungen unter "IPSec-Einstellungen / Gateway" angegeben.

- Authentisierung am VPN Gateway:

  Die nötigen Parameter befinden sich in den Profil-Einstellungen unter "Identität". Verwendet wird immer "Extended Authentication (XAUTH)". Benutzername und Passwort werden entweder aus der Konfiguration unter diesem Parameter oder aus einem Zertifikat ausgelesen. Ein zu verwendendes Zertifikat wird im Monitor-Menü unter "Konfiguration / Zertifikate" konfiguriert, wobei das Aussteller-Zertifikat des anzuwählenden Gateways mit dem Benutzer-Zertifikat zusammenpassen muss.

- Verschlüsselung:

  Zur Verschlüsselung dient entweder ein Pre-shared Key oder der Private Key aus einem Zertifikat. Beide Alternativen werden in den Profil-Einstellungen unter "Identität" eingestellt. Wird der "Pre-shared Key" verwendet, muss das "Shared Secret" hier eingetragen werden. Wird der "Pre-shared Key" nicht verwendet, wird automatisch das Zertifikat benutzt. Welche Verschlüsselung benutzt werden muss gibt das Gateway vor.

- Kompression:

  Kompression wird nur genutzt, wenn sie auch vom Gateway unterstützt wird. Eingestellt wird sie in den Profil-Einstellungen unter "Erweiterte IPSec-Optionen / IP-Kompression verwenden".

Beachten Sie, dass grüne Ampellampen eine stehende Verbindung und ggf. anfallende Gebühren signalisieren!

5.3 Client Logon

Nur für Windows-Version verfügbar.

Erfolgt das Client Logon am Network Access Server vor dem Windows Logon an der remote Domäne, indem die Logon Optionen genutzt werden (siehe → Monitor, Logon Optionen), so erfolgt der Verbindungsaufbau prinzipiell genau so, wie oben unter "Verbinden" beschrieben.

Nach der Auswahl des Zielsystems wird mit Klick auf den OK-Button der Verbindugsaufbau eingeleitet.

Lokal anmelden:

Ein Klick auf diesen Button bricht den Dialog zum Verbindungsaufbau ab.

Wurde die Verwendung eines (Soft-)Zertifikats konfiguriert – wie bei der Testverbindung mit SSL – so muss zunächst die PIN eingegeben werden.

Die weiteren Stationen des Verbindungsaufbaus erfolgen genau so, wie oben unter "Verbinden" beschrieben, bis die Verbindung steht.

5.4 Passwörter und Benutzernamen

Das Passwort (siehe →Netzeinwahl, Passwort) benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 256 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom

Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Auch wenn Sie für den Verbindungsaufbau "automatisch" gewählt haben (siehe oben →Verbindungsaufbau zum Zielsystem), müssen Sie die Verbindung beim ersten Mal manuell aufbauen und das Passwort eingeben. Für jeden weiteren automatischen Verbindungsaufbau wird das Passwort selbständig übernommen, bis der PC erneut gebootet oder das Zielsystem gewechselt wird. D.h. für eine Reihe von "automatischen" Verbindungsaufbaus wird das Passwort nach der ersten Eingabe und dem ersten Verbindungsaufbau selbständig übernommen, auch wenn die Funktion "Passwort speichern" (siehe →Netzeinwahl) nicht aktiviert wurde. Erst ein Boot-Vorgang löscht das einmal eingegebene Passwort. (Beachten Sie zu Windows auch → Logon Optionen).

Soll das Passwort mit dem Booten nicht gelöscht werden, so muss die Funktion "Passwort speichern" aktiviert werden (siehe →Netzeinwahl). Bitte beachten Sie dabei, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

5.4.1 Benutzername für NAS-Einwahl

Der "Benutzername" für die Netzeinwahl muss immer in der Konfiguration für das Ziel eingegeben werden. Ohne diesen Benutzernamen kann keine Einwahl an den NAS erfolgen. (Siehe →Netzeinwahl)

5.4.2 Benutzername und Passwort für VPN-Einwahl

Benutzernamen und Passwörter für die Einwahl zum VPN Gateway (siehe → Tunnel-Parameter) können in der Konfiguration des Zielsystems vollständig eingegeben werden. Sie bleiben über einen Boot-Vorgang hinaus für die VPN-Einwahl erhalten. Werden sie nicht eingegeben, so werden sie bei der VPN-Einwahl in einem Dialog abgefragt.

Oben: Dialog zur Abfrage des nicht in die Konfiguration eingegebenen "Benutzer (VPN)" beim Monitor (links) und Windows 2000/ XP beim Client Logon (rechts).

5.5 Verbindungsabbruch und Fehler

Ereignet sich ein Fehler, so wird die Verbindung nicht hergestellt und die Fehlerursache im Monitor angezeigt (beachten Sie dazu den Abschnitt "Fehler- und ISDN-Meldungen").

5.6 Trennen

Mit der Funktion "Trennen" wird der Abbau der aktuell bestehenden Verbindung manuell durchgeführt. Wenn Sie die Möglichkeit behalten wollen, jederzeit die Verbindung manuell abbauen zu können, setzen Sie den Verbindungsaufbau auf "manuell" und deaktivieren den automatischen Timeout, indem Sie ihn auf Null (0) setzen (→Verbindungsaufbau).

Wenn die Verbindung abgebaut wird, wechselt die farbliche Darstellung der Verbindungslinie bis sie verschwindet und die Ampellampen des Monitors für die gesamte Offline-Dauer von grün zu rot.

5.7 Trennen und Beenden des Monitors

Besteht eine Verbindung noch, und wird der Monitor beendet, so wird nicht automatisch die Verbindung getrennt. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung von der Software verlangt (siehe Bild unten).

Klicken Sie in diesem Bestätigungsfenster auf "Nein", so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um eine bestehende Verbindung korrekt zu beenden!