

## Universelle, zentral manglebare IPSec Client-Software für Linux

- ▶ **Hochsicherer Zugriff auf das zentrale Datennetz**
- ▶ **Integrierte, dynamische Personal Firewall**
- ▶ **Weltweite Einwahl in das Firmennetz**
- ▶ **Kompatibilität zu VPN Gateways unterschiedlicher Hersteller**
- ▶ **Starke Authentisierung mit Zertifikaten**
- ▶ **Endpoint Security und zentrales Management**



### Universalität

Der NCP Secure Enterprise Linux Client ist eine Komponente der ganzheitlichen NCP Secure Enterprise Solution. Die Kommunikationssoftware dient dem universellen Teleworking in beliebigen Remote Access VPN-Umgebungen. Auf Basis des IPSec-Standards können hochsichere Datenverbindungen sowohl zu NCP Secure Enterprise Servern als auch VPN-Gateways aller namhaften Anbieter hergestellt werden. Der Datentransfer erfolgt unabhängig vom Mediatyp über Festnetze, öffentliche Funknetze, LANs (z.B. im Filialnetz), das Internet sowie Nahbereichs-Funknetze wie Wireless LANs am Firmengelände und an Hotspots. Mittels beliebiger Endgeräte unter Linux (beispielsweise Desktops, Laptops, Notebooks, Pocket PC, Handheld, Handy) können Teleworker von jedem Standort auf zentrale Datenbestände und Anwendungen zugreifen.

### Sicherheit

Universelle Einsatzmöglichkeiten fordern umfangreiche Sicherheitsmechanismen zur Abwehr von Angriffen in jeder Remote Access-Umgebung. Auch an Hotspots während des An- und Abmeldevorganges. Die wichtigsten, integrierten Security-Bausteine sind neben dem VPN-Tunneling: Datenverschlüsselung, eine dynamische Personal Firewall, die Unterstützung von OTP-Token (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure). Mittels der Personal Firewall können Regelwerke für: Ports, IP-Adressen und Segmente sowie Applikationen definiert werden. Ein weiteres Sicherheitskriterium ist „Friendly Net Detection“, d.h. die automatische Erkennung von sicheren und unsi-

chernen Netzen. In Abhängigkeit davon werden die entsprechenden Firewall-Regeln aktiviert bzw. deaktiviert.

Alle Konfigurationen können zentral vom Administrator eingegeben und durch den Anwender nicht veränderbar eingestellt werden. Mechanismen des zentralen Managements (s.u.) ermöglichen eine automatische Übernahme aller Konfigurationsparameter in den Client. Der NCP-Dialer bietet zudem Schutz vor kostenintensiven Fremddialern.

### Komfort

„Easy-to-use“ – d.h. einfache Installation und Bedienung der Client Software. Eine grafische, intuitive Benutzeroberfläche informiert über alle Verbindungsstati. Der Teleworker arbeitet wie am Büroarbeitsplatz. Entsprechend komfortabel gestaltet sich auch die Domänenanmeldung. Automatische Updates\* sorgen für aktuelle Software- und Konfigurationsstände.

### Zentrales Management\*

Die NCP Secure Enterprise Management Software bietet alle Funktionalitäten und Automatismen für Inbetriebnahme und Betrieb von Remote Access-VPNs. Im Rahmen der Endpoint Security werden alle sicherheitsrelevanten Parameter vor einem Zugriff auf das Firmennetz überprüft. Die Sicherheitsrichtlinien sind zwingend und vom Anwender nicht umgeh- bzw. manipulierbar.

\*) optional

## Technische Daten

<b>Betriebssysteme</b>	Ab Linux Kernelversion 2.4.10 (u.a. SuSE 9.3 Kernelversion 2.611.4-20a, SuSE 10.0 Kernelversion 2.6.13-15, Fedora Core3 Kernelversion 2.6.9-1.667)
<b>Security Features</b>	Der Enterprise Client unterstützt alle IPSec Standards nach RFC
<b>Personal Firewall Firewall Configuration*</b>	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (FND), Auswertung von: aktueller Netzwerkadresse, IP-Adresse und MAC-Adresse des DHCP-Servers; automatische FND, Secure Hotspot Logon; differenzierte Filterregeln bezüglich: Protokolle, Ports und Adressen, Schutz des LAN-Adapters, zentrale Administration mit Client Firewall Configuration Plug In*
<b>Virtual Private Networking</b>	IPSec (Layer 3 Tunneling), RFC-konform; IPSec-Proposals können determiniert werden durch das IPSec -Gateway (IKE, IPSec Phase 2); Event log; Kommunikation im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPSec Modes: Tunnel Mode, Transport Mode
<b>Verschlüsselung (Encryption)</b>	Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits; Diffie-Hellman Groups 1,2,5 Seamless Rekeying (PFS); Hash Algorithmen: SHA1, MD5
<b>Authentisierungsverfahren</b>	IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens; Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready.
<b>Starke Authentisierung – Standards PKI Enrollment*</b>	X.509 v.3 Standard; Entrust Ready PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2 and 2.0; Smart Card ReaderInterfaces: PC/SC, CT-API; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-key Certificate Revocation List, <i>vorm. CRL</i> ), CARL (Certification Authority Revocation List, <i>vorm. ARL</i> ), OCSP. CMP* (Certificate Management Protocol),
<b>Endpoint Security</b>	Endpoint Policy Enforcement*
<b>Networking Features</b>	LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface
<b>Netzwerkprotokolle</b>	IP
<b>Dialer</b>	NCP Secure Dialer
<b>IP Address Allocation</b>	DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
<b>Übertragungsmedien</b>	Festnetze: analoges Fernsprechnetz, ISDN, xDSL, LAN Funknetze: WLAN, GSM, GPRS, UMTS (abhängig von eingesetzter Hardware), Internet
<b>Line Management</b>	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; WLAN-Roaming (Handover); Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert; Timeout (zeit- und gebührengesteuert); Budget Manager
<b>Datenkompression</b>	IPCOMP (lzs), Deflate
<b>Point-to-Point Protokolle</b>	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
<b>Internet Society RFCs und Drafts</b>	RFC 2401 –2409 (IPSec), RFC 3498, RFC 3947: IP Security Architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
<b>Client Monitor Grafische Benutzeroberfläche</b>	Mehrsprachig (Deutsch, Englisch, Französisch); intuitive Bedienung; Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files, Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus; Integrierte Unterstützung von Mobile Connect Cards (PCMCIA); Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre

Voraussetzungen:\*) NCP Secure Enterprise Management und NCP Secure Enterprise Server