

Universelle, zentral managebare IPSec Client-Software für Windows 32/64 Betriebssysteme

- ▶ **Hochsicherer Zugriff auf das zentrale Datennetz**
- ▶ **Integrierte, dynamische Personal Firewall**
- ▶ **Kompatibilität zu IPSec VPN Gateways unterschiedlicher Hersteller**
- ▶ **Starke Authentisierung mit Zertifikaten**
- ▶ **Endpoint Security und zentrales Management***
- ▶ **Intuitive grafische Benutzeroberfläche**
- ▶ **Frei gestaltbares Textfeld im Client-Monitor**



Universalität

Der NCP Secure Enterprise Client ist eine Komponente der ganzheitlichen NCP Secure Enterprise Solution. Die Kommunikationssoftware dient dem universellen Telearbeit in beliebigen Remote Access VPN-Umgebungen. Auf Basis des IPSec-Standards können hochsichere Datenverbindungen sowohl zu NCP Secure Enterprise Servern als auch zu VPN-Gateways aller namhaften Anbieter hergestellt werden. Der Datentransfer erfolgt unabhängig vom Mediatyp (any network) 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 (any device) können Telearbeiter von jedem Standort (any location) auf zentrale Datenbestände und Anwendungen (any application) 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 Password) und Zertifikaten in einer PKI (Public Key Infrastructure). Alle Sicherheitsparameter können optional vor dem Verbindungsaufbau zum Produktivnetz überprüft werden (Endpoint Policy Enforcement)*. Mittels der Personal Firewall sind Regelwerke für: Ports, IP-Adressen und Segmente sowie Applikationen definierbar. Ein weiteres Sicherheitskriterium ist „Friend-

ly Net Detection“, d.h. die automatische Erkennung von sicheren und unsicheren 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. Die integrierte Unterstützung von Mobile Connect Cards für UMTS, GPRS, WLAN macht die zusätzliche Installation der mitgelieferten Benutzeroberfläche des Kartenlieferanten überflüssig. Der Telearbeiter 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 die Inbetriebnahme und den wirtschaftlichen Betrieb von Remote Access-VPNs. Ein wesentliches Plug In ist das Endpoint Policy Enforcement zur Umsetzung der Endpoint Security. Alle Sicherheitsrichtlinien sind zwingend und vom Anwender nicht umgeh- bzw. manipulierbar.

*) optional

Technische Daten

Betriebssysteme	Windows (32 Bit): Windows Vista (x86), Windows 2000, Windows XP Windows (64 Bit): Windows Vista (x64) , Windows XP 64
Security Features	Der Enterprise Client unterstützt alle IPSec Standards nach RFC
Personal Firewall Firewall Configuration*	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (Auswertung von: aktueller Netzwerkadresse, IP-Adresse und MAC-Adresse des DHCP-Servers); Secure Hotspot Logon; differenzierte Filterregeln bezüglich: Protokolle, Ports und Adressen, Schutz des LAN-Adapters, zentrale Administration mit Client Firewall Configuration Plug In*
Virtual Private Networking	IPSec (Layer 3 Tunneling), RFC-konform; IPSec-Proposals können determiniert werden durch das IPSec -Gateway (IKE, IPSec Phase 2); Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPSec Modes: Tunnel Mode, Transport Mode
Verschlüsselung (Encryption)	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
Authentisierungsverfahren	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.
Starke Authentisierung – Standards PKI Enrollment*	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),
Endpoint Security	Endpoiint Policy Enforcement*
Networking Features	LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface
Netzwerkprotokolle	IP
Dialer	NCP Secure Dialer, Microsoft RAS Dialer (für ISP-Einwahl mittels Einwahl-Script) NCP Connection Manager für internationale Einwahl via GoRemote (<i>vorm. GRIC</i>), UuNet, Infonet, MCI
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
Übertragungsmedien	Festnetze: analoges Fernsprechnet, ISDN, xDSL, LAN Funknetze: WLAN, GSM (inkl. HSCSD), GPRS, UMTS, HSDPA, Internet
Line Management	DPD mit konfigurierbarem Zeitintervall ; Short Hold Mode; WLAN-Roaming (Handover); Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert; Timeout (zeit- und gebührengesteuert); Budget Manager
Datenkompression	IPCOMP (Izs), Deflate
Point-to-Point Protokolle	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs und Drafts	RFC 2401 –2409 (IPSec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
Client Monitor Grafische Benutzeroberfläche	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

Voraussetzung: *) NCP Secure Enterprise Management