

Universelle IPSec Client-Software für Windows 32/64-Betriebssysteme

- ▶ **Hochsicherer Zugriff auf das zentrale Datennetz**
- ▶ **Integrierte, dynamische Personal Firewall**
- ▶ **Kompatibilität zu VPN Gateways unterschiedlicher Hersteller**
- ▶ **Unterstützung aller IPSec-Protokollerweiterungen**
- ▶ **Starke Authentisierung mit Zertifikaten – Software und Hardware**
- ▶ **Integrierte Unterstützung von Mobile Connect Cards**
- ▶ **Frei gestaltbares Textfeld im Client-Monitor**



Universalität

Der NCP Secure Entry Client für Windows 32/64 Betriebssysteme ist eine Kommunikationssoftware für den universellen Einsatz in beliebigen Remote Access VPN-Umgebungen. Auf Basis des IPSec-Standards können hochsichere Datenverbindungen 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 Teleworker von jedem Standort (any location) auf zentrale Datenbestände und Anwendungen (any application) zugreifen. Sprachdaten (VoIP) werden priorisiert übertragen. Integrierte QoS (Quality of Service) sorgen für eine verzögerungs- und verzerrungsfreie Kommunikation.

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 Sicherheitskri-

terium ist „Friendly 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 erfolgen – für den Anwender nicht veränderbar - grundsätzlich durch den Administrator.

Komfort

„Easy-to-use“ – d.h. einfache Installation und Bedienung des NCP Secure Entry Clients. Eine grafische, intuitive Benutzeroberfläche informiert über alle Verbindungsstati. Detaillierte Log-Informationen sind ebenfalls über diese Oberfläche einsehbar. Der integrierte Konfigurations-Assistent ermöglicht das einfache Anlegen von Telefonbucheinträgen. Die integrierte Unterstützung von Mobile Connect Cards für UMTS, GPRS, WLAN macht die zusätzliche Installation der mitgelieferten Benutzeroberfläche des Kartenlieferanten überflüssig. Der Teleworker arbeitet an beliebigen Standorten (mobil oder stationär) transparent und sicher wie am Büroarbeitsplatz. Entsprechend komfortabel gestaltet sich auch die Domänenanmeldung in der gewohnten Weise wie im lokalen Netz. Vor dem Login am Domänencontroller wird ein VPN-Tunnel vom Client zum zentralen VPN-Gateway etabliert. Somit werden bereits alle Anmeldedaten verschlüsselt und sicher übertragen.

Technische Daten

| | |
|--|---|
| Betriebssysteme | Windows (32 Bit): Windows Vista (x86), Windows 2000, Windows XP (inkl. SP2) Windows (64 Bit): Windows Vista (x64) , Windows XP 64 |
| Security Features | Der Entry Client unterstützt alle IPSec Standards nach RFC und erfüllt auch die höchsten Sicherheitsanforderungen. |
| Personal Firewall | 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 |
| 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; ORSA SecurID Ready. |
| Starke Authentisierung - Standards | 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. |
| Networking Features | LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface |
| 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 Fernsprechnetz, 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 |
| Weitere Features | Priorisierung von VoIP (QoS), UDP-Encapsulation |
| 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, Polnisch); 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 |

Weitere Informationen zu NCP Secure Communications-Produkte finden Sie im Internet unter: www.ncp.de
Eine 30-Tage Vollversion des Secure Entry Clients (Win32/64) können Sie hier kostenlos testen:
http://www.ncp.de/deutsch/services/testsoftware/index_entry.html