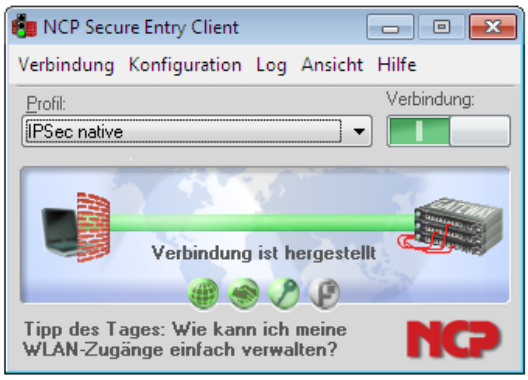
Datenblatt

NCP Secure Entry Client (Win32/64)

Next Generation Network Access Technology

Universelle VPN Client Suite für Windows 32/64 Bit Betriebssysteme - Windows 7, Windows Vista, Windows XP

- **Kompatibilität zu VPN Gateways (IPsec-Standard)**
- **Importfunktion für unterschiedliche Dateiformate**
- **Integrierte, IPv6-fähige, dynamische Personal Firewall**
- **Fallback IPsec / HTTPS (VPN Path Finder Technology)**
- **FIPS Inside**
- **Budget Manager zur Kostenüberwachung**
- **Integrierte Unterstützung von UMTS-/LTE-Hardware**
- **Integration aller für Remote Access erforderlichen Sicherheits- und Kommunikationstechnologien**
- **Kostenlose 30-Tage Vollversion**



Universalität und Kommunikation

Der NCP Secure Entry Client (32/64) ist eine Kommunikationssoftware für den universellen Einsatz in beliebigen Remote Access VPN-Umgebungen. Mobile und stationäre Teleworker arbeiten in der gewohnten Weise wie am Büroarbeitsplatz. Auf Basis des IPsec-Standards können hochsichere Datenverbindungen zu VPN Gateways aller namhaften Anbieter hergestellt werden. Der Verbindungsaufbau erfolgt unabhängig von Microsofts DFÜ-Dialer über beliebige Netze (Kabel- und Funknetze, LAN, WLAN, Internet). Mittels beliebiger Endgeräte mit Windows 32 oder 64 Bit-Betriebssystemen, können Teleworker von jedem Standort, weltweit auf das zentrale Datennetz zugreifen. WLAN-Roaming bzw. IPsec-Roaming sorgt für die Aufrechterhaltung der VPN-Verbindung auch dann, wenn der Access Point bzw. die IP-Adresse wechselt. Die NCP Path Finder Technology ermöglicht Remote Access auch hinter Firewalls, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert.

Sicherheit

Die Sicherheitsmechanismen des NCP Secure Entry Clients bieten einen umfassenden Schutz des Endgerätes und Firmennetzes vor jedweden Attacken unberechtigter Dritter. Das gilt auch an Hotspots, insbesondere während des An- und Abmeldevorganges am WLAN.
Wichtigste Security-Bausteine sind neben der Datenverschlüsselung: eine dynamische Personal Firewall, die Unterstützung von OTP-Tokens (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure). Das Kryptografiemodul, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051).

Mittels der Personal Firewall können Regelwerke für: Ports, IP-Adressen, Segmente und Applikationen definiert werden. Desweiteren wird der neue IPv6-Standard unterstützt.
Die „Friendly Net Detection", d.h. die automatische Erkennung von sicheren und unsicheren Netzen, aktiviert in Abhängigkeit davon die erforderlichen Firewall-Regeln. Die NCP Firewall ist im Gegensatz zu herkömmlichen Firewalls bereits beim Systemstart aktiv.
Alle Client-Einstellungen können durch den Administrator gegenüber Veränderungen durch den Anwender gesperrt werden.

Usability und Wirtschaftlichkeit

„Easy-to-use" für Anwender und Administrator – d.h. die einfache Bedienung und Installation des NCP Secure Entry Clients ist einzigartig am Markt. Die grafische, intuitive Benutzeroberfläche informiert über alle Verbindungs- und Sicherheitsstati vor und während einer Datenverbindung. Detaillierte Log-Informationen sorgen im Servicefall für rasche Hilfe durch den Helpdesk. Die Mediatype-Erkennung wählt automatisch das jeweils schnellste, vorhandene Netz aus. Ein Konfigurations-Assistent ermöglicht das einfache Anlegen von Profilen. Die integrierte Unterstützung von Mobile Connect Cards für WLAN (Wireless Local Area Network) sowie WWAN (Wireless Wide Area Network) gilt uneingeschränkt für alle unterstützten Windows Betriebssysteme. Unter Windows 7 sorgt die Unterstützung der Mobile Broadband Schnittstelle für die performante Nutzung von 4G-/LTE-Hardware. Eine Installation der Benutzeroberfläche des Kartenlieferanten ist nicht erforderlich. Auch die Domänenanmeldung gestaltet sich so einfach wie im lokalen Netz – natürlich hochsicher. Ein Textfeld im Monitor kann beliebig gestaltet werden, z.B. Firmenlogo, Supporthinweise.
Usability bedeutet auch Kosteneinsparungen durch Verringerung des Schulungsaufwands, weniger Dokumentation und Entlastung des Helpdesk. Für den wirtschaftlichen Betrieb sorgt u.a. der Budget Manager, durch Vorgabe und Überwachung eines vorgegebenen Volumen- oder Zeit-Budgets bzw. des Providers.

FIPS 140-2 Inside

Technische Daten

Betriebssysteme	Windows (32 Bit): Windows7, Windows Vista, Windows XP Windows (64 Bit): Windows7, Windows Vista, Windows XP
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (Automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand des IP-Adressbereiches oder eines NCP FND-Servers*); FND-abhängige Aktion starten; Secure Hotspot Logon; differenzierte Filterregeln bezüglich: Protokolle, Ports, Anwendungen und Adressen, Schutz des LAN-Adapters; IPv4 und IPv6 Unterstützung.
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; IPsec-Proposals können determiniert werden durch das IPsec -Gateway (IKEv1/IKEv2, IPsec Phase 2); Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Tunnel 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; Seamless Rekeying (PFS); Hash Algorithmen: SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-18.
FIPS Inside	Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051). Die FIPS Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: - Diffie Hellman-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit) - Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit - Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES
Authentisierungs-verfahren	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; Multi-Zertifikatskonfiguration;Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme; RSA 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, 2.0 und 3.0; Smart Card ReaderInterfaces: PC/SC, CT-API; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; CSP zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher; PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-Key Certificate Revocation List, *vorm. CRL*), CARL (Certification Authority Revocation List, *vorm. ARL*), OCSP.
Networking Features	LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface, integrierter, vollständiger WLAN- (Wireless Local Area Netzwork) und WWAN-Support (Wireless Wide Area Network, Mobile Broadband ab Windows 7)
Netzwerkprotokoll	IP
Dialer	NCP Secure Dialer, Microsoft RAS Dialer (für ISP-Einwahl mittels Einwahl-Script) NCP Connection Manager für internationale Einwahl via GoRemote (*vorm. GRIC*), UuNet, Infonet, MCI (auf Anfrage).
Seamless Roaming	Automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium (LAN/WLAN/3G/4G) ohne IP-Adresswechsel, so dass über den VPN-Tunnel kommunizierende Anwendungen nicht beeinflusst werden, bzw. die Anwendungs-Session nicht getrennt wird. Voraussetzung: NCP Secure Enterprise VPN Server
VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist (Voraussetzung: NCP VPN Path Finder Technology am Gateway erforderlich)
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	Internet, xDSL, LAN, WLAN, GSM (inkl. HSCSD), GPRS, UMTS, HSDPA, analoges Fernsprechnetz, ISDN,

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 (Verwaltung von Verbindungszeit und/oder –volumen für GPRS/UMTS und WLAN, bei GPRS/UMTS getrennte Verwaltung für Roaming im Ausland)
Datenkompression	IPCOMP (lzs), Deflate
Weitere Features	UDP-Encapsulation; WISPr-Support (T-Mobile Hotspots); IPsec-Roaming bzw., WLAN-Roaming (Voraussetzung: NCP Secure Enterprise Server); Importfunktion der Dateiformate:*.ini, *.pcf, *.wgx und *.spd.
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, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
Client Monitor Intuitive, grafische Benutzeroberfläche	Mehrsprachig (Deutsch, Englisch, Französisch); Client Info Center; Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files (farbige Darstellung, einfache Copy&Paste-Funktion); Test-Werkzeug für Internet-Verfügbarkeit; Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus; Integrierte Anzeige von Mobile Connect Cards (PCMCIA, embedded); individuell gestaltbare s Textfeld; Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre; Automatische Prüfung auf neue Version.

*) NCP FND- Server kann kostenlos als Add-On hier heruntergeladen werden:
http://www.ncp-e.com/de/downloads/download-software.html

Optional: Zentrales Management und Endpoint Security (Upgrade auf NCP Secure Enterprise Client)

Weitere Informationen zum NCP Secure Entry Client finden Sie hier:
http://www.ncp-e.com/de/produkte/ipsec-client.html

Eine kostenlose 30-Tage Vollversion können Sie hier herunterladen: http://www.ncp-e.com/de/downloads/download-software.html