SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

NCP SECURE COMMUNICATIONS

Datenblatt

NCP Secure Entry Client Windows

Universelle VPN Client Suite für Windows

- Kompatibilität zu VPN Gateways (IPsec-Standard)
- Importfunktion für unterschiedliche Dateiformate
- IPv6-fähige dynamische Personal Firewall
- Windows 10, & 8.x
- Custom Branding Option
- VPN Bypass
- FIPS Inside
- Starke Authentisierung (z.B. Zertifikat), Biometrie
- Quality of Service Unterstützung
- Multi-Zertifikatsunterstützung
- Unterstützung von elliptischen Kurven (ECC)
- Unterstützung von 3G/4GHardware (LTE)
- Seamless Roaming für unterbrechungsfreies Arbeiten trotz Wechsel des Übertragungsmediums
- Kostenlose 30-Tage Vollversion

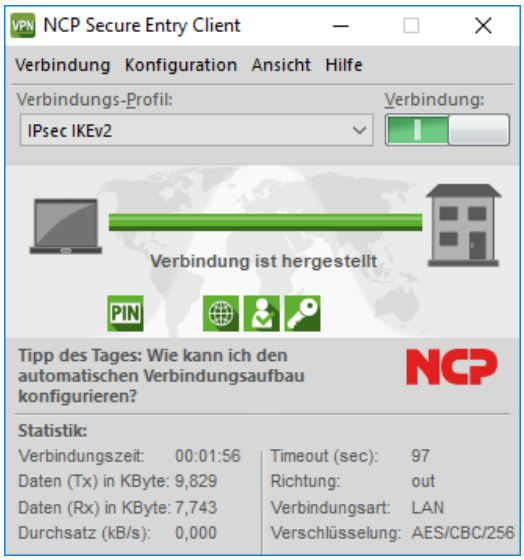
Universalität und Kommunikation

Der NCP Secure Entry Client ist ein Baustein der ganzheitlichen NCP Remote Access VPN-Lösung. Auf Basis des IPsec-Standards lassen sich hochsichere Datenverbindungen auch zu VPN Gateways anderer Anbieter herstellen. Der Verbindungsaufbau erfolgt unabhängig vom Microsofts DFÜ-Dialer über beliebige Netze. Mobile Mitarbeiter können mit Windows-Endgeräten von jedem Standort weltweit auf das zentrale Datennetz zugreifen.

„Seamless Roaming“ bietet beim Mobile Computing eine sichere „Always On-Verbindung“. Es wählt automatisch das schnellste Übertragungsmedium aus, wobei die Anwendungs-session während eines Medienwechsels oder einer kurzzeitigen Unterbrechung erhalten bleibt. Dieses Feature erfordert als Gegenstelle den NCP Secure VPN Enterprise Server.

Die von NCP entwickelte VPN Path Finder Technology ermöglicht Remote Access auch hinter Firewalls bzw. Proxys, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert.

Hierbei wird automatisch in einen modifizierten IPsec-Protokoll-Modus gewechselt, der den zur



Verfügung stehenden HTTPS-Port für den VPN-Tunnel nutzt. Dieses Feature erfordert als Gegenstelle den NCP Secure VPN Enterprise Server.

Um Mitarbeitern eine sichere Anmeldung an der Windows-Domäne VOR der Anmeldung am Windows-System zu ermöglichen, unterstützt der Client die Domänenanmeldung mittels Credential Service Provider. Hierfür baut der Client eine VPN-Verbindung in die Firmenzentrale auf. Die Benutzer-anmeldung am lokalen Windows System geschieht daraufhin durch diesen VPN-Tunnel, so dass er an der zentralen Windows Domäne / Active Directory authentifiziert wird. Des Weiteren unterstützt der Client bereits in der Pre-Logon-Phase die sichere Anmeldung an einem WLAN-HotSpot, d.h. der Client ist durch die integrierte dynamische Firewall zu jedem Zeitpunkt der Anmeldung am HotSpot optimal geschützt. Für den Anwender macht es also keinen Unterschied, ob er sich im Büro oder an einem HotSpot seiner Wahl befindet.

Sicherheit

Der NCP Secure Entry Client verfügt über zusätzliche Sicherheitsmechanismen wie eine integrierte dynamische Personal Firewall. Diese ist administrierbar, so dass Regelwerke für Ports, IP-Adressen, Segmente und Applikationen zentral vom Administrator definiert werden können. Das Feature „Friendly Net Detection“ erkennt anhand der im Client

vorgegebenen Sicherheitsregeln, ob sich der Anwender in einem sicheren oder unsicheren Netz befindet. Es aktiviert je nach Netz die entsprechenden Firewall-Regeln. Dies gilt auch im Umfeld von Hotspots, hier insbesondere während des An- und Abmeldevorgangs am WLAN. Die NCP Firewall ist im Gegensatz zu herkömmlichen Firewalls bereits beim Systemstart aktiv.

Weitere Security Features sind die Unterstützung von OTP-Lösungen (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure) und die Verifizierung der Signatur nach dem Prinzip der elliptischen Kurven (ECC).

Des Weiteren verfügt der VPN Client über eine biometrische Authentisierung vor der VPN-Einwahl, zum Beispiel über Fingerabdruck- oder Gesichtserkennung. Die Authentisierung erfolgt direkt nach dem Klick auf den Verbinden-Button in der Client GUI, wobei der Verbindungsaufbau erst gestartet wird, wenn diese erfolgreich abgeschlossen ist. Besitzt der Rechner keine Hardware zur biometrischen Authentisierung oder ist diese nicht aktiviert, kann sich der Benutzer auch wahlweise über sein Passwort authentisieren. Ein ebenso verfügbarer Endpoint Policy-Check verhindert den Zugriff ungenügend geschützter Endgeräte auf das zentrale Datennetz.

Mit der Home Zone-Funktion kommt ein für den Homeoffice-Bereich speziell eingerichtetes Nutzungsprofil zum Einsatz. Sobald der User auf den Button "Home Zone" klickt, schaltet der Rechner automatisch in diesen Modus um. Es greifen nun vom Administrator vordefinierte, spezielle Firewall-Regeln, die nur für den Homeoffice-Bereich gelten. Diese erlauben dem Anwender beispielsweise die Nutzung seines Druckers oder Scanners im Homeoffice-Netzwerk. Verlässt der Anwender den Home Zone-Bereich werden die anderen Firewall-Regeln wieder aktiviert.

Durch die Quality of Service-Funktion wird Bandbreite für konfigurierte Applikationen, wie beispielsweise VoIP, reserviert. Die Priorisierung ausgewählter Datenquellen am Anwenderrechner geschieht für den Datentransport im VPN-Tunnel in Senderichtung. Für den Anwender ergibt sich daraus eine ungestörte VoIP-Kommunikation durch den VPN-Tunnel auch bei hohem Datenaufkommen.

Mittels der neuen Bypass-Funktion im NCP VPN Client kann der IT-Administrator den Client so konfigurieren, dass trotz deaktiviertem Split-Tunneling bestimmte Anwendungen vom VPN ausgenommen und die Daten am Tunnel vorbei ins Internet geschickt werden. Das hat den Vorteil, dass Anwendungen wie beispielsweise Videostreaming die Server nicht länger mit Terabytes an Daten überhäufen.

Die „Multi-Zertifikatsunterstützung“ ermöglicht VPN-Verbindungen mit unterschiedlichen Firmen, die jeweils ein eigenes Benutzerzertifikat erfordern. Es lassen sich mehrere Zertifikats-einstellungen festlegen und diese pro Profil zuordnen. Das Kryptografiemodul, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747).

Usability und Wirtschaftlichkeit

Die einfache Bedienung des NCP Secure Entry Clients ist einzigartig am Markt. Der im Client integrierte Dialer baut automatisch die Verbindung ins Internet auf. Die Mediatyp-Erkennung wählt beim Aufbau der VPN-Verbindung das jeweils schnellste, vorhandene Übertragungsnetz aus. Die Seamless Roaming-Funktionalität ermöglicht während der VPN-Verbindung den automatischen Wechsel auf das optimale Verbindungsmedium, ohne die VPN-Verbindung zu beinträchtigen.

Die grafische, intuitive Benutzeroberfläche informiert den Anwender über alle Verbindungs- und Sicherheitsstati vor und während einer Datenverbindung. Detaillierte Log-Informationen sorgen im Servicefall für rasche Hilfe durch den Helpdesk. Ein Konfigurationsassistent ermöglicht das einfache Anlegen von Profilen. Der Client unterstützt WLAN (Wireless Local Area Network) und WWAN (Wireless Wide Area Network, UMTS, 3G, 4G). Die Konfiguration der mobilen Daten-verbindung wird automatisch aus der eingesetzten SIM-Karte und

dem zugehörigen Provider erstellt. Dies ist im Ausland von Vorteil, wenn Anwender die SIM-Karten eines günstigen Providers vor Ort nutzen möchten.

Unter Windows sorgt die Unterstützung der Mobile Broadband Schnittstelle für die performante Nutzung von 4G-/LTE-Hardware. Eine Installation der Benutzeroberfläche des Kartenlieferanten ist nicht erforderlich.

Einen wirtschaftlichen Betrieb ermöglicht der Budget Manager. Über ihn lassen sich Volumen-/Zeit-Budgets oder Provider bestimmen und überwachen.

Ein frei gestaltbares Banner in der Client GUI steht für Firmenlogo oder Supporthinweise zur Verfügung. Zudem ist die Client-GUI an ein barrierefreies Arbeiten angepasst und unterstützt u.a. den Betrieb von ScreenReadern.

Betriebssysteme	Microsoft Windows 10 & 8.x (auf x86 bzw. x86-64 Prozessorarchitektur)
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; Homezone; differenzierte Filterregeln bezüglich: Protokolle, Ports, Anwendungen und Adressen, Schutz des LAN-Adapters; IPv4 und IPv6 Unterstützung
VPN Bypass	Die VPN-Bypass-Funktion gestattet Anwendungen festzulegen, die trotz deaktiviertem Split Tunneling außerhalb der VPN-Konfiguration direkt ins Internet kommunizieren dürfen. Alternativ ist es möglich, Domänen bzw. Zieladressen zu bestimmen, zu denen die Datenkommunikation am VPN-Tunnel vorbei stattfinden soll.
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, 14-21, 25-30
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 #1747). 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

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; Multi-Zertifikatskonfiguration; Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme (u.a. RSA SecurID Ready)
Starke Authentisierung	Biometrische Authentisierung ab Windows 8.1 X.509 v.3 Standard; PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2, 2.0 und 3.0; Smart Card Reader Interfaces: 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	IPv4 / IPv6 Dual Stack
Dialer	NCP Internet Connector, Microsoft RAS Dialer (für ISP-Einwahl mittels Einwahl-Script)
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 VPN 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, LAN, WLAN, GSM (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA, analoges Fernsprechnetz

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) Verbindungsmodi: automatisch, manuell, wechselnd (Der Verbindungsaufbau ist davon abhängig, wie die Trennung zuvor stattgefunden hat)
APN von SIM Karte	Der APN (Access Point Name) definiert den Zugangspunkt eines Providers für eine mobile Datenverbindung. Die APN-Daten werden bei einem Providerwechsel automatisiert aus der jeweiligen SIM-Karte in die Client-Konfiguration übernommen
Datenkompression	IPCOMP (lzs), Deflate
Quality of Service	Priorisierung konfigurierter Datenströme innerhalb des VPN-Tunnels in Senderichtung
Weitere Features	Automatische Mediatyp-Erkennung, UDP-Encapsulation; WISPr-Support (T-Mobile Hotspots); IPsec-Roaming bzw., WLAN-Roaming (Voraussetzung: NCP Secure Enterprise VPN Server); Importfunktion der Dateiformate: *.ini, *.pcf, *.wgx und *.spd., Multi Zertifikatsunterstützung
Point-to-Point Protokolle	PPP over ISDN, PPP over GSM, 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, IKEv2-Authentisierung nach RFC 7427 (Padding-Verfahren)
Client Monitor Intuitive, grafische Benutzeroberfläche	Mehrsprachig (Deutsch, Englisch, Spanisch, 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 gestaltbares Textfeld; Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre; Automatische Prüfung auf neue Version

*) NCP FND-Server kann kostenlos als Add-On hier heruntergeladen werden:
https://www.ncp-e.com/de/service/download-vpn-client/

Weitere Informationen zum NCP Secure Entry Client (Win32/64) finden Sie hier:
https://www.ncp-e.com/de/produkte/ipsec-vpn-client-suite/vpn-clients-fuer-windows-10-8-7-macos/
Eine kostenlose 30-Tage Vollversion können Sie hier herunterladen:
https://www.ncp-e.com/de/service/download-vpn-client/

Optional: Zentrales Management und Endpoint Security → Upgrade auf NCP Secure Enterprise Client (Win32/64)

NCP PATH FINDER

FIPS 140-2 Inside

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg
Germany

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com