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

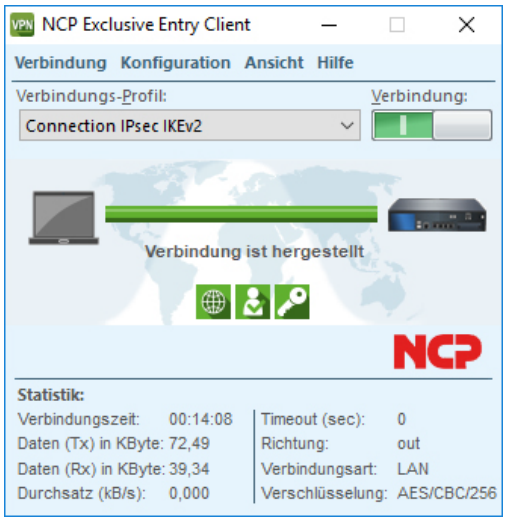
NCP
SECURE COMMUNICATIONS

Datenblatt

NCP Exclusive Entry Client

VPN Client Suite für Windows

- Für Juniper SRX
- Microsoft Windows 10, 8.x, 7
- Importfunktion für unterschiedliche Dateiformate
- Dynamische Personal Firewall
- VPN Bypass
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- FIPS Inside
- Starke Authentisierung (z.B. Zertifikate), Biometrie
- Unterstützung von 3G/4G Hardware (LTE)



Kommunikation

Der NCP Exclusive Entry Client für Windows 32/64 Bit Betriebssysteme ist ein leistungsfähiger VPN-Client für die Juniper SRX Serie. Bevorzugt kommt der NCP Exclusive Entry Client in kleineren VPN-Projekten mit bis zu 100 mobilen Arbeitsplätzen zum Einsatz, in denen keine NCP Exclusive Remote Access Lösung inklusive zentralem Management erforderlich ist. Auf Basis des IPsec-Standards lassen sich hochsichere Datenverbindungen zu Juniper SRX Gateways herstellen. Der Verbindungsaufbau erfolgt unabhängig vom Microsofts DFÜ-Dialer über beliebige Netze. Mitarbeiter können mit Windows-Endgeräten von jedem Standort weltweit auf das zentrale Datennetz zugreifen.

Die von NCP entwickelte VPN Path Finder Technology ermöglicht Remote Access auch hinter Firewalls bzw. Proxies, 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.

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 vor einer Anmeldung durch den Benutzer auf. Die Benutzeranmeldung 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 dieser 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 Exclusive Entry Client verfügt über zusätzliche Sicherheitsmechanismen wie eine integrierte dynamische Personal Firewall. Die zugehörige Konfiguration – enthält Regelwerke für Ports, IP-Adressen, Segmente und Applikationen – lässt sich durch ein Passwort schützen, so dass der Anwender die Firewall nicht versehentlich deaktivieren kann. Das Feature „Friendly Net Detection“ erkennt zuverlässig, ob sich der Anwender in einem sicheren oder unsicheren Netz befindet. Es aktiviert je nach Netzwerkumgebung die entsprechenden Firewall-Regeln. Dies gilt auch im Umfeld von Hotspots, hier insbesondere während des An- und Abmeldevorgangs am HotSpot-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 des Anwenders 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.

Die Home Zone-Funktion ist ein speziell für den Homeoffice-Bereich erstelltes Feature. 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 andere Firewall-Regeln aktiviert.

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.

Das Feature „Multi-Zertifikatsunterstützung“ ermöglicht VPN-Verbindungen mit unterschiedlichen Firmen, die jeweils ein eigenes Benutzerzertifikat erfordern. Es lassen sich mehrere Zertifikatseinstellungen festlegen und diese pro Profil zuordnen.

Das Kryptografiemodul, ist nach FIPS 140-2 zertifiziert (Zertifikat #1741).

Grundsätzlich lassen sich alle Client-Einstellungen durch den Administrator sperren. Somit werden Veränderungen seitens der Anwender verhindert.

Usability und Wirtschaftlichkeit

Die einfache Bedienung des NCP Exclusive Entry Clients ist einzigartig am Markt. Der im Client integrierte Dialer baut automatisch die Verbindung ins Internet auf. Die Mediatype-Erkennung wählt beim Aufbau der VPN-Verbindung das jeweils schnellste, vorhandene Übertragungsnetz aus. Die 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 Datenverbindung 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.

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 (Custom Branding Option) zur Verfügung. Zudem ist die Client-GUI an ein barrierefreies Arbeiten angepasst und unterstützt u.a. den Betrieb von Screen-Readern.

Betriebssysteme	Microsoft Windows 10, 8.x, 7 (auf x86 bzw. x86-64 Prozessorarchitektur)
Juniper SRX/vSRX OS	Junos OS 15.1X49-D80 oder höher vorausgesetzt
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall Firewall Configuration	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, Applikationen und Adressen, Schutz des LAN-Adapters; IPv4- und IPv6-Unterstützung; zentrale Administration
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 (CBC, CTR, GCM) 128,192,256 Bits; Blowfish; DES, Triple DES ; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-1, 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	IKEv1 (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKEv2 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, USB Tokens und Zertifikate mit ECC-Technologie Multi-Zertifikatskonfiguration; Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme (u.a.RSA SecurID Ready)
Starke Authentisierung	X.509 v.3 Standard; biometrische Authentisierung ab Windows 8.1
Standards PKI Enrollment	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, CMP* (Certificate Management Protocol)
Networking Features	LAN Emulation: Virtual Ethernet-Adapter, vollständiger WWAN-Support (Wireless Wide Area Network, Mobile Broadband ab Windows 7)
Netzwerkprotokolle	IP
Dialer	NCP Internet Connector oder Microsoft RAS Dialer (für ISP-Einwahl mittels Einwahl-Script)
VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist
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, ISDN
Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; 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
Weitere Features	UDP-Encapsulation, WISPr-Support (T-Mobile Hotspots), IPsec-Roaming bzw., WLAN-Roaming, Split Tunneling
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); 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 Unterstützung von Mobile Connect Cards; Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre

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

FIPS 140-2 Inside

Hinweis:
Aus dem NCP Exclusive Entry Client für Juniper SRX wurde am 1. Januar 2022 Juniper Secure Connect.

Der NCP Exlcusive Entry Client wurde zum 31. Dezember 2021 für den Vertrieb abgekündigt (END-OF-SALE), der Support des Produktes endet zum 31. Dezember 2024 (END-OF-LIFE).

Optional: Zentrales Management und Endpoint Security → Upgrade auf NCP Exclusive Remote Access Client

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