



NCP Secure Enterprise Client für Windows



Betriebssysteme	Microsoft Windows 11 & 10 (x64)
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-Servers¹); FND-abhängige Aktion starten; Secure Hotspot Logon; Home Zone; 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) mit 128, 192, 256 Bit; (<i>Blowfish 128/448 Bit und Triple-DES 112/168 Bit: Deprecated – nur Legacy-Support</i>) • Dynamische Verfahren (Schlüsselaustausch): RSA bis 4096 Bit; ECDSA; Diffie-Hellman-Gruppen 14–21, 25–30 (NIST- & Brainpool-Kurven); (<i>DH-Gruppen 1, 2, 5: Deprecated – nur Legacy-Support</i>) • Hash-Algorithmen: SHA-256, SHA-384, SHA-512; (<i>SHA-1: Deprecated – nur Legacy-Support</i>)

FIPS Inside



Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-3 zertifiziert (Zertifikat #4985).

Die FIPS Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- Diffie Hellman-Gruppe: Gruppe 14 oder höher (DH ab einer Länge von 2048 Bit)
- Hash-Algorithmen: SHA 2, SHA 256, SHA 384 oder SHA 512 Bit

Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit

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

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

PKI Enrollment

CMP (Certificate Management Protocol)

Network Access Control

Endpoint Policy: Überprüfung Aktualität des Virenschanners, vorhandene Hotfixes/Service Packs, gestartete Dienste, etc.

Networking Features

LAN Emulation: Virtual Ethernet-Adapter, vollständiger WWAN-Support (Wireless Wide Area Network, Mobile Broadband)

Netzwerkprotokolle

IPv4 / IPv6 Dual Stack

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 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, 4G/LTE, 5G
Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; Timeout (zeit- und gebührengesteuert); Budget Manager (Verwaltung von Verbindungszeit und/oder -volumen für Mobilfunk und WLAN, bei Mobilfunk 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	Automatische Mediatyp-Erkennung, UDP-Encapsulation, WISPr-Support (T-Mobile Hotspots), IPsec-Roaming bzw., WLAN-Roaming (Voraussetzung: NCP Secure Enterprise VPN Server)
Point-to-Point Protokolle	PPP over Ethernet, LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet-Society RFCs und Drafts	<i>IPsec-Architektur & Protokolle:</i> RFC 4301 (IP Security Architecture), RFC 4303 (ESP), RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 3948 (UDP Encapsulation / NAT-T), RFC 5685 (IKEv2 Redirect), RFC 3527 (DHCP Link Selection), RFC 3173 (IPCOMP); <i>Kryptografie & Authentisierung:</i> RFC 7427 (IKEv2 Signature Authentication), RFC 8221 (ESP Cryptographic Suites), RFC 8247 (IKEv2 Cryptographic Suites), RFC 5639 / RFC 6954 (Brainpool Elliptic Curve Groups); <i>Legacy / Abwärtskompatibilität:</i> RFC 2401–2409 (IPsec v1 / IKEv1, XAUTH, IKECFG, DPD nach RFC 3706)

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;
Anzeige des Verbindungsstatus;
Integrierte Unterstützung von Mobile Connect Cards;
Konfigurations- und Profil-Management mit Passwortschutz,
Konfigurationsparametersperre

Management via SEM

Um diese Client-Software zentral verwalten zu können, wird eine aktuelle SEM-Version mit folgenden Plug-ins benötigt:

- License Plugin
 - Client Configuration Plugin
 - Firewall Plug-in
-



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
