Datenblatt

NCP Secure Entry macOS Client

Universeller VPN Client für macOS

- Kompatibilität zu VPN Gateways (IPsec-Standard)
- macOS 10.15, 10.14, 10.13
- VPN-Profil-Importfunktion für unterschiedliche Dateiformate
- IPv4/6 Dual Stack Unterstützung
- Integrierte, dynamische Personal Firewall
- Fallback IPsec / HTTPS (VPN Path Finder Technology)
- Starke Authentisierung (z.B. Zertifikate), Biometrie
- FIPS Inside
- Unterstützung Apple Zertifikatsspeicher
- Kostenlose 30-Tage-Vollversion

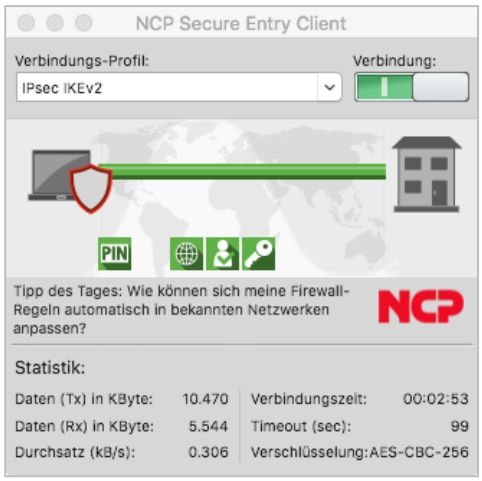
Universalität und Kommunikation

Der NCP Secure Entry macOS Client stellt auf Basis des IPsec-Standards hochsichere Datenverbindungen zu VPN Gateways aller namhaften Anbieter hergestellt her. Der Verbindungsaufbau erfolgt über beliebige Netze (auch iPhone Tethering). Mobile Mitarbeiter können mit Mac-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. Dieses Feature erfordert als Gegenstelle den NCP Secure VPN Enterprise Server.

Sicherheit

Der NCP Secure Entry Client verfügt über zusätzliche Sicherheitsmechanismen wie eine integrierte dynamische Personal Firewall. 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.

Weitere Security Features sind die Unterstützung von OTP-Lösungen (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure).

Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747).

Usability und Wirtschaftlichkeit

Die einfache Bedienung und Installation des NCP Secure Entry Mac Clients ist einzigartig am Markt. Die grafische, intuitive Benutzeroberfläche informiert über alle Verbindungs- und Sicherheitsstatus vor und während einer Datenverbindung. Wahlweise lässt sich die Benutzeroberfläche des Clients auch platzsparend in der Menüleiste von macOS minimiert darstellen. Detaillierte Log-Informationen sorgen im Servicefall für rasche Hilfe durch den Helpdesk. Ein Konfigurations-Assistent ermöglicht das einfache Anlegen von Profilen.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 · V 4.00
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Datenblatt

NCP Secure Entry macOS Client

Betriebssysteme	macOS 10.15 Catalina, 10.14 Mojave, macOS 10.13 High Sierra
Security Features	Unterstützung aller IPsec-Standards nach RFC
Personal Firewall	▪ Stateful Packet Inspection ▪ IP-NAT (Network Address Translation) ▪ Friendly Net Detection (autom. Umschaltung der Firewall-Regeln bei Erkennung des Netzwerkes anhand des IP-Adressbereiches, der Mac-Adresse des DHCP-Servers oder des NCP FND-Servers*) ▪ Differenzierte Filterregeln bezüglich: Protokolle, Ports und Adressen ▪ Unter den „Optionen“ zu „Bekannte Netze“ der Firewall-Konfiguration wurde der Parameter „VPN-Verbindungsaufbau im bekannten Netz nicht zugelassen“ eingefügt. Ist diese Option eingeschaltet, so ist kein zusätzlicher VPN-Tunnelaufbau mehr möglich, wenn sich der Client bereits im bekannten Netz befindet.
Virtual Private Networking	▪ IPsec Tunnel Mode ▪ IPv4/6 Dual Stack Unterstützung ▪ IPsec-Proposals werden über das IPsec-Gateway ausgehandelt (IKE, Phase 2) ▪ Kommunikation nur im Tunnel ▪ Message Transfer Unit (MTU) Size Fragmentation und Re-assembly
Verschlüsselung (Encryption)	*Symmetrische Verfahren:* AES-CBC 128, 192, 256 Bit; AES-CTR 128, 192, 256 Bit; AES-GCM 128, 256 Bit (nur IKEv2); Blowfish 128, 448 Bit; Triple-DES 112, 168 Bit; *Dynamische Verfahren für den Schlüsselaustausch:* RSA bis 4096 Bit; ECDSA bis 521 Bit, Seamless Rekeying (PFS); Hash Algorithmen: SHA, SHA-256, SHA-384, SHA-512, MD5; Diffie-Hellman-Gruppen: 1, 2, 5, 14-21, 25-30 (ab Gruppe 25: Brainpool Kurven
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 die folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: ▪ DH-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 und 256 Bit oder Triple DES
Schlüsselaustausch Verfahren	IKEv1 (Aggressive Mode und Main Mode): Pre-shared key, RSA, XAUTH; IKEv2: Pre-shared key, RSA, EAP-MS CHAPv2, EAP-MD5, EAP-TLS, EAP-PAP, Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383);

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 · V 4.00
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Authentisierungsverfahren

Internet Key Exchange (IKE):
- Aggressive Mode und Main Mode
- Quick Mode
- Perfect Forward Secrecy (PFS)
- IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP)
- Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure)

Benutzer-Authentisierung:
- XAUTH für erweiterte Benutzer-Authentisierung
- One-Time-Passwörter und Challenge Response Systeme
- Zugangsdaten aus Zertifikaten (PKI)

Unterstützung von Zertifikaten in einer PKI:
- Multi-Zertifikats-Konfiguration für die Schnittstellen PKCS#11 und zertifikatsbasierte Authentisierung mittels Zertifikaten aus dem Dateisystem als PKCS#12Container

Geräte-Authentisierung:
- Zertifikatsbasierte Authentisierung mittels Zertifikat aus dem macOS-Schlüsselbund

Seamless Rekeying (PFS)

IEEE 802.1x:
- Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Erweiterte Authentisierung gegenüber Switches und Zugriffspunkten (Layer 2)
- Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): - gegenüber Switches und Zugriffspunkten auf der Basis von Zertifikaten (Layer 2)

RSA SecurID Ready

Starke Authentisierung - Standards

Biometrische Authentisierung
X.509 v.3 Standard;
PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards);
PKCS#12 Interface für Soft Zertifikate;
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)

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 · V 4.00
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Datenblatt

NCP Secure Entry macOS Client

Networking Features	
Sichere Netzwerk Schnittstelle	Interface Filter ▪ NCP Interface-Filter stellen die Schnittstelle zu allen Netzwerk-Interfaces der PPP- und Ethernet-Familie her. ▪ Volle Unterstützung von Wireless Local Area Network (WLAN) ▪ Volle Unterstützung von Wireless Wide Area Network (WWAN)
Netzwerkprotokoll	IP
Verbindungs-Medien	LAN Unterstützte Verbindungsmedien für Apple oder Medienschnittstellen und Management Tools von Drittherstellern: ▪ LAN / Ethernet ▪ WLAN ▪ Mobilfunk ▪ iPhone Tethering
VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist (Voraussetzung: NCP Secure Enterprise VPN Server)
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
Line Management	DPD (Dead Peer Detection) mit konfigurierbarem Zeitintervall; Timeout; VPN on Demand für den automatischen Aufbau des VPN-Tunnels und die ausschließliche Kommunikation darüber
Datenkompression	IPCOMP (LZS), Deflate
Weitere Features	UDP-Encapsulation; Importfunktion der Dateiformate: *.ini, *.pcf, *.wgx, *.wge und *.spd.
Unterstützte Standards Internet Society RFCs und Drafts	RFC 4301 (IPsec), RFC 4303 ESP, RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IKEv1, RFC 3526, ISAKMP, RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 5685 (Redirect), RFC 7383 (Fragmentation), RFC 7427, 3279 Section 2.2.3, 3447 Section 8 (Signature Authentication), RFC 5903, 6954, 6989, 4754 (ECC), RFC 2451, 3686 (AES with ESP), 5930 (AES-CTR), 4106 (AES-GCM), 5282, 6379 (Suite B), RFC 3447 Section 8 (Padding)
Client Monitor	Mehrsprachigkeit (Englisch, Deutsch) ▪ Monitor & Setup ▪ Online Hilfe und Lizenz
Intuitive, grafische Benutzeroberfläche	Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files (farbige Darstellung), Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre; Monitor kann firmenspezifisch mit Firmenlogo und Support-Informationen ausgestattet werden. Start des Monitors optional automatisch nach Systemstart als Applikation oder als Icon in der Menüleiste

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 · V 4.00
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Tipp des Tages	In die Oberfläche des Client-Monitors ist ein Feld für Konfigurationstipps und Anwendungsbeispiele integriert. Mit einem Mausklick auf dieses Feld wird eine HTML-Seite mit Beschreibung zum jeweils wechselnden Tagestipp geöffnet, die über Handhabung und Leistungsmerkmale des Clients informiert
Projekt-Logo	Über ein zusätzliches Informationsfeld in der Monitor-Oberfläche, dem Banner, wird per Mausklick eine lokale HTML-Seite geöffnet. Das Banner kann durch Ihr Firmenlogo ersetzt werden, die lokale HTML-Seite durch eine andere Ihrer Wahl. Beide Dateien befinden sich im Installationsverzeichnis des Entry Clients unter /ProjectLogo als logo_de.png und secure_entry_banner_de.html. Zusätzlich kann eine Quick-Info angezeigt werden, wenn der Mauszeiger das Banner-Feld bzw. das Logo berührt

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

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

Weitere Informationen zum NCP Secure Entry Mac Client finden Sie hier:
https://www.ncp-e.com/de/produkte/ipsec-vpn-client-suite/vpn-clients-fuer-windows-10-8-7-vista-macos/

Eine kostenlose 30-Tage Vollversion können Sie hier herunterladen:
https://www.ncp-e.com/de/service/download-vpn-client.html

FIPS 140-2 Inside

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 · V 4.00
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com