Secur IT y
made in Germany
Trust Seal
www.teletrust.de/itsmig

NCP

Produktinformation

Enterprise-Features, die einen Unterschied machen

Features der NCP Enterprise VPN-Lösung

NCP hat über 35 Jahre Erfahrung in der Entwicklung hochsicherer Remote-Access-Lösungen. Im klassischen Szenario geht es bis heute um Filialvernetzung und die Anbindung von bis zu mehreren tausend Endanwendern an die Firmenzentrale – über verschiedene Einwahlmedien und Authentifizierungsvarianten.

Beim Thema VPN gibt es große Unterschiede zwischen einfachen Clients und professionellen Business-Lösungen mit zentralem Management. Hier eine kurze Übersicht:

- ✔ Integrierte Personal Firewall (Friendly Net Detection, sichere Hotspot-Anmeldung und Home-Zone-Funktion)
- ✔ Endpoint Security
- ✔ Systemunabhängigkeit
- ✔ Seamless Roaming
- ✔ NCP VPN Path Finder Technologie
- ✔ Quality of Service (QoS)
- ✔ starke Authentisierung (z. B. biometrische Merkmale wie Fingerabdruck oder Gesichtserkennung)
- ✔ Windows Pre-Logon
- ✔ IPv4 / IPv6 Dual Stack
- ✔ Cloud-Kompatibilität

Viele dieser Funktionen erfüllen die Anforderungen für cloudbasierte Security-Technologien und moderne Zero-Trust-Konzepte. Dadurch arbeiten die NCP-VPN-Lösungen selbst mit aktuellen Techniken und Standards wie SASE, SD-WAN, SSO durch SAML oder Zero Trust zusammen.

Integrierte Personal Firewall

Die integrierte Personal Firewall der NCP Secure Enterprise Clients bringt zahlreiche zusätzliche Sicherheitsfunktionen mit, die den Anwender dabei unterstützen, von unterwegs eine sichere Datenkommunikation aufzubauen ohne selbst eingreifen zu müssen. Bei einer gleichzeitigen Reduzierung der Fehlerquellen und des Support-Aufwands für die IT-Administration.

Die Firewall hat den Vorteil gegenüber Drittanbieterprodukten, dass sie auf die Netzwerkumgebung des Clients, mittels Friendly Net Detection, reagieren kann. Befindet sich ein Endgerät in einem öffentlichen oder einem vertrauenswürdigen/bekannten Netz, werden die Firewall-Regeln automatisch angepasst und der VPN-Tunnel entsprechend auf- oder abgebaut.

+ zusätzliche Sicherheit
+ Zeitersparnis in der IT-Administration

Friendly Net Detection

Automatische Anpassung der Firewallregeln in bekannten bzw. vertrauenswürdigen oder öffentlichen Netzwerken

Hotspot-Anmeldung

Bei der Nutzung eines öffentlichen Hotspots müssen sich Anwender häufig über eine Website des Hotspot-Betreibers anmelden und müssten dafür am VPN-Tunnel vorbei kommunizieren – was im Business-Umfeld meist nicht gestattet ist. Das Deaktivieren der Firewall durch den Anwender ist aber eine denkbar schlechte Lösung. Genau diese Problematik wird mit der im NCP Secure Client integrierten Hotspot-Anmeldung adressiert.

Durch eine Erweiterung müssen sich User hier nicht ungesichert mit dem Hotspot-Provider verbinden, sondern nutzen einen sicheren, funktionsreduzierten Webbrowser, der durch den NCP-Client gestartet wird.

+ Sicherheit
+ Nutzerfreundlichkeit

Sichere Hotspot-Anmeldung

Einfach und dennoch sicher an öffentlichen Hotspots anmelden und arbeiten ohne die Sicherheitseinstellungen lockern zu müssen.

Home Zone

Mit der Vorgabe, sämtliche Kommunikation ausschließlich durch den VPN-Tunnel zu führen, hat der Anwender im Homeoffice das Problem auf seine Peripherie im lokalen Netzwerk, z. B. Drucker, nicht zugreifen zu können.

Die Firewall des NCP Secure Clients kann so konfiguriert werden, dass Anwender lokale Netzwerkgeräte wie einen Drucker im Homeoffice verwenden können. Gleichzeitig erfolgt der Internetzugriff dennoch nur durch den VPN-Tunnel.
Hierfür wird das lokale Netzwerk im Homeoffice vom Anwender als Home Zone definiert, um ein weiteres Firewall-Regel-Set zur Anwendung zu bringen.

+ Nutzerfreundlichkeit

Home Zone

Über diese Firewall-Konfiguration im Homeoffice lokale Netzwerkgeräte wie Drucker oder Scanner verwenden

Endpoint Security

Vor einem Zugriff auf das Firmennetz werden alle sicherheitsrelevanten Parameter durch den NCP Secure Client überprüft. Dies bezieht sich beispielsweise auf den Status von Virenscannern, Dienste- Informationen, Zertifikaten oder Softwarestand des Endgerätes.

Die Einhaltung der Sicherheitsrichtlinien ist zwingend und vom Anwender nicht manipulierbar.
Bei Abweichungen wird der Zugang verwehrt oder die Anwender erhalten ausschließlich Zugriff in eine Quarantänezone, um das System zu aktualisieren.

+ Sicherheitsrisiken minimiert

Endpoint Security

Vor dem Netzwerkzugriff erfolgt eine automatische Überprüfung sicherheitsrelevanter Parameter (Virenscanner, Zertifikate usw.).

Integrierbarkeit in bestehende Infrastruktur

Die NCP-Lösung kann in jede bestehende Infrastruktur integriert werden und ist zu den Produkten aller gängigen Firewall-Hersteller (z. B. Cisco, Juniper etc.) kompatibel. Somit sind Investitionen auch dann sicher, wenn später Veränderungen oder ein Austausch in der Umgebung notwendig werden.

Die NCP-Clients stehen für gängige Endgeräte wie Notebooks, Smartphones und Tablets mit den Betriebssystemen Windows, macOS, Linux, iOS und Android zur Verfügung. Eine intuitive, in allen Betriebssystemen wiedererkennbare Oberfläche sorgt bei den Nutzern für eine hohe Akzeptanz.

+ Investitionssicherheit

Systemunabhängigkeit

Die universellen NCP-Clients gibt es für gängige Notebooks, Smartphones und Tablets mit Windows, macOS, Linux, iOS oder Android.

Seamless Roaming

Beim mobilen Arbeiten von unterwegs kommt es häufig zu Medienwechseln zwischen WLAN und 3G/4G. Da eine VPN-Verbindung die Kommunikation absichern, aber nicht einschränken soll, ist unterbrechungsfreies Arbeiten eine wichtige Anforderung.

Der VPN Client von NCP wechselt während einer Session für den Anwender unbemerkt das Verbindungsmedium und leitet den VPN-Tunnel dynamisch um. Voraussetzung als Gegenstelle ist ein aktueller NCP Secure Enterprise VPN Server. Ständige Verfügbarkeit von Anwendungen wird somit Realität.

+ Nutzerfreundlichkeit

Seamless Roaming

Vor dem Netzwerkzugriff erfolgt eine automatische Überprüfung sicherheitsrelevanter Parameter (Virenscanner, Zertifikate usw.).

Patentierte NCP VPN Path Finder Technologie

Einschränkungen in der Nutzung von IPsec-VPN-Diensten erschweren Geschäftsreisenden im Ausland in immer mehr Ländern den Zugriff auf das eigene Netzwerk und somit die Arbeit von unterwegs.

Die VPN Path Finder Technologie ermöglicht einen sicheren externen Netzwerkzugang auch in IPsec-feindlichen Umgebungen hinter Firewalls, deren Einstellungen IPsec-basierten Datenverkehr verhindern.

+ Sicherheit
+ Nutzerfreundlichkeit

Path Finder Technologie

VPN auch in IPsec feindlichen Umgebungen, selbst wenn entsprechende Verbindungen durch die Firewall geblockt werden

Starke Authentisierung

Für ein Höchstmaß an Sicherheit unterstützen die NCP-Clients verschiedene Authentisierungsmethoden, unter anderem auch biometrische Merkmale wie Fingerabdruck oder Gesichtserkennung. Bei Apple-Geräten werden entsprechend Face ID und Touch ID unterstützt.

Weitere unterstützte Möglichkeiten zur Multi-Faktor-Authentifizierung sind die integrierte Advanced Authentication, OTP-Token (One Time Password) und digitale Zertifikate in einer PKI (Public Key Infrastructure).

+ **Sicherheit**
+ **Nutzerfreundlichkeit**

Biometrische Authentisierung

Für eine starke Authentisierung unterstützen die Clients unter anderem biometrische Merkmale (z.B. Fingerabdruck).

Quality of Service (QoS)

Das Quality of Service Modul (QoS) im NCP Secure Client für Windows bietet die Möglichkeit, bestimmten Anwendungen im VPN-Tunnel eine zugesicherte ausgehende Datenrate zuzuweisen. Dies kann vor allem im Homeoffice mit einem schwächeren Daten-Upload nützlich sein.

Auf diese Weise können Verzögerungen oder Unterbrechungen verhindert werden, beispielsweise für eine bessere Sprachqualität bei VoIP-Telefonie ohne Abbrechen oder eine verzögerungsfreie Übertragung von Bild und Ton beim Videostreaming über Skype oder YouTube.

+ **Sicherheit**
+ **Nutzerfreundlichkeit**

Quality of Service (QoS)

VoIP oder Skype ohne Abbrüche und Verzerrungen durch zugesicherte ausgehende Datenraten im VPN-Tunnel

Windows Pre-Logon

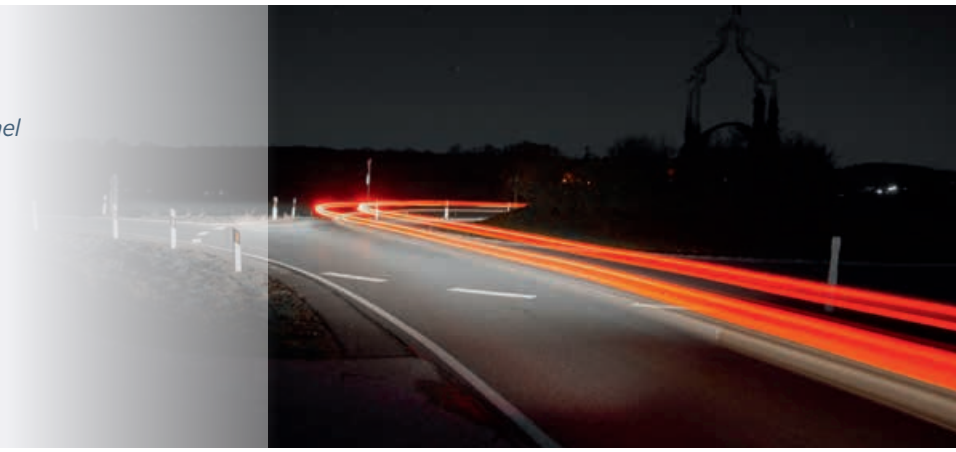
Durch die Windows Pre-Logon Funktionalität kann ein Anwender bereits einen VPN Tunnel zur Firmenzentrale aufbauen, noch bevor er sich im lokalen Windows System anmeldet.

Diese erfolgt dann bereits über den VPN-Tunnel und ist in der Windows Domain bzw. im Active Directory authentisiert.

+ **Sicherheit**
+ **Nutzerfreundlichkeit**

Windows Pre-Logon

Sichere Anmeldung an der Windows Domäne durch bereits im Vorfeld aufgebauten VPN-Tunnel zur Firmenzentrale



IPv4 / IPv6 Dual-Stack

Mit Blick auf die Zukunftssicherheit ist die Produktpalette von NCP voll IPv6-fähig. Die Client- und Server-Software ist so ausgelegt, dass IPv4- und/oder IPv6-Kommunikation möglich sind sowie ein Dual-Stack-Betrieb.

Somit lassen sich auch Szenarien abdecken, bei denen im öffentlichen Netz mit IPv6-Adressen gearbeitet wird, während im internen Firmennetz weiterhin IPv4 zum Einsatz kommt oder an beiden Stellen beide zum Einsatz kommen.

+ **Sicherheit**
+ **Komfort in der IT-Administration**

IPv6 Dual Stack

Die NCP Client- und Server-Software unterstützt IPv4- und/oder IPv6-Kommunikation sowie Dual Stack-Betrieb.

	Windows	macOS*	iOS	Android	Linux
Personal Firewall	✔	✔			✔
Friendly Net Detection	✔	✔			✔
Hotspot-Anmeldung	✔				
Home Zone	✔				
Endpoint Security	✔	✔			✔
Seamless Roaming	✔				
Path Finder Technologie	✔	✔	✔	✔	✔
Biometrische Authentisierung	✔	✔	✔	✔	
QoS	✔				
Windows Pre-Logon	✔				
IPv4/IPv6 Dual Stack	✔	✔	✔	✔ *(in Planung)*	

**Personal Firewall und Friendly Net Detection sind in den macOS Clients ab Version 4.0 bis ausschließlich Version 4.6 enthalten*

NCP

Sie haben Fragen oder möchten einen Termin für eine Produktdemonstration vereinbaren? Dann kontaktieren Sie uns!

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg

Tel.: +49 911 9968-0
vertrieb@ncp-e.com
www.ncp-e.com

Wir freuen uns auf ein Gespräch mit Ihnen!

Weitere Infos auf unserer Webseite!