



SecurITy  
made  
in  
Germany

Trust Seal  
www.teletrust.de/itsmig

# NCP

## Produktinformation

Leistungsstarke Enterprise VPN-Lösung  
und Entry Clients für Einzelplätze





Weitere Infos auf unserer Webseite!

Das BSI empfiehlt das Einrichten eines Virtual Private Network (VPN) als erste von fünf einfachen Maßnahmen für IT-Sicherheit im Homeoffice.

**IT-Sicherheit im Homeoffice im Jahr 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)**



## Modern Remote Access at its best!

Eine leistungsstarke und flexible Remote-Access-Infrastruktur wurde in der Pandemiesituation zu einem entscheidenden Business-Continuity-Faktor für Unternehmen. Wer schnell und skalierbar auf ungeplante Situationen reagieren kann und dabei sicher angebunden ist, bleibt bei jedem Bedarf produktiv.

Lesen Sie hier, welche Möglichkeiten Sie mit einer zentral administrierbaren NCP Next Gen VPN-Lösung haben. Egal, ob Sie Einzelplatzlizenzen brauchen oder tausende mobile Nutzer anbinden wollen, die NCP-Lösungen garantieren IT-Security Made in Germany, die in Nürnberg entwickelt wird:

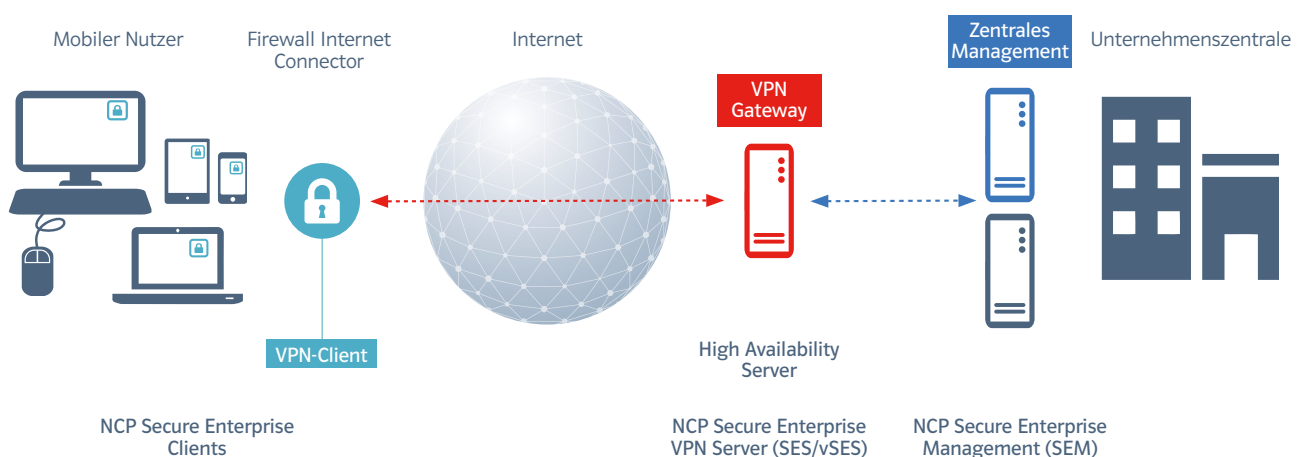
- ☑ für Einzelplätze und kleine Installationen die **NCP Secure Entry Clients**
- ☑ für große Installationen und Standortvernetzung die **NCP Secure Enterprise VPN-Lösung** (zentrales Management, VPN Gateway und Enterprise VPN Clients)

Weitere Lösungen kommen für Kommunikation der Geheimhaltungsstufe VS-NfD und auch in Industrie 4.0/IIoT wie z. B. für sichere Fernwartung zum Einsatz.

Unsere Produkte erfüllen zudem 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, SSE, SSO durch SAML oder Zero Trust zusammen.

### Die NCP-VPN-Lösung ist modular aufgebaut und besteht aus drei Bausteinen:

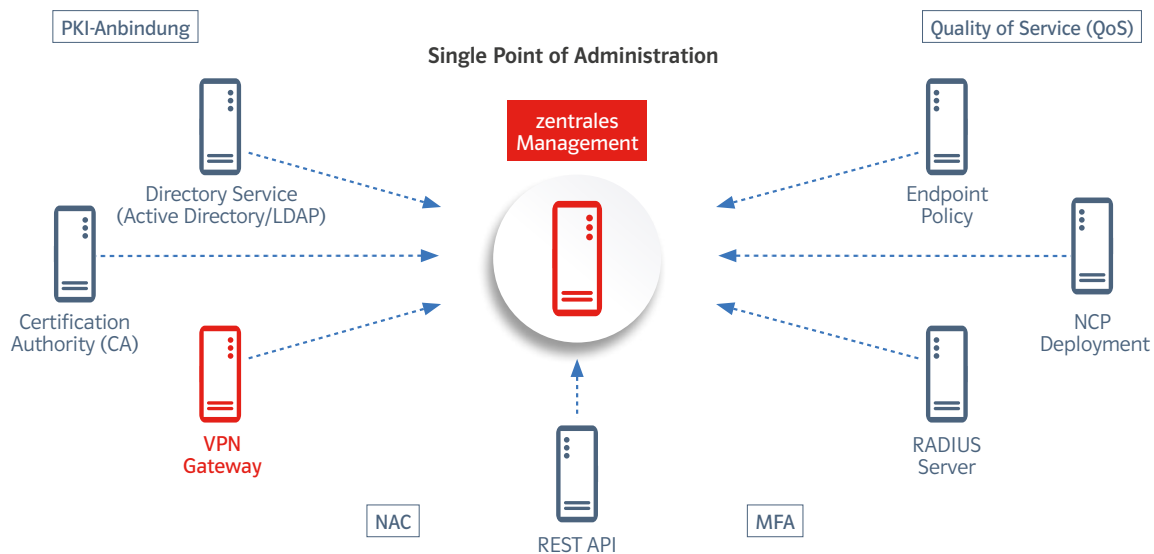
- zentrales Management zur Verwaltung der Infrastruktur
- Secure Gateway (optional als virtuelle Appliance)
- Clients für Windows, macOS, Linux, Android und iOS



# NCP Secure Enterprise Management

Mit dem **NCP Secure Enterprise Management (SEM)** können Sie Ihr Remote-Access-Netzwerk bequem von zentraler Stelle aus administrieren. So müssen Administratoren nicht mehr eine Vielzahl an Insellösungen und

entsprechend viele Konsolen bedienen. Das SEM fungiert als Single Point of Administration, über den sich Policy-Änderungen im laufenden Betrieb vornehmen lassen.

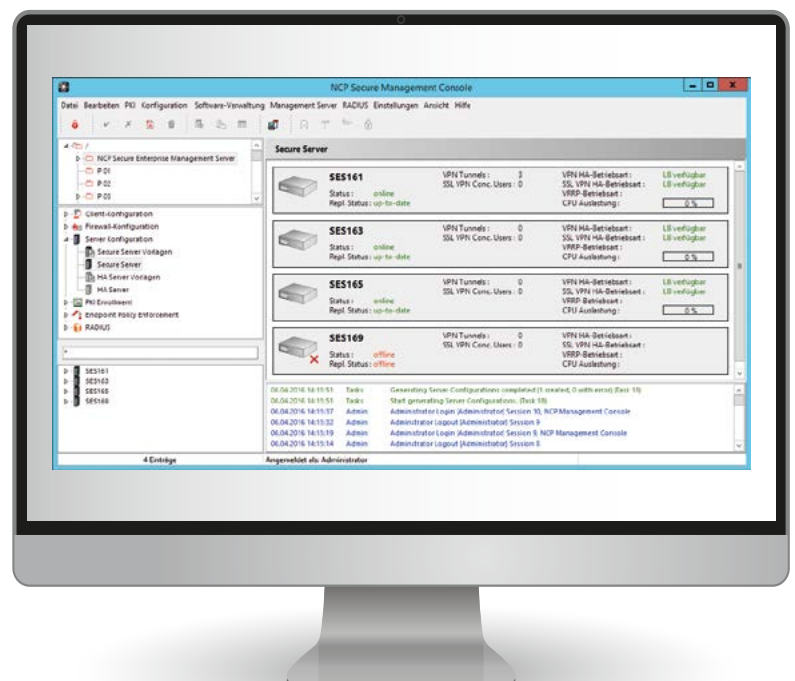


*Zu den Funktionen, die das leistungsstarke Secure Enterprise Management bereitstellt, zählt das zentrale Konfigurieren und Verwalten von VPN-Clients und Servern.*



## Ihre Vorteile mit dem NCP-VPN-Management:

- automatisierter Massen-Rollout
- zentrale Client-/Server-Konfiguration, Zertifikats- und Lizenzmanagement
- automatisierte Software-Updates
- Integration in Benutzerverwaltung (LDAP, Active Directory etc.)
- Mandanten- und Provider-Fähigkeit
- umfassendes Monitoring und Berichtswesen
- integrierter RADIUS-Server
- Advanced Authentication
- Automatisierung mit REST APIs



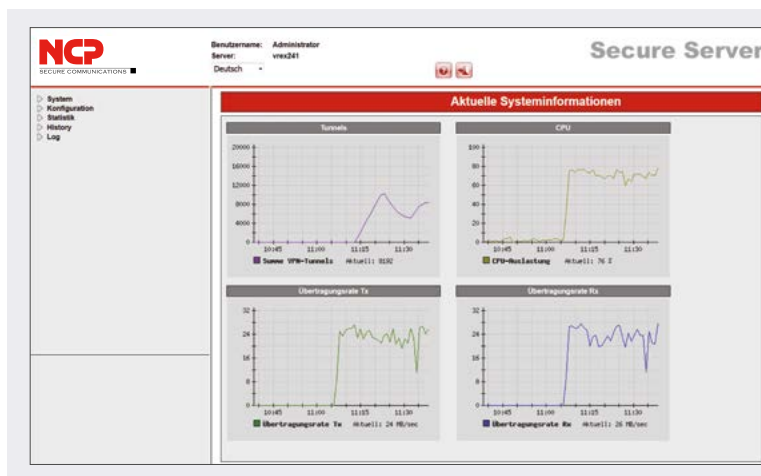
# IPsec VPN Gateway Software

Der **NCP Secure Enterprise VPN Server (SES)** ermöglicht durch seine modulare Softwarearchitektur und hohe Skalierbarkeit den bedarfsgerechten Ausbau Ihres Remote-Access-Netzwerkes und Ihrer Standortvernetzung.

Dadurch können Sie eine leistungsfähige VPN-Infrastruktur aufbauen, die sich jederzeit flexibel Ihren Anforderungen anpasst und mit Ihrem Unternehmen wächst – auch, wenn Sie mit 500 Anwendern starten und in Zukunft ein Vielfaches davon anbinden müssen.

## Ihre Vorteile mit dem NCP Secure Enterprise VPN Server

- softwarebasiert und mandantenfähig
- Verwaltung von mehr als 10.000 gleichzeitigen Sessions pro System
- Integration von IP-Routing und Firewall-Funktionalitäten
- universell einsetzbar z.B. für Remote Access, Standortvernetzung und IIoT
- integrierte Zwei-Faktor-Authentifizierung + TOTP
- Hochverfügbarkeit durch Failsafe und Loadbalancing
- Policy-Änderungen „on the Fly“
- NCP VPN Path Finder Technology (Fallback IPsec/HTTPS)
- Network Access Control
- Endpoint Security (in Verbindung mit SEM)
- Zertifikats-basierte Authentisierung auch für iOS-Endgeräte
- Flexible Traffic-Steuerung mit Domain Based Split Tunneling



*Die modulare Softwarearchitektur und hohe Skalierbarkeit des SES/vSES ermöglichen es, Remote Access und Standortvernetzung bedarfsgerecht auszubauen.*

*Die Leistungsfähigkeit des Systems kann auf mehr als 10.000 Nutzer erweitert werden und im High Availability (HA)-Verbund sogar um ein x-faches.*

## Virtuelle VPN Appliance

Der **NCP Virtual Secure Enterprise VPN Server (vSES)** besteht aus dem VPN-Server, High-Availability-Services und einem gehärteten Betriebssystem. Zur Installation bedarf es lediglich einer gängigen Virtualisierungsumgebung. Das Betriebssystem bietet aufgrund verschiedener Härtingsmaßnahmen höchste Sicherheit.

Hervorzuheben sind vor allem die Skalierbarkeit des Systems sowie das ganzheitliche Update-Konzept. Als All-in-One Lösung erspart Ihnen die Appliance im Einsatz viel Aufwand und den Aufbau von internem Spezialisten-Knowhow.



### Folgende Vorteile zeichnen den vSES aus:

- gehärtete All-in-One-Lösung
- kompatibel zu gängigen Virtualisierungslösungen
- hohe Skalierbarkeit durch Multi-Prozessor/-Core-Unterstützung
- VPN Path Finder Technology (Fallback IPsec/HTTPS)

# IPsec VPN Client Suite

Mit den **NCP Secure Enterprise Clients** binden Sie Ihre Nutzer unkompliziert und sicher an Ihr Firmennetz an – unabhängig vom Betriebssystem und Endgerät. Durch die zentrale Administration über das SEM können alle Clients selbst bei mehreren hundert oder tausenden Benutzern individuell und in Gruppen konfiguriert und verwaltet werden.

Da Sie Rollouts und Updates für mobile Nutzer in den meisten Fällen ohne physikalischen Zugriff auf die Endgeräte vornehmen können, sinkt Ihr Administrationsaufwand merklich.

Unsere Enterprise Client Suite umfasst folgende Betriebssysteme:



Windows



macOS



iOS

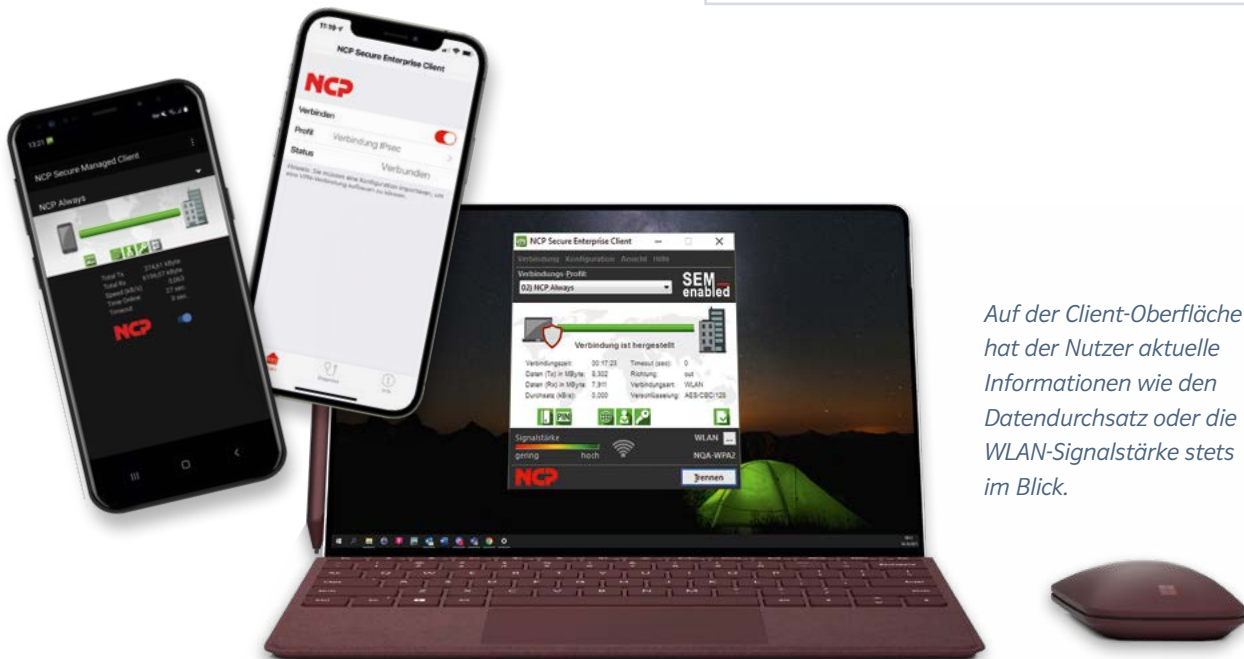


Android



Linux

Alle aktuellen Versionen  
unter diesem Link:



Auf der Client-Oberfläche hat der Nutzer aktuelle Informationen wie den Datendurchsatz oder die WLAN-Signalstärke stets im Blick.

## Viele Probleme, eine Lösung: ein VPN-Client mit intelligenter Firewall

Beim Zugriff auf Firmenressourcen von externen Standorten aus gibt es viele verschiedene Szenarien und Berechtigungslagen: Homeoffice, fremde Netze bei Kunden und Partnern oder öffentliche Hotspots und das Ganze auch im Ausland. Der NCP Client meistert die Herausforderung auf einfache und sichere Weise.

Zahlreiche hilfreiche Funktionen lösen die angesprochenen Probleme, ohne dass der Anwender es merkt oder falsch eingreifen kann:

- **Friendly Net Detection** – befindet sich ein Endgerät in einem öffentlichen Netz oder in einem vertrauens-

würdigen/ bekannten Netz? Die Firewall-Regeln werden angepasst und der VPN-Tunnel entsprechend automatisch auf- oder abgebaut

- **Hotspot-Login** – durch eine spezielle Erweiterung müssen Sie sich nie wieder für die Anmeldung ungesichert mit dem Hotspot-Provider verbinden
- **Home Zone-Funktion** – die Firewall des NCP Client wird automatisch so konfiguriert, dass die Anwender zwar lokale Netzwerkgeräte wie einen Drucker verwenden können, der Internetzugriff aber nur durch den VPN-Tunnel erfolgen darf

## IPsec VPN Clients für Einzelplätze mit Windows, macOS oder Android

Die **NCP Secure Entry Clients** eignen sich für Einzelplätze und kleine Installationen (mit beispielsweise 100 mobilen Mitarbeitern). Sie ermöglichen eine sichere Einwahl ins Firmennetzwerk und sind für Windows, macOS sowie Android erhältlich.

Eine grafische, intuitive Benutzeroberfläche informiert den Anwender über den Verbindungs- und Sicherheitsstatus vor und während einer Datenverbindung. Administratoren können durch Parametersperren und die Konfiguration als One Click Solution Sicherheitsrisiken minimieren. Alle Clients sind zu gängigen Gateways im Markt kompatibel (z.B. Cisco, Juniper Networks, Palo Alto, etc.) und können problemlos in vorhandene Netzwerkstrukturen integriert werden.



*Die NCP Secure Entry Clients sind prädestiniert für kleine Installationen mit bis zu 100 Arbeitsplätzen.*

*Die einfache Bedienung des NCP Secure Entry Clients ist einzigartig am Markt. Eine grafische, intuitive Benutzeroberfläche informiert den Anwender über den Verbindungs- und Sicherheitsstatus vor und während einer Datenverbindung.*



Auch wenn die Entry-Lösung „kleiner“ ist als die gemanagte Enterprise Client Suite, so verfügt sie über einen großen Funktionsumfang. Gegenüber einfacher VPN-Software anderer Hersteller punkten die NCP Secure Entry Clients mit zahlreichen in der Praxis hilfreichen Features:

- sichere Hotspot-Anmeldung mit WLAN-Manager
- Seamless Roaming
- Home Zone
- biometrische Authentisierung
- "Quality of Service"-Unterstützung
- viele weitere!



Weitere Infos auf unserer Webseite!

# Hauptfeatures der NCP-VPN-Gesamtlösung im Überblick



## Path Finder Technologie

VPN auch in IPsec feindlichen Umgebungen, z. B. Hotspots oder restriktiven Staaten



## Always On

arbeiten wie in der Firma – anytime & anywhere



## Seamless Roaming & Internet Connector

automatische Medienerkennung/-auswahl und Wechsel zwischen LAN/WLAN/Mobilfunk ohne Nutzer-Interaktion



## Endpoint Policy Check

Qualifizierung des Endgerätes und Überprüfung sicherheitsrelevanter Parameter, z. B. Virens Scanner, OS-Version, Domainzugehörigkeit, etc.



## Domain Based Split Tunneling

Flexible Traffic-Steuerung auf Anwendungsebene nach dem Zero-Trust-Prinzip



## Personal Client Firewall

integrierte dynamische Firewall mit Zusatzfeatures (Friendly Net Detection, Hotspot-Login, Home Zone)



## Friendly Net Detection

automatische Anpassung der Firewall-Regeln in vertrauenswürdigen Netzwerken



## Hotspot-Login

sichere Nutzung öffentlicher Hotspots (VPN-Zugriff trotz Captive Portal)



## Home Zone

Nutzung lokaler Netzwerkgeräte wie Drucker im Homeoffice trotz ausschließlicher Kommunikation durch den Tunnel



## Mandantenfähigkeit

mehrere Kunden oder Unternehmensbereiche zentral, aber unabhängig und getrennt voneinander verwalten



## Windows Pre-Logon

Anmeldung im lokalen Windows-System erfolgt über den bereits vorher aufgebauten VPN-Tunnel und wird in der Windows-Domain bzw. im Active Directory authentisiert



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!