Produktinformation

Leistungsstarke Enterprise VPN-Lösung und Entry Clients für Einzelplätze

Modern Remote Access at its best!

Eine leistungsstarke und flexible Remote Access-Infrastruktur ist heute ein entscheidender Faktor für die Geschäftskontinuität. Unternehmen, die flexibel und skalierbar auf unvorhergesehene Anforderungen reagieren können, bleiben auch unter veränderten Bedingungen produktiv.

Erfahren Sie, wie Sie mit den VPN-Lösungen von NCP sichere und flexible Remote Access-Infrastrukturen realisieren können.

Ob Sie einzelne Arbeitsplätze absichern oder tausende mobile Nutzer sicher anbinden möchten: NCP bietet die passende Lösung – entwickelt in Nürnberg mit dem Anspruch IT-Security „Made in Germany ":

- ✓ **NCP Secure Entry Clients**: Für Einzelarbeitsplätze und kleinere Installationen.
- ✓ **NCP Secure Enterprise VPN-Lösung**: Für große Installationen und die sichere Standortvernetzung mit zentralem Management, VPN Gateway und Enterprise VPN Clients.

Weitere vom BSI zugelassene Lösungen kommen für die Kommunikation der Geheimhaltungsstufen VS-NfD, EU RESTRICTED und NATO RESTRICTED zum Einsatz.

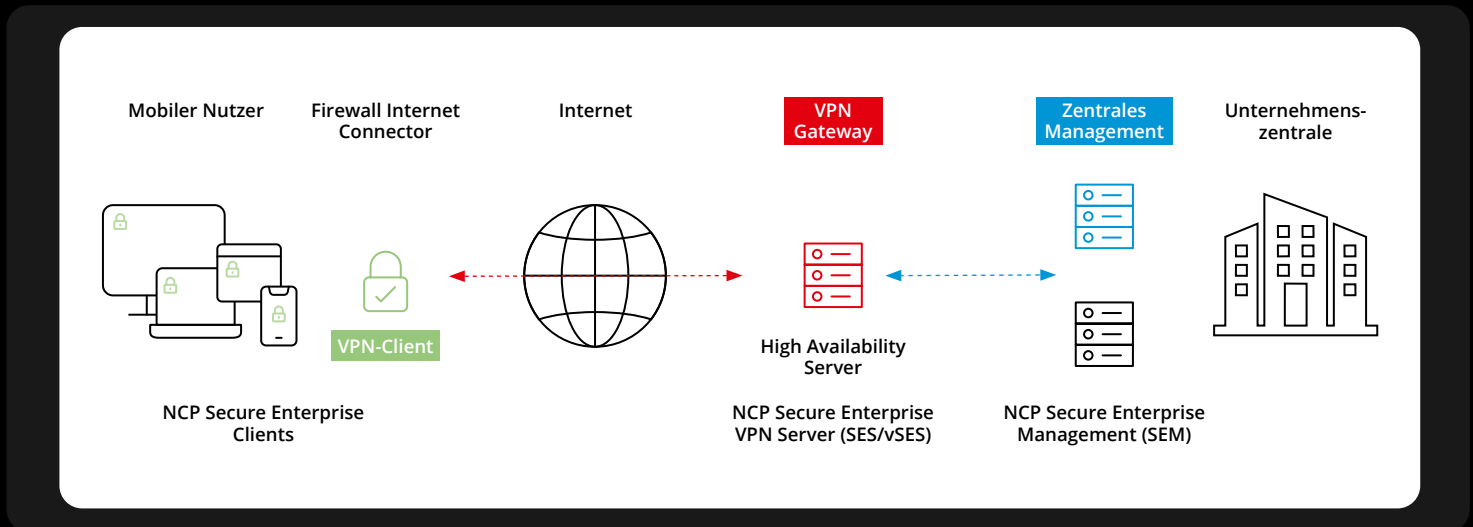
Die NCP VPN-Lösungen lassen sich zudem in moderne IT-Sicherheitsarchitekturen integrieren und unterstützen Konzepte und Technologien wie SASE, SD-WAN, SSE, Single Sign-On (SSO) über SAML sowie Zero Trust.

„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)

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

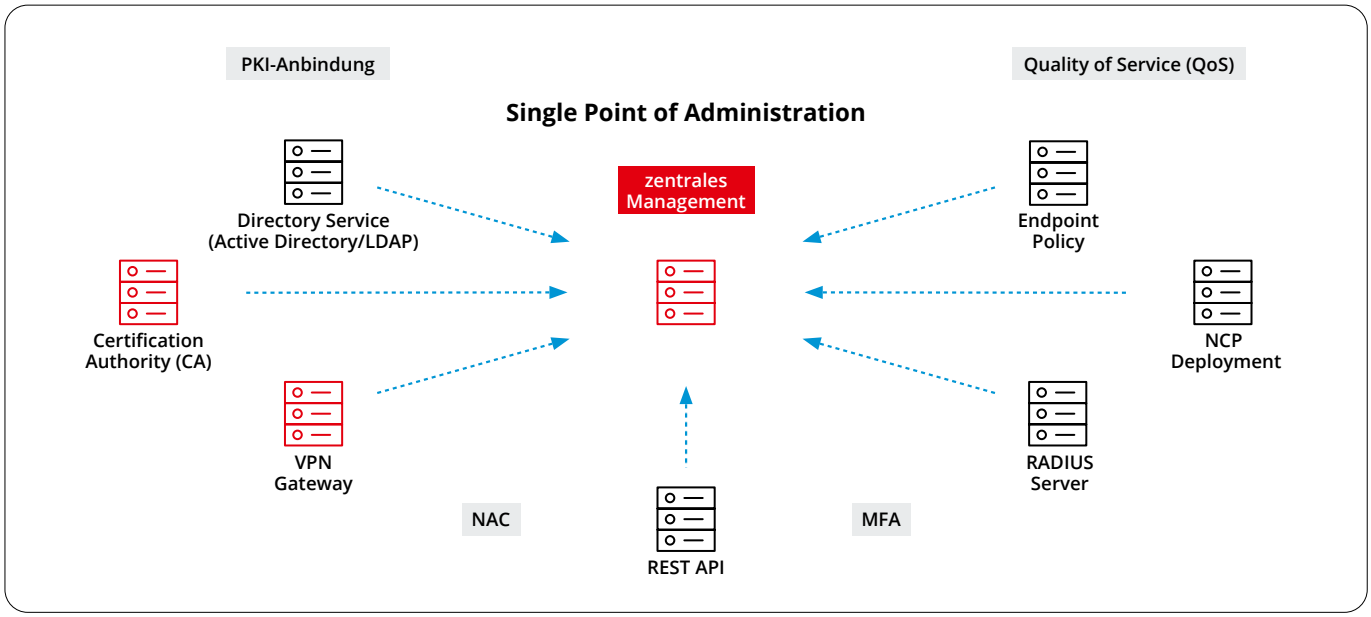
- zentrales Management zur Verwaltung der Infrastruktur
- Secure Gateway (optional als virtuelle Appliance)
- Clients für Windows, macOS, Linux, Android und iOS



NCP Secure Enterprise Management

Mit dem **NCP Secure Enterprise Management (SEM)** verwalten Sie Ihre gesamte Remote Access-Infrastruktur zentral über eine einzige Administrationsoberfläche.

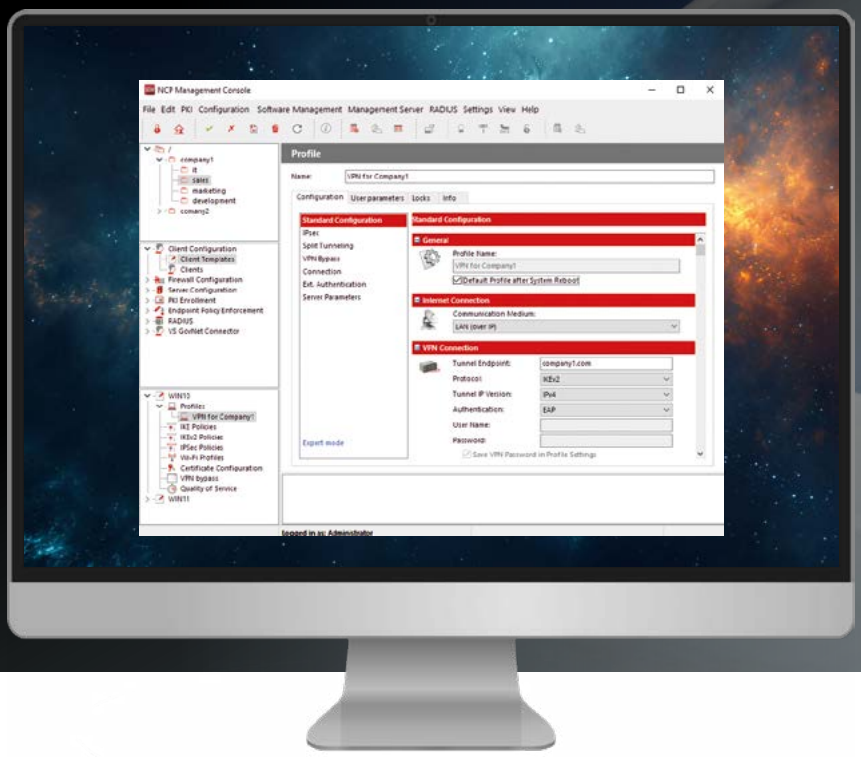
Als „Single Point of Administration" vereinfacht das SEM die Verwaltung und ermöglicht es Administratoren, Richtlinien auch im laufenden Betrieb anzupassen.



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

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

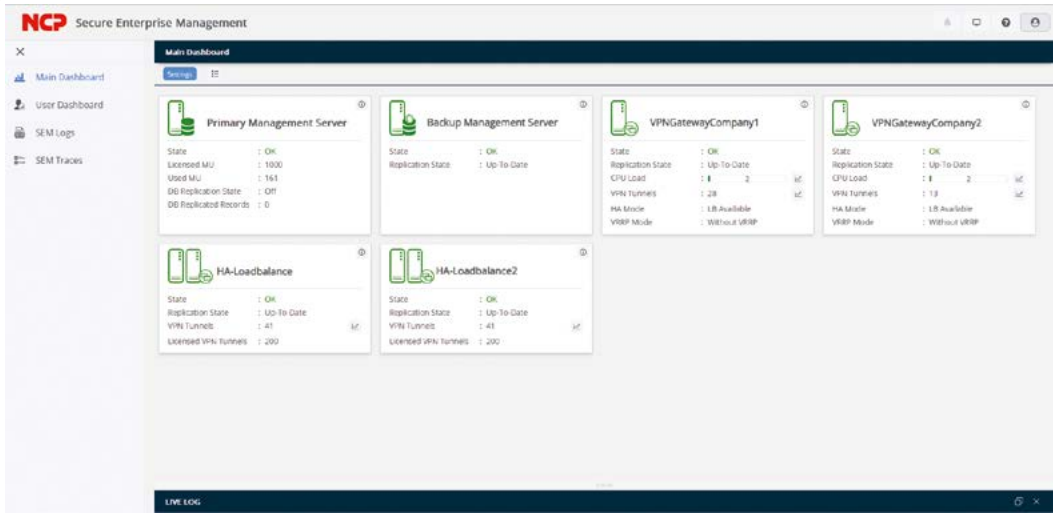


IPsec VPN Gateway Software

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)
- Zertifikatsbasierte 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 Härtungsmaßnahmen 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-Know-how.

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

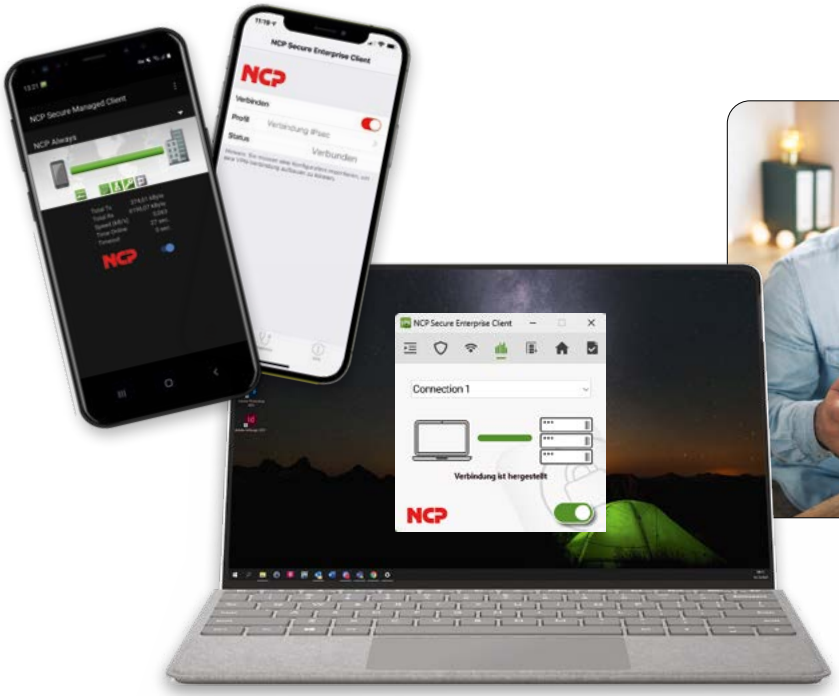
Mit den **NCP Secure Enterprise Clients** binden Sie Ihre Nutzer unkompliziert und sicher an Ihr Firmennetz an – unabhängig vom Betriebssystem und Endgerät. Durch die zentrale Administration über das SEM können alle Clients selbst bei mehreren mehreren Hundert oder Tausend Benutzern individuell und in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

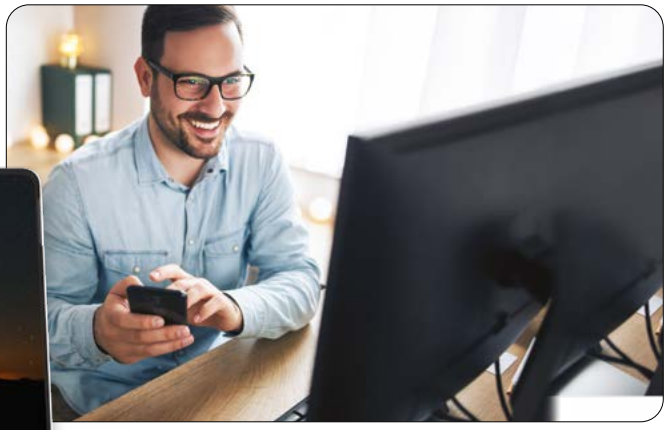
Da Sie Rollouts und Updates für mobile Nutzer in den meisten Fällen ohne physikalischen Zugriff auf die Endgeräte vornehmen können, sinkt Ihr Administrationsaufwand merklich.

Unsere Enterprise Client Suite umfasst folgende Betriebssysteme:

Windows **macOS** **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 Netzwerke von Kunden und Partnern oder öffentliche Hotspots und auch bei internationalen Einsätzen. 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:** Erkennt, ob sich das Endgerät in einem öffentlichen oder vertrauenswürdigen Netzwerk befindet. Auf dieser Grundlage werden die Firewallregeln angepasst und der VPN Tunnel automatisch auf- oder abgebaut.
- **Hotspot Login**: Ermöglicht die Anmeldung an öffentlichen Hotspots, ohne dass dafür eine ungesicherte Verbindung zum Hotspot Provider hergestellt werden muss.
- **Home Zone-Funktion**: Konfiguriert die Firewall des NCP Clients automatisch so, dass Anwender lokale Netzwerkgeräte wie Drucker nutzen können, während der Internetzugriff ausschließlich über den VPN Tunnel erfolgt.

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 Mitarbeitenden). Sie ermöglichen eine sichere Einwahl ins Firmennetzwerk und sind für Windows, macOS sowie Android erhältlich.

Eine intuitive grafische 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.

Weitere Infos auf unserer Webseite!

Trotz ihrer Ausrichtung auf Einzelarbeitsplätze und kleinere Installationen bieten die NCP Secure Entry Clients einen großen Funktionsumfang. Gegenüber einfacher VPN Software anderer Hersteller punkten sie mit zahlreichen praxisorientierten Funktionen:

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

Hauptfeatures der NCP VPN-Gesamtlösung

ZeroTrust

Path Finder-Technologie
PN 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 Nutzerinteraktionen

Endpoint Policy Check
Qualifizierung des Endgeräts und Überprüfung sicherheitsrelevanter Parameter, z. B. Virenscanner, 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 Zusatzfunktionen (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 Str. 2
90449 Nürnberg

Tel.: +49 911 9968 222
vertrieb@ncp-e.com

www.ncp-e.com

Wir freuen uns auf ein Gespräch mit Ihnen.

Weitere Infos auf unserer Webseite!