NCP
SECURE COMMUNICATIONS

Rethink Secure Communication

Next Generation Network
Access Technology

www.ncp-e.com

Next Level Remote Access VPN

Seit der Firmengründung im Jahr 1986 ist es erklärtes Ziel von NCP, Inbetriebnahme, Nutzung und Management eines Remote Access Netzwerkes für Unternehmen und Anwender so einfach und übersichtlich wie möglich zu gestalten.

Über die klassische Anbindung der Endgeräte von Mitarbeitern hinaus haben sich die Anforderungen natürlich stark gewandelt. Heute sind Unternehmen weltweit mit Standorten bis in die Produktion zu einzelnen Maschinen, Geräten und Sensoren vernetzt. Datenkommunikation ist längst nicht mehr nur ein Thema der Mitarbeiter.

Erfahrung und Kontinuität

- über 30 Jahre Remote Access-Kompetenz
- 100% in Privatbesitz
- Made in Germany
- bewährtes Partnernetzwerk
- OEM-Verträge mit der Deutschen Telekom AG, Lancom, WatchGuard, Sophos, bintec elmeg und vielen anderen
- weltweit mehr als 35.000 Kunden

Branchenkompetenz – Zu unseren Kunden zählen

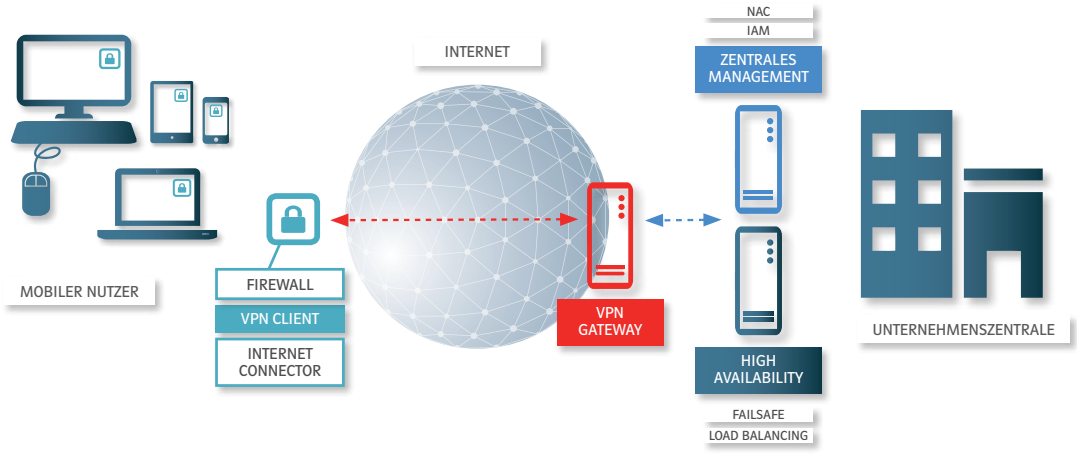
- Finanzdienstleister
- Banken und Versicherungen
- Fertigungsindustrie
- Einzelhandel
- Regierungsstellen
- Gesundheitsdienstleister
- Bildungs- und Forschungseinrichtungen
- Provider und OEM-Partner

Innovationskraft

- Anbieter des ersten zentral gemanagten VPN Clients für iOS
- patentierte VPN Path Finder Technologie
- erste Lösung für einfaches, transparentes VPN Management
- einzigartige intelligente Firewall in den VPN Clients

Ihre Vorteile

- hochskalierbare Software-Lösung
- Unterstützung aller marktgängigen Betriebssysteme
- kompatibel zu beliebigen IPsec VPN Gateways
- One Click Solution (für User und Administratoren)
- einfache Integration in vorhandene Infrastruktur
- integrierte zentral gemanagte Personal Firewall
- zentrales VPN-Management (Single Point of Administration) von mehr als 100.000 Usern
- zentrale Software Updates und Administration



„Insgesamt konnten unsere Kommunikationskosten im Ausland um den Faktor 10 gesenkt werden."

Peter Reichel, Max Bögl - Bauunternehmung GmbH & Co. KG

„Die entscheidenden Kaufgründe für die NCP-Software bestanden in skalierbarer Plattform, Bedienkomfort für Administratoren und Endanwender, die Nähe zu NCP, Unterstützung zahlreicher Betriebssysteme und Zertifikatslösungen. Die kurzen und direkten Kommunikationswege machen die fachlich fundierte Zusammenarbeit mit NCP sehr angenehm und wirkungsvoll."

Stefan Rech, Ratiodata GmbH

„Die GUI ist so intuitiv und einfach zu bedienen. Alle Informationen, die der Anwender benötigt, werden in einfachen Bildern dargestellt. Unsere Mitarbeiter benötigen kaum Schulung."

Daniel Torres, Hisco Inc.

VPN Management

Garant für den einfachen Betrieb eines VPN

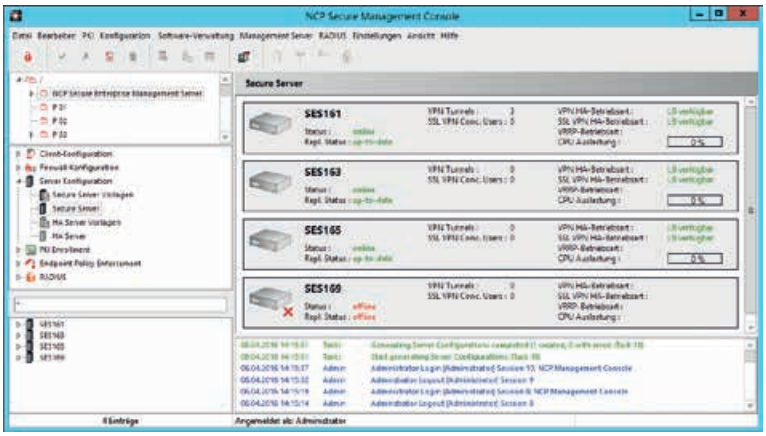
Mit dem Secure Enterprise Management (SEM) können Sie Ihr Remote Access-Netzwerk bequem von zentraler Stelle administrieren. So müssen sich Ihre Administratoren nicht mehr mit einer Vielzahl von Insellösungen und entsprechend vielen Konsolen herumschlagen. Das SEM fungiert als „Single Point of Administration".

Single Point of Administration

Alle erforderlichen Aktivitäten wie die Überprüfung der Einhaltung von Sicherheitsrichtlinien (Network Access Control NAC), Software und Konfigurationsupdates, Verwaltung von Usern, Lizenzen und Zertifikaten erfolgen automatisiert.

Ihre Vorteile mit dem NCP VPN Management:

- mehr als 100.000 externe Anwender/Systeme mit nur einem Administrator verwalten
- automatisierter Massen-Rollout
- zentrale Client/Server Konfiguration
- Zertifikatsmanagement
- Lizenzmanagement
- automatisierte Software Updates
- Integration in Benutzerverwaltung (LDAP, Active Directory etc.)
- umfassendes Monitoring und Berichtswesen
- kostengünstige Skalierung und Hochverfügbarkeit
- mandantenfähig
- Policy-Änderungen „On the Fly"
- integrierter RADIUS-Server
- Advanced Authentication



Mit dem Secure Enterprise Management von NCP jede Menge Zeit sparen

Die VPN Client Suite

Für Sie ist wichtig, dass eine VPN Client Suite alle gängigen Betriebssysteme und Endgeräte abdeckt und noch dazu komplett zentral über ein einziges Management System verwaltet werden kann?
Für uns stehen zusätzlich ein hoher Nutzenfaktor für Unternehmen und eine einfache Handhabung für Anwender im Fokus.

Daher umfasst die NCP Secure Enterprise Client Suite folgende Betriebssysteme:

- Windows 10, 8.x und 7
- macOS
- iOS
- Android
- Linux

Einfache Handhabung für Anwender durch einheitliche GUI

Alle Mitarbeiter-Devices auch in Umgebungen mit mehreren hundert oder tausend Benutzern von einer zentralen Stelle aus verwalten:

- reduziert den Aufwand für Administratoren
- schafft eine übersichtliche Infrastruktur
- spart Kosten ein

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: Home-Office, fremde Netze bei Kunden und Partnern oder öffentliche HotSpots und das Ganze auch im Ausland. Der NCP Secure 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 vertrauenswürdigen/bekannten Netz? Die Firewall-Regeln werden angepasst und der VPN-Tunnel entsprechend 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

Ihre Vorteile mit der NCP VPN Client Suite:

Sämtliche Module des NCP Secure Enterprise Clients lassen sich über das NCP Secure Enterprise Management zentral administrieren. Dadurch ist der VPN Client prädestiniert für den Einsatz in großen Umgebungen.

- IPv6-fähige dynamische Personal Firewall
- Friendly Net Detection
- Starke Authentisierung
- Multi-Zertifikatsunterstützung
- sichere HotSpot Anmeldung

- kompatibel zu beliebigen VPN Gateways (IPsec)
- Budget Manager zur Kostenüberwachung
- zentrales Management
- Custom Branding Option

- einfach zu bedienende Oberfläche (One Click)
- eigener Internet Connector mit integrierter Mobilfunk-Kartenunterstützung
- automatische, standortabhängige Anpassung der Firewall-Regeln durch den NCP VPN Client
- automatische Medienerkennung

- WLAN-Verwaltungstool
- Seamless Roaming: unterbrechungsfreies Arbeiten auch beim Wechsel des Übertragungsnetzes
- durchgängig stabile VPN-Verbindungen
- patentierte NCP Path Finder Technologie: Remote Access auch hinter Firewalls, deren Einstellungen einen IPsec-basierten Datenverkehr grundsätzlich verhindern

Das VPN Gateway

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

Starten Sie im kleinen Umfang und erweitern Sie die Leistungsfähigkeit „on-the-fly" – je System von 1 bis mehr als 10.000 User oder im High Availability (HA) -Verbund um das x-fache darüber hinaus.

Ihre Vorteile mit dem NCP VPN Gateway:

- softwarebasiert und mandantenfähig
- kompatibel mit gängigen IPsec VPN Gateways
- Verwaltung von mehr als 10.000 gleichzeitigen Sessions pro System
- Integration von IP-Routing und Firewall-Funktionalitäten
- universell einsetzbar z.B. für Filialvernetzung, Remote User und IIoT
- integrierte Zwei-Faktor-Authentifizierung
- 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 von iOS Endgeräten

Das NCP VPN Gateway ist die zentrale Plattform für die externe Datenkommunikation eines Unternehmens.

Virtuelle VPN Appliance

Der Virtual Secure Enterprise VPN Server 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 und macht weiteres Härten oder Sicherheitspatches unnötig. 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.

Sichere Datenkommunikation für Industrielle Umgebungen – IIoT / Industrie 4.0

Hochsichere Maschinen-Kommunikation

Industrie 4.0 bedeutet die Digitalisierung aller Prozesse entlang der gesamten Wertschöpfungskette von Bestellungen bis hin zur Produktion und die massive Vernetzung aller darin enthaltenen Akteure, sowie darüber hinaus die Verzahnung der klassischen Unternehmens-IT, wie z. B. ERP-Systeme mit den operationalen Netzen der Produktion, der sog. OT. NCP hat für die verschiedensten Industrie 4.0 bzw. Industrial Internet of Things (IIoT)-Szenarien Software-Komponenten für den sicheren Datenaustausch und deren Überwachung entwickelt.

Mehrwerte durch zentrale Komponenten

Das IIoT Remote Gateway kann flexibel, je nach Kundenanforderung, direkt auf Anlagen und Maschinen oder auf dafür vorgesehenen vorgeschalteten Hardwarekomponenten installiert und verwendet werden. Die dadurch verschlüsselten Maschinen-Daten, nimmt das zentrale IIoT Gateway vom IIoT Remote Gateway entgegen und übermittelt diese an weiterverarbeitende Systeme, wie Edge-Devices oder Cloud-Plattformen. Die dadurch sichergestellte Daten-Integrität und -Authentizität bildet die Grundlage für Themen, wie KI, Big Data oder Machine Learning, die allesamt auf eine korrekte Datenbasis angewiesen sind.

Über verschlüsselte Verbindungen sind IIoT Remote Gateway und das zentrale IIoT Gateway sicher miteinander vernetzt. Die sehr hohe Skalierbarkeit der Lösung, ermöglicht die komfortable und einfache Schaffung weitere verschlüsselter Tunnel zur Datenkommunikation, die bspw. dazu dienen, Live-Videostreams der Maschinen-Überwachung, in eine Leitzentrale zu übertragen. Auf diese Weise lassen sich die verschiedensten Anwendungsfälle klar trennen.

Mehrere NCP Komponenten an verschiedenen Stellen der Infrastruktur gewährleisten als Gesamtlösung die Kontrolle und sichere Datenverschlüsselung:

- ein zentrales **IIoT Gateway**
- ein **IIoT Remote Gateway** innerhalb der industriellen Infrastruktur, als NCP Software beispielsweise auf einer Anlage, Maschine oder einem System
- ein **IIoT Management** zur Verwaltung, Steuerung und Überwachung
- **virtuelle VPN Appliance** prädestiniert für die Anwendung in einer Cloud

Schutz der Produktion

Um einen adäquaten Schutz der Produktion zu gewährleisten, ist es essentiell Gruppen sogenannter „IIoT-Inseln" von logisch zusammenhängenden Maschinen und Anlagen zu bilden, die zentral verwaltet, sicherheitstechnisch gesteuert (ID-Management, Updates, etc.) und überwacht werden.

Durch diese „IIoT-Segmentierung" kann ein sehr hoher Schutz für die Produktion des Unternehmens etabliert und Angriffsvektoren eingegrenzt werden. Die klaren Mehrwerte sind neben einer sauberen Struktur, das Eindämmen von Cyberangriffen oder Incidents auf die jeweilige Insel. Somit wird der Vorfall isoliert und die Verbreitung etwaigen Schadcodes massiv eingeschränkt.

Die restliche Produktion ist davon unberührt. Dadurch fällt nicht nur ein möglicher Schaden geringer aus, sondern eine schnellere Wiederherstellung der Betroffenen Anlagen wird ermöglicht.

Ein zentrales Management, wie das IIoT Management ist daher zur Steuerung, Überwachung der Infrastruktur unerlässlich.

Sicherheit

Sämtliche Verbindungen zwischen den Endgeräten und dem IIoT Remote Gateway bzw. zwischen dem zentralen IIoT Gateway und dem IIoT Remote Gateway sind mit modernsten Algorithmen (z. B. Suite B Cryptography) verschlüsselt. Weitere Security Features sind zentral verwaltbare Maschinen-Zertifikate in einer Public Key Infrastructure (PKI). Dadurch wird eine eindeutige Authentifizierung aller Endgeräte gewährleistet. Die Gültigkeit von Zertifikaten wird bei jedem Verbindungsaufbau anhand von Sperrlisten offline oder online gegenüber der Certification Authority (CA) überprüft.

Usability und Wirtschaftlichkeit

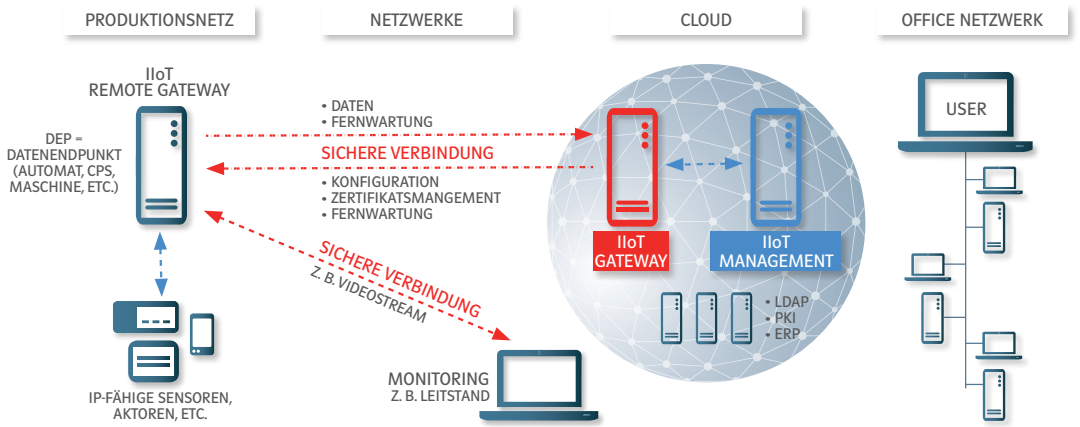
Die NCP Industrie 4.0 Lösungen lassen sich einfach in vorhandene Produktionsinfrastrukturen integrieren. Die Software ist, neben der Windows-Plattform, kompatibel zu vielen gängigen Linux-Distributionen. Konfiguration und Verwaltung der Komponenten erfolgen über das IIoT Management.

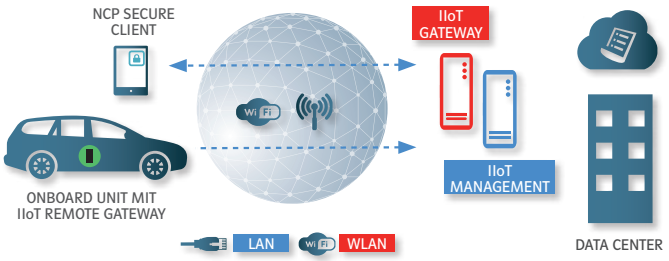
Mandantenfähigkeit

Dieses Feature prädestiniert das Management System für den Einsatz in Cloud-Umgebungen oder in Industrie 4.0-Strukturen, innerhalb derer mehrere Produktionsstandorte gemeinsam eine Plattform nutzen. Dies erfolgt durch Gruppenzuordnung und eine komfortable Rechtevergabe.

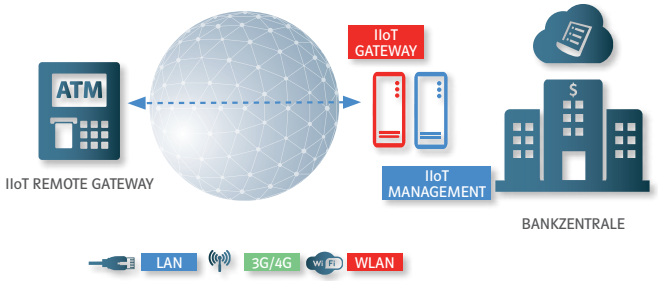
Die Administratoren werden so angelegt, dass jeder ausschließlich Zugriff auf seinen Produktionsstandort, sprich seine zu verwaltenden Einheiten hat. Ein Übergriff auf Daten anderer Zellen in deren geschützten Bereichen ist ausgeschlossen.

Übersicht einer IIoT Infrastruktur





Connected Cars – Flottensteuerung



ATM - Bankautomaten

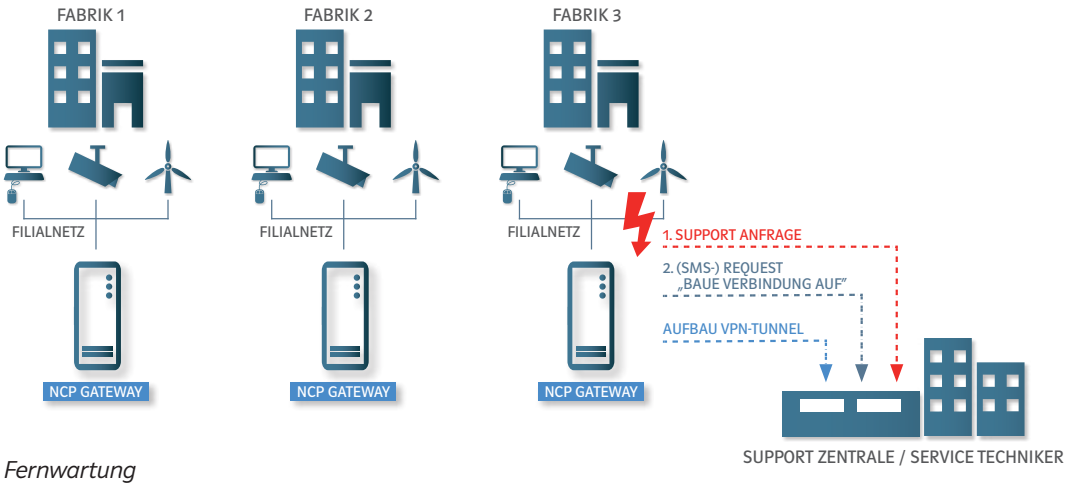
Fernwartung – gezielte sichere Ansprache einzelner Systeme

Zugänge zur Fernwartung von Maschinen und Systemen erfordern Flexibilität und Verfügbarkeit bei gleichzeitiger Sicherheit. Sowohl die Absicherung der Verbindungen selbst, als auch Schutzmaßnahmen vor möglicherweise kompromittierten Netzen und Endgeräten der Hersteller stehen im Fokus.

Identisch konfigurierte Netze stellen in der Fernwartung ein Problem bei der Identifizierung von Zielsystemen dar. Eine gezielte Ansprache bis hin zum richtigen Endpunkt ist mit den NCP Komponenten möglich und bereits technisch gelöst – durch eindeutige temporäre IP-Adressen und Authentisierungsmerkmale der Gateways und Clients (hardware- oder softwarebasiert).

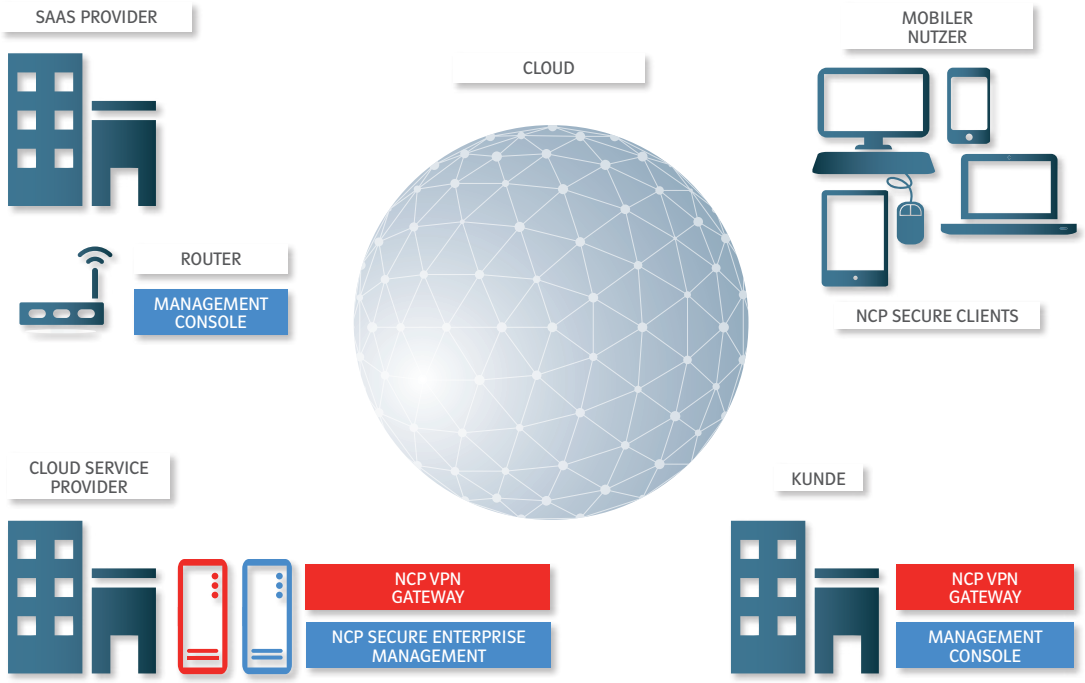
Grundlegend für eine Fernwartungslösung im hochautomatisierten Industrie4.0- / IIoT-Umfeld ist ein klares Konzept und eine Risikoabschätzung. Im Vorfeld muss geklärt werden, welche Maschinen, Anlagen und Steuerungen brauchen überhaupt externen Zugriff. Gerade die Sicherheit steht hier im Fokus und sollte von Beginn an höchste Priorität haben. Ein unerlaubter Zugriff kann negative Konsequenzen bis hin zum Totalausfall der gesamten Produktionsprozesse haben.

Weiterhin sollte bei der Fernwartungslösung nach dem Minimalprinzip vorgegangen werden. Hierbei ist die Granularität essentiell. Es muss sichergestellt werden, dass bspw. nur die betroffene authentifizierte Maschine, in einem definierten Zeitfenster, eine aktive verschlüsselte Verbindung zu genau dem autorisierten Fernwartungstechniker aufbaut. Das heißt der Verbindungsaufbau darf nur von Innen heraus aus Ihrem Produktionsnetz erfolgen. Der Fernwarter wird dabei immer und ausschließlich nur auf sein Zielsystem beschränkt.



Fernwartung

VPN „Out of the Cloud"



Sicherer Fernzugriff auf das Firmennetz aus der Cloud – „VPN as a Service"

Die Marktanforderung

Outsourcing des VPN-Betriebes und Managements an einen Dienstleister.

Die Lösung

Der Provider hat zwei Alternativen:

- vorhandene Ressourcen in der Cloud nutzen
- für Kunden eine eigene VPN-Infrastruktur aufbauen

Vorteile für den Kunden

- keine Investitionen in Hardware, Software und Expertenwissen im eigenen Haus nötig
- monatliche Kosten anstatt Einmal-investition mit jährlicher Abschreibung
- geringerer eigener Administrations-aufwand
- schnelle Implementierung

Vorteile für den SaaS-Provider

- langfristige Kundenbindung
- softwarebasierte, virtualisierbare VPN-Lösung
- Mandantenfähigkeit
- hohe Skalierbarkeit
- Single Point of Administration
- geringe Betriebskosten
- geringer Personalaufwand
- Sperren von Client-Parametern
- zentrales Management aller Clients über nur eine Konsole
- vollautomatischer Betrieb

NCP
SECURE COMMUNICATIONS

NCP engineering GmbH
Dombühler Str. 2 · 90449 Nürnberg
Tel: 0911-99 68-0 · Fax: 0911-99 68-2 99
E-Mail: info@ncp-e.com · www.ncp-e.com