NCP
SECURE COMMUNICATIONS

Rethink Secure Communication

Next Generation Network Access Technology

www.ncp-e.com

Next Level Remote Access VPN

Since the company was founded in 1986, NCP has been committed to making deploying, using and managing remote access networks as easy and clear as possible for companies and users.

Meanwhile the scope of remote access has evolved significantly beyond simply connecting employees end devices to the company network which now connects many different offices and locations right down to individual machines, devices and sensors in industrial production.

Expertise and continuity

- Over 30 years of remote access expertise
- 100% privately owned
- Security made in Germany
- Proven partner network
- OEM contracts with Deutsche Telekom AG, Lancom, WatchGuard, Sophos, bintec elmeg and many others
- More than 35,000 customers worldwide

Industry expertise

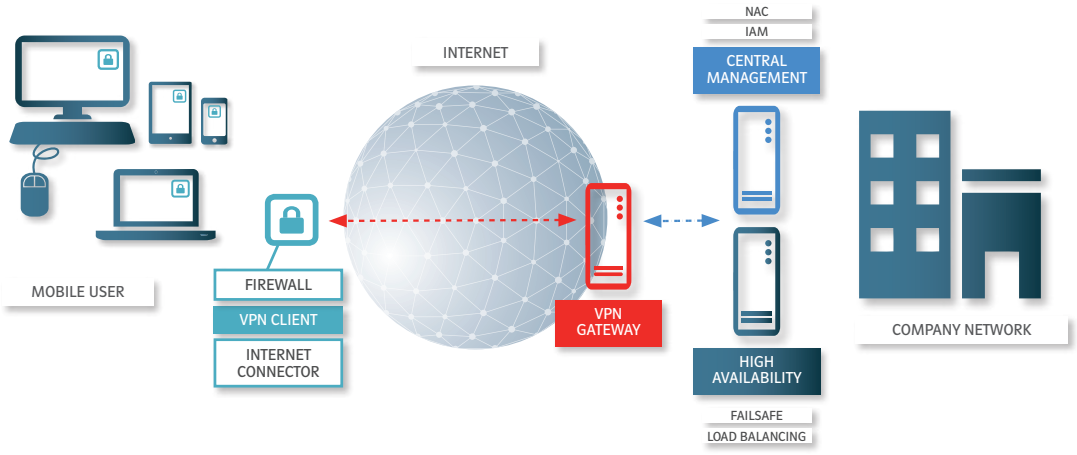
- Finance
- Banking and insurance
- Production
- Retail
- Public sector
- Healthcare
- Education and research
- Providers and OEM partners

Technology pioneer

- First centrally managed VPN client for iOS
- Patented VPN Path Finder technology
- First solution for simple, transparent VPN management
- Unique smart firewall in the VPN clients

Benefits

- Highly scalable software solution
- Support of all common operating systems
- Compatible with any IPsec VPN gateway
- One click solution (for users and administrators)
- Easy integration into existing infrastructure
- Centrally managed personal firewall
- Central VPN management (single point of administration) supporting more than 100,000 users
- Central software and license update



„Overall, our communication costs abroad could be reduced by a factor of ten"

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

„The key reasons for purchasing NCP software included a scalable platform, ease of use for administrators and end users, proximity to NCP, support for multiple operating systems, and certificate solutions. The short and direct communication channels make working with NCP experts pleasant and effective."

Stefan Rech, Ratiodata GmbH

„The GUI is intuitive and easy to use. All the information the user needs is displayed in a simple form. Our employees hardly need training."

Daniel Torres, Hisco Inc.

VPN Management

A safe bet for easily managing VPN

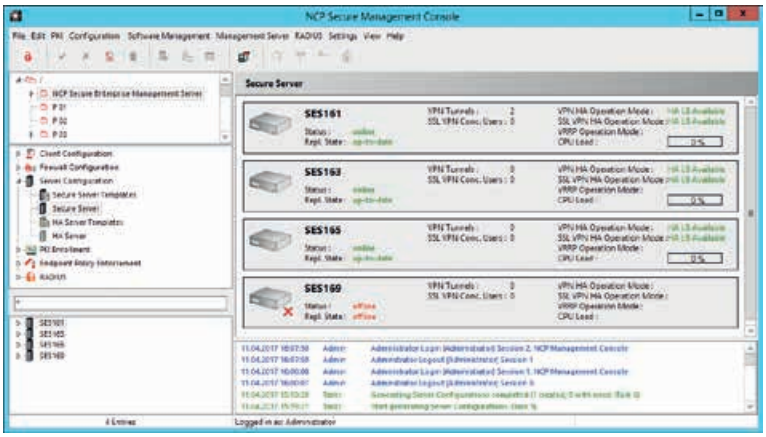
Secure Enterprise Management (SEM) means that companies can conveniently manage a remote access network from a central location. As a single point of administration, SEM means that administrators no longer have to battle with decentralized solutions and an array of management consoles.

Single point of administration

All important activities such as Network Access Control (NAC) compliance checks, software and configuration updates, user administration, licenses, and certificates, are automated.

Benefits of NCP VPN management:

- Manage more than 100,000 external users/devices with just one administrator
- Automated mass rollout
- Central client/server configuration
- Certificate management
- License management
- Automated software updates
- Granular monitoring and reporting
- Integration in user administration (LDAP, Active Directory etc.)
- Cost-effective scaling and high availability
- Multi-tenancy
- Dynamic policy changes
- Integrated RADIUS server
- Advanced authentication



Save time with NCP Secure Enterprise Management

Customers VPN Client Suite

Our clients want a VPN client suite which supports all major operating systems and end devices and which can be managed entirely through one central management system.

We are also committed to delivering a solution which generates a high return on investment for companies and is easy to use.

NCP Secure Enterprise Client Suite supports the following operating systems:

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

Easy to use with a standardized GUI

Manage all employee devices even in environments with several hundred or thousands of users from one central location:

- reduces the burden on administrators
- creates a clear infrastructure
- saves costs

VPN Client with smart firewall adapts to solve complex scenarios

There are many different scenarios and authorization levels for accessing company resources from external locations: Home offices, networks with customers and partners, public hotspots and international networks. The NCP Secure Client masters this challenge in a simple and secure way with several helpful features which are seamless for end users and do not risk being configured incorrectly:

- **Friendly Net Detection** – is a device connected to a public, unknown network or is it in a friendly, known network? The firewall rules are adjusted and the VPN tunnel is established accordingly
- **HotSpot-Logon** – this feature ensures that users always connect securely to a hotspot.
- **Home Zone Function** – the NCP Client's firewall is automatically configured so that users can use local network devices such as printers, but Internet access is only allowed through the VPN tunnel

Benefits of NCP VPN Client Suite:

All NCP Secure Enterprise Client modules can be managed centrally through NCP Secure Enterprise Management which is ideal for enterprise environments.

- IPv6-enabled dynamic personal firewall
- Friendly net detection
- Strong authentication
- Multi-certificate support
- Secure hotspot logon

- Compatibility with any IPsec VPN gateway
- Budget manager for cost control
- Central management
- Custom branding option

- Easy-to-use interface (One click)
- Internet connector with integrated 3G/4G support
- Automatic, location-dependent adaptation of the firewall rules by the NCP VPN Client
- Automatic media detection

- Wi-Fi management tool
- Seamless roaming: uninterrupted working even when switching network
- Consistently stable VPN connections
- Patented NCP Path Finder technology: Remote access behind firewalls which prevent IPsec-based traffic

VPN Gateway

The modular software architecture and high scalability of the NCP Secure Enterprise VPN Server (Gateway) enables companies to expand remote access networks and branch networks as required.

Start out small and boost performance dynamically when needed, from 1 to more than 10,000 users per system and even more through a High Availability (HA) cluster.

Benefits of NCP VPN Gateway:

- Software-based and multi-tenancy
- Compatible with any IPsec VPN gateway
- More than 10,000 simultaneous sessions per system
- IP routing and firewall features
- Universal solution for branch networks, remote users and IIoT
- Two-factor authentication
- High availability through failsafe and load balancing
- Dynamic policy changes
- NCP VPN Path Finder technology (Fall back IPsec/HTTPS)
- Network Access Control
- Endpoint security (with SEM)
- Certificate-based authentication of iOS devices

NCP VPN Gateway is the central platform for external remote access to the company network.

Virtual VPN Appliance

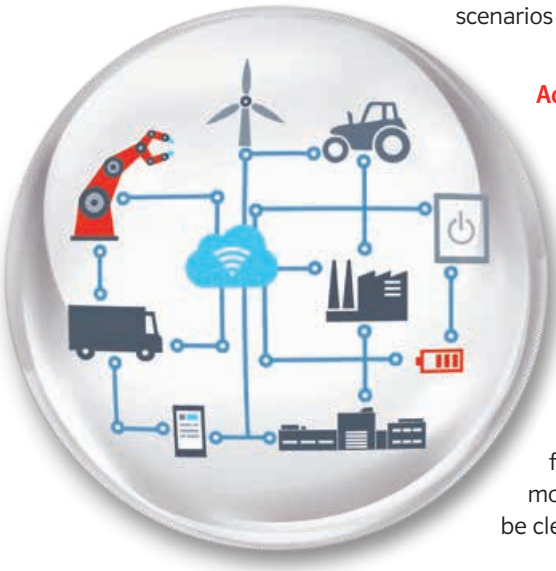
The Virtual Secure Enterprise VPN Server comprises the VPN Server, High Availability Services and a hardened operating system. It can be installed on a standard virtualization platform. As the operating system is already optimized for maximum security, this saves effort otherwise needed for developing hardening measures and applying security patches. Virtual Secure Enterprise VPN Server is designed for scalability and has a comprehensive update feature.

From the outset, this virtual appliance delivers a complete solution saving effort and reduces the need for in-house expertise.

Secure communication for industrial internet of things (IIoT) environments

Highly secure machine communication

IIoT entails the digitalization of all processes along the entire value chain from managing orders to production and networking all components at scale, including the integration of existing software such as ERP systems within the production network. NCP has developed software components for secure communication and monitoring security for diverse Internet of Things (IIoT) scenarios and industrial sectors.



Added value through central components

The IIoT remote gateway can be installed and used directly on systems, machines or dedicated upstream hardware components. The central IIoT Gateway receives the encrypted machine data from the IIoT Remote Gateway and transmits it to upstream systems such as edge devices or cloud platforms. This ensures data integrity and authenticity required for cutting-edge applications such as AI, Big Data or Machine Learning.

Encrypted connections ensure that the IIoT Remote Gateway and the central IIoT Gateway are linked securely. The high scalability of the solution ensures that additional encrypted tunnels can be set up for secure data communication, for example streaming live video to monitor machines from the control room. In this way, applications can be clearly separated.

Using several NCP components at strategic points in the infrastructure helps companies to gain control and encrypt data securely:

- a central **IIoT Gateway**
- an **IIoT Remote Gateway** within the industrial infrastructure installed on a machine or system
- **IIoT Management** for administration and monitoring
- **virtual VPN appliance** ideal for cloud applications

Protecting industrial systems

To protect industrial systems adequately, it is essential to form logical groups of connected machines and systems that are centrally managed, monitored and secured (ID management, updates, etc.).

Segmenting IIoT devices in this way can establish a very high level of security in industrial production and limit attack vectors. This is not only good organizational practice but also ensures that the implications of cyber attacks or other incidents are restricted to a specific network segment. This isolates any security incidents and massively limits the spread of any malicious code to other production systems.

This not only reduces the potential damage, but also means that affected systems can be recovered faster.

Central management, such as IIoT Management, is therefore indispensable for controlling and monitoring production infrastructure.

Security

All connections between the end devices and the IIoT remote gateway or the central IIoT gateway and the IIoT remote gateway are encrypted with advanced algorithms (for example using Suite B cryptography). For additional security, all machine certificates can be managed centrally in a public key infrastructure (PKI). This ensures unique authentication for all end devices.

Each time a connection is established, certificates are validated against Certification Authority (CA) revocation lists (online or offline).

Usability and cost effectiveness

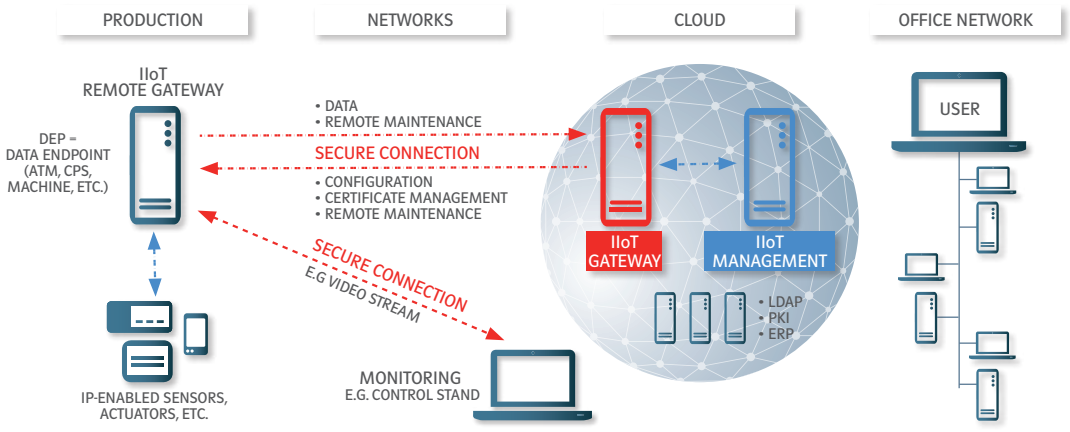
NCP IIoT solutions can be easily integrated into existing infrastructure. The software is compatible with Windows systems and many popular Linux distributions. IIoT Management is used for configuration and management.

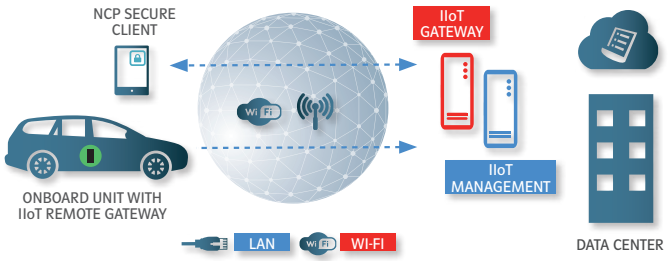
Multi-tenancy

This feature is ideal for cloud environments or in IIoT infrastructure, where multiple production sites share a platform. This is done using group assignment and a convenient rights management system.

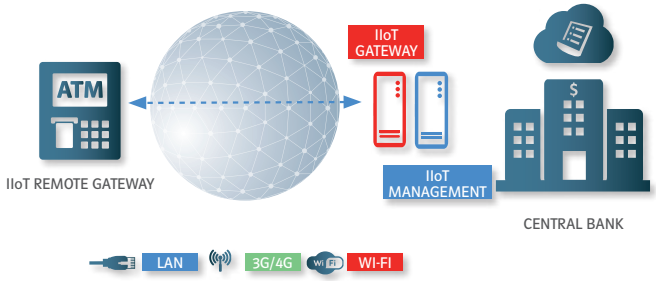
Administrators can only access the production sites they are assigned to. This means that data is kept secure and cannot be accessed from other protected areas.

IIoT infrastructure





Connected Cars – Fleet Management



ATMs

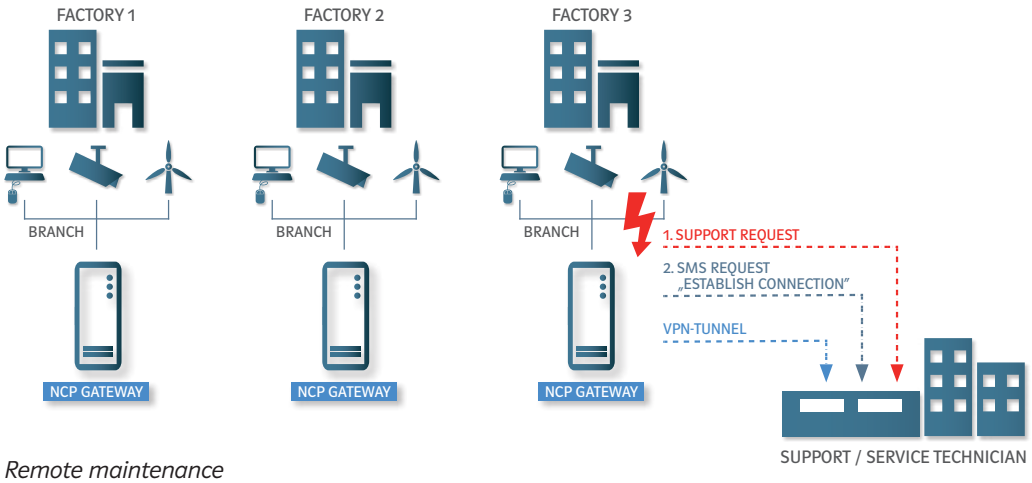
Secure remote maintenance for granular access to individual systems

Remote maintenance requires flexible, highly available and secure access to machines and systems. This includes securing connections as well as protective measures against potentially compromised networks and end devices.

During remote maintenance, identifying target systems can pose a challenge if networks are configured identically. The NCP components allow direct communication up to the correct destination through unique temporary IP addresses and authentication data of the gateways and clients (hardware or software-based).

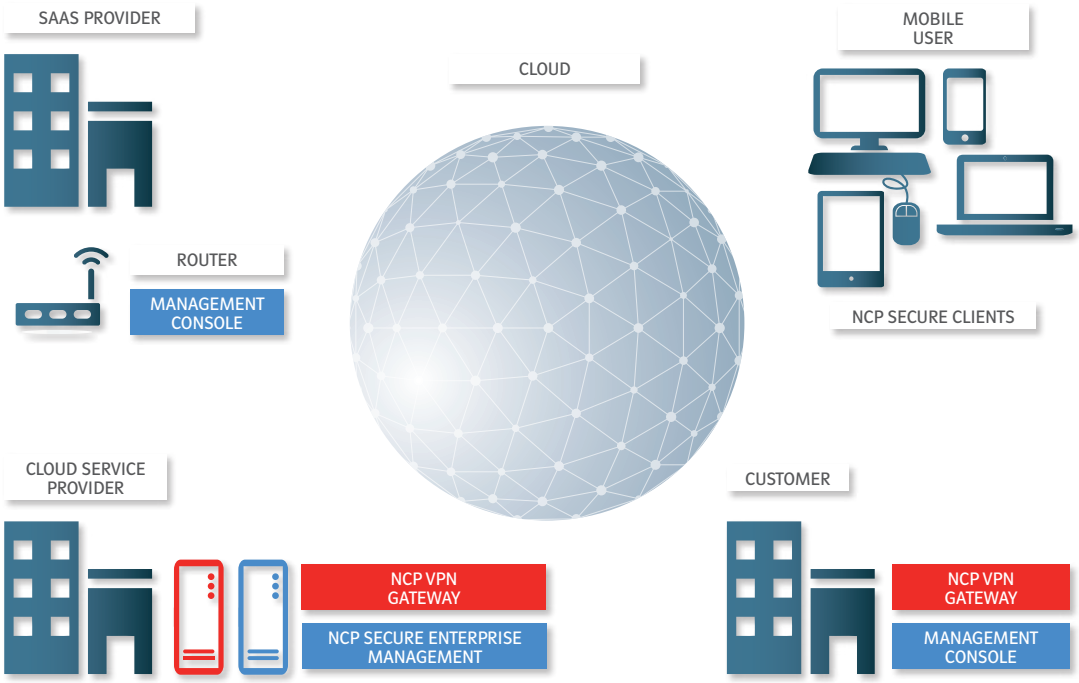
A clear remote maintenance concept and risk assessment are essential for remote maintenance solutions in the highly automated IIoT environment. It must be clarified in advance which machines, systems and controls need remote access at all. Security must have the highest priority right from the start. Unauthorized access can have negative consequences right up to catastrophic failure of the entire production process.

Remote maintenance should also be based on the principle of minimum privilege. Granularity is essential for a secure solution. For example, remote maintenance systems must ensure that only the affected, authenticated machine can establish an encrypted connection to the authorized service technician's system, meaning that connections must be established from inside the production network. Remote technicians are therefore only granted access to a specific system requiring maintenance at any given point in time.



Remote maintenance

VPN from the cloud



Secure remote access to the company network from the cloud – VPN as a Service

Scenario

Outsourcing VPN operation and management to a service provider.

Solution

The provider has two alternatives:

- Use existing resources in the cloud
- Develop their own VPN infrastructure for customers

Customer benefits

- No investment in hardware or software and expertise needed in-house
- Monthly costs instead of a one-off investment with annual depreciation
- Reduced in-house administration costs
- Fast implementation

Benefits for SaaS providers

- Long-term customer loyalty
- Software-based virtual VPN solution
- Multi-tenancy
- High scalability
- Single point of administration
- Lower operating costs
- Lower HR costs
- Lock client configuration
- Central management of all clients via a single console
- Completely automated

NCP
SECURE COMMUNICATIONS

NCP engineering, Inc.
678 Georgia Ave. · Sunnyvale, CA 94085
Phone: +1 (650) 316-6273
E-mail: sales@ncp-e.com

NCP engineering, Inc.
601 Cleveland Street · Suite 501-25
Clearwater, FL 33755
E-mail: sales@ncp-e.com

NCP engineering GmbH
Dombuehler Str. 2 · 90449 Nuremberg, Germany
Phone: +49 911 99 68 0
E-mail: info@ncp-e.com

www.ncp-e.com