SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

NCP
SECURE COMMUNICATIONS

Case Study

Remote Access for NRW

Remote Access for NRW

Working from home via the Internet in the state administration network in North Rhine-Westphalia

Reliable remote access is essential in ensuring that administrative processes run smoothly across an entire federal state at all times. IT.NRW now offers around 48,000 North Rhine-Westphalia state administration employees the opportunity to securely access resources they require to work, rather than it only being accessible in the office.

Using a multi-tenancy Virtual Private Network (VPN) solution from NCP, IT.NRW has set up a specially routed and protected network for its customers.

Only authorized individual users may communicate securely via this network and access the networks securely regardless of their location.

As an MSSP (Managed Security Service Provider), IT.NRW operates the central IT infrastructure on behalf of the Ministry of Economic Affairs, Innovation, Digitalization and Energy of the state of North Rhine-Westphalia.

Around 3,000 employees are involved in setting up and supporting the remote access environment for the state administration. The service can be used by all authorities and institutions in the state that are connected to the state administration network (LVN). Remote access provided through the LVN has become essential for making the state IT infrastructure flexible and productive in everyday operations as well as in times of crisis.

IT.NRW provides its services via the LVN – a network infrastructure divided into many subnetworks via which all authorities and institutions of the state administration of North Rhine-Westphalia can handle their data communication. Network nodes are distributed regionally in North Rhine-Westphalia and connected through high-speed connections to form this network. A personal, secure area is reserved for each LVN user and the data stream is controlled by individually configured communication relationships.

This ensures that data remains confidential within customer networks.

Highly secure with multi-tenancy support

Security and functional requirements were defined for implementing the remote access concept. These communication guidelines define the general conditions for the further development and operation of the communication infrastructure of the state administration and govern its use.

IT solutions in the field of state administration place high demands on the security and quality of all system components. IT.NRW sought a remote access solution that offers maximum security in its architecture and functions at both the client and service level. In a network with several thousand users, the usability and management of the remote access solution also played a decisive role. IT.NRW needed VPN software that is easy to use and connects to the network and its security infrastructure exclusively via a VPN tunnel. Furthermore, they needed to manage all communication and security parameters centrally.

In remote access implementations like that of IT.NRW, in which several customers share a VPN platform, multi-tenancy was also an important requirement. This means managing the requirements of different customers on the same server network, while keeping their data separate.

After evaluating various solutions, IT.NRW chose NCP engineering Inc. expertise to provide them their VPN solution.

One-click connection

NCP Secure Enterprise Client Suite enables access to the network for remote users from their end device. The NCP software connects the VPN tunnel with a single click and locally applies the personal firewall rules depending on the remote access environment.

Before users can gain access to the protected LVN, they must authenticate with multi-factor authentication involving possession and knowledge factors: Remote workers receive a smart card (possession factor) along with the VPN software. The key for virtual entry into the LVN is securely stored on the smart card. This key is authorized by entering an individual password (knowledge factor). After the user is authenticated, the VPN client sets up a VPN tunnel, which means that users can access all network applications and services from their remote workstation via the NCP Secure Client Suite, just like in the office.

A NCP Secure Enterprise VPN Server is installed for each customer and is the gateway for the VPN client connections. The IT.NRW data center houses a redundant VPN server systems and the NCP Secure Enterprise Management (SEM).

The VPN server handles the user authentication, termination of the VPN tunnel and forwarding the connection through further tunnels to customer networks.

The architecture of the VPN server is designed for high scalability and IT.NRW can adapt the number of tenants to current needs at any time. This flexibility has proven its worth, especially during the coronavirus pandemic: IT.NRW was able to quickly expand its services to the required extent and easily increase the remote access rate of the connected employees from around 50 to 100 percent. A special pandemic licensing system made it possible to add extra capacity and the technical implementation went smoothly thanks to the scalability of the NCP solution.

Convenience for IT administrators and remote workers

For IT administrators, a VPN rollout of this magnitude involves many activities that must be set up and monitored. These include managing the VPN gateway, central distribution and updating client software, digital soft- or hardware certificates, identity and rights management via the SEM console and checking endpoint security before accessing the LVN. All these activities can be managed centrally through a single console.
For example, complete groups and their user profiles can be updated with just a few clicks using a template. Each update is fully automated for customers. As soon as the remote workers connect to their network, a screen informs them about upcoming updates for their device.

The configuration parameters of the VPN Client Suite are created centrally in such a way that they cannot be bypassed or manipulated by the user. These parameter locks can be defined granularly and allow administrators to create precise access control lists. They also prevent users from unintentionally misconfiguring the VPN client.

Unnecessary menus and options are hidden, making the software easy to use for remote workers, who don't need to learn how to use different software interfaces.

IT.NRW flexibly aligns its range of services in accordance with the needs of its customers. During the initial installation, customers receive support with the installation of the client and server software as well as with the configuration of link profiles. Comprehensive training for IT administrators is also provided. IT.NRW also provides 2nd level support for the clients and the VPN servers of the customers and liaises with 3rd level support provided by NCP.

Meanwhile, IT.NRW serves 60 authorities with its remote access VPN solution, ranging from state ministries, district governments, prisons and environmental agencies to forestry authorities.

"The VPN servers are stable and the administration for currently 48,000 remote workers is almost completely automated thanks to NCP Secure Enterprise Management. The support effort for such a large number of users is relatively minimal," summarizes IT.NRW.

IT.NRW is currently working on the conversion of its VPN gateways from a fail-safe to a load balancing system to optimize the availability of the infrastructure in the long term. This spreads the data stream from the VPN clients evenly over several gateways, distributing the load of many simultaneous users effectively.

IT.NRW is already setting the course for a future with potentially higher numbers of remote access users and can guarantee reliable remote access options for the employees of the state administration at any time, even in the event of even greater use of VPN capacities.

> *"Thanks to NCP Secure Enterprise Management, the administration of the currently 48,000 remote accesses is almost completely automated."*
>
> ***IT.NRW***

Benefits of NCP solution:

- ☑ Software-based, (virtual) VPN solution
- ☑ Multi-tenancy
- ☑ Single point of administration
- ☑ Low operating costs
- ☑ Low personnel costs
- ☑ Low training costs
- ☑ Cost effective
- ☑ Minimal investment in hardware
- ☑ Software and expertise in-house
- ☑ Fast implementation
- ☑ Maximum scalability
- ☑ Mature technology
- ☑ Infrastructure with high availability and data security

About NCP engineering Inc.

NCP engineering Inc. develops software solutions for highly secure corporate communication via public networks and the Internet. NCP's expertise include remote access, IP routing, VPN and firewall technologies, identity and access management (IAM), network access control (NAC), strong authentication and integration of PKI infrastructures. NCP solutions deliver excellent usability, central management and compatibility, and can be easily integrated into existing IT infrastructures.

www.mey-agentur.de

NCP

SECURE COMMUNICATIONS

Do you have any questions or would you like to make an appointment for a product demonstration? Please contact us with any questions:

NCP engineering Inc.
Headquarters North America
1932 US Highway 19 N,
Suite 401
Clearwater, FL 33764

Phone: +1 650 316-6273
Fax: +1 650 251-4155
sales@ncp-e.com
www.ncp-e.com

We look forward to discussing how we can help you.