



SecurITy
made
in
Germany
Trust Seal
www.teletrust.de/itsmig

NCP
SECURE COMMUNICATIONS ■

Case Study

Remote Access für NRW



Remote Access für NRW

„Mobiles Arbeiten via Internet“ im Landesverwaltungsnetz Nordrhein-Westfalen

Um jederzeit reibungslose Verwaltungsabläufe für ein komplettes Bundesland sicherstellen zu können, ist eine verlässliche Remote-Anbindung der behördlichen Mitarbeiter unverzichtbar. Aus diesem Grund bietet der Landesbetrieb Information und Technik Nordrhein-Westfalen (IT.NRW) mittlerweile rund 48.000 Beschäftigten der Landesverwaltung in NRW die Möglichkeit, nicht nur vom stationären, sondern auch vom Remote-Arbeitsplatz sicher auf die dienstlich benötigten Informationen zuzugreifen. Durch den Einsatz einer mandantenfähigen Virtual-Private-Network-Lösung (VPN) von NCP wurde ein speziell geschaltetes und geschütztes Netzwerk aufgebaut. In diesem kommunizieren über personalisierte Zugänge ausschließlich die dort angeschlossenen Teilnehmer und erhalten auch aus dem Homeoffice oder von unterwegs aus sicheren Zugang zu ihrem jeweiligen Behördennetz.

IT.NRW vereint alle klassischen Funktionen eines MSSP-Dienstleisters (Managed Security Service Provider) und betreibt im Auftrag des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen die zentrale IT-Infrastruktur des Bundeslandes.

Rund 3.000 Mitarbeiter stellen alle Service-Leistungen zur Einrichtung und zum Support der Remote-Work-Umgebung der Landesverwaltung zur Verfügung. Diesen Service können alle Behörden und Einrichtungen des Landes in Anspruch nehmen, die an das Landesverwaltungsnetz (LVN) angeschlossen sind. Die damit einhergehenden Homeoffice-Möglichkeiten sind mittlerweile zu einem Grundpfeiler geworden, um die IT-Infrastruktur des Landes im Alltagsbetrieb wie auch in Krisenzeiten flexibel und lückenlos produktiv zu gestalten.

Seine Dienstleistungen stellt IT.NRW über das LVN bereit – zur Verfügung steht eine in viele Subnetze unterteilte Netzinfrastruktur, über die alle Behörden und Einrichtungen der Landesverwaltung Nordrhein-Westfalens ihre Datenkommunikation abwickeln können. Regional in Nordrhein-Westfalen verteilte Netzknoten, die über schnelle Leitungen miteinander verbunden sind, bilden die technische Basis. Für jeden LVN-Teilnehmer ist ein persönlicher, abgesicherter Bereich reserviert und der Datenfluss wird über individuell konfigurierte Kommunikationsbeziehungen geregelt. Damit ist Diskretion innerhalb des Kundennetzes garantiert.



Hochsicher und mandantenfähig

Für die Umsetzung des Betriebskonzeptes wurden sicherheitsrelevante und funktionale Anforderungen definiert. Diese Kommunikationsrichtlinien legen die Rahmenbedingungen für die Weiterentwicklung und den Betrieb der Kommunikationsinfrastruktur der Landesverwaltung fest und regeln deren Nutzung.

Der Einsatz von IT-Lösungen im Bereich der Landesverwaltung bedingt hohe Ansprüche an die Sicherheit und Qualität aller eingesetzten Systemkomponenten. IT.NRW suchte daher nach einer Remote-Access-Lösung, die es aufgrund ihrer Architektur und Funktionen sowohl server- als auch clientseitig ermöglicht, den Sicherheitslevel auf höchstem Niveau zu halten. Um dies in einem Netzwerk mit mehreren tausend Anwendern gewährleisten zu können, spielten auch die Bedienbarkeit und das Management der Remote Access-Lösung eine entscheidende Rolle. Vorgabe war es, dass der Umgang mit der VPN-Software für den Anwender einfach zu handhaben ist und die Verbindung zum Firmennetz und dessen Security-Infrastruktur ausschließlich über einen VPN-Tunnel erfolgen muss. Zudem sollten sämtliche Kommunikations- und Sicherheitsparameter in einer zentralen Managementkomponente zusammengefasst sein.

In Remote Access-Strukturen wie bei IT.NRW, in denen mehrere Kunden gemeinsam eine VPN-Plattform nutzen, war die Mandantenfähigkeit des Systems eine weitere Vorgabe. Die Lösung musste in der Lage sein, auf nur einem Server oder Software-System mehrere Kunden parallel zu bedienen und dabei die Datenströme strikt voneinander getrennt zu halten.

Nach der Evaluierung verschiedener Produkte entschied man sich für die VPN-Lösung der NCP engineering GmbH.



Mit nur einem Klick im Netz

Die NCP Secure Enterprise Client Suite kommt auf den Endgeräten der Remote-User zum Einsatz. Die NCP-Software erledigt durch einen einzigen Klick den Aufbau des VPN-Tunnels und - in Abhängigkeit von der jeweiligen Remote-Access-Umgebung - die Auswahl der richtigen Firewall-Regel.

Bevor die Benutzer Zugang in das geschützte LVN erhalten, müssen sie sich mit „Besitz und Wissen“ authentisieren: Dies erfolgt über eine SmartCard (Besitz), die diese Remote-Beschäftigten zusammen mit der VPN-Software erhalten. Auf dieser SmartCard ist der Schlüssel für den virtuellen Eintritt ins LVN sicher hinterlegt. Die Freigabe dieses Schlüssels erfolgt über die Eingabe eines individuellen Passworts (Wissen). Nach erfolgreicher Authentisierung baut der VPN-Client einen transparenten VPN-Tunnel auf, d. h., den Usern stehen am Remote-Arbeitsplatz über die NCP Secure Client Suite alle Netzwerkapplikationen und -funktionalitäten wie am Büro-Arbeitsplatz zur Verfügung.

Als Gegenstelle zu den VPN-Clients ist bei allen Kunden ein NCP Secure Enterprise VPN Server installiert. Im Rechenzentrum von IT.NRW befindet sich ein redundant ausgelegtes VPN-Server-System sowie das NCP Secure Enterprise Management (SEM). Der VPN-Server übernimmt die Überprüfung (Authentisierung) der VPN-Nutzer, die Terminierung des VPN-Tunnels sowie die Weiterleitung der Verbindung durch weitere Tunnel in die jeweiligen Kundennetzwerke. Die Architektur des VPN-Servers ist auf hohe Skalierbarkeit ausgelegt, so dass IT.NRW die Zahl der Mandanten jederzeit dem aktuellen Bedarf anpassen kann. Vor allem während der Corona-Krise hat sich diese Flexibilität bewährt: So konnte IT.NRW seine Services schnell im benötigten Maße ausbauen und die Remote-Access-Quote der angebundenen Mitarbeiter problemlos von rund 50 auf 100 Prozent steigern. Ein spezielles Pandemie-Lizenzsystem hat dabei die Rahmenbedingungen für den Aufbau der zusätzlich benötigten Kapazitäten geschaffen, während die Umstellung auf technischer Seite aufgrund der Software-Skalierbarkeit der eingesetzten Lösung reibungslos vorstattenging.

Komfort für Administration und Remote-Worker

Für die Administration fallen bei einem VPN-Betrieb dieser Größenordnung viele Tätigkeiten an, die überwacht und angestoßen werden müssen. Dazu gehören die Verwaltung des VPN-Gateways, das zentrale Verteilen und Aktualisieren der Client-Software, das Management der Ausgabe für digitale Software- oder Hardwarezertifikate, die SEM-Konsole hinsichtlich Identitäts- und Rechte-Management sowie die Sicherheitsüberprüfung der Endgeräte (Endpoint Security) vor deren Zugriff auf das LVN. Über nur eine Konsole lassen sich sämtliche Tätigkeiten komfortabel steuern. So können beispielsweise komplette Gruppen beziehungsweise deren Benutzerprofile mithilfe eines Vorlagenkonzepts mit nur wenigen Klicks aktualisiert werden. Jedes Update läuft bei den Kunden vollautomatisch ab. Sobald sich die Remote-Beschäftigten mit ihren Zielnetzen verbinden, informiert ein zusätzliches Bildschirmfenster über anstehende Updates für den eingeloggten PC.

Die Konfigurations-Parameter der VPN Client Suite werden von zentraler Stelle so angelegt, dass sie von vom Anwender nicht umgehbar oder manipulierbar sind. Diese Parametersperren lassen sich granular definieren. Somit können präzise Zugriffsschutzlisten erstellt werden. Diese verhindern gleichzeitig eine gewollte oder ungewollte Fehlkonfiguration des VPN-Clients durch die User.

Für die Remote-Worker wurde die Bedienung dahingehend weiter vereinfacht, dass nicht relevante Menüs und Einstellungsmöglichkeiten ausgeblendet wurden und die User sich somit nicht mit unterschiedlichen Software-Oberflächen auseinandersetzen müssen.

IT.NRW richtet sein Dienstleistungsangebot flexibel an den Kundenbedürfnissen aus. Bei der Erstinstallation erhalten die Kunden Unterstützung bei der Installation der Client- und Server-Software sowie bei der Konfiguration der Linkprofile. Des Weiteren erfolgt eine umfassende Schulung der IT-Administratoren. IT.NRW bietet zusätzlich 2nd Level

Support für die Clients und die VPN-Server der Kunden und fungiert als Schnittstelle zum 3rd Level Support durch NCP.

Inzwischen bedient IT.NRW 60 Behörden mit ihrer Remote-Access-VPN-Lösung, angefangen von Landesministerien, Bezirksregierungen bis hin zu Justizvollzugsanstalten, Umweltämtern und Forstbehörden.

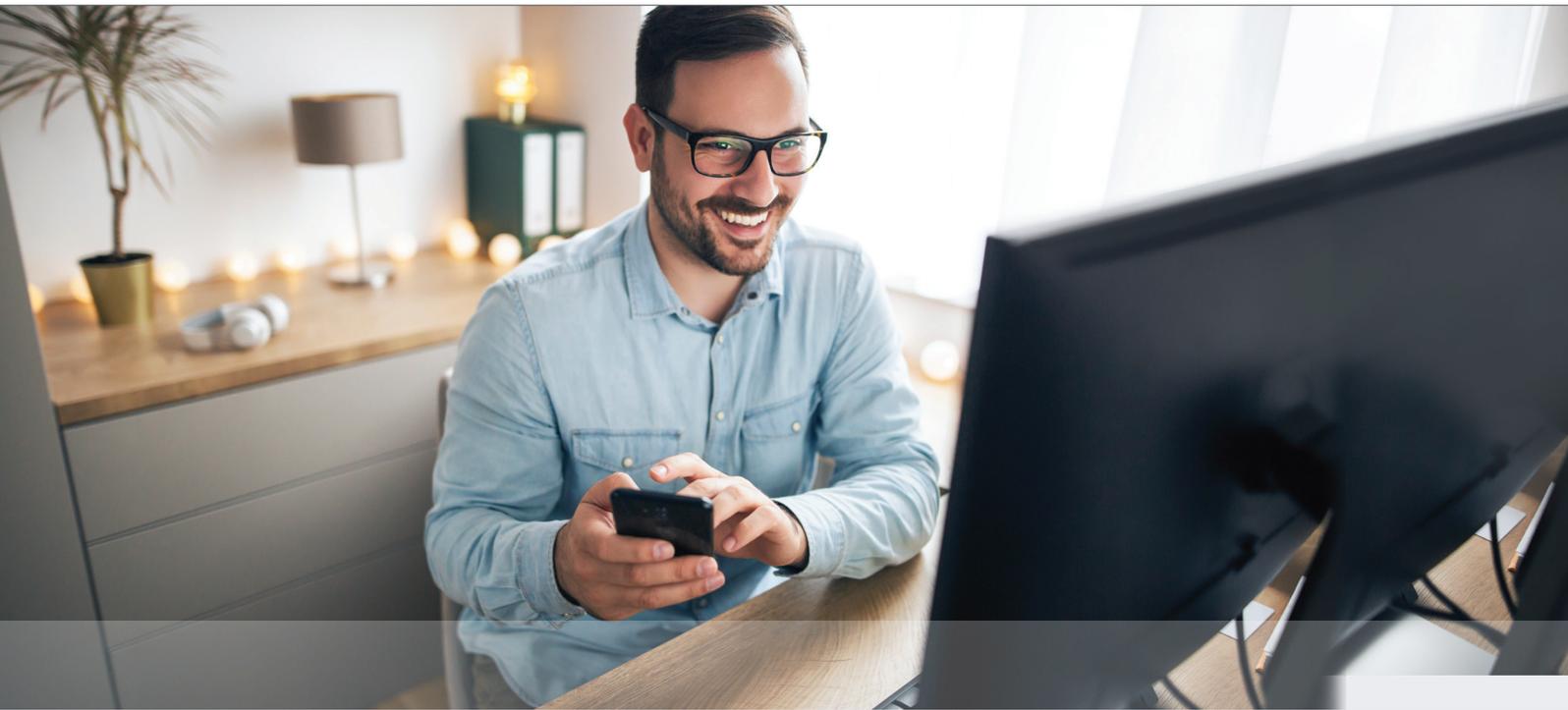
„Die VPN-Server laufen stabil und die Administration für die derzeit 48.000 fernangebundenen Mitarbeiter findet dank des NCP Secure Enterprise Managements nahezu vollautomatisch statt. Der Support-Aufwand für so eine große Anzahl an Usern ist im Verhältnis minimal“, resümiert IT.NRW.

Um die Verfügbarkeit der Infrastruktur auf langfristige Sicht weiter zu optimieren, arbeitet IT.NRW aktuell an der Umstellung seiner VPN-Gateways von einem Failsafe- auf ein Loadbalancing-Prinzip. Hierbei wird der Datenstrom der VPN-Clients gleichmäßig auf mehrere Gateways ausgebreitet, wodurch sich die Last vieler zeitgleicher Nutzer-Zugriffe besser verteilen lässt. Auf diese Weise stellt IT.NRW bereits heute die Weichen für eine Zukunft mit potenziell höheren Remote-Access-Nutzerzahlen und kann auch im Falle einer noch stärkeren Nutzung der VPN-Kapazitäten jederzeit verlässliche Fernzugriffsoptionen für die Mitarbeiter der Landesverwaltung garantieren.

„Die Administration der derzeit 48.000 Remote-Zugänge findet dank des NCP Secure Enterprise Managements nahezu vollautomatisch statt.“

IT.NRW





Die NCP-Vorteile auf einen Blick:

- ☑ softwarebasierte, virtualisierbare VPN-Lösung
- ☑ Mandantenfähigkeit
- ☑ Single Point of Administration
- ☑ geringe Betriebskosten
- ☑ geringer Personalaufwand
- ☑ geringer Schulungsaufwand
- ☑ preiswertes Angebot
- ☑ geringe Investitionen in Hardware, Software und Expertenwissen im eigenen Haus
- ☑ schnelle Implementierung
- ☑ hohe Skalierbarkeit
- ☑ ausgereifte Technologie
- ☑ Infrastruktur mit hoher Verfügbarkeit und Datensicherheit

Über NCP engineering, GmbH

Die NCP engineering GmbH ist Hersteller von Softwarelösungen für die hochsichere Unternehmenskommunikation über öffentliche Netze und das Internet. NCPs Kernkompetenzen liegen auf den Gebieten Remote Access, IP-Routing, VPN und Firewall Technologien, Identity und Access Management (IAM), Network Access Control (NAC) sowie Strong Authentication und Integration von PKI-Infrastrukturen. Einfache Bedienung, zentrales Management und Kompatibilität sind wesentliche Eigenschaften der NCP-Lösung. Die Integration in bereits bestehende IT-Infrastrukturen ist problemlos möglich.



NCP

SECURE COMMUNICATIONS ■

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 das Gespräch!