Case Study

RATIODATA

REMOTE ACCESS AS A FULL MANAGED SERVICE – RATIODATA SETS THE PACE

Even security services such as a virtual private network (VPN) can be outsourced into the cloud. Ratiodata, IT partner of the cooperative finance group FinanzGruppe and wholly owned subsidiary of Fiducia & GAD IT AG, has specialized in this area for a number of years and has considerable expertise in the finance sector. Ratiodata currently employs around 1200 people at twelve locations and offices throughout Germany.

The company the complex legal and compliance requirements specific to the banking and finance sector. It is one of the largest banking IT providers and market leader for manufacturer-independent services in Germany.

Ratiodata's portfolio of products and services includes management and nationwide services for stationary and mobile IT infrastructure, workstation equipment and network and security solutions.

Ratiodata offers its services to FinanzGruppe companies, financial service providers and other customers in banking and finance. Its current portfolio includes companies and banks in the DZ BANK Group and other clients of Fiducia & GAD IT AG.

Secure and highly available access

Ratiodata's Remote Access Service (RAS) offers customers secure and highly available access to internal networks and applications, regardless of an employee's access route and location. Through hardware or software security certificates for authenticating users and encrypting data, the RAS offers the highest level of security.

Multi-client capable remote access platform

Ratiodata (previously VR networks) started using NCP's IPsec VPN technology in 2000 with six NCP Secure Enterprise VPN Servers that provided remote access to about 7000 users. To date, the service has been expanded to 20 VPN servers that provide access for 28,000 users to the network from external locations in Germany and worldwide.

NCP's remote access solution has made it possible to implement these requirements for various devices connected to the Internet via ISDN, GSM, GPRS, UMTS, modem, DSL and LAN. Further features of the remote access solution are certificate-based authentication (USB token, soft certificates, smart card) in a PKI (Entrust CA) and an IPSec VPN infrastructure with NCP Secure Enterprise Clients (Win32/64), NCP Secure Enterprise CE Client, several NCP Secure Enterprise VPN Servers, NCP Secure Enterprise Load Balancing Server and NCP Secure Enterprise Management..

Convincing solution approach

Ratiodata originally decided on NCP's solution thanks to the high scalability of the platform, the ease of use for administrators through centralized VPN management as well as broad compatibility with different platforms

and operating systems. Support for Linux, various Windows versions and MacOS was also an important factor that is only offered by a few providers.

Several unique features that are key to a complete package for security and remote access requirements also influenced the decision: The powerful integrated personal firewall for each endpoint, endpoint security checks, the integrated dialer to select the best connection method and the multilingual user interface for international clients.

Benefits:

- Multi-client capability
- High availability thorough load balancing server
- Powerful integrated personal firewall for all end devices
- Endpoint security checks
- Multilingual user interface
- Reduced effort for managing large installations
- Savings in training and support

Case Study

RATIODATA

In addition, the software had to support all connection media – Wi-Fi at hot spots, mobile 3G/4G access and direct support of GPRS/UMTS cards, including the reduction of data transfer through compression (which was crucial to reducing costs at the time).

Benefits

DNCP's experience using IPsec VPN technology ensured that all functional requirements of Ratiodata and its clients were met including the integration of digital certificates for a higher security level in user authentication. The solution has significantly reduced the effort of managing such a large installation. This allowed Ratiodata to benefit from significant savings in training and support for users and administrators.

The integrated personal firewall with support for advanced configuration options and user scenarios as well as the load balancing server for high availability of the system also contributed to savings as it avoided the need for extra security hardware.

Growing requirements – Hotspots, TrustSec, major incidents

The number of users has risen sharply since the platform was set up. Home office and access from other external locations has also expanded rapidly from just a few years ago, thanks to low cost and widespread public Wi-Fi. Ratiodata has taken this into account by expanding the gateway platform to 20 servers. In the process, the company also benefited from the considerable increase in performance of the NCP gateway software.

In hotels and other public spaces, Wi-Fi access with individual authentication has long replaced ISDN connections. The NCP solution supports hotspot logon through a separate browser with which opens the firewall for a short time. This means that customers can allow their employees to access Wi-Fi networks without modifying their own services, such as the browser configuration or proxy settings.

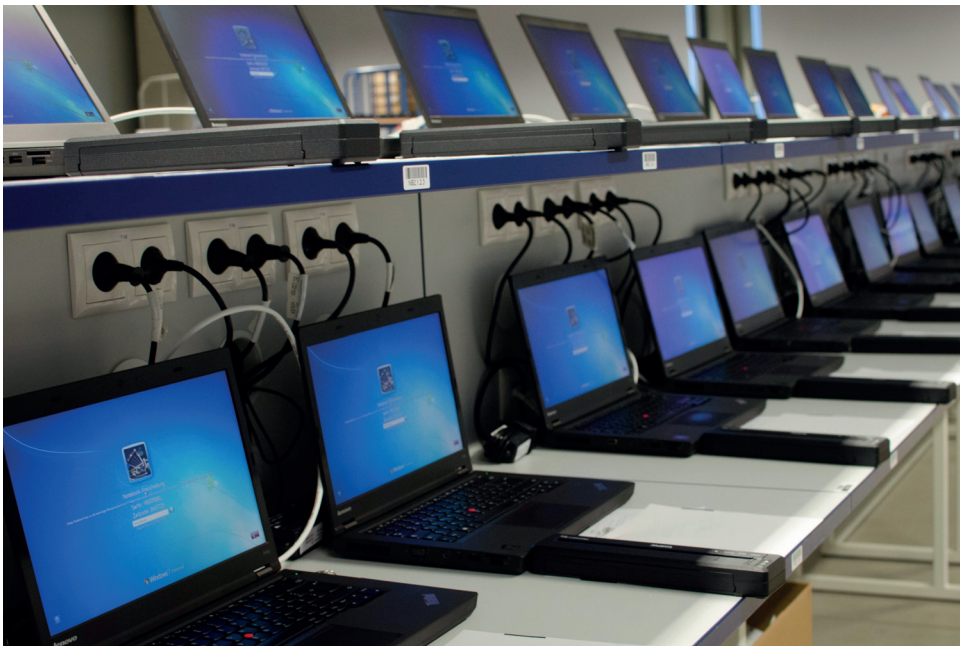
Even highly complex scenarios have been implemented elegantly with the NCP solution. This includes Cisco's TrustSec security tagging, in which the client is assigned to an address pool depending on Active Directory group membership, which is identified on entry to the network.

Security is also a concern when major incidents or pandemics occur. Swine flu and the f movement are examples of incidents that forced a considerable proportion of employees to work from home as RAS users. Flexible licensing options allow customers to do this in an emergency without having to procure a license for each potential user.

Service for different clients

At the beginning of each project, Stefan Rech from Ratiodata advises his customers to take a close look at the deployment environments of their employees and to think about possible usage scenarios. "It's not just about the number of users, it's about the environment in which they use their devices," says Rech. "Which media are used for the connection? Do commercial hotspots have to be integrated or are the employees traveling internationally? If so, we also need information on the mobile networks they will use abroad."

From the start, Ratiodata collects information on the decentralized infrastructure with the customer, for example the number of users as well as the type of end devices and operating systems in



Case Study

RATIODATA

use. Depending on the VPN solution, the operating systems and versions used must be compatible with the VPN clients.

In addition, information about the integration into the customer's directory and metadirectory structures is required, for example to assign remote access authorizations to individual users and groups for Active Directory integration. As a service provider, Ratiodata adapts to the needs of its customers in these administrative processes. Generally, data is imported from the Active Directory but HR software can also be integrated.

Stefan Rech speaks from experience: "We always try to automate as far as possible and tap into the master database. But whatever the technical solution, it must fit into the customer's environment. Smaller companies usually outsource the user administration, the larger ones want to do it themselves. They often have entire departments that take care of user administration."

The customer has a duty to cooperate and is responsible for their own data.

Even with later changes, customers have several options open to them to cover all eventualities. For example, if an employee leaves the company or a new employee is hired, data needs to be synchronized. In small installations, an email to the account manager or a standard change request form is often sufficient.

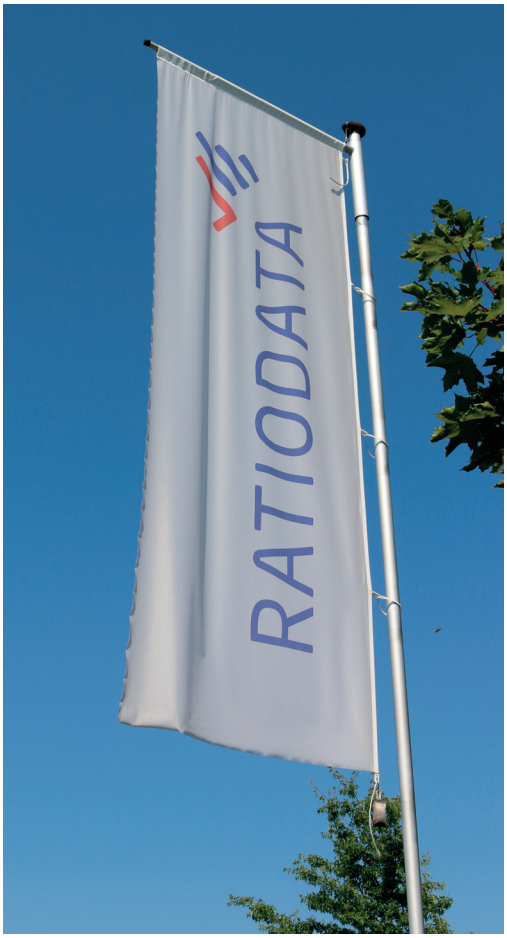
Through a fixed contact person, customers always have a duty to cooperate and cannot completely hand over responsibility to the service provider. From a legal perspective, the responsibility for the data remains with the company, which means the company must ensure that personal data is treated in accordance with the data protection regulations, even in cooperation with a service provider.

Technical balancing act in hosting various customers

At the start, distributing client software was a major task. Ratiodata uses the NCP Secure Enterprise VPN Server for its gateways, which includes software distribution through NCP Secure Enterprise Management (SEM). Experience has shown that distribution software via SEM is the preferred method. This allows administrators to define which group receives an update and the client is downloaded and installed the next time users in that group log on via a sufficiently fast network connection. The solution also works with any other solution.

When hosting many thousands of VPN connection, Ratiodata is faced with the challenge of meeting high load requirements. This is covered by scalability and load balancing in the overall solution. A management console that can handle multiple gateways as well as separate clients supports both the vendor's processes and the security needs of customers. Whether they accept a shared VPN gateway or require a separate solution is determined by the customer's security concept.

Due to its specialization in the financial sector and high regulatory compliance requirements, Ratiodata uses redundant gateways and network access for its solution. Stefan Rech explains: "We are ISO 27001 certified and host our solution via two redundantly connected data centers. This also benefits customers with lower availability needs." The VPN gateways are also redundant and connected via a high availability protocol so that they support load sharing.



Case Study

RATIODATA

About NCP engineering, Inc.

Since its inception in 1986, NCP engineering has delivered innovative software that allows enterprises to rethink their secure remote access, and overcome the complexities of creating, managing and maintaining network access for staff.

Headquartered in the San Francisco Bay Area, the company serves 35,000-plus customers worldwide throughout the healthcare, financial, education and government markets, as well as many Fortune 500 companies. NCP has established a network of national and regional technology, channel and OEM partners to serve its customers.

To learn more about NCP engineering, visit **www.ncp-e.com**. Reach the company on its blog, VPN Haus, or on Twitter at **@NCP_engineering**.must be compatible with the VPN clients.

Headquarters
NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
Germany
Phone: +49 911 9968-0
Fax: +49 911 9968-299
Email: sales@ncp-e.com

www.ncp-e.com

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