CASE STUDY

GERMAN FEDERAL EMPLOYMENT AGENCY IMPROVES MOBILE TELEWORKING VIA THE INTERNET

Employees of the German Federal Employment Agency (Bundesagentur für Arbeit - BA) are now able to connect to a central server of their agency when working remotely from a mobile workstation (MWS). Using top-notch remote access VPN technologies, they are now able to use all specialized applications. In the Virtual Private Network (VPN) tried and tested security mechanisms are responsible for the required confidentiality in the Wide Area Network (WAN).

Introducing a new remote access VPN solution in 2009, BA, wanted to optimize remote access via VPN for on-call duties, remote use of technology and teleworking. Apart from being able to access email programs and word processors, all employees should be able to access all of the agency's specialized IT processes which they have available at their regular workstation. With that, network access via the Internet replaced the formerly existing technical restriction of the communication mediums.

VIRTUALLY VIA THE INTERNET

The goal was to enable a large number of teleworkstations to use dial-up services which were free-of-charge, internet access points that were independent of any service provider and mobile services (like GPRS, 3G) - all of this tightly secured in an highly secure VPN. The use of the VPN technology has established as a default solution for remote access of mobile and stationary users to central resources. The VPN technology secures integrity (data cannot be changed during transmission), confidentiality (listening-in is impossible) and authentication of the data's source (confirmation that data is from the correct sender). Apart from its advantages in security, a VPN offers a high savings potential because its uses the internet as communication medium instead of expensive leased lines (or ISDN dial-up connections).

However, despite all the required security, the operation of the VPN is to be transparent for the user and the security mechanisms should not hamper the user in his or her work. BA selected NCP's solution because easy handling of the VPN software was a key requirement. Easy handling increases the users' acceptance and minimizes time and money spent on instruction and training. BA further required a scalable VPN platform and the security of mobile end-devices.

ONE CLICK NETWORK ACCESS

The selection of the supplier of the VPN solution was based upon a formal tender. BA assessed the suggested solution according to the agency's requirements and extensively tested the solution for its functionality.

After a successful test phase, developers created interfaces between the firewall and the VPN platform. They deployed the VPN platform in parallel to the existing system and with the help of automated installation scripts the users were able to decide on the time of the actual transition.

BA uses about 15,000 licenses of NCP engineering GmbH's remote access VPN software on its Windows-based mobile end-devices. NCP's VPN Client Suite is based on the IPsec standard and has a dialer of its own; it establishes

Aim:

- Future-proof, provider independent Internet access, dial-up services free of charge, mobile services (like GPRS, 3G)
- Easy and intuitive handling incl. possibilities of automatic dial-up medium recognition
- Scalability
- Security of platform and end-devices
- Managed service of remote access

the connection to the Internet Service Provider (ISP) and sets-up a tunnel to the VPN server. An integrated dynamical personal firewall protects the remote computer from attacks from the Internet and against other participants

of the local network. A BA employee only has to click once to trigger the whole connection setup process. The VPN client automatically selects the appropriate transmission medium via the Internet or 3G and sets up a VPN tunnel to the BA network. Depending on the rights of the BA teleworker, he or she has full access to all assigned and available BA applications.

SCALABLE SOLUTION - ACCORDING TO NEED

NCP's Secure Enterprise VPN server is the remote side to the VPN clients. The VPN server handles authentication of the VPN users, termination of the VPN tunnel and forwarding the connection through further tunnels to the BA network. The VPN server's architecture is designed to be scalable so that BA is able to adapt the number of supported users to the current need. NCP's Secure Enterprise Management (SEM) is a further component of the managed VPN platform. Through SEM, administrators can automatically push out new client configurations. As soon as the teleworker connects to the BA network, an additional window shows a pending update for this mobile workstation (MWS). All configuration parameter of the VPN client suite are created in the Management System in such a way that the user can neither bypass nor manipulate them.

As of 2010, the IT systems producer provides BA and its users a comprehensive, scalable remote access solution, tailored to their needs. The system is very stable and BA employees widely accepted it

German Federal Employment Agency - Section Information Technology

The IT section of the German federal employment agency is made up of the departments IT management, IT system house and pre-support.
IT system house is the operative IT service provider of BA. It is in charge of the whole data center structure for 1.800 connected properties. Operating over 160.000 networked PC workstations and the corresponding IT infrastructure (e.g. 11.400 servers, three central high availability data centers), the information technology section maintains one of Germany's most extensive IT environments and is constantly developing it.

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 30,000-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.

NCP
SECURE COMMUNICATIONS

NCP engineering, Inc.
678 Georgia Ave.
Sunnyvale, CA 94085

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