The essential elements of secure remote access

…without the management headaches

Contacts:

Fran Howarth
Quocirca Ltd
Tel +31 5691 1311
fran.howarth@quocirca.com

Bob Tarzey
Quocirca Ltd
Tel +44 1753 855794
bob.tarzey@quocirca.com

Virtual private networks (VPNs) are the technologies most widely used by organisations today in the provision of remote access to their networks for employees, business partners and suppliers. Of the VPNs available, IPSec (Internet Protocol Security) VPNs provide the most complete remote access solution, although they have traditionally been seen as costly and difficult to deploy. A new generation of IPSec VPNs, which can enable organisations to gain a centrally managed and high security remote access solution without the administrative burdens and overheads generally associated with IPSec VPN deployments, is now emerging.

- **Remote access is now a fact of life, but is not always easy to administer or manage.**
  Although VPN technologies have evolved as the solutions of choice for achieving remote access needs, SSL VPNs can be limited in their capabilities for achieving full remote access and IPSec VPNs have traditionally had large management and administrative overheads associated with them as they relied on the manual installation of software agents on each device under management.

- **Next-generation IPSec VPNs streamline the management headaches associated with deployments in large complex environments.**
  By providing centralised management capabilities, next-generation IPSec VPNs automate the processes associated with the administration, management and maintenance of VPNs through provision of one single point of administration.

- **IPSec VPN implementations can help organisations to improve their security procedures and achieve regulatory compliance objectives, such as data protection.**
  Market-leading IPSec VPNs are supplied with powerful personal firewalls that handle security settings, preventing users from tampering with the security controls that have been set. They also enable checks to be made on the security levels applied to each endpoint under management and can enforce that the correct security tools are deployed on each machine, according to set security policies.

- **Security is only as good as the weakest point.**
  As the number of technology systems in use in an organisation proliferates, including databases, enterprise directories, operating systems and devices that allow mobile networking, the ideal IPSec VPN solution should provide coverage for a wide range of systems and devices in use today—as well as extending coverage to new forms of technology as they emerge and come into everyday use.

- **Full logging and reporting capabilities help organisations to tie all actions to the identity of the user performing those actions to prevent data leakage.**
  By automating those processes involved in deploying, managing and maintaining IPSec VPNs, all events can be logged and suitable reports can be communicated to management and used for security audits—especially where strong authentication is used to tie the user of a device to their identity.

CONCLUSION: VPNs have emerged as the leading technology for achieving remote access, with IPSec as the leading choice for providing access to the full range of applications in use by organisations today. However, implementing IPSec VPNs in a large, complex environment has been viewed as an expensive management headache. The next generation of IPSec VPN technologies move towards solving this through centralised management, high levels of security and automation of all the processes involved. This makes them easier to manage and reduces the overall cost of ownership of such technology implementations dramatically.

Introduction

Location, location, location. Perhaps a hackneyed phrase, but location is a growing issue for organisations. Very little business today is conducted at one single office location and few businesses today serve just one isolated geographic location.

This is not the only driver behind the increased need that companies have for providing remote access to their core computer networks. Employees work remotely more often than they used to—from home, on business trips or whilst servicing customers in the field. Because most business today is conducted electronically, organisations are progressively opening up access to their networks to business partners to allow greater, more efficient collaboration, and access is also being provided, in some cases, to customers.

This can create headaches for those in charge of policing who accesses what—especially given that much of this traffic can be reliant on insecure communications channels, and the internet in particular. In today's highly regulated world, organisations are under considerable pressure to prove that no one has tampered with their computer networks or the data that they contain. In recent research conducted by Quocirca, 82% of 250 organisations surveyed cited data protection legislation as the most important regulation that their businesses faced—over two-and-a-half times more than for any other government or industry-specific legislation in existence.

The onus is on an organisation to provide highly secure remote access to its computer networks, including knowledge of who accesses what and when, over all communications channels and from every type of device. There are a wide variety of technology choices that companies can make, but not all are easy to manage—especially when scaling up to protect extremely large, complex and decentralised networks. This paper will describe the essential elements that organisations should consider when looking to achieve highly secure remote access capabilities.

Limitations of first-generation virtual private networks

In the not so distant past, the most common method for accessing networks remotely was by use of a dial-up connection, with users authenticated by a user name and password combination, or perhaps a one-time password from a security token. Organisations looking for secure connectivity within their organisations generally built their own private networks using dedicated communications lines, but this was often a very expensive undertaking.

Over time, the use of public communications networks, including the internet, has increased and these have become essential communications tools for business. To cater to the requirements of organisations needing to securely transfer sensitive data over public and private networks, the virtual private network (VPN) was developed and is now the leading technology used for achieving remote access.

A VPN is a virtual network that is built on top of existing communications networks and provides a secure communications mechanism for transmitting data and information between networks through use of a tunnelling protocol. This means that the data being transferred is encapsulated and hidden from public view in order to provide a secure path for data to travel over a public network. This provides a much less expensive option than leasing dedicated telephone lines and provides companies with several layers of protection, including ensuring the confidentiality, integrity and authentication of communications, as well as access control.

VPNs come in many flavours. The first to come onto the market deployed PPTP (point-to-point tunnelling protocol) or L2TP (layer 2 tunnelling protocol). However, IPSec (Internet Protocol Security) emerged in the 1990s as the frontrunner owing to its superior encryption capabilities. Because it was for some time the de facto standard, there is a large installed base of IPSec implementations worldwide, with the most common use being for office-to-office connections, such as a branch office connecting to headquarters, or for a small number of trusted users accessing the corporate network.

Traditionally, IPSec deployments have required that a software agent be installed on every end point connecting to the network and that administrators configure the settings for each device by visiting each device in the network. This made it costly and complicated to manage in many cases—especially in large, complex deployments. There were also concerns about the security of IPSec VPNs because, once a device is connected to the IPSec VPN, it was able to access the entire computer network and all files contained there. Therefore, a stolen or hijacked device, where the user managed to crack the access credentials for the VPN, had full, unfettered access to the main central network. An easier way was needed of restricting what users could access without the expense and hassle of configuring each device separately.

As more and more workers began to work remotely from the late 1990s on, and as organisations looked to open access to some applications to business partners, companies began looking for cheaper, more effective alternatives that would allow easy access, but for which the set-up burden was reduced. This led to the development of SSL (secure socket layer) VPNs, which require just a browser for access and can therefore be set up remotely. This makes them suitable for large numbers of remote workers and for casual or ad hoc access, for example, in an environment where people access through a shared kiosk or computer terminal.

However, SSL VPNs are primarily aimed at providing access to web-enabled applications since they cannot work with applications that use a binary object stack such as Java applets or ActiveX controls. These require that related objects work together and therefore cannot be used in isolation through a tunnel. For client-server applications such as Microsoft Outlook, which deploys a standard client that is not customised for each organisation, connectors must be deployed so that a user can reach the application. For other enterprise tools, such as customer relationship management systems, the problem is trickier as many organisations apply some level of customisation to such applications, meaning that a custom connector would have to be written, which is a more expensive option. As well as this, SSL VPNs cannot work with peer-to-peer applications such as VoIP, which are coming into much greater use in organisations as they allow phone costs to be slashed and for better centralisation of usage and auditing to be carried out.

Since SSL VPNs have so many limitations, they do not constitute a complete solution for remote access and the majority of organisations typically use a combination of the two VPN flavours. For providing web application access for remote employees and ad hoc access, many organisations choose SSL VPNs, but for network layer access that appears to users the same as if they were physically located in the office, with access to all the files and applications that they need, use of an IPSec VPN is the answer.

This still left the problem, with first-generation IPSec VPNs, of manual administrative and maintenance processes and a way had to be found to reduce the burdens associated with their deployment. This led technology vendors to develop a new breed of IPSec VPN, where all processes are automated and the creases ironed out. The diagrams and discussion below are intended to describe the essential elements that organisations should look for in the ideal next-generation IPSec VPN deployment.

The promise of next-generation IPSec VPNs

Figure 1: First-generation IPSec VPNs
© Quocirca 2008

Configurations
Software agents and updates
Certificates
Maintenance

Scales to around 100 users, using inflexible security configurations and lack of integrated certificate rollout mechanism

HQ

IPSec VPN server

Backend data stores

Communication via:
- Modem
- ISDN
- LAN
- WLAN (via external dialler, such as Microsoft RAS Dialler)
- 3G (via ISP dialler)

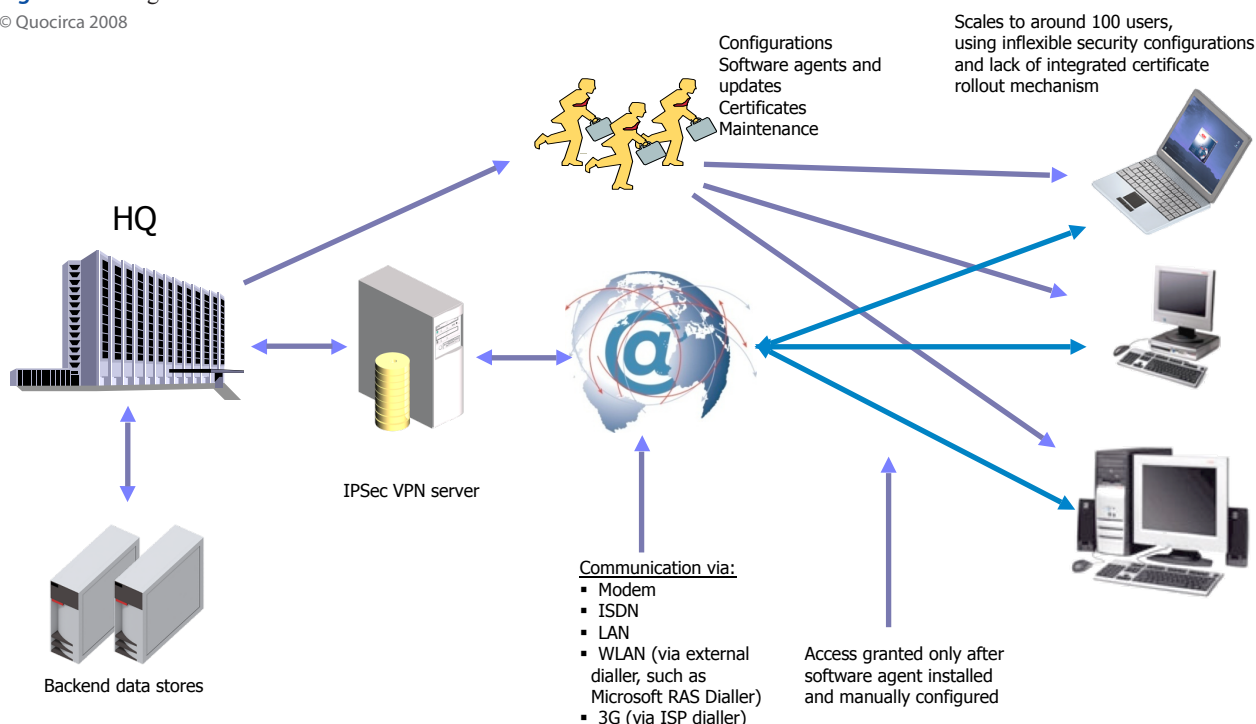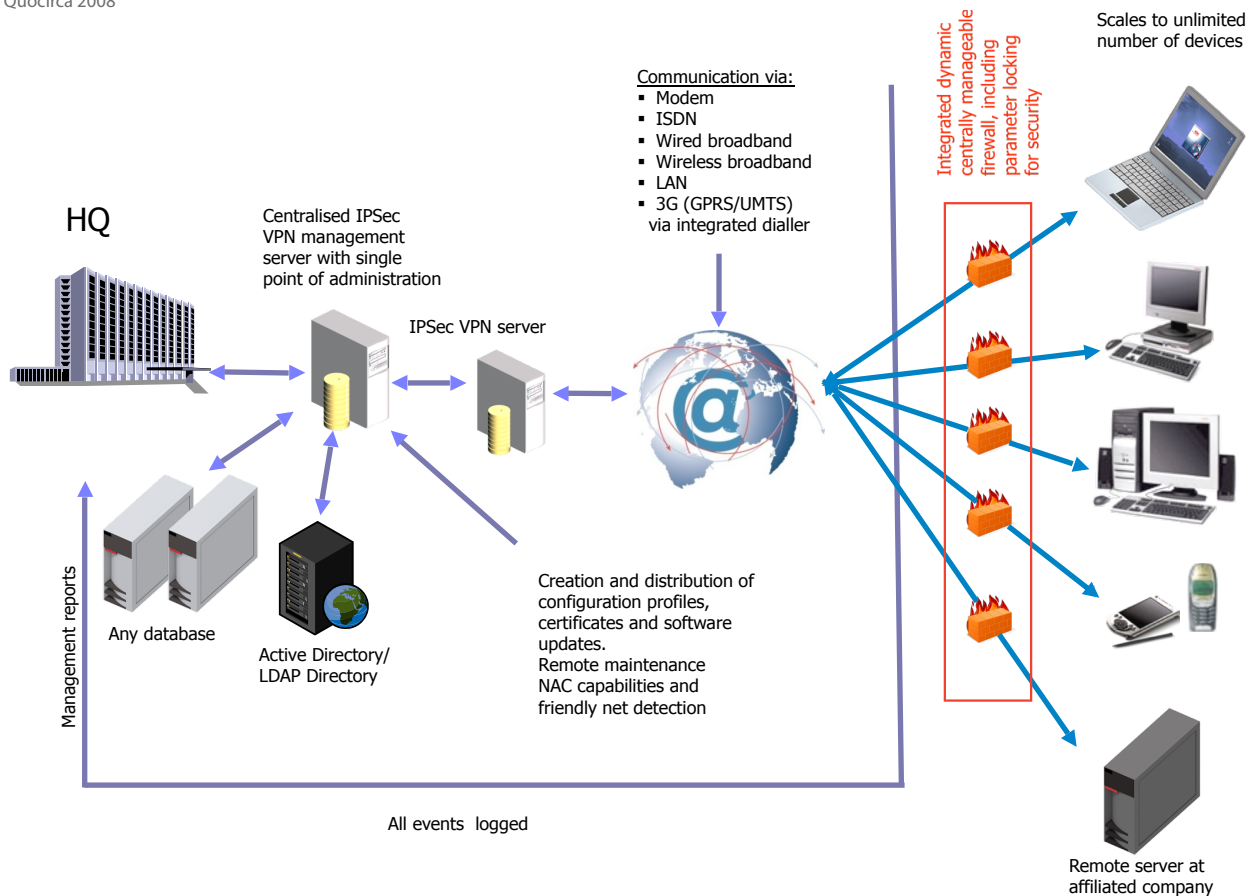Access granted only after software agent installed and manually configured

Figure 2: Next-generation IPSec VPNs
© Quocirca 2008

What to look for in the ideal IPSec VPN

Centralised management capabilities

The problems associated with traditional IPSec VPNs can now be a thing of the past. Instead, next-generation IPSec VPNs are now available on the market that have solved the management and administration headaches associated with the labour-intensive processes required for old-style IPSec VPNs. This is possible through provision of a centralised management server, which allows for the automated creation and distribution of software configurations, digital certificates, policies and software updates to all devices under management. Central to this is the provision of a powerful personal firewall through which all configurations are handled. This is an essential aspect of the solution as it is through the firewall that restrictions are set on what users can access through each particular device—without the ability to enforce such restrictions through use of access control lists, users would essentially still be able to access all resources on the network.

To create the configurations that are pushed out to all managed devices, the central management server should interface with databases and directories in use in the organisation in order to associate user identities with the access rights associated with each role in the organisation. Organisations should therefore look for a platform that supports a wide range of database and directory products to ensure that all such systems are included so that all applications can be accessed. Since operating systems are used for accessing those applications, companies should also look for broad operating system support—including support for Linux and Microsoft Vista, both 32 and 64-bit versions, and for operating systems used for mobile devices, such as Symbian and Windows Mobile.

An organisation needs to develop policies at a company level to determine what applications certain classes of users and devices may access. This has to be at a granular level, as the point, and means, of access may be just as important as the fact that the person is mobile. They should then look for a solution that provides good policy management and automated enforcement capabilities, along with rules for authentication and access levels associated with each class of application. To ease this process, templates should be available for the different roles in the organisation that can be customised according to need.

Authentication and access control

For tying user profiles with associated access rights, today's IPSec VPN solutions work with a centralised RADIUS (remote authentication dial-in user service) server that enables the remote access server to communicate with a central database shared among remote access servers. This is used to authenticate users requesting a service and works as a centralised administration service. This means that the central man-

agement server can also log all access attempts, making billing for each individual service possible as all authentication and access events are tied to the identity of the user requesting each service.

For an added layer of assurance that users are who they say they are and can only access the resources to which they have been assigned the rights to use, organisations should consider using strong authentication for tightening access and authentication controls. Any VPN platform chosen should natively support a wide range of authentication mechanisms, including soft and hard digital certificates through provision of public key infrastructure capabilities, and support for strong authentication tokens, such as smart cards, security tokens and biometrics. This means that it can also serve as a complete physical access control system by proving where the person was who logged on to the system, as well as providing virtual access control to the network.

Security controls

In order to ensure that the VPN system is secure, the included personal firewall should be capable of enforcing the endpoint security of all devices connecting to the system according to the policies set by the organisation. This should include network access control (NAC) capabilities to detect what applications are running, right down to the version of that application, as well as what security tools are in place, such as anti-virus software and personal firewalls on the device under control, according to policies. The VPN system should be able to block access or quarantine devices that do not conform to set policies, with the ability to push updates to devices not conforming to policy, or force them to collect an update from the central management server before they are allowed to access the network. Traditionally used for securing fixed line network connectivity, the proliferation of mobile devices used by organisations is leading VPN vendors to provide NAC capabilities for mobile devices to ensure that remote users can securely access the network via mobile phones and smart phones.

In order to ensure that the service is available should part of the network fail, organisations should investigate security services offered by the VPN vendor being considered, including the provision of high availability guarantees such as integrated replication services, and the provision of disaster recovery services.

Logging and reporting capabilities

To ensure that security policies are watertight and to provide evidence of how computer resources have been used for audit and regulatory compliance purposes, all network access should be logged and reported on so that usage patterns can de discerned and problems caused by unusual or suspicious behaviour can be flagged. Such capabilities not only allow organisations to report on all access attempts according to the identity of the user, but also allow the actions of administrators to be tracked in a complex environment. For example, since administrators are responsible for creating and making changes to configurations pushed out to users, all such actions should be logged and tied to the identity of each individual administrator. Leading IPSec VPN solutions allow different levels of administrator rights to be set, from super administrators who can delegate responsibilities to others, to administrators with limited management and administration rights in order to provide additional controls through segregation of duties.

Not only should logging and reporting capabilities be robust and mandatory for VPN systems, they should also provide additional benefits for the management of such solutions. For example, they can be used to automatically track which software licences are being used on each device in the network and to monitor the number of licences available to ensure that companies are not paying too much for licences that they are not using, helping them to control costs. Logging capabilities also allow for billing for services to be integrated into the management system.

Support for a wide range of communication methods

Because IPSec VPNs often use phone lines for gaining access to networks, the costs associated with access can be quite high, increasing the overall cost of ownership of such systems. In order to control those costs, the new generation of IPSec VPNs include an integrated dialler that is administrated by the central management system. By centrally configuring phonebooks with all available access methods, users can choose the type of connection that they wish to use, which can be a local area network (LAN), via a modem, or mobile communications networks. This means that users can choose free communications methods supported by IPSec, including free wireless LANs from public hotspots such as hotels and VoIP (voice over internet protocol) lines.

Case studies

MAN Nutzfahrzeuge

Background

Celebrating its 250th anniversary in 2008, MAN is a supplier of trucks, buses, diesel engines, turbo machinery and industrial services. It is a public company with revenues of €15.5 billion in 2007 that is headquartered in Munich in Germany and employs some 55,000 persons in 120 countries worldwide.

As a highly distributed organisation, covering offices, manufacturing plants, distributors and vehicle maintenance services, MAN was looking for a solution that could allow its facilities worldwide to access the applications residing on its corporate network in Munich.

Approach taken

MAN has been using remote access technology from German vendor NCP for more than ten years, having started using its dial-up product during the 1990s. As new products have been introduced, it has upgraded to the new technologies and now has some 6,600 remote workers using technology from NCP for accessing MAN's corporate network. It has taken a hybrid approach to remote access—using IPSec VPN technology for providing access to employees, SSL VPNs for contractors and ad hoc access where IPSec is not possible because the machines are not managed by NCP, and a secure shell (SSH) VPN for opening one tunnel as required to provide information on demand such as maintenance history and configurations for a truck being serviced in a remote manufacturing plant.

All of these technologies are managed through a central shared IT services facility, manned by just five employees, and contract partners where servers have been deployed in remote locations. Because of this, it is essential for MAN that the remote access solutions it uses can be easily configured and managed from one central location, with all updates pushed out at the click of a button. It has installed NCP's Secure Enterprise Solution at its headquarters in Munich, including integrated load balancing and NCP's secure VPN gateway.

For MAN, the choice of NCP's next-generation IPSec technology was an easy one to make as it is the only technology available that provides central management capabilities—vastly cutting down on the overheads connected with managing a large, complex network of users. For MAN, this includes providing access not only to its own employees, but also for those of affiliated companies. Therefore, it needed a solution that was easy to manage, not just for one company but also for many others associated with it via remote servers.

Benefits gained

The central management server configures access for users in a very granular fashion. For added security for affiliated companies being managed through the system, the tree structure configuration of the product means that different companies and users are separated from each other, so that one company cannot see the settings for another company being managed under the same system. The IT services team of MAN can then assign administrator rights for the other companies using the IPSec VPN technology to configure the system for their users—with administrator rights limited so that administrators can configure the software for their users, without the ability to change any of the security parameters set centrally by the super administrators at headquarters.

For MAN, it is vital that it is able to configure each device under management as required, pushing updates only to those devices that need them, right down to an individual machine level. The central management also allows MAN to bill for all new users for which the system is configured as well as only for those licences that are actually being used. With all other technology systems that MAN has evaluated, this required that all devices were brought into headquarters for configuration and for updates; with NCP's system, this can be done remotely in a fully automated fashion—without the end user even knowing that a change had been made.

Because it is such a geographically distributed organisation, MAN's employees use a variety of communications methods to connect to the central VPN server, ranging from analogue dial-up lines to 3G UMTS (universal mobile telecommunications service) broadband mobile connections. Therefore, not only is support for a wide range of communications protocols and devices vital for MAN, but a particular benefit of using NCP's technology is the provision of an integrated dialler, with optional international phonebooks for picking the most convenient connection. Since MAN has a subscription to iPass, which provides flat-rate pricing, this allows users to select cheaper services from iPass, where they are available, reducing the overall cost of ownership for the system.

Although MAN is a long-term customer of NCP, it surveys the market every year to evaluate the products offered by other VPN vendors, but it has so far found no other product that satisfies its needs. It has been unable to find another product that offers the breadth of functionality of NCP's technology, which it defines as being a suite of products. The particular differentiators that it sees in the technology are the centralised management capabilities, the integrated dialler, support for mobile connectivity, the powerful personal firewall that is built-in, and the intuitive graphical interface, which also helps service personnel in troubleshooting clients owing to the ease of use. In addition to this, MAN's IT personnel state that NCP is extremely supportive of their needs and have been open to working with MAN over the years to add extra functionality to the product as required.

VR Netze

Background

VR Netze is a subsidiary of GAD, which provides data processing and IT services for some 500 Volksbanken and Raiffeisenbanken (cooperative banks), as well as software development services for the Genossenschaftlicher Finanz-Verbund cooperative, and DZ Bank, the fourth largest bank in Germany. VR Netze provides telecommunications and network services, including managed data and voice network services, and secure remote access services to the GAD group and its 470 member banks, to the members of the DZ Bank group (R+V Versicherung, Union Investment, Reisebank and others), and other companies. For DZ Bank AG, VR Netze's services cover ten locations in Germany and five international branches. Since all business processes and the IT infrastructure for supporting DZ Bank AG's operations were centralised in Frankfurt in Germany, users from international branches in London, New York, Hong Kong and Singapore have accessed applications housed in Frankfurt via a wide area network.

The services offered by VR Netze to its clients are reliant on a very highly secure communications infrastructure for accessing the applications and services that it offers remotely. As part of this, it is essential that its clients can access those services over a range of channels, including those accessing the network over the local area network, via mobile devices, or for teleworkers working from flexible locations. It was also looking for a technology solution that would allow it to perform administration processes and maintenance of computer systems remotely.

Approach taken

VR Netze first started using IPSec VPN technology from NCP in 2000, deploying six secure enterprise VPN servers for providing remote access for approximately 8,000 users. Today, that implementation has expanded to 12 VPN servers for 20,000 users to access its network remotely from locations in Germany and worldwide. In addition to individual users, the VPN servers are used to connect many hundreds of bank branch offices, including control over the ATMs (automated teller machines) that are in operation at those branches.

According to VR Netze, the deciding factors in licensing IPSec VPN technology from NCP were the high levels of scalability of the platform, the ease with which administrators could manage and maintain the system through one centralised management system for all servers used, and the broad support for a wide range of platforms and operating systems. It required support for Windows XP and Vista operating systems, including the 64-bit versions—support for which it could find from few other vendors—as well as for Linux.

Other deciding factors in choosing NCP over the competition was that its technology provided an all-in-one solution for security and remote access requirements through the inclusion of a powerful personal firewall for each device, endpoint security checks, an integrated dialler for choosing the most effective communications channel for connection and the multilingual user interface for international clients. It was also looking for a product that supports all types of media currently in use, including WLAN access for those using the connections from hotspots, 3G mobile access and direct support of GPRS/UMTS cards—including the ability to decrease data volume transfer through compression, which is a significant cost factor when using GPRS/UMTS cards. It is looking to use NCP's support for the Symbian mobile operating system in the near future.

Benefits gained

VR Netze's experiences with using NCP's IPSec VPN technology is that it has fulfilled all of the functional requirements that VR Netze had defined, as well as those of its clients, including the integration of digital certificates for higher assurance of the identities of users. The technology has significantly reduced management and administrative headaches associated with managing such a large deployment. This has allowed it to make considerable savings in terms of training of users and administrators, and in supporting the deployment. Other savings have been in the form of not having to purchase additional security hardware owing to the high levels of security in the product itself, including the personal firewalls and the load balancing server for high availability that is included with the product.

Going forwards, VR Netze is looking to increase its investment by deploying additional IPSec VPN servers and increasing the number of sites and users that are covered by the technology. It is currently also testing NCP's SSL VPN technology for providing more ad hoc access to web-based applications for those users that do not need access to other applications on the network.

DATEV

Background

Formed in 1966, DATEV is a cooperative that develops software applications and provides IT services to tax consultants, auditors and lawyers—the majority of which are SMBs—as well as their clients. The cooperative currently has more than 39,000 members and achieved a turnover of €614 million in 2007, when it employed around 5,500 persons. DATEV has operated internationally since 2000, and now has 26 branches in Germany, an information office in Belgium, and associated companies in Poland, the Czech Republic, Austria, Hungary, Slovakia, Italy and Spain.

Included among its services is the processing of seven million payslips per month. About a further two million payroll statements are processed by tax consultants that are members of the cooperative, using software developed by DATEV. Other services offered include transferring contribution records and payment orders online to insurance companies or banks, and handling tax assessments and bank statements online. Overall, tax consultants that are members of the cooperative handle the financial accounts of some 2.4 million of Germany's medium-sized companies using software developed by DATEV.

Because DATEV produces so much mission-critical software for its customers, and transfers highly sensitive data to and from customers, it requires that the highest level of security possible be built into the processes that it uses. Its differentiator is that it guarantees constant reliability to its clients, including data protection assurances, owing not only to the highly sensitive nature of the information that is being transferred over DATEV's network, but also because such professional confidentiality is specified under the Tax Advisory Act. This means that DATEV would face legal consequences if any data fell into the wrong hands.

Approach taken

DATEV has been using IPSec VPN technology from NCP since 1995 in order to provide it with the level of security that it required for providing remote access for its employees to its network. Originally, it licensed NCP's VPN technology for ISDN connections but, as use of other communications methods and devices has grown, it has upgraded to NCP's secure enterprise management system in order to allow greater flexibility for its clients. Today, this is used to manage more than 2,000 IPSec VPN clients centrally from its headquarters in Germany.

One of the key elements in its decision to continue to use NCP's IPSec VPN technology is that the vendor adds support for new technology and devices as they are brought out onto the market, including the Microsoft Vista operating system, Windows Mobile operating systems versions 5 and 6, Linux, UMTS, WLAN and EDGE (enhanced data GSM environment). The use of mobile technologies is particularly important to DATEV, allowing more than 600 employees in consulting, sales and field service functions to access the network from home, when travelling or in a meeting. This has allowed it not only to save on travel costs and increase productivity but, compared to the ISDN dial-up connection previously used, has also resulted in telephone charges being halved—providing savings measured in six digits.

Benefits gained

DATEV has also seen benefits in using NCP's technology in terms of improved security. A key element is support for smart cards for authentication—a USB-based smart card for computer access and a micro SD card for mobile phones and PDA access. Use of such cards is mandated by DATEV for providing a higher level of strong authentication for complying with security requirements, including those of the Tax Advisory Act. The fact that security and policy enforcement is handled centrally is also appreciated by DATEV, as this prevents users from changing the configurations and parameters set centrally to bypass security controls put in place.

Going forwards, DATEV will look to expand its IPSec VPN implementation as required, particularly adding support for new technologies as they are introduced. It is also looking at expanding the use of SSL VPNs—but in the first case only for customers, and not for employees accessing the network, owing to the need for higher levels of security and application access for this group of users.

Conclusions

In today's business world, providing remote access to the corporate network is no longer a nice-to-have, it is essential for communicating and transacting with employees, business partners and customers for competitive advantage. For achieving this, VPN technologies have become the most widespread and viable solution. However, VPN products on the market, until recently, either provide only limited levels of access or are unwieldy and difficult to manage.

But IPSec VPNs, in particular, have come of age and can now provide highly secure remote access in a wide range of scenarios at a much lower overall cost in terms of administration, management and maintenance than first-generation products. As the case studies above indicate, organisations implementing such technologies are finding the solutions not only extremely valuable, but easy to manage. The headaches associated with managing large-scale IPSec VPN deployments are now a thing of the past.

About NCP

NCP engineering GmbH, headquartered in Nürnberg, Germany, is a provider of application and industry-neutral communication software for highly secure data transmission in public networks and the internet. Core competencies are in the areas of IP routing, central management of remote systems, as well as encryption, VPN and firewall technologies. Under the guiding principle of "Secure Communications" the firm develops products and solutions for the areas of mobile computing, teleworking, e-commerce, online banking, production data acquisition, system control (remote maintenance), and branch office networking. NCP product technology guarantees integration and compatibility with products from other manufacturers. NCP relies on collaboration with technology partners and OEM partners, and on sales via distributors and certified system houses for national and international marketing. Customers include companies, government agencies, and organisations.

Press contact
NCP engineering GmbH
Juergen Hoenig
Phone: +49 911/99 68 - 151
Fax: +49 911/99 68 - 299
E-mail: jhg@ncp-e.com

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry in the following key areas:

• Business process evolution and enablement

• Enterprise solutions and integration

• Business intelligence and reporting

• Communications, collaboration and mobility

• Infrastructure and IT systems management

• Systems security and end-point management

• Utility computing and delivery of IT as a service

• IT delivery channels and practices

• IT investment activity, behaviour and planning

• Public sector technology adoption and issues

• Integrated print management

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption—the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Sponsorship of specific studies by such organisations allows much of Quocirca's research to be placed into the public domain at no cost. Quocirca's reach is great—through a network of media partners, Quocirca publishes its research to a possible audience measured in the millions.

Quocirca's independent culture and the real-world experience of Quocirca's analysts ensure that our research and analysis is always objective, accurate, actionable and challenging.

Quocirca reports are freely available to everyone and may be requested via www.quocirca.com.

Contact:
Quocirca Ltd
Mountbatten House
Fairacres
Windsor
Berkshire
SL4 4LE
United Kingdom

Tel +44 1753 754 838

quocirca