

Planning and Design of a Virtual Private Network

Jörg Hirschmann

Today Virtual Private Networks (VPN) are an essential part of a secure IT policy. But a VPN must be well planned.

The starting point for the implementation of a VPN is the new organisation of business and decision-making processes as well as the decentralisation of work places. The issue is then to protect company data or even personal data from unauthorised third parties on the transmitting network and prevent third parties from accessing remote devices (hard drives, memories of PCs, Handheld PCs, Pocket PCs etc.) as well as the company network (backdoor attacks).



Jörg Hirschmann

Jörg Hirschmann (38) works for NCP Engineering GmbH in Nürnberg since 1994.

After finishing his German equivalent A-levels and an apprenticeship as an industrial salesman he was employed in the computing department of Schöller from 1989 to 1991. There he gained his first experiences in databases and with training of co-workers in the area of mainframe computer systems. In the next years he was active in the database branch before he became a remote access specialist for NCP in 1994.

Here he worked in different fields: support, consulting, system engineering and training, areas he now heads as technical director. Customers and sales partners equally value his technical know-how as well as his practical competence.



Important for mobile co-workers: Connecting to the company central may not become a science unto itself. Simplicity in the design is vital.

However “VPN is not always VPN” – there are different ways to commence with the realisation. In focus are integrated solutions opposed by isolated solutions, i.e. a universal VPN infrastructure for all external data transmission – including wireless LANs.

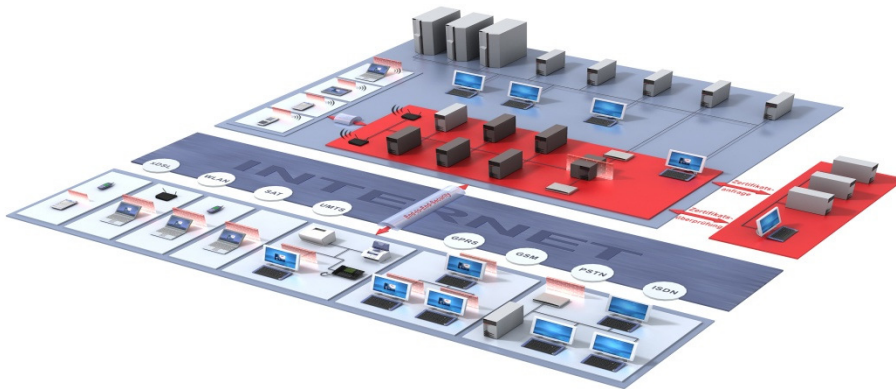
Alternative VPN Methods and Technologies

Today when one speaks of virtual private networks, one is referring to IP supported VPNs.

IP-VPNs are often equated with internet VPNs today, since these methods, are at this time, are the simplest and most inexpensive and therefore most widely used solution (named VPN in the following). Basically the traditional IP-VPN technologies are divided into layer 2 and layer 3 VPNs. Protocols such as L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunnelling Protocol) and PPTP (Point to Point Tunnelling Protocol) belong to the layer 2 VPNs. Layer 3 VPNs have IPsec as standard. These VPN technologies mentioned allow the establishment of end-to-site and site-to-site VPNs. Layer 2 VPN standards describe the tunnelling but not the encryption and authentication. As a result,

Checklist “Requirements of the Manufacturer”

- Which areas are the core competences in? Router (IP routing) or firewall (security) or communications and security? Hardware or software solutions? Branch networks over landlines or remote access and branch networks over public switch networks?
- Are the products subject to special export regulations?
- Where are the headquarters of the manufacturer? Where is the security solution programmed? Are parts of the security stored in national security agencies?
- How is the support being managed? Are there time differences and language barriers? In case of a problem is a short reaction time possible?
- What does it look like with individual software requirements? Does it “work as designed” or are there adjustments necessary which are defined by your needs?
- Are the security details based upon statements from the manufacturer or are there findings from external tests (independent institutions, companies with high security requirements)?
- Does the manufacturer have meaningful references? Large companies, middle-sized companies, agencies, MSSP (Managed Security Service Provider)



additional security protocols are used. Examples are EAP/MD5, EAP/TLS and L2sec. Layer 2 VPNs basically accept data from the most diverse protocols (IP, IPX, ATK, etc).

The current standard for the set up of IP-VPNs is the IPSec protocol. It sets specifications for tunnelling as well as security and accepts data based on IP. An IPSec VPN architecture is largely independent of the VPN components of different manufacturers. In addition to the technologies listed above, some manufacturers have brought combinations onto the market. An example of this are the Microsoft operating systems. These employ a process which fundamentally uses L2TP protected by IPSec (L2TP over IPSec).

Alternatives to the layer 2 and layer 3 processes have appeared in the last years which are not based on the traditional processes. The most well-known of these are the SSL-VPNs. In this technology the authentication and encryption takes place in the user level. Because of the partial dependence on the user level the SSL VPN technology consists of several different processes based on the SSL protocol. SSL VPNs can only be used in end-to-site connections (RAS) and require SSL compatible applications.

With IP-VPN technology the following kinds of VPNs can be set up :

- Remote Access VPN (Remote Dial In) : access of mobile and stationary co-workers into the company network.
- Branch Office VPN corresponds to the site-to-site VPN : data transmission between branch offices and the company central office.
- Intranet VPNs : Only co-workers of the company have access to the central data network.
- Extranet VPNs : Some co-workers and selected business partners have access to the central data network.

Planning

The decision to introduce a VPN solution is not an issue of momentary needs. Due to the rapid pace of technological development (GSM, GPRS, UMTS, HSDPA, WIMAX, DSL, WLAN, WAN-Hotspot etc.) the solution must keep an eye on the future as well. The purchase price of hardware and software should also not be the deciding point in the solution. Solutions which, at the start, have a relatively low price prove to generally be more expensive on a day to day basis. Hardware and software costs for the operation of a remote access system (planning time generally 3 years minimum) make up only 10% of the total costs. The lion's share of the costs go to personal and operating expenses. In larger remote access projects the rollout and operation of (possibly) thousands of computers often ends up to be more difficult than expected. During the planning phase it is not enough to have a few computers in a laboratory or to configure a few experienced users with which to collect empirical data for real time operation. In addition, it is advisable to visit companies of the same size and in the same branch and using the same alternative VPN solutions from different manufacturers in order to be able to assess suitability in a large scale operation.

The basic decision criteria for the selection of the right VPN solution are : the mode of work (mobile or stationary), the working environment (single user or networked PC in a LAN), the communication relationships (Dial In, Dial Out), the communication partners (human – machines, machines – machines) and the mode of operation (autonomous or over a provider – outsourcing).

Checklist Technology for VPN Planning

How is the usability of the client software formed? Easy to use? Does the client have an intuitive graphical user interface? Are special instructions necessary (training)?

Does the client possess all necessary security and communication mechanisms?

Integrated personal firewall, integrated support of mobile connect cards etc.

Is a comfortable domain login possible? Can the personal firewall be centrally managed?

Is the client compatible with VPN gateways of different manufacturers? Does it support all IPSec protocols, extensions (XAUTH, NAT-T...)?

How does the authentication with the central VPN take place?

Onetime password, certificate (software, smart cards, USB tokens, MMC cards)

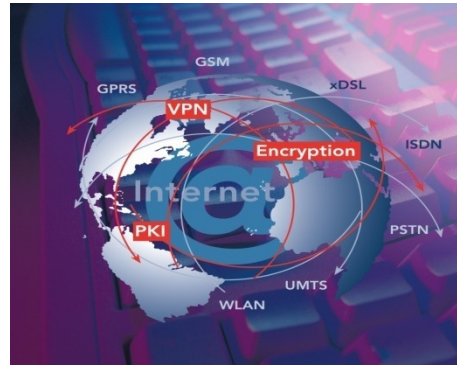
Can the end-to-end security principle be maintained at hotspots? (secure hotspot)

Can different company areas be displayed with the VPN solution – key word “mandatory ability” or “VPN gateway sharing”

Should the VPN gateway be modularly expandable and scalable (arbitrary tunnel development)

How does set-up, roll out and administration of the remote PCs and remote VPN gateways take place (single point of administration)? Are the computers in a central area or distributed on site? How does the set up of individual users take place? Is management possible from a single console? Can all of the configuration parameters of a user be blocked in order to prevent operating errors on site? How are claims, distribution and administration of certificates managed? How is the client software updated? Is endpoint security needed or desired?

What kind of VPN components should be installed: hardware (appliance) or software (standard PC)?



User Authentication

In VPNs it is not sufficient to gain access to a company network with just a user name and a password. State of the art methods of authentication are onetime password tokens, certificates as soft certificates, on smart cards or other form factors such as multi media cards (MMC) with cryptochips. Important here is the transparent integration of arbitrarily powerful authentication mechanisms in the VPN components.

High Availability Services

High demands are set upon the availability of central communication components in remote access projects. The access to databases and resources must be guaranteed uninterrupted round-the-clock, 365 days a year. A VPN solution should possess High Availability Services in order to guarantee the highest degree of availability and reliability.

Management

Next to performance, scalability and security in all their different facets, the ability to administrate is one of the most important selection criteria of a remote access VPN. Missing updates of the components, insufficient permission management or missing an update of a key all make a securely designed system no longer secure. All remote components (clients and gateways) must be administrated and monitored. Setting up, operation and

deleting users must be performed from a single console. The problem of VPN management is complex. It reaches from the automatic roll out of client software, over the software distribution, the remote help desk, the administration of certificates and endpoint security. Every access to the company network must be able to be security-related tested. This includes a graphically arranged preparation of all recorded data for the administrators. Further requirements of a VPN management tool are : Administration of clients of different operating systems (Linux, Windows, XP/2000/CE...), remote management over WAN connections (DSL, ISDN, analogue), scalability and mandatory functionality (e.g. strict possibilities for the separation of different business departments).

Conclusion

Security solutions on the basis of VPN technology must be able to be measured whether they really offer a universal barrier of all peripheral and central components and systems in all remote access environments. The construction of a company-wide security architecture is a continual process. Adjusting to a change in needs or the immediate reaction to a new danger must be possible using the new security solution. Above all a VPN solution must be able to be superimposed on an existing IT infrastructure and thereby protect underlying investments.

General Checklist for Planning a VPN

- In order to find the optimal solution in the market different questions must be answered.
- How many co-workers are to work with the system mobile or stationary? (effect on the development of the central VPN gateway (number of simultaneous connections – tunnel)
- From which locations is the company network to be accessed? Local / regional / national / international (effect on the transmission network)
- Which remote devices are to be used? Desktop PCs / laptops / notebooks / thin clients / Pocket PCs / Handheld PCs / Tablet PC (effect on support operating systems of the VPN clients)
- Which applications will be used on the remote computer? (effect on the efficiency of the remote device and the kind of transmission medium)
- Do your teleworking employees alternate? Is work divided between office and home or mobile? (effect on the scope of services of the VPN client)
- Which security level is necessary? Dependent on the data transmitted and the security policy (effect on the type of user authentication)
- Can central IT components such as user-defined databases, RADIUS directory service, etc. be used? Support of standards (compatibility)