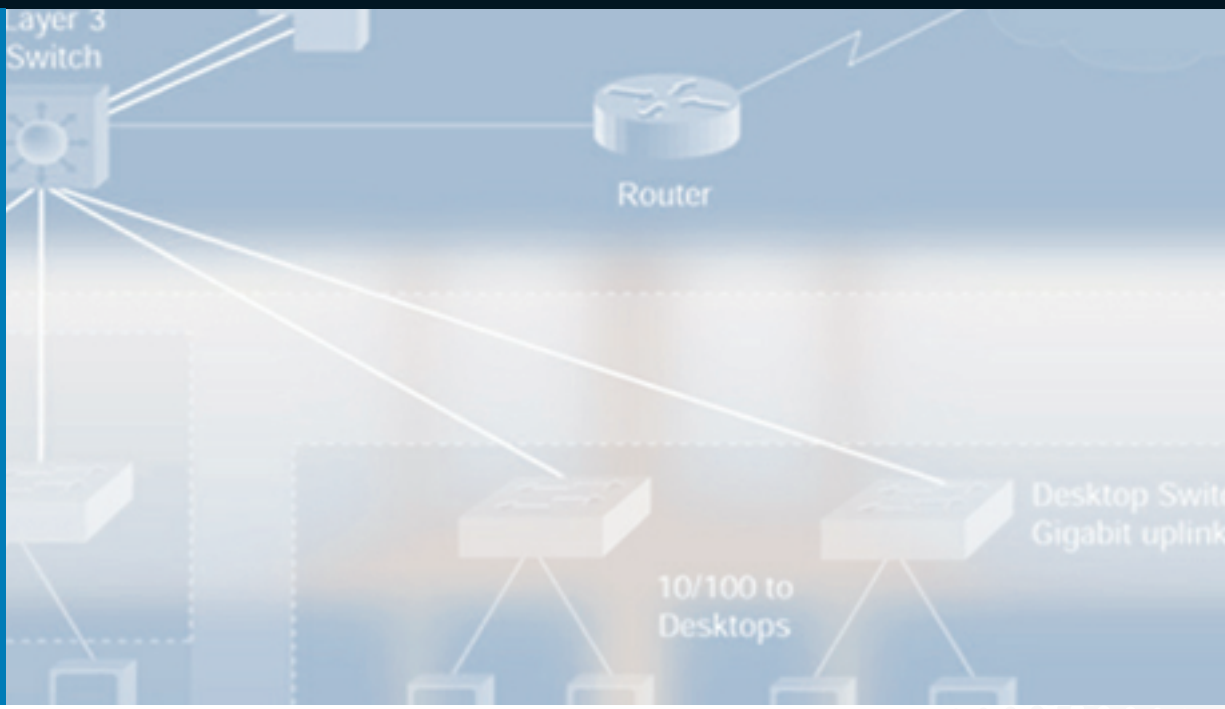
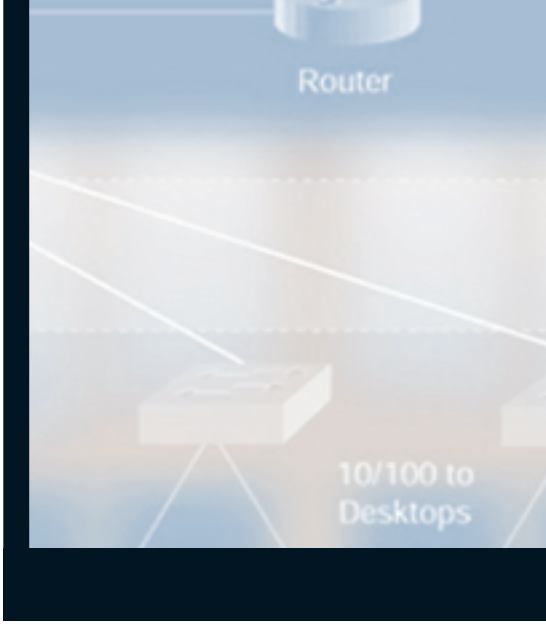
E-Seminar



Intranet VPN

Internet Technology Solution

Seminar



Intranet VPN

Internet Technology Solution

Seminar

Welcome

Welcome to the Technology Solutions E-seminar on Intranet VPNs.

In our networked economy, businesses rely more and more on their company network as a key part of their infrastructure. Without this network, it becomes difficult, costly or even impossible to do business. For a company with remote offices, it is crucial that these remote locations have full access to the company network, to enable seamless communication and increased productivity.

Until recently, companies had only a few options for creating this access: a dial-in service, or a leased-line-based Wide Area Network.

Today, a new, less expensive and more flexible option is available: Virtual Private Networking

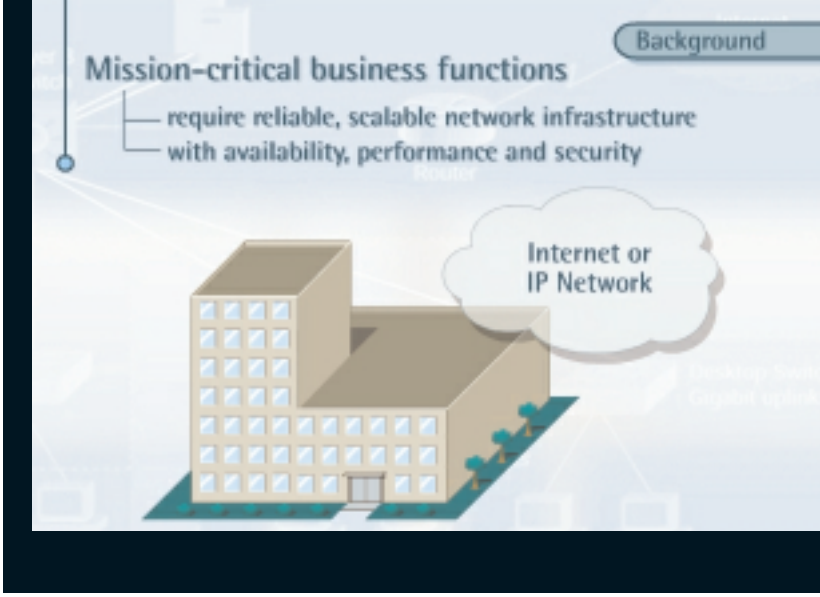
Objectives

In this seminar, we will discuss the technical aspects of Virtual Private Networks, or VPNs, and more particularly, of Intranet VPNs

We will first discuss the concept and definition of Virtual Private Networking.

We will also discuss the potential benefits of using a VPN in your company.

Finally, you will learn about the key aspects of implementing an Intranet VPN in your company.



Background

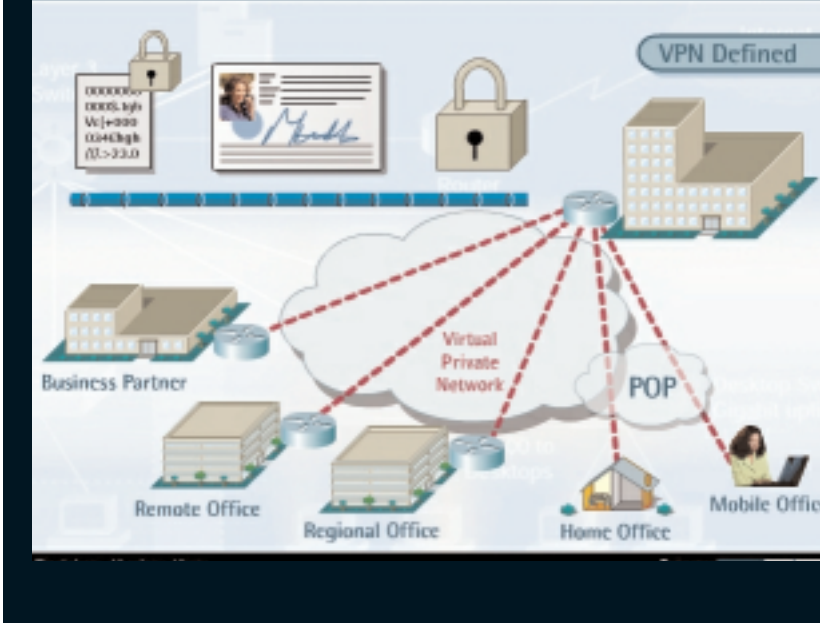
Over the last few decades, many companies built and used mission-critical applications over private Local Area Networks – or LANs – and private Wide Area Networks – or WANs. Access to this private data communications infrastructure was tightly controlled, and there were no external connections to networks like the Internet as we know it today.

Nowadays, the Internet is seen more and more as an enabler of Business Solutions, such as E-Commerce, Supply Chain Management and Customer Relationship Management. Companies can use the Internet to communicate with their customers, to buy and sell products, to connect with business partners, or to connect their own offices and sites to each other.

The greatest characteristics of the Internet are its openness and the fact that it is available almost anywhere in the world. These features however also represent some threats, such as security risks or bandwidth constraints.

Companies who truly want to conduct mission-critical business functions over the Internet, and over their own internal network, require a reliable and scalable network infrastructure, with predictable application availability, performance and security.

Virtual Private Networking today addresses most of these requirements.



VPN **Defined**

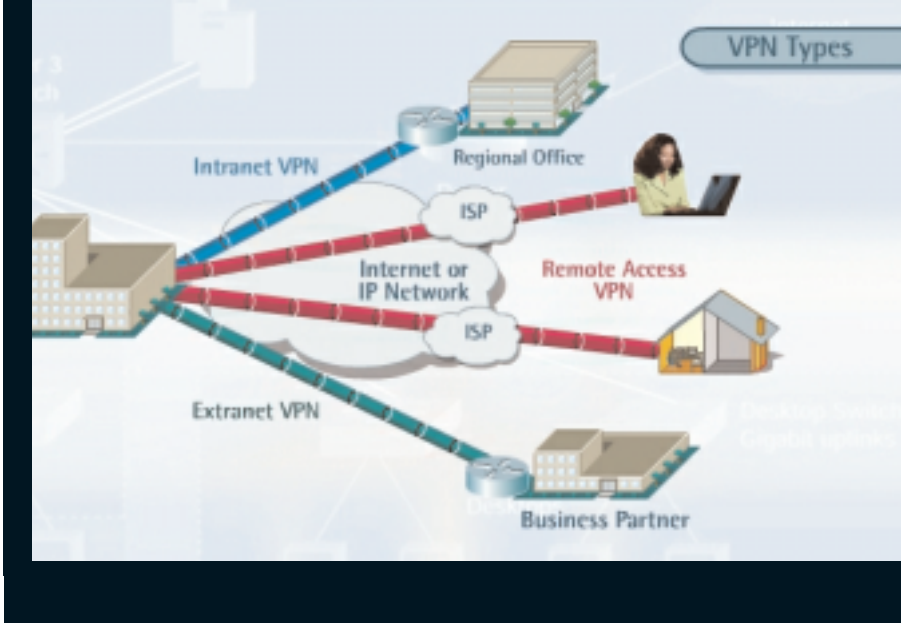
So what is a good definition of Virtual Private Networking?

Simply defined, a VPN is a company network deployed on a shared infrastructure, and employing the same security, management and performance policies that are usually applied in a private network.

VPN technology provides a way of using public network infrastructures, such as the Internet, to provide private, secure access to applications and company resources to employees in remote or home offices, to business partners, and even to customers.

A VPN can be established over different underlying transport networks: the public Internet, service provider IP backbones, as well as service provider Frame Relay and ATM networks. Today, more and more VPNs are based on IP networks.

VPN technology uses a combination of tunnelling, encryption, authentication, and access control mechanisms and services used to carry traffic over the Internet, a managed IP network or a service provider's backbone.



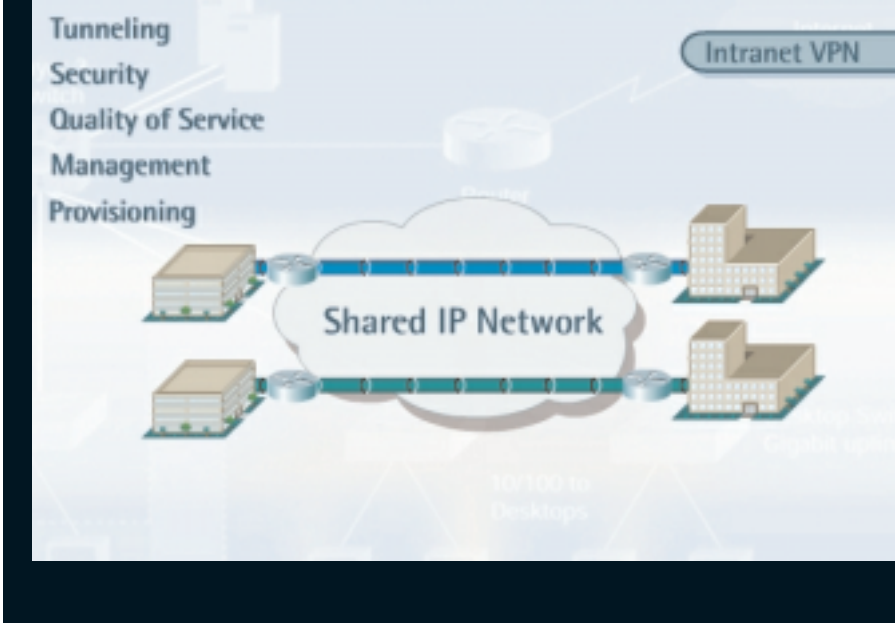
VPN **Types**

Just as there is an endless variety of physical network topologies, there are also many Virtual Private Network architectures possible. Most VPN topologies however fall into one of the following three categories: Intranet VPNs, Remote Access VPNs, and Extranet VPNs.

Intranet VPNs provide site to site internal connectivity within the company. The collection of all internal company sites, connected in this way, is often referred to as the company's Intranet. Intranet VPNs provide the same level of connectivity and reliability as a fully private network.

Remote Access VPNs extend the internal network to telecommuters, mobile workers and remote offices.

Extranet VPNs extend a company network to include suppliers, business partners or customers. This can be interesting for a number of Internet Business Solutions which involve intense business-to-business communication. For more information, please refer to the Technology E-Seminar on Extranet VPNs.



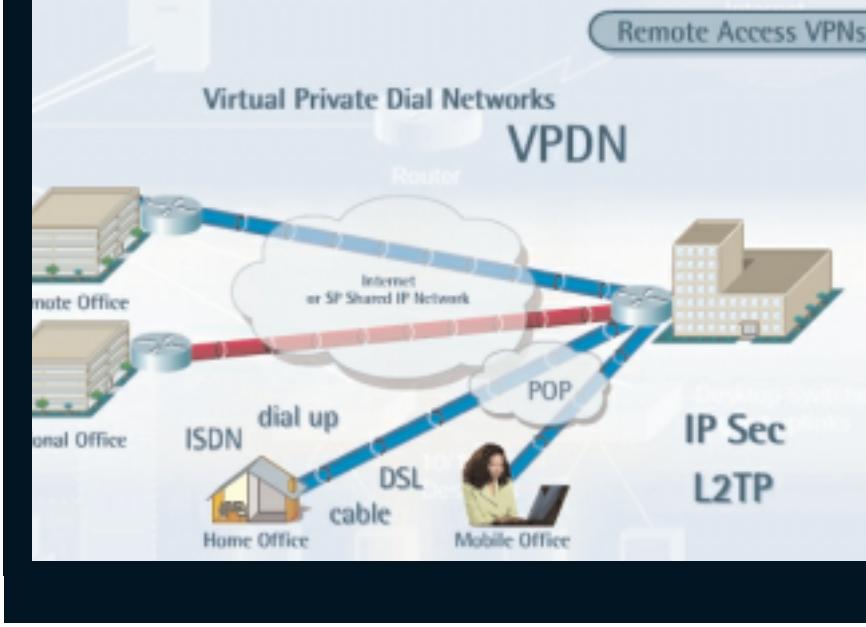
Intranet **VPN**

So, Intranet VPNs extend internal company resources and applications from a central office to employees in regional or branch offices. Intranet VPNs are typically full-time connections, which are created through secure tunnels across an IP network.

With any VPN implementation scenario, Service Providers become partners in the solution. They can either deliver basic connectivity, or completely outsourced VPN solutions

Service Providers either provide the Internet connections to create secure tunnels, or they provide a company with a part of their shared IP network, which is typically created for the purpose of handling IP VPNs for companies. In other words: many VPNs, of different companies, can be created on the same shared IP backbone infrastructure of a Service Provider. This is one of the reasons why VPNs are far less expensive for companies than full private networks based on a WAN infrastructure.

It is of course very important that every company's traffic is completely separated and invisible from any other company's traffic, and that network performance is not influenced. A complete VPN solution therefore incorporates tunneling, security, Quality of Service, management, and provisioning capabilities, to create a reliable communications infrastructure.



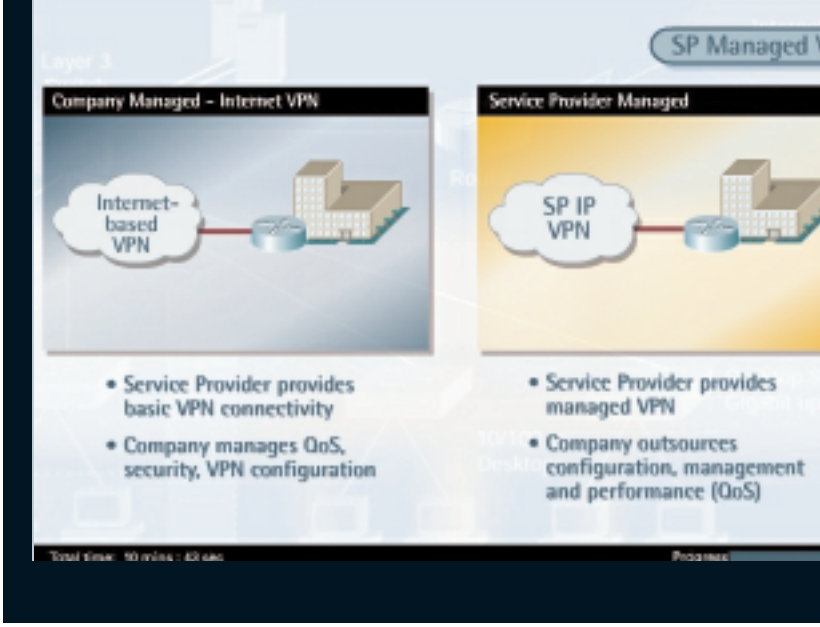
Intranet VPN Seminar

Remote **Access**

Remote Access VPNs, sometimes referred to as Virtual Private Dial Networks or VPDNs, provide remote users access to the company's Intranet, whenever, wherever and however they require.

In general, teleworkers or mobile users will connect to a local Point of Presence, or POP, of the Service Provider, to access their company's network. Through this provider network, or the through the Internet, tunnels are routed to the corporate gateway. These tunnels are secured and encrypted by, for instance, the IPSec or the LT2P protocols.

Remote access to the company network can happen in flexible ways, using technologies such as dial-up, ISDN, DSL or cable. For more information about dial-up or broadband access technologies, please refer to the Technology E-Seminar on Remote Access.



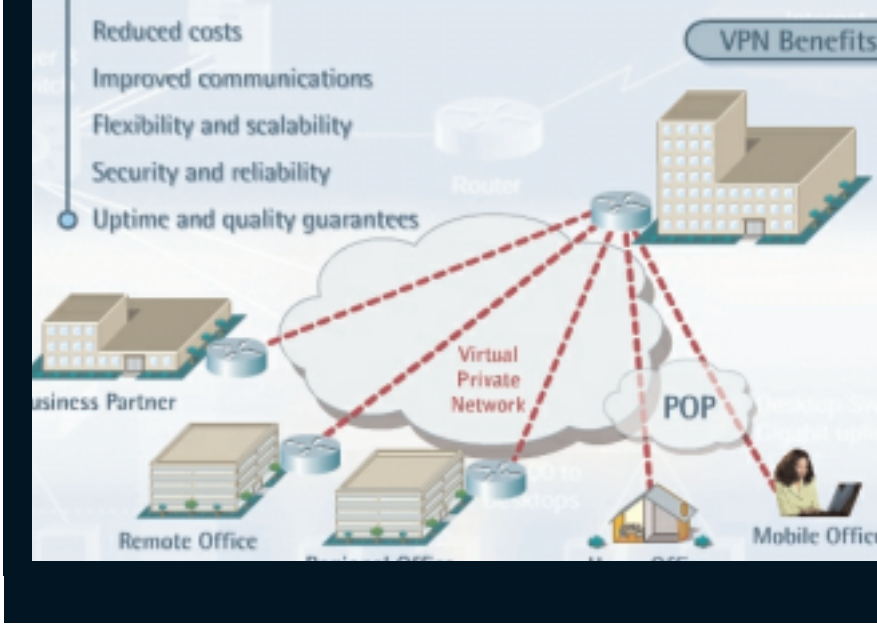
SP Managed

Another decision your company will need to take is whether it will own and manage the VPN, or will buy a Managed VPN Service from a Service Provider.

If you decide to own and manage your VPN, you should be aware of the complexity of the technology and the required staff to configure and maintain your VPN.

Also, since you will use the Internet to transport the data from the remote sites to the central office, there will be no guarantee of any Quality of Service, and performance of your VPN could be affected at Internet traffic peak times.

On the other hand, many Service Providers also offer Managed VPN Services, which combine security capabilities with performance guarantees. In this case, the Service Provider designs the site-to-site or remote access VPN solution your company needs, and configures and manages it on your behalf. The provider can guarantee certain levels of performance by routing the VPN traffic over its own access links and backbone network, and by using the Quality of Service capabilities of the router networking software.



Benefits

So what can a VPN mean for your business? What are the most important advantages?

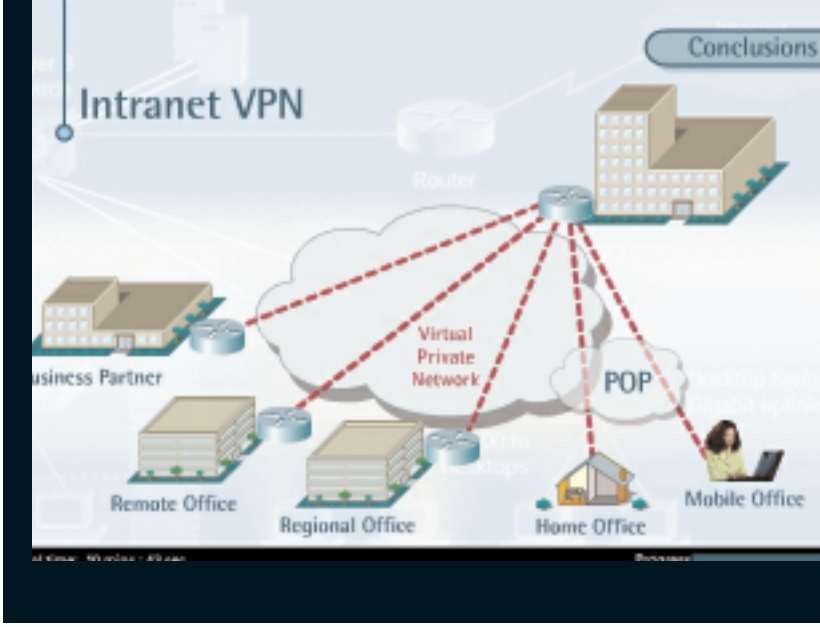
Well, VPN technology provides a reliable way to maintain your company's privacy, while streamlining operations, reducing costs, and allowing for flexible network administration.

First, VPNs can reduce a company's communication costs, because they use the Internet or a shared Service Provider IP network instead of leased lines. Prior to VPNs, many companies with remote offices communicated through expensive Wide Area Networks or costly dial-up connections between their different business locations.

A VPN can also significantly improve a company's communications: remote offices, mobile employees and teleworkers can use the VPN to access the company Intranet from anywhere and at any time.

VPNs are very flexible and scalable. They can easily be adapted to a company's changing needs. The process of network administration is simplified, and remote users or new sites can be added easily.

Finally, VPNs can maintain security and reliability through the use of tunnelling protocols and encryption software. Uptime and quality levels can be guaranteed by the Service Provider, with credit reimbursements for outages.



Conclusion

Let's summarise the most important points.

Intranet VPNs provide an interesting and affordable way for internal company communications, because they operate on a portion of the public or shared communication infrastructure. They use encryption and tunnelling to protect confidential information, and provide the same level of reliability and performance as traditional Wide Area Networks.

Intranet VPNs enable businesses to refocus their energy on core business objectives instead of networking needs, and reduce operations and bandwidth costs.