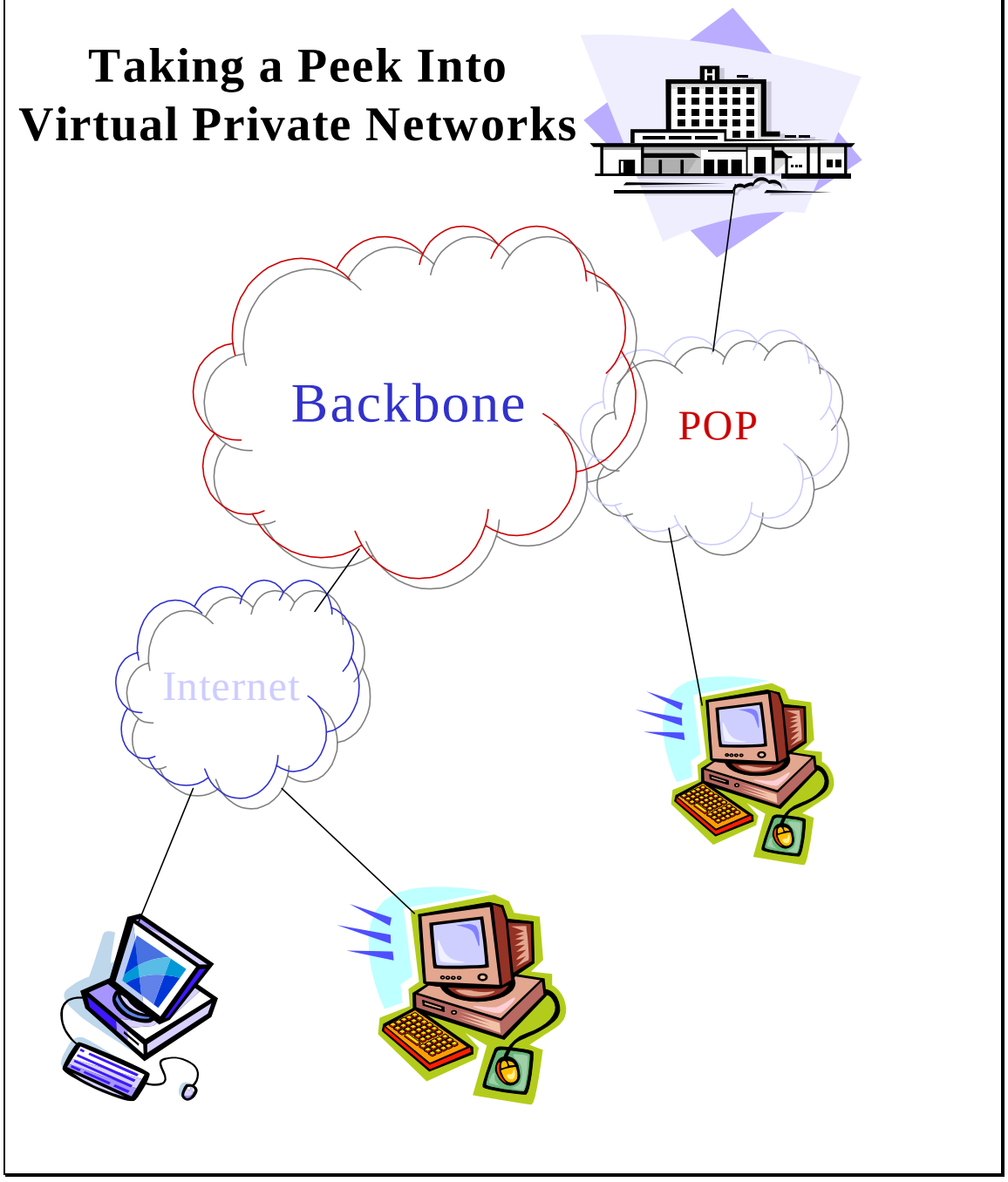
Taking a Peek Into Virtual Private Networks



Joseph Alvarez
Global TechPro, LLC
5659 Columbia Pike #200
Falls Church, Virginia 22041

Virtual Private Networks, VPN for short, has been a popular buzzword. For years, voice and data services were delivered using what the telephone companies called virtual private networks. In fact, the phone companies consider just about all software-defined networks VPNs.

But the current generation of VPNs is very different. The working definition of a VPN is the following: a combination of tunneling, encryption, authentication, and access control technologies and services used to carry traffic over the Internet, a managed IP network or a provider's backbone. The traffic reaches these backbones using any combination of access technologies, including T1, frame relay, ISDN, ATM or simple dial access.

Now that a definition is nailed down, the next question to consider is, what are VPNs used for? The answer: VPNs reduce communications costs. However, the general idea behind using a VPN is that a company reduces the recurring telecommunications charges that are incurred when connecting remote users and branch offices to resources in corporate headquarters.

Several distinct VPN applications are emerging, each with its own performance requirements. Which in turn dictate a set of equipment and service requirements. The emerging application areas are remote access, site-to-site connectivity, and extranets.

Key to acronyms
PPTP—Point to Point Tunneling Protocol
L2TP—Layer 2 Transfer Protocol
TCP—Transfer Control Protocol
GRE—Generic Routing Encapsulation
SSH—Secure Shell
L2F—Layer 2 Forwarding
CHAP—Challenge Handshake Authentication Protocol
PAP—Password Authentication Protocol
SPAP—Shiva Password Authentication Protocol
MPPE—Microsoft Point-to-Point Encryption
IPSec—Internet Protocol Security
VPN—Virtual Private Network

DSL—Digital Subscriber Line

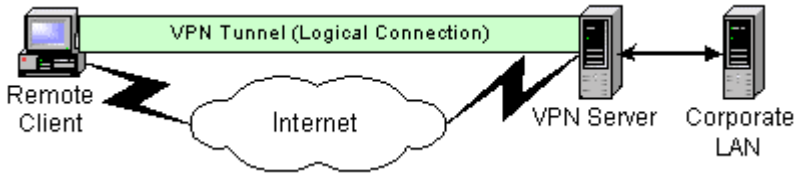
XML—Extensible Markup Language

ASP—Application Service Provider

RAS—Remote Access Services

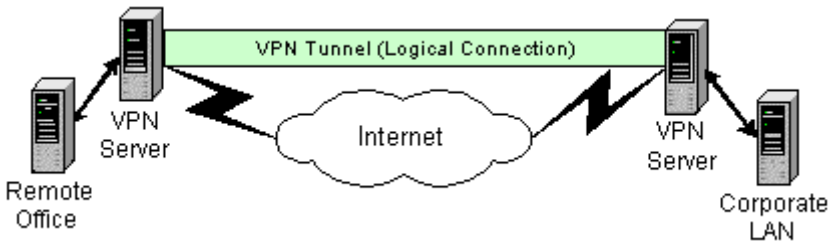
ISDN—Integrated Service Digital Network

The basics of VPN



The graphic above depicts a client-to-server VPN where a remote user connects to a corporate VPN server using point-to-point tunneling protocol (PPTP). The use of PPTP allows enterprises to extend their own corporate network through private "tunnels" over the public Internet. Using this type of interconnection, a company no longer needs to lease its own lines for wide-area communication. Instead, enterprises can securely use the public networks because the communication packets are encrypted before they are sent through the tunnel.

The graphic below depicts a basic server-to-server VPN. Both of these diagrams show very simplified solutions. In reality, VPN servers often sit behind a firewall and are part of the corporate network's "Demilitarized Zone." Setting up a VPN usually involves some trial and error on the part of both the clients and the server. Once VPN is up and running, however, it is typically reliable if you have a dependable Internet connection on both ends.



Remote Access

When it comes to remote-access VPNs, the basic concept is to give telecommuters and mobile workers a way to get back to a corporate network over the Internet or a service provider's backbone. In a remote-access VPN, a user dials into a service provider's point of presence, establishes a tunnel back to headquarters over that provider's network or the Internet, and authenticates himself or herself to gain access to the corporate network. That is in contrast to the traditional dial-access approach whereby a user dials into a bank of modems, a remote-access server or concentrator located within the corporate headquarters.

There are a number of reasons to use a VPN for remote access. First, there is cost savings on the calls. Rather than having a user make a long distance phone call or use an 800 service to dial directly into the company, the VPN approach lets the user make a local phone call to the provider's point of presence (POP). The cost savings of dialing up locally can be substantial. Some companies say they cut their telecommunications charges from $1,000 to $2,000 per month per person with dial access to less than $20 per month per person when using a flat monthly rate ISP service. Further savings can come from reducing the operational costs associated with supporting remote users. For example, when using a VPN, companies can get rid of their modem pools and remote-access servers. Additionally, companies may be able to save other communications charges. For example, before using a VPN, a company may have a dedicated link to an ISP for Internet access and a channelized T1 line into a remote access server to support dial-in users.

A complete cutover to a VPN would eliminate the need for the T1 line for dial access. The traffic from these users would be rolled over onto the existing Internet access line. Thus the monthly cost of a T1 line to support dial access could be cut out.

Branching Out

The next general application of VPNs is for site-to-site connectivity. As in the remote-access scenario, branch offices are connected to corporate headquarters through tunnels that transport traffic over the Internet or via a provider's backbone. Again a company might be able to reduce communications costs by paying only for the access line from a branch office to the service provider's POP, rather than paying for a long distance link to headquarters.

Many sites have multiple access lines: one to carry data back to headquarters and a second for Internet access. In fact, some industry studies have found that as many as 72 percent of sites have multiple access lines. Using VPN technology for site-to-site connectivity would let a branch office with multiple links get rid of the data line and move traffic over the existing Internet access connection.

Additionally, site-to-site VPNs can cut communications costs significantly if a company has many international sites. Typically, the cost to link a European site to a North American headquarters office can be quite high when using leased lines or data services such as frame relay. A VPN built around a service provider with points of presence in countries where there are branch offices would allow the international sites to pay only for dedicated Internet access to that point of presence. That would be much less expensive than the paying for a long distance link back to the United States.

Letting In Strangers

The third emerging application for VPNs is extranets. There are a number of ways to create extranets that do not involve VPN technology, but VPN-based extranets give IT managers another option. The basic idea of VPN-based extranets is to use the access control and authentication services with a VPN implementation to deny or grant customers, trading partners and business associates access to specific information that they may need to conduct business. With a VPN-based extra-net application, the outside party would get to the corporate firewall by tunneling across the Internet or a service provider's network. The ability to get behind the firewall is controlled by the VPN access control services.

It's difficult to estimate the cost savings of using a VPN vs. another networking technology for extranets. For many companies, VPN-based extranets simply allow them to do business they could not do before. So some IT managers use a soft-dollars argument for justifying a VPN-based extranet.

The argument typically goes like this: An extranet gives certain customers or classes of customers privileges they did not have before and that other customers do not have at all.

For example, a brokerage house could set up classes of users so that a client that spends the minimum amount gets to trade electronically; a higher-spending customer gets to trade and gets an Internet account thrown in for free; and a premium client gets all of this and access to internal stock market research. All of which can be done using VPN authentication and access control services.

The selling point for this VPN application is that it builds customer loyalty. Once the client gets to that second or third level of service with Internet access and proprietary research thrown in, these intangibles may be enough to keep a client from switching to another brokerage firm.

A harder cost analysis might be possible if the VPN extranet replaces something else. For instance, some companies that do business with trading partners using electronic data interchange (EDI) are looking to VPN extranets to reduce costs. Typically, EDI applications require custom software and the use of a value-added network (VAN) provider. Such VANs typically charge anywhere from $6 to $12 per hour for connectivity. A VPN extranet would allow trading partners to connect using traditional service providers at much lower costs.

Case Study

Company X is looking to complete a simple goal, to cut their current remote access cost in half. Looking at a variety of possible solutions Company X has opted to use Windows 2000's new VPN Technology to meet this goal.

After analyzing current capital expenditures Company X deemed that the best possible solution to achieve this was in fact two solutions. First Company X will get their employees to dial into local Internet Service Providers (ISPs). Second, Company X will connect some of their smaller sites and offices using public infrastructure such as digital subscriber line (DSL) technology to supply high-speed WAN bandwidth.

Like most companies Company X is zealous about data security. VPN technology and Windows 2000 now provides them with extra capabilities to keep their data secure. This wouldn't have been possible without VPN technologies such as PPTP, L2TP/IPSec.

Virtual Private Networking provides Company X with the flexibility to create a range of networking solutions. Windows 2000's VPN services help solve remote access by means of a variety of mechanisms. Users can dial directly into the corporate network or access the network via the Internet or a connected third-party network. So whether Company X's employees are working remotely at an office, at home, or on the road, they have easy access to the information they need to get their jobs done.

One of the biggest benefits Company X gets from their VPN is that it's an integrated product with a single point of management. User management integrated into Active Directory lowers costs because just one database needs to be maintained. When with other products in the past, you had more of a management burden.

Building on its success with its VPN for its remote users, Company X will evaluate another initiative. Enabling certain workers, such as reservations agents, to work from home. Many neighborhoods surrounding Company X's headquarters have access to DSL or cable modem technology, which provide decent response times for network services.

Company X's success with VPN technologies utilizing the windows 2000 suite helped cut their communication cost in half, and provide a more pleasant working experience for its employees

Why Change?

So why are VPNs even necessary? The answer is that the costs of using traditional remote access technology is skyrocketing and will only get higher as more users and sites need to be connected. To understand why costs are increasing, it is necessary to look at the total cost of ownership for remote access. During the past few years, several market research firms have done remote-access costs studies. Consistent findings have revealed that equipment costs are only about 15 percent to 20 percent of the total cost of ownership when connecting users and sites. The bulk of the cost to support remote access for a three to five year period comes from two areas:

recurring telecommunications costs and the operational costs to support the users and manage the equipment.

Companies often have additional hidden costs when supporting large numbers of sites or users. For instance, some businesses simply have telecommuters or travelers submit their phone expenses with their normal expense reports. This is a productivity buster since the user must take the time to photocopy each phone bill and the accounting department must deal with the submissions.

A number of companies use 800 services to avoid such hassles and to make it much easier for their users to connect when on the road. Even the best rates on 800 services--about 5 cents per minute--amount to phone bills of $120 per month per user for about two hours of connect time each day. That adds up to $144,000 a year for 100 users. The hidden management and recurring telecommunications costs of traditional access technologies will only grow as more users and more sites are added. Telecommunications costs are simply proportional to the number of users. If you double the number of people dialing in, you also double the phone charges.

VPNs offer a way to keep costs in check. First, they can reduce the recurring communications charges. VPNs use the relatively free bandwidth of the Internet or a service provider's network to connect a user to a corporate network or carry traffic between sites. For dial access, the basic idea is to replace that long distance phone call to the company with a local call into a service provider's point of presence. If a flat monthly rate Internet account is used, the cost savings can be significant. It would cost $19.95 per month vs. $120 a month when using the 5-cent-per-minute 800 service for two hours a day every business day.

Flat monthly rate ISP accounts are fine for some applications, but increasingly, IT managers want more than a flat-rate account can deliver. That is leading some IT managers to look at usage-based services that may cost more than a flat-rate account, but guarantee network availability and latency across that provider's network.

Another way VPNs can save communications costs and possibly reduce management costs is by reducing the amount of access gear required. In the dial-access scenario,

a company would typically have one or more dedicated T1 lines that connect to a remote-access server and that are only used for the dial-access users to get into the company network. Additionally, the company would have a high-speed Internet-access line. If every one of the dial-access users switched from direct dial to VPN access, the T1 lines used for dial access could be eliminated since the user would enter the network over the existing high-speed Internet access lines. This would also eliminate the cost of the T1 lines to headquarters for dial access. Moving all users over to VPN access also eliminates the need for a remote-access server. So that piece of equipment could be removed, thus freeing up whoever had to manage it from these duties. Similar savings can occur in site-to-site connectivity scenarios. Many sites have multiple access lines, one for traditional data connections, such as frame relay or T1 lines, and another for Internet access. If branch offices are linked to a corporate headquarters over a VPN connection, it might be possible to reduce the number of traditional data lines company wide And the WAN-access equipment might be able to be consolidated.

In Closing

VPNs are revolutionizing the way companies work and grow. In today's economy where asset consolidation is on the forefront of everybody's to do list, VPNs are leading the way in cost reductions and productivity improvement. When you take all of these factors into account, it becomes very easy to see why VPNs are attracting so much attention.

References

Web sites with helpful information:

- By Salvatore Salamone
  http://www.internetwk.com
  Comprehensive articles on Virtual Private Networking. A good start to finish understanding of the technologies associated with tunneling.

- By Jason Hinler
  http://www.techrepublic.com
  Basic introduction to the world of Virtual Private Networks.

- Microsoft Corporation
  http://www.microsoft.com
  The official site for all Microsoft related VPN technologies.