VPN Mania

An Industry Update on Virtual Private Networks

BY ERIC ZINES

Over the past two years, virtual private networks (VPNs) have been one of the most talked-about concepts in the networking industry. Network managers have become well-versed in the many benefits of VPNs: they are relatively inexpensive, are based on standards, provide global coverage, and are the shortest path to creating a secure extranet. Despite the hype, however, the workings of VPN technology remain a mystery to many network managers.

Many managers are still struggling with the basics. In a recent VPN market study performed by TeleChoice (www.vpdn.com), we asked information technology managers how comfortable they were with the technologies, products, and services that constitute the VPN universe. Only about 20 percent responded that they felt knowledgeable. We've also done a number of educational VPN seminars for IT managers, and most of the questions that we get are still fundamental. Here are a few:

- What problems can I solve with a VPN?
- What are the advantages of VPNs over competing technologies?
- Are other businesses successfully building VPNs? Who are they?
- Should I outsource my VPN or build it in-house?
- What will happen next in the VPN market?

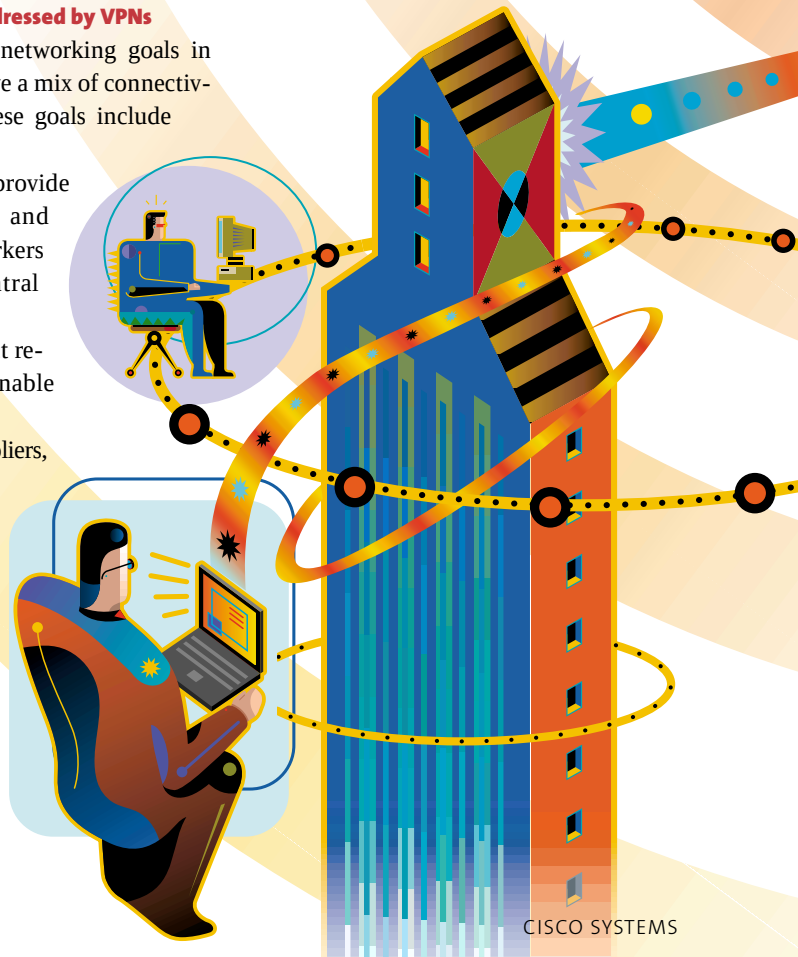
Enterprises are eager to reap the benefits of VPNs, but they're also eager to learn more first. So, let's look at some of those all-important fundamental questions.

Business Problems Addressed by VPNs

VPNs address three networking goals in organizations that have a mix of connectivity requirements. These goals include the following:

- Gain the ability to provide remote, traveling, and telecommuting workers with access to central network resources
- Securely interconnect remote offices to enable corporate intranets
- Supply partners, suppliers, and customers with controlled access to selected network resources

Historically, remote access has been the strongest of the three drivers for VPN adoption, but this situation is changing. While remote access remains at the top of



the list for VPN implementers, the goals of establishing extranets and building site-to-site intranets have emerged. In fact, as shown in the pie chart, an equal percentage of network managers will be building VPN-based extranets and VPN-based remote-access solutions by mid-2000. The goal of interconnecting internal offices is close behind.

An important benefit of VPN solutions is that the same network infrastructure can be used to support all three primary VPN goals. A single VPN can support remote-access users, site-to-site intranets, and extranets. As long as you begin with a scalable solution, VPNs can be implemented in any order and extended to change with your needs.

Why Choose a VPN Solution?

Many users believe that the primary justification for VPNs is the cost savings that can be achieved using VPN technology. In some cases, VPNs enable enterprises to save between 30 and 70 percent over competing remote-access solutions. For connectivity outside the USA, the savings can reach 90 percent. For site-to-site solutions in the USA, VPN savings over private-line solutions can be as high as 70 percent.

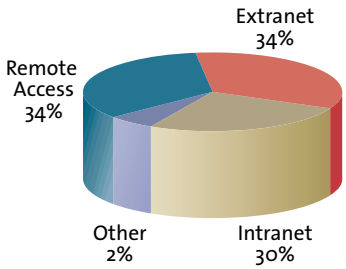
While VPNs will save over competing technologies in many cases, it would not be accurate to say that they are always the less expensive solution. Comparing IP VPN to Frame Relay pricing, for example, is extremely complex. Contrary to popular opinion, it may be less expensive to build smaller, nonmeshed networks with Frame Relay, especially given the recent trend toward lower Frame Relay service prices.

It's impossible to say for certain if, or how much, VPNs will save a particular company. The needs of individual networks and enterprises differ vastly. The only way to know for sure is to test the business case for yourself. Compare both capital equipment costs and ongoing operational expenses for VPNs and competing solutions. Be sure to factor in the potential financial benefits of simple remote access and partner extranets.

The real benefits of VPNs lie not in cost savings, but in coverage and openness. VPNs—particularly Internet VPNs—are unmatched in their potential for global coverage. No other network service offers the global footprint available by using the Internet or other public IP VPN services. The same can be said about the openness of the standards-based IP protocol. If there's an

Continued

THREE VPN APPLICATIONS



Why users say they'll build VPNs:

- Remote access VPNs
- Site-to-site (intranet) VPNs
- Extranet VPNs

Source: TeleChoice, Inc.

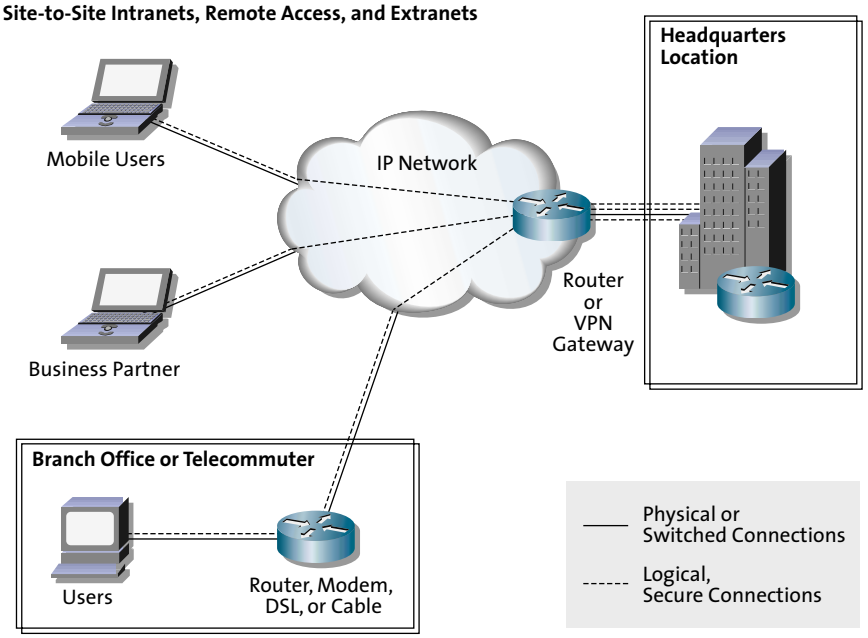
ADDED JUSTIFICATION: Intranets and extranets are catching up to remote access as the drivers behind VPN deployment.

ILLUSTRATION BY STEVEN LYONS

Mania, Continued

TYPES OF VPNs

Site-to-Site Intranets, Remote Access, and Extranets



ACCESS FOR EVERYONE: VPNs address the mix of internal and external connectivity requirements within an organization.

extranet in your future, no other network infrastructure will get you there more directly than a VPN.

Who's Building VPNs?

VPN solutions have already achieved widespread adoption. Roughly 30 percent of those who have WANs are now piloting or using a VPN. Another 35 percent of WAN users have plans to implement VPNs in the coming year. Does this mean that users are choosing VPNs instead of traditional WAN technologies, or that they're ripping out Frame Relay to install VPNs? No. It turns out that most customers view VPNs as a complementary service for now; approximately 90 percent of VPN users also have other network solutions in place.

Many users are still in the pilot phase with their VPNs and are testing to see how the solutions will fit with what they already have. Others view VPNs as an additive solution. They are taking advantage of the technology to solve a particular problem, such as establishing remote-access VPNs or extranets, but they have no intention of replacing functioning, nondepreciated Frame Relay networks. From a market perspective, this trend means that VPNs are actually expanding the size of the market for WAN services, rather than significantly eating into revenue from other services.

One of the most exciting aspects of VPNs is that everyone can find some benefit in these solutions. In the earliest days of the technology, the most likely adopters were the largest and the smallest of companies. Large enterprises viewed VPNs as a means of containing escalating WAN costs; connecting remote users; and integrating partners, suppliers, and customers into their networks. Very small companies adopted VPNs because they were the first real WAN or remote-access solutions that they could afford.

Today, VPNs are equally appealing to companies of all sizes. Even midsized companies, which are almost always the last to adopt new technology, are finding compelling reasons to implement VPNs. Many view VPNs as a competitive advantage, specifically because of their global coverage and the relative ease with which they can be extended to create extranets.

VPNs also have universal appeal across industry types. The earliest adopters included the usual suspects: high-technology firms, computer services, and communications companies. Enterprises in other

Continued

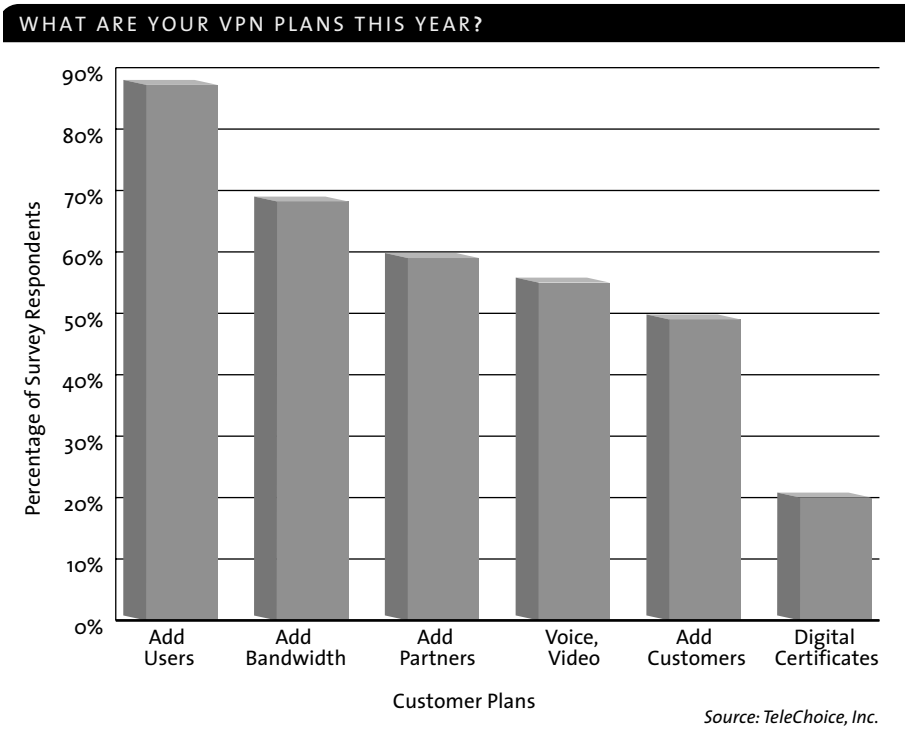
VPNs FOR BEGINNERS

To use the most basic definition, an IP VPN is a private network that's built within a public or shared IP infrastructure.

Virtual refers to the fact that customers share the infrastructure rather than using dedicated private lines to build their networks. The shared network could be the public Internet or a specially managed, shared network that's built exclusively for VPN customers.

Private reflects the need to address security issues, because IP was designed as an open protocol. Customers and network service providers must take measures to protect data within the customer's company walls and while in transit across the network.

Network—No other networking solution can match the potential of VPNs for global coverage and the ability to create extranets.



MORE OF EVERYTHING: VPN pilots are expanding across the enterprise to accommodate additional internal users, partners, customers, and IP applications.

industries—including insurance, real estate, manufacturing (see story, "Driving E-Business," page 70), and finance—have since found VPNs beneficial. As the technology gains acceptance, success stories are coming from other industries, as well, including education, health services, transportation, and government. Even the US military takes advantage of VPN benefits.

Outsourcing vs. Do It Yourself

It's also interesting to look at who is implementing VPN solutions. Are enterprises deploying these solutions themselves, or are they looking for help from a managed service provider? Actually, the answer is "yes" to both questions. Only a few short years ago, all VPNs were do-it-yourself solutions implemented by network managers, because there were no VPN services available.

Managed VPN services are gaining acceptance rapidly. Service providers are finding innovative ways of delivering real value to customers in the form of security consulting, policy development, solution design and configuration, and ongoing management and reporting. Results of a recent TeleChoice VPN study show nearly a 50-50 split between those who will build VPNs themselves in the next year and those who will outsource the solution.

The Road Ahead

Clearly, with all of the interest in VPN products and services, we can expect tremendous growth in the adoption of these technologies. By late 2000, about 70 percent of enterprises with networking needs will be testing VPNs or using them in a production environment. Aside from growth in adoption, though, what else should we expect to see?

On the standards front, we should expect more robust features to be added to one of the most important VPN technical standards, IP Security (IPSec). Work conducted by the Internet Engineering Task Force (IETF) will expand the management capabilities of this protocol and provide more options for how networks authenticate users with IPSec.

From a service provider perspective, expect more solutions for delivering predictable IP performance on VPNs. Deployment of technologies such as Multiprotocol Label Switching (MPLS) is allowing service providers to offer quality-of-service (QoS) guarantees and class-of-service (CoS) frameworks within their service networks.

Network managers who already have VPNs will be expanding them. Those who implemented successful pilots of the technology are now extending the solutions across entire enterprises. As the chart at left shows, VPN managers will be adding users, bandwidth, and outsiders to their networks in the months ahead.

One final note: if you're reading this article, chances are that you have some interest in VPN solutions from Cisco. If so, our research has some encouraging news. When asked whose equipment they were using to construct their VPNs, the majority of respondents to the TeleChoice VPN study replied that they are using Cisco products. And they report that they're happy with their VPNs. ▲▲

ERIC ZINES

Eric Zines, a senior consultant and analyst with TeleChoice, Inc., focuses on the rapidly changing VPN market. Along with tracking and interpreting trends, Zines provides consulting services to VPN service providers and vendors. He is also a regular speaker at industry trade shows and is frequently quoted in the industry press. Zines was behind the launch of the VPDN.com Web site, a resource for learning about the VPN market.