IP VPNs Gain Momentum

By out-tasking their IP VPNs to a managed services provider, SMBs can save time and money.

Large enterprises have been at the forefront in the adoption of IP virtual private networks (VPNs). They are using the security, scalability, extensibility, and multiservice capabilities of IP VPNs as a lower cost alternative to legacy data networks such as Frame Relay and ATM. But service providers like BellSouth see an even broader market opportunity for IP VPNs within the million-strong, small- and medium-sized business (SMB) market.

"Our VPN solution is generally targeted at BellSouth customers that need to outsource data networking. Many of these businesses are using BellSouth's VPN service to cost-effectively add smaller locations to their corporate networks," says Amy Hollister, a senior marketing manager for BellSouth.

These businesses can cut costs by out-tasking their IP VPN needs to service providers. By opting for a managed IP VPN, SMBs find that they can save capital and are better able to focus on their core business—and it frees up their IT staff to do the sort of the work that makes employees more productive. Moreover, they can make the transition to VPN in steps by starting, for example, with out-tasking remote access or by using an IP VPN as a backup or alternative to a site's Frame Relay or private-line connection.

One of the ways in which BellSouth has made its IP VPN service more attractive to SMBs is by using DSL as a last-mile access technology for telecommuters and branch offices to securely share corporate resources over its IP/Multiprotocol Label Switching (MPLS) core. The price point is low enough to prompt customers that have never considered a WAN before to cost justify the business operations impact of having real-time connectivity. "We've got customers with small or remote offices that previously were using Frame Relay access to our VPN service, but with DSL they are getting more bandwidth for less money, and that's very attractive to SMBs that want to add locations to their WAN," Hollister says.

The Market

Although defined in various ways, there are slightly under one million SMBs in the US. The Yankee Group estimates there are 810,000 small businesses employing from 21 to 99 people and almost 92,000 medium-sized businesses with 100 to 499 employees. These SMBs, moreover, have emerged as an important customer segment when it comes to spending on information and telecommunications technologies.

Another analyst firm, AMI Partners, estimates that small businesses in the US spent about $142 billion on IT/telecommunications in the 12-month period that ended October 2003, while spending by medium-sized businesses during the same period was US$57 billion. AMI Partners defines a small business as having

from one to 99 employees, and a medium-sized business as having 100-499 employees.

Among small businesses that have been aggressive in adopting technology—or what the AMI Partners firm terms Tier 1 small businesses—more than half use a WAN. The analyst notes that Internet access for this group has reached "saturation," with nearly half of the businesses using DSL for Internet access. Of the top-tier, medium-sized businesses, 92 percent have a WAN and all have Internet access (typically T1/T3 connections), according to AMI Partners.

Many of these businesses use a combination of legacy WAN technologies, such as private lines or Frame Relay, to link company locations to corporate headquarters, and IP VPNs to enable telecommuters, mobile workers, a small branch office, and even a business partner to exchange information. Although no one example paints a complete picture of the networking needs of SMBs, the case of Arizona State Savings and Credit Union is illustrative: The credit union has about 350 people in almost two dozen locations. Five sites acting as hub sites connect through leased lines to a data center in Glendale, Arizona, with smaller locations in turn linked by leased lines to the hubs in a traditional hub-and-spoke network topology.

Kim O'Connor, senior network engineer for the credit union, says the credit union uses IP Security (IPSec) VPNs for remote access, typically for LAN-to-LAN large file transfers with other organizations and for giving the credit union's IT staff and senior managers access to the company's network from their laptops.

The credit union is hardly alone in its use of an IP VPN. A recent Cisco global survey of network professionals found that, for SMBs, the top application for IP VPNs is to replace the dialup infrastructure used by teleworkers with secure Internet access to corporate resources. More broadly, SMBs also see IP VPNs as an intranet to securely communicate between sites as well as an extranet for facilitating business with partners.

Though the amount that many SMBs spend on their IP VPNs might be small, it is expected to increase significantly over time. According to the Cisco survey, although between one-third and one-half of SMBs spend less than US$1,000 per month on hardware, software, network connectivity, and self-managing their IP VPNs, another one-third spend substantial amounts—as much as from $1,000 to $4,999 every month—and about 10 percent spend as much as $5,000 to $9,999 per month.

Out-Tasking VPNs

Instead of spending money and effort on self-serviced VPNs, SMBs that out-task will find that service providers deliver VPNs in two ways, depending upon the technology. IPSec, the dominant IP VPN technology in North America, and the new version of Layer 2 Tunneling Protocol—L2TPv3—can be provided as customer premises equipment (CPE)-based managed services where the service provider manages and configures the VPN on the CPE router at each customer and business partner location. The other option is to deliver the VPN from the edge of a service provider's network, or what is known as a network-based service. The choices here are MPLS, L2TPv3, and IPSec. One other IP VPN technology gaining popularity is Secure Sockets Layer (SSL), which enables per-application (for example, e-mail, Telnet, or FTP) VPNs using a Web browser.

The leading technology today for a managed, network-based VPN is IP/MPLS. This rapidly growing technology offers scalability because it can support tens of thousands of VPNs across a common network; it allows traffic engineering to increase network availability;

Powering Scalability and Flexibility with IP/MPLS

For SMBs that want encryption, IPSec is currently the preferred building block for IP VPNs. Aside from Point-to-Point Tunneling Protocol (PPTP), which is generally used by teleworkers over dialup or broadband connections, other IP VPN technologies are MPLS, L2TPv3, and Generic Routing Encapsulation (GRE). Other than MPLS, which does not provide encryption, all of the aforementioned IP VPN technologies offer encryption and use tunneling methods across an IP network to establish point-to-point connections. Hence these are termed *overlay networks*, and it is because of their overlay nature that they present the same scalability problem inherent in scaling Frame Relay/ATM networks for customers who want to directly connect each location with every other location through Frame Relay/ATM virtual channels. This is a key reason why IP VPNs—other than MPLS-based VPNs—are configured in a hub-and-spoke topology in which branch locations connect either directly to the data center or to hub sites, and the hub sites to the data center. Unlike overlay networks, IP/MPLS enables any-to-any connections.

The scalability problem of point-to-point IP VPNs is further compounded when new sites are added to an intranet or an extranet. However, Cisco has developed a mechanism called Dynamic Multipoint VPN (DMVPN) that alleviates the scalability issue in point-to-point IP VPNs by simplifying operations and management of point-to-point IP VPNs to provide effects that are similar to the any-to-any connectivity of IP/MPLS.

and, very importantly, it can provide quality of service (QoS). Because of these attributes, more than 200 carriers worldwide have deployed IP/MPLS in their network cores. They are using their IP/MPLS backbones as a single, converged platform for data, voice, and video traffic as well as to transport other Layer 2 services such as Frame Relay, ATM, and Ethernet.

Unlike other IP VPN technologies, IP/MPLS VPNs provide inherent full meshing or any-to-any connectivity between locations, thus enabling IP traffic to run over an IP/MPLS infrastructure without having to build point-to-point tunnels to connect every location to every other location (see sidebar, "Powering Scalability and Flexibility with IP/MPLS"). The scalability problem of point-to-point technologies is not just an issue that affects large enterprise customers; it even has an impact on smaller businesses that might want secure any-to-any communications between as few as a handful of locations. Additionally, IP/MPLS can be combined with IPSec to offer SMBs an integrated architecture for secure site-to-site and remote access. This, in fact, is exactly what BellSouth has done.

BellSouth offers both network-based IP/MPLS for site-to-site IP VPNs and IPSec VPNs for remote access over the Internet. Because IP/MPLS is technology agnostic, the carrier's customers can use various BellSouth services such as DSL, Frame Relay, and private lines for secure communications between their own locations and with business partners across BellSouth's private IP/MPLS network. IP/MPLS completely separates one customer's IP traffic from another customer's IP traffic in a way analogous to Frame Relay/ATM networks. But off-net customers, or those customers not directly using various BellSouth connectivity services, can also become part of BellSouth's IP/MPLS-based VPN. This is because the VPN can be extended across the Internet to a mobile worker or telecommuter who has IPSec running on the PC, or a branch office with IPSec-based CPE. In the case of these off-net users, their IPsec traffic would terminate at a BellSouth gateway, and from there would be carried across BellSouth's IP/MPLS network. On-net users, on the other hand, would get secure, centralized access to the Internet through BellSouth's network-based firewall and would also receive the benefit of the carrier's intrusion detection system (IDS).

"By putting together a WAN, which is really what we are providing with our network-based VPN, we offload the day-to-day management of a network for a business that doesn't have the staff to do it," says BellSouth's Hollister. "So if you look at a customer that's taking advantage of both our site-to-site and remote-access VPN capabilities as well as our centralized Internet access [via the firewall], these definitely represent a cost saving for customers. And even if you were to take just the remote user VPN services, the management and administration time it would take to deploy a remote-access solution alone would be pretty high."

Managed VPNs: A Partnership

Although eventually SMBs will want to move all of their data traffic to IP VPNs, later they will want to leverage their IP connections to support their voice and video needs. They can do this by taking advantage of the different classes of service (CoS) enabled by IP/MPLS and backed by very granular service-level agreements (SLAs) because of the traffic engineering and QoS capabilities of IP/MPLS networks.

"We've got customers with small or remote offices that previously were using Frame Relay access to our VPN service, but with DSL they are getting more bandwidth for less money, and that's very attractive to SMBs that want to add locations to their WANs."

—Amy Hollister, Senior Marketing Manager, BellSouth

SMBs that out-task their VPNs will find that the cost benefit of their relationship with the service provider will increase over time. This is because IP VPNs can serve as foundation for other managed services such as firewall, Internet gateway, IDS, telecommuter access—as BellSouth is doing—as well as IP telephony, managed LAN, storage, etc. When a service provider is able to extract more value from its network by offering more services, the additional revenues generated from these services enables the service provider to offer customers a multiservice package for less cost.

Managed IP VPNs offer customers more capability for less cost while also saving time and effort in order for them to focus more on their core business. Such benefits make managed IP VPNs a true win-win proposition for SMBs. ■

FURTHER READING

- *Power Up Your Small-Medium Business: A Guide to Enabling Network Technologies* (Cisco Press, 2004, ISBN 1-58705-135-4)
  cisco.com/packet/163_9a1
- Cisco Security and VPN solutions for SMBs
  cisco.com/packet/163_9a2
- Security Technical Implementation Guide for SMBs
  cisco.com/packet/163_9a3
- Article on "What You Need to Know About MPLS" (*iQ Magazine*)
  cisco.com/packet/163_9a4
- Article on "DMVPN Extends Business Ready Teleworker" (*Packet* Second Quarter 2004)
  cisco.com/packet/163_9a5