VPN Services For Site-To-Site Connectivity

Irwin Lazar

Service providers are rolling out IPSec, MPLS and virtual router-based VPN services. Is one of them right for you?

Is it time to consider converting your site-to-site WAN to an IP-VPN? To improve network flexibility and reduce operating costs, many large enterprises are evaluating the use of VPN devices, as well as the newer VPN services that have been announced over the past year, including those based on Multiprotocol Label Switching (MPLS), virtual routers and IP Security (IPSec). Even if they have already adopted remote access VPNs, enterprises should come up to speed on the various site-to-site VPN options to determine which best matches their network requirements.

Unlike remote access VPNs, which allow Internet-based modem access to enterprise networks and applications, site-to-site VPNs are meant to replace private-line and frame relay connections among enterprise locations. Using VPN products from companies such as Check Point, Cisco and NetScreen, enterprises can "roll their own" IP-VPNs and extend their networks anywhere there is access to the public Internet, often cutting WAN costs by 50 percent or more (see *BCR*, May 2002, pp. 28–32).

These "roll-your-own" IP-VPNs are typically based on the IP Security (IPSec) protocols developed by the IETF. IPSec is well understood and offers strong encryption, but it also has several drawbacks related to both scalability and integration with existing network configurations:

- Enterprises must (as the name suggests) buy, configure and manage their own "roll-your-own" IPSec-VPNs, adding management complexity to the network. Thus, the WAN cost savings must be balanced against additional management costs. Enterprises with a large geographic reach may find it especially difficult to assume the management of VPN endpoints.
- IPSec standards allow for interoperability, but managing a multivendor environment can be difficult, especially when setting up large numbers of VPN tunnels. Conversely, vendor-proprietary consoles make management relatively easy, assuming all the tunnel endpoints use that particular vendor's hardware.
- For extranet connectivity with partners, suppliers and/or customer sites, the use of IPSec-VPNs requires a public key infrastructure (PKI), such as those offered by Verisign and Entrust.
- IPSec also creates problems for private IP addressing (e.g., 10.0.0.0) and network address translation (NAT), which many enterprises currently employ. IPSec requires that tunnel endpoints have unique IP addresses, so NAT must be applied prior to traffic entering the VPN. NAT-aware VPN gateways can help, but careful planning is required.

Finally, "roll-your-own" IPSec-based VPNs running over the public Internet generally are not suitable for voice and video traffic, due to the latency introduced by the encryption/decryption process, coupled with the lack of predictable performance across the public Internet. Buffering can smooth out the delivery of streaming video, but buffering can disrupt live voice calls and videoconferences.

VPN Services

For enterprise customers who don't want to create their own site-to-site VPNs, service providers have come up with several options. For example, Virtela offers a managed IPSec-VPN service with latency and jitter guarantees, which uses proprietary routing techniques in the public Internet. Most of the major ISPs, including Sprint, WorldCom, AT&T, Qwest, Broadwing and others, also offer IPSec-based VPN services—with appropriate service level guarantees for latency and jitter—as long as all the sites connect directly into the provider's networks.

These IPSec-VPN services can reduce operational and connectivity costs, although not as much as the "roll-your-own"/public-Internet option. For example, we've seen clients reduce their WAN charges by up to 30–40 percent when switching from frame relay to a service provider's IPSec solution, while a "roll-your-own" solution would have saved 40–50 percent. Both solutions

Irwin Lazar is the manager of Burton Group's "Networks & Telecom Strategies" consulting practice, specializing in strategic network planning for large enterprises. He also runs the MPLS Resource Center (www.mplsrc.com and is the conference director for MPLScon. He can be reached at 703/742-9659 or ilazar@burton-group.com

require equipment to be added on the customer premises, and IPSec/NAT issues to be resolved, but these are the service provider's responsibility in the provider-based solution. Besides configuration management of the VPN, the provider is also responsible for issues related to scaling.

Within the U.S., we've had difficulty building a business case for IPSec-VPN services due to falling frame relay costs. Outside the U.S., we've found IPSec-VPN services are available, although it is often difficult to find a single vendor with a large enough geographic reach to support all enterprise locations.

Another alternative to the IPSec-VPN services are VPN services based on MPLS or on virtual routing. These have gathered a great deal of attention from the trade press, enterprises, service providers and hardware manufacturers. Many of our clients are actively investigating these services, and a few have begun deployments. So far, U.S. pricing for these new services looks to be about the same as for the IPSec-VPNs, although MPLS or virtual router meshes can be less expensive. One client told us that a European MPLS-VPN service came in at half what they are currently paying for frame relay.

Beyond the potential cost savings, MPLS-based VPN services are attractive to enterprises for several reasons:

■ **Native support for private IP addressing**—Packets are forwarded based on information contained within a label rather than by destination IP address, so packets using private IP addresses may be tunneled through a public IP network without the need for NAT between the LAN and the WAN.

■ **Easy meshing**—MPLS-VPN services enable interconnections between sites to occur within the service provider network, rather than being individually specified. Adding a site does not require changes to the existing sites. This allows fast and easy interconnection of a large number of sites, at potentially-significant cost savings compared with large frame relay and ATM meshes.

■ **No customer premises equipment**—Because MPLS encapsulation typically occurs within the provider network, no additional customer premises equipment is necessary.

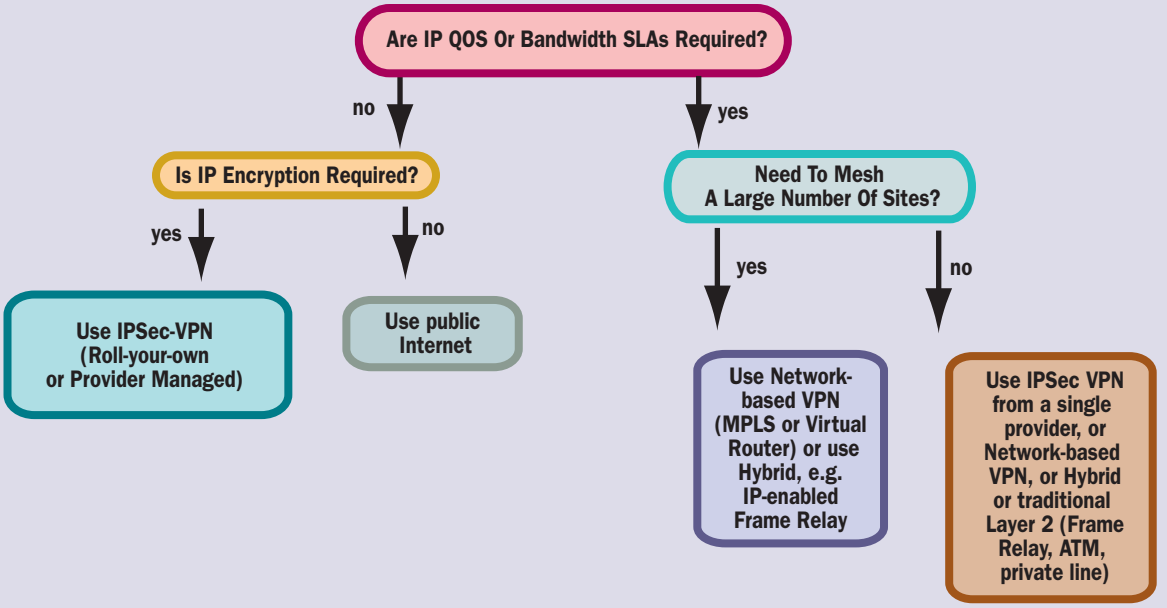
■ **Additional services**—MPLS hardware vendors such as Cisco offer software that lets providers bundle value-added services into their MPLS-VPN offerings. These include address management and assignment, managed Internet gateways and support for IP multicast.

Companies such as Masergy, Cable & Wireless and Equant are using MPLS to enable Layer 3 VPNs over their IP-based networks. Providers such as AT&T (IP-Enabled Frame Relay) and WorldCom (Private IP), are using MPLS as a way to marry IP with their legacy ATM and frame relay networks to provide IP-aware services. Customers of these services maintain their frame and ATM access, but packets are marked using the IP precedence bit as they enter the service provider network, and service levels for latency and jitter are guaranteed.

Not all carriers have embraced MPLS. For example, Sprint believes that MPLS is an overly complex way to provide IP-VPN services, and instead argues that IPSec will meet the majority of customer needs, and that tunneling protocols such as Layer 2 Tunneling Protocol Version 3 (L2TPv3) can be used to carry Layer 2 services over IP when necessary. Savvis uses a different approach, whereby network-based VPNs are

Pricing for MPLS-VPNs looks to be comparable to IPSec-VPNs

FIGURE 1 VPN Decision Tree



If you don't worry about unencrypted traffic over frame relay, don't worry about using MPLS-VPNs

established using virtual routers provisioned with Nortel Shasta devices, thereby isolating customer traffic via separate routing tables.

What About Security?

Another complaint about MPLS, often voiced by IPSec proponents, is that MPLS-VPNs aren't secure. MPLS-VPNs carry unencrypted IP traffic across a public IP network, these folks say, thus providing an opportunity for prying eyes to divert and read sensitive corporate data. The counter-argument, put forth by companies such as Cisco and by testing firm Miercom, is that there is essentially no difference between security within a public network at Layer 2 (e.g., ATM or frame relay), and security within a public network in which MPLS is used as the traffic-isolation mechanism. Compromising either would require someone to gain control of a service provider's router.

Our belief is that companies that are comfortable placing unencrypted IP traffic on a Layer 2 service like frame relay should not have any concerns about placing the same unencrypted traffic on an MPLS-VPN. In fact, MPLS services offered by companies such as AT&T and WorldCom run over the same ATM switches used to support their frame relay customers. For extra security, one could always encrypt IP traffic before it enters an MPLS tunnel, an approach championed by Quarry Technologies.

With All The Available Choices...

What is an enterprise to do? In our experience, IP-VPNs typically offer significant cost savings, reduced network management requirements and less-complex and less-costly meshing compared with traditional Layer 2 services. Therefore, we typically recommend IP-VPNs—provided they can support the customer's traffic types and the cost savings can be demonstrated.

Figure 1 (p. 53) provides a decision tree for selecting an appropriate VPN technology. If there are no requirements for SLAs that control such factors as latency and jitter, options include either the public Internet (if no security is required), or an IPSec-VPN (either outsourced or managed in-house). The choice between whether to buy a VPN service or roll your own will be based on a variety

MPLS And Other, Future VPN Flavors

MPLS isolates IP traffic flows via labels that are attached to the front of each packet, allowing service providers to build VPN "tunnels," or IP "permanent virtual circuits" (PVCs) or MPLS "Label Switched Paths" (LSPs) within their IP networks. Service providers can also leverage MPLS as a control plane for ATM and frame relay switches, enabling Layer 2 services that route traffic based on IP type of service classifications.

Looking ahead, MPLS proponents hope that carriers will also use MPLS to converge their Layer 2 ATM and frame relay networks with their Layer 3 IP networks. A set of IETF Internet drafts (often referred to as the "Martini" drafts, see www.ietf.org/html.charters/pwe3-charter.html) will allow carriers to deliver any Layer 2 service, including frame relay, ATM or Ethernet, over an MPLS-based IP infrastructure. What makes this approach attractive to its proponents is that it would allow carriers to build a single all-purpose MPLS-based network, then transition current frame relay, ATM and MPLS-VPN customers onto that infrastructure. This should enable them to migrate customers to the newer VPN services while reducing operating expenses—without cannibalizing existing services.

Another set of IETF drafts proposes "Layer 2 VPNs" (see www.ietf.org/html.charters/ppvpn-charter.html) that would enable pure IP networks (such as Masergy's) to offer Layer 2 transport services, thus providing carriers another easy migration path for current frame relay or ATM users. Metropolitan Ethernet players such as Telseon (recently acquired by OnFiber) will likely use this working group's specifications in their MPLS Ethernet encapsulation to offer site-to-site connectivity services with guarantees for latency and jitter. (For more on Draft Martini and Layer 2 VPNs, see *BCR*, March 2002, pp. 29–35 and pp. 41–45.)

Vendors such as Cisco and Juniper support a go-slow approach in which MPLS-VPN specifications (Internet RFC 2547bis) are deployed at the provider-customer edge, but tunneling protocols such as Generic Route Encapsulation (GRE) are used within the core (as described in IETF draft "draft-ietf-ppvpn-gre-ip-2547-01.txt"), thus eliminating the need to deploy MPLS within the carrier core.

Yet another VPN approach, championed by equipment manufacturers CoSine Communications, Nortel Networks and Lucent Technologies, and deployed by Savvis Communications, uses logical "virtual routers," rather than MPLS, to deliver network-based VPN services. In this approach, customer traffic is isolated within a service provider network via the creation of multiple logical "virtual routers" within a single physical provider edge router. Traffic between virtual routers may be carried within GRE, MPLS or IPSec tunnels□

of factors, including staff expertise, comfort with outsourcing, cost and geographic coverage of the selected outsourced partners.

If performance guarantees are required, the next decision factor is the number of sites that need to be interconnected. Enterprises with hub-and-spoke traffic flows can choose from a variety of services. The actual choice will depend on factors such as cost, service level guarantees, geographic availability and association with a primary vendor (and its service offerings).

Enterprises that need to mesh a large number of sites to provide any-to-any direct connectivity (based on application flows or for a network backbone) should consider VPN services, because they can typically cut WAN costs by as much as 50 percent when compared with frame relay or ATM meshes.

Enterprises with large global networks may have trouble getting VPN services in all locations

Another approach that has worked for many organizations is to use a low-cost IPSec-VPN over the public Internet for application traffic that isn't sensitive to network latency (such as storage, file transfer or mail replication), and use frame relay or an MPLS-VPN with SLA guarantees for latency-sensitive traffic such as voice, transaction processing or terminal services applications.

When A VPN Doesn't Make Sense

In our consulting experience, IP-VPNs offer tremendous potential for cost savings, improved network flexibility and faster network expansion. We've advised most of our enterprise clients to come up to speed on network-based VPNs, as we believe they will eventually replace frame relay and ATM as the standard mechanism for site-to-site connectivity.

However, IP-VPNs don't make sense for all enterprises, since network-based VPN services are relatively immature and aren't yet widely available, especially outside the U.S. and Europe. For enterprises with a large global presence, the only alternative may be to buy VPN services from regional service providers, a choice that adds additional management complexity, or to continue with the traditional Layer 2 (frame relay, ATM and private line) options. If network-based VPN services aren't available for all your locations, the decision comes down to IPSec or traditional Layer 2 services, a decision typically made by examining costs.

Conclusion

IPSec-VPN services are an attractive alternative to traditional frame relay and ATM services when performance guarantees aren't necessary. However, IPSec-VPNs add network complexity, including the need for key management, integration with NAT and additional CPE. They also introduce additional latency into end-to-end traffic flows.

MPLS-based VPNs can allow enterprises to reduce WAN costs and simplify their networks. Though these services are still under development, they represent the direction being undertaken by most major carriers. Enterprises that have not done so already should begin to investigate the plans of their service providers so that they can make an informed choice.

The best approach, as always, is a careful evaluation of service alternatives via the use of "Requests for Information" (RFI) or "Requests for Comment" (RFC). These structured approaches allow enterprises to carefully screen and evaluate services that are capable of meeting their unique requirements. In some cases, enterprises may find that the service they currently use is still the best choice; however in many, if not most, we expect that they will find real benefits in the newer VPN service alternatives□

Companies Mentioned In This Article

AT&T (www.att.com)
Broadwing (www.broadwing.com)
Cable and Wireless (www.cw.com)
Check Point (www.checkpoint.com)
Cisco (www.cisco.com)
CoSine (www.cosinecom.com)
Entrust (www.entrust.com)
Equant (www.equant.com)
Juniper Networks (www.juniper.net)
Lucent (www.lucent.com)
Masergy Communications (www.masergy.com)
Miercom (www.miercom.com)
NetScreen (www.netscreen.com)
Nortel Networks (www.nortelnetworks.com)
Quarry Technologies (www.quarrytech.com)
Qwest (www.qwest.com)
Savvis Communications (www.savvis.net)
Sprint (www.sprintbiz.com)
Telseon/OnFiber (www.onfiber.com)
VeriSign (www.verisign.com)
Virtela Communications (www.virtela.net)
WorldCom (www.worldcom.com)