Understanding VPN Technology Choices
Comparing MPLS, IPSec, and SSL

Background
Telecommunications networks are evolving naturally toward IP-enabled platforms as a replacement for private lines. Networks are also converging, since with IP technology, a single network can support both voice and data requirements. These converged networks are easier to manage, and should deliver high availability, network security, scalability and Quality of Service (QoS).

Three basic IP VPN technologies are used today to create network architectures: Multi Protocol Label Switching (MPLS), IP Security (IPSec) and Secure Socket Layer (SSL). Many companies are using combinations of these VPN technologies to design unique solutions that will meet their business needs. Understanding the options will help network managers make good choices and design an optimized infrastructure that makes the most of the available technology.

- MPLS is the baseline technology that supports a modern converged network, and provides its own built-in level of network security.
- IPSec is a technology that has been adapted from a host-to-host and remote access technology to one that supports networking.
- SSL is a technique for providing “client-less” network access by allowing secure transactions through a web browser.

In some cases, these technologies may be used alone. However, they’re more likely to be combined in some fashion to support different needs. A single enterprise may find requirements for all three, since each technology has its own strengths and weaknesses.

The MPLS Foundation
MPLS is a core enabling technology which supports the definition of a private IP routing domain on a packet switched network, using label-switched paths. Each packet that traverses an MPLS network carries a label that identifies its VPN membership, where it’s going, and the importance of the data payload. This supports a concept called Quality of Service (QoS), which allows some packets to be assigned a higher priority; therefore, assuring a higher level of performance. By keeping latency to a minimum, QoS enables a network to handle the more demanding requirements of Voice over IP (VoIP). In concept, an MPLS network is a mesh structure, rather than a traditional hub-and-spoke design. That means it can offer any-to-any connectivity, which allows for very efficient data transfer and highly dynamic load balancing.

As a mesh network topology, MPLS is ideally suited to a carrier or service provider model that provides connectivity to multiple customers with many sites. While serving multiple customers, the network must be configured to handle enterprise traffic in a unique, secure and scalable fashion. This is commonly accomplished by setting up the network’s own edge devices to recognize and process the traffic appropriately, creating a Virtual Private Network (VPN) within its own system of routers, cable and fiber. Using route distinguishers, MPLS enforces traffic separation between multiple VPNs on the same network. An MPLS VPN offers many advantages from the customer perspective. It’s easy to manage, highly secure, flexible, scalable and supports both small and large VPN deployments. As mentioned above, it can deliver the QoS functionality that’s needed to support a converged network of voice, video and data. It provides very robust end-to-end communications, as long as all the end-points are connected to the carrier’s own network.

An MPLS VPN can easily support various network computing paradigms for network applications (such as client-server, peer-to-peer and hub and spoke). MPLS can also enable multiple network services on a single network infrastructure (such as Frame Relay, Ethernet and ATM) where the synergies of L2 and L3 VPN connections may be provided. Plus, it supports high-speed access in a “technology agnostic” fashion – different types of IP-aware devices can be integrated easily into an MPLS platform. That makes network expansion a very straightforward exercise.

Perhaps the biggest inherent advantage of MPLS may be the flexibility it brings to disaster recovery. Because MPLS networks can support multiple iterations of the same application, running in physically separate locations, they will always be more robust and better able to cope with the loss of a single processing center.

MPLS VPNs offer many advantages; however, there are issues that may need to be addressed. For example, businesses no
longer have end-to-end control of routing. Companies need to work closely with their MPLS providers in order to understand how routing decisions will be made in the backbone. Some add-on hardware may be needed to meet special security requirements (such as encryption), or if the MPLS network needs to bridge to a point that lies outside the carrier’s network. Finally, customers supporting e-commerce applications may need to implement additional SSL components able to secure credit card transactions made through a web browser.

MPLS is becoming the primary technology used for a foundation infrastructure, especially for companies that want site-to-site, mesh-style connectivity. It can handle converged traffic (supporting data, voice and video). MPLS is a good option for enterprises needing to deploy value-added applications (multimedia, conferencing, e-collaboration) and business process applications (enterprise resource planning, customer relationship management). Deploying an MPLS network can allow a company to move toward IP-enabled call centers, providing cost efficiencies and improved customer experience.

Let’s take a closer look at how to address some of the issues associated with MPLS VPNs.

### Bridging with IPSec

IPSec is complementary to MPLS VPN technologies. Where an MPLS VPN is a networking technology, IPSec is a technology for defining encrypted and authenticated flows across a packet switched network. It was initially defined as a host-to-host encryption protocol, but has since evolved into a technology that can support gateway-to-gateway and host-to-host protection. IPSec is often thought of as a security technique, but in fact, it’s also a networking technology. IPSec could be used in addition to MPLS, or instead of MPLS, depending on business needs.

The key advantage of IPSec is that it provides a way of establishing a VPN connection through the Internet. IPSec can be used to extend access to the MPLS VPN by supporting remote users and supply chain partners. It is often used to meet connectivity needs that are outside the MPLS carrier’s space. IPSec can also provide added security to the MPLS VPN. For industries that are highly regulated, such as banking and healthcare, IPSec offers an extra level of protection through encryption and authentication.

IPSec enforces data confidentiality by encrypting packets before transmission. It helps ensure the integrity of data by authenticating packets, and validates the origin of data by authenticating the source of packets that are received. Finally, IPSec can help prevent attacks by identifying aged or duplicate packets.

IPSec is not a client-less solution. It does require some kind of application driver in hosts or a dedicated device to enable the connection. Each router must be configured to understand all the other routers in the network, which can be a maintenance nightmare if there are many locations involved. With IPSec, making structural changes, adding new locations or connecting with additional networks will involve a fair amount of configuration work. Compared to MPLS, an IPSec network will be harder to manage.

Businesses do not always have to choose between IPSec and MPLS. For example, a company with bandwidth limitations in its Frame Relay network would have trouble coping with the additional demands of VoIP and video. However, it may establish an IPSec network in parallel, and use this second network to support the video or voice traffic. In addition, the routers can be configured to fail-over to the IPSec network if the Frame Relay network went down. This second network can provide both additional bandwidth under normal circumstances, and an on-demand backup network for emergencies.

IPSec is a good choice for:

- Enterprises that need additional security measures beyond traffic separation
- Enterprises that communicate mostly through hub and spoke
- Enterprises that are looking to deploy a solution across an existing network
- Enterprises that need access to geographically dispersed employees

Within the basic IPSec technology, a recent development known as Dynamic Multipoint VPN (or DMVPN) allows for a “partial mesh” network. Using IPSec, it facilitates the creation of dynamic tunnels, which can be brought up and down based on traffic patterns. However, DMVPN tunnels do not need to be configured at each node, so it’s an approach that will reduce some of the configuration and maintenance overhead of IPSec. Each spoke has at least one “always up” connection to the hub, which serves as the routing database and adjacency server. The hub can also invoke an “on demand” connection to another spoke. A DMVPN approach can improve communication, streamline management and lower maintenance cost.
SSL for the Web

SSL, simply put, is a way to provide secure communications through a web browser. It secures connections by authenticating and encrypting traffic between users who are communicating. SSL is often used as an e-commerce technique, but can also be a tool for controlling remote access. However, it’s not really a networking technology, and is not designed for site-to-site VPNs.

The chief advantage of SSL is its ability to establish security in a client-less environment. That’s a serious plus in a world where many people work from home, or want to connect to corporate networks from Internet cafes. Compared to IPSec, SSL is less cumbersome to administer, and it can still be used as a tunneling technology. With SSL, enterprises can limit access to specific Web pages or internal resources, providing entry to only specific information the user should view.

In an environment where the IT department has limited control over the end devices, this technology might be the right choice. SSL can also be used as an add-on to complement an IPSec network, in order to deliver the ubiquitous access needed in a broadly available Extranet. The technology can also be used to access corporate resources from remote kiosks, and reduce the deployment of IPSec software clients.

SSL has its limitations. It’s reasonably straightforward for web applications, but legacy applications that are less Web savvy may require some downloadable client components. SSL-based VPNs do not support applications not coded for SSL, such as Telnet, FTP, IP telephony, multicast applications and applications that need QoS. An SSL server needs adequate processing and memory, as the technology is computing-intensive.

It is important to encrypt and remove any cookies and session information when using SSL clients in public areas. Vendors are beginning to offer technologies to ensure that employee and corporate data are not left behind in public machines. Even with these limitations, SSL may still play a role in the enterprise environment for companies that want to offer broad, client-less access to internal systems. The technology is best used for short duration access, communication with partners or customers, access to specified company network resources and browser-based connections from home personal computers or kiosks.

Summary

To see how all three of these technologies might work together, consider the business model of an airline. Here, MPLS is ideally suited for the carrier, bringing all the airline’s facilities together in a converged mesh design. IPSec components could be added to connect to supply chain partners, travel agents and others who might need regular and ongoing communications with the airline’s internal systems. Finally, an SSL component could support self-service ticketing through a Web site, dealing with the part of the business that needed clientless connectivity.

IP-enabled networks are certainly the way of the future, and an MPLS VPN is likely to be the network of choice for many large enterprises. The addition of IPSec and SSL protocols can reach beyond the limits of the MPLS carrier, and also provide additional capabilities on top of an MPLS platform. The intelligent combination of these technologies can cover most situations a company is likely to face.

Getting informed advice from a networking expert is the right way to start.

For more information visit AT&T’s Networking Exchange, at www.att.com.