Which VPN? Applications for IPsec and MPLS

IPsec and MPLS VPNs satisfy different site requirements but are often used together for maximum benefit.

There are several types of virtual private networks (VPNs). The two most prominent for supporting employee access to enterprise IT resources are IPsec and Multiprotocol Label Switching (MPLS) VPNs. It is possible to use just one type or the other, or to use both together in a hybrid deployment. What will typically determine whether a given location connects using an IPsec or an MPLS VPN are the following factors:

- The size of the site to be connected
- How much bandwidth you need at that site
- Your performance reliability requirements for that site
- The degree of direct connectivity to other corporate sites (and possibly extranet sites) that you need at the location
- Your WAN connectivity budget for the site

The primary differences between IPsec and MPLS VPNs are technical in nature and relate to their underlying network foundations. These differences affect speed, performance, reliability and cost, depending on implementation. However, when properly configured, both provide appropriate levels of network privacy and security for enterprise business use.

Most IPsec VPNs connect sites using public Internet transport, which is comprised of interconnected networks run by multiple carriers. These VPNs use industry-standard IP encryption technology (called "IPsec") to render the data transmitted private across network borders. There are a couple of different configurations available, which will be discussed in the next section.

MPLS VPNs connect sites using a single carrier's MPLS network. That carrier should have complete management control of the network, including the ability to enforce quality-of-service (QoS) policies on specific traffic flows. MPLS VPNs partition one customer's traffic from another's to keep it private across the infrastructure. The partitioning is created using special MPLS tags rather than encryption. A hybrid VPN is created when individual IPsec VPN sites connect to an enterprise MPLS VPN.

IPsec encryption is sometimes (although rarely) used in conjunction with an MPLS VPN infrastructure; in effect, running a VPN within a VPN. While this configuration might be considered security overkill, it is often selected by more security-sensitive organizations, such as government defense agencies and financial institutions.

Let's look a little more closely at which type of service you'll likely want to install at each of your sites based on the criteria listed above.

IPsec and MPLS VPN Applications

In many large organizations, both types of VPNs exist. What type best matches each location?

MPLS VPN Use Cases

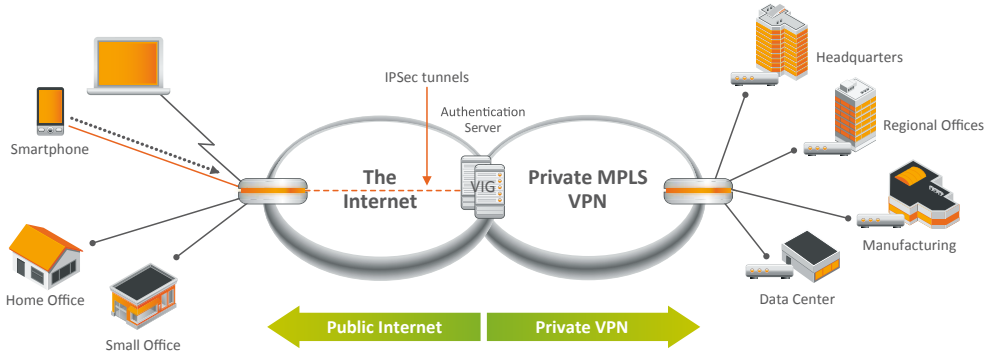
As noted, the MPLS VPN is a high-speed, single-carrier-operated network that maintains traffic separation between different customers streams using the network. It allows one of your sites to link directly at high speeds to any other of your MPLS VPN site(s) without going through the public Internet.

Central and regional data centers usually connect directly to the MPLS VPN service as do other large organizational sites. The MPLS VPN service is generally considered your enterprise's primary WAN service – in effect, your own private WAN – and is deployed at sites requiring significant bandwidth and performance reliability. Greater reliability and performance are possible over MPLS because it is under the control of a single operator and because MPLS technology supports traffic policy enforcement. This results in better quality transport for time-sensitive traffic, such as streaming real-time video/audio or live voice-over-IP (VoIP) calls. These apps perform better when they don't have to travel through a central hub site on their way from point A to point B.

IPsec VPN Use Cases

IPsec VPNs often complement the MPLS VPN service at smaller sites and work well for low-speed data transfers to corporate data centers. These sites might be small satellite offices, home offices and even traveling/mobile workers at an airport or coffee shop. IPsec-enabled sites and user devices can connect to the corporate MPLS VPN using readily available, low-cost remote-access broadband connections, such as DSL, cable modem, private-line and cellular data connections.

Mixing and matching VPN service types



It can be quite cost-effective to use IPsec VPN services in highly dispersed organizations with lots of small locations, such as retail chain stores, restaurants and small bank branches. Regardless of the physical wired or wireless connection type, IPsec VPNs can ultimately terminate directly at the corporate data center or at the enterprise's MPLS VPN point of presence.

Choosing the termination point depends on your network traffic patterns. If your organization is a largely "hub-and-spoke" configuration, with lots of small sites that need to communicate only with a data center, you might run IPsec VPNs only. If these sites might need connectivity to other corporate or extranet sites, you'd likely want to connect them to a corporate MPLS VPN service, which is highly meshed in nature and dedicated to your organization (see figure).

IPsec VPNs have a few configuration options:

On-premises encryption with public Internet transport. The IPsec encryption can take place on-site at your enterprise location in a router or firewall. Data remains encrypted across the last mile and public Internet. This is the least expensive option from a service-fee perspective, in that you create the encrypted tunnels yourself.

Network-based encryption with public Internet transport. This is a managed service option. Your network operator handles the encryption at your first point of presence in the WAN. Your traffic is encrypted across the public Internet but not across the "last mile" broadband link. This is a little more costly than the on-premises option above, in that you pay the service provider something each month to manage the encryption function; however, you offload the cost of encryption purchase and maintenance in-house.

Both options above are less expensive than MPLS services, but, because they traverse the public Internet, the same levels of performance are not guaranteed. The IPsec VPN option below helps improve performance.

Network-based encryption with "private" IP transport. This service is similar to the options previously described, except that all IPsec sites connect to a single carrier's IP network (not the multi-operator public Internet). Because a single operator manages and troubleshoots the network, performance is improved.

Summary

There are good reasons for running both IPsec and MPLS VPNs. Very highly distributed organizations with lots of satellite offices and very little need for direct, site-to-site communications among many sites will likely want to run mostly IPsec VPNs. Larger organizations wishing to run performance-sensitive applications among many sites will likely opt for MPLS VPN services at those sites, because MPLS VPNs have fundamental traffic engineering and QoS capabilities to support optimal performance.

Often a hybrid IPsec/MPLS VPN will be deployed, whereby satellite sites and mobile workers connect to the MPLS VPN across a public Internet connection. And in rare cases, IPsec traffic will traverse the MPLS VPN for a double layer of security. The attributes of the most commonly used VPNs are summarized in the box below.

VPN Type	Cost Level	Performance Level	Security Level
IPsec VPN (on prem, Internet based)	Lowest	Lowest	Very High
IPsec VPN (managed service, Internet based)	Medium Low	Medium Low	Very High
IPsec VPN (single carrier's IP network)	Medium	Medium-High	Very High
MPLS VPN	Highest	Highest	Very High

For more information please contact your AT&T Solution Provider.

at&t Solution Provider

05/21/13 AB-2703