Executive Summary
At first glance, it might seem logical that the public Internet, paired with IPsec encryption, could take on the job of your corporate WAN. Using the general public Internet in a few select sites as an access mechanism to your WAN backbone often does make sense. But overall, the Internet doesn’t meet the capacity, performance and uptime requirements of today’s converged applications. That’s because the public Internet generally treats all traffic the same, regardless of its importance or latency requirements.

While IPsec does a fine job of securing data in transit, there are additional types of security and enhanced WAN services you need to run a truly business-class network that delivers the user experiences employees are expecting. Simply put, the public Internet doesn’t match the performance, reliability and security of an MPLS VPN.
Introduction: Transport vs. Enhanced Service
Now that the public Internet is very fast and has a near-ubiquitous global reach, why would a business still need a Multiprotocol Label Switching Service (MPLS) virtual private network (VPN)? After all, you can encrypt data to protect it in transit over the Internet using established protocols such as IPsec. And a generic, consumer-class broadband connection is much less expensive than an MPLS VPN connection.

These statements are all true. But they are also short-sighted, because the ability to encrypt data in transit and low per-connection costs are where the benefits of a vanilla Internet access service come to a screeching halt.

The public Internet, with or without IPsec encryption, is focused strictly on the transport of data packets with no quality of service (QoS) enforcement, uptime guarantees, ability to expand or contract capacity as needed, multicast capabilities or integrated resistance to distributed denial of service (DDoS) attacks. You basically pump your packets into the Internet and hope for the best. The design of the public Internet has worked fine for e-mail and file transfers over the years, but isn’t suited to today’s dynamic converged application traffic patterns.

Specifically, consider a few reasons that an Internet/IPsec network doesn’t make the grade for business traffic.

Capacity Limitations
A single commercial Internet connection doesn’t have enough capacity to support converged applications and multimedia traffic. Video is the fastest growing application generating traffic today. When in use, it will overwhelm a consumer-grade broadband Internet connection and knock out all other traffic. As a remedy, enterprises end up purchasing and managing multiple connections to get the capacity they need during peak traffic periods, which adds cost and complexity to the equation.

Static Nature
IPsec Internet connections tend to be point-to-point and static in nature. They address situations where one site communicates exclusively with another site, reflecting the hub-and-spoke network traffic patterns of the 1990s. Today, users are dispersed across any number of locations including mobile ones and want to communicate with any of the others. They tend to communicate using multimedia applications that are collaborative in nature. These apps need the ability to run directly between any two sites, rather than through a hub site before jumping off to the receiving site, to achieve the low latency required for real-time communications to work properly.

Vulnerable to DDOS
Even if your traffic is encrypted, the Internet doesn’t protect you from service outages caused by distributed denial of service (DDoS) attacks. Your own IP addresses won’t be able to be spoofed if encrypted. But if others are, you’re susceptible to the resulting downtime.

No Support for Multicast Traffic
Another drawback is that you can’t efficiently send multicast communications to multiple select nodes using an IPsec connection. Generally the Internet does not support multicast. Add to that, when you create IPsec point-to-point tunnels, you could in theory support a multicast app, but you’d be replicating it over each IPsec tunnel asunicast, so you’d get no bandwidth savings like you would if the multicast replication was done in the network rather than at the source.

An MPLS VPN, on the other hand, is a business-grade service that avoids the public Internet and the delays, outages and risks that go with it. It has been engineered with QoS, resiliency, capacity flexibility and business continuity built in. It provides layers of enhanced services specifically targeted toward business-grade traffic, high availability and consistent user experiences. It also efficiently handles multicast transmissions in the network.

Security: Important but Alone Not Enough
VPNs were initially invented to secure customer traffic across public WAN infrastructures that customers would share. When they share a WAN, customers may benefit from substantial economies of scale, compared to the cost-prohibitive option of each enterprise building its own private network. “VPN” services build in some form of privacy through a shared network, though there are many technological ways to do so.

An IPsec VPN, for example, offers protection against data theft in transit across the shared public Internet using a specific type of industry-standard encryption. An MPLS VPN, in turn, offers segregation of data across a single operator’s business-class WAN infrastructure. It accomplishes this by segmenting each customer’s traffic from others using an industry-standard customer identification tagging technology known as “Multi-protocol label switching.”

Both IPsec and label switching (MPLS VPN) can be thought of as carving out a private tunnel for each customer through the WAN. Ultra-security-conscious companies can even take a belt-and-suspenders approach to security and encrypt their traffic across the MPLS VPN, creating a VPN within a VPN, so to speak.

In addition to keeping traffic private as it routes across a common network architecture, MPLS VPNs are not susceptible to DDoS attacks which are becoming increasingly common on the Internet. Since private address space is used with an MPLS VPN, customers are not susceptible to having their addresses hijacked, used as spoofed source addresses (as mentioned earlier), or other threats that exist in the public realm.

Paying for What you Get: The Value in MPLS
Along with supporting additional security, MPLS has been designed as a bona fide application networking platform for business, so it layers many other business-class network service enhancements on top of secure transport. These attributes are not available with general-purpose Internet/IPsec services and include the following:

- Inherent infrastructure redundancy for business continuity that translates into re-routing around failures in milliseconds rather than seconds or minutes.
- Class of service (CoS) capabilities to prioritize and manage traffic so that the most important or delay-sensitive traffic is delivered first.
• Direct site-to-site connectivity, sometimes called “any-to-any” connectivity. This inherent capability enables business sites and remote and mobile users to exchange voice, data and video traffic directly with one another, rather than requiring traffic to traverse an extra “hop” at a central site, which slows performance, to get to the preferred destination. Combined, CoS and any-to-any connectivity ensure the continual high performance of business applications and are a must for real-time applications such as voice and video. Increasingly, business users are taking advantage of real-time apps that embed voice and video — from room-based telepresence conferencing to FaceTime or Skype applications — in order to collaborate meaningfully across distributed geographies. Other apps of this sort that are becoming common are chat and social media.

• Single-operator management and control. Also, because MPLS VPNs are owned and operated by a single network service provider, that provider has the ability to engineer and manage the network so that your traffic behaves in accordance with your policies and priorities. The general Internet, on the other hand, is a conglomeration of many service providers who control only their own segment; once they pass traffic across network borders, any policies and priorities that have been specified for how to handle traffic disappear. In addition, your ISP can’t control or escalate an outage or service degradation whose root cause is in a physical segment of the Internet controlled by a different provider.

• Multicast capabilities for bandwidth savings.

The Upshot
You can encrypt data traversing a broadband access link using IPsec (or other protocol), but securing the business data in transit is where the benefit of the IPsec VPN ends. A business-grade VPN, such as an MPLS VPN service, on the other hand, mitigates additional types of risk while offering network service enhancements honed to make user experiences enterprise-grade, consistent and reliable. So the decision boils down to cost versus value and your business need. In some cases, a hybrid of both types is in order, which is discussed in the next section.

So Who Uses IPsec VPNs?
Now, if a single site only ever communicates with one other site, and the apps running between them have little sensitivity to delay, jitter or packet loss (such as bulk file transfers), the IPsec VPN option might suffice.

Some companies also use an IPsec VPN as a lower-cost access network into the MPLS VPN, where they can then pick up the CoS, uptime and high-performance benefits of the MPLS environment. However, the longer the “ride” on the MPLS network, the greater the uptime, performance and network security benefits of the MPLS environment. This is an important consideration, because the fact that you are mixing multiple types of real-time apps that are delay sensitive with others that aren’t drives complexity and very specific requirements from the network service you use. The public Internet doesn’t deal with any of this; it doesn’t distinguish between application types and doesn’t prioritize.

In addition, IPsec, which was initially created primarily for encrypting router traffic between two fixed sites, introduces a couple of other issues. IPsec adds significant overhead to the transmission; in other words, when you encrypt your packet flows using it, you have less network capacity to use for your application traffic. A 64-byte packet encrypted using IPsec Data Encryption Standard (DES) or Triple DES (3DES) would see an addition of 45 bytes to the original packet for a total of 109 bytes (a 70% increase). If you picture a congested highway then take away 70% of the road available to the cars and trucks, traffic slows by that much more.

Mobile WAN Access to an MPLS VPN

Mobile VPN scenario: Your MPLS VPN provider supplies software that routes mobile clients directly from its mobile WAN core to its private MPLS VPN (and the enterprise’s MPLS VPN service). Traffic bypasses the public Internet.

Mobility and Your VPN
If yours is like most organizations, you’re seeing an explosion of network traffic coming from your mobile user population. MPLS VPNs have been designed to accommodate that traffic in a couple of different ways.

For example, you can terminate all mobile device connections at a predetermined MPLS VPN gateway in your VPN provider’s network directly through the provider’s mobile WAN core. The gateway serves as an “on-ramp” to your MPLS VPN. You can accomplish this by installing a mobile VPN client application on user devices programmed by your MPLS service provider to terminate wireless connections at the MPLS gateway. Your provider supplies the software as an MPLS VPN mobility add-on service. The setup bypasses most of the public Internet and the security hazards, congestion and performance problems associated with it.

Another approach is to install a custom subscriber identity module (SIM) card in your mobile workers’ devices. This option generally addresses single-app or custom, vertical-app devices that the company wants to connect only to certain environments. The purpose of the SIM is to create a closed user group comprising those SIMs, which are programmed by your MPLS VPN provider to route the device to the mobile network operator’s data center. This setup also helps to bypass the public Internet.
Conclusion
It pays for businesses, in most cases, to bypass the public Internet from a performance and business continuity perspective. Most often, the way to do that is to use an MPLS VPN, the current gold standard for business-class network services for all the reasons described. Generally speaking, IPsec is best used for predictable, point-to-point and hub-and-spoke-style traffic and in situations where security is not paramount, given that protocols can be snooped and broken on the public Internet.

An MPLS VPN has been built as a fundamental dynamic networking platform containing all the security, performance, availability and flexibility needed to handle the any-to-any traffic patterns that today's networks must support. An MPLS VPN will not only protect your ability to send data and the use of app services against a variety of risk types; it may also unify your voice, video, data and mobility communications, enhancing their use with greater performance when compared to the public Internet. Better user experiences could translate into greater productivity and revenues, so using MPLS as an alternative to the public Internet will likely be worth the investment for most businesses.