

Is MPLS Right for Your Organization?

Web Log link: <http://www.mplslosangeles.com/mpls-vpls-IPSEC-QOS.html>

Justin Ream is Vice President of Operations for Tierzero.

It is an enormous challenge for Corporations with multiple sites to deploy a communications network to connect all of those sites together securely and reliably, never mind affordably. The buzz in the industry today is all around **MPLS**, and rightfully so. The following information is based on my experience designing and installing MPLS and should help you decide whether or not it's the right solution for your organization. Key factors to consider are budget, technical resources, contract expiration dates, and security risks among others.

History

MPLS arose from the need to create private wide area networks that scaled easily and economically. Before **MPLS**, the only way to connect remote sites was to do a star and hub topology and buy expensive point-to-point links.

Internet was an alternative, but it was complex and not secure. Before long, people developed firewalls with site-to-site VPN technology that allowed them **connect offices** via the internet using **IPsec encryption**. Aside from the expensive hardware, you almost needed a degree in rocket science to design and deploy it. While things were still complex, **MPLS** started to become mainstream, allowing remote sites to connect to a local provider that would then "Label Switch" traffic to another remote site. The price was about the same as a typical Internet link and accomplished the private connection between sites that managers needed.

Since **MPLS** was not supported by all carriers and not all carriers provided service nationwide or even worldwide, **MPLS** suffered from "gaps" in geographical coverage. For example, if you had a Verizon connection in Los Angeles and an Altel connection in New York, and both offered **MPLS**, you still couldn't really deploy **MPLS** because the system required the same carrier covering each end. Consequently, managers had to rely on **IPSEC tunnels**, which require expensive firewall equipment at each site, (like Cisco PIX, Netscreen, Checkpoint, or some other firewall). Typically consultants had to be hired to pull all of this together. So **MPLS** and IPsec were "competing" technologies, both providing viable solutions, but each with their own drawbacks.

The Money Issue

Which brings us to cost. Typically an **MPLS** link is about the same price as a T1 Internet link. So if you have one main site and five remote sites, and the average price on the T1 is \$500, you would usually buy two **MPLS** T1s at the main site, and five single **MPLS** T1s at each remote site. Your monthly cost would be \$3500. For five sites, you would need at least two T1s for internet access at the main site. That puts you at \$4500 per month. In an **IPSEC** multi-firewall configuration your remote sites already have internet access, so you would just need to buy seven Internet T1s, for a total of \$3500 per month. **MPLS** typically costs more than Internet T1s, not in loop costs, but to cover the price of the additional T1s required at the main site to reach the internet.

So Why MPLS?

So if **MPLS** is more expensive than Internet T1s using **IPSEC** firewall VPNs, why go **MPLS**? Well, **IPSEC** firewalls cost money. They are an up-front capital cost, and not a recurring charge. They also require technical know-how and resources to maintain, not just at the main site but at each remote site also. The more sites you have, the more firewalls to maintain. That is an indirect expense that comes in the form of employee cost. Some ISPs, such as ourselves here at Tierzero* offer **IPSEC** or GRE services which is a more affordable alternative.

IPSEC: Maybe We Should Take Another Look.

This is a particularly well written article that fairly espouses advantages and disadvantages of the MPLS network. This has been a broadly covered debate since 2003 and not all opinions on the matter have stood the test of time. The author and Tierzero contributors do a wonderful job capturing the very real high-level decision points that distributed enterprise IT leaders must consider. As a matter of record, Contingent does not disagree with any of the authors viewpoints. However, we will offer insight into how we mitigate risks in choosing to optimize an IPSEC VPN vs. migrating to MPLS.

Contingent does not employ "rocket scientists" but does employ network engineers that have diverse and extensive experience in designing and configuring networks of all kinds. Our skills in the appliance-based IPSEC arena are incomparable.

IPSEC VPN deployed using a standard edge device reporting to a core VPN concentrator has no geographic limitations. 100% coverage is possible without direct interconnection cooperation between the carriers like what is proposed with MPLS-ICI.

The EverWorX IPSEC VPN can be deployed using any of the devices the author mentions but when a client does not have an existing network or desires to upgrade Contingent has a cost effective approach. A new EverWorX IPSEC VPN uses a robust, PCI compliant edge device from Secure Computing that has a retail price of \$350.00. This solution supports most if not all of the functionality of a Cisco Pix at less than half the cost. Contingent routinely eliminates all up front costs and amortizes that cost over the life of the contract (typically 36 months).

Contingent's EverWorX IPSEC VPN can be deployed over any local loop WAN technology including xDSL, Cable, Fixed Wireless, Mobile Wireless, Satellite and as a last resort, T1. Contingent seeks the best available technology for a given location and provides T1 speeds at a fraction of the T1 cost. Even the main site can be treated like a remote site since the EverWorX core can be hosted in a Contingent collocation vastly simplifying the network design.

Safety

Security is another benefit factor for those considering **MPLS**. **MPLS** is very secure because it is virtually a private link. No Internet, no security threat. Many banks, government institutions and security agencies require the security of **MPLS** because the Internet is vulnerable to attacks, hackers and other malicious activity. **IPSEC** encryption is only as secure as your last employee. Internet T1s have public IP address space which leaves room for human error, such as bad firewall rules. **MPLS** T1s are private and since nothing is exposed, there is no exposure. The only place the network could be hacked into is through the Internet T1 connection, not the **M P L S** T1s. But that's why you have the firewall at the main site. Keeping track of one firewall is far easier than keeping track of six or more at every remote site. **MPLS** decreases your vulnerability from multiple points to a single point. This is good, very good.

Commitment

Contractual obligations are another key factor in the equation of WAN connectivity. All of your sites may not have all the same contract end dates. This is a drawback because **M P L S** usually requires you to move all circuits at once, if you don't want to end up double paying for service. One option is to hold on to your Internet connection to the main site while replacing your **IPSEC** Internet T1s with **MPLS** T1s. This way you fulfill your contractual obligations but still move your network to **MPLS**. If this doesn't work, then consider running a hybrid of **MPLS** and **IPsec** and as your contracts expire, you can move your circuits from the **IPSEC** to **MPLS**. Still some ISPs may allow you to move their Internet T1s to an **MPLS** T1 if they have the offering.

And So...?

In conclusion, **MPLS** can give you significant benefits in terms of simplicity, scalability and security. Its drawback is monthly expense and the need for packet classification and prioritization. **IPsec** VPNS can give you savings in monthly expense, but bring extreme complexity and maintenance obligations as well as higher upfront costs. These are the factors you need to weigh before opting for either solution.

If you have any questions, please feel free to contact me at jim.gurol@tierzero.com

*Tierzero is a Los Angeles based ISP specializing in **MPLS** and **IPsec** VPN.

The technical know-how to manage the **IPSEC** VPN in the EverWorX service lies with Contingent's professional staff. The Technical Assistance Center is manned 7x24 and is moderated by an SLA that stipulates that when the network is down for any reason, the client does not pay. The TAC is managing thousands of other **IPSEC** tunnels and has the tools and the leverage to support a network that would otherwise require costly resources the author cites.

The EverWorX design is extremely flexible and one of the safety features is that the security policies and access controls are managed at the Contingent core VPN concentrator where all access (if any) to the Internet is regulated. There do not have to be Internet access rights granted to the remote site and the remote site has but one connection back to the core via VPN tunnel.

EverWorX contracts can be written and priced on a coterminous basis or on a staggered basis. Clients can easily add and remove remote sites without penalty. The contracts have 30 day cancellation without cause features allowing for easy migration to alternatives.

Contingent is not a carrier and not a hardware VAR and not a carrier's agent so we deal with the interests of the client at the front and because we have a rigid service SLA we have little patience for underperforming elements of the **IPSEC** VPN network.

If you have questions, please feel free to contact me at mstuhfreyer@contingent.net

*Contingent is a Cincinnati based Managed Network Services provider specializing in managing well the right networks for its clients.