



IPVPN

High Level Overview of IPSec and MPLS IPVPNs

Date: 16/02/05

Author: Warren Potts

Version: 1.1

Abstract

This document provides a high level overview of the differences between IPSec and MPLS based VPNs





Review of IPSec and MPLS

The goal of VPNs is to provide inter-site connectivity over a shared infrastructure., whereby the users at the end sites enjoy the same access and integrity of service that would be available if accessed via a private network. Therefore any solution must be secure from external access and manipulation, be reliable, not detrimental to access speeds, scalable and not burdensome on resource.

There are 5 broad categories of service defined by Cisco that a VPN must adhere to.

Scalability	Must be scalable across VPN platforms ranging from a small office configuration through the largest enterprise implementations ubiquitously on a global scale; the ability to adapt the VPN to meet changing bandwidth and connectivity needs is crucial in a VPN solution. Additionally, in the fiercely competitive and dynamic market environment, large orders can be won and must be provisioned rapidly, hence the VPN must be highly scalable in order to accommodate unplanned growth and changes driven by customer demand. A typical MPLS deployment must be designed for highly scalable solutions, enabling tens of thousands of VPNs over the same network for maximum revenue and profitability
Security	Ensures business-critical traffic remains confidential via security mechanisms such as tunneling, encryption, traffic separation, packet authentication, user authentication, and access control.
Quality of Service	Ensures prioritization of mission-critical or delay-sensitive traffic and manages congestion across varying bandwidth rates. Quality of service (QoS) functions such as queuing, network congestion avoidance, traffic shaping, and packet classification, as well as VPN routing services utilizing an optimal routing protocol
Manageability	Essential for cost-effective provisioning to enforce security and QoS policies, management and billing, with advanced monitoring and automated flow-through systems to quickly roll out new services and support service-level agreements (SLA).
Reliability	For predictable and extremely high service availability that business customers expect and require

There are two VPN technologies that are widely available in the market. IPSec and MPLS. A line by line comparison is shown over

Category	IPSec	MPLS
Scalability	<p>Large scale rollouts need careful planning. Need to define key distribution and management, peering connections between sites and capacity planning of key infrastructure. Meshed networks need careful control</p> <p>Ideally suited to hub and spoke networks</p> <p>IPSec is suited where there is a mix of On Net and Off Net connections i.e. where connections are required across legacy services</p>	<p>MPLS easily scales to tens of thousands of connections and no need to determine peering policies between sites as this facility is inherent within the service</p> <p>Suited to hub and spoke or meshed services</p> <p>All connections must be ON Net</p>





	There may be interoperability issues between differing IPSec devices	Any device may be used to connect to the VPN
Quality of Service	<p>It is not possible to implement QoS across an IPSec network although it is possible to prioritise traffic at the router.</p> <p>There is a latency impact for encapsulation and encryption especially with low end CPE. This problem is compounded if ON Net and Off Net connections are used as the Internet carries no SLA. Additionally if routing to a remote site across a hub site all data will have to be encrypted and decrypted twice.</p>	<p>As all connections are ON Net and as PLS has inherent CoS mechanisms and traffic engineering capabilities, QoS guarantees and SLAs can be provided.</p> <p>No encapsulation and encryption issues in fact Label switching is faster than traditional routed networks.</p>
Security	<p>Provided via encryption and tunnelling methodologies</p> <p>All connections are Internet facing on public addresses, each node must be made secure.</p> <p>Each session/VPN membership is determined by digital certificate or pre-shared key. Certificates must be managed</p>	<p>Provided by traffic segregation</p> <p>Connections generally are on Private Address space (RFC 1918). These are not routable across the Internet. A closed VPN can have no access to the Internet</p> <p>VPN membership determined by initial VPN provisioning</p>
Reliability	<p>In a hub and spoke design, loss of the hub can lead to loss of the entire network</p> <p>In large networks a time server may be required to ensure that all devices are kept in synch increasing complexity of the service.</p>	<p>Loss of one site will not prevent other sites talking to each other.</p> <p>No additional hardware is required.</p>

The above services have concentrated on physical characteristics of the two VPN technologies the next section outlines through an example the potential differences in costs.



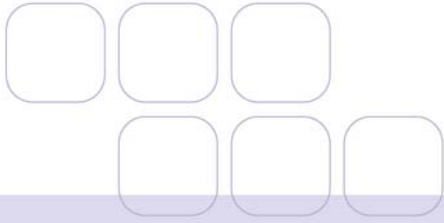


Cost Comparison - MPLS and IPSEC

The example below assumes that a company wishes to create a closed user group with 30 remote sites connecting to a head office site

Item	IPSec	MPLS	Notes
DSL Connections	£540/month	£930/month	This assumes that the IPSec connection is built on a WADSL service @ £18 month against £31 month for MPLS services. Prices based on Tiscali price book.
Labour content to manage rollout of DSL and adds moves and changes	£90/month		This is the project management and provisioning overhead to rollout the DSL network and provide subsequent management
Head Office Leased Line	£1000/month	£900/month	Services based on 2Mb connection. MPLS connection is slightly cheaper as no Internet access is required.
Management of Routers	£200/month	£200/month	
Management of firewalls	£500/month		No firewalls are required for MPLS therefore no cost.
Recurring costs per month	£2230/month	£1830/month	
Total Yearly costs	£26760	£21960	MPLS has cheaper opex costs in this example
Site Routers Zyxel 660Rs	£1500	£1500	
Site Firewalls Watchguard Soho	£5400		No site firewalls required by MPLS. To simplify the model no labour has been shown for configuring the Site firewalls, however this should also be brought in .
HQ Router Cisco 1700	£2000	£2000	
HQ firewall Watchguard 4500	£5000		No site firewalls required by MPLS
Total Capex	£13900	£3500	MPLS has cheaper capex
Total 1 year contract	£40660	£25460	
Total 2 year contract	£67420	£47420	





Note

1. It would be possible to go for cheaper firewalls however that needs to be assessed against the integrity of the network, ease of management and remote accessibility, feature sets and support. Although the ones featured could be considered budget.
2. The Wholesale DSL service has business hours support, Tiscali MPLS has 24 x7
3. The MPLS business VPN traffic has priority across the Tiscali core compared to Wholesale traffic.
4. MPLS traffic will take feature services such as QoDSL and VoiP when available.

