MPLS and IPSec VPNs Optimizing Security on the Business WAN

The need for end-to-end, secure connectivity has been driven by rapid business growth. Learn about several MPLS and IPSec VPN technologies.

CONTENTS

VPN Technology 2
What is MPLS 3
What is IPSec 4
A Comparison 5
Quality of Service 6
Complementary Technologies 7
Integrating IPSec with an MPLS VPN 7
The SonicWALL Solution 8
**Abstract:** The need for end-to-end, secure connectivity has been driven by rapid business growth, mergers and acquisitions and a move to an information-based business environment. Information is the currency of modern commerce and sharing information is what makes a company successful. Older business models revolved around maintaining individual silos of information, and each department or division within a company tended to be protective of their data. No longer. Over time, the business WAN has evolved, to the point where organizations now demands, and is provided with, high-speed connectivity, support for multiple protocols, multi-site connectivity and superior quality of service. In addition, rapid expansion, combined with the phenomena of telecommuting and the need to provide out-of-network access to clients and partners through extranets, has heightened the need for a new model of communication. Today's organization maximizes its competitive advantage by connecting each area to provide an enterprise-wide view of information, to provide the greatest level of service to the customer and to offer partners and key clients direct access to the data they need most.

This shift towards information sharing, as opposed to information hoarding, requires a firm foundation in secure networking technology. Use of technologies such as ATM and Frame Relay made it possible to connect multiple locations, helping to usher in this new era of openness in modern business. However, both of these technologies were, and still are expensive, and require a substantial investment in equipment and engineering time. Today, IPSec and IP make wide-area networking more affordable, since a company can take advantage of a service provider’s shared resource, or even the public Internet, to create their VPN at a small percentage of the cost for using a leased line or service provider network. In this way, organizations can connect multiple sites over a wide geographic area in a more affordable fashion.

**VPN Technology**

Today's new model of connectivity and information sharing brings up the problem of security. Information must be shared, but it must be shared securely. A VPN is a type of logical association of users within a larger network. The VPN sends traffic in a more secure private tunnel, through a public, shared network. This public network may be the Internet, or in the case of MPLS, a service provider network.

ATM and Frame Relay networks introduced greater capacity and speed to the WAN, as well as greater manageability through the use of virtual circuits carried over the Frame Relay or ATM cloud. However, these two networking technologies are limited in their ability to carry multiple types of traffic and are giving way to newer VPN alternatives based on Internet Protocol (IP). These VPNs allow for more flexibility in sending multiple types of information over the network. VPNs based on IPSec and MPLS represent the next phase of wide area networking, allowing for the creation of multiservice networks that can carry any type of traffic.

The concept of the VPN remains the same, although modern VPNs have evolved to include more functionality, security and the ability to carry multiple types of traffic. And like most technology, the cost has been driven down as newer innovations offer improvements at a lower price point. For example, while ATM offered organizations the ability to create multiple VPNs over a wide area, deploying an ATM network is costly and required a major forklift upgrade of equipment, and its reach is limited to sites that lie within the ATM cloud. IPSec VPNs, on the other hand, allow for this secure remote connection to be established over a shared infrastructure that is already in place, using an open standard. On the provider side, it's getting more difficult for providers to protect their installed base of Frame Relay and ATM installations, as more customers find the advantage of IP-based VPNs offer far more utility and cost-savings.

Transmitting corporate data over the public Internet naturally brings up a great many security concerns. At its most basic level, a VPN of any type, by virtue of its ability to separate data streams and group together different sets of users logically, does offer basic security by restricting the view of users to only that which is on their own VPN. However, the use of isolation as a sole security measure is limiting, and inadequate for most corporate implementations. VPNs based on IPSec technology go a step further by using encryption and authentication technology to create a secure, private tunnel through an otherwise unsecured IP network. Incorporating a security appliance with a Unified Threat Management (UTM) architecture is another essential step to prevent blended attacks from infiltrating the network.
VPNs are constantly evolving, and a study by Infonetics Research noted that technology change is the main reason companies replace their VPN products. According to the Infonetics study, security is a major concern for companies implementing VPNs, with over a third of the respondents citing security as a barrier to implementation.

**What is MPLS**

Multiprotocol Label Switching (MPLS), an IETF standard that integrates Layer 2 (network) information into Layer 3 (IP) systems, is a type of IP VPN that is implemented as a managed service over a service provider's proprietary network. MPLS was designed to replace older Frame Relay and ATM technologies. Unlike those older technologies, but like IP, MPLS is a multiprotocol technology that can carry multiple types of traffic over the same pipe.

As a marketing tool, MPLS has been very useful to service providers, who are anxious to continue to provide lucrative managed service contracts. Many service providers are suffering from declining revenues from traditional voice services, and diminished revenue as customers migrate from high-margin Frame Relay and ATM services to low-margin IPSec VPNs that use the public Internet as a backbone. Unlike the IPSec VPN, MPLS runs over a service provider's proprietary network, and is usually offered as a managed service, and is therefore much more profitable for service providers.

Using MPLS, it is possible to create a connection between any two or more fixed endpoints within the service provider network. However, unlike IPSec, an MPLS network does not deploy equipment at the customer premises, and it requires every endpoint to be on the service provider's network. It is therefore not often used when connectivity to disparate geographic locations are required, and is impractical for remote, mobile connectivity applications. It is used, however, more often for connecting multiple large divisions or branch offices of a company that lie within a defined geographic region.

MPLS adds a label to each IP packet, making it possible to keep all packets from the same session into the same "flow." In the MPLS network, each packet is assigned a label by the label edge router (LER). Packets are sent through a label switch path (LSP), where the label switch router (LSR) forwards the packets based on the label that has been attached to it. At every hop, the LSR removes the existing label and applies a new one, which tells the next LSR where to send it.

The LSP is useful for routing around congestion and link failures, and to guarantee performance levels. This technology provides for effective site-to-site routing in a managed network, without requiring end-user intervention. The LSP is similar to the circuit switched paths created by the ATM network. Unlike ATM though, MPLS natively supports multiple protocols, including IPv6 and IPSec, IPV4, ATM, Frame Relay and Ethernet. As such, the LSP is similar to the circuit switched paths created by the ATM network. Also like ATM, MPLS does provide a guarantee of bandwidth for various traffic flows, making it very useful for scenarios where latency-sensitive traffic is being sent.

Because of the nature of the LSP, it is possible for a provider to route traffic based on data type or by customer category. Because of the labeling function, the network is able to separate high-priority traffic such as voice or video into separate data streams. But while MPLS is useful in creating site-to-site connections, it is not practical in creating client-to-site connections or to establish remote telecommuting functionality. Because MPLS requires a service provider network, it is not possible to connect all locations unless the service provider has established an infrastructure in that location. MPLS was not designed to establish connections from remote, mobile workers to headquarters; an IPSec or SSL VPN must be used to establish this type of telecommuting environment. In addition, while it is useful in creating a multiprotocol channel, it does not, by itself, offer much in the way of security in the transport of that data. A MPLS VPN provides for traffic isolation in the same way as ATM or Frame Relay, but does not include any function for encryption without the addition of IPSec. It is therefore possible for attacks to occur in which one VPN may intrude on another. It is difficult however, and if properly configured, attacks become very difficult. But the possibility of misconfiguration still looms large, and attackers being opportunistic, will look for these opportunities.
In fact, MPLS was not designed to be a secure protocol. The intent of the creators of MPLS was to create a way to label packets for more effective transfer, and it does that very well. However, MPLS does not encrypt those packets and they can be vulnerable to attack, wiretaps and other types of devastating hacks. It is also possible to spoof the customer address space or the MPLS label itself. That is not to say at MPLS is a deficient technology, just that a MPLS deployment should not be without an added security function. It is possible to establish a security point at the customer premises, typically with a separate firewall appliance deploying an IPSec VPN.

MPLS delivers full mesh connectivity to all points on the network. There may be some advantage to having every location on the network exposed to every other location, although with high speed networking and adequate bandwidth, these advantages become minimal. Technologies that pre-dated MPLS, such as Frame Relay, used a hub-and-spoke architecture. The hub model does present a distinct advantage that MPLS overlooks, that is, it is much easier to deploy security measures centrally, and prevent viruses, worms, spyware and other threats from infiltrating the network.

For example, suppose that a company's Dallas office has a DS3 connection to an MPLS network, and a branch office in London has a fractional DS3. If Dallas becomes infected with a blended threat, it could flood the MPLS link, saturating the London connection and causing a Denial-of-Service attack. In another possible scenario, let's suppose that a bank has a network of ATM machines. These often run an old version of Windows that is prone to attack from a blended threat. Suppose a technician hooks up a laptop to the network, and that laptop has been unknowingly infected with a worm. Every single ATM machine would become infected simultaneously, and the datacenter would be flooded with traffic, bringing down the system.

In light of these potential threats, the only solution for companies using MPLS technology is to protect the network by isolating traffic before it gets onto the WAN, by deploying a multi-purpose security device at each connection point to the MPLS network. The necessary protection can be achieved through deploying a security appliance that uses a Unified Threat Management (UTM) approach, which combines multiple security features including firewalling, anti-virus, and intrusion detection and prevention, onto a single hardware platform.

What is IPSec

The ubiquity of broadband connectivity has driven the internetworking marketplace, as more organizations take advantage of increasingly inexpensive solutions to connect branch offices, remote teleworkers, partners and key clients to headquarters. However, broadband in and of itself does not natively connect remote sites, you must layer on top of it a technology such as IPSec (IP Security) to create a VPN over that broadband link. IPSec was developed from the outset as a standard to authenticate and encrypt data in an IP network, and to protect the privacy of the network's resources.

TCO is a major driver in the implementation of IPSec. Using an IPSec implementation, users can purchase least-price Internet connectivity, while still establishing a secure, fully-meshed wide area network using the best available technology. And as a connectionless technology, IPSec VPNs, especially when remote SSL-VPN capability is added for individual, remote telecommuters, establishes a broad range of connectivity, allowing connections to be established between virtually any two or more points in the world.

While IP-based VPNs such as those based on MPLS lack strong security, IPSec was designed from the beginning as a secure protocol. The IPSec VPN offers data confidentiality and integrity, and lends itself to remote access solutions in multiple locations. Part of the IPv6 IETF protocol, IPSec includes encryption, authentication and key management, to ensure that the three pillars of VPN security—integrity, authentication, and key management—are all addressed, thereby overcoming all of the security vulnerabilities that would otherwise be present in TCP/IP.

IPSec has become a standard for implementing VPNs, not only because of its inherent security, but also because it does not require any changes to be made to individual client workstations.
In addition to connecting to headquarters though, most organizations also want to provide each end point with Internet access. Since the IPSec VPN itself runs over the public Internet, this is a straightforward addition requiring no additional equipment. There are options for connecting MPLS VPNs to the Internet, usually involving the deployment of a separate Internet connection.

Although IPSec VPNs typically place equipment at the customer premises, many service providers do offer IPSec VPN services where they are responsible for management of the IPSec gateway. In a managed offering such as this, the service provider will typically provide a performance guarantee of some sort.

### A Comparison

MPLS and IPSec are not, as some vendors position them, competitive technologies; rather, each is useful for different functions. The MPLS (IP VPN) is useful in creating fixed, site-to-site connections, but less practical for creating client-to-site, remote site or telecommuting environments. Moreover, the IP VPN is less robust in terms of the providing security to data being transported. IPSec, on the other hand, was designed from the ground up to provide an ultra-secure connection. When a VPN is created using the IPSec protocol, data is secured both by encryption and authentication.

<table>
<thead>
<tr>
<th>Feature</th>
<th>MPLS VPN (IP VPN)</th>
<th>IPSec VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-to-site connectivity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Full mesh connectivity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>QoS and bandwidth management</td>
<td>Yes (CoS)</td>
<td>Yes (granular QoS)</td>
</tr>
<tr>
<td>Client-to-site connectivity</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>AES-256 bit encryption</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>PKI-based authentication</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Available worldwide</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Service provider interoperability</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Service provider contract requirement</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cost to deploy</td>
<td>$$$$$</td>
<td>$</td>
</tr>
<tr>
<td>Monthly bandwidth cost</td>
<td>$</td>
<td>$</td>
</tr>
</tbody>
</table>
Finding an optimal path through the network, whether it is the Internet or a service provider's proprietary net, is a vital concern. In terms of re-routing, MPLS has the ability to store a secondary path through the network. If the main path is inaccessible, MPLS can reroute traffic to a backup path. However, if the backup path is also down, a new path must be created manually. IPSec uses dynamic routing protocols, on the other hand. It automatically detects path failures, and routes around them.

IPSec is firmly established and mature, and it offers end-to-end authentication and encryption to provide the best security environment. MPLS, on the other hand, is a newer specification, but does have use as a replacement for ATM or Frame Relay in connecting major fixed locations. IPSec, because it runs over the public Internet, can be implemented virtually anywhere; MPLS is limited to connectivity within the service provider's network.

Because of its labeling technique, traffic does move efficiently through the service provider network. Also, it offers strong bandwidth and service level guarantees. IPSec VPNs however, can also include bandwidth management functionality—and the rapidly decreasing cost of additional bandwidth makes it possible and cost-effective to deploy enough bandwidth on the IPSec VPN to achieve the same level of performance (if not more) than the MPLS VPN, and at lower cost.

On the downside, MPLS lacks the strong encryption and authentication of IPSec. That's not to say that an MPLS network has no security at all. MPLS does inherently provide for separation of VPN streams, which creates a level of privacy that is established through a strategy of isolation, which makes it difficult for an attacker to gain access to one area through a separate VPN opening. But while MPLS VPNs separate traffic, they do not encrypt packets or provide for authentication. If rigorous security is desirable, traffic can be encrypted before encapsulated into MPLS, using IPSec.

Given these considerations, the position that MPLS is a replacement for an IPSec VPN is incorrect. MPLS is an effective replacement for ATM or Frame Relay, in establishing major site-to-site connectivity; and it should be established alongside IPSec VPNs for maximum security and reach.

Quality of Service

ATM networks did introduce the concept of QoS early on, minimizing things like jitter, latency and packet loss. Despite its significant expense, these QoS characteristics became a high priority for some organizations, who saw the need to make the investment. While QoS may be less important for standard data transmission, today it has become even more vital, as the need to transmit multiple protocols, including both data and voice, over the same wire, has increased. The introduction, development and acceptance of VoIP in particular has underscored the dramatic need for QoS in the organization network, as applications such as these are quite intolerant of latency and other irregularities.

In terms of Quality of Service (QoS), MPLS does provide guaranteed bandwidth between the site and the service provider network. It delivers site-to-site routing and baseline management functionality without end-user intervention. However, QoS is only for the whole connection. The MPLS network only knows what is in the packet header. This level of differentiation has become extremely important recently, especially with service providers rolling out "triple play" offerings that carry voice, video and Internet over the same pipe.

It's important to note the difference between Quality of Service (QoS) and Class of Service (CoS). Class of Service is a term used to describe the differentiation of traffic on a network; this is exactly what the labeling function of MPLS was designed for. Quality of Service, on the other hand, refers to the network's performance, and the mitigation of things like latency and jitter. MPLS was designed to provide class of service functionality, providing the ability to manage and route different kinds of data streams effectively. Whereas class of service shapes the entire data stream by separating data streams for data, video or VoIP, enabling the network's routing function to apply different priorities to different data streams, quality of service functions more at the individual packet level, and is layered on top of the class of service parameters.

While CoS does exist for all traffic traversing an MPLS, or for that matter, an ATM or Frame Relay network, it's also important to note that classification must take place before the traffic hits the carrier's edge router. In
addition to classification markings, the best networking environments will also incorporate bandwidth management and QoS markings.

In grouping different categories of traffic together, MPLS is able to differentiate classes of service, which does provide an efficiency from the service provider level, as well as indirectly, quality of service for the consumer, since their traffic is in a category grouping all its own. MPLS in this way, provides guaranteed bandwidth between site and ISP, and between ISP and remote site. However, this guarantee is only for the whole connection. Apart from the labeling function, it cannot differentiate between traffic types, such as voice and data—and can therefore not provide a true QoS environment.

**Complementary Technologies**

There has been some significant debate about which protocol will become the de facto standard for VPN connections, but this debate misses the point. In reality, organizations and service providers can use both MPLS and IPSec to create an optimal, secure environment that takes advantage of the strength of both. For service providers, it is possible to create a broader offering and to gain a competitive edge in the marketplace; for organizations, deploying an integrated IPSec/MPLS environment will create a complete, and fully secure intranet/extranet with secure remote VPN capability.

The goal of establishing a VPN solution is to create seamless connectivity between the main office and employees, clients, remote offices and anyone outside of the firewall who needs to have access to internal contents. While the MPLS network does carry with it some advantages, particularly in larger site-to-site connections, its reach is limited in that it is a connection-oriented technology, and a branch office outside of the MPLS cloud cannot gain access. IPSec, on the other hand, is a connectionless technology, and can extend to just about anywhere in the world, since it can run over the public Internet. Corporate extranets are getting larger as more partners require access, and MPLS may be impractical for a very large extranet. Integrating IPSec will make it possible to extend the reach of MPLS and establish the connectivity that a modern organization requires.

**Integrating IPSec with an MPLS VPN**

IPSec can add a greater measure of cost-effectiveness, regardless of whether it is used on top of the public Internet, private IP internetwork, or an MPLS network. For a service provider implementing an MPLS network, IPSec VPNs can be added and linked to the VPN network core for greater advantage, scalability, security and QoS functionality. MPLS is typically offered as a managed service, and the VPN originates and terminates in the service provider’s IP network. An IPSec VPN on the other hand, originates and terminates at CPE, and is often managed by the company client—although some providers do offer IPSec-based VPNs as a managed service as well—making a combined offering a natural and logical choice.

In addition to extending the reach of the MPLS network, integration of the two technologies may be used to achieve redundancy—using the IPSec VPN as the redundant link, instead of having to create a more costly redundant MPLS network. Integrating the two technologies is straightforward, and the MPLS Working Group has an existing specification for MPLS-in-IP encapsulation, which provides the advantage of using IPSec to send MPLS packets securely over a non-MPLS network, while adding authentication and encryption to protect the data.

Some service providers already offer a combined approach, providing customers with a flexible VPN environment that can address any need.
The SonicWALL Solution

Firewall appliances are the most common devices for deploying VPNs. According to Infonetics, those who deploy VPNs, especially in the education and retail segments, are cost-sensitive, and budget is often a major barrier to the deployment of a VPN. This is why IPSec VPNs, deployed by the SonicWALL® line of network security appliances, are very often the first choice of organizations around the world. SonicWALL addresses the issue of classification to a much higher degree than other solutions, incorporating not only classification (CoS) markings, but also QoS markings and bandwidth management—the top three elements that are most critical to enterprise customers.

![Figure 2. SonicWALL Branch Office Topology](image)

SonicWALL's family of network security appliances form a first line of defense against all Internet security threats. Creating a Unified Threat Management (UTM) environment, SonicWALL enhances security by combining multiple security functions into the same device and under the same management umbrella. In addition, UTM prevents viruses, worms and spyware from spreading across the WAN. Without it, an organization lacks the vital ability to quarantine sites that may become infected—thereby leaving a door open that could infect the entire intranet. In the case of an MPLS network, UTM is particularly vital to add to the mix, making the combination of MPLS with SonicWALL IPSec VPNs a smart choice.

The SonicWALL UTM solution protects against both internal and external threats, including blended threats. It examines multiple access points and scans every network layer; and its deep packet inspection engine scans against multiple application types and protocols and matches files against a large signature database. SonicWALL's deep packet inspection (DPI) goes a step beyond stateful packet inspection, matching all downloaded, e-mailed and compressed files against its database of attack signatures.

By adding SonicWALL to your MPLS environment, your VoIP environment will be enhanced with active call monitoring, logging and reporting. Also, you will be able to prevent DoS attacks and other malicious traffic from reaching VoIP endpoints. In addition, you will retain QoS markings across VPN/WAN links, and you will
enjoy bandwidth management capabilities and the ability to reserve WAN bandwidth for high priority traffic (QoS). SonicOS will be able to classify and mark traffic, to take advantage of WAN traffic shaping. QoS functionality is included onboard the SonicWALL appliance, which uses standard 802.1p and Differentiated Service Code Points (DSCP) Class of Service (CoS) designators to provide powerful bandwidth management that is essential for VoIP and other enhanced IP services.

Active Call Monitoring, Logging and Reporting

SonicWALL includes an ICSA-certified deep packet inspection firewall, IPSec VPN for remote access, IP address management features, and support for anti-virus, anti-spyware, intrusion prevention and content filtering, all in a single, easily manageable platform. SonicWALL’s family of security appliances can make a useful addition to an MPLS network, to add the necessary functionality that the MPLS network does not have.

The high level of integration afforded by SonicWALL’s unified approach all rides on the hardened SonicOS operating system, so the appliance is not vulnerable to the common attacks that take advantage of holes and vulnerabilities in commercial operating systems. SonicOS provides for ISP failover and hardware failover, WAN redundancy and load balancing and object-based management for simple, consistent management of security policies. SonicWALL appliances come with a full range of VPN capabilities, suitable for everything from remote telecommuters to SOHO implementations up to enterprise environments with thousands of VPNs.

©2005 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.  G151_US.v2