World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 06-10, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2205

Deploying Site-To-Site VPN Connectivity: MPLS Vs IPSec

R. Udayakumar, K.P. Thooyamani and Khanaa

School of Computing Science,
Bharath University, Chennai-73, India

Abstract: When it comes to connecting multiple sites with WAN links, there are now a variety of viable choices. Naturally, the solution that is right for your business will vary depending on the size of your company, the type of traffic you need to transmit and your preferences for security, latency and reliability. *This* Paper entitled "Deploying Site-o-Site VPN Connectivity: MPLS Vs IPSec" is mainly related in comparing VPN implementation using MPLS and IPSec based on their features. *The* drawbacks to encrypted IPSec VPN tunnels are that there is overhead (latency) associated with the encryption, security is of much greater concern and reliability can be decreased due to the complexities of the Internet whereas MPLS is usually done by giving the customer a dedicated IP circuit with private IP addressing on it.

Key words: VPN tunneling · MPLS · IPSec · Tunneling Protocol · QoS · Reliabiltiy

INTRODUCTION

Virtual Private Networks: Virtual private network technology is based on the idea of tunneling. VPN tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server and finally de-encapsulated on the receiving side [1, 2].

Types of VPN Tunneling: VPN supports two types of tunneling-voluntary and compulsory. Both types of tunneling are commonly used. In voluntary tunneling, the VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). Then, the VPN client application creates the tunnel to a VPN server over this live connection.

In compulsory tunneling, the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels.

Compulsory VPN tunneling authenticates clients and associates them with specific VPN servers using logic built into the broker device. This network device is sometimes called the VPN Front End Processor (FEP), Network Access Server (NAS) or Point of Presence Server (POS). Compulsory tunneling hides the details of VPN server connectivity from the VPN clients and effectively transfers management control over the tunnels from clients to the ISP. In return, service providers must take on the additional burden of installing and maintaining FEP devices [3, 4].

VPN Tunneling Protocols: Several computer network protocols have been implemented specifically for use with VPN tunnels. The three most popular VPN tunneling protocols listed below continue to compete with each other for acceptance in the industry. These protocols are generally incompatible with each other.

Point-To-Point Tunneling Protocol (PPTP): Several corporations worked together to create the PPTP specification. People generally associate PPTP with

Corresponding Author: R. udayakumar, School of Computing Science, Bharath University, Chennai-73.

Microsoft because nearly all flavors of Windows include built-in client support for this protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.

Layer Two Tunneling Protocol (L2TP): The original competitor to PPTP for VPN tunneling was L2F, a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create new standard called L2TP. Like PPTP, L2TP exists at the data link layer (Layer Two) in the OSI model-thus the origin of its name.

Internet Protocol Security (IPSec): IPsec is actually a collection of multiple related protocols. It can be used as a complete VPN protocol solution, or it can used simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (Layer Three) of the OSI model.

How IPSEC Works on a Cisco Router: Figure 1 offers a simplified view of how IPSec works on a Cisco router. Two routers set up a virtual IPSec tunnel between each other using common algorithms and parameters. Red traffic is traffic flowing through the router that's meant to go to the Internet and not through the VPN tunnel. Green traffic is meant to go from one site to the other through the IPSec VPN tunnel [5, 6].

It's important to understand the flow of this process where data enters the router and goes to the external interface because of default gateway routing. Once that data hits the external interface, it checks the source, destination and service of that traffic to determine whether it needs to go into the crypto map. The crypto map shown in Figure A uses an Extended ACL called "Crypto-list". You'll see this Extended ACL used in our IPSec template.

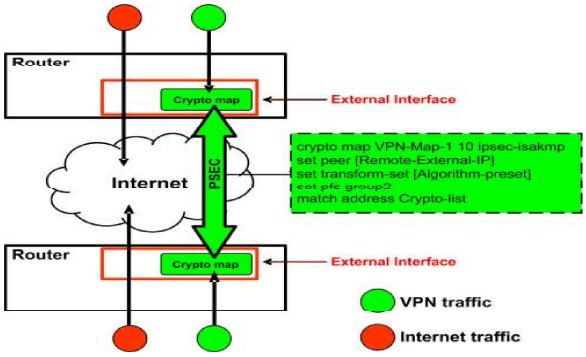

Fig 1:

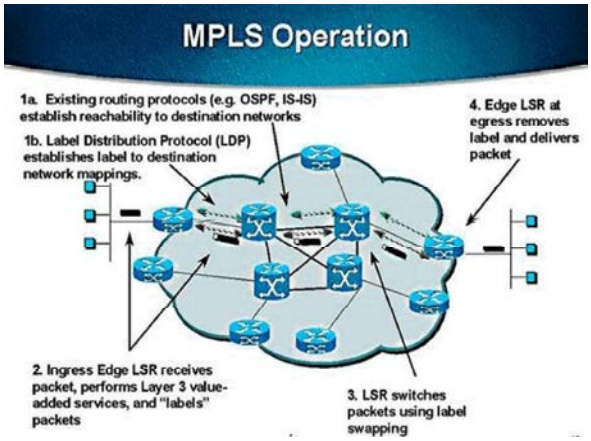

Fig 2:

MPLS: Multiprotocol Label Switching (MPLS) enables Enterprises and Service Providers to build next-generation intelligent networks that deliver a wide variety of advanced, value-added services over a single infrastructure. This economical solution can be integrated seamlessly over any existing infrastructure, such as IP, Frame Relay, ATM, or Ethernet. Subscribers with differing access links can be aggregated on an MPLS edge without changing their current environments, as MPLS is independent of access technologies. Integration of MPLS application components, including Layer 3 VPNs, Layer 2 VPNs, Traffic Engineering, QoS, GMPLS and IPV6 enable the development of highly efficient, scalable and secure networks that guarantee Service Level Agreements. Cisco IOS MPLS delivers highly scalable, differentiated, end-to-end IP services with simple configuration, management and provisioning for providers and subscribers. A wide range of platforms support this solution, which is essential for both Service Provider and Enterprise networks.

MPLS Benefits: The initial goal of label based switching was to bring the speed of Layer 2 switching to Layer 3. Label based switching methods allow routers to make forwarding decisions based on the contents of a simple label, rather than by performing a complex route lookup based on destination IP address. This initial justification for technologies such as MPLS is no longer perceived as the main benefit, since Layer 3 switches (ASIC-based routers) are able to perform route lookups at sufficient speeds to support most interface types[7, 8].

However, MPLS brings many other benefits to IP-based networks. Forwarding packets based on labels rather than routing them based on headers results in several important advantages:

- Since a packet is assigned to a FEC when it enters the network, information that cannot be gleaned from the network layer header, can be used for FEC assignment. For example, classification of packets based on the source of the packets.
- Packets can be assigned a priority label, making Frame Relay and ATM-like quality-of-service guarantees possible. This function relates to the CoS field.
- The considerations that determine how a packet is assigned to a FEC can become ever more and more complicated, without any impact at all on the routers that merely forward labeled packets.
- Packet payloads are not examined by the forwarding routers, allowing for different levels of traffic encryption and the transport of multiple protocols.
- In MPLS, a packet can be forced to follow an explicit route rather than the route chosen by normal dynamic algorithm as the packet travels through the network. This may be done to support traffic engineering, as a matter of policy or to support a given QoS.

In addition to all the above advantages, one of the most important advantages of MPLS is that it is independent of the layer 2 and layer 3 technologies and hence allows integration of networks with different layer 2 and layer 3 protocols [9, 10].

What Are the Services Possible?: The MPLS VPN network provides a common infrastructure for carrying a wide range of services. Some of the most popular services include:

Multimedia Services: It is possible to distribute voice, video and data across the MPLS VPN network, just as it's done in a LAN environment. This service facilitates the exchange of information rapidly between the various sections of the organization.

Intra Office Voice Calls: The MPLS VPN network is capable of carrying voice calls. It gives high priority for voice thus ensuring QoS (Quality of service). This presents huge savings for a company, especially if the volume of intra-office calls is high.

VoIP: The MPLS VPN network can carry VoIP traffic, which may also include the service providers' VoIP traffic.

Video Conferencing: The MPLS VPN network enables users to set up video conferencing with certain equipment. This service is especially popular among enterprises as it saves time and travel costs. Universities can run a virtual campus through interactive video sessions. Interconnection among Universities can greatly advance the cause of research and development, as well as academic progress.

Data Transfer: High-speed data transfer is possible across this network. Since this is a dedicated network, the delay is non-perceptible and error free. This is an ideal solution to meet all the data transfer requirements of any organization.

E-mail: By setting up e-mail servers across their Internet, companies can transfer mail using the MPLS VPN network. This eliminates the need for any other type of official correspondence, while at the same time ensuring prompt delivery of information which greatly enhances the speed and efficiency of workflow within an organization.

ERP: Many companies use ERP solutions for online business transactions with peer companies, dealers, customers, branch offices, factories etc. Working online in this manner requires highly robust and congestion free networks, which is made possible by MPLS VPN networks of BSNL [12, 13].

Access VPN: Employees, while on the move, may require to be constantly in touch with their organization's database for critical information, including product catalogue, pricing, marketing material, inventory check etc. Such users can access their MPLS VPN network through a dial-up Internet account, irrespective of their location.

Intranet: There is hardly any organization which does not have its own intranet for work flow management and for meeting their information requirements. Such intranet solutions can be run across the MPLS VPN network thus enabling integration of operations across the country.

Extranet: Companies may prefer to exchange information with other similar companies to speed up business transactions. The MPLS VPN network is capable of providing the extranet facility by interconnecting the VPNs, depending on the customer's requirement.

Internet: Customers preferring a common infrastructure for intranet and Internet access can have access to the Internet via the MPLS VPN network. However, this will be only according to the customer's preference.

Multicast: One of the important new features that MPLS VPN offers is multicasting. This is especially useful for applications such as video conferencing and customer specific broadcasting.

Let's suppose multiple customers at Chennai need to view a video clip being transmitted from New Delhi. With multicast it is possible to send a single signal over a long distance, which is replicated at the destination for multiple viewers. So after reaching Chennai, the signal is replicated into multiple signals for further transmission to specific customers. This saves bandwidth as multiple transmissions of the same video need not be sent from the source. Moreover, customers can join and leave the multicast group as they please. This solution is especially useful for services like Video on demand [14, 15].

Comparison Chart of MPLS Vs IPSec:

Feature	MPLS VPN
	Reliability
	You will have to receive all MPLS circuits through a single carrier, which helps with reliability. However, some carriers offer MPLS using DSL as the local loop, and choosing this can result in less reliability.
	MPLS will be more reliable than IPSec VPNs
	there is less complication in the tunneling and firewall configuration.
	The cost for the local loops for each choice
Cost	same. The MPLS tunneling, through the
	have a price tag associated with it, but it
	more than a managed IPSec VPN service
	or more than the staff required to manage and
	troubleshoot an IPSec VPN.
	MPLS should be more secure than IPSec
	Security
	if you don't allow your MPLS circuits to connect
	directly to the Internet, which some carriers offer

through the carrier's MPLS cloud. For the best security, use MPLS as a private network only. Used as a private network, MPLS offers the same security as a frame relay network. However, keep in mind that as with frame relay, data sent over an MPLS network is not encrypted.

IPSec site-to-site VPN: Receiving all your IPSec VPN circuits through the same carrier will increase reliability (but decrease fault tolerance) over using multiple Internet carriers. But due to the multiple VPN concentrators and the encryption configuration, an IPSec VPN can be less reliable than MPLS.

Unlike MPLS, IPSec VPN requires VPN concentrators, which will boost the upfront cost. Once you have the hardware, the staff required to maintain and troubleshoot the IPSec VPN tunnels may be the same as, or more than, the MPLS service from the carrier.

Network intrusions are a greater concern with IPSec VPN tunnels since you are running them through an Internet circuit. That Internet circuit is open to connections from around the world. A misconfigured firewall can open your IPSec VPN network to the Internet. Security is of even higher concern if you use split tunneling on your VPN concentrators. However, IPSec VPN tunnels beat out MPLS when it comes to protecting the data that is traversing the WAN, because the IPSec VPN data will be encrypted with IPSec. The MPLS data is not encrypted, only tunneled.

QoS QoS may be included with the carrier's MPLS offering or it may cost extra. Either way, with MPLS QoS, you can prioritize certain traffic all the way through the carrier's network. This is great for latency-sensitive applications, like VoIP. QoS features are limited. Once you send your encrypted data over the Internet, little can be done to prioritize it.

REFERENCE

1. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Application of Soft Computing Techniques in weather forecasting : Ann Approach, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 15(12): 1845-1850
2. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Improving Web Information gathering for personalised ontology in user profiles, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1675-1679.
3. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Detection of Material hardness using tactile sensor, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1713-1718.
4. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Blue tooth broad casting server, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1707-1712.

5. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Weed control system of tea garden using GIS based database Management system, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1702-1706.
6. Saravanan, T. and R. Udayakumar, 2013. Comparision of Different Digital Image watemarking techniques, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1684-1690.
7. Saravanan, T. and R. Udayakumar, 2013. Optimization of Machining Hybrid Metal matrix Composites using desirability analysis, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1691-1697.
8. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. Images segmentation via Gradient watershed hierarchies and Fast region merging, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1680-1683.
9. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. A Approach for Visualization of Atherosclerosis in Coronary Artery, Middle-East Journal of Scientific Research, ISSN:1990-9233, 18(12): 1713-1717.
10. Saravanan, T., G. Saritha and R. Udayakumar, 2013. A Robust H-Infinity Two Degree of Freedom Control for Electro Magnetic Suspension System, Middle-East Journal of Scientific Research, ISSN:1990-9233, 18(12): 1827-1831.
11. Udayakumar, R., V. Khanna, T. Saravanan and G. Saritha, 2013. Retinal Image Analysis Using Curvelet Transform and Multistructure Elements Morphology by Reconstruction,Middle-East Journal of Scientific Research, ISSN: 1990-9233, 16(12): 1798-1800.
12. Udayakumar, R., V. Khanna, T. Saravanan and G. saritha, 2013. Cross Layer Optimization For Wireless Network (Wimax),Middle-East Journal of Scientific Research, ISSN: 1990-9233, 16(12): 786-1789
13. Udayakumar. R, A. Kumaravel and Rangarajan, 2013. Introducing an Efficient Programming Paradigm for Object-oriented Distributed Systems,Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4596-4603.
14. Udayakumar R, V. Khanaa and K.P. Kaliyamurthie 2013. Performance Analysis of Resilient FTTH Architecture with Protection Mechanism,Indian Journal of Science and Technology, ISSN: 0974-6846, 6(6): 4737-4741.
15. Udayakumar, R, V. Khanaa and K.P. Kaliyamurthie 2013. Optical Ring Architecture Performance Evaluation using ordinary receiver, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(6): 4742-4747.