International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244
Impact Factor: 6.690

BENEFITS OF SUPERSEDING PUBLIC INTERNET WITH MPLS VPNS FOR CLOUD INTERCONNECTIVITY

Raghav Gurbaxani, Sir M Visvesvaraya Institute of Technology

Abstract— *The age of virtualization is upon us where the internet (and cloud) has given us unprecedented access to resources around the globe. Indebted to the revolution of cloud, we are able to access our resources from any location and from any device at any time across the globe. Thus cloud has empowered businesses and operations.*

However, accessing these resources over the public internet which is shared by billions of users is a risky endeavor and the data stored over the cloud is susceptible to security breaches by masqueraders.

This paper concentrates on suggesting the increase in adoption of MPLS VPNs which provide a highly secure method of sharing data over the cloud and minimize the risk of security contraventions.

Keywords: *Multi Protocol Label Switching, Virtual Private Network, Cloud, Private Line,VLAN, SSL etc.*

I. INTRODUCTION

The cloud provides solutions for businesses and individuals to virtualize their operations and stay connected to corporate resources spread across the globe. The cloud is full of unexplored possibilities and has the potential to further revolutionize our internet experience.

A. The current cloud scenario (business perspective)

The global cloud services have been proliferating at an extraordinary rate as businesses and individuals are moving from the traditional setup to a cloud based approach. The global cloud services business is currently at $125 billion (approx.) and is expected to grow at over twenty percent till the year 2020 to reach $170 billion dollars. These figures delineate what a significant role cloud plays in today's industry and how it is affecting today's businesses.

B. The problem

Today, most of the companies have their resources hosted on the cloud. Accessing these critical resources (secure information about the company's administration, clients, revenue,

business etc) through the public internet which is shared by billions of other users can have a deleterious effect as they are susceptible to being intercepted by hackers.

In order to optimize the operations running over the cloud, it is imperative to eradicate these security obstacles and move to a more secure form of communication. The MPLS VPN provides a high performance network enabled cloud technology with unparalleled speed, flexibility and security.

If an organization has multiple business locations that need to communicate, they require network connections that go beyond their corporate boundaries. They need to incorporate a service provider into the scenario who can facilitate this conveyance of data.

C. Point to point private lines

Instead of sharing resources over the internet, some businesses opt to establish their own private lines which connect one location to another. These companies may opt for the following kinds of lines - T1 lines, DS3 connections, Ethernet over copper, fiber optic Ethernet or SONET.

The advantage of private lines is that they are dedicated for one's private use, low in latency jitter & packet loss and they ensure high grade network security.

Although this may seem like an excellent choice for connecting to remote locations together in order to facilitate orderly transmission of the data, this method of disseminating data can be very expensive as each location would require its own link (or a switch or router to communicate between sites). In addition to this, as the number of business sites increases, it becomes difficult to set up more number of private links.

The high cost of private lines for multiple locations and long distances, along with greater complexity in handling the inventory calls for a more effective technological convention for interconnecting company resources.

D. Internet VPNs

The internet offers an inexpensive solution to this hurdle as it is ubiquitous, provides easy access and is extremely cost effective. The internet provides superlative connectivity and seems like a natural solution for connecting company locations.

However the use of the internet poses the threat of security (it is probably the least secure network available) as it is easily accessed by everyone and anyone, which means there isn't

a dedicated corridor for data transmission which means anyone who can tap into the data stream can access all this secure information.

By subsuming the internet for connection we are also putting the performance characteristics at a risk as the internet is a public resource and thus the secure data has no priority over the rest of the data over the internet. The system is self routing, so we are incognizant about the route that the packets take and thus oblivious to the path that the secure company information is taking. While the internet may provide seamless operations for common internet applications such as email, web browsing or file transfers; It can cause real headaches for highly interactive or real time processes such as called services, VoIP telephone calls and video conferencing.

II. MPLS VPN : THE SOLUTION

The panacea to the aforementioned problem of using the public internet is by using an MPLS connection.

MPLS (Multi Protocol Layer Switching) which can handle all kinds of multifaceted protocols ranging from Ethernet to TDM uses a proprietary technology to route data known as label switching.

Label switching is a system to encapsulate each packet into a special label which contains the information about source, destination and priority. The label is added when the packet enters the network and removed when it leaves. While on the network, only the label is used to forward packets. The IP content of the packet is ignored; this is equivalent to the internet VPN process and thus MPLS networks are known as MPLS VPN for that reason.

Security is provided by the network being privately run, accessible only to subscribers. It is difficult to tap into the MPLS network as there are no public access points and because of the proprietary label switching process which doesn't depend on internet protocol.

From a security perspective, the data may be encrypted before handing over to the MPLS network.

As MPLS networks are operated by major telecommunication carriers on their own fiber optic networks, they are conscientiously engineered to provide sufficient resources to handle the traffic users. This gets rid of the network congestion and latency & jitter issues. Also the data traffic can be elevated to a priority delivery status such that the highly sensitive voice and data communications are not affected by large files transferring at the

same time. This means that an MPLS network significantly ameliorates the performance aspect of the communication.

Although the MPLS connection is more expensive than simply using the internet for accessing the cloud, it provides a far more reasonable price than multiple dedicated private lines for each location. With the MPLS VPNs provided by the telecomm provider, the user only pays for the bandwidth used for each location. For a reasonable price, the customer is able to secure a high performance solution which helps secure and dedicated transfer of data.

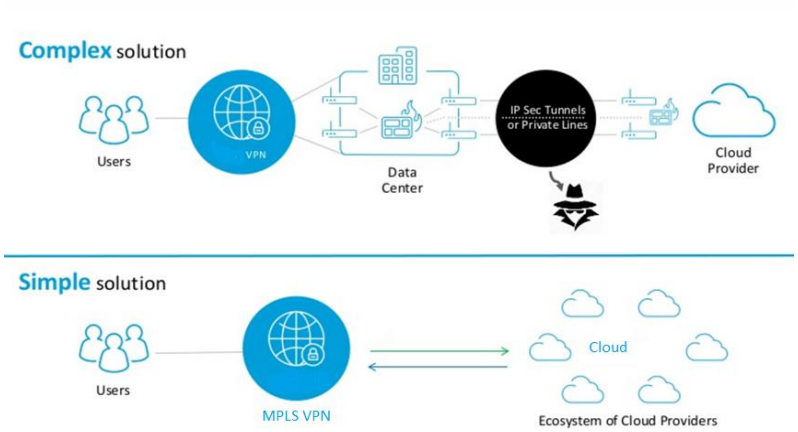

Fig 1: Represents the contrast between the traditional connections which might go through a data center causing hairpin connection problems, whereas through the MPLS it follows a direct end to end path from user to cloud

III. WORKING

MPLS VPNs can be used as a cloud network enablement (CNE) technology that joins with cloud solution provider (CSP) computing services to deliver a managed, end-to-end solution via the network. It provides a highly secure direct connection between a virtual private network (VPN) and the cloud resources, which creates an integrated cloud computing environment.

The existing MPLS VPN is extended (VPN, Enhanced VPN, IP-Enabled Frame Relay, or MPLS PNT) into the cloud service via application programming interfaces (APIs). As a result, it combines the scalability and dynamics of the cloud with the network security inherent in private virtual environments.

The cloud service is enabled to function as another node on the MPLS VPN network and supports mobile VPN integration and common security policies for mobile and wire line

endpoints. Because they're integrated, the network and computing resources expand and contract in tandem, on demand, to rapidly accommodate workload changes.

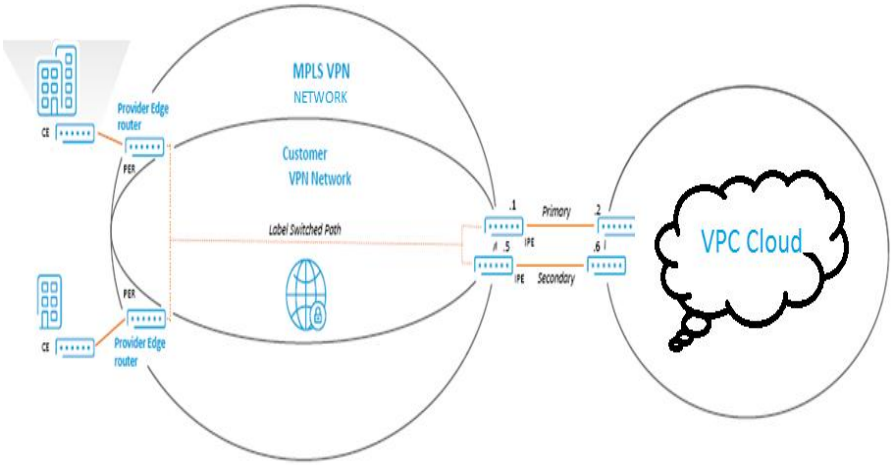

Fig 2. Shows how CE and PE routers are connected to VPC cloud over MPLS network.

The telecomm providers which provide the MPLS infrastructure have a colossal fiber network on which the MPLS infrastructure is supported.

The customer sides are connected to the MPLS network through the customer edge and provider edge routers. An AVPN (label switched) network is employed which has no resources riding over the public internet. The data from the CE and PE take the shortest path over the MPLS network to the infrastructure provider end through the cross connects.

The VPN follows network provisioning to add sites on the customer network, which might be done programmatically with the help of APIs.

Ones a VLAN is established, it sets up a BGP (Border Gateway Protocol) pairing session. Two redundant peering connections are established by subnetting the IP space provided by the customer network as primary and backup links.

This physical connectivity is orchestrated by software through a self service portal (enterprise side) which allows user to connect to his destination using VLAN.

Meet-me-points (an interface) are created across the globe with cloud service providers

The application programming interfaces (APIs) are used to pre-integrate the cloud service and the private network, on which the selected cloud solution providers' data center is an endpoint. By extending the VPN all the way to the cloud service, our patented networking technology separates the VPN traffic from other cloud traffic—down to the virtual LAN (VLAN) and virtual machine (VM) level.

IV. FEATURES &BENEFITS

A) ***Enhanced Security***: As MPLS VPNs operate by establishing a direct tunnel between user and cloud end points, the data is highly secure as compared to being exposed to the susceptible public internet.

B) ***Performance***: MPLS VPNs reduce latency by up to fifty percent and enhances agility. Due to the dedicated tunnel, it also provides high bursting capability. Moreover as a secure dedicated path is established, the end user is cognizant how the data packets will flow as opposed to the internet where the route taken by packets is completely unknown.

C) ***Scalability***: The VPN may be upgraded or downgraded to match the customer's bandwidth requirement. The customer pays only when the service is used and for the amount of bandwidth used.

D) ***Cost***: Although the MPLS connection is more expensive than using the inexpensive public internet, it provides a great cost advantage over private lines and data centers which require huge cost inlays.

E) ***Centralized Routing***: In addition to this, since the MPLS VPNs are monitored by the telecommunication provider, the customer does not need to worry about the routing as it follows an automated centralized routing.

V. COMPANIES OFFERING MPLS VPNS

Currently the MPLS VPNs are being offered by AT&T (AT&T Netbond), Verizon (Service Interconnect), and SingTel (Cloud Interconnect).

A few CSPs such as Microsoft (Microsoft ExpressRoute) and Amazon (Directconnect) also provide these services.

VI. CONCLUSION

The aforementioned paper calls for a growth in adoption of MPLS VPNs over the public internet, especially for large corporations which contain sensitive information over the cloud. MPLS VPNs is a boon which encompasses the benefits of both a public cloud and a private cloud.

ACKNOWLEDGMENT

The proposition described in this paper is supported by the personnel of AT&T. The thesis of this paper was developed during my apprenticeship at AT&T, while working on MPLS VPNs for cloud interconnection solutions.

REFERENCES

[1] E. Rosen, A. Viswanathan, R. Callon, “Multiprotocol Label Switching Architecture “, RFC3031, IETF, Jan. 2001. F Palmieri “VPN scalability over high performance backbones evaluating MPLS VPNs against traditional approaches”.

[2] G Kaur, D Kumar “ MPLS technology on IP backbone network”.

[3] Microsoft ExpressRoute presentation.

[4] Presentation on AT&T Netbond with AWS Direct Connect.

[5] Book on MPLS; technology and applications by BS Davie and Y Rekhter.