© 2018 IJSRSET | Volume 4 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Study of Different Virtual Private Networks and Their Applications

Phalke Akshay Pragnesh
PG Student Department of Information Technology Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India

ABSTRACT

A virtual private network is an important requirement in companies today. With the help of virtual private network user can communicate or exchange data across a public network as if their computing devices are directly connected to the private network. Virtual private network can be classified in site-to-site and remote access VPN. Depending on its type a virtual private network can be used for a specific purpose. This paper studies and analyze different virtual private networks and their applications based on its type.

Keywords: VPN, Secure communication, Site-to-Site, Remote Access

I. INTRODUCTION

A virtual private network is an important requirement for today's organizations. A big organization may have multiple branches. A secure communication between these branches is a key requirement. VPN is a solution for secure communication between different branches of an organization. VPN can be categorized in Site-to-Site and remote access VPN. Site-to-Site VPN is also known as router-to-router VPN. When offices of the same company are connected by Site-to Site VPN is known as intranet VPN. When office of one company is connected to the office of other company is known as extranet VPN. Remote access VPN is used by remote users. For example users who travels frequently and wants to connect to company's location remotely by using a laptop can use remote access VPN. DM-VPN, MPLS VPN are examples of Site-to-Site VPN and EZ-VPN and SSL-VPN are the examples of remote access VPN. VPN is based on different security protocols. Each protocol provides different security levels and features. It uses protocols like IPsec, L2TP, PPTP, SSL, TLS etc. IPsec authenticates the session and encrypts the data packets while connection. IPsec operates on two different modes, Tunnel mode and transport mode. These modes are used to protect data transfer between two networks. L2TP stands for layer 2 tunneling protocol. L2TP is combined with the IPsec to create secure VPN tunnel, so that data can be transferred in a secure manner across the tunnel. PPTP stands for point-to-point tunneling protocol. Here point-to-point protocol is being used to encrypt the data. SSL is used for remote users. SSL establish a VPN connection where browser acts as client. Here user access is restricted to some applications.

II. DIFFERENT VPN TECHNOLOGIES

Different types of VPN technologies are used by organizations. Every organization has its own needs based on which different VPN technologies are being used. In this section features of different VPN technologies are described.

MPLS-VPN: - MPLS stands for multi-protocol label switching. MPLS is a label switching technology. It delivers IP packets faster than normal IP routing. MPLS-VPN provides privacy and quality of service. In MPLS-VPN users can be grouped so that particular services can be provided to the particular group of users. MPLS-VPN provides cost effective IP service. It allows internet service providers to provide different management capabilities. MPLS-VPN is useful for an organization which uses applications such as ERP, CRM, multimedia conferences etc. It is also useful for multicast applications. MPLS-VPN uses VRF to separate routes of different organizations. Here provider edge routers of ISP have no knowledge of core routers. This feature enhances the security of data transmission.

DM-VPN: - DM-VPN stands for dynamic multipoint virtual private network. DM-VPN is a solution which includes IP-sec and GRE to create secure tunnels over the wan. It provides secure, dynamic and scalable solution for data transmission across the internet. Basically DM-VPN provides connectivity between HUB and SPOKES. Here hub consists of fixed IP address and spokes can have dynamic IP addresses. DM-VPN provides spoke to spoke communication without going via hub. It is based on NHRP and multipoint GRE tunnel interface.

EZ-VPN: - EZ-VPN is known as easy virtual private network. It reduces the IP-sac's client configuration. It uses unity client protocol. This protocol allows most IP-sec parameters can be defined on EZ-VPN server. Now when any EZ-VPN client wants to initiates IP-sec tunnel connection EZ-VPN server sends IP-sec policies to the client to establish IP-sec tunnel connection. These tunnels can be created manually or automatically or it can be traffic triggered. So remote client can easily communicate to the EZ-VPN server.

SSL-VPN: - SSL-VPN stands for secure socket layer virtual private network. It uses SSL function of web browser to provide remote access VPN. So user can create VPN connection by using a web browser from a location which have internet connectivity. So it increases the availability and reduces the cost. SSL-VPN uses SSL and TLS to create secure connection between remote users and organization. SSL-VPN does not require a special client software on client machine.

III. APPLICATIONS OF DIFFERENT VPN TECHNOLOGIES

VPN technologies provides secure communication between organizational branches or between remote user and organization. Different organizations may have different requirements of secure connection. In this section applications of different VPN technologies are described.

MPLS-VPN: - MPLS-VPN stands for multi-protocol label switching virtual private network. MPLS-VPN is used in organizations based on its different features.
One important feature of MPLS-VPN is connectionless service. When connection less services are being used tunnel and encryption is not needed for data security. In this way it reduces the complexity. MPLS-VPN provides different value added services like multicasting, Quality of service, Telephony etc. It also provides scalability and security because of its connection less architecture. MPLS-VPN allows customers to use their present address space without using NAT (network address translation). NAT (network address translation) is required only in the case where VPNs with same address want to communicate. So consumers can use their own private IP addresses and communicate over internet. It also provides CoS (class of service) which addresses predictable performance, implementation of policies and multiple service support.

MPLS-VPN can be used over multipoint GRE so that we can get best quality of service with reduced configuration and expanses. It reduces internet service provider's complex configurations to connect different sites. This idea can be implemented over service provider's core network. It provides layer-3

VPN services without using Label-Switched Path (LSP), Carrier Supporting Carrier (CsC), or a Label Distribution Protocol (LDP). [1]

MPLS-VPN can be used with IP-sec technology. All-in-one campus card can be designed based on these technologies. It provides benefits of MPLS-VPN like high speed data transmission, quality of service and scalability. It also provides IP-sac's benefits like security and dependability. Campus card can be used with multiple campus in the multi service systems like management, finance, Teaching etc. [2]

MPLS-VPN can be used for e-government network. Multicast domain can be implemented on MPLS domain. Using this multicasting method, every site on provider edge router belongs to the same VPN is added to one multicasting domain, these sites can send and receive packets across service provider network. This idea reduces the cost. [3]

DM-VPN: - DM-VPN stands for dynamic multipoint virtual private network. DM-VPN is a solution for organizations require encrypted connectivity between branches. DM-VPN can be used in industries like banking, insurance, retail etc. Here in these industries branches needs to connect to HQ. For example ATM and POS machines can be deployed on branches. With the use of DM-VPN these branches can connect to the HQ securely. Some organizations needs to connect to its business partner's site. DM-VPN is a solution for secure connection between these two sites. It also provides quality of service integration.

DM-VPN can be deployed on organizational or ISP's backbone network. It can be used with IP-sec to secure the traffic going via tunnel. DM-VPN can also be used over an EZ-VPN for securing the traffic going through tunnel and also useful for remote users with dynamic IP addresses. [4]

DM-VPN can be used in large organization to connect different sites of an organization. It overcome the disadvantages of traditional VPN. It uses MGRE tunnels that reduces additional configurations. [5]

EZ-VPN: - EZ-VPN stands for easy virtual private network. It is used for remote users who wants to connect to company's server remotely. Users who moves frequently with dynamic IP addresses can use this VPN technology. [4]

Organizations who use a centralized server and employs related to sales who needs to move frequently can use this VPN feature. For example insurance company's employee needs to travel for business purpose so they can connect to companies HO with the use of easy VPN. Here security policies are defined on server and then they are pushed to client's machine who wants to remotely connect to the server. [6]

SSL-VPN: - SSL-VPN stands for secure socket layer virtual private network. Many companies have the requirement of secure access of a particular application for remote users. SSL-VPN can be a solution for this requirement. It has lowest cost of ownership. [7]

SSL-VPN is https based technology. It needs to audit the resources to access to the user, so it records a large number of resources log at the time of resource access. Users who carried out access resources only care about the access to the resources, not about every visit to the same resources that provided us the possibility of optimization. Bloom filter algorithm can shield duplicate resource log output. So in this way performance can be optimized. [8]

SSL-VPN can also be used for Linux host. But without TUN device it cannot be deployed on Linux host. To overcome this limitation, a new kind of SSL VPN system is developed. This system is based on simulated virtual NIC based on loopback interface. With the help of simulated virtual NIC, SSL VPN client can be deployed on Linux hosts without TUN devices. It is a new model of SSL VPN system, compared with traditional SSL VPN system. [9]

IV. CONCLUSION

Different VPN technologies are available. Depending on organizational requirement VPN technology is been selected. For Site-to-site we can use MPLS-VPN or DM-VPN. MPLS-VPN provides faster and secure data delivery. It does not require tunnel interface or encryption. DM-VPN uses tunnel interface to create tunnel over the wan. It also require encryption of data. For this purpose it uses IP-sec. For remote access an organization can use EZ-VPN or SSL-VPN. EZ-VPN enables user to Access Company's network. Here EZ-VPN server pushes policies to clients. SSL-VPN provides more enhanced level of security. It is browser based technology. SSL-VPN client can only access specified applications based on his role.

V. REFERENCES

[1]. Tasnim Tamanna, Tasmiah Fatema ," MPLS VPN Over mGRE Design and Implementation for a Service Provider's Network Using GNS3 Simulator", IEEE, 2017

[2]. Mu Zhang, ZhongPing Tao," Application Research of MPLS VPN All-in-one Campus Card Network Based on IPSec", IEEE, 2012

[3]. LIU Fen-hao, XU Jun-ming, QIN Hui-bin ," Multicast Domain on E-Government MPLS VPN", IEEE, 2008

[4]. Hongru Li , P.W.C. Prasad , Abeer Alsadoon , L. Pham , A. Elchouemi"An improvement of Backbone Network security using DMVPN over an EZVPN structur", IEEE, 2016

[5]. Huaqi Chen" Design and Implementation of Secure Enterprise Network Based on DMVPN", IEEE, 2011

[6]. Yusuf Bhaiji " Network Security Technologies and Solutions".

[7]. Joseph Steinberg, Tim Speed" Ssl Vpn: Understanding, Evaluating, and Planning Secure, Web-based Remote Access".

[8]. Hongxin Li,Lin Cheng,Mingming Xiang,Jiawei Cai" SSL VPN resources log optimization techniques based on Bloom Filter algorithm". IEEE 2016

[9]. Zhu Yanjun, Wang Binjun, Zhang Wei " SSL VPN System Based on Simulated Virtual NIC". IEEE 2013