Virtual Private Network – A Survey

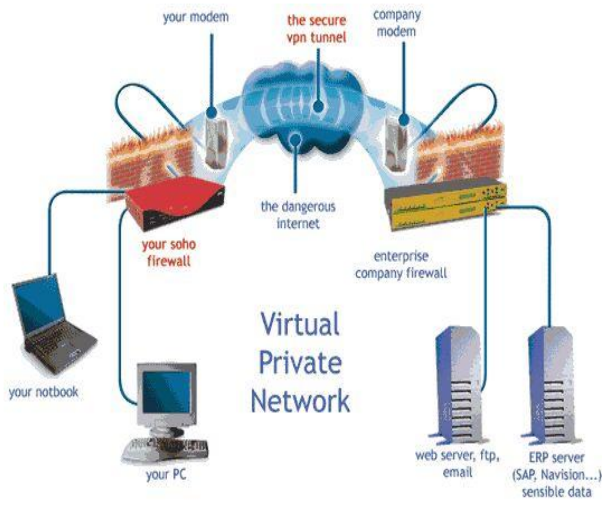
[1]M.Krithikaa, [2]M.Priyadharsini and [3]C.Subha,
[1]Scholar, [2,3]Assistant Professor,
[1,2,3]IT Department Sri Krishna Arts and Science College, Coimbatore, TamilNadu, India.

Abstract: In this paper we introduced the concept of Virtual Private Network extends a private network across a public network, such as the internet. It enables the user to send and receive data across shared public network as if their computing devices were directly connected to the private network. This VPN services is fully dedicated to the small and medium size companies.

Keywords: *Internet: Virtual Private Network, Packets, Protocol, Tunneling, Encapsulation, Vendors.*

I. INTRODUCTION

A virtual private network (VPN) is a network that uses public mean of transmission (internet) as its wan link. A VPN is a type of private network that uses public telecommunication. That provides remote access to an organization's networks via the internet instead of using lines to communicate. A VPN can be created by connecting offices and single users includes mobile users to the nearest service provides POP (poi of presence).



Why VPNS?

Separate private networking solutions are expensive and cannot be updated quickly to adapt to change in business requirements. The internet is inexpensive but does not by itself ensure privacy.

Who Uses VPN's?

VPN's can be found in homes, workplaces or anywhere else as long as an ISP (Internet service provider) is available.

Features in VPN

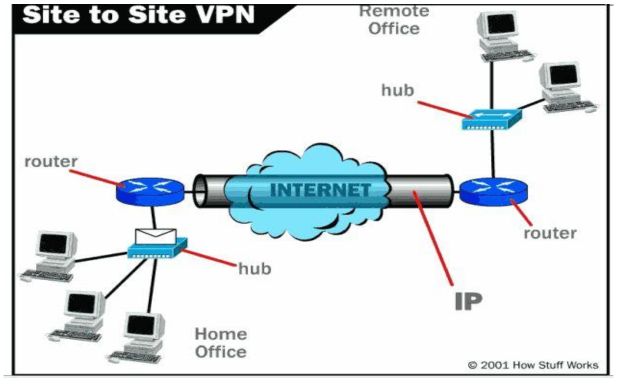
- Provides extended connections across multiple offices in fixed locations to establish secure connections with remote computers.
- Improved security mechanism for data by using encryption techniques.
- IPSec and SSL are two solutions of VPN, which is widely used in WLAN.
- Saves time and expenses.

II. TYPES OF VPN

Virtual private network is of three types:

A. Remote - Access VPN

Remote-access, also called as virtual private dial-up network (VPDN), is a user to LAN connection. A good example of a company that needs a remote-access VPN would be larger firms with hundreds of sales peoples in the field. It provides secure, encrypted connection between a company's private network and remote users through a third-party service provider.



B. Site-To-Site VPN (Internet - Based)

If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.

C. Site-To-Site VPN (Extranet-Based)

When a company has a close relationship with other company (for example, a partner, supplier or customer) they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

III. VPN DEVICES

Devises in VPN are further divided into 3 categories as:

A. Hardware

A hardware VPN is a virtual private network (VPN) based on a single, stand-alone devices. The device, which contains a dedicated processor, manages the authentication, encryption, and other VPN functions and provides hardware firewall. Hardware VPN's provides more and more security than compared to firewall programs for the small and home business computers. But hardware VPN is more expensive than software VPN. Because of the cost, hardware VPN's are a most realist option for large business than for small business or branch offices. Several vendors offer devices that can function as hardware VPN's.

B. Firewall

A well designed VPN are several methods for keeping your connection and data secure. You can set firewalls to restrict the number of open ports, what types of packets are passed through and which protocols are allowed through. A firewall approach is still relatively costly.

C. Software

The main advantage in software approach is that user's network does not change. No extra devices are needed to be installed, and management of the network remains the same. However, one point to consider when adding software to existing hardware is performance. VPN tunneling and encryption tasks will be carried out in software, taking CPU cycle from other processes.

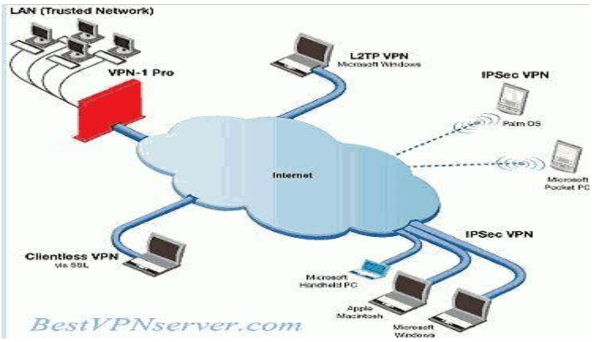
IV. PROTOCOLS USED IN VPN

- PPTP - Point to Point Tunneling Protocol.
- L2tp - Layer Two Tunneling Protocol.
- IPSec - Internet Protocol Security Protocol.
- SOCKS - is not used as much as the one above.

All the three protocols emphasize encryption and authentication, preserving data integrity that may be sensitive and allowing client/servers to establish an identity on the network.

1. PPTP - Point to Point Tunneling Protocol.

This type of protocols is widely supported by Microsoft as it is build into various flavors of windows OS. PPTP initially has weak security features; however Microsoft continues to improve its support.



2. L2tp - Layer Two Tunneling Protocol

L2tp protocol is originally a competitor to PPTP, and was implemented primarily in Cisco products. It also exits data link layer of OSI model.

3. IPSec - Internet Protocol Security Protocol

This type of protocol provides an enhanced security features such as better encryption algorithm, and more comprehension authentication. It has two encryption modes as Tunnel and Transport. Tunnel encrypts the header and the payload of each packet, while transport encrypts only the payload. It also encrypts data between various devices, such as:

- Router to router
- Firewall to router
- PC to router.

V. VPN TECHNOLOGIES

- Tunneling – Using Encapsulation
- Authentication
- Access Control
- Data Security

A. Tunneling

A virtual point-to-point connection made through a public network. It transports encapsulated datagram's.

B. Authentication

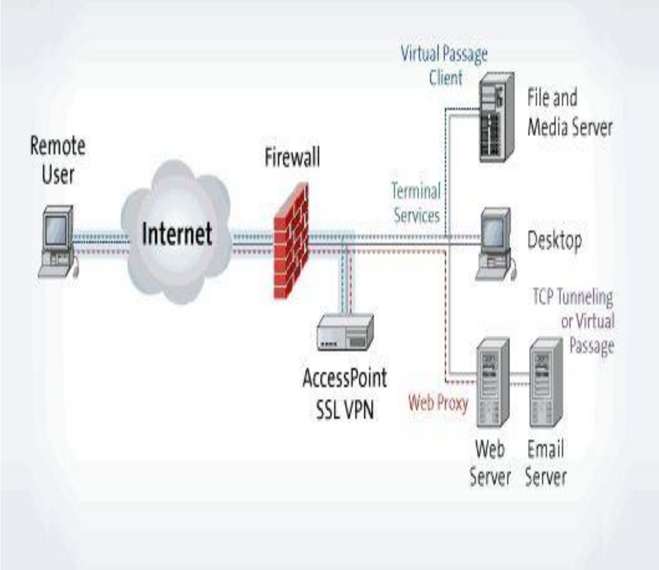
By default VPN does not provide enforce strong authentication. A VPN connection should be established by an authenticated user. Most VPN implementations provide limited authentication methods as PAP used in PPTP, transports both user name and password in a clear text.

C. Access Control

Instead of connecting directly to the network first it switches over to the access servers. VPN includes two tunneling technologies to make a connection between the user and the enterprise.

D. Data Security

A well defined VPN's uses several methods for keeping user's connection and data secure: Firewall, Encryption, IPSec and AAA server. Users can set firewall to restrict the number of ports, what types of packets are passed through and which protocols are allowed through.



VI. TUNNELING IN VPN

Most VPN's rely on tunneling to create a private network that reaches across the internet. Essentially, tunneling is the process of placing entire packets within another packet and sending it over a network. Tunneling requires three different types of protocols such as passenger protocol, encapsulating protocol and carrier protocol.VPN tunneling supports two types as:

- Voluntary Tunneling
- Compulsory Tunneling

1. Voluntary Tunneling

It is the tunneling process where the VPN connection setup.

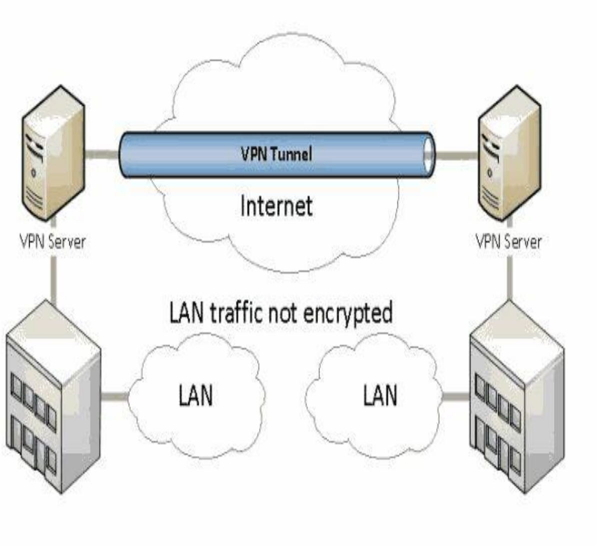
2. Compulsory Tunneling

It is the tunneling process where the carrier network provider manages the VPN connection setup.

Most VPN's rely on Tunneling to create a private network that reaches across the internet. Essentially, tunneling is the process of placing an entire packet within another packet and sending it over a network.

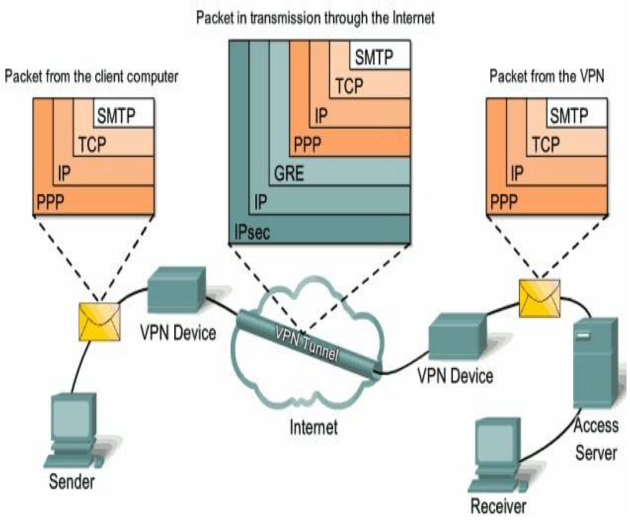
Tunneling requires three different types of protocols as

- Passenger Protocol – The original data (IPX, IP) being carried.
- Encapsulated Protocols – The protocol (GRE, IPSec, L2F, PPTP, and L2TP) that is wrapped around the original data.
- Carrier Protocol – The protocol used by the network that the information is travelling over.



A. VPN Packet Transmission

Packets are first encrypted before sent out for transmission over the internet. The encrypted packet is placed inside an unencrypted packet. The unencrypted outer packet is read by the routing equipment so that it may be properly routed to its destination. Once the packet reaches its destination, the outer packet is stripped off and the inner packet is decrypted.

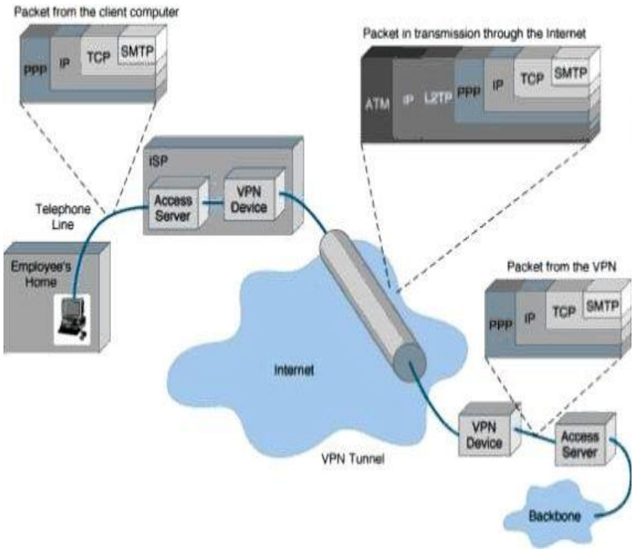


B. Encapsulation of Packets in VPN

Advantages of VPN

- There are two main advantages of VPN's, namely cost saving and scalability.

- VPN's lower costs by eliminating the need for expensive long-distance leased lines.
- A local leased lines or even broadband connection is all that's needed to connect the internet and utilize the public network to surely tunnel a private connection.
- Data transfers are encrypted
- Cost is low to implement.



Disadvantages of VPN:

- VPN connection is slow.
- Because the connection travels over public lines, a strong understanding of network security issues and proper precautions before VPN deployment are necessary.
- VPN connection stability is mainly in control of the internet scalability, factors outside an organization control.
- Differing VPN technology. May not work together due to immature standards.
- Bad hardware and low speed connection on the user end.

CONCLUSION

Today we are living in era of optimizing hardware resources and moving toward larger enterprises day by day. The VPN server is fully based on cloud service. It is the short way of connecting a computer to a remote network.

References

[1] http://www.csun.edu/~vcact00f/311/termprojects/330class/vpnpresentation.ppt

[2] http://vpn.shmoo.com/

[3] http://info.lib.uh.edu/services/vpn.html

[4] http://www.zlin.ba.ttu.edu/doc/vpn-rsvp.ppt

[5] http://zlin.ba.ttu.edu/doc/vpn-RSVP.ppt

[6] http://www.ijarcsse.com/../V2I900209.pdf

[7] http://www.engpaper.net/vpn-research-paper