Client Server Synergy using VPN

Chetan S. More[1] Aman Anand[2] Kushagra Raizada[3] Manuj Srivastava[4]
[1]Assistant Professor [2,3,4]Student
[1,2,3,4]Department of Electronics and Telecommunication Engineering
[1,2,3,4]Bharati Vidyapeeth Deemed to be University College of Engineering, Pune, India-411046

Abstract— This paper is an introduction to Virtual Private Network which extends to a private network through a public network, that is the internet. Through VPN the users can 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. VPNs can be categorized as Secure or Trusted VPNs, Client-based or Web-based VPNs, Customer Edge-based or Provider Edge-based VPNs, or Outsourced or In-house VPNs. These categories often overlap each other. In order to decide what VPN solutions to choose for different parts of the enterprise infrastructure, the chosen solution should be the one that best meets the requirements of the enterprise.

Key words: Internet: Virtual Private Network, Packets, Protocol, Tunneling, Encapsulation, Vendors

I. INTRODUCTION

A virtual private system (VPN) is a system that utilizations open mean of transmission (web) as its wan connection. A VPN is a kind of private system that utilizations open media transmission. That gives remote access to an association's systems by means of the web as opposed to utilizing lines to impart. A VPN can be made by associating workplaces and single clients incorporates versatile clients to the closest administration gives POP (poi of presence).

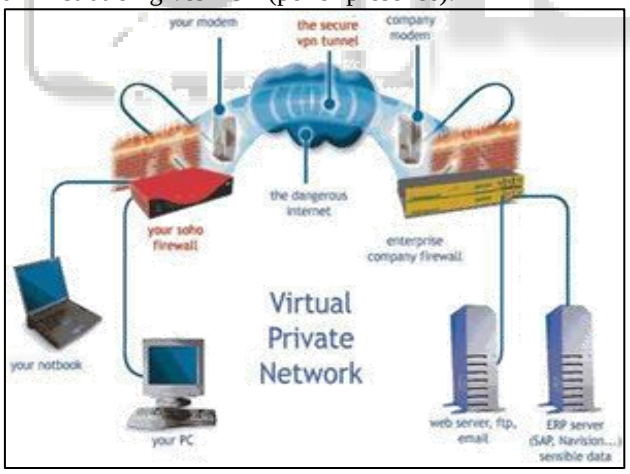

Fig. 1:

A. *Where VPN's are used?*

VPN can be used for personal purposes at home or in offices if public network is available.

B. *Features in VPN*

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

II. TYPES OF VPN

Virtual private network is of three types:

a) Remote - Access VPN
b) Site-To-Site VPN (Internet - Based)
c) Site-To-Site VPN (Extranet-Based)

A. *Remote - Access VPN*

Remote-access, likewise called as virtual private dial-up network (VPDN), is a client to LAN association. A decent case of an organization that needs a remote-access to VPN would be bigger firms with many deals people groups in the field. It gives secure, scrambled association between an organization's private system and remote clients through a third party service provider.

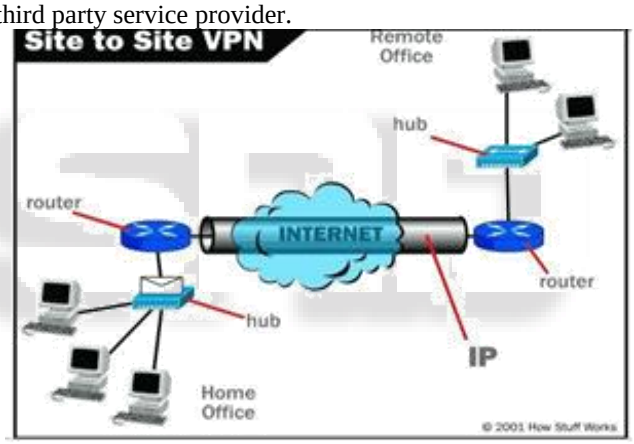

Fig. 2:

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

On the off chance that an organization has at least one remote areas that they wish to participate in a solitary private system, they can make an intranet VPN to associate LAN to LAN.

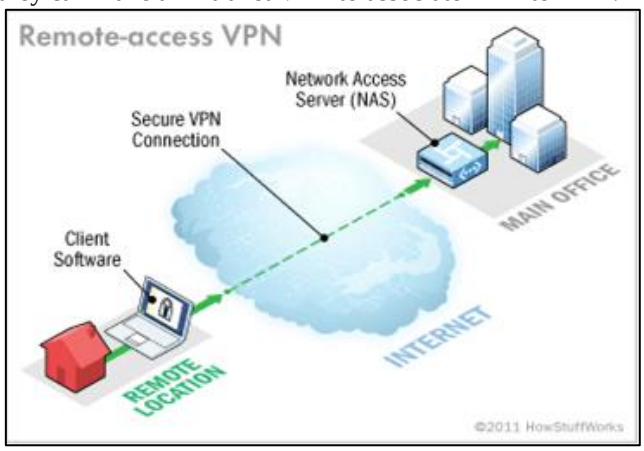

Fig. 3:

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

At the point when an organization has an association with other organization (for instance, an accomplice, provider or client) they can construct an extranet VPN that interfaces LAN to LAN, and that enables the majority of the different organizations to work in a mutual domain.

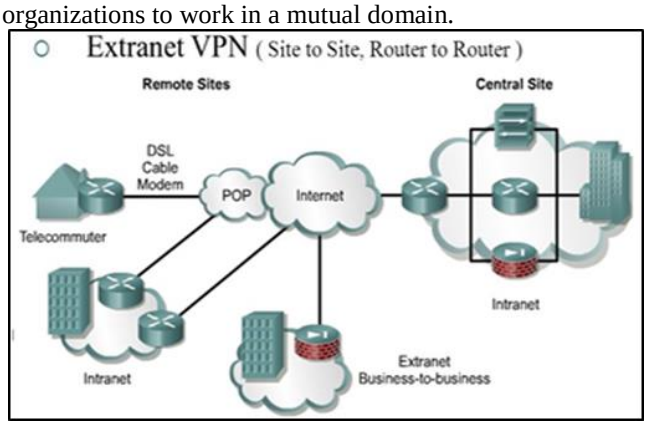

Fig. 4:

III. TECHNOLOGY USED

A. Browser

Any Web browser's job is twofold: given a pointer to a piece of information on the Net (a URL) it has to be able to access that information or operate in some way based on the contents of that pointer for hypertext web documents.

B. HTML

It defines a set of common styles for Web pages: headings, paragraphs, lists, and tables.

C. JAVA Script

Using JavaScript, one can add functionality to web pages, which in the fast would have demanded access to complex CGI-based programs on a web server.

D. Web Server

A Web server is the program that runs on a Web site and is responsible for replying to Web browser requests for files.

E. JAVA Servlets

Servlets are small programs that execute on the server side a Web connection.

F. JAVA DataBase Connectivity (JDBC)

A Database is a collection of data that is organized so that it may easily search and updated.

IV. VPN DEVICES

Devises in VPN are further divided into 3 categories as:

A. Hardware

An equipment VPN is a virtual private network (VPN) in view of a solitary, remain solitary device. The device, which contains a committed processor, deals with the validation, encryption, and other VPN works and gives equipment firewall. Hardware's VPN gives increasingly security than contrasted with firewall programs for the little and domestic venture PCs. Be that as it may, equipment VPN is more costly than programming VPN. Due to the cost, equipment VPN's are a most pragmatist alternative for expansive business than for independent venture or branch workplaces. A few sellers offer gadgets that can work as equipment VPN's.

B. Firewall

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.

V. PROTOCOLS USED IN VPN

1) PPTP - Point to Point Tunneling Protocol.
2) L2tp - Layer Two Tunneling Protocol.
3) IPSec - Internet Protocol Security Protocol.
4) 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.

A. PPTP - Point to Point Tunneling Protocol.

Point-to-Point Tunneling Protocol (PPTP) is a protocol which is used by corporations to secure their own corporate network by using encrypted tunnels over a public network. By using this protocol a organization does not need to lease its own lines for WAN communication but can use the Public network securely using VPN. PPTP operates on TCP port 1723.

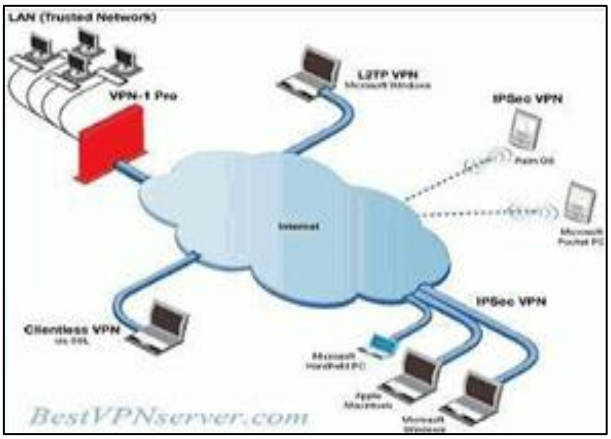

Fig. 5:

B. L2tp - Layer Two Tunneling Protocol

L2TP is considered the next version of PPTP which is the standard encryption and VPN protocol on Microsoft platform. It uses 3DES or AES-256 bit to encrypt traffic; AES-256 is one of the most secured and advanced encryption standards which governments use to protect sensitive information and data.It also exits data link layer of OSI model.

C. IPSec - Internet Protocol Security Protocol

Internet Protocol security (IPSec) is an open standard system which helps to ensure secure communications over Internet Protocol (IP) networks by using several cryptographic services. IPSec provides data integrity, data authentication, data confidentiality and data accountability. IPSec is used at the layer 3 (Internet Layer) therefore, it provides security for almost all protocols in the TCP/IP model.

VI. VPN TECHNOLOGIES

1) Tunneling – Using Encapsulation
2) Authentication
3) Access Control
4) 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.

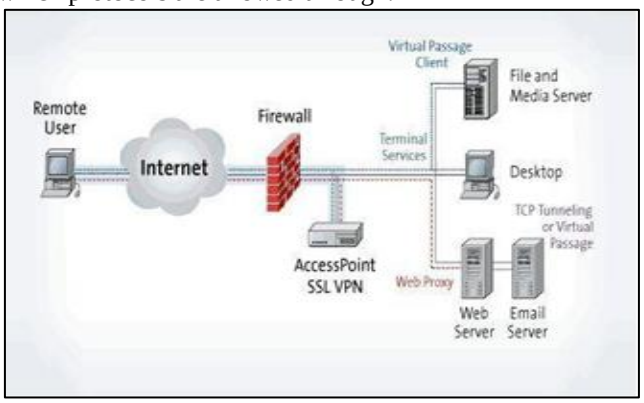

Fig. 6:

VII. 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.

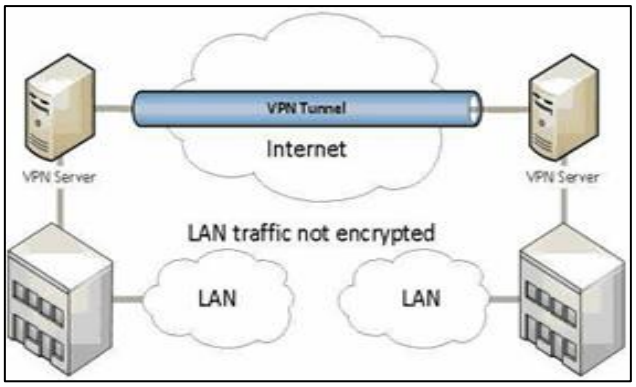

Fig. 7:

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.

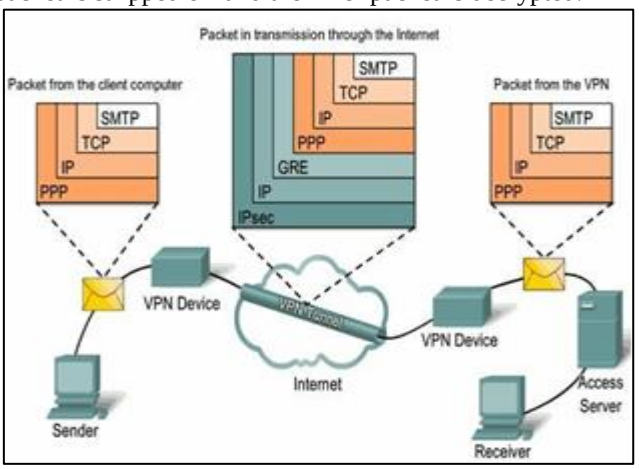

Fig. 8:

B. Encapsulation of Packets in VPN

1) Advantages of VPN

1) There are two main advantages of VPN's, namely cost saving and scalability.
2) VPN's lower costs by eliminating the need for expensive long-distance leased lines.
3) 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.

4) Data transfers are encrypted
5) Cost is low to implement.

2) Disadvantages of VPN

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

VIII. 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://zlin.ba.ttu.edu/doc/vpn-RSVP.ppt
[2] http://www.csun.edu/~vcact00f/311/termprojects
[3] http://www.ijarcsse.com/./V2I900209.pdf
[4] 330class/vpnpresentation.ppt
[5] http://info.lib.uh.edu/services/vpn.html
[6] http://vpn.shmoo.com/
[7] http://www.engpaper.net/vpn-research-paper
[8] http://www.zlin.ba.ttu.edu/doc/vpn-rsvp.ppt

