RESEARCH ARTICLE OPEN ACCESS

A Survey on Virtual Private Network

Amith Singh[1], Afridi Mallick [2]
1 (Bachelor of Computer Application Department, St. Joseph's Evening College, and Bangalore)
2 (Bachelor of Computer Application Department, St. Joseph's Evening College, and Bangalore)

Abstract:

In this paper we introduced the concept of VPN 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 large companies.

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

I. INTRODUCTION

A virtual private network allows the Accessing of private network services for a network over a public or shared medium such as the Internet service provider (ISP) backbone network. VPN is used to transport traffic for multiple other VPNs, as well as possibly non-VPN traffic. VPNs allow using technologies such as Frame Relay (FR) and Asynchronous Transfer Mode (ATM), virtual circuits (VC). These have been available for a long time, but over the past few years IP and IP/Multiprotocol Label Switching (MPLS)-based are become more popular.

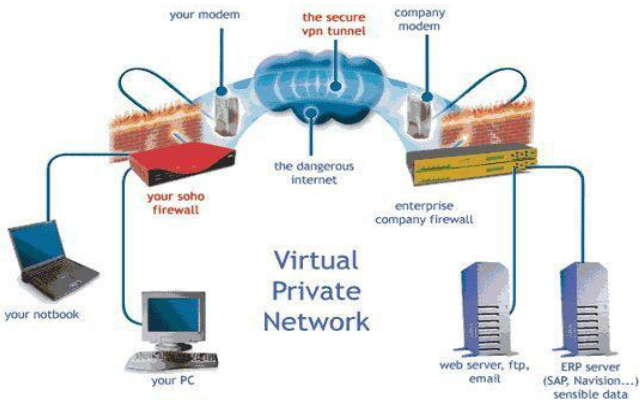

Fig. 1 Overview of VPN

II. FEARURES IN VPN

- Provides extended connections across multiple networks in fixed locations to establish secure connections with remote networks.
- Improved security for data by using encryption techniques.
- IPSec and SSL are two technologies of VPN, which is widely used in WLAN.
- Saves time and expenses [1]

III. TYPES OF VPN

A. Remote - Access VPN

Remote-access is also called as virtual private dial-up network, which provides a user to LAN connection. A good example of a company that needs a remote-access VPN which is larger firms with many sales peoples in the field. VPN provides encrypted, secure connection and data transmission between a company's private network and remote users to connect through a third-party service provider which is also referred as IPS. [1]

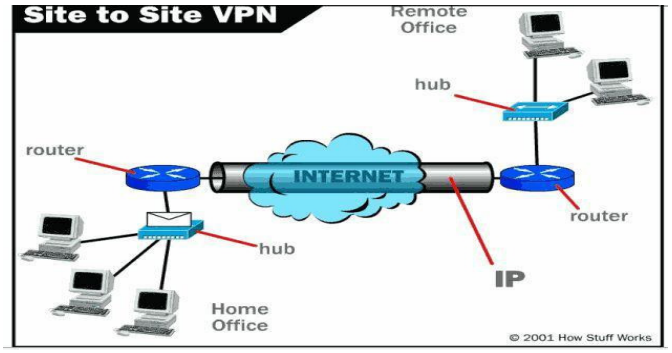

Fig. 1 example 1, Site to Site VPN

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

Site-to-site virtual private network allows offices in multiple fixed networks to establish secure connections with each other over a public media such as the Internet. Site-to-site virtual private network extends the company's network, making computer resources from one location available to users at other locations. [1]

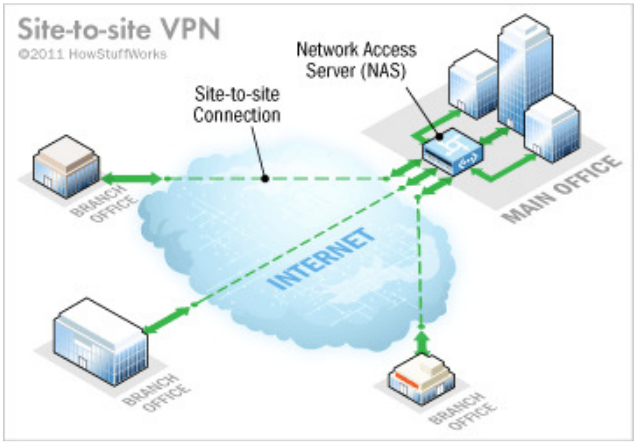

Fig. 2 example 2, Site to Site VPN

In this scenario introduced in builds on the site-to-site (Extranet-Based) scenario by providing a business partner access to the same headquarters network. In this scenario, the headquarters network and business partner network are connected through a secure IPSec tunnel and the business partner is given access only to the headquarters public server to perform various IP-based network activities, such as placing and managing product orders.

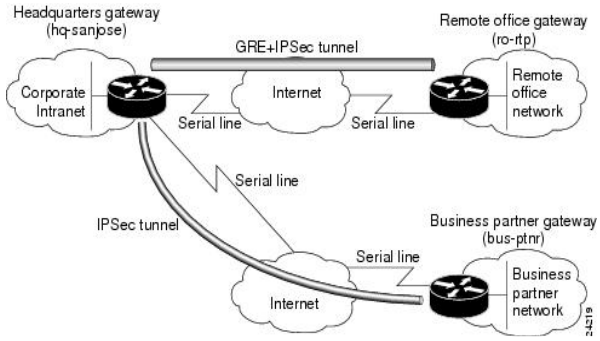

Fig. 3 example 3, Site to Site VPN

IV. VPN DEVICES

Devises in VPN are further divided into 3 categories as:

A. Hardware

A hardware virtual private network is a VPN based on single devices. The gadget, which contains a committed processor which deals with the authentication, encryption, and other VPN works and gives equipment firewall. Equipment virtual private system gives more security than contrasted with firewall programs for the little and domestic venture PCs systems. Be that as it may, equipment virtual private system is more costly than programming VPN. Along these lines the value, equipment VPN's are a most regular alternative for extensive association than for little association or branch workplaces. A few customer offer gadgets that can work as equipment VPN's. [2]

B. Firewall

A proper designed VPN network provides 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. [2]

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 managing of the network remains the same. However, when adding software to existing hardware is performance. VPN tunnelling and encryption tasks will be carried out in software, taking CPU cycle from other processes. [2]

V. PROTOCOLS USED IN VPN

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

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

1. PPTP - Point to Point Tunnelling Protocol.

Point-to-Point Tunneling Protocol or PPTP makes a tunnel and encloses the data packet, this type of protocols is commonly supported by Microsoft as it is built into various versions of windows OS. PPTP has weak security features; however Microsoft continues to improve its support. [3]

2. L2TP - Layer Two Tunnelling Protocol

L2TP creates a tunnel between two L2TP connection points, 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]

3. IPSec - Internet Protocol Security Protocol

Internet Protocol Security or IPSec is used to secure Internet communication across an IP network, In 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 mode and Transport mode encryption. 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. [3]

VI. VPN TECHNOLOGIES

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

A. Tunnelling

A VPN tunnel works by encapsulating data in an encrypted data packet, A Virtual point-to-point connection made through a public network. [4]

B. Authentication

VPN by default 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. [4]

C. Access Control

While user connecting directly to the network first it switches over to the access servers. VPN includes two tunnelling technologies to make a connection between the user and the enterprises.

D. Data Security

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. [4]

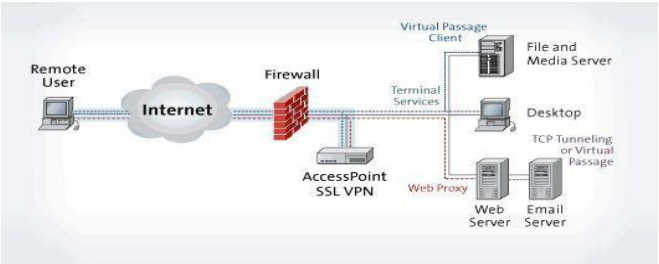

Fig. 1 VPN Technologies

VII. TUNNELING IN VPN

Tunnelling Protocols and the Basic Tunnelling Requirements

Since they depend on the very much characterized PPP protocol, Layer 2 protocol, (for example, PPTP

and L2TP) acquire a suite of helpful highlights. These highlights and their Layer 3 partners address the fundamental VPN requirements, as laid out below. [5]

A. User Authentication.

Layer 2 tunnelling protocols acquire the client authentication plans of PPP, including the EAP techniques talked about underneath. Many Layer 3 tunnelling plans expect that the endpoints were notable (and confirmed) before the passage was set up. An exemption to this is IPSec Internet Key Exchange (IKE) arrangement, which gives shared authentication of the passage endpoints. Most IPSec executions including Windows 2000 help PC based certificates just, as opposed to client certificates. Therefore, any client with access to one of the endpoint PCs can utilize the passage. This potential security shortcoming can be wiped out when IPSec is combined with a Layer 2 convention, for example, L2TP. [5]

B. Token card support.

Utilizing the Extensible Authentication Protocol (EAP), Layer 2 tunnelling protocols can bolster a wide assortment of authentication techniques, including one-time passwords, cryptographic adding machines, and keen cards. Layer 3 tunnelling protocols can utilize comparable techniques; for instance, IPSec characterizes open key testament authentication in its IKE arrangement. [5]

C. Dynamic address assignment.

Layer 2 tunnelling supports dynamic task of customer tends to in light of the Network Control Protocol (NCP) arrangement instrument. For the most part, Layer 3 tunnelling plans accept that an address has just been doled out preceding start of the passage. Plans for task of locations in IPSec tunnel mode are presently a work in progress and are not yet accessible. [5]

D. Data compression.

Layer 2 tunnelling protocols support PPP-based pressure plans. For instance, the Microsoft usage of both PPTP and L2TP utilize Microsoft Point-to-Point Compression (MPPC). The IETF is exploring comparable components, (for example, IP Compression) for the Layer 3 tunnelling protocols. [5]

E. Data encryption.

Layer 2 tunnelling protocols support PPP-based information encryption instruments. The Microsoft execution of PPTP supports discretionary utilization of Microsoft Point-to-Point Encryption (MPPE), in view of the RSA/RC4 calculation. Layer 3 tunnelling protocols can utilize comparable techniques; for instance, IPSec characterizes a few discretionary information encryption strategies, which are consulted amid the IKE trade. The Microsoft usage of the L2TP convention utilizes IPSec encryption to shield the information stream from the VPN customer to the VPN server. [5]

F. Key Management.

MPPE, a Layer 2 encryption component, depends on the underlying key produced amid client authentication, and after that revives it intermittently. IPSec unequivocally arranges a typical key amid the IKE trade, and furthermore invigorates it occasionally. [5]

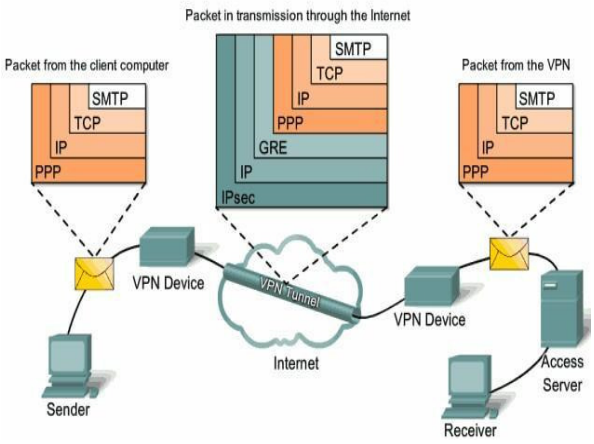

Fig.1 Encapsulation of packets in VPN

VIII. GENERAL VPN SECURITY CONSIDERATIONS

The accompanying is general security guidance for VPN arrangement:

1. VPN associations can be reinforced by the utilization of firewalls. [6]

2. An IDS/IPS (Intrusion Detection/Prevention System) is prescribed so as to screen assaults all the more adequately. [6]

3. Against infection programming ought to be introduced on remote customers and system servers to keep the spread of any infection/worm if either end is tainted. [6]

4. Unsecured or unmanaged frameworks with straightforward or ought no authentication to not be permitted to make VPN associations with the inner system. [6]

5. Logging and examining capacities ought to be given to record organize associations, particularly any unapproved endeavours at get to. The log ought to be investigated consistently. [6]

6. Preparing ought to be given to arrange/security heads and supporting staff, and in addition to remote clients, to guarantee that they take after security best practices and approaches amid the usage and progressing utilization of the VPN. [6]

7. Security strategies and rules on the fitting utilization of VPN and system support ought to be dispersed to mindful gatherings to control and represent their utilization of the VPN. [6]

8. Putting the VPN passage point in a Demilitarized Zone (DMZ) is prescribed keeping in mind the end goal to ensure the inner system. [6]

9. It is prudent not to utilize part tunnelling to get to the Internet or some other shaky system at the same time amid a VPN association. In the event that split tunnelling is VPN Security Page 20 of 23 utilized, a firewall and IDS ought to be utilized to identify and keep any potential assault originating from shaky systems. [6]

10. Superfluous access to inside systems ought to be confined and controlled. [6]

IX. Limitations of a VPN

Despite their popularity, VPNs are not perfect and have their own limitations and is true for any technology. Organizations must consider issues like the few listed below when deploying and using virtual private networks in their operations:

1. VPNs need detailed information of network security issues and cautious configuration to ensure sufficient security on a public network like the Internet.
2. The reliability and implementation of VPN over Internet is not under an organization's direct control. Instead, the ISP is responsible for its resolution and their quality of service.

3. In the past, VPN products and solutions from different sellers have not been compatible always due to issues with VPN technology and standards. Attempting to mix and match devices may cause technical problems, and using device from one provider may not give as great a cost savings. [7]

X. CONNECTING VPN

During research process, we have gone through vpnforuk.com, a site which provides free VPN services. Here is an example for a secure connection VPN in windows using PPTP protocol: [8]

A.

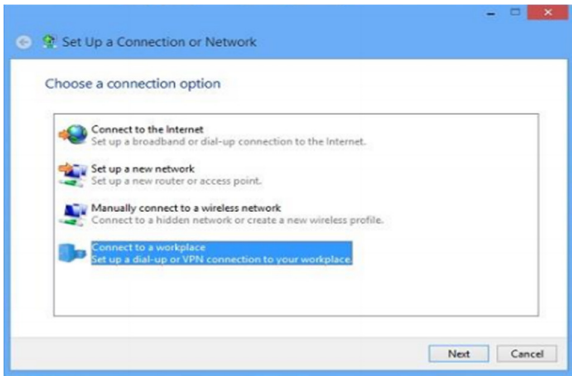

Fig. 1 Connect to a workspace

B.

Fig. 2 Use my internet connection

C.

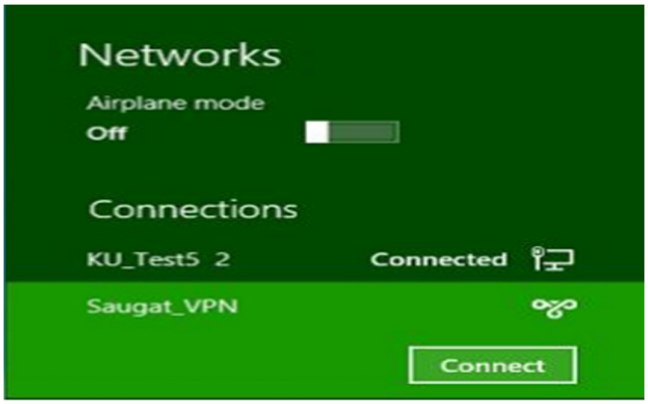

Fig. 3 Now Ready to connect to the VPN

D.

Fig. 4 Connecting to vpnforuk.com

E.

Fig. 5 Network Authentication to connect to VPN connection

F. IP Address before and after connecting to VPN: Once the connection is established the IP address is changed to UK IP address. Hence, it proved that VPN hide the original IP address. [8]

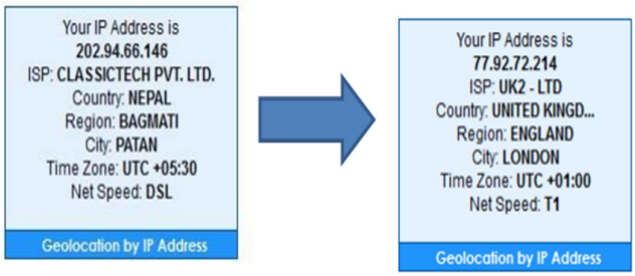

Fig. 6 Change of IP Address after connecting to VPN

Advantages of VPN

- Saving and scalability are the two main advantages of VPN
- 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. [8]

Disadvantages of VPN

- 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.
- VPN connection is slow. [8]

CONCLUSION

System security is one of the drifting themes in present days. As world is more helpless, VPN significance has expanded. Business association these days isn't constrained to one place. In this way, they need security in cheap value which can satisfy by utilizing VPN and its cutting edge burrowing convention which has been incomprehensible for anybody the experience it. It has been brilliant cake for the individuals who work more out in the open bistro arrange than sitting in same place consistently. It is giving new name to the security and information exchange through the web.

REFERENCES

1. *Krithikaa, Priyadharsini, and Subha, "Virtual Private Network – A Survey," vol. 3(1), 2016.*
2. *CSUN. [Online]. https://www.csun.edu/it/vpn*
3. *J. Myles Powell. (2010) Digital Commons. [Online]. http://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1056&context=honors*
4. *webopedia. [Online]. https://www.webopedia.com/TERM/V/VPN.html*
5. *(2017, September) Microsoft. [Online]. https://msdn.microsoft.com/en-us/library/bb742566.aspx*
6. *(2008, February) infosec. [Online]. https://www.infosec.gov.hk/english/technical/files/vpn.pdf*
7. *Zhao Aqun, Yuan Yuan, and Ji Yi, "Research on Tunneling Techniques in VPNs," The National 863 High Technology Plan Project, pp. 691-697, 2000. [Online]. https://www.researchgate.net/publication/289120789_VPN_research_Term_Paper*
8. *Saugat Bhattarai. (2016, January) Research Gate. [Online]. https://www.researchgate.net/publication/289120789_VPN_research_Term_Paper*