e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:06/June-2022 Impact Factor- 6.752 www.irjmets.com

ROLE OF VIRTUAL PRIVATE NETWORK OVER INTERNET

Saurabh Kadam*1, Pradip Yadav*2

*1,2Software Engineering ASM Institute of Management & Computer Studies, India.

ABSTRACT

Network security becomes a major consideration of the current era. Internet provides an enormous ease in almost all the regions like online banking, online shopping, communications, businesses or organisations. Thus, the communication network requires the security of the confidential data stored or transfer over the internet. Due to the quick development of computerized gadgets and their entrance to the internet caused insecurity to user data. Now a days, security and privacy threats has become more and more complicated which amplify the requirement for a modernized protected medium to secure the valuable data into the internet. In this paper, introduced Virtual Private Network (VPN) is a great way to protect devices and information from the hackers. VPN is a private network which operates over a public network transit the encrypted information so that attackers are not able to use it. The purpose of VPN is to provide the different security elements such as authenticity, confidentiality and data integrity that's why these are becoming trendy, low-priced and easy to use. VPN services are available for smart phones, computers and tablets. This paper also concerns about the development, protocols, tunnelling and security of VPN. It is a rising technology which plays a major role in WLAN by providing secure data transmission over Internet.

I. INTRODUCTION

1) Virtual Private Network (VPN)

What is VPN?

VPN also known as Virtual Private Network is a technology that encrypts your internet traffic on unsecured networks to protect your online identity, hide your IP address, and shield your online data from third parties.

Virtual Private Network basically allows you to create a secure connection to another network over the Internet.

What is the role of VPN?

VPNs use real-time encryption and send your internet data through a secure virtual tunnel to minimize the possibility of anyone tracking what you do online.

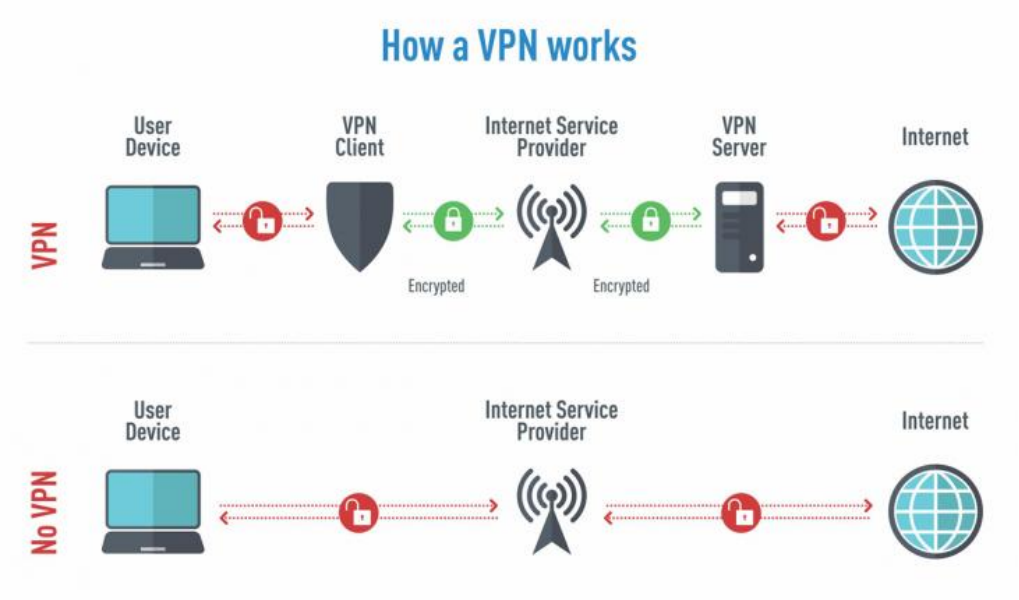
VPN technology was originally developed to allow remote business workers to securely connect to corporate networks in order to access resources when gone from the office. Although VPNs are still used in this way, the term now usually refers to commercial VPN services that allow users to access the internet privately through their servers.

Use of VPN?

VPN offers you privacy, security, and when you use VPN, cybercriminals, your ISP (Internet Service Provider), and regular snoopers have a hard time tracking your actions online.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:06/June-2022 Impact Factor- 6.752 www.irjmets.com

VPN gives you a layer of protection that no other online security tools are able to provide. With a new IP and virtual location, you become much harder to track and able to enjoy online privacy.



2) History of VPN

VPN technology was first used in 1996 when a Microsoft employee developed the PPTP. The protocol created a more secure private connection between a user device and the internet. In 1999, the specification was published. In the early 2000s, VPNs were mostly associated with and used by businesses. Fifteen years ago, VPN access was a new concept to most business. Their origin can be found in Virtual Circuit. Virtual Circuits service is considered superior to a connection -less service for handling long messages. VCs are easy to execute on highly connected networks. The structure of the VC is to generate a logical path from the source port to the destination port. This path may integrate numerous hops between routers for the configuration of the circuit. The final, logical path or virtual circuit acts in the same way as a direct connection between the two ports. In such a way, two or more applications could communicate over a shared network. VC technology forges ahead with the adjoining of encryption facilities to the router systems. This new facility stared converting data into a code to prevent unauthorized access. Afterwards, other tools were added as tokens authentication. Unfavourably, the communication lines were still insecure and these leads to the evolution of secure communication over open network, a VPN.

3) Advantages of VPN

- VPNs get rid of Geo – restrictions.
- Online privacy is no longer at risk.
- Protects from cybercriminals.
- Data transfer is encrypted.
- Regional leased lines or even cable networks are all you need to connect to the internet and use the public network to tunnel a private connection for sure.
- Cost saving.

4) Disadvantages of VPN

- VPN may decrease your speed.
- Dropped connections.
- VPN isn't legal in all countries.
- Quality VPN could cost money.
- It might be difficult to setup connection for business users.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:06/June-2022 Impact Factor- 6.752 www.irjmets.com

II. METHODOLOGY

This topic is chosen in order to become more familiar theoretically in the field of secure network connection using tunnel. Network security becomes a major consideration of the current era. Internet provides an enormous ease in almost all the regions like online banking, online shopping, communications, businesses or organisations. To complete this research, I have done the following things:

1) Various articles in the Internet were thoroughly examined and information was collected.
2) Several e-books and books from the library were used to find the content about the topics.
3) Consultation with friends was also done which helped in conduction the research in more depth.
4) For practical test, I have used Turbo VPN software for mobiles as well as desktop testing free VPN service.

III. ANALYSIS

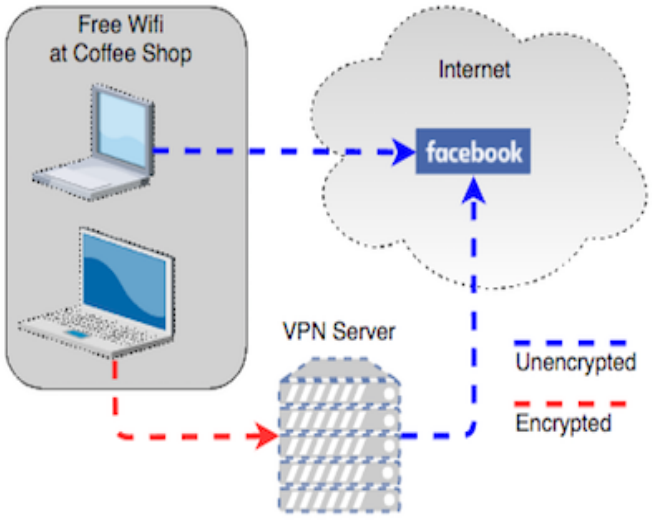
VPN is growing very fast as the security is the major concern in the world. Modern technology has shown great changes the way we work few years ago. People started to work remotely and are seeking more security for their work. So, in upcoming days VPN would be the prime requirement for every organization and business people. Moreover, those who are sensitive towards their personal information VPN technology would be their first choice.

Virtual Private Network (VPN) is basically of 2 types:

Remote Access VPN:

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.

An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.



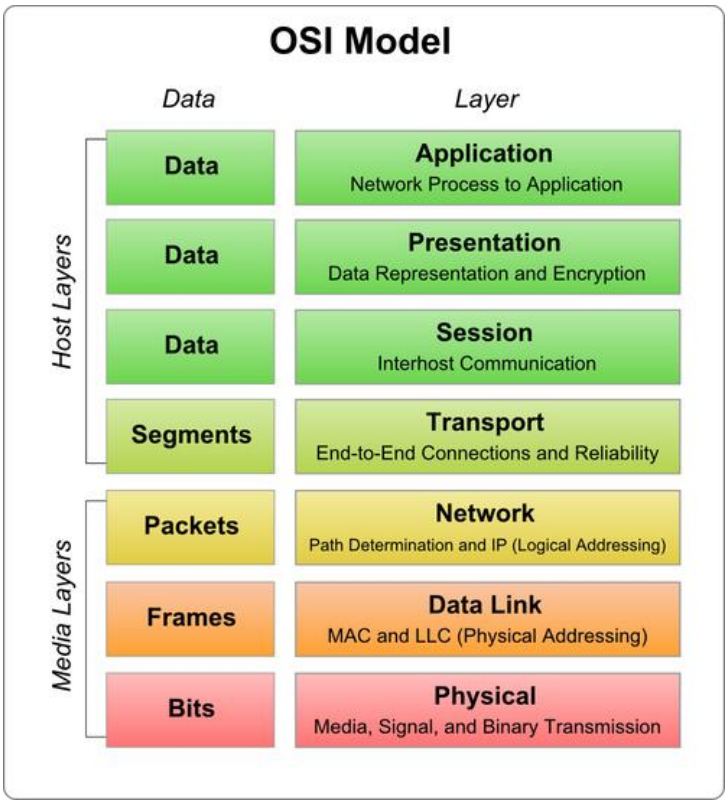
Site to Site VPN:

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

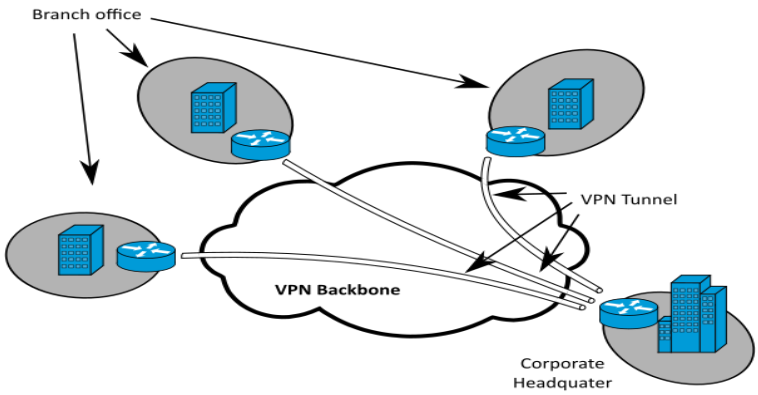
- Intranet based VPN: When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- Extranet based VPN: When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:06/June-2022 Impact Factor- 6.752 www.irjmets.com

Basically, Site-to-site VPN create a imaginary bridge between the networks at geographically distant offices and connect them through the Internet and sustain a secure and private communication between the networks. In



Site-to-site VPN one router acts as a VPN Client and another router as a VPN Server as it is based on Router-to-Router communication. When the authentication is validated between the two routers only then the communication starts.



Types of Virtual Private Network (VPN) Protocols:

1. **Internet Protocol Security (IPSec):**

Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection.

IPSec runs in 2 modes:

- Transport mode
- Tunneling mode

The work of transport mode is to encrypt the message in the data packet and the tunneling mode encrypts the whole data packet. IPSec can also be used with other security protocols to improve the security system.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:06/June-2022 Impact Factor- 6.752 www.irjmets.com

2. Layer 2 Tunneling Protocol (L2TP):

L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.

3. Point–to–Point Tunneling Protocol (PPTP):

PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

4. SSL and TLS:

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have "https" in the initial of the URL instead of "http".

5. OpenVPN:

OpenVPN is an open-source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol.

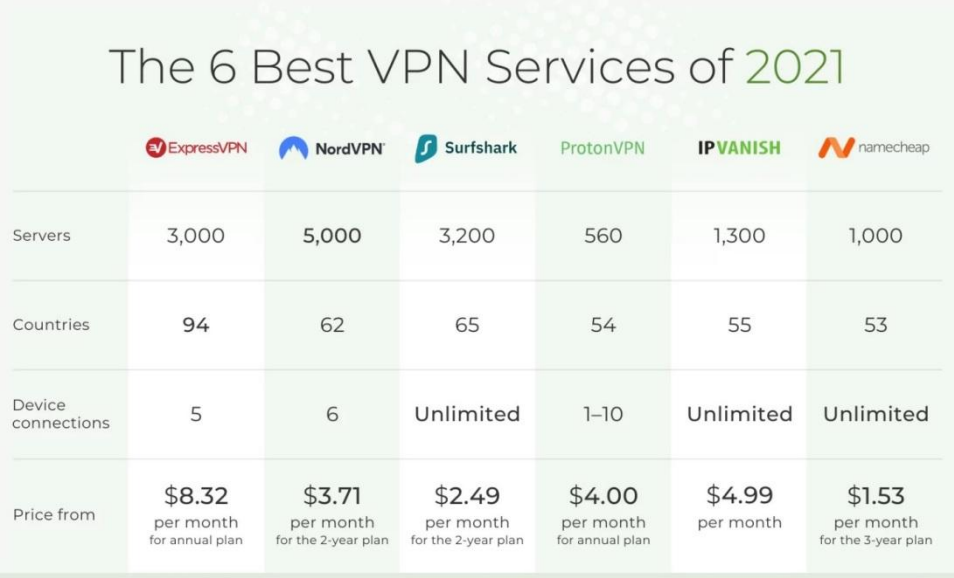
6. Secure Shell (SSH):

Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

Popular VPN Services in 2021

Most used VPN Services in 2021 are –

- ExpressVPN
- NordVPN
- Surfshark
- ProtonVPN
- IPVanish
- namecheap



IV. CONCLUSION

VPNs enable users and companies to communicate over the public internet to remote servers, branches or the business while retaining secure communication. VPNs are highly secure, versatile, inexpensive communication tool. In this paper, we defined various VPN technologies which includes SSL and IPsec are popular. We also listed various types of VPNs and noted that their versatility makes it possible for the user to select which facility they want. VPNs can provide a range of authentication, integrity and encryption algorithms. For the future Virtual Private Networks are expected for safe communication. In the coming years, the VPN industry will be predicted to be very high. It is essential that the chosen requirements meet the needs of consumer and to retain their versatility.

V. REFERENCES

[1] https://en.wikipedia.org/wiki/Virtual_private_network
[2] https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/?ref=gcse
[3] www.webopedia.com/TERM/V/VPN.html
[4] www.computer.howstuffworks.com/vpn.htm
[5] www.searchenterprisewan.techtarget.com/definition/virtual-private-network