The vital role of VPN in making secure connection over internet world

Article *in* International Journal of Recent Technology and Engineering · March 2020

DOI: 10.35940/ijrte.F8335.038620

2 authors:

Chamandeep Kaur
Jazan University
17 PUBLICATIONS **137** CITATIONS
SEE PROFILE

Dr. Yogesh Kumar Sharma
K L University
86 PUBLICATIONS **121** CITATIONS
SEE PROFILE

The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World

Yogesh Kumar Sharma, Chamandeep Kaur

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.***

Keywords: Encryption, Protocol, Tunnelling, Virtual Private Network (VPN).

I. INTRODUCTION

A. Virtual Private Network (VPN)

VPN is a networking framework which is effect over public network to secure confidential data shared on the public network. It rose as a cost effective and upright resolution in different networking and telecommunication organizations. It won't give some other outer assistance among them and it won't permit some other association to intrude on them. Virtual Private Network (VPN) are most supportive part of any IT business because it saves the huge cost of infrastructure by using the open Internet to create highly protected communication medium from corporate office to isolated sites and users.

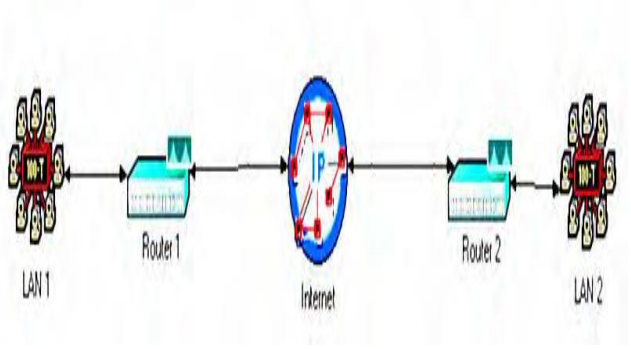

Fig. 1: Virtual Private Network (VPN)

B. History

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. Unfavorably, the communication lines were still insecure and these leads to the evolution of secure communication over open network, a VPN.

C. How does VPN work?

Generally, VPN is a subscriptions-based model. It means the user must has to download an application from its provider and signs up for a granted time period to use their private network to protect the different devices. The price will differ between providers but usually, this is a monthly payment which will steadily decrease based upon the time length of the subscription period (monthly or yearly). Free VPN applications are also available in the App Store for various OS. Before using VPN, Remember, your VPN provider may keep a record of your online activities which may well be shared with the authorities, should they enquire.

Revised Manuscript Received on March 09, 2020.
***** Correspondence Author
Dr. Yogesh Kumar Sharma*, Department of Computer Science and Engineering, Shri JJT University, Churela, Jhunjhunu, Rajasthan, India. Email: dr.sharmayogeshkumar@gmail.com
Chamandeep Kaur, Department of Computer Science and Engineering, Shri JJT University, Churela, Jhunjhunu, Rajasthan, India. Email: tanutn83@gmail.com

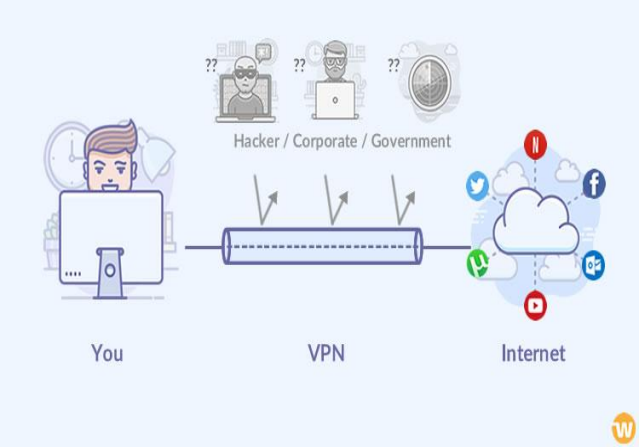

Fig. 2: How does VPN work?

D. Why we use VPN?

From the consumer's point of view, the major benefits of VPNs are that they are significantly cost-effective. The solution to using VPN technologies is the high speed leased line. Such lines are costly, difficult to manage and difficult to keep. The internet provides reliability for VPN users. Even very remote locations have connection to the internet using dial – up modems. VPNs guarantee safe communication for dial – in users. The internet provides the VPN with the accuracy of services. Mobile users may not be able to use leased lines to connect with the corporate site and so the only possible solution is VPN technology.

E. Advantages

- 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.

II. STRUCTURE OF VIRTUAL PRIVATE NETWORK (VPN)

A. Tunnel

Tunnelling is a method in which one network packet is wrapped in another. The encapsulated packet is called the tunnelled packet and the external packet is called the transport packet, which encapsulates. All the information contained in the packet is encrypted at the lowest level, the OSI model's link level. As with VPNs, tunnelling concept has been available for many years. It has been used to bridge internet portions that have been disjoined capacities or policies. On the top of the internet protocol, the tunnel acts as a router.

B. Remote Access Virtual Private Network

Remote Access VPN allows a user to connect a private network remotely access all their services and resources. The user-private network communication exists through the Internet and the connection is secure and private. Remote Access Virtual Network is useful for both home users and business users.

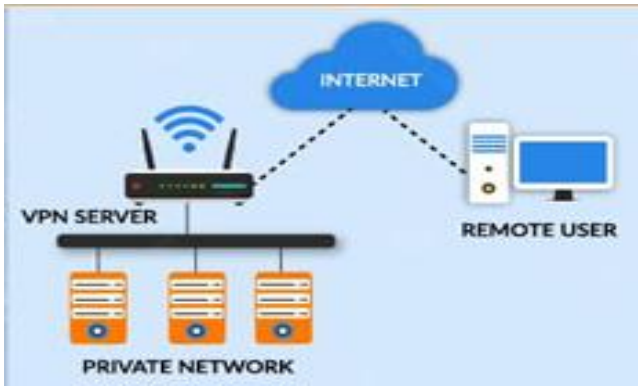

Fig. 3: Remote Access VPN

C. Site-to-Site Virtual Private Network

Site-to-Site VPN builds a virtual connection between the networks at geologically isolated offices and links them over the internet and maintains secure, private network communication. In this one router acts as a VPN client and another act a VPN server as it is focused on connectivity between network and user. If only the authentication between the two routers is only checked then the connection begins.

Fig. 4: Site-to-site VPN

III. VIRTUAL PRIVATE NETWORK (VPN) PROTOCOLS

A. Point-To-Point Tunnelling Protocol (PPTP)

PPTP builds a tunnel and surrounds the data packet. Point-To-Point Protocol is used to encrypt the data between the links. Point-To-Point Tunnelling Protocol is one of the most frequently used VPN protocols for dial-up networks, originally developed by Microsoft and has been in use since Windows was first released. Apart from Windows, PPTP is also used on both Linux and Mac.

B. Internet Protocol Security (IPSec)

IPSec is used throughout an IP network to protect Internet communication. To provide encryption, IPSec is often combined with other VPN protocols, but can also be used by itself. It is widely used VPNs from Site to Site and many iOS applications. IPSec runs in two modes: Tunnelling and Transport mode.

C. Layer 2 Tunnelling Protocol (L2TP)

L2TP is a tunnelling protocol often paired with other VPN security protocols such as IPSec to establish a highly secure VPN connection. Layer 2 Tunnelling Protocol creates a tunnel between two L2TP connection points, and the data is encrypted by the IPSec protocol and secure communication between the tunnels.

D. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

SSL and TLS create a VPN connection where the web browser serves as a host and the user's access applications is restricted rather than the entire network. Online shopping portals are commonly using the protocol SSL and TLS. Web browsers can easily switch to SSL as they are embedded with SSL and TLS. SSL connections have "https" in the first of the URL instead of "http".

E. OpenVPN

OpenVPN is an open source VPN widely used for Point-to-Point and Site-to-Site link development. It uses a standard SSL and TLS based authentication protocol. OpenVPN enables users to secure their data using virtually unbreakable AES-256-bit key encryption.

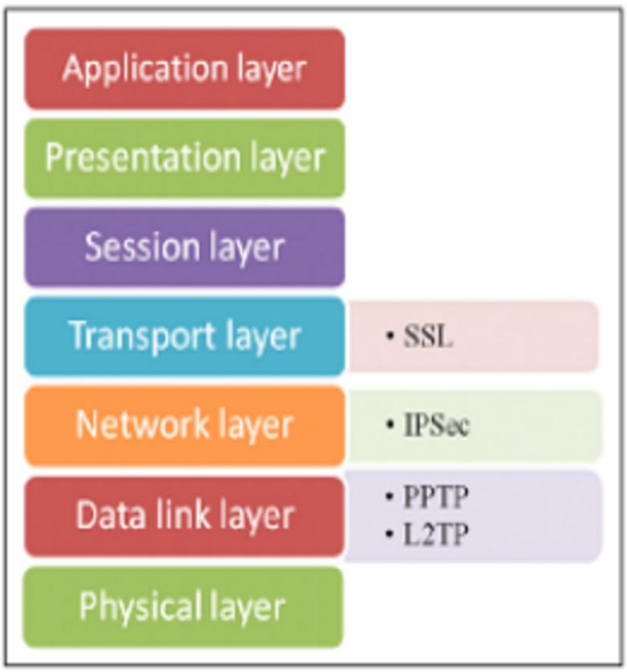

Fig. 5: VPN Protocols on OSI Model

VI. TRENDY VIRTUAL PRIVATE NETWORK SERVICES PROVIDER IN 2020

List of VPN service providers by whatismyipaddress.com are as follows:

Provider	Countries	Devices	P2P	Monthly
CyberGhost	61	7	Yes	$2.75
NordVPN	59	6	Yes	$3.49
ExpressVPN	94	5	Yes	$6.67
Surfshark	50	Unlimited	Yes	$1.99
Hotspot Shield	22	5	Yes	$7.99
Hide My Ass	210	5	Yes	$3.99
PureVPN	141	5	Some	$4.16
Private Internet Access	25	5	Yes	$3.33
SaferVPN	34	3	No	$2.50
VyprVPN	65	Up to 5	Yes	$2.50
Tunnel Bear	20	5	No	$4.17
StrongVPN	21	1	Yes	$5.83
SlickVPN	46	5	Yes	$4.00
IP Vanish	60	5	Yes	$6.49

V. VPN TECHNOLOGIES TO SOLVE INTERNET SECURITY ISSUES

Virtual Private Network uses several tools to protect data flowing over the Internet. Some of the technologies used by VPN are as follows:

A. Firewalls

An Internet firewall uses such strategies to check out network addresses on ports or packets solicited on incoming connections to determine which traffic is permissible on a network. Though most VPN services do not execute firewalls straightly by themselves, they form an integral part of a VPN. The aim of firewall is to prevent unwanted traffic from accessing your network while own users of VPN can access it. Packet filtration is the most popular firewall that prevents the crossing of the gateway router from specifying the IP address. Example of VPN support router is Cisco Private Internet Exchange (PIX) which support the Packet filtration.

B. Authentication

Authentication is a key to VPNs as its guarantees the exchanging parties share data with the right client or server. It is an analogous to "sign on" to a username and password scheme. The majority of VPN authentication is totally based on a shared key. The keys are run by using a hashing algorithm, producing a hash value. The other party that holds the keys ought to generate its personal hash value and compare it to that obtained from the other end. The hash value sent to an attacker over Internet is insignificant, so someone who sniffs the network would not be able to gather a password. Examples of authentication system are RSA and CHAP.

C. Encryption

Encryption is frequently seen as important as authentication, because it secure the data being transmitted from the packet sniffing. VPNs employ two common techniques for encryption: Public and Hidden (private) key: The public key encryption requires a private and public key. You reveal your private key to all but keep your private key to you only.
In hidden key encryption, all the parties that need to the encrypted information have a specific passphrase or secret password, which is used for encrypting as well as to decrypt the information.

Capitalize only the first word in a paper title, except for proper nouns and element symbols. For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [8].

VI. 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.

REFERENCES

1. Kanuga Karuna Jyothi, Dr. B. Indira Reddy "Study on Virtual Private Network (VPN), VPN's Protocols And Security", Int © 2018 IJSRCSEIT | Volume 3 | Issue 5.
2. Komalpreet Kaur, Arshdeep Kaur "A Survey of Working on Virtual Private Network" © 2019 IRJET | Volume 6 | Issue 9.
3. https://scholar.google.com/citations?hl=en&user=OOI01CwAAAAJ
4. https://www.servercake.blog/types-virtual-private-network-vpn/
5. https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/
6. D. Simion, M.F. Ursuleanu, A. Graur, A.D. Potorac, A. Lavric "Efficiency Consideration for Data Packets Encryption with in Wireless Tunneling for Video Streaming" INT J COMPUT COMMUN 8(1):136-145
7. https://whatismyipaddress.com/vpn-comparison
8. https://scholar.google.com/citations?hl=en&pli=1&user=ks9yhS0AAAAJ
9. Charlie Scotte et al., "Virtual Private Network" Second Edition, O'Reilly, January 1999
10. Ayhan ERDOĞAN, Dz. Yzb. "Virtual Private Networks (VPNs): A Survey", https://pdfs.semanticscholar.org/bd27/4a3195cb2de780c87727ec6e6248dffb80e5.pdf
11. https://scholar.google.com/citations?user=Js1wB70AAAAJ&h1=en&scioq=Dr.+Yogesh+kumar+sharma

AUTHORS PROFILE

Dr. Yogesh Kumar Sharma, presently working as a Associate Professor (HOD / Research Coordinator) Department of Computer Science Engineering and IT at Shri Jagdishprasad Jhabarmal Tibrewala University", Chudela, Jhunjhunu (Rajasthan). He completed his Ph.D. in Faculty of Computer Science, from Shri Jagdishprasad Jhabarmal Tibrewala University", Jhunjhunu (Rajasthan) in the year 2014. His research areas Data Communication & Networking, Operating System, Computer Organization and Architecture, Data mining, Cloud Computing, Software Engineering etc. In his research life he Published 4 books & 75 Papers in National and International journals, 25 National and International conferences, 03 workshops. Under his guidance 05 research scholars awarded Ph.D. Presently 08 research scholars working under his guidance. He invited as a Guest Lecturer for Students in M.Sc. I.T. (Master Program in Information Technology) on the behalf of National University of Science and Technology, Muscat, Oman, Nov. 2019. He is Paper Setter, Answer Sheet Evaluator (Copy Checker) and Practical Examiner in University of Rajasthan, Jaipur, Pandit Deendayal Upadhyay University (Shekhawati University), Sikar, Maharaja Ganga Singh University, Bikaner, University of Kota, Kota, Board of Secondary Education Rajasthan, Ajmer. Ph.D. Thesis Evaluator and Ph.D. Final Viva-Voce Examiner in OPJS University, NIMS University, Mewar University. Published 2 patents on Title: Parallel Processing System to Reduce Complexity in Data-Mining of Industrial & Social Big-Data. And Title: Computer Implemented Method for Detecting Downlink Control Channel in Long Term Evolution Wireless Communication. He has a member of IAENG, IACSIT, CSTA and UACEE.

Chamandeep Kaur, presently pursuing her Ph.D. in Computer Science, from Shri JJT University, Jhunjhunu, Rajasthan. She's M.C.A. from Punjab Technical University, Jalandhar, Punjab with a rich teaching and mentoring experience of 12 years. She has published 5 research papers in International and Scopus journals and attended 6 Notional/ International conferences. Her area of research is Cloud Computing, IoT, Operating System, Big Data, Data Securities. She's also working with Jazan University as a Lecturer in Computer Science Department, Jizan, KSA where she's teaching undergraduate students as well as guiding in their graduation project. She is a member of IEEE.