IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

VPN: Overview and Security Risks

Rohit Ramesh Jadhav and Parth Sandeep Sheth
Students, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *Virtual Private Networks (VPN) gives anonymity and online security whilst using the web by creating a private network from our public internet connection. VPNs cloak Internet Protocol addresses such that our online activities cannot be traced. Initially, VPNs were only being utilized by huge corporate organizations, which could bear its cost, to safely and privately share records between workplaces situated in various parts of the world. Currently in 2020, now over a quarter of the world's population uses VPN to access the internet anonymously. This paper presents an introduction to VPN technology, its working, its types, some of the VPN Protocols, comparison between free and paid VPN services, and security issues associated with VPN use.*

Keywords: VPN (Virtual Private Network), Protocols, Security issues, Risks, PPTP, Open VPN

I. INTRODUCTION

VPN stands for Virtual Private Network, which is essentially a private connection over the internet. It can be implied as an Internet within the Internet. VPN is a wide term that includes several different protocols. PPTP (Point to Point Tunneling Protocol) was developed by Microsoft's Mr. Gurdeep Singh Pall in 1996, which permitted the users to create a reliable and secure internet connection. This was a milestone event and many experts considered it as the beginning of an era of VPN. VPN were generally utilized only by organizations and huge associations. The security breaches happening from 2002 to 2008 were the key factors responsible for the development of VPN as a technology. There is a wide array of clarifications that caused people to start using VPNs, and the significant ones are as follows: increase in online protection, increased online security, and permit to utilize web uninhibitedly as it allows a user to go around online limitations and website restrictions. Moreover, VPNs are utilized to secure internet connections, guarantee advanced security, forestall malware and hacking, and open geo-hindered content and cover user's Internet Protocol (IP) and MAC addresses. VPNs are generally used as an important tool for remaining sheltered and secure over the web, and are simple to use and moderately priced. VPN's function is to create a private connection between numerous people and multiple gadgets over the Internet, which is secured, private, and encrypted from meddling eyes, hackers, malwares, and others who might be interested to know where one is browsing from, or what is being browsed. Formerly created for large organizations and governments, it was never meant for the purposes for which it is used in today's world. The world of internet has started to share sensitive information and is at an exposed risk of being hacked or other loss of secret data when using unsecured Internet connections; hence, the need for VPN is great, justifying the development of VPN technology. More secured connections than the average connections are the need of the hour to allow the remote users to access and use data safely and securely.

II. WORKING OF VPM

When you use a VPN to access the internet, it basically redirects your device's internet connection through your preferred VPN server in place of your Internet Service Provider (ISP) to make sure that when your information is communicated to the web, it originates from the VPN rather than your device. When you use a VPN to access the internet, the VPN acts as a

middleman thus masking your IP address (a series of numbers your ISP allocates to your device) so that your identity is protected from trackers. Besides, if your information is some way or another intercepted, it will be incoherent until it arrives at its last destination. A private tunnel is generated from your device to the web when using your preferred VPN, obscuring your sensitive data through encryption. Encryption is the term used to portray how your

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

information is kept hidden whilst using a VPN. Encryption conceals your data to such a degree (fundamentally transforming it to rubbish) so that it cannot be interpreted without the use of a concrete phrase, which is recognized as the password or key. The key or password essentially is used to translate the complex code that your data has been changed into. Just your device and the VPN server know this key. The way of deciphering your data is recognized as decoding, which involves making scrambled data comprehensible again through the application of the password. For example, shopping on your preferred e-commerce platform with your debit or credit card, when you enter the credentials ofits final destination. Encryption process varies from different VPN service providers, but in short, the encryption process involves the following:

1. At a point when you use a VPN to access the internet, your sensitive data travels through a secure tunnel where it is ciphered. It means that your transformed data travels between your device and the VPN.
2. Your device now appears to be on the same local network as your desired VPN. Now, one of the IP addresses of the VPN server's is used accessing the internet instead of actual IP address thereby protecting your identity.
3. You may now access the web anyway you see fit, knowing that your private information is safe as the VPN acts as a barrier.

The degree to which your data is encoded depends a lot upon the encryption mechanisms used by your preferred VPN suppliers.

III. Types of VPN

VPNs are fundamentally of two basic types:

1. **Remote Access VPN:** Remote Access VPN allows a client to link to a secure and private network therefore the client can access all its services and resources remotely. A link is established between the client and the private network through the Internet and the link is secure and private. Remote Access VPN is beneficial for both home users and business users. Suppose, if a worker of an organization is out of station, he/she may use a VPN to connect to the organization's private network to remotely access the files, records and resources on the private network. VPN services are primarily used to bypass the regional restrictions on the web and access the blocked websites by either private users or home users. Clients mindful of Internet security likewise use VPN services to upgrade their Internet security and protection.
2. **Site to Site VPN:** It is usually utilized in the massive companies. Businesses or corporations with workplaces spread across the globe may use Site-to-Site VPN to link the network of one workplace to the network of another workplace across the globe. Another terminology for Site-to-Site VPN is Router-to-Router VPN.

A Site-to-Site is used to generate an imaginary bridge between the networks of geographically distant workplaces of an organization and link them through the web to sustain a secure and privatized communication. A Site-to-Site VPN includes one router which acts as a VPN client while another router which acts as a VPN server as it's based on Router-to-Router communication. At the point when the verification is approved between the two routers at exactly that point the communication begins

IV. Comparison Between Free VPN And Paid

Ensuring web protection, access to geo-blocked content without interruption, good security, requires expenditure in secured web infrastructure and continually developing IT world.

4.1 Free VPN

It is a service that along with necessary VPN software application (GUI), gives us access to a VPN server network, without charging any cost. But nothing is free. Free VPN might sell your personal or browsing data, hence compromising your online privacy, defeating its most important purpose. Free VPNs might give other clients, access to your connection, by routing someone else's traffic through your device, and their data traffic routed through yours. Some free VPNs are found to be selling your unused bandwidth on the internet market. The security provided by Free VPNs is easily crackable and weak. This is because they use weak encryption techniques, as using strong encryption

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

algorithms is expensive and unprofitable. One of the most undesirable measures of using Free VPN is the Advertisements. Most part of Free VPNs profit is made by the ads they sell to their clients as it is annoying to close an ad after every click on your device. Free VPNs are known to slow down your internet connection speed; hence such VPNs cannot be used for streaming videos, play games or for downloading purposes.

The slowdown is because of the encryption process, the VPN software is using to secure the data sent and received by you. But yes, if you are willing to accept its limitations then it is alright to use a Free VPN as some Free VPNs do provide good privacy and are secured as good as the paid ones.

4.2 Paid VPN

It is chargeable but they do offer the services they charge for. They offer legitimate security for your data and have high priority for your privacy. None of the paid VPNs share your data or keep atrack on your activity. They have strong end-to end, AES 256-bit encryption to mask your data so to prevent any kind of data leak or network attacks. There are no restrictions on speed limits or bandwidth hence enabling the users to stream online videos or download on the internet. With Paid VPNs users have more access to geo blocked websites, as the network and infrastructure spans all around the world.

V. Overview of VPN Protocols

5.1 PPTP

Point-to-point tunnelling protocol was one of the earliest and extensively used protocol, developed by Microsoft, and it was specifically designed for dial-up connections. However, as innovation progressed, PPTP's fundamental encryption was immediately split, trading off its basic security. But due to low encryption standards, PPTP protocol was one of the fastest. Also, PPTP is as yet utilized in specific applications, most suppliers have since moved up to quicker more solid protocols used in recent times. Operating systems like Linux and MAC also use PPTP apart from Windows.

5.2 IPsec

Internet protocol security protocol is used on a network level. IPsec provides security to the Internet Protocol communication by authenticating the session and encipher each data packet all along the connection. It is often used with other security protocols like SSL or L2TP but can be used solely as well. IPsec is secured and also faster than SSL. Configuring an IPsec VPN can be a complicated task.

5.3 L2TP/1PSec

L2TP is the abbreviation for Layer 2 Tunnel Protocol. It replaced the PPTP protocol and is combined with the IPsec protocol to institute high security VPN connection. This protocol works as follows: It generates a tunnel between two connections; both using L2TP and the data packets exchanged between them are enciphered by the IPsec protocol providing a secure connection between the two. It is a highly secured protocol with no known susceptibility.

5.4 IKEv2

IKEv2 is the abbreviation for Internet Key Exchange version 2. Microsoft and Cisco have mutually developed this protocol. Secure key exchange session is carried out by this protocol before communication begins. Like L2TP (and IKEv1), IKEv2 is ordinarily combined with IPsec for encryption and validation. IKEv2 has a feature for which it well known, that it is excellent at restoring the connection if it drops out or fails due to any reason. This feature of the protocol is useful in mobile devices like handsets, tablets and laptops as these devices keep switching between networks from 3G to 4G LTE or from mobile data to Wi-Fi. This VPN protocol is fast as well as secured as it is combined with IPsec.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

5.5 OpenVPN

As the name suggests, it is an open source protocol. Being open source, its underlying code can be accessed by the developers, hence making it a highly configurable protocol. It is not only popular because it is open source, but because it also has best security standards like AES-256 bit key encryption with 2048-bit RSA authentication. As it provides very good security, it compensates in speed, as it is not the fastest when compared to other protocol like PPTP

VI. Security Issues Involved While Using A VPN

VPN Most important and crucial factor for big companies and organizations is Security. A secure and solid infrastructure is required by the organizations for devices to alleviate the risks of malignant activities, both internally as well as externally. Hence, they make use of VPNs to avoid such risks. But there are some VPN providers who might just do exactly opposite for what the technology is intended for. Some issues are:

6.1 Logging

Utilizing a VPN while you are surfing anonymously turns out to be really trivial if the supplier is currently the person who logs them rather than your ISP. Sadly, that is the thing that happens when you pick a supplier who keeps logs. You become presented to extreme VPN security hazards just on the grounds that you no longer have authority over your protection. Utilization logs are the most hazardous ones since they track data about what you do on the web while utilizing a VPN. Connection logs are more "honest" since it's only information about the connection itself, not what you do with the VPN. Nonetheless, they're as yet not alright since they abuse your security.

6.2 Data Leak

It is the point at which you're utilizing a VPN to conceal your traffic and IP address, however they actually spill through the end-to-end tunnel the VPN uses. DNS leaks, IP leaks are genuine instances of such incidents. On the off chance that they happen, they essentially make utilizing a VPN silly. Presently, these sorts of leaks can happen on the grounds that the VPN supplier didn't design their connections well enough. However, they can likewise occur because

6.3 Weak Privacy Policies

A VPN supplier can guarantee they regard your protection and offer first class security in their advertising manual, while their Privacy Policy tells otherwise. But if you look closely enough at the policies, you will be able to find out supplier likewise keeps any logs or not. Also, banking on the wording in a provider's Privacy Policy, they may quietly and ambiguously specify that they gather client information and offer it with outsiders (advertisers and third-parties). Free VPNs are the ones that normally do this.

6.4 Badly-configured Encryption

On the off chance that the VPN provider didn't use strong encryption standards, they may have committed genuine errors while arranging the encryption the VPN will utilize. Indeed, free VPNs are probably going to have defective encryption. The surveillance organizations and cybercriminals may really figure out how to catch your web traffic, and decipher it by misusing or by using brute-force attacking the frail encryption.

6.5. Malware Attacks

In case you're not cautious enough, you may wind up dealing with major VPN security risks — like malware being infused into your gadget when you download a VPN client, which will begin keeping an eye on your exercises, spamming you with malignant promotions, and taking your personal information and monetary information. In case you're amazingly unfortunate, you may open your gadget to ransom ware which will encode your information, and request a major payoff in return for it.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

6.6 Usage of Traditional Protocol like PPTP

The PPTP convention may be quick and advantageous; however it's a big risk to utilize in the event that you wish to protect your data. Free VPNs make use of PPTP protocol to avoid high costs, and make good profits while risking the data security and privacy of their customers.

6.7 IP Addresses being used as Exit nodes

Essentially, it's the point at which a VPN supplier runs their organization off of clients' data transfer capacity and IP addresses. The clients "volunteer" their transfer speed and IP address for that, however many don't understand they're doing it since they don't read the supplier's TOS and Privacy Policy properly. Having your IP address utilized as an exit node is risky on the grounds that it essentially implies other VPN clients will utilize it when they're on the web. Along these lines, a cybercriminal could do illicit stuff on the Internet

VII. CONCLUSION

VPN is one of the widely used technologies in the world; nearly a quarter of the world's population uses VPN to access the internet anonymously. To conclude between the services provided by free and paid VPN, it is really user dependent choice, as users are the ones to decide the purpose for use. For example, if you need to send a confidential mail using a mall's Wi-Fi, a Free VPN might do the job, but if you wish to download a huge file from the internet anonymously then you would want to consider a Paid VPN. This paper explains the VPN technology, provides insights of the various protocols used in VPN and also lists the security issues related to VPN. This paper might help the user to choose their desired VPN provider and guide them to look for necessary features based on their requirements.

ACKNOWLEDGMENT

We would like to acknowledge the University of Mumbai, Mumbai, India to give us the opportunity to do the research work under the title "VPN: Overview and Security Risks". We would like to acknowledge the college L B.H.S.S.T's ICA Bandra East, Mumbai, India to support us during the research process. We would like to express gratitude to our Professor Mrs. Aquilla Shaikh and Professor Mrs. Khyati Manvar for their continuous support during the research process.

REFERENCES

[1]. Chetan S. More, Aman Anand, Kushagra Raizada, Manuj Srivastava, "Client Server Synergy using VPN", International Journal for Scientific Research & Development, pp166-169, 2018
[2]. Zhang Zhipeng, Sonali Chandel, Sun Jingyao, Yan Shilin, Yu Yunnan, Zang Jingji, "A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks", International Conference on Computing Methodologies and Communication, pp 510-515, 2018
[3]. Abdulrahman Mueed Ali Alshehri, Hosam Lafi Aljuhani, Aboubakr Salem Bajenaid, "Security Issues Of Virtual Private Networks: A Survey", International Journal of Computer Science and Information Security, pp 63-67, 2018
[4]. M.A. Mohamed, M.E.A. Abou-El-Seoud, A.M. ElFeki, "A Survey of VPN Security Issues", International Journal of Computer Science Issues, pp 106-111, 2014
[5]. Jayanthi Gokulakrishnan, "A Survey Report On Vpn Security & Its Technologies", Indian Journal of Computer Science and Engineering, pp 135-139, 2014
[6]. https://www.le-vpn.com/history-of-vpn/
[7]. https://www.geosurf.com/blog/history-of-vpn-thequest-for-a-better-internet/
[8]. https://blog.seattlepi.com/microsoft/2010/03/13/shouldmicrosoft-have-patented-its-vpn-in-the-90s/