MJRET

OPEN ACCESS

Multidisciplinary Journal of Research in Engineering and Technology

www.mjret.in

eISSN:2348-6953

Study on Virtual Private Networks

[1]Ms.Shreya Sairam, [2]Ms.Lavina Jadhav

[1,2] MET Institute of Computer Science,
Bandra West, Mumbai, India

Abstract*: Companies have an aim to keep their establishments networked. Rather than using expensive leased lines, internet solutions are preferred. Since the web is a public network, not much attention was paid to security up to now. When an access-desired network is made using public network infrastructure like global Internet to connect remote users or regional offices to company's private network is claimed to be Virtual Private Network(VPN). By using VPNs individuals, business groups and branch offices can all acquire the same kind of private connection to a branch office regardless of the tools they are using, the connection speed, or their location. This paper presents a comprehensive study of VPN to become more familiar theoretically in the field of secure network connection using tunneling.*

Keywords: *VPN, authentication, tunneling, encryption, cost, flexible.*

1. INTRODUCTION

The internet has evolved from modest beginnings of just four computers in 1969 that formed the ARPANET to an estimated 4.5 billion people in 2020(Stats). Businesses have come to depend on and influence real-time information. While the openness and availability of the web has facilitated explosive growth, the necessity for privacy has been a constant problem. Businesses that have computers in numerous physical locations are faced with the issue of the process to communicate privately with their various offices across long distances. To commune across long distances some large businesses chose to lease private phone lines from the service provider. This would ensure that only the company's information was conveyed on the line. The leased line transmitted only the information that the leasing company placed on it. The company purchased the line regardless if they transferred 1 megabyte or 1 terabyte. The leased line solution for personal communication was so expensive that several businesses simply couldn't afford this method of communication. The only solution to this was the Virtual Private Network(VPN). VPNs are used by remote clients to securely connect to the company's networks. The generic definition of a VPN is that it's a short lived , secure IP connection over a public IP network, like the web. By using VPNs individuals, business groups and branch offices can all acquire the same type of private connection to a branch office regardless of the tools they are using, the connection speed, or their location. Permanent devoted lines are not part of the web based VPN; rather, connections are established as they are needed and are stopped as soon as the data has been transmitted. Functionality of a VPN is precisely an equivalent as the other private network. Occupies its own private address space on the general public network, thus making it inaccessible from the opposite users thereon network. VPNs allow remote users to access private

networks safely over the internet. A remote user in one part of India can establish a secure network connection using a VPN to a LAN in another part of India and only incur the call cost for the local internet connection. A virtual private network gives secure access to LAN resources over a shared network infrastructure like the web. It is often conceptualized as creating a tunnel from one location to a different, with encrypted data travelling through the tunnel before being decrypted at its destination. Remote users can hook up with their organization's LAN or the other LAN. They can access resources like email and documents as if they were connected to the LAN as normal. Security elements like confidentiality, authentication and data integrity are often given in these VPNs. By using VPN technology it's possible to attach to a faculty LAN from anywhere within the world via the web , and to access it securely and privately without incurring the massive communication costs related to other solutions. They are inexpensive and are also highly flexible. Virtual private networks (VPNs) offer low-cost, secure, dynamic access to non-public networks. Such access would otherwise only be possible by using an upscale leased line solution or by dialing directly into the local area network (LAN). Recently, there has been swift growth and deployment of virtual private network (VPN)

2. HOW DOES A VPN WORK

A VPN allows you to create a tunnel, a connection from your home computer to a server somewhere else in the world; and that connection is encrypted. When you access something on the internet it goes through that tunnel and then it arrives at the other server and it goes on to the internet and will finally arrive at the web server or the service you are trying to use but the IP address will no longer be your IP address that's on that data packet. It will actually be the IP address of the VPN server and what happens is when it replies, it replies to the VPN server. The VPN services knows who it is for and it goes back down to the encrypted connection to this client who has connected to it. This allows a whole bunch of possibilities; for example your local telecommunications provider and your local government have no idea about the sites that you are accessing when you go through the VPN because its all encrypted. Once it goes out of the VPN server, it goes back into the open, it goes back pass through all the routers and things it needs to get to the website, and the website itself will register the fact that certain addresses has come to it but the address now will be that of the VPN server. It poses to be in a different country so if you try to access media videos streaming content or buy things then actually it might set the price or give access or block access now depending on where the VPN server is not depending on where you are. If you are using an open Wi-Fi then actually the initial connection from your laptop out to the internet is actually completely encrypted. Its compatible with any type of OS available across many types of devices. And once that connection is made all that data traffic and everything that you do will go through that VPN out into the internet in a different country and then further abroad wherever it needs to go.

3. TYPES OF VPNs

There are 2 types of VPN:

A. Remote Access VPNs:

Remote access VPNs are also called virtual dial-up networks (VPDN). These are user to-LAN connections used when employees of an organization who are in remote locations ought to connect with the company's private network. an organization that desires to line up a remote-access VPN usually outsources to an ESP or enterprise service provider. The ESP sets up a NAS (network access server and also provides remote users with the software they have for his or

her computers. Then users simply dial the NAS using a toll-free number and access the network via their VPN customer software. VPNs offer a decent third-party service for encrypted, secure connections between remote users within a personal network.

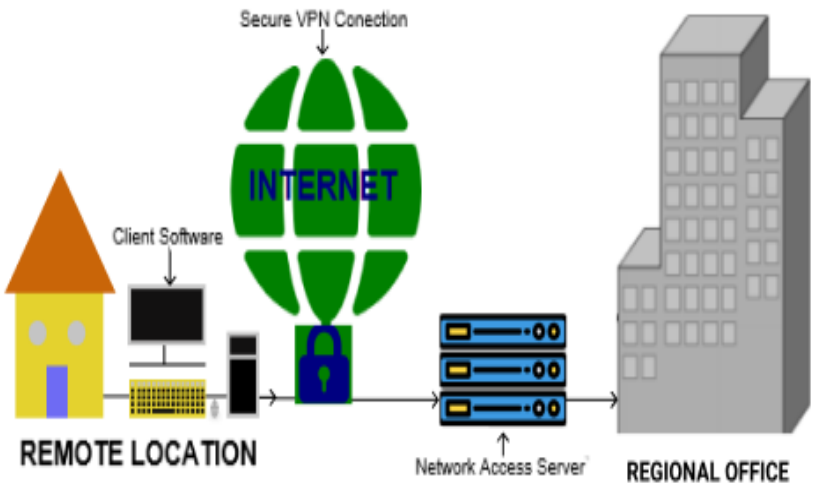

Fig 1 : Remote Access VPN

B. Site to Site VPNs:

Site-to-Site VPN is also called Router-to-Router VPN. Mostly used in the corporates. Permits offices in various fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location accessible to employees at other locations. An example of a corporation that needs a site-to-site VPN may be a growing corporation with dozens of branch offices around the world.

There are two sorts of site-to-site VPNs:

Intranet-based - Intranets, within the context of VPNs, are semi-permanent Wide Area Network (WAN) connections over a public network. They connect corporation head-offices to their branch-offices. In these connections, there's usually a high level of trust between the two communicating entities and therefore the corporate head-office usually controls both the source and destination nodes. The most appropriate VPN solution for this scenario is one where performance is preferred to safety. The importance of communication is in the speed with which the data is transferred from office to office. Security issues like confidentiality aren't important during this scenario. Having said that, however, a startling fact is that nearly half the unwanted intruders on a company network are company employees. If the corporate is bothered about proprietary information being leaked to employees then different levels of trust are applied to branches or individual users with firm access control. this kind of VPN is far more complex than the simpler, less secure implementations.

Extranet-based - The major worry in an extranet VPN solution is the versatility of the system. Extranet VPNs must be interoperable with reference to platforms, protocols, and authentication and encryption methods. Extranets are mainly accustomed to connect business partners. during this respect, all aspects of communication must be secure. Particularly the aspect of confidentiality is now important. it's vital that the information doesn't lose its integrity in transit and thus extranet VPNs must be the foremost secure VPNs. the standard structure of such systems is to possess a VPN proxy server resident behind a firewall. during this way, any traffic that passes the firewall is often filtered by the VPN server in step with the company's security policy.

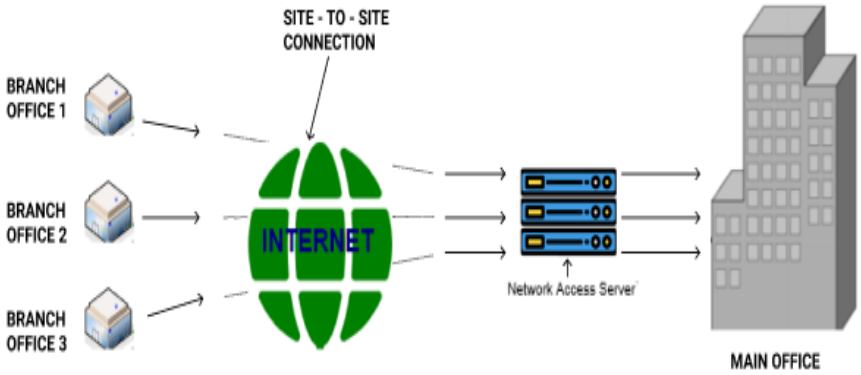

Fig 2 : Site-to-siteVPNs

4. COMPONENTS TO ESTABLISH / SETUP VPN

1. Authentication:

Tunnel endpoints must be authenticated before secure VPN tunnels are often established. Customized remote-access VPNs may use passwords, biometrics, two-factor authentication, or other cryptographic methods. Network-to-network tunnels often use passwords or digital certificates. They permanently store the key to permit the tunnel to establish automatically, without mediation from the user.

2. Tunneling:

Virtual private network technology depends on the concept of tunneling. VPN tunneling involves setting up and maintaining a logical network connection. On this connection, packets are established in a very specific VPN protocol format that is encapsulated within another base or carrier protocol then passed on between VPN client and server, and at last de-encapsulated on the receiving end. VPN supports two sorts of tunneling - voluntary and compulsory. Both sorts of tunneling are commonly used.

3. Encryption:

You must use data encryption to produce data confidentiality for the information that's sent between the VPN client and also the VPN server across a shared or public network, where there's always a risk of unauthorized interception. you'll be able to configure the VPN server to force encrypted communications. Users who hook up with that server must encrypt their data or a connection isn't allowed. VPN encryption doesn't provide end-to-end encryption. End-to-end encryption is encoding between the client application and also the server hosting the resource or service that is accessed by the client application. to induce end-to-end encoding, you'll use IPSec to form a secure connection after the VPN connection is created.

5. WHY WOULD YOU USE A VPN?

There are certain advantages cause of which one must use a VPN.

1. **A VPN hides your online identity:**

Since a VPN hides your IP address and encrypts your online traffic, it essentially makes sure your digital footprints can't be tracked on the web . Online hackers won't be able to use your real IP address to search out out personal details about you, and government surveillance agencies won't get to observe what you are doing online by snooping on your traffic. Besides it also helps you elude government surveillance, which also helps keep your privacy safe from advertisers.

2. **VPNs Help You Bypass Geo-Blocks:**

Did you ever try and access an internet site only to be met with the subsequent message (or a variation on it): "Sorry, the content you requested isn't available in your area." That's Geo-restriction technology in action. It's basically some way for content providers to manage which geographic areas their websites, movies, music, and television shows are available in. They normally do this because they have to adjust to copyright regulations, licensing regulations, and various legal procedures too. How does a VPN help with that issue? Here's something you would like to understand first – websites can normally hide content behind Geo-restrictions because they will see your Geo-location when you're online. Essentially, the platform you wish to access sees the connection request your device sends – and also the IP address the request comes from. Once the web site knows your real IP address, it can track your Geo-location easily. If it's blacklisted, you'll be denied access or redirected to a distinct page. Since a VPN can hide your real IP address, it can easily assist you to bypass Geo-blocks since the platform you would like to access will think you're from the "right" nation.

3. Secure your online connections:

Wi-Fi is everywhere nowadays, and it's extremely convenient to use – especially if you've got a decent mobile data plan. The sole problem with free Wi-Fi is that it's often unsecured, meaning you're putting your personal data at risk whenever you utilize it. After all, cybercriminals can determine a great deal about you – which may result in them stealing your MasterCard details, bank account details, Email login credentials. If you utilize a VPN, though, you won't have to be compelled to worry about those dangers. Why? Because a VPN uses encryption to secure your online communications, effectively ensuring nobody can monitor them. Basically, if any hacker would try and inspect your connection traffic, they'd just see gibberish. this is often also why VPNs are such an honest choice for accessing work files remotely too. If you ever ought to check a client file while you're taking a break at a cafe and using their Wi-Fi, your best choice is to use a VPN to be sure no would-be hackers can compromise your connection and work data.

4. Help you avoid online price discrimination:

Online retailers and airline companies sometimes prefer to display different prices to their website visitors based on which nation they're from. They typically do this to better segment their markets, and also to drive more profit. Of course, having to pay more cash for a similar product/service simply because you're from a distinct part of the globe is hardly fair. Since a VPN hides your IP address, it masks your real geopositioning too. So, if you're from a more developed country, you may try making it look like you're from a less developed area of the globe to induce a much better price. Just please

remember that a VPN isn't 100% bound to always assist you to deal with online price discrimination. Why? Because websites might sometimes use cookies (files that are downloaded to your device) to "remember" your device, which might lead to you being exposed to higher prices once you revisit the web site. Usually, it's best to also clear your cache besides just employing a VPN.

6. LIMITATIONS OF A VPN

1. Can sometimes slow down your internet speed:

Because the connection to the web with a VPN is rerouted and encrypted through the VPN server, your internet connection could be stalled slightly. This is often why it's important to see the speed of a VPN once you try it out. Most premium VPN services like NordVPN and ExpressVPN won't hamper your internet too much, but the speed rarely stays constant. Most internet users won't notice the difference. Folks that do things online that require a speedy connection can have some problems with the incorrect VPN. As an example , gamers that want to play online multiplayer games should check out the most effective VPNs for gaming, to make sure they won't experience any lag.

2. Some VPN providers log user data:

The idea of getting a subscription from a VPN provider is that you just route your internet traffic through their servers. They encrypt your data and allow you to make use of one of their many servers to also hide your IP address. This implies that you just ought to believe in your VPN that they won't abuse the information that travels through their servers. You have essentially bought safety and anonymity. Many VPN providers keep their end of the discount and completely ignore your personal data. they do not log what you are doing nor store your data. However, some VPN providers do log your data. Many free VPNs do that and a few providers make it clear in their license agreement that they may do that. This, of course, defeats the whole purpose of getting a VPN service in any respect. But these aren't the worst offenders. The really troubling cases are paid VPN providers who claim they do not log but are found later to try and do so.

3. A VPN is not legal in all countries:

Even though it'd be considered suspicious, the utilization of a VPN is legal in most countries. In fact, most big companies and corporations use a VPN as a part of their security. There are some exceptions though. Some countries want to possess complete control over the items their citizens get to check on the web. Since a VPN is often accustomed to bypass government censorship it's illegal in some totalitarian countries. In some countries, like Russia and China, you'll only use government-approved VPNs. The utilization of a VPN isn't necessarily illegal there, but they need to stay control over it. Some quality VPN providers like NordVPN though, have developed special "obfuscated servers" which should be possible to use in countries like China although it's not allowed by the government. In other countries like North Korea , the utilization of a VPN is totally banned, meaning you're not allowed to use a VPN. However, this is often only a drag if you reside in one of the countries that restrict or bans the utilization of VPNs.

7. CONCLUSION

Business organization nowadays isn't limited to at least one place. Hence, they're in need of security at an inexpensive price which may be fulfilled by employing a VPN. This technology is cost-effective and provides an efficient and efficient transmission of information among the network. We categorized all the various kinds of VPNs and noted that their flexibility allows the customer to decide

on which facilities are desired. The corporate can formulate a security profile for his or her offices and choose the VPN solution best suited to their needs. VPNs are still in their infancy and therefore the full potential for VPNs is yet to be exploited.

REFERENCES

[1]. https://www.webopedia.com/TERM/V/VPN.html

[2]. https://thebestvpn.com/what-is-vpn-beginners-guide/

[3]. https://vpnoverview.com/vpn-information/what-is-a-vpn/

[4]. https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

[5]. https://www.essaytown.com/subjects/paper/virtual-private-network-vpn/605140

[6]. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/