JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Empirical Study on Virtual Private Network

[1]Prof. Sunita Totade, [2]Dr. V. R. Dhawale, [3]Sakshi U. Choudhary, [4]Gauri P. Alone, [5]Falguni D. Joshi

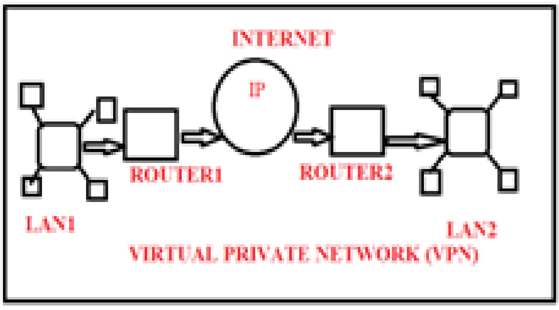
[1]HOD, Department of MCA, Vidyabharti Mahavidyalaya, Amravati, India
[2]Assist.Prof., K.K. Wagh Institute of Engineering Education and Research, Nashik, India
[3,4,5]Student, Department of MCA, Vidyabharti Mahavidyalaya, Amravati, India

Abstract: Now a days, network security becomes an essential part of human life. Everyone wants that his or her network should be secure and free from every kind of malicious activities. Network security is important because it keeps sensitive data safe from cyber-attacks and ensure the network is usable and trustworthy. Virtual Private Network provides us a protected network connection, whenever we use public network connection Virtual Private Network encrypt our internet traffic and hide our online identity. Due to this, third-party applications cannot get our data. Virtual Private Network connects our mobiles or PCs to server computer so that internet connection of server computer can be easily used. Virtual Private Networks are legal networks. Our data remains secure from hackers, public networks and government and third-party applications. The intention of this paper is to enlighten the structure of Virtual Private Network and how it is easy to use for individual and other sectors ae well. At the beginning we have introduced about Virtual Private Network and then working of VPN.

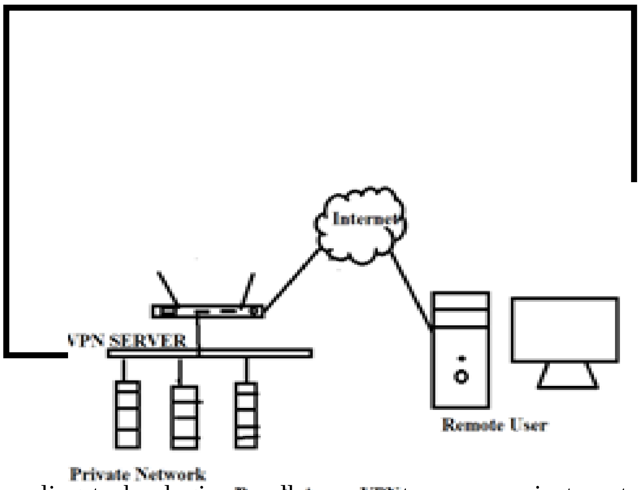
Keywords: Tunnel, Encryption, Remote Access VPNs, Personal VPNs, Mobile VPNs, Site-to-Site VPNs, WAN

I. INTRODUCTION

A Virtual Private Network (VPN) is a part of data security which provides security to its users from hackers, government, public networks and third-party applications. Virtual Private Network provides users an encrypted server and conceal user's IP address from corporations, government agencies and hackers. Virtual Private Network protects user identity even if they are using public or shared Wi-Fi and keep user's data private and safe from any prying internet eyes. Virtual Private Network or VPN is a technology which used for connecting the components and resources of one network over another. In common usage, a Virtual Private Network (VPN) is a private corporate network whose Wide Area Network (WAN) connections are made over a shared public network, usually the Internet.



VPN was firstly developed by Microsoft in 1996.The purpose behind it is that to provide secure access of Internet network of company to the remote employees of the company, here remote employees are the employee who works from outside location. By doing this productivity of company get increased and observing this other companies also started using VPN services. A Virtual Private network extends a private network across public network and enables users to send and receive data across shared or public networks as their devices are directly get connected to the private network. The benefits of VPN consist of increase in functionality, security and management of the private network. A VPN is created by establishing a virtual point-to point connection through the use of dedicated circuits or with tunneling protocols over existing networks. A VPN available from the Public Internet can provide some of the benefits of a Wide Area Network (WAN).



Remote Access VPN

II. WORKING OF VPN

Virtual Private Networks use tunneling technologies to allow users to access private network resources through the Internet or other public network. When user get connected to secure Virtual Private Networks then their internet traffic passes through encrypted tunnel which is not seen to any entity such as hackers, government and not even by Internet Service Provider of user. Due to use of VPN data is not readable to these entities. To understand how VPN exactly works let us take two different situations first is without using VPN and second is with using VPN-

2.1. Without using VPN

When without using VPN, we access internet then Internet Service Provider (ISP) also connect on the site which is success by us as they are providing Internet Service to us. Internet Service Provider gives us unique IP address, as ISP handle our internet data, they can get to know what we are browsing on internet so in that case our privacy not remains secure. Internet Service Provider can see what we are browsing over the Internet.

2.2. With using VPN

When we get connected to Internet through VPN then VPN established secure connection through VPN server this works when we have proper application installed in our devices. Application of VPN which present in our device for usage of VPN service is known as VPN client. As our internet traffic is still passing through ISP, but ISP is unable to see the final destination of the traffics. And websites we visit cannot see our original IP address as VPN masked our IP address. A VPN creates a private tunnel within a public connection (ex. the internet). VPN software allows it users to send and receive data transfers securely. VPN use different types of VPN Protocols to encrypt web connections and make them private. Furthermore, different versions of VPN software exist.

III. TERMINOLOGIES

1.Virtual: - It means existing, seen or happening online or on a computer screen, rather than in person or in the physical world.

2.Private: - It means belonging to or intended for one particular person or group and not to be shared by others.

3.Network: - A network consists of two or more computers that are linked in order to share resources, exchange files, or electronic communications.

4.Encryption: - Encryption is a method by which information is converted into secret code that hides the information's true meaning.

5.WAN (Wide Area Network): - A wide area network (WAN) is a geographically distributed private telecommunication network that interconnects multiple local area networks (LANs).

6.ISP (Internet Service Provider): - Internet Service Provider (ISP) refers to a company that provides access to the internet to both personal and business customers.

7.IP Address: -An IP address is a unique address that identifies a device on the internet or a local network.

8.Tunnel: - It is a kind of passage, similarly in networking, tunnels are a method for transporting data across a network using protocols that are not supported by that network. Tunneling works by encapsulating packets: wrapping packets inside other packets.

VI. SECURITY AND PRIVACY OF VPN

VPN provides you online privacy and anonymity by creating a private network from a public internet connection. VPN mask your IP address so that your online activities are virtually untraceable. VPN service establishes secure and encrypted connections to provide greater privacy than a secured Wi-Fi hotspot. A virtual private network is a key privacy tool that should be used whenever logging onto the internet from a public place or any other spot that offers access to free public Wi-Fi. A VPN creates a type of tunnel that hides your online activities. Virtual Private Network can hide a lot of information that can put your privacy at high risk. Here are five of them-

- Your Browsing History
- Your IP Address
- Your location for streaming
- Your devices
- Your web activity – to maintain internet freedom

A virtual private network is an internet security service that allows users to access the internet as though they were connected to a private network. VPNs use encryption to create a secure connection over unsecured internet infrastructure. Encryption is a way of scrambling data so that only authorized parties can understand the information. It takes readable data and alters it so that it appears random to attackers or anyone else who intercepts it; so, we can say that encryption is "secret code". VPNs are one way to protect corporate data and manage user access to that data. VPNs protect data as users interact with apps and web properties over the Internet, and they can keep certain resources hidden.

V. TYPES OF VIRTUAL PRIVATE NETWORK

Virtual Private Network services mainly falls in four types, viz., Remote Access VPNs, Personal VPNs, Mobile VPNs and Site-to-Site VPNs.

5.1. Remote Access VPNs Service

A Remote Access VPN lets us use the internet to connect to a private network. The internet is an untrusted link in the communication. VPN encryption is used to keep the data private and secure as it travels to and from the private network. User can connect to another network using private encryption tunnel. User can get connect to public network or company network through this VPN. Remote Access VPN are also sometimes called client-based VPNs or client-to-server VPNs.

5.2. Personal VPNs Service

A Personal VPN service connects you to a VPN server which act as intermediate between your device and the online services which you want to access. The Personal VPN is sometimes called as a consumer or commercial VPN which encrypts our connection, hides your identity online and lets you spoof your geographic location. A Personal VPN service is differing from a Remote Access VPN as it doesn't give you access to a private network instead of that a Personal VPN works by giving you access to the public internet but over encrypted connection.

5.3. Mobile VPNs Service

While remote access VPNs let you connect to a local network from anywhere, they assume that the user will stay in one location. If the user disconnects the IP tunnel closes. A Mobile VPN is better option than a Remote Access VPN if the user is unlikely to have a stable connection, on the same network, for the entire session. With a mobile VPN, the VPN connection persists even if the user switches Wi-Fi or cellular network, loses connectivity, or switches their devices off for a while. A Mobile VPN can be used with any device and any connection: it doesn't have to be a mobile phone on a mobile network.

5.4. Site-to-Site VPNs Service

Whereas a Remote Access VPN is designed to let individual users to connect to a network and use its resources, a Site-to-Site VPN joins together two networks on different sites. It is also known as Router-to-Router VPN. It is mainly used in corporate environment which have their offices and headquarters at different locations, in this case Site-to-Site VPN creates a closed internal network where each and every location get connected with each other and connect them into a single network. Site-to-Site VPN is also known as intranet. Site-to-Site VPNs are also sometimes known as network-based VPNs.

Depending on who owns the networks being joined, there are generally two different forms of Site-to-Site VPN:

- **Intranet-Based VPN**: When the network being connected belong to a VPN single company, the combined VPN is known as an intranet-based VPN. This enables a company to establish a single wide area network (WAN) that spans two or more of its offices. Users in the company can access resources from other sites as easily as if they were on their own site.
- **Extranet-Based VPN:** When the networks being connected belong to different companies, the combined VPN is known as extranet-based VPN. An extranet VPN is used, for example, when a company wants to connect to its supplier's, so they can trade more efficiently.
- **VI. USES OF VIRTUAL PRIVATE NETWORK**
- VPN is used whenever user feel that privacy is most vital factor for users.
- Users can use VPN while Travelling, Streaming, while using public Wi-Fi, Playing Games, Online Shopping. VPN can be used in that devices which can access internet.
- Devices like Laptops, Tablets, Smart phones, Voice assistant, Smart applications, Smart TV can access internet through VPN Services. VPN provides service on multiple platforms.
- As VPN are legal and it is used by the companies to protect their data from hackers and it is also used by individual.
- VPN are also used in the countries having highly respected government.
- VPN can be used for one's own security over public network.

VII. CONCLUSION

Security of data is very important for everyone, as there are many different sources and services are available in the market but among them Virtual Private Networks services provides better privacy and security to the users. VPN hides our original online identity and activities or work we perform on internet from hackers and third-party applications. User can switch as often as he or she lies with no limits using different locations; using VPN one can download or access content from anywhere; VPN can access on various platforms like Windows, Mac, iOS, Android, Linux, routers, etc. Virtual Private Networks make users relax in terms of online security and privacy.

REFERENCE

1. 1.Kanuga Karuna Jyothi, Dr. B. Indira Reddy "Study on Virtual PrivateNetwork (VPN), VPN's Protocols And Security", Int © 2018IJSRCSEIT | Volume 3 | Issue 5.
2. Komalpreet Kaur, Arshdeep Kaur "A Survey of Working on VirtualPrivate Network" © 2019 IRJET | Volume 6 | Issue 9.
3. 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-vpnand-its-protocols/
6. D. Simion, M.F. Ursuleanu, A. Graur, A.D. Potorac, A. Lavric"Efficiency Consideration for Data Packets Encryption with inWireless Tunneling for Video Streaming" INT J COMPUT COMMUN8(1):136-145
7. https://whatismyipaddress.com/vpn-comparison
8. 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