International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study on Virtual Private Internet – Methods and Techniques

J.Sowmiya[1], T.S.Keertana[2], V.Sandhiya[3],V.J.Harishmitha[4]

Department of Computer Science, R B Gothi Jain College for Women, Chennai - 600052

A B S T R A C T

A Virtual Private Network (VPN) is a technique of using public telecommunications infrastructure to offer secure communication between members of a group. It uses a tunnelling mechanism and other security techniques to ensure privacy. A virtual network (VPN) is a network that is established on top of an existing physical network to offer a secure communications channel for data and other information sent between two endpoints. SSL stands for Secure Sockets Layer (SSL). Virtual private networks (VPNs) are secure remote access networks that allow users to access a company's resources. To carry traffic via the Internet (or a managed Internet protocol (IP) network or a provider's backbone), a mix of tunnelling, encryption, authentication, and access control is employed. Simply said, a VPN provides users with a secure connection.

Keywords: Virtual private networks, Secure Sockets Layer, Internet Protocol Security.

1. Introduction

. A virtual private network, or VPN, creates a private network from a public internet connection, giving you online privacy and confidentiality. VPNs conceal your internet protocol (IP) address, making your online activities almost invisible. Most significantly, VPN services create safe and encrypted connections that provide more privacy than even a protected Wi-Fi hotspot. (VPN) can help with many of the challenges that today's private networks have. The VPN allows for more flexible IT support. Global VPNs provide access to all areas throughout the world at a fraction of the expense of dedicated connections. VPN services offer remote access to the intranet at a significantly reduced cost, making it possible to accommodate a mobile workforce. The VPN architecture allows for a secure connection.

The virtual private network (VPN) is a novel solution to the problem of providing efficient, dependable, and simple telecommunications to large, geographically dispersed groups of users. VPN replaces previous private networks with a flexible design that is simple to administer while also providing improved services. Interconnection requirements and network complexity increase as the number of business sites in the private network grows. Network management and traffic engineering are becoming increasingly crucial and costly. Indeed, the size and complexity of certain major private networks can dwarf that of smaller PTTs.

It is here that the virtual private network first demonstrates its merits, allowing private networks to maintain a very straightforward network operation. They were crucial in transforming the Internet into a powerful business tool. Instead of using a costly private network, today's VPNs use packet encryption to establish secure connections between a remote user and a corporate or other network. However, they have usually only linked a few nodes that are controlled and configured by a company's IT department. Many firms today need to let managers, employees, partners, suppliers, consultants, e-commerce customers, and others to access networks from their own PCs, laptops, publicly available computers such as those at airport self-service, and even mobile devices. This data is especially useful in assisting enterprises in determining how to best deploy VPNs in their individual network settings. Because a VPN may be utilised

over existing networks like the Internet, it can also help with secure data transfer across public networks. An SSL VPN is made up of one or more VPN devices that users can connect to via their web browsers. The SSL or its successor, the Transport Layer Security (TLS) protocol encrypts traffic between the web browser and the VPN equipment. An SSL VPN or a TLS VPN can be used to describe this type of VPN. SSL VPN stands for Secure Socket Layer Virtual Private Network. Remote users can access Web apps and client/server applications over SSL VPNs.

2. Types of VPN

VPN stands for Virtual Private Network that allows an user to connect to a private network over the internet securely and privately. It is basically many types;

- IPSec
- Remote Access VPN
- Site-to-site VPN
- Point-to-point tunnelling protocol
- OpenVPN
- Internet key exchange
- NordVPN

IPSec: It's a group of protocols that are used together to set up encrypted connection between devices. It is used to set up VPNs ,and it works by encoding IP packets, along with authenticating a source where the packets come from ..

Benefits:

*Transparent to end user

*It is a firewall is friction to bypass

Remote Access VPN:

It permits a user to connect to a private network and access to all services and resources remotely

It is Useful for home users and business users both.The internet security also use VPN services to augment their internet security and Privacy…

Benefits:

* Provide Network Scalability

* Reduce Support Costs

* Avoid bandwidth Drowning

Site to Site VPN:

It is also called as Router -to-Router VPN and is commonly used in large companies

It is used to connect the network of one office location to network at another office location.

Benefits:

*Cost effective security

*Secure connection for remote work

3. Working Procedure for VPNS

When you turn on a VPN, it establishes an encrypted connection (also known as a "tunnel") between your device and a VPN service's distant server. All of your internet traffic is sent through this tunnel to the server, which then forwards it to the public internet. Data returning to your device follows the same path: from the internet to the VPN server, across an encrypted connection, and back to your machine. Remember that you don't need the help of another company to set up a VPN. There are a few alternatives for creating your own, including Outline. It's not difficult to do, but you'll either need your own server or rent one. While some efforts are being made to make self-hosted VPNs more accessible, it's best left to tinkerers who want to get their hands (digitally) filthy. Several VPNs claim to provide some level of security against malicious files. The concept is that files travelling via the VPN Company's networks are scanned before they reach your machine. A VPN can help you avoid being monitored online by hiding the contents of your web traffic from some observers. However, a VPN can only offer limited security against the most common online risks, such as malware, social engineering schemes, and phishing sites. There are more effective approaches to deal with these dangers.

4. Conclusion

A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone.

REFERENCES

1. Ramachandran Venkateswara, Virtual private networks IEEE potentials 20 (1), 11-15, 2001
2. D Wood, V Stoss, L Chan-Lizardo, GS Papacostas, ME Stinson 1988 International Conference on Private Switching Systems and Networks, 132-136, 1988
3. Virtual Private Networks - Charlie Scott, Paul Wolfe, Mike Erwin - Google Books" https://books.google.co.in/books?hl=en&lr=&id=OuFQ3t7eF4IC&oi=fnd&pg=PR9&dq=info:aaSvLMo1TC0J:scholar.google.com/&ots=hgmYAtBG2D&sig=sKuPYt1yFoWnaUa0STzjfj80Xz4&redir_esc=y#v=onepage&q&f=false
4. R. Younglove , Source: Volume 11, Issue 6, December 2000, p. 260 – 262 DOI: 10.1049/cce:20000602, Print ISSN 0956-3385, Online ISSN 1741-0460
5. https://doi.org/10.1016/B978-0-12-803843-7.00058-2
6. M Praneesh and Jaya R Kumar. Article: Novel Approach for Color based Comic Image Segmentation for Extraction of Text using Modify Fuzzy Possiblistic C-Means Clustering Algorithm. IJCA Special Issue on Information Processing and Remote Computing IPRC(1):16-18, August 2012. Published by Foundation of Computer Science, New York, USA.