Overview of Virtual Private Networks: History, Function, Types, Popularity, and Future

Nathan Mortell

ABSTRACT

Virtual Private Networks (VPN) are used to create a secure connection between your devices and the Internet. By using tunneling and encryption to mask your IP address, it allows you to stay anonymous while having a connection to the Internet and helps keep the location of the user private by hiding the IP address. This paper will discuss the history of VPNs, the multiple functions and types, the rising popularity of VPNs for businesses and for personal use, and the potential future.

Keywords: VPN, Security, Network, Protocol, Encryption, WAN, LAN, Tunnel

INTRODUCTION

The Internet is the most popular and readily available form of communication known today since it's a global network of connected computers that can share information with one another. 'To put things into perspective, "In comparison to 2015, when 35.3 million adults used the internet daily in the United Kingdom, 41.8 million adults did so in 2016."' [6] The Internet will continue to grow, and with it, privacy and security will always be a prominent issue to maintain. From businesses constantly transferring confidential information across the globe, to individuals simply accessing the Internet from their home, it's essential that all data going through public space is kept encrypted and secure from unwanted parties. There have been multiple means of doing this since the early days of the Internet, but the most popular and modern method of keeping your data secure is to use a VPN. A virtual private network, or VPN, is used to create a digital connection between your devices and a remote server via a point-to-point tunnel either owned by a VPN provider or created locally using a variety of means. VPNs encrypt your Internet traffic and disguise your online identity, making it more difficult for third parties to track your activities online and potentially intercept your data. 'By its very definition, a VPN connection is: Virtual because no physical cables are involved in the connection process. Private because through this connection, no one else can see your data or browsing activity. Networked because multiple devices- your computer and the VPN server- work together to maintain an established link.' [1]

HISTORY

The history of protecting and encrypting browser data can be dated to before the creation of the Internet, and when the concept of linking multiple computers was becoming a reality. 'In the late 1960s, the

Advanced Research Projects Agency (ARPA) developed a method to link distant computers. They introduced a system in 1969 that relied on packet switching, where data packets were transferred between machines. This system, known as ARPANET, grew throughout the 1970s, connecting multiple educational and research institutions.' [2] This, however, had limitations since it operated off of the network control protocol (NCP), which had the limit of only being able to connect computers within the same network. The solution to this would come 20 years later with the creation of TCP/IP. 'By the 1980s, ARPANET officially adopted the Transmission Control Protocol (TCP), also known as Transmission Control Protocol/Internet Protocol (TCP/IP). The new approach transitioned from NCP to a system allowing diverse device connections, giving rise to what's now termed the internet.' [2] TCP/IPs work by having four layers: link, Internet, transport, and application. An IP consists of unique digits identifying each device online. To make this process more convenient, in 1984, the Domain Name System (DNS) was born, which made mapping simple domain names to IP addresses. After the creation of IP and DNS, the Internet became much easier to access to the broader public and was no longer just limited to educational and research institutions. 'The inaugural online platform emerged in 1985, allowing users to enter chat rooms and engage in digital communities. Named America Online (AOL), this system relied on dial-up, where users dialed their internet service provider (ISP) to access AOL.' [2] As the Internet rapidly grew in popularity, growing concerns about being able to communicate securely and privately online sparked the development of early IP encryption and is the precursor to the modern VPN. 'In 1993, a team from Columbia University and AT&T Bell Labs finally succeeded in creating a kind of first version of the modern VPN, known as SwIPe: Software IP encryption protocol.' [7] This had a significant influence on the development of IPsec and is still an encryption protocol that's used today.

FUNCTION

The core function behind a VPN is that it's able to hide your IP address by redirecting it through a specially configured remote server run by a VPN host. 'This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.' [7] This is done by a process called tunneling. 'Tunneling or encapsulation is a technique of packaging one network packet inside another. The encapsulated packet is called the tunneled packet and the outer, encapsulating packet is called the transport packet. All the information in the packet is encrypted at the lowest level, which is the link level of the OSI model.' [5] The ability to make a tunnel is very straightforward, the outer IP header is added onto the original header and between the two is the security information specific only to the VPN tunnel. The outer header directs towards the source and

destination of the tunnel while the inner header identifies the original header and the receiver of the packet. The most common form of tunneling is point-to-point tunneling (PPTP). ‘This benefits home users and users who work at a business. A security aspect when accessing the VPN is that the user must login using an approved password. PPTP VPN is the most commonly used form due to the fact that it is compatible with operating systems such as Windows, Linux, and Mac.’ [6] Another type of protocol is Internet Protocol Security (IPsec), which is used in an IP network to establish a secure connection within the Internet. ‘How the IPsec protocol works is that it secures the IP communication by validating “each session and individually” encrypting the data packets along the connection.’ [6] There are two types of IPsec security protocols, as shown in Figure 1 below:

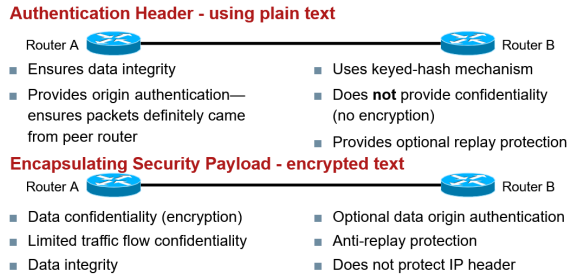

Fig. 1. IPsec Security Protocols [4]

The benefit of using IPsec is that it can protect against on-path attacks, where someone is either eavesdropping on a connection between two individuals or pretending to be one of them. As an example, if you were using the public wifi provided by a coffee shop, and without your knowledge, someone managed to get authentication to view all incoming and outgoing data. Having the additional layer of a VPN with IPsec protocols will prevent your data being traceable.

TYPES

There are multiple types of VPNs, and each has a different purpose and form of connection. The most common form of connection is a remote-access VPN, which is a client device that connects to a private network from a different location. See Figure 2 for an overall layout. ‘The VPN server provides access to the resources of the network to which the VPN server is connected. The packets sent across the VPN connection originate at the VPN client. The VPN client authenticates itself to the VPN server and, for mutual authentication, the VPN server authenticates itself to the VPN client.’ [5] Anyone connecting to a remote-access VPN can do so from a different geographical location and has the ability to join a closed network to access all its services and resources. However, in order for people to establish a connection, the VPN must use the same protocol as the client. ‘The reason to why it is an advantage for businesses and individuals at home to use remote access VPN, is that it is convenient for those who work in a different country, so it would mean that the business can function the same way even if the staff member was working in the office.’ [6]

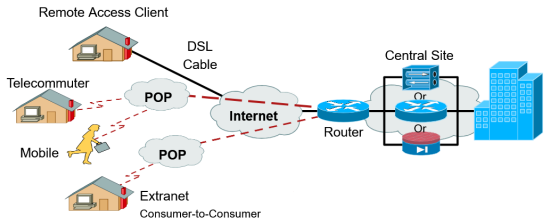

Fig. 2. Remote Access VPNs [4]

Site-to-site VPNs are typically used in businesses that need to communicate between different buildings across the geographic locations. See Figure 3 for an overall layout. 'A site-to-site VPN connection connects two portions of a private network or two private networks.' [5] The main difference between remote access and site-to-site is that, 'those who need to access any resources from the organization would need to be using the remote access VPN in comparison to site to site VPN, an individual would access the resources if they were physically at one of the offices branches for retrieving the resources from the main headquarters of the organization.' [6]

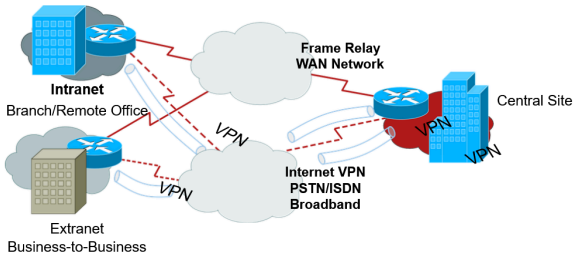

Fig. 3. Site-to-Site VPNs [4]

POPULARITY

The rising popularity of VPNs can be attributed to the fact that the majority of your time on the Internet could potentially be monitored. In the post-Snowden world, it's hard for people not to think about how their data could be secretly gathered and stored. While VPNs can't fully stop this, they can still do an excellent job at giving you online privacy and protection on public Wi-Fi. VPNs also have the major benefit of bypassing geo-restrictions (EXAMPLE) on an area and how they can be remotely accessed. They are also very easy to get, either through making your own or getting a subscription to one of the many VPN providers. When looking for a provider, it's important that they have the following features.

'**Strict no-logs policy**: A strict no-logs policy will not "log", or collect and save, any personal information from your network while you are browsing.

User-friendly apps for devices: VPNs should be able to provide proper guides, tips, and instructions about how to best use their service.

Large server coverage: Premium VPNs will allow you to connect you to any location with servers across the globe.

Multiple Simultaneous Connections: Premium VPNs will allow you to be able to use the VPN on multiple devices.

256-bit encryption: This is the highest-level encryption currently available that will protect personal information and browsing activity. '[3]

The strict no-logs policy is an important one to consider, most VPN providers store memory data in RAM. RAM is volatile memory, which means that all data is erased when the server is powered off or restarted.

This removes the chance of there being any persistent data, and in case of an emergency, all the servers can be powered off.

FUTURE

The potential future applications of VPNs are exciting. One such advancement in VPN technology is that Blockchain could be used to make decentralized VPN services or dVPNs. ‘A dVPN runs on a peer-to-peer network that leverages blockchain technology. Decentralized nodes, operated by volunteer hosts, eliminate single points of failure and ensure that no single entity has control over every user’s data. Due to a dVPN’s more democratic functioning, they are also seen as being more resistant to censorship and government data sharing.` [8] When it comes to a normal VPN provider, they must run regular audits of the entire network to prove that they are trustworthy. For dVPNs, each volunteer node host must prove they are trustworthy due to the decentralized nature. Another upcoming application comes in the form of VPNs protecting all your local networked devices. As more standard household appliances become a part of the IoT or Internet of Things, this can increase the chances of there being holes in your network due to unsafe connections. This could be fixed by fully controlling all your devices through a VPN. ‘A VPN can encrypt and protect communications for all of your devices. Unlike the typical personal VPN that requires you to connect each individual device, IoT VPNs extend across an entire network to safeguard all devices.’ [8] The current drawback of this is that many VPN providers have a limit on the amount of devices that can be connected at a time.

CONCLUSION

Having a VPN can be seen as a core component of safely traversing the Internet in modern times for both personal use and for businesses. What started off with the ability to only link computers between educational/research institutions would grow over time to now shape what the modern Internet has become. The fact that VPNs can be secure, remotely accessed, run on multiple devices simultaneously, and can set an individual’s location to be anywhere the VPN server has coverage is truly incredible. VPNs are also customizable, with examples being the remote-access VPN that are commonly used in homes and for personal use. While site-to-site is used for businesses to establish a private connection between different offices over the Internet. Overall, this paper is designed to help individuals or businesses understand the importance of VPNs and why they are important for keeping your data safe and secure while on the Internet.

REFERENCES

[1] "What is a VPN? How VPNs work and why you should use one." https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn

[2] "What is the history of VPN?," *Palo Alto Networks*. https://www.paloaltonetworks.com/cyberpedia/history-of-vpn

[3] S. A. Cho, "The power of Virtual Private Networks (VPN) in privacy protection | Office of Information Security | Washington University in St. Louis," Mar. 28, 2024. https://informationsecurity.wustl.edu/the-power-of-virtual-private-networks-vpn-in-privacy-protection/

[4] "MINS 346 Data Communications & Networking Week 13 Part 2," *Google Docs*. https://docs.google.com/presentation/d/1XucAIFRYiMiXNKk2n-ucvUHqX6yux0VxxYH4Vhv0pHo/edit?slide=id.gfbcccf3bcb_0_32#slide=id.gfbcccf3bcb_0_32

[5] Jyothi, K & Reddy, B Indira. (2023). CSEIT1835225 | Study on Virtual Private Network (VPN), VPN's Protocols And Security.

[6] Hussain, Junaid, Virtual Private Networks: Fundamentals, Security Issues and Solutions (December 12, 2022). Available at SSRN: https://ssrn.com/abstract=4478285 or http://dx.doi.org/10.2139/ssrn.4478285

[7] "What is VPN? How It Works, Types of VPN," *Kaspersky*, May 05, 2023. https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

[8] S. Singleton, "The future of VPNs: Decentralized and post-quantum security," *PCWorld*, Jan. 01, 2025. https://www.pcworld.com/article/2547145/future-of-vpns-decentralized-and-post-quantum.html