# What Even are VPNs?

Almost everyone knows what a VPN is, most have probably even used one. But, do people even know what VPN stands for? Do they know why the need for them arose? Or do people know how they work? The answer that the majority of the population would give to those questions is no. Before I started researching for this paper I also would have said no to all those questions. My aim for this paper is to explore the history of how VPNs arose and why they were needed, explain how VPNs work, and finally explain vulnerabilities with VPN’s.

To begin, let's start with the history of the internet and why the need for VPNs arose. In 1969 the Advanced Research Projects Agency (ARPA) developed a method that could link together distant computers; it involved switching data packets between machines known as ARPANET. This system had its limitations, however, it could only connect devices that were on the same network. They solved this issue in the 1980s with the introduction of Transmission Control Protocol/Internet Protocol (TCP/IP). The combination of TCP and IP allowed for devices connected to the internet to communicate with each other using their IP addresses and TCP to deliver the data. This also allowed for the broader public to be able to use the internet as it was previously only educational and research institutes that used it. Next in the early 1990’s HTTP was introduced which allowed access to online resources via hyperlinks, this led to the World Wide Web (WWW). Now that the internet was so widely accessible security and privacy concerns began to arise. This is what sparked the development of IP-layer encryption which in turn led to the creation of IPsec which authenticates and encrypts every IP packet in data traffic. IPsec is still used today. After the introduction of IPsec microsoft introduced Point-to-Point Tunneling Protocol (PPTP), this system created a virtual data tunnel and ensured more secure data transmission. PPTP was a big milestone for VPN technology as the tunnel system is still used in modern VPNs. PPTP was then further developed into L2F which now addressed multiple types of internet traffic and allowed for enhanced encryption methods. In the early 2000s the internet was becoming a necessity in everyday life and companies functionings and thus security concerns were once again risen and VPNs arose as an essential tool to combat the ever growing security concerns. VPNs have since evolved from being something that was solely used by companies to protect their private data to an easily accessible resource that anyone can use.

Now that we have an understanding of the history of the internet and where the need for VPNs arose let's explore how VPNs actually work. To begin, what does VPN even stand for? It stands for Virtual Private Network, VPNs transfer data securely across the internet by creating an encrypted tunnel between the user and server. The first step in using a VPN is the initiation phase. This phase begins with authenticating the user. It authenticates the user via certificates from trusted certificate authority, there can also be a password needed to access the VPN. This protects the user from unauthorized access from the local and wider internet. The next step is the client-server handshake. In this handshake the user and server agree on a VPN security protocol that will be used and a cipher suite that will dictate the encryption method and key exchange method that will be used. Next the tunnel is established. The client and server here agree on a tunnel protocol (like IPsec that was mentioned before). This tunnel selection is what determines how secure the client's data will be. The key exchange process is next, which is often exchanged using the Diffie-Hellman algorithm. Once that is complete the tunnel is successfully set up and the client now has a secure channel for their data! There are two types of tunnels, split vs full. A split tunnel allows for the user to directly access noncorporate traffic, this can lead to vulnerabilities. A full tunnel ensures that all of the client's traffic is sent through the VPN.  Now comes the actual data transferring. To do this it starts with the IP address that the client was assigned via their VPN, this replaces the client's actual IP address. Data packets are then transferred through the established tunnel and at the end of the tunnel the VPN decrypts the data and forwards it to the destination. The next task that a VPN must do is maintain and manage the connection to do this it must constantly ensure protection, stability link, and data integrity. To do this it can use methods like checksums or sequence numbers. In order to keep the connection between the user and the VPN alive, the VPN uses heartbeats and keepalive messages. The final step is to terminate the connection between the user and the VPN. The client begins by telling the server it wants to end the session or the server itself begins to terminate the connection. The VPN then begins to dismantle the tunnel that it created which can be done by sending a termination packet. The VPN then ensures that things like IP address and other data associated with the session are deleted. Some VPNs also log the session. The VPN session has now been fully completed.

VPNs seem great, no? You can freely use the internet without any concern for your security! Unfortunately, however, VPNs are not without their vulnerabilities. VPNs are vulnerable to man-in-the-middle (MITM) attacks and can lead an attacker to eavesdrop and even manipulate data when the client thought it was secure. If a VPNs configuration, settings, or configuration are mismanaged they can lead to data leaks. There are also malicious VPNs masquerading as legitimate services that can lead to a person downloading malware or using a VPN that isn’t protecting their data but leaking it instead. If a VPN has a weak protocol its encryption is weak and can lead to easier hacking or MITM attacks. VPNs that log sessions can be vulnerable if the service sells their users logged data.

Hopefully now an average person can grasp how VPNs came about, how they function, what they do, and their vulnerabilities. VPNs are a wonderful tool, however they are not perfect yet and are ever evolving. Choosing what VPN to use is of utmost importance as that is what determines how secure your connection and data transferring is, and if you choose the wrong one it could even lead to your data being leaked that's why it is important to be able to understand how they work and be able to differentiate between a malicious VPN, an average VPN, and a secure VPN with strong encryption methods and a secure tunnel.

Sources:

“How Does a VPN Work?” *Palo Alto Networks*, www.paloaltonetworks.com/cyberpedia/how-does-a-vpn-work#setup. Accessed 21 Nov. 2024.

“How Vpns Work: A Closer Look at Virtual Private Networks.” *Medium*, Medium, 30 Oct. 2023, medium.com/@MakeComputerScienceGreatAgain/how-vpns-work-a-closer-look-at-virtual-private-networks-e8a352937de8.

Netalit. “5 Biggest VPN Security Risks.” *Check Point Software*, Check Point Software, 5 Aug. 2024, www.checkpoint.com/cyber-hub/network-security/what-is-vpn/5-biggest-vpn-security-risks/.

“What Is the History of VPN?” *Palo Alto Networks*, www.paloaltonetworks.com/cyberpedia/history-of-vpn#:~:text=Who%20introduced%20VPN%3F,creating%20a%20virtual%20 private%20network. Accessed 21 Nov. 2024.