March 1, 2019
CS-02-2019

Virtual Private Network (VPN)

OVERVIEW

A virtual private network (VPN) creates an encrypted connection from a device to a network over the Internet. A VPN allows for a private connection while still using public Internet. As shown in Figure 1, a VPN can act as an intermediary where data is encrypted, routed through a private server (owned by the VPN provider), and then travels to the intended destination like Google or Facebook.

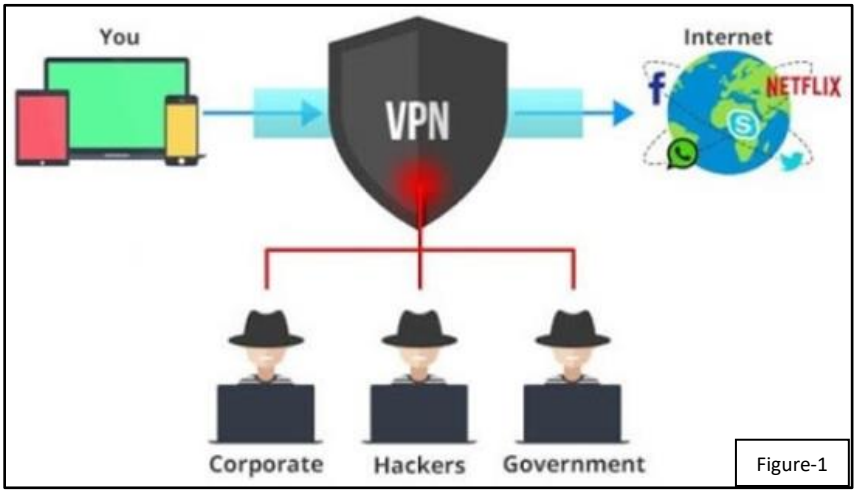

Figure-1

Websites may collect information on who visits or uses their services, such as Internet Protocol (IP) address and location data, but by using a VPN they will only be able to see the information from the VPN server and not where it originated.

Additionally, because the traffic is encrypted between the device and the network, traffic is unable to be seen as it travels across the web. The encryption of transmitted data adds a level of security from individuals looking to steal private information.

VPN USES

Desktops, laptops, smartphones, and tablets can all connect to a VPN and be used for a wide range of purposes. One of the most common uses for VPNs is the protection of private information utilizing encryption and IP address manipulation. In a business or corporate setting, a VPN can allow an employee to work away from the office and virtually connect to the corporate network. A site-to-site VPN can also connect corporate offices to far away branch offices.

ENCRYPTION

Most commonly a VPN is intended for accessing the Internet through unsecured networks such as those in hotels or coffee shops. Public, or free wi-fi, is generally insecure and offers no means of security for private information.

These networks are widely used by the public for communication over social media networks, email, online shopping, etc., and are prime targets for malicious actors. Data traveling unencrypted over public wi-fi is susceptible to a common vulnerability called a man-in-the-middle attack. As shown in Figure 2, this attack occurs when a malicious actor places a device between the victim's device and the server designed to reroute and intercept all the victim's traffic to the attacker's device first. By connecting to a personal VPN while accessing public wi-fi, transmitted data will be encrypted and hidden from prying eyes. Thus, the use of a VPN is encouraged whenever dealing with private information while using public wi-fi.

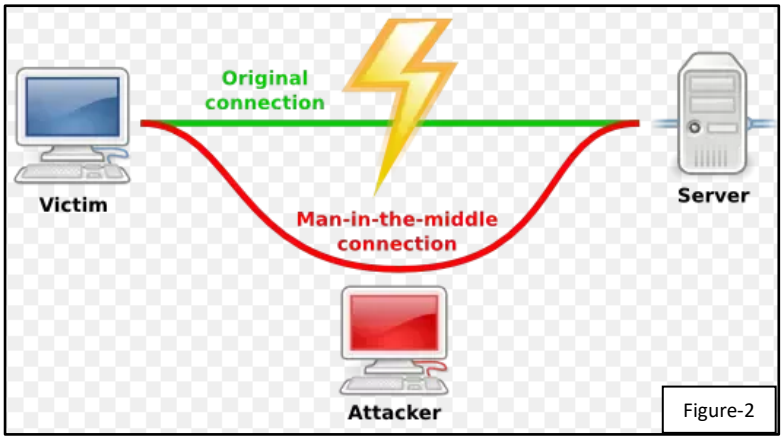

Figure-2

Voice-over-IP (VoIP) technology such as Skype, Lync, Zoom, or any other online voice chatting application is vulnerable to eavesdropping by malicious actors. Regular VoIP users should be cognizant of the level of information they disclose over these applications and consider using a VPN connection.

IP & IDENTITY MASKING

As discussed previously, websites such as search engines catalog web searches and generate search history for users. This data is then attached to the IP address and are subsequently used to customize advertising or sold to third parties for marketing campaigns. VPN services allow connections to servers around the world, thus enabling IP address manipulation. A VPN can cloak your IP address and keep search history and Internet activity private. Reporters or journalists can mask their true identity when conducting research. A user in China who would normally not be able to see content from other countries due to China's censorship practices, can select to access a VPN server in the United States, inevitably being able to view United States websites and content.

INTRANET TUNNELLING

There are several different types of VPNs that can be used in a business or corporate setting. One of the most common uses is a remote access VPN which securely connects a device outside the corporate office to the onsite corporate network or intranet. Shown in Figure 3, a remote access VPN provides a secure way to connect users and devices remotely to a corporate network, enabling an employee to work away from the office, or virtually. A remote access VPN can also use additional technology to authenticate the user or device. This authentication is available to check whether a device meets certain requirements before it is allowed to connect remotely.

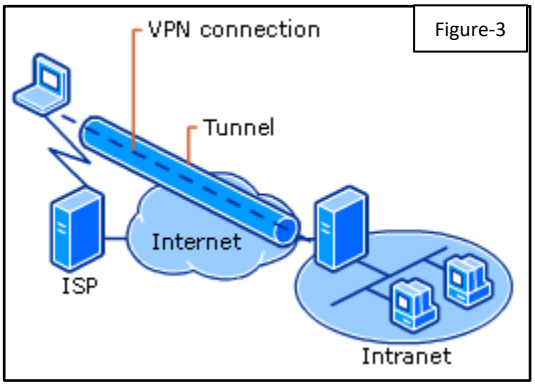

Figure-3

SITE-TO-SITE

A site-to-site VPN can connect the corporate office to branch offices over the Internet. Site-to-site VPNs are used when distance makes it impractical to have direct network connections between offices. Leasing private lines to connect offices can be very costly. Instead, most companies opt to geographically connect separated private Local Area Networks over the public Internet. To protect their data, they set up VPNs between offices, encrypting the data as it's transmitted.

FREE VPN VS. PAID VPN SERVICES

FREE VPN SERVICES

There are countless free VPN services available and a list of TechRadar's, "The best free VPN 2019" can be found at https://www.techradar.com/vpn/best-free-vpn. Free VPN services can help add privacy from potential hackers, bypass Internet restrictions, and hide your IP address, but with potential disadvantages. Some VPN services monitor and log data from their users. This data can then be used for advertising or sold to third parties. In a recent study covering 283 free VPN apps on Android, it was found that nearly 40% injected malware onto user devices for "malvertising". It was also found that 18% of free VPNs didn't encrypt traffic at all. In some cases, VPN services offer a limited free-trial, or test-run of their service before requiring an upgrade to the paid version. Some offer limitations on the amount of data or traffic that can be used per day or for a designated period of time. "Read the fine print" when signing up for a free VPN service; it may be safer to use a paid service.

PAID VPN SERVICES

According to CNET's January 17, 2019, article "The Best VPN Services of 2019", a few of the top ranked paid VPN services for 2019 such as NordVPN, IPVANISH, TunnelBear, CyberGhost, and TorGuard, generally cost less than $5.00 a month. Comparing paid VPN services is vital and there are several articles and comparison reviews publicly available, see resources. Key things to look for between service providers include, but are not limited to: number of simultaneous devices connected, number of IP addresses available, number of accessible servers, geographical diversity in servers, the services nationality origin (trusting a foreign VPN company with private data may not be the best idea), logging policy, connection capabilities and restrictions, operating systems supported (iOS, Android, macOS, Windows, etc.), price, and payment methods. Additionally, with paid VPNs, there can be added functionality like the ability to block ads, or double (multi-hop) VPN which uses multiple servers to tunnel Internet traffic.

DISADVANTAGES

It is common for a VPN to hinder Internet connectivity speed, limit download and upload speeds, and reduce loading speed for certain websites. Using an IP address from another location or country can present challenges as well. Websites can block incoming traffic from specific locations or countries and sometimes do so for legal reasons. For example, online gambling sites will deny access to users who are using a VPN because they cannot confirm the user's true location. There is also a possibility of blacklisting or using an IP address supplied by a VPN service that has been flagged. This flag is essentially a denial of access to certain websites based on historical activity from the IP address being used. IP addresses are assigned randomly by the VPN providers, thus can be shared. An IP address could have been used by someone on a free trial period, or to conduct nefarious activity. Using a VPN should not be the only security measure used, but they can add a much-needed level of security for a user.

Resources

1. https://www.sans.org/reading-room/whitepapers/vpns/extending-business-network-virtual-private-network-vpn-36985
2. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html
3. https://www.allthingssecured.com/vpn/faq/free-vpn-vs-paid-vpn/
4. https://www.lifewire.com/reasons-to-use-a-vpn-for-private-web-browsing-2483583
5. https://www.zdnet.com/article/vpn-services-the-ultimate-guide-to-protecting-your-data-on-the-internet/
6. https://www.cnet.com/best-vpn-services-directory/
7. https://www.makeuseof.com/tag/major-vpn-protocols-explained/
8. https://www.pcmag.com/article2/0,2817,2403388,00.asp
9. https://www.techradar.com/vpn/best-free-vpn.