Braxten Loppnow

CSC407-VPNProject

General Information

- Author: Braxten Loppnow
- Date: 5/5/2021
- Description: With more homes and businesses implementing free and public Wi-Fi, installing antivirus software, and creating stronger passwords may no longer be the minimum requirements for basic cybersecurity. There are ever expanding groups of hackers, third parties, and ISPs constantly monitoring networks and watching what you do on the internet. This project is to show how VPNs can help keep you or your business protected.

Three Main Ideas

1. When using unsecured or unprotected Wi-Fi, it can be easy for companies or even suspicious individuals to monitor and take your personal data, as well as spy on your browsing habits and turn them against you without your knowledge.

2. With the rise of cybercrime and device/internet monitoring by various sources, VPNs are slowly becoming the new standard for safe and secure browsing.

3. There are many ways to implement a VPN onto a network whether it be home or business. While not an actual service, OpenVPN seems to be the backbone for many VPN services, like AirVPN, and provides much of the protection and privacy while using a VPN service.

What is a VPN? / Why You Should Care

VPN stands for Virtual Private Network. It is used as a sort of tunneled connection between your device and the destination that you chose. Once your device is connected to a VPN, it acts as though as if it's on the same local connection as the VPN. So, if your VPN is in the UK, it makes it look like your device is in the UK. As far as any website is concerned, geographically, you're not in your local coffee house. Also, when using a VPN, all of your device's data, transmitted and received, is encrypted. This means that nobody can monitor or hijack your online activity or information. During the course of the CSC-407, We have talked about Dynamic/Remote-Access VPNs. We even had conducted an in-class virtual lab using Juniper Pulse Secure and SRX. With that, we were trying to give a remote machine a secure way, through the SRX, into the network using a dynamic/remote-access VPNS.

For this project, I decided to discuss about OpenVPN and its many features.

What is OpenVPN?

OpenVPN is an open-source protocol that allows developers access to copy or modify its infrastructure and can use either TCP or UDP to transmit data. This means that OpenVPN is a VPN service on it own, it can be used as a port utilized by other services. It uses the TLS/SSL protocol and can travel through firewalls and network address translators. OpenVPN uses OpenSSL, which is an open-source software

library used by a variety of applications that help keep connections secure and prevents others from eavesdropping in and monitoring the data. One of the best benefits of OpenVPN is that it is free to use. One of the more notable VPN services to utilize the OpenVPN protocol is AirVPN.

What is AirVPN?

AirVPN is a virtual private network service provider based in Europe. It works on Windows, macOS, and Linux, as well as iOS and Android. AirVPN owns and maintains over 100 servers, hundreds server locations, and hundreds of IP addresses spread across the world. It is considered to be one of the better VPN providers by many. It uses the OpenVPN protocols for its connection, namely OpenVPN UDP, and OpenVPN TCP. It also helps strengthen encryptions and keep personal and online data private. Overall, using the services provided by OpenVPN and the latest VPN tech, AirVPN provides great protection and provides an excellent way to keep your devices connected, yet secure.

Process

Before choosing AirVPN, it was aa tough choice on what to go with for this project for testing a VPNs ability and see what it looks like when hackers or companies are trying to take your data. The reason I chose AirVPN was because it had a lot of the OpenVPN structure that I had discussed earlier, and a three-day plan was quite cheap. In order to monitor the web data, I went with Wireshark. Wireshark is one of the most popular network packet analyzing tool out there. It captures data and can turn it into a readable format. It was what I need to show the differences between using VPN and not using VPN. I also created some ingoing and outgoing firewall rules to open up a few ports, like 1194, to allow OpenVPN to, hopefully, show up on Wireshark.

Also, I had to find a website running on http for the purposes of the test as it would be easier to read the data and show what unsecured network traffic looked like. I found one with testingmcaffesites.com. For gathering data on Wireshark to show off what VPNs can do, I switched between various VPN servers from different countries. I collected a set packets with no VPN and was able to gather a plethora of information about the site being browed by my PC. I then collected a set of packets using AirVPN to access the same site. With VPN on, I was able to see how the TCP/UDP data was different along with how the data is encrypted when being tunneled through the VPN.

Future Direction

Since this project was based on the uses and functions of VPNS as a whole, with some network monitoring, there a many more "rabbit holes" one could go down. There many different services out there than what was discussed in this project. The future of commercial VPNs and VPN technology seems very bright. And with Donald Trump passing an anti-privacy bill back in 2017, one could study to see if the uses of VPN are expanding with the general public's knowledge of VPNs and VPN services since then.