Atanque, Juhn Emmanuel F.

BSIT 4-4

What is VPN?

VPN stands for “Virtual Private Network”. When we browse the internet, our devices use an ip address that identifies your device on the internet. Let’s say that the driver is the user, his car is the device that has its ip address as its plate number and the road he’ll be traveling on his Internet Service Provider (ISP) such as PLDT or Converge. Browsing the internet can be like travelling on the road to reach your destination, but consider that just like the plate number in a car, ip address is visible, hence if the road had cameras on the side, your destination which is the sites your trying to reach can be seen and they know exactly what car arrived there. The ISP roads might show your connection’s destination which are the sites you browse and the data you send and receive. VPN works by creating a tunnel for your connection to travel through so that third parties such as people who are interested in your late night browsing or the government won’t be able to see your Ip address. Thus making you truly anonymous in the web.

What are the types of VPN? Discuss Each

There are two main types of VPN which is the Remote access VPN and the Site-to-Site VPN. The Remote access VPN functions exactly like how the tunnel that magically appeared in the previous example – it hides your car’s plate number which is the ip address of your device from being seen in the open road which is you Internet Service Provider by providing a tunnel to travel in. This is the most commonly used type of VPN for people to protect the data they send in the internet and hide their internet activities such as their 2 PM search history.

The Site-to-Site VPN is similar to the remote access VPN but what makes it different is the destinations which are both Local Area Network(LAN). Using the car-on-road model I’ve been forcing, the road will only have two destinations. Let’s say the driver wants to deliver the goods to a regular customer which means he’ll have to drive to the customer’s location. But again, the road he’ll be traveling on is visible and his plate is visible so his destination can be seen and his goods can be found out. The Site-to-Site VPN will provide a tunnel between only two users so that they can keep their transactions hidden. This type of VPN is commonly used by companies who may have collaborations with other companies to keep their data is confidential.

What are the features of a VPN?

First feature is Strong Encryption which is its ability to hide your Ip address and data such as login credentials or credit card info. The best encryption that you should look for in a VPN is having a AES 128 encryption because it's the kind of encryption that companies like Microsoft and Apple use. It's said that not even a super computer can crack this encryption.

Second Feature is the Secure VPN Protocol. This is a feature that a VPN provider should offer which is letting the client connect to a server using OpenVPN. OpenVPN protocol is responsible for handling client-server communications and is the most secure protocol out there.

Third feature is the DNS Leak Protection. DNS is translating requests of a user into Ip address for him to arrive to a site. This can actually be leaked directly to your Internet Service Provider instead of running it to your VPN though this rarely is a case. Still it is recommended to choose a VPN that provides DNS Leak Protection.

Last key feature is a VPN kill switch. This is an emergency feature that if your connection to a VPN server suddenly drops, it will cut of all your devices internet connection. This is done to suddenly leaking your personal info and ip address.

What are the benefits of using VPN?

VPN keeps your data and internet activities hidden from others. It does it by hiding your Ip address and all the data you receive and send in the internet. Some people might think that isn't incognito mode enough to be anonymous in the internet. Not really. Have you ever tried going incognito and going to youtube. You won't have your account cause you're supposedly hidden but notice that the recommendations are content from the Philippines. This means that your device's location is still visible and you're search history isn't truly safe. VPN can hide your internet traffic, credit card or login credentials, and other data that you may be using on the internet. This will hide your device on the web so you become truly anonymous so that people such as you ISP, hackers, neighbor, FBI, or the government won't see your web history.