**VPN**

DeepaNatarajan

Department of Information Technology, Bellevue University

CIS 515: IT Infrastructure

Professor James Krohn

May 22, 2021.

A VPN is a cryptographically secured transmission path through an untrusted network (Panko & Panko, 2018). Because the transmission is encrypted, it is as if the data is travelling over its own private network. A common crypto graphic system for VPN is SSL/TLS.SSL is Secured Socket Layer and TLS is Transport Layer System. It hides the online activity by disguising the ip address and making the location invisible. It is also secure against any external attacks. The encryption takes place in real time.

**Process:**

If a person uses internet to surf, then the VPN server becomes the source of the data. VPS encrypts all the surfing data. This encryption can be decoded by the key, which only the host and the VPN has. As a result, the internet service provider or the third parties cannot see the website visited or the data that was transmitted. Different VPNs use different encryption processes, but function in three steps:

* Once the party uses the internet for browsing, the VPN creates a secure tunnel between the device and the internet. So, the ISP or the third party cannot detect the tunnel.
* The device will be on the local network with the VPN, which will assign an IP address for the device instead of the actual one.
* And the internet can be used with the help of the protection provided by VPN

**Types**:

Internet Protocol Security (IPSec) is designed to connect and protect the endpoints in three ways.

* Host-to-host VPNs connect two host often in the same site. The security is handled by two host with no additional help.
* Site-to-site VPNs connects two corporate sites. This carries greater traffic between the two sites compared to the host-to-host VPNs.
* Host-to-Site VPNs, protect the traffic between a site and a remote corporate client. This is also called remote access VPN.

**Protocols:**

There are five common protocols in VPN. (Harkness, 2019).

* PPTP:

Point to point tunneling protocol. It is the oldest protocol used between the windows 95 and the dial up connection. Because it lacks all the additional features that a modern protocol has, this system can provide a faster connection. This protocol is used in some applications, which does not need heavy encryption.

* L2TP/IPsec:

Layer 2 Tunnel Protocol, is a replacement of PPTP, it is paired with security protocol IPsec. It is extremely secure once implemented.

* OpenVPN:

This is an open-source protocol where the developers can access the code. It has grown popularity because of the usage of the algorithms and the encryption, authentication methods.

* SSTP

Secured socket tunneling protocol. It is popular because of its integration with Microsoft vista. It is not an open-source software, so developers have no access to the source code. It utilizes 2048-bit SSL/TLS certificates for authentication and 256-bit SSL keys for encryption

* IKEv2

Internet Key Exchange Version 2. This protocol provides secure key exchange sessions. This protocol is very good at reestablishing the connection once it is lost and good at switching different type of networks, for example between Wi-Fi to cellular.

**Benefits:**

**VPN** encrypts the data so the hackers or the criminals cannot decrypt the data.

* + Secure encryption: To read the data, you need an encryption key. With the help of a VPN, your online activities are hidden even on public networks.
  + Hides the geolocation and browsing data: VPN assigns a different IP address for the devices, so no one can identify the users actual IP address. The VPN never store the logs, so the browsing data is never recorded.

**Conclusion:**

With the increase in internet usage, multiple devices and working from home options, huge amount of data is being transmitted over the internet. The bests way to protect is by encrypting the data, which is what VPN does. The benefits are several, many providers have come up with VPN’s not only for the corporate use but also for the home users on any devices. Along with the anti -virus software’s, VPN can help people from data theft.

**Reference**

Harkness.A., (2019, May 15). *5 Common VPN protocols explained.* <https://www.netmotionsoftware.com/blog/connectivity/vpn-protocols>

Kaspersky. (n.d.). *What is VPN? How It Works, Types of VPN.*Retrived May 15, 2021, from <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

Panko, R., & Panko, L.J., (2018). Business Data Networks and Security. (11th ed.). Pearson Publications.