Virtual Private Network

Ann Funk

ICTN 6870 | ADVANCED NETWORK SECURITY

Table of Contents

Abstract

Virtual Private Networks are increasing in popularity every day. This is due in large part to computer users wanting to keep their browsing habits private. The popularity is also due to the fact that VPNs are a relatively low cost, flexible and easy to use. While they may be easy, there is still a lot to learn about VPN's.

In this paper we dive a little deeper into what a VPN actual is and how they can be used in everyday situations. We will talk about compulsory virtual private network tunneling and voluntary virtual network tunneling giving examples of each and how they are used in VPNs. Virtual Private Network Tunneling Protocols will also discussed. While we will not cover every protocol, we will talk about the most popular ones, PPTP, L2TP, IPSec, and SSL/TLs.

Introduction

In recent news, internet privacy has become a very hot topic. This is due in part to the governments recent repeal of internet privacy rules. These new changes will allow companies like Verizon, Comcast and AT&T to have an intimate look into American internet users online habits. They will be able to track, collect, share and sell this intimate data to the highest bidder. All done without the consent of the consumer. These changes have left some looking for ways to help protect their privacy. Many are turning to virtual private networks, or VPNs.

Virtual Private Networks are not new. In fact, they have been in use since 1996, when a Microsoft employee developed the peer-to-peer tunneling protocol. "This technology was originally developed by big companies and organizations and it wasn't meant for the end users. Companies needed secure and private network to join their offices situated on different physical locations because only a private network with security can hold their secrets and personal information they don't want to publicize." (C, 2015) Like most technology, virtual private network usage has evolved from just being used by business to that of an everyday user. It is estimated that there are over half a billion people worldwide with concurrent VPN connections. (Bridgwater, 2013)

With so many people using VPN's it would be easy to assume that most know what it is, how it works, and how to use them. Unfortunately, this isn't the case. In this paper we will explore the definition of a VPN and discuss the different types, and protocols used in virtual private networks.

What is a VPN?

A virtual private network has many different definitions. In fact, when you do a search for virtual private network you get a return of about 126 million results. This can be a little daunting to some but once you start looking at all the results, a clear definition can be found. "A VPN or Virtual Private Network is a method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet" (What is a VPN, B, (n.d)). This technology links two or more sites together using the internet. Once the sites are connected, data can then be transmitted from each site using a VPN tunnel. This tunnel is an encrypted line and any data transmitted through it is securely transmitted. This simply means that only you and your VPN server can see the data.

So now that we know what a Virtual Private network is the next logical question would be how are they used. Since VPNs are an easy to use tool, it can be used to do an assortment of things.

Hoffman, (2016) describes some of the things a VPN can do:

- **Access a Business Network While Travelling:** One of the most common uses for a VPN is the ones that are uses commercially. VPNs are frequently used by business travelers to access their business' network, including its local network resources, while on the road. The local resources don't have to be exposed directly to the Internet which increases security.
- **Access Your Home Network While Travelling**: You can also set up your own VPN to access your own network while travelling. This will allow you to access a

Windows Remote Desktop over the Internet, use local file shares, and play games over the Internet as if you were on the same LAN (local area network).

- **Hide Your Browsing Activity From Your Local Network and ISP**: If you're using a public Wi-Fi connection, your browsing activity on non-HTTPS websites is visible to everyone nearby, if they know how to look. If you want to hide your browsing activity for a bit more privacy, you can connect to a VPN. The local network will only see a single, secure VPN connection. All the other traffic will travel over the VPN connection. While this can be used to bypass connection-monitoring by your Internet service provider, bear in mind that VPN providers may opt to log the traffic on their ends.
- **Access Geo-Blocked Websites**: Whether you're an American trying to access your Netflix account while travelling out of the country or you wish you could use American media sites like Netflix, Pandora, and Hulu, you'll be able to access these region-restricted services if you connect to a VPN located in the USA.
- **Bypass Internet Censorship**: Many Chinese people use VPNs to get around the Great Firewall of China and gain access to the entire Internet. (However, the Great Firewall has apparently started interfering with VPNs recently.)
- **Downloading Files**: Yes, let's be honest – many people use VPN connections to download files via BitTorrent. This can actually be useful even if you're downloading completely legal torrents – if your ISP is throttling BitTorrent and making it extremely slow, you can use BitTorrent on a VPN to get faster speeds.

The same is true for other types of traffic your ISP might interfere with (unless they interfere with VPN traffic itself.)

Types of VPN

Now that we know what a VPN is and some of its uses, let's talk more about the distinct types of VPN. There are two distinct types of VPN. One is called Remote Access VPN and the other is known as Site-to-Site VPN. Each of these can be used over the internet or intranet.

Remote access VPN's can be used by both business and home users. With this type of VPN, a user can connect to a private network and access its services and resources remotely. This connection is connected between the user and private network via the internet. This connection is done via the internet instead of a dedicated line due to cost. If a dedicated line was used, this could be extremely expensive and not very customizable. Besides, "connection over the wild internet does not make a difference to the end user because it appears as if the data is being sent over a dedicated private link" (Fornero, 2016)

A Site-to-Site VPN, sometimes known as Router-to-Router VPN, is a connection that is mainly used by corporations. That's because a site-to-site VPN extends a company's network, making resources from one company site available to the company's other sites in different geographical locations. "Every host in each private network needs to communicate with every host in the other private network." (Guthridge, 2013) A virtual bridge between networks that are owned by the same

company but in different geographical locations is created and this bridge maintains secure and private communication between the sites.

Virtual Private Network Tunneling Types

VPN Tunneling is a very important aspect to virtual private networks. It is responsible for performing data encapsulation. Tunneling enables the encapsulation of a packet from one type of protocol within the datagram of a different protocol. "Technically, no tunnel exists and the process doesn't resemble a tunnel, but the term "tunneling" somewhat describes the end result of traffic being able to pass through a non-secure environment without concerns about eavesdropping, data hijacking, or data manipulation." (Smith, 2011) There are two distinct types of tunneling that are supported by VPNs. The first type is voluntary tunneling. With this type of tunneling, the client is the first one to make a connection to the network provider. Once this connection is established, the VPN application creates a tunnel to the VPN server.

The second type of tunneling that is supported by VPNs is called compulsory tunneling. In this type of tunneling, the network provider is the one that manages the connection setup to the VPN. A client will make a connection to the network provider and once the connection is made the network provider will then negotiate a VPN connection between the client and VPN server. This allows for a one step procedure for the client since all they have to do is connect to the network provider, unlike the two-step process for voluntary tunneling. Clients using this form of tunneling are automatically authenticated and associated with specific VPN servers. The ISP is thus in charge of the management of the tunnels connecting clients to the ISP.

Virtual Private Network Tunneling Protocols

There are several network protocols that have been implemented at different layers to use with VPN tunnels. While we will not address all of the protocols used, we will address four of the most popular that are used.

Data Link Layer – PPTP and L2TP

Point-to-Point Tunneling Protocol or PPTP is s protocol developed by Microsoft over 20 years ago to help route traffic over unsecured networks. It is still in use today and is one of the most popular protocols. This voluntary tunneling protocol encrypts the data being sent and then puts that data into packets. Since the data has been encapsulated, encrypted and authentication is required to unencrypt it, the data is safe to transmit over any type of network. PPTP only needs three things to establish a connection to the server: user name, password, and server address. This protocol supports session key encryption up to 128-bit, operating systems including Windows, Linux, IOS, Android, and Mac. The wide range of operating systems it supports give it a huge advantage over other protocols. Also it is one of the fastest protocols due to is low level of encryption

PPTP has some disadvantages. The fact that this protocol is a few decades old might make it a lot less secure than some of the other protocols. Also there have been recent new articles stating this protocol has been hacked by different government agencies. This protocol would not be a good option for anyone who wants to maintain anonymity online and is mostly used to access geo-restricted content.

Layer 2 Tunneling Protocol or L2TP is a protocol that was developed by IETF and recognized by several tech companies such as Microsoft, 3CoM and Cisco. This protocol is a combination of PPTP and L2F protocols. Using the best of the two protocols, it provides the fast connectivity of PPTP and is cheap, flexible and accessible attributes of L2F. One of the main features of the L2PT tunnel is that the tunnels that were established with PPP are not terminated and in fact are extended to the gateway of the host network. L2TP also has several benefits.

Gupta (2003) listed the key benefits of the L2TP protocol as:

- L2TP supports multiple protocols and networking technologies, such as IP, ATM, FR, and PPP> As a result, it can support separate technologies with a common access infrastructure.
- L2TP allows various technologies to fully leverage the intermediate access infrastructure of the Internet and other public networks, such as PSTNs.
- L2TP does not require implementations of any extra software, such as additional drivers or operating system support. Consequently, neither the remote user nor the private intranet needs to implement special software.
- L2TP allows remote users with unregistered (or private) IP address to access a remote network across a public network
- L2TP authentication and authorization is performed by the host network gateways. Therefore, ISPs do not need to maintain a user authentication database or access rights for remote users. In addition, private intranets can also define their own access and security policies. This makes the process of tunnel establishment much faster than earlier tunneling protocols.

Network Link Layer – IPSEC

IPSec or Internet Protocol Security is a suite of protocols developed by the Engineering Task Force (IETF). This suite of protocols was developed to provide security at the network layer of the OSI model. Since IPSec was designed to work on the third level of the OSI model it was imperative that it was compatible with current IP networks but also with those to come. There are two modes of operation for IPSec. Transport mode is responsible for encrypting the message in a data packet. Once this is done, Tunneling mode will take over. In tunneling mode, the whole data packet is encrypted again.

One of the most important concepts of IPSec is the IPSec Security Associations. "A security association is a logical unidirectional connection between the communicating parties using IPSEC, and it defines: the authentication protocols, the cryptographic algorithms, the encryption keys, the key lifetime and key change time, the source address, the cryptographic synchronization information." (Popescu, 2010) The Security Association is comprised of three fields: SPI (Security Parameter Index), destination IP address, and the security protocol. Since security associations are considered unidirectional in nature, two of the SAs must be defined between the communicating ends. Each one should be defined in each direction.

Transport Layer – SSL/TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) is a VPN protocol that is used on the transport layer of the OSI model. When using this protocol a connection will be established where the browser acts as the client and the user is only allowed to access certain applications. This method is most often used by

websites that support online shopping. When creating an SSL session the protocol will go through two phases. The first phase is called the Handshake phase. During this phase a cryptographic algorithm negotiation is provided. This will authenticate the ends and establish the MACs and encryption keys. The second phase of an SSL session is the data transfer. In this phase, the data is protected by the SSL connection established earlier.

Conclusion

Virtual Private Networks are increasing in popularity every day. This is due in large part to computer users wanting to keep their browsing habits private. The popularity is also due to the fact that VPNs are a relatively low cost, flexible and easy to use. While they may be easy, there is still a lot to learn about VPN's.

In this paper we dove a little deeper into what a VPN actual is and how they can be used in everyday situations. We spoke on compulsory virtual private network tunneling and voluntary virtual network tunneling giving examples of each and how they are used in VPNs. Virtual Private Network Tunneling Protocols were also discussed. While we did not cover every protocol we did talk about the most popular ones, PPTP, L2TP, IPSec, and SSL/TLs.

Works Cited

Bridgewater, A. (2013, November 4). VPNs: The past, present and future. Retrieved April 1, 2017, from http://www.computerweekly.com/feature/VPNs-The-past-present-and-future

C. (2015, June 08). The History of VPN | The Beginner's Guide to VPN. Retrieved April 1, 2017, from https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-history/

*Fornero, K. (2016, May 10). Extending your Business Network through a Virtual Private Network (VPN). Retrieved April 4, 2017, from https://www.sans.org/reading-room/whitepapers/bestprac/extending-business-network-virtual-private-network-vpn-36985

Gilbert, B. (n.d.). What Is A VPN? Retrieved April 03, 2016, from https://www.whatismyip.com/what-is-a-vpn/

Gupta, M., ebrary, I., NIIT (Corporation), & Books24x7, I. (2002;2003;). Building a virtual private network (Paperback ed.). Cincinnati, Ohio: Premier Press.

*Gutridge, C. SANS Institute. (2003, March 01). IPSec Tunnel Creation. Retrieved April 1, 2017. from https://www.sans.org/reading-room/whitepapers/vpns/ipsec-tunnel-creation-1107

*Khiat, A., Bahnasse, A., Bakkoury, J., & El Khaili, M. (2017). Study, evaluation and measurement of IEEE 802.16e secured by dynamic and multipoint VPN IPsec. International Journal of Computer Science and Information Security, 15(1), 276-281. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1879104762?accountid=10639

Hoffman, C. (2016, December 02). What Is a VPN, and Why Would I Need One? Retrieved April 8, 2017, from https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

*Popescu, G. (2010). A Comparative Analysis of the Secure Virtual Private Network

Tunneling Protocols. Journal of Mobile, Embedded and Distributed Systems, 2(2), 91-100. Retrieved from http://jmeds.eu/index.php/jmeds/article/view/A-Comparative-Analysis-of-the-Secure-Virtual-Private-Network-Tunneling-Protocols

Smith, J. (2011). Tunneling Protocols. Retrieved April 8, 2017, from http://etutorials.org/Networking/Cisco Certified Security Professional Certification/Part III Virtual Private Networks VPNs/Chapter 9 Cisco IOS IPSec Introduction/Tunneling Protocols/