# Global Information Assurance Certification Paper

# Extending your Business Network through a Virtual Private Network (VPN)

*GIAC (GSEC) Gold Certification*

Author: Kaleb Fornero, f_kaleb_40@hotmail.com
Advisor: Adam Kliarsky
Accepted: May 10th, 2016

Abstract

Let's journey back in time. A voyage to a magical time in the world. A time when Warhead candies, Tamagotchi, and America Online ruled the majority of our free time. Yes… it's the 1990's. Not only did the nineties see a rapid expansion of the internet, but an increased concern about protecting individual and company information while it is sent racing through cyberspace. This paper looks not only at the various architectures/types of the Virtual Private Network (VPN) but also describes the benefits and risks of extending a business network via this technology.

# 1. Introduction

It's safe to assume that most individuals reading this paper have leveraged a Virtual Private Network (VPN) at some point in their life, many on a daily basis. To ensure everyone is on a level playing field we first need to answer a fundament question: What is a VPN?

If you Google® VPN, you will get around 29 million results. When looking through these results, one definition begins to take shape: "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?" - Gilbert, B. (n.d)). Let's dig into the main points of this statement.

## 1.1. It's a Method Used to add Security and Privacy

For a company to use a VPN, it takes end-user training, infrastructure, and employees to maintain it. So why use it? Why spend precious resources on this technology? It comes down to the privacy, safety, security, and integrity of their information. In the early days of information security, it was thought that if a company's sensitive information never left its air gaped and private network, it would be safe. If the countless news stories relating to the breaches, data exposures and compromises of so many companies has taught us anything, it is that we all know the Internet, and even sometimes a company's internal networks can be a dangerous place. A place where the motivations of "bad actors" and the threat vectors they leverage can change at a moment's notice.

VPN connections can utilize an arsenal of different encryption protocols to combat an ever-changing and often unknown threat. While the number continues to increase over time, there are two main types:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunnel Protocol with Internet Protocol Security (L2TP/IPsec)

### 1.1.1. Point-to-Point Tunneling Protocol (PPTP)

Introduced in mid-July 1999, "Point-to-Point Tunneling Protocol was developed by a consortium founded by Microsoft for creating VPN over dial-up networks, and as such has long been the standard protocol for internal business VPN" (Crawford, 2014). Since Microsoft first introduced PPTP as a regular feature of Windows 95, it has been one of the standards for implementing VPN "like" products for business and home users

alike. Since it is merely a protocol, PPTP can be set up and run as a service without the need to install new software. Since the protocol itself does not have any built-in security, the confidentiality of the VPN tunnel relies on the encryption of its traffic from another source. MS-CHAP v2 is the most popular of these encryption types and allows even modern versions of Microsoft Operating Systems to implement multiple levels of authentication natively in the Windows PPTP stack.

A true testament to security, when it first came out, researchers across the world have published countless articles outlining security flaws with PPTP and the MS-CHAP v2 authentication. Some of these findings were so severe that they would allow an adversary to crack the encryption "within 2 days, and although Microsoft has patched the flaw it has itself issued a recommendation that VPN users should use L2TP/IPsec or SSTP instead" (Crawford, 2014). Despite this recommendation and the numerous publications of flaws the PPTP protocol and MS-CHAP v2 authentication is still one of the most commonly used VPN tunnel and authentications methods used today.

### 1.1.2. Layer 2 Tunnel Protocol with Internet Protocol Security (L2TP/IPsec)

Just like PPTP, L2TP does not provide any encryption to the data it is transporting, it is simply a tunneling protocol commonly used to support Virtual Private Network connections. Due to this, the protocol is almost always implemented along with IPsec. "L2TP/IPsec is built-in to all modern operating systems and VPN-capable devices, and is just as easy and quick to set up as PPTP" (Crawford, 2014).

At a high level, L2TP/IPsec works by wrapping the original data packet inside a new packet. This new packet can have new routing information and source/destination IP addresses. This type of wrapping protects the company's potentially sensitive information by traversing the public or private network from anyone listening to their traffic. At this time "IPsec encryption has no major known vulnerabilities, and if properly implemented may still be secure" (Crawford, 2014).

## 1.2. To private and public networks…

There are two main categories of VPN connections, Internet-based and Intranet-based connections. We are all familiar with the Internet-based communications these are the ones some use on a daily basis to connect back to the home office. Internet-based connections leverage low-cost, if not free, public internet connections and allow employees to connect and complete their work from anywhere in the world.

The second category of VPN connection types is Intranet-based. These types of connections are very similar to their internet-based counterparts we discussed earlier. The main difference being, the traffic traverses a company's internal network. Some companies have adopted this strategy for all of their internal network activity or reserve it for their most sensitive and private information. Why is this done? One not so simple word… security. These companies treat their internal network the same as a public internet connection. They assume there are "bad actors" actively listening and trying to intercept their in-house traffic. While there are certainly advantages to a company's overall security posture from this approach, there can be a significant financial commitment for the company through the design and maintenance of the system.

## 2. VPN Architecture Types:

Like most things in life, there are multiple ways to leverage a single technology. A Virtual Private Network (VPN) is no different. As we discussed earlier, this technology can be broken into two broad categories Internet and intranet-based connections. Beyond this, each grouping can then be broken down further into the following sub-categories:

- Internet-based Connections
  - Remote Access VPN Connections over the Internet
  - Site-to-Site VPN Connections over the Internet
- Intranet-based Connections
  - Remote Access VPN Connections over an Intranet
- Site-to-Site VPN Connections over an Intranet

### 2.1. Remote Access VPN Connections over the Internet

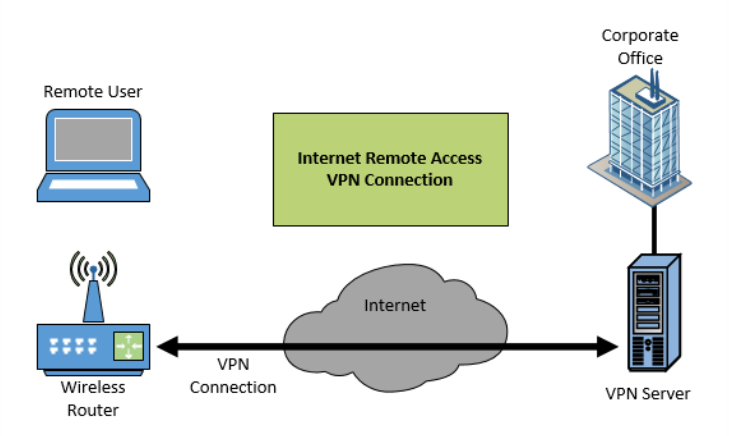


*Figure 3.1 – Internet Remote Access VPN Connection*

Let's start our journey with the VPN architecture we are most familiar with, the teleworker or "road warrior". These individuals will leverage a type of VPN connection known as a Remote Access VPN Connection over the Internet. When working from an offsite location, there is a need to send and receive information to the home office. There is the opportunity for a dedicated line or connection back to the "mother ship", but these are extremely expensive and not very customizable. What is far more common today is to leverage the inexpensive or even free, public internet connections to connect back to the home office. Best of all "connection over the wild internet does not make any difference to the end user because it appears as if the data is being sent over a dedicated private link" ("How VPN Works", 2003).

As you can see in figure 3.1, the remote user connects directly to their home network and Internet Service Provider (ISP) to access the internet. The user then established a VPN connection through the Internet to the corporate office's VPN server. This type of connection is by far the cheapest and easiest for a company to set up and maintain and allows the remote user to access a file share, server, etc. from wherever they are located just like they were physically in the office.

## 2.2. Site to Site VPN Connections over the Internet

Having remote workers is a great perk for any company, but what about if your workforce travels to offices scattered across the country or globe? Is there a VPN solution that could accommodate this type of activity? There is! It is called a Site to Site VPN Connection over the Internet. Think of large a financial institution. The corporate office may be located in California, but have branch banks all across the country. The computers at the branch office will need to report data back to the corporate office in real time, just like it was in the same building. To accommodate this type of activity a company can set up a VPN connection, through the Internet, between two VPN Routers (as seen in figure 3.2). This connection would be constant and act as an extension of the corporate office's computer network.

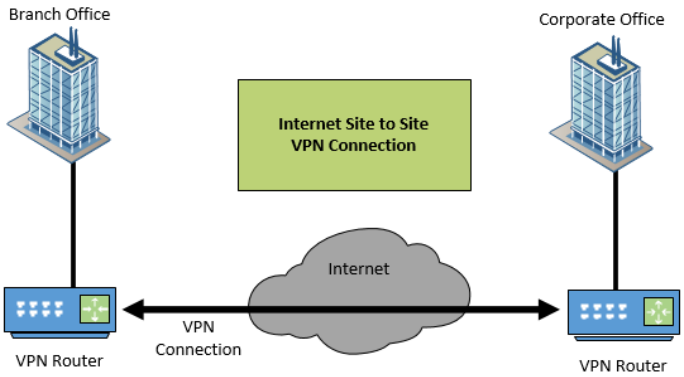


*Figure 3.2 – Internet Site to Site VPN Connection*

## 2.3. Remote Access VPN Connections over the Intranet

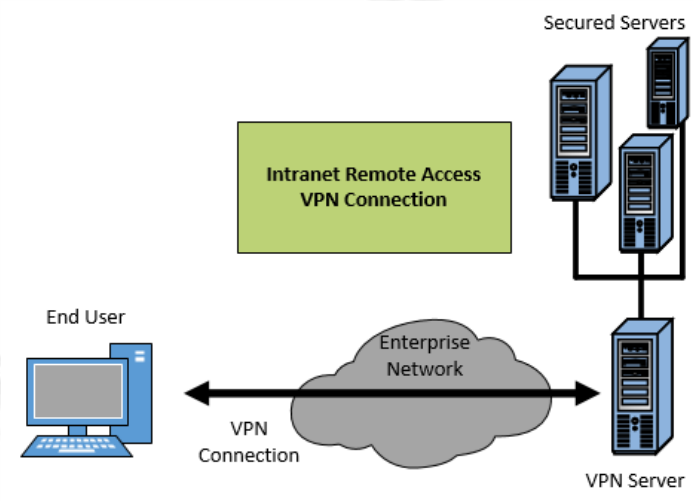


*Figure 3.3 – Intranet Remote Access VPN Connection*

As we read in the previous examples, there are two main ways to leverage a VPN connection over the Internet, Site to Site connections and Remote Access connections. These same two methods can also apply to a company's internal network or intranet.

Just like its counterpart, the Remote Access VPN Connection over the Intranet works by creating a VPN connection through a network. The end user still connects to a VPN server, but the main difference is that the established connection tunnels through the company's internal network rather than

the internet. No Internet Service Providers (ISPs) are involved in this type of communication.

Let's explore an example to better understand why a company would implement this technology. Company X is a medium sized business with a vast potential for growth. Their claim to fame is the mixture they use to make plastic widgets. This solution makes their widgets twice as sturdy and last five years longer than their nearest competitor. Company X stores the formula for this mixture on a set of secured servers inside their trusted network. No one other than the Chief Executive Officer, Chief Information Security Officer, and Head of Manufacturing is allowed or should ever see this formula. If the formula were as to be obtained by one of their competitors or posted online, the damages to their company would be significant, and they would likely go bankrupt.

In this extreme example, we can see why a company would want to protect this information from even its internal network. While the likelihood of an individual listening to their internal network traffic may be small, the resulting business impact would be so catastrophic that the organization wants to minimize its potential as much as possible.

## 2.4. Site to Site VPN Connections over the Intranet

Similar to its counterpart, a constant VPN connection between two sets of secured environments can be created through a company's internal network. This type of setup is best when data needs to be shared or backed up consistently between the separate environments, but the sensitivity of the information demands an extra layer of security.

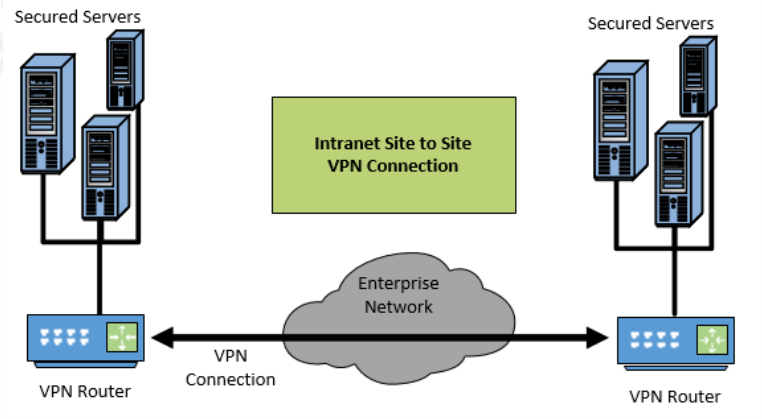


*Figure 3.4 – Intranet Site to Site VPN Connection*

For this type of connection, a company would set up two VPN routers to sustain the constant connections. The two sets of secured servers (or other types of devices) can connect these respective routers, and the VPN tunnel would traverse the company's internal network.

As you can see through these examples, the topology and architecture of VPN connections can take many different forms to fit a variety of situations. It can allow the road warrior to connect back to the home office or ensure the confidentiality of communications on an internal network. Though there are many variations, one simple fact remains consistent VPN technologies can provide a business of any size cost savings and security. These and many other benefits will be discussed in the next section of this paper.

## 3. Benefits of VPNs

For many of us, "the virtual private network (VPN) is fast becoming a necessity, and not merely a luxury, for enterprises" (Kelly, 2004). In today's world, there are limitless technologies offering riches or cost savings. With so many out there it's hard to know which ones are accurate and which ones are just a sales pitch. In the previous section, we discussed the various types of VPN architectures and how they are being used.

Let's take a step back even further and talk through why a company would even entertain the idea of implementing a VPN infrastructure. While we will not dive into the specifics around VPN vendors, we will explore the core benefits a VPN infrastructure can offer an organization: Security, Geographic Redundancy of Resources, Remote Workforce, and Cost Savings.

### 3.1. Security

These days the security of one's information is no longer a buzz word. Countless news articles and blogs from the front lines paint a picture of data breaches and data destruction that will keep even the most hardened security expert awake at night. With the current information security threat landscape full of cyber-attacks, espionages, and data leaks, every corporation out there is looking for better ways to protect their company's valuable information.

The "mantra of any good security engineer is: ‘Security is a not a product, but a process'" (Schneier, "Risks of Relying on Cryptography", 1999), VPN technologies can offer another layer of protection for their information. In the first section of this paper, we talked through what a VPN was and the main ways in which VPN traffic tunneled through an intranet or the internet (PPTP and L2TP). Both of these technologies are simply protocols used to route traffic. They do not provide encryption or security to the traffic they send.

VPN tunneling protocols can leverage two main types of encryption (depending on the protocol used) to provide this security. To state it simply, "Data encryption for PPP or PPTP connections is available only if MS-CHAP, MS-CHAP v2, or EAP-TLS is used as the authentication protocol. Data encryption for L2TP connections relies on IPSec, which does not require a specific PPP-based authentication protocol" ("How VPN Works", 2003). The encryption and subsequent decryption of information can be completed with pre-shared keys and takes place between the remote client and the VPN server. While intercepted packets are illegible to systems without these pre-shared keys, the length of the cipher itself plays a rather important role in the confidentiality of the information. This importance is due to there being methods of deciphering the encryption keys, and while these methods are not available to the average individual, the key size should be made as large as possible since it will take more time to decipher it.

## 3.2. Geographic Redundancy of Resources

It seems these days that disasters are becoming more frequent and impacting more and more portions of the country. While there are numerous types of disasters ranging from natural disasters to accidents, having "all of your eggs in one basket" is exposing the organization to an increased amount of risk mitigated through a network design change. In the second part of this paper, we discussed the various types of VPN architecture that exist today. The design of a site-to-site VPN connection over the internet, or a variation of it, can easily fit into most networks with minimal changes. This addition can then maintain a secure and constant connection to a remote data center, helping to protect the company's information resources.

Customers expect fast and reliable access to their information or response from a company. Having all of a company's vital information in a single location (no matter how unlikely the risk of disaster is) causes a single point of failure for an organization. Why is this a potential concern for a company? Considering that "while 94 percent of customers surveyed think waiting 5 to 10 minutes or less is reasonable, that doesn't mean they're happy about it; 48 percent assume your business is poorly run, while 52 percent will choose to simply shop somewhere else" (Kuklin, n.d.). If a company's information is lost or stolen, customers will have no trouble taking their business elsewhere.

## 3.3. Remote Workforce

One of the most valuable resources a company has is its employees. These also tend to be the hardest resource for a company to keep. In a competitive environment where the benefits a company can offer an individual are sometimes as important as the paycheck itself, any advantage is a good thing. Allowing an individual to work from home or a remote office location can be the difference between them staying with your organization or moving down the road to another.

Another concept behind a remote workforce is the opportunity of expanding the talent your company can acquire when the limitations of physical location are removed. For example, if a company located in a remote part of Montana has a job posting, the listing of candidates may be limited to those who live in that town or a few towns over. If this didn't make the job search hard enough, having top talent move to the remote town to work can be difficult to accomplish. A VPN solution offers a company a way around this issue. After implementing this solution, a company will not only have the ability to search for individuals outside of their home area but offer remote working to its top talent who are not willing to move to the home office location.

## 3.4. Cost Savings

Both the geographic redundancy of resources as well as a remote workforce can be accomplished through leased or direct lines allocations, but they are very costly and satisfy very different objectives. These differences are because "VPN technology exists to provide security. Leased lines exist to provide connectivity. VPNs and Leased Lines solve very different problems. That's not to say that leased lines are insecure, merely that their job is to provide connectivity, not encryption or authentication" ("Leased Line vs VPN - Which Technology Is Right For YOUR Business?", n.d.). While justifying this cost for a dedicated line to a branch office or redundant data center may be possible. When the subject of remote workers comes up, the costs to a company can go through the roof. For example, "let's say you wanted to provide 20 employees with remote access to their work PCs from home. It would be prohibitively expensive to pay for each employee to have a leased line. The only realistic option you have is to let them connect to your network over the top of (far cheaper) broadband connections" ("Leased Line vs VPN - Which Technology Is Right For YOUR Business?", n.d.).

What a VPN infrastructure offers organizations is the ability to leverage the public Internet for protected connections. This type of connection presents many of the same benefits to a dedicated internet line at a fraction of the cost and "The savings over

private networks, coupled with customer acceptance of the encryption technology to guard the connections, has made the VPN more palatable for businesses" (Kelly, 2004).

# 4. Disadvantages of VPNs

There is an old saying that if something seems too good to be true, it probably is. Just like every other technology on the market today VPN technology has a few disadvantages which need to be considered before implementing within any organization. While a full evaluation of this technology in a company's unique environment should be performed, we are going to dive into the two core items. First, the setup/maintenance of this technology will cause a company to incur initial and ongoing costs associated with the devices and people needed to sustain a stable VPN environment. Then we will explore the security concerns relating to the ability to bypass a company's physical and network controls by leveraging these types of connections.

## 4.1. Setup / Maintenance

Depending on the size of your organization, setting up a VPN network can be done with a relatively small number of appliances. With that being said, the larger the company, the more expensive the devices, the more devices that are needed, and more employees who are required to set up and maintain the environment. There is always the option for a company to outsource the development and maintenance of their VPN network and for many small businesses, this may be the best choice. There are standard costs and no need to employ expensive networking experts to maintain a VPN connection for a small remote workforce.

When it comes to medium and large businesses, the costs associated with outsourcing the product may be more expensive than hiring the professionals in house. There may also be a need to maintain the infrastructure from a security or liability standpoint. For most medium-sized businesses, all of the devices required to set up a VPN network can be obtained for under $10,000, where the real cost of a VPN infrastructure lies is in the design, development, implementation, and maintenance of the system. The review of this financial obligation is one where a company identifies and understands the risks and advantages of the solutions, how many user are going to leverage it, the security design and so forth. Once set up, the ongoing maintained of devices, troubleshooting connection issues, and updating devices can add up over time. Another consideration is the hiring and retaining of top talent who are aware of your organization's architecture to design and maintain the devices.

## 4.2. Security Concerns

With any product or technology on the market today, there are concerns regarding its safety. A VPN and its encryption are no different. There has long been speculation that intelligence agencies around the world have been working to implement backdoors in programs and "crack" encryption keys, but due to the sensitivity of these operations, it is problematic to confirm this information.

What we do know without a shadow of a doubt is that the only constant in the world is change. The protocols used today will soon be outdated and replaced with the new protocols and encryption of tomorrow. PPTP is a perfect example of this evolution. When it was created, PPTP was thought to be very secure. In today's environment, it is known to be very insecure, forcing even its co-creator, Microsoft, to recommend not using this method of data protection. Today, as well as for the foreseeable future, the best security methods still hold true. Limit the use and number of user with access to sensitive information.

### 4.2.1. Bypassing Physical Security to Gain Access to Information

We have talked several times in this paper about a VPN's ability to enable a remote workforce for a company at a reasonably low amount of cost. While this may be a great perk for employees and a way for a company to find telnet across the country, there is a risk associated with this. Without a remote workforce or VPN, an employee needs to be physically present in the office to complete their work. Being in the office often forces them to go through a company's physical controls before getting into the building and the continuous monitoring of them while they are in the office.

Photo IDs can be checked at the door, security cameras can record times stamps, and an image of what an individual is bringing into and out of the building can be taken. All of these controls help to play a part in ensuring the person a company hires and trusts to perform a role is, in fact, the individual performing the action. How does a VPN connection play into this and why does it introduce a risk to the organization?

With a VPN, a company can allow its employees to work from home, the coffee shop down the street, or anywhere else they would like. From a security standpoint, this takes out all of the physical security safeguards a company has put in place. All of the badge readers, ID checks, and security cameras are replaced with only a few security controls and passwords on the device connecting to the company network. Removing these items opens a company up to additional risk from not only lost or stolen

credentials, but laptops and tablets as well. It is far more challenging to ensure the individual connecting remotely to a company is, in fact, the person the company hired and the risks associated with this should be reviewed before any VPN connections are allowed.

### 4.2.2. Bypassing Network Protection (e.g. Firewalls) to Gain Access to a Network

Similar to the previous section covering risks associated with a VPN connection allowing someone to bypass physical security controls a company has in place, there is another concern around this same technology's ability to allow the bypassing of a company's network protections as well. The devil is in the details and the risk associated with this concern is directly tied to how the technology is implemented.

Most companies today have a DMZ, or demilitarized zone, that is their hardened front connections and devices connected to the internet. There is usually very limited trust in this environment, and it is designed to help prevent unauthorized individuals from accessing the potentially more vulnerable devices on an organization's trusted internal network. A VPN server can be placed in front of or behind the firewall(s) is this zone.

In addition to a few risks, each of these options brings with it a host of potential configuration changes to both the firewall and VPN server. When placing a VPN server in front of the perimeter firewall (figure 4.2.2.1) all traffic is decrypted before being sent through the firewall. Due to this decryption the filters and other various firewall rules are applied to a company's VPN traffic as if it was coming straight from the Internet. While this offers some advantages, placing the VPN server in front of the perimeter firewall may allow it to be an easier target and is more likely to be compromised or taken offline.

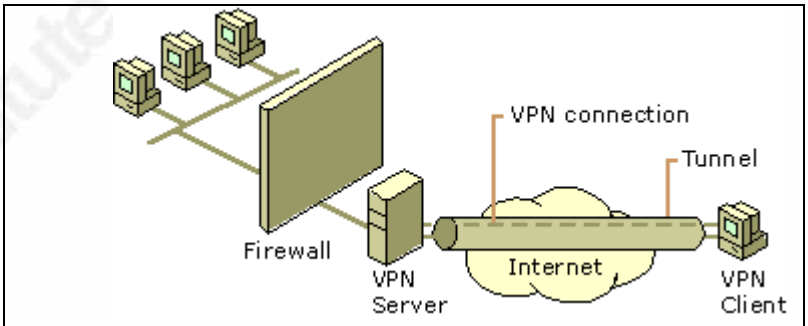


*Figure 4.2.2.1 – VPN Server Before a Perimeter Firewall*

*Source: https://technet.microsoft.com/en-us/library/cc958037.aspx*

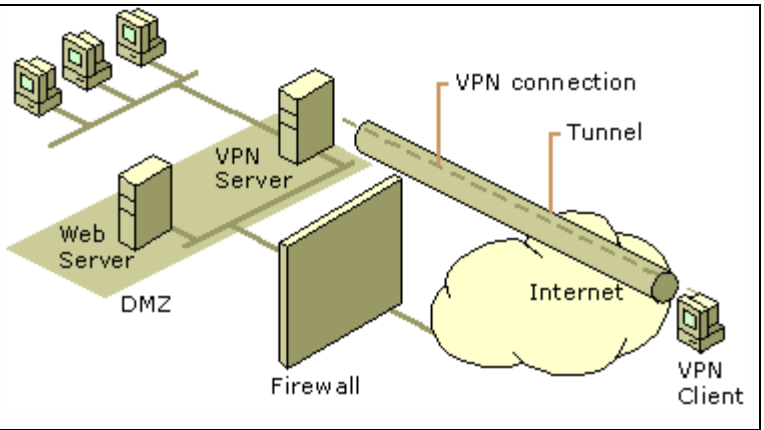


*Figure 4.2.2.2 – VPN Server Behind a Perimeter Firewall*

*Source: https://technet.microsoft.com/en-us/library/cc958037.aspx*

The far more frequent practice can be seen in figure 4.2.2.2 and is to place the VPN server behind the perimeter firewall in a company's Demilitarized Zone (or DMZ for short). This type of setup allows the VPN server to be protected by the same firewall filters and rules as the other DMZ devices while still providing VPN connections to the enterprise. The downside to this is that the VPN connections are tunneled (encrypted) through the firewall allowing the traffic to make it through the perimeter without the same filters and rules as other traffic. While these connections are designed to be from trusted sources, there is a risk to the enterprise if one of these trusted communications are compromised or spoofed. These connections are allowed to bypass the "hardened front door" (the perimeter firewall) and allowed straight into the DMZ.

## 5. Conclusion

Despite being developed over 20 years ago, VPN connections are still the standard method for expanding business networks to remote sites and remote workers. It is a truly scalable solution that can save a company a significant amount of money when compared to a leased or dedicated line solution.

As with any technology, there are benefits and risks associated with its implementation. While many types were discussed in this paper, no recommendations were made because each company is different. There are different risk tolerance levels, diverse industries, as well as geographical makeup. With so many variations, only the members of a company can determine if a VPN solution is right for them. The subject of implementing a VPN is a conversation many organizations have had and one that should be revisited from time to time. There are no silver bullet products out there and no one product that can address all of a company's concerns. It truly is that the "mantra of any good security engineer is: ‘Security is a not a product, but a process'" (Schneier,

"Risks of Relying on Cryptography", 1999). This statement holds true for VPNs as well as for any other technology a company investigates.

# References

How VPN Works. (2003, March 28). Retrieved March 29, 2016, from https://technet.microsoft.com/en-us/library/cc779919

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

Schneier, B. (1999, October). Risks of Relying on Cryptography. Retrieved April 09, 2016, from https://www.schneier.com/essays/archives/1999/10/risks_of_relying_on.html

Crawford, D. (2014, December 18). PPTP vs L2TP vs OpenVPN vs SSTP vs IKEv2. Retrieved April 09, 2016, from https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

Kelly, S. (2004, November 15). Necessity is the mother of VPN invention. Retrieved April 14, 2016, from http://www.comnews.com/cgi-bin/arttop.asp?page=c0801necessity.htm Internet Archive [https://web.archive.org/web/20041115214242/http://www.comnews.com/cgi-bin/arttop.asp?page=c0801necessity.htm]

Kuklin, P. (n.d.). How Long Will Customers Wait for Service? Retrieved April 14, 2016, from https://www.aabacosmallbusiness.com/advisor/long-customers-wait-231506422.html

Leased Line vs VPN - Which Technology Is Right For YOUR Business? (n.d.). Retrieved April 17, 2016, from http://www.hso.co.uk/leased-lines/leased-lines/leased-line-vs-vpn

VPNs and Firewalls. (n.d.). Retrieved April 17, 2016, from https://technet.microsoft.com/en-us/library/cc958037.aspx

Kaleb Fornero, f_kaleb_40@hotmail.com