Virtual Private Networks

An elaboration by Christian Janeczek

Table of Contents

[Definition 2](#_Toc413765575)

[What exactly is a Virtual Private Network? 2](#_Toc413765576)

[Why should you use a VPN? 2](#_Toc413765577)

[How does a Virtual Private Network work? 3](#_Toc413765578)

[Tunneling Protocols 5](#_Toc413765579)

[List of References 6](#_Toc413765580)

# Definition

## What exactly is a Virtual Private Network?

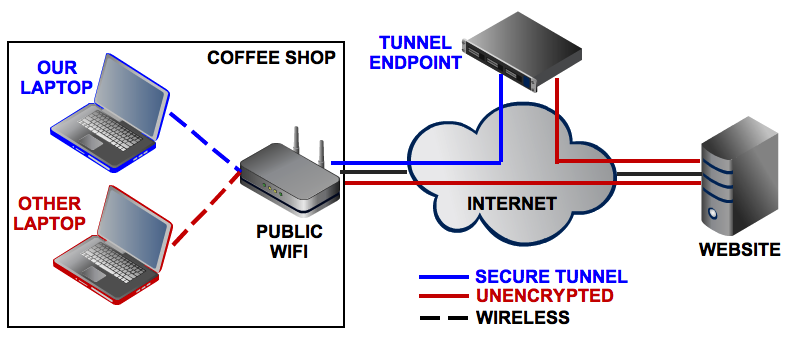
Virtual Private Networking itself allows you to connect to a remote offices’ or organizations’ internal LAN through a public telecommunication infrastructure such as the Internet. It provides secure access for remote offices or individual users to their organization’s network, so to say. Not only does it provide access, it also ensures privacy through security procedures and Tunneling protocols such as the *Layer Two Tunneling Protocol (L2TP)*. Data is encrypted at the sending end and decrypted at the receiving end.

## Why should you use a VPN?

There are at least four great reasons for using a Virtual Private Network and I am going to introduce and give you essential information about each of one them.

**First,** you can use it to connect securely to a remote network via the Internet. Most companies maintain VPNs so that employees can access files, applications, printers or just valuable data – the organization’s important resources. You can also set up your own VPN to safely access your secure home network while you’re on the road. So the ***Availability***plays a very important role concerning the use of Virtual Private Networking and is one of its most advantageous features.

**Second**, and probably the most important aspect of a VPN is ***Security.*** Virtual Private Networks are particularly useful for connecting multiple networks together securely. For this reason, most businesses rely on a VPN to share servers and other networked resources among multiple offices or stores across the globe. This little trick also allows connecting multiple home networks or other networks for personal use. The security is established via various Tunneling Protocols which I will come to later on in this very elaboration.



This diagram illustrates the difference between using an unencrypted connection and using a VPN-secured Internet connection at your average coffee shop.

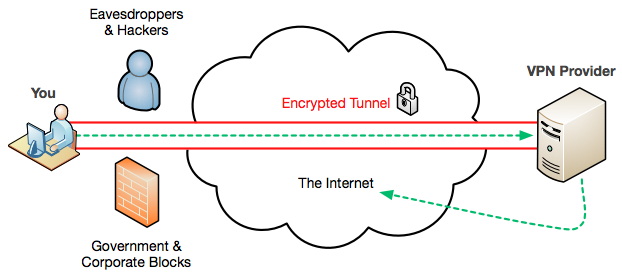
**Third**, connecting to an encrypted VPN while you are on a public or untrusted network, for example a Wi-Fi hotspot that are often found in hotels, coffee shops as well as bars, is a smart, simple security practice that can deal with any online ***Privacy*** issues someone might have. Virtual Private Networks not only encrypt your Internet traffic they also protect you from potential hackers or people who may be trying to snoop on your browsing via Wi-Fi to capture your passwords.

As long as your VPN is trustworthy and keeps no logs, VPN is a very secure and anonymous means of surfing the internet.

As mentioned before, it is also good for securing connections at public Wi-Fi hotspots and for evading firewalls used to censor the internet.

**Fourth** and finally: ***Authorization*.** One of the best reasons to use a VPN is to circumvent regional restrictions. The so called “Geo-blocking”, the practice of preventing users from viewing websites and downloading applications and media based on location can be bypassed. Journalists and political dissidents use VPNs to get around state-sponsored censorship all the time, but you can also use a VPN for recreational purposes, such as connecting to a British VPN to watch the BBC iPlayer outside the UK. If you connect with a British VPN server, you take the identity of a British citizen and are allowed access to all features which are restricted to foreign countries.

I have only mentioned advantages of Virtual Private Networking so far, but disadvantages do exist. For example, if you have a Cisco VPN software installed on your client you are most likely to connect to a Cisco VPN server. If you decide to connect to other vendor-specific VPN servers, e.g. Microsoft or OpenVPN you might have a few complications. It’s like two shoes that can only be worn as a pair.



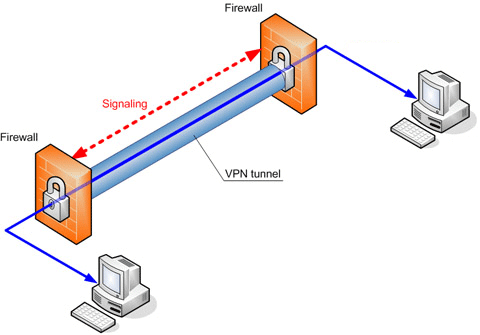
# How does a Virtual Private Network work?

To explain the main idea and functionality behind a Virtual Private Network, I would like to begin at the creation of the Internet itself. First, I would like you to understand, why the Internet was invented in particular.

One of the important reasons was the instantaneous communication around the globe during the time of wars. Before the creation of the Internet there were several stations, which were responsible for the maintenance of the communication. But what would happen if a potential nuclear attack destroys one of these stations? The communication-stations and their static structure would fall apart and it wouldn’t be possible to send and retrieve important data.

Especially for that reason, the arrangement of plenty routers was initialized. These routers were connected to each other, showing a completely dynamic structure, which could even withstand a nuclear attack, by recreating the route of communication somewhere else. The Internet gained the property of high availability but there was still one problem concerning the major security of the whole communication process.

A hacker could sit at one of these routers and listen as well as sniff at data packages passing by. This certain attack is called a “Man in the Middle” - Attack. For exactly that reason, Virtual Private Networks were invented. With the help of VPNs, the data, which is sent through the Internet is coated in a Tunnel, working with a specific Tunneling Protocol. There are many different Tunneling Protocols, some of which I will address later on in this elaboration.



You can imagine the Tunnel as some kind of wall, existing for the whole purpose of security. If an attacker should think about sniffing your data traffic, he first has to penetrate the tunnel’s wall. Part of the Tunneling Protocol is looking for this kind of penetration attempts and if an attack should be detected, the Tunnel recreates a new route with a new set of routers between the client and the server. Even if, in the worst case scenario, the attacker should penetrate the tunnel and gather the data traffic’s information, it still is encrypted and not readable with the correct key.

**As a little summary:**

The VPN’s Tunneling Protocol creates a tunnel, which is responsible for your data’s safety. An attacker has to penetrate the tunnel’s wall to get access to your encrypted data. Part of the Tunneling protocol has something called “Penetration Detection”, which is a process of recreating the connection with a completely new set of routers to escape the attacker’s grasp.

# Tunneling Protocols

There are a lot of different Tunneling Protocols at your disposal but in this elaboration, only the four most important ones are mentioned. Here’s a quick rundown, including the strengths and weaknesses of each.

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

The Point-to-Point Tunneling Protocol (PPTP) is the least secure VPN method, but it’s a great starting point for your first VPN because almost every operating system supports it, including Windows, Mac OS, and even mobile OSs like Android.

PPTP uses a control channel over TCP and a GRE (Generic Routing Encapsulation) tunnel operating to encapsulate PPP packets. Generic Routing Encapsulation is a tunneling protocol developed by Cisco System that can encapsulate a variety of network layer protocols inside virtual point-to-point links over an Internet Protocol.

**Advantages:** The easiest Tunneling protocol to use

**Disadvantages:** The most insecure Tunneling protocol

## Layer 2 Tunneling Protocol (L2TP)

The Layer 2 Tunneling Protocol is more secure than PPTP and is almost as widely supported, but more complicated to set up. It does not provide any encryption or confidentiality by itself. Moreover it provides privacy by relying on an encryption protocol that is passed within the tunnel.

**Advantages:** More secure than the Point-to-Point Tunneling Protocol

**Disadvantages:** More complicated to set up than the PPTP

## Internet Protocol Security (IPSec)

The Internet Protocol Security is more secure than PPTP and is almost as widely supported, but more complicated to set up. By authenticating and encrypting each IP packet of a communication session the security of the IPSec protocol suite for Internet Protocol communications is established.

**Advantages:** More secure than the Point-to-Point Tunneling Protocol

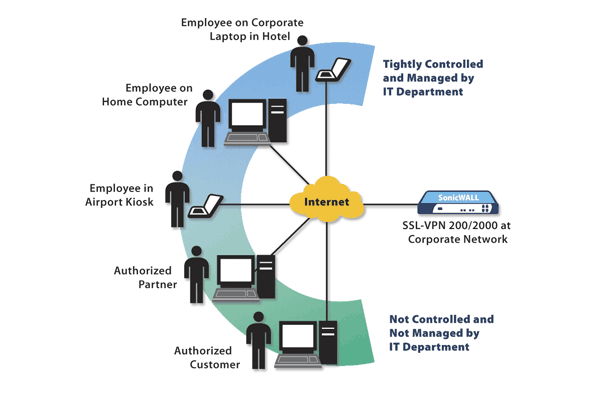
**Disadvantages:** More complicated to set up than the PPTP

## Secure Sockets Layer (SSL)

Secure Sockets Layer VPN systems are the most secure way of tunneling. For example, if you log on to banking sites and other sensitive domains, SSL is used to provide the highest level of security.

Most SSL VPNs are referred to as “clientless”, since a dedicated VPN client is not needed to connect to one of them. The connection happens via a Web browser and thus is easier and more reliable to use than PPTP, L2TP, or IPSec.

**Advantages:** The connection happens via a Web browser -> Easier and more reliable than the other Tunneling Protocols

**Disadvantages:** The most complex Tunneling protocol

An SSL VPN server is designed to be accessed via Web browser and creates encrypted channels so that you can safely access the server from **anywhere.**

# List of References

**[1] Virtuelle Private Netzwerke, Aufbau und Sicherheit;** Manfred Lipp;

ISBN 978-3-8273-2647-8

**[2] How and why to set up a VPN today;** Eric Geier;

<http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html>

**[3] Virtual Private Network;** Vangie Beal;

<http://www.webopedia.com/TERM/V/VPN.html>

**[4] Geo-Blocking;** Wikipedia;

<http://en.wikipedia.org/wiki/Geo-Blocking>

**[5] Virtual Private Network Definition;** Margaret Rouse; <http://searchenterprisewan.techtarget.com/definition/virtual-private-network>

**[5] VPN Tunnel Picture;**

<http://bestvpn.biz/wp-content/uploads/2013/10/vpn-tunnel.gif>

**[6] VPN Provider-You Image;**

<http://blog.rastating.com/content/images/2014/11/vpn-diagram.png>

**[7] Point-to-Point Tunneling Protocol;** Wikipedia;

<http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol>

**[8] Generic Routing Encapsulation;** Wikipedia; <http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation>

**[9] Layer 2 Tunneling Protocol;** Wikipedia;

<http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol>

**[10] IPSec;** Wikipedia;

<http://en.wikipedia.org/wiki/IPsec>

**[11] SSL-VPN Image;**

<http://core0.staticworld.net/images/article/2013/03/ssl-vpn-100029646-orig.png>