# Virtual Private Networks

Bogdan Ionescu

March 25, 2020

# Contents

# Chapter 1

# Virtual Private Networks

## 1.1   Importance of VPNs

In this day and age, networking is everywhere, especially considering the exceedingly fast expansion of the Internet. The Internet, the ultimate network of networks, has radically changed our day-to-day life. Just several years ago, simple everyday habits, such as quickly searching for a piece of information on Google, streaming your favorite songs or paying your bills with just a few clicks would have seemed possible only in a distant future. And yet here we are today, achieving even more impressive tasks, making use of all kinds of networks available within our laptops, phones, tablets and even home electronics, thanks to the IoT.

Unfortunately, the Internet's rapid development also comes with a few important drawbacks which are regrettably often overlooked — the most significant one being cybersecurity. *Cybersecurity* is the protection of computer systems and networks from the theft and damage of hardware, software or electronic data, as well as from the disruption of the services they provide.[1] Imagine the consequences if someone managed to obtain all of your credit card information when you are attempting to make an online payment. The damages rise significantly in the case of similar data theft at major companies, which could lead to huge amounts of loss in revenue. In fact, Juniper Research[2] estimates that cybercrime will cost businesses over \$2 trillion in 2019 alone.

Most often, networks are the first obstacle when trying to exploit systems, which is why network security represents such an important key aspect. Surprisingly enough, many protocols used in networking just a few years ago

---

[1] Wikipedia definition, `https://en.wikipedia.org/wiki/Computer_security`

[2] `https://www.juniperresearch.com/home`

offered no encryption capabilities whatsoever, which led to quite serious vulnerabilities. For example, simple data theft was quite uncomplicated then, when HTTP was predominantly used on the web. Since HTTP alone does not encrypt its data, the communication between our device and a website's server using this protocol would be in cleartext. If someone managed to intercept the network traffic between these two nodes, they would be able to obtain everything that we submit to that website, such as usernames, passwords and even credit card information.

Confidentiality and integrity over networks is also a crucial need for most companies. These usually maintain one or more private networks inside their offices, and only from within these controlled networks employees can access necessary resources. However, these resources must also be available to employees who may be connected to another (possibly also private) network. Such remote access allows employees to work from any part of the world, possibly in case of time-critical emergencies, where response time is vital. This connection must be encrypted in order to prevent traffic sniffing and provide integrity by allowing only authorized users to access the company's private networks. If these conditions are not met, severe breaches often occur, generally leading to a tremendous amount of sensitive data being leaked.

By now you might be thinking how important it is that an application encrypts its data. Unfortunately, sometimes it does not even matter which application we are using! Our outgoing network packets, regardless of what application we are using, will still have our public IPv4 or IPv6 address as a source. Although this may not seem like a serious problem, its implications are quite vast: IP address-based geo-blocking, IP range ban, traffic monitoring etc. These methods represent only a few of those often employed by media companies, governments, intelligence agencies[3], or even by countries (The Great Firewall of China[4]).

The question which therefore arises is straightforward and of interest to many of us: how can we achieve confidentiality, integrity and sometimes even anonymity over public networks, such as the Internet? This is where *Virtual Private Networks* (VPNs) prove greatly effective.

## 1.2    What Is a VPN?

A Virtual Private Network (VPN) extends a private network by allowing users who are not part of it to send and receive data over a public network,

---

[3]https://en.wikipedia.org/wiki/National_Security_Agency#AT&T_Internet_monitoring

[4]https://en.wikipedia.org/wiki/Great_Firewall

usually the Internet, as if they are directly connected to the private network. VPNs are build using *tunneling protocols*, which establish *tunnels* over public networks, in which the data is encapsulated and most often encrypted[5]. Classified by the type of topology of connections, VPNs usually are of three types: site-to-site, point-to-point (sometimes also called host-to-host), which are the most common, and a combination of the two, point-to-site.

Site-to-site VPNs establish a tunnel between two networks, thus allowing any authorized host in any of the two networks to make use of it, as shown in figure 1.1.
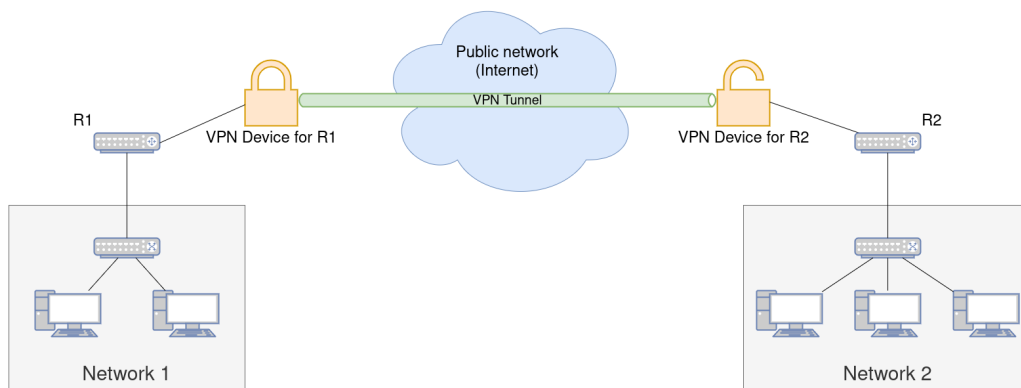


Figure 1.1: In this site-to-site architecture, the two VPN devices establish a secure tunnel through the public network. All traffic is encrypted from one site to another. VPN technology can also be directly available in some high-end routers, removing the need for two additional devices.

Advantages of site-to-site VPNs include scalability, being quite straightforward to add another site or device, and high availability, as the VPN tunnel does not depend on a device inside the network to initiate the secure connection (as would be the case with point-to-point architectures), which is why this approach is consistently used by most companies. However, for regular users who wish to remain as private as possible, site-to-site VPNs have a quite serious disadvantage. Since traffic is encapsulated and encrypted just as it leaves the site, by the VPN device or router, data is still vulnerable in the network until it reaches this point, or after it was decrypted, at the other site. As a result, anyone who can intercept our traffic at these stages is a potential threat. Although this scenario is not likely in a company, it is very probable, for example, for someone who wishes to secure his data from

---

[5]Encryption is a common, yet not inherent part of VPN connections.

a public place which offers free Internet connection, such as a coffee shop or restaurant.

Point-to-point VPNs establish a secure tunnel between two single hosts in usually separate networks, encryption and decryption taking place only at these points, therefore eliminating the aforementioned risk with site-to-site architectures.
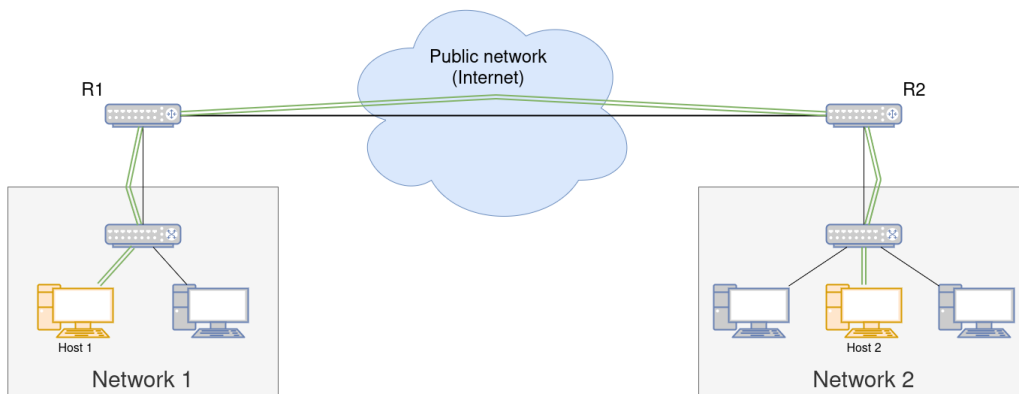


Figure 1.2: A point-to-point VPN tunnel between Host 1 and Host 2.

Point-to-point VPNs are used to form traditional consumer VPNs, where a user establishes a secure tunnel between his device and a server, which is then used as a proxy. In this situation, when the user connects to a website, for example, the network traffic is routed through the proxy server, thus appearing that the request was made from the server, not the user's device. This allows to bypass IP geo-blocking if the server is located in another region, a paramount need for VPN consumers.

Disadvantages of point-to-point VPNs generally concern their setup and management. If the user chooses an existing VPN service provider, these are quite straight-forward and usually require just an installation of an application on the desired device. However, VPN providers charge for their services, which is why many users choose to rely on self-hosted VPNs. In this case, it is the user's job to install and manage the VPN software on both the proxy server and his/her device.

## 1.3   VPN Tunneling Protocols

Now that we have seen how different VPN topologies operate, what networking protocols are actually used to build one?