Virtual Private Networks

Bogdan Ionescu

April 7, 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, online shopping, 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] Most often, networks, full of information, are the first frontier when trying to exploit systems, which is why network security represents such an important key aspect against cybercrime.

Inevitably, when having any communication over the Internet, a significant amount of data is being sent between you (more precisely, your device) and the other party, commonly a server or another person's device. Although this data can sometimes be quite harmless, such as a quick Google search for a cake recipe or just streaming some music, in some cases it may contain more sensitive and valuable information than you can think of. Personal messages while chatting with a close friend, credit card information when making an

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

online payment, passwords used when logging in to different websites, the video feed recorded by your webcam when having an online conference — these are only just a few examples of what kind of infomation leaves your private home network when accessing the Internet. Since the Internet is a public network, such data can be easily intercepted by other parties before reaching its destination, which often leads to catastrophic consequences.

By now you might think that if you are using an application which encrypts its data, you should be safe on the Internet. Unfortunately, this is often not the case, as there are many places where things can go wrong. For example, in many messaging systems, messages pass through intermediary parties, such as the application's servers, which store them, from where they are retrieved by the recipient. In such scenarios, data is generally encrypted only in transit — from the sender to the server, and from the server to the destination. Even if the servers encrypt the data at rest (which, surprisingly, does not always happen), they still must have access to the cryptographic keys used in this process, therefore information is still being vulnerable in case the actual servers are being targeted. Moreover, this allows the third party, or any other organization which has a backdoor to these servers, to freely recognize our data. Such invasion of privacy is prevented by using end-to-end encryption, a system where only the communicating users can read the messages, denying any other third party to access the cryptographic keys needed to decrypt the information.

Even if such encryption is used, with strong cryptographic ciphers, unlikely to be broken in attacks, we still might experience some troubles. Application data that leaves our home network, in order to be routed over networks, will have an Internet Protocol (IP) header added to it, which contains our public IP address and the destination IP address. These are unique, ISP-issued addresses which can be used to monitor and censor traffic, since every service we try to access will be identified by its IP address. This could also lead to IP address-based geo-blocking and IP range ban, methods often employed by media companies, governments, intelligence agencies and many others.

So far we have only talked about the consequences from the point of view of a casual user, but damages rise significantly in the case of cyber attacks against major businesses, usually leading to huge amounts of loss in revenue. In fact, Juniper Research estimated in 2015 that cybercrime will have cost businesses over $2 trillion by 2019 [1]. In order to mitigate cyber attacks, they usually maintain one or more private networks inside their offices and only from within these controlled networks employees can access necessary resources. Such resources can actually be part of the same network, thus making transfer of data safe, since everything happens inside

the private network, but inevitably some resources, such as cloud services, will be accessed through the Internet. Some employees must also be able to connect to the private network through the Internet even if they are part of another network, in order to access its resources, possibly in case of time-critical emergencies or just to work remotely from their homes. Therefore, many companies need a technology that allows secure communication between their private network and another host across a public network, or even to another different private network, such as communication between two private networks owned by different offices of the same company, located in distant regions.

The solution to all the aforementioned problems, and to many other vulnerabilities while using a public network, is a Virtual Private Network (VPN).

1.2 What Is a VPN?

Security over networks is usually described by three components: confidentiality, integrity and authenticity. Confidentiality, often achieved by encryption, guarantees that data can only be understood by authorized entities. Integrity ensures that the data has not been modified between these endpoints. Finally, authenticity proves that data originated from an authorized party, and not from another source. Apart from these three, another concept which is often massively desired over public networks refers to anonimity, which assures that information we send out does not divulge our identity. All of these can be achieved by VPNs, if implemented correctly.

A Virtual Private Network (VPN) extends a private network by allowing hosts which are not part of it to send and receive data over a public network, usually the Internet, as if they are directly connected to the private network. VPNs are build by establishing a way of communication between two nodes, one being part of the private network. The second node will forward its traffic to it, the first node acting like a proxy, therefore appearing as the traffic actually originated from within the private network from which it is part of. Since encryption is a common, yet not an inherent part of a VPN connection, this channel of communication is usually called a *tunnel* — only the two endpoints being able to understand the data passing through it.

in which the data is encapsulated and most often encrypted[2]. 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.

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

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.

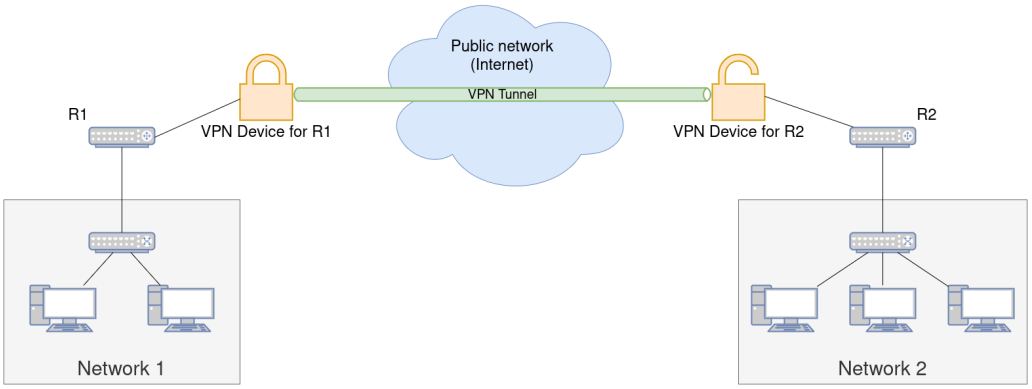

Figure 1.1: In this site-to-site architecture, the two VPN devices establish a secure tunnel through the public network. All traffic is encrypted from one site to another. VPN technology can also be directly available in some high-end routers, removing the need for two additional devices.

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 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.

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

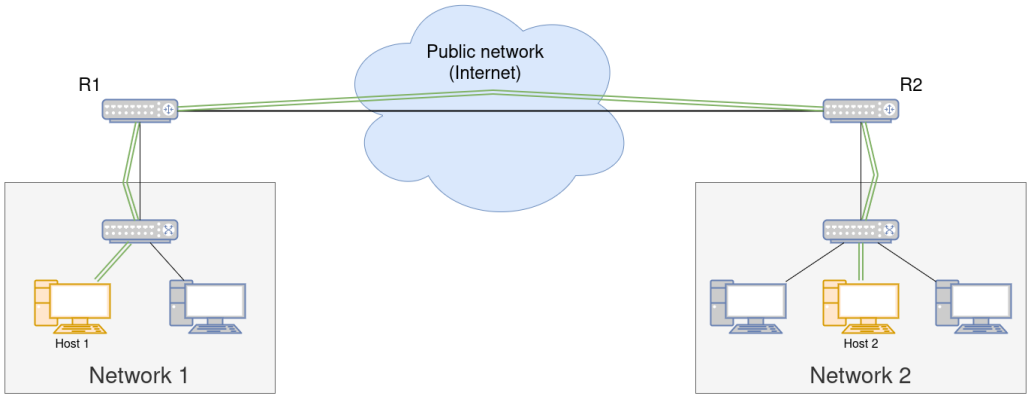

Figure 1.2: A point-to-point VPN tunnel between Host 1 and Host 2.

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 Tunneling Protocols

As mentioned in the previous section, a tunnel between two VPN devices (also sometimes called the endpoints of the tunnel) is established VPN tunnels are build using *tunneling protocols*. Tunneling protocols, just like every other network protocol, use encapsulation, in order to repackage certain traffic data, sometimes even modifying it.

For example, IP in IP[3] is a tunneling protocol which encapsulates an IP datagram within another IP datagram, as shown in figure 1.3.

[3] `https://tools.ietf.org/html/rfc2003`

Figure 1.3: A point-to-point VPN tunnel between Host 1 and Host 2.

Bibliography

[1] S. Smith. Cybercrime will cost businesses over $2 trillion by 2019. *Retrieved from Juniper Research: https://www. juniperresearch. com/press/pressreleases/cybercrime-cost-businesses-over-2trillion*, 2015.