Virtual Private Networks

Bogdan Ionescu

March 9, 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.

Surprisingly enough, simple data theft was quite uncomplicated a few years ago, when HTTP was predominantly used on the web. Since HTTP alone does not encrypt its data, the communication between our device and

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

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

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. It would be like having a discussion with a friend, without knowing that someone was eavesdropping the entire time! As you can probably tell, this represents a huge security flaw, besides an invasion of privacy, which is why nowadays most websites use HTTPS, which relies on TLS to encrypt HTTP data.

Unfortunately, as we will see in further chapters, protocols such as HTTPS only provide confidentiality and integrity, not anonymity, because our network packets 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 governments, intelligence agencies[3], or even by countries (The Great Firewall of China[4]). The question which therefore arises is simple: how can we achieve privacy and secrecy over the Internet? This is where Virtual Private Networks (VPNs) prove useful.

1.2 What Is a VPN?

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

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