John Faria
February 24th, 2020
VPNs – What Virtual Private Networks Can and Can't Do For Your Security

VPNs – What Virtual Private Networks Can and Can't Do For Your Security

The Cyber-Landscape

Every second there are approximately 90,000 gigabytes of network communications flying across the world[1], crossing the vast web of routers and computers to reach their destination. The traffic on the Internet consists of everything from private emails to financial transactions, entertainment media, personal photographs, and much more. Organizations such as your Internet service provider or local network administrator are responsible for routing your traffic to a destination, so what is to stop them from interfering with your traffic? In theory, these entities (or anyone else who has managed to gain such access) could read your traffic, change the information being sent, or simply deny your connection. Every second on the Internet millions of dollars are stolen by criminals[3]. The cyber-attacks include: the integrity of financial information being compromised, government organizations spying on billions of peoples' communications, and an untold number of communications being blocked by a ruling organization.

Kaspersy Cyberthreat Real-Time Map showing all of the obvious cyber-attacks occurring on the Internet at a specific moment.

Virtual Private Networks are commonly praised as the solution to the cyber-security crisis all Internet users face. Advertisements promise to protect users from cyber-criminals, prying government eyes, and anyone attempting to deny the user's connection to certain websites. Are VPNs really as powerful as advertisements claim? Will VPNs actually defend Internet users while they are browsing online? To answer this questions on VPN practicality we need to delve into what a virtual private network actually does for your Internet connection, and what your Internet connection looks like without a VPN.

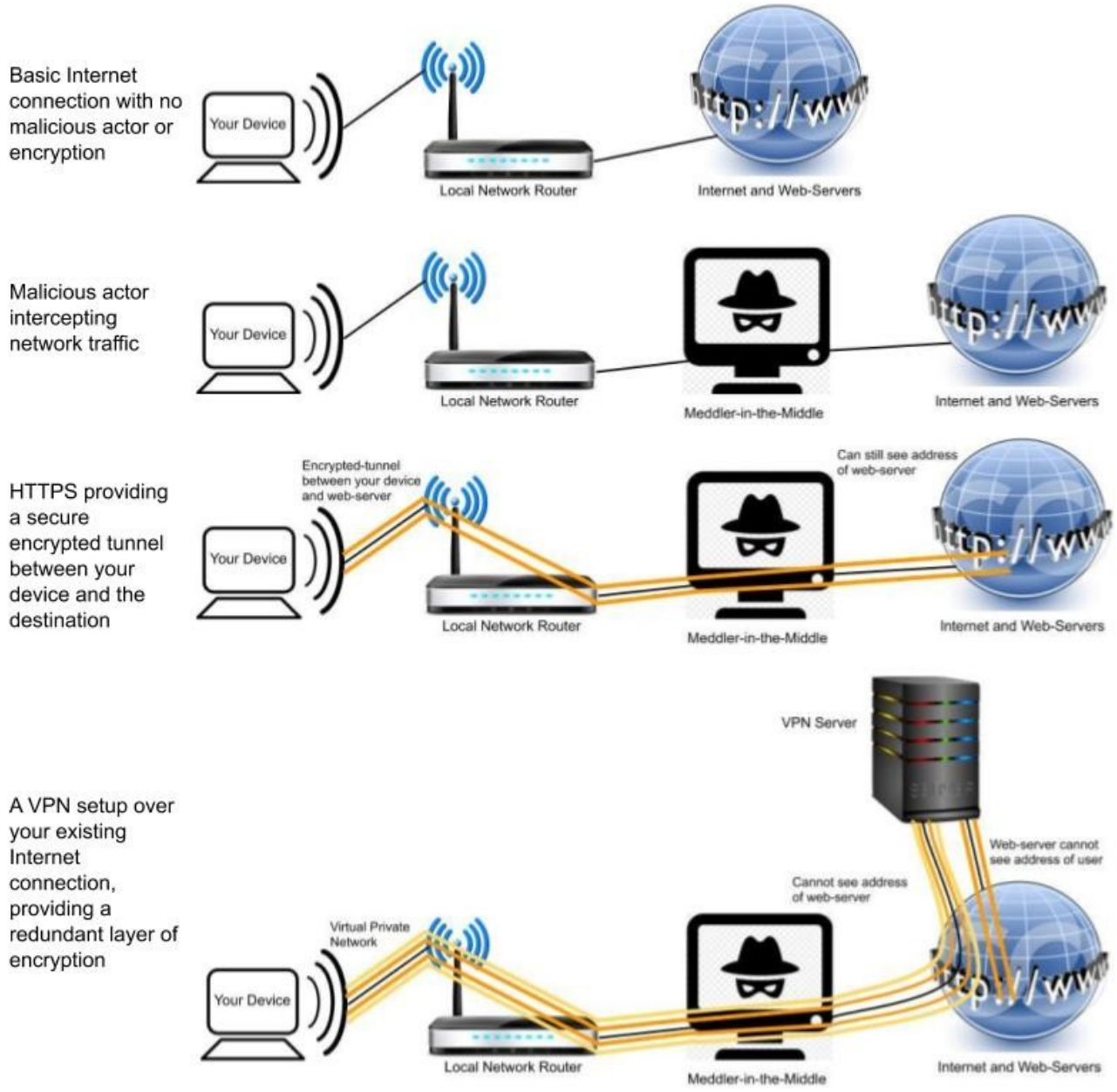
Network Connection Anatomy

When you are connected to the Internet, the three main pieces of data sent in your connection are: the destination address, the information that you want to send (which we will refer to as a payload), and your address. Any router that is responsible for transmitting your message will look at the destination address and pass the information on to the next router. There can be anywhere from a couple to a few dozen routers between you and your destination. Once the payload finally reaches the destination, the web-server you are connecting to will take note of your address, and send a response back to you. Any of the routers that your message passes through has the potential to be controlled by a malicious actor. Being the arbiters of the information users are trying to send, the all routers have the potential to spy-upon and even modify the payload. The payload could contain sensitive information such as: passwords, website verification keys, or program instructions to be executed. To combat the threat to the security of your communication payload, encrypted communications became a standard among websites by 2018[2]. You may have seen the presence of this standard in the form of the green lock on the left side of your web browser's URL bar. With the right encryption algorithm, the payload information being sent will be illegible to a meddler-in-the-middle. However, according to VPN providers, the security of your information online is still far from guaranteed and their service will protect you.

While the payload portion of the information you are sending is safe from being observed or modified, the destination and sender addresses are not encrypted (and the addresses cannot be encrypted, otherwise routers will not know where to send your information). A malicious actor could decide that they do not want you to communicate with that specific website, and thus they could deny you the availability of that information. Many organizations that control an Internet connection, such as office buildings or autocratic states, may block connections to websites that they do not want you visiting. It is also feasible that you do not want the routers that your traffic is passing through to log what websites you are visiting, or that you do not want the website to know who you are.

John Faria
February 24th, 2020
VPNs – What Virtual Private Networks Can and Can't Do For Your Security

Network Mappings of Internet Connections



Sources for the images used in this diagram are detailed in Images Cited

VPN Structure and Legitimate Uses

In such extreme cases of information security, where adversaries have significant control over your communications, a virtual private network is useful in helping to protect your Internet connection. When you connect to the Internet through a VPN, all of the information you are sending is wrapped in a second layer of encryption, including the target address. The message is then sent to a server hosted by your VPN provider, instead of being sent directly to the destination. The server will decrypt the first layer of encryption that is protecting the first layer of encryption on your payload as well as the target address. The VPN server will then send the encrypted data to the target address. Any meddler between you and your connection to the Internet will only be able to see you sending encrypted traffic to some unknown address (which is the address of your VPN server). As a bonus, the website you are connecting to will also only be able to see the address of the VPN server and therefore will not know your Internet address. Effectively, an encrypted tunnel has been formed between you and your VPN server. VPN

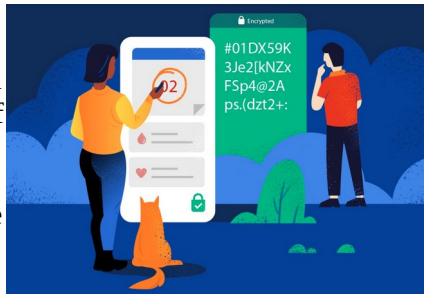
providers do their best to ensure that their servers have a connection to the Internet which is not hindered by any malicious actors, and therefore their users can trust that the connection is safe. However, some VPN providers, particularly the providers that offer free VPN services, will actually use your VPN connection to log the information that you are sending[3]. In most cases, by using a VPN you can trust that your connection to the Internet is safe from any restrictive firewalls, persons spying on what websites you visit, and you can even ensure that websites do not know who you are.

So when would it be worthwhile for you to use a VPN? Unless you are living in an oppressive country, someone who pirates digital media, or you are just seriously paranoid that a cyber-criminal is trying to intercept your Internet communications, then you really have no need for a virtual private network. The encryption schemes that almost all websites already use already protect the data that you are sending from having its confidentiality or integrity compromised. VPN providers are attempting to fool users into believing that their Internet connections are in great danger and that they need to pay for a VPN service to stay safe. There are a few cases where you may find yourself in need of a VPN, such as if you are attempting to connect to a website that is blocked by whoever is managing the local network or if you wish to hide what websites you are connecting to. For the average user who is not a criminal or computer network hobbyist, there is no need for a VPN. You are better off trusting the encryption standards that already exist on the Internet, not giving your money or sensitive information to fear-mongering VPN providers, and also taking simple steps to protect areas that are vulnerable than your internet connection.

Practical Internet Safety Tips

There is no way to completely ensure the safety of your information while you are using the Internet. Even if you are using a trustworthy VPN connection, this only guarantees that your destination is not being spied upon, or denied as you attempt to connect to a web-server. Cyber-criminals are clever, persistent, and can eventually find a way to steal your information. A VPN will do nothing to protect you from dangerous websites, malware being installed on your computer, scammers, or most other threats that Internet users face. So what should you do to stay safe? How can you ever possibly use the Internet in a secure manner?

First of all, you should recognize that security is relative. The topic of information security only ever gets more complicated and paranoid. For example, VPNs over-complicate what you truly need to connect to a web-server securely, by wrapping your messages in a redundant layer of encryption and re-routing your traffic. Despite this increased assurance, your connections can still theoretically spied upon by your VPN provider. Dedicated malicious actors may still find other ways to attack you. As long as you use reasonable precautions then you can be relatively secure on the Internet. Instead of relying on a VPN to secure your communications, you should just ensure that your web browser always uses HTTPS when you connect to a web-server. The web browser extension *HTTPS Everywhere* can be used to force your web-browser to make every connection using HTTPS[2]. If you wish to take other simple and actually effective steps to stay safe online you should: install an antivirus program on your computer, set-up multi-factor authentication on your important accounts, and be wary of where you store your sensitive documents. The Internet is a complicated and dangerous place. By understanding the basics of how the technology works you can know where your information is being sent and who has access to it. After having a basic understanding of how your sensitive and recognizing that you should always be careful of what you trust, it is possible for the average user to stay safe online.



On the Topic of Encryption, created by Afsal CMK to spread public awareness on HTTPS and looking for the green lock

John Faria
February 24th, 2020
VPNs – What Virtual Private Networks Can and Can't Do For Your Security

Works Cited

Berners-Lee, Tim. "One Second." *Internet Live Stats*, 23 Feb. 2020, www.internetlivestats.com/one-second/.

Budington, William. "HTTPS Everywhere." *Electronic Frontier Foundation*, 22 Jan. 2020, www.eff.org/https-everywhere.

Lau, Lynette. "Cybercrime 'Pandemic' May Have Cost the World $600 Billion Last Year." *CNBC*, CNBC, 23 Feb. 2018, www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html.

Image Citations (in order of appearance)

Kaspersky Cyberthreat Real-Time Map, Kaspersky Lab, screenshot of the real-time map available on Kaspersky's website at cybermap.kaspersky.com

Wireless Router Icon, artist unknown, www.clipartbest.com, available for free and public use

17596 Clipart Illustration of a Blue Globe with a Graph and URL for the World Wide Web, Leo Blanchette, available from gallagher247.files.wordpress.com/2010/12/17596-clipart-illustration-of-a-blue-globe-with-a-graph-and-url-for-the-world-wide-web.jpg

Server Remix 1, "Merlin2525", 1001freedownloads.s3.amazonaws.com/vector/thumb/64310/Server_Remix_1_by_Merlin2525.png, available for free and public use

On the Topic of Encryption, Afsal CMK, i.pcmag.com/imagery/articles/04R4UGJ6eMPXJ1qHMcc9Utu-3.fit_lim.size_1004x695.v_1571966520.png, created for public use and to spread awareness of cyber-security best practices.