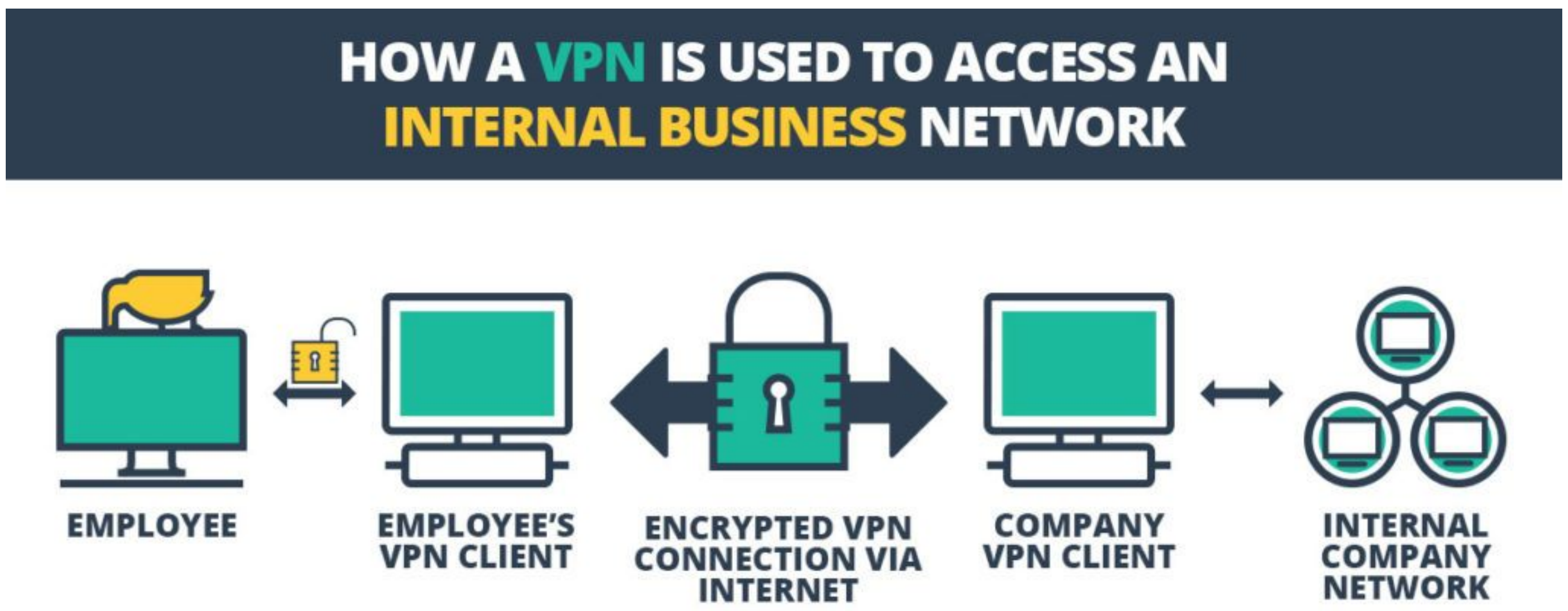
Virtual Private Networks

Dray Agha / 04 May 2020

When you're working from home, you'll still want to access your work's digital resources. If you're going to be accessing business documents and resources over the internet from your home, there are two things you really don't want: a stranger to SEE those work documents, and a stranger who could ALTER those documents.

A **Virtual Private Network** (VPN) offers a safe way, that you at home can access the resources on your business' network. A VPN uses cryptography to ensure that the data bouncing between home and work networks' is encrypted, i.e. it makes sure the communication in the **network** stays **private**. VPNs are like underground tunnels, that you can secretly use to go back and forth to your place of work.


HOW A VPN IS USED TO ACCESS AN INTERNAL BUSINESS NETWORK
EMPLOYEE
EMPLOYEE'S VPN CLIENT
ENCRYPTED VPN CONNECTION VIA INTERNET
COMPANY VPN CLIENT
INTERNAL COMPANY NETWORK

Not all VPNs are the same. Some are built to give secure, anonymous internet connection for individual users who live in hostile political environments. But the VPNs we're going to talk about are the ones that let you connect to a corporate network. A VPN's purpose is to seamlessly join a user to the work network, **as if they were sitting at their work desk** clicking away. It does this by assigning your computer at home an IP address as if it were on the business' network.

When you start up a home-to-business VPN, we need to have some form of **authentication**. We don't want a stranger to have an open path into the business network. These are typically in the form of username:password login. It may be inconvenient, but it's important to **have a strong password** that is of three random words- special characters will increase the strength– a Password Manager would be even better. A poor password will give a hacker the keys to the front-door of the business network.

Though VPNs are overwhelmingly good things, they do have **some disadvantages:**

- VPNs can mean that some programmes and websites **don't quite work properly**.
- Cheap/free VPNs may come **with poor encryption** or **poor security** configurations. Both can render the VPN **pointless** if an attacker is able to undermine the security tunnel and gain access to the business network.
- VPNs make your **internet slower**. This is because of the extra security step of encrypting and decrypting the data, as well as the fact that the VPN takes extra steps between your computer, your work network, and the service it will connect to.

- **VPN companies aren't perfect.** On occasion, hackers have gained entry into the VPN providers' servers and stolen the secret cryptographic keys that can unlock the encryption that your VPN tunnel uses to keep your data safe from prying eyes. Before downloading a free or cheap VPN, do some homework and find some reports and comparison charts that lay out who the reputable VPN providers are.

VPNs are a fascinating use of cryptography and are incredibly user-friendly. When more of us are working from home than ever, it is important we do all we can to keep our networks secure and resilient.

Further guidance:

- https://www.ncsc.gov.uk/blog-post/introducing-new-guidance-virtual-private-networks-vpns
- https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks

Dray Agha is a PhD Researcher based in the Information Security Department at Royal Holloway University of London