1. Qu’est-ce qu’un VPN?

VPN signifie « Virtual Private Network » et décrit la possibilité d'établir une connexion réseau protégée lors de l'utilisation de réseaux publics. Les VPN chiffrent votre trafic Internet et camouflent votre identité en ligne. Il est ainsi plus difficile pour des tiers de suivre vos activités en ligne et de voler des données. Le chiffrement est effectué en temps réel.

2. Origines du VPN

Dès les débuts d’Internet, il a été nécessaire d’avoir un protocole d’échange de données sécurisé. L’histoire du VPN débute en 1996, quand un employé de Microsoft a développé le “point-to-point tunneling protocol” (PPTP), autrement dit un tunnel sécurisé à l’intérieur d’un réseau. Véritable précurseur du VPN, le PPTP permet de créer un lien sécurisé entre une connexion privée et le reste d’Internet.

Face à l’évolution des moyens techniques, et surtout l’évolution des techniques de piratage, il a été nécessaire de renforcer la sécurité de la connexion elle-même. Les antivirus se chargeaient très bien de protéger l’utilisateur de son côté, mais étaient inefficaces pour protéger les données avant qu’elles n’arrivent sur l’ordinateur de l’utilisateur.

3. Fonctionnement

Une connexion VPN camoufle votre trafic de données en ligne et le protège contre tout accès externe. Les données non chiffrées peuvent être consultées par tous ceux qui ont accès au réseau et qui souhaitent les voir. Avec la présence d'un VPN, les pirates et les cybercriminels ne peuvent pas déchiffrer ces données.

4. Avantages

- Chiffrement sécurisé : pour lire les données, vous avez besoin d'une clé de chiffrement. Sans cela, il faudrait des millions d'années à un ordinateur pour déchiffrer le code en cas d'attaque par force brute. Avec l'aide d'un VPN, vos activités en ligne sont camouflées même sur les réseaux publics.

- Camouflement de vos allées et venues : les serveurs VPN agissent essentiellement comme vos mandataires sur Internet. Comme les données démographiques de localisation proviennent d'un serveur situé dans un autre pays, il n'est pas possible de déterminer votre position réelle. En outre, la plupart des services VPN ne stockent pas les journaux de votre activité. Certains fournisseurs, en revanche, enregistrent votre comportement, mais ne transmettent pas ces informations à des tiers. Cela signifie que toute trace potentielle de votre comportement d'utilisateur reste cachée en permanence.

- Accès à des contenus régionaux : le contenu Web régional n'est pas toujours accessible de partout. Les services et les sites Web contiennent souvent des contenus auxquels on ne peut accéder que depuis certaines parties du monde. Les

connexions standards utilisent des serveurs locaux dans le pays pour déterminer votre position. Cela signifie que vous ne pouvez pas accéder au contenu que vous consultez à domicile pendant que vous êtes en déplacement, et que vous ne pouvez pas accéder à du contenu international depuis chez vous. Grâce à la modification de la position par le VPN, vous pouvez passer à un serveur d'un autre pays et « changer » de position.

- Transfert de données sécurisé : si vous travaillez à distance, vous aurez peut-être besoin d'accéder à des fichiers importants sur le réseau de votre entreprise. Pour des raisons de sécurité, ce type d'informations exige une connexion sécurisée. Pour avoir accès au réseau, une connexion VPN est souvent exigée. Les services VPN se connectent à des serveurs privés et utilisent des méthodes de chiffrement pour réduire le risque de fuite de données.

Sources :

- https://www.kaspersky.fr/resource-center/definitions/what-is-a-vpn
- https://geeko.lesoir.be/2018/09/04/5-choses-que-vous-ignoriez-sur-les-vpn/#:~:text=L'histoire%20du%20VPN%20d%C3%A9bute,et%20le%20reste%20d'Internet
- https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel
- https://nordvpn.com/fr/what-is-a-vpn/