Réseau et Sécurité - Rapport: Réseaux Privés Virtuels (VPN)

SANNA Thomas

November 14, 2024

Università di Corsica Pasquale Paoli

Contents

Chapter 1

Introduction

Un réseau privé virtuel (VPN) est une technologie qui permet d'établir une connexion sécurisée et chiffrée sur un réseau moins sécurisé, tel qu'Internet. Les VPN sont largement utilisés pour protéger la confidentialité des utilisateurs, sécuriser les communications et contourner les restrictions géographiques.

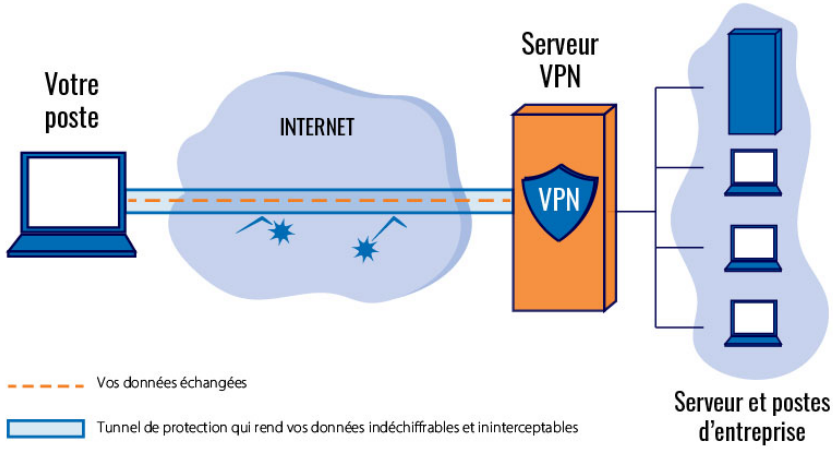

Figure 1.1: Illustration d'un VPN, source : `https://www.alliance-informatique.fr/wp-content/uploads/2022/06/schema-vpn-5.jpg`

Chapter 2

Fonctionnement d'un VPN

2.1 Architecture de base

Un VPN fonctionne en créant un tunnel sécurisé entre l'appareil de l'utilisateur et un serveur VPN. Ce tunnel est chiffré, ce qui signifie que les données transmises sont illisibles pour quiconque intercepterait la communication.

2.1.1 Attribution du VPN à l'utilisateur

Pour attribuer un VPN à un utilisateur, celui-ci reçoit des informations de connexion, telles qu'un nom d'utilisateur, un mot de passe et parfois des certificats de sécurité. L'utilisateur configure ensuite son appareil (ordinateur, smartphone, etc.) avec ces informations pour établir une connexion sécurisée au serveur VPN. Le serveur VPN attribue une adresse IP virtuelle à l'utilisateur, masquant ainsi son adresse IP réelle et permettant de sécuriser ses communications.

2.2 Types de VPN

Il existe principalement trois types de VPN, chacun ayant des caractéristiques et des utilisations spécifiques [BUR22] :

2.2.1 VPN client-to-site

Le VPN client-to-site, également connu sous le nom de VPN d'accès à distance, permet à un utilisateur individuel de se connecter à un réseau privé à distance. Ce type de VPN est couramment utilisé par les employés pour accéder aux ressources de l'entreprise depuis leur domicile ou lors de déplacements. Le client VPN installé sur l'appareil de l'utilisateur établit une connexion sécurisée avec le serveur VPN de l'entreprise.

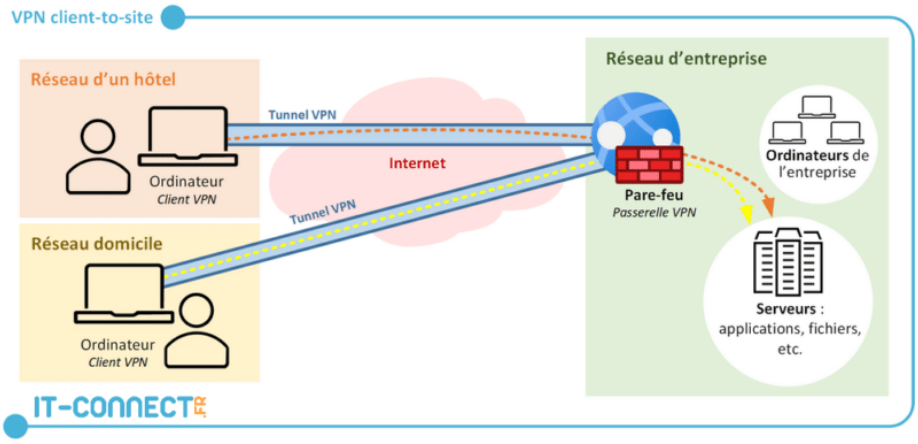

Figure 2.1: Illustration d'une architecture Client-to-Site, source : `https://www.it-connect.fr/les-tunnels-vpn-pour-les-debutants`

2.2.2 VPN site-to-site

Le VPN site-to-site connecte deux réseaux locaux (LAN) distincts sur Internet, permettant aux utilisateurs de chaque réseau de communiquer comme s'ils étaient sur le même réseau local. Ce type de VPN est souvent utilisé pour relier les bureaux distants d'une entreprise, facilitant ainsi le partage de ressources et la collaboration entre les sites.

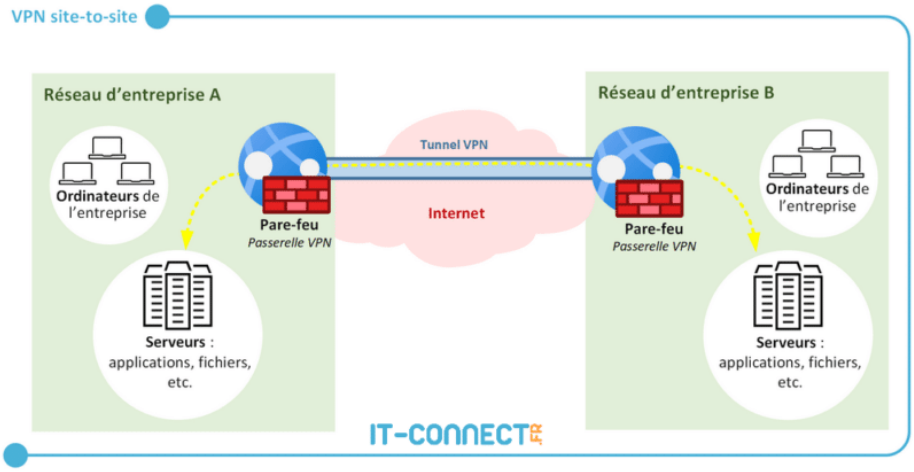

Figure 2.2: Illustration d'une architecture Site-to-Site, source : `https://www.it-connect.fr/les-tunnels-vpn-pour-les-debutants`

2.2.3 VPN grand public

Le VPN grand public, ou VPN commercial, est destiné aux utilisateurs individuels qui souhaitent protéger leur vie privée en ligne et contourner les restrictions géographiques. Ces VPN sont fournis par des services VPN commerciaux et permettent aux utilisateurs de se connecter à des serveurs situés dans différents pays, masquant ainsi leur adresse IP réelle et chiffrant leur trafic Internet.

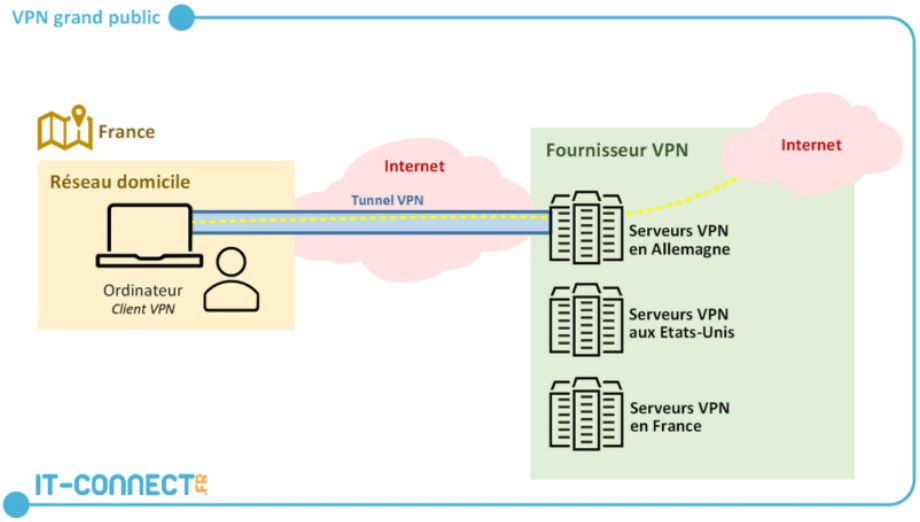

Figure 2.3: Illustration d'une architecture Grand Public, source : `https://www.it-connect.fr/les-tunnels-vpn-pour-les-debutants`

2.3 Protocoles VPN

Les VPN utilisent divers protocoles pour établir et sécuriser les connexions. Ces protocoles sécurisent principalement les connexions entre l'utilisateur et le serveur VPN. Une fois que les données atteignent le serveur VPN, elles sont transmises sur Internet de manière sécurisée, mais la protection dépend également des protocoles utilisés par les services finaux. Parmi les plus courants, on trouve :

- **PPTP (Point-to-Point Tunneling Protocol)** : Un des plus anciens protocoles VPN, facile à configurer mais considéré comme moins sécurisé. Il utilise le protocole GRE (Generic Routing Encapsulation) pour encapsuler les paquets de données. Bien que rapide, il présente des vulnérabilités connues et est généralement déconseillé pour les applications nécessitant une sécurité élevée.

- **L2TP/IPsec (Layer 2 Tunneling Protocol)** : Combine L2TP avec le protocole de sécurité IPsec pour offrir une sécurité renforcée. L2TP crée le tunnel et IPsec assure le chiffrement des données. Ce protocole est plus sécurisé que PPTP, mais peut être plus lent en raison du double encapsulage des données.
- **OpenVPN** : Un protocole open-source très sécurisé et flexible, utilisant SSL/TLS pour le chiffrement. OpenVPN peut fonctionner sur n'importe quel port, ce qui le rend difficile à bloquer par les pare-feu. Il est considéré comme l'un des protocoles VPN les plus sécurisés et est largement utilisé par les services VPN commerciaux.
- **IKEv2/IPsec (Internet Key Exchange version 2)** : Offre une connexion rapide et stable, particulièrement utile pour les appareils mobiles. IKEv2 est connu pour sa capacité à rétablir rapidement les connexions après une interruption, ce qui le rend idéal pour les utilisateurs mobiles qui passent fréquemment d'un réseau à un autre.
- **WireGuard** : Un protocole VPN relativement nouveau qui promet des performances élevées et une sécurité robuste. WireGuard utilise des algorithmes de cryptographie modernes et est conçu pour être plus simple et plus rapide que les protocoles VPN traditionnels. Il est de plus en plus adopté par les services VPN en raison de son efficacité et de sa facilité de déploiement.

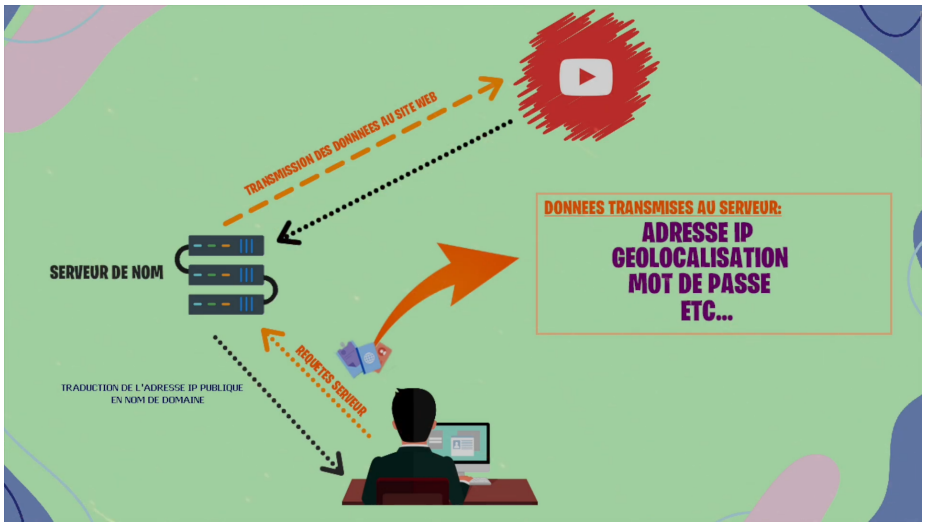

Figure 2.4: Illustration de la navigation sans VPN, source : `https://www.youtube.com/watch?app=desktop&v=IWss3sGV4mI`

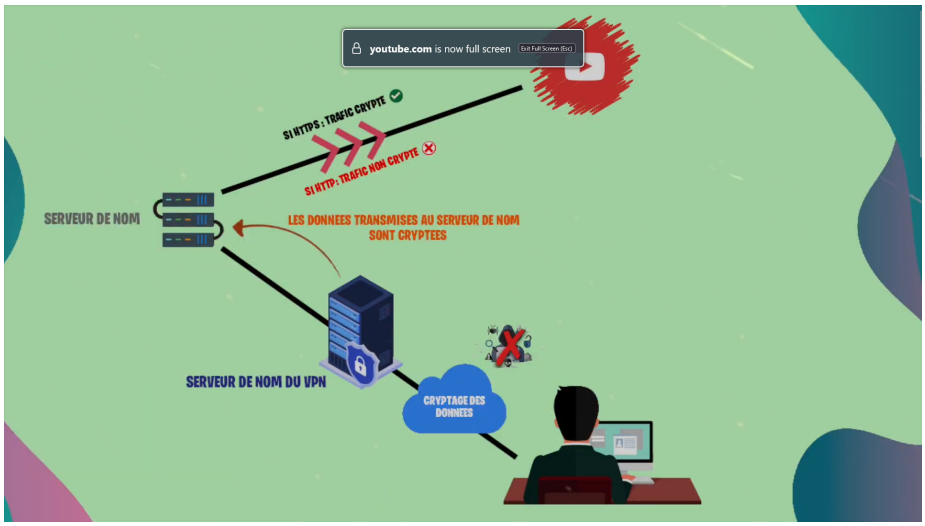

Figure 2.5: Illustration du chiffrement VPN, source : `https://www.youtube.com/watch?app=desktop&v=IWss3sGV4mI`

2.4 Chiffrement

Le chiffrement est une composante essentielle des VPN. Il transforme les données en un format illisible sans la clé de déchiffrement appropriée. Les algorithmes de chiffrement couramment utilisés incluent AES (Advanced Encryption Standard) et RSA (Rivest-Shamir-Adleman). AES est souvent utilisé en raison de sa rapidité et de sa sécurité, tandis que RSA est utilisé pour l'échange de clés sécurisées.

2.5 Création d'un Tunnel VPN

Le processus général de création d'un tunnel VPN est le suivant [Jon24] :

- **Encapsulation** : Les méthodes d'encapsulation courantes comprennent le protocole IP-in-IP et l'encapsulation générique de routage (GRE).
- **Interface réseau virtuelle** : Crée un adaptateur réseau virtuel sur le périphérique client, servant de point d'extrémité du tunnel.
- **Établissement d'un canal sécurisé** : Établit un canal de communication chiffré à l'aide d'algorithmes et de clés négociés. (Avec des protocoles tels que SSL/TLS, IPsec, etc.)
- **Test du tunnel** : Peut envoyer un paquet de test pour vérifier qu'il fonctionne correctement.
- **Mécanismes de maintien en vie** : Établit des protocoles pour maintenir le tunnel, en évitant les dépassements de délai de connexion.
- **Paramètres de qualité de service (QoS)** : Configure les paramètres pour gérer les priorités du trafic dans le tunnel.

Ce processus garantit que les communications entre l'utilisateur et le serveur VPN sont sécurisées et protégées contre les interceptions et les attaques.

Chapter 3

Anonymisation et Confidentialité

3.1 Masquage de l'adresse IP

L'une des principales raisons pour lesquelles les utilisateurs choisissent d'utiliser un VPN est de masquer leur adresse IP réelle. En se connectant à un serveur VPN, l'adresse IP visible par les sites web et services en ligne est celle du serveur VPN, et non celle de l'utilisateur.

3.2 Protection contre la surveillance

Les VPN protègent également contre la surveillance en chiffrant les données. Cela empêche les FAI (fournisseurs d'accès à Internet), les gouvernements et les pirates informatiques de surveiller les activités en ligne de l'utilisateur.

3.3 Contournement des restrictions géographiques

Les VPN permettent de contourner les restrictions géographiques en faisant apparaître l'utilisateur comme s'il se connectait depuis un autre emplacement. Cela est particulièrement utile pour accéder à des contenus restreints ou censurés dans certaines régions.

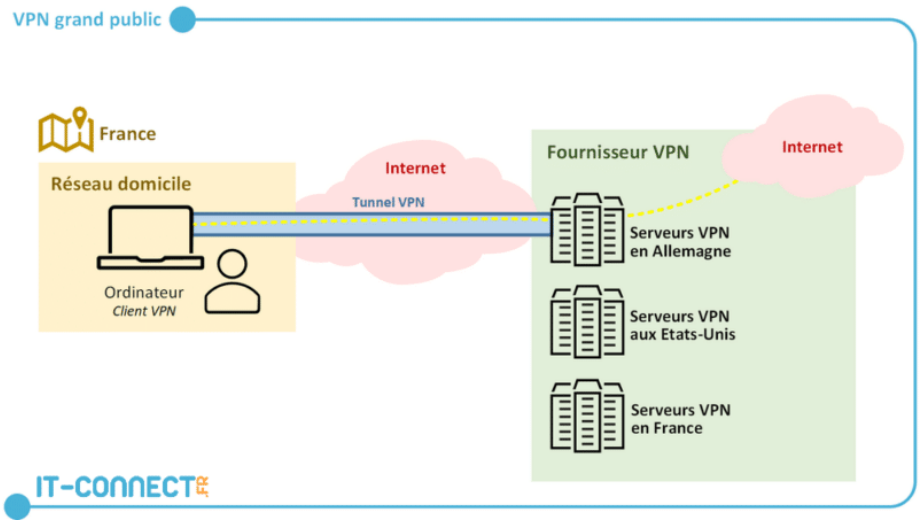

Figure 3.1: Illustation de plusieurs serveurs situés aux quatres coins du monde, source : `https://www.it-connect.fr/les-tunnels-vpn-pour-les-debutants/`

Chapter 4

Sécurité des Réseaux et VPN

4.1 Menaces et Attaques

Les réseaux sont constamment menacés par diverses attaques, telles que les attaques par déni de service (DoS), les attaques de l'homme du milieu (MitM), et les intrusions non autorisées. Les VPN aident à atténuer ces menaces en sécurisant les communications.

4.2 Meilleures Pratiques

Pour maximiser la sécurité lors de l'utilisation d'un VPN, il est recommandé de :

- Utiliser des protocoles de chiffrement forts.
- Choisir des fournisseurs VPN réputés qui ne conservent pas de journaux d'activité.
- Mettre régulièrement à jour les logiciels VPN pour bénéficier des dernières améliorations de sécurité.

Chapter 5

Conclusion

Les VPN sont des outils puissants pour protéger la confidentialité et la sécurité en ligne. En chiffrant les communications et en masquant l'adresse IP de l'utilisateur, ils offrent une couche supplémentaire de protection contre la surveillance et les attaques. Cependant, il est crucial de choisir un service VPN fiable et de suivre les meilleures pratiques pour garantir une sécurité optimale.

Bibliography

[BUR22] Florian BURNEL. *Les tunnels VPN pour les débutants*. 22/03/2022. URL: https://www.it-connect.fr/les-tunnels-vpn-pour-les-debutants/#A_VPN_client-to-site.

[Jon24] JP Jones. *Comment fonctionne un VPN ?* Actualisé le 31/10/2024. URL: https://www.top10vpn.com/fr/cest-quoi-un-vpn/comment-fonctionne-un-vpn/.