VPN Principe et fonctionnement

Table des matières

Introduction

Les VPN (Virtual Private Network) sont des réseaux virtuels privés qui permettent la connexion entre deux réseaux à travers un tunnel sécurisé.
Au départ, il est utilisé dans les entreprises pour relier des sites distants afin de permettre le télétravail.
Ainsi, un employé peut se connecter au réseau d'une entreprise de manière sécurisé.

Les VPN ont pris de l'ampleur depuis Hadopi et des services payants sont proposés dans le but de cacher son IP sur les réseaux P2P.
Si on demande la définition à des internautes, on aura comme réponse "Ce sont des services pour anonymiser est se cacher" alors que ce n'est pas vraiment l'objectif premier.

Cet article explique ce que sont les VPN à travers les exemples et les mises en garde concernant les services payants.
Le but est de répondre aux questions suivantes :

- A quoi ça sert ?
- En quoi un VPN sécurise votre connexion ?
- Comment cacher son adresse IP ?

Qu’est ce qu’un VPN ?

Le VPN est un service qui permet de connecter deux réseaux à travers un tunnel sécurisé.
C'est à dire que les données qui transitent par ce tunnel sont chiffrées afin notamment de protéger contre les attaques MIM (Man in the Middle) (l’homme du milieu).

Les VPN
Voici un schéma classique d'une connexion où un employé se connecte depuis son domicile, un hôtel ou un autre point public.
En se connectant au serveur de son entreprise, un réseau virtuel est créé entre son ordinateur et son entreprise qui permet d'accéder au réseau de l'entreprise.
L'intégralité de la connexion entre ces deux réseaux transite à travers ce réseau privé virtuel.

VPN Principe et fonctionnement

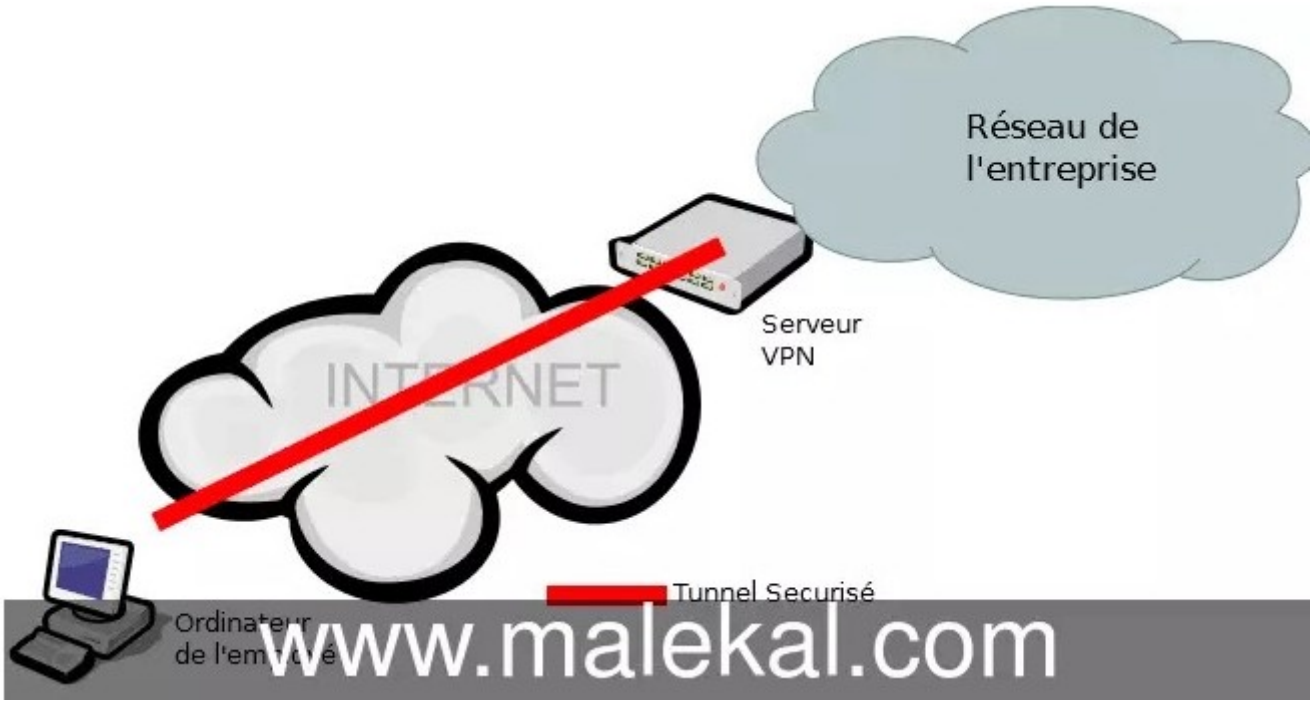


Schéma d'un tunnel sécurisé à travers un VPN

A partir de là, son PC se comporte comme s'il était sur le réseau LAN de l'entreprise (moyennant les autorisations et règles du pare-feu).
Le VPN permet d'établir un tunnel sécurisé entre son PC et le réseau de l'entreprise à travers la connexion internet.
Il relie alors le réseau du PC à celui de l'entreprise.
Cela est très utile pour du télétravail.
Pour ce faire, on a deux parties :

- Le serveur VPN dans l'entreprise
- Le client VPN sur le PC de l'employé

Un client est installé sur l'ordinateur de l'employé qui contacte le serveur de l'entreprise.
Il existe de multiples clients, comme par exemple Cisco AnyConnect.

VPN Cisco Annyconnect

Ou encore en logiciel libre, on peut utiliser OpenVPN.

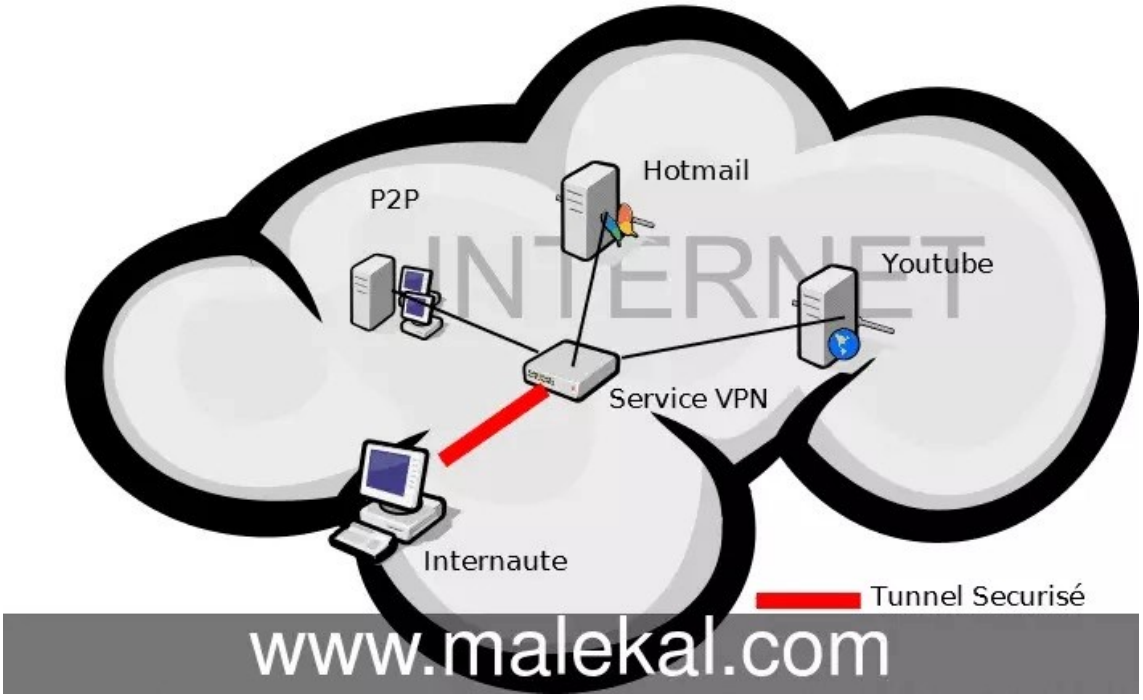
VPN Principe et fonctionnement

OpenVPN pour Linux ou Windows

Fournisseurs VPN grand public

Depuis peu il existe des services VPN grands publics (NordVPN, ExpressVPN, CyberGhost, ProtonVPN, ...).
Ces derniers misent sur la sécurité et l'anonymisation pour vendre des solutions clés en main.
Du moins c'est le discours marketing.

1. L'internaute s'inscrit et paye un abonnement à un fournisseur VPN.
2. Ensuite il installe le client sur son ordinateur ou smartphone Android.
3. Puis il authentification avec son compte.
4. A partir de là, il choisit les serveurs disponibles auxquels se connecter. Généralement, on choisit le serveur selon la localisation géographique.
5. La connexion au serveur s'établit et tout le trafic internet passe alors par le VPN.
6. Les services internet voient alors l'IP du serveur VPN et plus celle la connexion internet et du fournisseur d'accès.
7.



L'idée des VPN grands publics est donc de connecter votre appareil (PC, Smartphone) à un serveur VPN et de rediriger tout votre trafic internet dessus.
Il sert donc d'intermédiaire pour se connecter aux services internet finaux (Youtube, Netflix, site internet, jeux en ligne, etc).
Ainsi ces derniers voient l'adresse IP du serveur VPN et non celle de votre fournisseur d'accès.

La connexion VPN

Ci-dessous on détaille un peu le fonctionnement, mais en gros le principe est de lancer la connexion au réseau privé.
Une fois active, tout le trafic interne passe par ce dernier.

VPN Principe et fonctionnement

L'établissement d’une connexion VPN

En pratique, un serveur VPN a pour but de s'y connecter depuis son ordinateur.

Lors de la connexion au serveur, le client (et donc l'ordinateur) reçoit une adresse locale du réseau virtuel.
C'est celle du tunnel sécurisé.

On peut choisir le pays et un mode de connexion particulier. Il peut y avoir un interface graphique de connexion.
Le fournisseur VPN dispose de serveurs dans différents « datacenters » dans le monde..
Le client VPN s'y connecte.

- L'ordinateur reçoit une IP du réseau virtuelle : 10.8.0.2
- De l'autre côté, le serveur a aussi sa propre adresse dans le réseau virtuel : 10.8.0.1.

Sécurité et anonymisation

Masquer l’adresse IP

Nous venons de voir comment cela fonctionne.
Les solutions proposées visent donc à faire passer tout votre trafic internet par le tunnel sécurisé.
Le serveur et service internet verra alors l'adresse IP du serveur et non votre adresse IP personnelle.
Il s'agit donc ici de masquer votre adresse IP pour un semblant d'anonymisation.

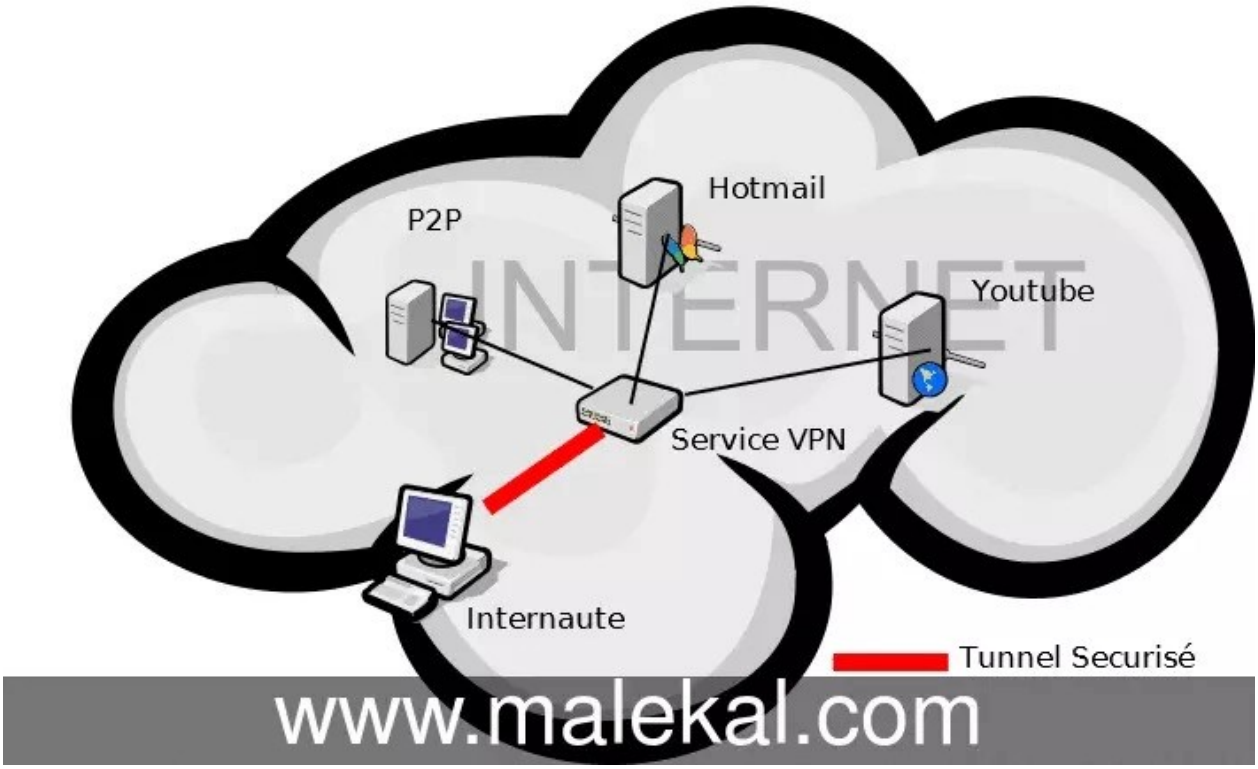


Schéma d'une connexion VPN avec son réseau privé virtuel

Tunnel sécurisé

Le second aspect est que le trafic passe par un tunnel sécurisé qui ne peut pas être lu par un attaquant.
Cela permet donc de chiffrer la connexion ce qui s'avère utile lorsque vous vous connectez depuis une connexion non sûre.
Par connexion non sûre, on parle des connexions publiques et partagées comme les écoles, MacDonald, etc.
Par contre, chez vous cela n'a pas d'intérêt.

En effet, sur ces connexions vous pouvez faire l'objet d'attaque de type MiTM.

Limites de la sécurité des VPN

Il ne sert qu'à masquer son adresse IP et ne protège pas contre toutes les techniques de pistage et suivi d'internautes.

Bien entendu, si tout le trafic passe par le serveur, il est tout à fait possible de "lire" ce qui passe notamment si vous ne vous connectez pas à des sites sécurisés (HTTPs).
Si ces services se connectent comme relai, ils sont aussi capables de suivre votre activité sur internet.
En clair, aucun problème pour opérer du pistage utilisateur et enregistrer votre activité rattaché à votre compte utilisateur.
J'avais déjà mis en garde les utilisateurs avec cet article : Hadopi et connexions VPN : Attention!

Quand utiliser un VPN

Avez-vous besoin d'un VPN ?

Utiliser ce système sur un ordinateur de bureau n'est pas très utile sauf cas particuliers.
Pour un surf au quotidien depuis son ordinateur de bureau personnel chez soi, cela n'apporte aucune sécurité supplémentaire.

Et donc c'est plutôt lorsque vous vous connectez à des réseaux publics et peu sûr que cela s'avère utile.

En général, vous en avez besoin pour les cas suivants :

- Pour les connexions partagées, publiques non sûres.
- Masquer votre adresse IP, par exemple pour les gamers et éviter les attaques DoS (deni de service).
- Changer de zone géographique. Par exemple, vous êtes français et à l'étranger et des services internet (streaming, etc) vous sont interdits. Notez toutefois que certains services bloquent les VPN. Toutefois cela ne fonctionne pas avec Netflix qui bloque les VPN.