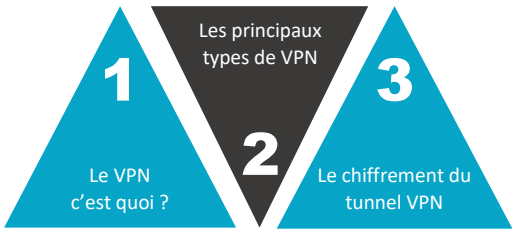
TUTOS-INFO
L'informatique par l'exemple

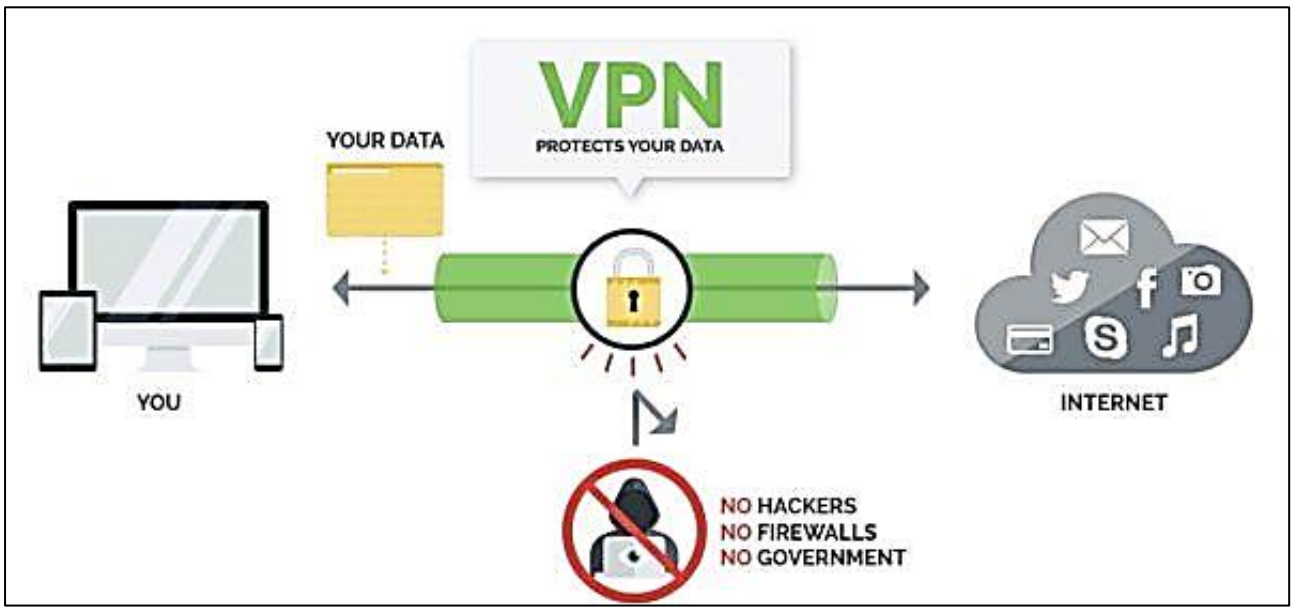
DOCUMENT

Comprendre la notion de VPN



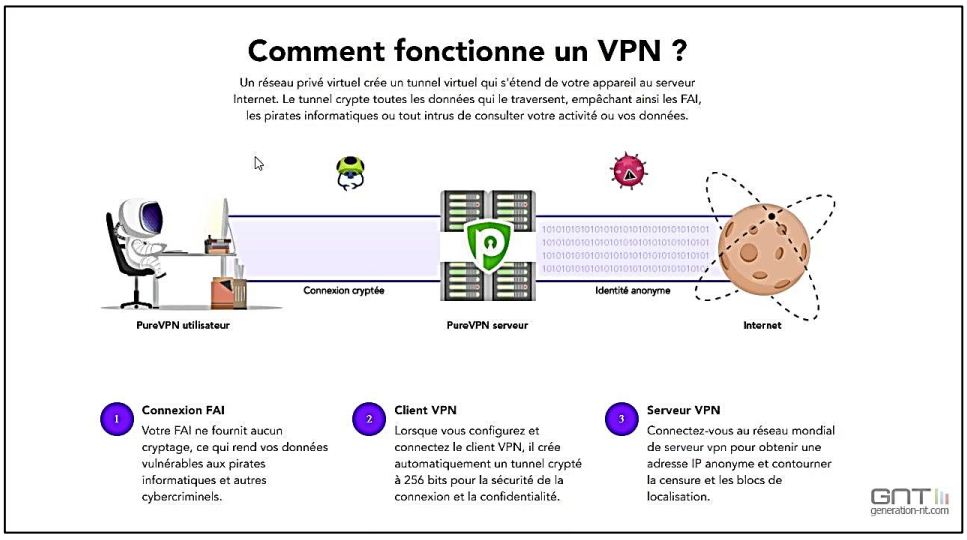
1 – LE VPN C'EST QUOI ?

VPN est l'abréviation de « **Virtual Private Network** » (réseau privé virtuel) et désigne un service qui ***protège votre connexion Internet et votre confidentialité en ligne***. **Il crée un tunnel chiffré** pour vos données et protège votre identité en ligne ***en masquant votre adresse IP***.



Dans un cadre professionnel, le VPN permet, par exemple, de se connecter au serveur de son entreprise de manière sécurisée puisque les données transitent via un tunnel chiffré. Dans certains cas plus « extrêmes », certaines personnes utilisent un VPN pour masquer leur adresse IP et modifier leur emplacement virtuellement de façon à garantir une sécurité supplémentaire pour leurs messages sensibles et leur navigation.

Voici ce qui se passe en coulisses :



1. Lorsque vous vous connectez à un service de réseau privé virtuel, celui-ci ***authentifie votre client auprès d'un serveur VPN***.

2. Le serveur applique ensuite un ***protocole de chiffrement*** à toutes les données que vous envoyez et recevez.

3. Le service VPN crée un « ***tunnel*** » chiffré sur Internet. Cela sécurise les données qui circulent entre vous et votre destination.

4. Pour garantir la sécurité des données, un VPN va « envelopper » vos données dans des ***paquets*** qui seront ***chiffrés par encapsulation***. C'est l'élément central du tunnel VPN, qui assure la sécurité des données pendant leur transfert.

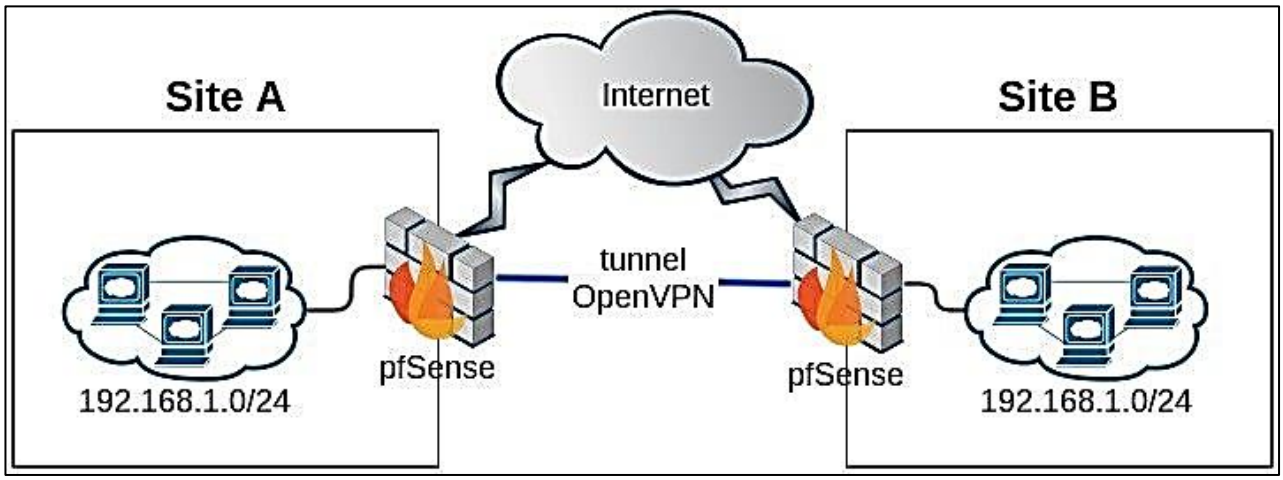
5. Lorsque les données parviennent au serveur destinataire, le paquet externe est supprimé via un processus de déchiffrement.

2 – LES PRINCIPAUX TYPES DE VPN UTILISES EN ENTREPRISE

LE VPN DE TYPE « SITE A SITE »

Les VPN « **site à site** » sont principalement utilisés par les entreprises, en particulier les grandes entreprises.

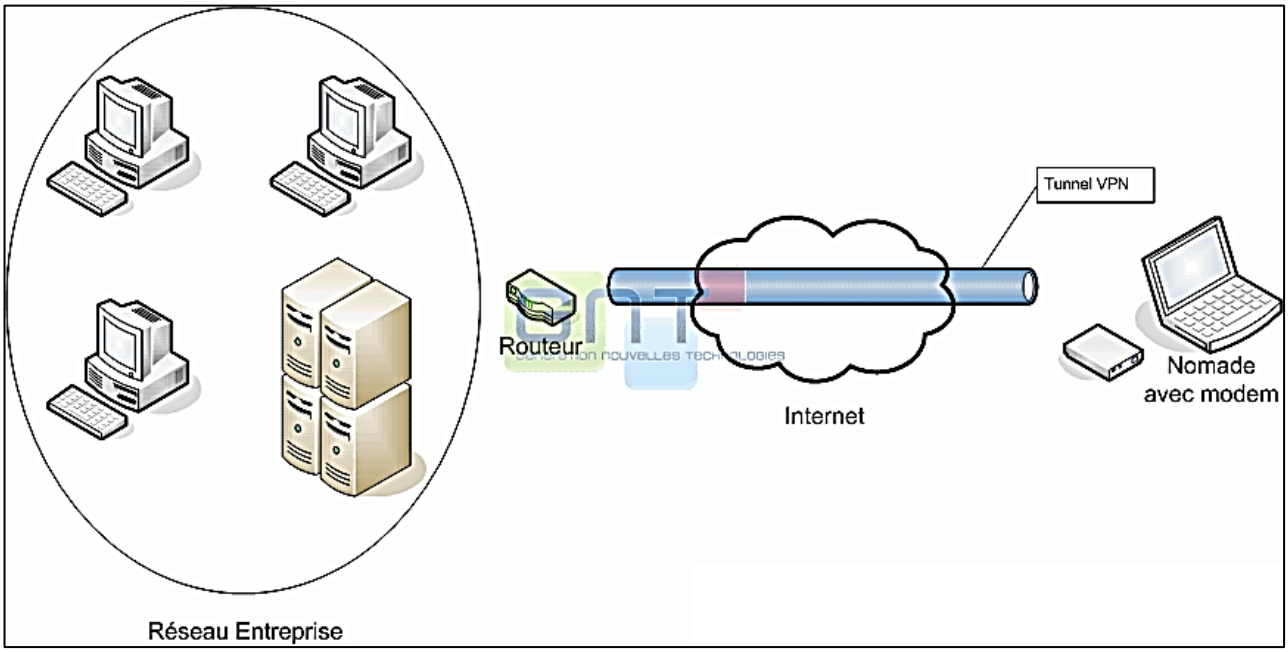
Ils permettent aux utilisateurs, dans certains emplacements sélectionnés, d'accéder aux réseaux des autres sites distants en toute sécurité. C'est un excellent moyen de connecter tous les bureaux et de permettre aux différentes succursales de partager les ressources.



LE VPN DE TYPE « ROAD WARRIOR »

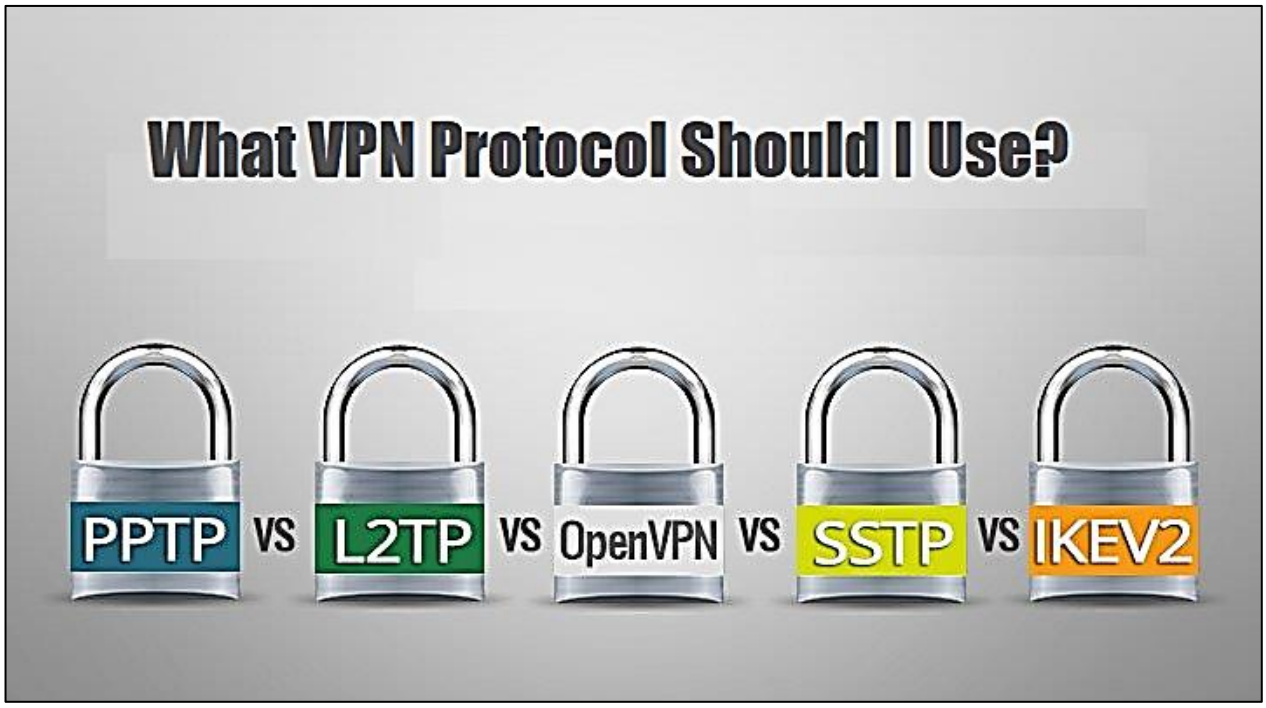
Un **VPN d'accès à distance** (« **road warrior** ») permet aux utilisateurs de se connecter à un réseau distant, généralement en utilisant un logiciel particulier.

Il rend le ***télétravail*** plus sûr et plus facile, car les employés peuvent accéder aux données et aux ressources de l'entreprise où qu'ils soient et en toute sécurité puisque les données transitent via le tunnel chiffré.



3 – LE CHIFFREMENT DU TUNNEL VPN

Les utilisateurs de VPN ont comme principale préoccupation la confidentialité. Il existe différents **protocoles de chiffrement VPN** pami lesquels :



OPEN VPN

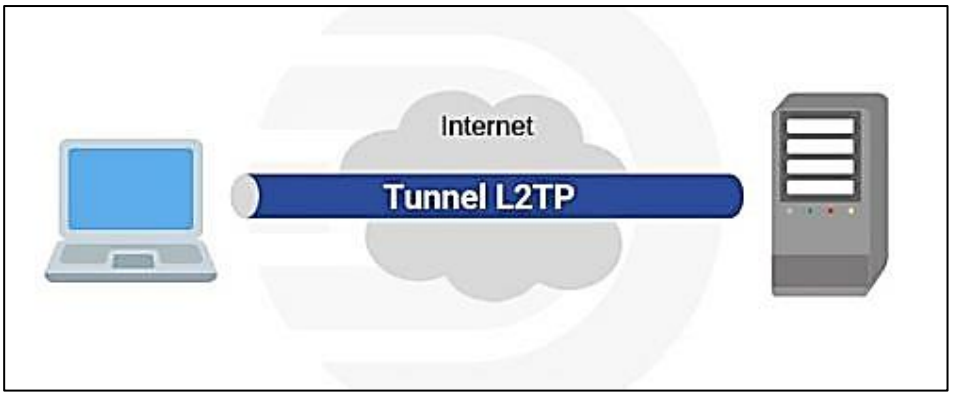
OpenVPN est le **protocole de chiffrement le plus populaire**, actuellement utilisé par la majorité des fournisseurs de VPN dans le monde.

L'une des plus grandes forces d'OpenVPN est qu'il est hautement configurable. Il offre également un bon équilibre entre vitesse et sécurité, car vous pouvez l'utiliser à la fois sur les ports TCP et UDP. Si le port TCP est une option plus sûre, l'UDP est plus rapide.

En ce qui concerne le cryptage, OpenVPN est de premier ordre. Il utilise la bibliothèque OpenSSL, ce qui signifie qu'il a accès à tous les chiffres qui s'y trouvent. Il utilise également un protocole de sécurité personnalisé basé sur SSL/TLS qui fournit un cryptage allant jusqu'à 256 bits.

L2TP

L2TP, pour **Layer 2 Tunnel Protocol**, est un protocole tunnel qui permet aux données de passer d'un réseau à un autre. Contrairement à OpenVPN, L2TP est strictement un protocole de tunneling.



Il ne fournit pas le cryptage à lui seul. Pour cette raison, L2TP est souvent associé à un protocole de cryptage pour assurer la sécurité.

Il a été créé en 1999 et est basé sur deux protocoles de tunneling plus anciens appelés L2F et un protocole PPTP. Nous parlerons de ce dernier point dans une section ultérieure. Bien qu'une nouvelle version du protocole, connue sous le nom de L2TPv3, ait été introduite en 2005 pour ajouter des fonctions de sécurité, L2TP est resté pratiquement le même qu'à ses débuts.

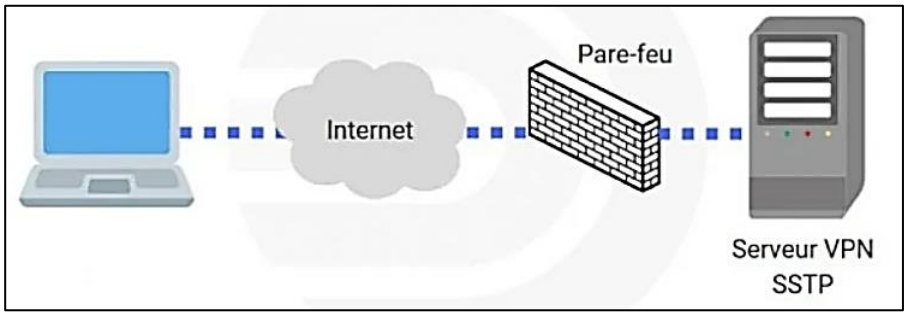
L2TP utilise deux types de paquets : les paquets de contrôle et les paquets de données. Les paquets de contrôle servent à établir une connexion VPN et à ouvrir le tunnel entre vous et le serveur auquel vous accédez. Parce que c'est la fonction centrale du protocole tunneling, L2TP possède des fonctions de fiabilité telles que la confirmation de paquets, liée aux paquets de contrôle.

Les paquets de données n'ont pas de telles caractéristiques. L2TP envoie des paquets dans un datagramme UDP, ce qui signifie qu'ils ne sont pas vérifiés lors de leur envoi. Cela permet une connexion plus rapide, mais moins fiable.

Le problème avec L2TP (Layer 2 Tunneling Protocol) seul est que les paquets que vous envoyez ne sont pas cryptés. Ils sont encapsulés, mais il n'y a pas d'algorithme cryptographique pour cacher les données. Pour cette raison, vous trouverez très probablement ***L2TP associé à IPSec*** dans votre client VPN.

IPSec Layer 2 **fournit le cryptage**, encapsulant le paquet déjà encapsulé lorsqu'il passe par le tunnel L2TP. Cela signifie que les adresses IP source et de destination sont cryptées dans le paquet IPSec, créant ainsi une connexion VPN sécurisée.

SSTP



Le protocole **SSTP** (Secure Socket Tunneling) est une technologie propriétaire de Microsoft qui a été développée pour Windows Vista. Bien qu'il s'agisse d'un protocole développé par Microsoft, SSTP peut également être utilisé sous Linux. Cela dit, il n'est pas supporté sous MacOS et ne le sera probablement jamais.

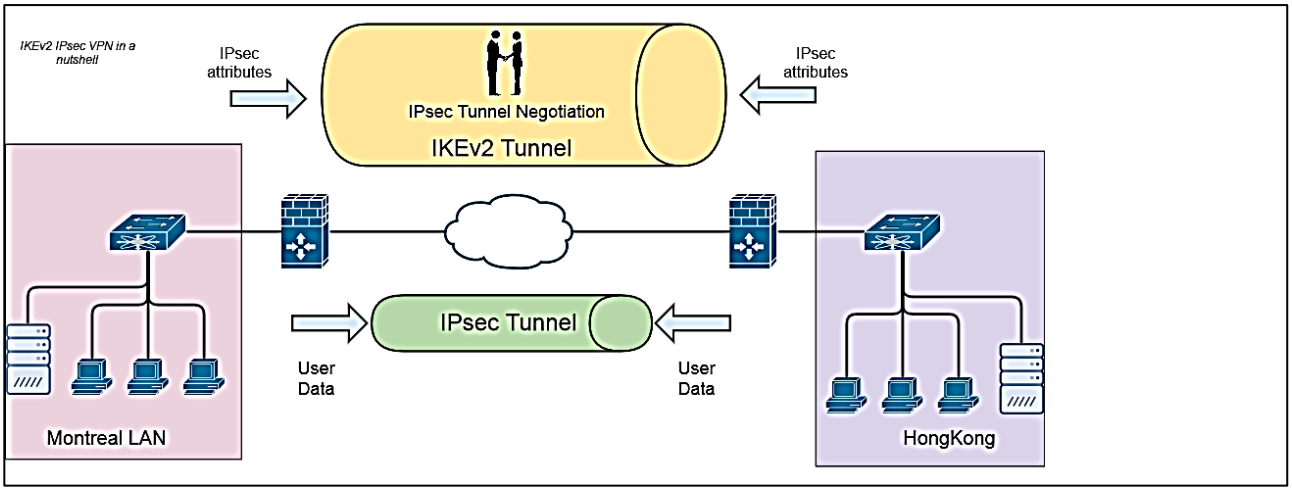
Comme OpenVPN, SSTP permet au trafic point à point de passer par un canal SSL/TLS. Pour cette raison, il a les mêmes avantages et inconvénients que l'utilisation d'un tel système. Par exemple, il utilise SSL/TLS sur le port TCP 443, ce qui le rend excellent pour passer à travers la plupart des pare-feu car le trafic semble normal.

Le problème avec cela, qui est le même problème avec l'utilisation de TCP sur OpenVPN, est que vous êtes vulnérable à une défaillance TCP appelée "TCP Meltdown". TCP doit attendre la confirmation avant de renvoyer un paquet. Il a des fonctions intégrées pour détecter et tenter de résoudre les problèmes si un paquet n'a pas été confirmé.

Dans un tel cas, un paquet TCP d'une couche peut tenter de résoudre un problème, provoquant une surcompensation du paquet de la couche supérieure. Lorsque cela se produit, les performances d'une connexion TCP diminuent considérablement. Cela peut être évité avec OpenVPN en utilisant le port UDP à la place. Avec le SSTP (Secure Socket Tunneling Protocol), le problème est inévitable.

Bien que le SSTP soit disponible dans certaines applications VPN, il est rarement utilisé. Il est mieux que L2TP pour contourner les pare-feu, mais OpenVPN est tout aussi bon. Le problème avec le SSTP est qu'il n'est pas aussi configurable qu'OpenVPN, il est donc plus sensible aux problèmes, comme le TCP Meltdown.

IKEV2



IKEv2 est un ***protocole de tunneling***, qui est **<u>généralement associé à IPSec</u>** pour le chiffrement. Il présente de nombreux avantages, tels que la capacité de restaurer une connexion sécurisée après des interruptions d'Internet.

Il s'adapte également bien à l'évolution des réseaux. Il constitue donc un excellent choix pour les utilisateurs de téléphone qui passent souvent d'une connexion Wi-Fi domestique à une connexion mobile ou se déplacent entre des points d'accès.

Internet Key Exchange est un <u>protocole développé par Microsoft et Cisco</u> en 1998. Techniquement, ce n'est pas un protocole VPN. IKE est utilisé pour configurer une association de sécurité dans la suite de protocoles IPSec. L'association de sécurité comprend des attributs tels que le chiffrement et la clé de cryptage du trafic.

Néanmoins, il est souvent traité comme un protocole VPN, appelé IKEv2, qui est simplement la deuxième version d'IKE, ou IKEv2/IPSec. Contrairement à L2TP/IPSec, qui n'utilise IPSec que pour le cryptage, <u>IKE utilise IPSec</u> pour le transport des données. IKEv2 utilise par ailleurs le port UDP 500.

En ce qui concerne le niveau de sécurité, c'est aussi bon que L2TP ou SSTP, en supposant que vous ayez confiance en Microsoft. Il peut prendre en charge plusieurs versions d'AES et vous le trouverez très probablement jumelé à une clé 128 bits ou 256 bits dans votre application VPN.

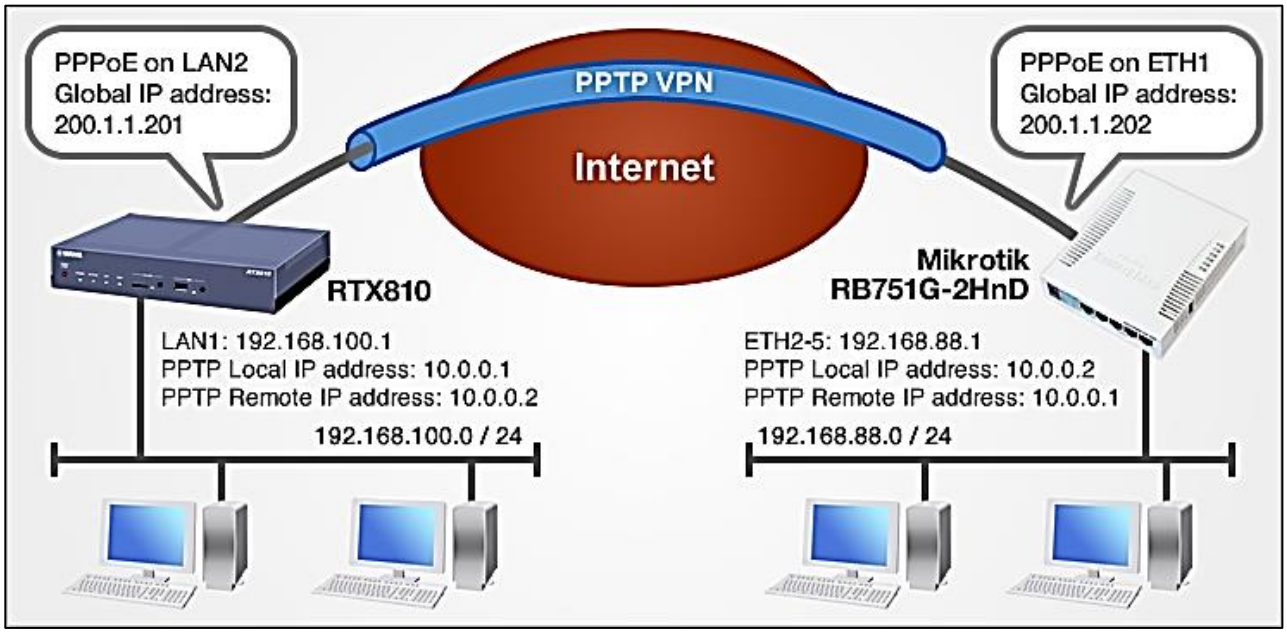
Ce n'est pas juste une autre option, cependant. IKEv2 est généralement le protocole le plus rapide offert par les VPN.

IKE utilise des paquets UDP et commence à créer l'association de sécurité après l'envoi des premiers paquets. L'association de sécurité est ensuite transférée à la pile IPSec, qui commence à intercepter les paquets IP pertinents et à les chiffrer ou les déchiffrer selon le cas.

Pour cette raison, IKE fonctionne bien pour se reconnecter après qu'une connexion VPN ait été interrompue. Sur une connexion filaire ou WiFi, c'est moins préoccupant car ils sont généralement statiques et stables. Pour les appareils mobiles, cependant, IKE est beaucoup plus séduisant.

Les réseaux LTE 3G et 4G évoluent constamment au fur et à mesure que votre téléphone ou votre tablette bouge avec vous. Vous pouvez passer de la 4G LTE à la 3G ou perdre temporairement la connexion. Comme IKE se reconnecte rapidement, c'est un choix idéal sur les appareils mobiles. IKEv2 a même été intégré aux appareils BlackBerry.

PPTP



Point-to-Point Tunneling Protocol est un protocole de tunnelage daté et non sécurisé qui ne devrait pas être utilisé si vous êtes préoccupé par le niveau de sécurité offert. Malgré cela, certains fournisseurs VPN l'incluent encore dans leurs applications.

Le meilleur cas d'utilisation pour PPTP est l'accès externe au réseau interne d'un bâtiment d'entreprise, ce pourquoi les VPN ont été développés en premier lieu. PPTP ne spécifie pas le cryptage. Il s'appuie plutôt sur le protocole point à point pour exécuter des fonctions de sécurité.

En raison de la forme basique de cryptage, PPTP est rapide. C'est presque la même vitesse que votre connexion Internet normale. Dans un cas d'utilisation personnelle, c'est à peu près aussi sûr que votre connexion Internet normale. C'est pourquoi nous vous recommandons d'utiliser un protocole PPTP uniquement si vous faites quelque chose que vous ne pouvez pas faire sans VPN, comme l'accès à un réseau externe.

Cependant, ne vous attendez pas à ce que cette connexion soit sûre. Il existe de nombreux outils pour casser les tunnels PPTP, dont certains peuvent simplement extraire la clé de la méthode d'authentification et d'autres peuvent trouver la clé en quelques heures en utilisant une attaque de force brute.

De plus, *la NSA est connue pour espionner activement les réseaux PPTP* en raison de sa faible sécurité. A moins que vous n'ayez une raison spécifique de l'utiliser, nous vous recommandons d'éviter le PPTP, même si c'est une option disponible dans votre application VPN.

IPSEC

IPsec est l'abréviation de Internet Protocol Security (protocole de sécurité internet). IPsec est un protocole VPN utilisé pour sécuriser les communications par internet sur un réseau IP. Un tunnel est mis en place dans un endroit éloigné et vous permet d'accéder à votre site central. Un IPsec sécurise le protocole de communication internet en vérifiant chaque session et avec un cryptage individuel des paquets de données pendant toute la connexion.

Il y a deux modes d'opération dans un VPN IPsec. Le mode transport et le mode tunnel. Les deux modes servent à protéger le transfert des données entre deux réseaux différents. Avec le mode transport, le message dans le paquet de données est crypté. Avec le mode tunnel, le paquet de données entier est crypté.

Un des avantages d'un VPN IPsec, c'est qu'il peut être utilisé en plus d'autres protocoles de sécurité pour un système de sécurité renforcé. Si un IPsec est un bon VPN à avoir, un des désavantages associés à l'utilisation de ce protocole est la grosse quantité de temps que le client doit passer à l'installer avant de pouvoir l'utiliser.

SSL ET TLS

SSL signifie Secure Sockets Layer et TLS Transport Layer Security. Ils fonctionnent ensemble comme un seul protocole. Les deux sont utilisés pour construire une connexion VPN. Dans cette connexion VPN, le navigateur internet sert de client et l'accès utilisateur est restreint à certaines applications seulement plutôt qu'un réseau entier. Les protocoles SSL et TLS sont principalement utilisés par des sites de vente en ligne et des fournisseurs de service.

Un VPN SSL et TSL vous offre une session sécurisée du navigateur de votre PC au serveur de l'application. C'est parce que les navigateurs internet passent facilement au SSL sans intervention de l'utilisateur. Les navigateurs web possèdent déjà SSL et TSL de façon intégrée. Les connexions SSL commencent par https au début de l'URL au lieu de http.

MPLS VPN

Un Multi-Protocol Label Switching (Multi-protocole de commutation d'étiquettes), ou un VPN MPLS, est ***utilisé pour des connexions de type Site-à-Site***. C'est principalement dû au fait que les MPLS sont très flexibles et adaptables. Le MPLS est une ressource normalisée utilisée pour accélérer le processus de distribution de paquets de réseau avec de multiples protocoles.

Les VPN MPLS sont des systèmes basés sur fournisseurs d'accès. On dit ça quand un site ou plusieurs sont connectés pour former un VPN avec le même fournisseur d'accès ISP.

Toutefois, le plus gros inconvénient des VPN MPLS c'est que le réseau n'est pas facile à mettre en place, par rapport aux autres VPN. Il est aussi très difficile à modifier. De plus, les VPN MPLS sont souvent bien plus **chers**.

HYBRIDE VPN

Un VPN hybride ***combine à la fois un MPLS et un IPsec***. Habituellement, ces deux types de VPN sont utilisés séparément. Mais il est possible de les utiliser en même temps. On peut par exemple utiliser le VPN IPsec comme soutien du VPN MPLS. Les VPN IPsec nécessitent de l'équipement du côté du client, comme mentionné ci-dessus. Habituellement, il faut un routeur ou un appareil de sécurité multi-tâches. Grâce à ces appareils, les données sont cryptées et forment le tunnel VPN comme évoqué précédemment. Les VPN MPLS sont utilisés par un porteur, ce qui signifie que l'équipement doit être dans le réseau du porteur.

Pour réussir à connecter ces deux VPN, un portail est établi pour éliminer le tunnel IPsec mais aussi le relier au VPN MPLS tout en préservant la sécurité qu'offrent ce réseau. Les VPN hybrides sont utilisés par les entreprises car c'est le choix le plus approprié pour leurs sites. Les MLPS ont beaucoup d'avantages par rapport aux connexions internet publiques, mais le coût est élevé. Utiliser un VPN hybride vous permet d'accéder au site central via un site secondaire. Les VPN hybrides coûtent assez cher mais sont très flexibles.

En conclusion, il est difficile de faire le bon choix de VPN. Pour pouvoir déterminer quel VPN est fait pour vous, commencez par définir le type de sécurité que vous souhaitez avoir. Le choix de VPN peut varier selon si vous êtes étudiant, auto-entrepreneur, ou si vous possédez une grosse entreprise avec plusieurs bureaux. Vous devriez également déterminer à quel point votre sécurité doit être développée pour savoir s'il vous faudra quelque chose de complexe comme un VPN hybride. Le coût total entre également en compte dans cette décision. Combien d'argent êtes-vous prêt à dépenser pour la sécurité de votre connexion internet ? Une fois que vous aurez répondu à ces questions, il vous sera plus facile de choisir quel type de VPN est fait pour vos besoins.