Internet.

Les V. P. N.

Qu'est-ce qu'un V. P. N. ?

Un VPN ("**Virtual Private Network"** ou réseau privé virtuel**)** permet d'établir une connexion réseau protégée lors de l'utilisation de réseaux publics.
Un VPN est donc un procédé de communication qui crée une connexion sécurisée entre des appareils, via Internet. Les VPN servent à transmettre des données de manière sûre et anonyme sur des réseaux publics. Ils fonctionnent en masquant les adresses IP des utilisateurs et en chiffrant les données de manière à ce qu'elles soient illisibles pour toute personne non autorisée à les recevoir. Ce chiffrement est effectué en **temps réel**.
Beaucoup de VPN relient différents sites d'entreprises comme s'il s'agissait de liaisons de point à point, inaccessibles à d'autres internautes. Cependant, en utilisant un routeur, celles-ci peuvent généralement accéder à différents sites Internet par une passerelle bien protégée. Ces VPN sont généralement appelés VPN professionnels.

Historique des VPN

Depuis que les humains utilisent Internet, un mouvement s'est créé visant à protéger et à chiffrer les données des navigateurs Internet. Le Département de la Défense des États-Unis a déjà participé à des projets visant à chiffrer les données de communication par Internet dans les années 1960.

Les prédécesseurs du VPN

Leurs efforts ont abouti à la création d'**ARPANET** (Advanced Research Projects Agency Network), un réseau de commutation de paquets, qui a, à son tour, entraîné le développement du protocole Transfert Control Protocol/Internet Protocol (TCP/IP) (protocole de contrôle de transmissions/protocole Internet).

Le protocole **TCP/IP** comportait quatre niveaux : **lien, internet, transport et application**. Au niveau de l'internet, les réseaux et les appareils locaux pouvaient être connectés au réseau universel, et c'est là que le risque d'exposition est devenu évident. En 1993, une équipe d'AT&T Bell Labs et de l'université de Columbia a finalement réussi à créer une sorte de première version du VPN moderne, connue sous le nom de swIPe : protocole de chiffrement IP de logiciel.

L'année suivante, Wei Xu a conçu le réseau IPSec, un protocole Internet de sécurité qui authentifie et chiffre les paquets d'informations partagés en ligne. En 1996, un employé de Microsoft du nom de Gurdeep Singh-Pall a créé le protocole PPTP (Peer-to-Peer Tunneling Protocol).

Les premiers VPN

Au moment même où Gurdeep Singh-Pall concevait le protocole PPTP, Internet se popularisait, et le besoin de systèmes de sécurité sophistiqués prêts à être utilisés par les consommateurs s'est fait sentir. Les logiciels antivirus de l'époque parvenaient à empêcher les logiciels malveillants et les logiciels espions d'infecter un système informatique. Par contre, les particuliers et les entreprises réclamaient également des logiciels de chiffrement capables de masquer leurs données et leur historique de navigation sur Internet.

Les premiers VPN ont pris leur essor au début des années 2000, mais ils n'étaient généralement utilisés que par les entreprises. Toutefois, après une vague d'atteintes à la sécurité, notamment au début des années 2010, le marché grand public des VPN a commencé à prendre de l'ampleur.

A quoi sert un VPN "grand public" ?

Les services de VPN sont principalement utilisés pour envoyer des données en toute sécurité sur Internet. Les trois principales fonctions des VPN grand public sont les suivantes :

1. Confidentialité

Sans réseau privé virtuel, vos données personnelles telles que les mots de passe, les informations relatives aux cartes de crédit et l'historique de navigation peuvent être enregistrées et vendues par des tiers. Les VPN utilisent le chiffrement pour préserver la confidentialité de ces informations, surtout lors de la connexion à des réseaux Wi-Fi publics. Cependant, de plus en plus de sites utilisent aussi le chiffrement lors de connexions sécurisées (indiquées par "https" et par un cadenas).

2. Anonymat

Votre adresse IP contient des informations sur votre localisation et votre activité de navigation. Tous les sites web sur Internet suivent ces données à l'aide de cookies et de technologies similaires. Ils peuvent vous identifier à chaque fois que vous les consultez. Une connexion VPN permet de masquer votre adresse IP afin que vous restiez anonyme sur Internet. Cependant, votre fournisseur d'accès (FAI) sait tout de même quand vous naviguez sur Internet ; un VPN lui masquera le nom des sites Internet que vous visitez. Votre fournisseur d'Internet le saura bien évidemment (indispensable pour vous connecter aux sites demandés) et celui-ci ne sera pas forcément plus fiable que votre fournisseur d'accès.
En conclusion : Un VPN vous procurera l'anonymat sur les sites visités, mais reportera vos données de navigation de chez votre fournisseur d'accès chez votre fournisseur de VPN.

3. Sécurité

Un service VPN utilise le chiffrement pour protéger votre connexion Internet contre tout accès non autorisé. Il peut également faire office de mécanisme d'arrêt, en mettant fin à des programmes présélectionnés en cas d'activité suspecte sur Internet. Cela réduit la probabilité que les données soient compromises. Ces fonctions permettent aux entreprises de donner un accès à distance aux utilisateurs autorisés sur leurs réseaux professionnels.

Comment fonctionne un VPN ?

N'oubliez pas que **seules les données Internet sont chiffrées**. Les données qui n'utilisent aucune connexion cellulaire ou Wi-Fi ne circulent pas sur Internet. Par conséquent, votre VPN ne chiffrera pas vos appels vocaux ni vos messages habituels (SMS ou MMS) !

Une connexion VPN redirige les paquets de données de votre machine vers un autre serveur distant avant de les envoyer à des tiers sur Internet. Les principes clefs de la technologie VPN sont les suivants :

Protocole de tunneling

Un réseau privé virtuel crée principalement un tunnel de données sécurisé entre votre machine locale et un autre serveur VPN situé à plusieurs kilomètres. Lorsque vous êtes en ligne, ce serveur VPN devient la source de toutes vos données. Dès lors, d'autres tiers ne peuvent plus voir la source de votre trafic Internet. Votre FAI le peut, mais ne peut généralement décoder vos données chiffrées.

Chiffrement

Il existe différents protocoles VPN ou méthodes de sécurité. Le plus ancien est le **PPTP** (protocole de tunnellisation point à point), qui est encore utilisé aujourd'hui, mais qui est largement considéré comme l'un des moins sûrs. Les autres sont **IKEv2**, **L2TP/IPSec**, **SSL**, **TLS**, **SSH**, **Wireguard** et **OpenVPN**. En tant que protocole open source, OpenVPN est l'un des plus sûrs car toute vulnérabilité dans sa programmation est rapidement corrigée.
Les protocoles VPN comme IPSec brouillent vos données avant de les envoyer dans le tunnel de données. IPsec est une suite de protocoles de sécurisation des communications IP (Internet Protocol) par authentification et cryptage de chaque paquet IP d'un flux de données. Le service VPN agit comme un filtre, rendant vos données illisibles d'un côté et ne les décodant que de l'autre. Cela empêche l'utilisation abusive des données personnelles, même dans le cas où votre connexion réseau deviendrait compromise. Le trafic réseau est beaucoup moins vulnérable aux attaques et votre connexion Internet est plus sécurisée. Notez que la policez ou l'armée disposent de moyens de décodage très performants et qu'il vaut donc tout de même mieux éviter de vous livrer à des trafics frauduleux !
Privilégiez la norme AES-256 (norme de chiffrement avancé), qui est la norme de chiffrement la plus élevée à ce jour, pratiquement impossible à déchiffrer.

Les doubles VPN sont un type de service VPN qui utilise le chaînage de serveurs VPN pour acheminer le trafic Internet à travers deux réseaux VPN distincts. Également appelés **VPN à double saut** ou **VPN multisauts**, les VPN à double saut chiffrent deux fois les données du réseau, offrant ainsi une connexion VPN encore plus confidentielle et plus sûre. Ces VPN sont plutôt utilisés pour des communications professionnelles.

Pourquoi utiliser un VPN ?

Pour un accès sécurisé à l'Internet public

Les réseaux privés virtuels rendent l'activité web en déplacement plus sûre pour tout le monde. Aujourd'hui, nous sommes habitués à lire des articles d'actualité au café, à consulter nos e-mails au supermarché ou à nous connecter à nos comptes bancaires sur nos appareils mobiles. Ce type de connexion Internet est extrêmement vulnérable au piratage, car l'activité web se déroule sur le Wi-Fi public. L'utilisation de services VPN lors de la connexion à des hotspots Wi-Fi publics non sécurisés permet de protéger à la fois vos données et votre appareil.

Pour garder votre historique de recherche privé

Ce n'est pas un secret que votre fournisseur de services Internet et votre navigateur web suivent votre historique de recherches. Ils peuvent vendre votre historique de navigation à des fins de marketing et ne s'en privent pas. Par exemple, la recherche d'articles sur les fuites de robinets

peut déboucher sur des annonces ciblées concernant des plombiers locaux. Une connexion VPN va alors vous protéger contre l'utilisation abusive de ces données.

Pour accéder aux services de streaming dans le monde entier

Lorsque vous voyagez en dehors de votre pays d'origine ou que vous désiriez voir des contenus d'autres pays, inaccessibles depuis le vôtre, il se peut que ces services de streaming ne soient pas disponibles en raison de conditions contractuelles et de réglementations. Votre connexion VPN vous permet de changer l'adresse IP visible de votre pays d'origine et d'accéder à vos émissions préférées où qu'elles se trouvent, quoique de plus en plus de ces sites repèrent les adresses IP des fournisseurs de VPN et refusent de leur envoyer des données en streaming !

Pour protéger votre identité

En préservant votre anonymat, les services VPN vous protègent de la surveillance numérique. Ils empêchent que vos commentaires et conversations sur Internet soient suivis et préservent votre droit à la liberté d'expression, **à condition de ne pas utiliser votre véritable identité sur les plateformes de réseaux sociaux !** M'enfin . . .

Limites d'anonymat des VPN

Pas de protection contre les cookies : Si la protection par VPN vous permet de préserver votre confidentialité et de chiffrer votre trafic, il n’est pas possible pour un VPN de bloquer les cookies, dont certains sont nécessaires au bon fonctionnement des sites. Les cookies de suivi peuvent toujours être stockés dans votre navigateur et permettre de vous identifier. Vous pouvez supprimer les cookies de suivi ou utiliser un navigateur privé, pour empêcher le suivi sur le web.

Pas de confidentialité totale : Alors qu’un VPN cache vos données à votre fournisseur d’accès à Internet, les gouvernements, la police ou l'armée, les pirates et autres fouineurs, **et le fournisseur de VPN** lui-même, peuvent voir votre activité en ligne s’ils le souhaitent. C’est pourquoi il est très important de choisir un fournisseur de VPN digne de confiance qui ne garde pas de trace de vos habitudes de navigation sur Internet et ne les revend pas !

Comment configurer un VPN ?

Il existe 2 manières courantes d'accéder aux services VPN pour les particuliers (grand public) :

1. Utiliser un fournisseur de VPN

Vous pouvez choisir un service VPN auquel vous pouvez accéder soit à partir de votre navigateur, soit en téléchargeant une application ou un logiciel sur votre appareil. Il s'agit de services par abonnement qui sont généralement facturés sur la base de l'utilisation par appareil. Dès lors, ils peuvent être assez coûteux à mettre en place. En outre, chaque appareil doit être configuré individuellement. Il en existe cependant de gratuits souvent fournis par les producteurs d'antivirus.

2. Utiliser un routeur VPN (ou pas !)

Pour cela, il est nécessaire d'acheter un routeur avec une connexion VPN préinstallée ou d'installer soi-même un logiciel VPN sur son routeur domestique. L'avantage de cette approche

est que chaque appareil accédant à Internet via ce routeur est automatiquement protégé. La plupart des box permettent également de configurer un VPN (voire deux pour les box "pro"), mais elles ne chiffrent pas toujours les données, auquel cas il faudra installer un logiciel de cryptage dans les appareils s'y connectant.

Comment choisir un fournisseur de VPN ?

Avec autant d'options à disposition, le choix d'un bon service VPN peut certes être quelquefois difficile. . .

1. Politiques de journalisation

Les meilleurs fournisseurs de VPN ont des politiques d'enregistrement minimales ou nulles pour éviter les utilisations hors limites des données de leur côté.

2. Logiciels mis à jour

Les meilleures connexions VPN utilisent le protocole de tunneling le plus récent. Le protocole OpenVPN offre une sécurité plus éprouvée que les autres. Il s'agit d'un logiciel open source compatible avec les principaux systèmes d'exploitation.

3. Limite de bande passante

Tous les services présentent des limites d'utilisation des données. Ne comptez pas utiliser un débit de 8 Gbit/s ! Vous devrez choisir un fournisseur de VPN qui répond à vos besoins en matière de données tout en respectant votre budget. Evidemment, les fournisseurs de VPN gratuits ne sont pas ceux offrant la meilleure bande passante.

4. Emplacement des serveurs VPN

Vous devez vous assurer que votre fournisseur de VPN dispose d'un serveur situé dans le pays où vous avez besoin d'un accès Internet privé. Quoique de plus en plus de fournisseurs de VPN ont des accès dans différents pays.

Comment choisir entre les VPN payants et les VPN gratuits ?

Les VPN gratuits sont utiles si vous ne disposez que d'un budget limité. Néanmoins, il est important de noter que la principale source de revenus des fournisseurs de VPN gratuits est la publicité. Vous pouvez donc vous attendre à des publicités ciblées ou de vente des données dont les conditions seront cachées dans les conditions générales.

La plupart des VPN gratuits :

- ne proposent pas les protocoles VPN les plus récents ;
- ne proposent pas de support technique de qualité ;
- ont une bande passante faible et un débit plus lent pour les utilisateurs gratuits
- ont une distribution géographique limitée de serveurs VPN.

Alors, V. P. N. "grand public", ou pas ?

En conclusion, une personne qui utilise Internet pour des activités courantes comme la lecture d'emails, le shopping en ligne, ou le streaming de contenus locaux, et qui n'a pas de préoccupations particulières en matière de confidentialité (ne vit pas dans un pays à forte censure ou répression), l'investissement dans un VPN payant n'est pas prioritaire. Il est important de peser les avantages par rapport aux coûts et à la complexité avant de prendre une décision.

Pourquoi les entreprises utilisent-elles des VPN ?

Les VPN constituent un moyen rentable, rapide et sûr de connecter les utilisateurs distants au réseau du bureau. Étant donné que les connexions VPN se font généralement sur l'Internet public, elles sont très souvent moins coûteuses que les liaisons WAN (réseau étendu) dédiées ou les liaisons longue distance. Les connexions VPN offrent aux entreprises un accès Internet privé à large bande passante par rapport aux liaisons LAN ou WAN (réseau étendu) dédiées et coûteuses ou aux liaisons longue distance.

Quels types de VPN d'entreprises existe-t-il ?

Il existe de nombreux types de VPN, mais il y en a trois principaux types :

Les VPN SSL

Bien souvent, tous les employés d'une entreprise n'ont pas accès à un ordinateur portable de l'entreprise qu'ils peuvent utiliser pour travailler à domicile. Lors de la crise du coronavirus au printemps 2020, de nombreuses entreprises ont été confrontées au problème lié au manque d'équipements pour leurs employés. Dans ce cas, les employés ont souvent recours à un appareil privé (PC, ordinateur portable, tablette, téléphone mobile). Dans ce cas, les entreprises se tournent vers une solution **SSL-VPN**, qui est généralement mise en œuvre par le biais d'un boîtier matériel correspondant.

La condition préalable est généralement l'utilisation d'un navigateur compatible avec le format HTML-5, qui est nécessaire pour appeler la page d'identification de l'entreprise. Les navigateurs compatibles avec le format HTML-5 sont compatibles avec pratiquement tous les systèmes d'exploitation. L'accès est protégé par un nom d'utilisateur et un mot de passe.

Les VPN de site à site

Un **VPN site à site** est essentiellement un réseau privé destiné à camoufler les intranets privés et à permettre aux utilisateurs de ces réseaux sécurisés d'accéder aux ressources de chacun.
Un VPN site à site est utile si vous disposez de plusieurs sites au sein de votre entreprise, chacun ayant son propre réseau local (LAN) connecté au WAN (Wide Area Network). Les VPN site à site sont également utiles si vous disposez de deux intranets distincts entre lesquels vous souhaitez envoyer des fichiers sans que les utilisateurs d'un intranet n'accèdent explicitement à l'autre.

Les VPN site à site sont principalement utilisés par les grandes entreprises. Leur mise en œuvre est complexe et n'offre pas la même souplesse que dans le cas des VPN SSL. Cependant, ils constituent le moyen le plus efficace de sécuriser les communications au sein de grands services

et entre ceux-ci. Ces VPN sont presque toujours protégés par des chiffrements multi-sauts réalisés par les routeurs des entreprises elles-mêmes.

Les VPN de client à fournisseur

La connexion via un **client VPN** peut être illustrée comme si vous connectiez votre PC à domicile à l'entreprise au moyen d'un câble d'extension. Les employés peuvent se connecter au réseau de l'entreprise depuis leur domicile via la connexion sécurisée et agir comme s'ils étaient assis au bureau. Toutefois, un client VPN doit d'abord être installé et configuré sur l'ordinateur.

Cela signifie que l'utilisateur établit une connexion directe par l'intermédiaire de son fournisseur VPN. Cela permet essentiellement d'éviter l'étape de la tunnellisation VPN. Ainsi, au lieu d'utiliser le VPN pour créer un tunnel de chiffrement afin de camoufler la connexion Internet existante, le VPN peut automatiquement chiffrer les données avant de les transmettre à l'utilisateur.

Il s'agit d'une forme de VPN de plus en plus courante qui s'avère particulièrement utile pour les fournisseurs de réseaux Wi-Fi publics non sécurisés. Ce type de VPN chiffre les données jusqu'au fournisseur et empêche ainsi des tiers d'accéder à la connexion réseau et de la compromettre. Il empêche également les FAI d'accéder à toute donnée chiffrée (quelle qu'en soit la raison) et contourne la plupart des restrictions imposées à l'accès de l'utilisateur à Internet (par exemple, si le gouvernement de ce pays limite l'accès à Internet).

L'avantage de ce type d'accès VPN est une plus grande efficacité et un accès universel aux ressources de l'entreprise. À condition qu'un système téléphonique approprié soit disponible, l'employé peut, par exemple, se connecter au système à l'aide d'un casque et agir comme s'il était sur le lieu de travail de son entreprise. Par exemple, les clients de l'entreprise ne peuvent même pas distinguer si l'employé travaille dans l'entreprise ou à son domicile.

Bibliographie :

https://www.01net.com/vpn/vpn-pour-nuls/