Association Loisirs et culture

Tout ce que vous avez toujours voulu savoir sur les réseaux privés virtuels (VPN) sans jamais oser le demander.

Jean Marie Herbaux

Table des matières

Qu'est-ce qu'une connexion VPN et pourquoi est-ce un sujet de discussion si fréquent ? Ce terme s'immisce dans toutes les conversations sur Internet dernièrement, et pour cause : si les VPN n'étaient autrefois que des gadgets de fiction, ils représentent désormais des outils indispensables. Dans le cadre de l'utilisation la plus simple, les VPN protègent votre *confidentialité en ligne* afin que vous ne soyez pas ciblé, suivi ou discriminé en raison de votre emplacement géographique.

Qu'est-ce qu'un VPN ?

Un VPN, ou « réseau privé virtuel », est une connexion chiffrée et sécurisée entre deux réseaux ou entre un utilisateur et un réseau. Un VPN vous permet de naviguer sur le Web en toute confidentialité.

Comment fonctionne-t-il ?

Pour mieux comprendre son fonctionnement, il suffit de s'imaginer qu'Internet est une autoroute virtuelle et que nous assurons sa sécurité. Nous consultons nos sites Web préférés, effectuons des achats, vérifions nos comptes bancaires et nous informons sur les actualités via nos médias de prédilection, jouons à des jeux, et bien plus encore.
Sans VPN, quiconque le souhaite est en mesure de vous suivre sur ces autoroutes numériques. Les pirates peuvent ainsi connaître vos activités en ligne, votre identité, vos sites préférés : il leur suffit de se servir. Pire, ils peuvent vous suivre jusque chez vous. Vous êtes facilement pistables.

Un VPN fonctionne comme une cape d'invisibilité en assurant votre anonymat. « Vous troquez ainsi votre moto de surveillance contre une voiture de location aux vitres teintées ». Vous bénéficiez de la protection du chiffrement des données et êtes cachés derrière une « adresse IP » fictive.
Le VPN chiffre toutes vos activités en ligne, tout ce que vous envoyez et ce que vous recevez. En accédant à Internet uniquement via un VPN, la source de votre connexion (IP) indique l'un des nombreux routeurs du VPN, et non le vôtre.

Pourquoi avons-nous besoin d'un VPN ?

Maintenant que vous savez ce qu'est un VPN, étudions les raisons pour lesquelles il vous en faut un. Car vous en avez désormais besoin plus que jamais.

La neutralité du Net

C'est le principe selon lequel tous les FAI doivent traiter toutes les données Internet de la même façon, sans discrimination ni favoritisme. En décembre 2017, la Federal Communications Commision des Etats-Unis (FCC) a abrogé la neutralité du Net, ce qui signifie que vous pouvez désormais être confronté à des conditions ou discriminations en fonction de ce que vous souhaitez faire en ligne.
En avril 2017, la FCC a fait le premier pas dans cette direction en renversant une règle stipulant que les FAI devaient obtenir l'autorisation de leurs clients pour partager ou vendre leurs données spécifiques. Désormais aux Etats-Unis, les FAI sont libres de vendre au plus offrant votre numéro de

sécurité sociale, vos informations de géolocalisation, les informations concernant votre état de santé, votre historique de navigation et toute autre information qu'ils collectent à votre sujet. L'utilisation d'un VPN assure votre confidentialité, même auprès de votre propre FAI, afin que personne ne puisse suivre vos activités ou consulter vos données.

L'autre bonne raison d'utiliser un VPN

C'est l'augmentation du nombre de cafés modernes où vous pouvez voir autant d'ordinateurs portables... Tout hotspot Wi-Fi public est une véritable bénédiction pour les pirates, même chez vous. Si vous souhaitez naviguer sur Internet tout en dégustant votre café, l'utilisation d'un VPN bloquera l'accès de tout pirate qui tenterait de vous espionner via le hotspot Wi-Fi que vous utiliserez peut être.

Compte tenu de cette récente déréglementation et de la croissance de la cybercriminalité sophistiquée, Internet ressemble de plus en plus au Far West. Les VPN assurent cependant votre protection dans toute cette folie.

Quels sont les avantages et inconvénients d'un VPN ?

Les VPN offrent de nombreux avantages. Puisque vous êtes anonyme à l'intérieur de votre voiture de location aux vitres teintées, personne ne peut savoir où vous vous trouvez réellement. Avant d'emprunter l'autoroute cybernétique, vous pouvez faire votre choix parmi une vaste sélection d'adresses IP. Si le fournisseur de VPN est suffisamment robuste, il propose une vaste sélection d'adresses IP aux coordonnées géographiques variées.

Par exemple, si vous visitez Paris et êtes confronté aux restrictions d'accès liées à votre emplacement géographique à un site que vous consultez régulièrement aux États-Unis, il vous suffit de sélectionner une adresse IP située aux États-Unis dans le service VPN. Votre voiture de location virtuelle est alors équipée de plaques d'immatriculation américaines et vous permet d'accéder à votre site préféré. De la même façon, pour accéder à un site disponible uniquement en France, sélectionnez une adresse IP située dans l'hexagone et vous voilà français comme par magie ! Voici donc quelques cas d'utilisation où un VPN peut s'avérer très pratique.

Avantages

Regardez du contenu où que vous soyez :

Si vous voyagez à l'étranger et que vous essayez d'accéder à un compte de streaming que vous utilisez dans votre pays, vous pourriez découvrir que certaines émissions ne sont pas disponibles dans le pays où vous voyagez. Cependant, si vous sélectionnez une adresse IP située dans votre pays d'origine, vous pouvez accéder à toutes vos émissions préférées comme si vous étiez chez vous.

Sites Web bloqués :

Certaines institutions, telles que les écoles, bibliothèques et lieux de travail limitent l'accès à des pages Web spécifiques telles que les réseaux sociaux. Cependant, la connexion chiffrée qu'offre votre VPN passera outre ces restrictions.

Contourner la censure :

Chaque gouvernement établit ses propres règles et certains s'avèrent très stricts afin de contrôler les informations. Bien que le contournement des restrictions gouvernementales puisse certainement être jugé illégal dans certains de ces pays, nous pensons que la liberté d'expression est une bonne chose.

Élimination de la discrimination tarifaire :

La discrimination tarifaire peut vous toucher de deux façons. La première est la discrimination en fonction de votre emplacement géographique : les personnes résidant à San Francisco ou New York

ont de meilleurs revenus en raison du coût de la vie supérieur dans ces villes. Les entreprises le savent et certaines programment leur site pour afficher un prix supérieur pour les internautes consultant leurs produits depuis ces villes. (Cette pratique est courante au sein des compagnies aériennes.)
La seconde source de discrimination tarifaire provient du suivi de vos achats et de vos préférences par votre FAI. Lorsqu'il identifie que vous achetez régulièrement un produit spécifique, il peut vendre vos informations au fabricant du produit et vous pouvez constater une hausse du prix de ce produit due au fait que le fabricant sait que vous allez l'acheter. La confidentialité et l'anonymat qu'offre un VPN vous épargne ce type de ciblage.

Ne soyez plus suivi :

Il est essentiel de garder cette règle à l'esprit : ne laissez personne suivre vos activités, qu'il s'agisse de pirates, de cybercriminels, d'entreprises, du gouvernement ou même de votre propre FAI. Affranchissez-vous de la répression, du ciblage et de la discrimination.

Inconvénients

En termes de comparaison, les inconvénients sont négligeables par rapport aux avantages. Cependant, mieux vaut que vous les connaissiez.

Débit potentiellement réduit

Lorsque vous vous connectez via un VPN, votre trafic Web passe par davantage d'étapes qu'habituellement, ce qui peut entraîner un ralentissement notable. Étant donné que ce point a toujours été le principal reproche à l'encontre des VPN, les développeurs en ont pris bonne note. Beaucoup d'entre eux ont réussi à optimiser la vitesse et les performances, si bien que les utilisateurs de leur VPN peuvent regarder des programmes et jouer de manière fluide sans aucun problème.
Défis QoS : QoS signifie « quality of service » (qualité de service) et indique les performances d'un service ou d'un réseau. Il n'existe pas encore de norme en vigueur pour estimer et rapporter de telles mesures pour les VPN. En l'absence de métriques à analyser, vous devez vous fier aux tests professionnels et au bouche-à-oreille pour connaître les solutions les plus fiables.

Blocages de VPN

Certaines entreprises tiennent compte du fait que les VPN donnent carte blanche à leurs utilisateurs. Pour y faire face, certaines commencent à bloquer l'accès aux adresses IP de VPN connus. Il n'est cependant pas si simple de déjouer les VPN : ils activent alors de nouvelles adresses IP.
Confidentialité non TOTALE : tandis que le VPN fait son travail en assurant votre sécurité et en chiffrant vos activités, les *cookies* de votre navigateur peuvent toujours permettre de vous identifier. Il ne tient qu'à vous de les désactiver.

Quels sont les appareils pouvant utiliser un VPN ?

Est-il possible d'utiliser un VPN sur iPhone ? Un VPN permet-il aux appareils Android d'échapper aux pirates ? La réponse à ces deux questions est oui. Tout appareil connecté à Internet bénéficie de la confidentialité offerte par un VPN et les services VPN proposent généralement une connexion pour plusieurs appareils.
Cependant, si les ordinateurs, tablettes et téléphones peuvent tous être connectés à un VPN de façon individuelle, ce n'est pas si simple pour les appareils appartenant à la catégorie des objets connectés (IoT). Pour de tels appareils, la meilleure solution consiste à configurer une protection VPN sur votre routeur. Ainsi, tout ce qui entre et sort de ce hub principal est protégé. *Certains routeurs sont vendus avec un logiciel VPN intégré.*

Les types de chiffrements

Il existe trois types de chiffrement principaux : hachage, cryptographie symétrique et cryptographie asymétrique. Chaque type a ses avantages et ses inconvénients mais ils permettent tous de brouiller vos données de sorte à ce qu'elles ne puissent pas être utilisées par autrui.

La plupart des VPN offrent une couche supplémentaire de protection grâce à un système de résolution DNS propre. Le DNS (domain name system, système de noms de domaine) est le carnet d'adresses d'Internet, qui fait correspondre les URL texte et leurs adresses IP appropriées. Le DNS vous permet de saisir le nom d'un site tel que « *alcphalempin.fr* » plutôt qu'une longue chaîne numérique. Les cybercriminels peuvent surveiller les requêtes DNS pour suivre vos activités en ligne mais le système de résolution DNS d'un VPN est conçu pour déjouer leurs plans grâce à un chiffrement supplémentaire.

Historique des VPN

Les VPN n'ont pas toujours été les produits de grande consommation qu'ils sont aujourd'hui. Microsoft a développé le premier VPN en 1996 en vue de donner à ses employés l'accès au réseau interne de l'entreprise depuis leur domicile. C'est ainsi qu'est né le poste de travail à distance.
Ce modèle a permis de multiplier la productivité de l'entreprise par deux (« Vous voulez dire que je peux travailler sur ces feuilles de calcul en pyjama ? ») et d'autres entreprises ont commencé à l'adopter à leur tour. Ce type d'utilisation des VPN est pratique courante de nos jours : il s'agit d'une fonction standard de l'entreprise moderne sur le plan mondial.

Ensuite, les avantages d'un système de protection VPN pour assurer sa confidentialité ont lancé la mode des VPN sur le secteur de la consommation. Les développeurs ont alors identifié que ce « *tunnel* » sécurisé permettant d'accéder à un réseau pouvait être utilisé pour se connecter au plus vaste réseau du monde : Internet. La plupart des internautes veulent protéger leur confidentialité et rester anonymes en ligne, et les VPN sont devenus la solution clés en mains idéale pour cela.

Différents types de VPN

Il existe deux types de VPN de base. *Un VPN à accès distant* permet aux utilisateurs de se connecter à un autre réseau via un tunnel privé et chiffré, qu'il s'agisse d'Internet ou du système interne de leur entreprise.
L'autre type de VPN, *un VPN site-à-site*, est également appelé *VPN routeur-à-routeur*. Ce VPN est principalement utilisé dans les environnements professionnels, en particulier lorsqu'une entreprise possède des sièges sociaux à différents endroits. Le VPN site-à-site est utilisé pour créer un réseau interne fermé sur lequel les différents bureaux peuvent se connecter les uns aux autres. Ce modèle est appelé *intranet*.

Il existe différents protocoles VPN ou méthodes de sécurité. Le plus ancien est le PPTP, point-to-point tunneling protocol (protocole de tunnel point-à-point), qui est encore utilisé actuellement mais considéré par beaucoup comme l'un des moins sécurisés. Les autres sont les protocoles IPSec, L2TP, SSL, TLS, SSH et OpenVPN. Nombre d'utilisateurs préfèrent OpenVPN car il s'agit d'un logiciel open source, ce qui signifie qu'en cas de découverte d'une vulnérabilité dans la programmation, quelqu'un la signalera toujours rapidement et elle sera corrigée dans les plus brefs délais.

Comment choisir un VPN ?

Il existe un vaste choix en matière de VPN. Certains préféreront essayer un *VPN gratuit*. Les VPN gratuits représentent une bonne opportunité d'essayer et de voir comment fonctionne un VPN. Nous vous recommandons d'opter pour un essai de 7 jours.
Après l'avoir essayé, vous voudrez passer à la version payante (certes, elle coûte quelques deniers, mais vous bénéficierez de toute la bande passante et des serveurs dont vous avez besoin pour accéder au contenu que vous souhaitez où que vous vous trouviez, ainsi que d'une protection en cas de connexion à un réseau Wi-Fi public (hotspot).
Points à prendre en compte lors de l'essai d'une version gratuite :

1) Ils utilisent parfois des protocoles moins sécurisés, tels que PPTP.

2) Ils disposent de moins de serveurs, si bien que vous partagez la bande passante avec d'autres utilisateurs, ce qui entraîne une réduction des débits.
3) Ils contiennent parfois des publicités.
4) Ils imposent généralement des limites de téléchargement.

Gardez simplement ces éléments à l'esprit lors de votre période de test. Une fois que vous serez convaincu de la nécessité d'un VPN, vous disposerez en effet de meilleures performances avec un service VPN payant.

Quels critères faut-il prendre en compte lors du choix d'un VPN ?

Les services VPN payants offrent de meilleures performances, mais chacun a ses particularités. Voici les éléments à prendre en compte lors de la recherche du VPN idéal :

Réputation : pour avoir une bonne idée de la qualité du VPN, lisez les avis des clients et les tests professionnels. Par ailleurs, depuis que les règles de confidentialité des FAI ont été abolies, de nombreux VPN factices ont vu le jour : veillez à vous intéresser à un vrai service VPN.

Adresses IP partagées : choisissez un VPN offrant des adresses IP partagées. Le fait d'être noyé parmi de nombreux utilisateurs anonymes ajoute une couche supplémentaire de confidentialité à votre anonymat.

Serveurs : en termes de performances, plus les serveurs sont nombreux et plus la navigation sera fluide puisque tous les utilisateurs n'utilisent pas le même. En outre, plus vous êtes proche d'un serveur et plus votre connexion sera rapide et fiable.

Chiffrement : le chiffrement AES-256 (advanced encryption standard) offre le meilleur niveau de chiffrement à l'heure actuelle. Il est presque impossible à déchiffrer, car il possède davantage de combinaisons qu'il y a d'étoiles dans l'univers.

Protocole : évitez tant que possible les protocoles les moins sécurisés tels que PPTP et optez pour OpenVPN, qui est le plus fiable.

Journaux de données : il est préférable que votre service VPN déclare ne PAS conserver de journaux de données (c'est-à-dire son propre enregistrement de vos activités sur Internet). Lisez la politique du VPN pour savoir s'il collecte vos informations.

Assistance clientèle : les meilleurs VPN offrent une assistance clientèle en cas de problème.

Fonctionnalités : gardez à l'esprit qu'elles dépendent de vos besoins et veillez à ce que le VPN que vous choisissez est compatible avec ce dont vous avez besoin. Par exemple, certains VPN ne vous permettent pas d'utiliser BitTorrent, contrairement à d'autres. Certaines autorisations de téléchargement VPN sont limitées à un certain nombre, tandis que ce n'est pas le cas pour d'autres. Certains proposent des fonctionnalités de blocage des publicités, de pare-feu, de coupe-circuit, de connexion simultanée, etc. Identifiez ce dont vous avez le plus besoin pour votre utilisation.

Essai gratuit : de nombreux VPN offrent une période d'essai gratuit, profitez-en pour vous en faire une idée concrète. Évaluez la facilité d'utilisation et les performances du VPN avant de vous décider à l'acheter.

Vous êtes prêt. Vous comprenez désormais l'origine, l'évolution et la nécessité des VPN à l'heure actuelle. Faites le bon choix pour profiter au mieux de votre liberté en ligne.

Installez le VPN Avast SecureLine (vous pouvez l'essayer gratuitement !) pour assurer la sécurité de votre connexion à Internet.

Gardez à l'esprit que la confidentialité est un droit et non un privilège.

Inspiré du blog :
https://blog.avast.com/fr/qu-est-ce-qu-un-vpn-et-en-quoi-consiste-t-il-votre-guide-essentiel

Conclusions :

Nécessité d'un VPN :

La plupart des suites de sécurité (appelés plus simplement antivirus) proposent dans leur suite des VPN. Certains même sont gratuits ou proposent une période d'essai. Il est difficile d'en conseiller l'un plutôt que l'autre tant les options sont variées. Il vous revient donc de mettre en parallèle vos besoins et leurs options.

Les navigateurs sécurisés :

Depuis quelques temps des navigateurs et des moteurs de recherche affirment vous protéger sur le net. C'est sans douter vrai mais cela ne remplacera jamais entièrement un bon VPN qui viendra alors en complément.

Brave le navigateur sécurisé (voir la fiche descriptive sur ce site http://alcphalempin.fr/wp-content/uploads/2020/03/Brave.pdf)

Qwant le moteur de recherche. https://www.qwant.com/?l=fr