SGBLE

Geste de savoir

Avez-vous besoin d'un VPN ?

27 mai 2023

Table des matières

Introduction 1
1. Mise en garde technique 1
2. Qu'est-ce qu'un VPN? 2
3. Revues technique des louanges 2
3.1. Le VPN protégerait et sécuriserait vos données 2
3.2. Le VPN permettrait de ne pas savoir où vous allez 3
3.3. Première conclusion 5
3.4. Le VPN vous rendrait anonyme 5
3.5. Le VPN protégerait vos appareils 6
3.6. Le VPN protégerait contre les «hackers», les «brouteurs» et les sites malveillants 6
3.7. Le VPN permettrait de se connecter avec l'adresse IP d'un autre pays . 6
4. Annexe: les VPN en général 6
Conclusion 7

Introduction

Avez-vous entendu parler de VPN? Après avoir entendu tant d'éloges à leur sujet, pensez-vous en avoir besoin vous aussi ou doutez-vous encore de son utilité dans votre cas?

Il apparaît en effet difficile de ne pas perdre le nord[1] face à ces nombreux boniments ornés de jargon technique impressionnant (intimidant ?).

Cet article a un but précis: passer en revue et questionner d'un point de vue technique les affirmations les plus courantes des fournisseurs de VPN et des influenceurs qui en font la promotion. J'essaierai de me limiter aux faits techniques, sans prendre spécialement parti.

Cet article s'intéresse exclusivement aux offres de VPN commerciaux grand public dont les publicités inondent nos réseaux. Ainsi, tenons-nous en à une définition qui se borne à ce qui semble généralement être venté. Ne sera donc pas traitée la question de savoir si vous avez besoin de votre propre VPN dans une entreprise ou pour interconnecter vos serveurs à travers plusieurs *datacenters*.[2]

1. Mise en garde technique

Dans l'article suivant, deux présupposés sont faits pour alléger le propos:

— les couches de sécurité sont implémentées correctement: versions de TLS récentes, vérification des certificats systématique, utilisation de *cipher suites* et d'algorithmes réputés sûrs;
— l'utilisation d'un VPN est jugée «sans fuite»: pas de *DNS leaks* ou de *WebRTC leak*.

2. Qu'est-ce qu'un VPN ?

Le fonctionnement basique dans notre cas est le suivant: un tunnel est établi entre votre machine et le serveur du fournisseur VPN. Tout le trafic réseau (tous les paquets IP) passe par ce tunnel. On peut voir ce tunnel comme un câble branché entre votre machine et un serveur du fournisseur VPN, plutôt qu'entre votre machine et votre box (routeur de l'opérateur). Votre porte d'entrée sur l'Internet n'est donc plus votre box, mais le serveur du fournisseur VPN. Ce câble a une particularité: il est chiffré jusqu'au serveur du fournisseur VPN. Nous verrons ce que cela signifie en pratique.

3. Revues technique des louanges

3.1. Le VPN protégerait et sécuriserait vos données

Par «protéger» et «sécuriser», entendons-nous sur deux choses: protéger les données signifie qu'il n'est pas possible d'intercepter la communication pour la lire (confidentialité) grâce au chiffrement, et qu'il n'est pas non plus possible d'altérer la communication pour détourner l'information à des fins malveillantes (authenticité).

Techniquement, un tunnel chiffré tels ceux qui sont fournis par les prestataires implémentent les vertus cardinales susmentionnées. Mais une question doit impérativement se poser pour en apprécier les implications.

? Ça protège. Mais ça protège quoi et ça protège de qui?

Un tunnel vous protège essentiellement de deux acteurs: le fournisseur d'accès à Internet (FAI) qui achemine vos données vers le reste de l'Internet et les autres machines qui pourraient être sur le même réseau local (LAN) que le vôtre.

3.1.1. Réseau local et partagé

Le réseau local, c'est ce qui est constitué des tous les appareils connectés (en filaire ou Wi-Fi) à un même routeur/*box*. À la maison, le réseau local est supposément privé car seuls vos équipements sont sur ce réseau en principe de confiance. Mais la notion de réseau local s'étend aussi dans le cas d'une connexion Wi-Fi partagée au parc ou au café. Vous partagez alors le même réseau local que d'autres utilisateurs, lesquels ne peuvent pas être réputés dignes de confiance. Il en va

1. Aabu
2. Mais je vous mets un petit quelque chose en annexe si vous voulez approfondir 🍊

de même avec l'entité qui possède et gère ce point d'accès (la café, la municipalité qui met du Wi-Fi dans le parc, *etc.*)

Au sein d'un même réseau local, il est possible de *sniffer* le trafic et d'intercepter les communications facilement, surtout en Wi-Fi. Cela inclut le fait d'espionner vos communications ou de les altérer.

D'après notre définition, cela n'est pas un problème avec le VPN: le tunnel est établi entre votre machine et le serveur du fournisseur VPN. Les curieux partageant votre réseau local ne peuvent donc pas intercepter les communications, ni les altérer de façon malveillante.

3.1.2. Fournisseur d'accès à Internet (FAI)

Au delà de la *box* et du réseau local, il y quelqu'un d'autre: le FAI. Le FAI a bien entendu accès au contenu des communications que vous lui demander de transporter. De la même façon qu'un acteur malveillant sur le réseau local, le FAI peut potentiellement lire et agir sur votre trafic.

3.1.3. Et le HTTPS dans tous cas ?

?

De nos jours, les sites Web officiels (banques, réseaux sociaux, plateforme d'achat en ligne) implémentent systématiquement la couche de sécurité HTTP**S** (TLS), de même que les prestataires en général pour d'autres protocoles (exemple: SMTPS et IMAPS pour vos emails). Le VPN est-il alors nécessaire?

Il est vrai qu'une simple couche HTTP*S* (et TLS en général) suffit à contrer les attaques évoquées plus haut, même sur une connexion Wi-Fi on ne peut plus douteuse.[1] La question se pose donc bien. L'utilisation d'un protocole sur TLS (HTTPS, SMTPS, IMAPS, …) rendrait-il l'utilisation d'un VPN superflue pour autant?

Certains petits sites Web ne sont pas sécurisés et certains services non-Web non plus. Dans ce cas, le VPN permet au moins de protéger les données initialement en clair jusqu'à la terminaison du tunnel. Mais pas au delà: quand c'est la fin du tunnel, les données initialement en clair ne sont plus chiffrées et continuent leur route en clair. Pour cette raison, l'utilisation d'un VPN n'est pas un prétexte pour se passer des protocoles sécurisés comme HTTPS qui eux assurent la sécurité de votre machine jusqu'au serveur final (au delà de celui du VPN). Je ne peux donc que vous encourager à veiller à utiliser des protocoles sécurisé *partout*, VPN ou pas.

Nous verrons dans la section suivante un autre aspect qui pourrait rendre l'utilisation d'un VPN pertinente malgré tout.

3.2. Le VPN permettrait de ne pas savoir où vous allez

Le DNS est souvent cité comme exemple de protocole qui n'est jamais chiffré. C'est vrai dans la plupart des cas, bien qu'il soit parfaitement possible de faire passer le DNS sur une couche sécurisée comme *DNS over TLS* ou encore *DNS over HTTPS* (pris en charge par Firefox). Cela

pourrait devenir la norme et des efforts semblent être faits dans ce sens, mais ce n'est pas la norme en 2021.

Connaître le contenu de vos requêtes DNS mettent en péril votre vie privée: il est aisé de connaître les sites que vous consultez (voire plus encore) en observant ce trafic-là.

Mais pour peu que les requêtes DNS passent elles aussi par le tunnel VPN, les équipements du réseau local et le FAI ne pourront donc pas savoir quels noms de domaine vous voulez résoudre. Il s'ensuit qu'il ne sera donc pas possible non plus de deviner aisément quel site vous comptiez visiter d'après vos résolutions DNS.

Quand même vous utiliseriez une méthode de résolution DNS sécurisée (disons *DNS over HTTPS* sous Firefox), il reste malgré tout un trou dans la raquette: le maudit *SNI*…

La section suivante est un peu technique, n'hésitez pas à la sauter si vous ne comprenez pas. Retenez cependant cela: malgré HTTPS (et TLS en général), il est possible de savoir quel site vous vouliez plausiblement visiter même s'il ne sera pas possible de savoir ce qui se dit entre ce site et votre machine par la suite (grâce au chiffrement).

Quand une session TLS s'établit, il y a un *handshake* qui permet de négocier certains paramètres et de générer les clefs de chiffrement à utiliser. Le client indique **en clair** le nom du serveur qu'il souhaite atteindre[2]. C'est le *SNI* : *Server Name Indication*. Or, ce SNI est en clair et il n'est pas vraiment possible de faire autrement[3].

Regardons l'exemple d'un *handshake* TLS entre moi et un site Web proposant le HTTPS dans un outil d'analyse réseau (tel qu'un acteur malveillant pourrait utiliser):

```
# tcpdump port 443 -v -A -n
12:26:08.645713 IP (tos 0x0, ttl 64, id 34468, offset 0, flags [DF], proto TCP (6), length 569)
    10.8.42.54.38008 > 92.243.7.44.https: Flags [P.], cksum 0x75f3 (correct), seq 1:518, ack 1, win 502, options [nop,nop,TS val 1257528485 ecr 550319964], length 517
E..9..@.@.A.
..6\..,.x.......T.....u......
J.\. .7\........... v!.....x.d~.v.d...$......./z.. .;......o..K.c.........N.."Q...."......+./.....,.0.
.   ........./.5............zestedesavoir.com.........
.............................h2.http/1.1.........3.k.i... fG....y...@..E..Z...E....0..K).....A.Qb....f<.
..'.^#K.....,`...e.>..v..b..P..8..f.y..".c;R.....$.!...+.....................................-........@....L....................................................................).K.&. ..r..N6....;.....g.."......T.6}..X..! .D....w.o.O....(.$.$.j....Xs./O.
```

Regardez bien et apercevez ce `zestedesavoir.com` en plein milieu. Même si les données qui suivront seront parfaitement chiffrées et inexploitables, ce *hadnshake* permet quand même aux acteurs (FAI et utilisateur du réseau partagé) de savoir que je vais sur https://zestedesavoir.com/ .

Ici, un VPN empêcherait que ce SNI soit visible par votre FAI. En effet, tout le trafic passant par le tunnel chiffré, même ce qui est en clair (dont le SNI) serait protégé. Néanmoins, le même avertissement que tout à l'heure s'applique encore: à la fin du tunnel, ce SNI est en clair à nouveau quand il sort du serveur du fournisseur VPN (et le fournisseur du VPN peut le voir, ce SNI).

3.3. Première conclusion

Le VPN peut effectivement protéger vos données vis-a-vis de votre FAI et des autres utilisateurs d'un même réseau local. Y compris ce qui est en clair de base. Il permet, en plus de protéger les communications (ce que faisait déjà HTTPS), de se prémunir contre la surveillance du FAI qui ne peut pas savoir où le visiteur va pendant ses navigations.

Mais gardons ce qui suit à l'esprit:

— les données sont livrées à elles-mêmes une fois sorties du tunnel VPN. Entre le serveur VPN et le serveur cible que vous voulez visiter, il y a encore un peu de route pendant laquelle des données (dont le SNI) peuvent être inspectées par des opérateurs que vous ne connaissez même pas (c'est le cas aussi sans utiliser de VPN);
— le FAI ne saura pas quels sites vous visitez, certes. Mais le fournisseur du VPN, lui, pourra voir tout ce que le FAI aurait pu voir si vous n'utilisiez pas de VPN. Le fournisseur VPN voit le SNI et les requêtes DNS (si non chiffrées), il voit donc où vous allez et il peut prendre des notes comme l'aurait fait votre FAI;
— l'utilisation d'un VPN ne vous dispense pas d'utiliser des protocoles sécurisés tels que HTTPS, SMTPS ou encore IMAPS pour accéder à vos service. Si vous n'acceptez pas que votre FAI puisse lire vos secrets, alors vous ne devriez pas non plus laisser le fournisseur VPN les lire.

Vous avez donc échangé votre FAI contre votre fournisseur VPN. Les pouvoirs de surveillance que vous arrachez au FAI, vous les octroyez aussitôt au fournisseur VPN. Soyez donc bien conscients que vous gagnez au change que si le fournisseurs VPN peut être raisonnablement réputé plus sûr que votre FAI.

3.4. Le VPN vous rendrait anonyme

Cela est peu probable.

Il est vrai que, via un VPN, un site Web que vous visitez ne pourra pas connaître votre adresse IP originale, laquelle pourrait servir à vous identifier personnellement.

Mais le fait est que l'on n'a nullement besoin de connaître votre «vraie» adresse IP pour vous identifier. Il y a une panoplie de techniques plus moins simples pour cela: cookies, *fingerprinting* de votre navigateur ou tout bêtement le fait d'être connecté à vos services habituels pendant votre navigation avec les cookies tiers.

Si vous voulez être anonyme, le VPN ne sera pas la réponse technique adéquate de façon générale.

3.5. Le VPN protégerait vos appareils

Non. Ce n'est tout simplement pas le travail d'un VPN. Votre appareil peut présenter une vulnérabilité exploitable indépendamment de l'utilisation d'un VPN.

Ironiquement, il est intéressant de noter qu'une machine connectée à un VPN augmente sa surface d'attaque: une interface réseau en plus, fût-elle virtuelle, c'est une porte d'entrée en plus sur votre machine. Prions pour qu'il n'y ait donc pas de compromission des serveurs de votre fournisseur VPN, ni de mauvais réglage de sa part.

3.6. Le VPN protégerait contre les « hackers », les « brouteurs » et les sites malveillants

Dans le cas général, non hélas. Les attaques de ce genre reposent le plus souvent sur le *Social Engineering*. Un VPN n'est pas une réponse technique à ce genre de problèmes. De façon générale, il n'y a d'ailleurs pas de solution technique à cela.

Parmi les failles classiques et techniques pouvant impacter l'utilisateur pendant la navigation, citons la faille XSS ou la ré-utilisation de cookie via CSRF. L'utilisation d'un VPN ne changera ici **rien** au bon déroulement de l'exploitation de telles failles. Les contre-mesures existent mais se trouvent ailleurs.

3.7. Le VPN permettrait de se connecter avec l'adresse IP d'un autre pays

Oui, c'est vrai. Le VPN permet donc de contourner par exemple le géo-blocage ou la censure. Précisons néanmoins que de tels contournements peuvent parfois aller à l'encontre des CGU/CGV du service mettant en place ces mesures.

Ajoutons aussi à cela qu'il n'est pas spécialement difficile de différencier une connexion «réelle» d'une connexion utilisant un VPN ou un proxy. L'usage des VPN pourrait se populariser au point où les services de vidéo à la demande soient assez motivés pour le contrer. Si cela arrive, il faut rester conscience qu'elles pourront sans doute le faire sans grande difficulté (diverses astuces permettent de deviner de façon plus ou moins fiable cela).

4. Annexe : les VPN en général

Nous n'avons parlé que des VPN racontés selon les influenceurs des réseau sociaux. Laissez-moi, à mon tour vous parler de la véritable puissance des *vrais* VPN!

1. En supposant que l'implémentation soit correcte et que le certificat soit bien valide. Si votre navigateur vous alerte d'un problème de certificat invalide quand vous tentez de vous connectez à un sites en HTTPS alors que vous êtes sur un réseau partagé: **N'ACCEPTEZ SURTOUT PAS.**
2. C'est comme l'indication d'un *vhost* via le *header* `Host` en HTTP, mais dans le protocole TLS.
3. Une alternative avait été proposée et vaguement implémentée: ESNI (*Encrypted SNI*) mais ça ne semble pas avoir pris. Soyons patients et attendons de voir ce que ECH (*Encrypted Client Hello*) nous réserve à l'avenir.

Si l'on s'en tient à une définition dérivée du nom *VPN*, on pourrait dire qu'il s'agit d'un dispositif permettant de créer un réseau de machines sans qu'il soit nécessaire pour autant de mettre en place une liaison physique (filaire ou sans-fil) entre eux. Ce qui nous servira de «câbles virtuels», ça sera une connexion déjà existante. La liaison est donc souvent logicielle (virtuelle). Pour réaliser cette prodigieuse chose, l'astuce est assez simple: encapsuler un protocole (IP ou Ethernet, typiquement) dans une couche transport reposant sur une liaison déjà existante.

Il est bien entendu possible de faire un VPN par dessus un autre VPN, et ainsi de suite. (attention, il y a un peu d'*overhead*, malgré tout)

Remarquez que je n'ai en aucun cas parlé de sécurité ici. Le chiffrement ou la sécurité en général n'est pas une caractéristique inhérente d'un VPN. Tant que vous fabriquez un réseau en vous appuyant sur un autre réseau sous-jacent, c'est déjà du VPN techniquement, qu'il y ait ou non du chiffrement (exemple: VXLAN, qu'il est alors possible de faire passer sur IPSec ou WireGuard si la sécurité est requise).

L'intérêt est souvent de faire un réseau privé étendu: avec un VPN, on peut faire comme si l'on avait un même réseau local sur plusieurs points séparés physiquement. Par réseau local, j'entends un même *broadcast domain*. OpenVPN (configuré en `layer 2`) et VXLAN le permettent, par exemple. Conceptuellement, c'est comme si vous aviez un swicth virtuel branchés à plusieurs serveurs qui seraient absolument n'importe où physiquement. Puissant, n'est-ce pas?

Un autre intérêt serait de permettre d'avoir un réseau caché et privé, lequel ne pourrait être routé que parmi les machines autorisées. Cela est très utilisé en entreprise où les services internes seront accessibles via le VPN et pas au delà. En bonus, cela permet aussi à des employés d'accéder à ce réseau privé sans pour autant être physiquement sur les lieux. Pour le télétravail, c'est plutôt intéressant. Dans ce cas, c'est comme si le serveur VPN était un routeur virtuel entre les machines.

Enfin, il est tout à fait possible de faire le pont entre un réseau virtuel et un réseau physique. Cela est appelé un *bridge* et cela permet d'acheminer du trafic sur une connexion déjà existante s'il n'est pas possible de router ses adresses IP directement depuis une certaine localisation. Cette technique est assez utilisées chez des opérateurs Internet qui n'ont pas forcément d'infrastructure physique présente dans une zone, mais qui veulent quand même faire passer leur trafic IP.

À noter que les VPN commerciaux grand publics ne permettent pas tout cela en général. Vous voyez qu'il s'ait ici plutôt de techniques de réseaux. Il faut le faire vous-même ou alors souscrire à une offre professionnelle.

Si l'aventure des VPN vous tente, utilisez le code `apt install wireguard` ou `apt install openvpn` et bénéficier de votre *propre* infrastructure VPN dès à présent! Sans engagement!

Conclusion

J'espère que cette revue technique des affirmations habituelles vous aidera à faire mieux la part des choses afin de déterminer vos besoins réels.