

Ce qu'est vraiment un VPN

Il change qui peut te voir, pas si quelqu'un le peut.

Pour faire simple : un VPN empêche ton fournisseur d'accès ou le Wi-Fi d'un aéroport de voir où tu te connectes. Cette information ne disparaît pas : elle est transmise à l'entreprise du VPN, qui la voit à son tour. Ce qui voyageait déjà chiffré, comme tes e-mails ou ta banque, l'était déjà auparavant. Il sert à quelques usages précis et est souvent vendu comme s'il servait à bien plus.

Pendant des années, j'ai entendu parler des VPN sans m'y intéresser, tout comme pour les antivirus : je n'utilise pas d'antivirus, ou presque jamais. J'ai des sauvegardes en temps réel de tout dans trois endroits différents, et je fais très attention à ce que je télécharge, aux liens sur lesquels je clique et aux sites que je visite. Ce n'est pas une sécurité absolue, mais c'est ce qui fonctionne pour moi. Un jour, j'ai vu une offre de VPN à un peu plus de deux euros par mois et j'ai souscrit par curiosité. Il fonctionne bien, mais il ne m'a pas servi à grand-chose : par exemple, tester un service qui n'était alors accessible qu'aux États-Unis. Est-ce que je me sens plus en sécurité ? Non. S'ils me le proposent à nouveau à ce prix, je renouvellerai peut-être ; sinon, non. Ce n'est que mon expérience, cela ne prouve rien. Je me suis donc demandé ce que fait exactement un VPN. Voici comment je l'ai compris.

Imagine que tu glisses une lettre dans la boîte aux lettres avec l'adresse du destinataire bien visible. Le facteur voit à qui tu l'envoies, même s'il ne peut pas la lire si elle est cachetée. Ce facteur, c'est ton opérateur internet. Un VPN place ta lettre dans une autre enveloppe, adressée à un intermédiaire qui l'ouvre et la réexpédie. Ton facteur habituel ne voit plus l'adresse réelle. Il voit seulement que tu écris à cet intermédiaire.

La personne ou l'entité qui contrôle le réseau d'où tu te connectes, par exemple le Wi-Fi d'un aéroport, ne voit plus où tu vas. Mais l'intermédiaire voit maintenant ce que voyait ton opérateur, et parfois plus, car tout ton trafic passe par lui. La surveillance ne disparaît pas : elle change de mains. D'où le nom.

De plus, presque tout ce que tu fais aujourd'hui, comme ouvrir ta messagerie ou consulter tes comptes bancaires, voyage déjà chiffré jusqu'au serveur de destination grâce au cadenas du navigateur. C'est vrai avec ou sans VPN. Le VPN ajoute une protection uniquement sur le premier tronçon, jusqu'à son propre serveur. Ensuite, le trajet reste le même.

C'est pourquoi il y a des choses qu'il ne peut pas te promettre, même s'il est parfois vendu ainsi. Si tu t'es connecté à ton compte e-mail ou à ta banque, ce service sait qui tu es, avec ou sans VPN. Il ne garantit pas non plus que personne ne surveille ton trafic : il change seulement qui le regarde. Lorsqu'une entreprise affirme qu'elle « ne conserve aucun journal », ce n'est qu'une promesse, au même titre qu'une grande plateforme affirmant « vos messages sont chiffrés, nous ne les lisons pas ». Un audit peut l'attester à un moment donné, mais cela reste un acte de foi, pas une garantie garantie par conception.

Et le contenu d'une conversation ne change pas. Si ton application de messagerie chiffre déjà de bout en bout, le VPN n'ajoute rien. Si elle ne le fait pas, le VPN ne règle rien non plus : il protège le cheminement du message, pas ce que l'application ou son serveur en font une fois arrivé.

Rien de tout cela ne le rend inutile. Cacher où tu te connectes sur un Wi-Fi public, face à un opérateur qui voudrait vendre cet historique ou à un pays qui bloque un service, est un travail utile qu'il accomplit bien. Le

marketing, lui, promet bien souvent plus que ce que cette couche technique peut offrir.

La vraie question à se poser, face à un VPN ou tout service qui promet de te protéger, n'est pas « est-ce chiffré ? ». Probablement oui, au moins sur une partie du trajet. La question est celle-ci : à qui suis-je en train de confier la confiance que j'ai retirée à un autre ? Et que me reste-t-il si cette confiance n'est pas méritée ?

Un VPN, quand il fait bien son travail, ne fait que changer l'intermédiaire de ta connexion. Une application comme Solo2, dont les messages ne transitent par aucun serveur, supprime l'intermédiaire de la conversation. Elles ne s'opposent pas : elles répondent à des problèmes différents.

Les confondre est une façon très courante de se croire plus protégé qu'on ne l'est réellement.

Note éditoriale : quand ces Cuadernos nomment des entreprises ou des produits, ce n'est pas pour accuser. Ceux qui les construisent font un travail que des millions de personnes utilisent et apprécient. Ce que nous soulignons est structurel — le modèle, pas la marque. Les marques apparaissent comme exemples car ce sont celles que le lecteur reconnaît.

Sources et lectures complémentaires

- Le protocole HTTPS et le chiffrement de transport sont des normes ouvertes, documentées publiquement par l'IETF.
- Dans cette même collection : « Quand il n'y a personne au milieu » et « Vous n'êtes pas anonyme » développent, sous d'autres angles, cette même distinction entre structure et promesse.

[← Précédent](#) [Tu n'es pas anonyme](#)

Lectures recentes

- [Réflexion · 29 juin 2026 Tu n'es pas anonyme](#)
- [Réflexion · 27 mai 2026 Ce qu'une signature ne peut pas réparer](#)
- [Analyse · 26 mai 2026 Confidentialité réelle vs apparente : les questions à se poser](#)

Emporte cet article où tu en as besoin.

[↓ Markdown](#) [↓ Texte brut](#) [↓ PDF](#)

Le fichier est téléchargé sur ton appareil. À partir de là, tu peux l'enregistrer, l'importer dans Solo2 ou le partager comme tu le souhaites. Cuadernos ne décide pas de la destination pour toi.

Cachet de cire · SHA-256 10afb612ab39c7a3994657f7da7c8677ab5c43354c9b59f5fd757b025dc7a3f2

[Fonctionnalités](#) [Tarifs](#) [Installer](#) [Nouveautés](#) [Blog](#) [Pro](#) [Aide](#) [À propos](#) [Contact](#)
[Transparence](#) [Vérification](#) [Confidentialité](#) [Conditions](#) [Cookies](#)

Cuadernos Lacre · Une publication de [Menzuri Gestión S.L.](#) ·
écrite par R.Eugenio · éditée par l'équipe de [Solo2](#).

Ce site n'utilise pas de cookies. Tout ce que charge ton navigateur est écrit ou supervisé par nous et hébergé sur nos serveurs européens : le compteur de visites anonyme (Umami, auto-hébergé) et le minimum de JavaScript nécessaire pour le sélecteur de langue et ta préférence de thème clair/sombre, qui est enregistrée sur ton propre appareil. Sans ressources tierces, sans trackers, sans profilage, sans partage de données. Si tu souhaites nous suivre : [RSS](#).