

Accueil / Meilleur VPN : Comparatif 2025

## Du FAI au VPN, qui manipule vraiment vos requêtes DNS (et pourquoi ça compte)



Par **Chloé Claessens**

Spécialiste cybersécurité

Publié le 04 octobre 2025 à 09h11



13

**Changer de DNS est souvent présenté comme une simple optimisation de vitesse ou de sécurité. En réalité, c'est un geste qui déplace un pouvoir d'observation colossal. Car derrière chaque requête tapée dans votre navigateur, un acteur sait précisément où vous allez sur le web, même si tout le reste est chiffré.**



Du FAI au VPN, qui manipule vraiment vos requêtes DNS (et pourquoi ça compte). © Wit Olszewski / Shutterstock

On parle beaucoup des VPN, des bloqueurs de traqueurs et du chiffrement HTTPS. Le

DNS, lui, reste dans l'ombre alors qu'il en dit long sur nos habitudes de navigation. Chaque fois que vous ouvrez un site, votre appareil demande l'adresse IP correspondante à un serveur DNS. Traditionnellement, c'est votre fournisseur d'accès à Internet qui assure ce rôle. Mais depuis quelques années, les cartes sont rebattues avec l'arrivée de résolveurs publics, du chiffrement DoH ou DoT et des **VPN** qui promettent de tout sécuriser. Dans les faits, la question n'est pas tant de savoir si vos requêtes sont visibles, mais à qui elles profitent.

## DNS et vie privée, un angle mort souvent sous-estimé

Lorsque vous tapez une URL dans votre navigateur ou qu'une application doit contacter un service en ligne, votre appareil commence par traduire ce nom de domaine en adresse IP, sorte de matricule propre à chaque équipement connecté à Internet qui leur permet de se localiser les uns les autres et de communiquer entre eux.

Comme il serait peu pratique pour nous de retenir des suites de chiffres chaque fois que l'on souhaite se rendre sur un site web précis, ce travail de traduction s'appuie sur le DNS (*Domain Name System*), un immense annuaire distribué qui fait correspondre les noms lisibles par les humains (*clubic.com*, par exemple) aux adresses compréhensibles par les machines.

Pour consulter cet annuaire, votre appareil interroge un serveur DNS, aussi appelé résolveur, chargé de trouver la bonne correspondance entre un nom de domaine et une adresse IP, puis de la renvoyer. Par défaut, ce serveur est généralement celui de votre fournisseur d'accès à Internet. Il ne voit pas les URL complètes ni le contenu de vos échanges, protégé par HTTPS, mais il sait exactement quels domaines vous consultez, quand et à quelle fréquence.

Ce n'est certes pas votre historique complet, mais ça s'en rapproche ; ces informations suffisent déjà à dresser un profil précis de vos habitudes de navigation et servent aussi aux opérateurs pour gérer leur réseau ou appliquer certains blocages prévus par la loi. Dans ce dernier cas, ces serveurs sont même dits « menteurs » car ils modifient leurs réponses pour empêcher l'accès à certains sites. Ces blocages sont évidemment légaux et généralement légitimes, notamment pour protéger les ayants droit, mais ils rompent avec l'idée d'un Internet ouvert et neutre et créent un précédent susceptible d'étendre demain ces pratiques à des formes de censure politique ou sociale, comme on l'a déjà vu en France en 2024 avec le **blocage de TikTok en Nouvelle-Calédonie** pour tenter de réprimer le soulèvement du peuple kanak.



Les résolveurs DNS traduisent les noms de domaines en adresse IP pour permettre à vos équipements de communiquer avec les serveurs web. © SuPatMaN / Shutterstock

## S'affranchir du DNS des FAI, un choix pas si neutre

Face à ce pouvoir d'observation et à cette capacité de filtrage confiés aux FAI, de nombreux internautes choisissent de s'affranchir du DNS fourni par défaut pour déléguer la résolution des noms de domaine à un acteur tiers. C'est ce qu'on appelle un DNS public. Parmi les plus connus, on peut citer ceux de Google (8.8.8.8), Cloudflare (1.1.1.1) ou Quad9, souvent présentés comme plus rapides, plus fiables, parfois plus respectueux de la vie privée.

Attention toutefois, cela ne signifie pas pour autant que le problème de confiance disparaît ; il change simplement de mains. Les requêtes ne passent plus par l'opérateur, mais elles deviennent visibles pour un nouvel intermédiaire, soumis aux lois de son pays et libre d'en faire l'usage qu'il juge opportun. Google admet ainsi conserver certains logs techniques à court terme et des données agrégées pour ses propres analyses. Cloudflare promet de supprimer les adresses IP sous vingt-quatre heures et fait auditer ses pratiques par un

cabinet indépendant. Quad9, fondation suisse, revendique un fonctionnement sans collecte commerciale et limite ses enregistrements aux besoins de sécurité. Ces engagements sont détaillés dans leurs politiques de confidentialité, censées éclairer les internautes, mais rien ne garantit qu'ils ne puissent évoluer ou être remis en cause par une contrainte légale.

Il faut enfin savoir qu'un DNS public peut permettre de contourner certains blocages lorsqu'ils reposent uniquement sur la résolution de noms de domaine. Dans ce cas, changer de résolveur suffit parfois à atteindre un site que l'opérateur avait rendu inaccessible. Cette possibilité n'annule pas les autres formes de filtrage : si le blocage s'appuie sur l'adresse IP ou sur des techniques plus poussées, le changement de DNS n'aura aucun effet. On en profitera aussi pour rappeler que les fournisseurs de DNS publics appliquent parfois leurs propres filtres, par exemple pour bloquer les domaines malveillants ou liés au phishing, de manière à renforcer la sécurité de la navigation. Une intention louable sur le papier, mais qui redéfinit, là encore, qui décide de ce qui est accessible.

## **Le chiffrement DoH et DoT, un progrès qui ne règle pas tout**

Pour limiter l'exposition des requêtes DNS, deux protocoles ont été introduits ces dernières années : DNS over HTTPS (DoH) et DNS over TLS (DoT). Ils chiffrent les échanges entre votre appareil et le résolveur choisi, empêchant un tiers d'espionner ou de modifier les requêtes en chemin. C'est un vrai progrès, surtout sur les réseaux Wi-Fi publics ou dans des environnements où le trafic est étroitement surveillé.

Mais si ce chiffrement protège le trajet, il ne change rien à la confiance que vous accordez au résolveur. Qu'il s'agisse de Google, de Cloudflare ou de votre FAI, celui qui traduit vos noms de domaine voit toujours l'intégralité des sites que vous consultez.

DoH et DoT sont désormais intégrés dans la plupart des systèmes et navigateurs, mais chacun le fait à sa manière. Firefox a ouvert la voie en activant par défaut le DoH vers Cloudflare pour les utilisateurs américains. Chrome, de son côté, n'impose pas un fournisseur unique : il tente de mettre à niveau le DNS que vous utilisez déjà si son équivalent DoH est connu, tout en permettant de définir une URL personnalisée. Edge propose un réglage « DNS sécurisé » avec plusieurs fournisseurs pré-renseignés et la possibilité d'indiquer son propre résolveur. Chez Apple, le chiffrement DNS est géré directement au niveau du système depuis iOS 14 et macOS 11, Safari suivant simplement

ce paramétrage.

Ces intégrations n'ont pas rendu l'écosystème entièrement centralisé, la majorité des internautes continuant d'utiliser les DNS de leur FAI. Mais la popularité des services DNS publics et les activations par défaut renforcent clairement la position de quelques acteurs privés majeurs, à commencer par Google, dont le navigateur concentre plus de 70 % des parts de marché dans le monde. Pas exactement un champion historique de la confidentialité.



DoH et DoT chiffrent les requêtes DNS pendant leur trajet, mais n'empêchent pas les résolveurs d'y accéder. © Zinetron / Shutterstock

## VPN et DNS, une confidentialité renforcée, mais pas absolue

Alors, quel choix reste-t-il ? Beaucoup se tournent vers les VPN en pensant résoudre définitivement le problème. En chiffrant l'intégralité du trafic jusqu'à l'un de leurs serveurs, ces réseaux privés virtuels masquent les requêtes DNS à votre fournisseur d'accès et à tout intermédiaire réseau. Mais la résolution des noms de domaine s'appuie alors sur l'infrastructure du réseau privé virtuel, souvent via ses propres résolveurs. On en revient donc à la même question : à qui faites-vous confiance pour manipuler vos requêtes ?

Certains clients VPN laissent toutefois la possibilité de définir un DNS personnalisé directement dans les réglages avancés de l'application. Dans ce cas, les requêtes sont chiffrées entre votre appareil et le serveur VPN, puis transmises au résolveur choisi. Le fournisseur de DNS voit donc les domaines consultés, mais il ne peut plus les relier directement à votre adresse IP réelle.

Combiné à un DNS chiffré (DoH ou DoT), ce mode de fonctionnement est aujourd'hui ce qui se rapproche le plus d'une confidentialité renforcée sur le plan technique, à condition, évidemment, de choisir un VPN transparent et audité sur sa gestion des données.



#### À DÉCOUVRIR

#### **Meilleur VPN, le comparatif en octobre 2025**

15 octobre 2025 à 08h38    Comparatifs services

## **Nos recommandations VPN pour mieux protéger vos requêtes DNS**

Chez Clubic, nous testons chaque année des dizaines de services VPN en toute indépendance. Nous examinons leur sécurité technique, la politique de confidentialité, la performance, mais aussi le rapport qualité-prix pour un usage quotidien. Voici ceux qui nous paraissent aujourd'hui les plus fiables si vous cherchez à mieux protéger vos requêtes DNS tout en bénéficiant d'une bonne vitesse et de fonctions avancées.

### **CyberGhost : abordable et bien équipé**