Fiche Pratique N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte V2.1

7 nov, 2026 · @Gabriel

Objectif : *Comprendre ce qu'un VPN fait réellement, ses limites, et comment aller plus loin pour un anonymat sérieux, y compris face à l'empreinte numérique du navigateur (fingerprinting). Cette version précise les outils à privilégier sur chaque plateforme.*

- ***Public visé :*** *Intermédiaire à avancé*
- ***Temps estimé :*** *30 minutes*
- ***Difficulté :*** *★★★☆☆ (Moyen)*
- ***Prérequis :*** *savoir installer une application et une extension de navigateur*
- ***Fiches associées :*** *N°32 (Tails), N°39 (empreinte numérique), N°45 (Warren VPN)*

1. Ce qu'un VPN fait vraiment (et ce qu'il ne fait pas)

Un VPN fait trois choses :

1. Il **chiffre** votre trafic entre votre appareil et le serveur VPN.
2. Il **masque** votre adresse IP : les sites voient celle du VPN.
3. Il **empêche votre fournisseur d'accès** de voir les sites que vous visitez… mais c'est désormais le fournisseur de VPN qui peut les voir.

Ce qu'un VPN ne fait pas :

- ❌ Il ne vous rend **pas anonyme**.
- ❌ Il ne vous protège **pas contre les traqueurs** (cookies, pixels, empreinte du navigateur).
- ❌ Il ne cache pas votre activité si vous êtes **connecté à vos comptes** (Google, Facebook…).
- ❌ Il ne supprime pas les **métadonnées** de vos fichiers.
- ⚠️ Contre les **fuites DNS et IPv6**, un bon client VPN protège (vérifiez-le) ; la fuite **WebRTC** se règle dans le navigateur.

Règle d'or : le VPN n'est qu'une couche parmi d'autres. L'anonymat est un curseur que vous ajustez en fonction de votre adversaire.

2. L'erreur n°1 : le navigateur connecté

La fuite d'identité la plus fréquente est aussi la plus simple : utiliser son navigateur habituel, connecté à ses comptes, pendant que le VPN est actif.

Pourquoi ? Si votre navigateur est connecté à Google (Gmail, YouTube…), Google associe l'adresse IP du VPN à votre compte. Les cookies et les services tiers (Google Analytics, reCAPTCHA…) font le reste.

Règle d'or : si votre objectif est l'anonymat, utilisez un **navigateur dédié**, sans connexion à vos comptes personnels.

3. Définir son modèle de menace

Avant de choisir un outil, posez-vous la question : **de qui ou de quoi voulez-vous vous protéger ?**

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte V2.1

Cas typique	Solution recommandée
Échapper au pistage publicitaire	Un bloqueur (uBlock Origin) et un navigateur protecteur ; le VPN n'y change presque rien
Cacher sa navigation à son fournisseur d'accès ou sur un Wi-Fi public	Un VPN de confiance (Mullvad, Proton VPN, y compris sa version gratuite)
Contourner une restriction géographique	Un VPN avec des serveurs dans le pays voulu (Proton VPN payant, Mullvad…)
Anonymat sérieux (comptes pseudonymes)	Mullvad payé anonymement + navigateur dédié (Mullvad Browser)
Journaliste, lanceur d'alerte	Tor Browser, ou Tails / Whonix
Résister à un blocage des VPN	Votre propre serveur (section 10), Tor avec des ponts

4. Qui possède vraiment votre VPN ?

Tous les VPN ne se valent pas. Certains appartiennent à des groupes dont l'historique pose question.

Kape Technologies (ex-Crossrider)

Crossrider, fondé en 2011, proposait un outil de création d'extensions de navigateur largement détourné par des logiciels publicitaires (adware). Racheté par l'homme d'affaires israélien Teddy Sagi, il est devenu Kape Technologies en 2018, groupe britannique et israélien basé à Londres.

Possède notamment :

- CyberGhost (2017) ;
- ZenMate (2018) ;
- Private Internet Access (2019) ;
- ExpressVPN (2021) ;
- et l'éditeur de sites de comparatifs de VPN Webselenese (2021).

À retenir : un comparatif de VPN peut appartenir à un vendeur de VPN. Croisez vos sources.

Et la politique « sans journaux » ?

Tous les fournisseurs doivent répondre aux décisions de justice de leur pays. Une politique « sans journaux » ne vaut que si elle est **vérifiée** : audits indépendants, rapports de transparence, et idéalement des saisies de serveurs restées sans résultat. Lisez la politique de confidentialité de votre fournisseur, quel qu'il soit.

5. Paiement vraiment anonyme

Un paiement anonyme ne suffit pas, mais un paiement nominatif suffit à vous identifier.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte V2.1

Moyen de paiement	Niveau d'identification
Carte bancaire, virement	Identité forte
PayPal	Identité forte
Bitcoin	Pseudonyme, mais traçable sur la chaîne
Monero (XMR)	Très discret (transactions opaques)
Espèces par courrier	Très discret (proposé par exemple par Mullvad)

Exemple : Mullvad coûte 5 €/mois, ne demande ni adresse e-mail ni nom (un numéro de compte suffit) et accepte les espèces par courrier ainsi que Monero et Bitcoin.

Deux pièges à éviter :

- l'adresse IP utilisée au moment du paiement ;
- l'adresse e-mail utilisée pour la facture.

⚠️ **Rappel :** un paiement anonyme ne sert à rien si vous vous connectez ensuite depuis un appareil ou des comptes déjà liés à votre identité.

6. Métadonnées : vos fichiers vous trahissent

Quand vous publiez un fichier, vous publiez aussi ses métadonnées :

Type de fichier	Métadonnées exposées
Photos	Position GPS, modèle de l'appareil, date et heure, parfois numéro de série
Vidéos	Logiciel, date, parfois position GPS
PDF	Nom de l'auteur, logiciel, dates
Documents bureautiques	Nom d'utilisateur, organisation, historique des modifications

Outils utiles :

- **ExifTool** : lecture et suppression des métadonnées en ligne de commande ;
- **mat2** : nettoyage de nombreux formats (en ligne de commande, et via l'application **Metadata Cleaner** sous Linux) ;
- **Signal** : retire les métadonnées des photos envoyées ;
- **Imprimer en PDF** : supprime une grande partie des métadonnées d'un document.

7. Système d'exploitation : là où ça se joue

Pour un anonymat sérieux, il devient difficile de rester sur Windows ou macOS.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte V2.1

Niveau	Recommandation
Débutant	VPN avec votre système actuel
Confirmé	Linux (Debian, Fedora, Linux Mint…)
Expert	GrapheneOS (mobile), Tails (clé USB), Whonix (machine virtuelle), Qubes OS

8. Hygiène du navigateur

Au minimum, en complément du VPN :

- un navigateur protecteur (Firefox, Brave, Mullvad Browser) ;
- **uBlock Origin** ;
- pas d'extensions superflues ;
- pas de connexion à Google, Facebook ou Apple dans ce navigateur ;
- DNS chiffré (DoH ou DoT) si vous n'utilisez pas de VPN.

Quatre niveaux :

Niveau	Configuration
1. Usage simple	Firefox ou Brave + uBlock Origin + VPN
2. Usage compartimenté	Un navigateur (ou un profil) par identité
3. Usage sérieux	Mullvad Browser + VPN, ou Tor Browser
4. Usage très sérieux	Tails ou Whonix

9. L'empreinte numérique du navigateur (fingerprinting)

Le **fingerprinting** identifie un navigateur en combinant de nombreuses informations : rendu graphique (Canvas, WebGL), traitement audio, polices installées, système, taille d'écran, fuseau horaire, langue… Un VPN n'y change rien.

Deux stratégies

Stratégie	Principe	Exemples
Uniformiser (recommandé)	Tous les utilisateurs présentent la même empreinte : vous vous fondez dans la masse	Tor Browser, Mullvad Browser
Brouiller	Des valeurs aléatoires changent votre empreinte d'un site ou d'une session à l'autre	Protections de Brave et de Firefox, extension Chameleon

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte V2.1

⚠️ **Le piège des extensions :** chaque extension ajoutée modifie le comportement du navigateur et peut vous rendre **plus reconnaissable**. Mullvad Browser déconseille d'ajouter des extensions de confidentialité, à part uBlock Origin déjà intégré.

Les outils recommandés

Outil	Ce qu'il fait	Pour qui
Mullvad Browser	Navigateur développé avec le Tor Project, sans le réseau Tor : configuration identique pour tous, mode « résistance à l'empreinte » de Firefox, polices limitées, fenêtre standardisée (letterboxing), uBlock Origin intégré	Usage sérieux, avec un VPN
Tor Browser	Même approche, avec le réseau Tor	Anonymat fort
Brave	Ajoute des variations aléatoires (Canvas, WebGL, audio) par site et par session	Usage quotidien
Firefox	Protections contre l'empreinte (bruit sur Canvas, polices et matériel standardisés) en **navigation privée** et en **protection renforcée stricte**	Usage quotidien
Chameleon (extension Firefox)	Modifie de nombreux paramètres (agent utilisateur, fuseau horaire, langue, WebRTC…)	Utilisateurs avancés qui savent ce qu'ils font

10. Installation et vérification par plateforme

10.1. Ordinateur (Windows, macOS, Linux)

Option A : Mullvad Browser (recommandé)

1. Téléchargez **Mullvad Browser** depuis le site de Mullvad (il est gratuit et fonctionne avec n'importe quel VPN).
2. Installez-le et lancez-le, sans modifier les réglages ni ajouter d'extensions.
3. Connectez votre VPN.

Option B : Firefox avec les protections intégrées

1. Ouvrez Firefox › **Paramètres** › **Vie privée et sécurité**.
2. Choisissez **Protection renforcée contre le pistage** › **Stricte**.
3. Installez **uBlock Origin** depuis addons.mozilla.org.

Option C : Firefox + Chameleon (avancé)

1. Installez **Chameleon** depuis addons.mozilla.org.

gabriel.ananda@mailo.com
CC BY SA

2. Cliquez sur son icône et activez, selon vos besoins, la protection WebRTC, l'usurpation du fuseau horaire et de la taille d'écran.
3. N'ajoutez pas d'autre extension anti-empreinte : elles se contrediraient.

Vérification :

1. Ouvrez **coveryourtracks.eff.org** (EFF) et lancez le test.
2. Ouvrez **browserleaks.com** pour vérifier l'adresse IP, le DNS et WebRTC avec le VPN actif.

Vous devez voir :

- l'adresse IP du VPN, sans fuite DNS ni WebRTC ;
- avec Mullvad Browser ou Tor Browser, une empreinte partagée par de nombreux utilisateurs ;
- avec Brave, Firefox ou Chameleon, une empreinte « randomisée ».

10.2. Android

Depuis décembre 2023, **Firefox pour Android** accepte des centaines d'extensions, installables depuis addons.mozilla.org.

1. Installez **Firefox** (ou **Tor Browser** pour Android).
2. Ouvrez **Menu** › **Extensions** et installez **uBlock Origin**.
3. Dans **Paramètres** › **Protection renforcée contre le pistage**, choisissez **Stricte**.
4. Vérifiez avec coveryourtracks.eff.org.

Alternative : **Brave** pour Android intègre ses protections sans extension.

10.3. iOS et iPadOS

Sur iPhone, les navigateurs reposent sur WebKit, le moteur de Safari (dans l'Union européenne, d'autres moteurs sont autorisés mais encore rares). Safari accepte des extensions et des bloqueurs de contenu depuis l'App Store, mais aucune extension ne remplace un navigateur conçu contre l'empreinte.

Solutions :

1. **Safari** : **Réglages** › **Apps** › **Safari** › activez **Protection avancée contre le pistage et l'empreinte** pour toute la navigation (et non seulement en navigation privée).
2. **Brave** pour iOS, qui intègre blocage et protections contre l'empreinte.
3. **Onion Browser**, recommandé par le Tor Project pour utiliser Tor sur iOS.
4. **Un VPN au niveau du routeur** pour protéger tous les appareils de la maison (section 12).

11. L'alternative : votre propre VPN sur un serveur

Principe : vous louez un VPS, vous y installez WireGuard, et votre trafic sort par l'adresse IP de ce serveur.

Avantages :

gabriel.ananda@mailo.com
CC BY SA

- moins souvent repéré comme VPN par les outils de détection (l'adresse est celle d'un hébergeur, pas d'un service VPN connu) ;
- bonnes performances ;
- contrôle total.

Inconvénients :

- adresse IP fixe et propre à vous : vous êtes reconnaissable ;
- l'hébergeur connaît votre identité (sauf paiement anonyme) ;
- aucun anonymat réel.

À retenir : un VPN personnel est utile pour contourner un blocage ou sécuriser un Wi-Fi public, mais ce n'est pas un outil d'anonymat.

12. Le VPN au niveau du routeur

Des failles et des comportements d'Android et d'iOS ont déjà permis à certains échanges de contourner le VPN de l'appareil (par exemple les vérifications de connectivité d'Android). Un VPN installé sur le routeur couvre tout le réseau.

Avantages :

- protection de tous les appareils (télévision, consoles, objets connectés) ;
- aucune application ne peut sortir du réseau sans passer par le VPN ;
- configuration unique.

Inconvénients :

- nécessite un routeur compatible (OpenWrt, WireGuard) ;
- configuration plus technique ;
- moins souple : tout le trafic passe par le VPN.

13. Tailscale + Mullvad : un compromis pour les utilisateurs avancés

Principe : Tailscale relie vos appareils entre eux (réseau privé), et une option payante permet de sortir sur Internet par les serveurs de Mullvad.

Avantages :

- simplicité ;
- accès à vos appareils et serveurs personnels ;
- adresse IP de sortie Mullvad.

Inconvénients :

- Tailscale connaît votre identité (connexion par un compte Google, Microsoft, GitHub…) et gère l'accès à Mullvad pour vous ;
- moins anonyme que Mullvad seul.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte V2.1

Cas d'usage : confort et vie privée au quotidien, pas anonymat.

14. DAITA : contre l'analyse de trafic (Mullvad)

DAITA (Defense Against AI-guided Traffic Analysis), développé par Mullvad avec l'université de Karlstad, mélange de **faux trafic** à vos échanges. Objectif : empêcher un observateur du réseau de deviner les sites visités à partir de la taille et du rythme des paquets chiffrés, même avec l'aide de l'intelligence artificielle. Le contenu restait déjà chiffré : DAITA protège contre l'analyse des **métadonnées** du trafic.

Activer DAITA :

1. Ouvrez l'application Mullvad.
2. Allez dans **Paramètres** › **Paramètres VPN** › **Paramètres WireGuard** › **DAITA** (le chemin peut varier selon la version et la plateforme).
3. Activez l'option.

Vous devez voir :

- la mention « using DAITA » à côté du nom du serveur une fois connecté.

Limites : disponible sur les serveurs compatibles uniquement ; consomme davantage de données et peut ralentir la connexion.

15. Et la régulation des VPN ?

Des projets de régulation (vérification d'âge, lutte contre le piratage) visent régulièrement les VPN, en Europe comme ailleurs. Un État ne contrôle que ce qui relève de sa juridiction :

- des fournisseurs établis dans d'autres pays (Mullvad en Suède, Proton en Suisse) restent accessibles tant qu'ils ne sont pas bloqués ;
- un serveur personnel ou Tor avec des ponts permettent de résister à un blocage technique.

⚠️ Restez dans la légalité : contourner un blocage peut être interdit dans certains pays.

16. En résumé

À retenir	Détail
Un VPN seul ne rend pas anonyme	C'est une couche parmi d'autres
L'erreur n°1 : le navigateur connecté	Utilisez un navigateur dédié
Le VPN ne bloque pas l'empreinte	Mullvad Browser, Tor Browser, Brave, Firefox strict
Trop d'extensions vous rendent unique	Préférez un navigateur conçu contre l'empreinte
Définissez votre modèle de menace	L'outil dépend de l'adversaire
Le paiement révèle votre identité	Monero ou espèces
Les métadonnées vous trahissent	Nettoyez vos fichiers (mat2, ExifTool)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte V2.1

À retenir	Détail
Le système compte	Linux, Tails, Whonix, GrapheneOS
VPN sur le routeur	Protège tous les appareils
Tailscale + Mullvad	Confort, pas anonymat
DAITA (Mullvad)	Contre l'analyse de trafic

Conclusion

Un VPN est un excellent outil, mais ce n'est qu'une couche. Pour un anonymat réel, vous devez :

1. **définir votre modèle de menace** (adversaire, risques) ;
2. **combiner plusieurs couches** : VPN, navigateur conçu contre l'empreinte, nettoyage des métadonnées, système adapté ;
3. **adopter une hygiène stricte** : navigateur dédié, aucun compte personnel, paiement anonyme.

À retenir absolument

- **Le VPN déplace la confiance** de votre fournisseur d'accès vers le fournisseur de VPN : choisissez-le bien.
- **Contre l'empreinte, mieux vaut ressembler à tout le monde** (Mullvad Browser, Tor Browser) qu'empiler des extensions.
- **Votre comportement compte plus que vos outils :** comptes connectés, paiement, métadonnées.

Test final :

1. J'ai écrit mon modèle de menace en une phrase.
2. Avec le VPN actif, browserleaks.com affiche l'IP du VPN, sans fuite DNS ni WebRTC.
3. J'utilise un navigateur dédié, sans mes comptes personnels.
4. J'ai testé mon navigateur sur coveryourtracks.eff.org.
5. Je sais retirer les métadonnées d'une photo avant de la publier.
6. Si tout est fait : vous savez ce que votre VPN protège… et ce qu'il ne protège pas ✅

Références

- Wikipédia – Kape Technologies (Crossrider, CyberGhost, ZenMate, PIA, ExpressVPN, Webselenese)
- Mullvad – Tarifs et moyens de paiement (espèces, Monero, 5 €/mois)
- Mullvad – DAITA disponible sur Linux et macOS (activation)
- Mullvad – Mullvad Browser (se fondre dans la masse)
- PC Gamer – Firefox renforce sa protection contre l'empreinte (navigation privée, mode strict)
- AlternativeTo – Plus de 450 extensions disponibles sur Firefox pour Android (décembre 2023)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte V2.1

- GitHub – Chameleon (sereneblue)

gabriel.ananda@mailo.com
CC BY SA