

Tendre vers une connexion internet confidentielle et anonyme

Info

Prérequis

- [Générer ses mots de passe et les gérer](#)
- [Mails militants](#) pour ProtonVPN

Intérêts de la mesure et menaces qu'elle permet de tempérer

En implémentant et respectant les préconisations de ce tutoriel, ta connexion internet tend à être anonyme et confidentielle.

C'est donc une réaction face à la menace de réquisition des données de trafic Internet auprès de ton Fournisseur d'Accès Internet (FAI) ou des outils et services que tu utilises notamment.

Difficulté

accessible (*installations classiques, pas de concepts compliqués*)

Temps requis 10min

Matériel requis

- téléphone et/ou ordinateur
- connexion Internet

Inconvénients

Aucun, si ce n'est une connexion légèrement ralentie (pour les offres gratuites)

Ce qu'on va faire dans ce tutoriel

- installer et configurer un VPN
- installer Tor



Vocabulaire

VPN : Virtual Private Network

Info



hello

VPN

Un VPN permet de créer un intermédiaire entre tes requêtes internet et ton FAI. Ton FAI ne peut plus savoir ce que tu cherches sur internet, et les sites que tu consultes ne peuvent plus connaître ton IP (qui permet de remonter à l'identité). Cependant, ton fournisseur de VPN connaît ces informations et peut être amené à les livrer aux flics. Il s'agit donc de faire confiance à ce fournisseur pour ne pas stocker ces données.

Pour en savoir plus sur l'utilité de l'outil VPN, il existe la *fiche outil* [VPN](#) qui détaille tout ça.

Nous conseillons les fournisseurs de VPN suivants :

- [Mullvad](#) (5€/mois pour 5 appareils) : nécessite la création d'un compte, disponible sur toutes les plateformes
- [Riseup VPN](#) (à prix libre) : pas de compte nécessaire, peut être un peu lent
- [Proton VPN](#) (en utilisant l'offre gratuite) : nécessite la création d'un compte, disponible sur toutes les plateformes

Ces 3 services sont considérés comme des hébergeurs de confiance. Mullvad et Proton ont fait l'objet d'audits de sécurité externe. Riseup est un collectif militant dont la longue histoire lui confère une bonne confiance.

Mullvad VPN permet d'avoir une meilleure stabilité et limite donc les situations pratiques où ton usage d'internet (par ex. [Faire une visio](#)) est dégradé et te pousse dans l'urgence à désactiver le VPN.

Attention



Sur ton ordinateur, si tu quittes l'application ProtonVPN, le VPN sera déconnecté et toute confidentialité perdue.

Mullvad VPN

Création d'un compte

Pour utiliser Mullvad, service exclusivement payant, il faut te créer un compte Mullvad et le créditer. Cela coûte 5€ par mois pour 5 appareils au maximum, et si tu mets par exemple 60€

de crédit ton compte sera valide pendant 1 an. Tu peux [créer un compte depuis un navigateur web](#), ce qui consiste simplement en la génération d'une série de 16 chiffres générés aléatoirement (pas de mail ou d'identifiant nécessaires).

Pour créditer ton compte, tu peux :

- payer par CB sur le site pour créditer le compte.

✓ Succès

Mullvad ne garde pas d'information de la transaction bancaire. Cependant, un numéro lié à ton compte sera inscrit dans la transaction et visible dans ton compte bancaire. Si des flics demandent à consulter tes comptes et voient ce numéro, il serait possible avec la coopération de Mullvad de connaître le compte que tu utilises (cf <https://mullvad.net/en/account/recover/card>

- demander à un.e pote à toi qui est moins à risque de faire l'achat pour toi
- acheter un coupon à gratter "Mullvad voucher" sur Amazon, le gratter et renseigner les chiffres apparus sur ton compte Mullvad. Cela va créditer le compte de la somme à laquelle tu as acheté ton coupon. Il n'y aura donc aucun lien entre la CB utilisée et le compte crédité ! Tu peux faire une commande groupée de coupons pour recharger les comptes Mullvad de tout ton comité local.
- envoyer de l'argent liquide par la poste [à partir d'un jeton généré depuis ton compte](#). Cela met 2-3 semaines pour être traité.

Installation

Sur Android : télécharge l'application directement sur ton magasin d'applications

Sur ordinateur : rends-toi sur <https://mullvad.net/fr/download/vpn/> pour télécharger directement l'application.

Riseup VPN

Installation

Sur Android : télécharge l'application directement sur ton magasin d'applications

Sur ordinateur : rends-toi sur <https://riseup.net/fr/vpn/> pour télécharger directement l'application, et suis les consignes relatives à ton système d'exploitation.



Attention



Contrairement à Mac ou Linux, il n'y a pas de killswitch (coupe-feu) sur windows, paramètre qui permet d'être sûr que toute connexion internet passe par le VPN.

Proton VPN

Installation

Sur smartphone : télécharge l'application directement sur ton magasin d'applications

Sur ordinateur : rends-toi sur <https://protonvpn.com/download> pour télécharger directement l'application.

Création d'un compte

À l'ouverture de l'application sur ton ordinateur ou ton téléphone, il te sera demandé de te connecter à ton compte : il faut donc en créer un. Crée-toi un compte mail dédié sur ProtonMail, et utilise cet email **uniquement** pour t'identifier dans l'application ProtonVPN.

Tu peux stocker les identifiants en suivant le tuto

[Générer ses mots de passe et les gérer](#)

Il te sera demandé un numéro de téléphone ou un mail comme moyen de récupération du compte, tu peux refuser.

Configuration pour tout type de VPN

Il faut t'assurer que la configuration de l'application empêche les connexions internet si le VPN est désactivé.

Sur Android : dans Paramètres > Réseaux > VPN > Paramètres, active "toujours actif" et "bloquer les connexions sans VPN". Tu peux aussi accéder à ce paramétrage système en utilisant la fonction recherche dans l'application Paramètres de ton téléphone ou depuis les paramètres de l'application.

Sur iOS : dans l'application ProtonVPN, active le coupe-circuit dans Paramètres > Options de sécurité. Dans Mullvad VPN, active-le dans Paramètres > Paramètres VPN

Sur ordinateur : dans les paramètres de l'application, assure-toi que les options suivantes sont bien activées : "lancement au démarrage", "kill switch" (ou "coupe-circuit") et "lockdown mode".

Tutoriel officiel du paramétrage du coupe-circuit sur ProtonVPN avec captures d'écran consultable [ici](#) (en anglais).

Tor

On parle ici uniquement du [Tor Browser](#), c'est-à-dire le navigateur web qui permet de se connecter au réseau Tor.

Le réseau Tor fait passer vos requêtes successivement entre au moins 3 serveurs, ce qui décorrèle l'IP source de l'IP de destination (c'est à dire entre vous et les sites que vous consultez). Il n'y a donc pas d'entité tierce qui puisse être capable de livrer vos informations aux flics.

Attention

À moins d'utiliser [Tails](#), uniquement les connexions s'effectuant dans la fenêtre du navigateur sont protégées par les techniques d'anonymisation de Tor et non pas l'ensemble des connexions internet comme c'est le cas avec un VPN.

Installation

Sur Android : tu peux télécharger l'application [Tor Browser](#) directement sur ton magasin d'applications

Sur iOS : [Tor Browser](#) n'est pas disponible sur iOS mais tu peux télécharger [Onion Browser](#) qui est un navigateur non développé par la fondation Tor et permet d'accéder à Tor dans le navigateur. Cependant, dû à des limitations de iOS, il ne permet pas les même garanties de sécurité que [Tor Browser](#).

Sur ordinateur : rends toi sur <https://www.torproject.org/fr/download/> pour télécharger directement l'application.

Configuration

Le navigateur Tor est configuré par défaut pour assurer ta sécurité. Ne change pas les paramètres de ton application à moins que tu saches très clairement ce que tu fais.