Comment configurer et utiliser un VPN

NDLR: Mise à jour décembre 2023

Il n'y a pas si longtemps, les réseaux privés virtuels (VPN) étaient l'apanage des entreprises et d'un certain type de personnes soucieuses de leur vie privée.
Aujourd'hui, il existe un marché florissant de VPN commerciaux avec des applications astucieuses à des prix abordables qui ne nécessitent aucun savoir-faire en matière de réseau pour être utilisées.
Il est difficile de se frayer un chemin à travers le battage publicitaire (et il y en a beaucoup), et une fois que vous avez trouvé un VPN, comment l'utiliser ?
Nous vous aiderons à comprendre ce que les VPN font le mieux, comment en choisir un bon et comment l'utiliser pour améliorer votre confidentialité en ligne.

Avez-vous besoin d'un VPN ?

Les VPN sont plus faciles à utiliser que jamais, mais expliquer à quoi ils servent ne l'est pas. Mais cela pourrait aider.
En 2021, la Federal Trade Commission a publié un rapport décrivant ce que les fournisseurs d'accès à Internet (FAI) savent de leurs clients (vous).
Un paragraphe particulier du rapport plaide en faveur des VPN :

> Cela signifie qu'un seul FAI a la possibilité de suivre les sites Web visités par ses abonnés, les émissions qu'ils regardent, les applications qu'ils utilisent, leurs habitudes énergétiques, leurs allées et venues en temps réel et leur emplacement historique, les requêtes de recherche qu'ils effectuent et le contenu de leurs communications par e-mail. [...]
> Ils utilisent ces données pour créer des segments publicitaires, y compris des segments qui révèlent des données sensibles telles que la race, la religion, l'origine nationale, l'orientation sexuelle, la situation financière, l'état de santé et les convictions politiques.

C'est là que les VPN peuvent vous aider.
Ces applications de protection de la vie privée empêchent même les personnes disposant d'un accès privilégié de voir vos données.
Mais, comme pour tout outil, il est essentiel de comprendre les limites d'un VPN.
Après tout, vous ne vous attendriez pas à ce qu'un gilet en Kevlar vous sauve d'une chute d'un avion ou qu'un parachute arrête une balle.

Lorsque vous activez un VPN, votre trafic est acheminé via un tunnel crypté vers un serveur exploité par la société VPN.
Cela signifie que votre FAI ne sera pas en mesure de voir votre trafic Web.
Même les opérateurs du réseau ne seront pas en mesure de jeter un coup d'œil à vos activités.

Étant donné que votre trafic semble provenir du serveur du VPN, votre adresse IP réelle est effectivement masquée.
Il est donc plus difficile de vous suivre lorsque vous vous déplacez sur le Web, et comme les adresses IP sont distribuées géographiquement, cela masque votre véritable emplacement.
Cela peut s'avérer utile si vous souhaitez usurper votre emplacement.
En vous connectant à un serveur VPN à Londres, vous avez l'impression d'accéder à Internet depuis le Royaume-Uni.

Comment fonctionne un VPN ?

Capture d'écran, pour visionner la vidéo, cliquer le lien suivant:

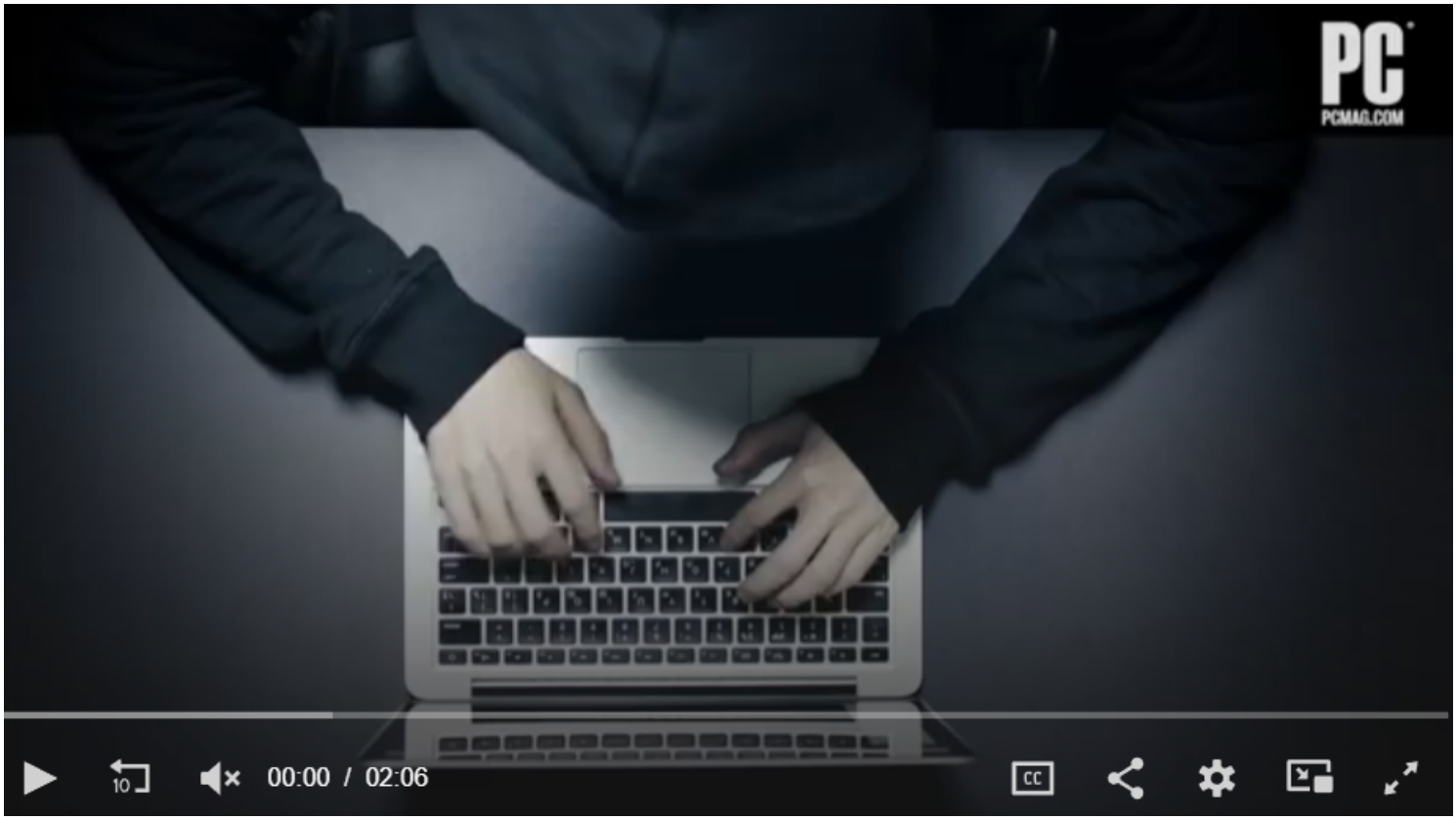
Comment configurer et utiliser un VPN | PCMag

Ce qu'un VPN *ne fera pas, c'est* anonymiser complètement votre trafic.
Pour cela, vous voudrez utiliser le réseau d'anonymisation gratuit Tor.
Au lieu de simplement faire passer vos données par un seul intermédiaire (tel qu'un serveur VPN), Tor fait rebondir vos données via plusieurs ordinateurs volontaires différents.
Il est donc beaucoup plus difficile pour quelqu'un qui essaie de suivre vos activités de voir ce que vous faites, mais notez que cela ralentira votre trafic Web.

De plus, les sites Web peuvent suivre vos mouvements grâce à des cookies, à l'empreinte digitale du navigateur, à des traqueurs en ligne et à d'autres outils délicats.
L'installation d'un bloqueur de publicité et l'utilisation de tous les outils de confidentialité que l'on trouve dans la plupart des navigateurs modernes peuvent rendre beaucoup plus difficile pour les annonceurs de suivre vos mouvements sur le Web.

Enfin, ce n'est pas parce que vous avez un VPN que vous pouvez oublier les bases de la sécurité.
Alors que certains services VPN prétendent pouvoir bloquer les logiciels malveillants, nous recommandons un logiciel antivirus autonome pour votre ordinateur, car ces outils sont conçus pour protéger votre ordinateur contre les logiciels malveillants.
Vous pouvez vous protéger contre les violations de mots de passe à l'aide d'un gestionnaire de mots de passe, car les mots de passe recyclés constituent un point de défaillance majeur.

Avec un gestionnaire de mots de passe, vous pouvez avoir des mots de passe énormes et aléatoires pour chaque site.
Lorsque vous verrouillez vos mots de passe, activez l'authentification multifacteur dans la mesure du possible.



Capture d'écran, pour visionner la vidéo, cliquer le lien suivant:

Comment configurer et utiliser un VPN | PCMag

Qu'est-ce que l'authentification à deux facteurs ?

Comment choisir un VPN

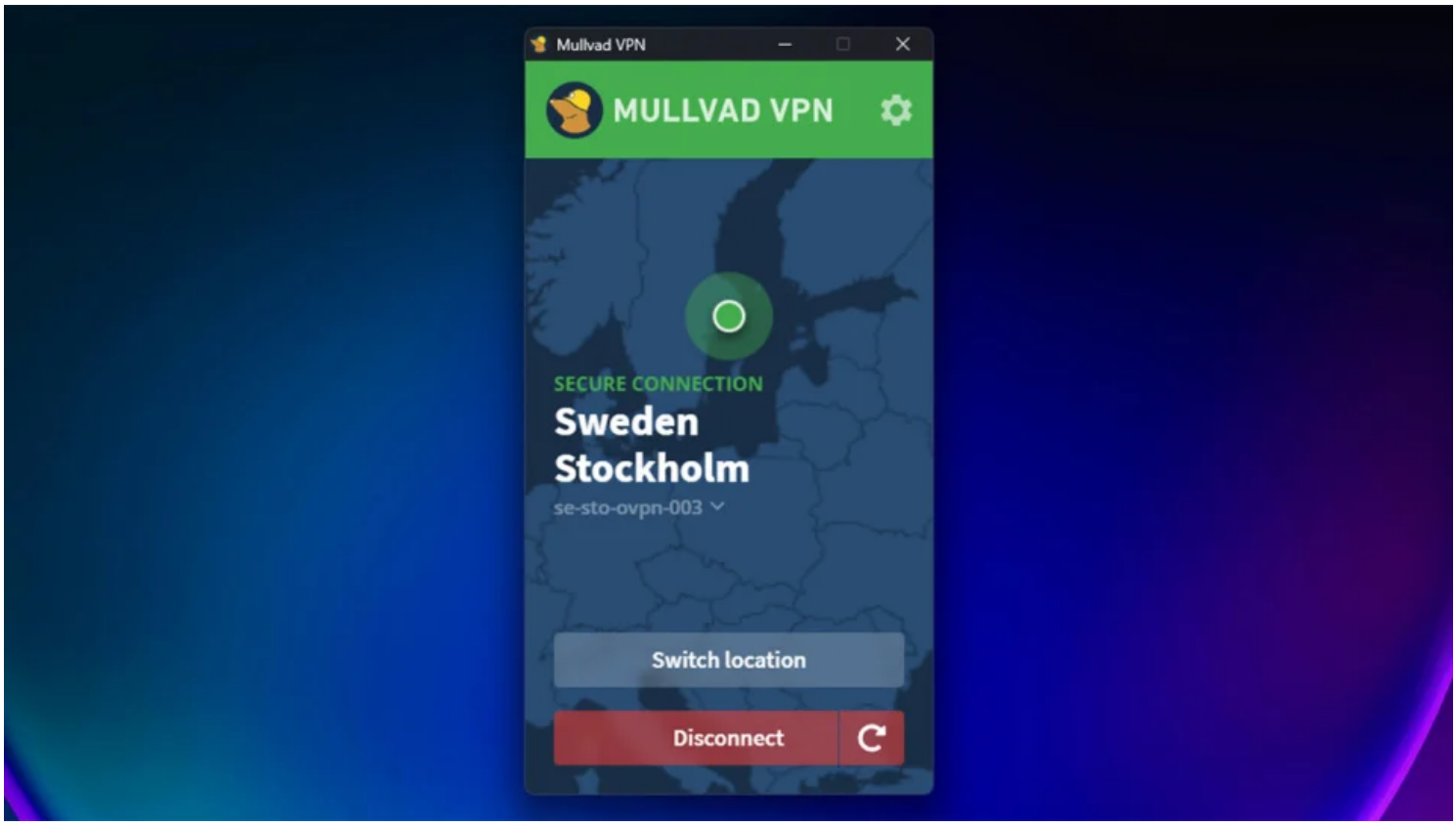
Lorsque nous testons et examinons les VPN, nous prenons en compte quelques indicateurs clés.
D'une part, un service VPN devrait vous permettre de connecter au moins cinq appareils simultanément.
Les meilleurs services dépassent désormais facilement cette exigence, et certains n'imposent désormais aucune limite aux connexions simultanées.
Une autre exigence de base est qu'un service VPN doit autoriser le trafic BitTorrent ou P2P sur ses serveurs, si vous prévoyez d'utiliser l'une ou l'autre de ces technologies. Presque tous les VPN les autorisent sur au moins certains de leurs serveurs, mais vous ne voulez pas vous mettre à dos l'entreprise à laquelle vous payez des frais mensuels.

En parlant de frais, le coût moyen que nous avons vu sur les services VPN examinés par PCMag est de 9,90 USD$ pour un abonnement mensuel.
Un service VPN qui facture plus par mois ne vous arnaque pas nécessairement. Néanmoins, il devrait offrir

quelque chose d'important, comme une excellente interface ou de nombreux emplacements de serveurs pour adoucir l'affaire.

Vous pouvez généralement obtenir une réduction si vous achetez des contrats à plus long terme.
Le prix moyen d'un abonnement VPN annuel que j'ai vu sur trois douzaines de produits est de 66,28 USD$.
Cependant, nous vous recommandons d'éviter les longs engagements jusqu'à ce que vous soyez sûr d'être satisfait du service.
Commencez par un abonnement à court terme ou, mieux encore, un abonnement gratuit pour tester un VPN chez vous.

Il est également utile de savoir où une société VPN est basée.
Il ne s'agit pas toujours de l'emplacement physique de l'entreprise, mais d'une distinction juridique qui explique la juridiction dans laquelle l'entreprise est domiciliée à des fins juridiques.
Les lois locales peuvent (ou non) signifier que ces entreprises ne sont pas redevables aux lois sur la conservation des données, ce qui les obligerait à conserver certaines informations (vos données, par exemple) qui pourraient être obtenues par les forces de l'ordre.



Contrairement à ce serveur VPN, Mullvad VPN est situé en Suisse. (Crédit : Mullvad VPN)

De nombreux lecteurs s'inquiètent de l'impact des VPN sur leurs vitesses Internet.
Chez PCMag, nous effectuons des tests de vitesse approfondis pour déterminer le VPN le plus rapide.
Cela dit, nous ne pensons pas que la vitesse devrait être le facteur principal lors du choix d'un VPN.
Il y a tellement de variations dans les performances qu'un service avec les meilleurs scores aujourd'hui pourrait être pokey demain.
Nous vous recommandons de tester un service sur votre réseau domestique pour voir comment il fonctionne,

en sachant qu'il y aura toujours un coût de performance et qu'il peut varier d'un jour à l'autre, voire d'une heure à l'autre.

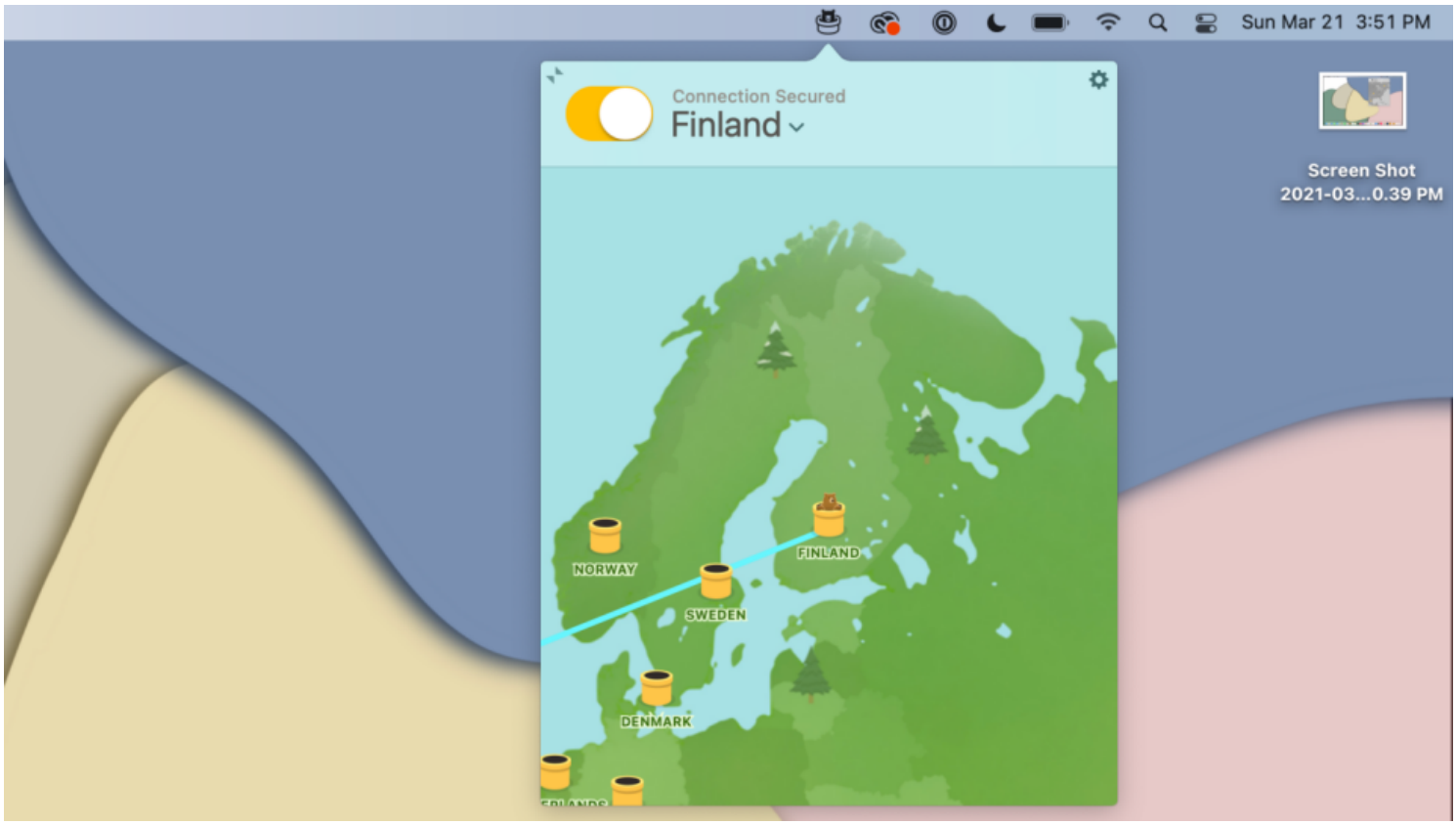
Une question que les lecteurs se posent souvent est de savoir s'ils peuvent faire confiance à un VPN.
Après tout, les VPN ont accès à tout le même trafic qu'un FAI, et ils peuvent essayer de le monétiser ou être un mauvais intendant de votre vie privée et transmettre des informations aux pirates ou aux forces de l'ordre.
Dans nos examens, nous passons beaucoup de temps à essayer de répondre à cette question en discutant avec les entreprises, en examinant leurs politiques, etc.
Parmi les signes d'un VPN digne de confiance, citons une politique de confidentialité claire et compréhensible, un rapport de transparence et des audits tiers qui examinent l'application de la politique et l'infrastructure.

Si l'emplacement, le prix ou les conditions d'utilisation ne vous rassurent pas, essayez un autre service.
Dans tous nos avis sur les VPN, nous rendons compte de tous ces problèmes et mettons en évidence tout ce que nous pensons être déroutant ou problématique.

Dois-je payer pour un VPN ?

Les VPN gratuits qui en valent la peine sont rares, mais ils existent.
Quelques services VPN proposent un essai gratuit, généralement pour une durée limitée. D'autres, comme TunnelBear VPN, proposent des abonnements gratuits, mais limitent les données que les abonnés gratuits peuvent utiliser.
Proton VPN est notre premier choix pour les VPN gratuits, car il n'impose aucune limitation de données aux utilisateurs gratuits.

Malheureusement, la plupart des VPN sont loin d'être gratuits, mais vous n'avez pas besoin de vous ruiner pour en obtenir un.
Notre liste de VPN bon marché est un excellent point de départ si vous êtes pressé.



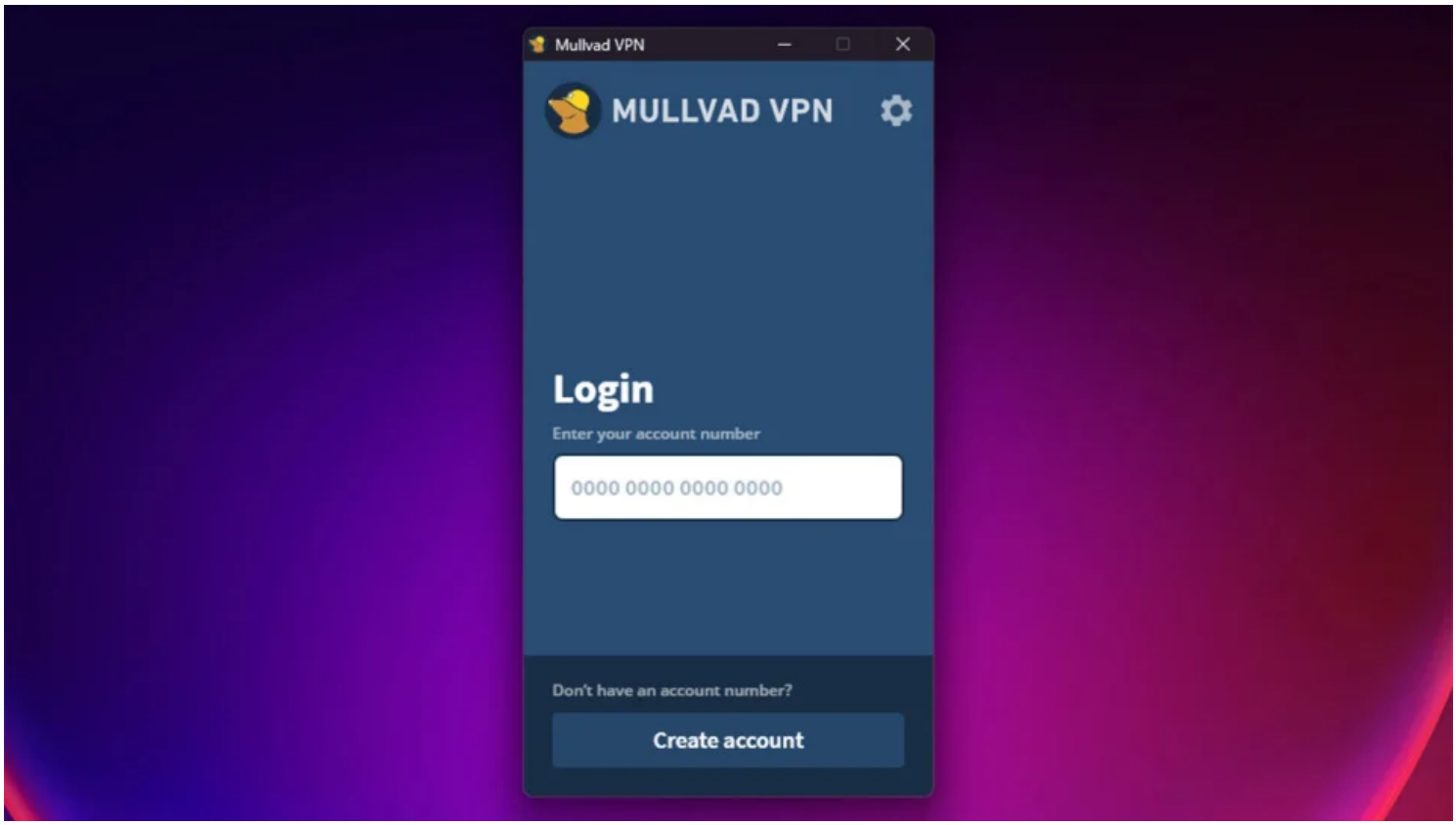
TunnelBear dispose d’une interface conviviale et propose un abonnement gratuit. (Crédit : TunnelBear VPN)

Premiers pas avec un VPN

Une fois que vous avez choisi un service, la première chose à faire est de récupérer l’application de l’entreprise, généralement à partir de la page Téléchargements du site Web du service VPN.
Téléchargez les applications pour votre appareil mobile pendant que vous y êtes.
Si le service VPN que vous envisagez ne propose pas d’application pour vos appareils, envisagez de trouver un autre service.

Certaines entreprises ont un ensemble d’applications disponibles sur les magasins d’applications et un autre sur le site Web de l’entreprise.
Cela semble être pour se conformer aux restrictions imposées par les propriétaires de magasins d’applications.
Il peut être difficile de déterminer ce qui fonctionnera pour vous, alors lisez attentivement la documentation de l’entreprise.

Une fois que vous avez installé les applications, vous êtes généralement invité à saisir vos informations de connexion.
Dans la plupart des cas, il s’agit du nom d’utilisateur et du mot de passe que vous avez créés lors de votre inscription au service.
Certaines entreprises, telles que IVPN et Mullvad VPN, lauréats du prix Editors' Choice, utilisent des systèmes de connexion protégeant la vie privée qui peuvent initialement prêter à confusion.
Assurez-vous de lire attentivement les instructions.



Mullvad VPN utilise un système de compte qui ne nécessite que votre numéro de compte pour y accéder. (Crédit : Mullvad VPN)

Une fois connectée, votre application VPN se connecte généralement au serveur VPN le plus proche de votre emplacement actuel.
Cela permet d'obtenir de meilleures vitesses lors de l'utilisation du VPN, car les performances se dégradent à mesure que le serveur VPN est éloigné de votre emplacement réel.
Et voilà : vos informations sont maintenant transmises en toute sécurité au serveur VPN.

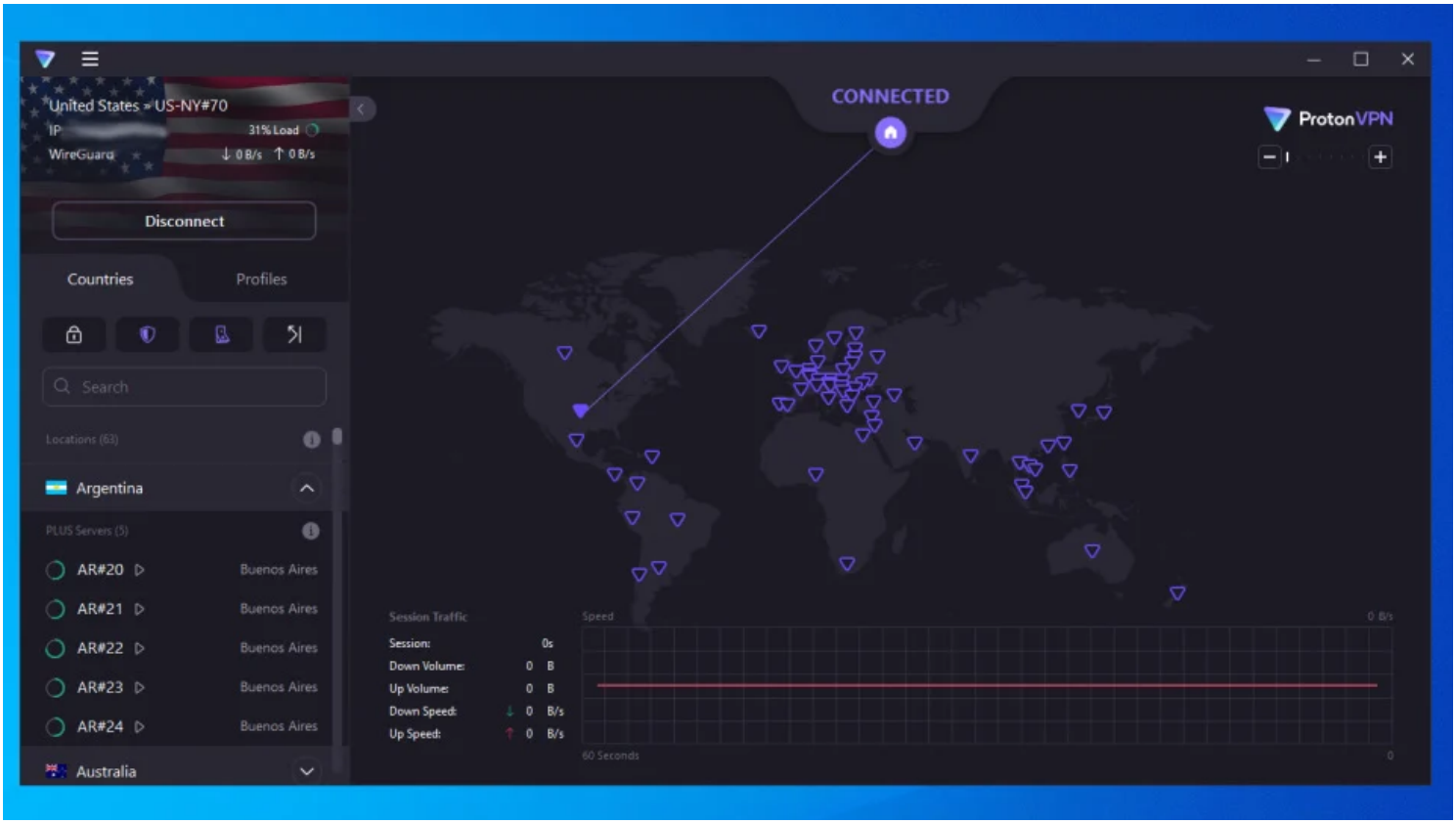
Certains lecteurs peuvent rechigner à installer une autre application sur leurs appareils.
Si vous avez une mentalité plus bricoleuse, vous pouvez ignorer l'application et le faire à l'ancienne.
Cela implique généralement de modifier les paramètres du système d'exploitation pour utiliser l'infrastructure du service VPN.
La plupart des services VPN disposent d'une documentation sur la configuration de votre appareil.

Cela dit, nous décourageons les gens de s'engager dans cette voie.
La configuration manuelle signifie que vous devrez maintenir *manuellement* à jour les informations du serveur sur votre ordinateur.
Vous ne pourrez pas non plus accéder à toutes les autres fonctionnalités fournies par le service VPN pour lequel vous payez déjà.
Consultez notre article sur la configuration d'un VPN dans Windows 11 pour en savoir plus si vous envisagez courageusement cette voie.

Comment choisir le bon serveur VPN

Parfois, vous ne voudrez peut-être pas être connecté au serveur recommandé par l'application VPN.
Peut-être souhaitez-vous usurper votre emplacement ou profiter des serveurs personnalisés fournis par votre VPN.
Ou peut-être que le serveur choisi par l'application ne fonctionne pas ou est très lent. Quelle que soit la raison, les meilleurs VPN vous permettent de passer rapidement et facilement à un autre serveur VPN.

Parfois, les applications VPN présentent leurs serveurs dans de longs menus ou des listes déroulantes.
Les meilleurs services VPN incluent des barres de recherche et des serveurs de mise en évidence pour des activités spécifiques telles que le streaming et l'utilisation de BitTorrent. De nombreuses sociétés VPN ont une carte interactive dans le cadre de leur application. TunnelBear VPN et NordVPN, par exemple, vous permettent de cliquer sur les pays pour vous y connecter aux serveurs.



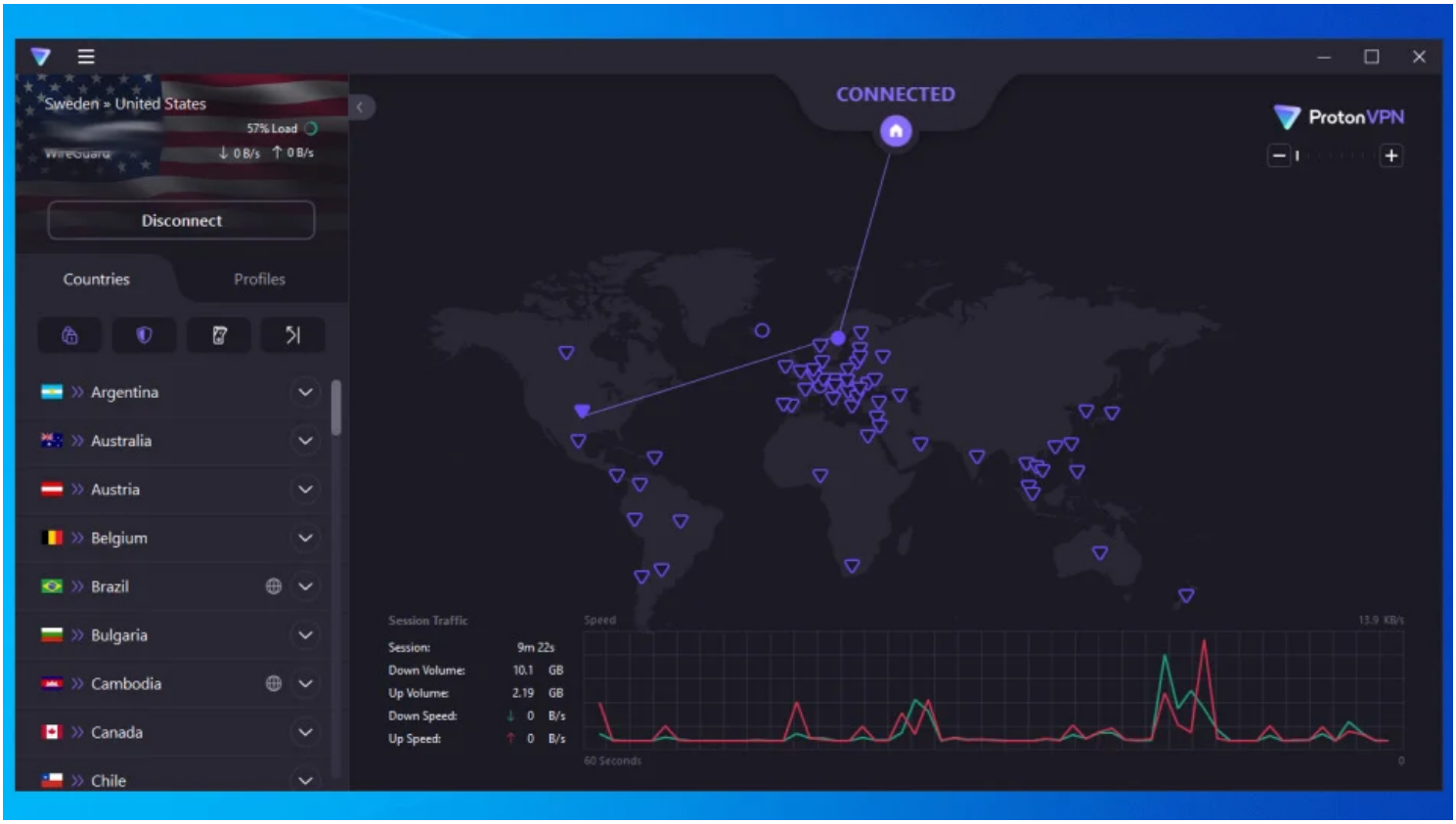
Proton VPN dispose d'une liste de serveurs disponibles, mais vous pouvez également utiliser une carte interactive. (Crédit : Proton VPN)

Le choix d'un serveur dépend entièrement de ce que vous voulez accomplir.
Pour de meilleures vitesses, vous devez choisir un serveur à proximité.
Pour accéder à du contenu verrouillé par région, vous aurez besoin d'un serveur local pour le contenu que vous souhaitez regarder.

Certaines sociétés VPN ont des serveurs spécialisés pour le streaming vidéo.
Ces serveurs spécialisés sont utiles car les services de streaming tels que Netflix bloquent les VPN.
Ces accords de licence conclus par Netflix avec les studios sont un problème, car ils fournissent un contenu différent pour différentes régions.

Recommandé par nos rédacteurs

Les meilleurs services VPN ont des options de sécurité améliorées, telles que l'accès à Tor ou aux VPN multi-sauts.
Tor, comme mentionné ci-dessus, est un moyen de mieux protéger votre vie privée et vous permet d'accéder à des sites Web cachés sur ce que l'on appelle le dark web.
Le VPN multi-sauts est similaire : au lieu de simplement acheminer votre trafic via un seul serveur VPN, une connexion multi-sauts vous tunnelise vers un serveur, puis un autre. Ces deux offres troquent la vitesse contre une confidentialité accrue.



Proton VPN qualifie ses connexions multi-sauts de Secure Core, car ses serveurs multi-sauts bénéficient de niveaux de sécurité physique supplémentaires. (Crédit : Proton VPN)

Au-delà de l'essentiel

L'ensemble des fonctionnalités de chaque VPN varie d'un service à l'autre, nous ne pouvons donc que généraliser ce que vous pourriez voir lorsque vous ouvrez les paramètres VPN.
Mais nous vous encourageons à lire la documentation et à cliquer sur certains boutons. La meilleure façon d'apprendre un outil est de l'utiliser.

La plupart des services VPN incluent un Kill Switch, qui empêche votre ordinateur de transmettre des informations si le VPN est déconnecté.
C'est utile pour empêcher de petits morceaux de données de se faufiler sans cryptage.
Si vous constatez soudainement qu'Internet est coupé, vérifiez si le Kill Switch de votre VPN s'est déclenché.

Certains VPN vous donnent la possibilité de sélectionner un protocole VPN.
Cela peut être intimidant car ils ont des noms étranges, et les entreprises fournissent rarement des informations à ce sujet et sur ce que le changement de protocole fera.
En général, c'est quelque chose que vous pouvez laisser tranquille.

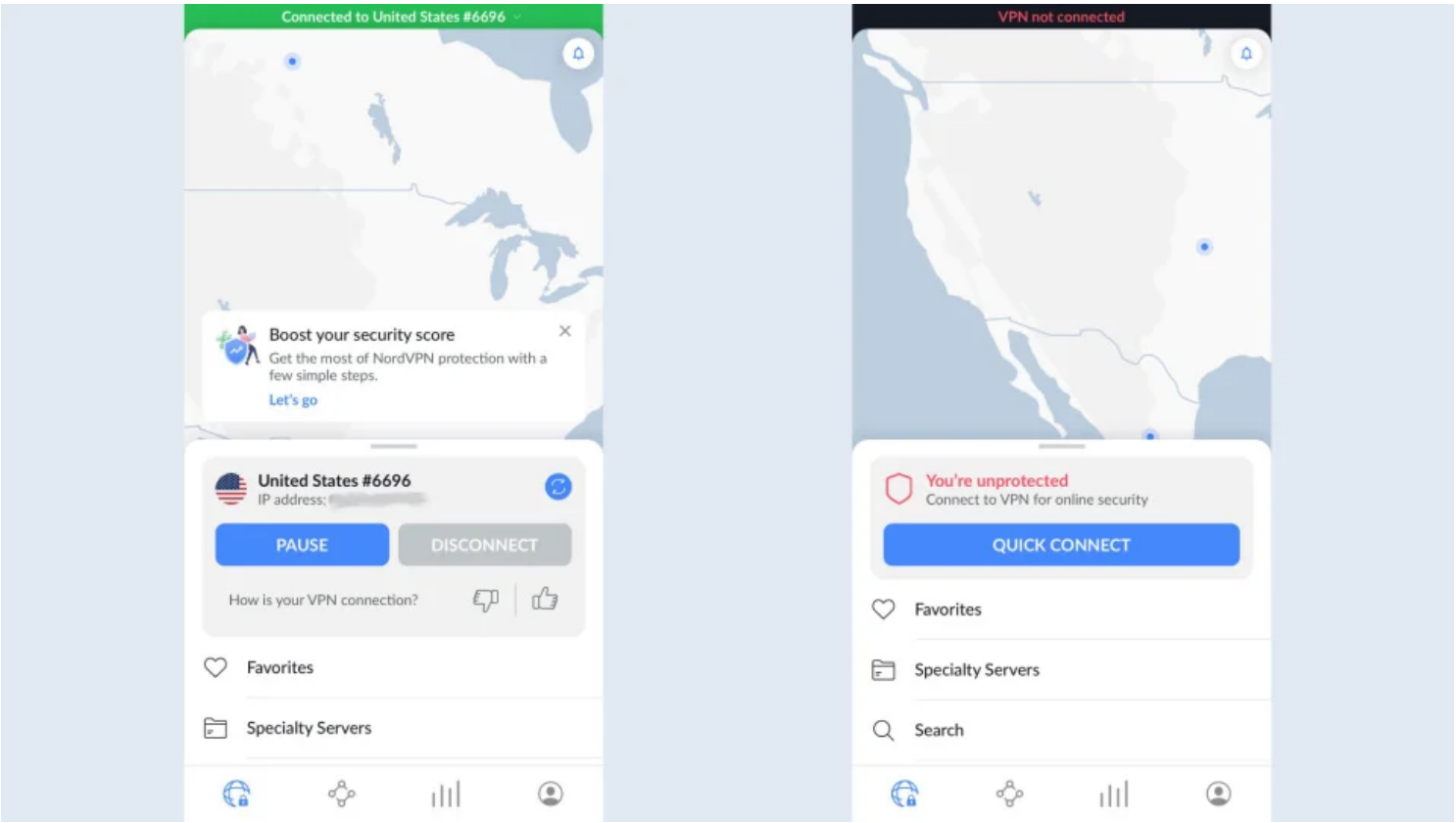
Si cela vous intéresse, WireGuard est le dernier protocole VPN.
Il est open source, dispose de la technologie de cryptage la plus récente et pourrait être plus rapide que d'autres protocoles.
OpenVPN et IKEv2 sont également de bons choix.
Notez que les protocoles disponibles peuvent également varier en fonction de l'appareil, alors vérifiez que votre VPN prend en charge tout ce que vous souhaitez pour vous y connecter en utilisant le protocole que vous avez choisi.

Quand dois-je utiliser un VPN ?

Le moment où vous devez utiliser un VPN dépend de l'utilisation que vous souhaitez en faire.
Si vous essayez d'accéder à du contenu verrouillé par région, vous laisserez probablement votre VPN désactivé jusqu'à ce qu'il soit temps de diffuser.
Si vous êtes préoccupé par la confidentialité, vous voudrez probablement activer votre VPN autant que possible.
Si vous vous inquiétez surtout des réseaux Wi-Fi douteux, votre VPN ne sort peut-être que lorsque vous voyagez.

Ne vous culpabilisez pas si votre VPN cause des problèmes et que vous devez le désactiver.
Au minimum, vous devriez utiliser un VPN chaque fois que vous utilisez un réseau que vous ne contrôlez pas, surtout s'il s'agit d'un réseau Wi-Fi public.

Les VPN pour Android et iPhone sont un peu plus délicats, en particulier si vous entrez et sortez fréquemment de la couverture cellulaire.
Chaque fois que vous perdez et récupérez la connectivité des données, le VPN doit se reconnecter, ce qui ajoute une attente frustrante.
Il est également moins probable que des personnes malveillantes puissent intercepter votre trafic cellulaire, bien que les chercheurs aient prouvé que c'était possible.



NordVPN a un design cohérent sur toutes les plateformes, y compris iOS. (Crédit : NordVPN)

La plupart des appareils se connectent automatiquement à n'importe quel réseau Wi-Fi d'apparence familière.
C'est pratique pour vous, mais il est trivialement simple d'usurper l'identité d'un réseau Wi-Fi.
Votre téléphone ou votre ordinateur portable peut se connecter à un pot de miel numérique sans que vous vous en rendiez compte.
Cette attaque et d'autres exotiques sont, par définition, rares.
Cependant, il est toujours utile de comprendre toutes les menaces.

Le split tunneling est le meilleur des deux mondes

Si vous craignez que les VPN ne ralentissent vos connexions ou ne bloquent un trafic important, vous devriez envisager un VPN doté d'une fonction de tunneling fractionné.
Les noms de cette fonctionnalité varient d'une entreprise à l'autre, mais l'essentiel est que vous pouvez décider quelles applications utilisent le VPN pour leur trafic et lesquelles peuvent transmettre sans lui.
TunnelBear VPN, lauréat du prix Editors' Choice, par exemple, inclut une option permettant de ne pas tunneliser les applications Apple pour s'assurer qu'elles fonctionnent correctement sur un Mac.
Les streamers vidéo fréquents et les joueurs qui ont besoin d'un VPN voudront peut-être étudier cette option.

Certains VPN ont des paramètres qui permettent à votre machine de communiquer avec des périphériques locaux (c'est-à-dire des périphériques LAN ou des périphériques sur le même réseau), ce qui peut également aider.
Cependant, n'oubliez pas que même avec le trafic LAN et le split tunneling, les applications qui vous

permettent de diffuser des médias à distance sur d’autres appareils, comme Chromecast et Apple AirPlay, ne fonctionnent souvent pas bien avec les VPN.

Les VPN devraient fonctionner pour vous

Loin d’être des outils de mise en réseau obscurs, les VPN modernes sont exceptionnellement faciles à utiliser.
La plupart sont maintenant des outils de configuration et d’oubli, comme ils devraient l’être.
Le plus gros problème de nos jours, c’est que les consommateurs ne comprennent pas ce qu’un VPN peut et ne peut pas faire.
Pire encore, certaines sociétés de VPN semblent se contenter de laisser cette confusion stimuler leurs ventes.

Un VPN rendra la surveillance de votre trafic Web plus difficile pour votre FAI et d’autres personnes.
Ils peuvent également vous aider à accéder à du contenu en streaming bloqué, ce qui rend plus difficile le suivi en ligne.
Tout le reste dépend du VPN que vous choisissez.
Une fois que vous aurez compris pourquoi vous voulez un VPN, vous serez en mesure d’en trouver un qui répond à vos besoins (à un prix que vous pouvez vous permettre) et qui s’adaptera à votre vie.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231214
"C'est ensemble qu'on avance"