

VPN 2023

Un VPN, ou réseau privé virtuel, relie deux ou plus appareils en toute sécurité pour garantir une navigation plus sûre et privée, surtout en accédant des réseaux privés et/ou publics.

L'utilisation d'un service VPN est particulièrement important lorsque vous vous connectez à des réseaux WiFi, par exemple dans un hôtel, un café ou dans un aéroport.

En utilisant un VPN, toutes les données envoyées entre ordinateurs, téléphones portables ou tablettes PC sur Internet sont cryptées, ce qui garantit des niveaux élevés de sécurité.

1 – Différents Produits VPN (Top10VPN)

1 – 1 – ExpressVPN - <https://www.expressvpn.com>

Créé il y a maintenant plus de 11 ans par Dan Pomerantz et Peter Burchardt, ExpressVPN a participé à la démocratisation des services VPN auprès du grand public alors que cette technologie était avant tout réservée aux entreprises. Depuis, la société a acquis une solide réputation dans le secteur et développe des fonctionnalités parfois uniques, comme **TrustedServer** (fonctionnement du serveur VPN uniquement en RAM) ou le protocole de communication **Lightway**.

POINTS FORTS

- Nombreux serveurs à travers le monde et beaucoup d'emplacements
- Excellents débits à l'étranger et en France
- Audit de la politique de confidentialité et de la sécurité
- Interface simple et efficace
- Support des torrents

POINTS FAIBLES

- Seulement cinq appareils en simultané
- Pas de bloqueur de pub
- Pas de connexion au réseau Tor
- Pas d'interface graphique pour Linux, tout se déroule via le terminal

1 – 2 -CyberGhost- <https://www.cyberghostvpn.com>

Basé en Roumanie, ce fournisseur se situe en dehors de la juridiction des « 14 yeux » de l'Europe et gère actuellement plus de 6 000 serveurs répartis dans 89 pays différents. Parmi tous les fournisseurs de services VPN sur le marché, CyberGhost fait partie de ceux qui me laissent un peu perplexe. Pour faire simple, si on ferme les yeux sur certains défauts critiques : une bonne protection de base, une vitesse convenable mais les adeptes du P2P n'y trouveront pas leur compte.

POINTS FORTS

- Un vaste réseau à travers le monde
- des fonctionnalités de sécurité unique – redirection automatique ,vers HTTPS, blocage du suivi, blocage des publicités et protection contre les virus
- Un choix important de protocoles de cryptage
- Des serveurs optimisés suivant les usages
- Une comptabilité multi-plateformes
- Des vitesses correctes t stables
- Un prix correct
- Fonctionne bien en streamng,y compris avec Netflix

POINTS FAIBLES

- Revoir les configurations après installation
- Règles sur l »anonymats et données personnelles à préciser
- Des options de paiements limitées
-

1 – 3 – PRIVATE INTERNET ACCESS – <https://www.privateinternetaccess.com/>

PIA ; PIA est près du sommet en matière de confidentialité, de sécurité et de blocage des trackers. Bien qu’il n’impressionne pas vraiment par ses vitesses, il regorge de fonctionnalités uniques et d’outils puissants, sans parler de sa capacité à déverrouiller des services de streaming TV populaires. Dans l’ensemble, c’est un VPN très performant et sécurisé qui vaut la peine d’être considéré.

Avantages :

- Sécurité renforcée
- Politique de non-enregistrement de journaux
- Multitude d’options de personnalisation
- Jusqu’à 10 appareils connectés simultanément
- Serveurs rapides

Inconvénients :

- Bloqué par certaines grandes plateformes de streaming
- L’interface de l’application laisse un peu à désirer
- Ne fonctionne pas de manière fiable en Chine
- Quelques informations obsolètes dans les forums et la documentation d’assistance

1 – 4 – Surfshark - <https://surfshark.com>

Surfshark est un fournisseur VPN qui a lancé son activité en 2018 et est rapidement devenu l’un de nos favoris. Surfshark est un VPN proposant un **chiffrement solide** et une **interface très conviviale**. Ses **tarifs abordables** et sa grande facilité d’utilisation en font un **fantastique VPN**. Ce nouveau venu joue sans aucun doute dans la même cour que des poids lourds de longue date

POINTS FORTS

- Très bons débits en France.
- Excellents débits à l'étranger.
- Nombre illimité d'appareils utilisables.
- Bloqueur de publicité intégré.
- Options avancées : P2P, connexion masquée, double VPN, split tunneling (liste blanche).
- Possibilité de se connecter à une IP fixe.
- Accès aux services de streaming étrangers.
- Assistance technique réactive.

POINTS FAIBLES

- Pas d'audit de l'application par une société tierce pour la politique de confidentialité.
- Pas de connexion au réseau TOR.
- Pas de prise en charge des adresses Ipv6.
- Débits en OpenVPN décevants.
- Ping globalement plus élevé que la concurrence

1 – 5 – atlasVPN – <https://atlasvpn.com>

Lancé en 2019, Atlas VPN fait partie d'une nouvelle génération de VPN prête à détrôner les ténors du marché. Son offre gratuite très généreuse lui a permis de rapidement constituer une base client conséquente. Le service s'est malgré tout fait racheter par Nord Security, la société mère de NordVPN, tout récemment.

Les plus

- Solution gratuite complète (accès limité à deux pays)
- Interface facile à prendre en main
- Nombreuses fonctions additionnelles pour la version payante

Les moins

- Service client peu réactif
- Moins de serveurs disponibles que chez la concurrence
- Entreprise domiciliée aux USA

1 – 6 – IPVANISH- <https://www.ipvanish.com>

IPVanish est un [VPN américain](#) qui est dans le jeu depuis longtemps, et il est largement considéré comme un fournisseur sûr, fiable et digne de confiance. Il est conçu pour l'utilisateur plus technique, il dispose d'un tas d'ajouts utiles et d'applications puissantes qui affichent toutes les données que vous pourriez souhaiter.

Les plus

- De solides performances

- Une connexion simultanée sur 10 appareils au maximum
- Pas de conservation des logs
- De nombreux serveurs
- Une interface sobre sous Windows

Les moins

- Une interface un peu désuète sur mobiles
- Uniquement disponible en anglais sur tous les supports
- Impossible de payer en cryptomonnaies
- VPN basé aux USA

1 – 7 – NordVPN – <https://nordvpn.com/fr/>

NordVPN est un fournisseur de VPN et le produit phare de la société de cybersécurité Nord Security. Nous accordons une importance primordiale à la libre expression des personnes, c'est pourquoi nous nous efforçons d'offrir à nos utilisateurs un accès à un Internet libre et sûr. Grâce à un travail sérieux, à un dévouement sans faille et à l'innovation technologique, nous avons créé le VPN le plus rapide du monde accompagné de fonctionnalités de pointe.

POINTS FORTS

- Les meilleurs débits en France.
- Excellents débits à l'étranger.
- Nombreuses options de connexion (double VPN, masquée, *split tunneling*, *kill switch*...).
- Nombreux serveurs et bonne répartition géographique.
- Politique de non-conservation des données auditée par une société tierce.

POINTS FAIBLES

- Ping (latence) globalement élevé.
- Pas de *split tunneling* sur macOS/iOS.
- Deux applications différentes sur macOS.
- Temps de réponse du support technique aléatoire.
- Pas d'audit de la structure technique.

1 – 8 – PrivateVPN – <https://privatevpn.com/fr/>

Derrière un tarif plutôt alléchant, PrivateVPN offre une prestation d'un bon niveau avec des débits corrects, le respect de la vie privée et une interface simple à prendre en main. Pas de fausse note donc, mais aucune originalité qui permette à ce VPN de se distinguer de la

concurrence, comme l'intégration du protocole de communication WireGuard.

POINTS FORTS

- Débits en filaire et 4G corrects.
- Interface sobre et logiciel facile à prendre en main.
- Support technique réactif par messagerie instantanée.
- Débloquent les principaux sites de streaming à l'étranger.
- Connexion masquée.

POINTS FAIBLES

- L'assistance technique ne fonctionne pas correctement sur le site avec bloqueur de pub/trackers.
- Pas de connexion avec un protocole de type WireGuard.
- Pas de split tunneling.
- Quelques fonctionnalités en moins sous macOS.

1 – 9 – PROTON <https://www.clubic.com/>

Lancé en 2017, Proton VPN constitue l'une des meilleures solutions pour qui désire protéger sa vie privée en ligne grâce à une sécurité accrue. Fort de récentes innovations, le service offre désormais des performances qui rivalisent avec celles des meilleurs VPN du marché. Proton VPN constitue l'un des fournisseurs VPN qui a le plus évolué au cours des derniers mois. Affichant de l'une des plus belles interfaces du marché, Proton VPN intègre désormais un accélérateur de VPN qui augmente jusqu'à 400 % les vitesses de connexion.

Avantages Proton VPN

- Le plus haut niveau de sécurité
- Interface moderne et intuitive
- Serveurs dédiés au streaming/P2P
- Protocole Stealth (fonctionne en Russie)
- Vitesse de connexion optimisée

inconvénients Proton VPN

- Infrastructure à enrichir

1 – 10 – Hide.me – <https://hide.me/fr/>

Idéal pour les utilisateurs experts et les gros consommateurs de vidéos sur Internet,. En dehors d'une interface hors d'âge, on ne peut que saluer les progrès réalisés en termes de vitesse et de stabilité. Sans oublier l'implémentation de nouvelles fonctions avancées aussi originales qu'efficaces. Bien que ses prix aient baissé, son plan mensuel demeure trop cher par rapport à d'autres concurrents

Avantages Hide.me

- Accès optimisé aux plateformes de streaming dont Netflix US
- Options de sécurité avancées
- Intégration du protocole VPN WireGuard
- Contournement de la censure chinoise
- IP fixes et 2 To de stockage offert

inconvénients Hide.me

- Prix mensuel prohibitif
- Interface vieillissante

1 – 11 – HMA (HideMyAss)- <https://www.hidemypass.com/fr-fr>

HMA est un bon VPN, mais il n'est plus du tout au niveau de notre classement du meilleur VPN, tant en termes de performances que de fonctionnalités. C'est un service conseillé avant tout aux néophytes qui recherchent un VPN presque entièrement automatisé et qui ne sont pas trop regardants sur la confidentialité de leurs données.

Avantages HMA VPN

- Streaming et P2P optimisés
- Grand nombre d'emplacements de serveurs
- Support client réactif en français

Inconvénients HMA VPN

- Peu de réglages avancés
- Ne prend pas en charge WireGuard
- Performances moyennes
- Configuration routeur complexe

1 - 12 – PureVPN - <https://www.purevpn.fr>

Basé auparavant à Hong-Kong, PureVPN a déménagé son siège social aux Îles Vierges britanniques pour pouvoir appliquer une véritable politique zéro-log. Grâce à l'implémentation de nouveaux serveurs 20 Gb/s au France et aux États-Unis, il se révèle ultra performant pour streamer des contenus sans aucune latence dans ces deux localisations. Ses performances en France et dans d'autres emplacements sont satisfaisantes, mais toujours pas à la hauteur de celles des ténors du marché. Ses tarifs parmi les plus bas du secteur en font toutefois une sérieuse alternatif

Avantages PureVPN

- Console de gestion web avancée
- Couverture multiplateforme étendue
- Streaming USA et UK
- Tarifs sur un et deux ans

inconvénients PureVPN

- Interface et ergonomie perfectibles

- Performances et stabilité irrégulières selon les pays

1 – 13 – PrivadoVPN – <https://www.privadovpn.com>

PrivadoVPN est un fournisseur relativement nouveau dans l'espace commercial des VPN. Le service a été fondé en 2019 et est basé en Suisse. D'après son marketing, il semble être plus axé sur la confidentialité et la sécurité que sur autre chose. Inégal au regard des prestations proposées, PrivadoVPN se montre très fort dans certains domaines (Kill Switch, vidéo en ligne, bonne protection de la confidentialité et de l'anonymat sur Internet), mais très mauvais dans d'autres (interface moyenne, absences de fonctionnalités, vitesse à améliorer).

Avantages PrivadoVPN

- Serveurs VPN colocalisés infogérés
- Performances
- Paiement en cryptomonnaie
- Débloque de nombreuses plateformes de streaming dont Netflix US

Inconvénients PrivadoVPN

- Traduction française partielle
- Interface peu intuitive
- Manque de fonctionnalités
- Couverture multiplateforme à améliorer

1 – 14 – Hotspot Shield- <https://www.hotspotshield.com/fr>

Hotspot Shield est un fournisseur VPN qui permet de protéger les données de l'utilisateur lors de ses connexions internet. L'idée principale : permettre un anonymat le plus total possible lors de la navigation sur le web. Dans cette optique, le logiciel crypte les données de connexion et permet aux clients de son service d'accéder à des sites ou logiciels parfois limités à une situation géographique, en plus d'offrir une confidentialité lors de la navigation.

Ses forces :

- Simplicité d'utilisation et interface
- Permet de contourner la censure en Chine
- Offre gratuite

Ses faiblesses :

- Processus d'installation
- Vitesses
- Conservation de certaines données
- Support client
- Tarification très élevée

1 – 15 – AVAST Secure Line - <https://www.avast.com/secureline-vpn>

Avast SecureLine VPN est un VPN fiable, simple à utiliser et multiplateforme qui propose plusieurs dizaines d'emplacements dans le monde entier. Il propose une

interface claire, intuitive et traduite en français. Bien connu pour son antivirus, l'éditeur *Avast!* propose également plusieurs outils de sécurité à l'image de Avast SecureLine VPN. Pour information, l'utilisation d'un VPN permet de préserver son anonymat en ligne grâce à une connexion sécurisée et à un tunnel chiffré.

Avantages

- Prise en main intuitive
- Protocoles sécurisés (OpenVPN, IKEv2/IPSec) et chiffrement AES-256
- Serveurs optimisés pour le streaming et le P2P
- Possède ses propres DNS
- Option Smart VPN

Inconvénient

- Basé en République tchèque (coopération ciblée avec les 5 Eyes)
- Nombre de serveurs peu élevé
- Performances en berne
- Collecte des données sensibles (horodatage des connexions, utilisation détaillée de la bande passante)
- Prix élevés pour le service proposé

1 – 16 – VyprVPN- <https://www.vyprvpn.com/fr/>

Avec plus de 2 millions d'utilisateurs dans le monde, VyprVPN fait partie des **poids lourds du marché des VPN**. Contrairement à la majorité de ses concurrents, il possède l'avantage de posséder ses propres serveurs répartis dans 70 emplacements dans le monde. Un service VPN, pour *Virtual Personal Network*, permet de garantir la confidentialité et la sécurité de l'utilisateur..

Avantage

- Fiabilité constante
- Sécurité solide
- Système DNS maison

Inconvénient

- Service chat souvent indisponible
- Support en anglais
- Choix de forfaits limité

1 – 17 – StrongVPN- <https://strongvpn.com>

Lancé en 2005, StrongVPN est sans aucun doute le VPN le plus ancien de notre sélection. Il propose un service dans la moyenne, mais bien trop minimaliste pour être indispensable. Et ce ne sont pas les 250 Go de stockage cloud en plus qui changeront la donne.

POINTS POSITIFS

- Des performances correctes avec Wireguard
- 250 Go d'espace de stockage dans le cloud en plus du service VPN
- 12 appareils couverts par une licence

POINTS NÉGATIFS

- Interface peu sexy
- Trop peu de fonctionnalités
- Peu de serveurs par rapport à la concurrence
- Tarifs dans la moyenne haute

1 – 18 – ZenMate - <https://zenmate.com/fr>

D'origine allemande, ZenMate a été fondé en 2011 par une start-up berlinoise avant de tomber sous le giron du géant de la cybersécurité Kape qui possède également CyberGhost et PIA. Très populaire dans certains pays pour son VPN partiellement gratuit, le fournisseur revendique aujourd'hui près de 50 millions d'utilisateurs.

Avantages

- Serveurs optimisés pour le streaming/TV et le P2P
- Environnement simple idéal pour les débutants
- Compatibilité Android TV

inconvenients

- Tarif mensuel trop élevé
- Paramétrages très limités
- Confidentialité

1 - 18 - Windscribe - <https://windscribe.net>

Windscribe est une société canadienne de sécurité informatique. Elle développe **une solution VPN**, mais également de nombreuses fonctionnalités annexes, qui sont disponibles par exemple en extensions de navigateurs. **Windscribe** a certes une formule payante, mais c'est du côté de son offre gratuite qu'il sort du lot. Avec celle-ci, vous pourrez tout de même profiter du split-tunneling, d'un bloqueur de publicité, et même d'une fonction baptisée "double hop" pour améliorer la sécurité de vos données sur n'importe quelle session.

Ses forces :

- VPN gratuit de qualité, malgré sa limite à 10 Go
- Simplicité d'installation et d'utilisation
- Support client de qualité

Ses faiblesses :

- Prix légèrement supérieur à la moyenne du marché
- Vitesse, notamment pour le téléchargement et le streaming.
- Nombre de serveurs
- Contournement de la censure
 - Sécurité

1 – 20 – Ivacy – <https://www.ivacy.com>

Malgré une commercialisation de son VPN depuis 2007, Ivacy reste un prestataire assez peu connu en France. L'entreprise, dont le siège social est situé à Singapour, précise bien dans sa politique de confidentialité qu'elle ne conserve pas les données de ses utilisateurs. Toutefois, aucun audit par une société tierce ne vient confirmer ses dires.

POINTS FORTS

- Disponible sur un grand nombre d'appareils et plateformes.
- Support technique par chat (anglais) disponible 24h/24 et 7j/7, rapide et efficace.
- Possibilité d'avoir une IP dédiée (option payante).
- Protection contre les virus et malwares.
- Netflix, Amazon Prime Video accessibles.

POINTS FAIBLES

- Débits globalement en retrait par rapport à la concurrence en mode IKEv2
- Pas de protocole de communication moderne comme WireGuard.
- Pas de blocage de la publicité.
- Pas de niveau de charge des serveurs.
- Interface en anglais.
- Split Tunneling et Kill Switch absent de la plateforme macOS.
- Absence de quelques fonctionnalités avancées (double VPN, masquage des connexions)

2 – Classements 2023 des VPN suivant les principaux sites internet

- 1) **Top10vpn** – <https://www.top10vpn.com>
- 2) **Les10 meilleursvpn** - <https://les10meilleursvpn.com>
- 3) **Clubic**- <https://www.clubic.com>

- 4) **Cnet France** - <https://www.cnetfrance.fr/produits/les-meilleurs-vpn-9882441.htm>
- 5) **Presse citron** - <https://www.presse-citron.net/vpn/>
- 6) **Journal du geek** - <https://www.journaldugeek.com/vpn/>
- 7) **Frandroid** - <https://www.frandroid.com/selection-meilleurs-vpn>
- 8) **01.net** - <https://www.01net.com/vpn/>
- 9) **Tom's Hardware** - <https://www.tomshardware.fr/comparatif-quels-sont-les-meilleurs-services-vpn/>
- 10) **Wizcase** - <https://fr.wizcase.com/vpn-reviews/>

Top 7 des meilleurs VPN gratuits de 2023 :

- ExpressVPN.
- CyberGhost **VPN**.
- Nord **VPN**.
- Atlas **VPN**.
- ProtonVPN.
- Hide.me **VPN**.
- Tunnelbear **VPN**.

Tableau de synthèse

Source :	1	2	3	4	5	6	7	8	9	10
ExpressVPN	1	3	3	4	1	1	6	1	3	1
CyberGhost	2	1	1	2	2	2	2	2	2	2
PRIVATE INTERNET ACCESS	3	2			5	6		6		3
Surfshark	4	4	4	3	4	4	3	4	4	
atlasVPN	5	5				5		5		
IPVANISH	6				8		8			6
NordVPN	7		2	1	3	3	1	3	1	
PrivateVPN	8									
PROTON	-	6	5		7	8	4	8	7	4
Hide.me	-		6			7				
HMA (HideMyAss)			8		9					
PureVPN			9		10		5		5	
PrivadoVPN			7	5						
Hotsptshield		7								

Avast secure line					6					
VyprVPN							7			8
StrongVPN							9			
ZenMate								7		7
Windscribe									6	
Ivacy										9

En conclusion de ces classements :

1 – ExpressVPN

2 – CyberGhost

3- NordVPN

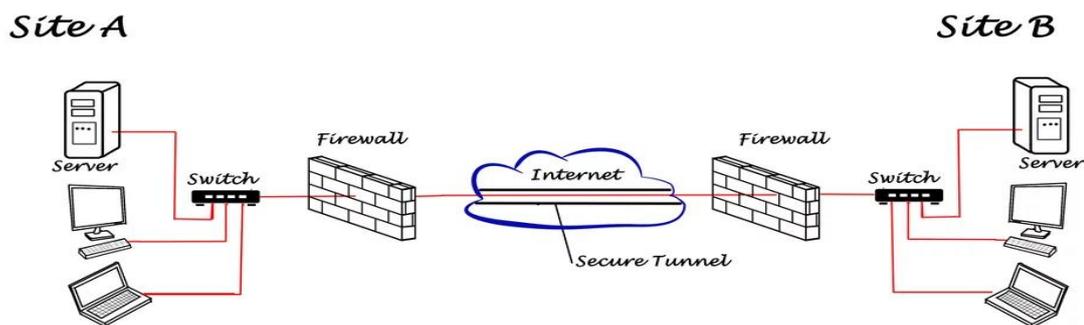
4- –Surfshark

5 -PROTON

Compléments : Rappel

Un VPN, c'est quoi ?

Qu'est ce qu'un VPN ? L'acronyme VPN signifie Virtual Private Network, réseau privé virtuel dans la langue de Molière. Derrière cet acronyme barbare se trouve une mesure de sécurité fort pratique pour éviter les vols de données lors de votre navigation Internet. Le VPN a aussi comme gros avantage de **masquer votre adresse IP réelle** - en général celle de votre Box - afin de vous donner accès à certains sites étrangers autrement inaccessibles.



Quel est le principe du VPN ? un programme est installé sur votre ordinateur/smartphone/tablette. Il va chiffrer toutes vos données sortant vers le vaste Internet et les faire transiter sur un serveur distant où elles seront ensuite déchiffrées avant de parvenir à leur but final. Ce "tunnel" chiffré évitera aux pirates de lire des données mal protégées comme vos mots de passe ou pire, le numéro de votre carte de paiement. Les sites que vous contacterez ne verront en général que du feu. Pour eux, seule votre adresse IP sera différente : c'est celle du serveur de votre fournisseur VPN qu'ils verront et non pas celle de votre Box. Grâce à ça, vous serez en mesure de vous connecter à certains sites étrangers bloquant parfois les adresses IP provenant de France. Plutôt pratique, non ?

Un VPN c'est quoi

Il est bon de rappeler que les VPN ne sont en aucun cas une mesure ultime contre toutes les nuisances du Web. Si vous téléchargez un fichier douteux sur un site encore plus douteux, même le meilleur VPN ne vous évitera pas une belle infection virale sur votre PC !

Par contre, si vous voyagez régulièrement et passez du temps dans les

aéroports, bars ou hôtels, **l'activation d'un VPN lors de connexion à des points d'accès WiFi ouverts** sera un vrai plus pour votre sécurité.

Les principaux cas d'utilisation d'un VPN sont :

- pour préserver ses données personnelles
- pour conserver son anonymat en ligne
- pour masquer son IP et son pays d'origine
- pour éviter la censure dans certains pays restrictifs (Chine, Iran, Russie...)
- pour accéder à des sites et des services étrangers habituellement inaccessibles
- pour accéder à des sites et des services français depuis l'étranger

La principale raison pour laquelle les gens utilisent un VPN est **la protection des données personnelles** : en quelques années, l'usage de VPN (réseaux privés virtuels en français) s'est largement démocratisé auprès des particuliers. Que cela soit sur un ordinateur fixe, un terminal mobile, voire un routeur ou une smart TV, ces services permettent de cacher son adresse IP derrière celle du serveur VPN et par extension de préserver son identité, ses données personnelles et sa localisation géographique. Ils constituent par exemple un moyen simple et efficace en déplacement de surfer en sécurité sur des réseaux publics (aéroports, gares, centres commerciaux, hôtels...) et éviter tous risques d'intrusions.

Le streaming et le téléchargement arrive loin derrière. un grand nombre de clients passe par un VPN pour accéder aux catalogues de services de streaming basés notamment aux USA (Netflix, HBO, Amazon Prime, Pandora...) ou pouvoir profiter des contenus français depuis l'étranger (MyTf1, Canal+, beIN SPORTS...). Il faut savoir également que certains fournisseurs présents dans ce classement du meilleur VPN n'autorisent pas le streaming et/ou les téléchargements sur les plateformes de partage P2P et torrents.

A quoi sert le Kill Switch ?

Pour une sécurité accrue, les meilleurs services intègrent la fonctionnalité appelée Kill Switch qui se charge de bloquer la connexion Internet en cas de bug ou de panne d'un serveur VPN. Cela permet d'empêcher toutes fuites de données jusqu'à ce que la connexion via un tunnel sécurisé et chiffré soit à nouveau active. Certains fournisseurs offrent même la possibilité de souscrire un abonnement sans avoir à fournir une adresse email et un nom et de payer

en cryptomonnaies (bitcoin, Ethereum....) afin d'assurer l'anonymat le plus total à leurs clients.

Pourquoi utiliser un VPN no log ?

Fort de ce constat, il est conseillé de privilégier des acteurs connus et reconnus offrant de sérieuses garanties sur la protection des données privées, ainsi que des outils de chiffrement fiables et simples à appréhender. À noter que les fournisseurs basés notamment aux États-Unis sont soumis au Patriot Act et peuvent donc être susceptibles de donner l'accès aux données de leurs clients si les autorités le leur demandent. Dans tous les cas de figure, il faut privilégier **les VPN no logs**, qui ne conservent aucun log de connexion ni aucune information d'aucune sorte.

Quel est le meilleur protocole VPN ?

Si vous choisissez de souscrire un abonnement à un VPN, c'est que vous souhaitez sécuriser vos communications. Dès lors, il est important de vérifier les sécurités utilisées par votre futur fournisseur. En règle générale, les meilleurs VPN fournissent tous un chiffrement AES 256 bits.

Le choix du **protocole VPN** est aussi important. OpeVPN a longtemps été considéré comme le plus fiable et il est encore très largement utilisé par défaut par les services VPN. Si de nombreux VPN utilisent encore PPTP, ce protocole est quant à lui peu fiable et âgé. Évitez donc les VPN qui ne s'appuient que sur lui. Une majorité de VPN propose désormais le protocole de dernière génération WireGuard, ou des variantes de ce dernier (NordLynx de NordVPN ou Lightway d'ExpressVPN, par exemple).

WireGuard a été développé par le spécialiste en sécurité informatique multiprimé Jason Donenfeld. Le protocole VPN repose sur une architecture simple et moderne ne comprenant que 4 000 lignes de code (contre plusieurs centaines de milliers pour OpenVPN) et s'avère de ce fait beaucoup plus facile à configurer et à déployer pour les fournisseurs. Autre avantage, son architecture simplifiée réduit le nombre de bugs et par conséquent les potentielles tentatives d'exploitation de vulnérabilités.

Au-delà de la sécurité, il est aussi sage de vérifier dans quel pays est hébergé votre fournisseur. Certains gouvernements ont en effet le pouvoir de réclamer

les données privées des utilisateurs dans des cas précis. N'hésitez donc pas à faire quelques recherches avant de vous lancer.

Est-ce qu'un VPN protège mon smartphone ?

Si vous souhaitez utiliser utiliser [un VPN pour votre smartphone](#) nous vous conseillons de vérifier les points suivants :

La compatibilité avec vos appareils : dans la plupart des cas, les VPN les plus connus sont répandus sur les plateformes fixes et mobiles classiques : Android, iOS, Windows 10/11, macOS. Les meilleurs services développent également des applications pour Android TV, les Chromebook, ou encore certains routeurs ou Box Internet. Lorsque vous voulez utiliser un VPN sur une distribution GNU/Linux, un routeur spécifique, une SmartTV, une console de jeux, Apple TV ou autres, il convient de s'assurer au préalable que le fournisseur propose des configurations manuelles dédiées.

La disponibilité d'une application mobile : Les fournisseurs les plus sérieux en ont généralement une régulièrement mise à jour pour Android et iOS. Si ce n'est pas le cas, il faudra mettre les mains dans le cambouis et aller rentrer les paramètres en dur dans votre précieux smartphone. Rien de bien compliqué, mais ce genre de manipulation peut vite devenir chronophage s'il faut configurer plusieurs appareils.

Les connexions simultanées sur plusieurs appareils : En dehors de quelques exceptions, la plupart des fournisseurs protègent entre cinq à dix appareils avec un même compte. Au-delà, il faudra payer une somme supplémentaire. Il faut également savoir que certains fournisseurs offrent également la possibilité d'installer leur VPN sur un routeur afin de protéger l'ensemble des appareils connectés au réseau.