# Trey Research Corporation

Réseaux privés virtuels : Vue d’ensemble technique pour Fabrikam, Inc.

15 décembre 2023

**Les réseaux privés virtuels (VPN)** constituent une solution de sécurité réseau très répandue qui permet de chiffrer le trafic réseau. [Les VPN agissent comme un tunnel sécurisé et chiffrent le trafic Internet, ce qui rend difficile pour les tiers de suivre les activités et de voler des données](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1.](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)

## Avantage de la mise en œuvre de VPN :

* En chiffrant le trafic internet, les VPN offrent une couche de confidentialité et de sécurité. Il est donc très difficile pour des tiers de retracer le suivi des activités et de voler des données.
* Les VPN permettent d’éviter le piratage lors de l’utilisation d’un réseau Wi-Fi public, par exemple dans un aéroport ou une bibliothèque. En effet, les VPN agissent comme un tunnel sécurisé et chiffrent le trafic internet.
* [Les VPN peuvent empêcher votre fournisseur de services Internet de savoir quels sites vous avez visités, car le trafic entrant vers et à partir de votre ordinateur voyage tous via les serveurs du VPN, ou les VPN de serveurs payent pour utiliser](https://www.bing.com/aclk?ld=e83gkJ29qbmUu8cYkNgVfaCjVUCUx3vCyorXNIwmWui8A8rISGT4ATMfXuQu_8nGJifMsVNZrD0_vVyNtSvYRynbmDYfM2jUvwoREzv_CIrOKnWn2gIEyYOWegOAxJPNIFOUp5hBSGQU35pxcSs4Qxqzw59vf63cS8Oh_e_94A9QZD8MND&u=aHR0cHMlM2ElMmYlMmZ3d3cudnBubWVudG9yLmNvbSUyZmluLXVzYS1iZXN0LXZwbiUzZmtleXdvcmQlM2R2cG4lMjUyMHJhbmtpbmclMjZnZW8lM2QxMTA3MzUlMjZkZXZpY2UlM2QlMjZ1dG1fc291cmNlJTNkYmluZyUyNmFkaWQlM2Q3NjIxMDA1Nzk0MzY4MCUyNm1zY2xraWQlM2Q3NTEzMDFiNzM2MTQxZTY2ZTBiZDY0MTA0MzJlYjBkYw&rlid=751301b736141e66e0bd6410432eb0dc) [1.](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)
* [Les VPN peuvent contourner les restrictions géographiques sur le contenu 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/) en masquant votre adresse IP et en chiffrant votre connexion Internet. Lorsque vous vous connectez à un serveur VPN, votre trafic Internet est acheminé via le serveur VPN, ce qui vous affecte une nouvelle adresse IP. [Cela permet d’apparaître comme si vous accédez à Internet à partir d’un autre emplacement, ce qui vous permet de contourner les restrictions géographiques sur le contenu](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## Inconvénients de la mise en œuvre des VPN :

* Les vitesses de connexion peuvent être plus lentes que votre isP. [Cela est dû au fait que les VPN ajoutent une couche supplémentaire de chiffrement et de routage à votre trafic Internet 2.](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)
* L’utilisation du VPN est interdite dans certains pays autoritaires. [Dans certains pays, les VPN sont interdits ou fortement réglementés](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/) [2.](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)
* L’utilisation de VPN gratuits risque d’exposer des publicités, des programmes malveillants et des fuites. [Les VPN gratuits peuvent vendre des données utilisateur à des annonceurs tiers ou injecter des publicités dans les pages](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/) [web 2.](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)

## Caractéristiques de l’installation :

* [Un VPN établit un tunnel chiffré entre le système exécutant le client VPN et un serveur VPN qui proxies ensuite le trafic via le tunnel vers le reste du réseau](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [d’entreprise 4.](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/) Procédez comme suit :
  1. Un client VPN est installé sur l’appareil de l’utilisateur, qui chiffre tout le trafic entre l’appareil et le serveur VPN.
  2. Le serveur VPN décrypte le trafic et le transmet à la destination prévue.
  3. Le serveur de destination répond à la demande en renvoyant le trafic au serveur VPN.
  4. Le serveur VPN chiffre le trafic et le transmet au client VPN.
  5. [Le client VPN déchiffre le trafic et l’envoie à l’appareil 1](https://www.bing.com/aclk?ld=e8OcZUYHFbvxJgBgmEWpxgCzVUCUz-UOb13n9w7mOCOGgLkPnDhd3Uh-ipDjPE6Hpo4QBuX2o2EUlY6g5-dRpoq53O3haHMQ8RcFRpVU95xD1yO9RVjEOu3gsgBNFb6xmA-Gvbq-gT8RFWo2P6R0BeJBd5LyAIvbSKlU_DPbqAqdr2ubUB&u=aHR0cHMlM2ElMmYlMmZ3d3cub3BlcmEuY29tJTJmZmVhdHVyZXMlMmZmcmVlLXZwbiUzZnV0bV9zb3VyY2UlM2RiaW5nJTI2dXRtX21lZGl1bSUzZHBhJTI2dXRtX2NhbXBhaWduJTNkVVMlMjUyMC0lMjUyMFBlcmZvcm1hbmNlJTI1MjBNYXglMjUyMC0lMjUyMEVOJTI2dXRtX2NvbnRlbnQlM2QlN2Jhc3NldEdyb3VwSWQlN2QlMjZtc2Nsa2lkJTNkZDVhYzJiMDEzNDM2MWVkNDRmNGE0ZWE2NDA1MDk5MjIlMjZ1dG1fdGVybSUzZHd3dy5vcGVyYS5jb20&rlid=d5ac2b0134361ed44f4a4ea640509922) de l’utilisateur.
* Pour installer et configurer un serveur VPN Server, procédez comme suit :
  1. Créez un profil VPN sur votre ordinateur.
  2. Cliquez sur Démarrer, puis sur Paramètres pour ouvrir le menu Paramètres.
  3. Dans le menu des paramètres, cliquez sur Réseau et Internet, puis sur VPN.
  4. Sélectionnez Ajouter une connexion VPN.
  5. Quelques tâches sont à effectuer dans la fenêtre Ajout d’une connexion VPN.
  6. Enregistrez les modifications que vous avez apportées.

## Risques et atténuations :

* Les attaquants savent depuis un certain temps que le travail à distance est un vecteur de menace. L’environnement de travail à distance est particulièrement attrayant pour les attaquants, et ce pour plusieurs raisons. Tout d’abord, l’environnement du réseau domestique n’est pas géré de manière professionnelle. Mais ce qui est plus inquiétant est que sur les réseaux domestiques, un grand nombre de systèmes ne sont pas corrigés régulièrement et qu’un certain nombre d’entre eux sont dépassés en termes de réduction des vulnérabilités. Pour pouvoir opérer sur un réseau d’entreprise, un attaquant qui a exploité un système doit éviter d’être détecté et résister aux mesures correctives. Ici aussi, le réseau domestique est plus convivial pour l’attaquant. En règle générale, la détection des menaces est pratiquement inexistante et la remédiation est tout à fait occasionnelle, se produisant par exemple lorsqu’un PC est réinstallé ou mis hors service parce qu’il fonctionne lentement. Pour sécuriser l’environnement de travail à distance, il est essentiel d’étendre les hypothèses de confiance zéro. [Ce n’est pas seulement le réseau qui doit être supposé hostile, mais tout ce qui n’est pas sous le contrôle](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [de l’entreprise 4.](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/)
* [Mettez à jour les VPN, les appareils d’infrastructure réseau et les appareils utilisés pour les environnements de travail avec les derniers correctifs logiciels et configurations](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [de sécurité 6.](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a)

## Meilleures pratiques en matière d’implémentation :

Les meilleures pratiques pour l’implémentation des VPN dans un réseau d’entreprise sont les suivantes :

* [Sélectionnez un VPN basé sur des normes qui utilise des normes acceptées, telles que internet Key Exchange/Internet Protocol Security (IKE/IPSec), qui sont généralement moins risquées et plus sécurisées que les VPN SSL/TLS (Secure Sockets Layer/Transport Layer Security) qui utilisent du code personnalisé pour envoyer le trafic via TLS 12.](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)
* Utiliser un VPN avec une cryptographie forte. Vérifier que les algorithmes de chiffrement, les algorithmes d’authentification et les protocoles utilisés par un VPN sont solides et porteurs de la validation FIPS. [Configurez tous les VPN pour utiliser l’authentification multifacteur (MFA) et remplacez l’authentification par mot de passe par l’authentification du client par le biais de certificats numériques (stockés sur des cartes à puce) si possible 12.](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)
* Gestion des vulnérabilités logicielles. L’exploitation des vulnérabilités des VPN est un vecteur d’attaque courant pour les cybercriminels. Choisir un fournisseur de VPN doté d’antécédents fiables en matière de correction des vulnérabilités, et lui demander de fournir une nomenclature logicielle (SBOM) pour garantir la mise à jour et la sécurisation du code tiers. Enfin, rechercher un produit capable de valider son code en cours d’exécution afin de détecter d’éventuelles intrusions. [Après avoir déployé un VPN, vérifiez et appliquez rapidement les mises à jour](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [logicielles 12.](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)
* Attendez-vous à des hausses de consommation. [Le personnel de sécurité informatique doit tester les limitations VPN en préparation de l’utilisation](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/) [massive 2.](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/)
* Évitez les VPN gratuits. [L’utilisation de VPN gratuits risque d’exposition aux publicités, programmes malveillants et fuites 3.](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/)