Société Trey Research

Réseaux privés virtuels : Aperçu technique de Fabrikam, Inc.

vendredi 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 complique sensiblement le suivi des activités et le vol de données par des tiers.[1].

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 d'accès à Internet de savoir quels sites vous avez visités, car le trafic entrant et sortant de votre ordinateur passe par les serveurs du VPN, ou par des serveurs VPN payants [1].
- Les VPN permettent de contourner les restrictions géographiques sur les contenus [2] 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, qui vous attribue une nouvelle adresse IP. Cela donne l'impression que vous accédez à Internet depuis un autre endroit, ce qui vous permet de contourner les restrictions géographiques sur le contenu.

Inconvénients de la mise en œuvre des VPN :

- Les vitesses de connexion peuvent être inférieures à celles de votre fournisseur d'accès. Cela s'explique par le fait que les VPN ajoutent une couche supplémentaire de chiffrement et de routage à votre trafic internet [2].
- L'utilisation des VPN est interdite dans certains pays autoritaires. Dans certains pays, les VPN sont interdits ou fortement réglementés [2].
- L'utilisation de VPN gratuits expose à des publicités, des logiciels malveillants et des fuites. Les VPN gratuits peuvent vendre les données des utilisateurs à des annonceurs tiers ou injecter des publicités dans les pages web [2].

Caractéristiques de l'installation :

- Un VPN établit un tunnel chiffré entre le système exécutant le client VPN et un serveur VPN qui achemine ensuite le trafic par proxy à travers le tunnel vers le reste du réseau de l'entreprise [4]. 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 de l'utilisateur [1].

- 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 [5].

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 considéré comme hostile, mais tout ce qui n'est pas sous le contrôle de l'entreprise [4].

- Mettre à jour les VPN, les dispositifs d'infrastructure de réseau et les dispositifs utilisés pour accéder à distance aux environnements de travail avec les derniers correctifs logiciels et les configurations de sécurité les plus récentes. [6].

Meilleures pratiques en matière d'implémentation :

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

- Choisissez un VPN qui utilise des normes acceptées, telles que IKE/IPSec (échange de clés Internet / Sécurité du protocole Internet), généralement moins risquées et plus sécurisées que les VPN SSL/TLS (Secure Sockets Layer/Transport Layer Security), qui utilisent un code personnalisé pour envoyer le trafic via TLS. [12].
- 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. Configurer tous les VPN pour qu'ils utilisent l'authentification multifactorielle (MFA) et remplacer l'authentification par mot de passe par l'authentification client au moyen de certificats numériques (stockés sur des cartes à puce), chaque fois que possible.[12].
- 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 le déploiement d’un VPN, vérifier régulièrement la présence de mises à jour logicielles et les appliquez sans tarder [12].

- Attendez-vous à des hausses de consommation. Le personnel chargé de la sécurité informatique doit tester les limites des VPN en prévision d’une utilisation massive. [2].
- Évitez les VPN gratuits. L’utilisation de VPN gratuits expose à des publicités, des logiciels malveillants et des fuites. [3].