Guide du débutant VPN ainsi que la définition et les avantages

Aminu Abdullahi :

Un VPN, ou réseau privé virtuel, est un service qui protège votre connexion Internet et votre vie privée en ligne. Il crypte vos données et masque vos adresses IP lorsque vous vous connectez à des services et des sites Web.
Un VPN peut également être utilisé pour contourner les restrictions géographiques et les mesures de censure.

Fonctionnement des réseaux privés virtuels

Un VPN cache une adresse IP aux observateurs extérieurs.
En acheminant votre connexion Internet via un tunnel crypté, vous pouvez prétendre être dans un autre pays.
Par exemple, si vous êtes aux États-Unis, mais que vous vous connectez à un serveur VPN au Canada, les sites Web penseront que vous vous connectez à partir de là.
Il est également beaucoup plus difficile pour les fournisseurs de services Internet (FAI) de surveiller ce que vous faites en ligne, et vous pouvez contourner les blocages géographiques qui restreignent le contenu en fonction de l'emplacement.

Un VPN utilise le cryptage pour brouiller tout le trafic jusqu'à ce qu'il atteigne le serveur VPN, où ces données sont déchiffrées et envoyées à leur destination.
Cela signifie qu'un FAI – ou toute autre partie – n'a aucune idée de ce qui se passe à l'intérieur du tunnel crypté.

Lorsqu'il est utilisé avec des sites Web HTTPS tels que des banques, du commerce électronique ou d'autres sites sensibles, cela peut aider à protéger les données telles que les mots de passe ou les informations de paiement lorsqu'elles circulent sur les réseaux publics.
Les VPN sont également utiles lorsque vous voyagez à l'étranger, permettant aux utilisateurs d'éviter de se connecter à des points d'accès Wi-Fi non sécurisés.

Que sont les protocoles VPN ?

Les protocoles VPN sont des règles régissant la façon dont les informations sont échangées entre deux réseaux ou plus.
Les types les plus courants de protocoles VPN sont OpenVPN, PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), SSTP (Secure Socket Tunneling Protocol) et Internet Key Exchange version 2 (IKEv2).

Ces protocoles peuvent créer des tunnels chiffrés pour connecter des ordinateurs distants comme s'ils se trouvaient sur le même réseau local.
Chacun a ses forces et ses faiblesses, il est donc essentiel d'en trouver un qui convient à vos besoins en matière de sécurité et de convivialité.

- **PPTP** a la latence la plus faible avec la compatibilité la plus large, mais il présente certaines limitations de chiffrement des données.
- **L2TP/IPsec** a de meilleures capacités de chiffrement des données que PPTP mais avec une latence plus élevée.
- **SSTP** fournit le meilleur cryptage de données disponible, mais peut être limité par le manque de support dans certaines applications.
- **IKEv2** offre une sécurité renforcée tout en maintenant la connexion très stable, ce qui le rend adapté aux appareils mobiles.
- **OpenVPN** a été développé comme une alternative open-source qui fonctionne bien sur les connexions sans fil et filaires et prend en charge plusieurs formes d'authentification, y compris via une clé pré-partagée, un certificat ou une méthode de combinaison nom d'utilisateur / mot de passe.

Comment fonctionne le cryptage VPN ?

Le cryptage VPN est un processus de transformation de données lisibles dans un format illisible.
Cela se fait à l'aide d'algorithmes, ce qui rend impossible pour quiconque n'a pas la clé de décoder l'information.
Lorsque vous vous connectez à un VPN, votre ordinateur envoie une demande au serveur VPN pour établir une connexion.

Une fois la connexion établie, votre trafic est acheminé via le tunnel sécurisé entre votre ordinateur et le serveur VPN.
Cela garantit que vos données sont protégées contre les oreilles indiscrètes et toute autre personne qui pourrait essayer d'espionner votre trafic.
Ce processus permet de protéger les informations sensibles, telles que les détails financiers ou les données personnelles, contre l'accès par des personnes non autorisées.

Qu'est-ce que le tunneling VPN ?

Dans le monde physique, un tunnel est un passage souterrain ou un chemin fermé qui permet aux personnes (ou, dans l'espace réseau, à un paquet VPN) de voyager sous un obstacle (c'est-à-dire des acteurs malveillants) jusqu'à leur destination.

Dans les VPN, le tunneling est le processus d'encapsulation et de cryptage du trafic réseau dans un « tunnel » sécurisé ou une connexion VPN.
L'objectif principal du tunneling VPN est d'assurer la confidentialité, la sécurité et l'anonymat lors de la transmission de données sur Internet.

6 avantages des VPN

L'avantage évident d'un service VPN est qu'il assure la confidentialité en gardant l'activité de l'utilisateur hors des regards indiscrets.
Certains des moyens et des résultats de ce processus comprennent le transfert de données sécurisé, le cryptage, l'anonymat IP, la protection des appareils, la disponibilité du streaming et la navigation privée.

1. Transfert de données sécurisé

Un VPN garantit que personne ne peut vous suivre.
Les données partagées lors de la connexion à des réseaux Wi-Fi publics tels que les cafés, les aéroports et les hôtels ne sont pas chiffrées.
En utilisant un service VPN avec des protocoles de cryptage robustes, vous pouvez naviguer en toute sécurité sur le Wi-Fi public sans vous soucier de l'interception de vos informations personnelles.
Avec un VPN, toutes les données envoyées vers et depuis l'appareil sont protégées par un cryptage de chiffrement AES-GCM 256 bits de qualité militaire.

2. Chiffrement

Qu'il s'agisse de courriels, de messages instantanés, d'applications de médias sociaux, d'applications bancaires ou d'historique de navigation, tout contenu sensible sera protégé contre l'interception lors de l'exécution sur une connexion VPN sécurisée.

Avec un VPN, les données sont cryptées avant de quitter l'appareil.
Une fois qu'il atteint le serveur, il est décrypté, ce qui signifie que quiconque intercepte les données ne verra que du charabia.
En d'autres termes, vos données restent en sécurité et privées parce que vous êtes la seule personne à y avoir accès.

3. Adresse IP cachée et emplacement

Lorsque vous utilisez un VPN pour la navigation privée, vous recevez une adresse IP anonyme au lieu d'une adresse réelle, ce qui vous permet de maintenir la confidentialité et la sécurité en ligne.
Cela s'étend à l'usurpation de votre emplacement physique : si vous vous connectez à un serveur VPN dans un autre pays, tout ce que vous faites en ligne semblera provenir du pays où se trouve le serveur VPN.

4. Protection de l'appareil

Les connexions VPN vous permettent de prendre le contrôle de leur confidentialité et de leur sécurité numériques, que ce soit à la maison ou en voyage.
La connexion à un serveur VPN empêche les gens d'espionner vos activités entre d'autres appareils (PC et ordinateurs portables) et des points d'accès Wi-Fi publics.

5. Vous permet de diffuser de n'importe où

Certains services de streaming de films et de séries TV imposent des restrictions géographiques sur les programmes que vous pouvez regarder en fonction de votre adresse IP.
Pour éviter ce problème, certains utilisateurs se connectent à un serveur VPN en dehors de leur pays.

Cependant, les services de streaming tentent souvent de bloquer les VPN en raison d'accords de licence.
Pour contourner ces limitations, abonnez-vous à un fournisseur qui propose des adresses IP dédiées.

6. Cache vos activités sur le Web et évite la censure

Les VPN offrent une couche de protection supplémentaire en gardant vos activités Web anonymes et en vous aidant à maintenir la liberté sur Internet.
Ils aident à protéger vos données, votre identité et votre emplacement.
Si vous utilisez un VPN pour protéger vos données, vous n'avez pas à vous soucier du suivi de votre activité par votre FAI.
Il est important de noter qu'ils permettent également aux citoyens des pays répressifs d'échapper à la surveillance gouvernementale et au blocage géographique.

Types de VPN

Il existe différents types de VPN.
Les quatre principaux types comprennent les VPN personnels, les VPN mobiles, les VPN d'accès à distance et les VPN de site à site.

- **Services VPN personnels :**
  Ce type est conçu pour l'internaute moyen.
  Il vous permet de diffuser des films indisponibles dans votre région, d'échapper à la censure du Web, de masquer les adresses IP et d'empêcher les étrangers d'espionner vos activités en ligne.
- **VPN mobiles :**
  Ceux-ci permettent aux utilisateurs d'accéder aux données d'entreprise et à d'autres applications de n'importe où, préservant ainsi la sécurité et la confidentialité des données.
  Ce type de VPN est idéal pour les employés distants en raison de sa capacité à persister pendant les sessions à travers des changements de connectivité physique tels que la perte de connectivité ou les commutateurs réseau.
- **VPN d'accès à distance :**
  Parfois appelés VPN basés sur le client ou VPN client-serveur, ils sont généralement utilisés par les télétravailleurs, les travailleurs mobiles et les employés distants qui ont besoin d'accéder aux ressources internes en toute sécurité afin de se connecter à distance à un réseau de travail.
- **VPN de site à site :**
  Ceux-ci sont couramment utilisés par les organisations pour connecter plusieurs sites distants à un seul réseau sécurisé.
  Un VPN de site à site est idéal pour les entreprises ayant différentes succursales, permettant à chaque site d'accéder aux ressources partagées de n'importe lequel des autres sites connectés.

Qui a besoin d'un VPN ?

Rien n'est garanti dans le monde de la cybersécurité, mais vous voulez une expérience Internet sans restriction avec une sûreté et une sécurité fiables, un service VPN est l'un de vos meilleurs paris.

Un VPN est idéal pour vous si vous devez faire l'une des choses suivantes :

- Chiffrez votre connexion Internet
- Effectuer un transfert de données sécurisé
- Protégez votre identité en ligne

- Contourner les restrictions géographiques
- Débloquer des sites Web

Un VPN vous aide à rester en sécurité en ligne en cryptant vos données, votre historique de navigation, vos mots de passe et plus encore.
Toutes ces informations sont cryptées et envoyées au serveur de votre choix.
Votre adresse IP sera également masquée, de sorte qu'elle ne peut pas être retracée jusqu'à vous.

Un VPN offre sécurité et confidentialité et a de nombreuses utilisations, telles que rester anonyme lorsque vous surfez sur le Web ou téléchargez des fichiers, se cacher des pare-feu, contourner les restrictions de contenu, vous protéger contre la cybercriminalité, etc.

Notez qu'un VPN *ne* vous protège pas contre les logiciels malveillants ou les virus contenus dans les fichiers téléchargés ou les sites Web exécutables.
Vous aurez besoin d'un outil antivirus fiable pour cela.

4 alternatives VPN pour les entreprises

Bien qu'un VPN soit une solution de sécurité réseau solide, il peut ne pas offrir suffisamment de sécurité pour votre réseau d'entreprise.
Voici d'autres alternatives remarquables aux VPN pour l'accès à distance sécurisé et la protection des données, notamment les postes de travail virtuels, la confiance zéro, les périmètres définis par logiciel et les courtiers de sécurité d'accès au cloud (CASB).

Dans certains cas, vous voudrez choisir la meilleure de ces solutions pour votre réseau, mais pour une protection maximale, vous souhaiterez peut-être en implémenter plusieurs sur votre réseau simultanément.

Infrastructure de bureau virtuel (VDI)

Un VDI est un type de virtualisation de bureau à distance qui permet aux utilisateurs de se connecter en toute sécurité à un espace de travail entièrement virtuel hébergé sur un serveur centralisé.
Cela vous permet, à vous et à vos employés, d'accéder aux applications d'entreprise sur n'importe quel appareil, y compris les ordinateurs de bureau, les appareils mobiles ou les clients légers.

Les cas d'utilisation VDI incluent l'accès tiers, la conformité règlementaire, les centres d'appels et le travail à distance.

Accès réseau Zero Trust (ZTNA)

Le concept de ZTNA est simple : aucune personne ou application ne devrait être digne de confiance tant qu'elle n'a pas vérifié son identité pour prouver sa légitimité.
Ce cadre de sécurité se concentre sur la vérification de l'identité et de la fiabilité des utilisateurs et des appareils avant d'accorder l'accès aux ressources de l'entreprise.

Au lieu d'accorder un accès large comme un VPN traditionnel, ZTNA fournit des contrôles d'accès plus granulaires et contextuels.

Les solutions ZTNA utilisent généralement une authentification forte, une microsegmentation et des tunnels chiffrés pour protéger les données.

Périmètre défini par logiciel (SDP)

SDP est un autre modèle de sécurité offrant une approche de contrôle d'accès plus fine.
Il crée un « nuage noir » autour de chaque application, les rendant invisibles et inaccessibles aux utilisateurs non autorisés.
Les utilisateurs et les appareils doivent être authentifiés et autorisés avant d'accéder à des applications ou des ressources spécifiques.

Cloud Access Security Brokers (CASB)

Les CASB agissent en tant qu'intermédiaires entre les utilisateurs et les services cloud, offrant une sécurité et un contrôle supplémentaires.
Ils offrent des fonctionnalités de cryptage des données, de contrôle d'accès, de protection contre les menaces et de prévention des pertes de données.
Les CASB peuvent aider à protéger les données lors de l'accès à des applications et des services basés sur le cloud sans compter uniquement sur un VPN.

Conclusion : les avantages du VPN dans l'entreprise

Le VPN est l'un des meilleurs moyens de sécuriser votre réseau contre les cybermenaces.
Bien que les VPN se soient avérés être une mesure de sécurité fiable, ils ne constituent pas une stratégie de protection réseau infaillible.
Il est préférable d'en utiliser un en tandem avec d'autres solutions de sécurité, telles que les CASB, les outils de prévention des pertes de données et l'accès réseau Zero Trust, entre autres.

Lorsqu'il s'agit de protéger votre réseau contre les acteurs malveillants, vous ne pouvez pas vous permettre de prendre des risques. Investir dans des solutions de sécurité complètes est le meilleur moyen de garantir la sécurité de votre organisation.

Il y a des tonnes de VPN sur le marché aujourd'hui. Voici notre guide des meilleurs services VPN pour sécuriser votre réseau d'entreprise.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230711
"C'est ensemble qu'on avance"