Glossaire VPN

AES
AES signifie Advanced Encryption Standard, qui est un chiffrement de bloc symétrique audité et utilisé par le gouvernement des États-Unis pour protéger les informations classifiées depuis 2002. AES est également appelé Rijndael, qui a été nommé d'après ses inventeurs Vincent Rijmen et Joan Daemen.

Antidémarrage (Kill Switch)
C'est une fonctionnalité qui met fin à la connectivité Internet si la connexion au serveur VPN est perdue. Kill Switch empêche votre véritable adresse IP de fuir.

Anonymat
L'anonymat est un état dans lequel quelqu'un ou quelque chose ne peut pas être identifié de manière unique. Par exemple, si vous publiez un commentaire en ligne sans vous inscrire au préalable, vous apparaissez comme anonyme. Personne ne sait qui a posté le commentaire. Dans le monde en ligne, les gens utilisent des VPN ou Tor pour obtenir l'anonymat en ligne.

Bloqueur de publicité (Ad Blocker)
Un bloqueur de publicités est une application logicielle qui empêche les publicités d'apparaître sur les sites Web ou dans les applications mobiles.

CA
CA signifie autorité de certification. Il vérifie et accorde aux sites Web un certificat numérique pour informer les utilisateurs qu'il s'agit d'un site Web légitime. La poignée de main SSL vérifie l'authenticité en examinant le certificat numérique pour vérifier que le site Web est réel et non un domaine configuré pour vous tromper

La censure
La censure est un processus par lequel les autorités réglementaires contrôlent ou suppriment le type de contenu qui peut être consulté, visualisé ou publié sur Internet. En Chine, par exemple, presque tous les sites de médias sociaux grand public sont bloqués.

Cryptographie
La cryptographie est le processus de conversion d'un texte ordinaire en un texte illisible. Elle est utilisée pour transmettre en toute sécurité des données sous une forme illisible particulière, de sorte qu'elles ne puissent être lues et traitées que par la personne à laquelle le message est destiné. C'est un peu comme un coffre-fort que l'on peut ouvrir avec le bon code d'accès. La cryptographie ne protège pas seulement les données contre le vol, elle est également utilisée pour l'authentification.

Le Web sombre (deep web)
Le dark web est une partie de l'Internet que vous ne pouvez pas accéder via un moteur de recherche comme Google. Le dark web est lié à de nombreuses activités criminelles louches et illicites. La seule façon d'accéder au dark web est via un navigateur anonyme appelé Tor.

Rétention des données
La conservation des données fait référence à une loi ou à une politique qui impose aux entreprises de conserver certaines informations sur leurs utilisateurs. Aux États-Unis, par exemple, les fournisseurs de services Internet peuvent conserver et vendre toutes les données des clients qui transitent par leurs serveurs.

DD-WRT
DD-WRT est un système d'exploitation open-source basé sur Linux pour les routeurs sans fil Wi-Fi 4 et Wi-Fi 5. Les routeurs qui fonctionnent avec le firmware DD-WRT peuvent être modifiés assez facilement. De nombreux fournisseurs de VPN proposent des applications VPN qui peuvent être directement installées sur les routeurs compatibles avec DD-WRT. Cela dit, n'oubliez pas que l'installation de DD-WRT peut annuler la garantie de votre routeur.

Attaques DDoS
DDoS signifie Déni de Service Distribué. C'est un type d'attaque dans laquelle trop de demandes sont envoyées à un serveur particulier. En conséquence, une attaque DDoS submerge la capacité d'un site Web à gérer plusieurs demandes et l'empêche de fonctionner correctement.

Inspection approfondie des paquets
L'inspection approfondie des paquets ou DPI est un type de technologie de filtrage des paquets réseau qui vérifie la partie données et l'en-tête d'un paquet pour filtrer les spams, les virus ou tout autre contenu malveillant. Fondamentalement, l'inspection approfondie des paquets localise, détecte et bloque les contenus indésirables qui n'auraient pas été détectés par le filtrage classique des paquets.

DNS
DNS est l'abréviation de Domain Name System (système de noms de domaine), qui est en quelque sorte le carnet d'adresses de l'internet. Le DNS convertit les noms d'hôtes tels que www.example.com en une adresse IP lisible par l'ordinateur, telle que 192.168.2.2. Ainsi, lorsque l'utilisateur tape CBS.com dans son navigateur, les résolveurs DNS convertissent le nom d'hôte en une adresse IP appropriée pour localiser la page web.4

Fuite DNS
Une fuite DNS se produit lorsqu'une application VPN n'utilise pas ses propres serveurs DNS anonymes et utilise les serveurs DNS par défaut hébergés par un fournisseur d'accès à Internet. Dans ce cas, une application VPN laisse filtrer des données privées et expose son utilisateur bien qu'il soit connecté à un serveur VPN sécurisé. Les VPN gratuits sont souvent sujets à des fuites.

DMCA
Le Digital Millennium Copyright Act (DMCA) est une loi qui protège le contenu en ligne contre la violation du droit d'auteur. DMCA Protection & Takedown Services est une autorité qui s'emploie activement à faire tomber le contenu qui a été produit illégalement.

Chiffrement
Le chiffrement est un processus consistant à convertir des informations brutes en code afin d'empêcher les personnes non autorisées d'y accéder. Le chiffrement convertit le texte brut en texte chiffré qui ne peut être déchiffré qu'avec la clé fournie par l'expéditeur au destinataire.

Clé de chiffrement
Une clé de chiffrement est constituée d'une chaîne de bits utilisée spécifiquement pour chiffrer ou déchiffrer certaines informations. Les clés de chiffrement sont générées par des algorithmes complexes qui garantissent que chaque clé est différente et unique. Plus la clé est longue, plus elle est difficile à casser.

Cybercensure
La cybercensure, ou censure d'Internet, est une forme de **géoblocage** destiné à empêcher les internautes d'un pays, résidents ou en transit, d'accéder à des services et contenus étrangers à des fins politiques et/ou idéologiques.

Pare-feu -
Un pare-feu est essentiellement un outil de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant d'un appareil en fonction de règles de sécurité prédéterminées. Un pare-feu crée une barrière entre les réseaux de confiance et les réseaux non fiables.

Les Cinq Yeux (FVEY)
Les Cinq Yeux sont une alliance internationale de partage de renseignements composée de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. Ces cinq pays sont connus pour espionner illégalement leurs propres citoyens et partager des informations de renseignement entre eux. L'existence des Five Eyes était un secret bien gardé jusqu'à ce qu'Edward Snowden divulgue un certain nombre de documents exposant l'alliance en 2013.

Fingerprinting
Le fingerprinting est une technique de tracking mise en place par certains services web et qui consiste à récupérer l'empreinte digitale d'un navigateur pour établir un profil de l'internaute, même si son adresse IP est masquée et que les cookies sont désactivés.

Commande de silence
Une ordonnance de silence est une ordonnance judiciaire qui empêche toute information d'être rendue publique ou divulguée à des tiers non autorisés. Une ordonnance de silence peut être délivrée à une entreprise pendant une enquête en cours pour empêcher que des informations relatives à l'affaire ne soient divulguées.

Géoblocage -Blocage géographique
Le géoblocage est le processus qui consiste à limiter les informations ou les sites web auxquels une personne peut accéder en fonction de son emplacement physique. Une base de données d'adresses IP est souvent utilisée pour appliquer les géoblocages. Les géoblocages sont généralement appliqués en raison de restrictions en matière de droits d'auteur ou pour se conformer aux règles et réglementations d'un pays.

Géo-usurpation
Le géo-spoofing est une technique grâce à laquelle quiconque peut utiliser un VPN, un proxy ou Tor pour masquer son adresse IP d'origine et obtenir une adresse IP complètement différente pour apparaître dans une autre partie du monde.

Grand pare-feu (GFW)

Le GFW (Great Firewall) est une technologie utilisée par le gouvernement chinois pour réguler l'internet dans le pays. L'objectif du GFW est de bloquer presque tous les sites web étrangers tels que Google, Facebook, YouTube, etc. Grâce au GFW, environ 800 millions de personnes en Chine ont accès à un internet très restreint.

Adresse IP

L'adresse IP est l'abréviation d'adresse de protocole internet. Elle est composée de chiffres ou de caractères et est associée de manière unique à un ordinateur ou à un réseau informatique. Une adresse IP ressemble à ceci (192.168.1.1). Tous les appareils connectés à l'internet ont une adresse IP unique, semblable à un numéro de téléphone. Les adresses IP permettent aux appareils informatiques de se connecter les uns aux autres sur l'internet.

Fuite IP

La fuite d'IP est un événement au cours duquel l'adresse IP réelle d'un utilisateur fuit même lorsqu'il est connecté à un réseau privé virtuel (VPN). Si vous effectuez un test de fuite d'IP et que vous voyez votre adresse IP par défaut au lieu de celle qui vous a été attribuée par votre fournisseur de VPN, c'est que votre adresse IP fuit. Cela se produit lorsqu'un VPN n'utilise pas ses propres serveurs cryptés et utilise les serveurs par défaut du fournisseur d'accès internet.

IPSec

IPSec signifie Sécurité du Protocole Internet. C'est un protocole de réseau qui crée une connexion cryptée entre les périphériques. Le but de ce protocole est de sécuriser les données transférées sur les réseaux publics. IPSec fonctionne en cryptant les paquets IP et en authentifiant leur source.

IPv4

IPv4 signifie Protocole Internet version 4. C'est la quatrième itération du Protocole Internet. IPv4 est l'un des protocoles de base responsables de toutes les communications Internet.

IPv6

L'IPv6 est la version la plus récente et la plus moderne de l'IPv4 et de ses prédécesseurs. La raison pour laquelle l'IPv6 est meilleur que l'IPv4 est qu'il offre un système de localisation et d'identification pour les ordinateurs sur l'internet. C'est grâce à l'IPv6 que tous les appareils qui communiquent sur le web ont leur propre adresse IP.

ISP (Internet Serbvice Provider) – FAI (fournisseur d'acces internet)

L'ISP est simplement l'abréviation d'un fournisseur de services Internet. C'est toute entreprise responsable de fournir une connexion Internet aux consommateurs. T-Mobile, AT&T, Comcast Tous sont des exemples de fournisseurs de services Internet (ISP).

Interrupteur d'arrêt – Kill Switch

Un interrupteur d'arrêt est une fonctionnalité de sécurité VPN qui vous déconnecte automatiquement d'Internet en cas de chute brutale de votre connexion VPN. Il est conçu pour empêcher votre adresse IP réelle de fuir en cas de déconnexion du serveur VPN.

Juridiction - La compétence

Dans le monde des VPN, la juridiction fait référence au pays dans lequel un fournisseur de VPN a son siège. Les juridictions sont importantes car elles déterminent si le fournisseur de

VPN est tenu par la loi d'enregistrer les données des utilisateurs ou non. Par exemple, les fournisseurs de VPN qui opèrent à partir des juridictions des Cinq Yeux conservent et partagent les journaux VPN.

Journal

Un journal est un fichier stocké par un serveur. Un fichier journal stocke toutes les actions qui se produisent sur un serveur avec des horodatages et des informations d'identification. Les journaux VPN stockent des informations sur la manière dont un utilisateur particulier utilise leur service. Les journaux VPN sont extrêmement préjudiciables à la vie privée des utilisateurs.

Man-in-the- middle {Attaques par homme du milieu}

Attaque homme du milieu ou MitM est une attaque où une entité malveillante se trouve au milieu et intercèpte et modifie secrètement les communications entre deux parties.

Malware

Malware est un terme générique pour tous les codes malveillants qui ne font que nuire. Virus, ransomware, rootkit, ver, spyware, sont tous des types de malware. Nous avons un article pour vous qui vous aidera à comprendre les différents logiciels malveillants qui existent aujourd'hui

Ouvrir VPN

OpenVPN est l'un des protocoles les plus sûrs et les plus utilisés dans l'industrie du VPN. Il est super sécurisé et est connu pour sa capacité à contourner les géo-blocages stricts. Mais au-delà du simple protocole, OpenVPN est aussi un logiciel qui permet aux utilisateurs d'établir une connexion point à point sécurisée. OpenVPN a été développé par James Yonan et a été rendu public en 2001.

Obfuscation

L'obscurcissement est une technologie qui ajoute une couche de furtivité au trafic VPN crypté. L'obscurcissement est utilisé pour déguiser le trafic VPN crypté et le faire apparaître comme du trafic HTTPS normal afin qu'il ne soit pas bloqué par les pare-feux. Cette technologie est largement utilisée dans des pays fortement censurés comme la Chine.

La confidentialité parfaite à l'avance

Le Perfect Forward secrecy est une méthode de cryptage qui crée des clés de session uniques pour chaque transaction. Ainsi, même si un pirate informatique parvient à accéder aux données d'une transaction sur un serveur, il ne pourra pas accéder aux autres données d'un groupe de transactions. Le Perfect Forward secrecy est un processus qui permet de s'assurer que toutes les transactions envoyées sur l'internet restent sécurisées.

Latence ou 'Le temps de ping'

Le ping ou la latence est le temps mesuré en millisecondes qu'il faut à un paquet de données pour se rendre sur un serveur et revenir à votre appareil. Idéalement, plus les pings sont bas, meilleures seront vos vitesses Internet.

Oignon sur VPN

Oignon sur VPN fournit une couche de sécurité en faisant passer le trafic Internet crypté via le serveur VPN puis via les nœuds de Tor. L'avantage est que le premier nœud du réseau Tor ne peut pas voir votre adresse IP

Point de Terminaison de Tunnel Protégé

PPTP ou Point-to-point Tunneling Protocol est un protocole réseau assez ancien qui est toujours utilisé par les fournisseurs de services VPN. Introduit en 1995, il est moins sûr qu'OpenVPN car il n'est pas crypté. Cependant, grâce à cela, PPTP est assez rapide, ce qui est idéal pour la diffusion en continu.

procuration

Un serveur proxy sert d'intermédiaire entre le client et le serveur. Il masque l'adresse IP du client et transmet les requêtes Internet à la destination. C'est comme un VPN mais sans cryptage et plusieurs autres fonctionnalités qui font du VPN une option beaucoup plus sécurisée.

Proxy

Toute ressource informatique telle qu'un serveur qui aide les utilisateurs à contourner les restrictions géographiques est appelée un proxy. Les réseaux privés virtuels sont des proxies qui acheminent le trafic des utilisateurs à travers des serveurs distants et les aident à contourner les blocs géographiques.

Site Web de l'oignon

Un site Web d'oignons fait partie d'un réseau anonyme et décentralisé accessible uniquement si vous connaissez l'adresse. Il faut un navigateur spécial comme **To**r pour afficher la page Web. Les sites Web portant le suffixe .onion ne sont pas indexés ni disponibles dans les bases de données DNS.

Ransomware

Le ransomware est un type de logiciel malveillant qui crypte tous les fichiers sur l'ordinateur d'une victime. L'attaquant exige alors une rançon en échange des précieuses données personnelles de la victime. En général, les pirates exigent une cryptomonnaie pour éviter de laisser des traces.

Rétention des données

La conservation des données est la pratique consistant à enregistrer les activités des utilisateurs sur Internet. Tels que les sites Web qu'ils visitent, à quelle heure ils visitent et d'où ils visitent. Les FAI suivent cette pratique sur ordre du gouvernement

Routeur

Un routeur est un dispositif de réseau qui est utilisé pour transférer des paquets de données entre des réseaux informatiques. Les routeurs sont responsables de diriger les paquets de données vers leurs destinations sur Internet.

Les connexions simultanées

Dans le contexte du VPN, les connexions simultanées font référence au nombre d'utilisateurs qu'un fournisseur de VPN autorise à utiliser un seul compte. Certains fournisseurs de VPN autorisent 5 appareils à se connecter en même temps, tandis que d'autres autorisent un nombre illimité d'appareils.

SmartDNS
SmartDNS est une fonctionnalité offerte par les fournisseurs de VPN qui permet aux utilisateurs de contourner les géo-blocages en utilisant des serveurs DNS basés sur la localisation de l'utilisateur ou sur le streaming qu'ils essaient de débloquer. Le SmartDNS n'est pas crypté, c'est pourquoi il n'est préférable que pour débloquer les services de streaming.

Split tunneling
Le split tunneling est une technique de mise en réseau qui permet à un utilisateur d'accéder à la fois à un réseau public et à un réseau privé, tout en maintenant les deux réseaux séparés l'un de l'autre. Cela se fait en acheminant une partie du trafic via le VPN (réseau privé virtuel) tout en permettant à d'autres trafics de circuler directement via le réseau local de l'utilisateur.

Charte des fouineurs
La Charte des fouineurs ou plus anciennement la Loi sur les pouvoirs d'enquête, proposée par l'ancienne secrétaire d'État à l'Intérieur Theresa May, impose aux FAI du Royaume-Uni de stocker les données des clients et de les partager avec les forces de l'ordre locales.

SSL
SSL signifie couche de sockets sécurisés. Cette technologie est responsable de sécuriser les données sensibles transférées entre deux ordinateurs. SSL empêche les entités malveillantes d'intercepter et de modifier toutes les données transférées en ligne.

Tor
Tor ou The Onion Router est un réseau open source qui permet aux utilisateurs de naviguer sur le web de manière anonyme. Le réseau Tor ne peut être accessible que via un navigateur Tor. Tor anonymise votre trafic web en le faisant passer par des nœuds dispersés.

Tunneling fractionné (bittorrent)
Le fractionnement du tunnel est une fonctionnalité offerte par les fournisseurs de VPN qui permet aux utilisateurs d'acheminer une partie de leur trafic via le tunnel VPN crypté tout en laissant le reste du trafic non crypté. Par exemple, permettre aux applications bancaires de passer par le tunnel crypté tout en excluant les applications de médias sociaux.

Tunnel
Un tunnel VPN est une connexion chiffrée entre votre appareil et le serveur VPN. Personne à l'extérieur du tunnel ne peut voir ou intercepter les données qui y transitent.

Le client VPN
Un client VPN est une application que vous installez sur votre téléphone, ordinateur portable ou routeur qui vous permet d'établir une connexion sécurisée avec un serveur VPN.

Le protocole VPN
Les protocoles VPN sont un ensemble de règles qui déterminent comment une application VPN établira une connexion sécurisée avec un serveur VPN. Certains protocoles offrent une sécurité puissante tandis que d'autres offrent des vitesses rapides. Quelques protocoles VPN courants sont PPTP, OpenVPN et IPSec.

Serveur VPN

Un serveur VPN est une ressource intermédiaire entre un utilisateur et Internet. Il est responsable de l'attribution à ses utilisateurs d'une adresse IP différente et de leur faciliter le contournement des blocages géographiques.

Adjudant canari

Un warrant canary est en fait un billet de blog par lequel les fournisseurs de services VPN informent leurs utilisateurs s'ils reçoivent une citation à comparaître du gouvernement pour divulguer des informations sur leurs clients. Cela permet de créer une certaine transparence entre le fournisseur et ses clients.

WebRTC

Web Realtime Communications permet aux navigateurs Web de gérer la vidéo et l'audio sans aucun plug-in. Firefox, par exemple, est un navigateur compatible WebRTC qui ne nécessite pas de plugin tel que Flash player pour la lecture vidéo et audio.

WireGuard

WireGuard est un protocole VPN open source moderne et efficace qui vise à fournir une communication rapide et sécurisée entre les appareils sur Internet.