L'ANONYMAT TOTAL SUR INTERNET - LE VPN

Cezar TOMA[1*],
Ana-Maria VECHIU[1]

[1]*Université Technique de Moldavie, Faculté Ordinateur, Informatique et Microélectronique, Département Génie Logiciel et Automatique, gr.FI-191, Chișinău, Moldova*

*L'auteur correspondant : Cezar Toma, toma.cezar@isa.utm.md

Résumé : *L'article explique ce qu'est un réseau privé virtuel, ses débuts, son fonctionnement, son utilité cruciale pour les internautes ainsi que ses inconvénients.*

Mots-clés : *Réseau privé virtuel (VPN), Interconnexion des systèmes ouverts (OSI), communication, objectifs, Protocole Internet (IP), type Client-Serveur, géo-restrictions, connexions (sessions), Microsoft, Cisco Systems, iOS (iPhone OS).*

Introduction

Pour comprendre les débuts de cette technologie, on doit avant tout élaborer sur l'histoire de l'Internet en général : pourquoi a-t-il été créé en première place ?

Durant le XXe siècle, l'armée américaine avait besoin d'un support fiable pour pouvoir maintenir la communication pendant les temps de tensions et de guerres. À l'époque, le seul moyen qui existait était vulnérable à toute attaque, car si un des centres de communication arrêtaient de fonctionner, l'ensemble du réseau était anéanti.

Des ingénieurs américains, pour le compte du ministère de la Défense, ont réussi, à travers de longues années d'expérimentations, de créer un réseau tel qu'on le connait aujourd'hui sous le nom de *« Internet »*. Avec celui-ci, l'information est acheminée par une multitude de routeurs, ce qui fait en sorte qu'il est pratiquement impossible d'interrompre la communication, ce qui assurait les besoins de l'armée.

Ces routeurs, il en existe des centaines de milles, voire des millions [1].

La communication peut changer de direction à tout moment si, par exemple, certains d'entre eux sont défectueux ou subissent une incursion informatique. Par contre, tout ce libre-échange d'information crée des nouvelles difficultés.

La première, par exemple, étant le fait que les données qui passent à travers ces routeurs peuvent facilement être intercepté par des pirates informatiques. Ils peuvent rassembler cette information et voir actuellement l'activité des utilisateurs.

L'information confidentielle peut se retrouver dans les mains de quiconque qui sait comment pénétrer ce réseau. Le besoin d'un réseau confidentiel ne cessait de croître, ce qui a amené l'apparition du réseau privé virtuel, aussi connu sous le nom de VPN.

Il a d'abord été créé pour les entreprises et les gouvernements, qui pour leur part, désiraient transmettre des informations confidentielles sans que leur discrétion soit corrompue. À long terme, ce besoin est devenu une quasi-nécessité pour les individus ayant accès à Internet. [1]

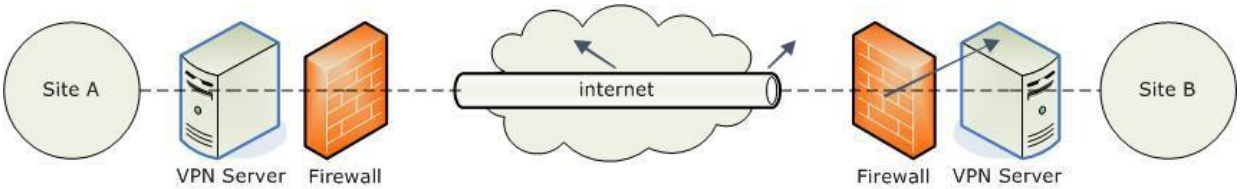

Figure 1. Principe d'un VPN simple

Le mode Tunneling

Parallèlement, l'idée d'un protocole de tunneling est apparue. C'est une notion à retenir pour comprendre le fonctionnement d'un VPN, utilisé même à l'heure actuelle. Il permet la connexion à distance à un réseau avec une adresse IP qui n'est pas locale.

Leur utilisation est simple par rapport à la complexité de la technologie.

Toutefois, tout se résume à l'idée que les paquets contenant les données qui circulent sont cryptés et reçoivent une nouvelle marque d'identification, avec une adresse IP différente, pour un anonymat quasi total. Cela signifie aussi que même si des pirates arrivent à collecter ces données, elles leur seront inutiles.

Le but d'un VPN est donc d'accéder Internet par une connexion privée, en changeant votre localisation et en assurant la confidentialité de l'information par cryptage (c'est-à-dire que les paquets qui contiennent les informations sont chiffrés).

Dans le même ordre d'idées, les tunnels ont la capacité de s'éteindre eux-mêmes s'ils détectent une attaque. Un nouveau chemin est alors recréé. Originairement, l'Internet est vulnérable d'un point de vu de la sécurité des données. C'est ici que l'utilisation d'un VPN s'avère être bénéfique de cette perspective [2].

La façon dont cela fonctionne peut paraître complexe : les paquets qui contiennent les informations qui exécutent le service de chiffrement et de livraison en créer une sorte de bouclier l'intérieur de toute influence extérieure. Ce service va chiffrer l'ensemble du paquet puis le ré encapsuler avec une nouvelle adresse IP pour obtenir une nouvelle marque d'identification [2].

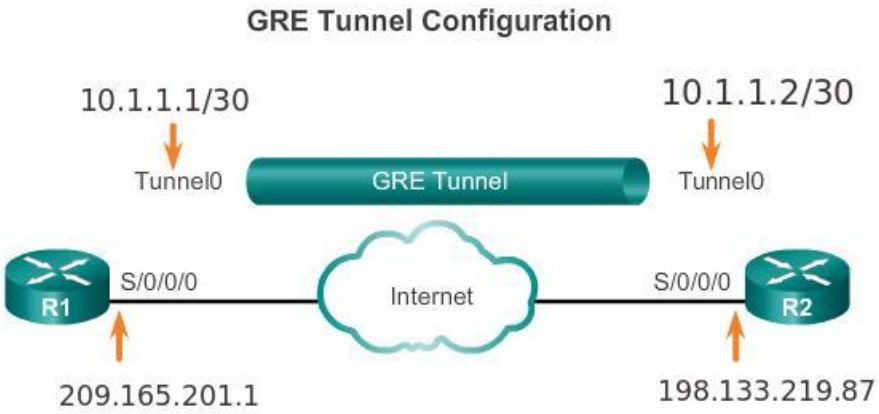

Figure 2. Le mode Tunneling

Censure et géo-restriction

À travers le monde, certains pays ont des restrictions pour des raisons : sociale, politique et de sécurité internationale. Des compagnies bloquent aussi l'accès du contenu de leurs sites Web et de leurs services basés sur l'emplacement de l'utilisateur.

Les géo-restrictions existent à cause des régulations de licence qui viennent en jeu lorsqu'il est question de diffusion dans un autre pays. Même si la consommation de média a tourné vers les abonnements, le système de licenciement est toujours resté en place.

Ces problèmes peuvent dorénavant être dépassés avec l'utilisation d'un VPN. Puisque l'adresse IP n'est pas locale, la localisation peut être transposé où l'on veut, selon les possibilités du fournisseur. En d'autres mots, l'adresse est masquée et votre emplacement est virtuel [2][3].

Utilisation

Un VPN possède une structure de type Client-Serveur, ce qui signifie que le logiciel permet aux clients de se connecter de façon sécuritaire à ce service. Il est nécessaire de savoir qu'il existe différents types de VPN, et certains sont construits selon des besoins spécifiques, comme le font Microsoft ou Cisco.

Généralement, l'utilisation de ce service est comme suivie : un client VPN doit être installé sur votre ordinateur et une adresse IP doit être fournie pour que vous puissiez introduire vos identifiants.

Votre connexion passera par Internet jusqu'au serveur et ce dernier va vérifier votre authentification.

Voici un exemple concret d'utilisation : si vous vous situez dans un bureau à Chisinau et que vous désirez vous connecter à un bureau à Paris, vous n'avez qu'à vous connecter à votre réseau VPN et le tour est joué, aussi simple que cela puisse paraître [3].

Pour établir une connexion VPN, il est nécessaire d'utiliser le modèle OSI, plus précisément les couches nommées « *hautes* », de présentation et de session. Le modèle OSI est une norme de l'Organisation Internationale de Normalisation, publiée en 1984, qui contient une liste de protocoles de communication hiérarchisés. Le niveau de la présentation a pour rôle de chiffrer et déchiffrer les données machine en données utilisables par n'importe quel autre dispositif [3].

Le niveau de session permet le contrôle de la communication entre les applications. En d'autres mots, établir, maintenir, gérer et fermer les connexions des applications.

Avantages

En fait, certains d'entre eux ont été énumérés ci-dessus. Mais il est essentiel d'élaborer sur d'autres aspects, qui sont bénéfiques à une utilisation quotidienne. Le cryptage AES 256 bits, permet, encore une fois, de vous permettre une tranquillité quasi totale lors de votre navigation.

De plus, les téléchargements sont maintenant hors de la vue du gouvernement ou du fournisseur en question.

La diffusion de flux vidéo est autant possible, c'est-à-dire sans restriction. Un aspect qui est moins mis en évidence serait les économies : les abonnements peuvent varier grandement, car vous simulez les tarifs selon les différents pays.

C'est le cas, par exemple, avec la réservation des billets d'avion. Une multitude de compagnies haussent leurs prix dépendamment de la localisation géographique.

Un VPN permet de contourner toutes ces barrières. Il est tout à fait possible, pour autant, d'avoir ce service sur les plateformes iOS et Android. Votre fournisseur d'accès à Internet ne pourra plus limiter votre bande passante. En outre, lorsque vous êtes dans un établissement scolaire, dans un hôtel ou à l'aéroport, vous serez en mesure de contourner les pare-feu mis en place [4].

Inconvénients

L'inconvénient principal lors de l'utilisation d'un VPN est, en réalité, la vitesse. Plus précisément la vitesse de téléchargement et de chargement des données. Puisqu'on n'est pas sur terre, la rapidité n'est pas la même. Votre vitesse sera celle de l'emplacement où vous vous situez. Par conséquent, la vitesse de chargement va drastiquement être rabaissée.

D'ailleurs, les fils électriques par lesquels sont transmises les connexions doivent aussi répondre aux exigences du service.

Les bâtiments qui possèdent des fils anciens et usés, par exemple, vont faire en sorte qu'il y a une perte de paquets lors de la connexion, ce qui va paraître au VPN qu'il s'agit en fait d'une pénétration pirate dans le système (ce qui n'est pas le cas).

Subséquemment, le réseau sera interrompu et va se recréer à l'infini, sans que vous puissiez l'utiliser.

Conclusion

Les gouvernements qui veulent avoir un contrôle sur la vie privée des gens, les fraudeurs qui espèrent faire du profit à votre nom et les corporations qui récoltent des millions de données sans que vous le sachiez : voilà la face cachée de l'Internet.

Le *World Wide Web*, tel qu'on le connait, n'est pas si simpliste qu'il en a l'air : le téléchargement de logiciels espions, l'exploitation des données personnelles et le freinage du flux de l'information sont des obstacles que l'on doit prendre de sérieuses précautions.

Le VPN est une alternative à toutes ces difficultés, et il va permettre le progrès de l'Internet, en ce qui concerne la sécurité des utilisateurs et plus les gens vont connaître ses avantages, plus le nombre de piratages et de vols d'identité va diminuer.

On peut conclure que les bénéfices liés à l'emploi d'un VPN dépassent largement le nombre d'inconvénients de celui-ci.

Bref, à présent, cette technologie devient petite à petit presque indispensable, aussi bien pour les entreprises, que pour les simples internautes.

Nous remercions: Mme Daniela Istrati, lecteur universitaire au Département Génie Logiciel et Automatique, Université Technique de Moldova, pour l'aide à l'élaboration de cet article

Bibliographie

1. Eli the Computer Guy. *VPN - Virtual Private Networking* [en ligne]. 21 avril 2011. [Accédé le 06.02.2020] Disponible : https://www.youtube.com/watch?v=q4P4BjjXghQ&fbclid=IwAR2tYwX6Flyei-X19UBoyTBKbSVwGTNSTZdJHyY2bR8gYt1JzFT83KOGvKg
2. Le VPN, *L'HISTOIRE DES VPN* [en ligne]. 11 avril 2019. [Accédé le 07.02.2020]. Disponible : https://www.le-vpn.com/fr/histoire-des-vpn/
3. Wikipedia, *Réseau privé virtuel*. [Accédé le 07.02.20] Disponible : https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel
4. VPN ACTU, *Les Avantages d'un VPN* [en ligne]. 13 février 2018. [Accédé le 08.02.20]. Disponible : https://vpnactu.fr/le-vpn-et-ses-avantages/