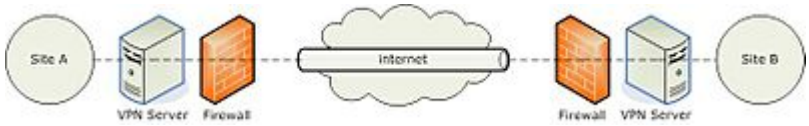
NOUVEL HAY MAGAZINE
SANS FRONTIÈRES

VPN ? (Virtual Private Network) , Réseau Privé Virtuel

En informatique, un **réseau privé virtuel**[1,2] (**RPV**) ou **réseau virtuel privé**[2] (**RVP**), plus communément abrégé en **VPN**[3] (de l'anglais : *virtual private network*), est un système permettant de créer un lien direct entre des ordinateurs distants, connectés à des réseaux locaux différents, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

On utilise notamment cette technologie en situation de télétravail ainsi que dans le cadre de l'informatique en nuage.



Types

Le VPN peut être de type point à point, utilisé entre un client et un concentrateur[4].

Dans une autre acception, le VPN peut exister sous la forme d'un réseau privé virtuel hermétique et distribué sur un nuage MPLS[5]. Les ordinateurs sur ce VPN y sont souvent raccordés physiquement, la notion de « virtuel » se rapportant alors au fait que l'infrastructure MPLS fait circuler plusieurs réseaux virtuels étanches entre eux.

De façon plus générale les VPN peuvent être classés selon les protocoles, services, et type de trafic (couche OSI 2 ou 3) pouvant circuler en son sein.

VPN client / concentrateur

La connexion entre les ordinateurs est gérée de façon transparente par un logiciel de VPN, créant un tunnel entre eux. Les ordinateurs connectés au VPN sont ainsi sur le même réseau local (virtuel), ce qui permet de passer outre d'éventuelles restrictions sur le réseau (comme des pare-feux ou des proxys).

Les principales techniques pour les postes clients

Le VPN SSL

Article détaillé : SSL VPN.

Aussi appelé « *clientless* », car il ne nécessite pas l'installation d'un logiciel client ; un navigateur Web compatible avec l'ouverture des sessions HTTPS SSL/TLS est suffisant.

Un tunnel VPN SSL ne permet pas de véhiculer différents protocoles de communication comme le VPN IPsec, mais des solutions existent ainsi :

Pour le protocole RDP, l'ouverture d'un bureau distant utilisera l'accès Web aux services Bureau à distance (*RD Web Access*) qui permet d'accéder aux programmes RemoteApp et aux services Bureau à distance.

Le VPN IPsec

Article détaillé : Internet Protocol Security.

L'installation d'un logiciel « agent » est nécessaire afin d'établir un tunnel vers un serveur VPN.

Un Tunnel VPN IPsec permet de véhiculer différents protocoles de communication tels que SSH, RDP, SMB, SMTP, IMAP, etc.

Une technique alternative consiste à utiliser du L2TP/IPsec6 qui associe ces protocoles pour faire passer du PPP sur L2TP sur IPsec, en vue de faciliter la configuration côté client sous Windows7.

Intérêt

Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local. Il permet d'avoir un accès au réseau interne (réseau d'entreprise, par exemple) ou de créer un réseau de pairs.

Un VPN dispose généralement aussi d'une « passerelle » permettant d'accéder à l'internet, ce qui permet de changer l'adresse IP source publique de ses connexions. Cela rend plus difficile l'identification et la localisation approximative de l'ordinateur émetteur par le fournisseur de service. Cependant, l'infrastructure de VPN (généralement un serveur) dispose des informations permettant d'identifier l'utilisateur : par exemple, les sociétés proposant des VPN gratuits ou payants peuvent récolter les données de navigation de leurs clients, ce qui relativise l'apparent anonymat de ces services. Cela permet aussi de contourner les restrictions géographiques de certains services proposés sur Internet.

Le VPN permet également de construire des « *réseaux overlay* », en construisant un réseau logique sur un réseau sous-jacent, faisant ainsi abstraction de la topologie de ce dernier.

L'utilisation de VPN n'est généralement pas légalement restreinte. Elle l'est en Chine. Jusqu'à mi-2017, le gouvernement semblait tolérer certains usages comme l'accès par un grand nombre de chercheurs chinois à des études publiées en ligne dans le monde mais inaccessibles en Chine en raison d'une censure du Net qui a classé non seulement Google Docs et Dropbox, mais aussi Google Scholar en liste noire. En septembre 2017, il semble que la Chine ait décidé d'encore resserrer l'accès des Chinois à Internet en accroissant la répression pour ceux qui utilisent des réseaux privés virtuels (VPN), donc non contrôlés par le gouvernement. La communauté scientifique internationale (relayée par la revue Science) craint que cette mesure puisse « sérieusement éroder la capacité des scientifiques chinois à rester en contact avec des pairs à l'étranger »8.

VPN sur les routeurs

Avec l’utilisation croissante des VPN, beaucoup ont commencé à déployer la connectivité VPN sur les routeurs. Ainsi, l’objectif étant de renforcer la sécurité et le chiffrement de la transmission de données en utilisant diverses techniques cryptographiques9. À domicile, les utilisateurs déploient généralement des

réseaux privés virtuels sur leurs routeurs pour protéger des périphériques : tels que des téléviseurs intelligents ou des consoles de jeux qui ne sont pas pris en charge par les clients VPN natifs. Les périphériques pris en charge ne sont pas limités à ceux capables d'exécuter un client VPN10.

De nombreux fabricants de routeurs fournissent des routeurs avec des clients VPN intégrés. Des utilisateurs remplacent les microprogrammes fournis par les fabricants par des microprogrammes open-source tels que DD-WRT, OpenWRT ou Tomato, afin de prendre en charge des protocoles supplémentaires tels que OpenVPN.

Chiffrement

Les connexions VPN ne sont pas nécessairement chiffrées. Cependant si l'on ne chiffre pas, cela peut permettre à des éléments intermédiaires sur le réseau d'accéder au trafic du VPN, ce qui peut être problématique si les informations qui y transitent sont sensibles. De plus, des techniques de DPI permettent à des pare-feux de filtrer le trafic du VPN s'il n'est pas chiffré.

Chiffreur IP

Un chiffreur IP est un équipement de sécurité du réseau informatique, réalisant la fonction passerelle pour un réseau privé virtuel11.

Un chiffreur IP est placé au point d'entrée et de sortie d'un réseau local afin d'établir un lien de communication entre plusieurs de ces réseaux locaux, en utilisant un réseau externe considéré comme non sûr. Ce réseau externe peut être, par exemple, Internet. L'établissement de ces liaisons permet de constituer un réseau privé virtuel chiffré, augmentant ainsi la sécurité de la transmission d'information d'un réseau à un autre, principalement en matière de confidentialité11.

Protocoles

Un réseau privé virtuel utilise un ou plusieurs protocoles parmi les suivants :

- GRE (*Generic Routing Encapsulation*) développé au départ par Cisco, à

l'origine protocole transportant des paquets de couche 3, mais pouvant désormais aussi transporter la couche 212

- PPTP (*Point-to-Point tunneling Protocol*) est un protocole transportant des trames de couche 2 (du PPP) développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (*Layer Two Forwarding*) est un protocole transportant des trames PPP (couche 2) développé par Cisco Systems, Nortel et Shiva. Il est désormais obsolète.
- L2TP (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'IETF (RFC 393113) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole transportant des sessions PPP (couche 2).
- IPsec est un protocole transportant des paquets (couche 3), issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il est associé au protocole IKE pour l'échange des clés.
- L2TP/IPsec est une association de ces deux protocoles (RFC 319314,6) pour faire passer du PPP sur L2TP sur IPsec, en vue de faciliter la configuration côté client sous Windows7.
- SSL/TLS, déjà utilisé pour sécuriser la navigation sur le web via HTTPS, permet également l'utilisation d'un navigateur Web comme client VPN. Ce protocole est notamment utilisé par OpenVPN.
- SSH permet, entre autres, d'envoyer des paquets depuis un ordinateur auquel on est connecté.
- MPLS permet de créer des VPN distribués (VPRN)15 sur un nuage MPLS16, de niveau 2 (L2VPN) point à point17, point à multipoint (VPLS), ou de niveau 3 (L3VPN) notamment en IPv4 (VPNv4)18 et/ou IPv6 (VPNv6 / 6VPE19,20), par extension et propagation de VRF (*Virtual routing and forwarding* – tables de routage virtuelles) sur l'ensemble du réseau MPLS.

VPN dans les environnements mobiles

Les réseaux privés virtuels mobiles sont utilisés dans des paramètres où un point de terminaison du VPN n'est pas fixé à une seule adresse IP, mais se déplace à la place sur divers réseaux tels que les réseaux de données d'opérateurs cellulaires ou entre plusieurs points d'accès Wi-Fi sans abandonner la session VPN sécurisée ou perdre des sessions d'application21. Les VPN mobiles sont largement utilisés

dans la sécurité publique où ils donnent aux agents des forces de l'ordre l'accès à des applications telles que la répartition assistée par ordinateur et les bases de données criminelles22, et dans d'autres organisations ayant des exigences similaires telles que la gestion des services sur le terrain et les soins de santé23,24.

Limitations du réseau

Une limitation des VPN traditionnels est qu'ils sont des connexions point à point et n'ont pas tendance à prendre en charge les domaines de diffusion ; par conséquent, la communication, les logiciels et la mise en réseau, qui sont basés sur la couche 2 et les paquets de diffusion, tels que NetBIOS utilisé dans la mise en réseau Windows, peuvent ne pas être entièrement pris en charge comme sur un réseau local. Des variantes de VPN telles que Virtual Private LAN Service (VPLS) et les protocoles de tunneling de couche 2 sont conçues pour surmonter cette limitation25.