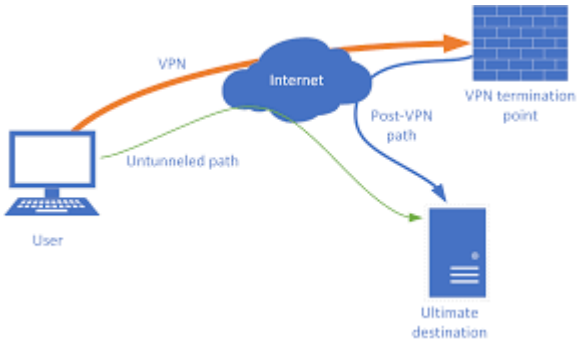
Tunnels réseau (VPNs, Proxy, etc.)

Tunnel réseau



Qu'est-ce qu'un tunnel réseau?

Un tunnel réseau est un mécanisme permettant l'encapsulation de trafic pour l'encryption de trafic IP entre deux points, pour relier deux sites distants comme s'ils faisaient partie d'un seul réseau local ou pour modifier la source apparente d'une connexion.

À quoi ça sert?

Utilisation personnelle d'un VPN

Le cas d'utilisation personnelle d'un service de VPN tel que Mullvad, SurfShark, NordVPN, etc. est d'encrypter le trafic entre le client et le fournisseur de VPN. Ceci permet de masquer notre trafic aux administrateurs de réseaux publics, que ce soit pour ajouter une couche de confidentialité ou pour contourner des règles de filtrage mises en place car le seul trafic qui sera observé sera du trafic encrypté vers une seule adresse : le serveur VPN. Il est important de noter qu'une fois le fournisseur de service VPN est traversé, le trafic n'est plus encapsulé sous un protocole VPN.

Un autre cas d'utilisation commun est de modifier la source apparente du trafic, que ce soit pour accéder à des ressources qui seraient bloquées à notre source courante (ex. du contenu restreint à une source géographique tel que des séries Netflix accessibles uniquement à partir d'un pays spécifique).

Utilisation en entreprise d'un VPN

Un VPN est généralement utilisé en entreprise pour permettre l'accès de ressoures d'un réseau distant tels qu'un NAS pour le partage de fichiers, une imprimante qui serait au bureau à partir d'un poste de télétravail, etc. Il est aussi souvent utilisé pour relier des sites réseau distants afin d'en faciliter leur administration et pour faciliter la transition d'employés entre deux sites d'une entreprise (ex. un employé d'Agnico Eagle qui doit circuler entre plusieurs mines n'aurait pas à changer de compte d'utilisateur en fonction de sa localisation)

Utilisation d'un proxy

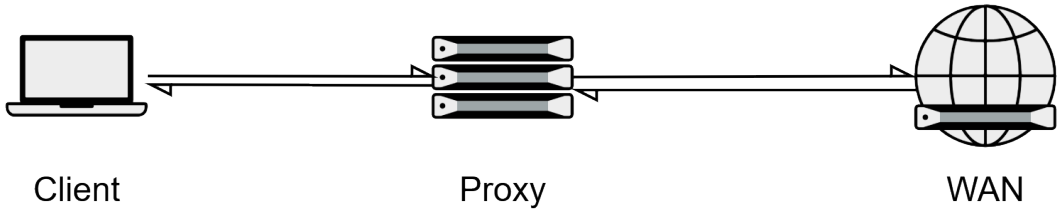
Deux types de proxy existent. Un proxy traditionnel est tout comme un VPN, un serveur auquel notre trafic sera acheminé pour changer sa source apparente. À moins qu'il s'agisse d'un proxy (SOCKS ou Socket Secure), le trafic n'est pas encapsulé dans ce contexte. Il peut aussi être utilisé pour permettre l'inspection et le filtrage de trafic (ex. le trafic d'hôtes dans un bureau vers des destinations de réseau étendu).

Un proxy inverse est plutôt comme une redirection de port. Plusieurs entrées DNS pourraient pointer vers le même proxy et en fonction de l'entrée DNS utilisée pour le contacter, il pourra rediriger le trafic vers le bon serveur web. Ceci permet d'héberger plusieurs sites web derrière une seule adresse IP.

Types de tunnels

Proxy (serveur mendataire/intermédiaire)

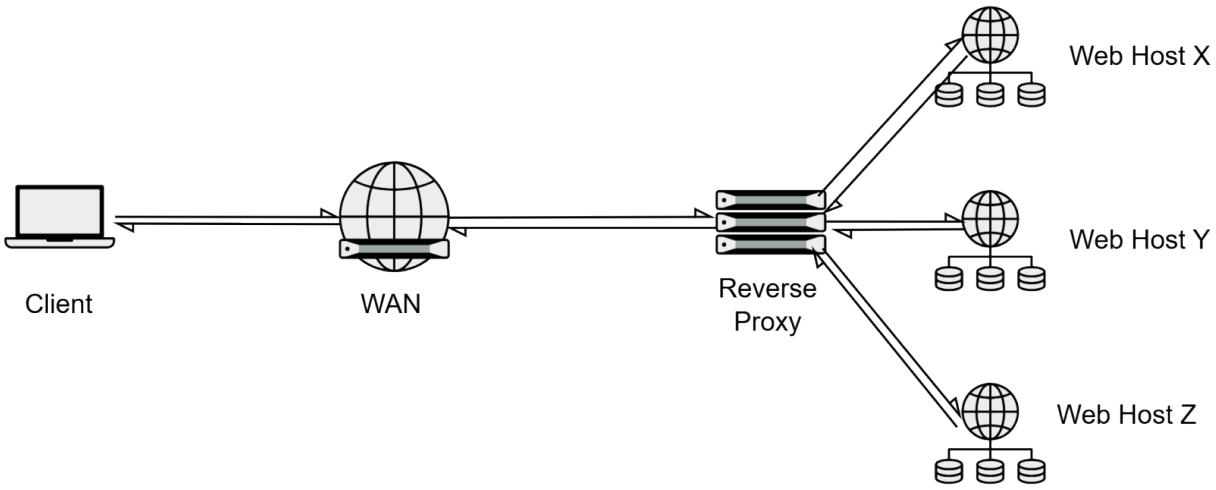
Direct



Un proxy direct est un intermédiaire entre un client et un serveur web. Celui-ci peut être utilisé pour masquer ou changer l'adresse IP d'origine de la demande de connexion, pour forcer une authentification avant d'accéder à un serveur, pour inspecter à but de filtrage le trafic le traversant ou pour effectuer de la mise en cache. Ce dernier cas d'utilisation permet de réduire la charge appliquée à une connexion internet en gardant une copie de la donnée à transmettre pour la redistribuer à d'autres clients au besoin..

Il est aussi à noter qu'ici, la requête n'a aucune encapsulation de plus que la requête HTTP(S). Aucun protocole de VPN.

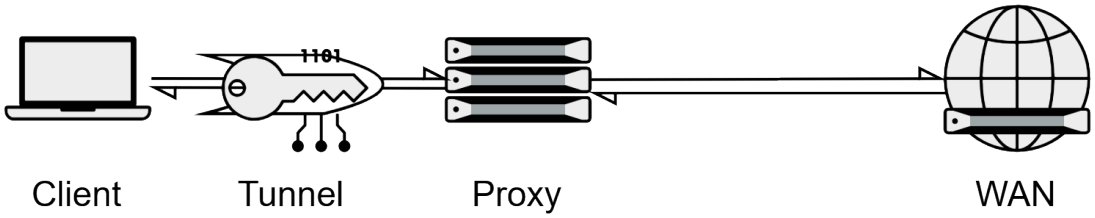
Inverse



Un proxy inverse est un intermédiaire entre un client et un serveur web qui dirigera la requête d'un client vers le serveur approprié. Il permet donc d'héberger plusieurs services web décentralisés et de diriger les requêtes entrantes au proxy inverse vers le bon serveur en fonction de l'adresse demandée dans la requête. Il pourrait aussi permettre une balance de charge vers plusieurs

serveurs offrant la même ressource et d'assurer une haute disponibilité en dirigeant les connexions en fonction de l'état des serveurs webs concernés.

SOCKS

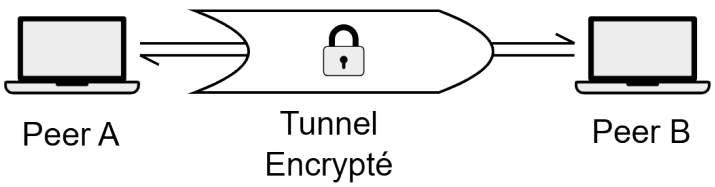


Un proxy SOCKS ou Secure Socket quant à lui achemine les données vers le serveur intermédiaire à travers un lien sécurisé/encrypté (ex. tunnel SSH) et permet de diriger tout type de trafic TCP et UDP plutôt que seulement HTTP/HTTPS/FTP/SFTP. Ceci est communément appelé un VPN de pauvre .

VPN

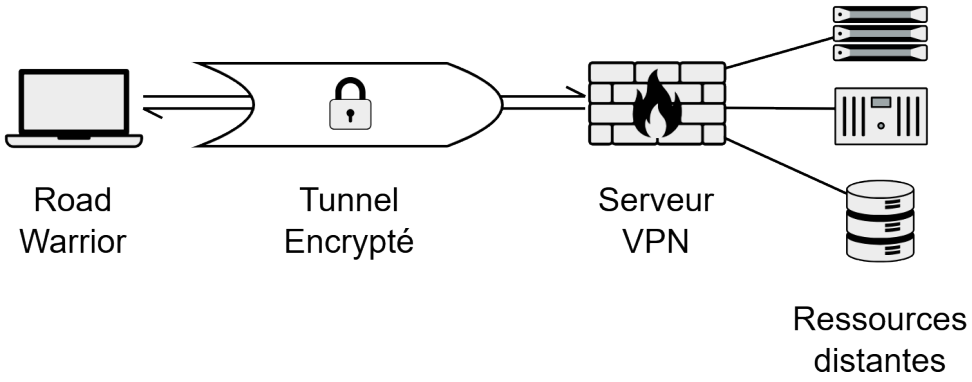
Un VPN contrairement à un serveur mandataire (proxy) doit établir un lien entre deux points préalablement à l'acheminement de données. Cet établissement de lien permet la négociation d'une méthode d'encapsulation et d'encryption du trafic entre les deux points. Celui-ci masque aussi l'adresse source et l'adresse de destination entre les deux points de terminaison de ce tunnel. Ceci permet entre autre l'encryption de trafic entre deux interlocuteurs ainsi que de faire communiquer deux adresses IP locales à travers un réseau étendu ou Internet même si ces adresses de sont pas routées ou routables, tant que les deux interlocuteurs puissent se contacter à travers ce réseau étendu.

Point à point



Un tunnel VPN point à point est généralement utilisé pour encrypter une communication entre deux appareils et permet de prévenir des attaques du type man-in-the-middle qui permettrait à un acteur malveillant de capturer une communication.

Point à site



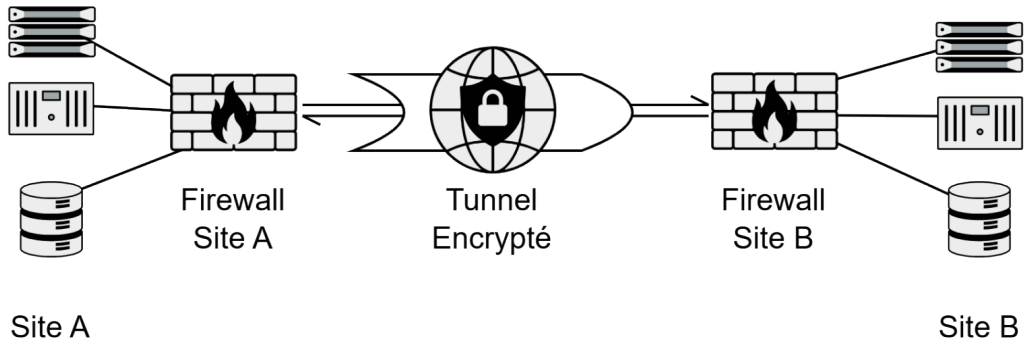
Comme tout type de tunnel VPN, un lien entre deux points doit tout d'abord être établi mais une fois ce lien établi, il est possible de créer des routes permettant d'accéder à des ressources distantes. Ce type de connexion est souvent nommée un "road warrior", représentant un client nomade se connectant à une infrastructure centralisée.

Le cas d'utilisation personnel le plus répandu est généralement entre un hôte et un serveur VPN public permettant d'encrypter notre trafic entre notre appareil et le fournisseur de VPN pour masquer notre trafic aux acteurs entre ces deux points. Ce type d'utilisation permet aussi de masquer notre identité vis-à-vis un service à contacter puisque nos connexions se trouvent derrière un NAT du fournisseur de VPN. Ceci peut être utile lors d'actions douteuses sur Internet ou pour accéder à des ressources qui sont limitées à certains réseaux IP (ex. limitation géographique).

Le cas d'utilisation professionnel le plus répandu est de permettre à un point d'accéder aux ressources d'un réseau distant (ex. un télétravailleur qui accèderait à un stockage réseau ou à un site intranet hébergé à un site centralisé) sans devoir créer de redirection de permettant l'accès au public à ces ressources.

Ce type de lien pourrait aussi être utilisé pour joindre un serveur privé virtuel (ex. Amazon Web Services ou Azure) à votre réseau local de façon transparente.

Site à site



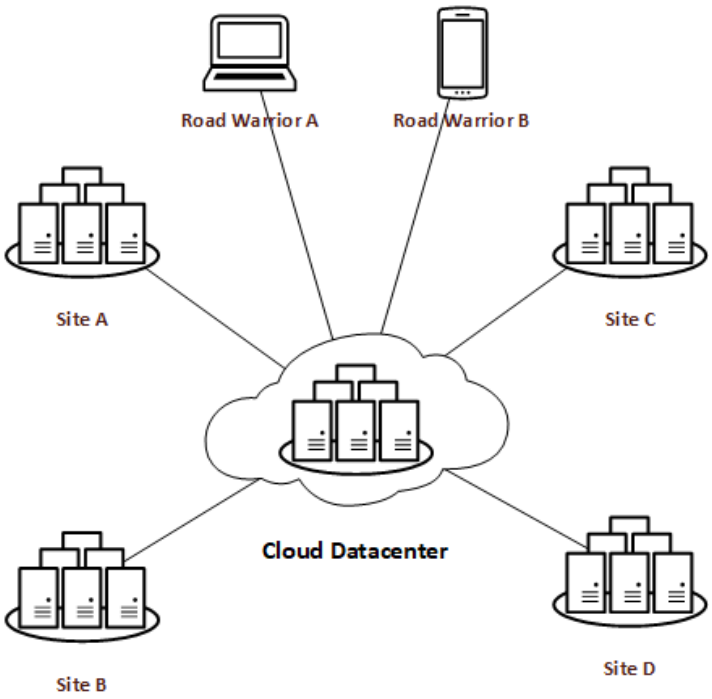
Un lien VPN de type site-à-site sert à établir un lien sécurisé entre deux réseaux locaux distants. On pourrait penser ici à un lien entre des bureaux distants et un centre de données. Ce type de lien permet de relier des réseaux locaux à travers un réseau étendu sans devoir router ces réseaux.

On pourrait penser ici à relier des réseaux IP réservés à utilisation privée non-routables sur Internet à travers une connexion traversant Internet. Un exemple de ceci serait de permettre à un employé d'Agnico Eagle d'accéder aux mêmes ressources (ex. NAS ou intranet) de la même façon et ce, peu importe le site de l'entreprise auquel se situe l'employé.

Ce type de lien pourrait aussi être utilisé pour joindre une infrastructure infonuagique (ex. Azure, AWS, Oracle Cloud Infrastructure) à votre réseau local comme s'il s'agissait d'un subnet dédié à des serveurs infonuagiques.

Site à multi-sites

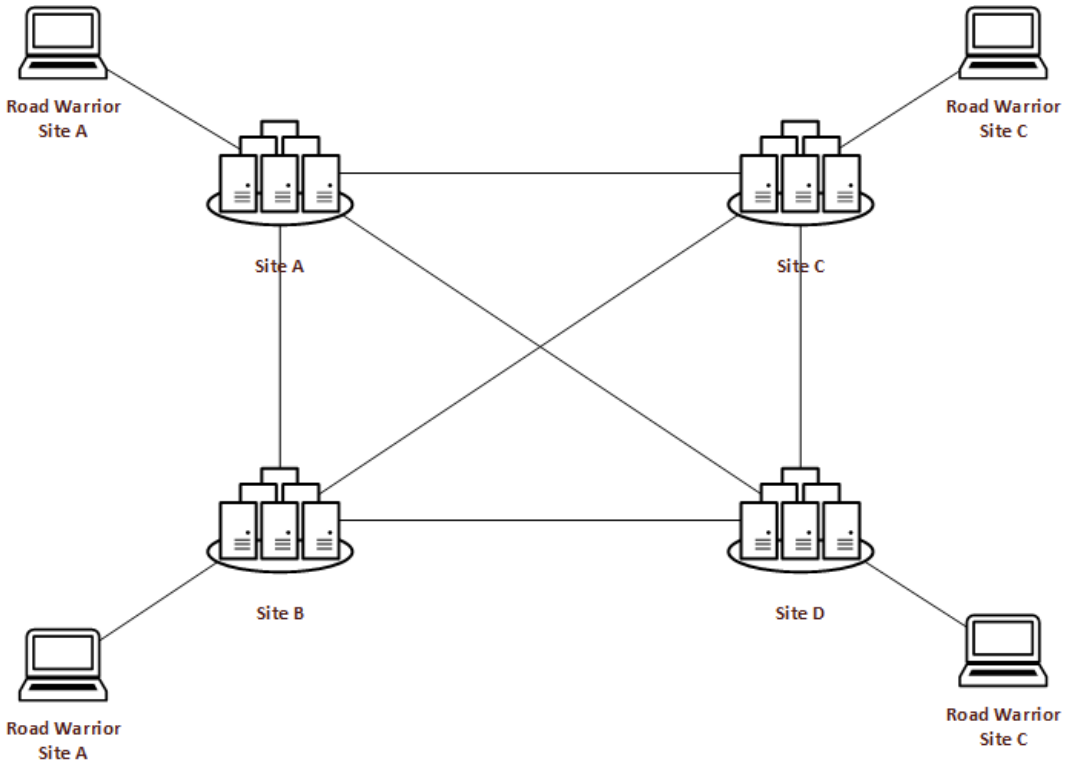
Hub-and-spoke (étoile)



Il est possible de relier ensemble plus de deux sites par différentes topologies. Une des topologies les plus populaires est une topologie de type "hub and spoke" puisqu'elle est aussi une des plus faciles à intégrer et à gérer. Cette topologie consiste à relier chaque site à un point central (généralement un centre de données, une plate-forme infonuagique comme Azure/AWS ou le site principal d'une entreprise). Cette configuration permet de centraliser les règles de quel site peut rejoindre quel autre site mais a le désavantage de nécessiter une bande passante considérable et des équipements performants puisque toutes les communications entre chaque site circulera par cette connexion et ces appareils.

Ce genre de topologie est préférable si certaines ressources telles que le contrôleur de domaine d'une forêt principale active directory, des bases de données ou des stockage réseau doivent être centralisées accessibles depuis plusieurs sites.

Mesh (maillé)



Il est aussi possible de relier plusieurs sites directement entre eux. Ceci implique que la configuration des règles de filtrage sont décentralisées et généralement que les road warriors devront être assignés à un site. Ce genre de configuration peut être préférable dans un contexte de petite à moyenne entreprise ou à utilisation personnelle (ex. entre vos amis et vous pour des jeux en réseau local/serveur de jeu ou un NAS de relève décentralisé chez un ami ou de la famille). Lorsque chaque site est relié à tous les autres sites, on parle alors d'un "full mesh". Un avantage est que l'on ne dépend pas d'un site central (quoi que celui-ci devrait être redondant).