Administration des Systèmes et Réseaux

LES RÉSEAUX PRIVÉS VIRTUELS (V.P.N)

Auteur: Bernard GIACOMONI - Autoentreprise GIACOMONI Bernard

Version	Date	Objet
1.0	26/11/2019	Version initiale

Table des matières

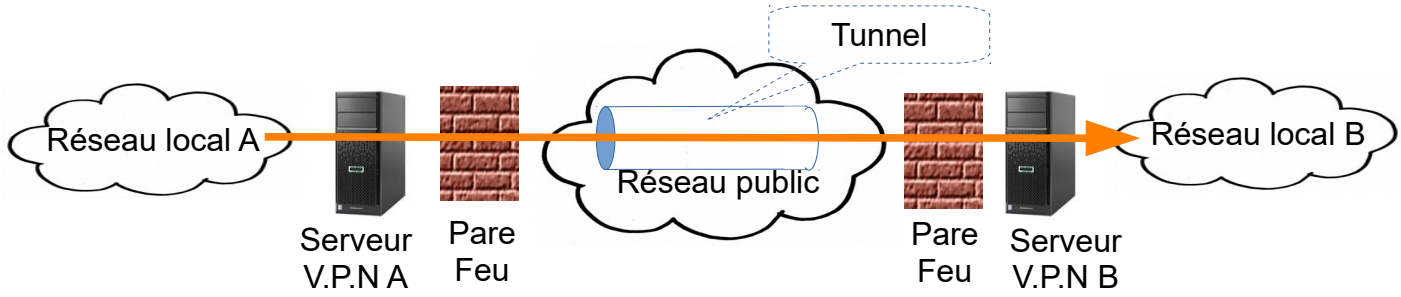
I.DÉFINITION:

Un réseau privé virtuel (Virtual Private Network: VPN), permet de créer un lien direct entre des ordinateurs distants connectés à travers un réseau de communication en isolant leurs échanges du reste du trafic de ce réseau.

II.PRINCIPES DE FONCTIONNEMENT:

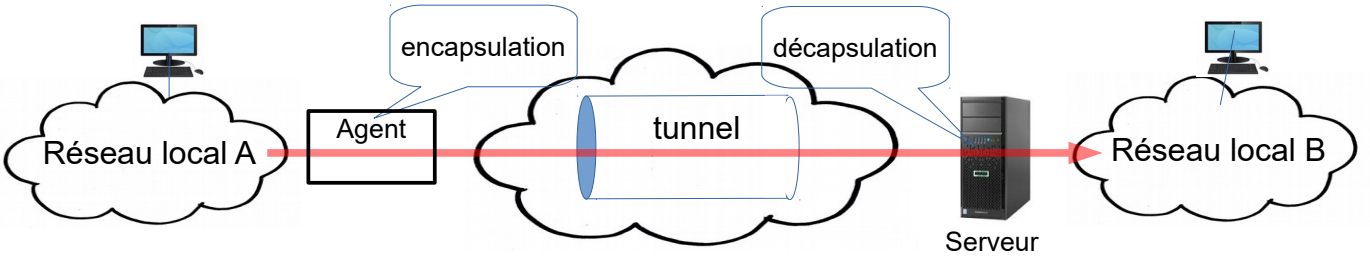
L'objectif est de permettre aux hôtes d'un réseau local A de dialoguer avec ceux d'un réseau local B, distants l'un de l'autre et connectés tous deux à travers une même infrastructure réseau, en isolant et en protégeant leurs échanges du reste du trafic. Cet objectif peut être atteint par l'utilisation d'un Réseau Public Virtuel (VPN).

Du point de vue physique, un VPN est implémenté à chacune des deux extrémités d'un TUNNEL par un logiciel SERVEUR VPN. Ces serveurs peuvent être intégrés dans les postes de travail, dans les routeurs ou même dans les pare-feux :



RAPPEL: En informatique de réseau, un TUNNEL est un mécanisme qui, mis en place entre deux nœuds non adjacents N1 et N2 d'un RÉSEAU PUBLIC, permet de rendre invisibles du reste du réseau les données de protocoles (comme les adresses IP source et destination) et même les données utiles (en cas de cryptage) des PAQUETS de données qui transitent par ce tunnel.

Dans la pratique, pour une transmission donnée, un logiciel "agent" situé en amont du tunnel encapsule les paquets émis dans la partie "données utiles" d'un nouveau paquet qui, lui , sera émis vers un SERVEUR situé à l'autre bout du tunnel. Celui-ci "décapsulera" les paquets d'origine avant de les transmettre à leur destinataire final. Le schéma ci-après explicite le mécanisme d'envoi d'un paquet du LAN A vers le LAN B :



REMARQUE: dans son essence, un serveur V.P.N n'est qu'un logiciel serveur de type particulier:

- S'il est installé sur un routeur, il peut être utilisé par l'ensemble des hôtes du réseau local auquel ce routeur appartient: il tient le rôle de "concentrateur VPN". Il dispose dans ce cas d'une PASSERELLE vers le réseau "englobant" (public ou privé);
- Un V.P.N peut également être installé sur un hôte particulier (poste client): dans ce cas, il ne permettra de connecter que ce client.

III.UTILISATION DES V.P.N:

Utiliser un V.P.N permet:

- De communiquer entre les deux réseaux locaux distants l'un de l'autre et reliés par une infrastructure d'interconnexion (publique ou privée) comme s'ils ne formaient qu'un seul réseau local;
- De masquer aux hôtes extérieurs les adresses IP réelles et les données échangées entre les extrémités du tunnel. En effet, les adresses et ports sources et destination des paquets circulant sur l'infrastructure d'interconnexion sont celles des serveurs VPN et non les véritables adresses et ports des machines communicantes;
- De créer des "réseaux virtuels" dans un même réseau physique pour séparer les différents flux de données y circulant (voix, video, données, etc.).

REMARQUES:

- Un V.P.N permet donc de raccorder "logiquement" deux réseaux locaux distants de manière à qu'ils ne forment plus qu'un seul réseau dont le trafic se trouve protégé de l'extérieur. On peut donc dire que les ordinateurs connectés au VPN sont sur un même réseau local "virtuel", ce qui permet de passer outre d'éventuelles restrictions éventuellement créées par les pare-feux ou les proxys.
- Les données circulant dans un V.P.N utilisent un TUNNEL dont le principe est d'encapsuler les paquets originaux: ceci suffit pour tromper les fonctions les moins évoluées des pare-feux (basées sur l'inspection des IP et des ports), mais ne résiste pas à une Deep Packet Inspection (D.P.I), qui s'intéresse au contenu des données transmises. Pour qu'un V.P.N puisse vraiment rendre opaques les données transmises, il est nécessaire de crypter les paquets originaux. Cependant, le cryptage ralentissant beaucoup la transmission, c'est une option qui ne convient pas forcément pour toutes les utilisations.

IV.DIFFÉRENTS TYPES DE VPN:

IV.1.INTRODUCTION:

Les différents types de V.P.N se distinguent les uns des autres essentiellement par le type de tunnel qu'ils utilisent. Nous citerons ci-après les deux types les plus courants:

IV.2.LES V.P.N S.S.L:

Comme leur nom l'indique, les V.P.N S.S.L (Secure Sockets Layer Virtual Private Network) fonctionnent en utilisant le protocole Transport Layer Security (TLS). Dans l'architecture TCP/IP, ce protocole fait partie la couche applicative.

De ce fait, un tel V.P.N est accessible par l'intermédiaire d'un simple navigateur web compatible avec l'ouverture des sessions HTTPS. Il existe aussi des "clients lourds" (comme OpenVPN) qui permettent de s'y connecter sans utiliser un navigateur.

Les inconvénients d'un V.P.N S.S.L sont que, se situant dans la couche application, il nécessite des applications adaptées et ne permet pas de véhiculer d'autre protocole que HTTP/HTTPS. Ils conviennent donc surtout à la consultation "anonyme" de sites web.

IV.3.LES V.P.N IMPLANTES AU NIVEAU DES COUCHES BASSES:

Ce type de V.P.N se positionne en général directement "au dessus" de la couche réseau. De ce fait, il ne nécessite aucune adaptation des applications utilisatrices: il suffit d'implanter un client au niveau du contrôleur de réseau. Un Tunnel VPN IPSec, par exemple, permet de véhiculer différents protocoles de communication tels que SSH, RDP, SMB, SMTP, IMAP, etc.

Ce type de 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.

V.IMPLANTATION D'UNE CONNEXION VPN:

V.1.INTRODUCTION:

Un échange V.P.N s'effectue entre un CLIENT V.P.N (parfois nommé AGENT VPN) et un SERVEUR VPN: au niveau d'un hôte utilisateur, il suffira d'utiliser ce client pour introduire les paquets que l'on veut émettre dans le tunnel (encapsulation+éventuellement cryptage), puis de les expédier vers le serveur V.P.N choisi. Le client effectue également la "décapsulation" des paquets qui lui sont renvoyés par le serveur et leur décryptage si nécessaire.

V.2.IMPLANTATION DANS UN NAVIGATEUR:

Il est possible d'implanter un client VPN dans un navigateur, moyennant l'ajout d'une extension (add-on) en général gratuite. Cependant, il s'agit dans ce cas de VPN de type SSL qui se limite à traiter le protocole HTTP. Ce type de solution est donc plus proche d'un PROXY que d'un VPN. Elle convient dans le cas où le besoin se limite à naviguer "discrètement" sur internet. Ce type de solution a parfois l'inconvénient de détériorer la qualité d'affichage des pages web (perte de définition, blocage des scripts javascript, etc.).

V.3.IMPLANTATION DANS UN SYSTÈME D'EXPLOITATION:

Il est également possible d'implanter un client VPN au niveau du contrôleur réseau d'un système d'exploitation. Dans ce cas, l'ensemble du trafic réseau de la machine hôte est redirigé vers le VPN.

Si le client est implanté dans le routeur internet d'un réseau local, l'ensemble des trafics des hôtes du réseau local utilisera le VPN pour communiquer avec l'extérieur.

V.4.INSTALLATION ET PARAMÉTRAGE D'UN VPN :

Après s'être inscrit auprès d'un fournisseur VPN gratuit ou payant (Open VPN, NordVPN, etc.) qui fournira en retour les informations nécessaires à la connexion et avoir installé un client VPN (si celui-ci n'est pas installé nativement dans le système d'exploitation, il fautra paramétrer ce client.

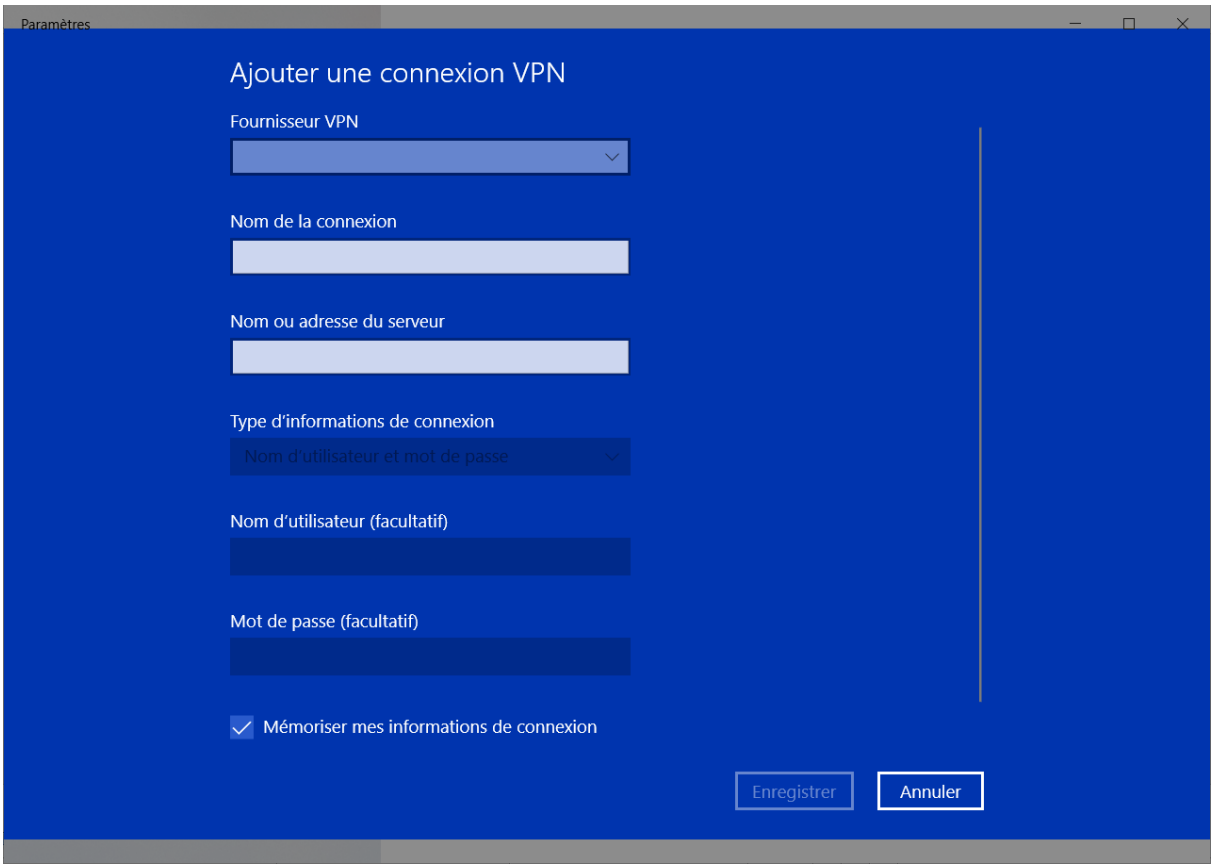
Le paramétrage revient surtout à :

- Identifier le fournisseur VPN ;
- Donner l'adresse IP ou le nom du serveur VPN à utiliser ;
- S'identifier auprès du fournisseur VPN (Id. et mot de passe).

CAS DE WINDOWS 10 :

Le paramétrage est possible en utilisant un menu qui peut être ouvert par :

Paramètres → Réseau et Internet → VPN → Ajouter une connexion VPN :



INSTALLATION DANS LINUX DEBIAN/UBUNTU :

L'installation (relativement complexe) s'effectue en ligne de commande, à partir de paquets Debian. Pour l'installation d'OpenVPN, voir https://doc.ubuntu-fr.org/openvpn. Une fois le client et le serveur installés, le paramétrage se fait par des menus graphiques.