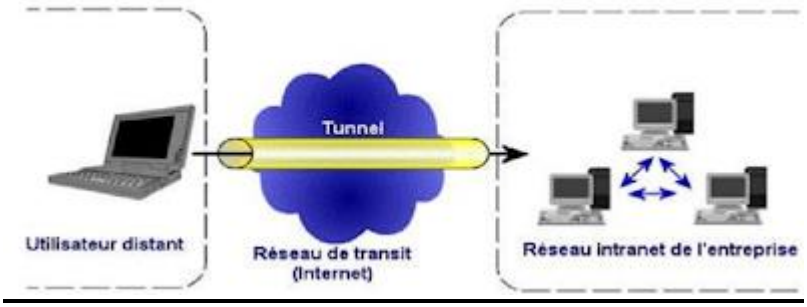
1) Introduction

VPN : Virtual Private Network ou RPV (réseau privé virtuel) en français est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de lison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique.

Jusqu'à l'avènement des VPN, les sociétés devaient utiliser des lisons Transpac, ou des lignes louées. Les VPN ont permis de démocratiser ce type de li son.

Schéma d'un accès VPN :



2) Principe de fonctionnement d'un VPN

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi,les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de **tunneling** consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant une en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

les avantages des VPN :

- Sécurité : assure des communications sécurisées et chiffrées.
- Simplicité : utilise les circuits de télécommunication classiques.
- Économie : utilise Internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée.

3) Les contraintes d'un VPN :

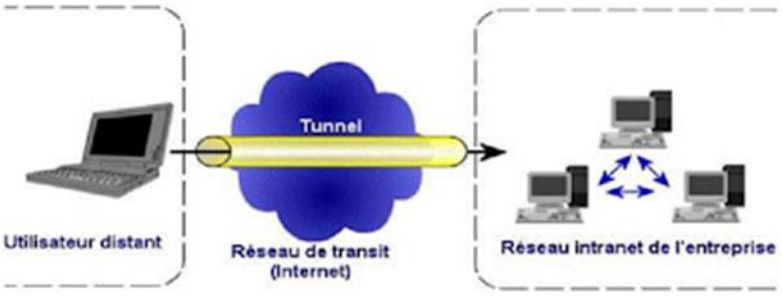
Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur : seuls les utilisateurs autorisés doivent avoir accès au canal VPN.
- Cryptage des données : lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace.
- Gestion de clés : les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multi protocole : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particuliers IP.

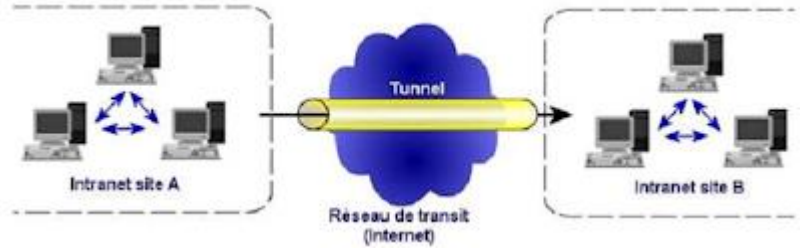
4) les différents types de VPN

Suivant les besoins, on référence 3 types de VPN :

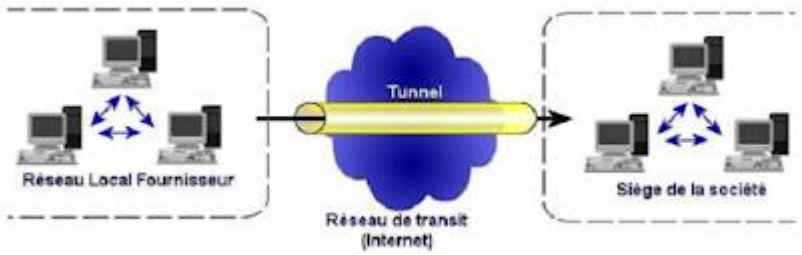
- **Le VPN d'accès** : il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.



- **L'intranet VPN :** il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploit ion de serveurs distants …



- **L'extranet VPN :** une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.



5) Les protocoles utilisés

Les protocoles utilisés dans le cadre d'un VPN sont de 2 types, suivant le niveau de la couche OSI auquel ils travaillent :

- Les protocoles de niveau 2 comme PPTP ou L2TP.
- Les protocoles de niveau 3 comme IPsec ou MLPS

5.1 le protocole PPP

PPP (Point to Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les

paquets Ip, Ipx et Netbeui dans des trames PPP, puis transmet ces paquets encapsulés au travers de la li son point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau

Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocoles PPTP ou L2TP.

5.2 Le protocole PPTP

PPTP (Point to Point Tuneling Protocol , définit par la Rfc 2637, est un protocole qui utilise une connexion PPP à travers un réseau Ip en créant un réseau privé virtuel (VPN).

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP.

Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur.

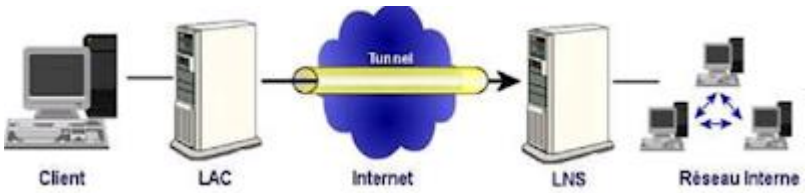
Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établit une connexion de type PPP et permet de faire circuler des données sur Internet.

Par la suite, une deuxième connexion est établi Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP.

5.3 Le protocole L2TP

L2TP (Layer Two Tuneling Protocol), définit par la Rfc 2661, est issu de la convergence des protocoles PPTP et L2F (Layer Two Forwarding). Il est actuellement développé et évalué conjointement par Cisco , Microsoft 3Com ainsi que d'autres acteurs du marché des réseaux. Il permet l'encapsulation des paquets PPP au niveau des couches 2 (Frame Relay et Atm) et 3 (Ip). Lorsqu'l est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. L2TP repose sur deux concepts :

les concentrateurs d'accès L2TP (Lac : L2TP Access Concentrator) et les serveurs réseau L2TP (Lns : L2TP Network Server). L2TP n'i ègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'Ipsec et L2TP



5.4 Le protocole Ipsec

Ipsec, définit par la Rfc 2401, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau Ipv4 étant largement déployé et la migration vers Ipv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à Ipv4 et Ipv6. Ces mécanismes sont couramment désignés par le terme Ipsec pour Ip Security Protocols. Ipsec est basé sur deux mécanismes. Le premier, AH, pour Authentification Header vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par ce "protocole" ne sont pas encodées. Le second, Esp, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement..

5.5 Les mécanismes de cryptage

Les protocoles sécurisés ont recours à des algorithmes de cryptage, et ont donc besoin de clefs. Un des problèmes principal dans ce cas est la gestion de ces clefs. Par gestion, on entend la génération, la distribution, le stockage et la suppression de ces clefs. Ces différentes tâches sont dévolues à des protocoles spécifiques de gestion de ces cléfs, à savoir :

- Isakmp (Internet Security Association and Key Management Protocol)
- Ike (Internet Key Exchange)

5.6 Le protocole SSL

Ssl (Secure Socket Layer) est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

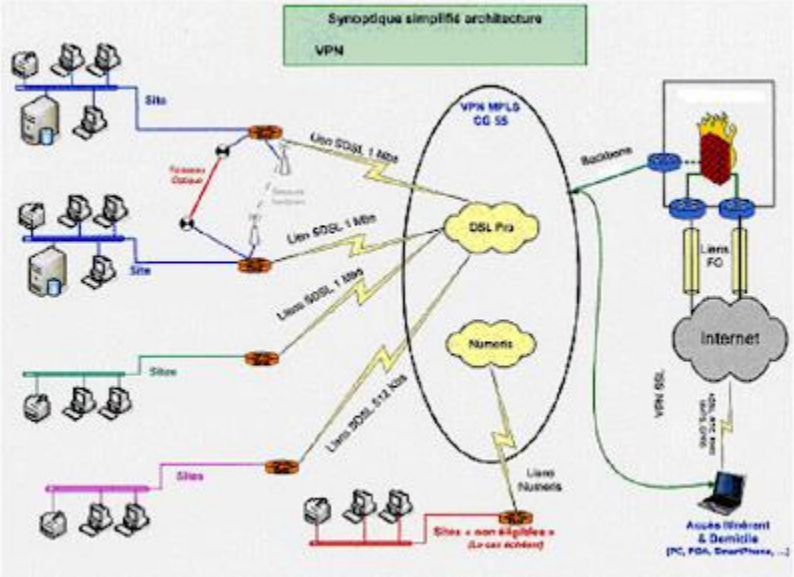
Ssl a deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.

SSL est le dernier arrivé dans le monde des Vpn, mais il présente un gros avantages dans la mesure ou coté client, il ne nécessite qu'un navigateur Internet standard. Ce protocole est celui qui est utilisé en

standard pour les transactions sécurisées sur Internet

L'inconvénient néanmoins de ce type de protocole est qu'il se limite au protocole https, ce qui n'est pas le seul besoin de connexion des entreprises.

6. Exemple d'infrastructure



Quelle est la différence entre VLAN et VPN ?

VLAN est un ensemble d'hôtes qui communiquent les uns avec les autres comme s'ils étaient connectés au même commutateur (comme s'ils se trouvaient dans le même domaine), même s'ils ne le sont pas, Les VLAN évitent aux ordinateurs de se trouver dans le même emplacement physique, mais dans le même domaine de diffusion, ce qui permet de grouper les hôtes de manière logique plutôt que leur emplacement physique. tandis que le VPN fournit une méthode sécurisée pour se connecter à un réseau privé via: un réseau public non sécurisé, tel qu'Internet depuis un emplacement distant. VPN permet de créer un sous-réseau plus petit en utilisant les hôtes d'un réseau plus vaste sous-jacent et un VLAN peut être considéré comme un sous-groupe de VPN. L'objectif principal du VPN est de fournir une méthode sécurisée pour se connecter à un réseau privé, à partir de sites distants..