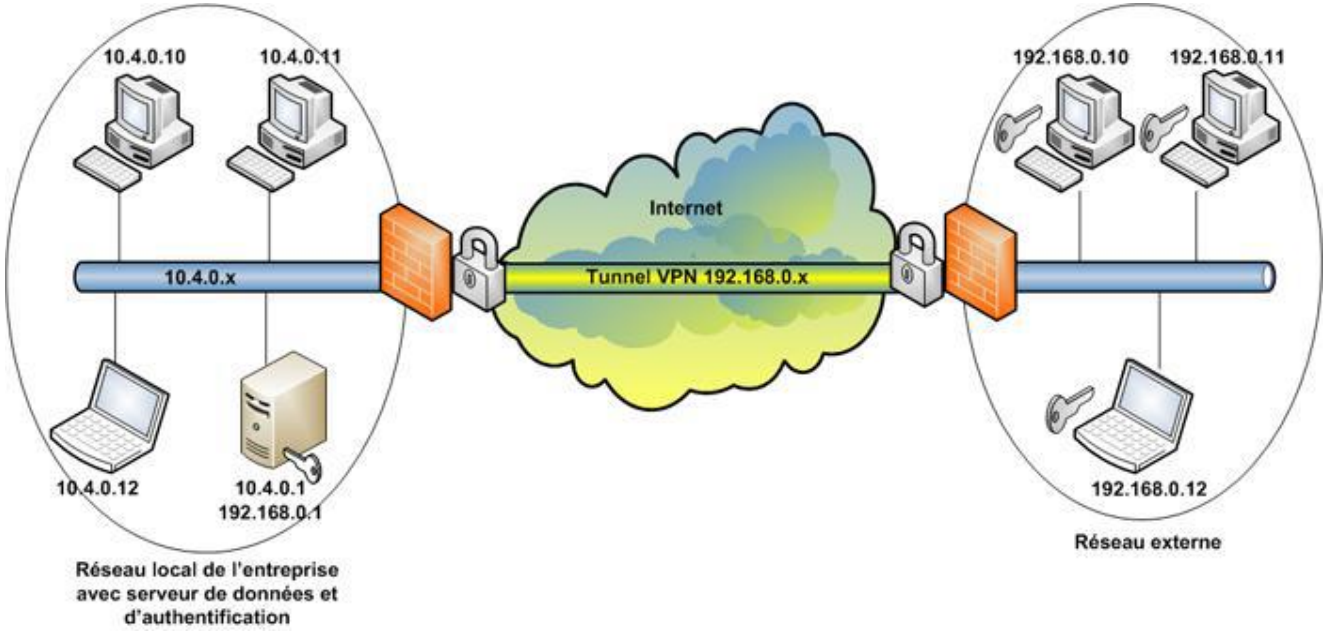
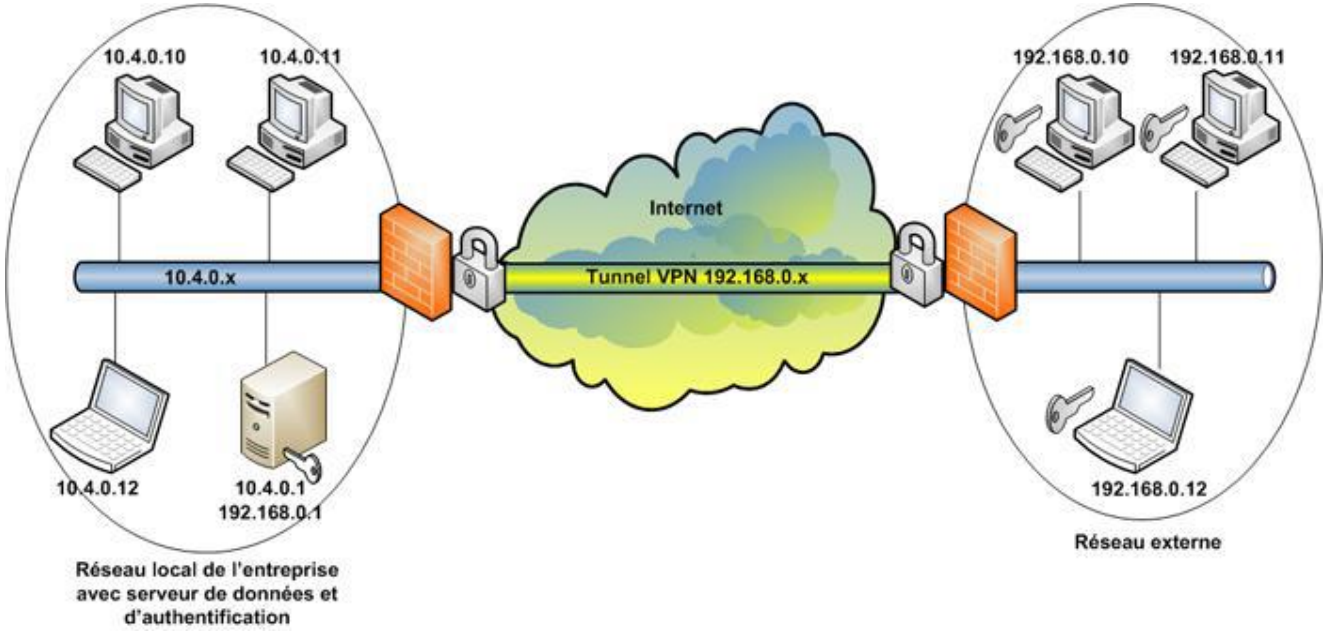
Virtual Private Network

- *Définition :*
- Le VPN (Virtual Private Network ou Réseau Privé Virtuel en français) est une technologie qui permet à un ordinateur distant d'accéder directement à un autre ordinateur en toute sécurité et cela en cryptant et décryptant les données qui transitent entre les différents ordinateurs/réseaux.



Virtual Private Network

- Il permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP différente et une localisation différente de celle de l'ordinateur.



Virtual Private Network

- **Les personnes utilisent un VPN** pour garder leur activité en ligne privée et garantir l'accès à des sites et services qui sans cela pourraient être restreintes.
- **Les sociétés utilisent un VPN** pour connecter des employés éloignés comme s'ils utilisaient tous le même réseau local dans un bureau central, mais avec moins d'avantages pour les personnes qu'un VPN personnel.

- **Les Pré requis pour créer une liaison VPN :**
- Une connexion haut-débit
- Un routeur intégrant les fonctions VPN
- Un système d’exploitation

Virtual Private Network

- **Un VPN est un réseau privé qui utilise un réseau publique comme backbone:**
- **Seuls les utilisateurs ou les groupes qui sont enregistrés dans ce vpn peuvent y accéder.**
- **Les données transitent dans un tunnel après avoir été chiffrées.**
- **Tout se passe comme si la connexion se faisait en dehors de l'infrastructure d'accès partagé comme Internet.**

Virtual Private Network

Les contraintes d'un VPN

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

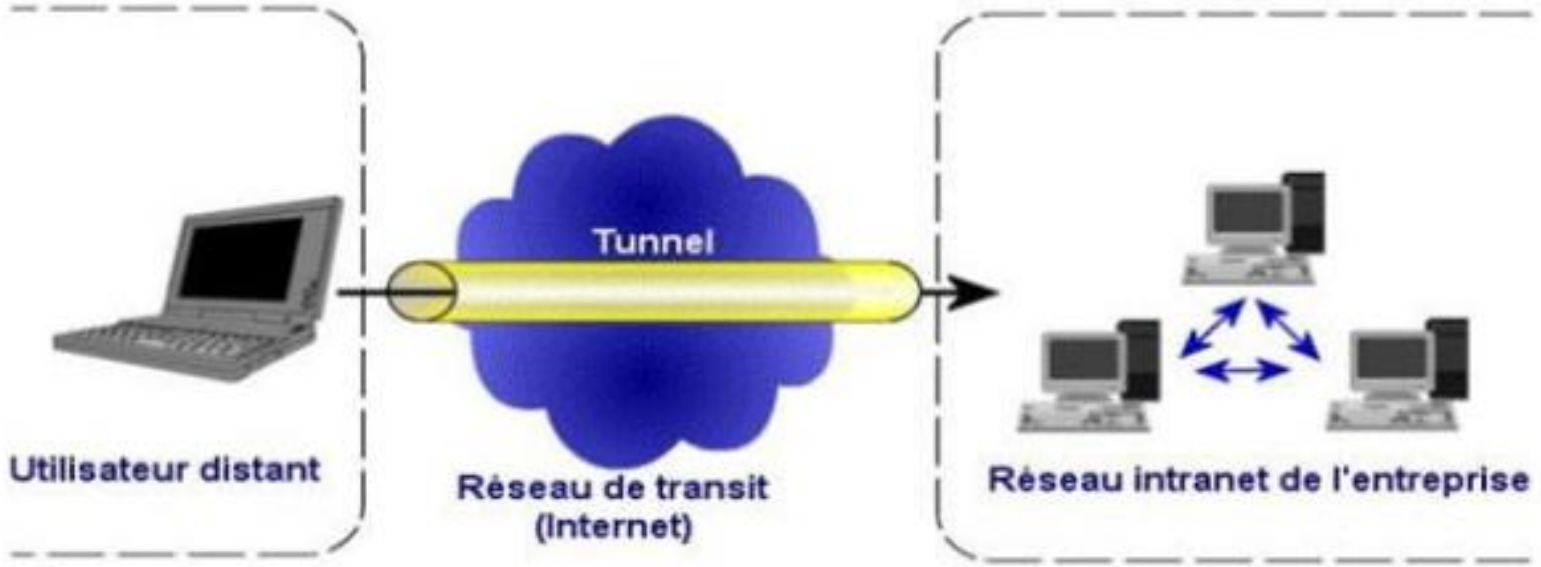
- Authentification d'utilisateur : seuls les utilisateurs autorisés doivent avoir accés au canal VPN.
- Cryptage des données : lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace.
- Gestion de clés : les clés de cryptage pour le client et le serveur 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 particulier IP.

Virtual Private Network

les différents types de VPN

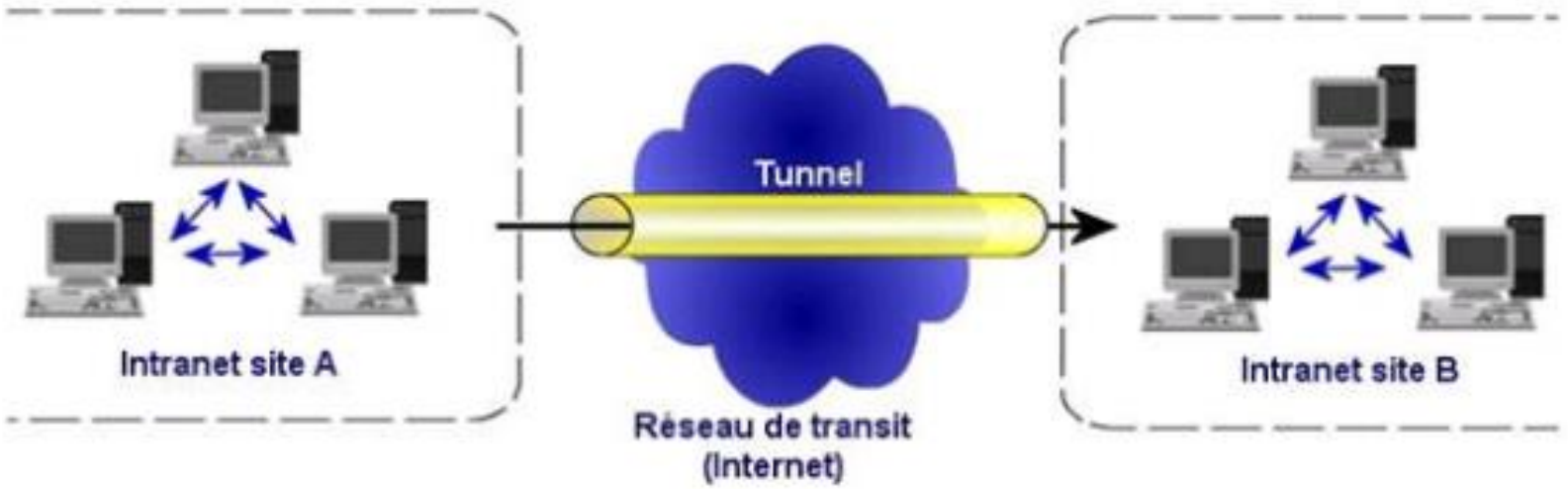
Suivant les besoins, on référence 3 types de VPN :

- 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.



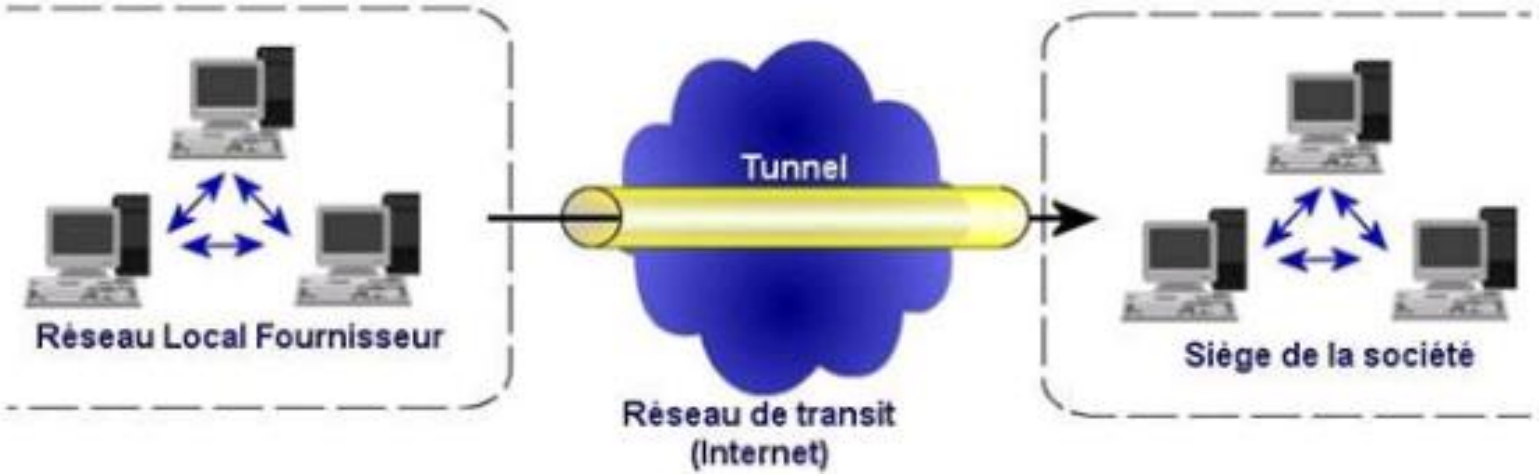
Virtual Private Network

- L'intranet VPN : il est utilisé pour relier deux ou plusieurs intranets d'uen 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, exploitation de serveurs distants …



Virtual Private Network

- 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 accés. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.



Virtual Private Network

Le tunneling

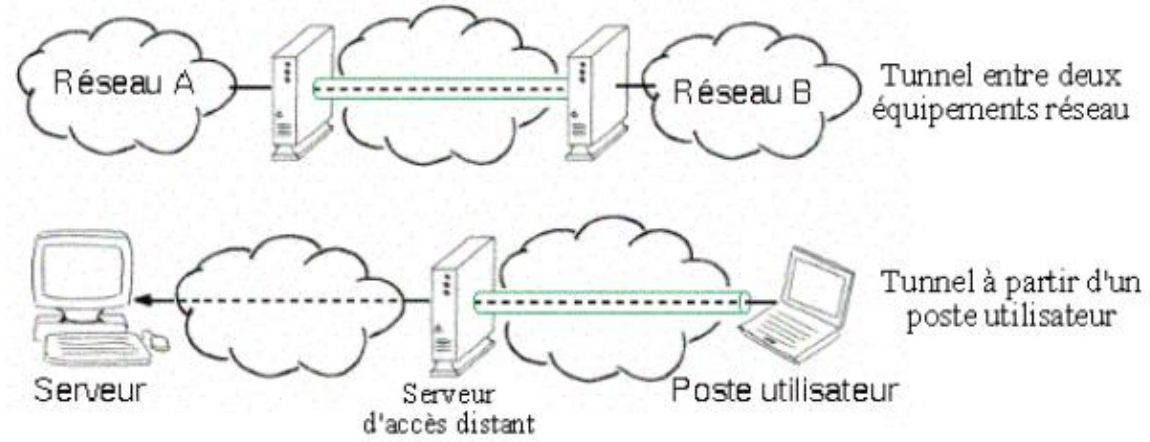
- Le VPN est basé sur la technique du tunnelling:
- Processus d'encapsulation, de transmission et de désencapsulation.
- Consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire.
- La source chiffre les données et les achemine en empruntant ce chemin virtuel.
- Le protocole de tunneling encapsule les données en rajoutant une entête permettant le routage des trames dans le tunnel.

Virtual Private Network

Le tunneling

- Un tunnel sert à transporter des données d'un point A vers un point B, au sens où les données qui "entrent" dans le tunnel en A "ressortent" nécessairement en B.

- **Exemples :**



Virtual Private Network

Le tunneling

- Principe de fonctionnement:
- Le transport de données se fait par encapsulation : Extrémité du tunnel: Les données à transporter sont insérées dans un paquet de protocole de "tunnélisation", puis dans un paquet du protocole de transport de données.
- L'autre extrémité du tunnel: Les données sont extraites du protocole de "tunnélisation" et poursuivent leur chemin sous leur forme initiale.

Virtual Private Network

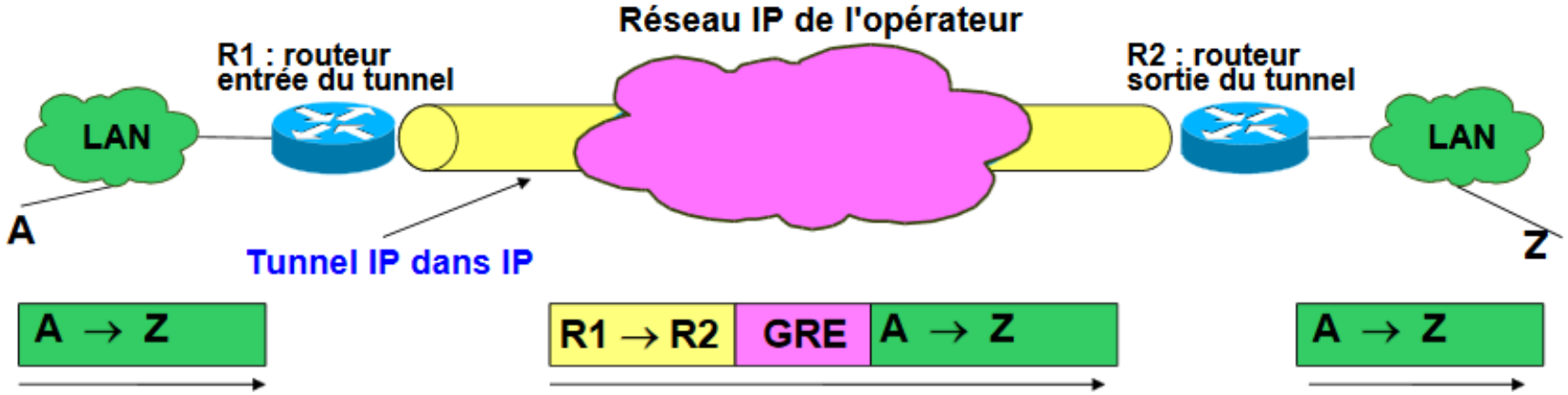
Le tunneling

- Le tunneling VPN comprend un double processus d'encapsulation des données et de cryptage des données.
- **Encapsulation des données :** L'encapsulation est le processus d'emballage d'un paquet de données Internet à l'intérieur d'un autre paquet.
- **Cryptage des données:** Sécuriser les données pour qu'elles ne soient accessibles qu'à leur destinataire.
- Plusieurs protocoles de cryptage ont été créés spécifiquement pour une utilisation avec des tunnels VPN. Les types les plus courants de protocoles de cryptage VPN incluent IPSec, PPTP, L2TP, OpenVPN, IKEv2, SSTP et OpenVPN.

Virtual Private Network

Le tunneling

- Principe de fonctionnement:
- Un tunnel est créé entre R1 et R2 :
  - Configuré dans les routeurs d'entrée et de sortie
- Le paquet ip privé (avec adresses IP privées) est encapsulé dans un paquet IP public:
  - Les adresses de R1 et R2 sont des adresses publiques
- Tunnel IP dans IP :
  - Le protocole GRE (Generic Routing Encapsulation) par exemple, permet d'encapsuler les paquets IP dans IP
  - L'entête GRE permet d'annoncer le type de paquet encapsulé (IPv4)



Virtual Private Network

Le tunneling

- Différents protocoles:
  - **Passenger Protocol** – Les données originales (IP...) à transmettre.
  - **Encapsulating Protocol** – Le protocole (GRE, IPSec, PPTP, L2TP) utilisé pour encapsuler les données originales.
  - **Carrier Protocol** – Le protocole employé par le réseau pour transporter les données. Le paquet d'origine (protocole Passager) est encapsulé dans le protocole d'encapsulation, qui est ensuite placé dans l'en-tête du protocole transporteur (généralement IP) pour la transmission sur le réseau public.

  - Le protocole d'encapsulation peut assurer également le chiffrement des données.

Virtual Private Network

- Catégories de protocoles
- Classement par Niveau OSI:
- Il existe deux catégories de protocoles VPN :

- Les protocoles nécessitant parfois/souvent du matériel particulier :
  - Les protocoles de niveau 2 (Couche Liaison) dans la pile TCP/IP : PPTP, L2F et L2TP,
  - Les protocoles de niveau 3 (Couche Réseau) dans la pile TCP/IP : IPSec
- Les protocoles ne nécessitant qu'une couche logicielle :
  - Les protocoles de niveau 4 (Couche Transport) : Lightway, OpenVPN

Virtual Private Network

- Classement par Système d'exploitation

Voici les protocoles classés par OS :

- Disponibles nativement sous Windows
  - PPTP et IPSec/L2TP
- Protocoles disponibles sous Linux et Windows par logiciel annexe :
  - OpenVPN
- Disponibles sous Linux
    - Tous

Virtual Private Network

Le tunneling

- **SÉCURITÉ DES PROTOCOLES INTERNET (Ipsec)**
- IPsec est une suite de protocoles de sécurité utilisés pour authentifier et chiffrer les données sur les réseaux VPN. Il comprend des normes pour établir un lien mutuel entre deux ordinateurs et l'échange de clés cryptographiques.
- Il permet de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

- Les clés chiffrent les données, de sorte que seuls les ordinateurs impliqués dans l'échange peuvent déverrouiller et afficher les données.

- IPSec est utilisé comme une solution complète de protocole VPN à lui seul, ou comme un protocole de cryptage au sein de PPTP, L2TP, et IKEv2.

Virtual Private Network

Le tunneling

- **SÉCURITÉ DES PROTOCOLES INTERNET (Ipsec)**
- Il existe deux modes pour IPSec :

1- le mode transport permet de protéger principalement les protocoles de niveaux supérieurs :

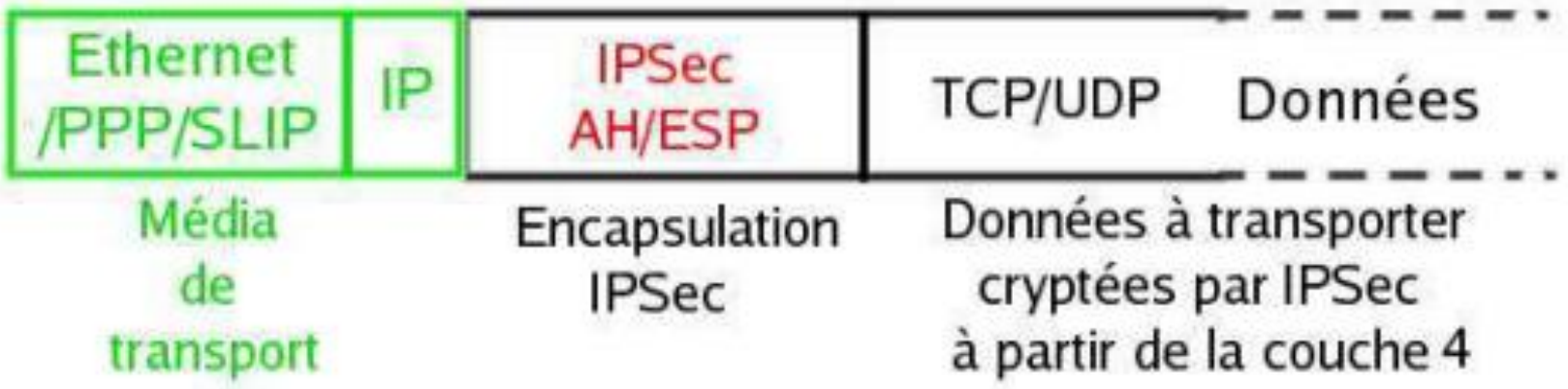
- IPSec récupère les données venant de la couche 4 (TCP/transport), les signe et les crypte puis les envoie à la couche 3 (IP/réseau). Cela permet d'être transparent entre la couche TCP et la couche IP et du coup d'être relativement facile à mettre en place.
- Il y a cependant plusieurs inconvénients :
  - l'entête IP est produite par la couche IP et donc IPSec ne peut pas la contrôler dans ce cas.
  - Il ne peut donc pas masquer les adresses

Virtual Private Network

Le tunneling

- **SÉCURITÉ DES PROTOCOLES INTERNET (Ipsec)**

● le mode transport permet de protéger principalement les protocoles de niveaux supérieurs :



Virtual Private Network

Le tunneling

- **SÉCURITÉ DES PROTOCOLES INTERNET (Ipsec)**

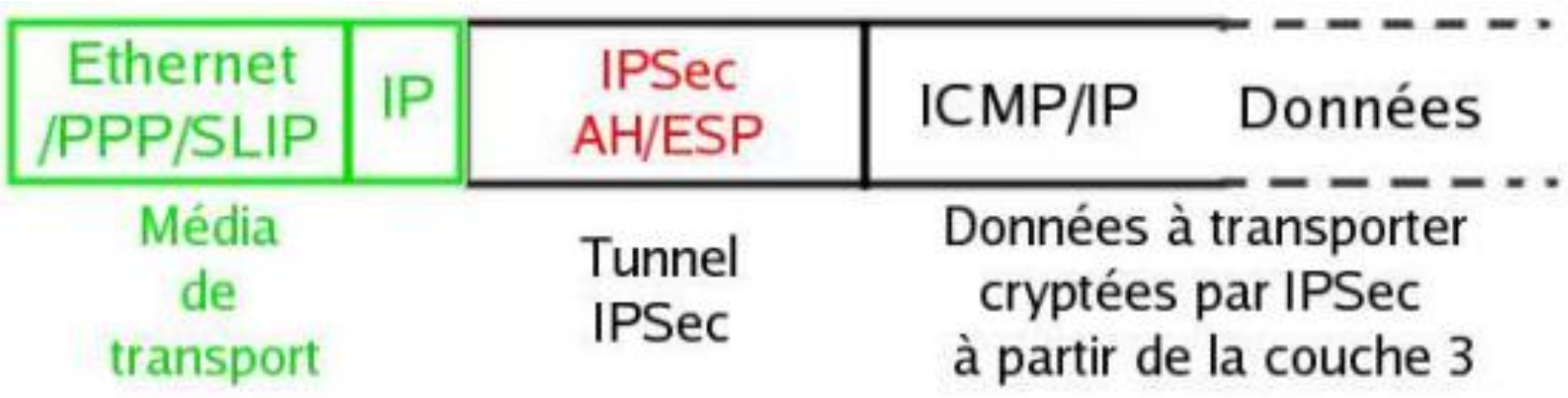
2-Le mode tunnel permet d'encapsuler des datagrammes IP dans des datagrammes IP

- les paquets descendent dans la pile jusqu'à la couche IP et c'est la couche IP qui passe ses données à la couche IPSec. Il y a donc une entête IP encapsulée dans les données IPSec et une entête IP réelle pour le transport sur Internet
- Cela a beaucoup d'avantages :
  - l'entête IP réelle est produite par la couche IPSec. Cela permet d'encapsuler une entête IP avec des adresses relatives au réseau virtuel et en plus de les crypter de façon à être sûr qu'elles ne sont pas modifiées.
  - On a donc des adresses IP virtuelles donc tirant partie au mieux du concept de VPN
  - On a le contrôle total sur l'entête IP produite par IPSec pour encapsuler ses données et son entête IPSec.

Virtual Private Network

Le tunneling

- **SÉCURITÉ DES PROTOCOLES INTERNET (Ipsec)**
- le mode tunnel permet d'encapsuler des datagrammes IP dans des datagrammes IP



Virtual Private Network

Le tunneling

- Les composantes d'IPSec:
- Le protocole IPSec est basé sur cinq modules :

1- IP Authentification Header (AH) gère:

• l'intégrité : on s'assure que les champs invariants pendant la transmission, dans l'entête IP qui précède l'entête AH et les données

• l'authentification pour s'assurer que l'émetteur est bien celui qu'il dit être

• il ne gère pas la confidentialité : les données sont signées mais pas cryptées

Le tunneling

2- Encapsulating Security Payload (ESP)

- **en mode transport**, il assure:

• confidentialité : les données du datagramme IP encapsulé sont cryptées

• authentification : on s'assure que les paquets viennent bien de l'hôte avec lequel on communique (qui doit connaître la clé associée à la communication ESP pour s'authentifier)

• l'intégrité des données transmises

- **en mode tunnel**, c'est l'ensemble du datagramme IP encapsulé dans ESP qui est crypté et subit les vérifications suivantes. On peut donc se passer de AH.

Le tunneling

3- Security Assocation (SA): définit l'échange des clés et des paramètres de sécurité. Il existe une SA par sens de communication. Les paramètres de sécurité sont les suivants :

- protocole AH et/ou ESP
- mode tunnel ou transport
- les algorithmes de sécurité utilisés pour encrypter, vérifier l'intégrité
- les clés utilisées

Le tunneling

4- La SAD (Security Association Database) stocke les SA afin de savoir comment traiter les paquets arrivant ou partant. Elles sont identifiées par des triplets :

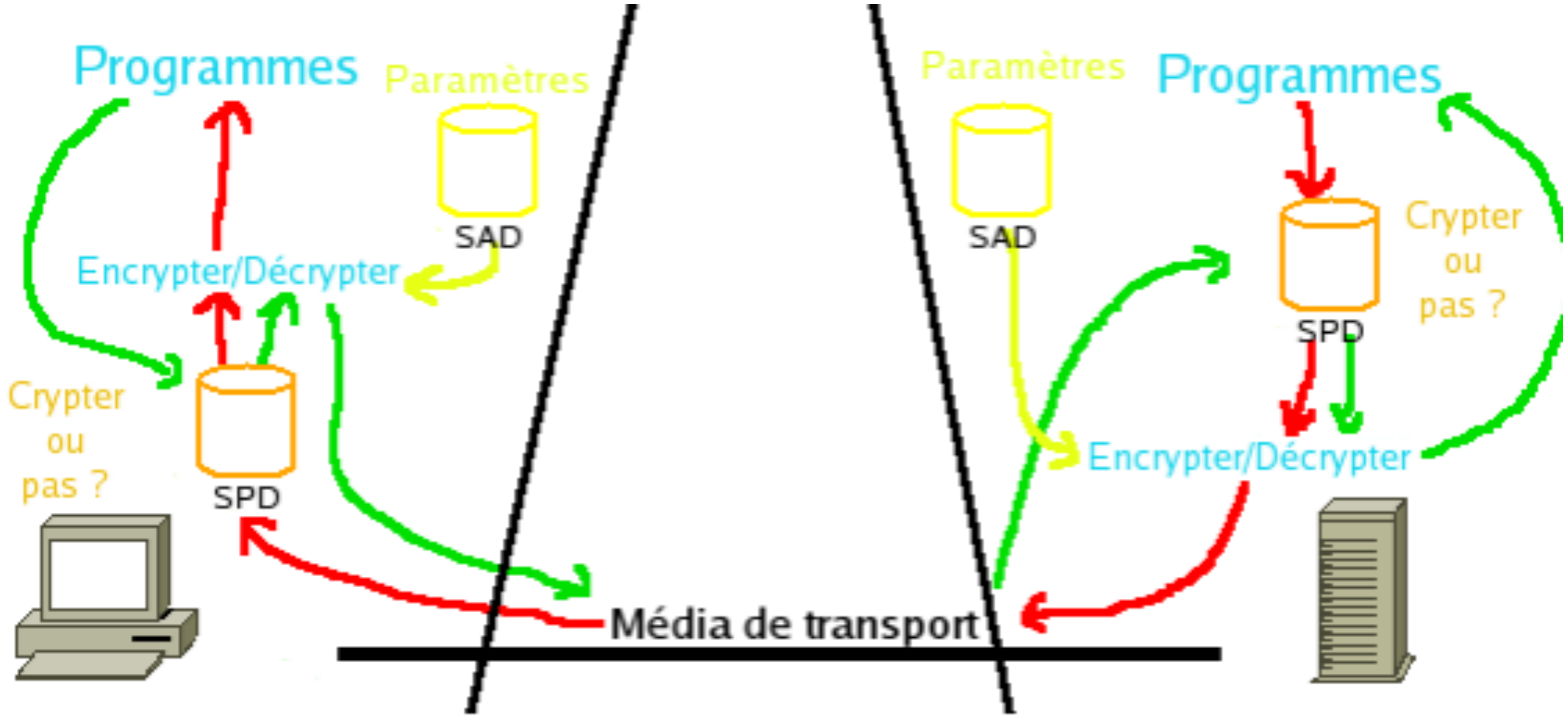
- adresse de destination des paquets
- identifiant du protocole AH ou ESP utilisé
- un index des paramètres de sécurité (Security Parameter Index) qui est un champ de 32bits envoyé en clair dans les paquets.

5- La SPD (Security Policy Database) est la base de configuration de IPSec. Elle permet de dire au noyau quels paquets il doit traiter. C'est à sa charge de savoir avec quel SA il fait le traitement.

Virtual Private Network

Le tunneling

- En résumé, le SPD indique quels paquets il faut traiter et le SAD indique comment il faut traiter un paquet sélectionné.



Virtual Private Network

Le tunneling

- L'échanges des clés nécessaires au cryptage des données dans IPSec peut se faire de façons différentes :

● à la main : pas très pratique

● IKE (Internet Key Exchange) : c'est un protocole développé pour IPSec. ISAKMP (Internet Security Association and Key Management Protocol) en est la base et a pour rôle la création (négociation et mise en place), la modification et la suppression des SA. Elle se compose de deux phases :

- la première permet de créer un canal sécurisé (par Diffie-Hellman) et authentifié à travers duquel on échange un secret pour dériver les clés utilisées dans la phase 2.
- la seconde permet de mettre en place IPSec avec ses paramètres et une SA par sens de communication. Les données échangées sont protégées par le canal mis en place dans la phase 1. A l'issue de ces deux phases, le canal IPSec est mis en place.

Virtual Private Network

Le tunneling

- **PROTOCOLE DE TUNNELAGE POINT À POINT**

- Le protocole PPTP a été développé par Microsoft et a été une norme depuis la fin des années 90. Il s'appuie sur un canal de contrôle TCP et l'encapsulation de routage générique pour fonctionner.

- Cela dit, PPTP n'est plus considéré comme sûr. PPTP a été remplacé par des protocoles plus sûrs, et est considéré comme obsolète aujourd'hui.

Virtual Private Network

Le tunneling

- **PROTOCOLE DE TUNNELAGE POINT À POINT**

- Il permet les opérations suivantes :

● L'authentification se fait par le protocole MS-CHAP (Challenge Handshake Authentification Protocol) version 2 ou avec le protocole PAP (Password Authentification Protocol)

● L'encryption se fait par le procotole MPPE (Microsoft Point-to-Point Encryption). Cela crée un tunnel de niveau 3 (Réseau) géré par le protocole GRE (Generic Routing Encapsulation).

● La compression peut se faire avec le protocole MPPC (Microsoft Point to Point Compression).

Virtual Private Network

Le tunneling

- **PROTOCOLE DE TUNNELAGE POINT À POINT**

- La connexion se passe donc ainsi :

● Le client se connecte à Internet par son modem par le protocole PPP (classiquement)

● Le client se connecte alors au serveur VPN par une connexion IP encapsulant les paquets GRE/PPP cryptés. Ainsi cela forme deux connexions l'une sur l'autre

  ○ la connexion normale à Internet : elle achemine le traffic vers/depuis Internet

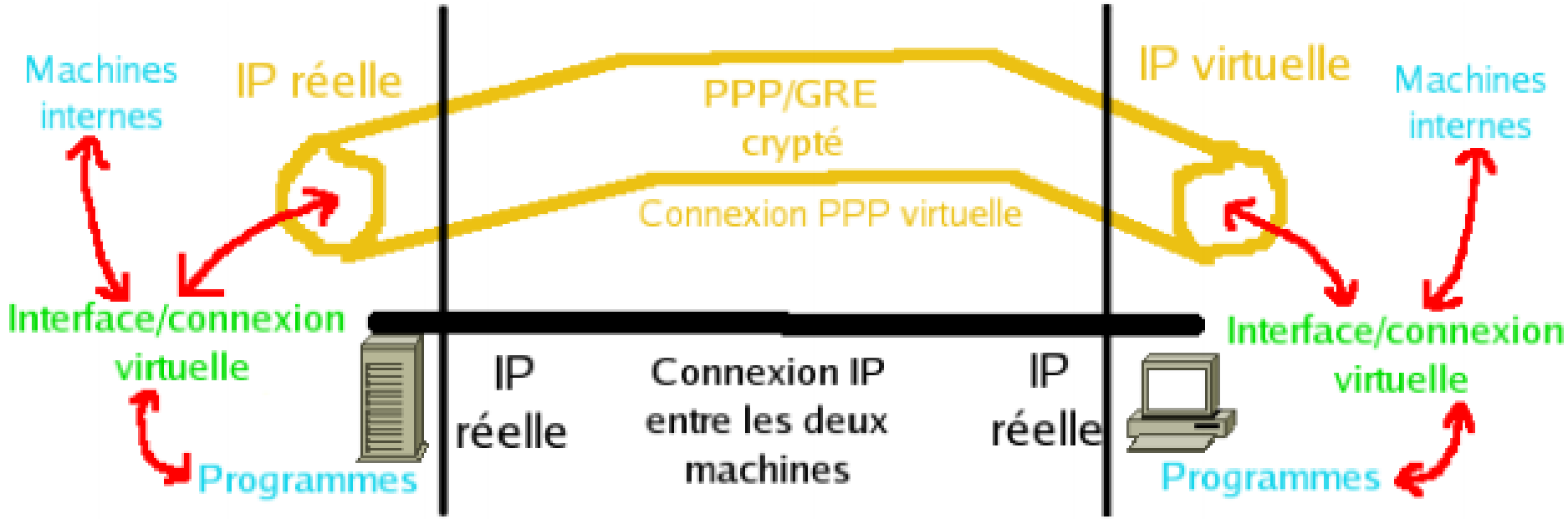
  ○ la connexion virtuelle au dessus de la connexion Internet : elle achemine le traffic vers/depuis le réseaux VPN

● A la fin de la connexion c'est le serveur qui ferme le tunnel

Virtual Private Network

Le tunneling

- **PROTOCOLE DE TUNNELAGE POINT À POINT**

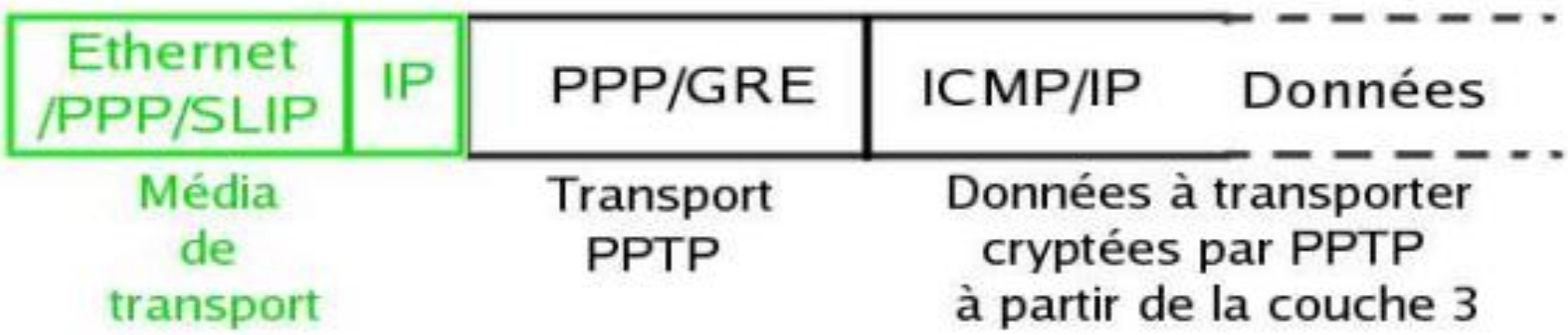


Virtual Private Network

Le tunneling

- **PROTOCOLE DE TUNNELAGE POINT À POINT**

- Un paquet d'une connexion PPTP ressemble donc à ceci :



Virtual Private Network

Le tunneling

- **PROTOCOLE DE TUNNELAGE DE LA COUCHE DEUX**

- L2TP appartient à Cisco et est considéré comme une meilleure version de PPTP. En tant que protocole de tunneling seulement, il ne fournit aucun cryptage. C’est pourquoi il est souvent associé à IPSec.

- La combinaison de ces deux protocoles est souvent appelée L2TP/IPsec, un protocole qui prend en charge jusqu’à 256 bits de cryptage et l’algorithme 3DES.

Virtual Private Network

Le tunneling

- **INTERNET KEY EXCHANGE VERSION 2**

- L'IKEv2 est un protocole d'association de sécurité développé par Microsoft et Cisco utilisé pour mettre en place une association authentifiée et cryptée entre deux ordinateurs.

- IKEv2 est souvent jumelé avec la suite de sécurité IPsec et est appelé IKEv2/IPsec. Ensemble, il fournissent jusqu'à 256 bits de cryptage et des clés cryptographiques robustes.

Virtual Private Network

Le tunneling

- **PROTOCOLE DE TUNNELAGE SÉCURISÉ DE SOCKET**
- SSTP est une norme de protocol appartenant à Microsoft qui fonctionne avec Windows, Linux et MacOS.
- Toutefois, il est principalement utilisé avec les plates-formes Windows. Il est considéré comme un protocole VPN stable et hautement sécurisé qui utilise la norme Secure Socket Layer 3.0.

Virtual Private Network

Le tunneling

- **Openvpn**

- OpenVPN est un protocole open source pris en charge par tous les principaux systèmes d'exploitation utilisés aujourd'hui (Mac, Windows et Linux) ainsi qu'Android et iOS.

- Il prend également en charge des plates-formes moins connues, y compris OpenBSD, FreeBSD, NetBSD et Solaris. Il dispose d'un cryptage jusqu'à 256 bits à l'aide d'OpenSSL , une boîte à outils robuste, de qualité commerciale et complète pour la sécurité de la couche de transport.

Virtual Private Network

Le tunneling

- **Lightway**

- Lightway, un protocole VPN de nouvelle génération d'Express VPN qui offre une vitesse, une sécurité et une confidentialité optimales (depuis 2020).

- Lightway utilise wolfSSL, dont la bibliothèque de cryptographie bien établie a fait l'objet d'un examen approfondi par des tiers selon la norme FIPS 140-2.