Réseaux

Virtual Private Network

Sommaire

Généralités

Un VPN ou RPV (réseau privé virtuel) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure.

Il permet d'utiliser les infrastructures publiques (Internet).

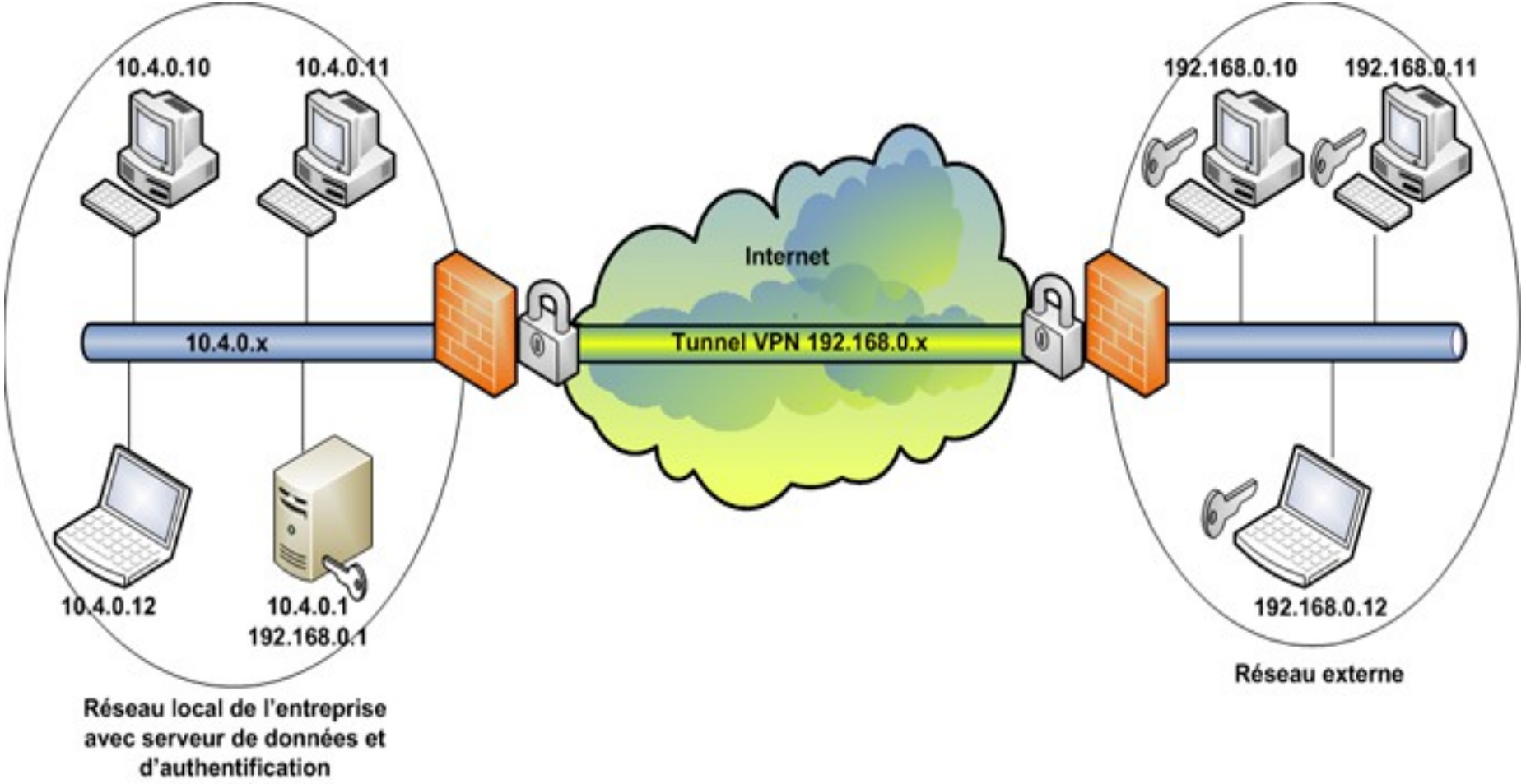
Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites de façon simple et économique.

Jusqu'à l'avènement des VPN, les sociétés devaient utiliser des liaisons Transpac, ou des lignes louées (LS).

Les VPN ont permis de démocratiser ce type de liaison.

Réseaux : Virtual Private Network

Généralités



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.

Les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le tunneling 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.

Pour assurer un accès aisé et peu coûteux aux intranets / extranets d'entreprise, les VPN d'accès simulent un réseau privé.

Ils utilisent en réalité une infrastructure d'accès partagé, 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 un en-tête.

Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Les principaux avantages d'un 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.

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 oeuvre les fonctionnalités suivantes :

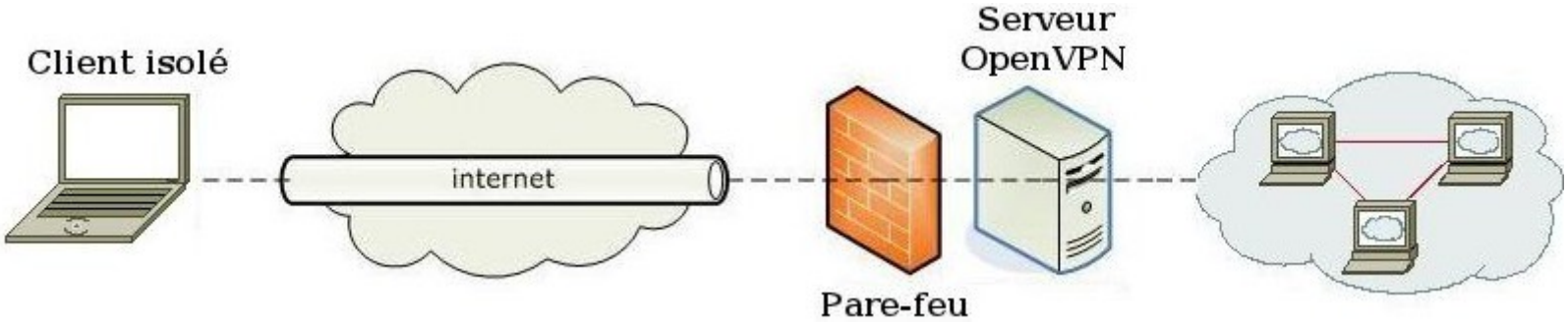
- Authentification d'utilisateur : seuls les utilisateurs autorisés doivent avoir accès au canal VPN;
- Cryptage des données : lors de leur transport sur Internet, les données doivent être protégées par un cryptage efficace;
- Gestion de clés : les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées (pertes, vols, licenciement);
- Prise en charge multi protocoles : la solution VPN doit supporter les protocoles les plus utilisés sur Internet (en particulier IP).

Les différents types de VPN

Suivant les besoins, on référence 3 types de VPN :

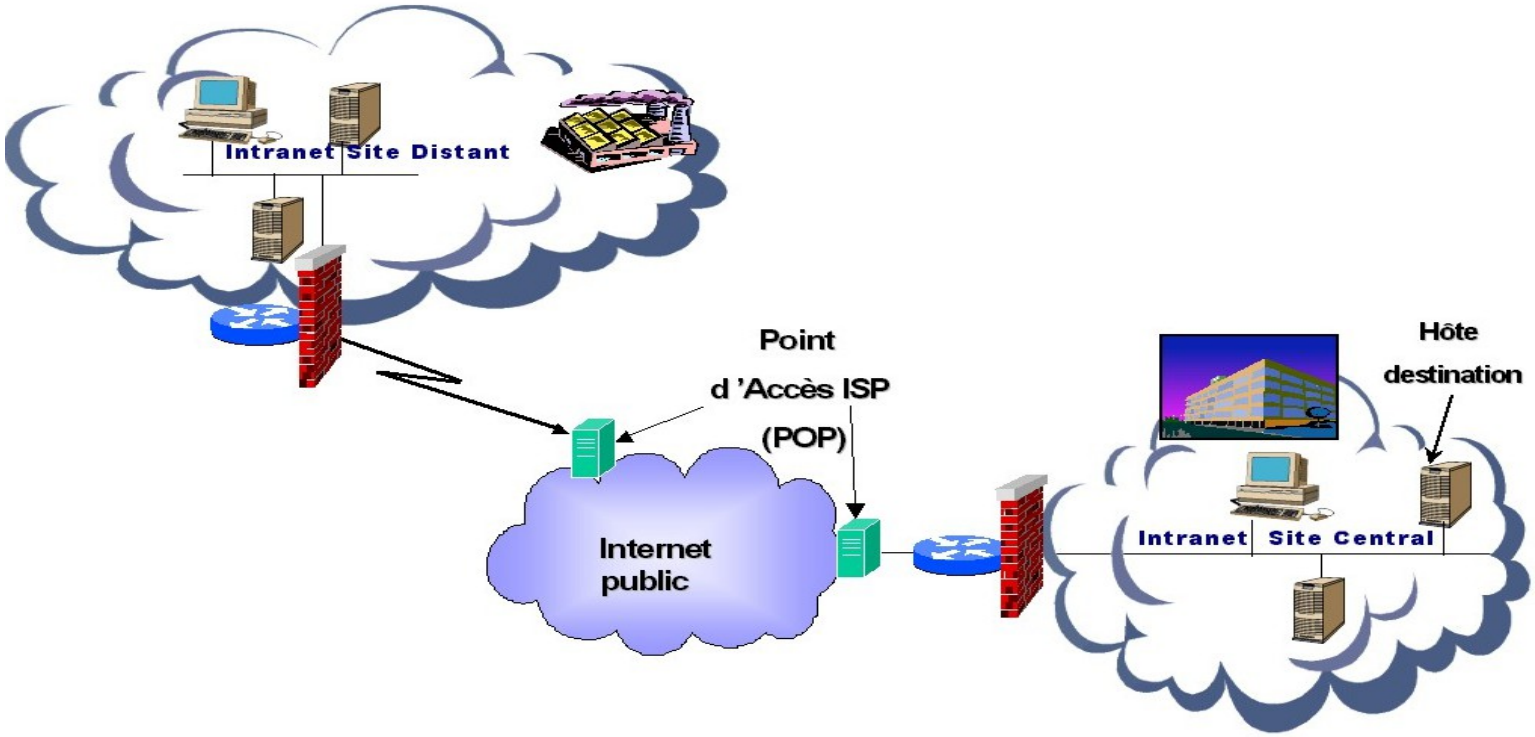
- Le VPN d'accès;
- L'intranet VPN;
- L'extranet VPN.

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 entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

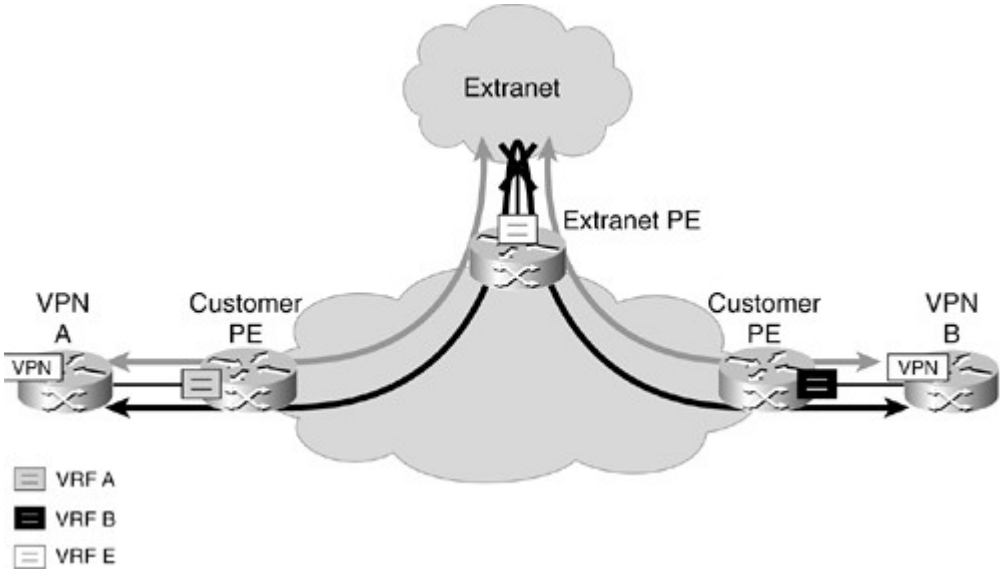
Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants …);



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 et il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès.

Souvent, seule une partie des ressources est partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.



Les protocoles utilisés

Les protocoles utilisés dans le cadre d'un VPN sont de 2 types, suivant le niveau OSI:

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

PPP (Point to Point Protocol)

PPP 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 liaison point à point.

PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau.

PPP n'est pas sécurisé mais sert de support aux protocoles PPTP ou L2TP.

PPTP (Point to Point Tunneling Protocol)

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

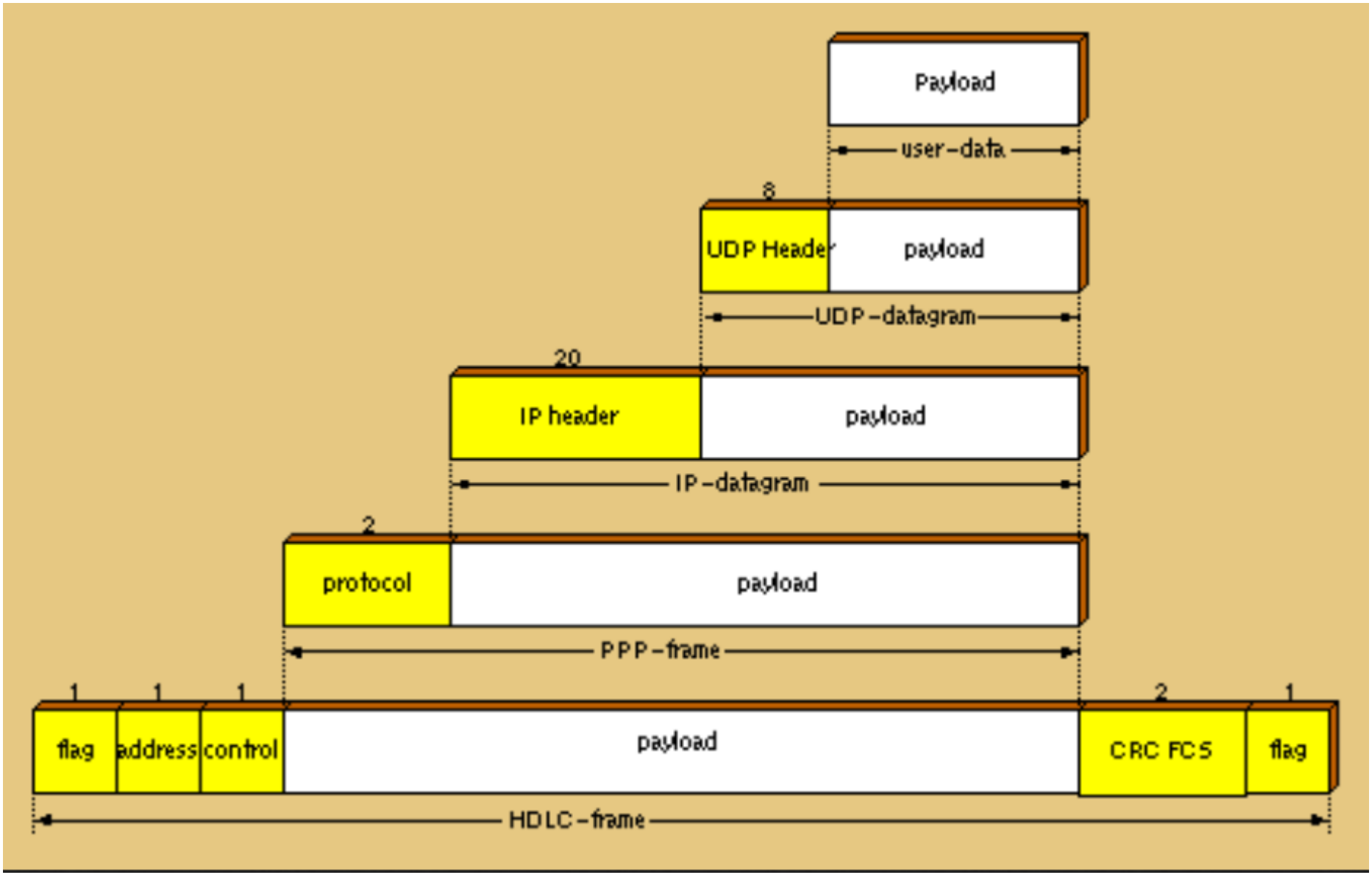
Le tunnel PPTP se caractérise par

- une initialisation du client ;
- une connexion de contrôle entre le client et le serveur ;
- la clôture du tunnel par le serveur.

Par la suite, une deuxième connexion est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP.

C'est cette deuxième connexion qui forme le tunnel PPTP.

Les protocoles utilisés



L2TP (Layer Two Tunneling Protocol)

L2TP, défini par la RFC2661, est issu de la convergence des protocoles PPTP et L2F (Layer Two Forwarding).

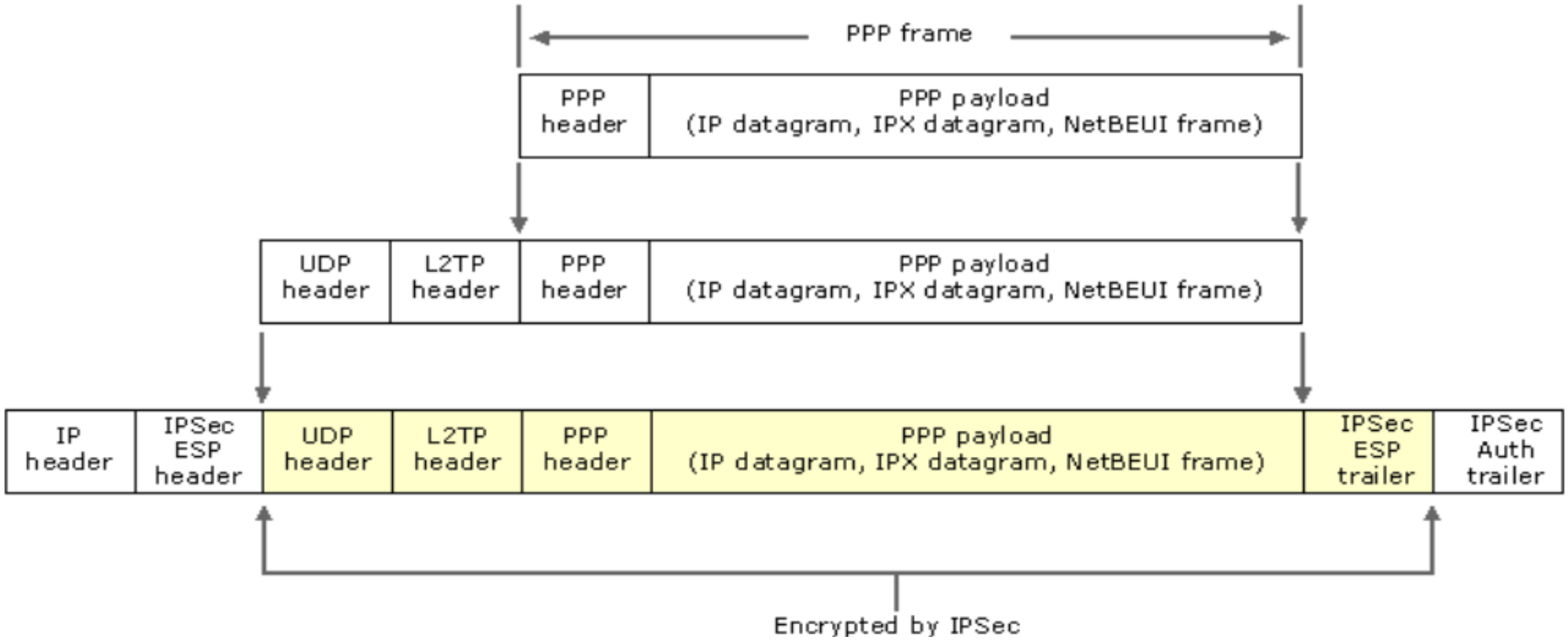
Il est actuellement développé et évalué conjointement par Cisco , Microsoft, 3Com ainsi que d'autres acteurs du marché des réseaux.

Il permet l'encapsulation des paquets PPP au niveau des couches 2 (Frame Relay et Atm) et 3 (Ip).

Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunneling sur Internet.

L2TP repose sur deux concepts : les concentrateurs d'accès L2TP (LAC) et les serveurs réseau L2TP (LNS).

L2TP n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'Ipsec et L2TP



IPSec

IPSec, défini par la RFC2401, 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 longue, il est 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:

- AH → Authentification Header
- ESP → Encapsulating Security Payload

Authentification Header

AH 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 mécanisme ne sont pas encodées.

Encapsulating Security Payload

ESP 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.

La gestion des clefs

Les protocoles sécurisés ont recours à des algorithmes de cryptage, et ont donc besoin de clefs.

Un des problèmes principaux 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 à savoir :

- ISAKMP (Internet Security Association and Key Management Protocol)
- IKE (Internet Key Exchange)

IPSec

IPSec peut fonctionner dans un mode transport hôte à hôte ou bien dans un mode tunnel réseau.

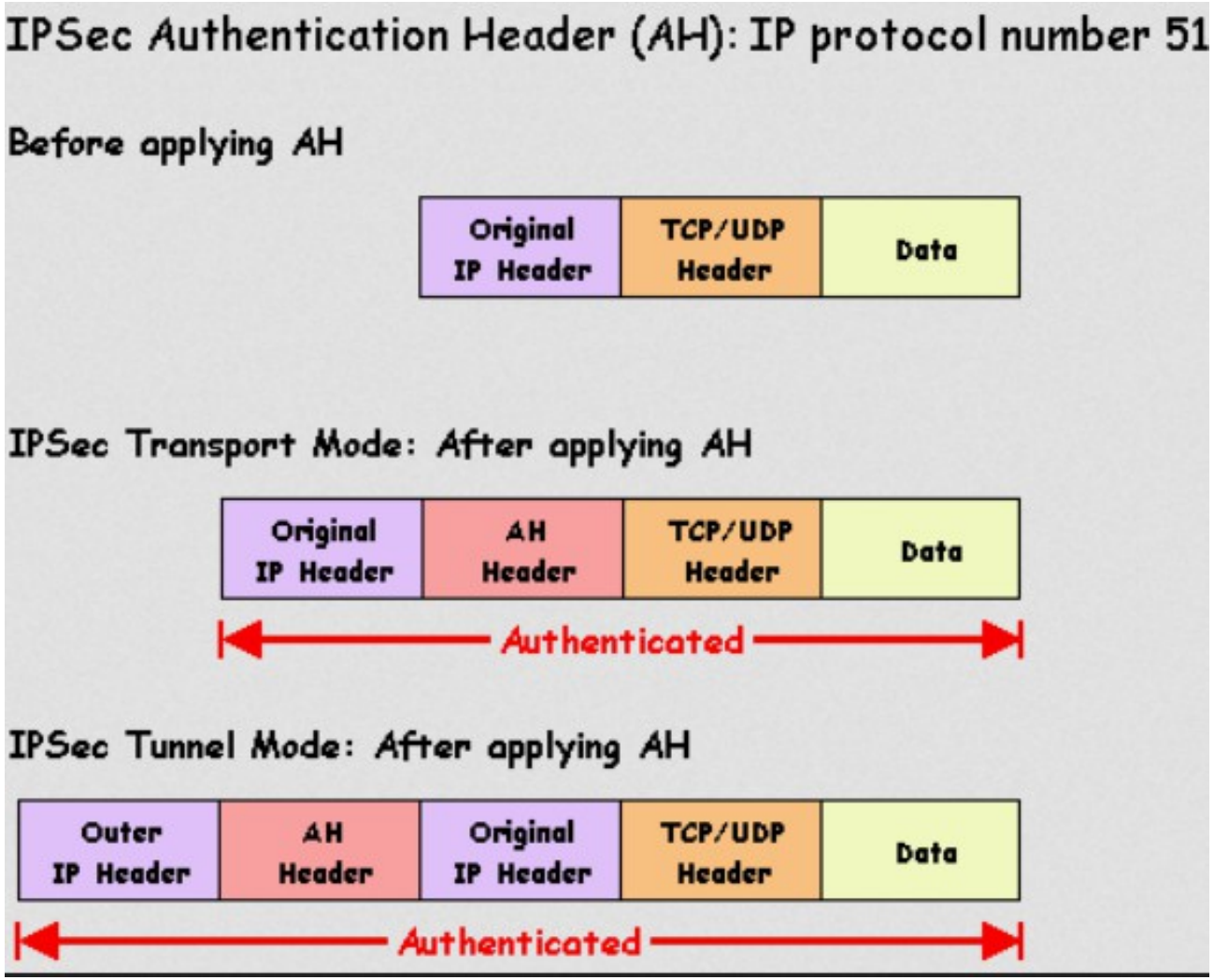
Mode transport

Dans le mode transport, ce sont uniquement les données transférées (le payload du paquet IP) qui sont chiffrées et/ou authentifiées.

Le reste du paquet IP est inchangé et de ce fait le routage des paquets n'est pas modifié.

Cependant, les adresses IP ne pouvant pas être modifiées sans corrompre le hash de l'en-tête AH généré par IPSec, pour traverser un NAT **il faut avoir recours à l'encapsulation NAT-T**.

Version sans NAT-T (NAT-Traversal)



Mode tunnel

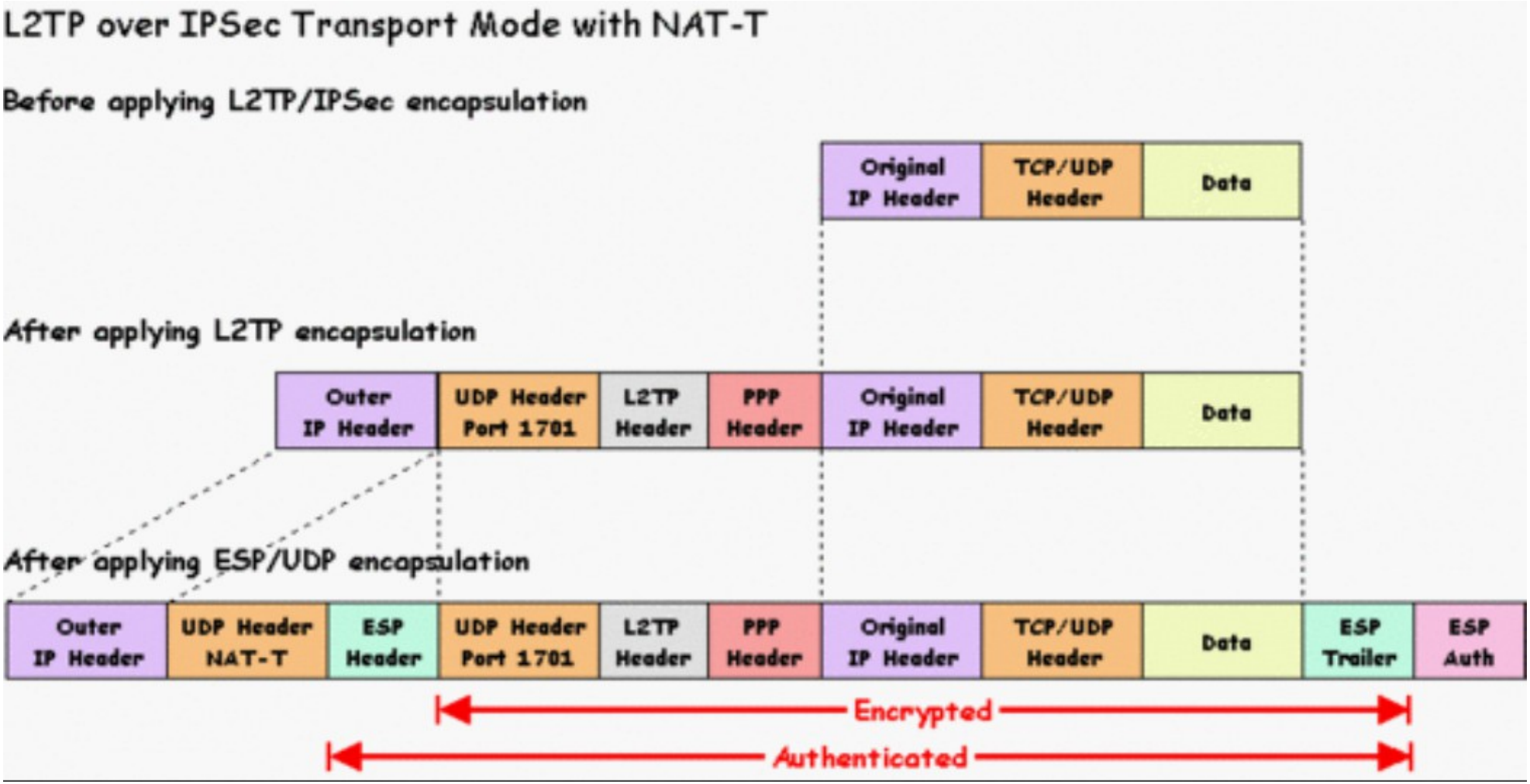
En mode tunnel, c'est la totalité du paquet IP qui est chiffré et/ou authentifié.

Le paquet est ensuite encapsulé dans un nouveau paquet IP avec une nouvelle en-tête IP.

Au contraire du mode transport, ce mode supporte donc bien la traversée de NAT.

Le mode tunnel est surtout utilisé pour créer des VPN permettant la communication de réseau à réseau (eg. entre deux sites distants).

Version avec NAT-T (NAT-Traversal)



SSL (Secure Socket Layer)

SSL (Secure Socket Layer) est un protocole de niveau 4 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 ;
- le chiffrement des données durant la connexion.

Les implémentations

Implémentations logicielles:

Racoon, s'intègre au noyau Linux et permet de gérer les authentifications suivantes:

- Mot de passe de groupe (tous les utilisateurs ont le même mdp)
- Login / password
- Certificats x509

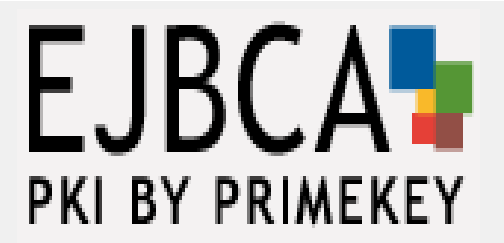
OpenVPN, s'intalle comme paquetage et permet de gérer les authentifications suivantes:

- Certificats SSL
- Login / password

Implémentations logicielles:

EJBCA (Enterprise Java Bean Certificates Authority), est certainement la PKI la plus aboutie (gratuite) et permet de gérer :

- La création de certificats;
- Le renouvellement ;
- Certificats x509 ;
- SCEP (Simple Certificates Enrollment Protocol)
- OCSP (Open Certificates Status Protocol)



Implémentations matèrielles:

Plusieurs marques proposent des passerelles VPN:

- Zyxel USG100

- Cisco ASA5505

- Sonicwall VPN2000

Distributions dédiées et gratuites :

- Monowall

- PfSense

- IpCop