Présentation des VPN

FABIEN COLMAGRO
MARGOT LORD
CLÉMENT NEGRE
JEAN PINEAU

Les VPN – 1

LES DIFFÉRENTS VPN

1.1 – Les VPN d’accès – Personnelle

Le type de VPN qui est le plus connu du public. Celui-ci est généralement utilisé pour accéder à internet sans subir les blocages qu’il peut y avoir sur le réseau d’un pays. Considéré comme « sécurisé » par le grand public, celui-ci dépend exclusivement du fournisseur de VPN. Accéder à une donnée malgré un blocage DNS, ne signifie pas que le trafic est sécurisé. Lors que celui-ci est bien mis en place, il peut permettre à des personnes d’accéder à de l’information auquel ils n’auraient pas accès de façon officiel, comme en Chine pour des journalistes ou le réseau est sur haute surveillance. A l’inverse, ils permettent des téléchargements illégaux, qui ont été bloqué dans un pays, en passant par un serveur localisé dans un autre.

1.2 – Les VPN d’accès – Entreprise

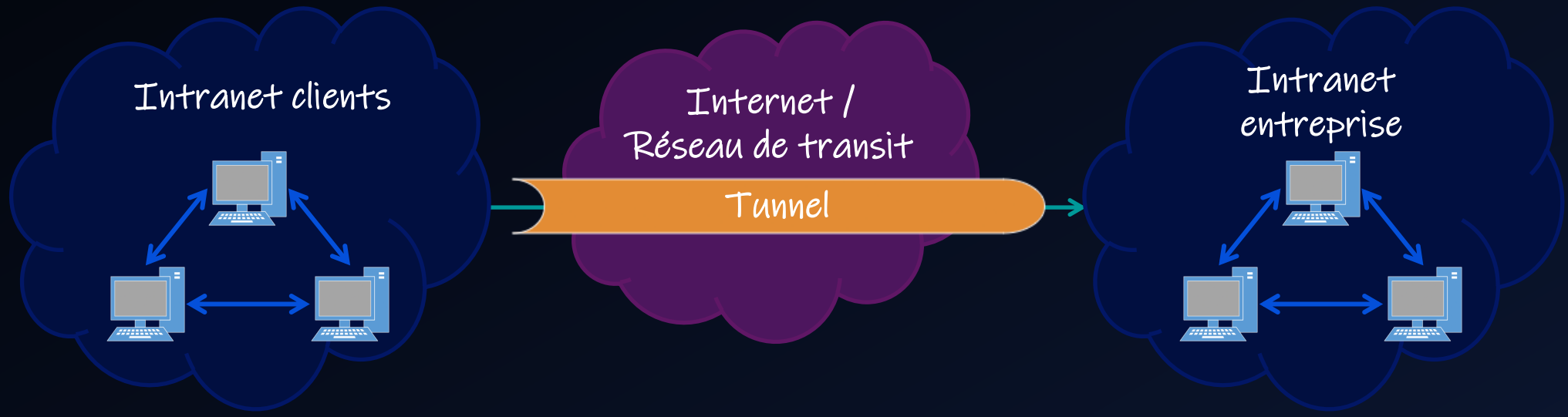
Le type le plus utilisé en télétravail, celui-ci permet de se connecter à l’entreprise depuis chez soi. Il a pour vocation d’accéder de façon sécurisée au réseau de l’entreprise. Il peut aussi permettre de profiter de la sécurité mise en place dans l’entreprise lorsqu’on va sur internet (pare-feu)

1.3 – Les VPN d’intranet – Site-to-Site

VPN rependu en entreprise, surtout lorsque celle-ci possède plusieurs sites physiques. Il permet d'interconnecter plusieurs sites, entre eux. Les VPN de ce type construisent un réseau virtuel qui unit des réseaux issus de localisations variées pour les connecter à Internet et maintenir des communications sécurisées et privées entre eux.

1.4 – Les VPN d’extranet

VPN très proche du précèdent, il a pour vocation de permettre aux entreprises clientes, d’accéder à certaine partie de notre Intranet. Ce type de VPN implique une authentification d’autant plus renforcée, étant donné que ceux qui l’utilise ne font pas parti de l’entreprise. De plus, un cloisonnement en interne et une gestion des espaces partagés est d’autant plus indispensable.

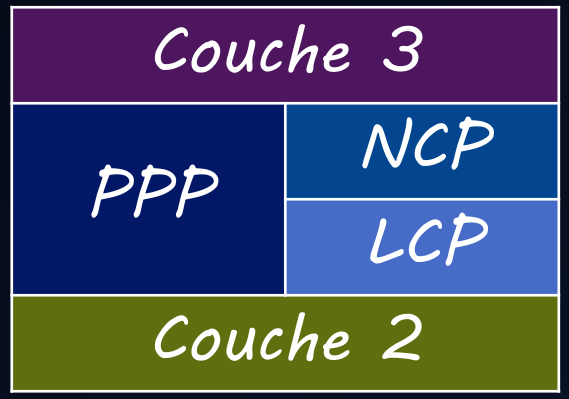


Les protocoles – 2

LES DIFFÉRENTS PROTOCOLES LIÉS AUX VPN

2.1 - PPP – Point to Point Protocole

> *« 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 liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau (NAS). Le protocole PPP est défini dans la Rfc 1661 appuyé de la Rfc 2153. »*
>
> source.pdf

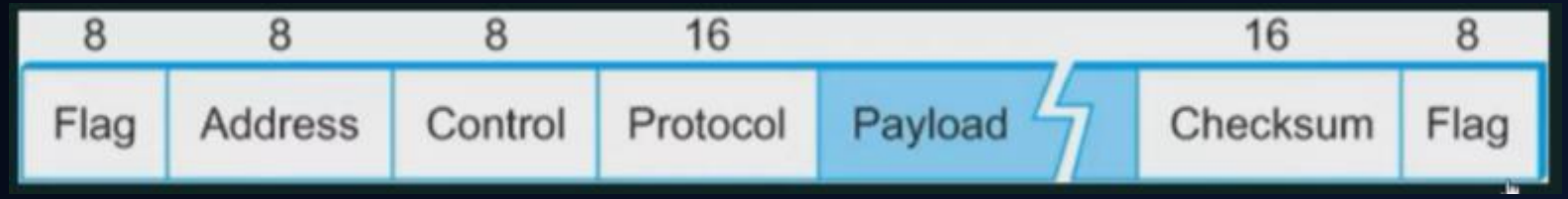


Trois composants :

- Encapsulation des datagrammes
- Contrôle de la liaison avec LCP (Link Control Protocol)
- Contrôle de la couche réseau avec NCP (Network Control Protocole)

Le protocole PPP permet une meilleure gestion des liaisons par rapport à HDLC car :

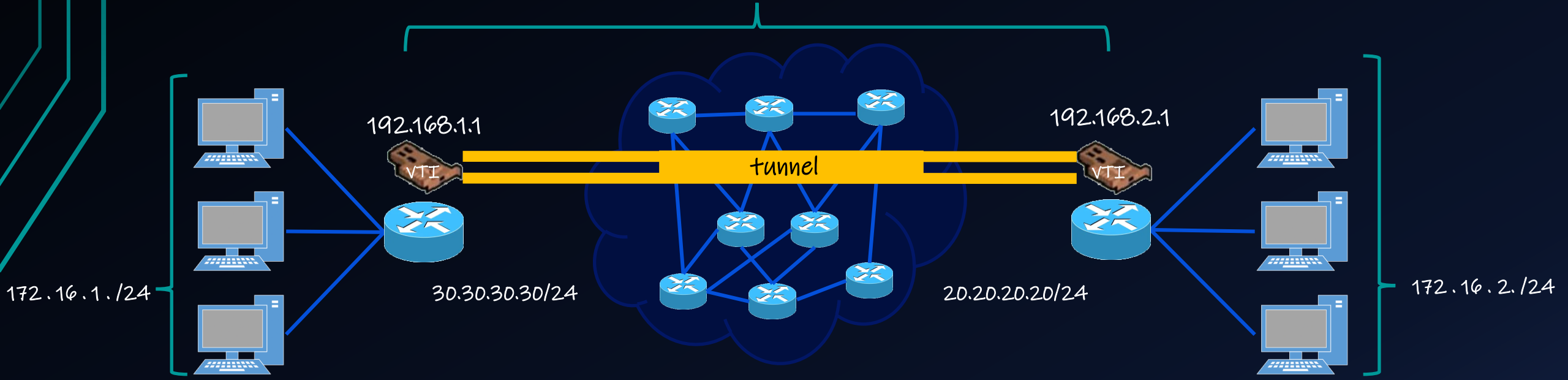
- Il **prend** en charge des mécanismes d'authentification, comme PAP ou CHAP.
- Il **permet** l'agrégation de lien (on parle de PPP Multi-link).
- Il **permet** la compression des données.



2.2 - GRE – Generic Routing Encapsulation

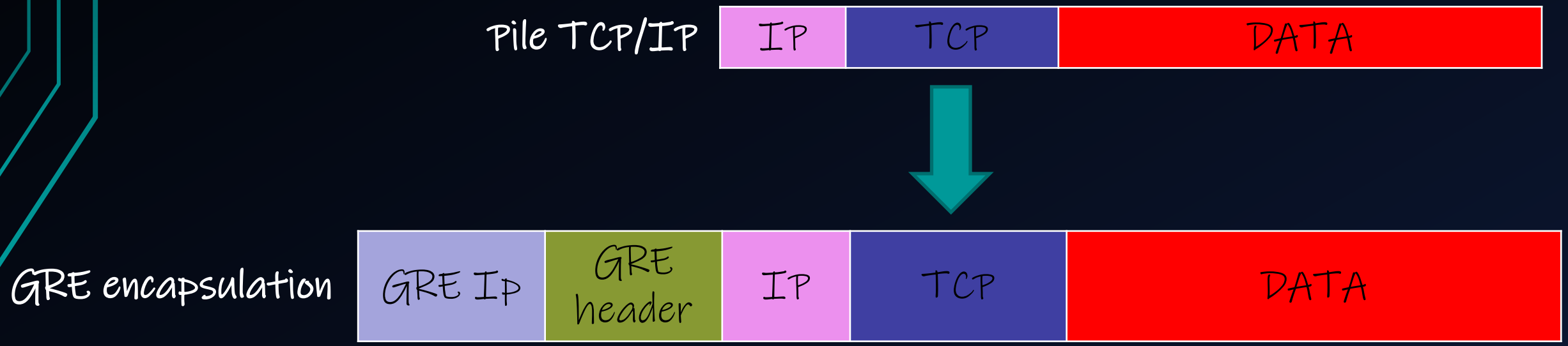
Generic Routing Encapsulation, est un protocole de mise en tunnel qui permet d'encapsuler n'importe quel paquet de la couche réseau. Il permet de connecter une partie du réseau à une autre partie du réseau.

Dans le schéma si dessous, le réseau 172.16.1/24 peut communiquer avec les machines en 172.16.2/24 comme si elles étaient dans le même sous réseau.



2.3 - GRE – Generic Routing Encapsulation

Generic Routing Encapsulation va ajouter au début de la couche 3 ses propres paquets.



GRE + PPP = PPTP

« PPTP, qui signifie Point-to-Point Protocol RFC 2637, est un prolongement de PPP (Point-to-Point Protocol). Il se base donc sur son système d'authentification et de chiffrage. Le client PPTP établit une connexion chiffrée, également appelé tunnel, avec le serveur PPTP. Plus précisément, le protocole encapsule les paquets de données avec PPP et les met dans une enveloppe IP, créant ainsi un tunnel pour qu'elles circulent sur un réseau IP. Dès lors, chaque fois qu'un routeur ou tout autre appareil rencontre ces données, il les traite comme un paquet IP. Une fois que les données sont reçues par le serveur PPTP, elles sont acheminées vers le Web ou le périphérique de destination. » https://www.monpetitforfait.com/vpn/aides/protocole-pptp

« Le principe du protocole PPTP est de créer des paquets sous le protocole Ppp et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 défini par le protocole. » source.pdf

Récapitulatif des avantages et inconvénients du protocole PPTP	
Avantages	**Inconvénients**
Un des protocoles VPN les plus rapides	Limite de cryptage de 128 bits qui ne garantit pas la sécurité des données
Très facile à configurer	Ne rend pas réellement anonyme en ligne
Compatible avec tous les appareils	Les pare-feu et les FAI peuvent facilement le bloquer
Une solution économique	Les agences gouvernementales réussissent à le cracker.

GRE + PPP = PPTP

PPTP présente l'avantage d'être complètement intégré dans les environnements Windows. Ceci signifie en particulier que l'accès au réseau local distant pourra se faire via le système d'authentification de Windows NT : RADIUS et sa gestion de droits et de groupe. Cependant la sécurité est le point faible du produit :

- Mauvaise gestion des mots de passe dans les environnements mixtes win 95/NT
- Faiblesses dans la génération des clés de session : réalisé à partir d'un hachage du mot de passe au lieu d'être entièrement générées au hasard. (facilite les attaques « force brute »)
- Faiblesses cryptographiques du protocole MsCHAP 1 corrigées dans la version 2 mais aucun contrôle sur cette version n'a été effectué par une entité indépendante.
- Identification des paquets non implémentée : vulnérabilité aux attaques de type « spoofing » source.pdf

L2F : Layer 2 Forwarding

L2F est un protocole aujourd'hui dépassé. Celui-ci n'est absolument pas sécurisé, car il ne propose aucun chiffrement ni aucune confidentialité.

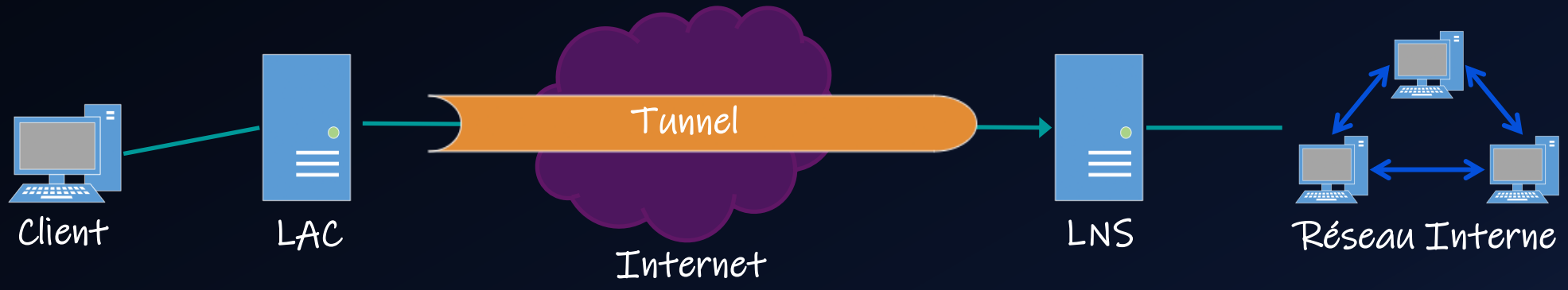
> *«Ce protocole VPN, maintenant **obsolète**, a été développé par Cisco Systems, Northern Telecom (Nortel) et Shiva. Il fut intégré dans Cisco IOS. Il servait à transporter des sessions PPP entre des NAS afin de les agréger sur un NAS principal lors de l'utilisation de PPP multi-lien (MLPPP).*
> *Il a été décrit dans la RFC 2341. Il est basé sur UDP et utilise le port 1701. »*
>
> https://fr.wikipedia.org/wiki/Layer_2_Forwarding

Nous ne le détaillerons pas d'avantage, car trop dépassé.

L2F + PPTP = L2TP

« L2TP, définit par la Rfc 2661, est issu de la convergence des protocoles PPTP et L2F. Il est actuellement développé et évalué conjointement par Cisco Systems, Microsoft, Ascend, 3Com ainsi que d'autres acteurs clés 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 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'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'Ipsec et L2tp.»

source.pdf



L2F + PPTP = L2TP

Lac : L2tp Access Concentrator

Les périphériques Lac fournissent un support physique aux connexions L2tp. Le trafic étant alors transféré sur les serveurs réseau L2tp. Ces serveurs peuvent s'intégrer à la structure d'un réseau commuté Rtc ou alors à un système d'extrémité PPP prenant en charge le protocole L2tp. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le Lac est l'émetteur des appels entrants et le destinataire des appels sortants.

Lns : L2tp Network Server

Les serveurs réseau L2tp ou Lns peuvent fonctionner sur toute plate-forme prenant en charge la terminaison Ppp. Le Lns gère le protocole L2tp côté serveur. Le protocole L2tp n'utilise qu'un seul support, sur lequel arrivent les canaux L2tp. C'est pourquoi, les serveurs réseau Lns, ne peuvent avoir qu'une seule interface de réseau local (Lan) ou étendu (Wan). Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface Ppp du concentrateur d'accès Lac. Le Lns est l'émetteur des appels sortants et le destinataire des appels entrants. C'est le Lns qui sera responsable de l'authentification du tunnel.

IPSEC

But visée par IPSEC ? La sécurité ! Les protocoles présentés précédemment n'est intègre pas / peu / pas assez. IPSEC est défini par la RFC 2401, c'est un protocole qui vise à sécuriser les échanges sur la couche réseau, aussi bien sur IPv4 que sur IPv6. Le besoin d'avoir un système multi plateforme étant dût au fait que même si IPv6 est inévitable, la migration depuis IPv4 est lente. Il fallait donc un protocole de sécurité commun. IPSEC est basé sur deux mécanismes :

Authentication Header (AH)

- Intégrité et authenticité des datagrammes IP
- Aucune confidentialité
- Données fournies et transmises pas encodées

Encapsulating Security Payload (ESP)

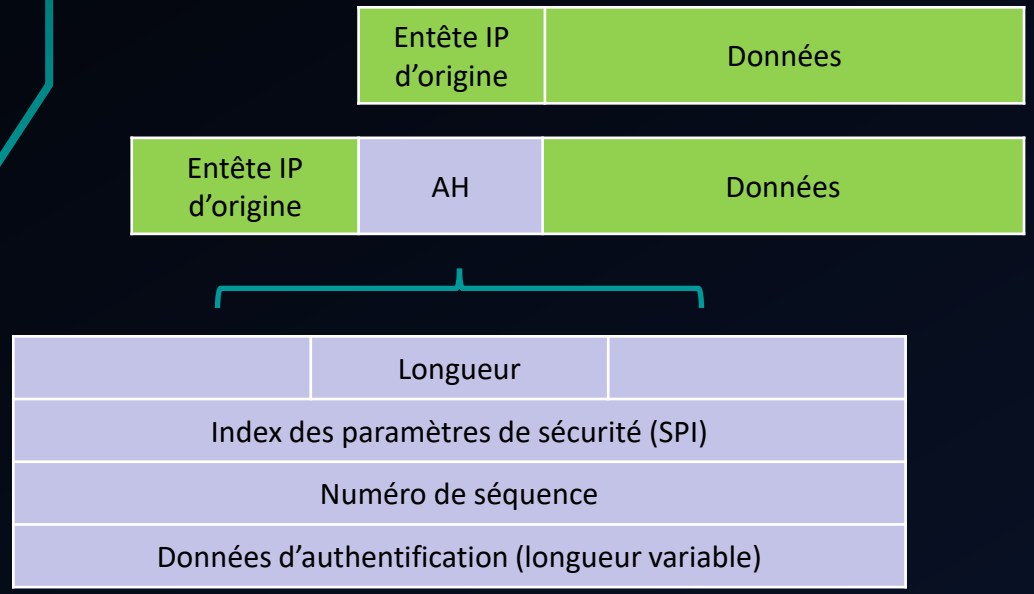
- Peut permettre l'authentification
- Utilisé principalement pour le chiffrement de l'information

Bien qu'indépendant, ces deux protocoles sont, généralement, utilisés ensemble. Pour finir, Ike (Internet Key Exchange) permet de gérer les échanges ou les associations entre protocoles de sécurité, nous ne le détaillerons pas ici.

IPSEC

Protocole AH

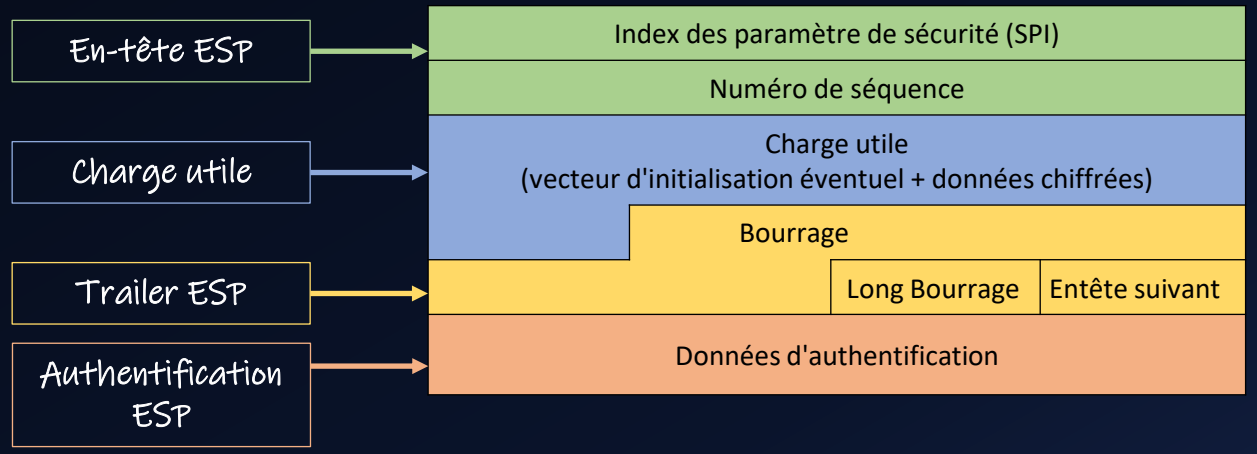
Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception, de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé "valeur de vérification d'intégrité" (Intégrity Check Value, Icv). La protection contre le rejet se fait grâce à un numéro de séquence.



Protocole ESP

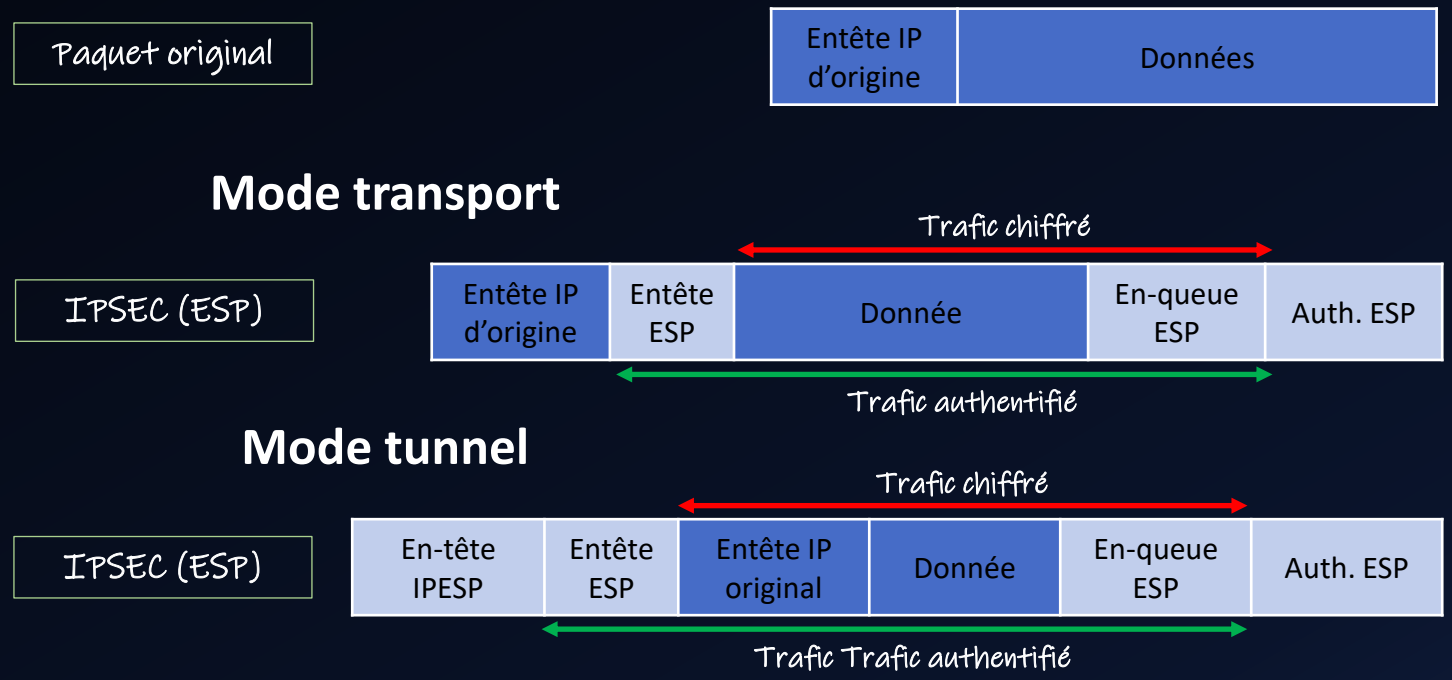
ESP peut assurer aux choix un / plusieurs des services suivants :

- Confidentialité
  - Confidentialité des données
  - Protection partielle contre l'analyse de trafic lors du mode tunnel
- Intégrité
  - Des données en mode non connecté
  - Authentification de l'origine des données
  - Protection contre le rejeu



Les deux modes de fonctionnement de IPSEC

- Mode transport
  - Prend un flux de couche 4
  - Signature et chiffrement fait puis transmit à la couche IP
  - TCP envoie ses données vers IPSEC comme il les enverrait vers IPv4.
  - Situé entre deux hôtes
  - Problèmes :
    - En-tête extérieur produite par la couche IP : pas de masquage d'adresse
- Mode Tunnel
  - Traverse la pile de protocole jusqu'à la couche IP (incluse)
  - Permet le masquage d'adresse
  - Entre deux parcelles de sécurité (routeur / firewall)



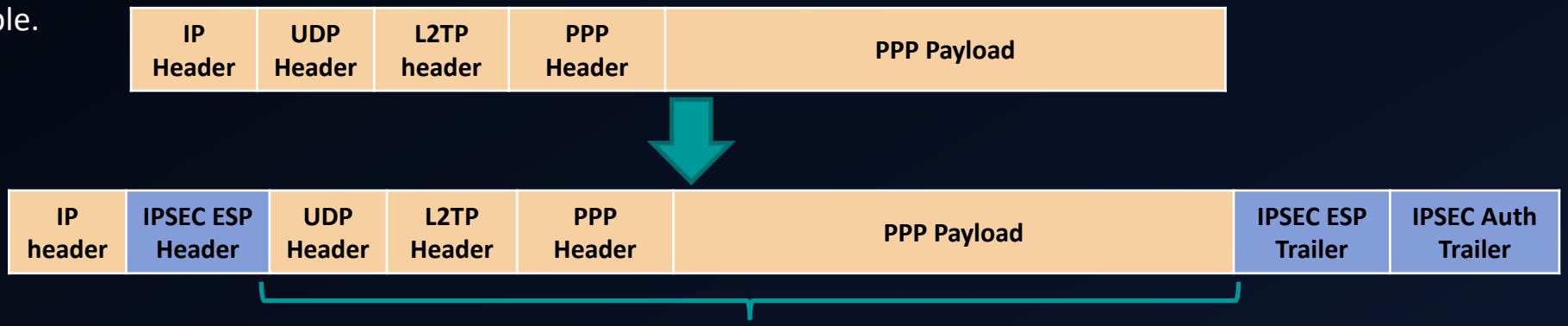
L2TP + IPSEC

Comme dit précédemment, L2TP ne s'utilise pas seul, la majeure partie du temps, il est combiné avec IPSEC. L'un s'occupe du tunnel, l'autre de la sécurité.

« IPSEC ne permet d'identifier que des machines et non pas des utilisateurs. Ceci est particulièrement problématique pour les utilisateurs itinérants. Il faut donc prévoir un service d'authentification des utilisateurs. Dans le cas de connexion dial-up(1) c'est l'identifiant de connexion qui sera utilisé pour authentifier l'utilisateur. Mais dans le cas de connexion via Internet il faudra prévoir une phase d'authentification supplémentaire à l'établissement du tunnel. »

source.pdf

Comme dit dans la citation, la combinaison n'est pas exempte de défauts. A cela s'ajoute que les opérations de chiffrement/déchiffrement réduisent les performances du réseau. C'est pourquoi l'achat d'un équipement dédié, couteux, devient indispensable.



(1) Via ligne téléphonique

MPLS

MPLS peut être utilisé pour créer un VPN. Celui-ci possède l'avantage de permettre de prioriser certaine partie du trafic grâce au QoS (Quality of Service).

> *« Le VPN IPSEC utilise l'accès internet (public) de chaque site pour leur permettre de communiquer. Les données échangées vont être cryptées afin d'assurer leur confidentialité.*
> *Le VPN MPLS, quant à lui, connecte les sites sur un réseau opérateur totalement privé.*
> *Parmi les avantages du MPLS figure une QOS qui permet de prioriser certains flux, superviser ceux-ci à partir d'une interface et placer un firewall en cœur de réseau pour unifier la sécurité de tous vos sites. »* https://www.proxyvpn.fr/vpn-vs-mpls

La principale différence entre MPLS est IPSEC est le fait que l'un transite sur un réseau privé et l'autre sur un réseau public. Cette technologie est à destination des grosses entreprises, qui ont besoin de beaucoup de bande passante.

Une fois de plus les deux technologies peuvent être utilisé en parallèle, mais pour deux usages distincts : Un VPN MPLS pour relier deux sites entre eux, et un VPN IPSEC pour les personnes en itinérance qui se connectent à l'entreprise.

VPN SSL / TLS : OpenVPN

Les VPN TLS s'appuient sur le protocole TLS. Ce dernier a remplacé l'ancien protocole SSL, pour sécuriser l'accès à distance. Ils permettent aux utilisateurs authentifiés d'établir des connexions sécurisées aux services internes HTTP et HTTPS ;

Il permet aux dispositifs disposant d'une connexion Internet d'établir une connexion VPN sécurisée d'accès à distance avec un navigateur web. Une connexion VPN SSL/TLS utilise un chiffrement de bout en bout (E2EE) pour protéger les données transmises entre le logiciel client du dispositif d'extrémité et le serveur par lequel le client se connecte à l'internet en toute sécurité.

Il existe deux principaux types de VPN SSL/TLS : le portail VPN et le tunnel VPN.

https://www.fibre-pro.fr/vpn-ssl/#Avantages_des_VPN_SSL

Description de OpenVPN

- Généralement, OpenVPN utilise un chiffrement OpenSSL 256 bits. Pour renforcer davantage la sécurité de la connexion, OpenVPN peut utiliser les algorithmes AES, Camellia, 3DES, CAST-128, ou Blowfish.
- Bien qu'OpenVPN ne supporte pas L2TP, IPSec et PPTP, il utilise son propre protocole personnalisé basé sur TLS et SSL.
- OpenVPN supporte l'amélioration des processus de connexion et d'authentification avec l'utilisation de plugins et de scripts tiers.
- Les clients peuvent en fait se connecter à des serveurs au-delà du serveur OpenVPN puisqu'il offre la prise en charge d'une configuration privée de sous-réseau.
- Pour protéger les utilisateurs contre les vulnérabilités de débordement de tampon dans les implémentations TLS/SSL, les attaques DoS, l'analyse des ports et les inondations de ports, OpenVPN s'appuie sur tls-auth pour la vérification des signatures HMAC. OpenVPN est également programmé pour supprimer les privilèges si nécessaire, et tourne dans un environnement dédié à CRL.
- OpenVPN fonctionne dans l'espace utilisateur au lieu de l'espace noyau.

https://www.cactusvpn.com/fr/beginners-guide-to-vpn/quest-ce-quopenvpn/

SSH

SSH est un cas un peu particulier. A l'origine il est là pour permettre une connexion chiffrée à un serveur distant. Il est notamment utilisé pour pouvoir travailler / contrôler un ordinateur à distance. Il peut néanmoins être utilisé comme tunnel. La mise en simple est très simple, mais est plus une solution d'appoint. Grace au tunnel effectué entre un ordinateur A et un ordinateur B, A pourra accéder à des ressources normalement disponibles que dans le réseau de B.

« ssh [ordinateur] –D 4444 » Cette simple commande permet de rediriger tous les flux de l'ordinateur « maison » sur notre port 4444. Dans le cas où nous voulons accéder à un service en ligne, il nous suffit d'utiliser Foxy Proxy pour pouvoir faire passer toutes nos recherche internet par la machine « maison ». Nous avons ainsi un tunnel sécurisé.

https://mrfey.fr/ARTICLES//SSH-tunneling