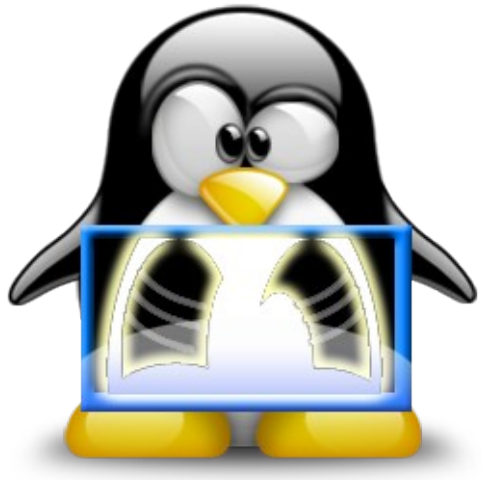
Tunnels et VPN

Cédric FOLL, Paul TAVERNIER, Nicolas PRUNIER



Plan

- Le principe des tunnels
- Les VPN

Les tunnels

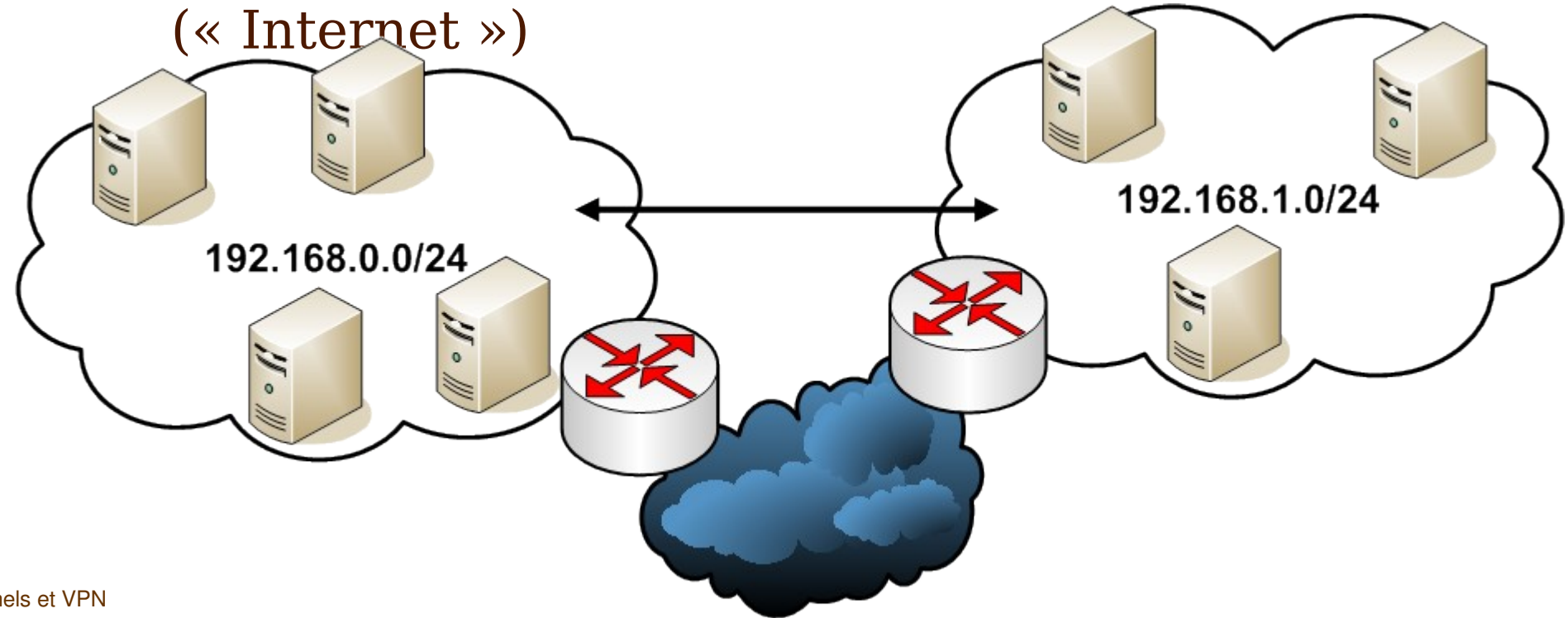
- Objectifs
  - Permettre de contourner des problèmes de routage ou de filtrage
    - Interconnecter deux sites IPv6 en passant par un réseau IPv4
    - Faire transiter un adressage privé (RFC1918) sur un réseau public
    - Propager un réseau de couche 2 au dessus d'un réseau de couche 3 (IP)
    - Contourner une politique de filtrage (firewalling)
    - ...

Quelques exemples...

- En général, on encapsule de la couche 2 ou 3 dans de la couche 3.
  - Tunnel GRE (generic router encapsulation)
    - Encapsulation de couche 3 au dessus de couche 3, supporté par la plupart des matériels.
    - Protocole IP numéro 47
  - IPSec, nativement sur IPv6, porté sur IPv4
    - Encapsulation d'un paquet de couche 3 chiffré et/ou signé dans un paquet de couche 3 (ESP) ou 4 (ESP over UDP ou TCP)
  - L2TP
    - Encapsulation d'un paquet de couche 2 dans un paquet de couche 4 (udp/1701)
  - IPv6 over IPv4 (et le contraire)

L'exemple de GRE

- Problématique
  - Deux sites en adressage privé et connectés à Internet veulent communiquer
    - Une machine d'un siteA (192.168.0.10) veut pouvoir atteindre la machine d’un siteB (192.168.1.10) au travers d’un réseau public (« Internet »)



Création de tunnel GRE

- Sur le routeur du siteA (194.167.110.1 et 192.168.0.250)
  - Création du tunnel
    - **ip tunnel add netb mode gre remote 194.167.110.128 local 194.167.110.1 ttl 255**
  - Montée de l'interface à laquelle on assigne une ip
    - **#ip link set netb up**
    - **#ip addr add 192.168.0.251 dev netb**
  - Ajout de la route pour atteindre le subnet du siteB par cette interface
    - **#ip route add 192.168.1.0/24 dev netb**
- Sur le routeur du siteB (194.167.110.128 et 192.168.1.250)
  - **#ip tunnel add netb mode gre remote 194.167.110.1 local 194.167.110.128 ttl 255**
  - **#ip link set netb up**
  - **#ip addr add 192.168.1.251 dev netb**
  - **#ip route add 192.168.0.0/24 dev netb**

Pour aller plus loin...

- Comment propager ses VLANS sur un site distant via un réseau public (« Internet »)?
  - Utiliser un tunnel de couche 2 tel que L2TPv3!

Les VPN

- La problématique
  - Disposer de sites interconnectés par un réseau public et faire « *comme si* » on disposait d'un réseau privatif
    - On crée donc un « *réseau privé virtuel* » (RPV) ou « virtual private network » (VPN)

Les (V)PN

- Un réseau privatif = infrastructure privative?
  - Une propagation de la couche 3? Construire une infrastructure privée entre les routeurs d'entrée de chacun de ses sites
  - Une propagation de la couche 2? Construire une infrastructure privée entre les switches de chacun de ses sites
- Avantages
  - La sécurité (personne ne peut écouter la trafic, ni l'altérer)
  - Le contrôle de bout en bout. Etant le seul utilisateur des liens, le trafic n'est pas gêné par le trafic d'autres clients.
- Inconvénients
  - ...c'est cher, donc peu « *scalable* »

Les VPN

- Beaucoup de technologies existent répondant à tout ou partie des inconvénients entrevus ci-avant
  - L'exemple de GRE
    - Ne répond qu'à une propagation de la couche 3 (et accessoirement se limite à IP)
    - Peut mieux faire…(confidentialité?)

Les VPN

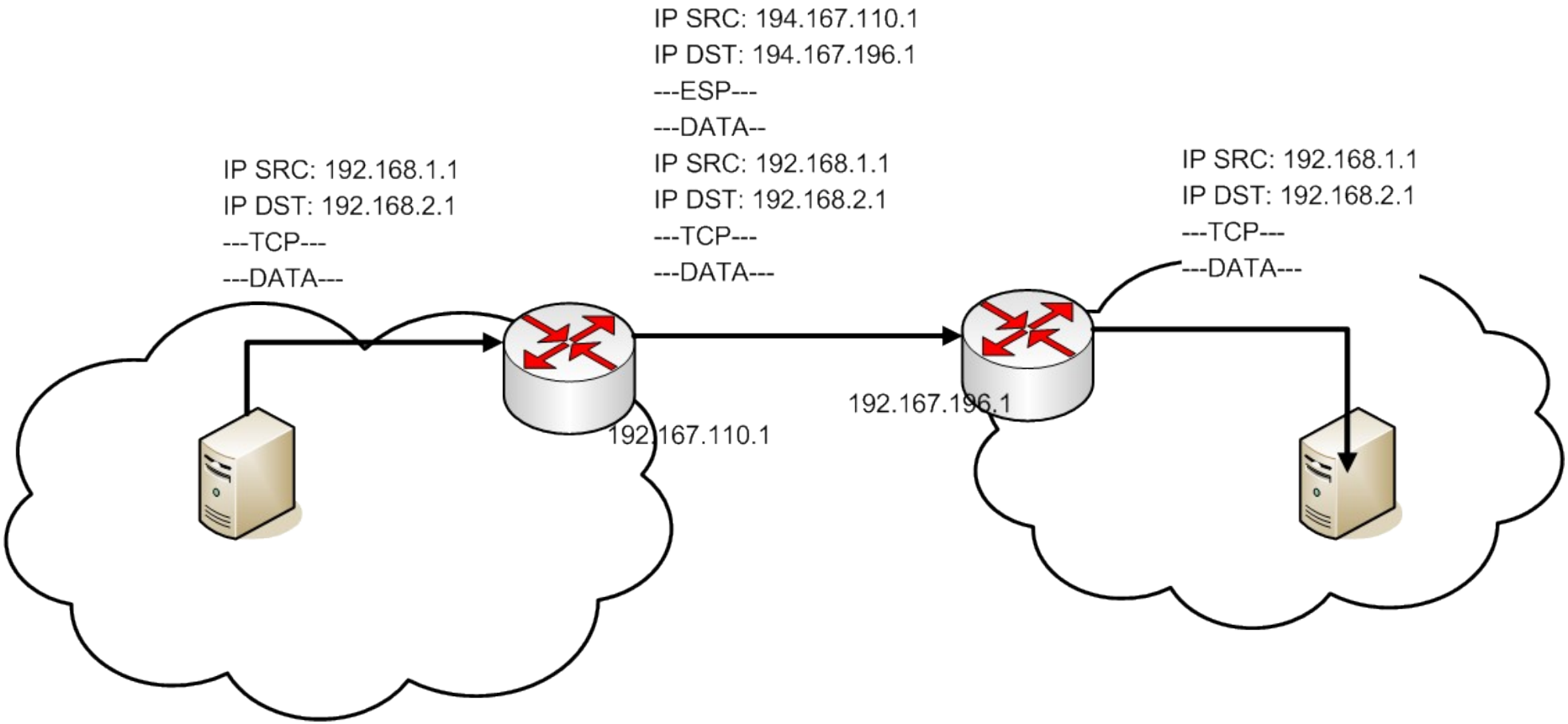
- Plan
  - GRE (déjà vu)
  - IPSec
  - MPLS
  - VPLS
  - L2TPv3, un MPLS digeste...
  - Group Encrypted Transport (GET) VPN
    - Le MPLS « IPsecisé » par Cisco

IPSec

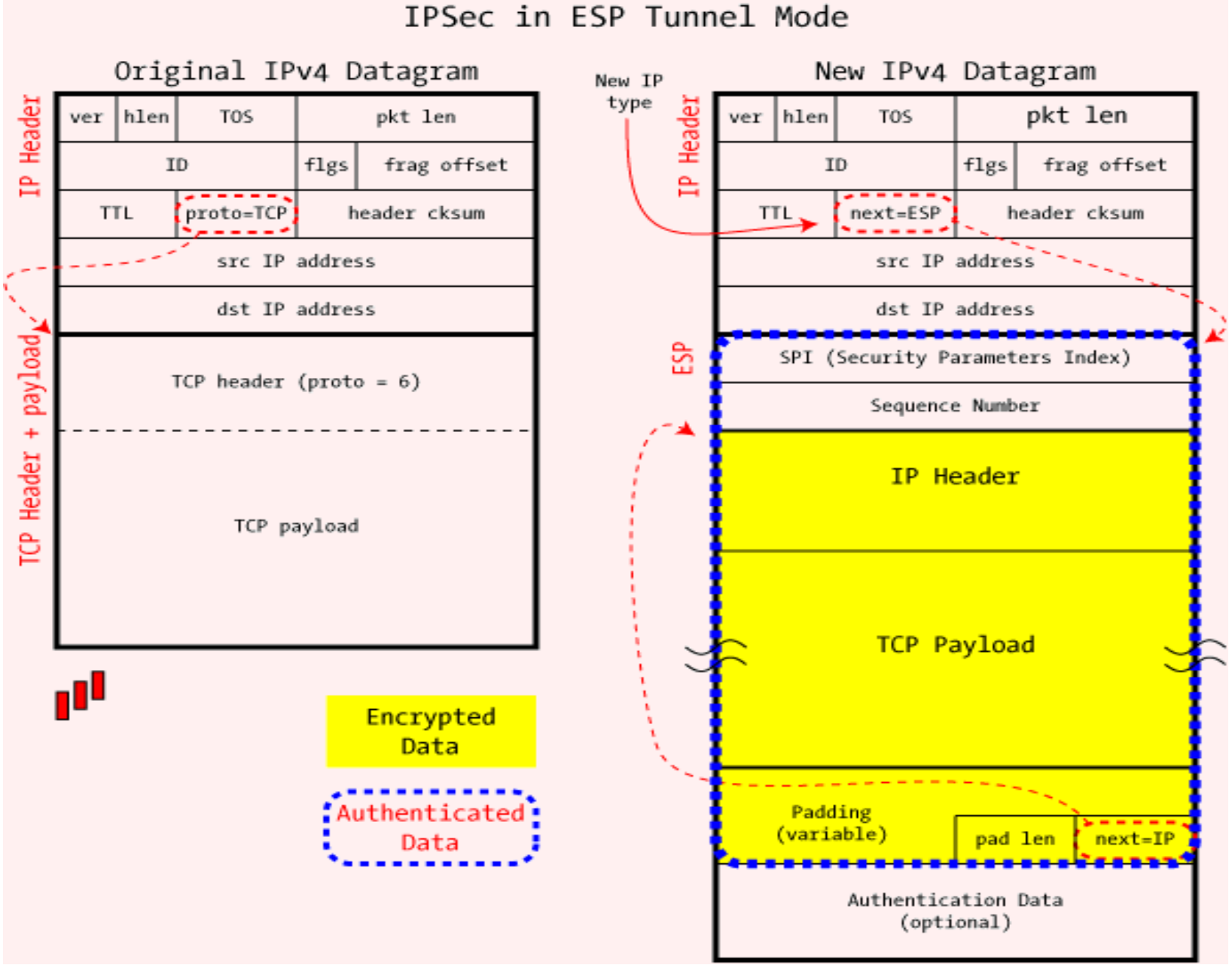
- Les paquets IP sont encapsulés par les routeurs IPSec (placés souvent « *en bordure* » (edge))
  - Le protocole de couche 4 est AH (Authentication Header) ou ESP (Encapsulating Security Payload)
    - AH: les paquets sont stockés en couche data et signés numériquement (hash).
    - ESP: les paquets sont stockés de manière chiffrée en couche data.
  - *Remarque*: il est possible d'utiliser IPSec autrement qu'en mode tunnel. Dans ce cas IPSec sert seulement à augmenter le niveau de sécurité, utilisé par exemple pour les postes nomades (utilisation marginale)

Solution IPSec

- Encapsuler un paquet IP dans un autre paquet (même chose pour GRE)



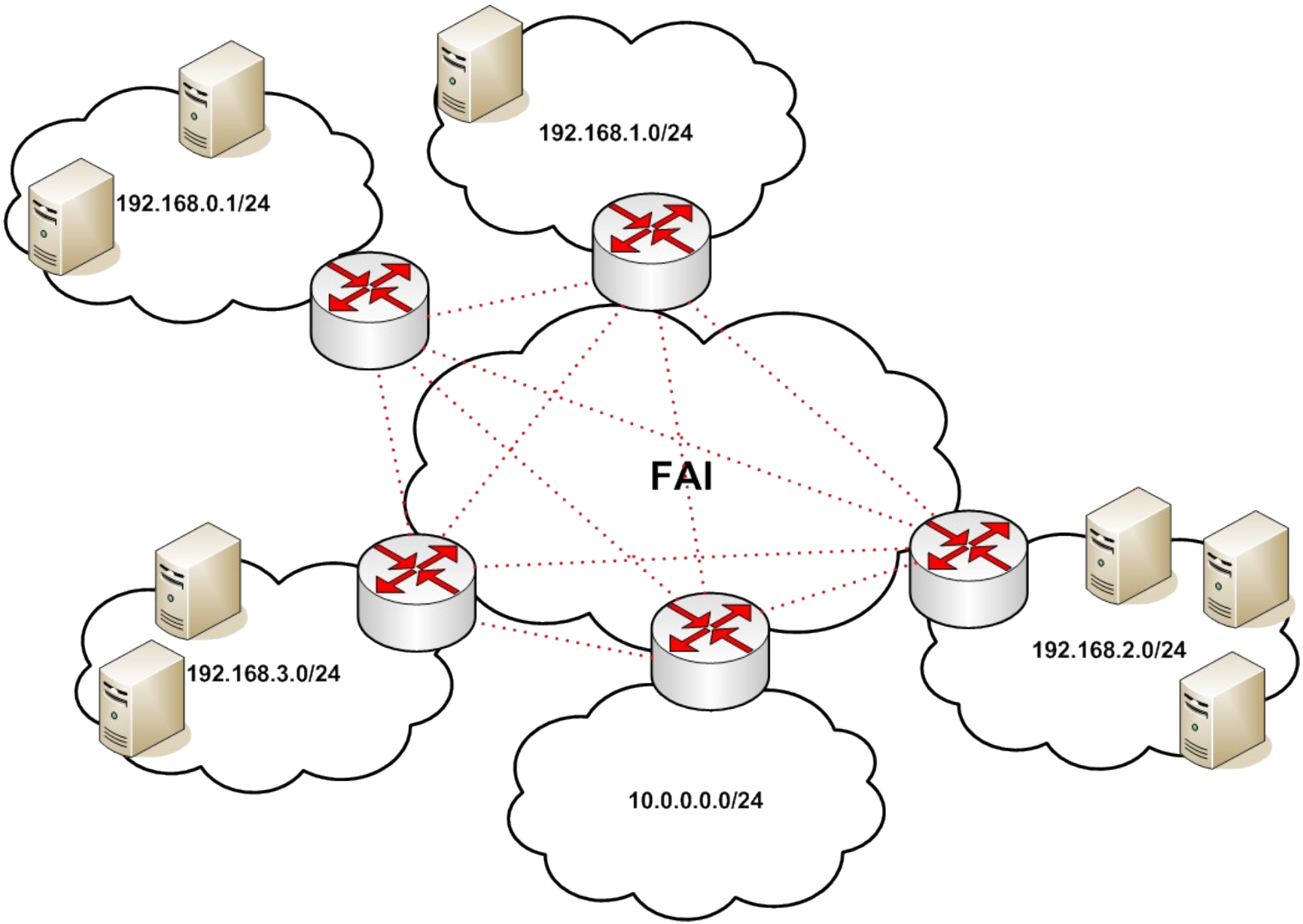
IPSec en mode ESP



IPSec

- Initialisation de la connexion
  - Via un secret partagé (Pre-shared Key)
    - Interprétable comme un échange Diffie-Hellman simplifié où les tiers possèdent un secret en commun (évitant une attaque de type MitM)
  - Via un mode dit « Infrastructure (PKI)
    - Public-Key Infrastructure
    - Les tiers reçoivent des couples de clés asymétriques (clés publiques-privées) authentifiées (signées) par une autorité de confiance

IPSEC: Présentation



IPSec

- Sur chaque routeur, obligation de définir une route pour chacun des réseaux distants à joindre
- Pour N routeurs, il faut définir N*(N-1) routes.
- L'ajout ou la suppression d'un routeur implique une intervention sur tous les autres

IPSec

- Les avantages...
  - Permet de réaliser un VPN simplement et à bas coût (un pc sous linux fait l'affaire).
  - Système robuste, mature, offrant un niveau de sécurité élevé
  - Peut évoluer (*scalable*) et s'appuyer éventuellement sur une PKI avec des avantages réels en terme de sécurité
    - Isoler depuis un point central (siège) un site en révoquant son certificat (un certificat X509 est créé avec la clé privée de l'AC. Il contient entre autres la clé publique du site, la signature de l'AC, etc.

IPSec

- Les inconvénients
  - La sécurité, en mode PSK. Si le secret partagé est connu par un tiers au du domaine de confiance, il faut reconfigurer tous les équipements IPSec
  - Performances moyennes. Peu adapté aux flux multimédias (VoIP)
    - Les mécanismes de chiffrement/déchiffrement «limitent» les débits et induisent potentiellement de la latence.
  - Impossible de déployer des mécanismes QoS
    - basés généralement sur des champs de la couche IP...qui sont ici chiffrés...Ils sont donc inexploitables par les équipements intermédiaires
  - Lourd en terme de configuration/déploiement
    - Dès que l'on ajoute un réseau au nuage VPN, il faut construire une route sur chacun des routeurs « edge » du nuage
    - Il faut un routeur IPSec sur chaque site relié au VPN

IPSec: A large échelle...?

- Réseau RACINE (Réseaux d'Accès et de Consolidation des INtranets de l'Education nationale)
  - Réseau interconnectant tous les collèges, lycées et sites administratifs (Rectorat, Administration Centrale) de l'éducation nationale française.
    - 10 000 sites interconnectés en IPSec (métropole et DOM/TOM)
    - Un backbone full mesh de 30 sites (Rectorats) composé de PIX 515E
    - Un réseau étoilé interconnectant les collèges et lycées (10 000 sites) au Rectorat dont ils dépendent. composé d'une distribution linux maison (http://eole.orion.education.fr/)
    - Un plan d'adressage IP normalisé à l'échelle nationale, basé sur la RFC1918
  - Une infrastructure complète (PKI) déployée, avec Autorité d'Enregistrement/Autorité de Confiance, publications de CRL, ...

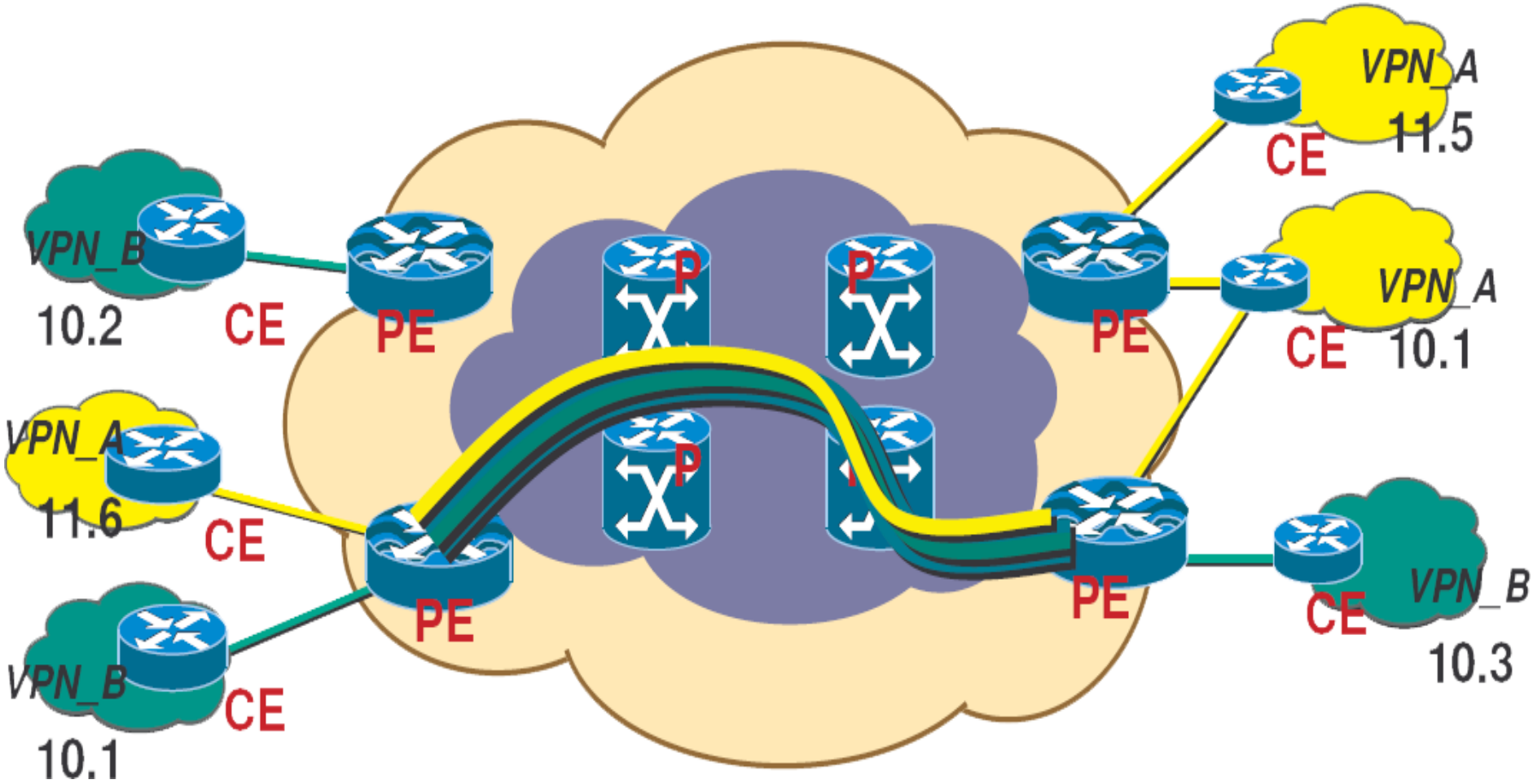
VPN IP par MPLS: Multiprotocol Label Switching

- Le sécurité du VPN (étanchéité) est confiée à un tiers (opérateur)
- Une technologie dite de « *couche 2,5* »
  - constituée d'équipements de couche 2 (Providers switches)...
  - ...et de couche 3 (Provider-Edge routers). L'opérateur marque en périphérie (PE) les flux de chacun de ses clients
    - sur chacun des PE de l'opérateur, une VRF (Virtual Routing and Forwarding) est créée pour chacun des « tags ».
- Technologie complètement transparente pour le « client final » (Customer Edge Routeur)
  - Le client peut se considérer seul utilisateur du réseau de son opérateur, et à ce titre peut propager librement son adressage privé (éventuellement RFC1918).

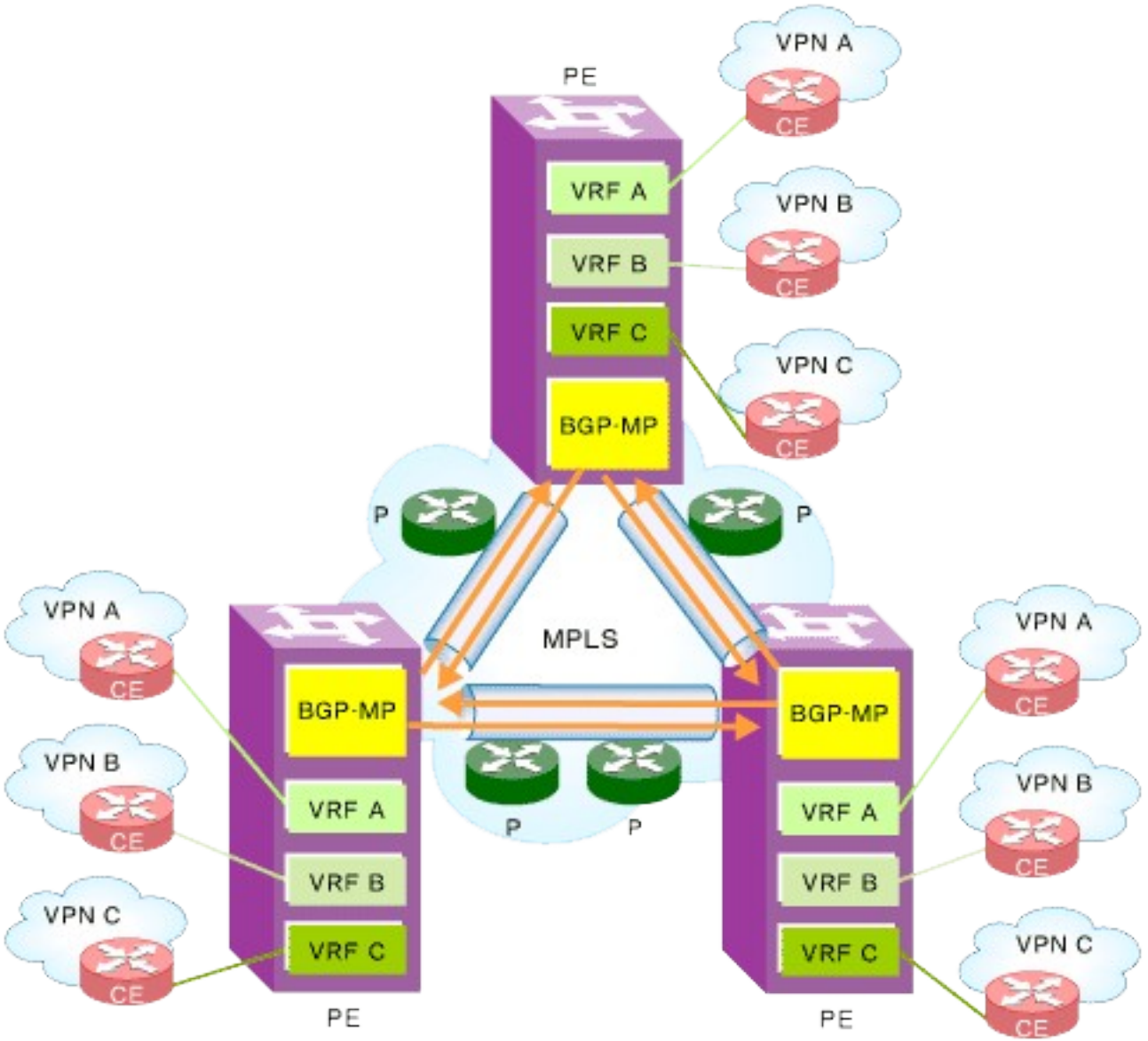
VPN IP par MPLS

- Configuration coté client (customer edge):
  - Aucune configuration nécessaire.
- Configuration coté ISP (provider edge)
  - Un tag est ajouté sur les paquets de chaque client.
  - Chacun des routeurs possède une table de routage spécifique pour chacun des clients (VRF).
    - Le routeur décide quelle VRF utiliser en analysant le tag MPLS sur le paquet reçu.
    - Les routes de chaque VRF sont échangées entre les routeurs de l'ISP via BGP.

VPN IP par MPLS



VPN IP par MPLS



VPN IP: MPLS-IPSec...

- Avec IPSec
  - Tout le routage est géré par le client ... et c'est un routage statique
  - Une opération (ie ajout/suppression) sur un réseau doit être répercutée manuellement sur tous les réseaux
- Avec MPLS
  - Le routage est pris en charge par l’opérateur, via des mécanismes dynamiques

VPN IP par MPLS

- Inconvénients par rapport à IPsec
  - Plus de chiffrement, un pirate réussissant à compromettrel'opérateur va pouvoir lire tous les échanges et altérer des données
  - C'est l'opérateur qui gère le VPN
    - L'opérateur doit le supporter

      on parle alors d'OSM, pour *Offre Sur Mesure*. On n'est clairement plus dans une offre grand public de type ADSL
    - Cela a un coût!

VPN IP par MPLS

- Avantages par rapport à IPSec
  - Sécurité de niveau 2. A moins de compromettre l'ISP, un pirate ne pourra jamais atteindre un LAN privé à moins d'être branché au bon endroit (et donc d'être correctement taggé)
  - Il est possible de gérer la QoS de bout en bout (la couche IP n’étant pas altérée, on peut classer/traiter les flux au coeur du réseau)
  - Plus de problèmes de routage à gérer
  - Plus besoin d'équipements de chiffrements en périphérie sur les sites (mais ce n’est pas exclusif)

MPLS, implémentation typique

- Pour le transport de la voix sur IP, ou autres flux dits « RTSP »
  - Des protocoles supportant mal des manipulations de la couche3 (de type NAT, etc.)
  - Les performances d'IPSec rendent le transport de la VoIP quasi impossible
  - QoS obligatoire
- Pour les petits sites reliés via Internet au siège.
  - Sur chaque site quelques PC en adressage privé et un routeur « d'entrée de gamme »
  - Reliés au siège via VPN MPLS (zéro-conf sur les sites distants).

Ethernet over MPLS (EoMPLS)

- MPLS permet également de véhiculer les protocoles de couche 2
  - L'opérateur encapsule dans les paquets MPLS les paquets Ethernet des clients
    - Possibilité alors de propager ses VLANs sur Internet (Les trames 802.1Q sont transportés)

L2TPv3

- Similaire à du GRE transportant du niveau 2
- Cisco remet le L2TP sur le devant de la scène (RFC3931, mars 2005)
  - Possibilité d'encapsuler n'importe quel protocole de couche 2 (et plus seulement ppp) et donc possibilité de propager ses VLANs.
- Une alternative séduisante à EoMPLS
  - On perd certaines fonctionnalités de QoS offertes par MPLS et le routage géré par l'ISP
  - On gagne son indépendance vis à vis de l'opérateur, la technologie ne reposant plus sur lui...mais sur les « edge » routeurs du client (siège-filiales)

Et si l'on en veut encore plus???

- On sait désormais propager « sa » couche 2
  - EoMPLS ou L2TPv3
- On gère la QoS de bout en bout
  - EoMPLS et dans une moindre mesure L2TPv3
- Quid de la confidentialité/intégrité ?
  - Gestion en extrémité en couche 7(ssh, https, smtps, pop3s, imaps, sftp, etc.)
    - Insatisfaisant coté NetAdmin (car dépendant des SysAdmin ;o)
    - Insatifaisant côté utilisateurs finaux (changement d'outils, de configurations, etc..)
  - Technologie de type GroupEncryptedTransport (GET) VPN popularisée par Cisco

Group Encrypted Transport (GET) VPN

- Comme son nom l'indique, on ne chiffre que la couche transport...
  - C'est de l'IPSec où la couche 3 n'est pas altérée
  - Le client doit s'appuyer sur un mécanisme, typiquement MPLS, pour propager son adressage privé sur le réseau opérateur.
    - On garde toute la souplesse de MPLS et les possibilités de QoS (la priorité des paquets est définie via un tag sur la couche IP)
    - On retrouve les mécanismes de chiffrements d'IPSec

SSL VPN

- Utilisé pour les accès des postes distants à l'intranet
- Encapsulation dans des tunnels SSL/TLS
- Compatible avec les nouveaux terminaux
- 2 modes principaux :
  - SSL Portal VPN :
    - Accès aux ressources via un portail HTTPS dédié
    - Les ressources sont orientés web.
  - SSL Tunnel VPN :
    - Permet l'accès à des ressources/protocoles non orientés web au travers du navigateur.
    - Un client est lancé via le navigateur (Java, ActiveX, ...)

En résumé

- Un tunnels permet d'encapsulé des paquets de couche X dans des paquet de couche Y avec X<=Y.
- Un VPN est un ensemble de tunnels permettant de faire transiter des flux de manière « privés » sur un réseau « publique ».
- Toutes les solution VPN ne sont pas forcément cryptés
- IPSEC est complexe à mettre en œuvre mais permet le chiffrement et assure l'indépendance vis à vis du FAIs
- MPLS est une offre FAI, généralement non crypté, mais ne necessitant pas de connaissance/configuration par l'utilisateur final