# Sécurité des Réseaux

Dr Salim Benayoune

## Contenu

- Introduction à la sécurité des SI
  - Notions de base et définitions
- La sécurité des réseaux
  - Les attaques sur les réseaux
  - La méthodologie d'attaque réseau
- Sécurisation des réseaux
  - Parefeux et Architecture sécurisée
  - Proxy et IDS
  - Les VPN
- La sécurité des système
  - Normes et durcissement
  - Les malwares et les techniques virales

# Sécurisation d'un réseau

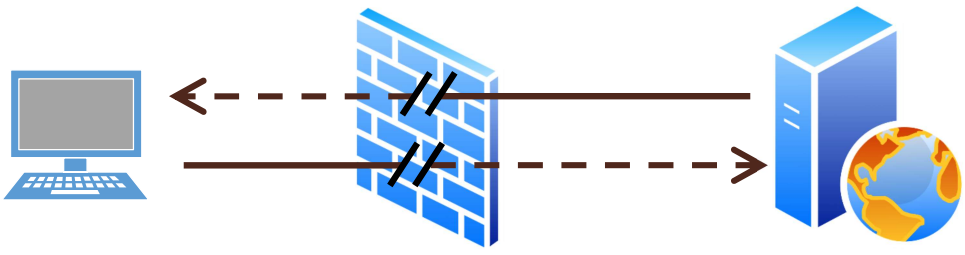
- Pare-feu
- Load-Balancer (Répartiteur de charge)
- Anti-virus
- IDS et IPS
- VPN
- Segmentation



# Sécurisation d'un réseau

***Pare-feu***

- **Équipement en coupure entre 2 ou plusieurs réseaux ;**
- Inspecte les paquets réseaux entrants et sortants d'un réseau à l'autre ;
- Implémente un **mécanisme de filtrage basé sur des règles :** il ne transmet donc que les paquets réseaux qui respectent les règles de filtrage implémentées dans la configuration du pare-feu.



Pour chaque flux entrant ou sortant, le pare-feu interroge ses règles de filtrage pour déterminer s'il doit laisser le paquet réseau passer ou non.

# Sécurisation d'un réseau

## *Pare-feu*

### Règles de filtrage :

- Historiquement, elles étaient basées sur les couches basses de la pile protocolaire (**réseau, transport**),
- Les pare-feu sont également capables de filtrer selon les données de la **couche applicative** (protocole et contenu des données).
  - Parefeu de nouvelle génération (NGFW)
  - Les **proxy et reverse-proxy peuvent être vus comme des pare-feu applicatifs dédiés**.
- Un **anti-virus** ou un **mécanisme de détection d'intrusion** peuvent également être implémentés sur le pare-feu de façon à détecter un malware en transit ou certaines attaques, mais **attention au DoS**!

### Avantage sécurité :

- L'exploitant d'un réseau peut donc restreindre le trafic entrant et sortant aux seules connexions qu'il estime légitime. Toutes les autres connexions sont donc bloquées. C'est le principe de l'***interdiction par défaut***.

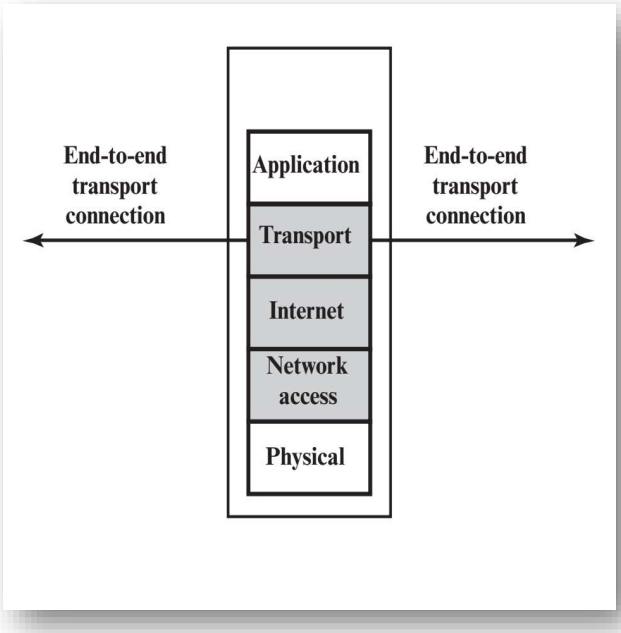


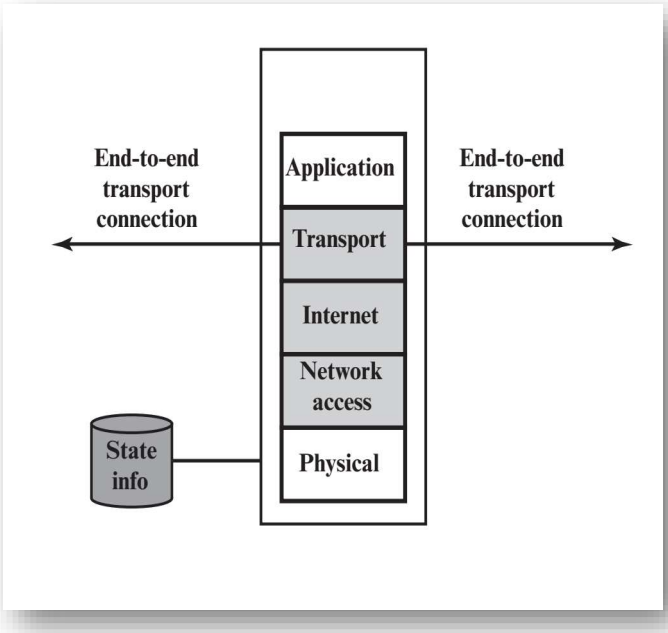
# Sécurisation d'un réseau

## *Pare-feu*

Types de parefeux

- Parefeu **sans état** (**stateless** firewall)
- Parefeu **avec état** (**stateful** firewall)

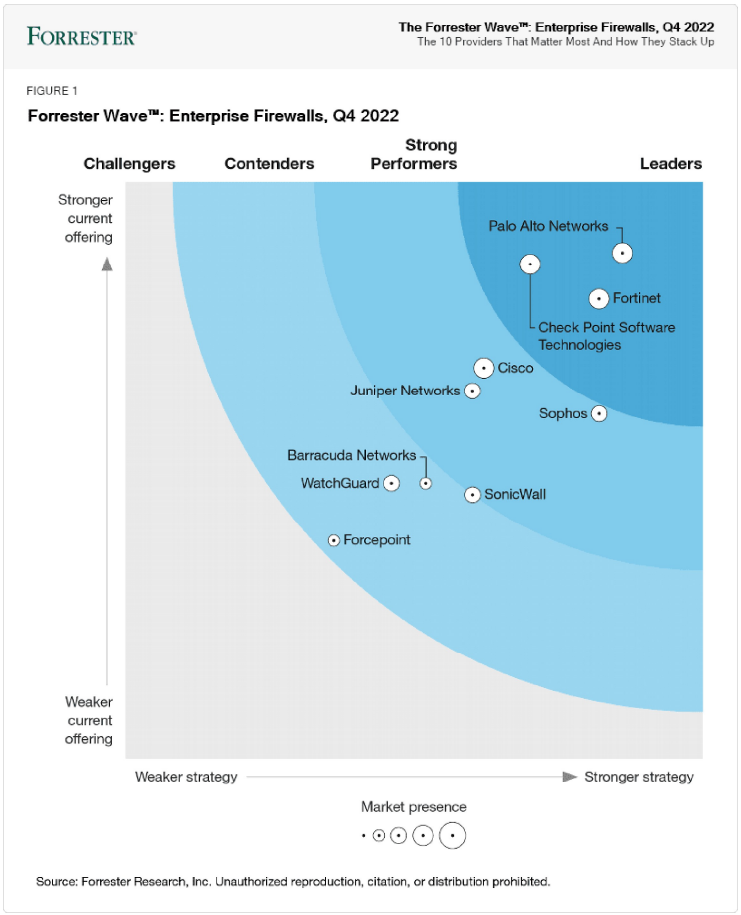


# Sécurisation d'un réseau

***Pare-feu***

- Solutions Parefeu :





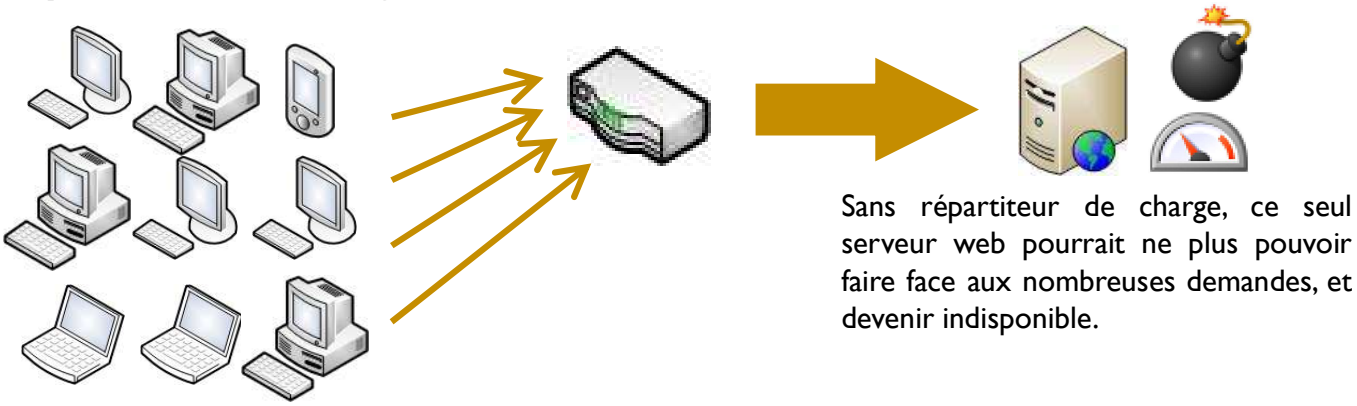

# Sécurisation d'un réseau

***Répartiteur de charge***

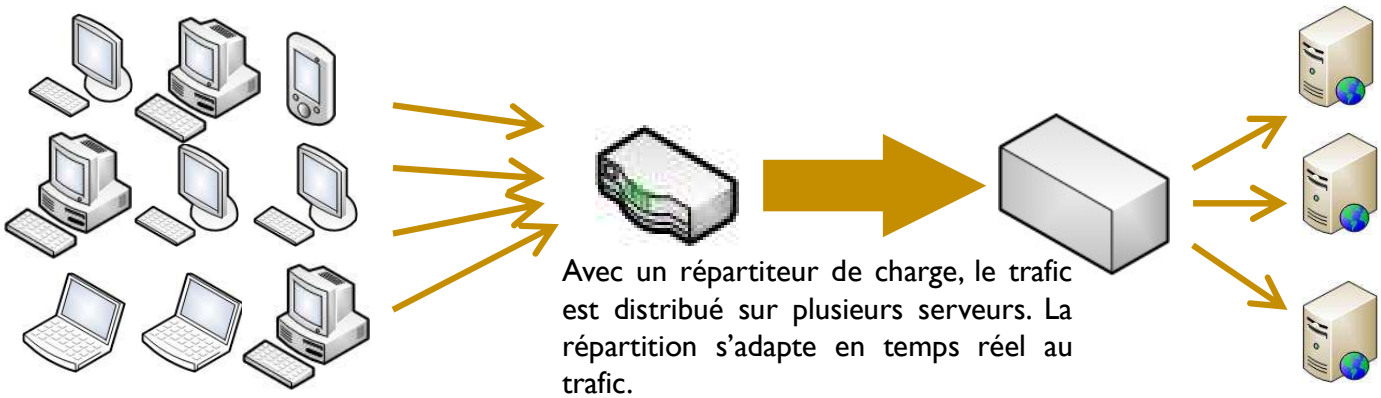
- « **Load-balancer** » en anglais ;
- Équipement rencontré sur les grosses infrastructures où les serveurs doivent faire face à de très fortes bandes passantes et charges élevées de trafic ;
- Équipement chargé de **répartir/distribuer la charge réseau** en fonction des caractéristiques de celui-ci et de la disponibilité des serveurs ;
- Avantage sécurité : permet de mieux se protéger contre les **dénis de service distribués.**
- Autres solutions : Agrégation de liens, GLBP/HSRP/VRRP, Cluster

# Sécurisation d'un réseau

## *Répartiteur de charge*



Sans répartiteur de charge, ce seul serveur web pourrait ne plus pouvoir faire face aux nombreuses demandes, et devenir indisponible.



Avec un répartiteur de charge, le trafic est distribué sur plusieurs serveurs. La répartition s'adapte en temps réel au trafic.



# Sécurisation d'un réseau

## *Anti-virus*

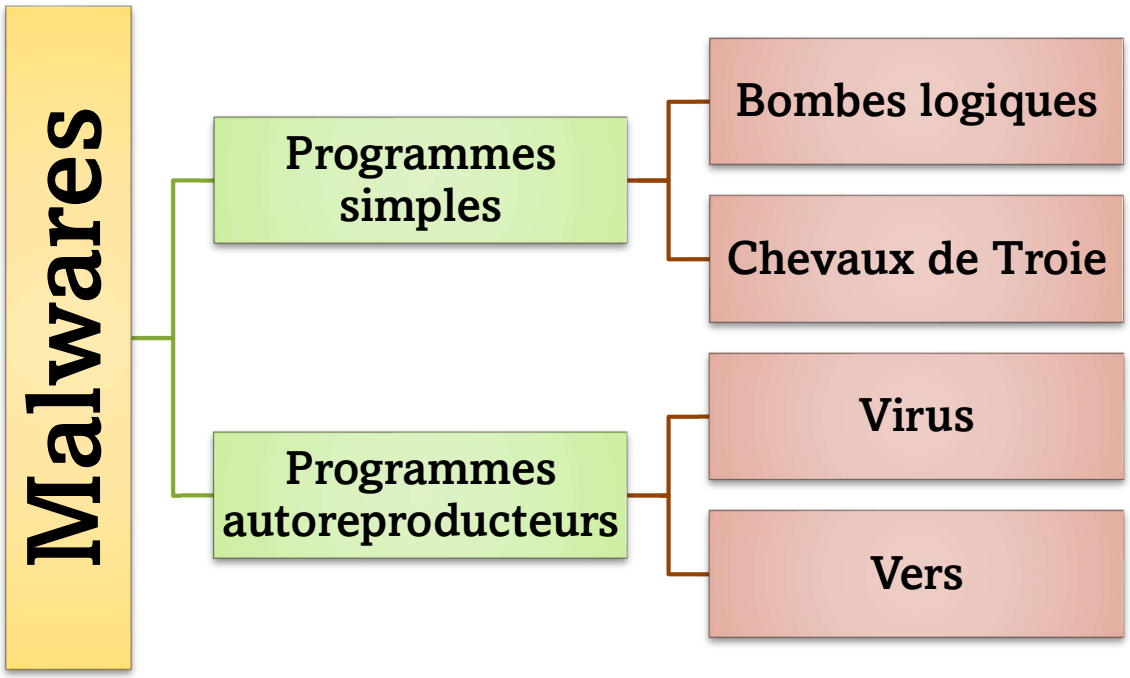
Logiciel chargé de détecter et stopper les **malware connus**

- Ces logiciels fonctionnent en général avec une base de données qui contient les signatures des malware connus. Ils analysent en permanence les fichiers et les exécutables du système hébergeant l'anti-virus ;
- **Limite des anti-virus :** ils ne détectent (en général) que les malware déjà répertoriés par les éditeurs. Ainsi, les nouveaux virus ou les malware ciblés ne sont souvent pas détectés. D'autre part, il est impératif que l'anti-virus soit mis à jour quotidiennement.
- Solution : utilisation des méthodes de **l'intelligence artificielle** (IA) comme l'apprentissage machine (Machine Learning) ou l'apprentissage profond (Deep Learning) pour détecter les comportement anormaux.

# Sécurisation d'un réseau

***Anti-virus***

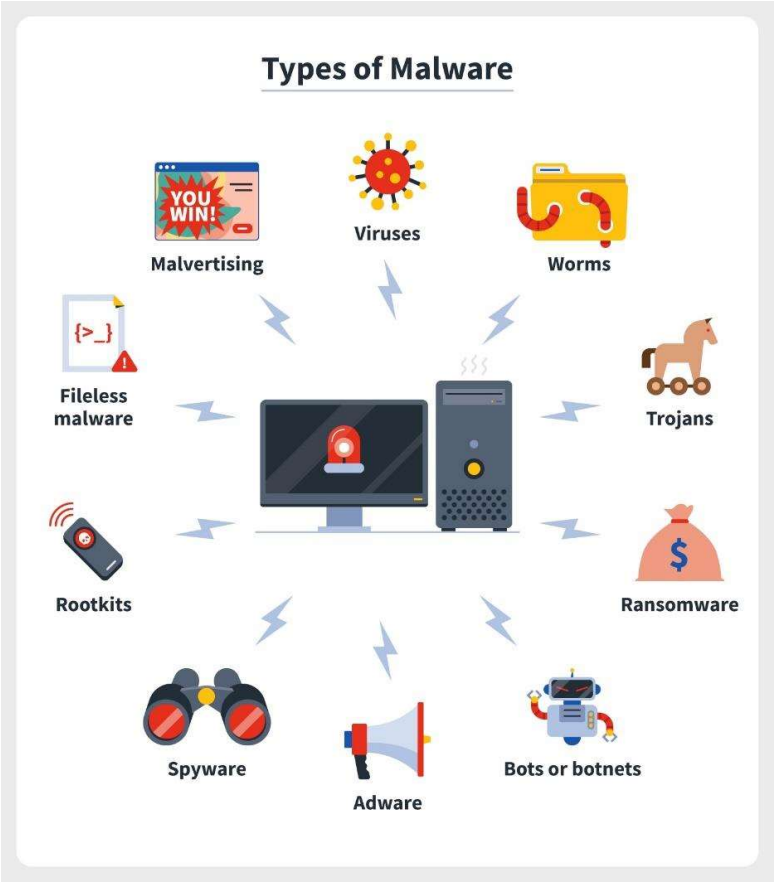
- Taxonomie :






# Sécurisation d'un réseau

***Anti-virus***

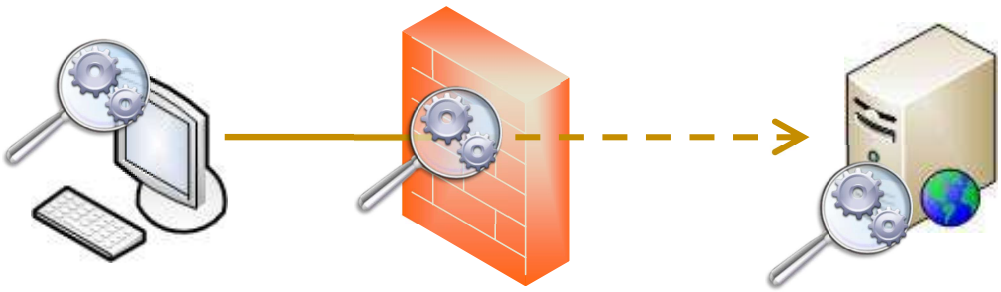


# Sécurisation d'un réseau

## *Anti-virus*

Un anti-virus peut être déployé :

- En **local :** sur un système (poste de travail ou serveur) afin de détecter les virus affectant cette machine ;
- En **coupure des flux réseaux :** sur un pare-feu afin d'analyser les flux réseau et détecter les malware avant même qu'ils n'atteignent leur cible. Ce fonctionnement peut être assimilé à un IDS (Intrusion Detection System), mécanisme présenté dans la section suivante.
- Evolution vers les solutions EDR (Endpoint Detection & Response)





# Sécurisation d'un réseau

## *IDS et IPS*

IDS **I**ntrusion **D**etection **S**ystem

IPS **I**ntrusion **P**revention **S**ystem

Chargés d'analyser le trafic réseau pour y **détecter des tentatives d'intrusion** :

- Soit en analysant **le comportement** des flux réseaux (IA) ;
- Soit en se basant sur une base de signatures identifiant des données malveillantes (principe similaire à celui des anti-virus).

En cas de détection d'une intrusion :

- Les **IDS alertent** les administrateurs, libre à eux d'intervenir ou non ;
- Les **IPS bloquent** les flux réseau concernés.

Les IDS/IPS demandent une **configuration fine** et maintenue :

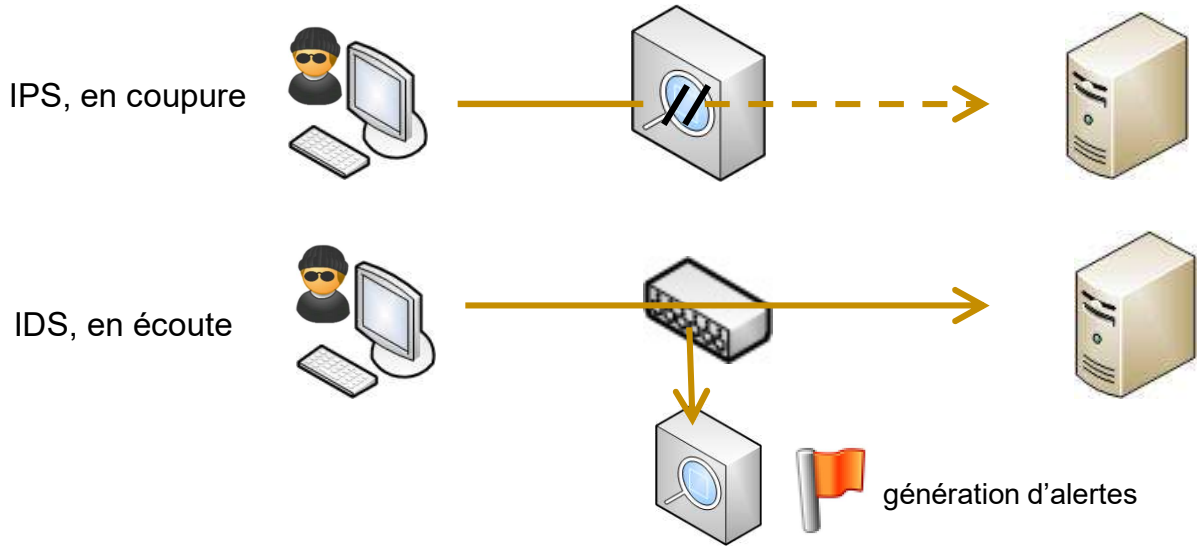
- Ils sont en effet connus pour présenter de nombreux **faux-positifs** (i.e. ils détectent à tort une tentative d'intrusion) ;
- De plus, les IDS/IPS basés sur des signatures ne peuvent détecter que les intrusions dont les caractéristiques techniques sont déjà connues et référencées.

# Sécurisation d'un réseau

## *IDS et IPS*

Un IDS peut être soit en coupure du flux réseaux, soit **positionné en écoute.**

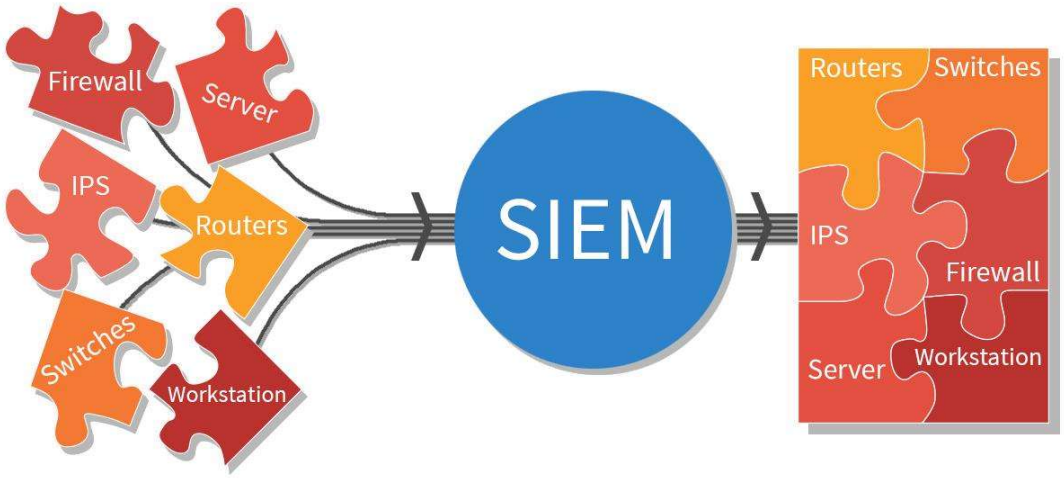
Un IPS **doit forcément** être en **coupure du flux** de façon à pourvoir bloquer le trafic lorsque cela est nécessaire.






# Sécurisation d'un réseau

- **SIEM** : Security Information and Event Management
  - Corrélation des logs



# Sécurisation d'un réseau

## *VPN*

### VPN **V**irtual **P**rivate **N**etwork

Un VPN est un **réseau virtuel** qui permet à **deux réseaux distants de communiquer en toute sécurité**, y compris si la communication s'effectue via des réseaux inconnus et auxquels nous ne faisons pas confiance.

Exemple avec une entreprise qui possède deux sites distants et qui ont besoin de communiquer entre eux via internet : comment faire passer les flux en toute sécurité via Internet que l'on ne maitrise pas ?



# Sécurisation d'un réseau

## *VPN*

Solution : grâce à des mécanismes cryptographiques, appliquer un **chiffrement des données, ainsi qu'un motif d'intégrité, à tous les flux entre les 2 sites**. On obtient ainsi un **tunnel virtuel** qui ne contient que des données chiffrées et protégées en intégrité :

- Les données qui passent sur Internet sont donc chiffrées et non compréhensibles par un attaquant qui écouterait les flux ;
- En cas de modification malveillante des flux, le mécanisme d'intégrité permettra au destinataire de déterminer que les données reçues ne sont pas intègres, et qu'il ne faut donc pas traiter ces données.

Il existe différents types de VPN, représentés sur les diapositives suivantes.

# Sécurisation d'un réseau

***VPN***

VPN de site à site, dont le tunnel est géré par les routeurs
**IPsec** – au niveau de la couche Internet

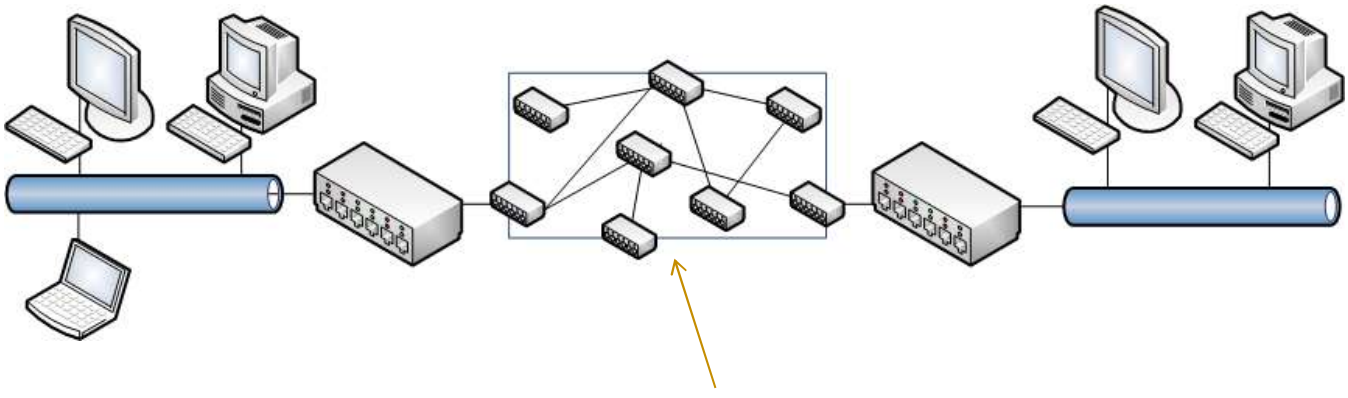
VPN entre systèmes
**TLS** – au niveau de la couche Transport (OpenVPN)



# Sécurisation d'un réseau

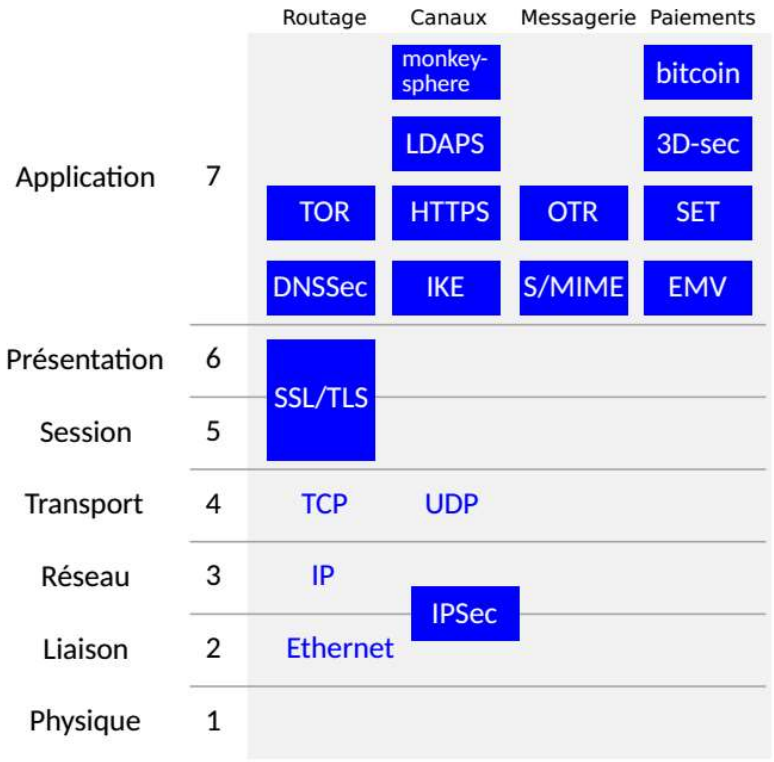
***VPN***

Il existe également des VPN qui n'ont pas recours à de la cryptographie, mais qui font appel aux **infrastructures d'opérateurs**. Dans ce cas, la protection du réseau est assurée par l'opérateur.



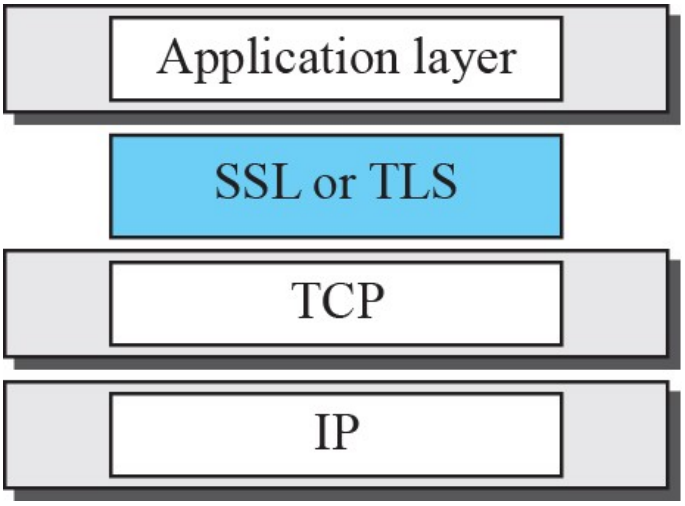
Réseau opérateur **MPLS**, dont le cœur est inaccessible aux clients se connectant sur ce réseau

# Sécurisation d'un réseau
## *Protocoles de sécurité et Modèle OSI*



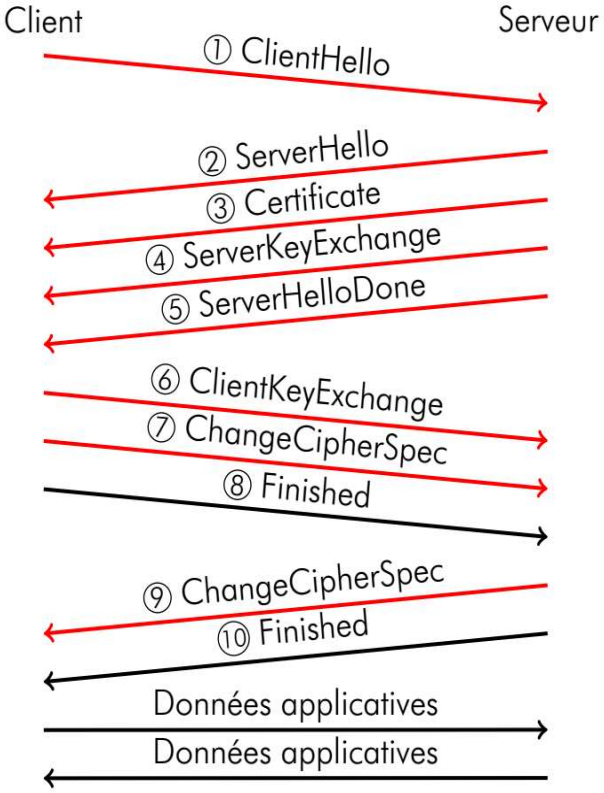



# Sécurisation d'un réseau
# Place de TLS dans le modèle TCP/IP



# Initiation générique d'une session TLS

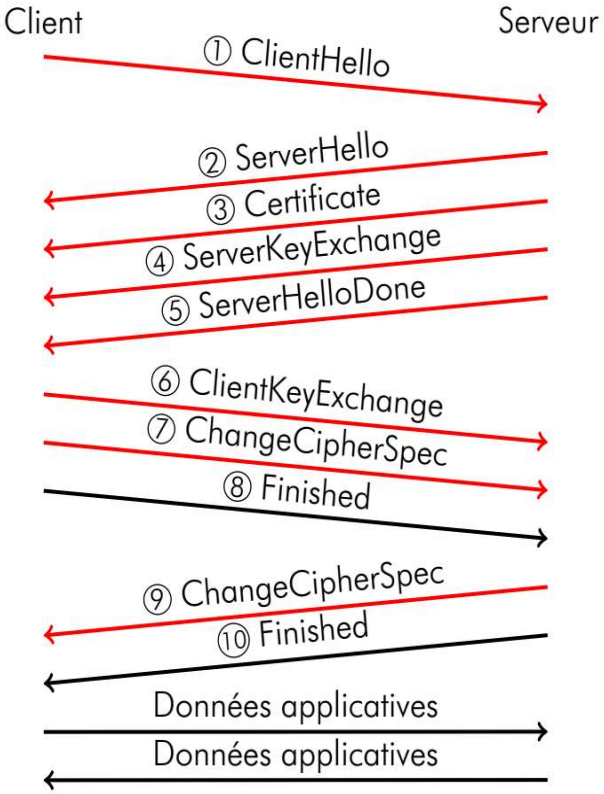
1. le client initie une requête en envoyant un message de type ClientHello, contenant notamment les suites cryptographiques qu'il prend en charge ;
2. le serveur répond par un ServerHello qui contient la suite retenue ;
3. le serveur envoie un message Certificate, qui contient en particulier sa clé publique au sein d'un certificat numérique ;
4. le serveur transmet dans un ServerKeyExchange une valeur éphémère qu'il signe à l'aide de la clé privée associée à la clé publique précédente ;
5. le serveur manifeste sa mise en attente avec un ServerHelloDone ;



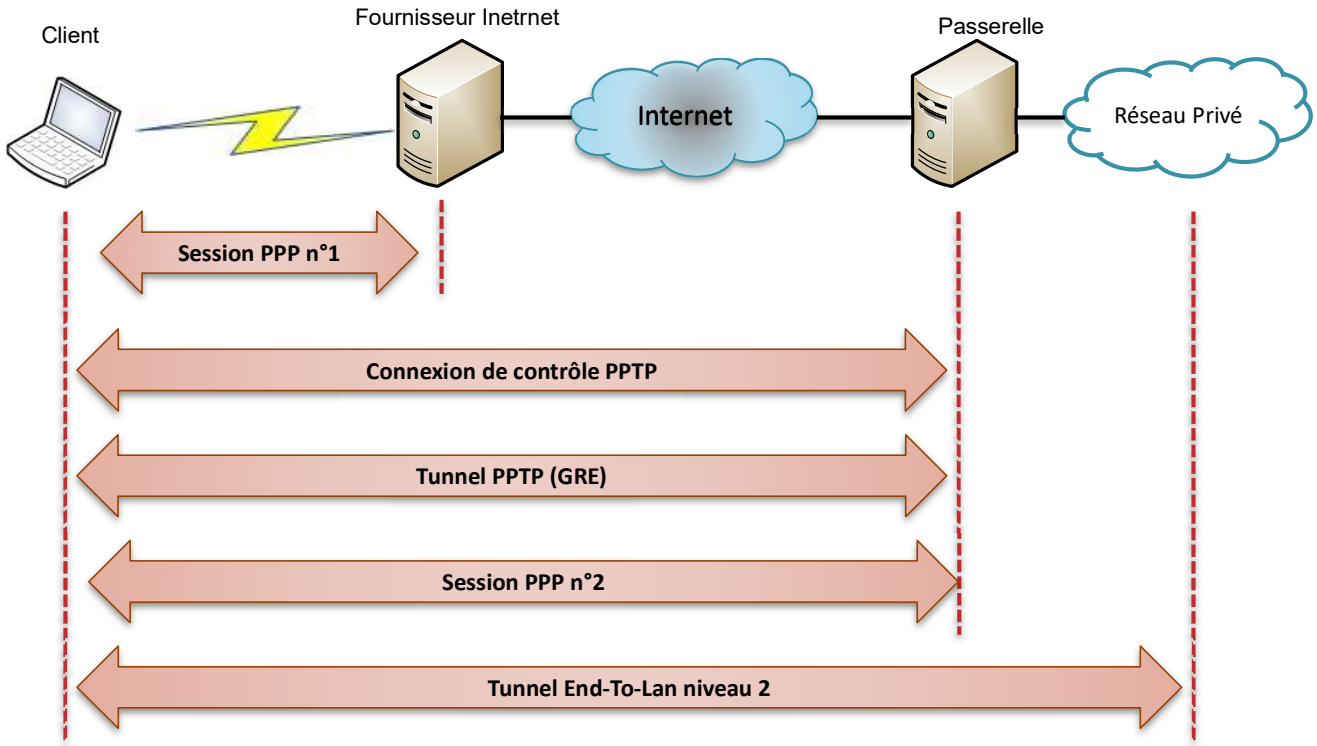



# Initiation générique d'une session TLS

6. après vérification du certificat et authentification de la valeur précédente, le client choisit à son tour une valeur éphémère qu'il chiffre à l'aide de la clé publique du certificat puis transmet dans un ClientKeyExchange ;
7. le client signale l'adoption de la suite négociée avec un ChangeCipherSpec ;
8. le client envoie un Finished, premier message protégé selon la suite cryptographique avec les secrets issus de l'échange de clés éphémères précédent ;
9. le serveur signale l'adoption de la même suite avec un ChangeCipherSpec ;
10. le serveur envoie à son tour un Finished, son premier message sécurisé.

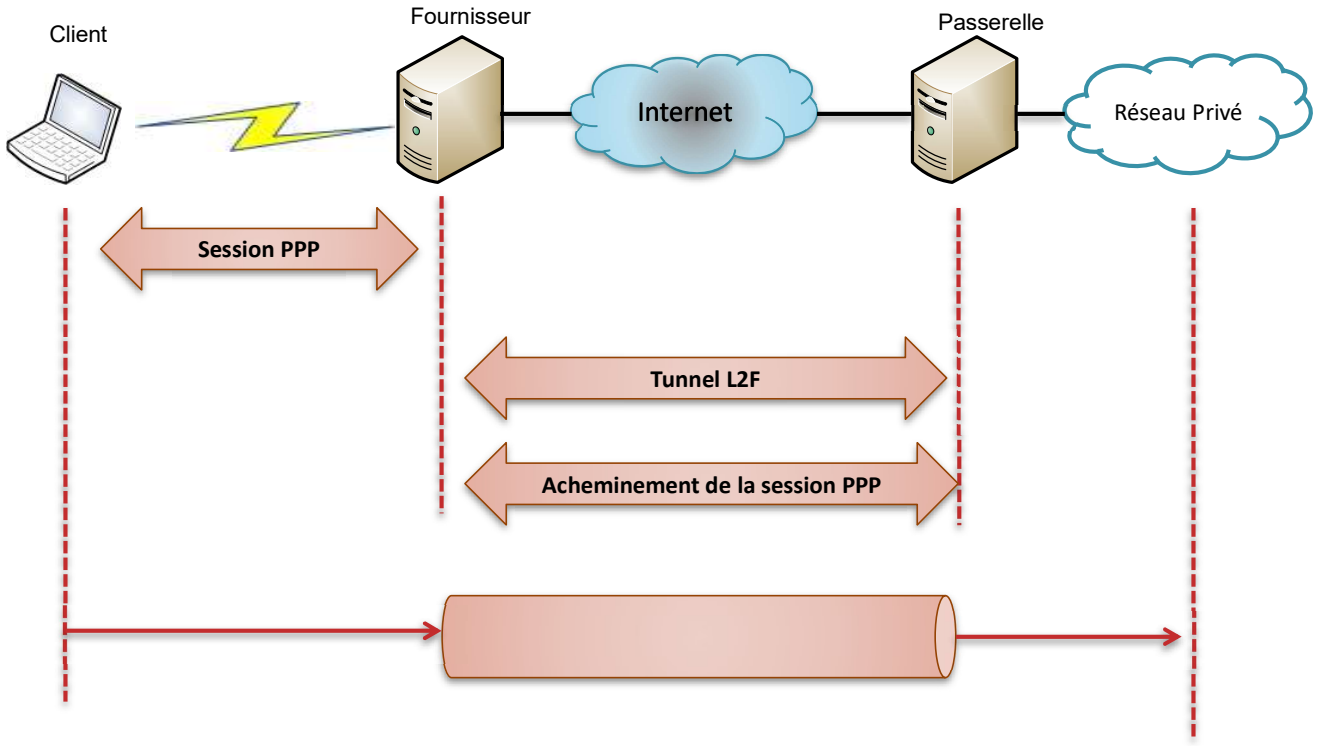


# Sécurisation d'un réseau :VPN PPTP





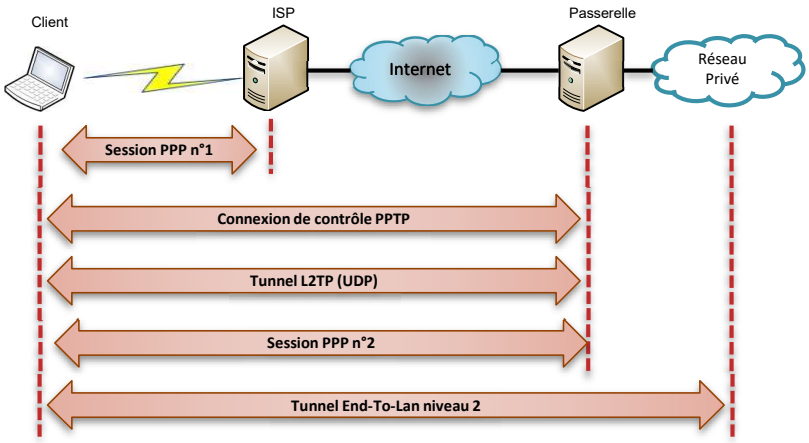

# Sécurisation d'un réseau :VPN L2F

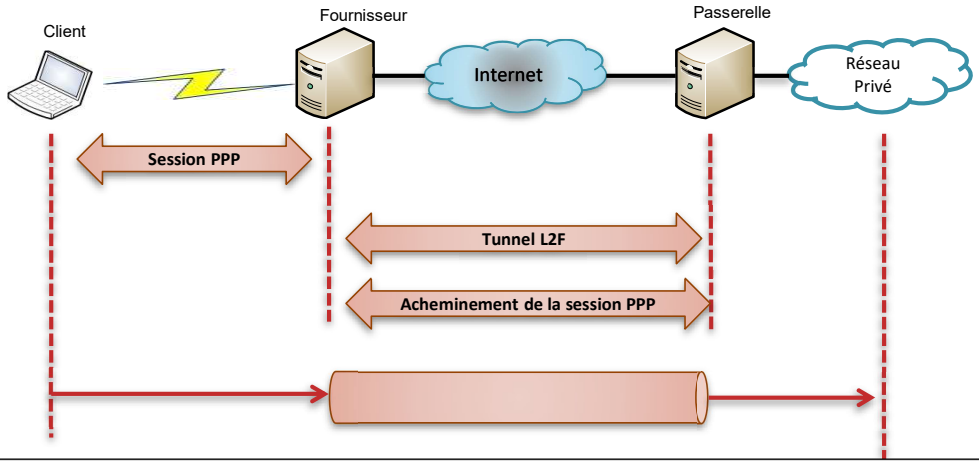



- Le fournisseur d'accès doit s'équiper du matériel compatible L2F (Cisco!)

# Sécurisation d'un réseau :VPN L2TP

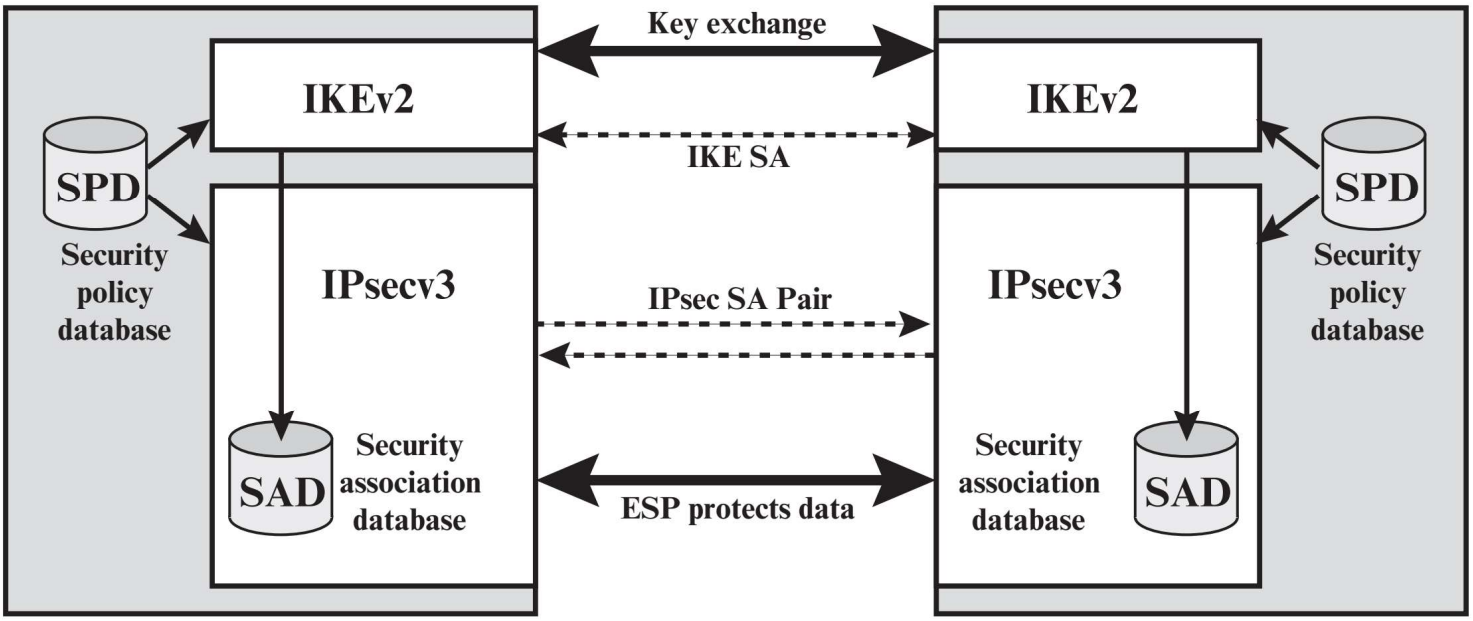
L2TP (Layer 2 Tunneling Protocol) est la combinaison entre les PPTP et L2F.



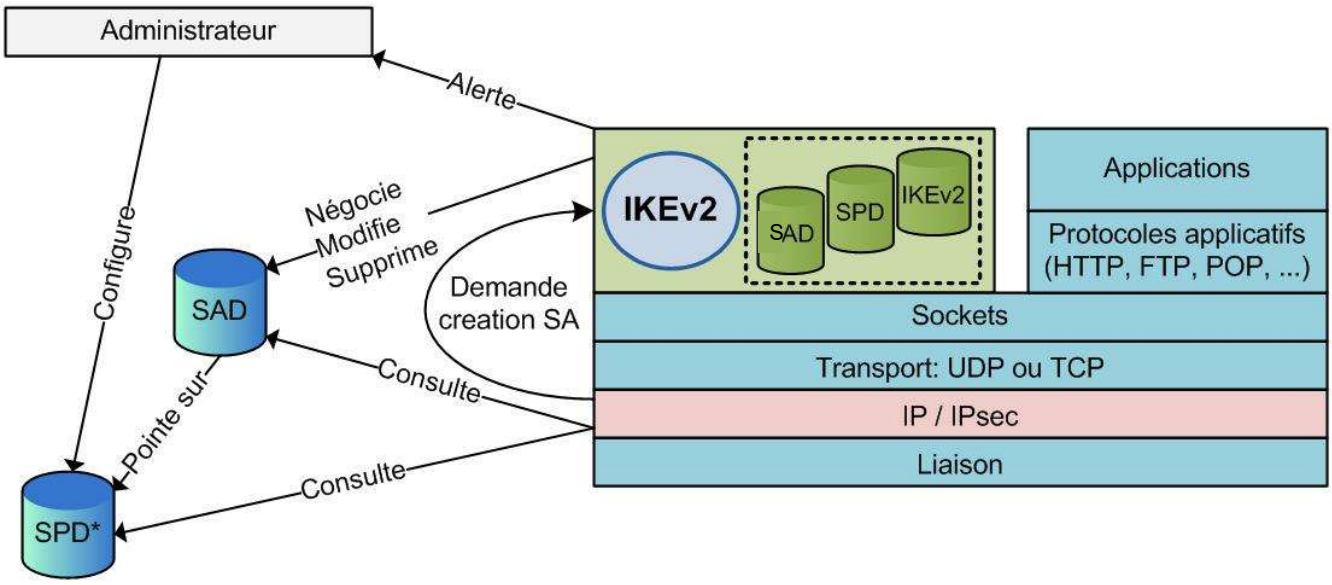






# Architecture IPsec



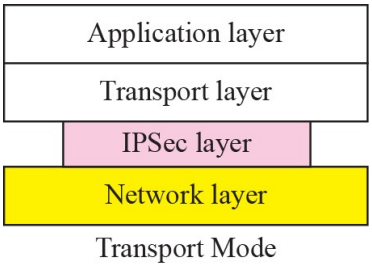
# IPSec : utilisation des bases



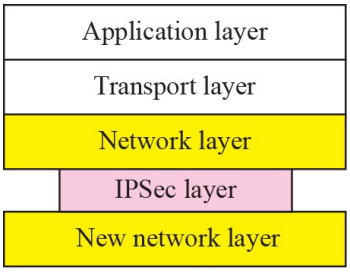



# IPSec : modes

- Mode **Transport** :
  - Protection du trafic IP point à point
  - Peut-être implémenté sur tous les équipements (ordinateurs, serveurs, routeurs, …etc)
- Mode **Tunnel** :
  - Le paquet IP initial est encapsulé dans un nouveau paquet protégé
  - Permet de protéger les communications entre deux réseaux (réseaux privés) ou entre une machine et un réseau (accès distant)



Transport Mode



Tunnel Mode

# Sécurisation d'un réseau

## *Segmentation*

Un principe majeur de la Sécurité est celui du **moindre privilège :**

On ne doit donner les droits d'accès à une ressource qu'aux seules personnes/entités ayant un besoin légitime d'y accéder.

Appliqué au domaine réseau, il est donc fait **recours à de la segmentation** afin de séparer le réseau en différentes zones.

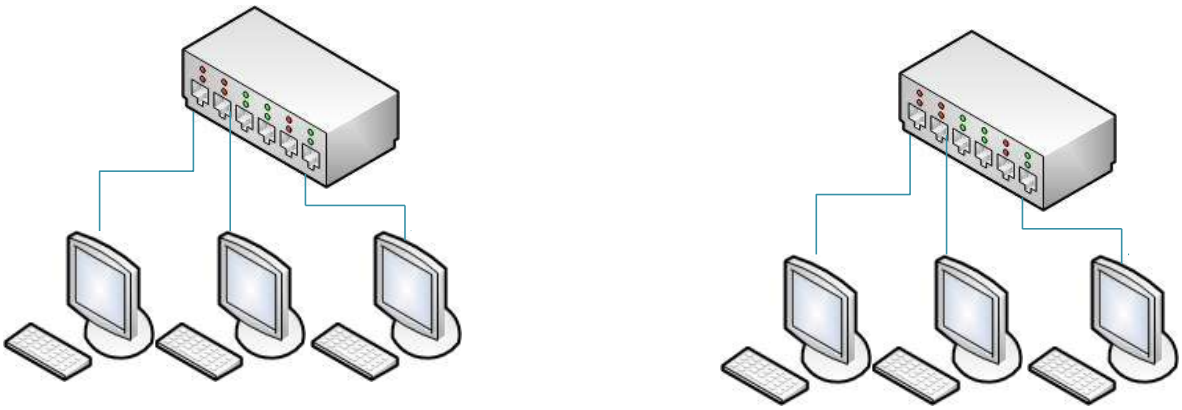
Les droits d'accès à ces zones doivent ensuite être **filtrés** afin de n'autoriser que les flux nécessaires entre chaque zone.



# Sécurisation d'un réseau

## *Segmentation*

Il existe plusieurs techniques pour procéder à de la segmentation. La technique la plus évidente : implémenter deux réseaux distincts non connectés.



Implémentation de deux réseaux physiques différents, non connectés.

Avantage : **étanchéité réseau parfaite** (aucune communication possible entre ces deux zones).
Inconvénient : adapté à certains réseaux très sensibles seulement, **peu adapté aux réseaux d'entreprise** qui ont besoin de communiquer.

# Sécurisation d'un réseau

## *Segmentation*

Autre technique de segmentation : **VLAN** (Virtual LAN).

Les VLAN sont des **réseaux virtuels implémentés par les switches**. Ceux-ci **restreignent la communication entre systèmes selon des règles configurées** sur l'équipement réseau :

- La segmentation peut se faire grâce aux ports Ethernet de chaque switch.
- La segmentation aussi se faire grâce aux adresses MAC des systèmes.
  - Attention : les adresses MAC des cartes réseaux pouvant facilement être modifiées par les utilisateurs, le filtrage sur les adresses MAC est à considérer – logiquement – avec précaution car le niveau de sécurité effectif est limité.