# Sécurité

## Sécurité des Systèmes d'Information
## Concepts, Organisation, Outils et Tendance

J. Saraydaryan

CPE - Lyon

# Sécurité des Réseaux

Sécurité des Systèmes d'information
Concepts, Organisation, outils et Tendance

J. Saraydaryan

CPE - Lyon

# Sécurité des Réseaux

I Rappel des concepts réseaux

II Les menaces sur les réseaux

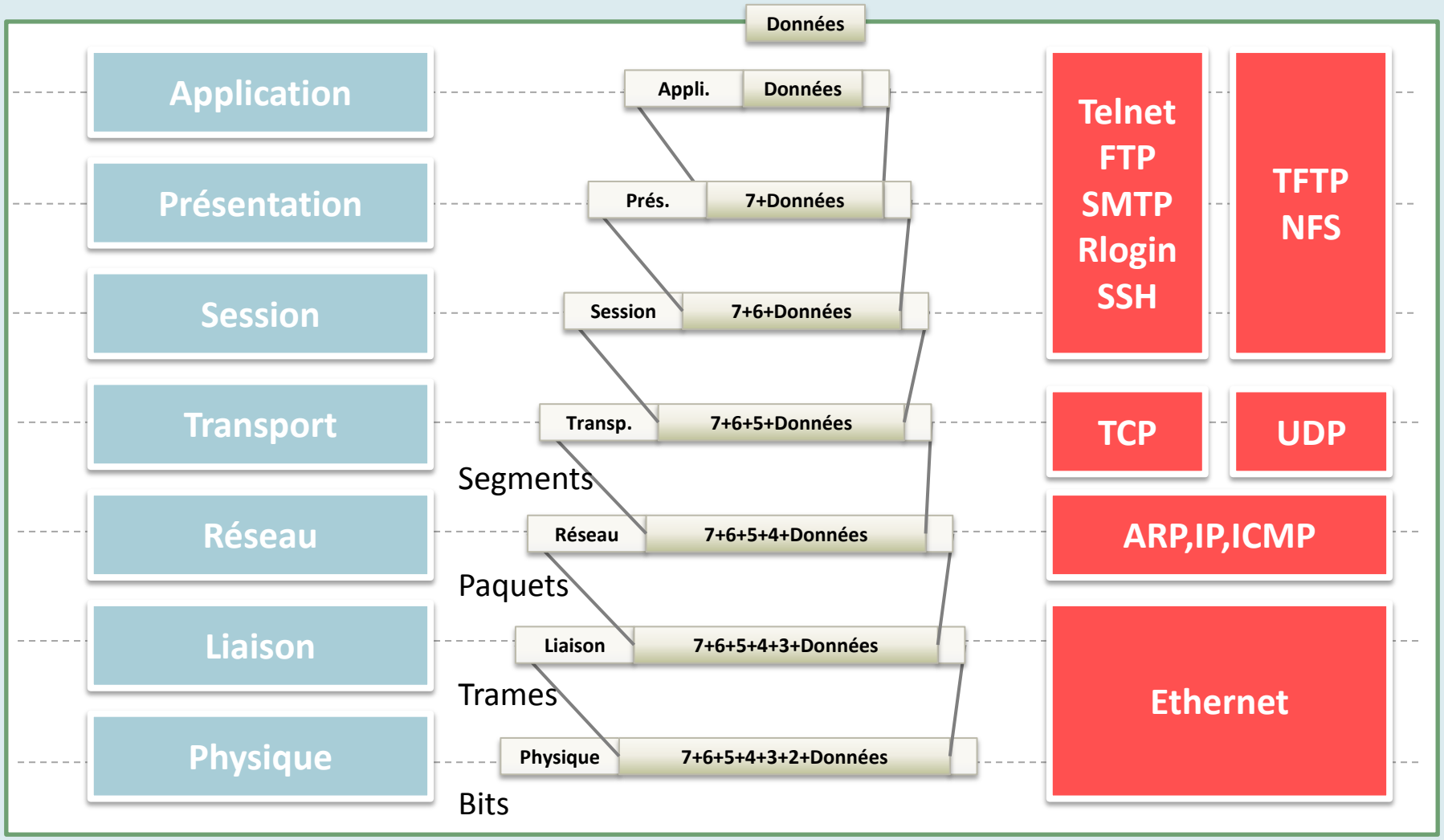
III La protection des réseaux

IV Contrôler sa sécurité

# Rappel des concepts réseaux

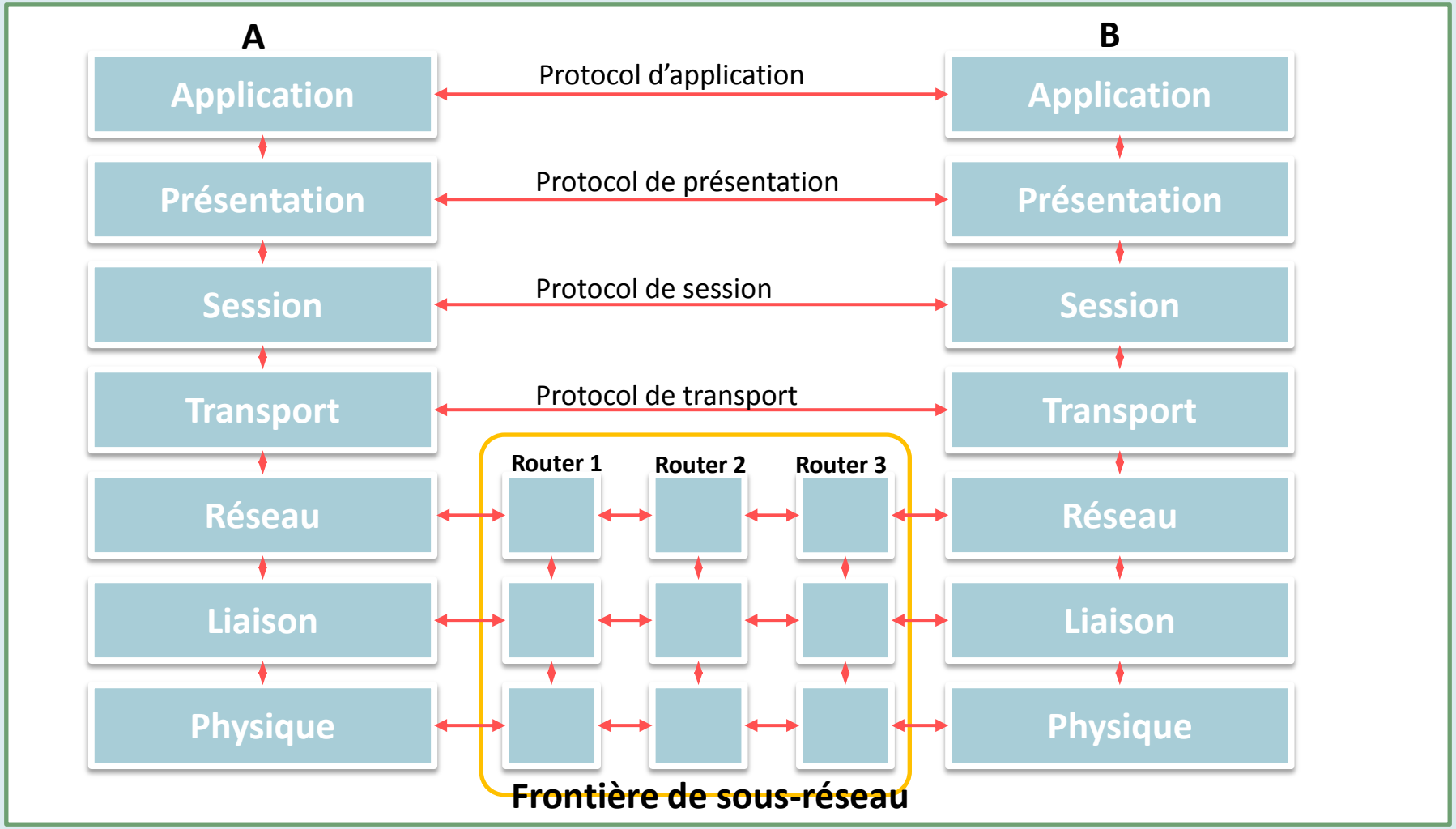
# Sécurité des Réseaux

- **Couches Réseaux**



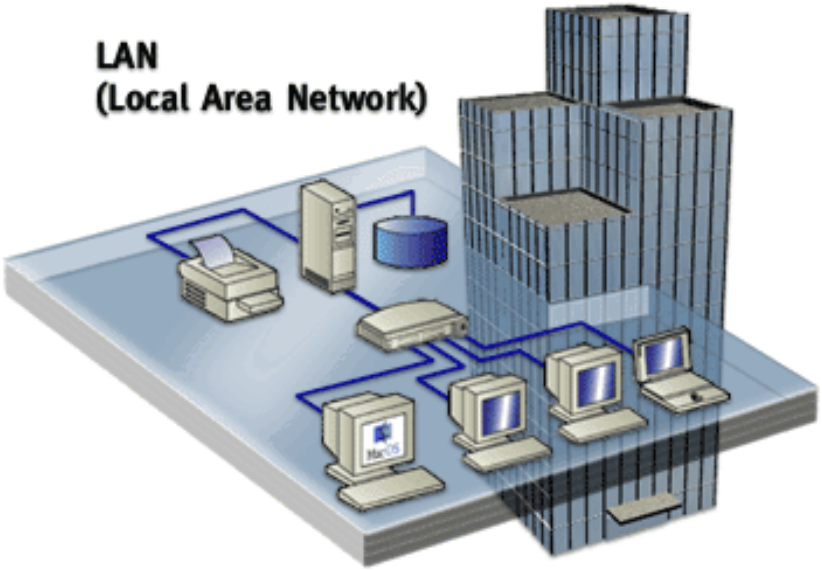
# Sécurité des Réseaux

- **Couches Réseaux**

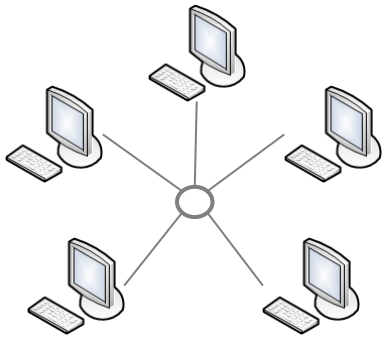


# Sécurité des Réseaux

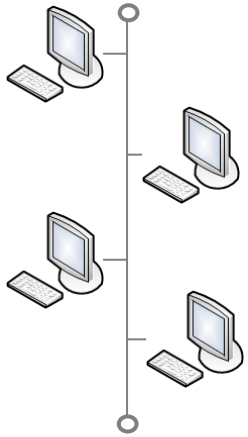
- **Local Area Network**



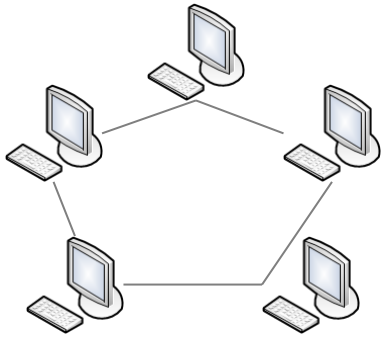

http://www.felinux.com.br/



Star



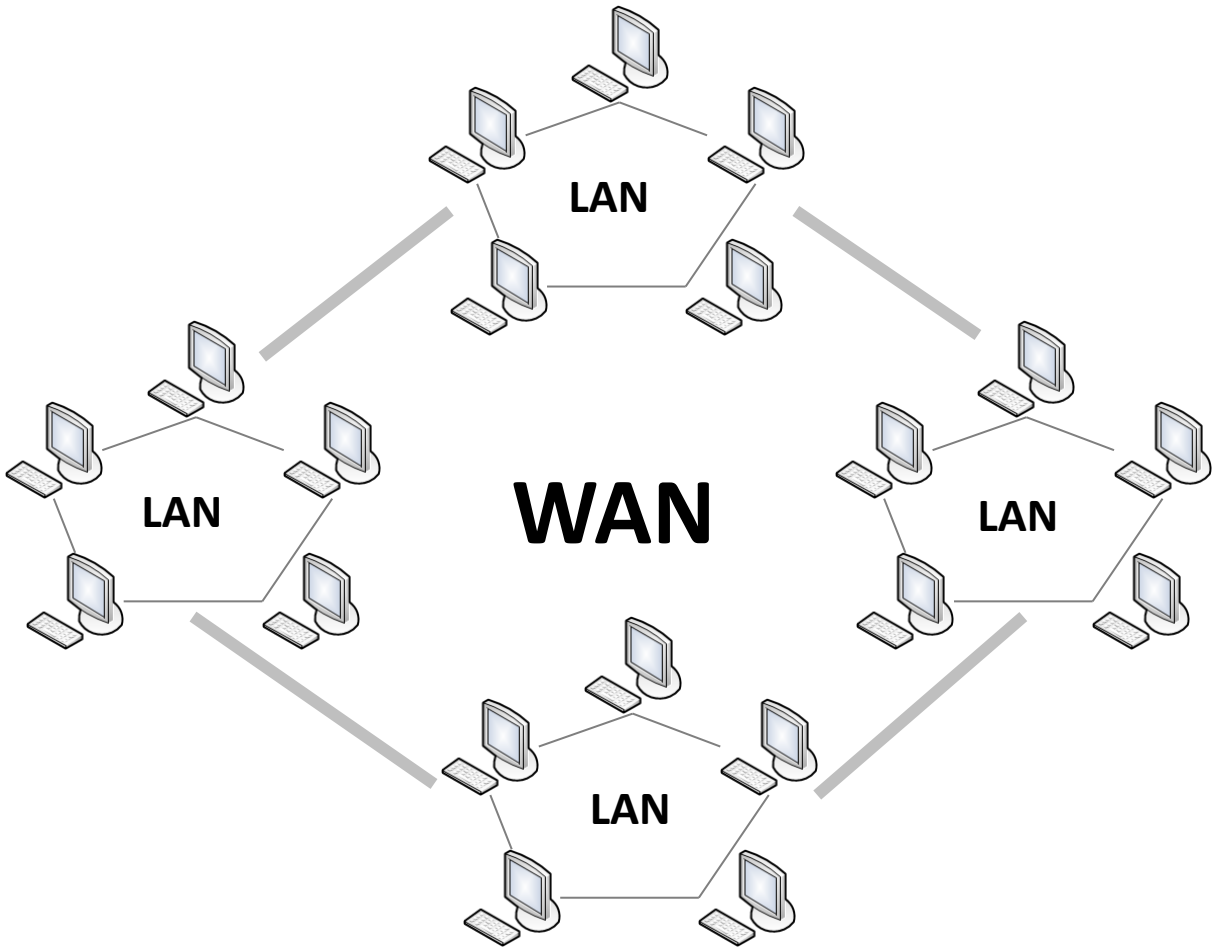
Bus



Ring

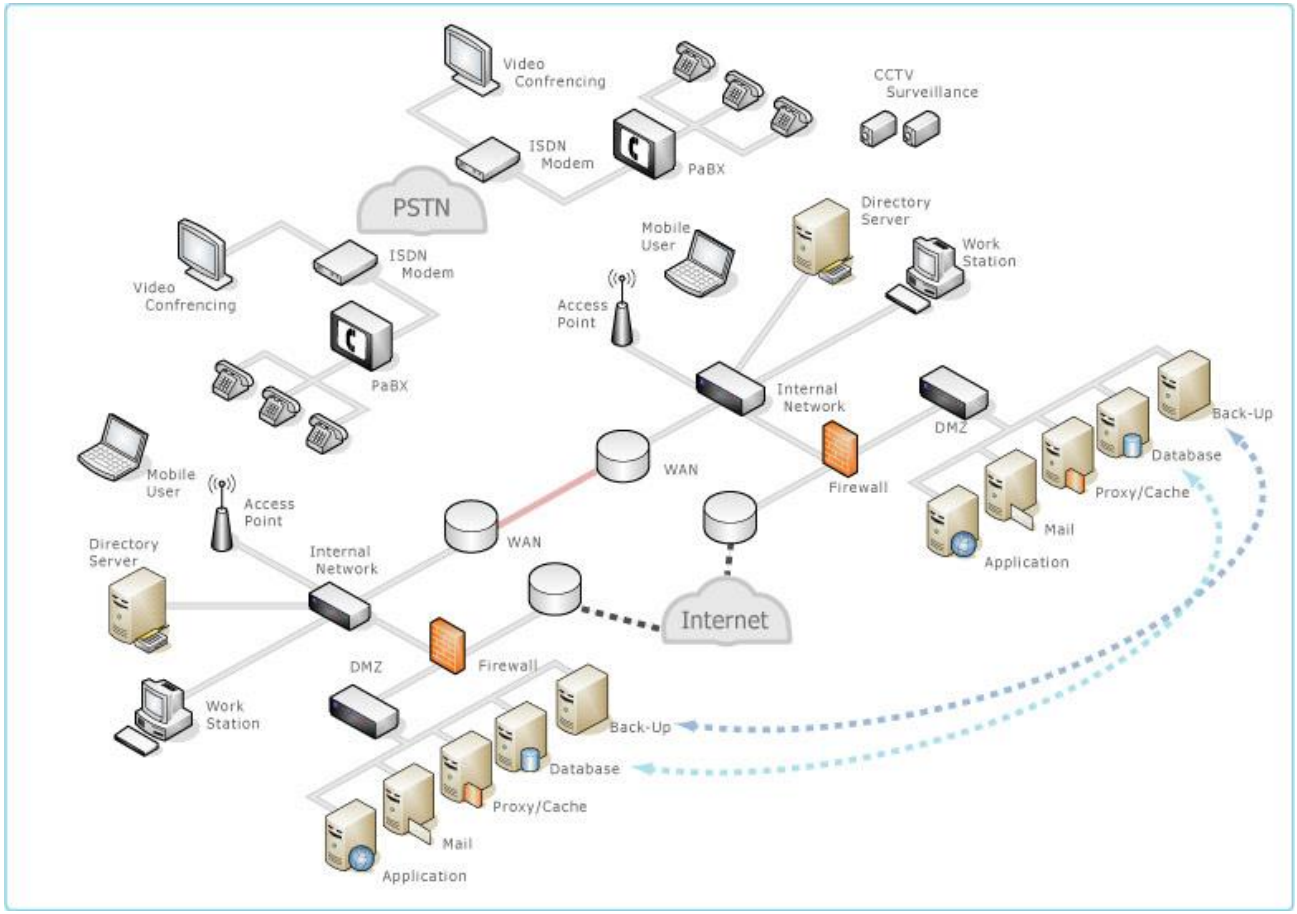
# Sécurité des Réseaux

- **Wide Area Network**



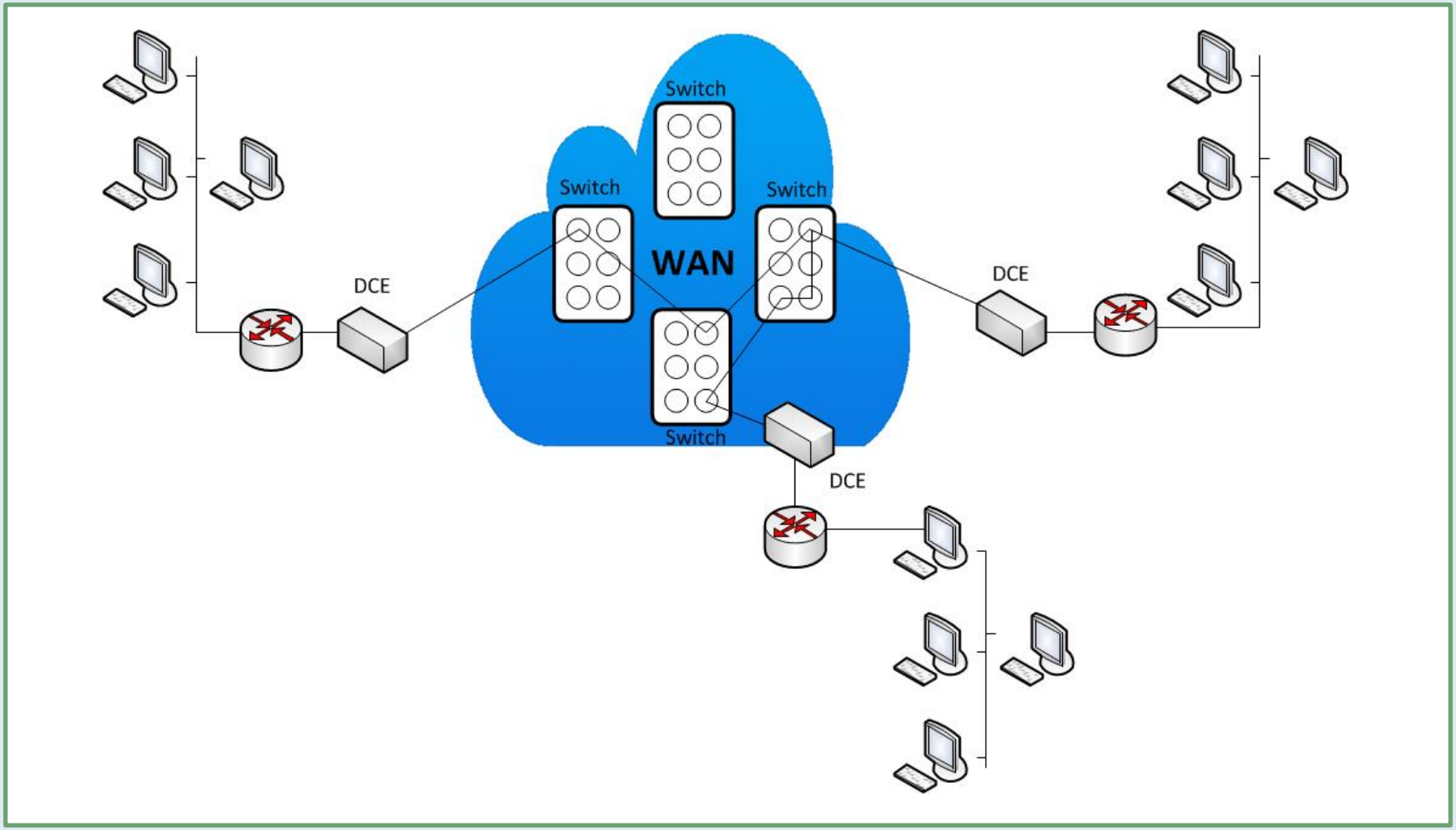
# Sécurité des Réseaux

- **Wide Area Network**



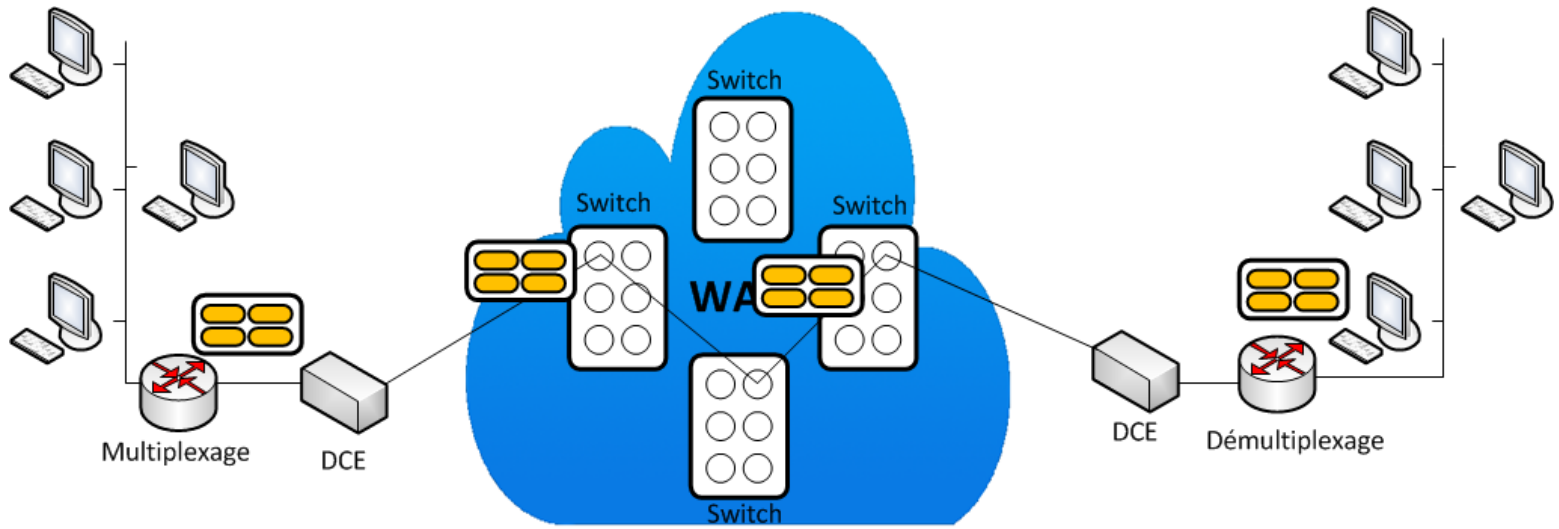
# Sécurité des Réseaux

- **Circuit Switching**



# Sécurité des Réseaux

- **Packet Switching**

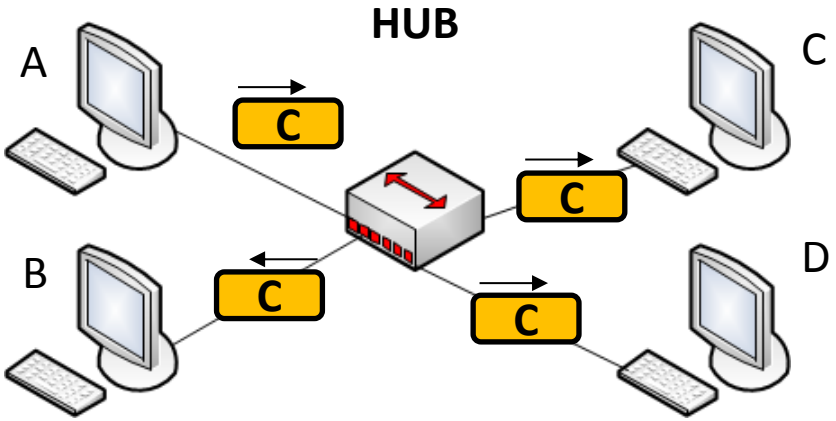


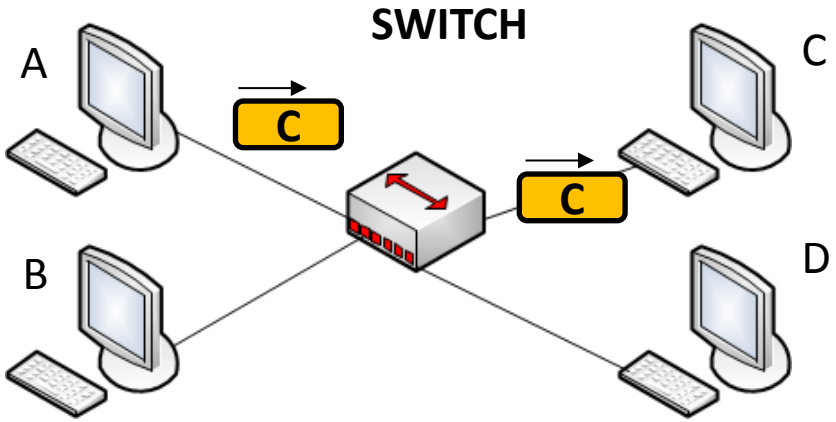
# Sécurité des Réseaux

- **Rappel des concepts réseaux**
  - **Les équipements**
    - Hub
    - Switch
    - Gateway
    - Router
  - Les services
    - DHCP
    - DNS

# Sécurité des Réseaux

- **Les équipements (1/3)**

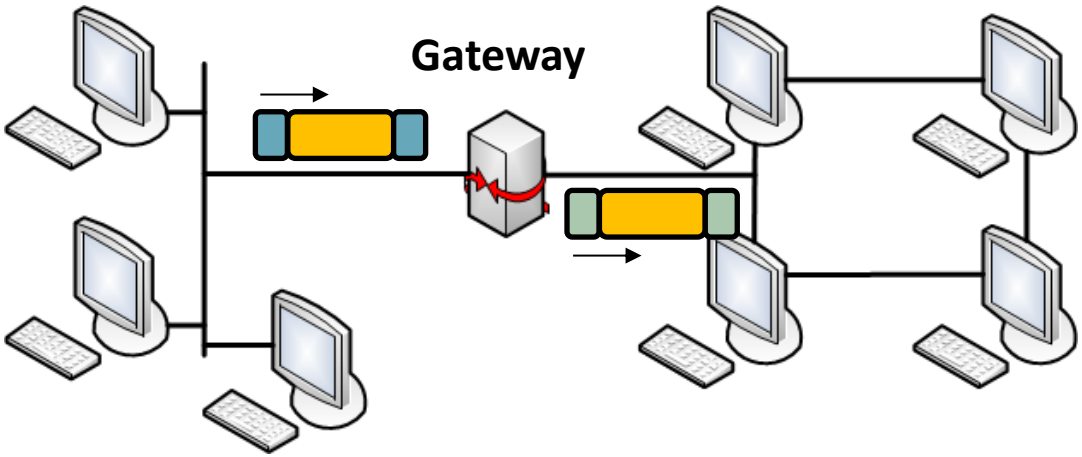



| Mac | Port |
|---|---|
| A | 1 |
| B | 2 |
| C | 3 |
| D | 4 |

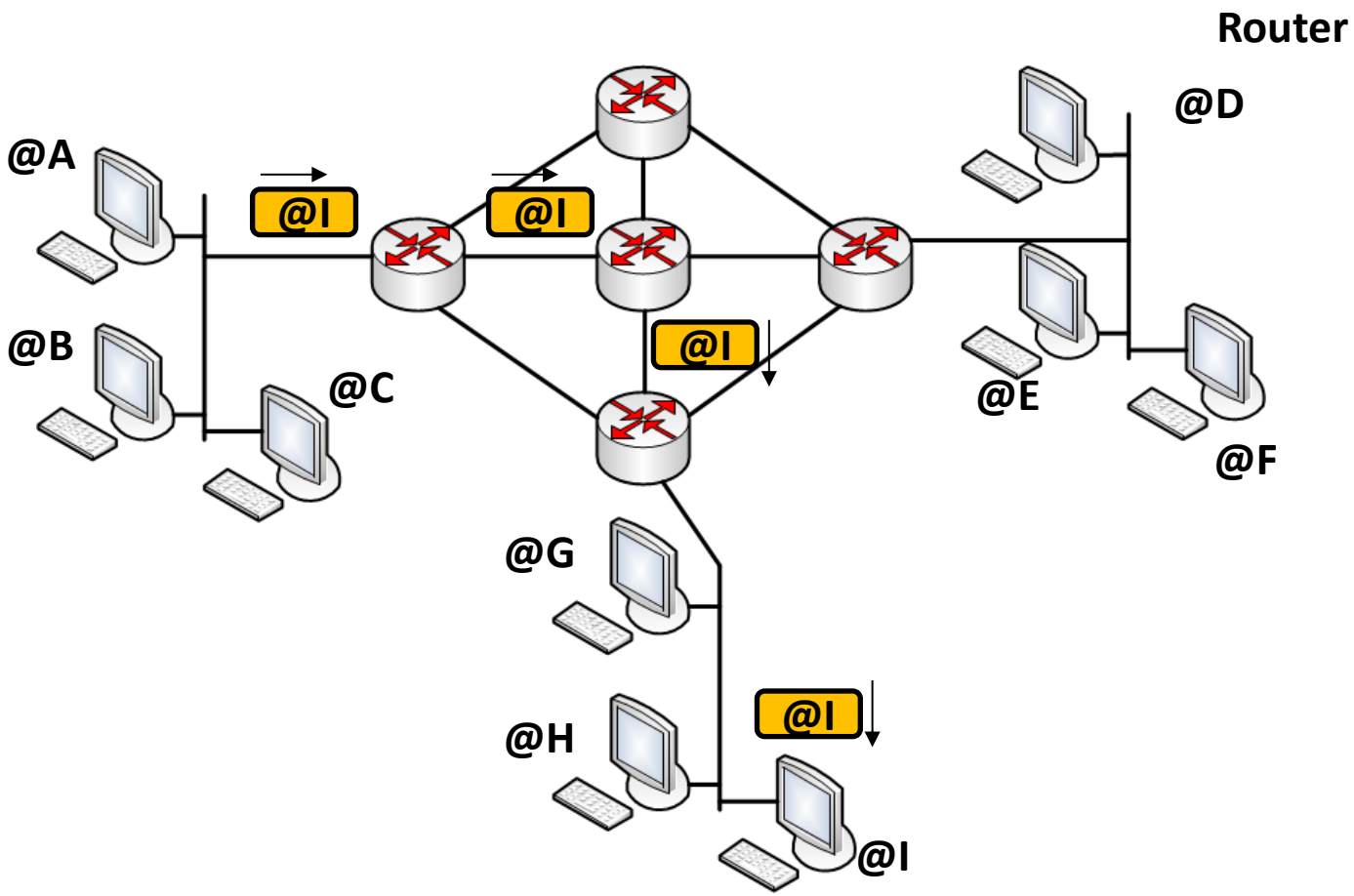
# Sécurité des Réseaux

- **Les équipements (2/3)**



# Sécurité des Réseaux

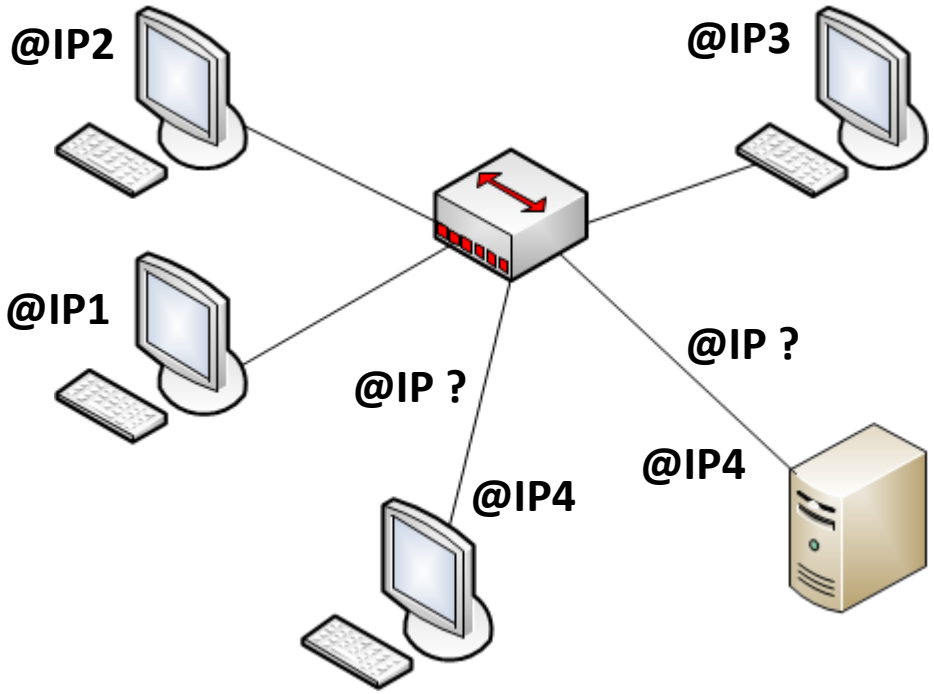
- **Les équipements (3/3)**



# Sécurité des Réseaux

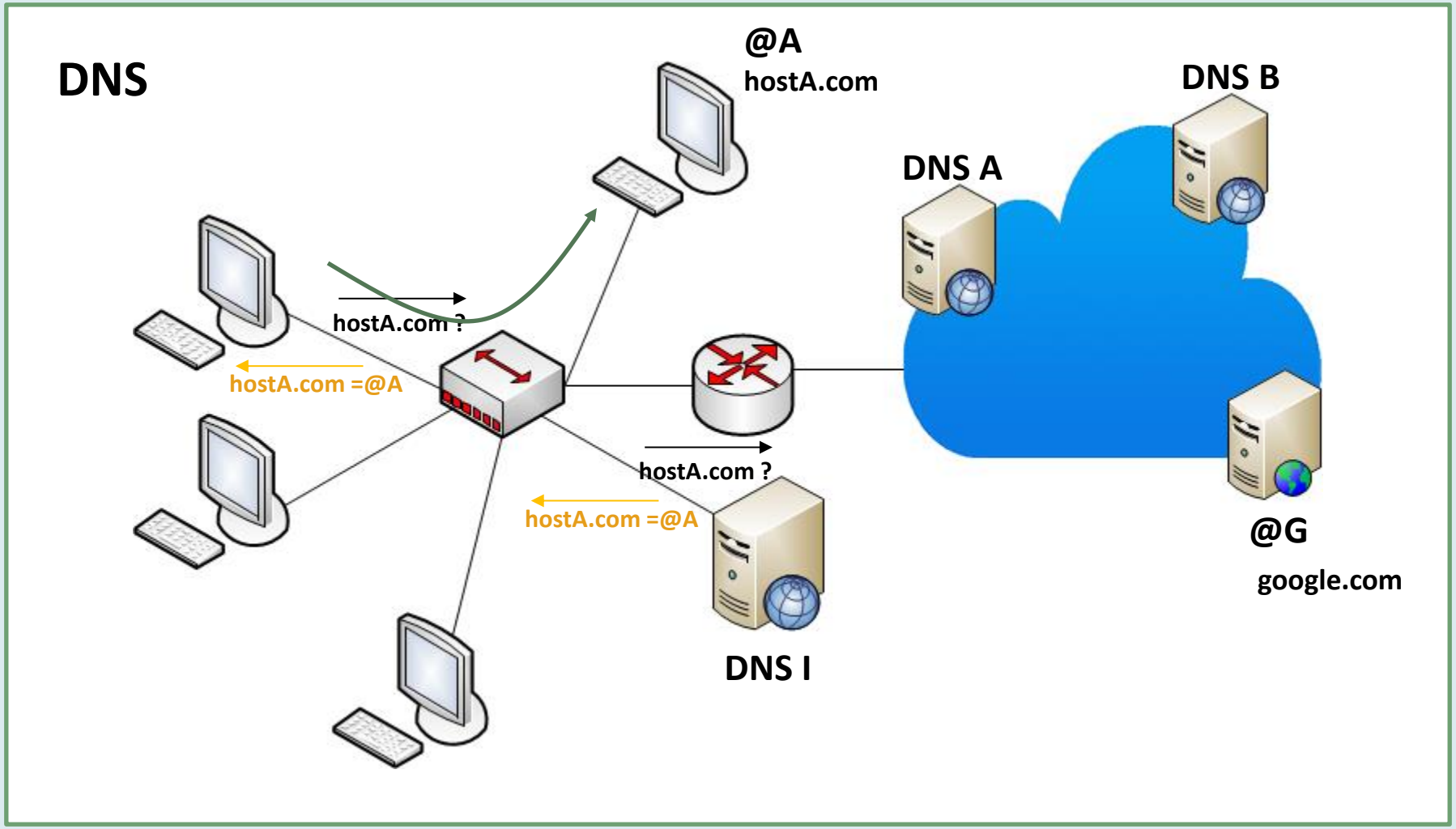
- **Les services (1/2)**

## DHCP



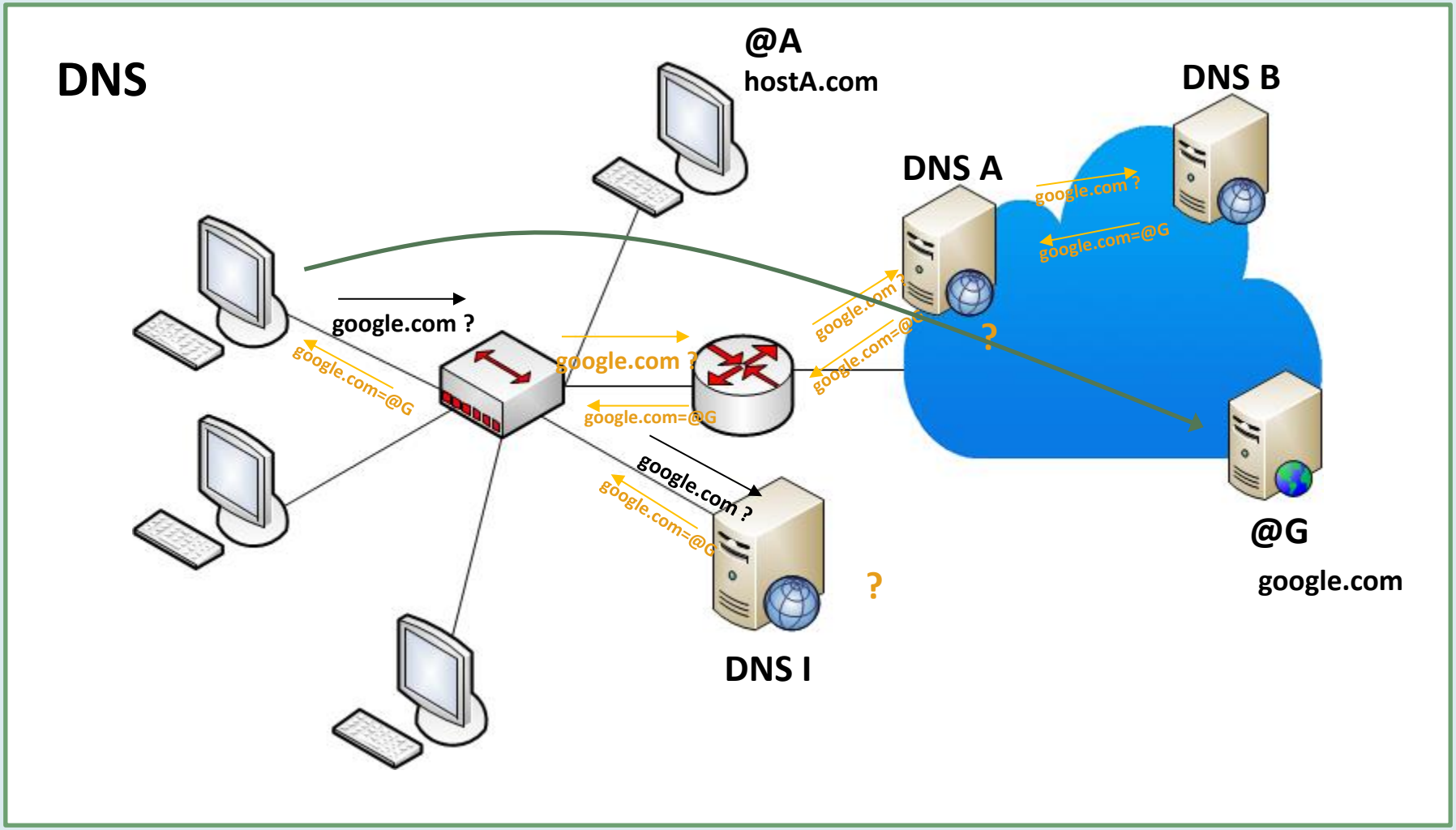
# Sécurité des Réseaux

- **Les services (2/2)**



# Sécurité des Réseaux

- **Les services (2/2)**



# Les menaces sur les réseaux

# Sécurité des Réseaux

- **Les menaces sur les réseaux**
  - Objectif des réseaux d'information

    *Communiquer avec d'autres services, systèmes, personnes locales ou distantes*
  - Constats sur les protocoles

    Protocoles de communication initialement conçus pour facilité la communication, l'échange et le partage de données et de services

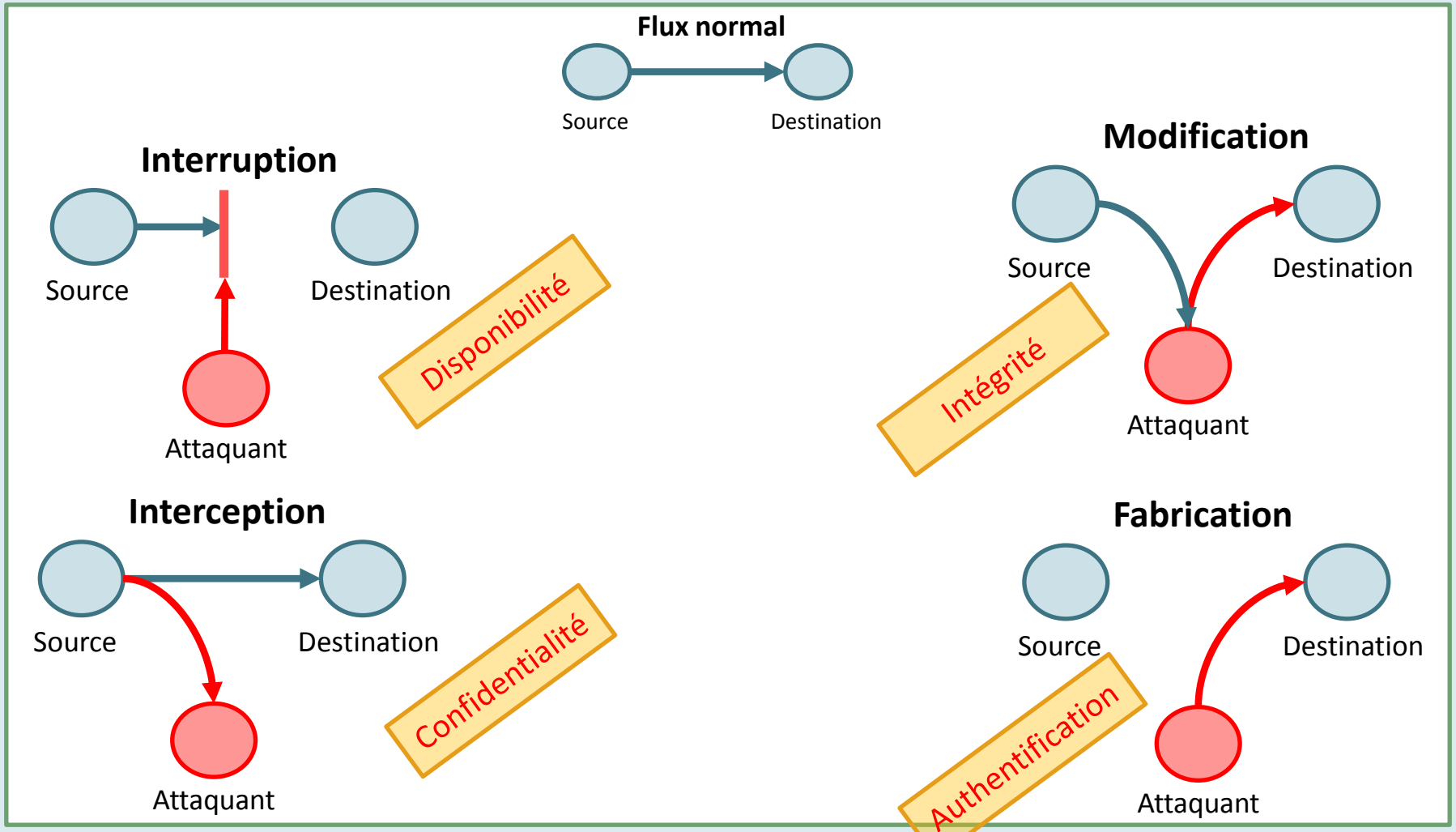
→ Pas de gestion de la confidentialité et de l'intégrité des données de facto

# Sécurité des Réseaux

- **Quelles sont les menaces ?**
  - Interruption : perte de disponibilité
  - Interception: (perte de confidentialité)
  - Modification (perte d'intégrité)
  - Fabrication (perte d'authentification)

# Sécurité des Réseaux

- **Quelles sont les menaces ?**

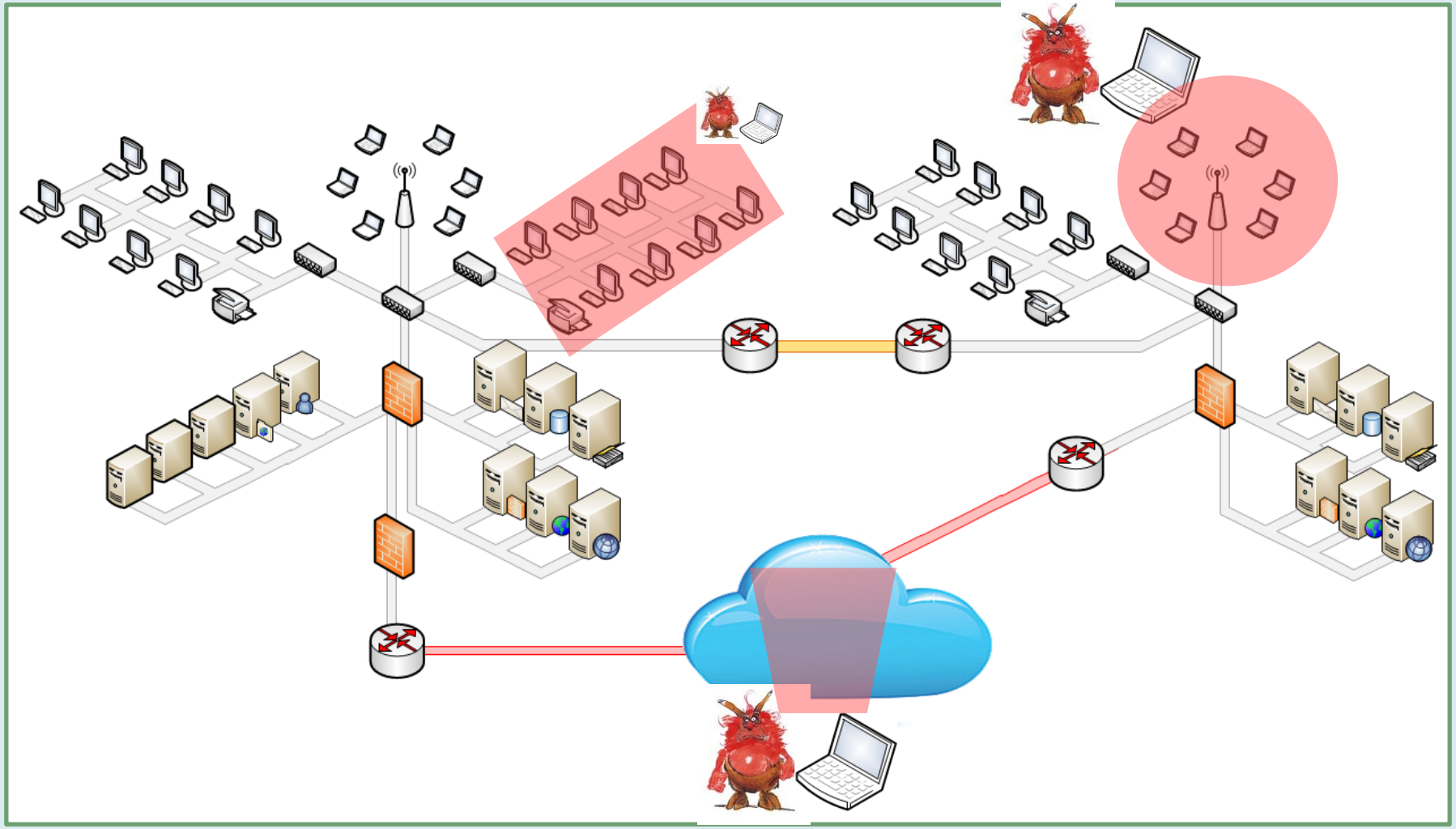


# Sécurité des Réseaux

- **Quelques exemples de menaces**
  - Sniffing
  - Collecte d'information
  - Interception, Modification de données
  - Usurpation d'identité
  - Denis de service

# Sécurité des Réseaux

- **Sniffing**

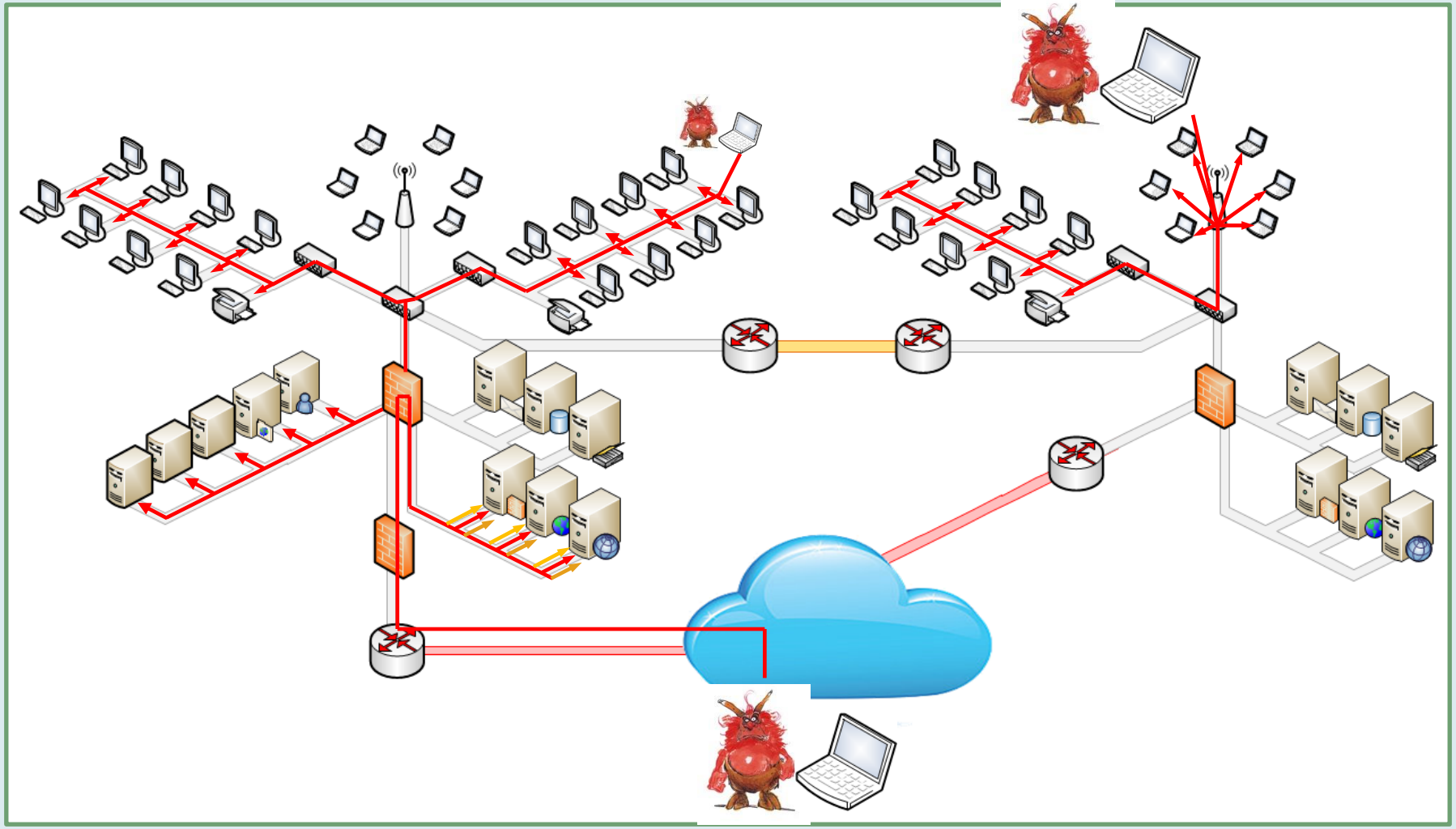


# Sécurité des Réseaux

- **Quelques exemples de menaces**
  - Sniffing
    - Collecte d'information confidentielle
    - Collecte de login mots de passes
    - Collecte d'information sur le systèmes (écoute passive)
      - Adresses MAC
      - Adresses IP
      - Protocoles utilisés
      - Services utilisés

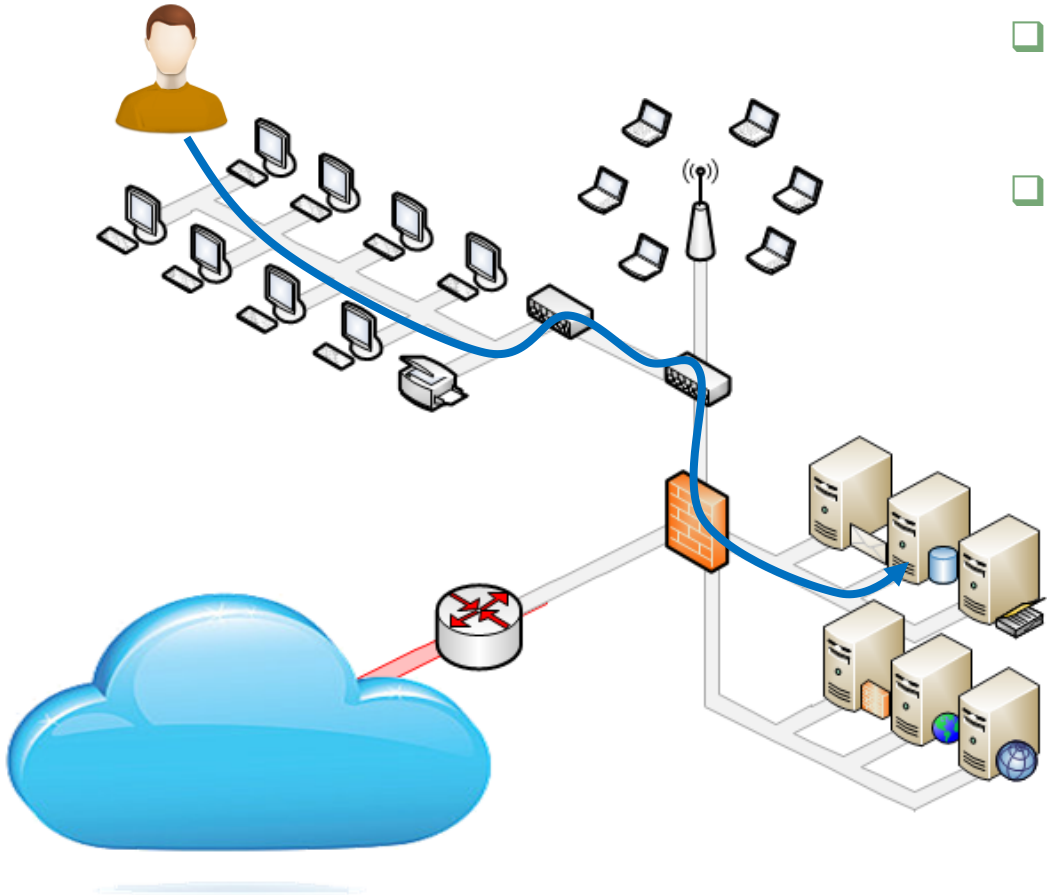
# Sécurité des Réseaux

- **Collecte d'information (active)**



# Sécurité des Réseaux

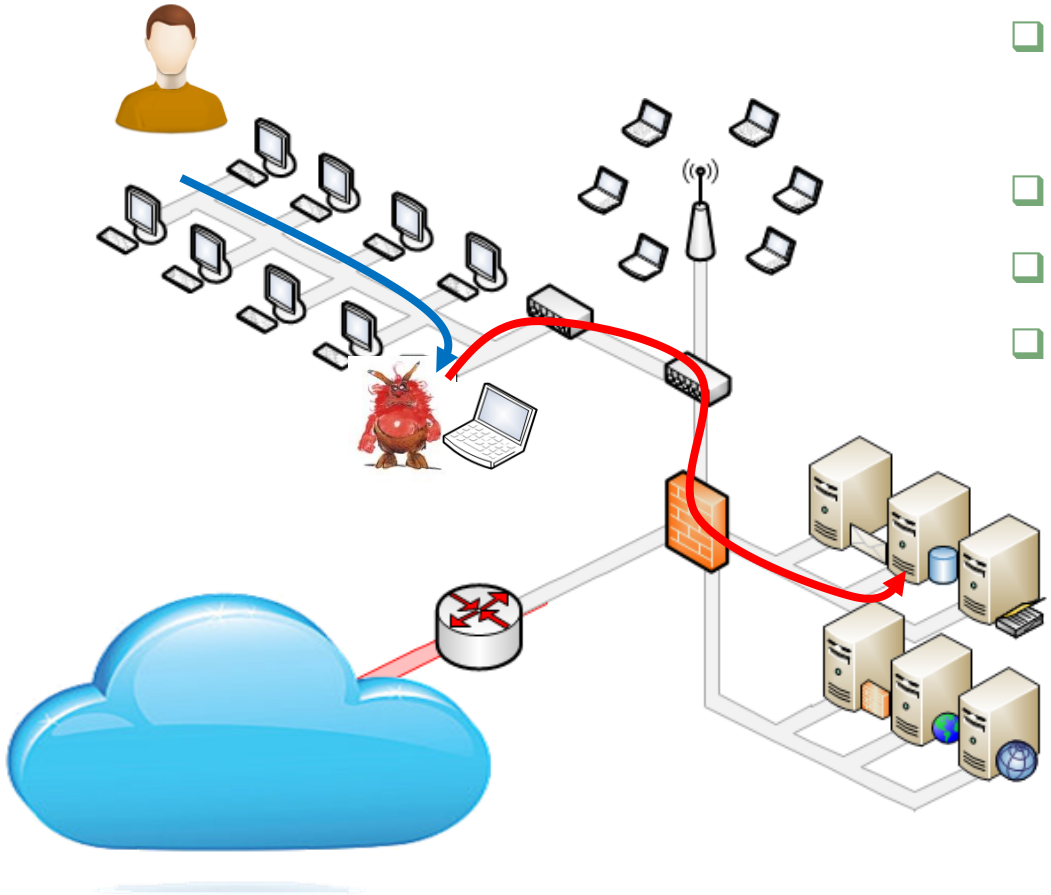
- **Interception / Modification**



- Envoi d'une requête à la base de données
- Requête de mise à jour des salaires des employés

# Sécurité des Réseaux

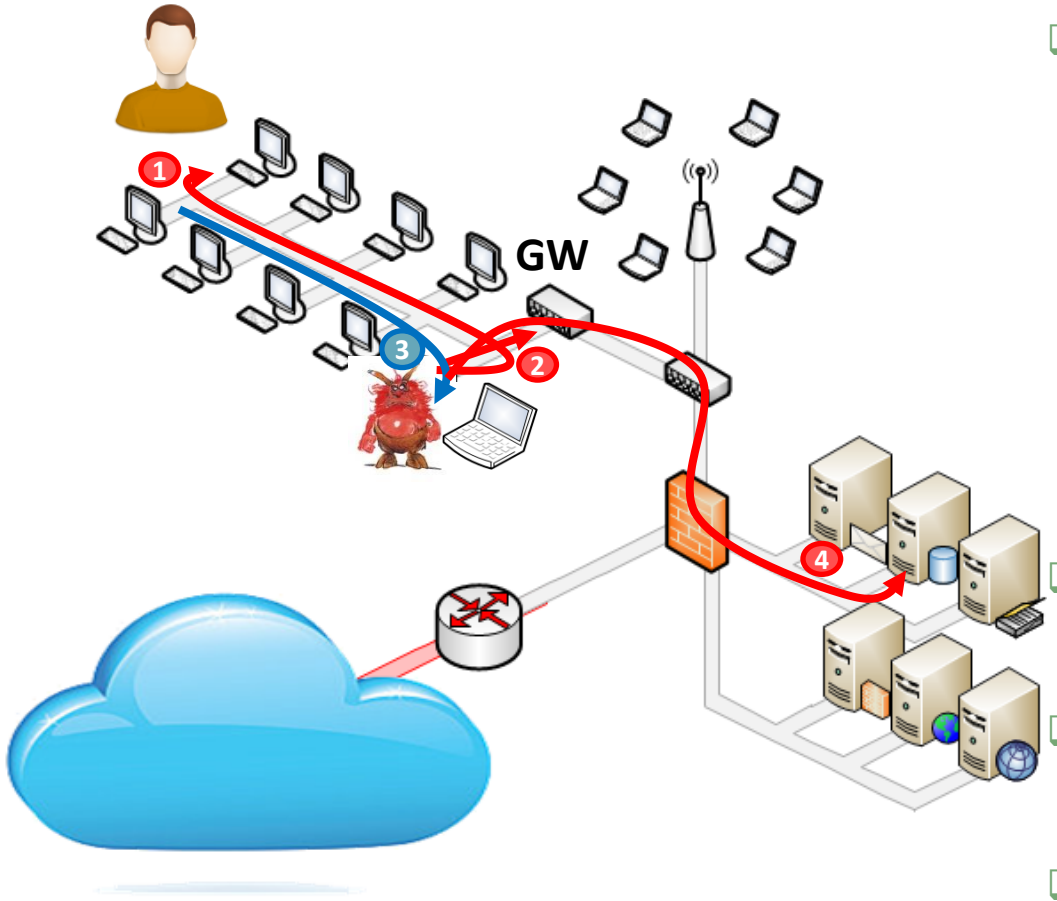
- **Interception / Modification**



- Usurpation d'identité de la base de données
- Récupération des requêtes
- Modification des requêtes
- Envoi des requêtes modifiées

# Sécurité des Réseaux

- **Interception / Modification**




- Usurpation d'identité de la passerelle
  - Attaque ARP de la machine de l'utilisateur (je suis la passerelle)
  - Attaque ARP de la passerelle (je suis utilisateur A)
- Récupération des requêtes de l'utilisateur A
- Modification de la requête de l'utilisateur A
- Envoi des requêtes modifiées

# Sécurité des Réseaux

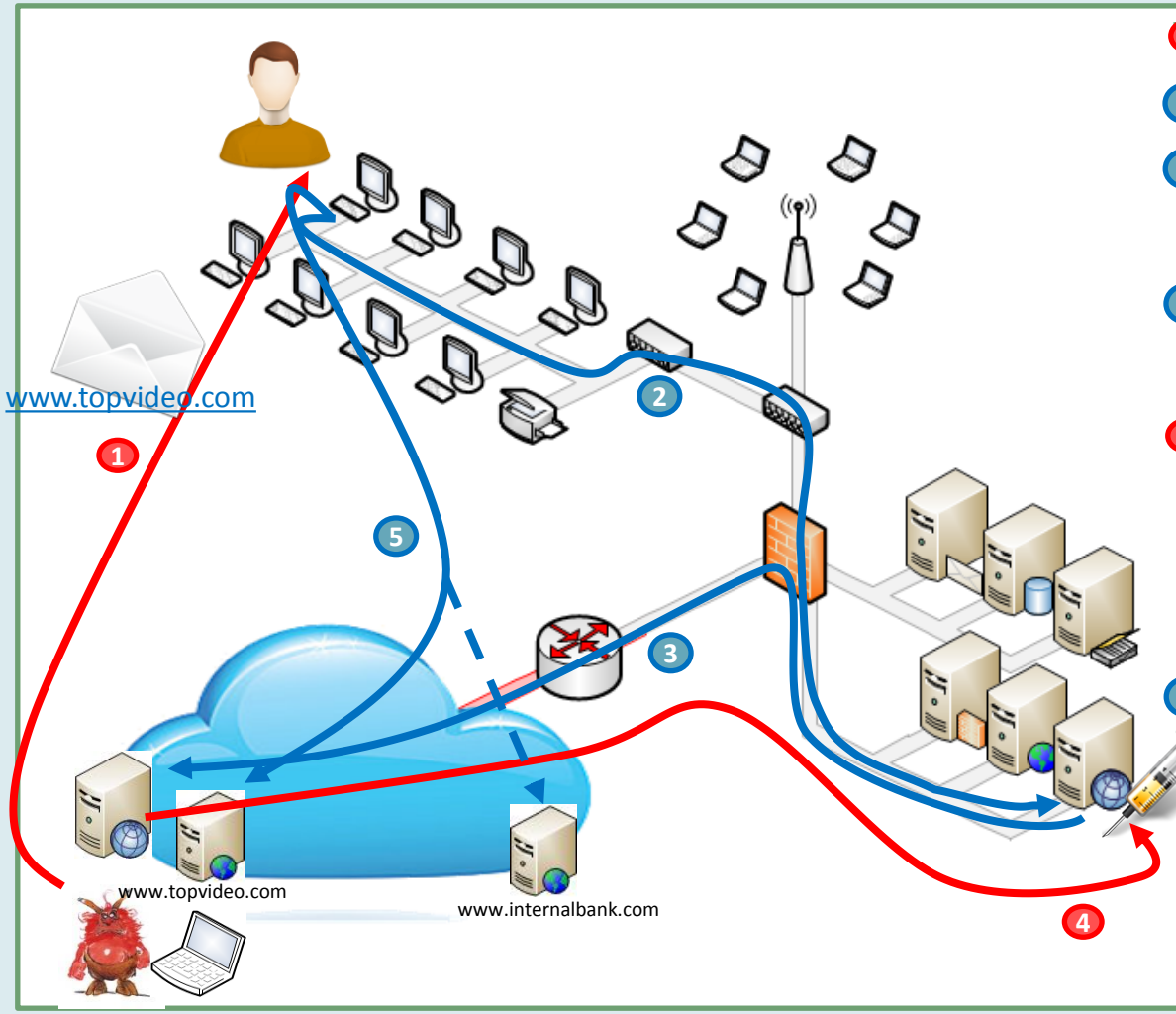
- **Quelques exemples de menaces**
  - Interception/Modification
    - Via session/TCP Hijacking
    - Via usurpation d'identité (arp attack)
    - Particulièrement facile sur un même segment réseau
    - Possible également sur internet

# Sécurité des Réseaux

- **Quelques exemples de menaces**
  - Usurpation d'identité
    - Attaque ARP (usurpation adresse MAC)
    - DNS poisoning (usurpation d'adresse IP)
    - Vol d'identité
      - Login/mot de passe (bruteforce/virus)
      - Certificat (virus, intrusion, fabrication)

# Sécurité des Réseaux

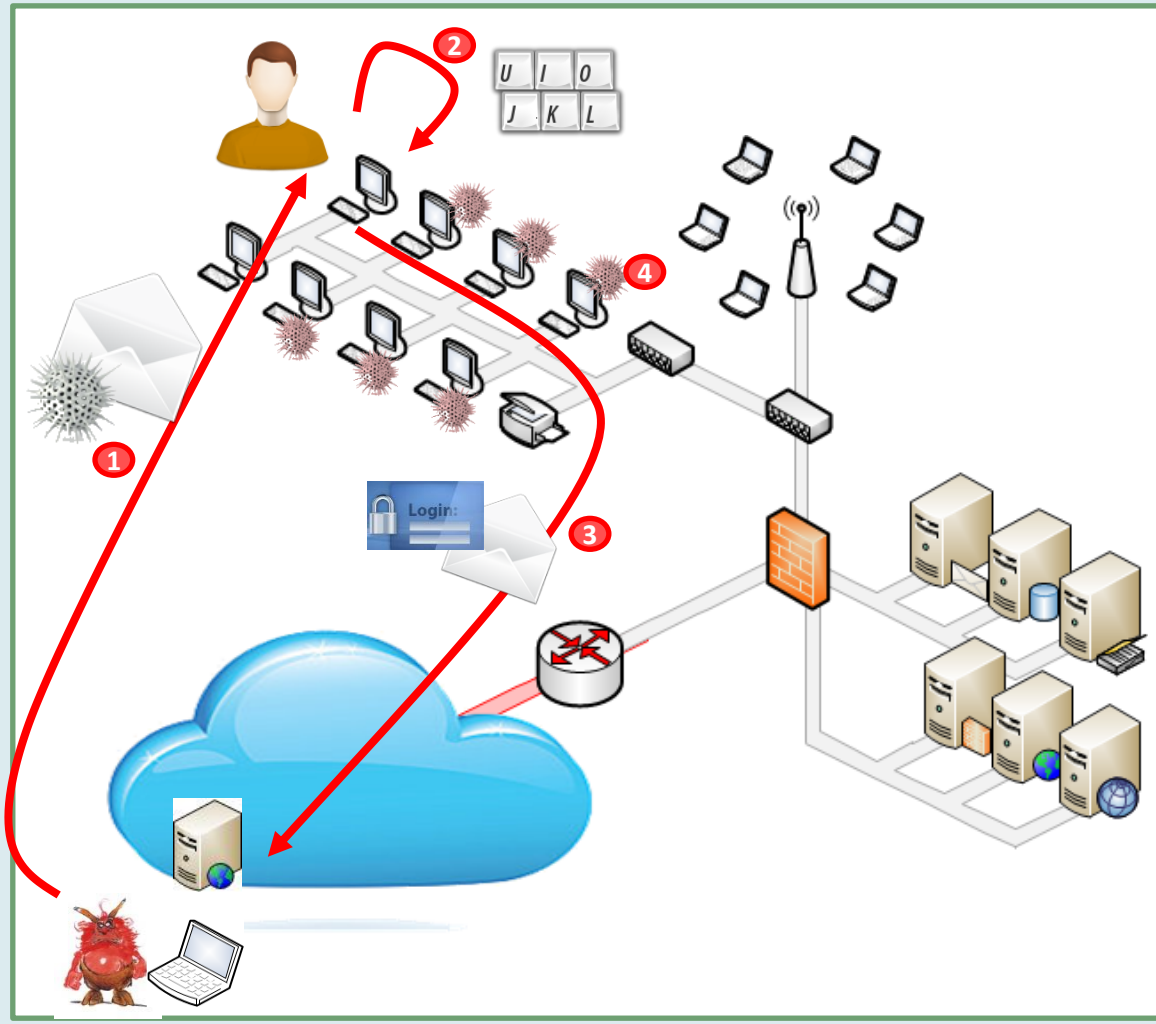
- **Usurpation d'identité (DNS poisoning)**




1. Envoi email attractif
2. Consultation du lien par l'utilisateur
2. Demande de résolution de www.topvideo.com
3. DNS interne retourne la demande au DNS compétent
4. DNS compétant (pirate) renvoie l'IP www.topvideo.com + fausses information (www.internalbank.com=@IPPirate)
5. TOUS utilisateurs souhaitant se rendre sur son site de banque se retrouve sur le site pirate

# Sécurité des Réseaux

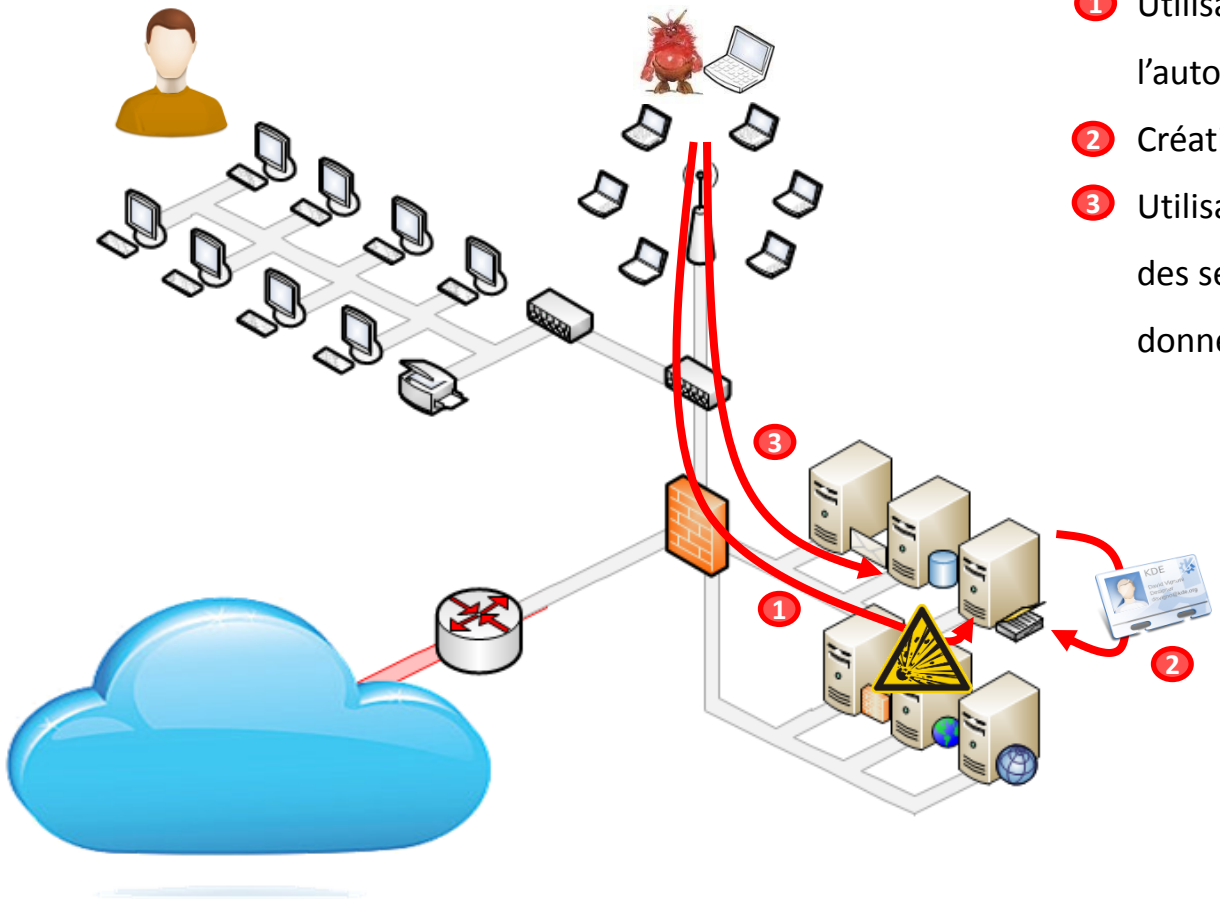
- **Usurpation d'identité (Vol d'identité)**




1. Envoi email vérolé
2. Ouverture du mail, installation du virus (keylogger)
3. Envoi des informations (login/pwd)
4. (Option) Propagation du virus

# Sécurité des Réseaux

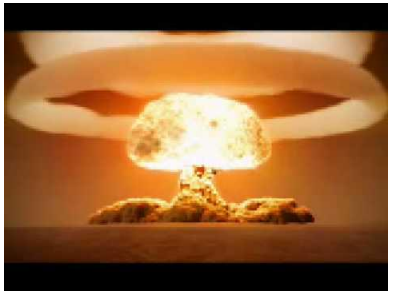
- **Usurpation d'identité (Vol d'identité)**




1. Utilisation d'une vulnérabilité sur l'autorité de certification
2. Création d'un certificat au pirate
3. Utilisation du certificat pour utiliser des services particuliers (base de données)

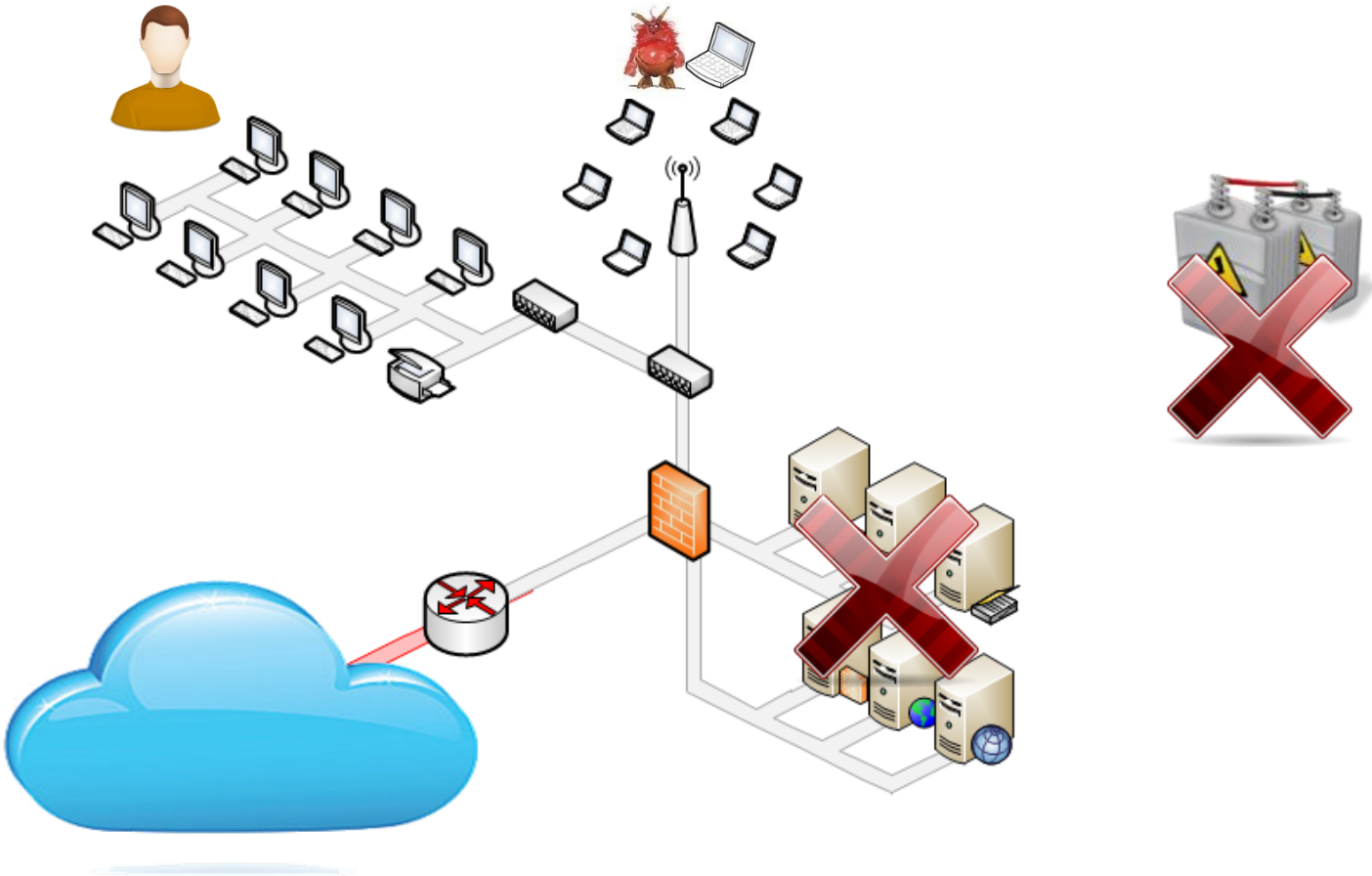
# Sécurité des Réseaux

- **Dénis de service**
  - Attaque physique
    - Coupure électrique
    - EMP
  - Attaque de composant logiciel
    - Exploitation de vulnérabilités du logiciel de l'OS
    - Saturation des communications
  - Attaques réseaux
    - Flooding Réseaux
    - Corruption DNS



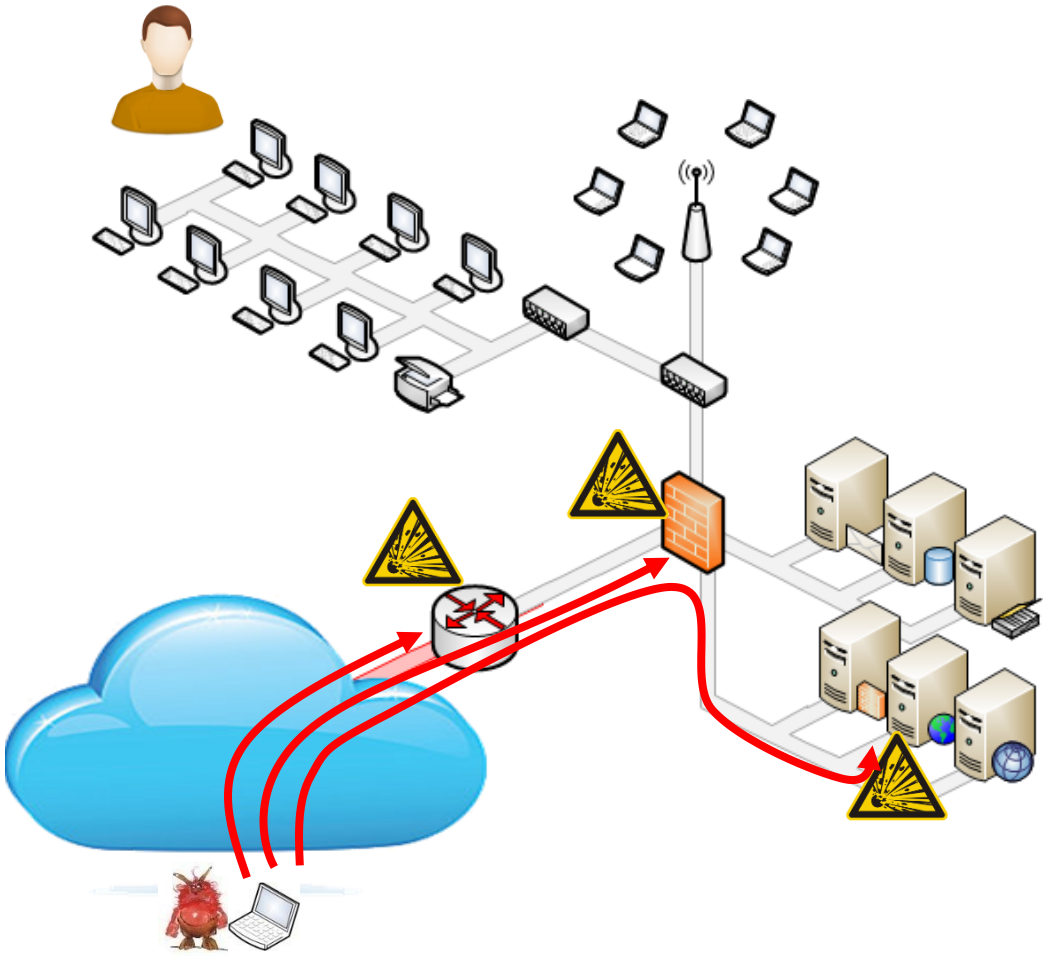
# Sécurité des Réseaux

- **DoS (Attaques physiques)**



# Sécurité des Réseaux

- **DoS (Attaques Logicielles)**



http://osvdb.org/8901

**8901 Cisco** CSS 11000 routers on the CS800 chassis allow remote attackers to cause a **denial of service** (CPU consumption or reboot) via a large number of TCP SYN packets to the circuit IP address

http://www.osvdb.com/show/osvdb/4427

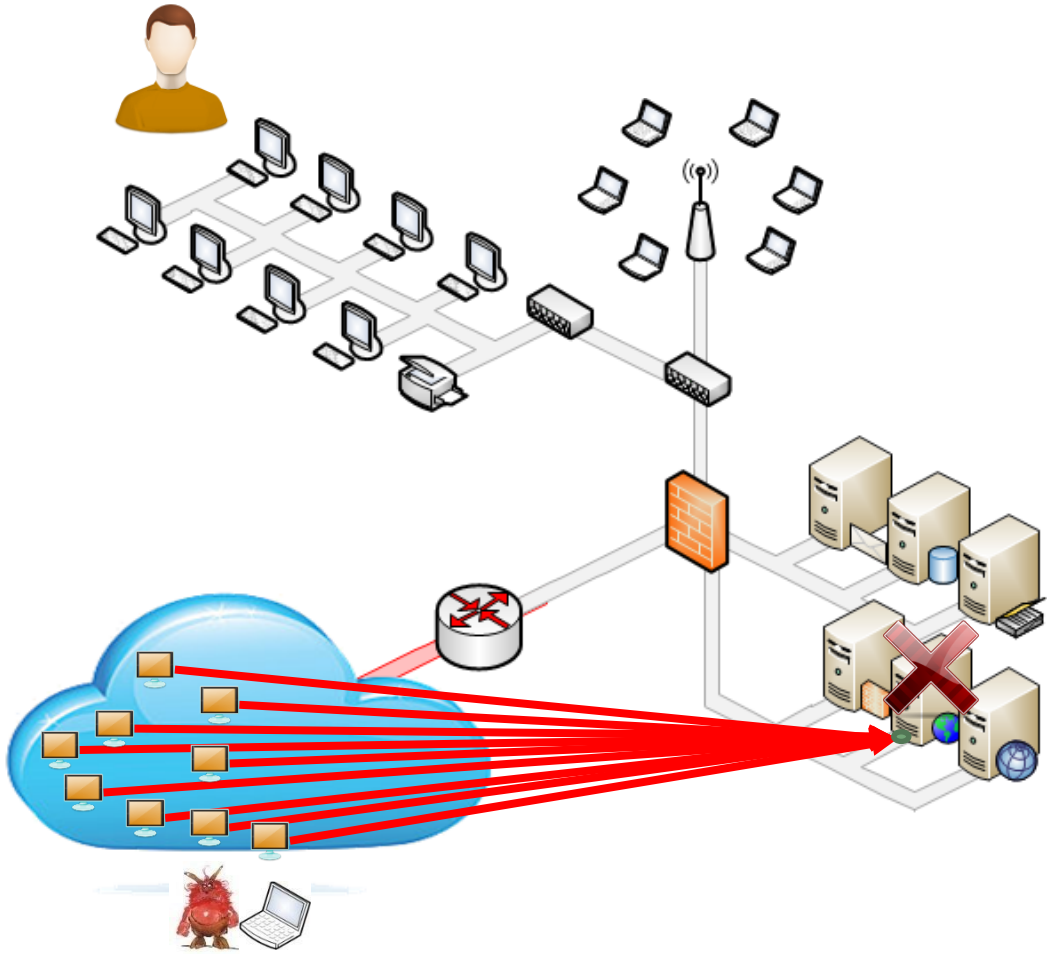
**4427 Check Point** FireWall-1 contains a flaw that may allow a remote **denial of service**. The issue is triggered when a remote attacker floods UDP port 264 causing the firewall to consume CPU resources or stop passing traffic

http://osvdb.org/78573

**78578 Apache Tomcat** 5.5.x uses an inefficient approach for handling parameters, which allows remote attackers to cause a **denial of service** (CPU consumption) via a request that contains many parameters and parameter values, a different vulnerability

# Sécurité des Réseaux

- **DoS (Attaques réseaux)**

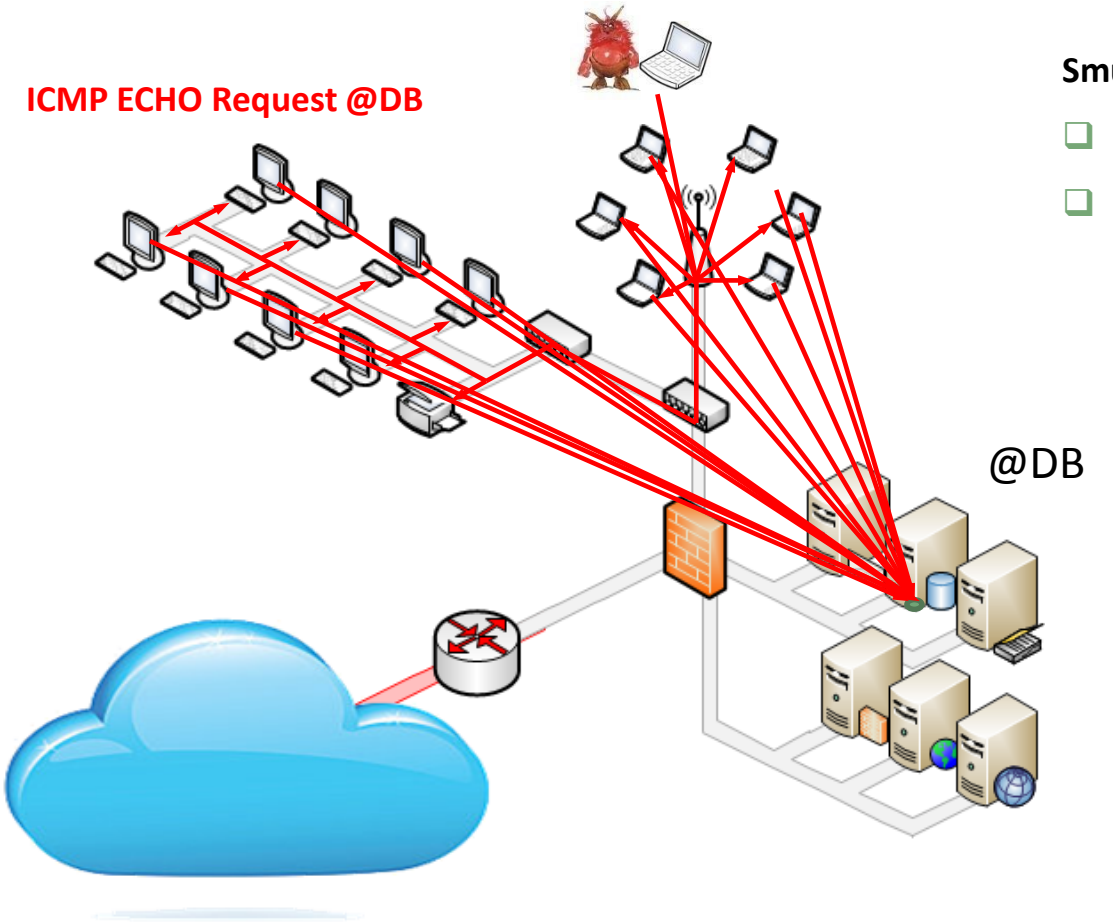


**Dos Distribué**

- Corruption de plusieurs machines sur le net
- Attaque simultanée sur une cible déterminée

# Sécurité des Réseaux

- **DoS (Attaques réseaux)**

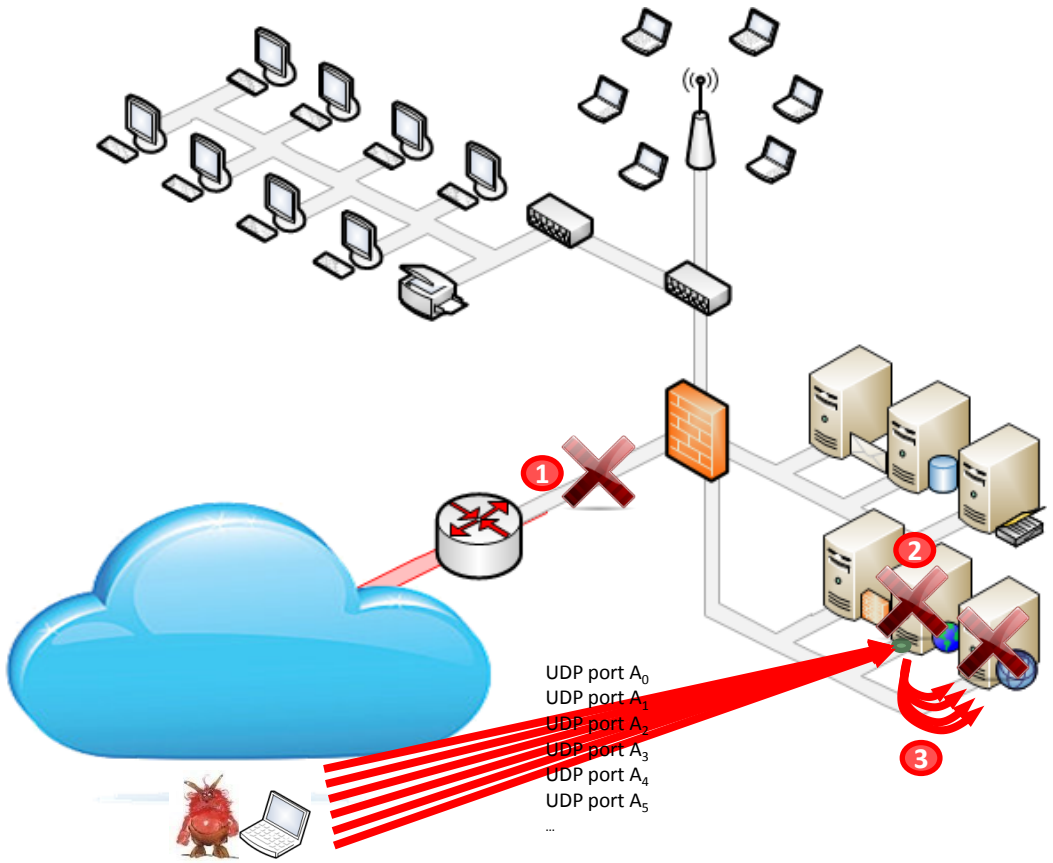



**Smurf attaque**

- Broadcat Ping echo request,
- Spoof l'adresse IP de retour

# Sécurité des Réseaux

- **DoS (Attaques réseaux)**




**UDP Flooding**

1. UDP prioritaire sur TCP → engorgement réseau
2. Lorsque paquet UDP reçu, vérification du service qui tourne sur le port visé, envoi d'un paquet ICMP destination unreachable
   →Consommation de ressource Dos
3. Si adresse initiale source spoofer, attaque par ricochets d'une autre machine

# La protection des réseaux

- Les outils de la sécurité
- La protection des communications
- La protection des réseaux wifi
- Les architectures de sécurité

# Sécurité des Réseaux

- **Les protections**
  - Les outils à l'aide de la sécurité réseau
    - Les firewalls
    - Les switchs, passerelles
    - Les proxies
  - La protection des communications
    - Les VPN
    - IPsec
    - EMail et PGP
  - La protection des réseaux wifi
  - Les architectures de sécurité

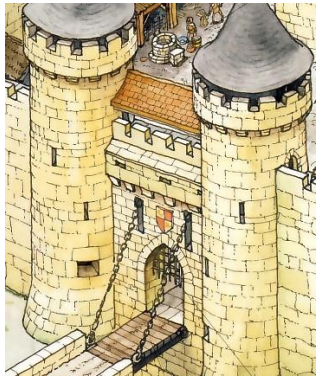
# La protection des réseaux

- Les outils de la sécurité
- La protection des communications
- La protection des réseaux wifi
- Les architectures de sécurité

# Sécurité des Réseaux

- **Les Firewall**
  - ❑ Objectif

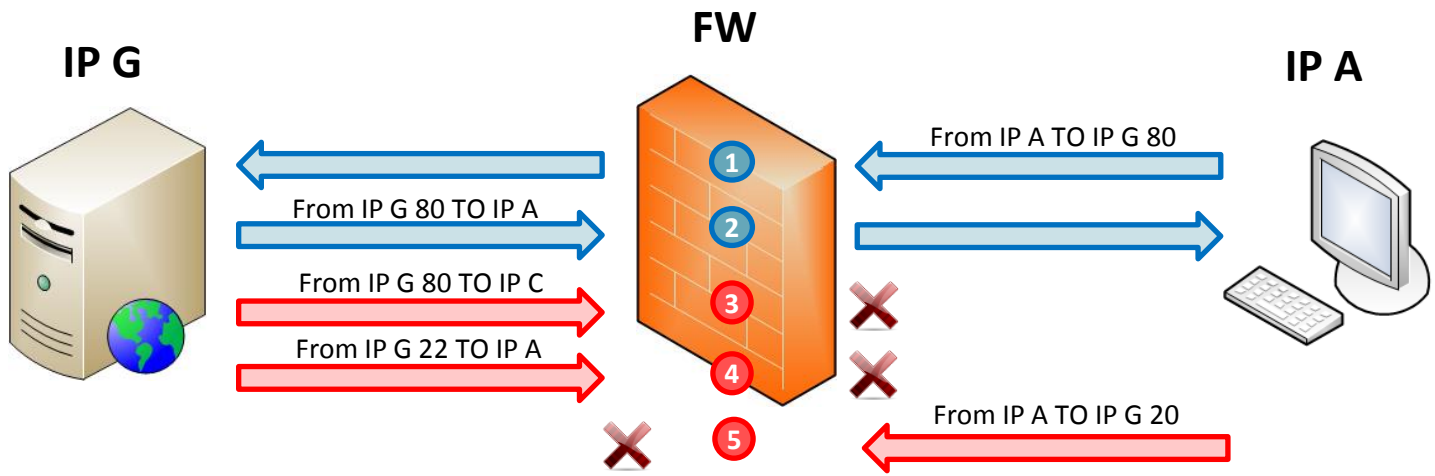
*Sélectionner les données pouvant accéder à une ou plusieurs parties du réseau. Toutes les données ne respectant pas les règles sont écartées*



  - ❑ Propriétés
    - 2 Types de firewall
      - StateFull
      - StateLess
    - Filtrage par couches
      - Initialement jusqu'au niveau 3 réseau
      - Etendu jusqu'aux couches applicatives 7

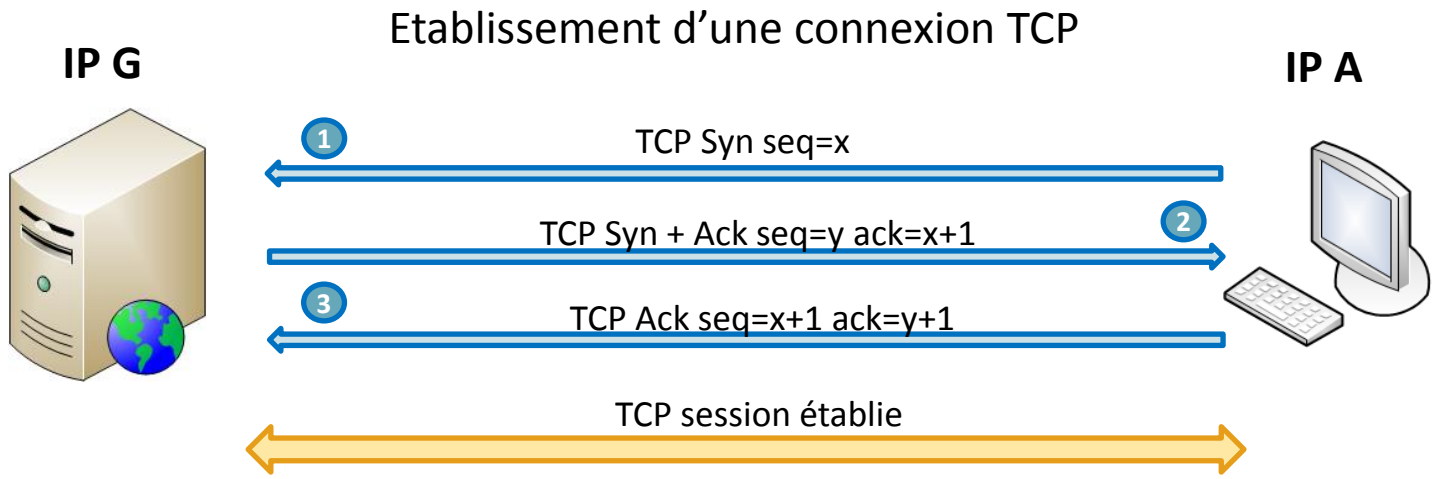
# Sécurité des Réseaux

- **Firewall (Statefull vs Stateless)**

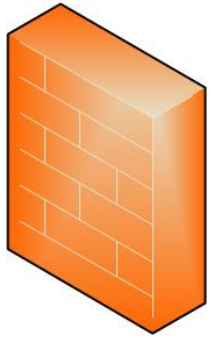



| | Source IP | Destination IP | Port | Dest. Port | Autorisation |
|---|---|---|---|---|---|
| 1 | IP A | IP G | ALL | 80 | Authorised |
| 2 | IP G | IP A | 80 | ALL | Authorised |
| 5 4 3 | ALL | ALL | ALL | ALL | Forbidden |

- **Firewall (Statefull vs Stateless)**

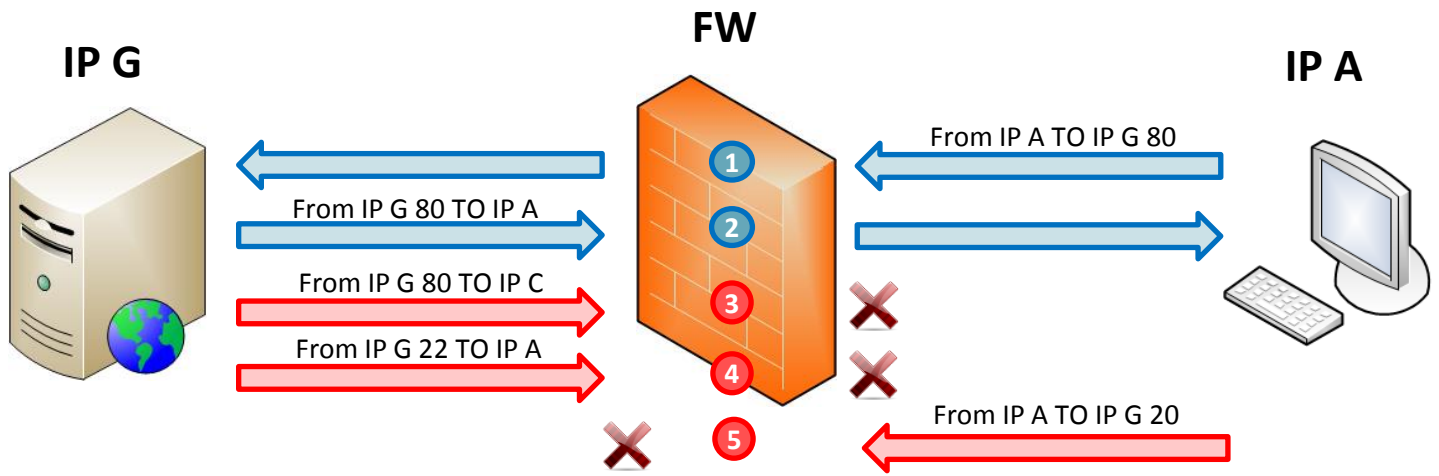



1. Etablissement d'une nouvelle connexion
2. Autorisation du TCP syn ack
3. Connexion établie, enregistrement des paramètres de la session TCP, attribution d'un TAG



# Sécurité des Réseaux

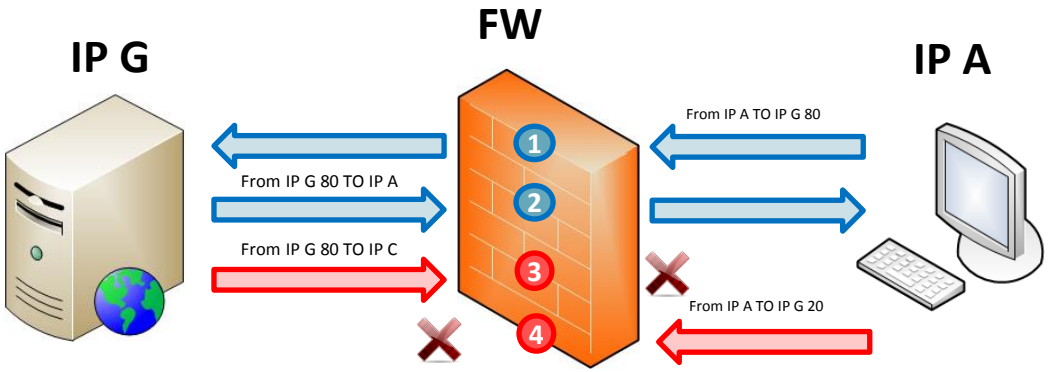
- **Firewall (Statefull vs Stateless)**

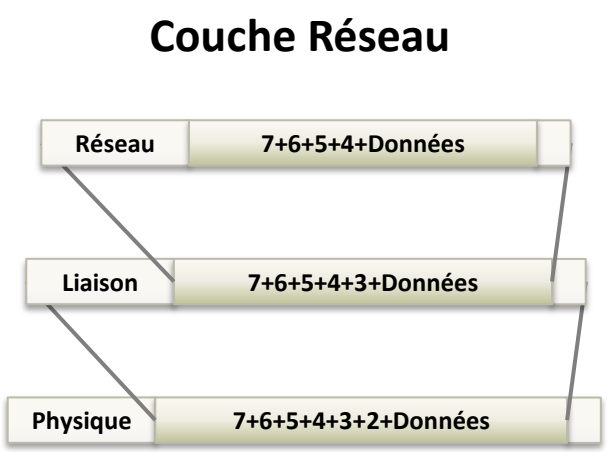



| | Source IP | Destination IP | Port | Dest. Port | Autorisation |
|---|---|---|---|---|---|
| 2 1 | IP A | IP G | ALL | 80 | Authorised |
| 5 4 3 | ALL | ALL | ALL | ALL | Forbidden |

# Sécurité des Réseaux

- **Firewall Filtrage par couche**

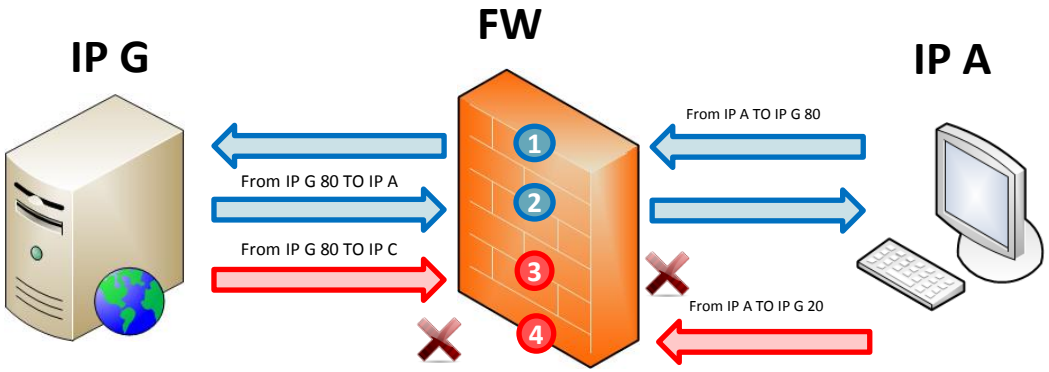


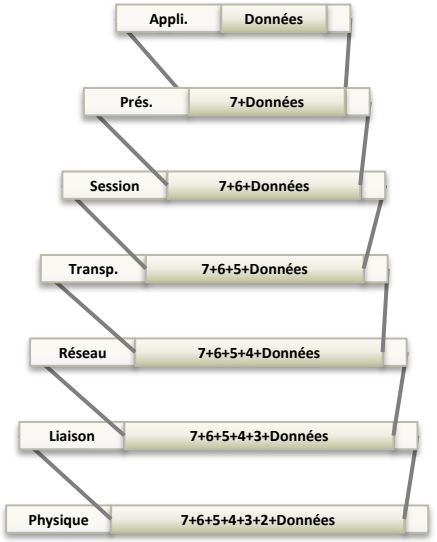

| | Source MAC | Destination MAC | Source IP | Destination IP | Port | Dest. Port | Autorisation |
|---|---|---|---|---|---|---|---|
| 2 1 | MAC A | MAC G | IP A | IP G | 80 | ALL | Authorised |
| 4 3 | ALL | ALL | ALL | ALL | ALL | ALL | Forbidden |

# Sécurité des Réseaux

- **Firewall Filtrage par couche**




## Couche Applicative




| | Source MAC | Dest. MAC | Source IP | Dest. IP | Port | Dest. Port | Protocole | Protocole Applicatif | Application | Autorisation |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 1 | MAC A | MAC G | IP A | IP G | 80 | ALL | TCP/IP | HTTP | Chrome.exe | Authorised |
| 4 3 | ALL | ALL | ALL | ALL | ALL | ALL | ALL | | | Forbidden |

# Sécurité des Réseaux

- **Segmentation des réseaux**
  - ❑ Objectif

*Découpage du réseau (couche 2-3) permettant de réduire la visibilité de l'ensemble du réseau.*

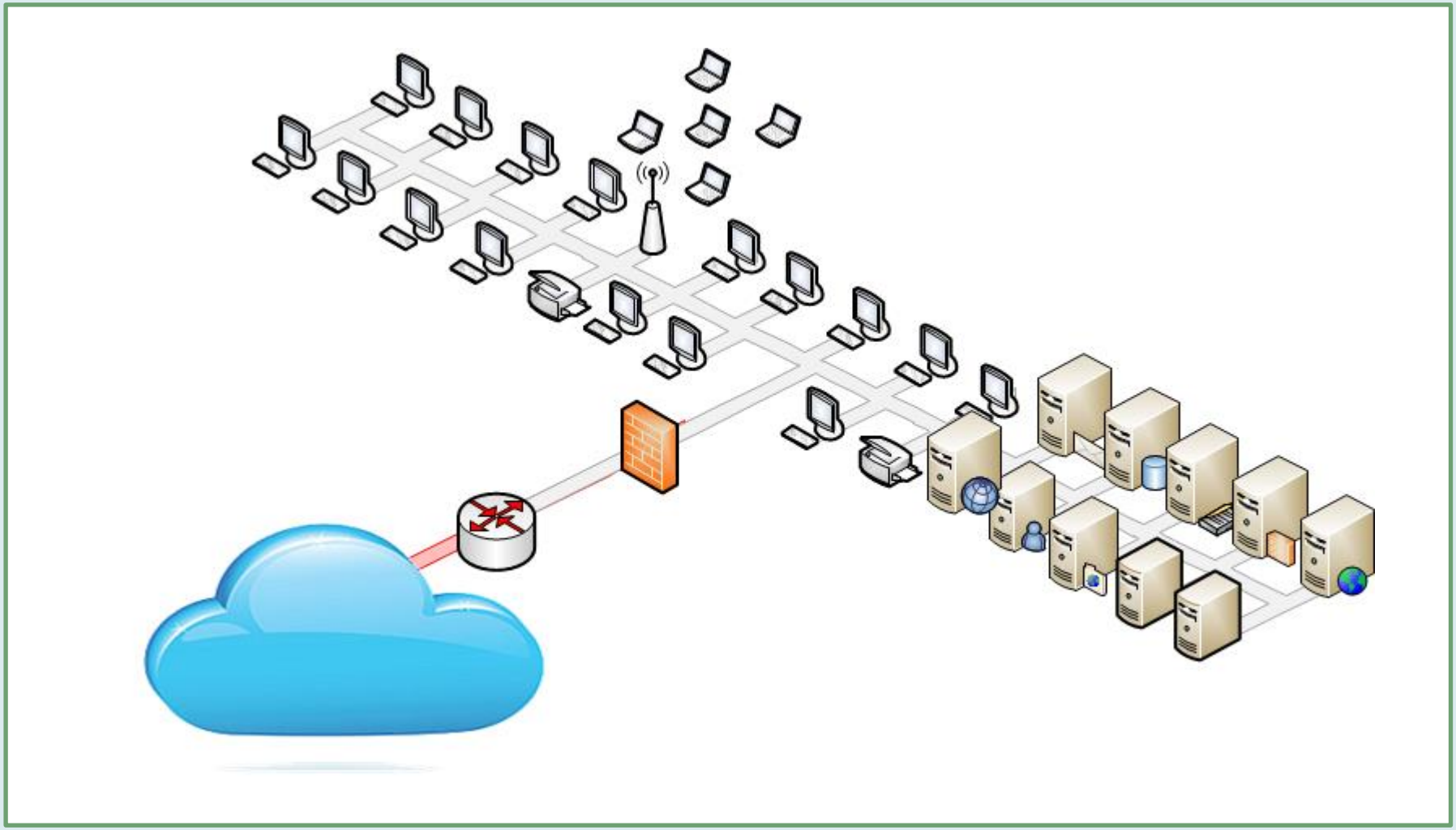
→ *Réduction du trafic réseau*

→ *Prévention des attaques par découverte et rebond*

  - ❑ Les outils
    - Passerelles
    - Switch
    - White liste sur adresse MAC

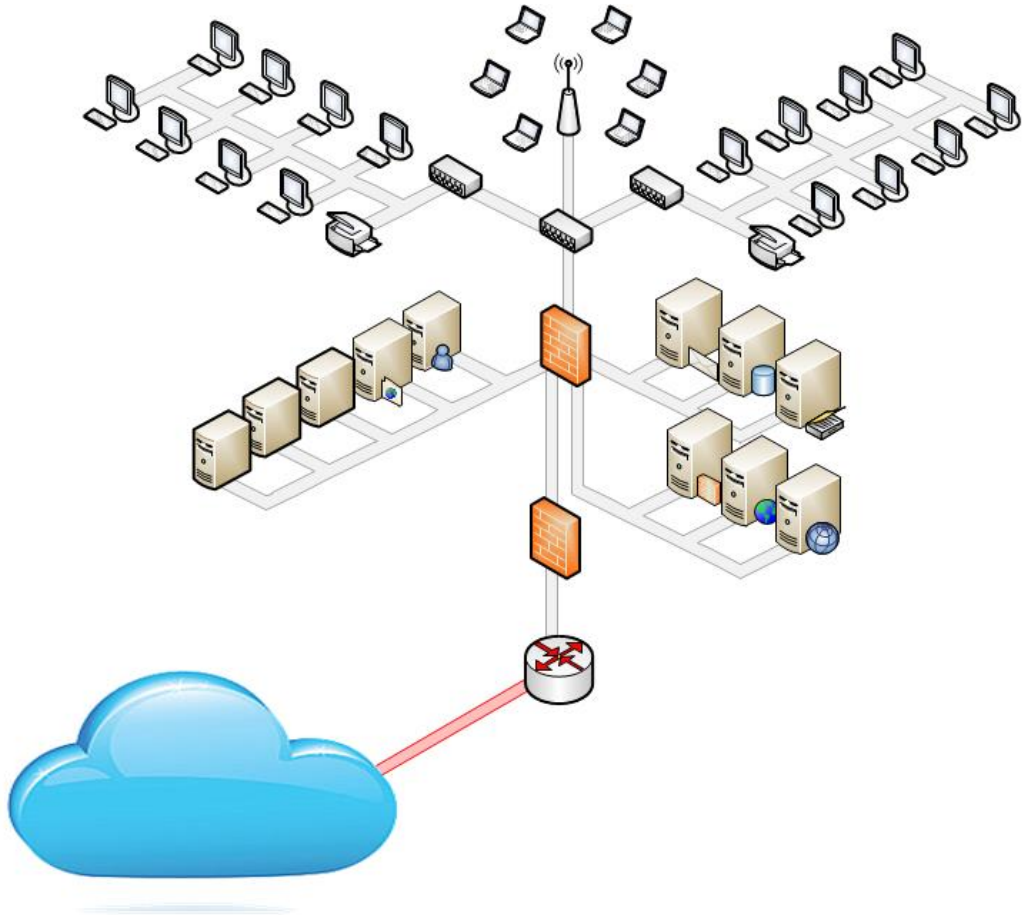
# Sécurité des Réseaux

- **Segmentation des réseaux: Quels sont les dangers ?**



# Sécurité des Réseaux

- **Segmentation des réseaux**



# Sécurité des Réseaux

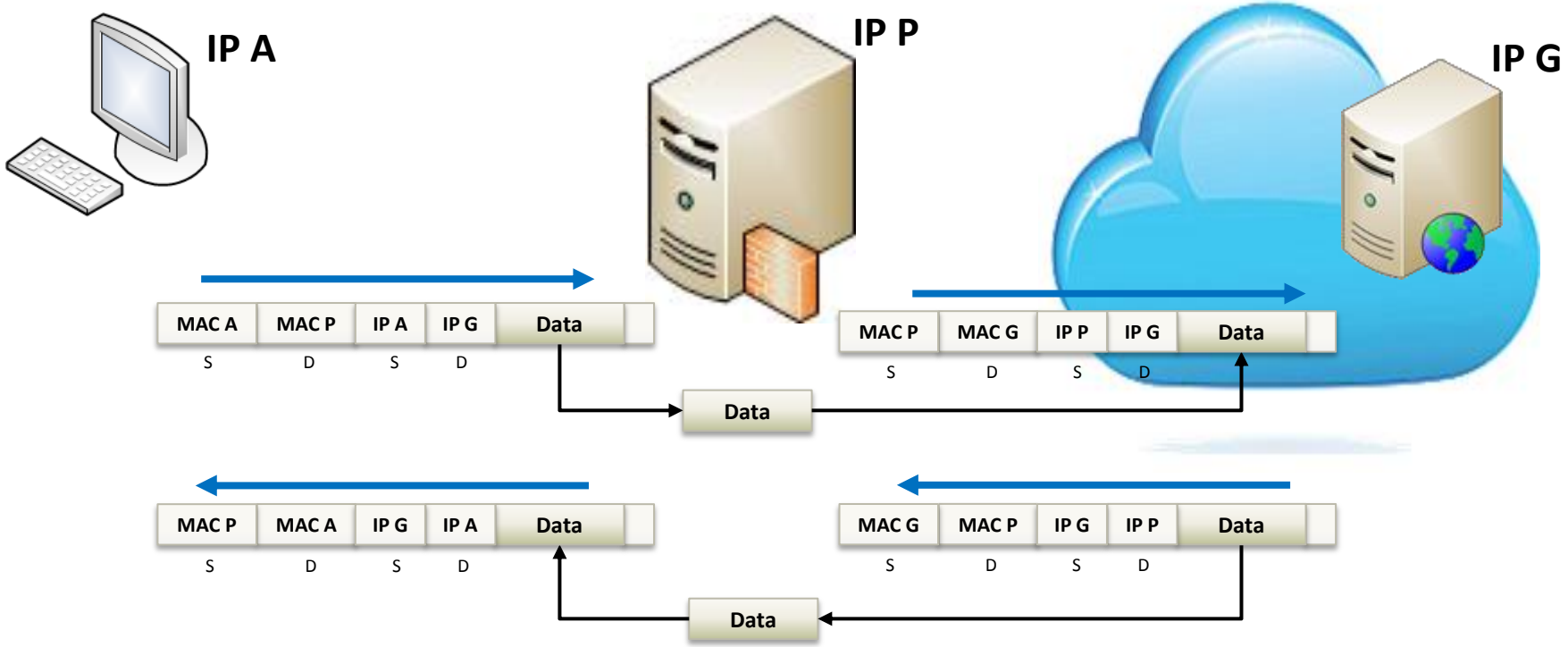
- **Proxy**
  - ❑ Objectif

*Rediriger les demandes du cœur de réseau vers un segment moins sécurisé. En étant un intermédiaire de communication le proxy permet de masquer le cœur du réseau.*

  - ❑ Propriétés
    - Redirige l'ensemble ou une partie des requêtes clientes vers l'extérieurs
    - Permet de stocker en cache des données visitées
    - Point d'accès centrale de communication, mise en place d'audit facilité

# Sécurité des Réseaux

- **Proxy**



# La protection des réseaux

- Les outils de la sécurité
- La protection des communications
- La protection des réseaux wifi
- Les architectures de sécurité

# Sécurité des Réseaux

- **La protection des communications**
  - ❑ Les VPN Virtual Private Network

*Un VPN est un canal de communication sécurisé et privé sur un réseau non sécurisé et mutualisé*

  - ❑ Propriétés
    - Un VPN est un canal virtuel et non pas un canal physique
    - Un VPN garantit la sécurité en termes de:
      - Contrôle d'accès (authentification, autorisation)
      - Confidentialité (chiffrement)
      - Intégrité de données

VPN: Réseaux Privés Virtuels(Virtual Private Networks), Taghrid Asfour 2012

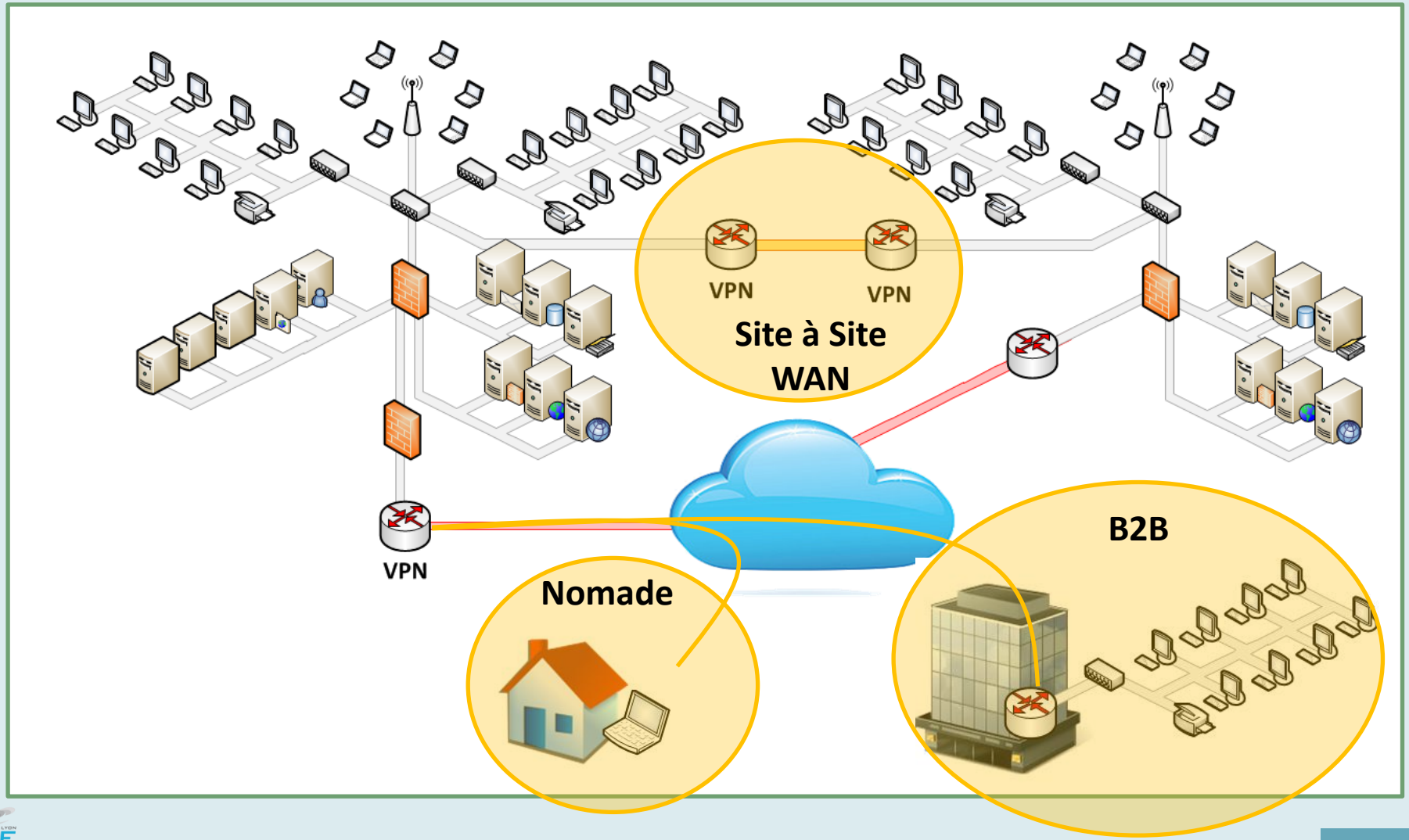
# Sécurité des Réseaux

- **VPN**
  - Utilisation
    - Connexion de réseaux (WAN)
    - Connexion de Nomade
    - Connexion Business To Business
  - Type de VPN
    - VPN SSH (niveau application)
    - VPN SSL/TLS (niveau session)
    - VPN Niveau 3 (niveau réseau)
      - IP-IP
      - GRE
      - IPsec

VPN: Réseaux Privés Virtuels(Virtual Private Networks), Taghrid Asfour 2012

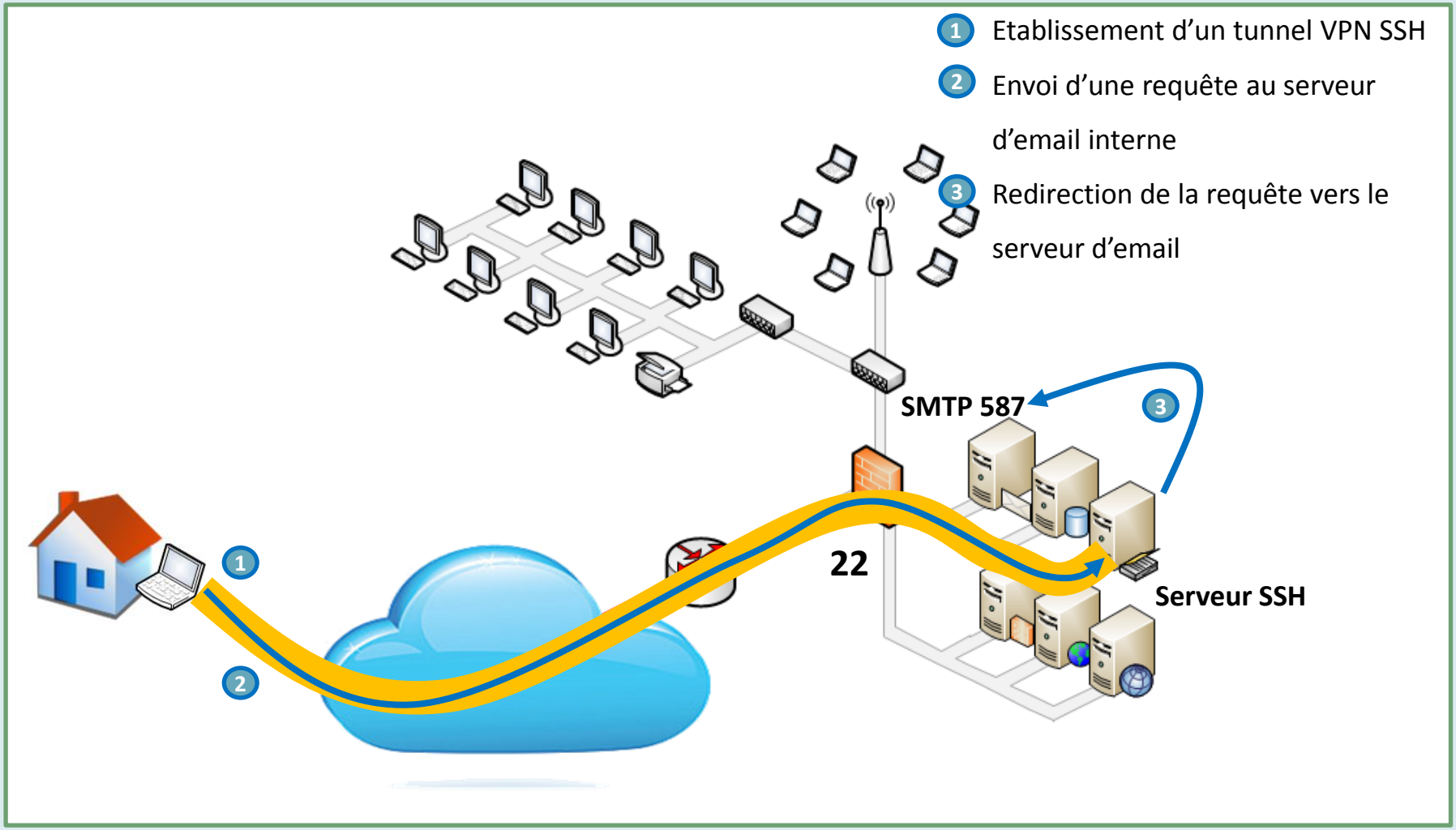
# Sécurité des Réseaux

- **VPN**



# Sécurité des Réseaux

- **VPN Secure Shell (SSH)**



# Sécurité des Réseaux

- **VPN SSL/TLS**
  - SSL et TLS sont implémentés au niveau de la couche session du modèle OSI
  - SSL et TLS sont souvent associés à un protocole applicatif
    - https: http+TLS
    - ftps: ftp+TLS
  - Permet de créer des VPN avec un simple navigateur web (côté client)

VPN: Réseaux Privés Virtuels(Virtual Private Networks), Taghrid Asfour 2012

# Sécurité des Réseaux

- **VPN SSL/TLS**
  - 2 types de VPN SSL
  - SSL Portail VPN
    - Le logiciel client (navigateur) accède à une page web sécurisée (https)

      Cette page gère l'authentification des utilisateurs (login + mot de passe)

      Cette page est le portail pour accéder à d'autres applications Web par la suite

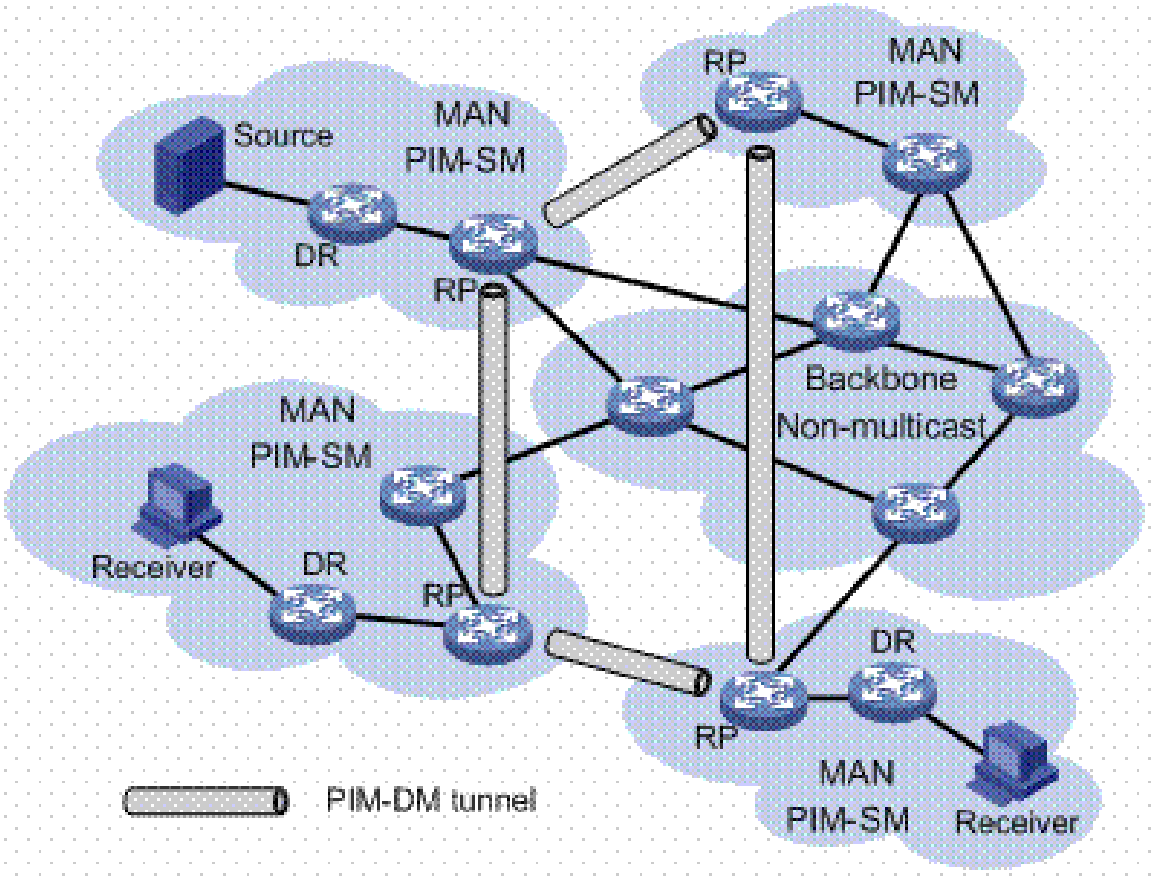
  - SSL Tunnel VPN
    - Le logiciel client établit une liaison sécurisée avec le serveur. Cette liaison permet d'accéder à plusieurs services réseaux simultanément, y compris ceux qui ne sont pas basés sur la technologie Web
      - Application Java, site avec Java Script ou Flash
    - Ceci nécessite que le logiciel client soit capable de gérer ces technologies

- **VPN Réseau**
  - Tunnel GRE (Gerneric Routing Encapsulation)
    - Encapsuler les données dans des paquets IP afin de pouvoir traverser le tunnel
    - Permet d'encapsuler tous types de paquets dans des paquets IP
    - Utilise une entête supplémentaire pour encapsuler d'autres paquets niveau 3 comme IP, IPX ou AppleTalk
    - Il n'y a aucun cryptage de données avec le tunnel GRE


VPN: Réseaux Privés Virtuels(Virtual Private Networks), Taghrid Asfour 2012

# Sécurité des Réseaux

- **Exemple de multicast avec tunnel GRE**




Source: http://www.h3c.com/portal/res/200806/24/20080624_797933_image008_641561_57_0.gif

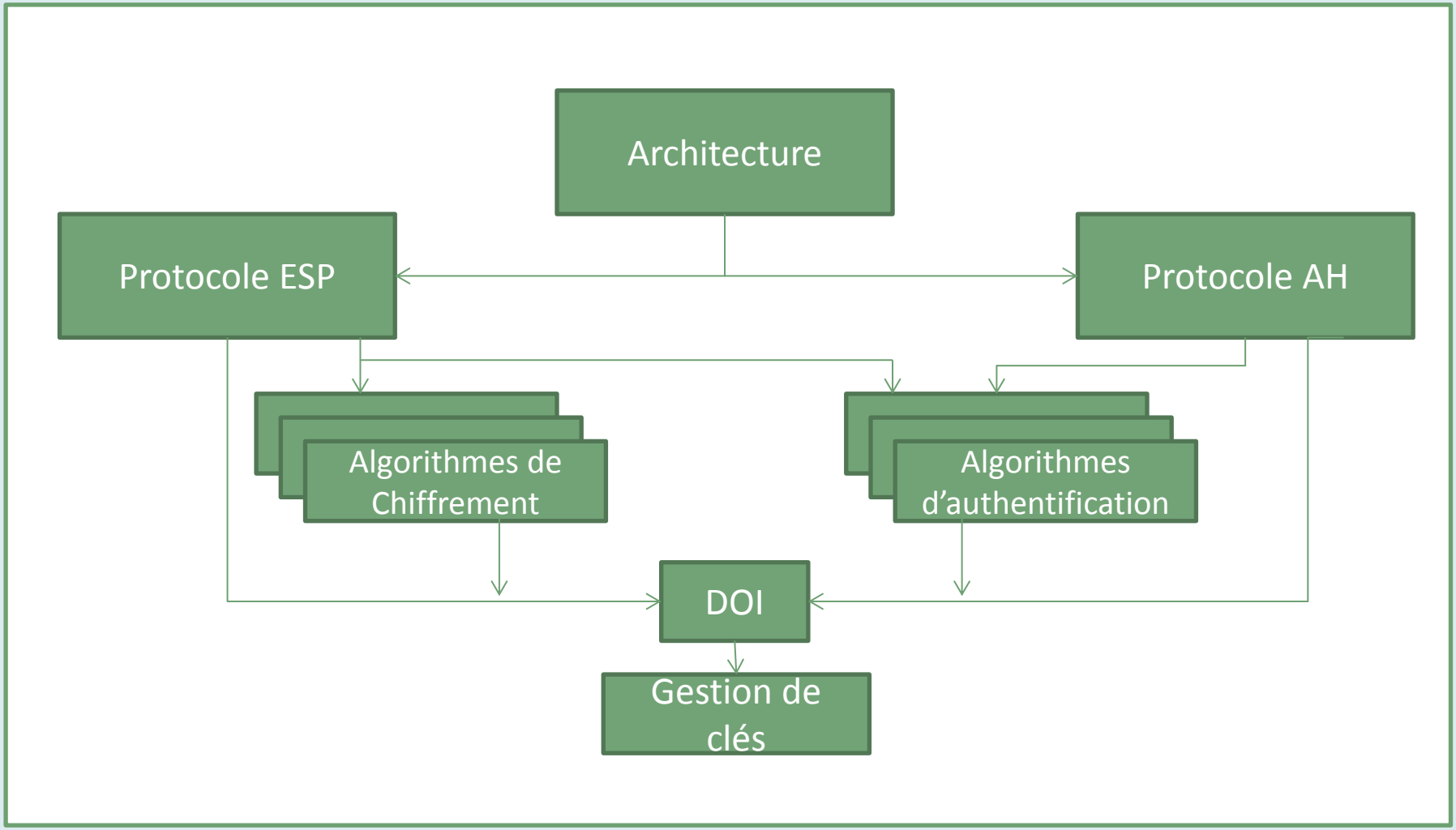
# Sécurité des Réseaux

- **VPN Réseau: IPsec**
  - Niveau 3 du modèle OSI
  - Permet de créer des VPN mais ce n'est pas son unique utilisation
  - Souvent utilisé pour connecter un site distant au réseau de l'entreprise via l'établissement d'un VPN IPsec
  - Obligatoire dans la pile IPv6, facultatif dans IPv4
  - Mis en œuvre dans chaque équipement réseau:
    - Permettre d'avoir une sécurité de bout en bout
    - Ou une sécurité sur un lien

VPN: Réseaux Privés Virtuels(Virtual Private Networks), Taghrid Asfour 2012

# Sécurité des Réseaux

- **VPN Réseau: IPsec**




VPN: Réseaux Privés Virtuels(Virtual Private Networks), Taghrid Asfour 2012

# Sécurité des Réseaux

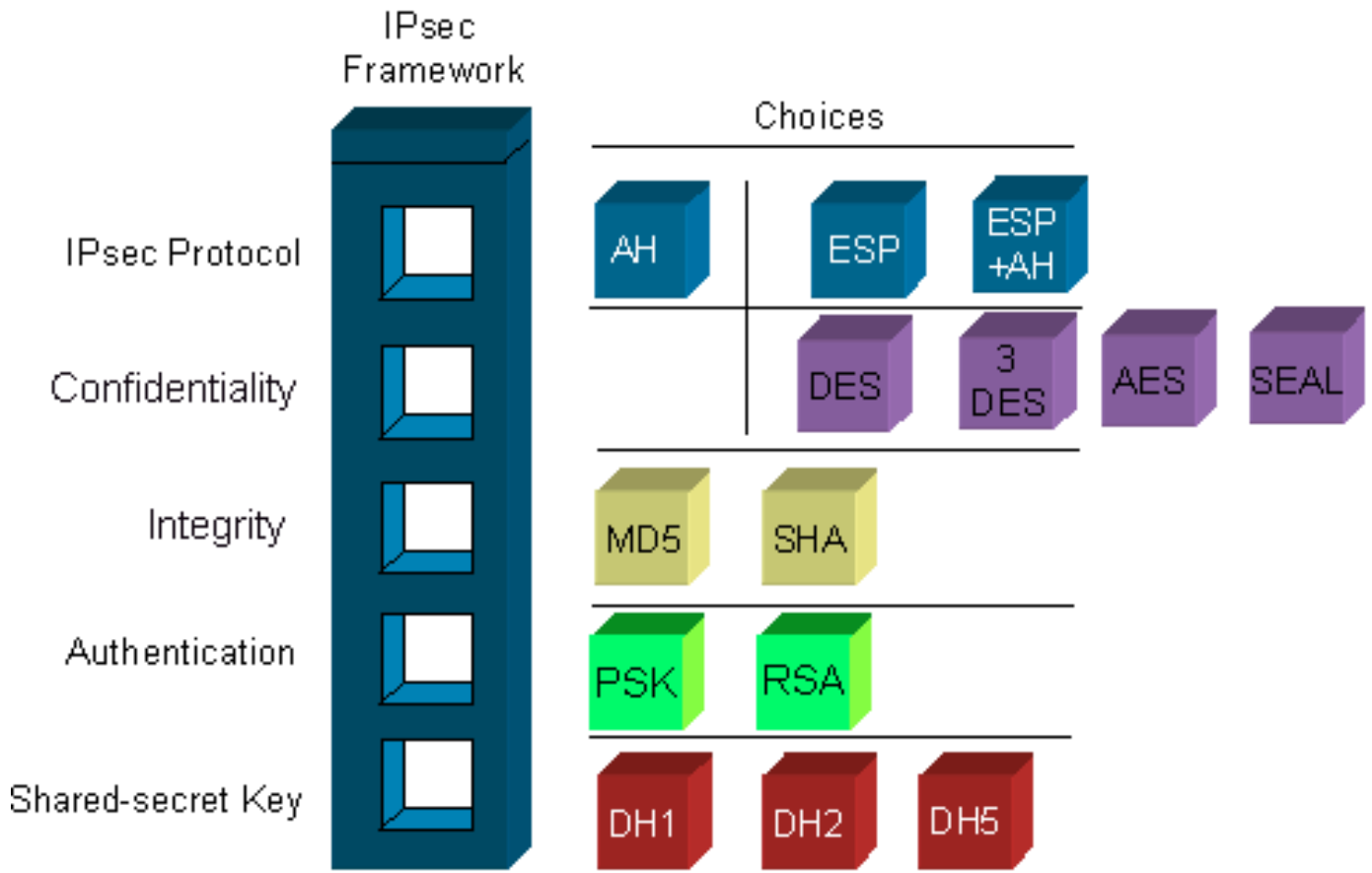
- **VPN Réseau: IPsec**

| | AH | ESP (avec cryptage uniquement) | ESP (Authentification + cryptage) |
|---|---|---|---|
| Contrôle d'accès | Oui | Oui | Oui |
| Intégrité de données | Oui | Non | Oui |
| Authentifier l'origine de données | Oui | Non | Oui |
| Protection contre le rejeu | Oui | Oui | Oui |
| Confidentialité | Non | Oui | Oui |

VPN: Réseaux Privés Virtuels(Virtual Private Networks), Taghrid Asfour 2012

# Sécurité des Réseaux

- **VPN Réseau: IPsec**




VPN: Réseaux Privés Virtuels(Virtual Private Networks), Taghrid Asfour 2012

# La protection des réseaux

- Les outils de la sécurité
- La protection des communications
- La protection des réseaux wifi
- Les architectures de sécurité

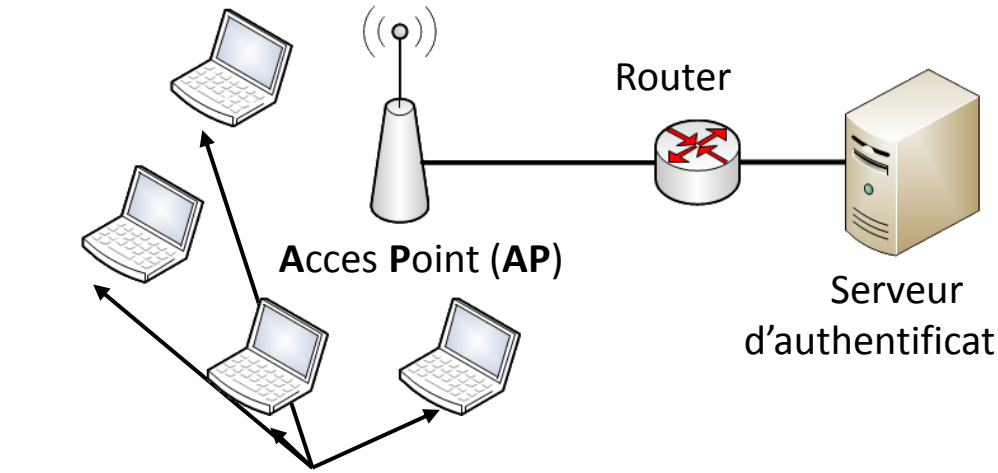
# Sécurité des Réseaux

- **La sécurité des réseaux wifi**
  - Communications sans fils uniquement le Wifi? Non
    - Bluetooth
    - ZigBee
    - Liaisons Infrarouge
    - Boucle Locale Radio (B.L.R)
    - GSM,GPRS,UMTS

  - Les utilisations
    - WPAN: WireLess Personal Area Network (Bluetooth,ZigBee,Liaison Infrarouge)
    - WLAN: WireLess Local Area Network (Wifi)
    - WMAN: Wireless Metropolitan Area Network (BLR,WiMax)
    - WWAN: Wireless Wide Area Network (GSM, GPRS, UMTS)
  - Mode d'architecture
    - Infrastructure
    - Ad-Hoc

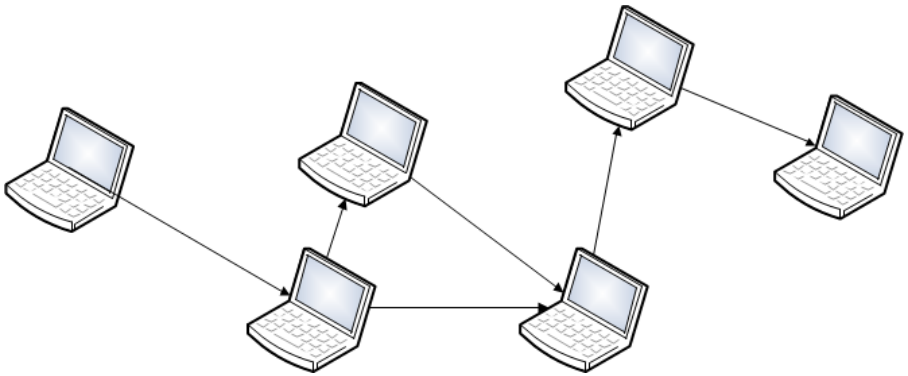
# Sécurité des Réseaux

- **La sécurité des réseaux wifi: Architecture et Terminologie**




Mode Infrastructure

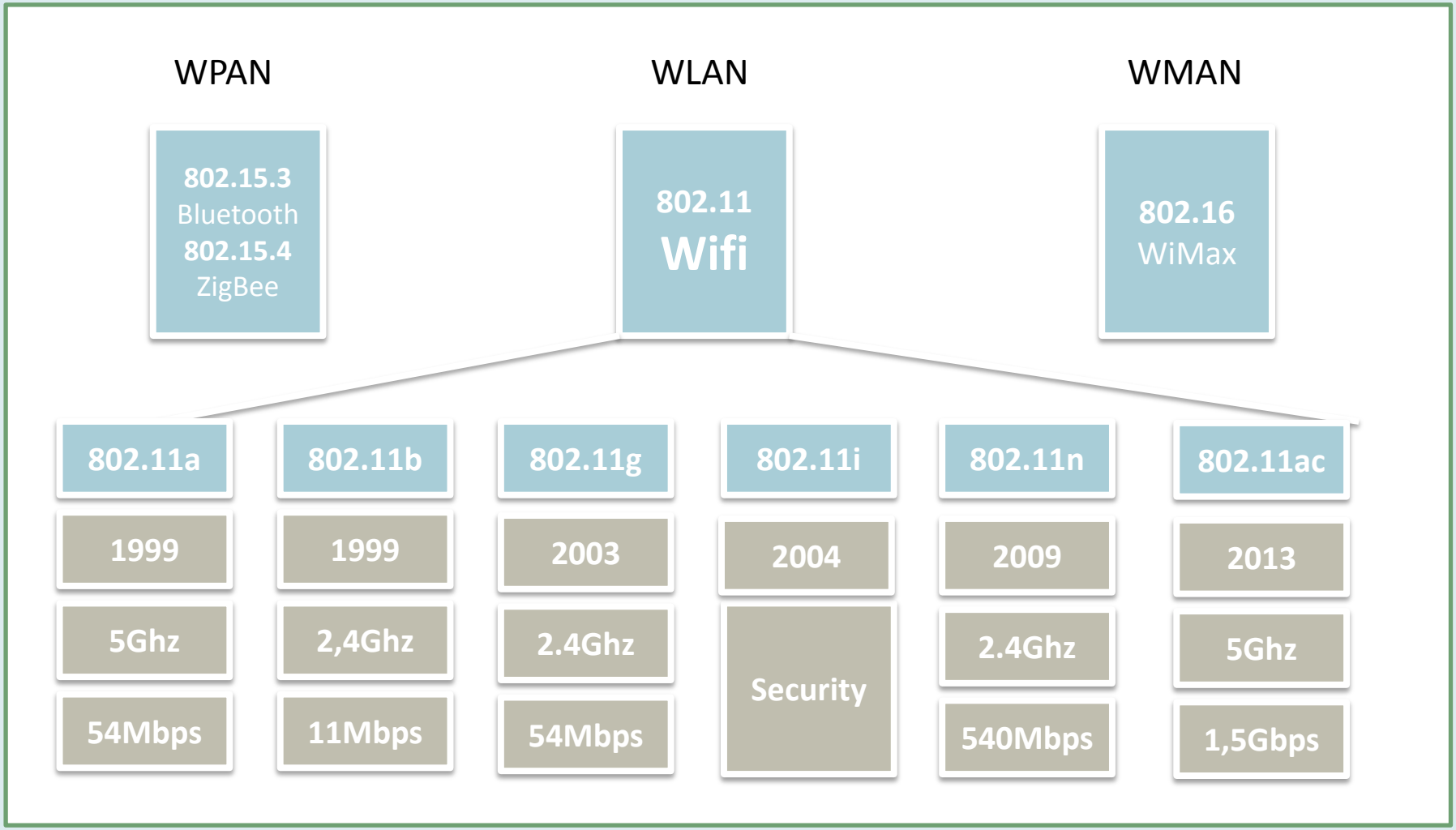
**Cellule** ou **B**asic **S**ervice **S**et (**BSS**)



Mode Ad-Hoc

# Sécurité des Réseaux

- **La sécurité des réseaux wifi: Les Normes**



# Sécurité des Réseaux

- **La sécurité des réseaux wifi**
  - Les faiblesses
    - Média radio = diffusion de l'information
      - Interception
      - Rejeu d'information
      - Fabrication
      - Spoofing
    - Sensibilité au brouillage
    - Configuration initiale non sécurisée
    - Phishing (faux point d'accès)

# Sécurité des Réseaux

- **La sécurité des réseaux wifi: Les Normes**

| | | 802.11i | |
|---|---|---|---|
| | WEP | WPA | WPA2 |
| Chiffrement | WEP<br>RC4 | WEP<br>TKIP<br>RC4+ clé 128 bits | WEP<br>TKIP<br>AES<br>WRAP<br>CCMP |
| Authentification | Clé WEP | WPA-PSK<br>WPA Entreprise Mode<br>802.11X | WPA-PSK<br>WPA Entreprise Mode<br>802.11X |
| Intégrité | ICV | MIC | MIC |

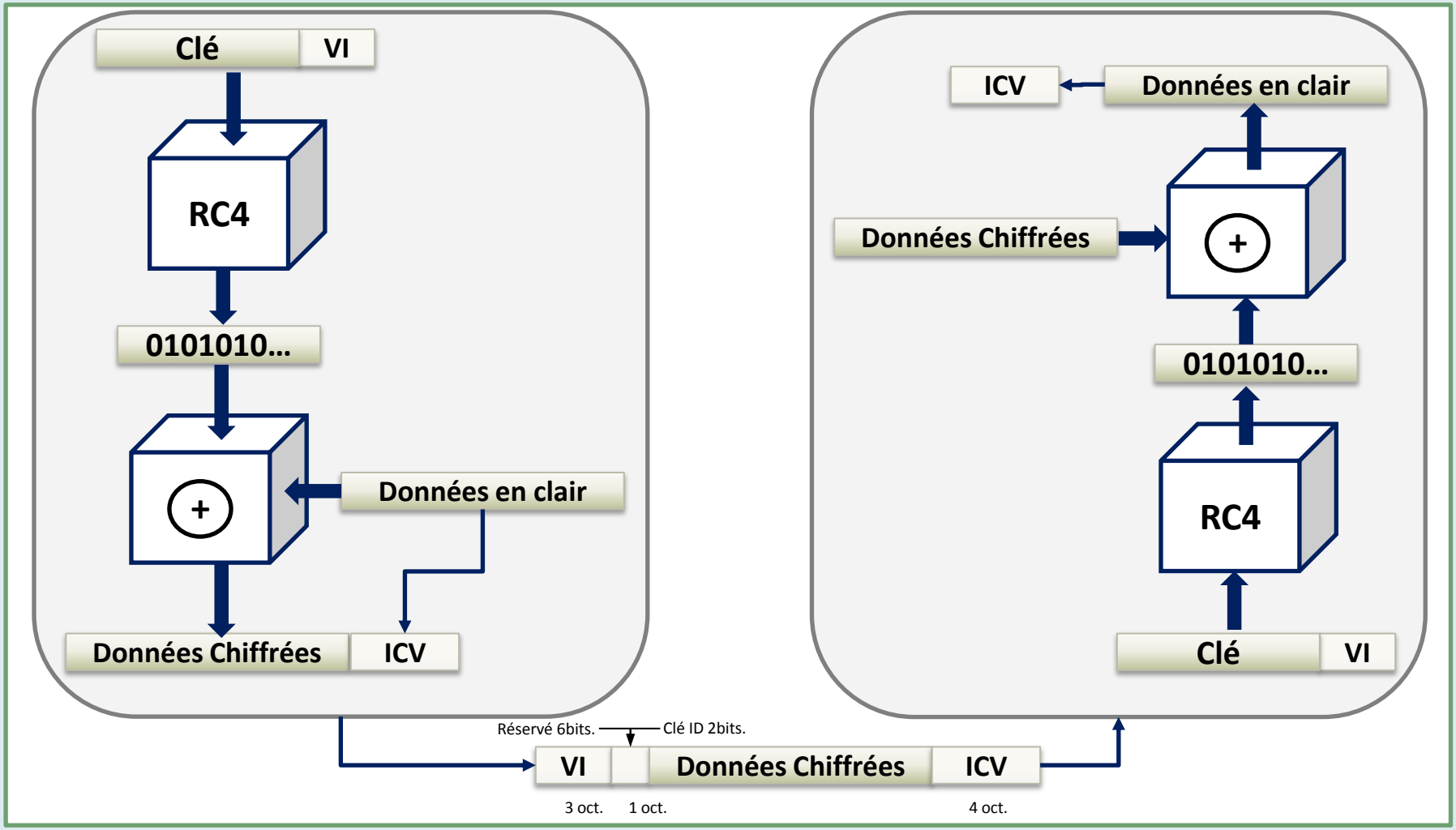
# Sécurité des Réseaux

- **Chiffrement Wired Equivalent Privacy (WEP)**
  - Spécifié dans le standard 802.11
  - Chiffrement communication client-AP grâce à une clé partagée (statique)
  - Taille de clé 64bits, 128 bits, 152 bits

  - Faiblesses
    - Clés de chiffrement statiques
    - Mauvaise utilisation des vecteurs d'initialisation
      - Réutilisation trop fréquente, chaine aléatoire pas assurée, collisions possibles
    - Mauvais contrôle d'intégrité
      - Collisions prouvées, modification possible sans visibilité dans le **I**ntegrity **C**heck **V**alue (**ICV**).

# Sécurité des Réseaux

- **Chiffrement WEP**



# Sécurité des Réseaux

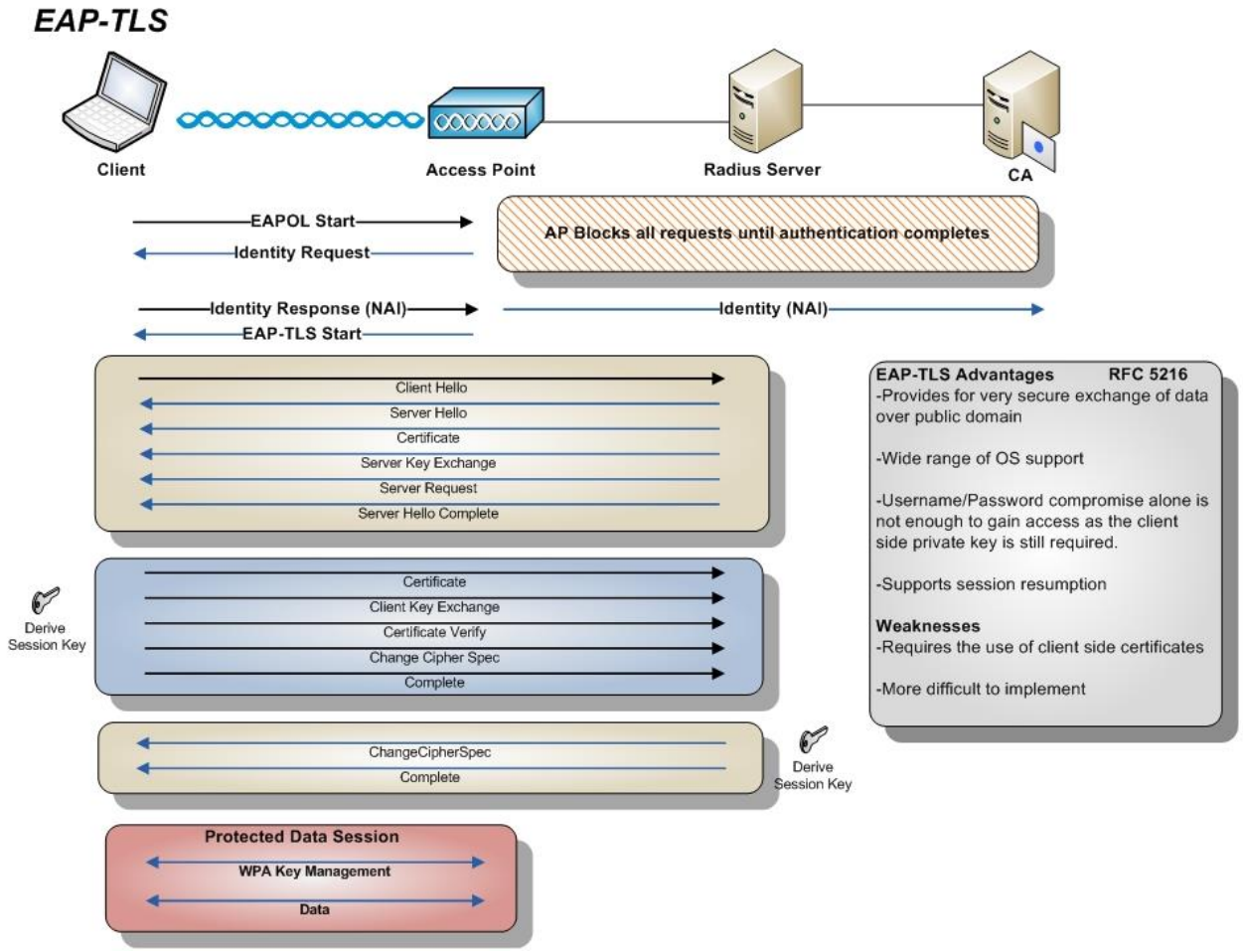
- **W**ifi **P**rotected **A**ccess **(WPA)**
  - Chiffrement
    - Spécifié dans le standard 802.11i
    - Chiffrement RC4 (correction de l'implémentation)
    - Taille de clé: 128 bits
    - Taille des VI augmentée 48 bits (6 octets)
    - **Introduction du protocole TKIP (Temporal Key Integrity Protocol)**
      - Chiffrement par paquet (une clé différente pour chaque paquet)
    - **Introduction du chiffrement AES (WPA2)**
  - Intégrité
    - Nouveau contrôle de l'intégrité Message Integrity Code (amélioration + compteur contre le rejeu)

# Sécurité des Réseaux

- **W**ifi **P**rotected **A**ccess **(WPA)**
  - Authentification
    - WPA-PSK (**P**re **S**hared **K**ey)
    - WPA Entreprise : authentification via un serveur radius
    - 802.1X: **EAP** (**E**xtensible **A**uthentication **P**rotocol) series
      - EAP-MD5 (Message Digest 5)
      - LEAP (Lightweight EAP) développé par cisco
      - EAP-TLS (EAP Transport Layer Security) norme **RFC 2716**
      - EAP-TTLS (EAP – Tunneled TLS)
      - PEAP (Protected EAP) développé par Cisco, Microsoft, RSA Secruity

# Sécurité des Réseaux

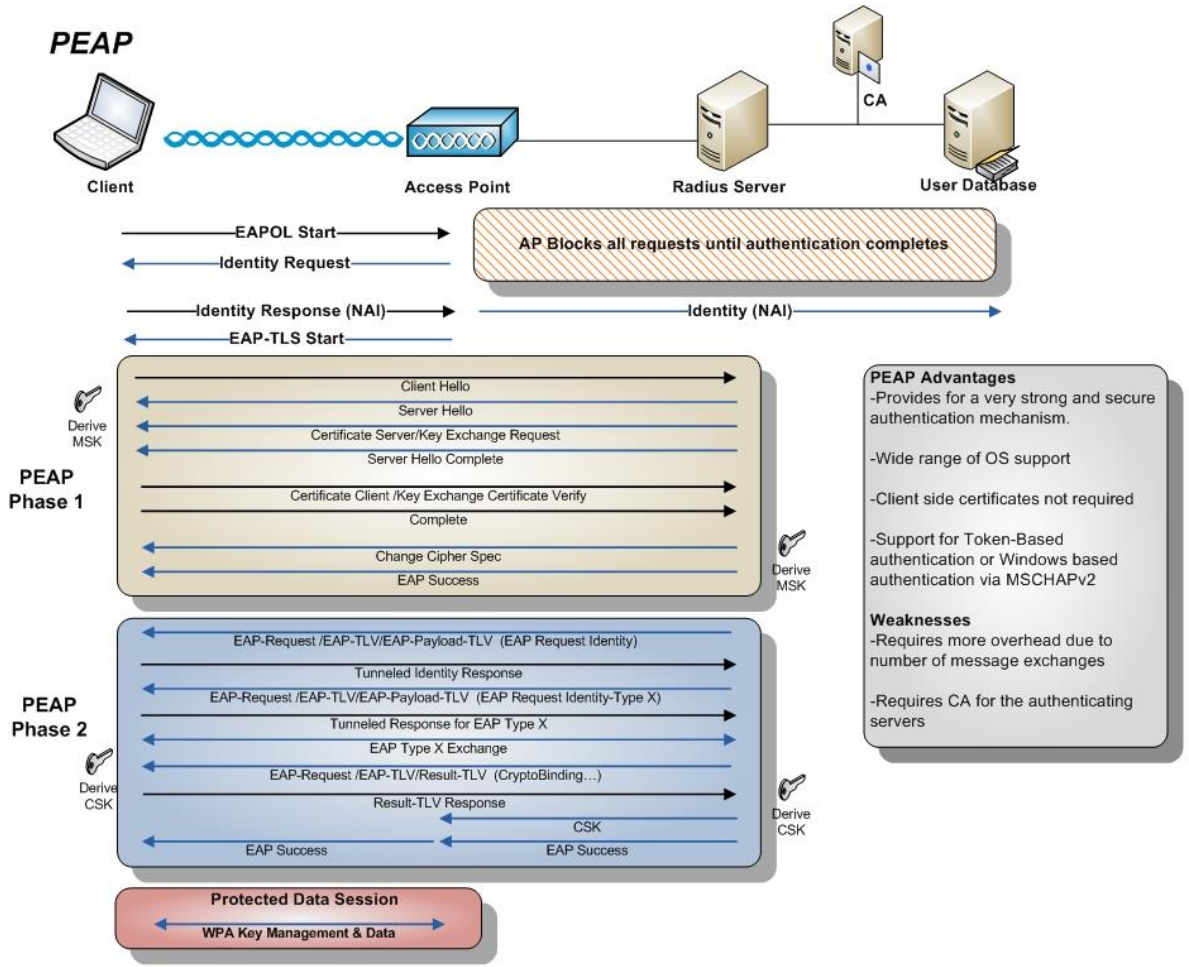
- **802.1X EAP- TLS**




http://layer3.wordpress.com/2009/08/16/eap-authentication-protocols/

# Sécurité des Réseaux

- **802.1X EAP- PEAP**




http://layer3.wordpress.com/2009/08/16/eap-authentication-protocols/

# Sécurité des Réseaux

- **Bilan des éléments de sécurité Wifi (1/4)**

| | WEP | TKIP | CCMP |
|---|---|---|---|
| Chiffrement | RC4 | RC4 | AES |
| Taille des clefs | 20 ou 104 bits | 64 bits pour authenticité et 128 bits pour chiffrer | 128 bits |
| Durée de vide | IV de 24 bits | IV de 48 bits | IV de 48 bits |
| Clef par paquet | Concaténation IV + clef | Mixing function | Pas de clef par paquet |
| Intégrité des données | CRC32 | Michael | CCM |
| Intégrité du header | Aucun | Michael | CCM |
| Rejeu | Aucun | IV croissant | IV croissant |
| Gestion des clefs | Aucun | 802.11i "4 way handshake" | 802.11i "4 way handshake" |
| Contraintes par rapport au matériel existant | Aucun | Aucune (simple mise à jour logicielle) | Besoin de nouveaux équipements |

http://prox-ia.blogspot.fr/2009/09/du-rififi-dans-le-wifi-le-wpa-malmene.html

# Sécurité des Réseaux

- **Bilan des éléments de sécurité Wifi (2/4)**

| | Authentication | Key distribution | Encryption | Algorithm |
|---|---|---|---|---|
| (none) | Open | None | None | None |
| WEP | Open or shared key (WEP) | Out of band | WEP | RC2 |
| WPA–Personal | Open, followed by shared secret = PSK | Out of band (PSK = PMK) | TKIP | RC4 |
| WPA-Entreprise | Open, followed by 802.1x, in which shared secret = certificate or other token | PMK from Authentication Server | TKIP | RC4 |
| WPA2–Personal | Open, followed by shared secret = PSK | Out of band (PSK = PMK) | CCMP | AES |
| WPA2-Entreprise | Open, followed by 802.1x, in which shared secret = certificate or other token | PMK from Authentication Server | CCMP | AES |

http://prox-ia.blogspot.fr/2009/09/du-rififi-dans-le-wifi-le-wpa-malmene.html

- **Bilan des éléments de sécurité Wifi (3/4)**

| EAP method | Identity privacy | Key generation | Authentication type | Tokens needed | Deployment constraints |
|---|---|---|---|---|---|
| **MD5** | No | No | Client authentication (one way) | Username /Password | Low |
| **OTP** | No | Yes | Client authentication (one way) | One Time Password | Low |
| **TLS** | No | Yes | Certificate based authentication (mutual) | Certificates on both client and server side | High |
| **TTLS + MSCHAP v2** | Optional | Yes | Certificate based authentication on server side + Username/Password on client side (mutual) | Certificate on server side + Username/Password on client side | Average |
| **PEAP + MSCHAP v2** | Optional | Yes | Certificate based authentication on server side + Username/Password on client side (mutual) | Certificate on server side + Username/Password on client side | Average |

http://prox-ia.blogspot.fr/2009/09/du-rififi-dans-le-wifi-le-wpa-malmene.html

# Sécurité des Réseaux

- **Bilan des éléments de sécurité Wifi (4/4)**

| Sécurité | Méthodes | 802.11 | 802.11i WPA | 802.11i WPA2 | Niveau de sécurité |
|---|---|---|---|---|---|
| Chiffrement | WEP | X | | | Très Faible Version initiale - vulnérable non recommandé |
| | TKIP | | X | X | Moyen Bien Meilleure protection que WEB mais cassé en 2009, non recommandé |
| | **AES** | | | **X** | **Haut Chiffrement recommandé** |
| Authentification | Clé wep | X | | | Faible Non recommandé |
| | WPA-PSK | | X | X | Faible Non recommandé - ou uniquement pour usage WPAN |
| | WPA-Entreprise | | X | X | Moyen bien meilleur résultat en association avec EAP |
| | EAP-MD5 | | X | X | Faible Non Recommandé (Faiblesse MD5) |
| | EAP-LEAP | | X | X | Moyen (nécessite un mot de passe fort) |
| | **EAP-TLS** | | **X** | **X** | **Haut (recommandé), déploiement complexe** |
| | EAP-TTLS | | X | X | Haut |
| | EAP-PEAP | | X | X | Haut |
| Intégrité | ICV | X | | | Faible vulnérable |
| | **MIC** | | **X** | **X** | **Haut** |
| | **CCMP (AES-CBC-MAC)** | | | **X** | **Haut** |

# Sécurité des Réseaux

- **Architecture de sécurité**
  - Regrouper des entités partageant les mêmes politiques et besoins de sécurité
  - Etudier et protéger les communications entre ces groupes ou Zones
  - Surveiller et contrôler la sécurité mise en place.

# La protection des réseaux

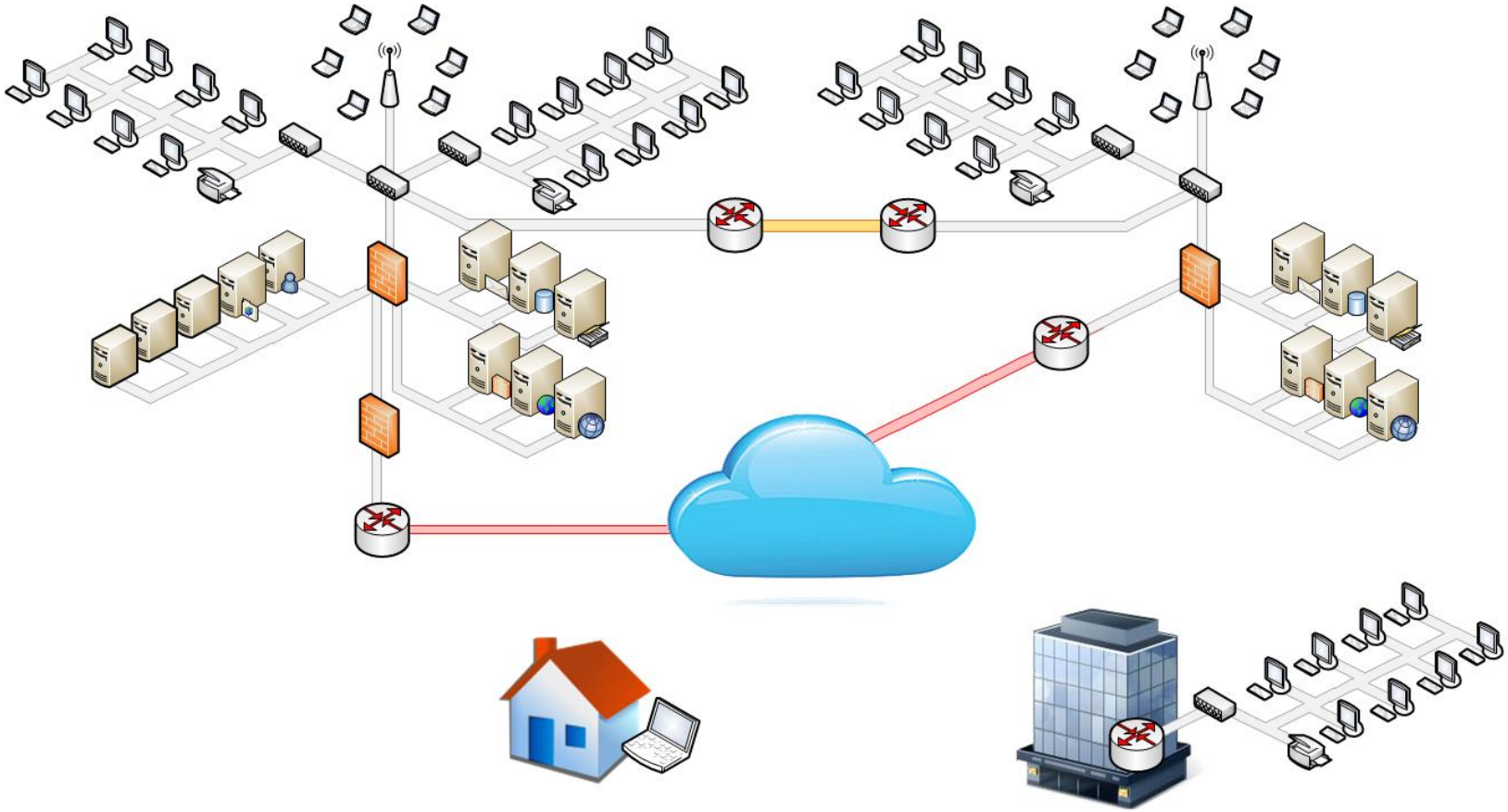
- Les outils de la sécurité
- La protection des communications
- La protection des réseaux wifi
- Les architectures de sécurité

# Sécurité des Réseaux

- **Architecture de sécurité: Les zones**
  - ❑ Plusieurs zones regroupant des services, machines partageant les mêmes politiques et besoins de sécurité peuvent être définies
    - Public Zone
      - Zone non contrôler correspondant aux différents réseaux d'opérateurs, services et entités extérieurs
    - Public Access Zone
      - Zone d'accès du domaine que l'on contrôle, cette zone contiendra les différents services et équipement scommuniquant avec l'extérieur
    - Operations Zone
      - Zone regroupant l'ensemble des utilisateurs et services interne au domaine contrôler (desktop, messagerie)
    - Restricted Zone
      - Zone regroupant les services critiques et les informations sensibles

# Sécurité des Réseaux

- **Architecture de sécurité: Les zones  A vous de jouer!**



# Sécurité des Réseaux

- **Architecture de sécurité: DMZ**
  - Demilitarized Zone

    Zone tampon servant d'intermédiaire entre les requêtes et informations provenant du réseau public et les zones du réseau internes (Operations Zone, Restricted Zone),

    Segment réseau entre une zone protégée et un zone non protégée

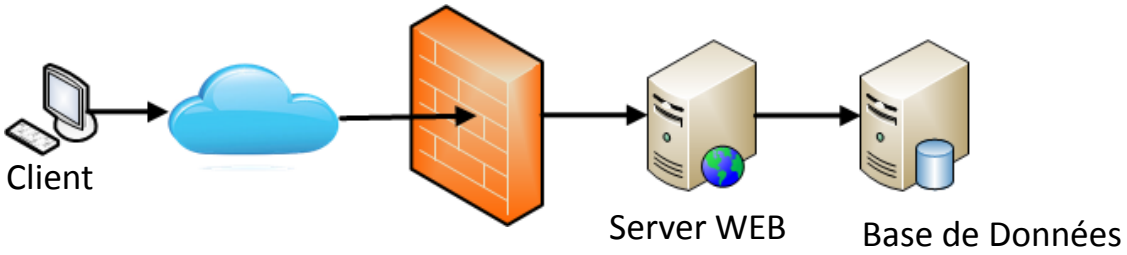
  - Une DMZ fait partie d'une Public Acces Zone

  - Utilisation des DMZ pour la réalisation d'architecture n-tiers

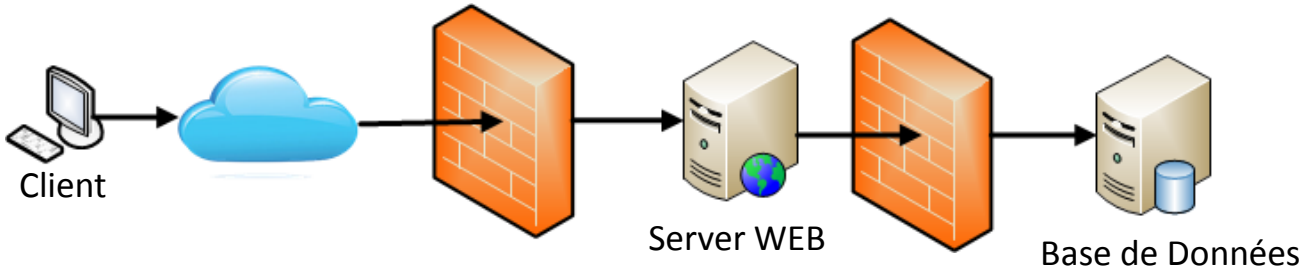
# Sécurité des Réseaux

- **Architecture de sécurité: Les DMZ**

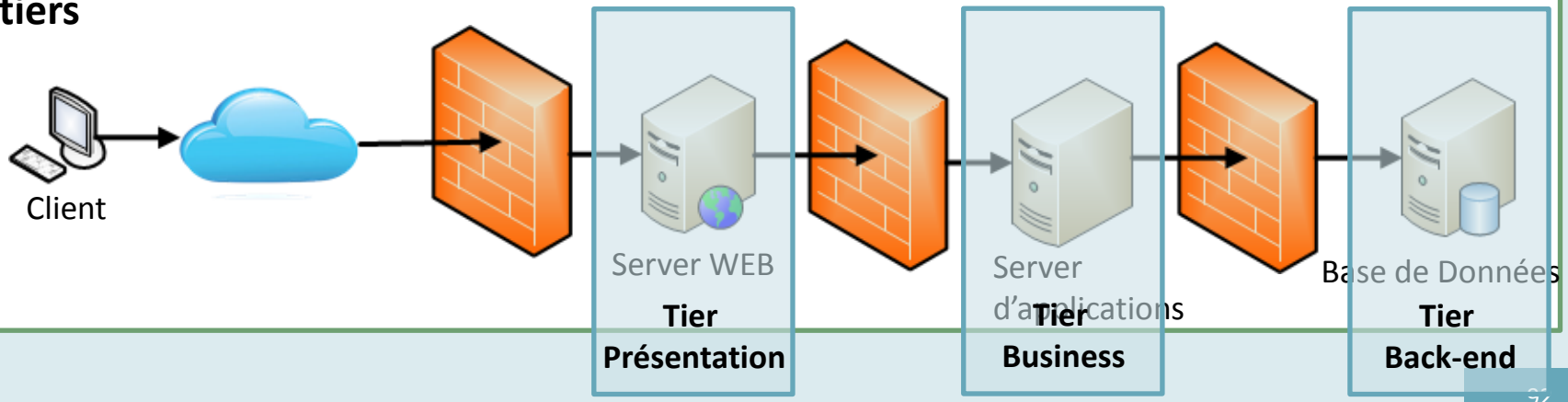
**1 tiers**




**2 tiers**

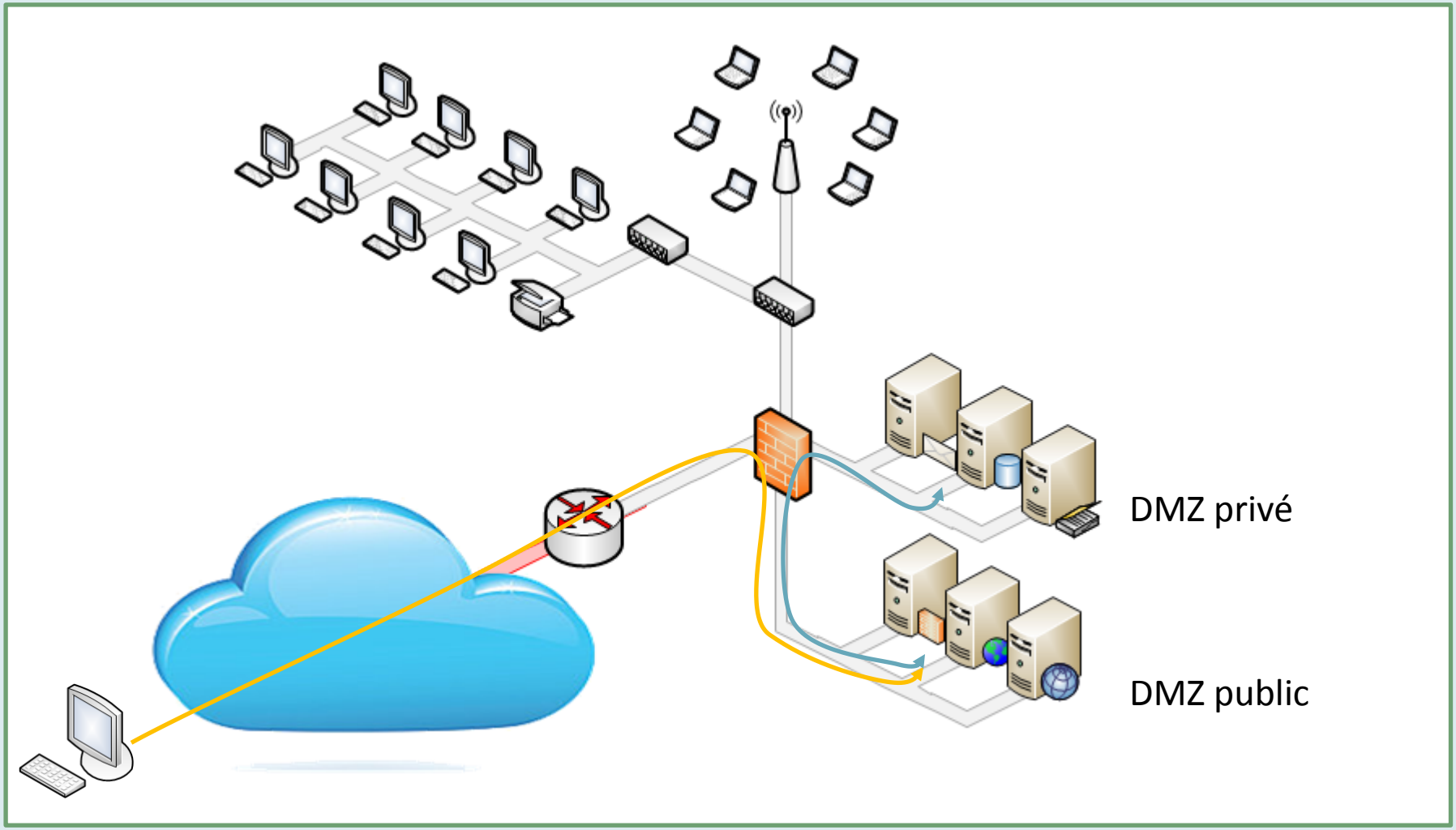



**3 tiers**



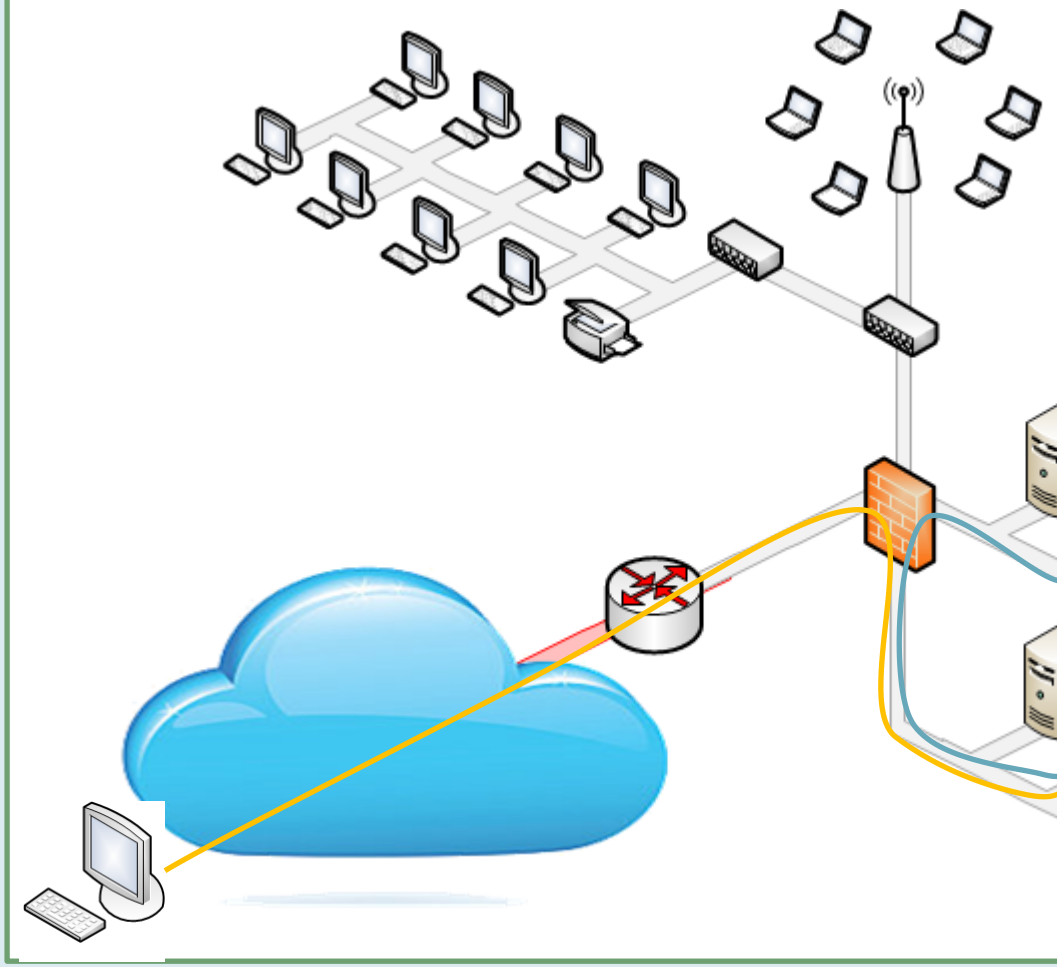
# Sécurité des Réseaux

- **Architecture de sécurité: Les DMZ**



# Sécurité des Réseaux

- **Architecture de sécurité: Les DMZ à vous!**



Décrivez les règles de firewall permettant d'autoriser :

- ce fonctionnement DMZ public/privé
- Permettant d'autoriser les utilisateurs intranet d'accéder à des sites webs extérieurs

DMZ privé

DMZ public

# Sécurité des Réseaux

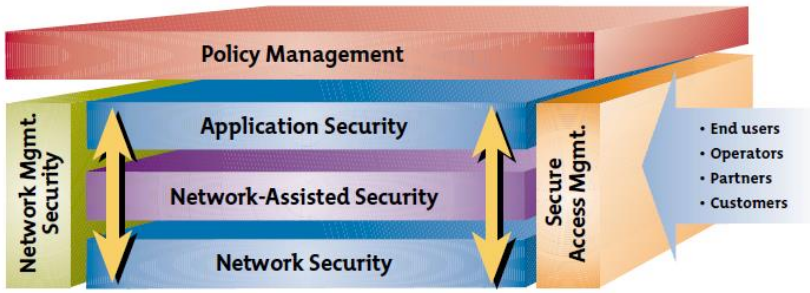
- **Architecture de sécurité: Les bonnes pratiques**

| Principles Useful for the Design of Network Security Architectures | |
|---|---|
| Fundamental IT systems security principle | Other rules expanding fundamental principles that are applied in specific conditions |
| **Compartmentalization** – IT system resources of different sensitivity should be located in different security zones (also known as Segmentation). | **Choke Point** – Access to IT system resources in the network should be provided through controlled, limited number of communication channels. |
| **Defense in Depth** – Protection of IT system resources is based on many security layers which complement and ensure one another (known also as Layered Protections). | **Defense in Multiple Places** – Security elements are distributed in different places of IT system.<br>**Defense through Diversification** – Safety of IT system resources should be based on the protection layers consisting of different kinds of safeguards (also known as **Diversity of Defense**). |
| **Adequate Protection** – Protections should be relevant to the threats and values of the resources being protected (i.e., risk analysis results), compliant with law and other regulations, and properly cooperative with other IT system elements. | **Simplicity** – The design and safeguards configuration should be simple and clear, and if technically possible, based on widely approved standards.<br>**Due Diligence** – Ensuring IT system safety requires continual activities that test that the protection mechanisms are operational and that security incidents are being detected and resolved. |
| **Least Privilege** – Subjects should have minimal privileges to IT resources which are necessary to perform company's business tasks. | **Information Hiding** – The IT system makes available only the information that is necessary for the company's business operations (also known as **Security through Obscurity**). In the designs of intrusion prevention systems the principle is known as **Attack Surface Reduction**.<br>**Need To Know** – IT system users and administrators should have access to the information relevant to their position and performed duties. |
| **Weakest Link in the Chain** – Security level of IT system depends on the least secured element of the system. | **Single Point of Failure** – Protection against failures is achieved by using redundant elements, so called High-Availability (HA).<br>**Fail-Safe Stance** – Access to IT system resources should be denied automatically in case of the safeguards failure (important for data-sensitive assets).<br>**Fail-Open Stance** – Network communication is passed through without control in case of the safeguards failure (important for mission-critical assets). |

Mariusz Stawowski,Network Security Architecture,ISSA Journal, 2009

# Sécurité des Réseaux

- **Architecture de sécurité: Les bonnes pratiques**




| Security functionality | | Network Security | Network-assisted Security | Application Security |
|---|---|---|---|---|
| L2 | Layer 2 VPN, EAP, and port security | Yes | | |
| NAT | Network Address Translation | Yes | | |
| AL | Access control List | Yes | | |
| IPsec | IPsec encryption | Yes | | |
| SRT | Secure dynamic routing | Yes | | |
| FW | Firewalling | Yes | Yes | |
| IDS | Intrusion detection | | Yes | Yes |
| SSL | SSL encryption | | Yes | Yes |
| CF | Content filtering | | Yes | Yes |
| VS | Virus scanning | | Yes | Yes |

White Paper, Unified Security Architecture for enterprise network security, Nortel Network

# Le Contrôle de sa sécurité

- IDS/IPS
- SEM

# Sécurité des Réseaux

- **Contrôler sa sécurité**
  - Pourquoi ?
    - La sécurité 100% n'existe pas !
    - Les systèmes évoluent ! Nouvelles vulnérabilités, nouvelles menaces
    - Connaitre son exposition au menaces
  - Comment ?
    - Les outils
      - IDS/IPS
      - Antivirus
      - SEM (Security Event Management)
    - Les Audits
      - Externes (tests de pénétration)
      - Outils automatiques (scanner de vulnérabilité)

# Le Contrôle de sa sécurité

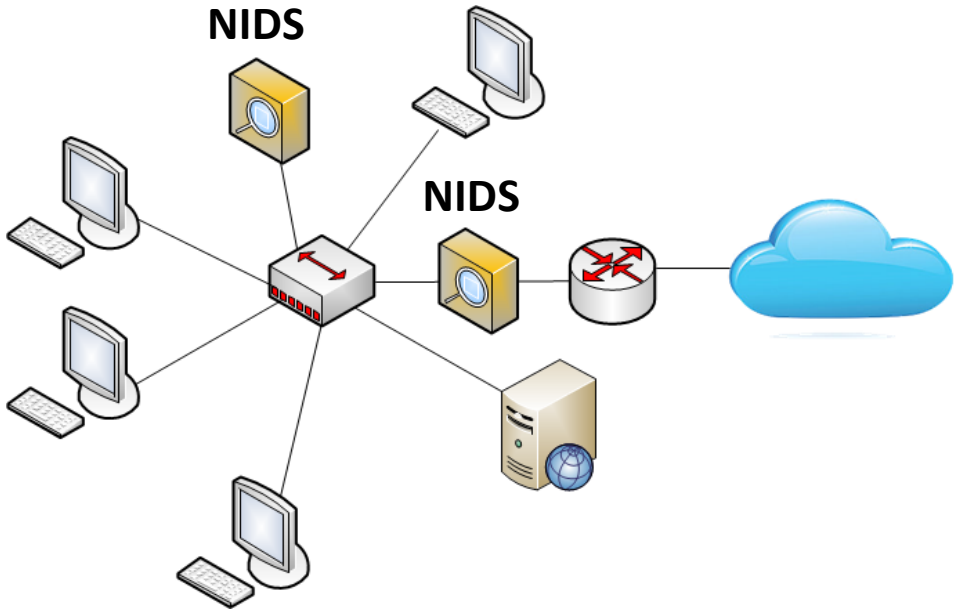
- IDS/IPS
- SEM

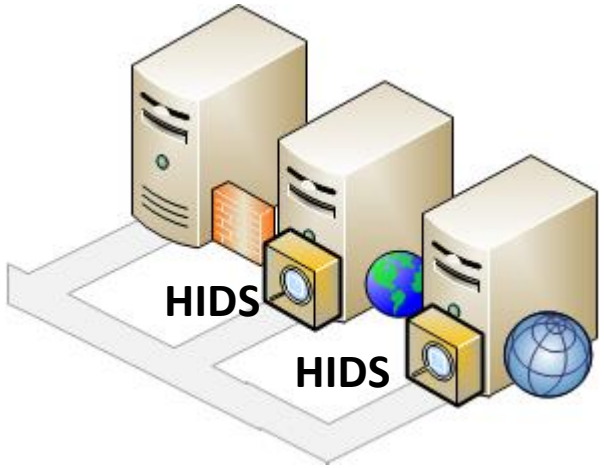
- **Contrôler sa sécurité: Les IDS**
  - **I**ntrusion **D**etection **S**ystem

    **Objectif:** *Détecter des traces d'attaques/intrusions (détection de signatures) sur un système (HIDS), sur le réseau (NIDS) ou des comportements déviants (analyse comportementale) menaçants*
  - Famille
    - Network Intrustion Detection System (**NIDS**)
    - Host Intrustion Detection System (**HIDS**)
  - Types d'analyses
    - Par signatures
    - Comportementales

# Sécurité des Réseaux

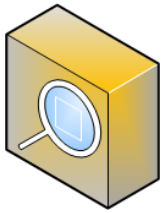
- **Contrôler sa sécurité: Les IDS**



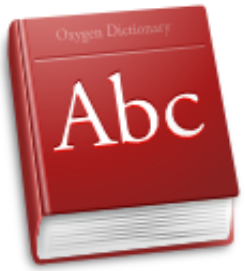
- **Contrôler sa sécurité: Les IDS**

**IDS**



**Analyse par signature**

**Liste de signatures d'intrusion**




alert tcp $EXTERNAL_NET any -> $HOME_NET 139
flow:to_server,established content**:"|eb2f 5feb 4a5e 89fb 893e 89f2|"**
msg:"EXPLOIT x86 linux samba overflow"

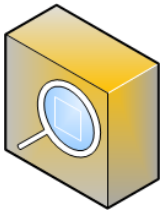
```
    16 4.101532000 134.214.56.46      134.214.49.16       DNS         73 Standard query 0x3bbb  A www.google.fr
⊞ Frame 16: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
⊞ Ethernet II, Src: HewlettP_c9:31:88 (a0:b3:cc:c9:31:88), Dst: Cisco_27:4c:cf (00:17:95:27:4c:cf)
⊞ Internet Protocol Version 4, Src: 134.214.56.46 (134.214.56.46), Dst: 134.214.49.16 (134.214.49.16)
⊞ User Datagram Protocol, Src Port: 59841 (59841), Dst Port: domain (53)
⊞ Domain Name System (query)

0000  00 17 95 27 4c cf a0 b3  cc c9 31 88 08 00 45 00   ...'L... ..1...E.
0010  00 3b 20 76 00 00 80 11  a3 51 86 d6 38 2e 86 d6   .; v.... .Q..8...
0020  31 10 e9 c1 00 35 00 27  3c 5c 3b bb 01 00 00 01   1....5.' <\;.....
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
0040  eb 2f 5f eb 4a 5e 89 fb  89 3e 89 f2              e.fr.... .
```

# Sécurité des Réseaux

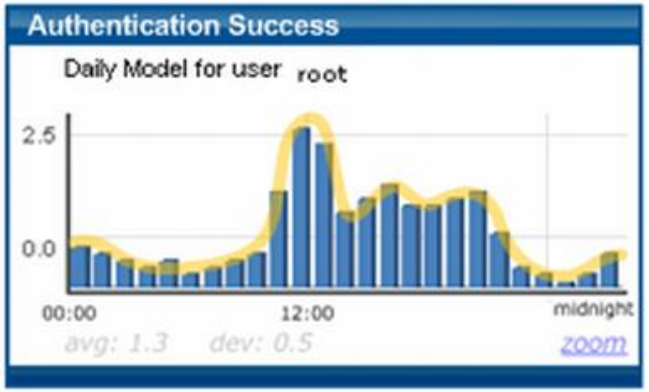
- **Contrôler sa sécurité: Les IDS**

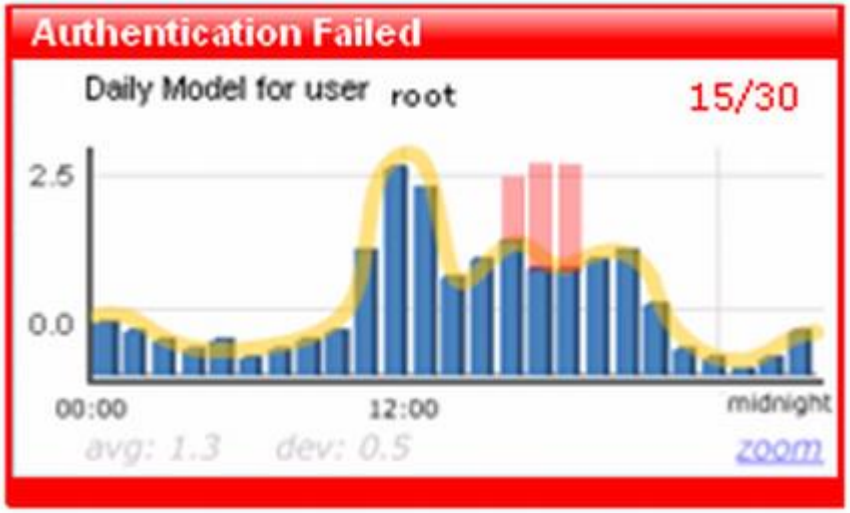
**IDS**



**Analyse Comportementale**

**Apprentissage, référence normale**

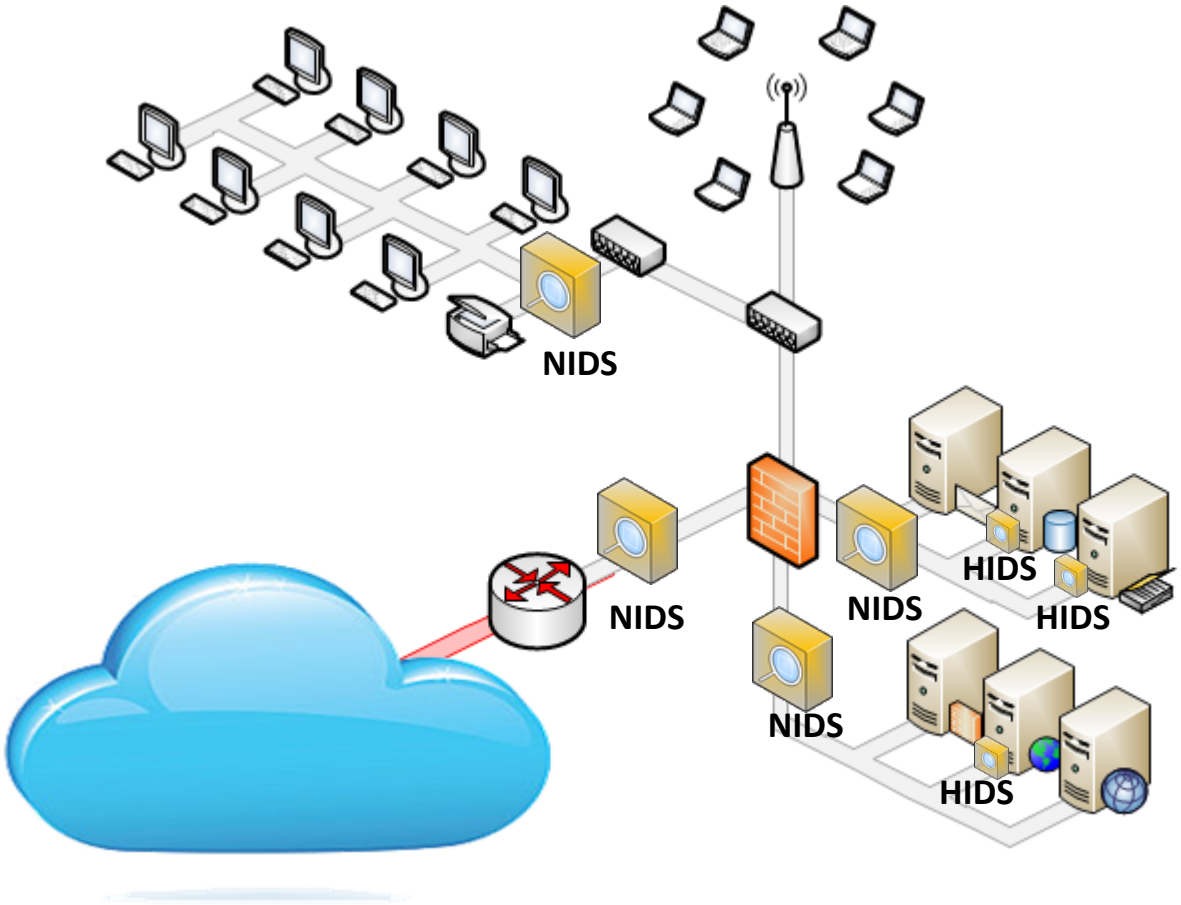



**Détection d'anomalies**

# Sécurité des Réseaux

- **Contrôler sa sécurité: Positionner ces IDS**



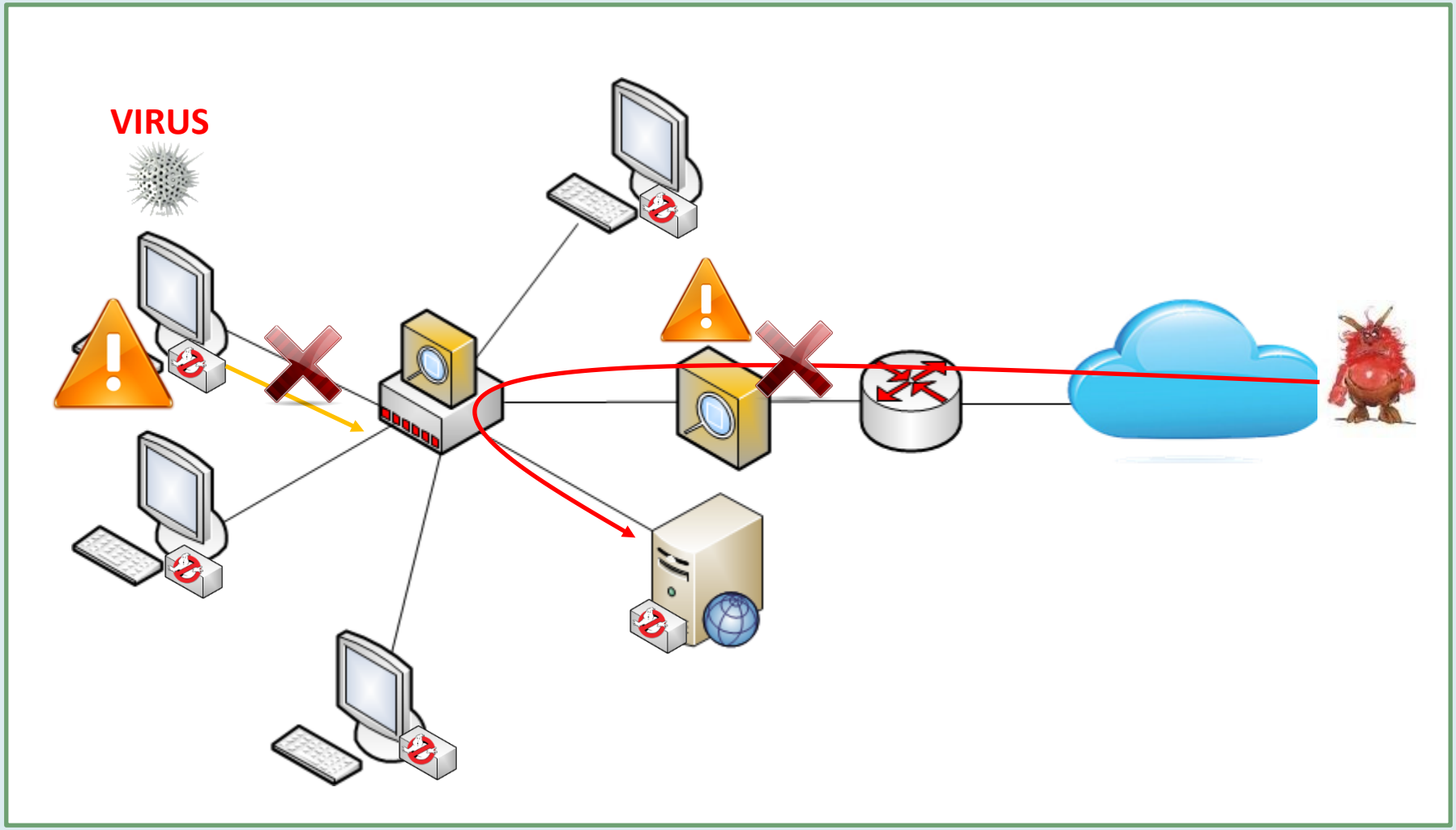
- **Contrôler sa sécurité: Les IPS**
  - **I**ntrusion **P**revention **S**ystem

    **Objectif:** *Détecter des traces d'attaques/intrusions et interrompre, isoler la source de la menace*


  - **Détection et réaction**
    - Isolement réseau (infection virale, intrusion)
    - Fermeture automatique de sessions (TCP)

# Sécurité des Réseaux

- **Contrôler sa sécurité: IPS**



# Le Contrôle de sa sécurité

- IDS/IPS
- SEM

- **Contrôler sa sécurité: Les SEM**
  - **S**ecurity **E**vent **M**anagement

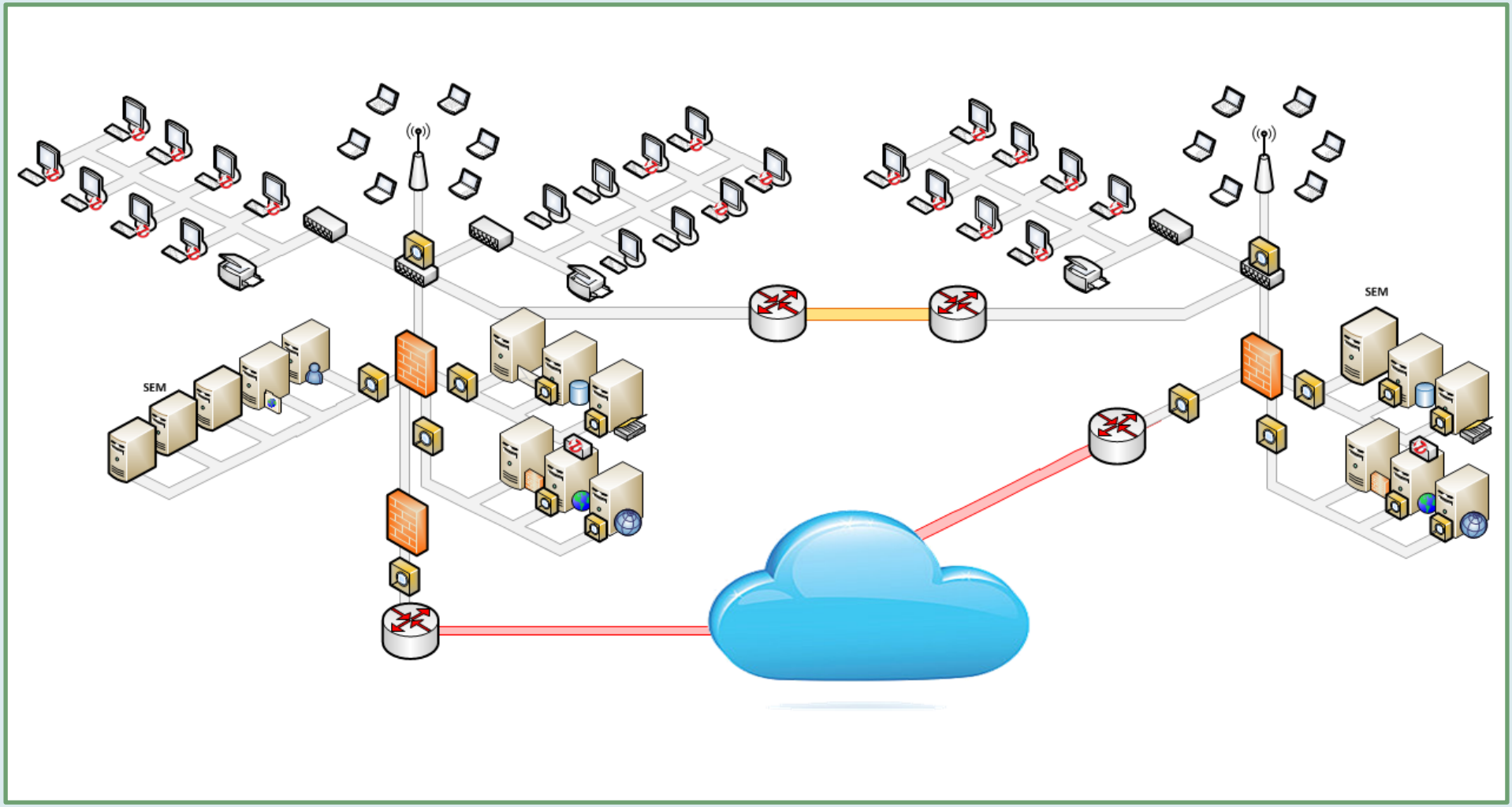
**Objectif:** *Collecter les informations du système, analyser, agréger , corréler les évènements, surveiller l'activé du **S**ystème d'**I**nformation*


- **Plusieurs composants**
  - Agents de collecte
  - Concentrateur d'information, réduction
  - Analyse de l'information
  - Présentation de l'information

- **A quoi ça sert ?**
  - Stocker les logs des systèmes (obligation légale)
  - Détecter des activités malicieuses indétectable sans vision globale

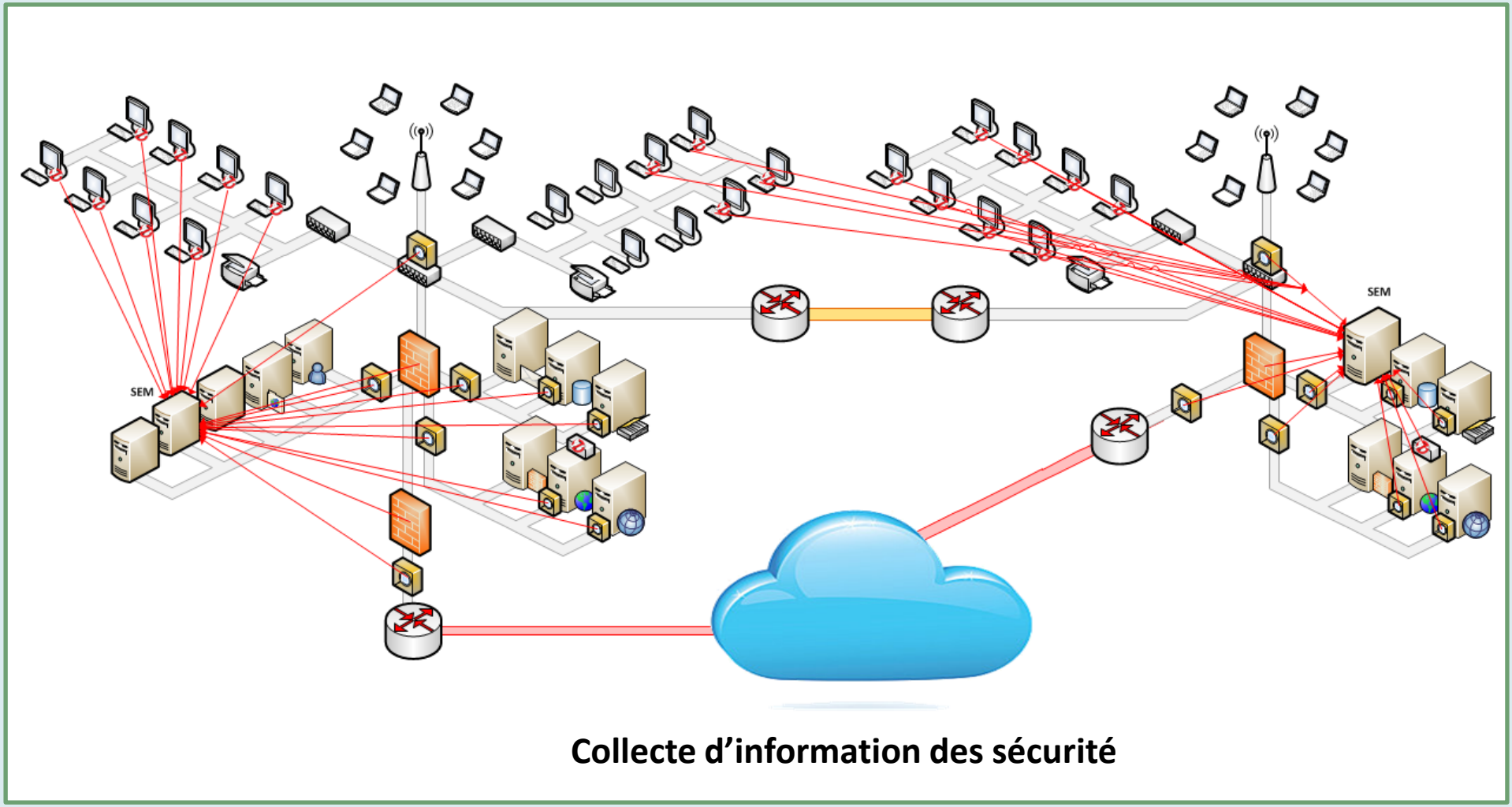
# Sécurité des Réseaux

- **Contrôler sa sécurité: SEM fonctionnement**



# Sécurité des Réseaux

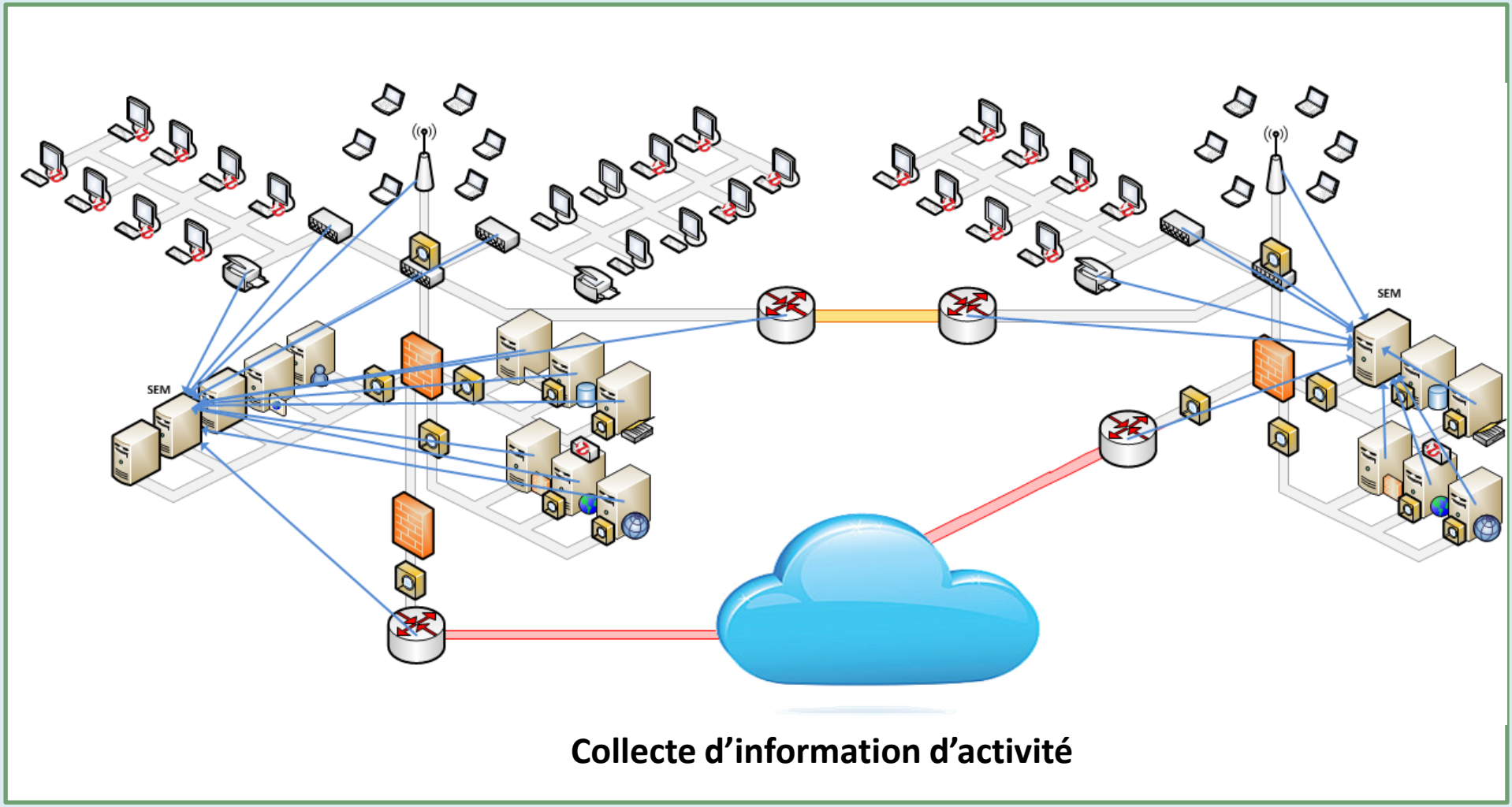
- **Contrôler sa sécurité: SEM fonctionnement**




**Collecte d'information des sécurité**

# Sécurité des Réseaux

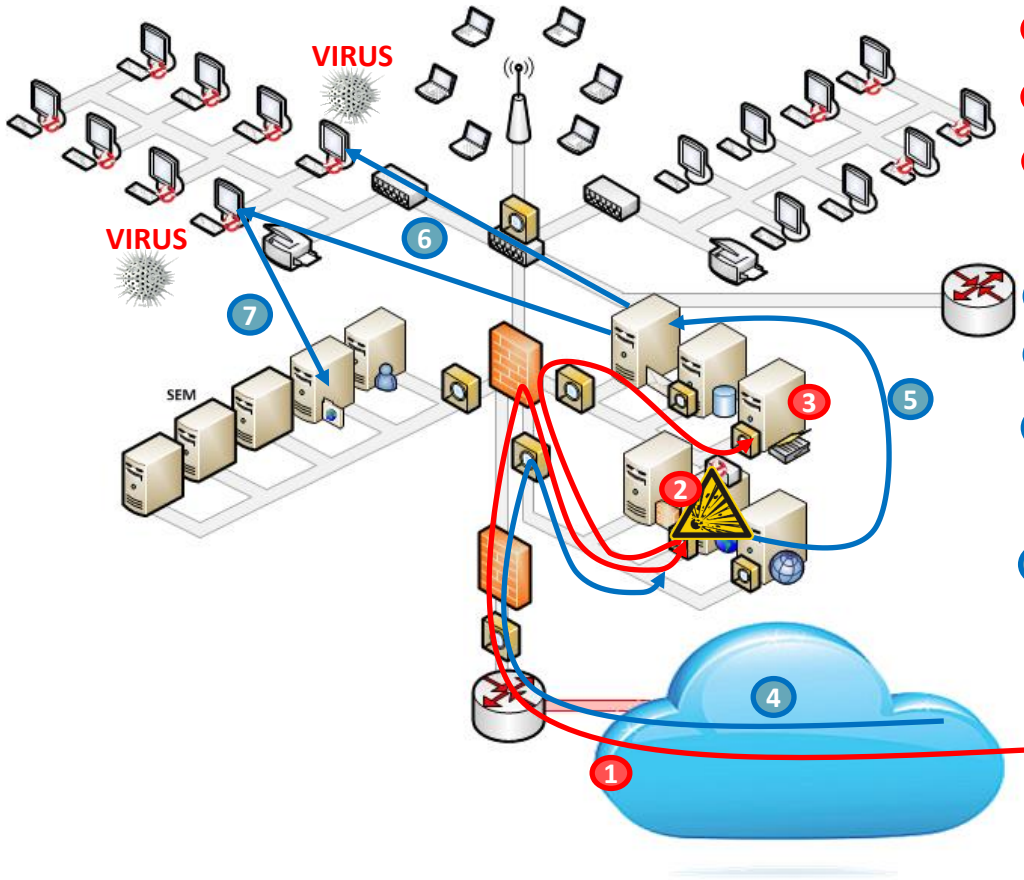
- **Contrôler sa sécurité: SEM fonctionnement**




**Collecte d'information d'activité**

# Sécurité des Réseaux

- **Contrôler sa sécurité: Exemple d'attaque détecté grave à la vision globale**




1. Accès au site internet
2. Exploit sur le site web
3. Récupération d'information de compte du serveur d'authentification
4. Reconnexion avec utilisateur valide
5. Utilisation de l'email du compte
6. Envoi de mail vérolé aux postes intranets
7. Poste intranet infecté récupère des information dans la zone sécurisée

Détection locale

Détection SEM

# Conclusion

# Sécurité des Réseaux

- **La sécurité des Réseaux**
  - Les systèmes d'information ainsi que les réseaux de communication ont comme objectif commun de rendre accessible de l'information.
    - → *Objectif premier: connectivité, productivité*
    - → *Objectif secondaire: la sécurité*
  - **La sécurité 100% n'existe pas**
    - Mettre en place des systèmes de sécurité n'est pas suffisant
    - Contrôler sa sécurité est indispensable
  - **Le niveau de sécurité d'une chaine d'information se mesure toujours par son maillon le plus faible !**
  - **Etudier toujours le ratio Usage / Sécurité**

# Questions ?