Cursus ENSEEIHT/2SN

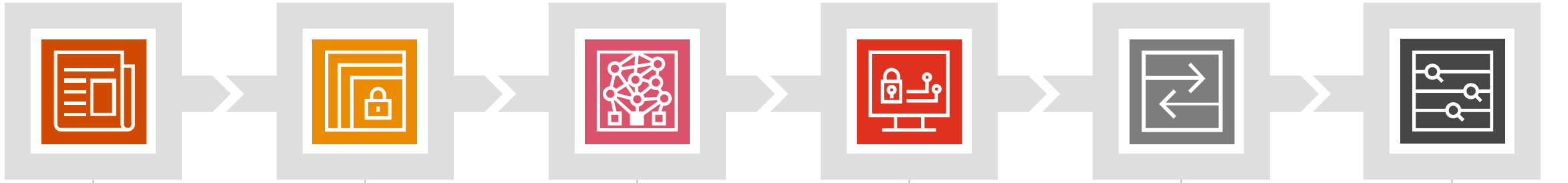
3. Sécurité des réseaux entreprise

Février 2022

pwc

INP TOULOUSE ENSEEIHT

Déroulement du module



01-Fév

1. Introduction à la sécurité des systèmes d'information

- Enjeux
- Propriétés
- Cyberattaques
- Organisation défense
- Géopolitique

08-Fév

2. Fondamentaux de cryptographie

- Terminologie
- Historique
- Crypto moderne
- Clés symétriques
- Clés asymétriques
- Signatures
- Applications
- Principes d'attaque

15-Fév

3. Sécurité des réseaux entreprise

- Couches OSI
- Défense périmétrique
- Défense en profondeur
- Switches, routeurs, parefeux, proxys
- IDS / IPS

22-Fév

4. Gestion des risques et des vulnérabilités cyber

- Cyber risques
- Approches par conformité / scénarios
- CVE / CVSS
- Buffer overflow
- Shellcode

03-Mar

5. Sécurité des protocoles de communication

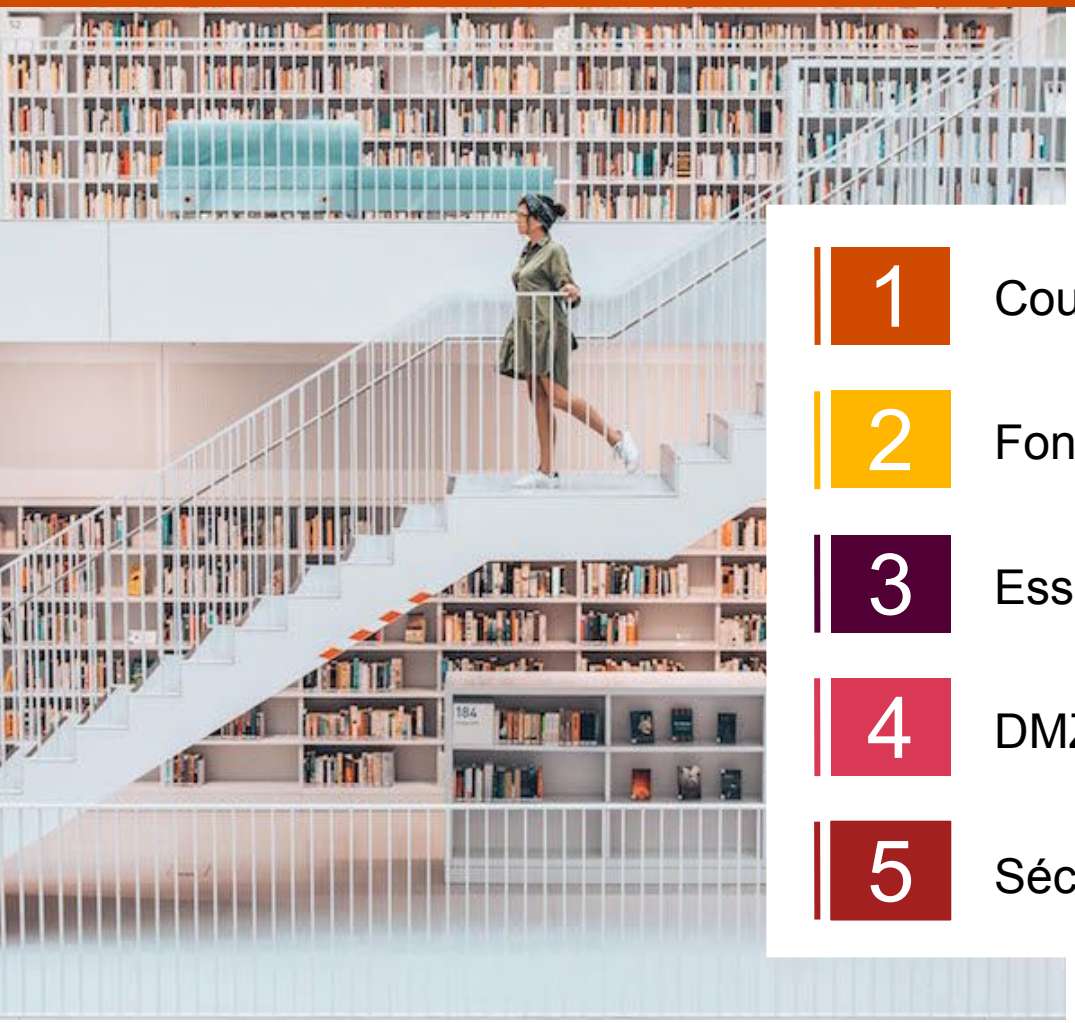
- Gestion des vulnérabilités en entreprise
- IoT
- Protocoles défaillants et protocoles sécurisés

08-Mar

6. Sécurité des applications web

- Introduction aux attaques notoires (OWASP top 10)
- Exploitation
- Défense
- Préparation TPs

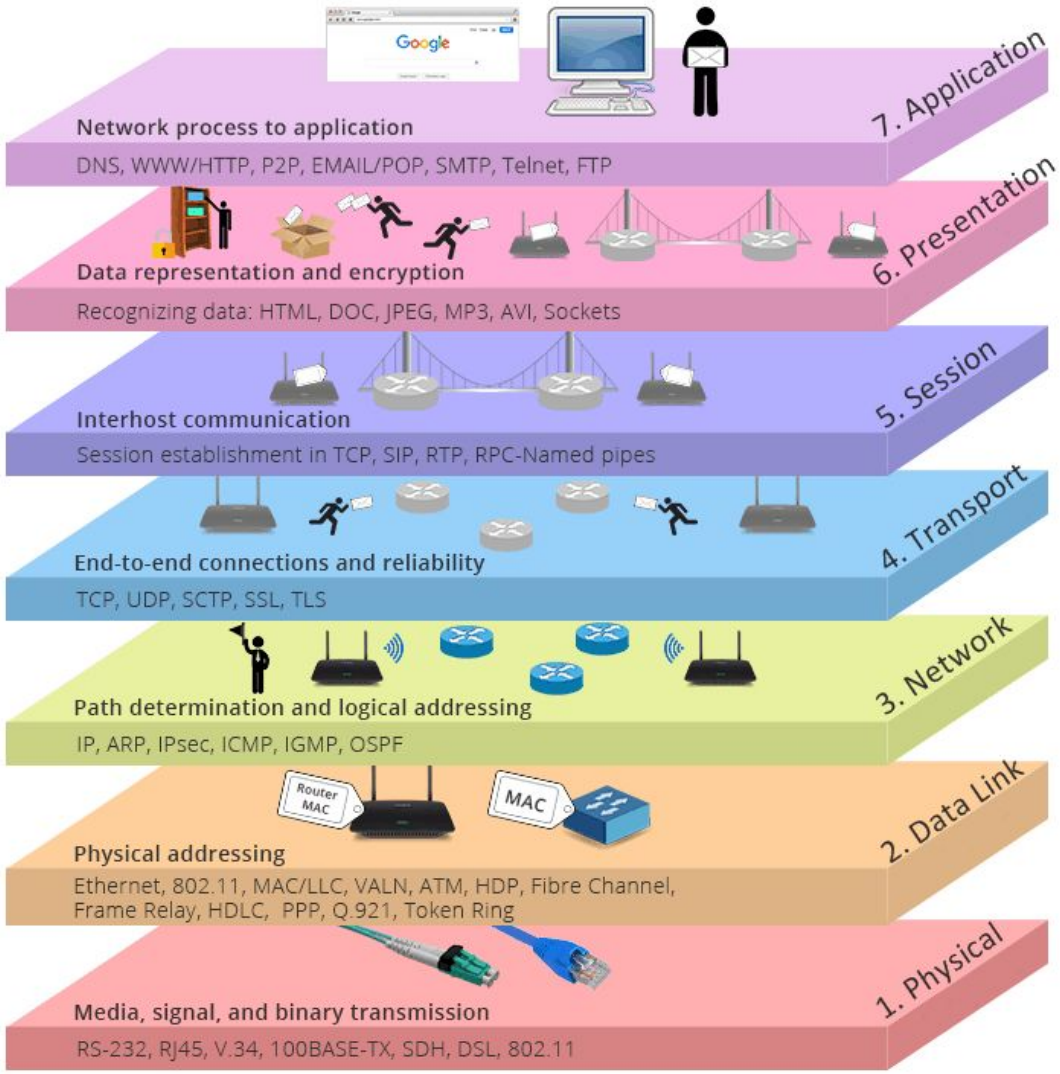
Agenda



1. Couches du modèle de référence OSI
2. Fondamentaux: switches & routeurs
3. Essentiels: parefeux & proxys
4. DMZ & architecture “sécurisée”
5. Sécurité en profondeur: IPS & IDS

Couches du modèle de référence OSI

Le modèle OSI (Open Systems Interconnection Model)



Norme de communication, en réseau, de tous les systèmes informatiques, proposée par l'ISO. Basée en 7 couches :

- Les couches “basses” ou “matérielles” :

1. Couche « physique » : transmission des signaux entre les interlocuteurs (bits). Compétence limitée à l’envoi et à la réception d’un flux de données.

2. Couche « liaison » : communications entre deux machines connectées. Capacité à identifier un destinataire via son adresse physique (MAC).

3. Couche « réseau » : communications de proche en proche, routage et adressage des paquets. Capacité à dépasser le plan d’adressage IP local.

- Les couches “hautes” ou “logicielles” :

4. Couche « transport » : gère les séquences de données (flux continu + QoS).

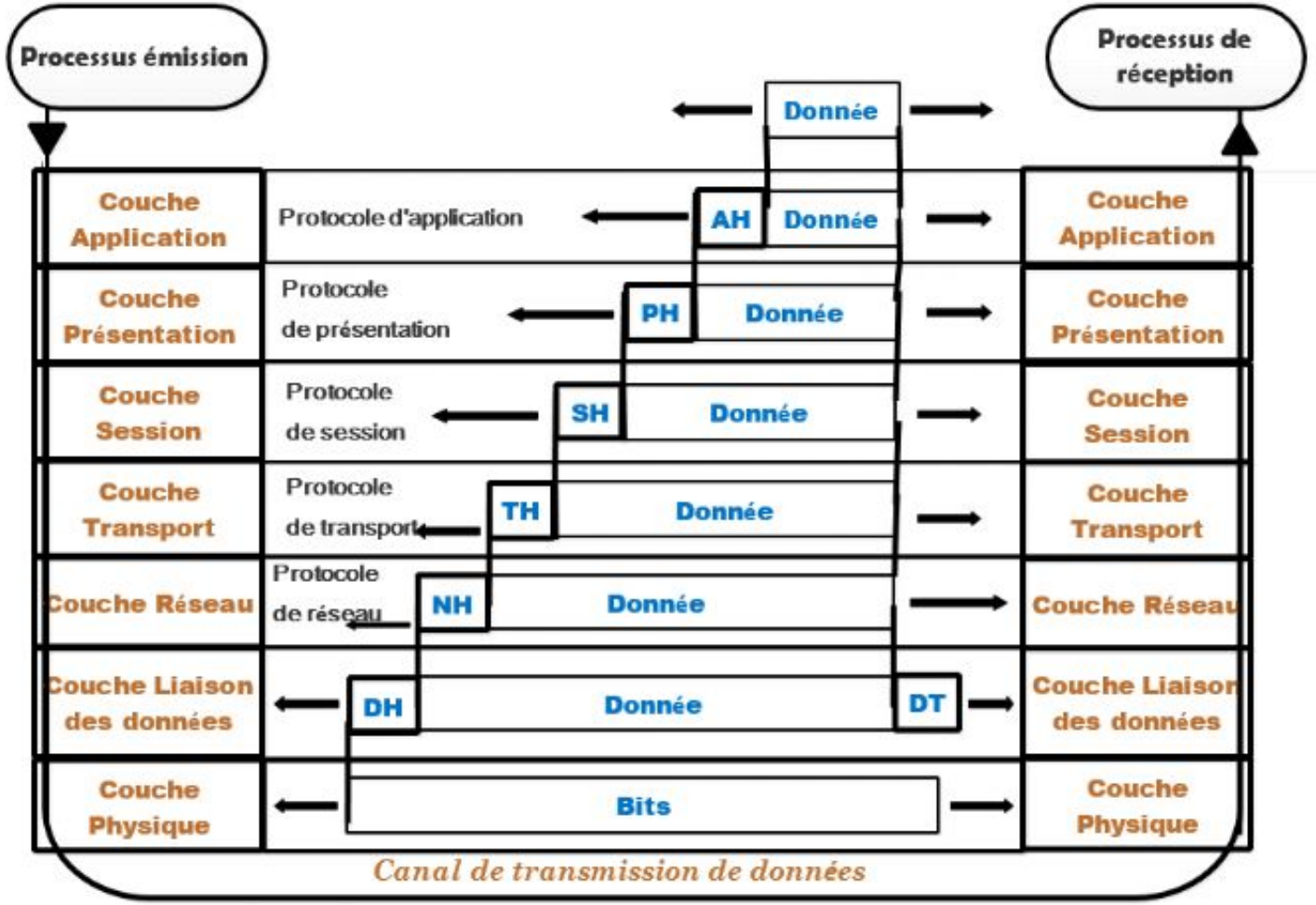
5. Couche « session » : synchronisation des échanges entre interlocuteurs.

6. Couche « présentation » : codage des données applicatives (e.g. encodage d’une vidéo lue sur un site internet par un visiteur).

7. Couche « application » : point d'accès utilisateur aux services réseaux.

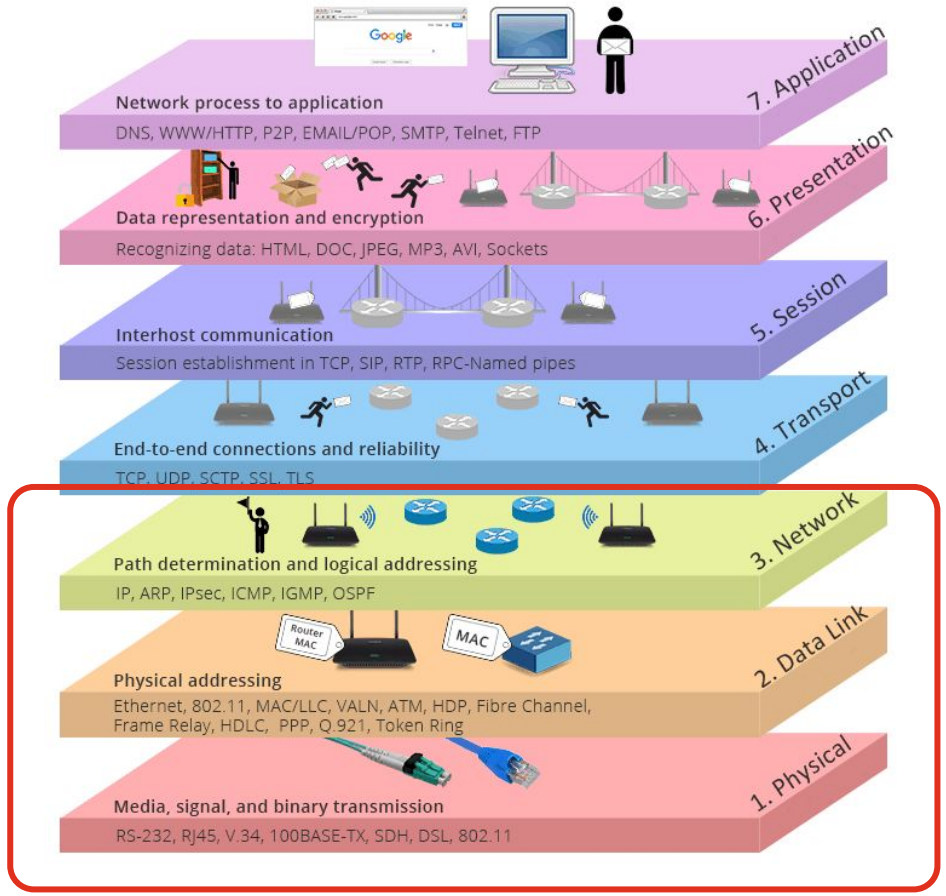
Source image: https://community.fs.com/fr/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

Le modèle OSI (Open Systems Interconnection Model)



Source image: https://www.memoireonline.com/01/20/11531/m_Deploiement-d-un-coeur-de-reseau-IPMPLS7.html

Le modèle OSI (Open Systems Interconnection Model)



Source image:
https://community.fs.com/fr/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

→ Focus de ce cours

Pourquoi? A leurs conceptions (années 70), ces protocoles (IP, ARP, TCP, UDP, ICMP,...) n'ont pas pris en compte la sécurité. La priorité était sur les enjeux opérationnels. L'éventualité que ces protocoles puissent être détournés de manière malveillante n'a pas été étudiée sérieusement (ou pas suivie).

- Absence d'**authentification** (émetteurs et récepteurs) ;
- Absence de **chiffrement** des données (donc transmises en clair) ;
- Le **routage** peut être modifié pour à rediriger un flux vers un autre destinataire.

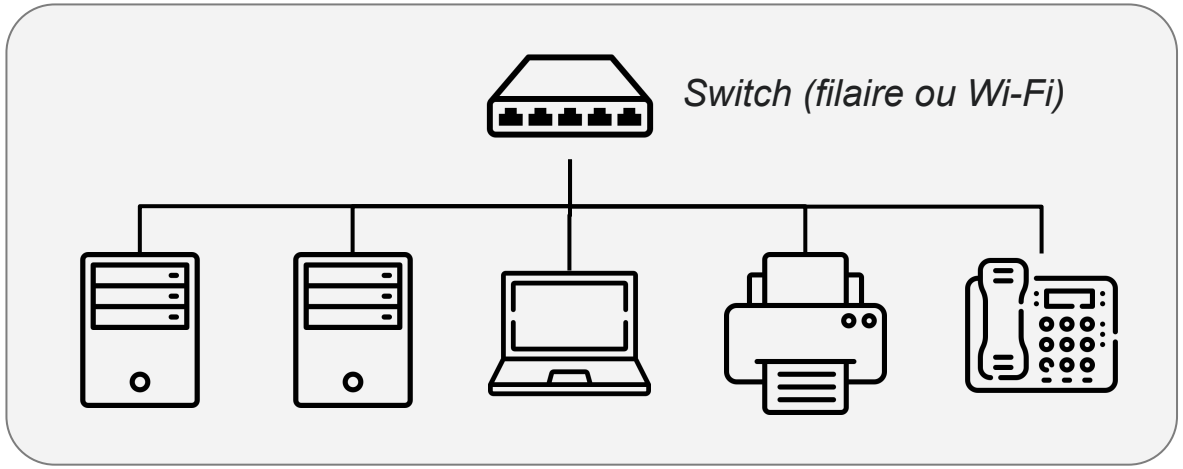
2

Fondamentaux: switches & routeurs

Switches (commutateurs) - Principe

Principe de fonctionnement

- **Switch** *ou commutateur* = multi-prise réseau
- Jusqu'au **Niveau 2** du modèle OSI
  - Basé sur les adresses MAC
- Permet à plusieurs équipements d'un même sous réseau de communiquer ensemble
- Utilise le protocole **ARP** (*Address Resolution Protocol*)
  - Garde en mémoire les adresses source, via une table de correspondance IP / MAC *(ci-contre)*
  - Envoie les paquets directement au destinataire (si l'adresse est connue), sinon le switch envoie un message broadcast sur tous les autres ports

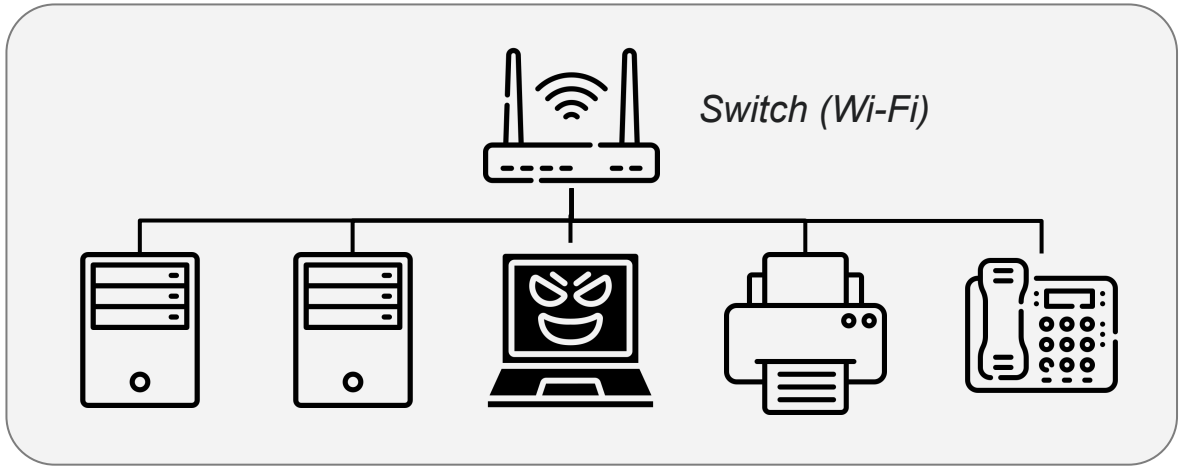



```
Interface : 192.168.1.21 --- 0x4
  Adresse Internet      Adresse physique      Type
  192.168.1.30          70-9e-29-4a-d0-81     dynamique
  192.168.1.31          84-a6-c8-36-ef-8e     dynamique
  192.168.1.254         c8-cd-72-5a-db-bd     dynamique
  192.168.1.255         ff-ff-ff-ff-ff-ff     statique
  224.0.0.2             01-00-5e-00-00-02     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  224.1.1.1             01-00-5e-01-01-01     statique
  226.178.217.5         01-00-5e-32-d9-05     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

Switches (commutateurs) - Ecoute passive

Reconnaissance / écoute passive

- Méthode utilisée par les attaquants pour effectuer une **première reconnaissance** sur un réseau, afin d'identifier les machines présentes, les protocoles utilisés etc.
- Aujourd'hui, si ce type d'attaques n'est **pratiquement plus possible en filaire**, il demeure **possible via Wi-Fi**.
    - Avant le développement des switches, les "hubs" (autre type d' équipement réseau) étaient largement utilisés.
    - Les hubs distribuaient tous les paquets à tous les destinataires (pas de différenciation par port, ou par adresse MAC).
    - Pour éviter un engorgement et diminuer la charge CPU, les cartes réseaux sont configurées par défaut pour dropper les paquets qui ne leur sont pas adressés.
    - Le mode "**promiscuous**" permet de configurer une carte réseau pour qu'elle accepte tous les paquets, y compris ceux qui sont destinés à une autre machine sur le même sous réseau.
    - Extrêmement difficile à détecter.



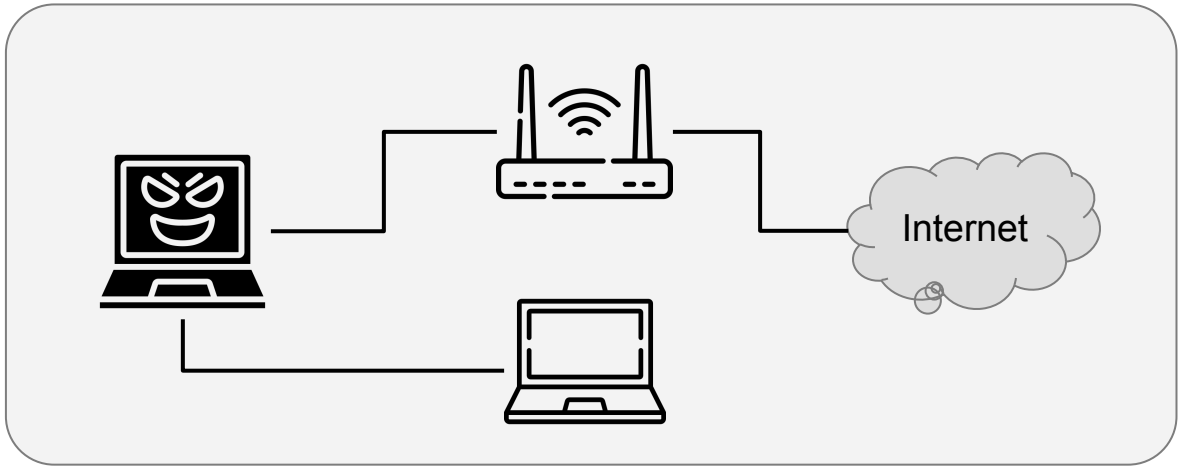
Switches (commutateurs) - ARP spoofing / poisoning

Attaque actives

- **ARP spoofing** : usurpation de l'adresse MAC de la victime afin de recevoir les messages qui lui sont destinés
- **ARP poisoning** : corruption de la table d'adressage ARP/IP du switch
- Ces deux principes permettent d'atteindre un résultat similaire : une situation de ***Man-In-The-Middle***, dans laquelle l'attaquant s'interpose entre le switch et la victime
- Autre attaque possible: déni de service en inondant le switch de requêtes ARP pour qu'il drop la table ARP/IP

Idées de défenses

- **Segmentation** : créer des zones réseaux pour limiter le risque qu'un attaquant prenne le contrôle de l'infrastructure
- **802.1X** : authentification sur un sous réseau (Wi-Fi & filaire)

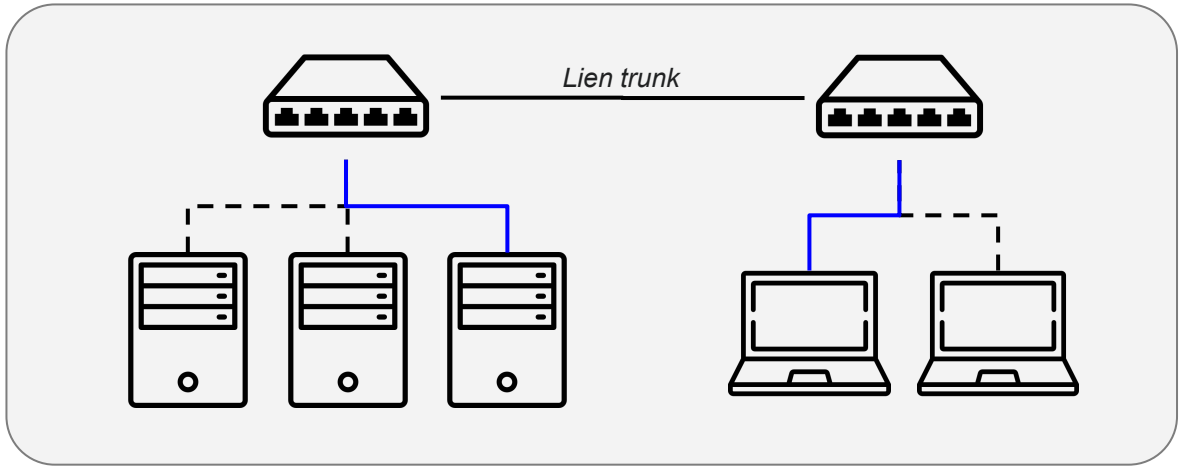



```
Interface: 192.168.43.65 --- 0x16
  Internet Address      Physical Address      Type
  192.168.43.1          08-00-27-89-03-db     dynamic
  192.168.43.220        08-00-27-89-03-db     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Switches (commutateurs) - VLANs et Standard 802.1X

Segmentation

- **Construction de zones réseaux**, en fonction des besoins métiers et utilisateurs, en respectant dans l'idéal **le principe de moindre privilège**
- Les switches permettent de créer des **VLANs** (virtual LANs) afin de dépasser les frontières physiques des sous-réseaux
    - Exemple ci contre avec 2 VLANs (bleu + pointillés) qui permettent aux équipements de communiquer malgré leur présence dans deux segments distincts
    - Un lien "trunk" est nécessaire entre les switchs pour qu'ils échangent les informations sur les VLANs et marquent les flux



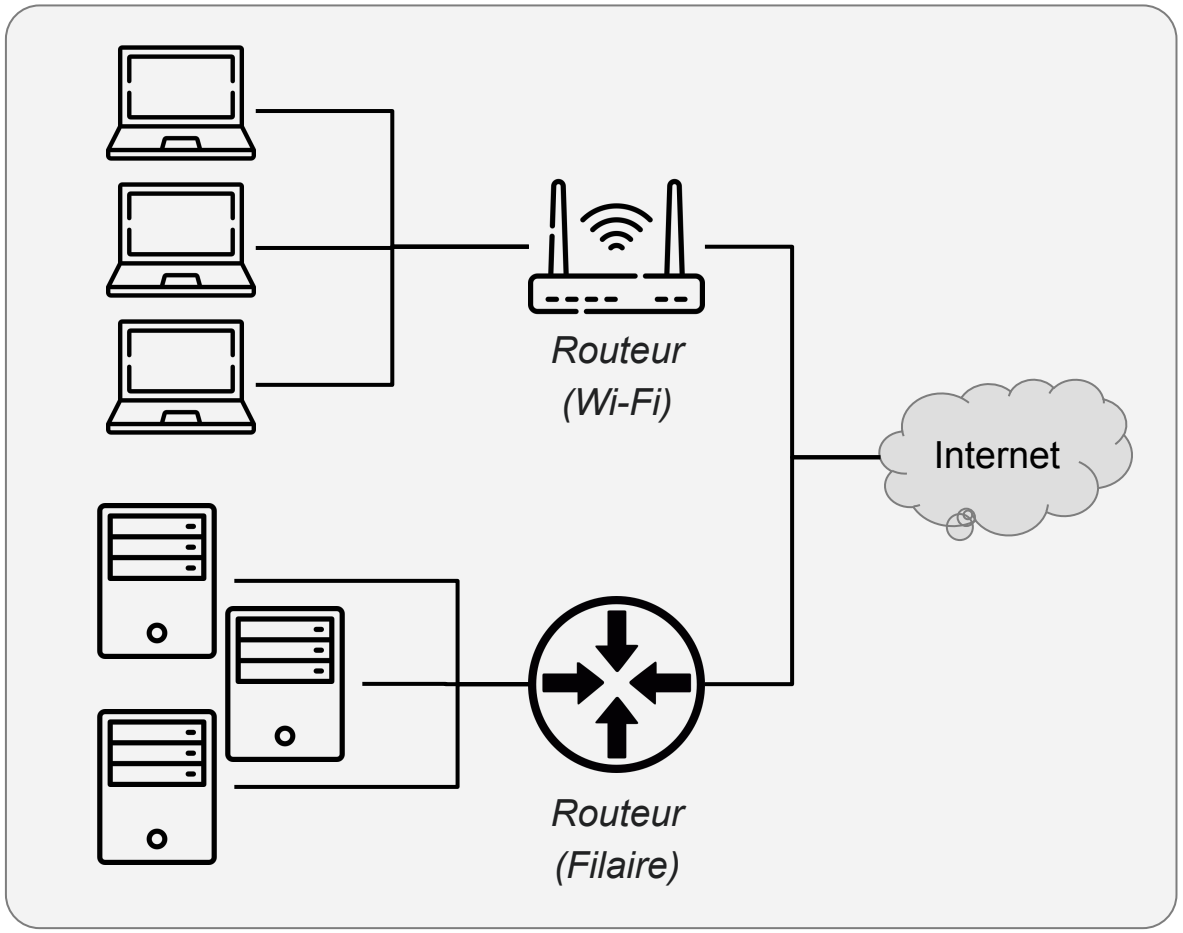
Standard 802.1X - Network Access Control (NAC)

- Permet une **authentification du matériel connecté**, une authentification **de l'utilisateur**, et une **attribution dynamique de VLAN**
    - Exemple: si vous branchez un PC perso sur le réseau ENSEEIHT, *à priori*, vous ne devriez pas avoir accès à internet
- Le standard va plus loin que les protocoles d'authentification Wi-Fi usuels, type **WPA2-Enterprise** (authentification via certificats ou serveur Radius) ou **WPA2-Personal** (Wi-Fi Protected Access 2 Pre-Shared Key / PSK : repose sur un secret commun).

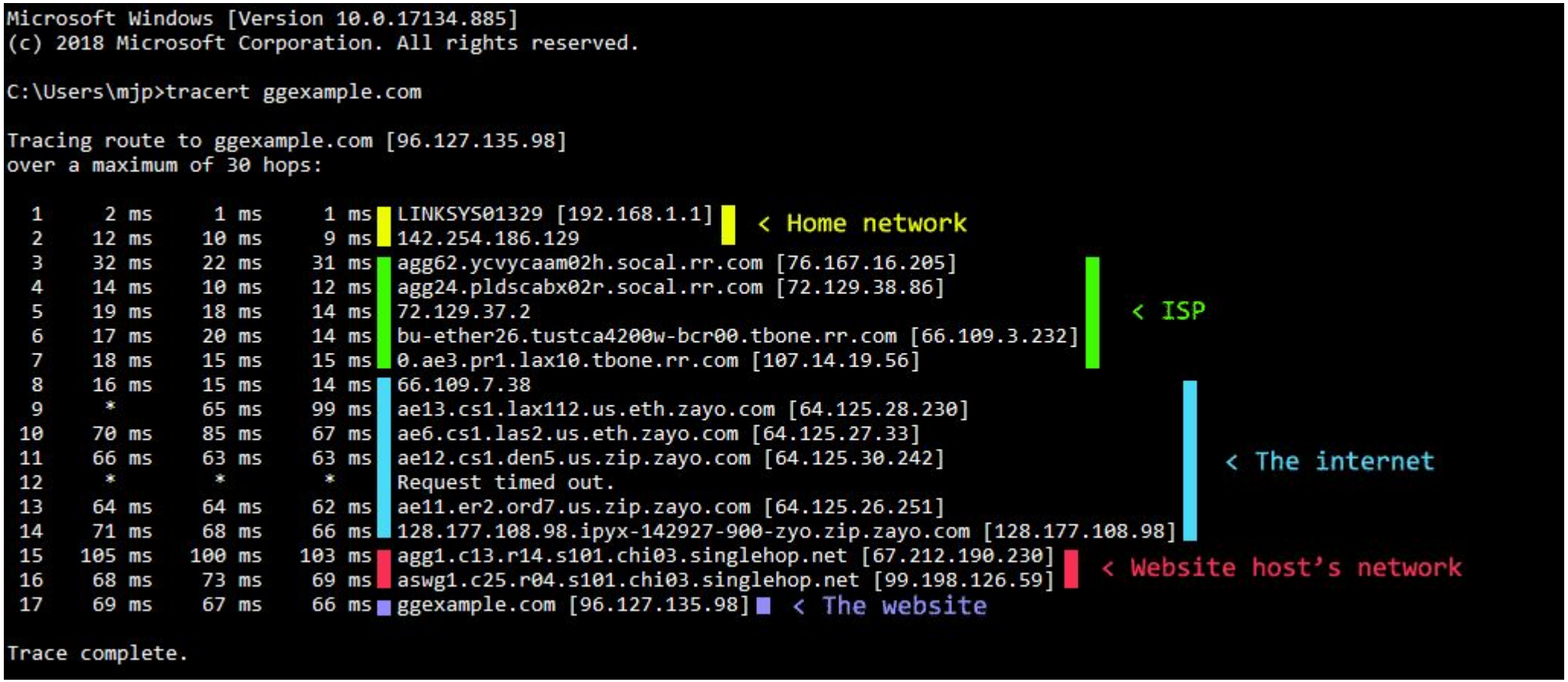
Routeurs - Principe

Principe de fonctionnement

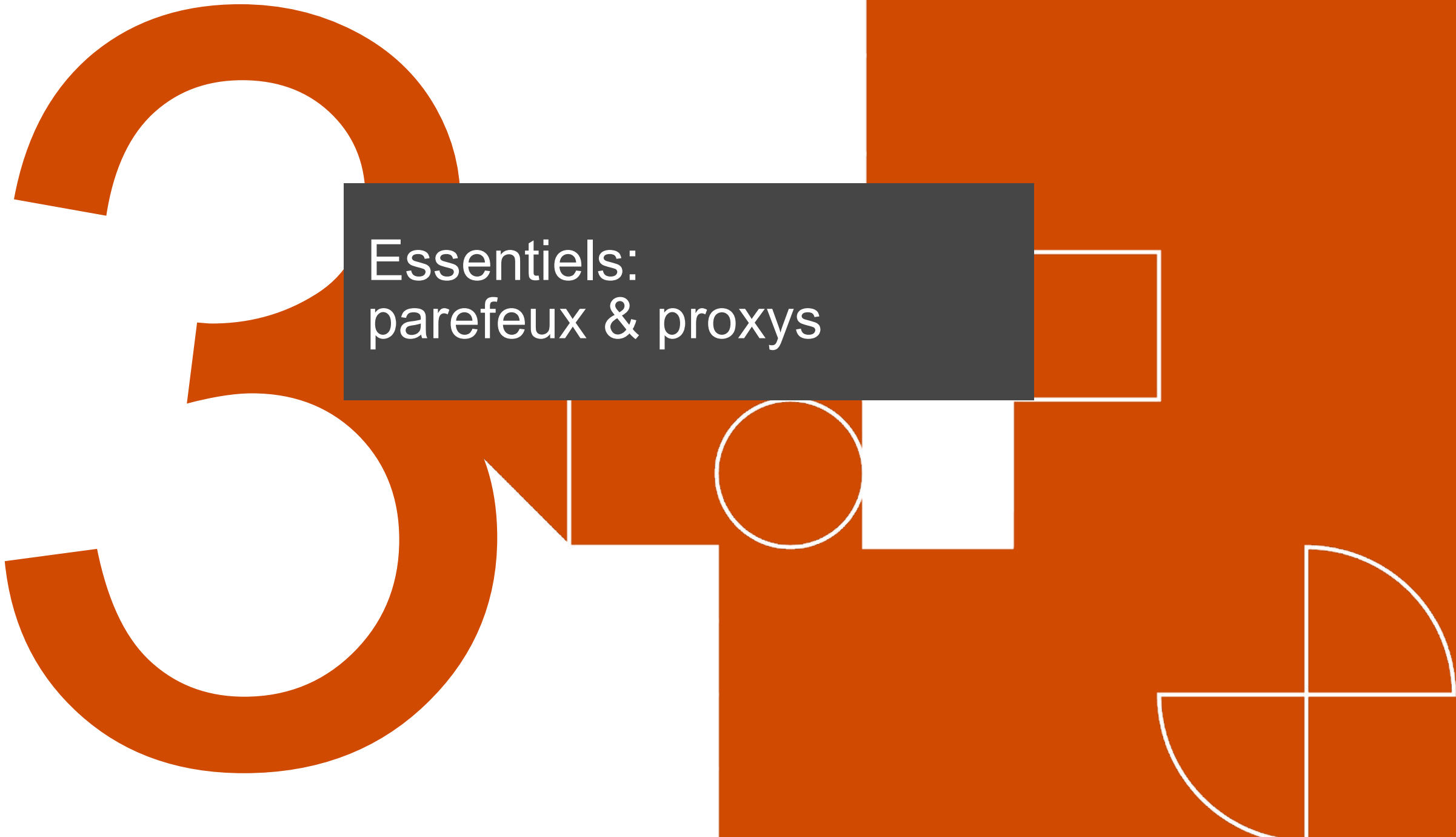
- **Rôle** = interconnection entre des réseaux différents
  - Par exemple internes (privés) // externes (publics)
  - En pratique : permet de se connecter à internet
- Dispose d'**au moins 2 IPs** (interne + externe)
  - IP interne = IP "passerelle" à indiquer aux équipements
  - IP externe = IP utilisée pour la réception des données
- **Niveau 3** de la couche OSI (IP)
- Equipement **intelligent**, administrable à distance
  - Filtrage d'adresses, de protocoles
  - Routage au niveau des réseaux
  - Amélioration et gestion du trafic (QoS)
- En pratique, la plupart des switches assurent aussi aujourd'hui des fonctions de routeur



Routeurs - Traceroute



Source image : https://www.greengeeks.com/support/article/how-to-run-a-traceroute-on-windows-mac-or-linux/

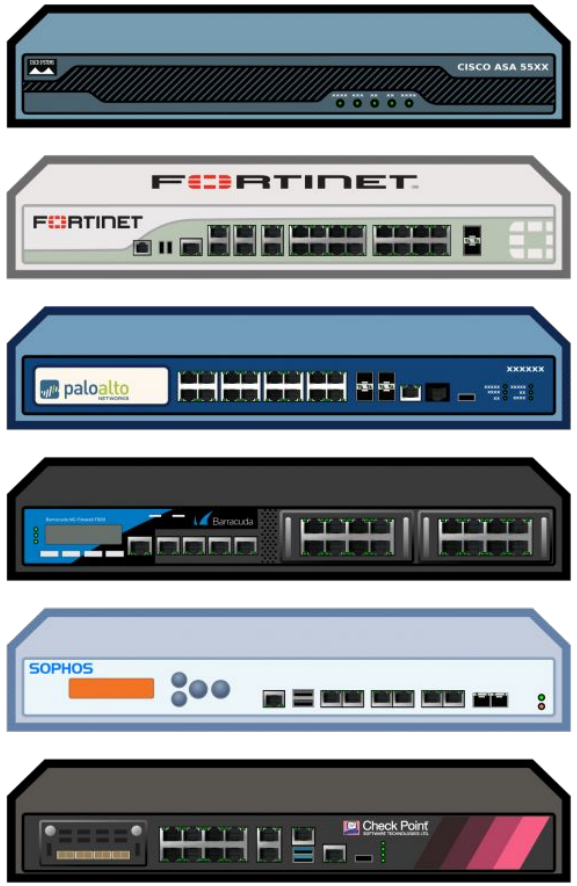


Essentiels: parefeux & proxys

Parefeux (firewalls) - Principe

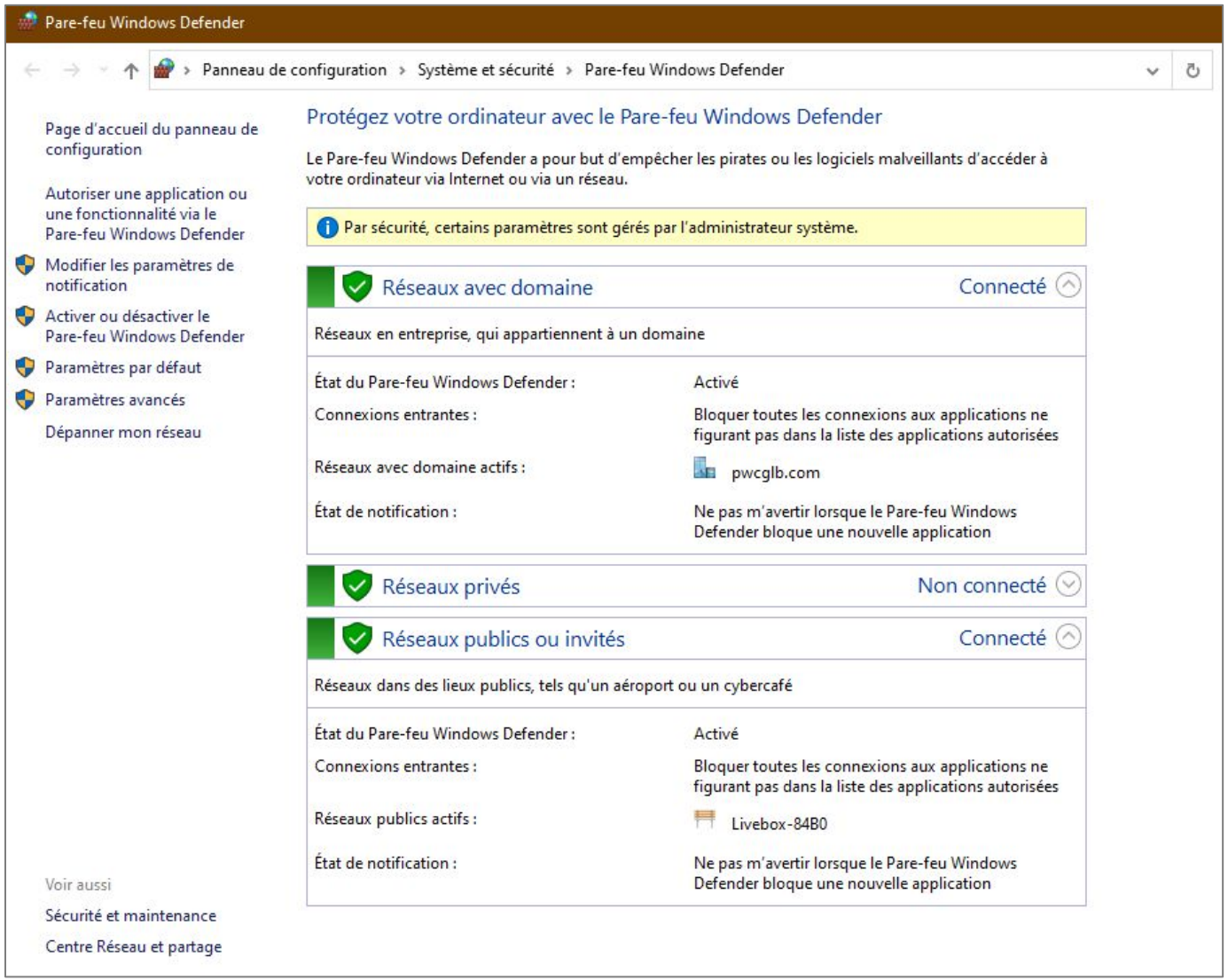
Principe de fonctionnement

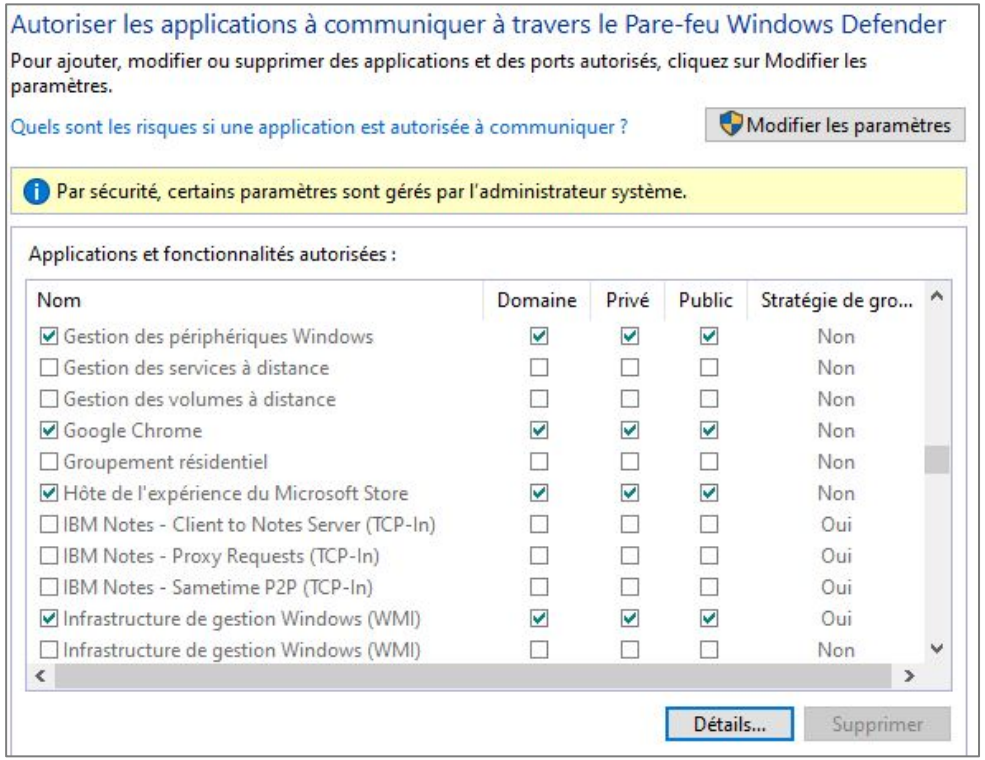
- **Rôle** = filtrage des flux réseaux (entrants & sortants)
- **Première ligne de défense → à minima 1 à l'entrée du réseau !**
- Utilisation de listes **ACL** (Access Control Lists)
  - Utilisé également dans les routeurs
  - Les données TCP/IP segmentées en paquets
  - Le parefeu examine le contenu des paquets et applique des règles
    - Transmission du paquet
    - Suppression du paquet
- Il peut s'agir aussi bien d'un équipement réseau **physique** (*voir ci-contre*) que d'un **logiciel embarqué** (e.g. Parefeu Windows)
- A minima, un parefeu doit couvrir la **couche 4 OSI** (transport) pour pouvoir faire du **suivi de connection** : "**Stateful Packet Inspection**"
- Certains parefeux professionnels couvrent toutes les couches OSI (niveaux 1 à 7) et disposent de capacités d'introspection applicatives



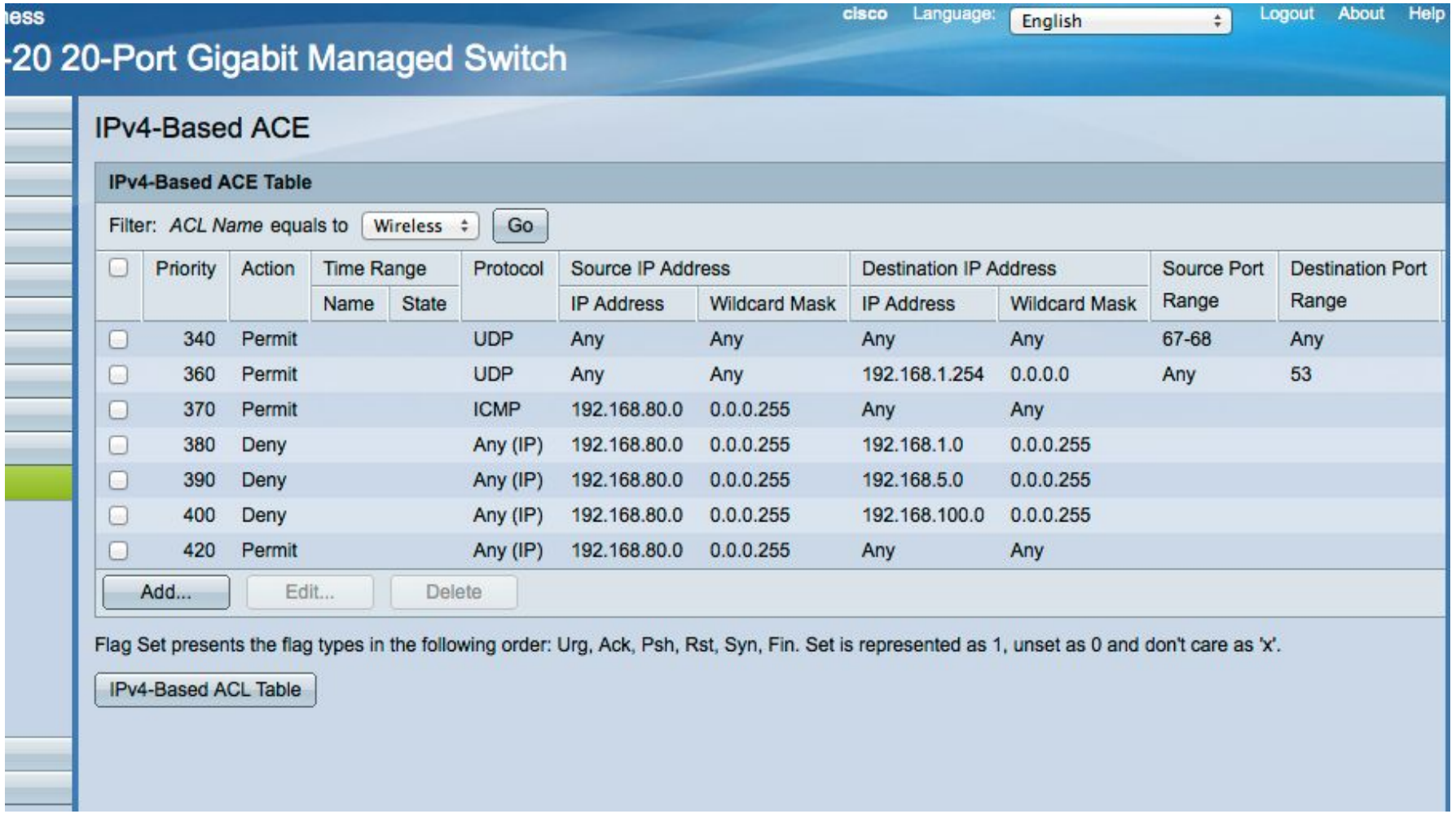
Source image: https://firewall.firm.in/hardware-firewall/

Parefeux (firewalls) - Parefeu personnel (Windows)





Access Control List (ACL)



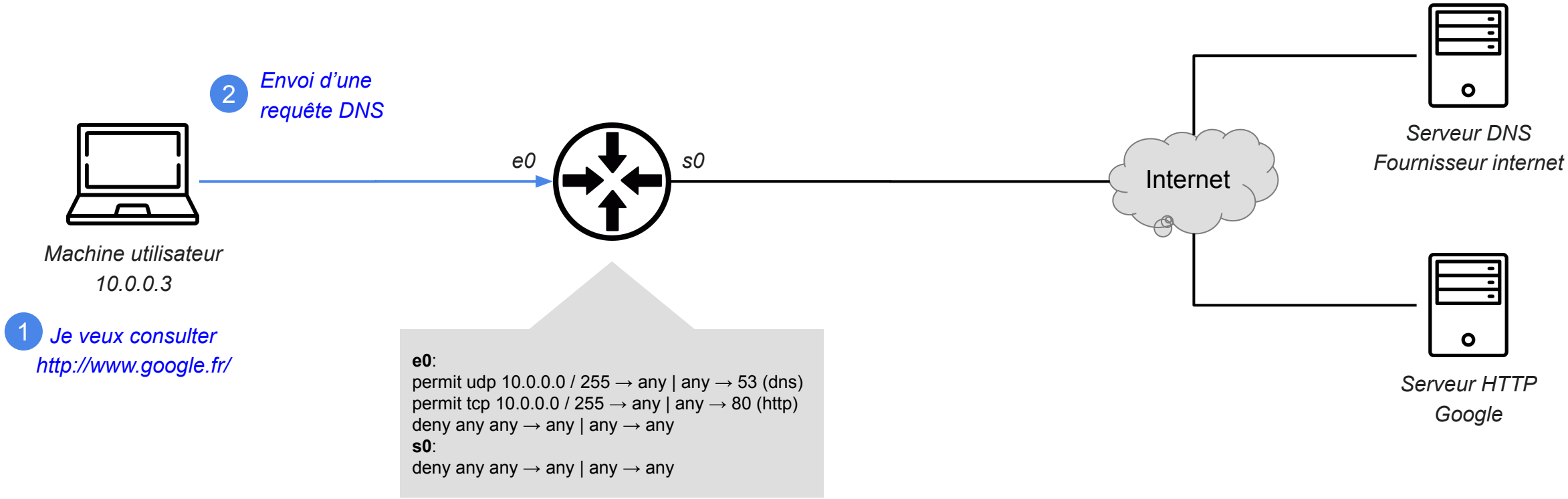
	Priority	Action	Time Range		Protocol	Source IP Address		Destination IP Address		Source Port	Destination Port
			Name	State		IP Address	Wildcard Mask	IP Address	Wildcard Mask	Range	Range
	340	Permit			UDP	Any	Any	Any	Any	67-68	Any
	360	Permit			UDP	Any	Any	192.168.1.254	0.0.0.0	Any	53
	370	Permit			ICMP	192.168.80.0	0.0.0.255	Any	Any		
	380	Deny			Any (IP)	192.168.80.0	0.0.0.255	192.168.1.0	0.0.0.255		
	390	Deny			Any (IP)	192.168.80.0	0.0.0.255	192.168.5.0	0.0.0.255		
	400	Deny			Any (IP)	192.168.80.0	0.0.0.255	192.168.100.0	0.0.0.255		
	420	Permit			Any (IP)	192.168.80.0	0.0.0.255	Any	Any		

Source image : https://community.cisco.com/t5/small-business-switches/sg300-ace-creation-quot-already-exists-quot/td-p/2371907

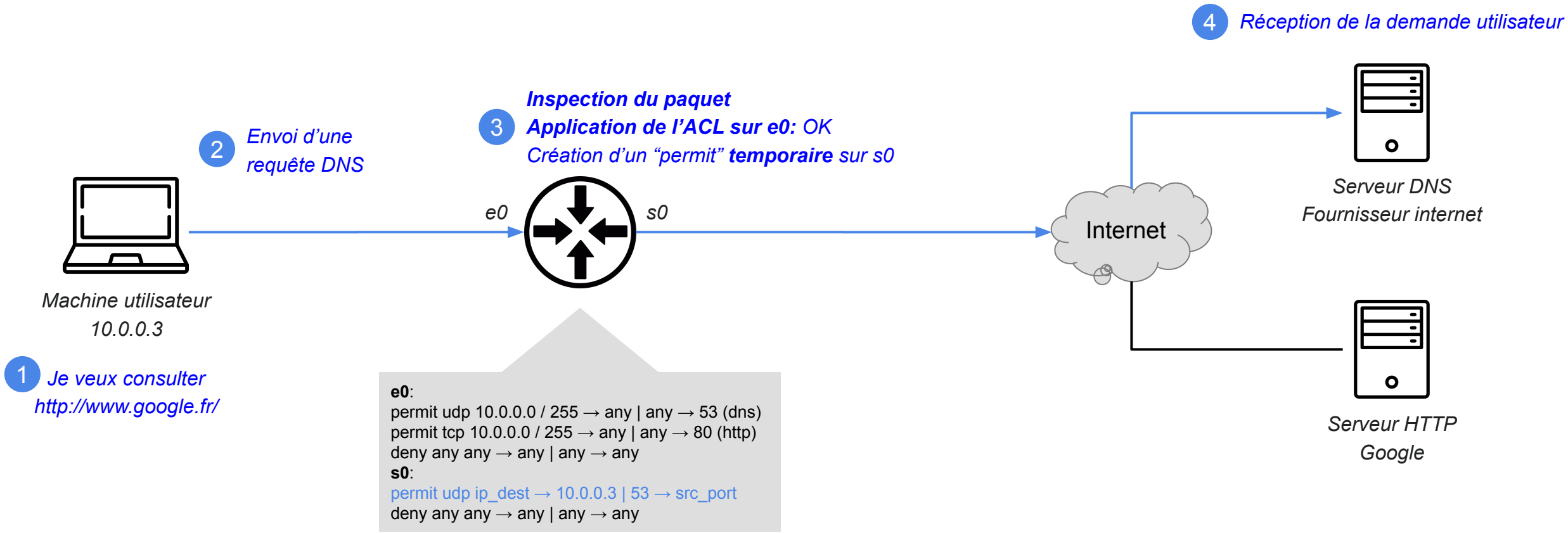
Bonnes pratiques

1. **Seuls les trafics des services autorisés doivent être permis (explicitement)**
2. **Toujours terminer les règles par un DENY ALL**
3. **Restreindre** l'accès aux interfaces d'administration (par exemple via un VLAN d'administration dédié)
4. Privilégier les accès chiffrés
5. Veiller à mettre à jours les **firmware** (qui s'avèrent régulièrement vulnérables)
6. Veiller à respecter une **politique de mots de passe** forte (complexité + MàJ)

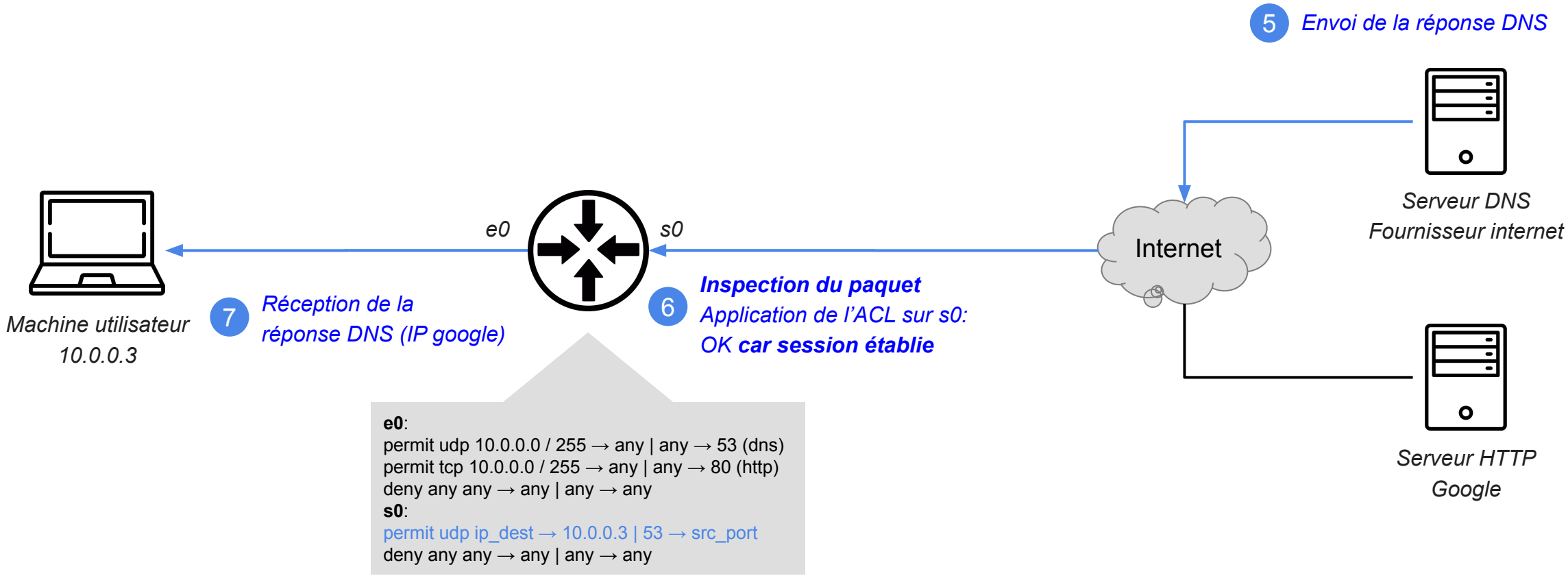
Fonctionnement des ACLs dynamiques (1/5)



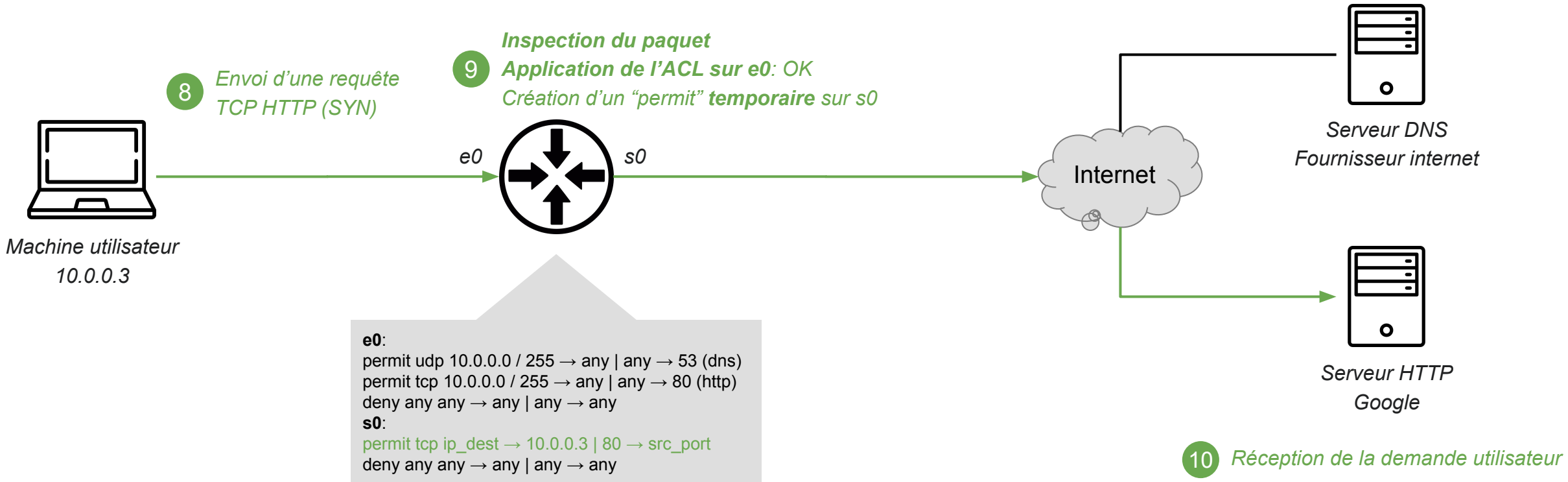
Fonctionnement des ACLs dynamiques (2/5)



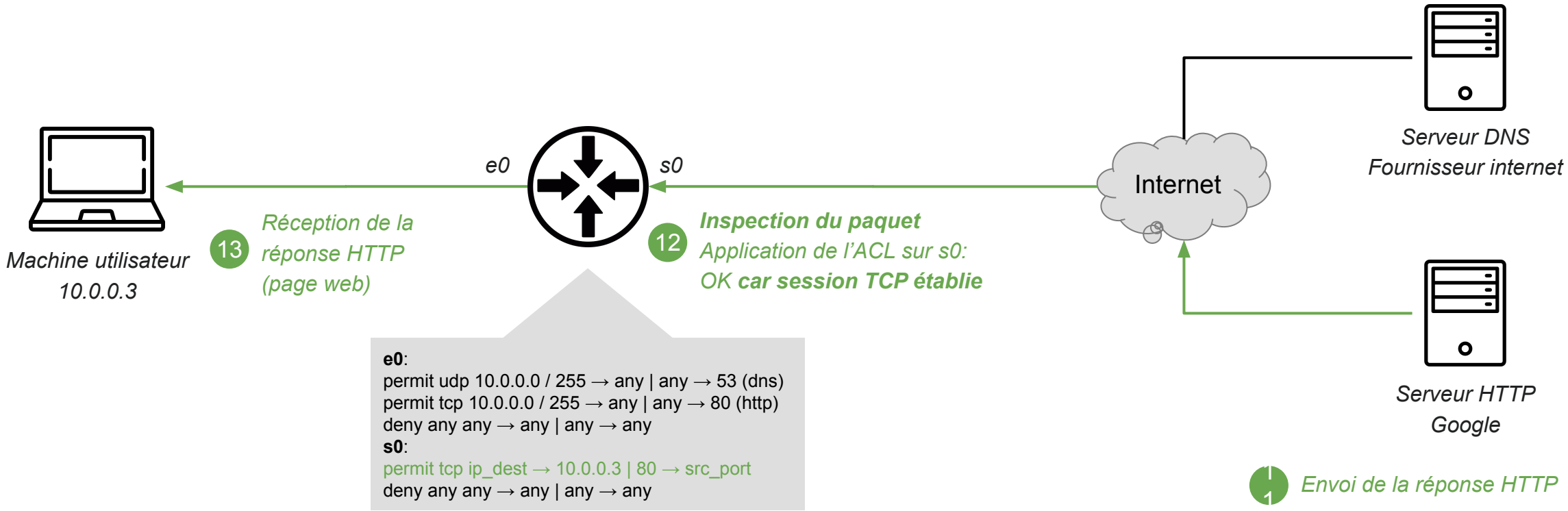
Fonctionnement des ACLs dynamiques (3/5)



Fonctionnement des ACLs dynamiques (4/5)



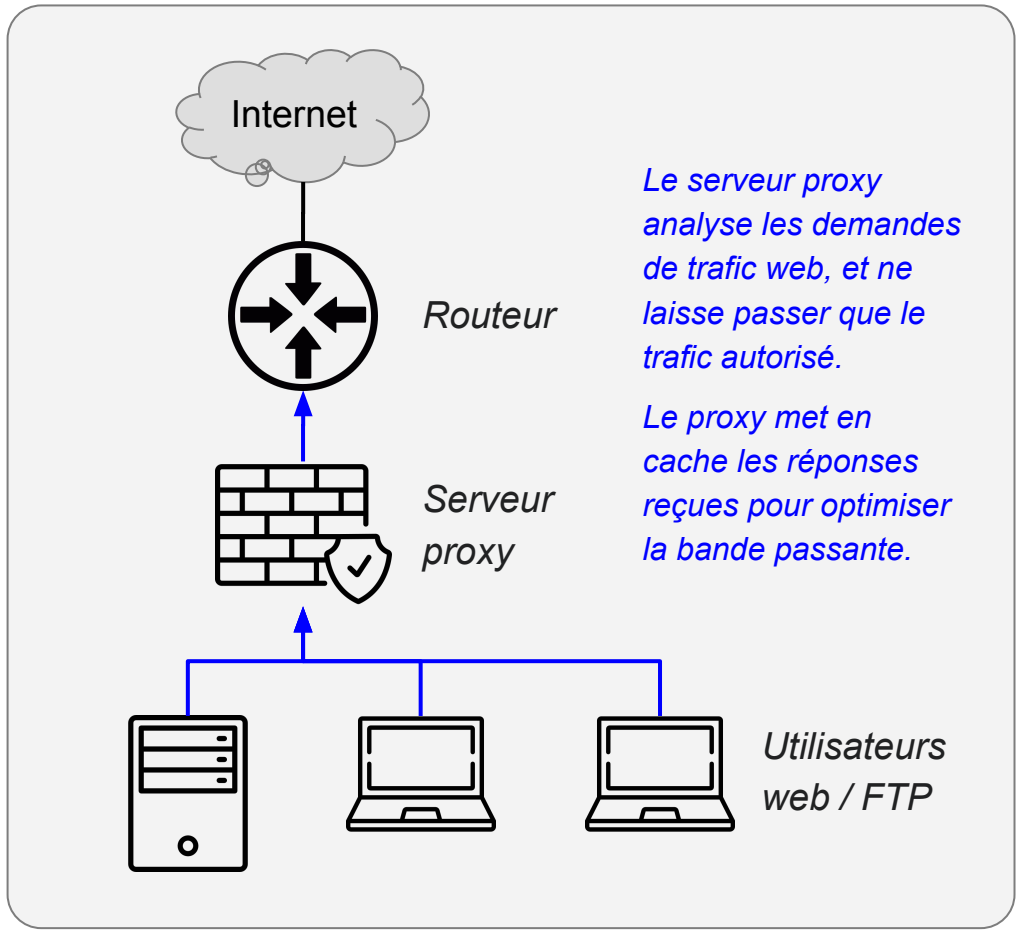
Fonctionnement des ACLs dynamiques (5/5)



Serveur proxy - Principe

Principe de fonctionnement

- **Rôle** = Intermédiaire / entremetteur
- **Cache de consultation Web** (ainsi que certains protocoles de transfert de fichiers comme FTP)
- **Objectif = surveiller et limiter le trafic applicatif** (couche OSI 7)
    - Un proxy sait faire la différence entre un flux vidéo Youtube, une payload Java, une intéraction via Javascript, un téléchargement de fichiers, ou un mail envoyé en SMTP
- Permet de **contrôler** et **enregistrer les demandes vers l'extérieur**
    - Seul le proxy peut traverser le routeur
    - Les autres machines sont interdites
    - En retour, le routeur ne parle qu'au proxy
- Les proxys utilisent souvent des mécanismes de **catégorisation** des contenus ou des IPs



Serveur proxy - Example de catégories Symantec Bluecoat

Source: http://sitereview.bluecoat.com/#/category-groups

Serveur proxy - Example de catégories Symantec Bluecoat

Symantec
A Division of Broadcom

CATÉGORIES

Catégories / Descriptions

Descriptions des catégories

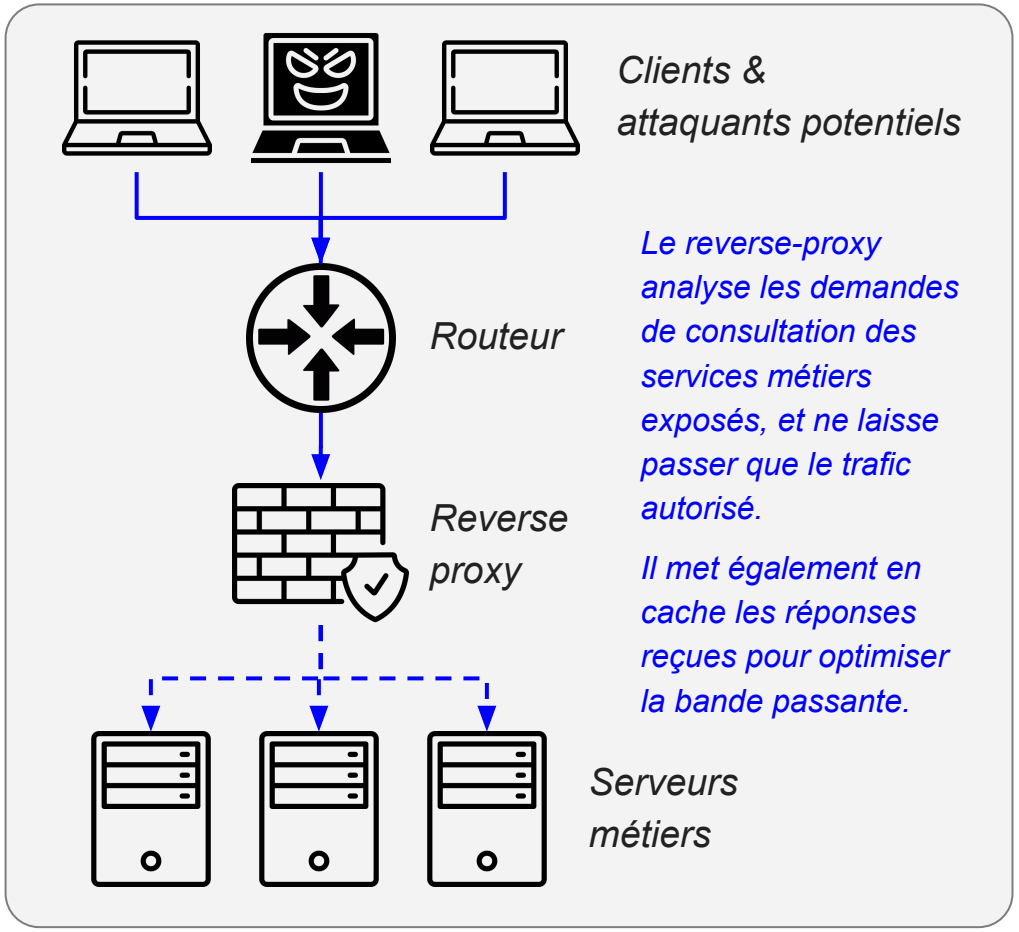
Avortement (Abortion)
Contenu pour adultes (Adult/Mature Content)
Alcool (Alcohol)
Spiritualité/croyances alternatives (Alternative Spirituality/Belief)
Art/culture (Art/Culture)
Ventes aux enchères (Auctions)
Clips audio/vidéo (Audio/Video Clips)
Courtage/opérations boursières (Brokerage/Trading)
Affaires/économie (Business/Economy)
Organismes caritatifs/à but non lucratif (Charitable/Non-Profit)
Chat (IM)/SMS
Pédopornographie (Child Pornography)
Infrastructure cloud (Cloud Infrastructure)
Sites compromis (Compromised Sites)
Sécurité des informations/de l'ordinateur (Computer/Information Security)
Réseaux de distribution de contenu (Content Delivery Networks)
Substances contrôlées (Controlled Substances)
Cryptomonnaie (Cryptocurrency)
Hôtes DNS dynamiques (Dynamic DNS Host)
Cartes électroniques/invitations (E-Card/Invitations)
Enseignement (Education)
Messagerie électronique (Email)
Publicité par courrier électronique (Email Marketing)
Spectacles et divertissements (Entertainment)
Stockage/partage de fichiers (File Storage/Sharing)
Finance
Contenu pour enfants (For Kids)
Jeux et paris (Gambling)
Jeux (Games)
Gore/Choquant (Gore/Extreme)
Administration/juridique (Government/Legal)
Piratage (Hacking)
Santé (Health)
Humour/blagues (Humor/Jokes)
Contenu informatif (Informational)
Appareils connectés à Internet (Internet Connected Devices)
Téléphonie par Internet (Internet Telephony)
Lingerie/maillots de bain (Intimate Apparel/Swimsuit)
Recherche d'emploi/carrières (Job Search/Careers)
Données sortantes malveillantes/réseaux de bots (Malicious Outbound Data/Botnets)
Sources malveillantes/malnets (Malicious Sources/Malnets)
Escroquerie/Légalité douteuse (Scam/Questionable Legality)
Moteurs/portails de recherche (Search Engines/Portals)
Education sexuelle (Sex Education)
Achats (Shopping)
Réseaux sociaux (Social Networking)
Société/vie quotidienne (Society/Daily Living)
Téléchargement de logiciels (Software Downloads)
Spam
Sports/loisirs (Sports/Recreation)
Suspect (Suspicious)
Technologie/Internet (Technology/Internet)
Tabac (Tobacco)
Traduction (Translation)
Voyages (Travel)
TV/flux vidéo (TV/Video Streams)
Sans catégorie (Uncategorized)
Raccourcisseurs d'URL (URL Shorteners)
Véhicules (Vehicles)
Violence/Intolérance (Violence/Intolerance)
Armes (Weapons)
Publicités web/analyse (Web Ads/Analytics)
Hébergement web (Web Hosting)
Infrastructure web (Web Infrastructure)

Source: http://sitereview.bluecoat.com/#/category-descriptions

Serveur reverse-proxy - Principe

Principe de fonctionnement

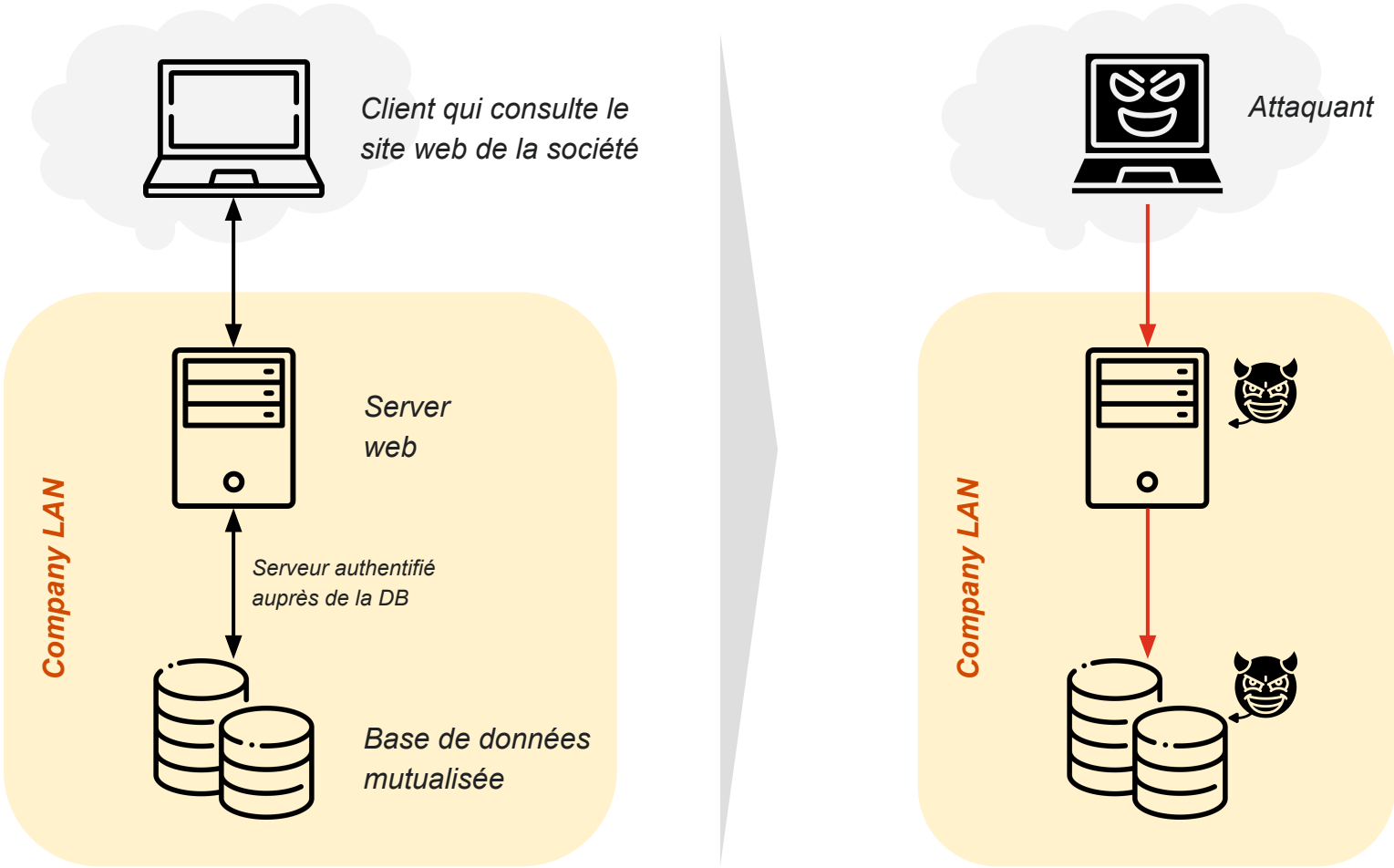
- **Rôle = fonction inverse d'un serveur proxy** : **mise en cache des serveurs internes en vue d'une consultation depuis internet**
- Le serveur reverse-proxy **filtre les demandes HTTP** (ou autres services métiers, en fonction des ports / protocoles exposés)
- **Le serveur reverse-proxy reçoit donc toutes les attaques**
  - Protection des serveurs internes
- **Objectif = surveiller et limiter le trafic applicatif** (couche OSI 7)
  - De l'extérieur vers les serveurs internes



4

DMZ & architecture “sécurisée”

DMZ (Zone Démilitarisée) - Problématique



Problème de sécurité

La prise de contrôle sur le **web serveur** pourrait permettre un **accès intégral** à la base de données derrière, puisque le serveur est authentifié.

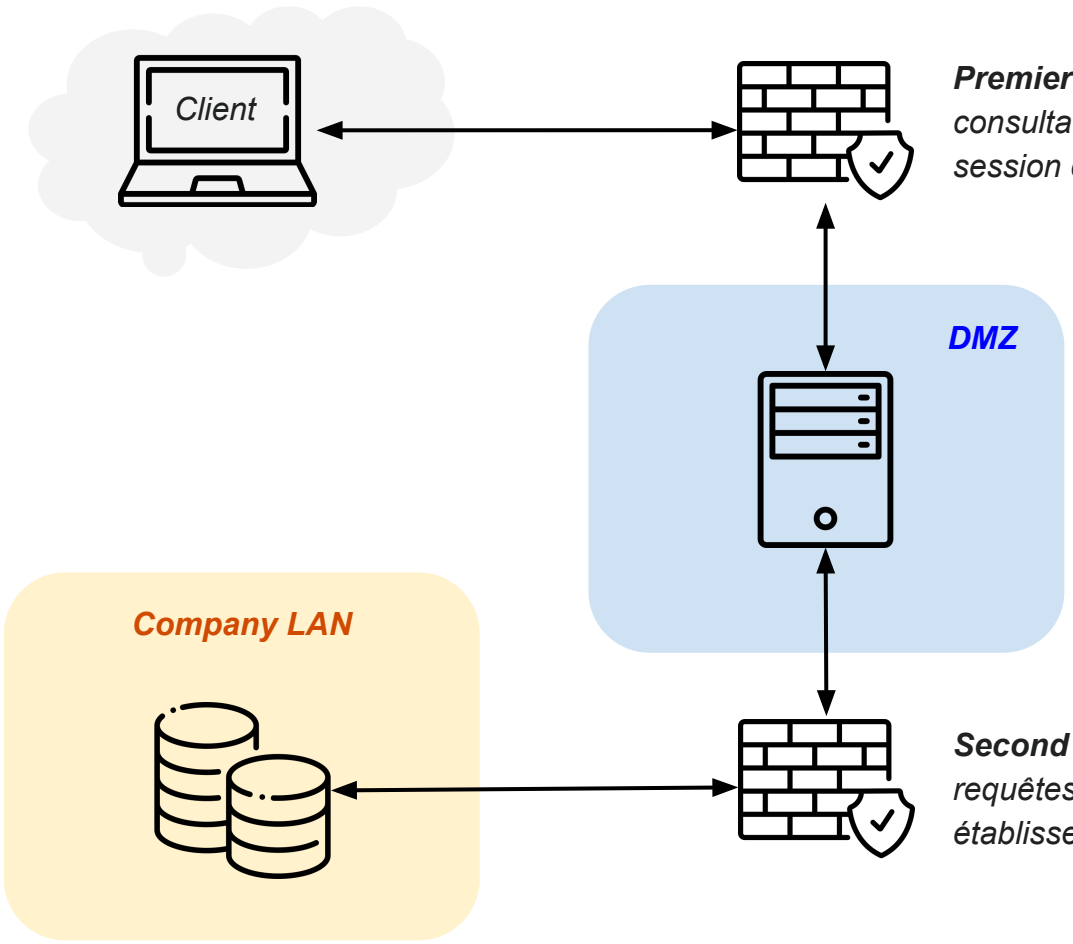
Il faut <u>à minima</u> de la rigueur dans la gestion des droits d'accès sur la DB, afin de limiter, dans le cas d'un DB mutualisée, l'accès aux autres tables et données qu'elles contiennent.

Néanmoins, grâce à son **accès direct et inconditionnel** à la DB, l'attaquant peut tenter de nouveaux exploits pour obtenir un accès root.

DMZ (Zone Démilitarisée) - Principe

Source image : https://on2it.net/en/broken-dmz-cybersecurity-model/

DMZ (Zone Démilitarisée) - Mise en place partielle



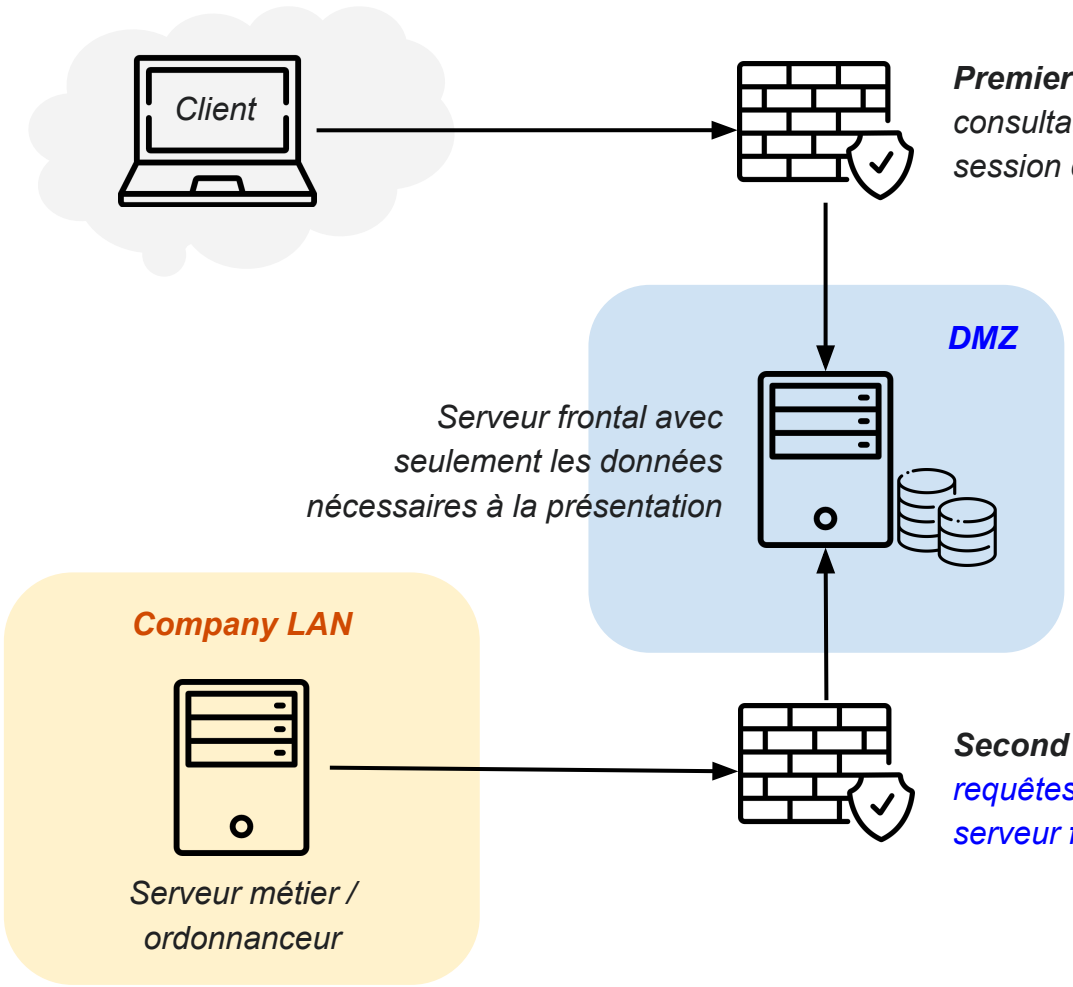
***Premier parefeu**, autorisant exclusivement les consultations clients (et l'établissement d'une session client-serveur web)*

***Second parefeu**, autorisant exclusivement les requêtes GET vers la base de données (et l' établissement d'une session serveur-BDD)*

Solution de sécurité - Mise en place partielle

La mise en place d'une DMZ permet de limiter les flux autorisés entre les clients (externes) et le serveur web, et donc de **réduire la surface d'attaque**. Elle permet également de mettre en place une seconde couche de sécurité entre le serveur et la base de données. **Néanmoins**, il ne s'agit pas ici d'une implémentation stricte car un flux existe entre le client externe et le LAN de la société.

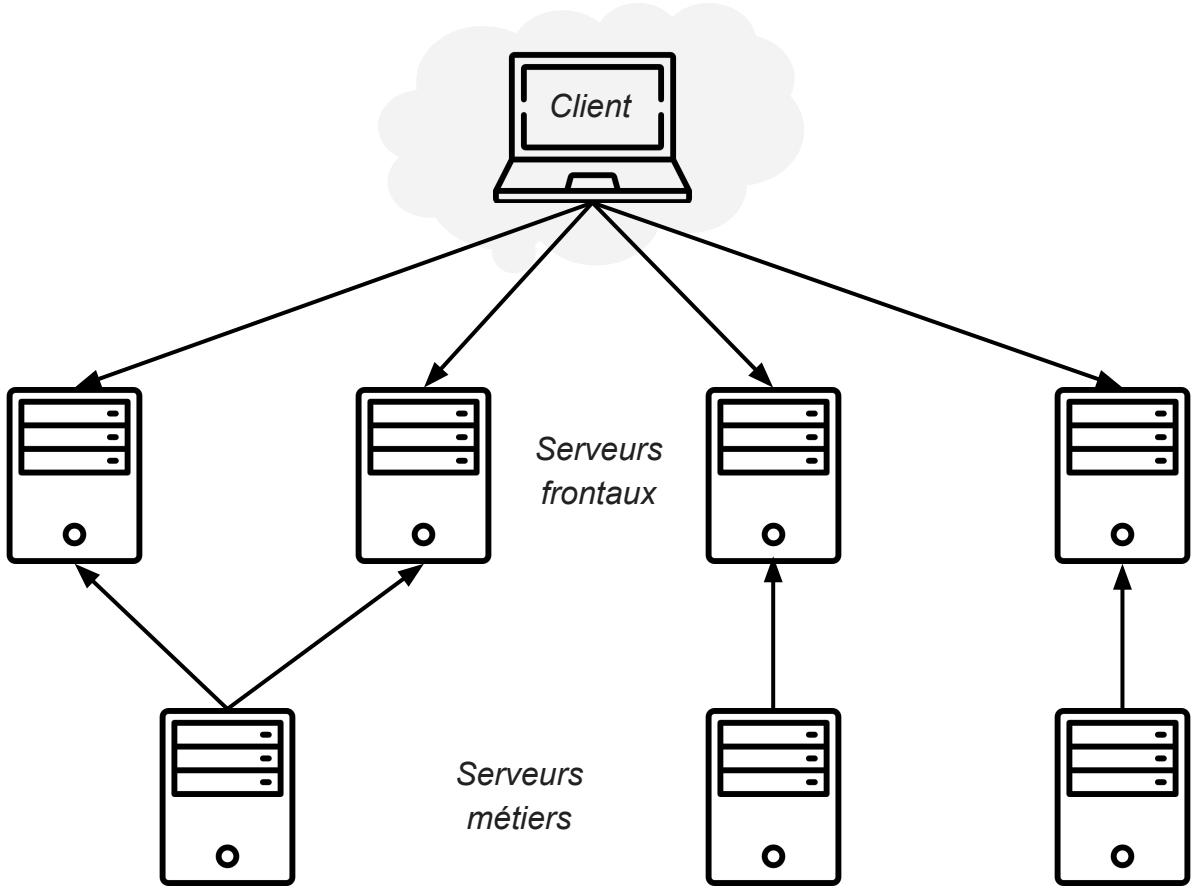
DMZ (Zone Démilitarisée) - Implémentation stricte



Implémentation stricte

Dans ce modèle, **le client n'a plus accès à la base de données applicative** (contenant toutes les données de l'application), mais seulement aux données qui sont "poussées" sur **l'interface de présentation**. **Le contrôle sur les données incombe au serveur métier, placé sur le LAN, qui met à jour régulièrement les données mise à la disposition des clients.**

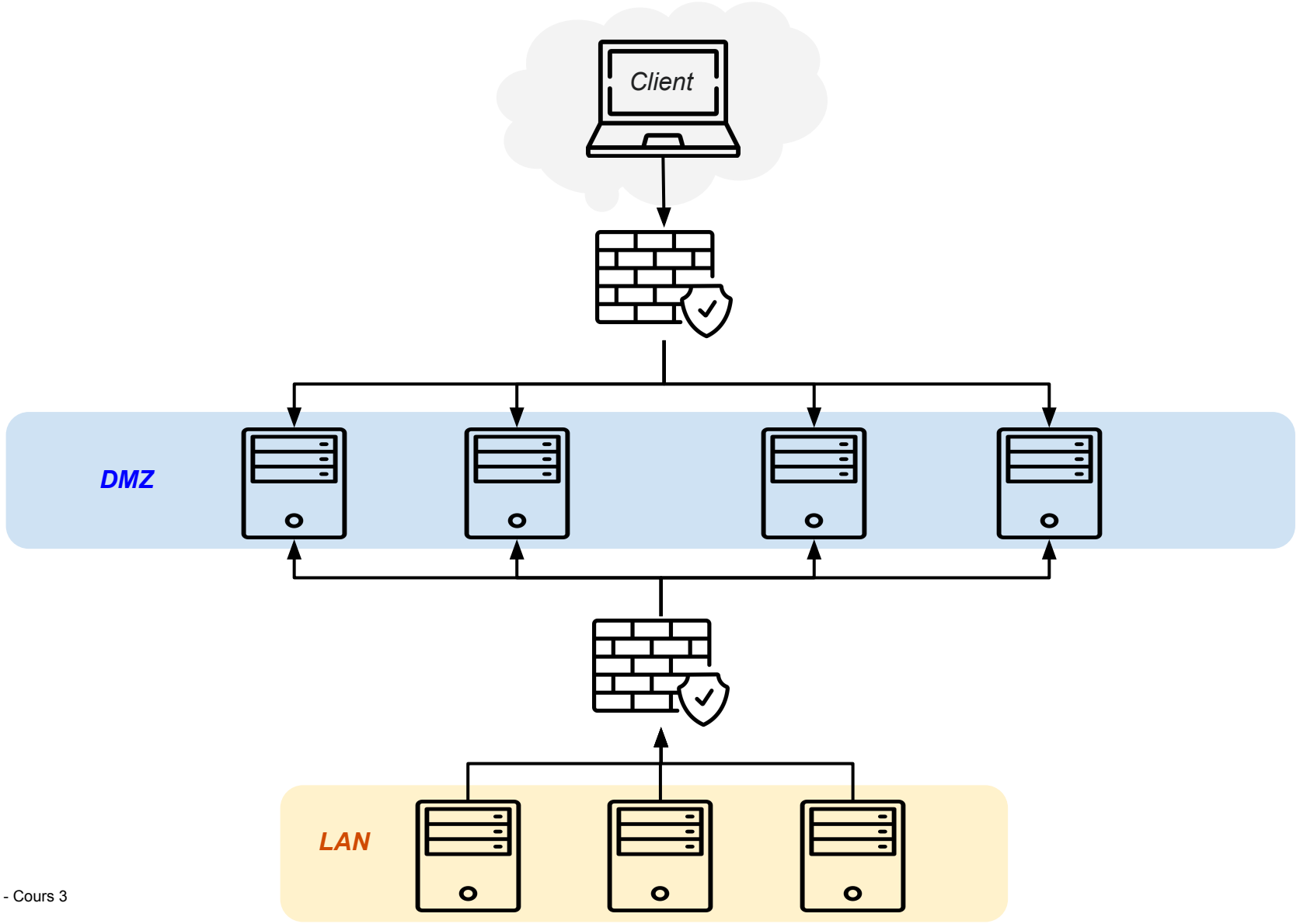
DMZ (Zone Démilitarisée) - Passage à l'échelle (1/4)



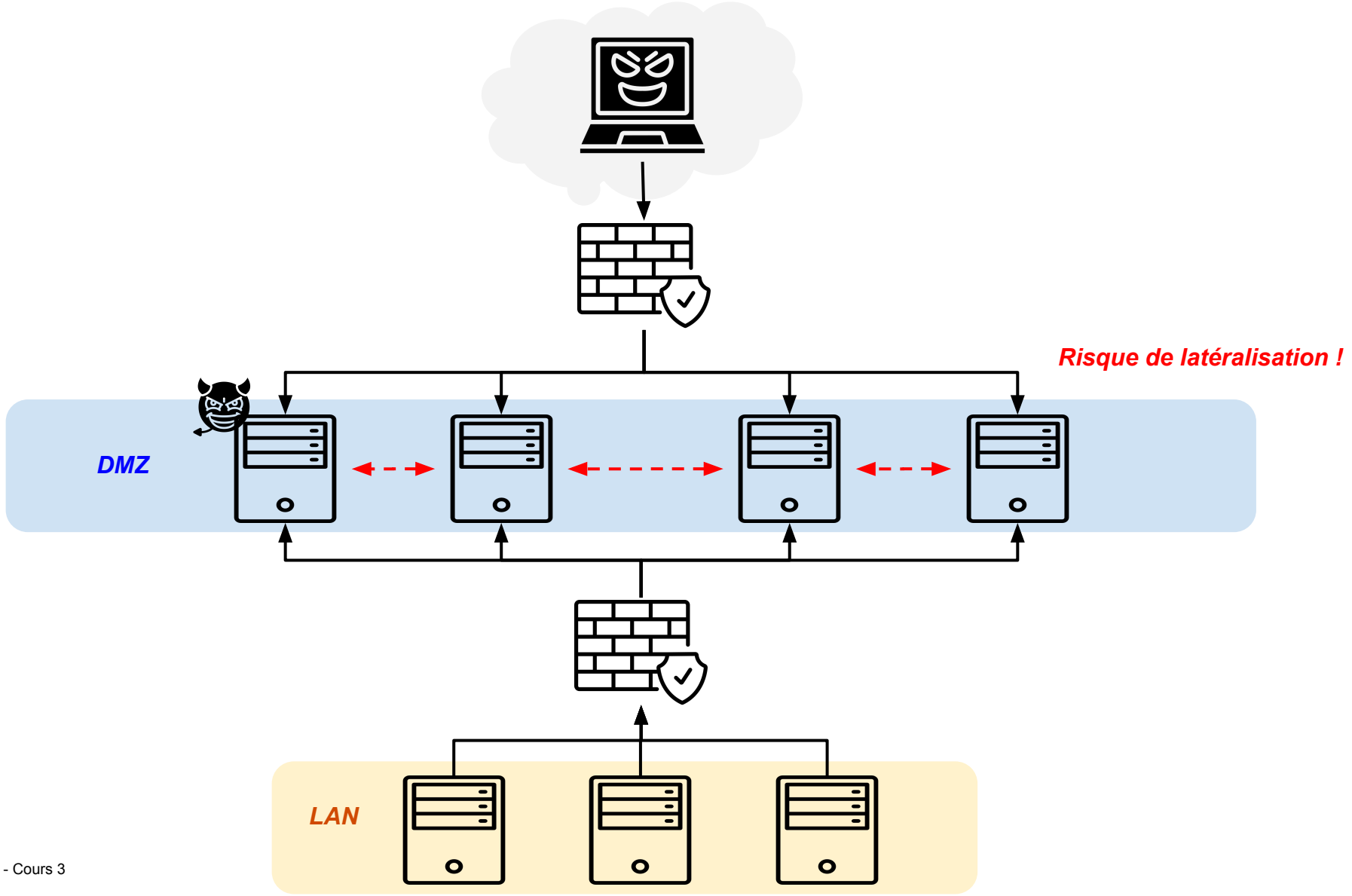
Problème de sécurité

Comment faire dans le cas d'une entreprise plus conséquente, avec plusieurs services web ou applications métiers exposés ?

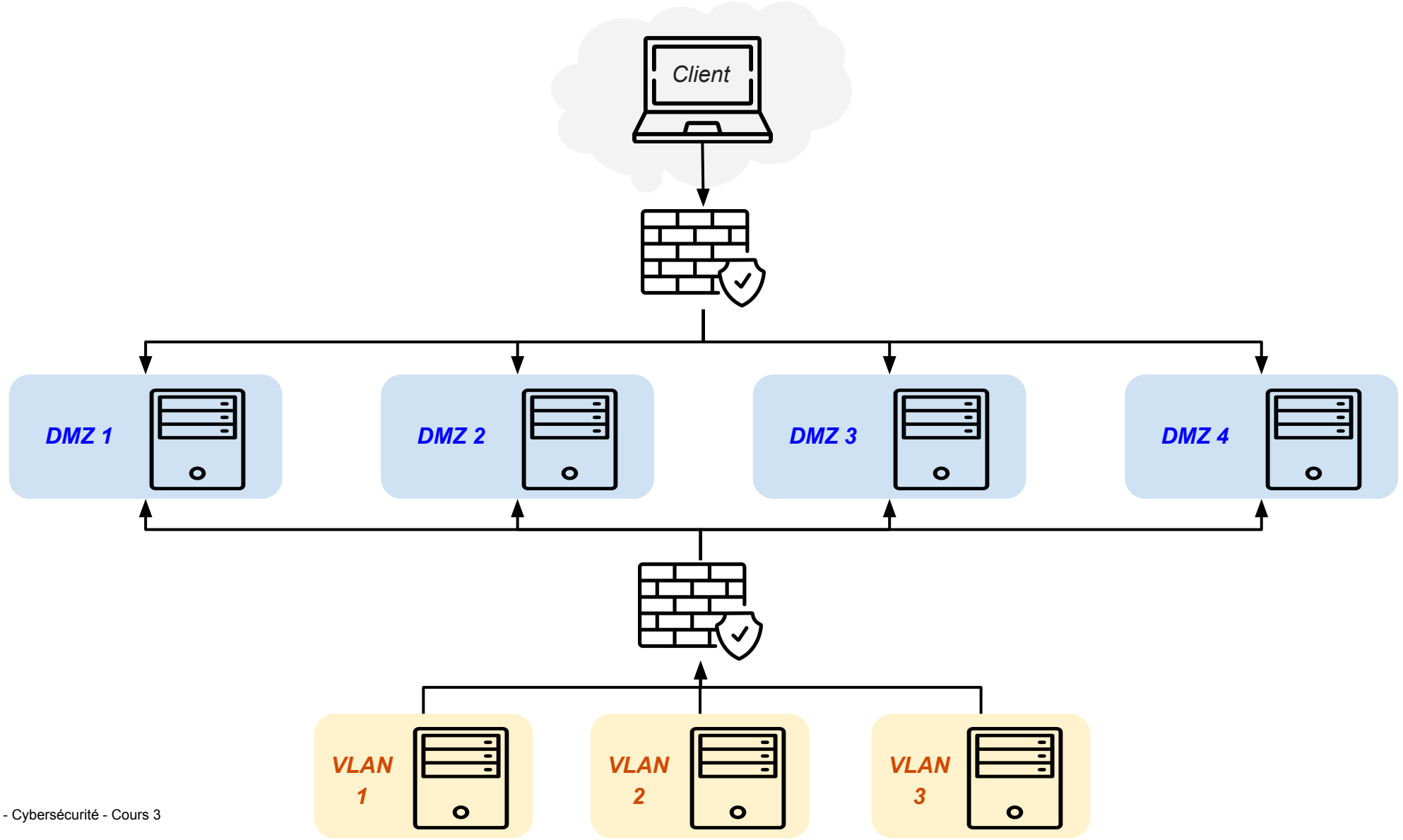
DMZ (Zone Démilitarisée) - Passage à l'échelle (2/4)



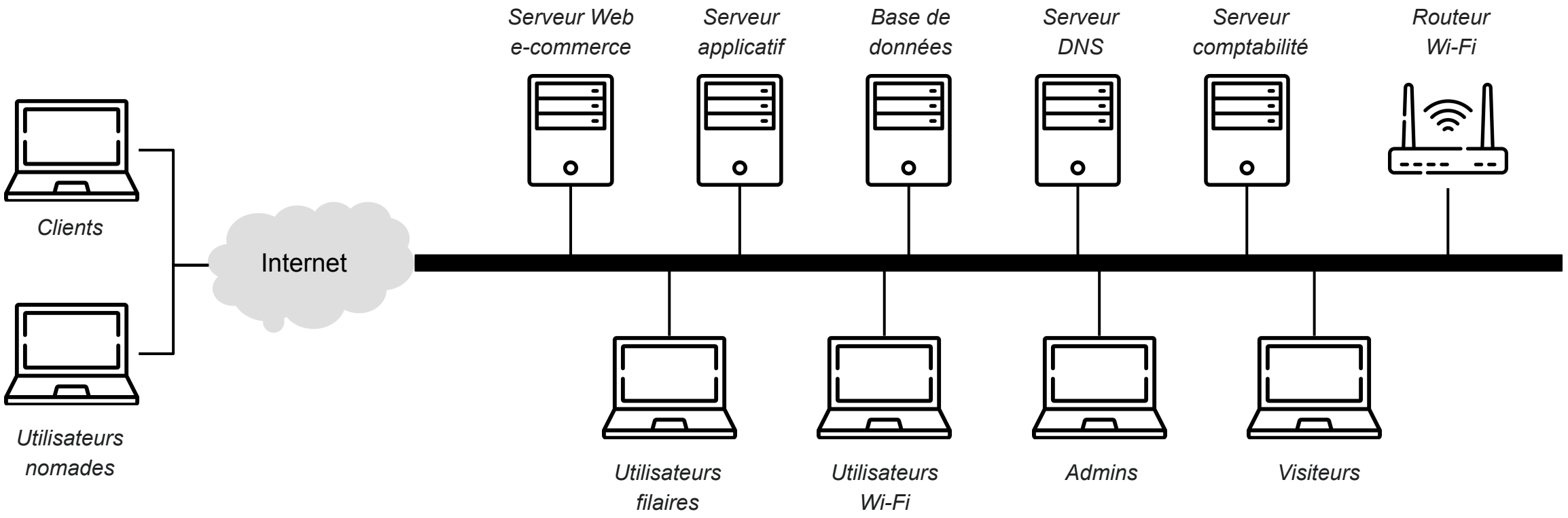
DMZ (Zone Démilitarisée) - Passage à l'échelle (3/4)



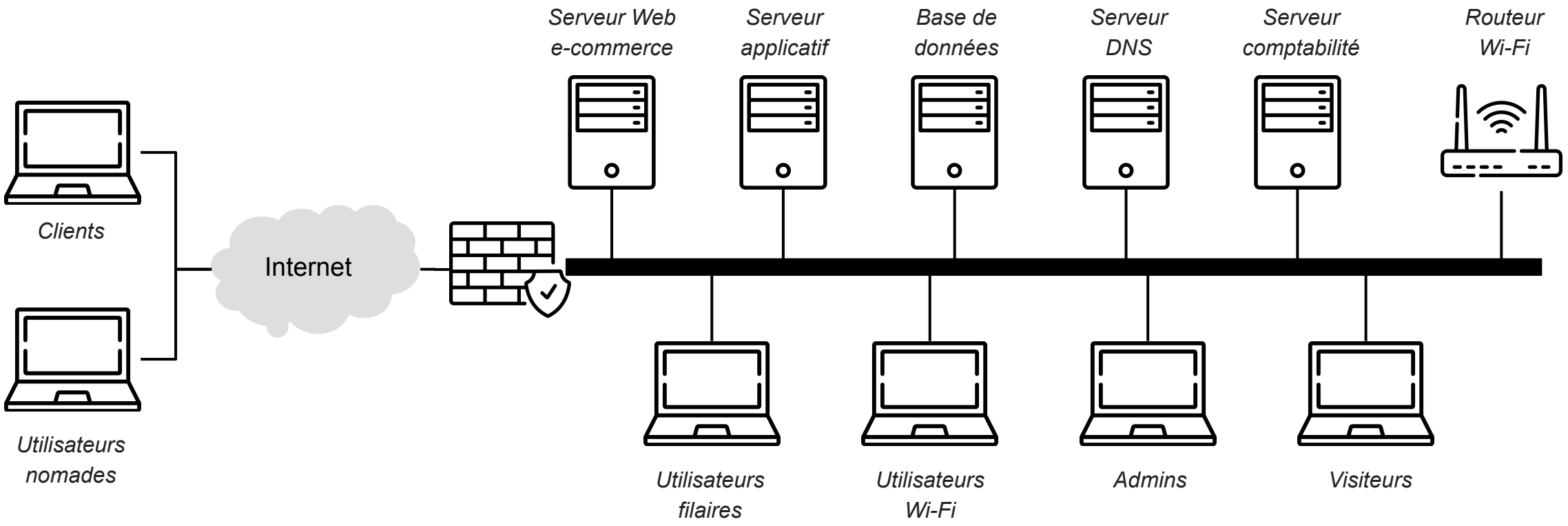
DMZ (Zone Démilitarisée) - Passage à l'échelle (4/4)



Exercice: sécuriser une PME - Situation initiale



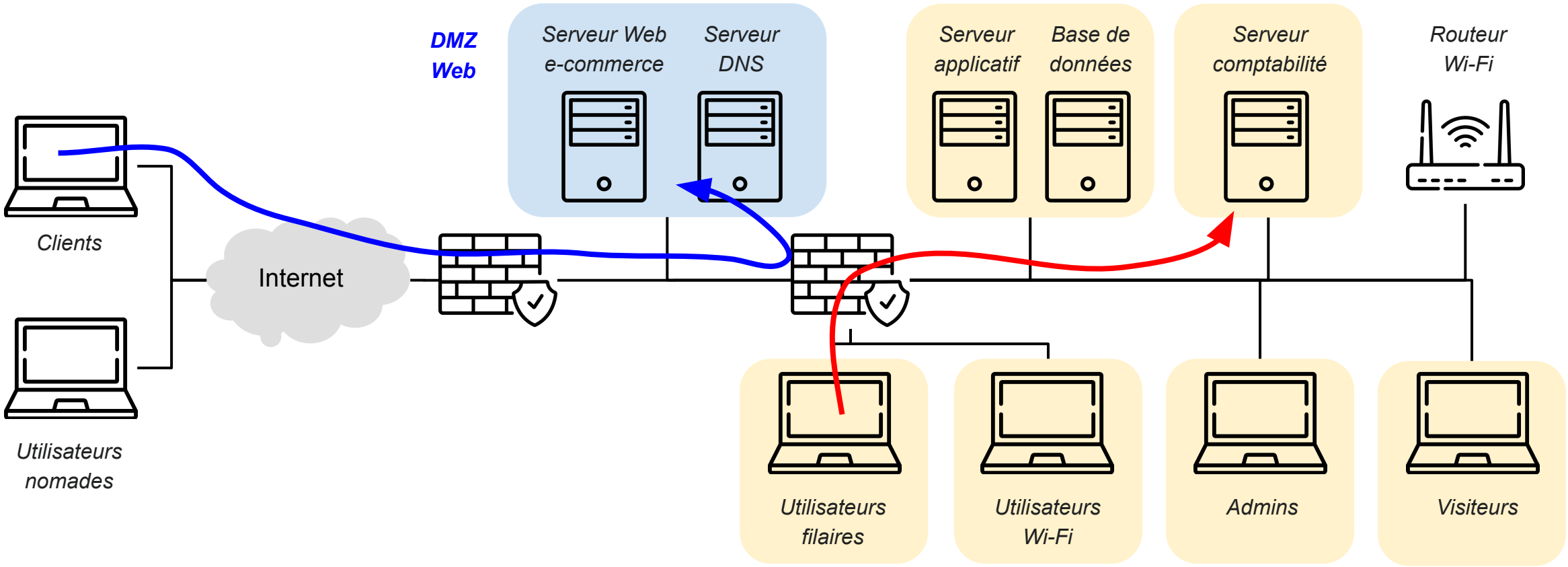
Exercice: sécuriser une PME (1/6)



Etape 1:

Mettre en place en parefeu pour bloquer l'accès au réseau entreprise depuis internet. Garder les flux Web et DNS ouverts.

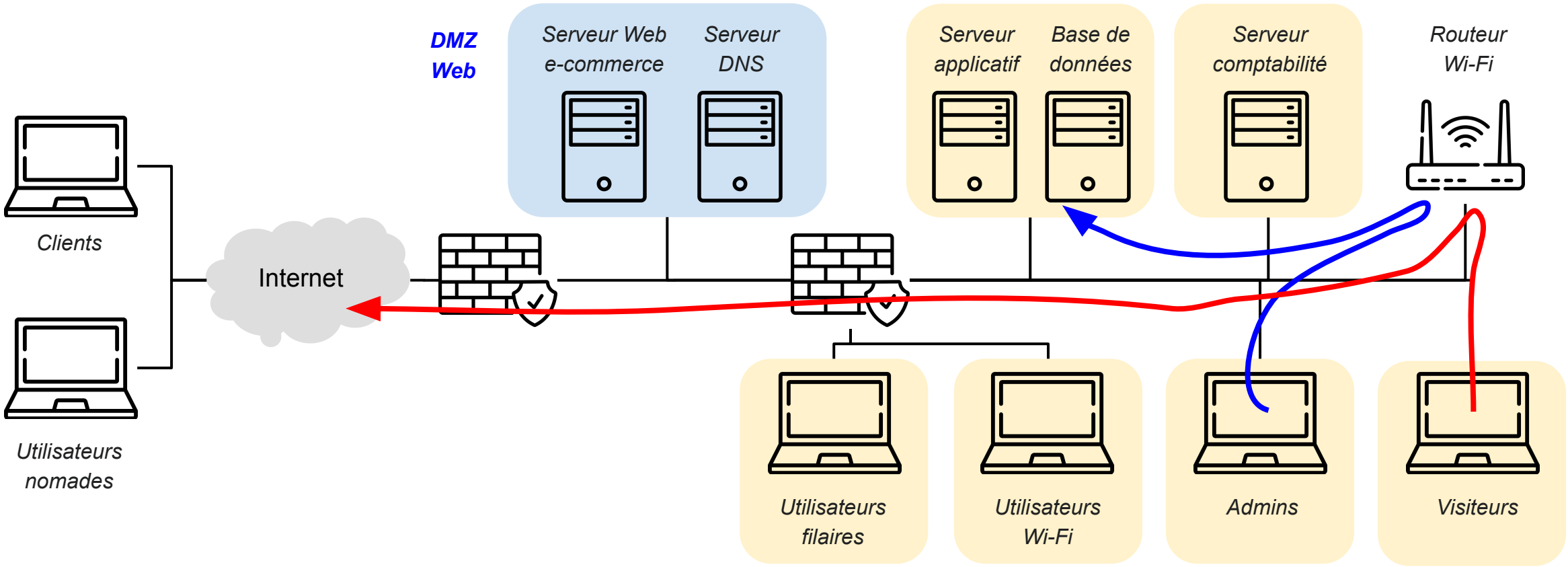
Exercice: sécuriser une PME (2/6)



Etape 2:

Mettre en place une DMZ avec les services exposés. Regrouper les systèmes et clients dans des VLANs séparés.

Exercice: sécuriser une PME (3/6)

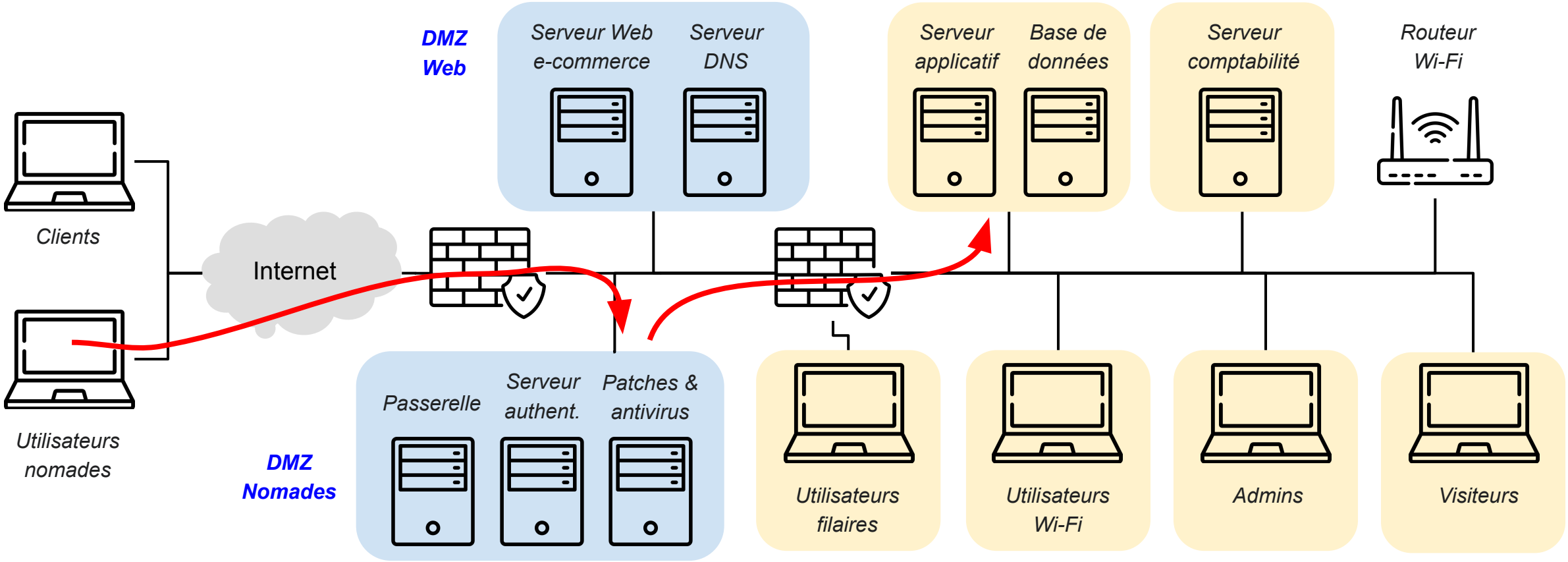


Etape 3:

Pour le Wi-Fi : mettre en place 2 SIDs différents (e.g. “guests” et “corporate” pour les utilisateurs du réseau).

Pour les visiteurs: accès internet uniquement. Pour les utilisateurs, accès aux services internes en fonction du rôle.

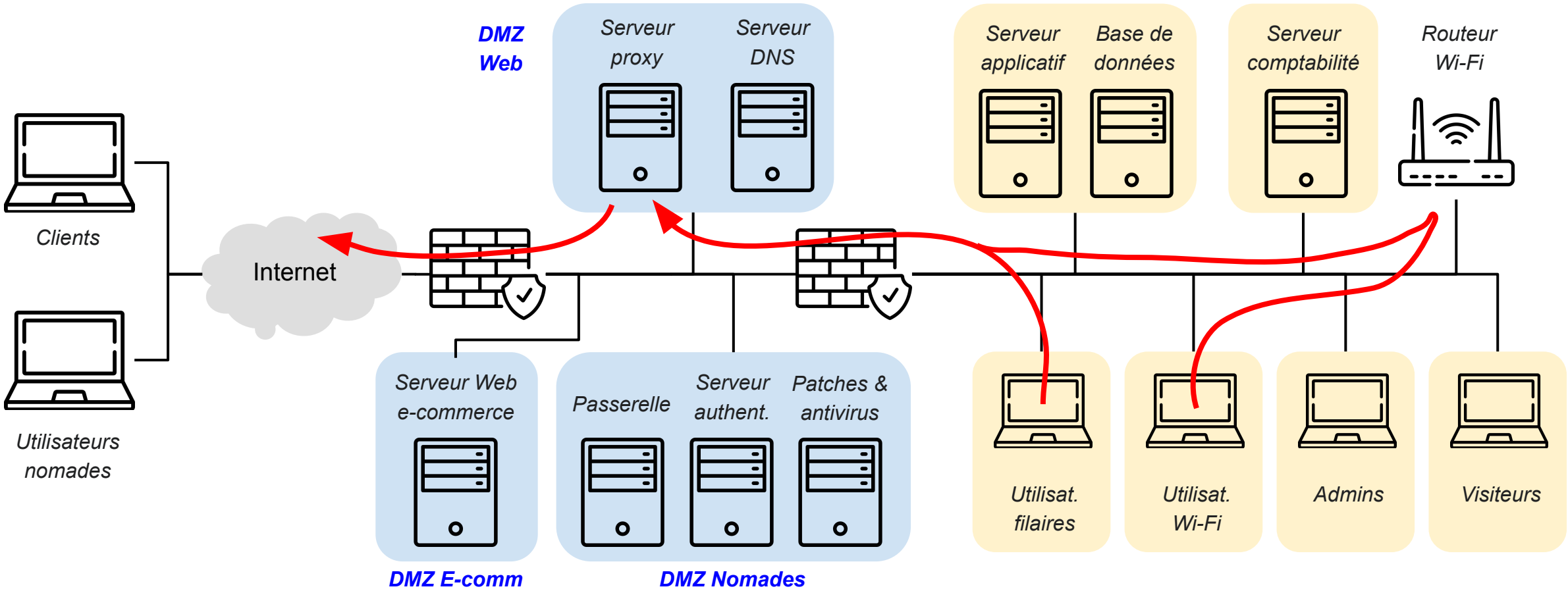
Exercice: sécuriser une PME (4/6)



Etape 4:

Mettre en place un sas d'authentification (et de vérification) pour les utilisateurs distants qui se connectent en VPN.

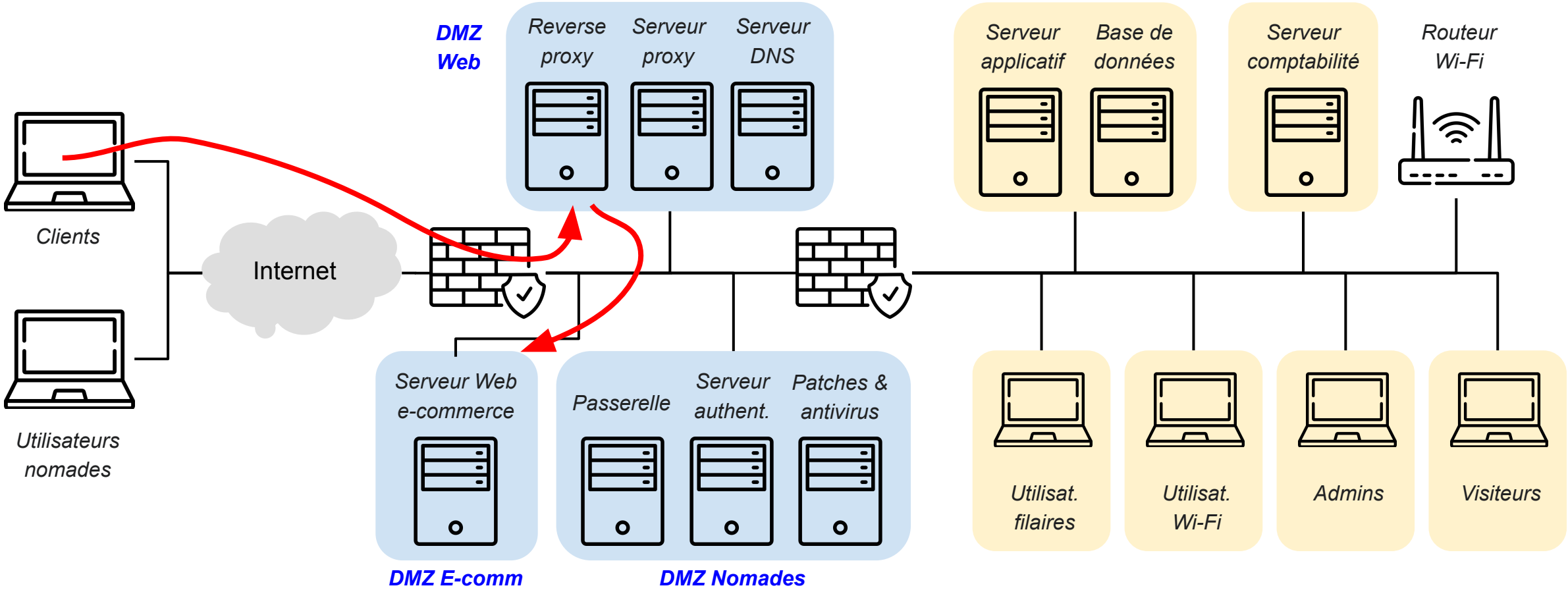
Exercice: sécuriser une PME (5/6)



Etape 5:

Mettre en place un serveur proxy pour contrôler les flux sortants.

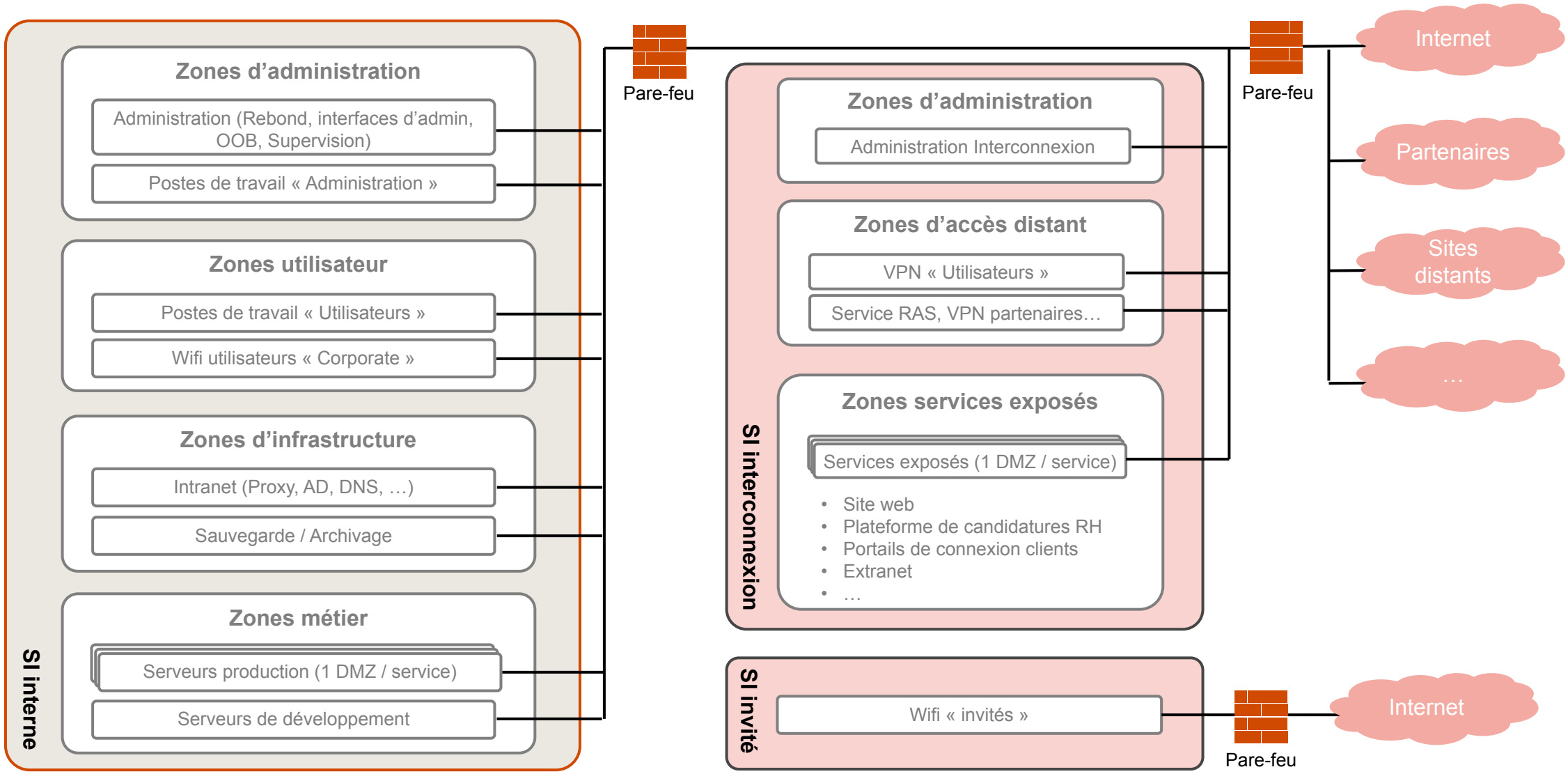
Exercice: sécuriser une PME (6/6)



Etape 6:

Mettre en place un serveur reverse-proxy pour contrôler les flux entrants vers le site e-commerce.

Exemple plus détaillé d'architecture "sécurisée"



Comment identifier un point d'entrée ?

Pour trouver une première IP

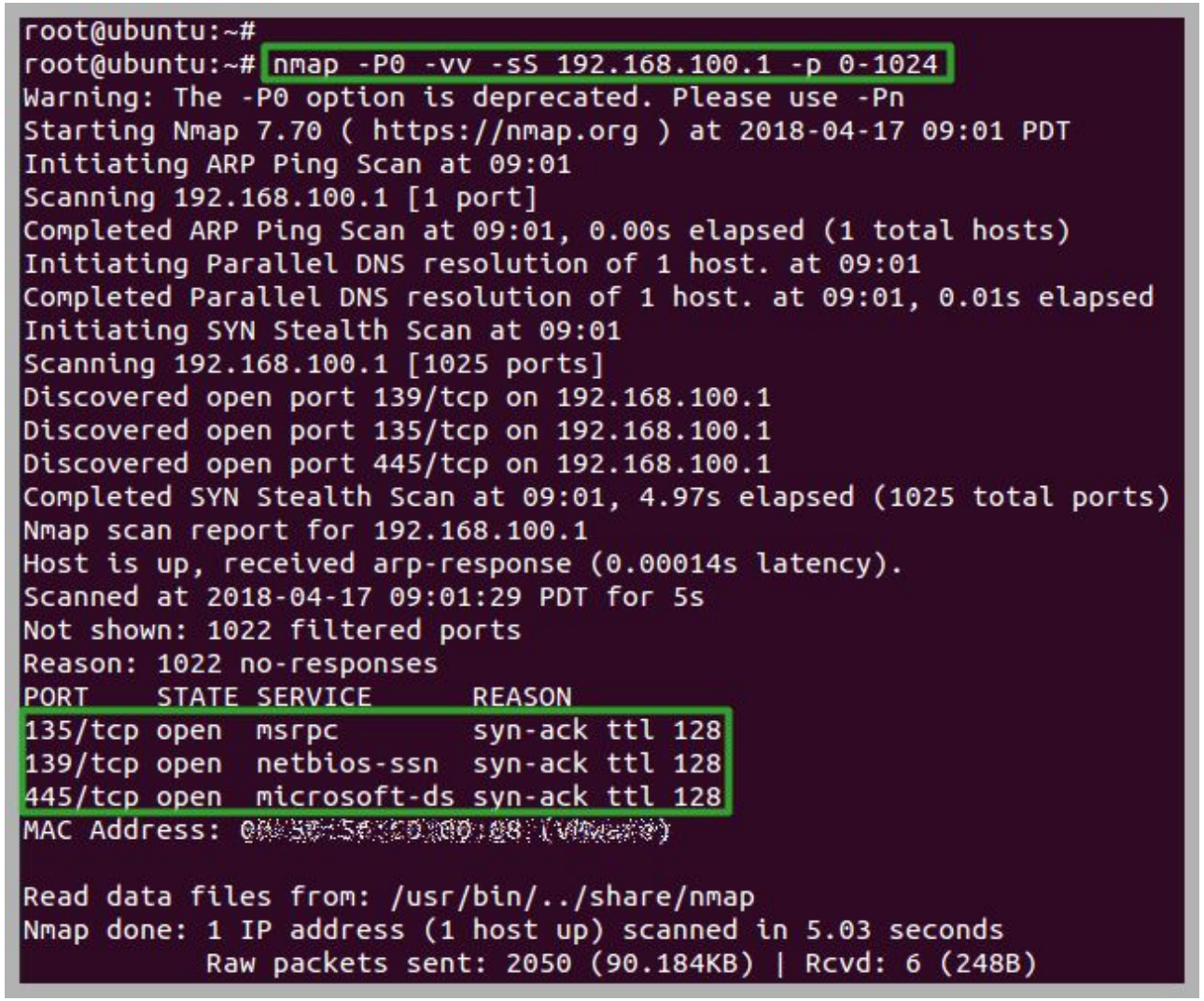
- **Requête DNS**

Utilisation de l'outil NMAP

Outil très largement utilisé - Référence

Sert à identifier les ports ouverts sur un serveur

- Scans par ping
- Scans "discrets" par requêtes SYN
- Scans étendus (au dela du port 1024)
- Scan de versions
  - Applications
  - OS
- Scans agressifs (pour un maximum d'infos)



Source: https://cysecguide.blogspot.com/2018/04/nmap-scan-network.html

5

Sécurité en profondeur: IPS & IDS

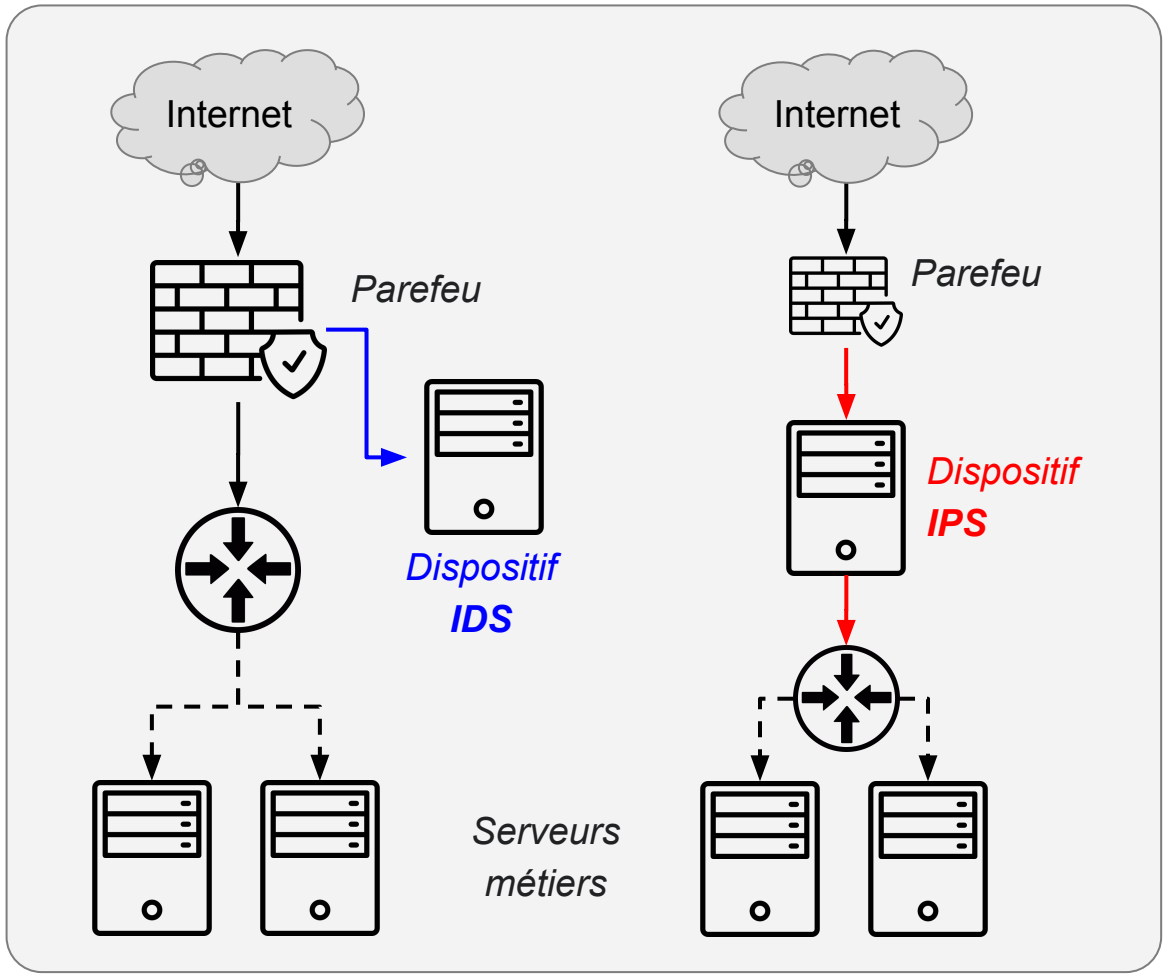
Intrusion Detection/Prevention Systems (IDS/IPS)

Pourquoi on ne s'arrête pas là ?

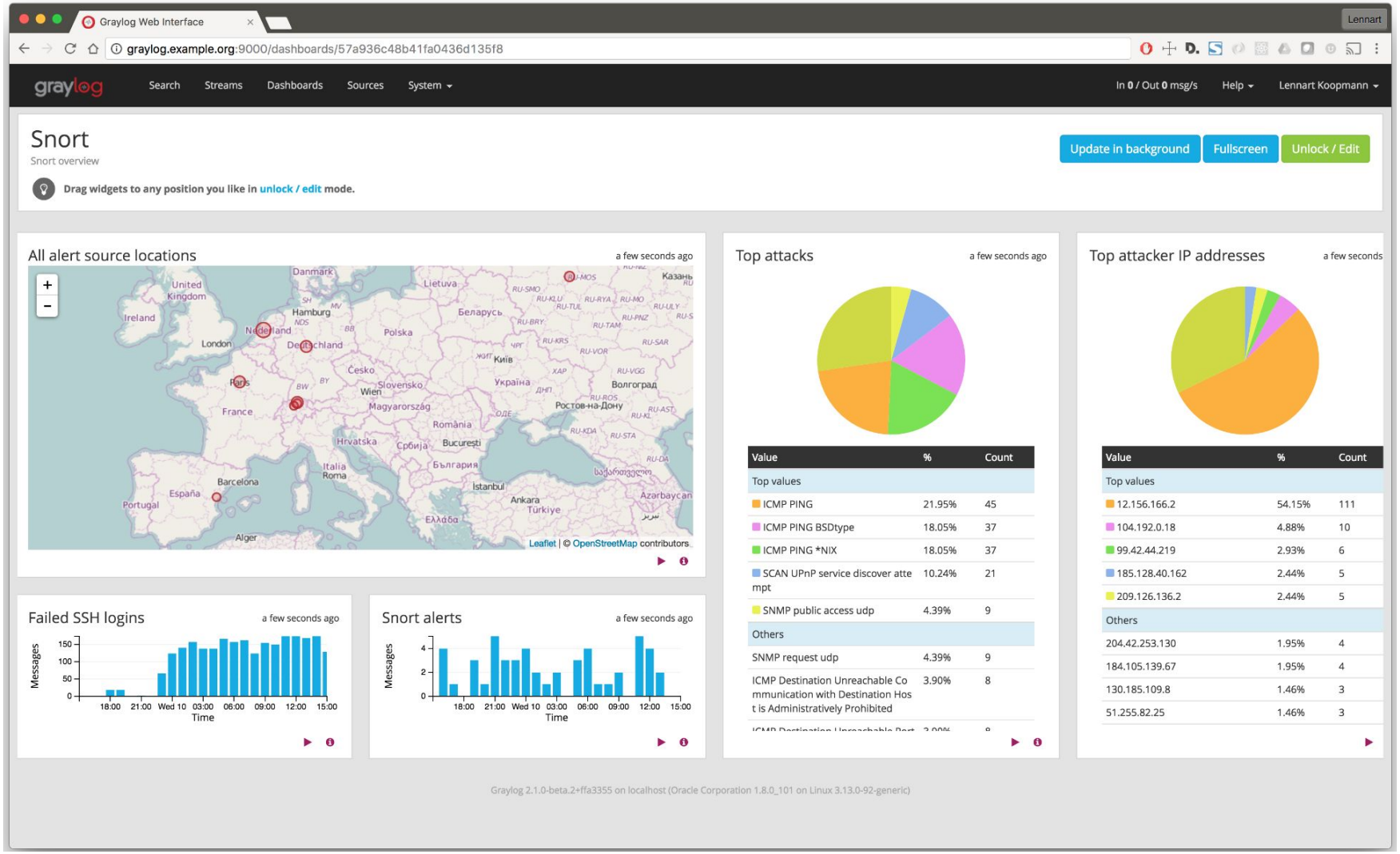
Les switches, routeurs, parefeux et proxys sont (principalement) des outils de **routage** et de **filtrage**. La sécurité proposée par ces équipements est fondamentalement basée sur des principes de **contrôle d'accès** (avec des listes et des règles). Ces équipements se basent sur les entêtes des paquets, et les métadonnées, mais très peu sur le **contenu effectif**.

Les IDS / IPS sont justement conçus pour analyser le contenu et le comparer à une base de menaces / scénarios d'attaques !

- Un **IDS** est un outil de **détection** et de **monitoring**
  - Ces outils ne prennent pas d'action, ils lèvent des alertes
  - Sans opérateur pour revoir les alertes, l'IDS ne sert à rien !
- Un **IPS** est un outil de **prévention** et de **contrôle**
  - Ces outils sont blocants : is rejettent les paquets dangereux
  - Risques de blocages métiers si les règles sont mal configurées
- Le même équipement peut être un IDS ou un IPS en fonction de sa mise en place. Les IDS/IPS existent en version "**réseau**" (équipement physique) et en version "**hôte**" (sous forme d'agent logiciel)
- Enorme poussée vers du machine learning pour dépasser les principes de règles statiques ne prenant en compte que des attaques connues !

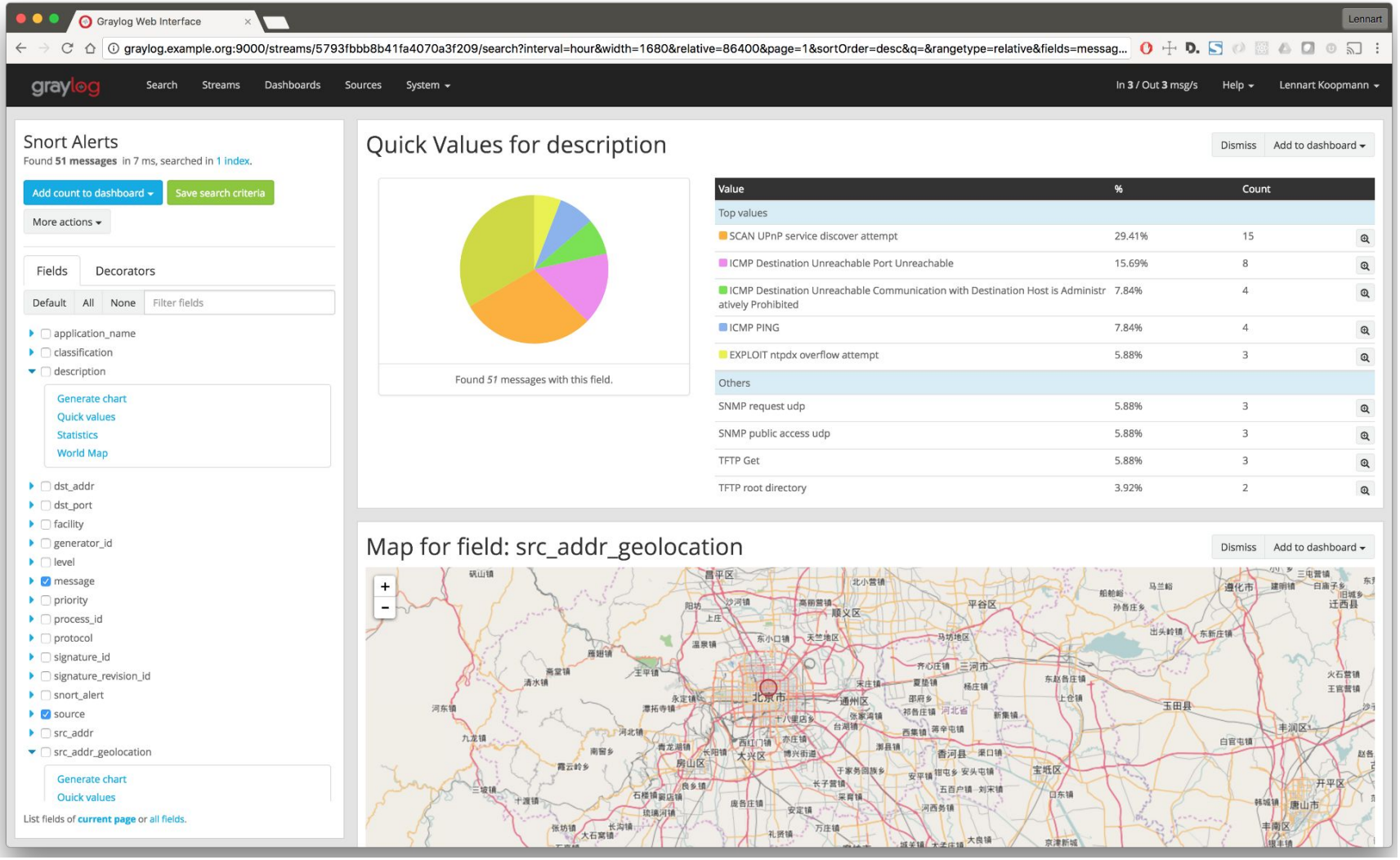


IDS - Exemple de dashboard sécurité (1/2)



Source image: https://www.graylog.org/post/visualize-and-correlate-ids-alerts-with-open-source-tools

IDS - Exemple de dashboard sécurité (2/2)



Source image: https://www.graylog.org/post/visualize-and-correlate-ids-alerts-with-open-source-tools

Que retenir ?

Que retenir ?

1. Le modèle OSI en 7 couches
2. La sécurité ne repose pas que sur de la crypto !
3. La sécurité doit être prise en compte dans l’architecture réseau
4. Rôle des switches, routeurs, parefeux, proxys, IDS/IPS
5. Principe de DMZ & exemple d’architecture “sécurisée”

Merci !
Des questions ?

pwc.fr