

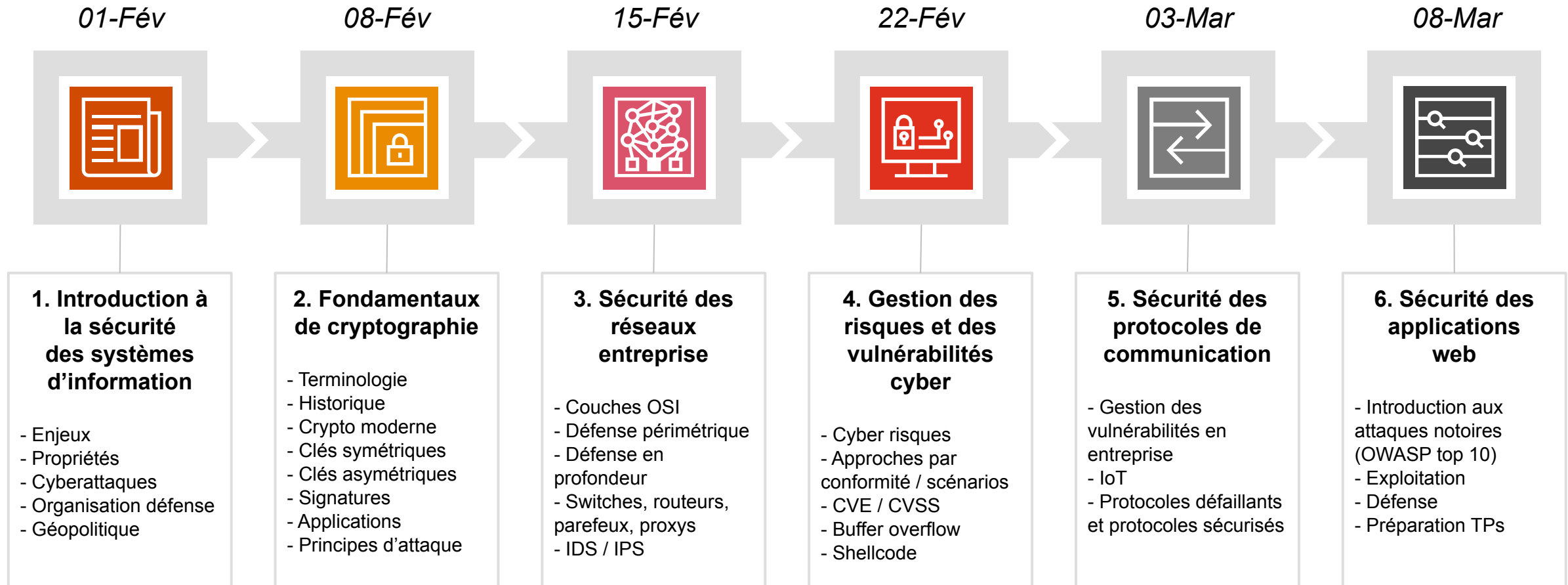
Cursus ENSEEIHT/2SN

3. Sécurité des réseaux entreprise

Février 2022



Déroulement du module



Agenda

1

Couches du modèle de référence OSI

2

Fondamentaux: switches & routeurs

3

Essentiels: parefeux & proxys

4

DMZ & architecture “sécurisée”

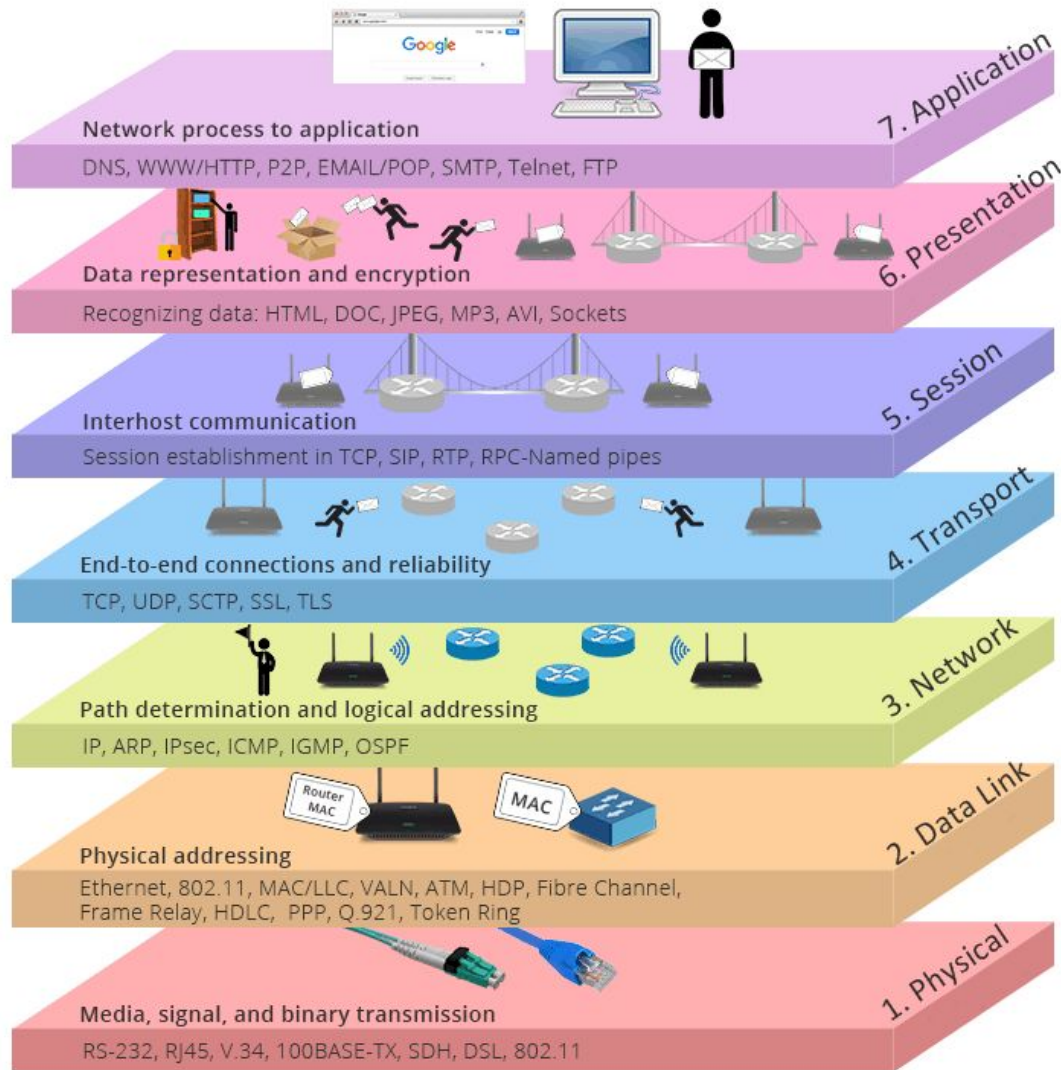
5

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” :

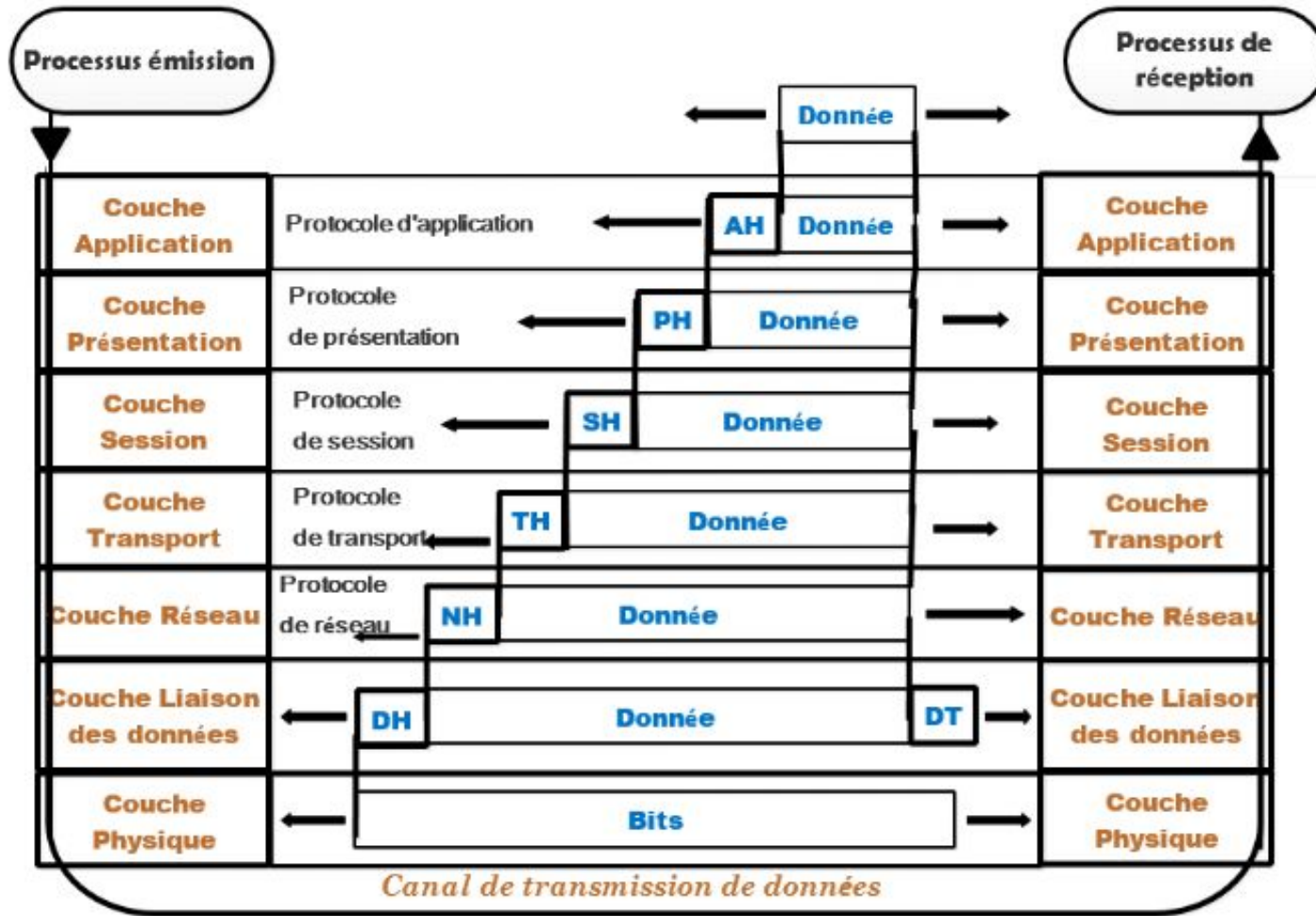
- 1. Couche « physique »** : transmission des signaux entre les interlocuteurs (bits). Compétence limitée à l'envoi et à la réception d'un flux de données.
- 2. Couche « liaison »** : communications entre deux machines connectées. Capacité à identifier un destinataire via son adresse physique (MAC).
- 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.

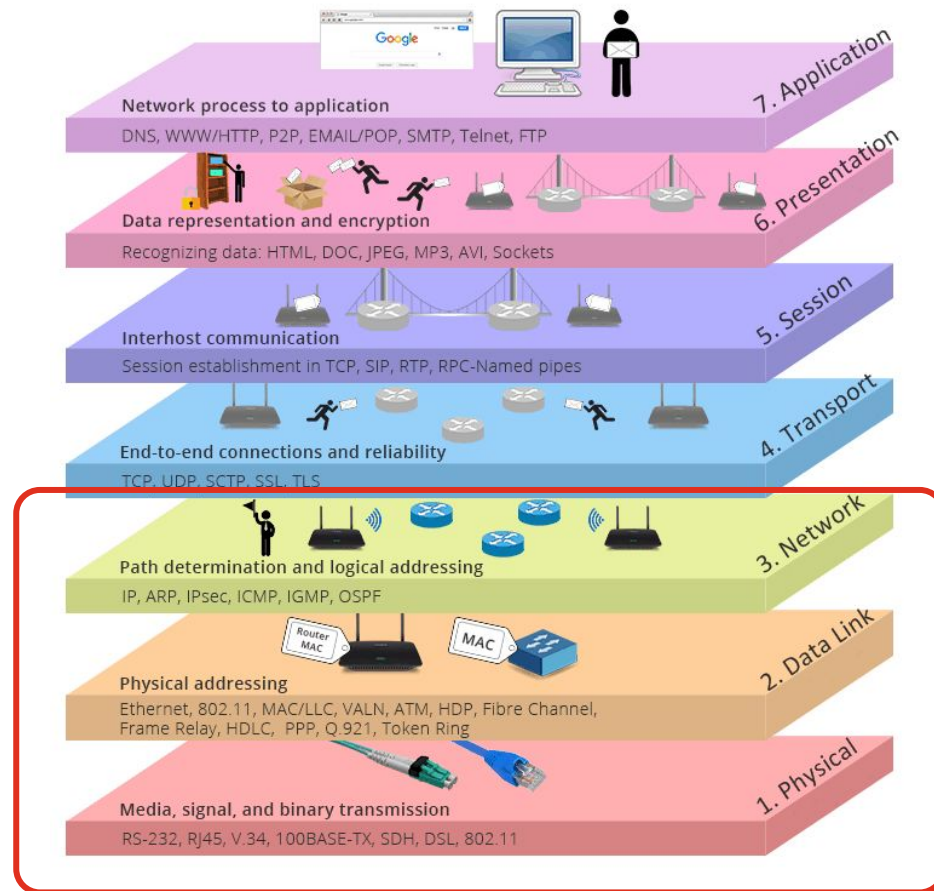
Source image: <https://community.fs.com/fr/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html>

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)



→ 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 **routing** peut être modifié pour à rediriger un flux vers un autre destinataire.

Source image:

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

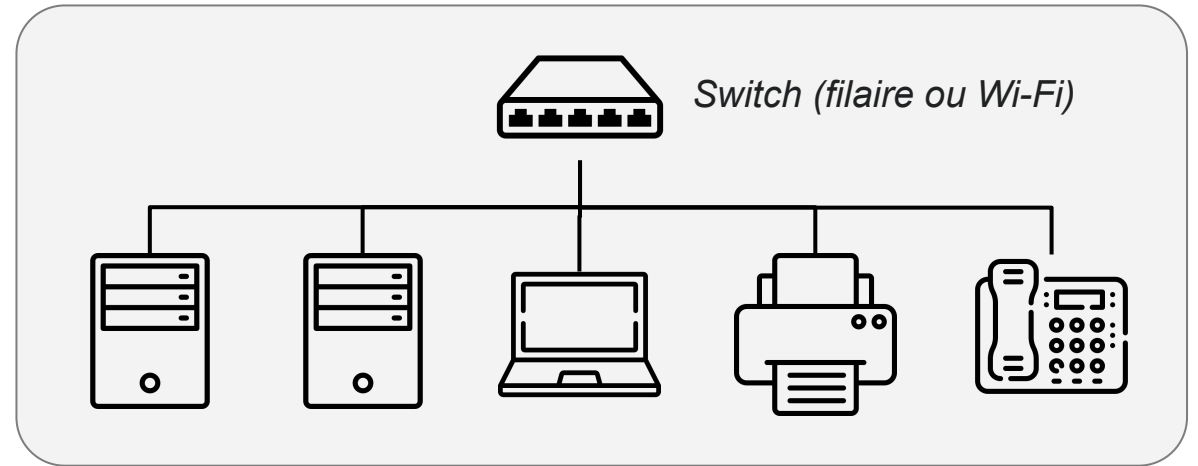


Fondamentaux: switches & routeurs

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

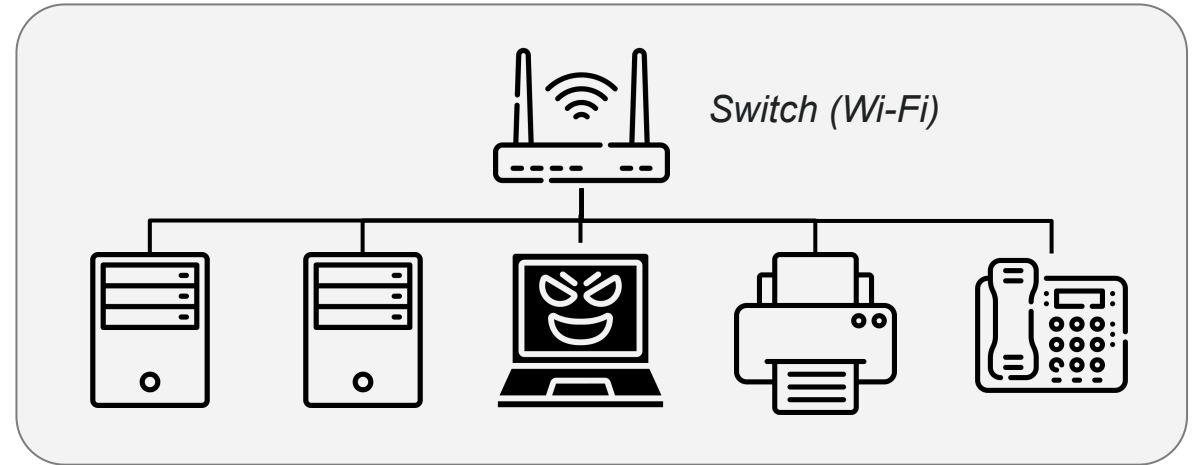


```
Interface : 192.168.1.21 --- 0x4
Adresse Internet  Adresse physique  Type
192.168.1.30      70-9e-29-4a-d0-81  dynamique
192.168.1.31      84-a6-c8-36-ef-8e  dynamique
192.168.1.254     c8-cd-72-5a-db-bd  dynamique
192.168.1.255     ff-ff-ff-ff-ff-ff  statique
224.0.0.2         01-00-5e-00-00-02  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 distribuait 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.



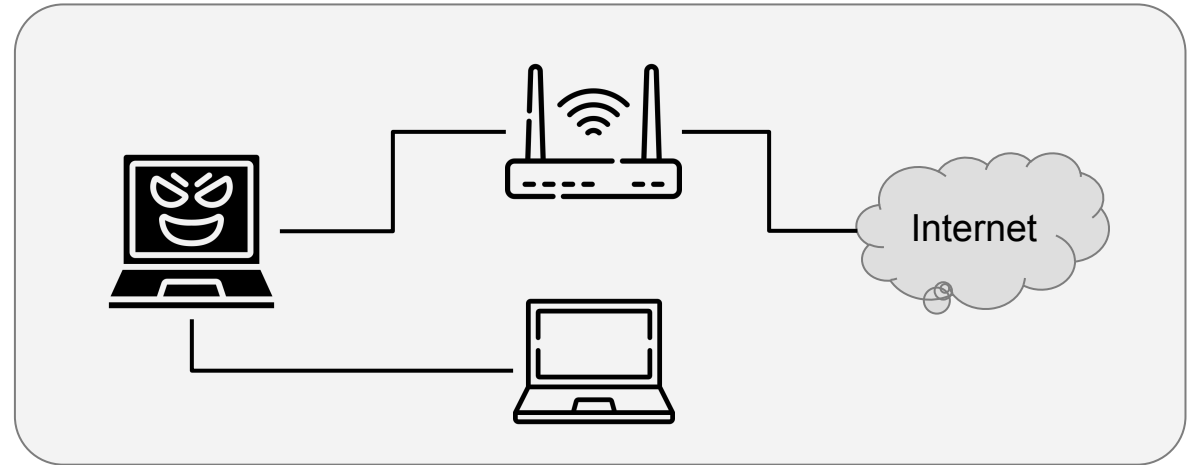
Switches (commutateurs) - ARP spoofing / poisoning

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)

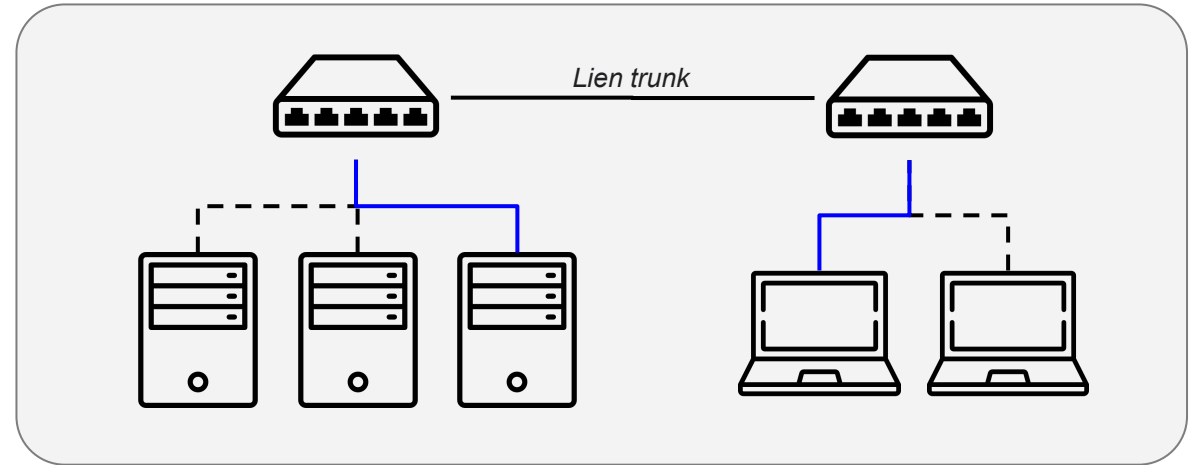


```
Interface: 192.168.43.65 --- 0x16
  Internet Address      Physical Address      Type
  192.168.43.1          08-00-27-89-03-db    dynamic
  192.168.43.220        08-00-27-89-03-db    dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22            01-00-5e-00-00-16    static
  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 switches pour qu'ils échangent les informations sur les VLANs et marquent les flux



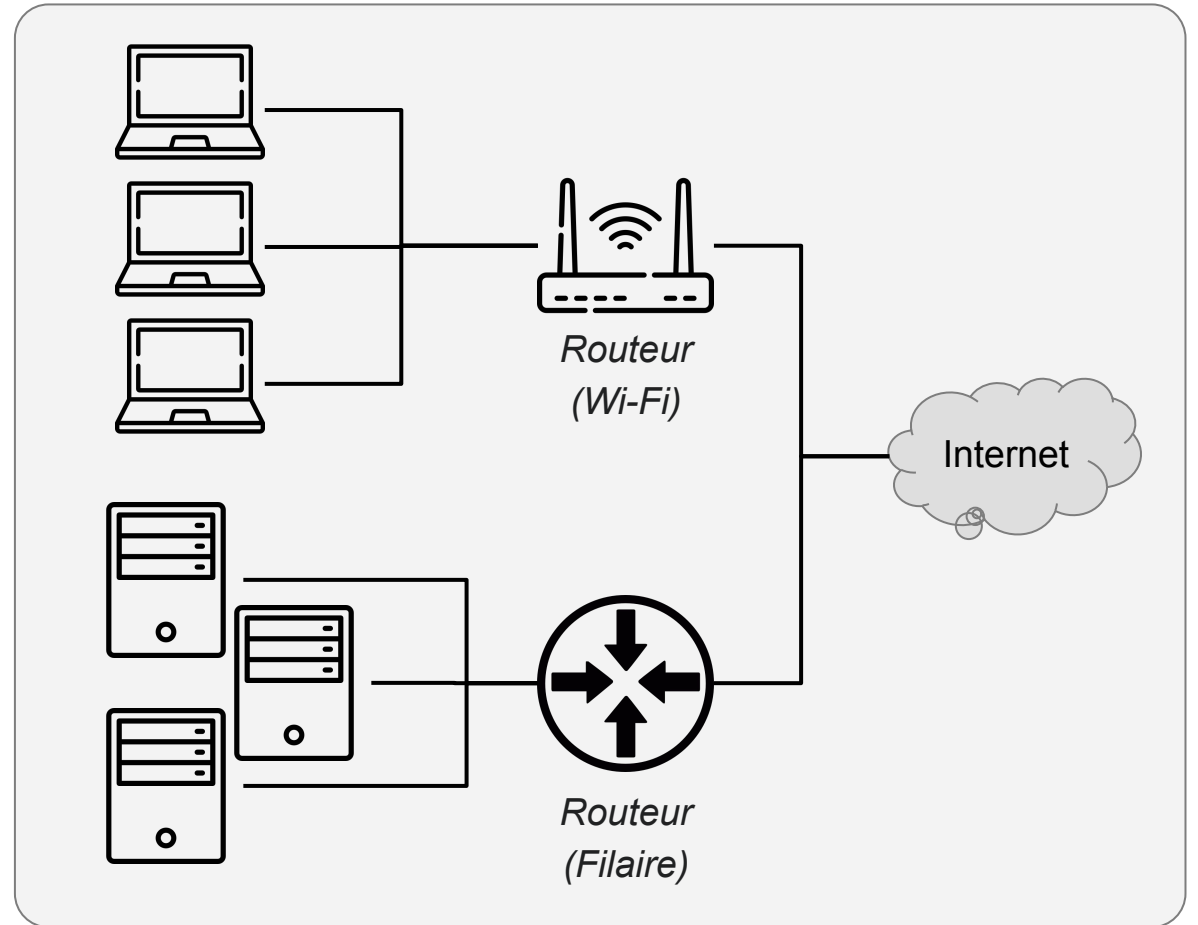
Standard 802.1X - Network Access Control (NAC)

- 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

```
Microsoft Windows [Version 10.0.17134.885]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mjp>tracert ggexample.com

Tracing route to ggexample.com [96.127.135.98]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  LINKSYS01329 [192.168.1.1] < Home network
  2    12 ms    10 ms     9 ms  142.254.186.129
  3    32 ms    22 ms    31 ms  agg62.ycvycaam02h.socal.rr.com [76.167.16.205]
  4    14 ms    10 ms    12 ms  agg24.pldscabx02r.socal.rr.com [72.129.38.86]
  5    19 ms    18 ms    14 ms  72.129.37.2 < ISP
  6    17 ms    20 ms    14 ms  bu-ether26.tustca4200w-bcr00.tbone.rr.com [66.109.3.232]
  7    18 ms    15 ms    15 ms  0.ae3.pr1.lax10.tbone.rr.com [107.14.19.56]
  8    16 ms    15 ms    14 ms  66.109.7.38
  9     *        65 ms    99 ms  ae13.cs1.lax112.us.eth.zayo.com [64.125.28.230]
 10    70 ms    85 ms    67 ms  ae6.cs1.las2.us.eth.zayo.com [64.125.27.33]
 11    66 ms    63 ms    63 ms  ae12.cs1.den5.us.zip.zayo.com [64.125.30.242]
 12     *        *        *      Request timed out.
 13    64 ms    64 ms    62 ms  ae11.er2.ord7.us.zip.zayo.com [64.125.26.251]
 14    71 ms    68 ms    66 ms  128.177.108.98.ipyx-142927-900-zyo.zip.zayo.com [128.177.108.98]
 15   105 ms   100 ms   103 ms  agg1.c13.r14.s101.chi03.singlehop.net [67.212.190.230]
 16    68 ms    73 ms    69 ms  aswg1.c25.r04.s101.chi03.singlehop.net [99.198.126.59] < Website host's network
 17    69 ms    67 ms    66 ms  ggexample.com [96.127.135.98] < The website

Trace complete.
```

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



Cisco ASA



Fortigate



Palo Alto



Barracuda



Sophos



Check Point

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

Parefeux (firewalls) - Parefeu personnel (Windows)

Pare-feu Windows Defender

Panneau de configuration > Système et sécurité > Pare-feu Windows Defender

Page d'accueil du panneau de configuration

Autoriser une application ou une fonctionnalité via le Pare-feu Windows Defender

Modifier les paramètres de notification

Activer ou désactiver le Pare-feu Windows Defender

Paramètres par défaut

Paramètres avancés

Dépanner mon réseau

Protégez votre ordinateur avec le Pare-feu Windows Defender

Le Pare-feu Windows Defender a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via Internet ou via un réseau.

Par sécurité, certains paramètres sont gérés par l'administrateur système.

Réseaux avec domaine Connecté

Réseaux en entreprise, qui appartiennent à un domaine

État du Pare-feu Windows Defender : Activé

Connexions entrantes : Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées

Réseaux avec domaine actifs : pwcglib.com

État de notification : Ne pas m'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application

Réseaux privés Non connecté

Réseaux publics ou invités Connecté

Réseaux dans des lieux publics, tels qu'un aéroport ou un cybercafé

État du Pare-feu Windows Defender : Activé

Connexions entrantes : Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées

Réseaux publics actifs : Livebox-84B0

État de notification : Ne pas m'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application

Voir aussi

Sécurité et maintenance

Centre Réseau et partage

Autoriser les applications à communiquer à travers le Pare-feu Windows Defender

Pour ajouter, modifier ou supprimer des applications et des ports autorisés, cliquez sur Modifier les paramètres.

Quels sont les risques si une application est autorisée à communiquer ?

Modifier les paramètres

Par sécurité, certains paramètres sont gérés par l'administrateur système.

Applications et fonctionnalités autorisées :

Nom	Domaine	Privé	Public	Stratégie de gro...
<input checked="" type="checkbox"/> Gestion des périphériques Windows	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Non
<input type="checkbox"/> Gestion des services à distance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Non
<input type="checkbox"/> Gestion des volumes à distance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Non
<input checked="" type="checkbox"/> Google Chrome	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Non
<input type="checkbox"/> Groupement résidentiel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Non
<input checked="" type="checkbox"/> Hôte de l'expérience du Microsoft Store	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Non
<input type="checkbox"/> IBM Notes - Client to Notes Server (TCP-In)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Oui
<input type="checkbox"/> IBM Notes - Proxy Requests (TCP-In)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Oui
<input type="checkbox"/> IBM Notes - Sametime P2P (TCP-In)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Oui
<input checked="" type="checkbox"/> Infrastructure de gestion Windows (WMI)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Oui
<input type="checkbox"/> Infrastructure de gestion Windows (WMI)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Non

Détails... Supprimer

Access Control List (ACL)

ess

Language: English

Logout About Help

20 20-Port Gigabit Managed Switch

IPv4-Based ACE

IPv4-Based ACE Table

Filter: ACL Name equals to Wireless Go

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

Add...

Edit...

Delete

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as 'x'.

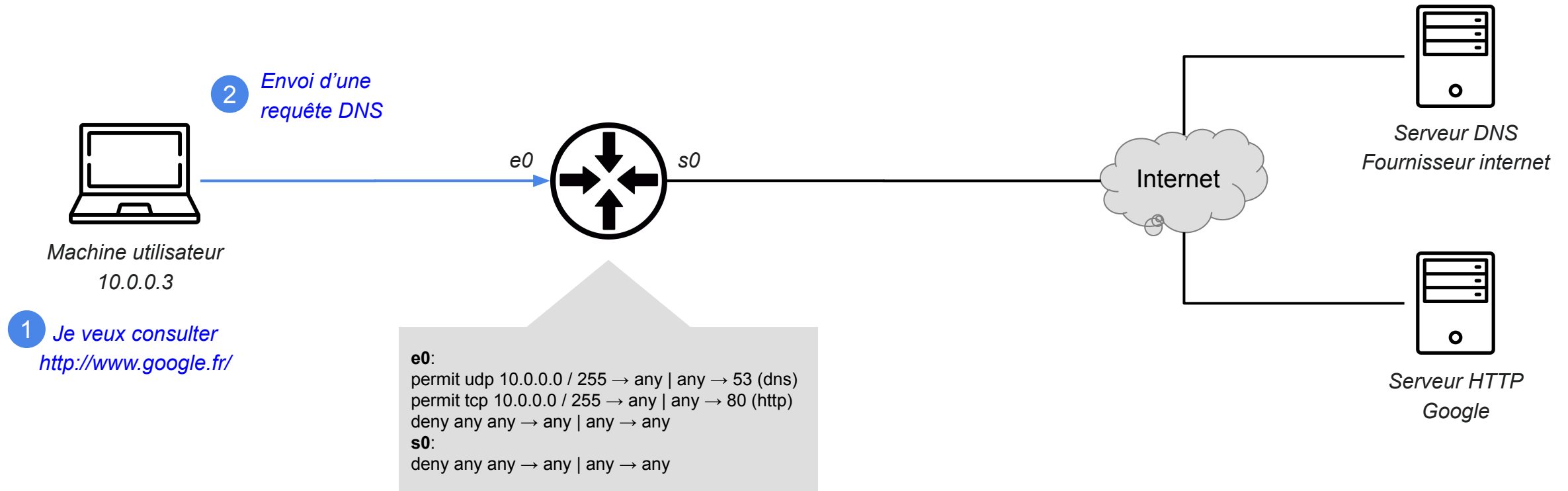
IPv4-Based ACL Table

Bonnes pratiques

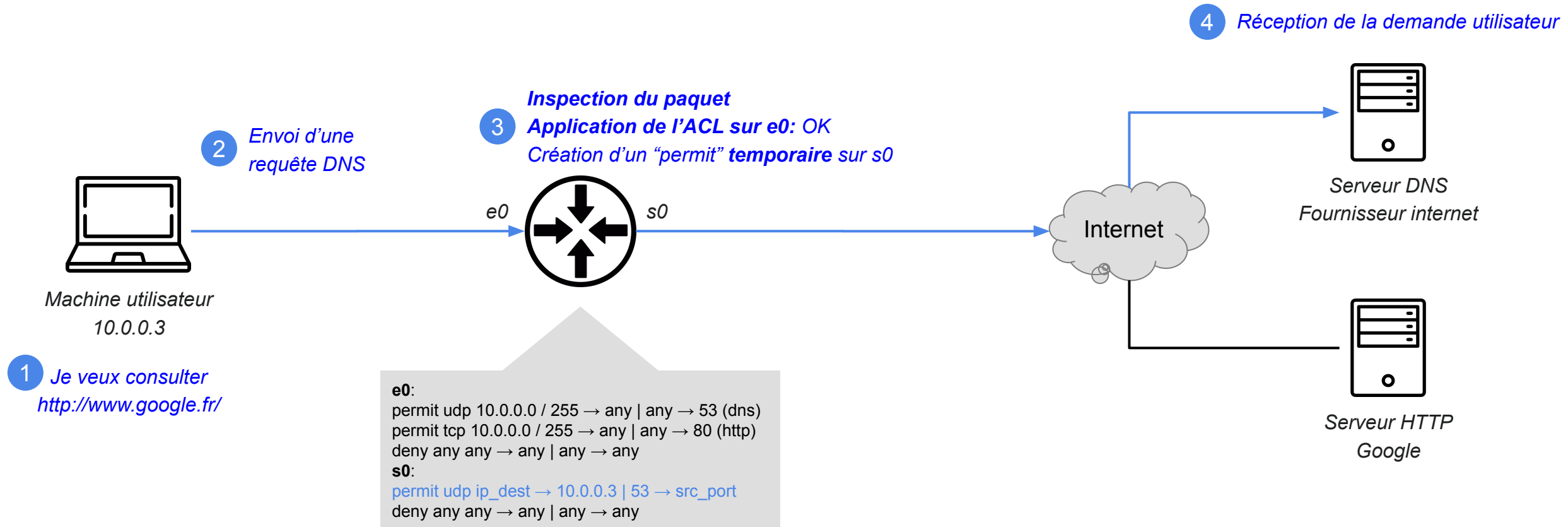
- 1. Seuls les trafics des services autorisés doivent être permis (explicitement)
- 2. Toujours terminer les règles par un DENY ALL
- 3. Restreindre l'accès aux interfaces d'administration (par exemple via un VLAN d'administration dédié)
- 4. Privilégier les accès chiffrés
- 5. Veiller à mettre à jours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

Source image : <https://community.cisco.com/t5/small-business-switches/sq300-ace-creation-quot-already-exists-quot/td-p/2371907>

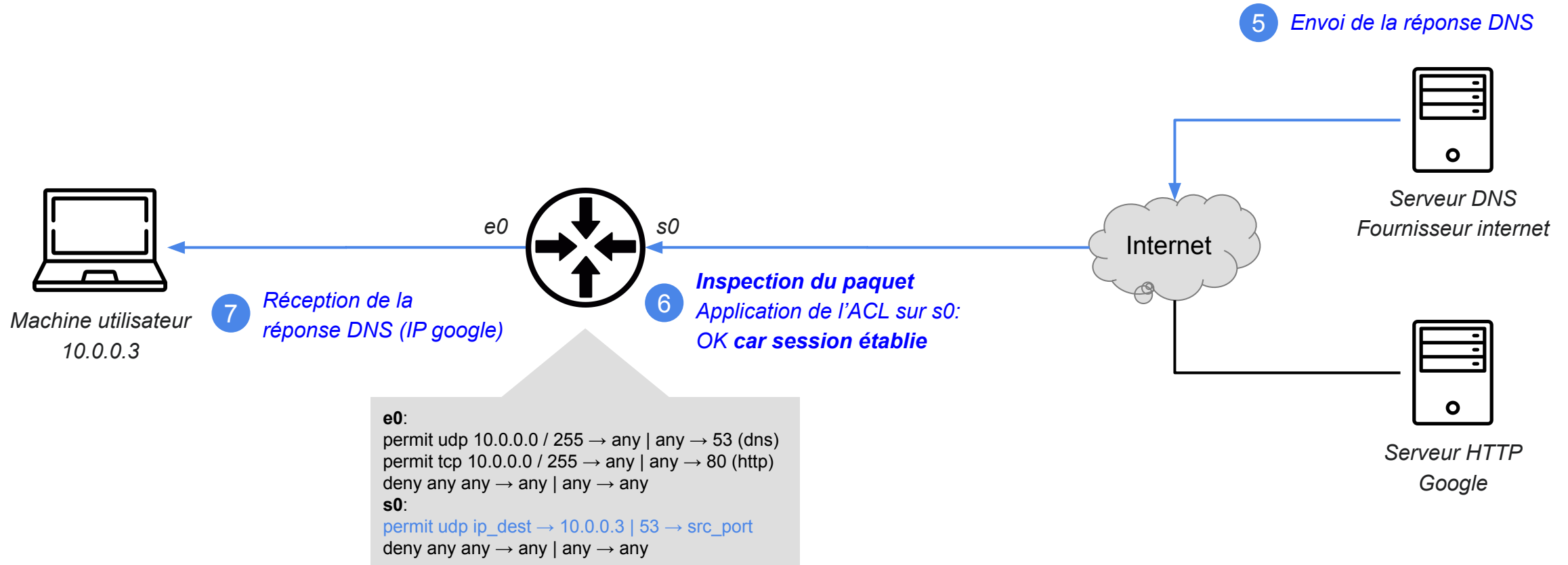
Fonctionnement des ACLs dynamiques (1/5)



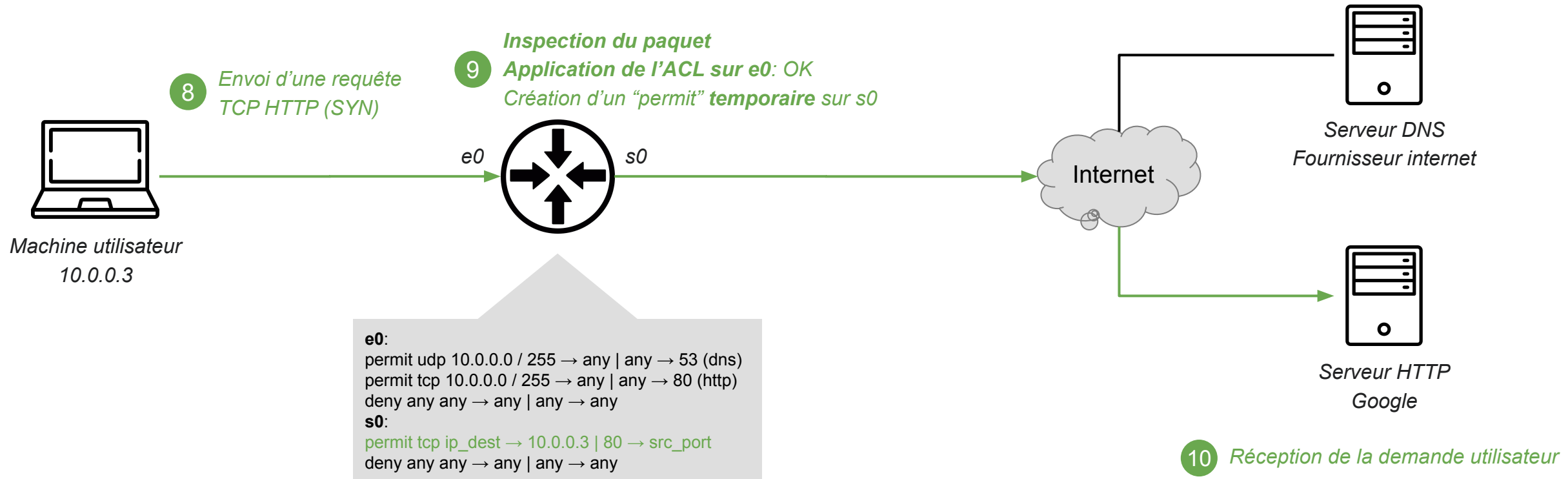
Fonctionnement des ACLs dynamiques (2/5)



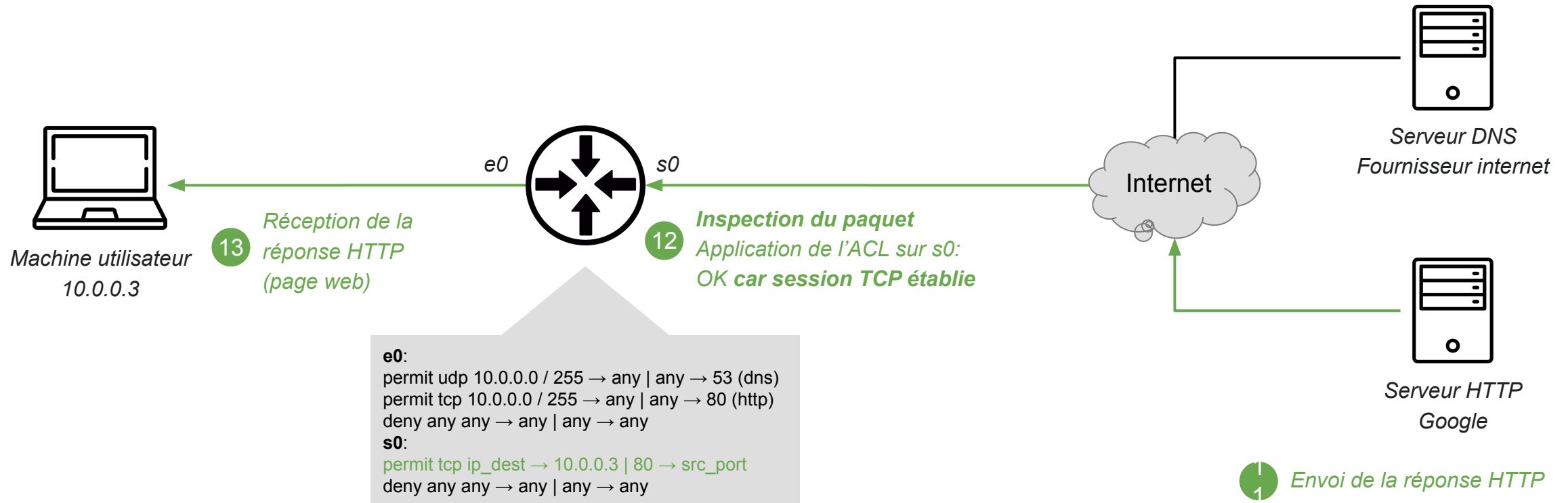
Fonctionnement des ACLs dynamiques (3/5)



Fonctionnement des ACLs dynamiques (4/5)



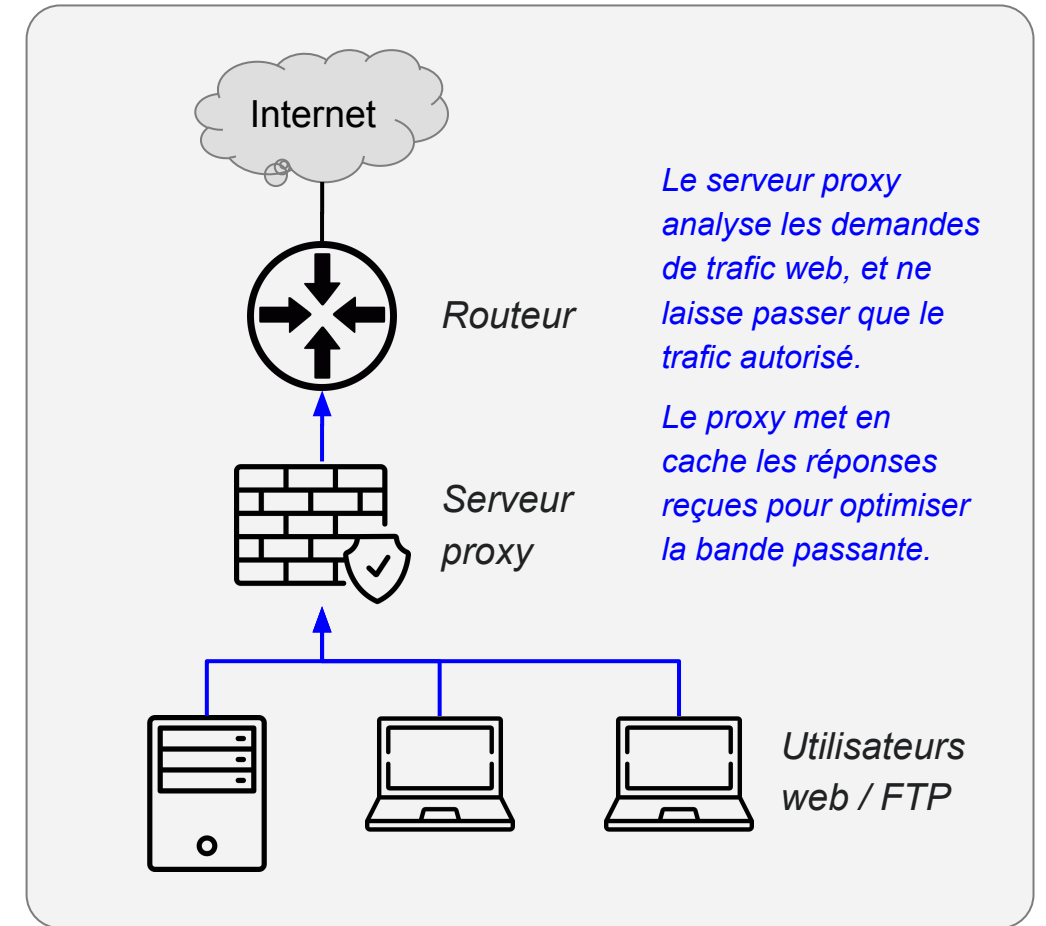
Fonctionnement des ACLs dynamiques (5/5)



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 interaction 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 - Exemple de catégories Symantec Bluecoat



The screenshot displays the Symantec Bluecoat proxy categories interface. It features three main sections: 'Responsabilité juridique' (Legal Responsibility), 'Sécurité' (Security), and 'Lié aux affaires' (Business Related). Each section contains a list of sub-categories. A dropdown menu is open on the right side, showing a list of categories including 'Non productif' (Non-productive), 'Société/gouvernement' (Society/government), 'Interaction sociale' (Social interaction), 'Multimédia' (Multimedia), 'Communication', 'Lié à la santé' (Related to health), and 'Loisir' (Leisure).

Section	Sub-category	
Responsabilité juridique	Pour les adultes	
	Problèmes de responsabilité	
Sécurité	Menaces de sécurité	
	Problèmes de sécurité	
	Transfert de fichiers	
Lié aux affaires	Commerce	
	Technologie	
	Lié aux informations	

Dropdown menu categories:

- Non productif
- Société/gouvernement
- Interaction sociale
- Multimédia
- Communication
- Lié à la santé
- Loisir

Serveur proxy - Exemple de catégories Symantec Bluecoat



Symantec
A Division of Broadcom

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)

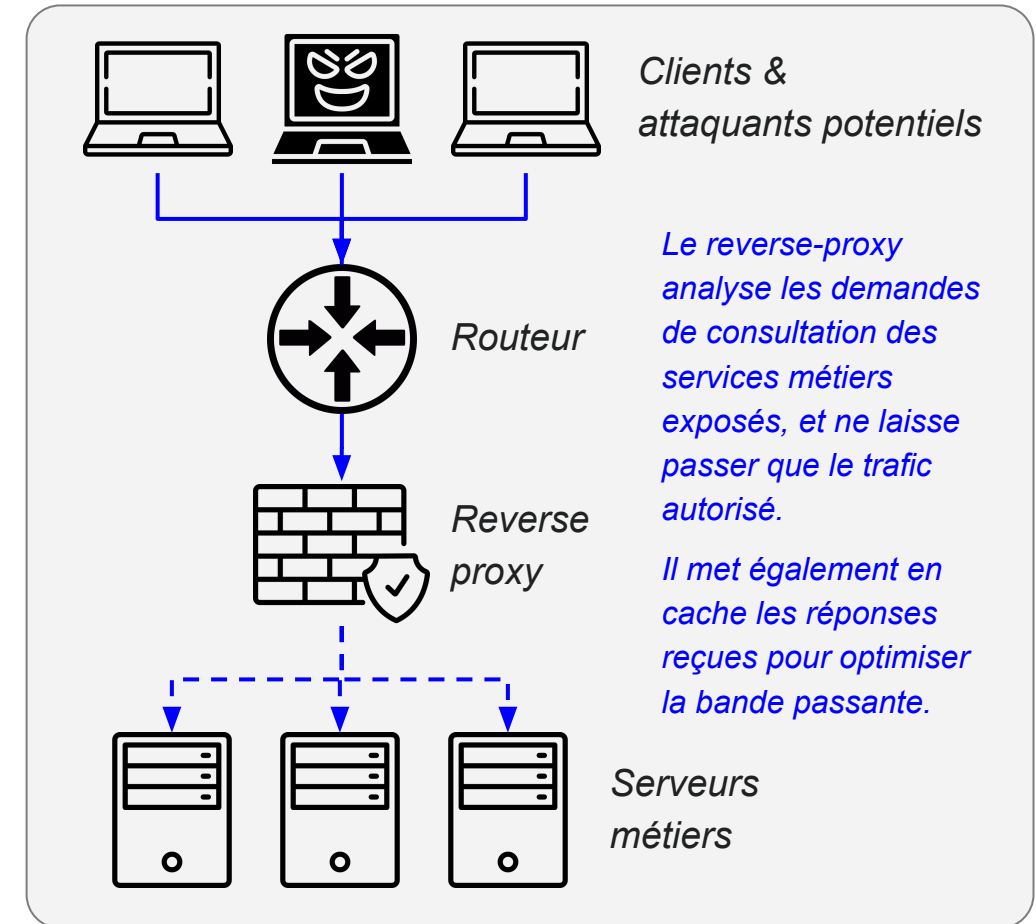
- Hôtes DNS dynamiques (Dynamic DNS Host)
- Cartes électroniques/invitations (E-Card/Invitations)
- Enseignement (Education)
- Messagerie électronique (Email)
- Publicité par courrier électronique (Email Marketing)
- Spectacles et divertissements (Entertainment)
- Stockage/partage de fichiers (File Storage/Sharing)
- 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)

Serveur reverse-proxy - Principe

Principe de fonctionnement

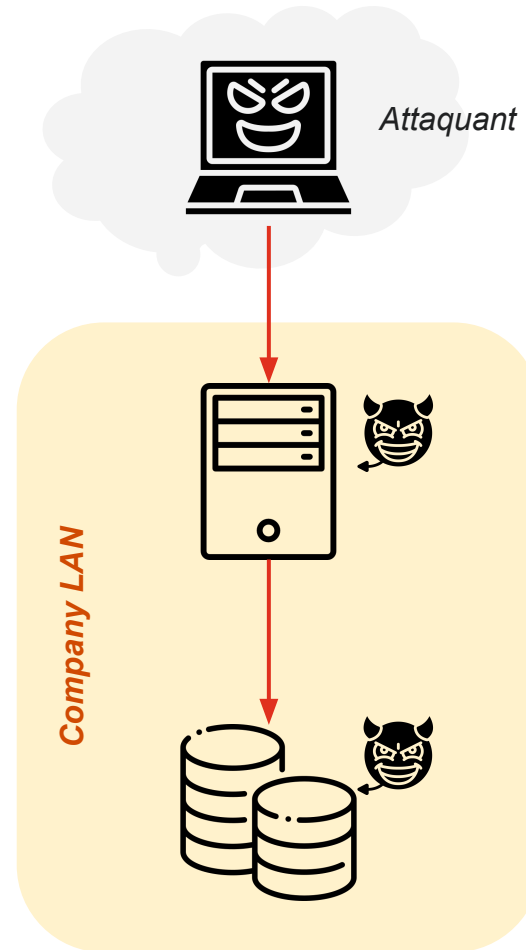
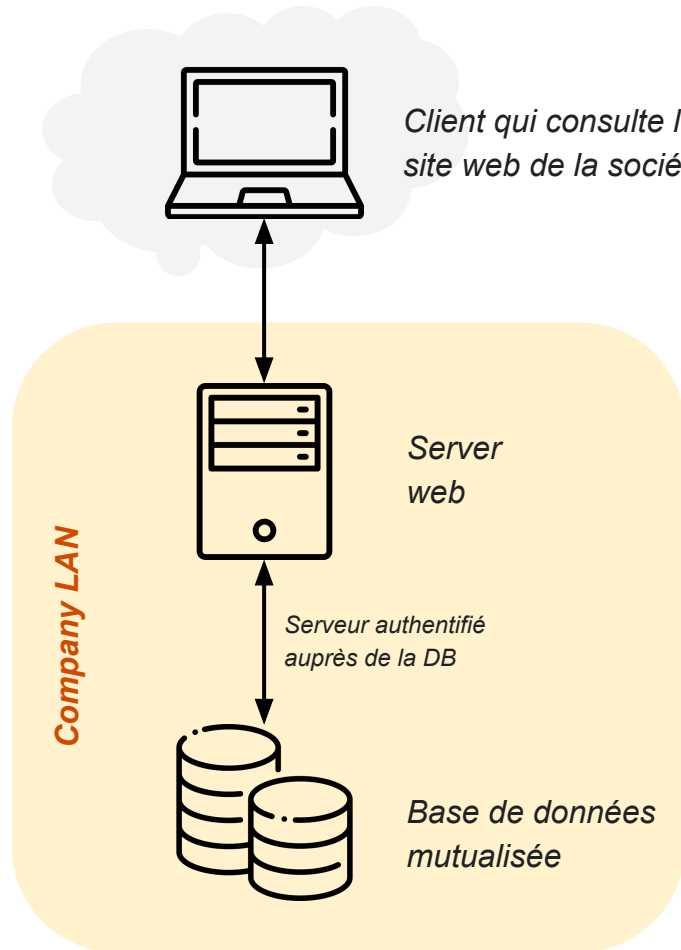
- **Rôle = fonction inverse d'un serveur proxy : mise en cache des serveurs internes en vue d'une consultation depuis internet**
- Le serveur reverse-proxy **filtre les demandes HTTP** (ou autres services métiers, en fonction des ports / protocoles exposés)
- **Le serveur reverse-proxy reçoit donc toutes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





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 à minima 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.

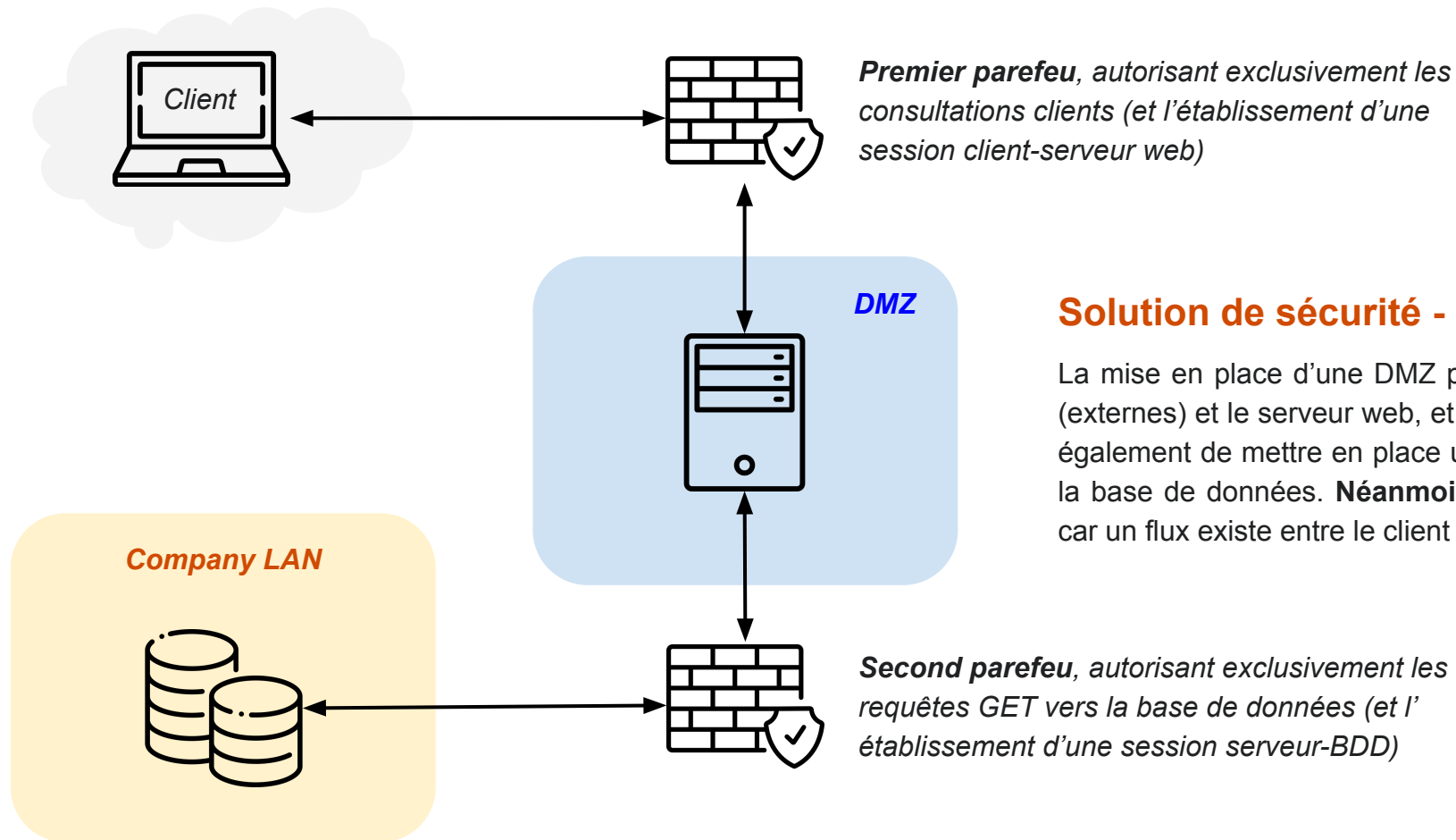
Néanmoins, grâce à son **accès direct et inconditionnel** à la DB, l'attaquant peut tenter de nouveaux exploits pour obtenir un accès root.

DMZ (Zone Démilitarisée) - Principe



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

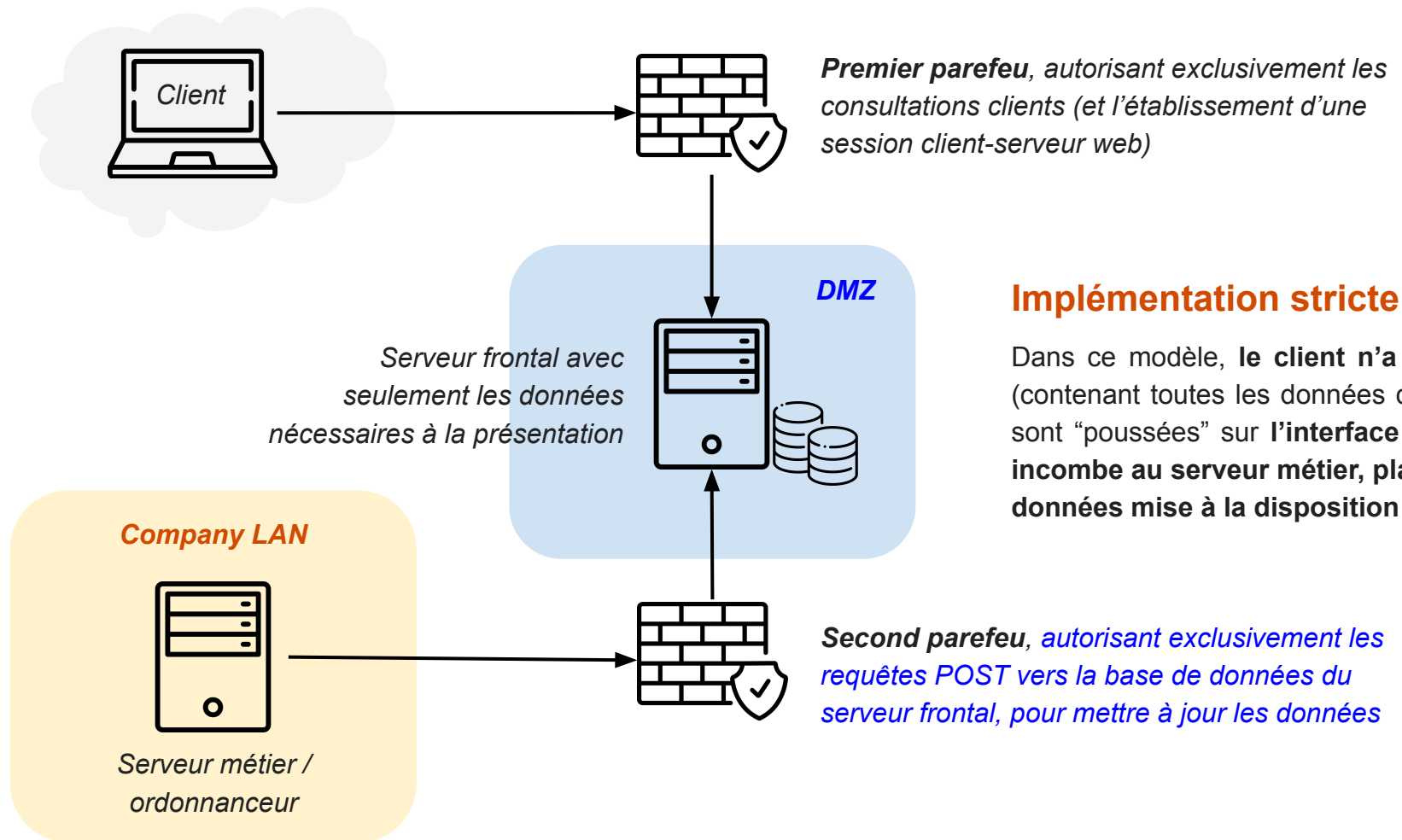
DMZ (Zone Démilitarisée) - Mise en place partielle



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.

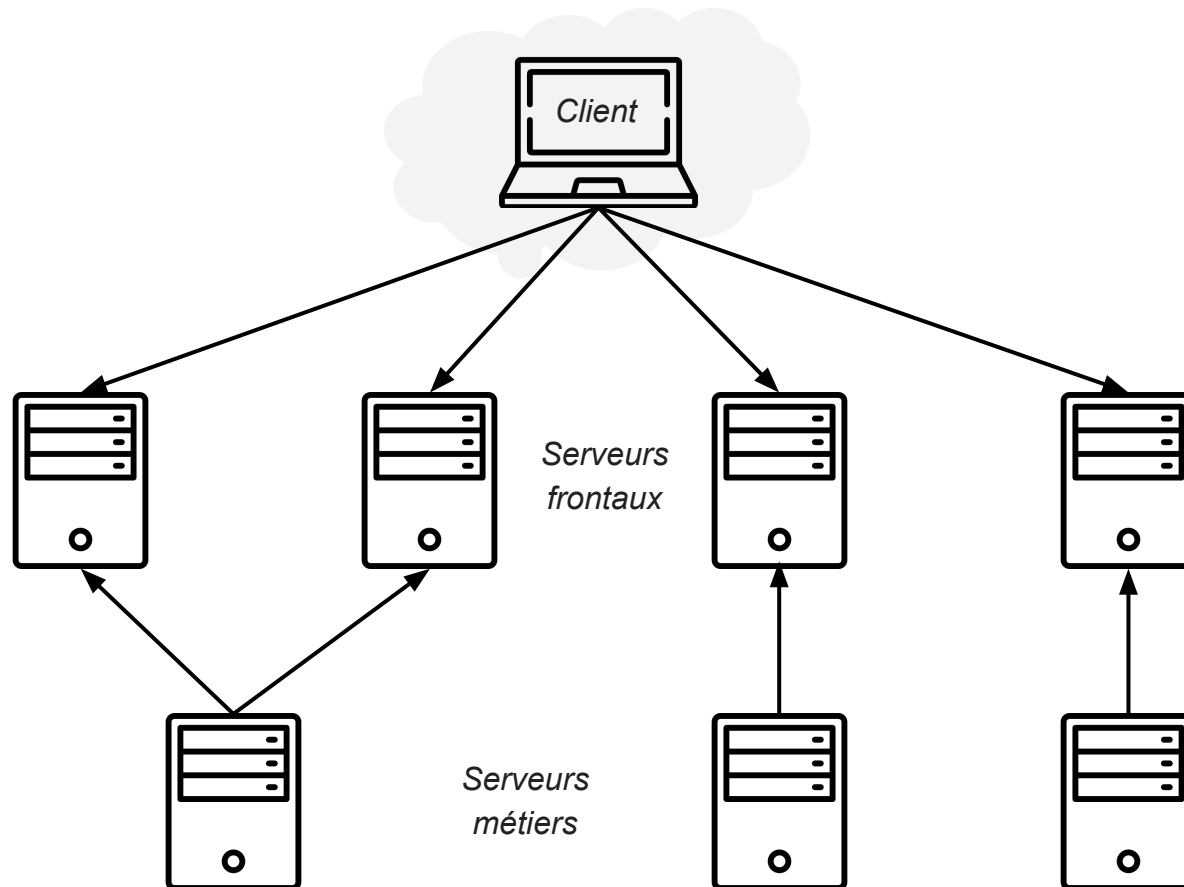
DMZ (Zone Démilitarisée) - Implémentation stricte



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.

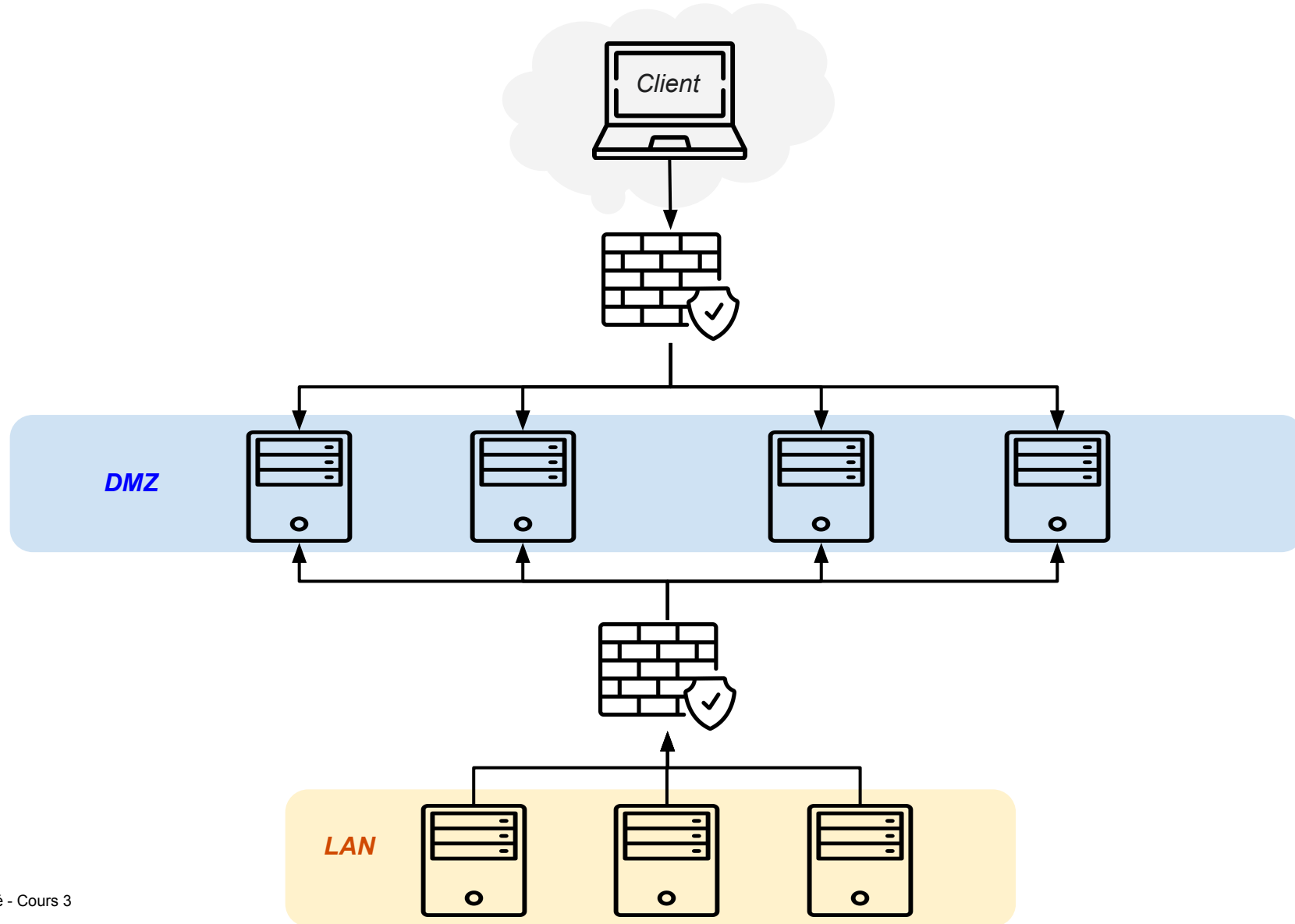
DMZ (Zone Démilitarisée) - Passage à l'échelle (1/4)



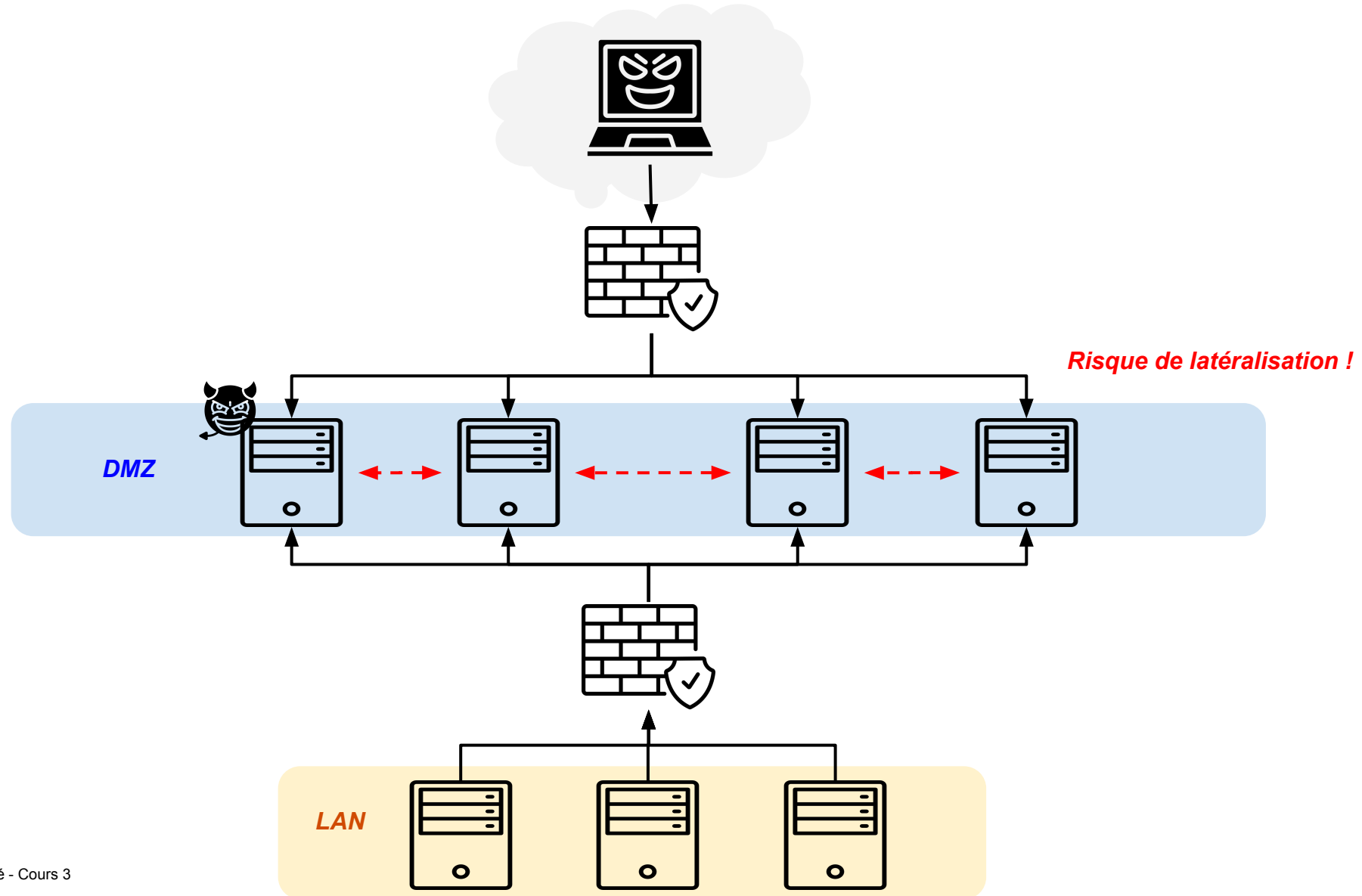
Problème de sécurité

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

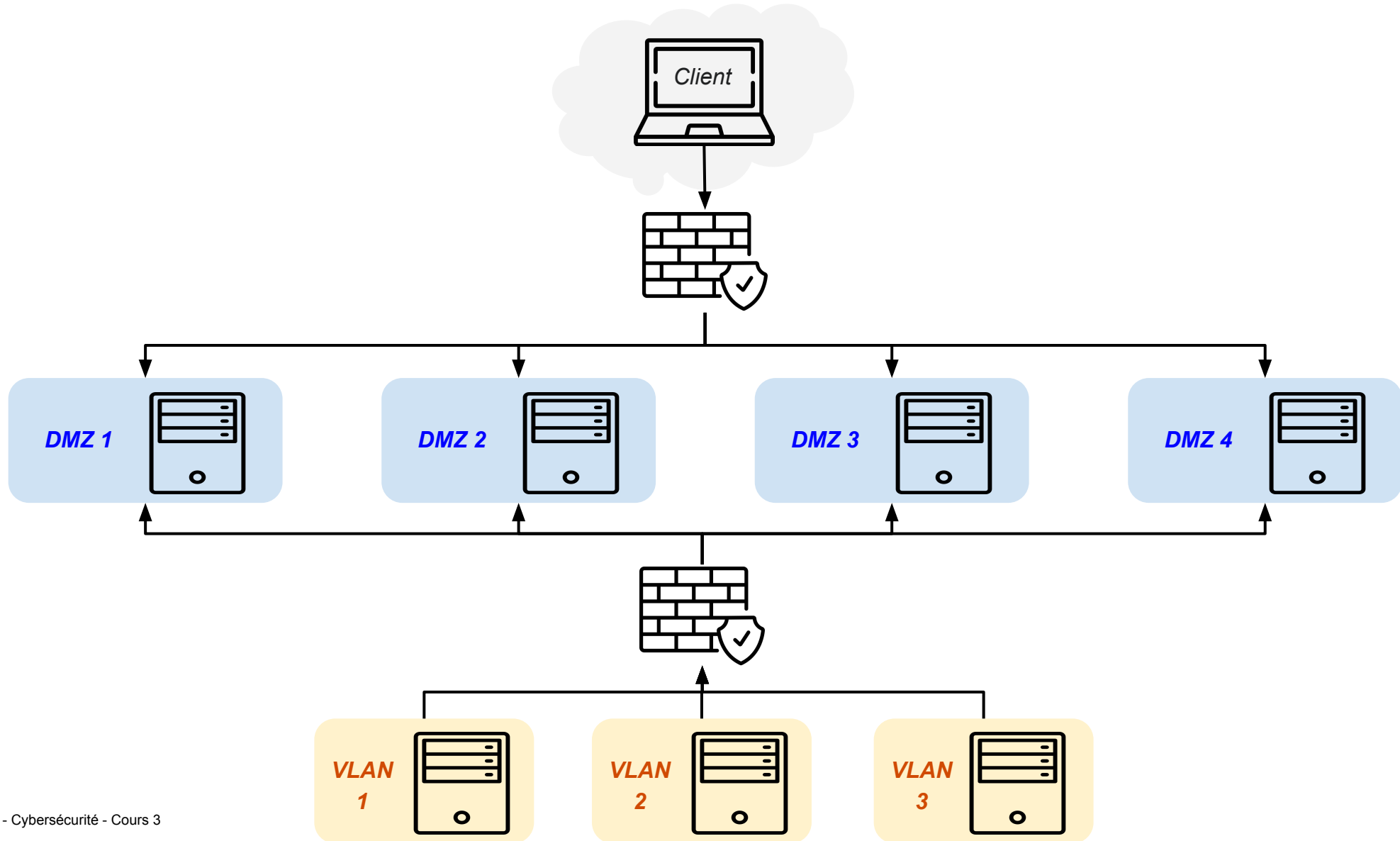
DMZ (Zone Démilitarisée) - Passage à l'échelle (2/4)



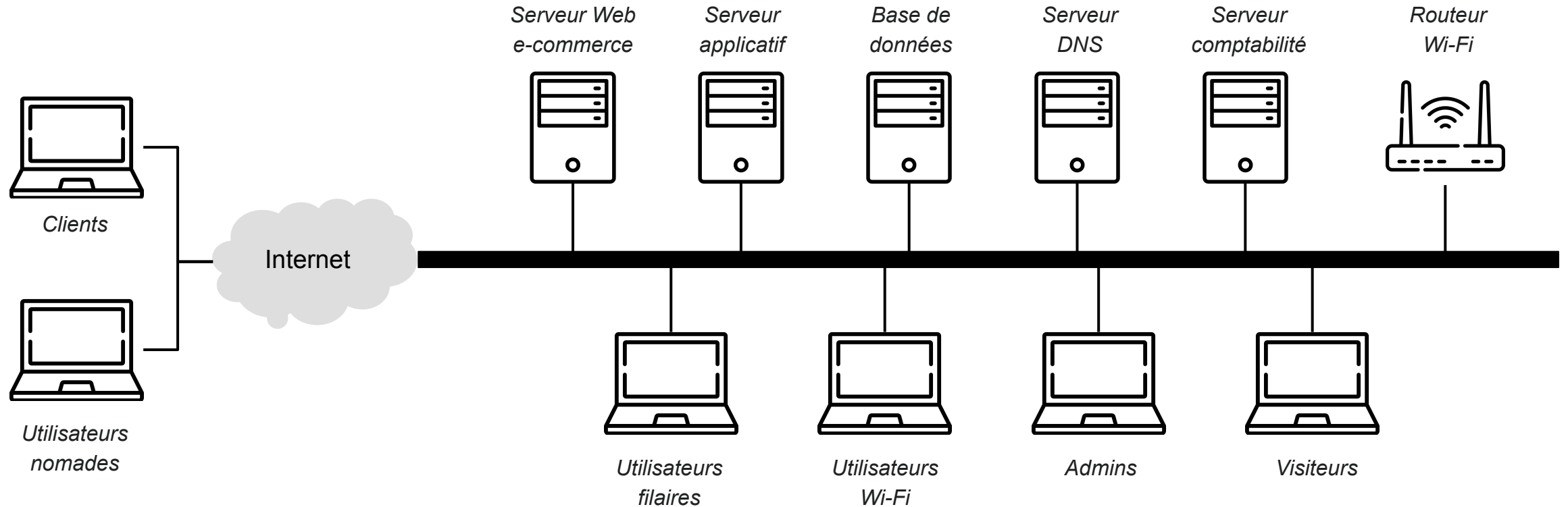
DMZ (Zone Démilitarisée) - Passage à l'échelle (3/4)



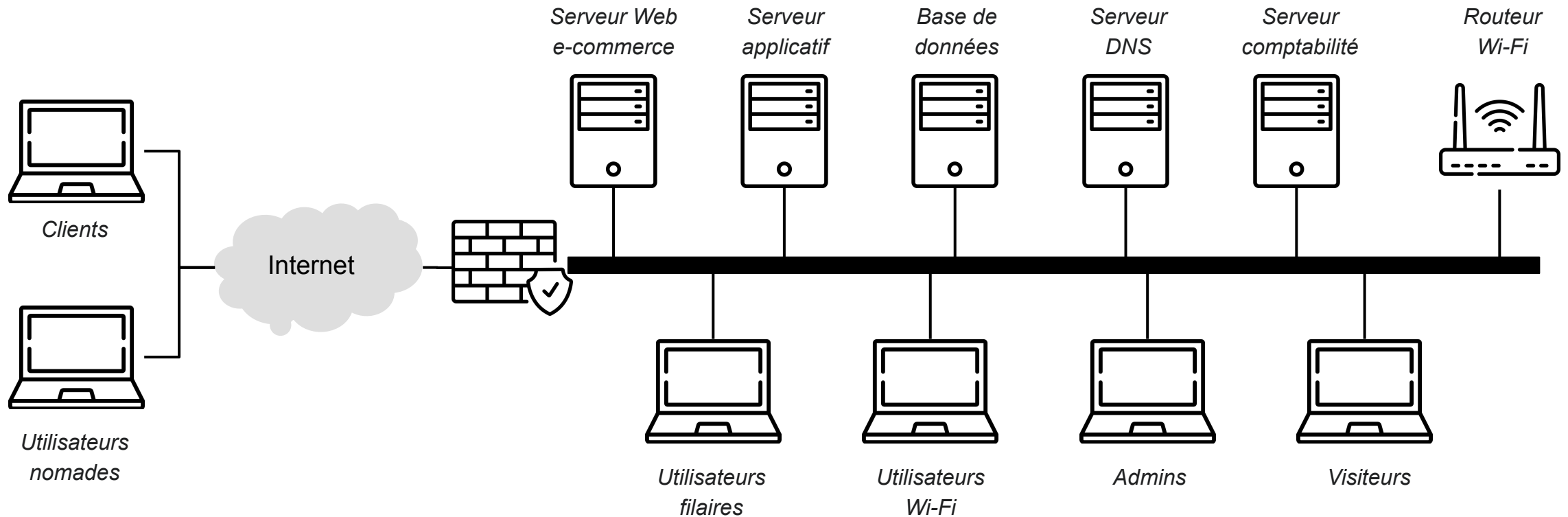
DMZ (Zone Démilitarisée) - Passage à l'échelle (4/4)



Exercice: sécuriser une PME - Situation initiale



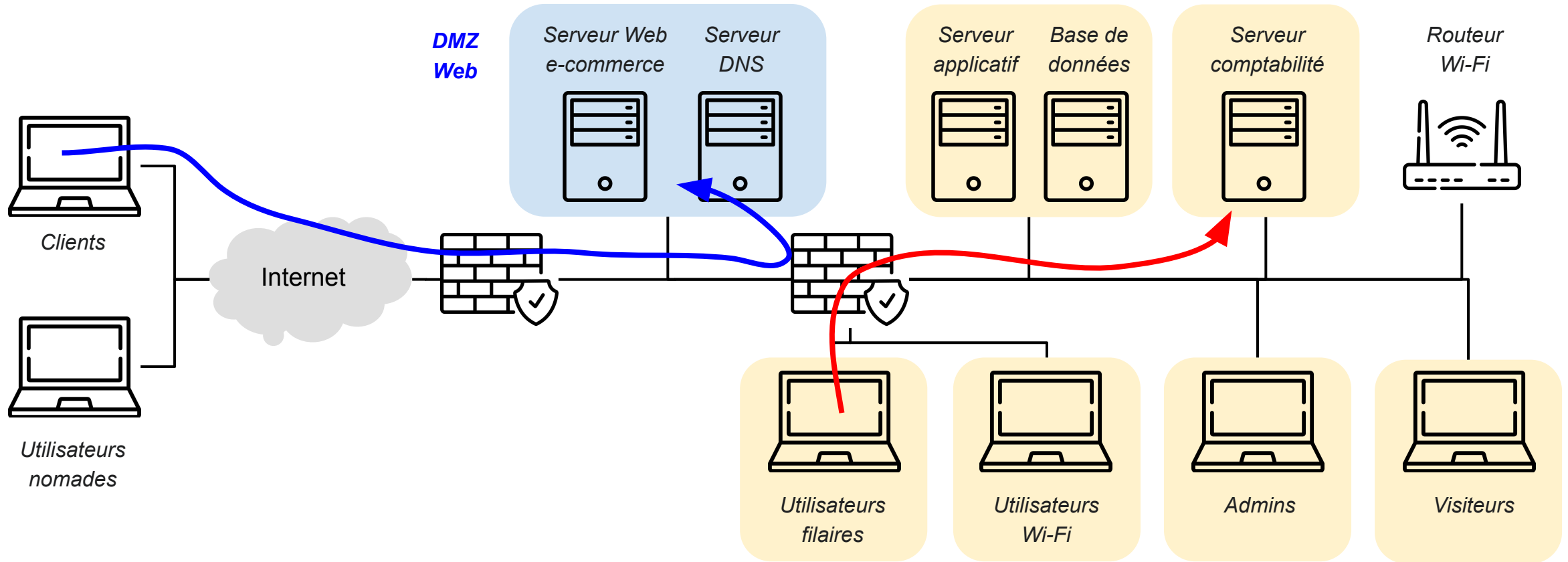
Exercice: sécuriser une PME (1/6)



Etape 1:

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

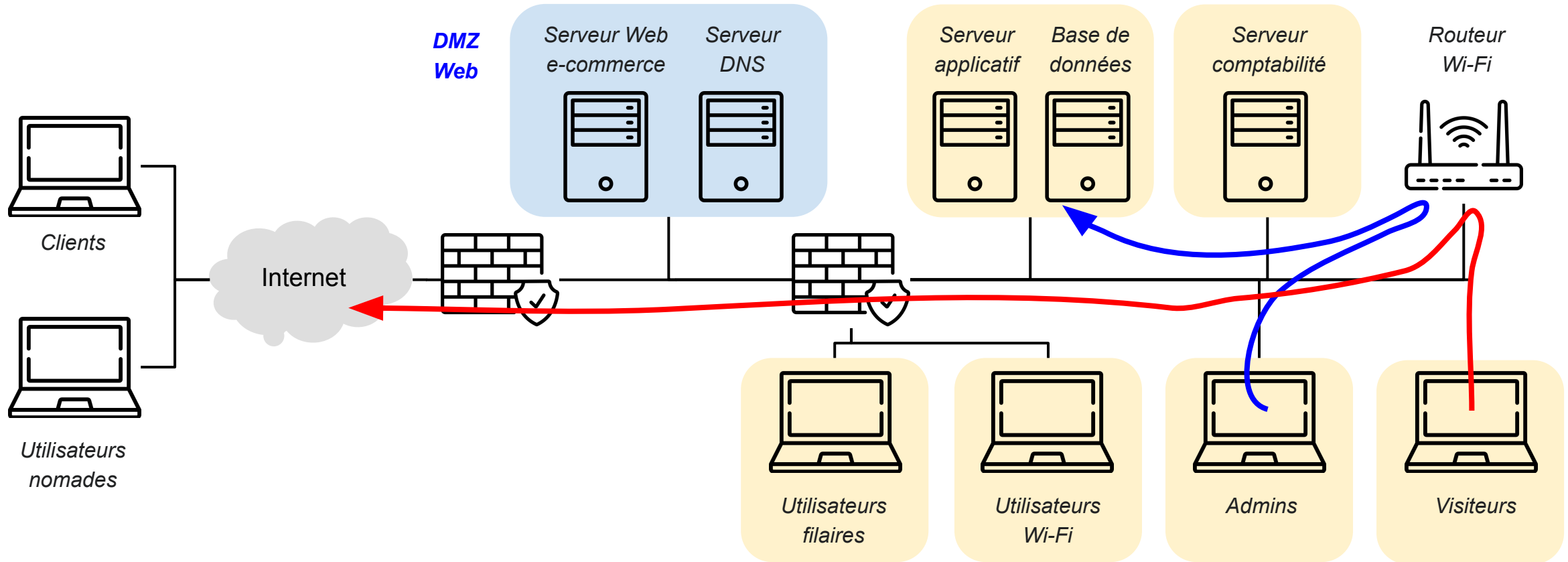
Exercice: sécuriser une PME (2/6)



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)

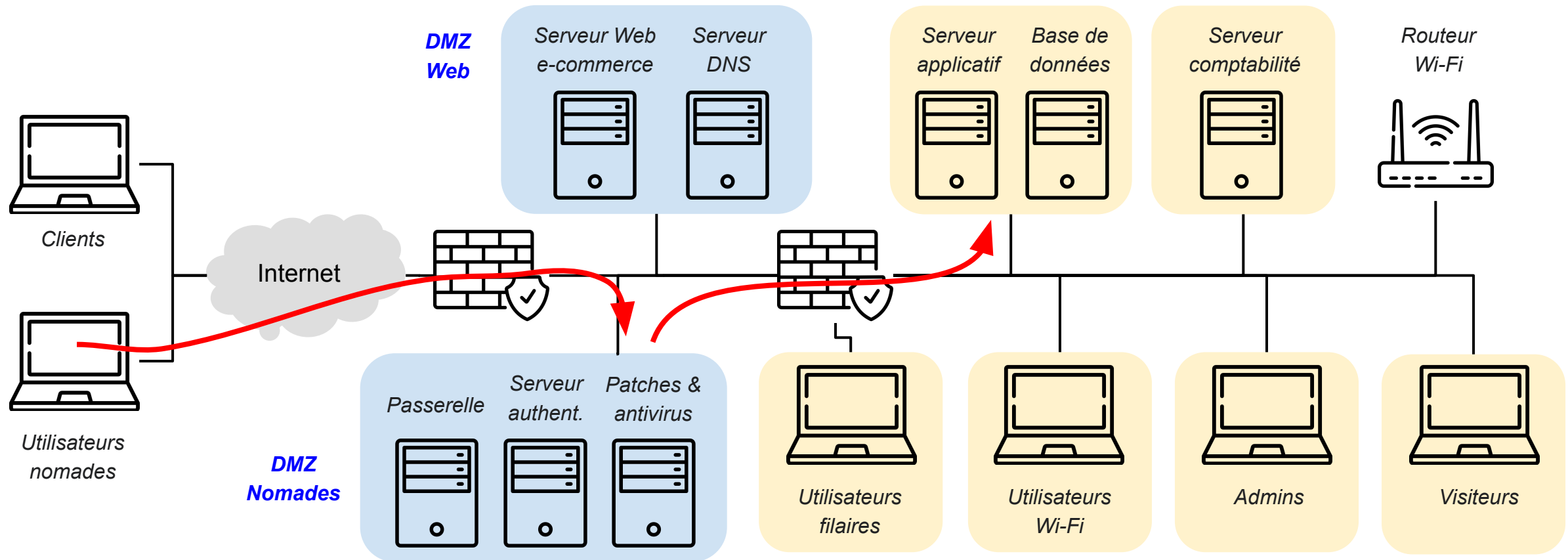


Etape 3:

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.

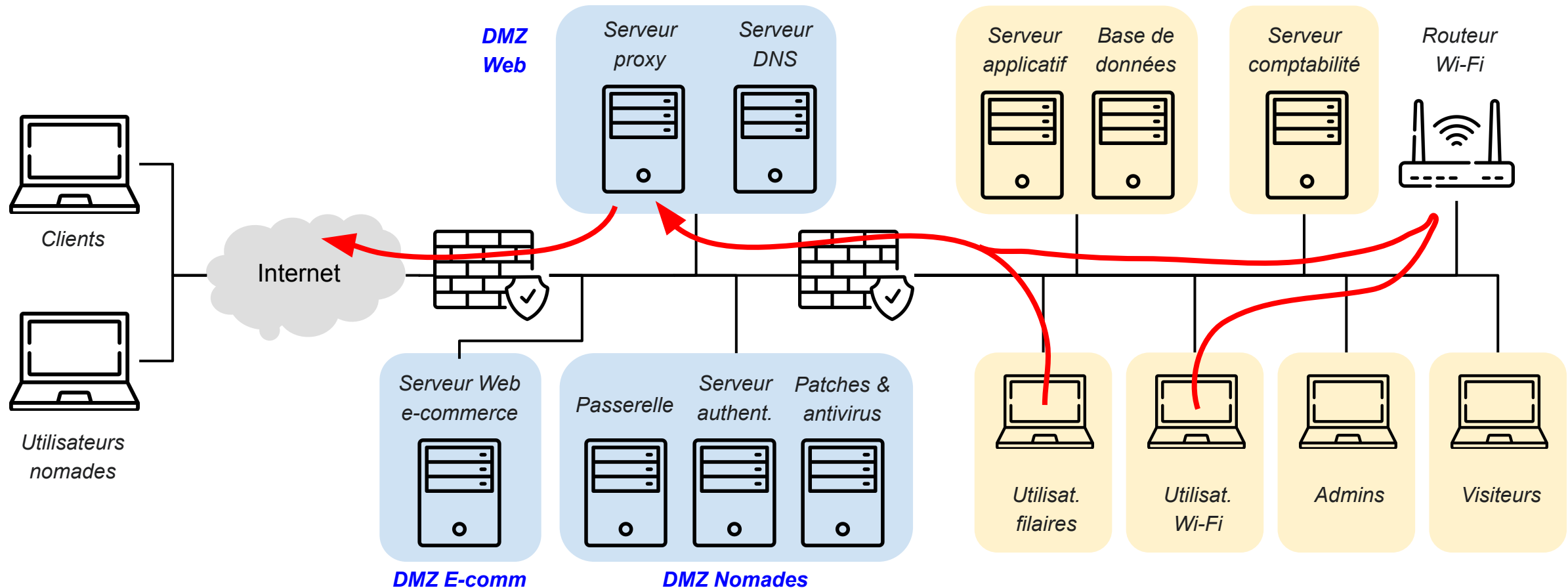
Exercice: sécuriser une PME (4/6)



Etape 4:

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

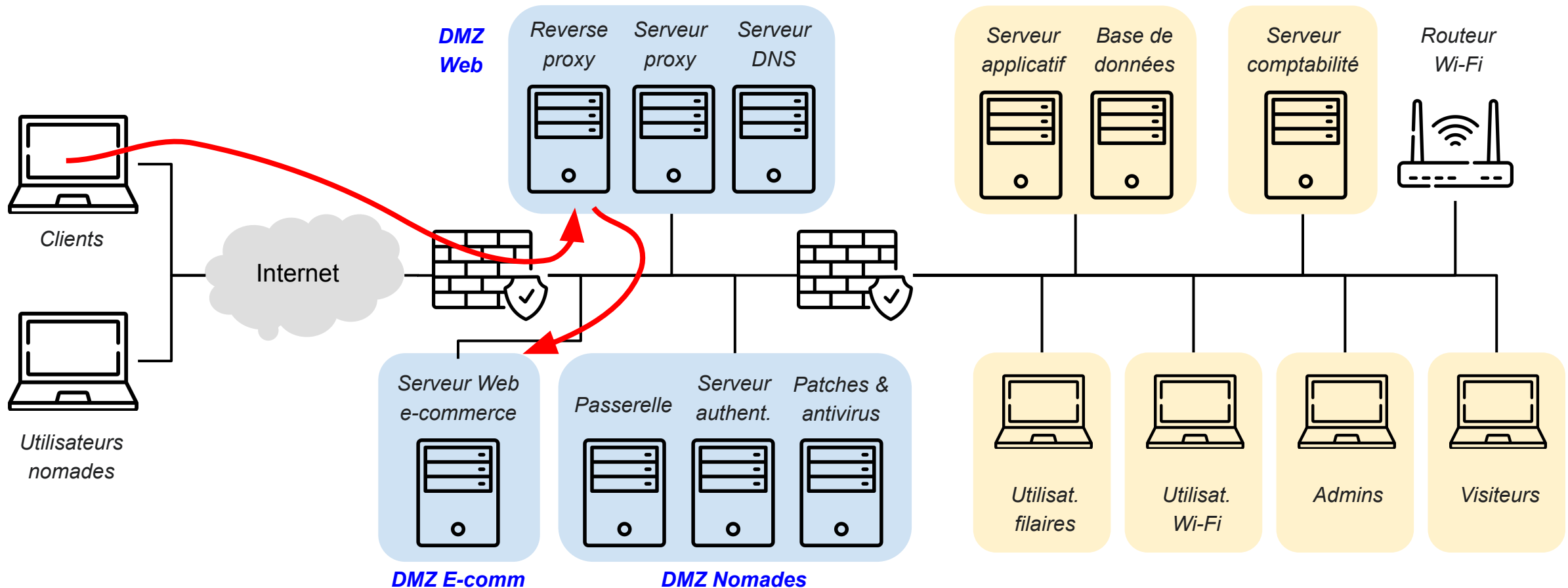
Exercice: sécuriser une PME (5/6)



Etape 5:

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

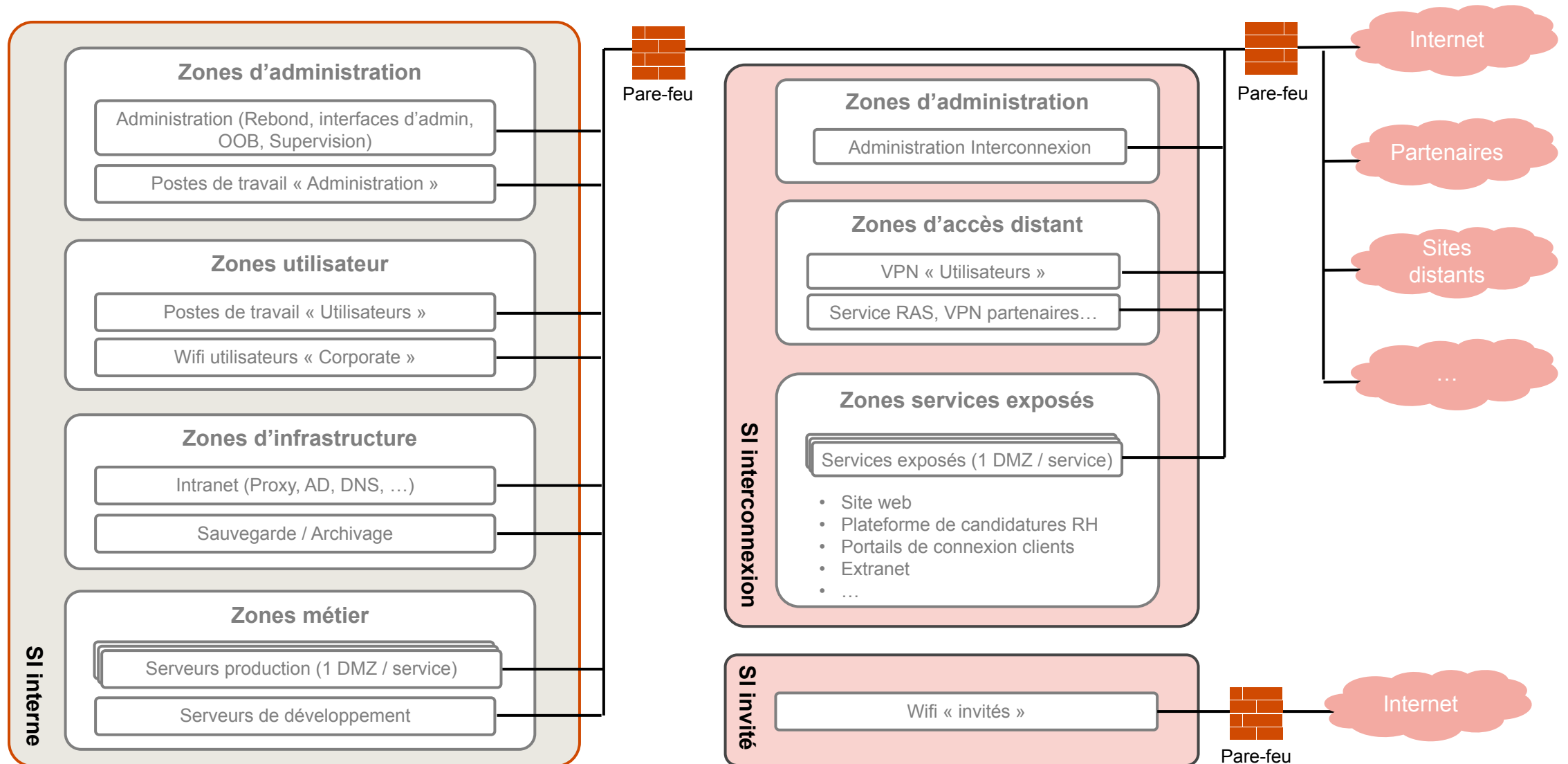
Exercice: sécuriser une PME (6/6)



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 delà du port 1024)
- Scan de versions
 - Applications
 - OS
- Scans agressifs (pour un maximum d'infos)

```
root@ubuntu:~#  
root@ubuntu:~# nmap -P0 -vv -sS 192.168.100.1 -p 0-1024  
Warning: The -P0 option is deprecated. Please use -Pn  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-17 09:01 PDT  
Initiating ARP Ping Scan at 09:01  
Scanning 192.168.100.1 [1 port]  
Completed ARP Ping Scan at 09:01, 0.00s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 09:01  
Completed Parallel DNS resolution of 1 host. at 09:01, 0.01s elapsed  
Initiating SYN Stealth Scan at 09:01  
Scanning 192.168.100.1 [1025 ports]  
Discovered open port 139/tcp on 192.168.100.1  
Discovered open port 135/tcp on 192.168.100.1  
Discovered open port 445/tcp on 192.168.100.1  
Completed SYN Stealth Scan at 09:01, 4.97s elapsed (1025 total ports)  
Nmap scan report for 192.168.100.1  
Host is up, received arp-response (0.00014s latency).  
Scanned at 2018-04-17 09:01:29 PDT for 5s  
Not shown: 1022 filtered ports  
Reason: 1022 no-responses  
PORT      STATE SERVICE      REASON  
135/tcp   open  msrpc        syn-ack ttl 128  
139/tcp   open  netbios-ssn  syn-ack ttl 128  
445/tcp   open  microsoft-ds syn-ack ttl 128  
MAC Address: 08:00:5E:12:00:08 (VMware)  
  
Read data files from: /usr/bin/../../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds  
Raw packets sent: 2050 (90.184KB) | Rcvd: 6 (248B)
```



Sécurité en profondeur: IPS & IDS

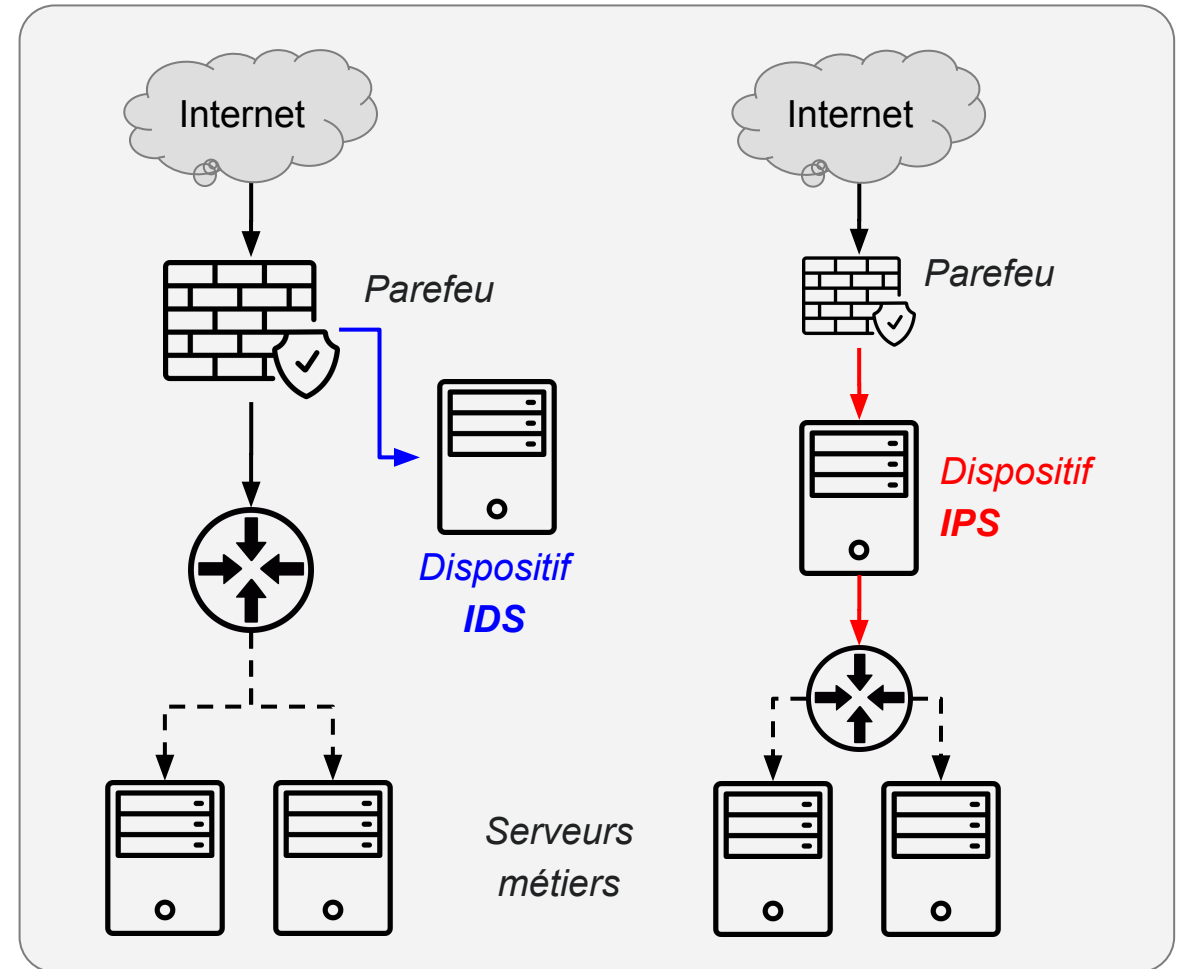
Intrusion Detection/Prevention Systems (IDS/IPS)

Pourquoi on ne s'arrête pas là ?

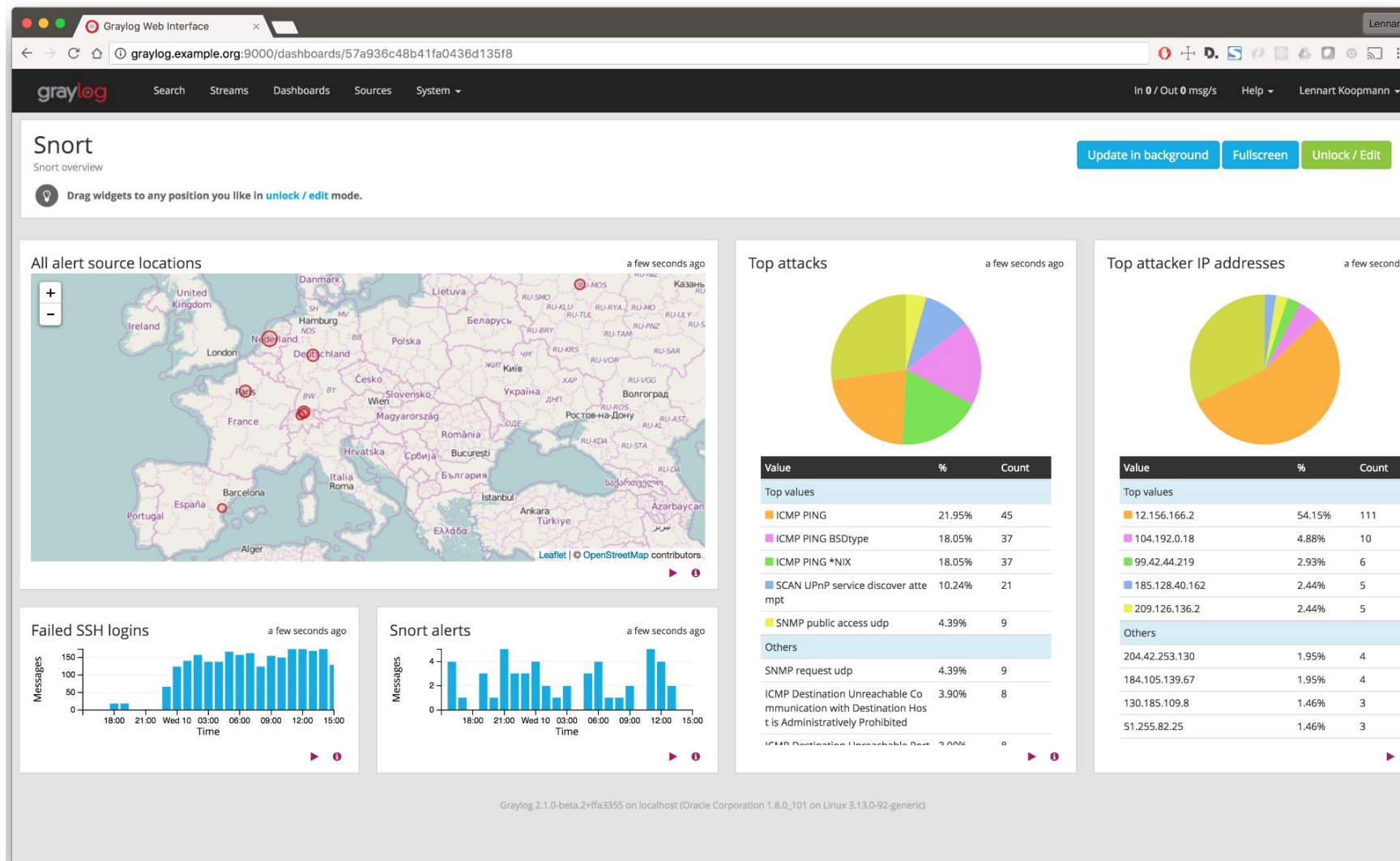
Les switches, routeurs, parefeux et proxys sont (principalement) des outils de **roulage** et de **filtrage**. La sécurité proposée par ces équipements est fondamentalement basée sur des principes de **contrôle d'accès** (avec des listes et des règles). Ces équipements se basent sur les entêtes des paquets,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

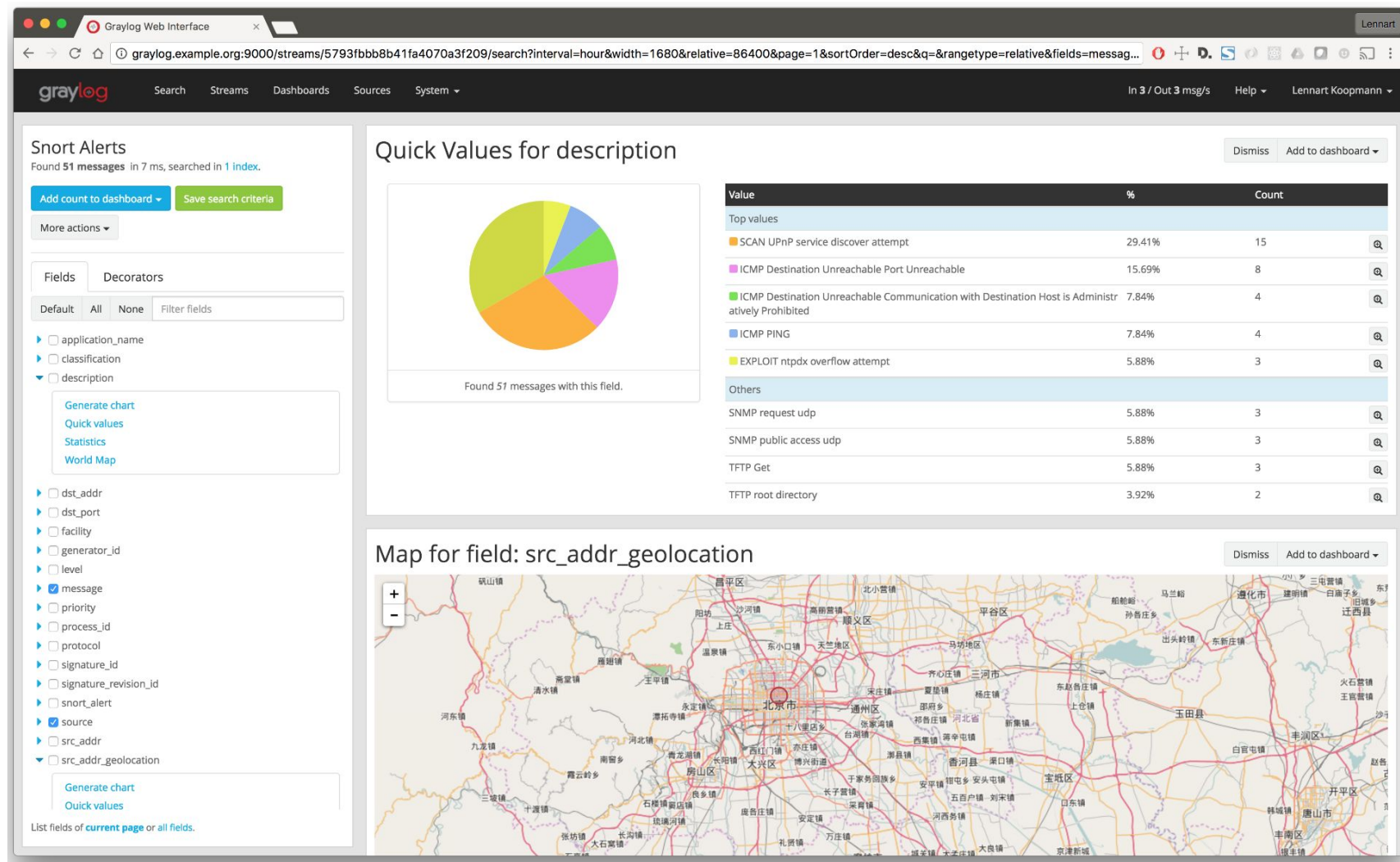
- Un **IDS** est un outil de **détection** et de **monitoring**
 - Ces outils ne prennent pas d'action, ils lèvent des alertes
 - Sans opérateur pour revoir les alertes, l'IDS ne sert à rien !
- Un **IPS** est un outil de **prévention** et de **contrôle**
 - Ces outils sont bloquants : ils rejettent 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)



IDS - Exemple de dashboard sécurité (2/2)





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](https://www.pwc.fr)

© 2022 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.