Université Grenoble Alpes

M25-2. Technologies de sécurité

cours@cyril-bras.fr

Introduction

Lorsqu'ils ont été conçus, le protocole IP et les protocoles associés (TCP, UDP, ICMP, routage…) n'ont pas pris en compte la sécurité

•« Concept sécurité » inconnu à l'époque, personne n'imaginait que ces protocoles pourraient être détournés à des fins malveillantes ;

•**Aucun mécanisme de sécurité n'est donc implémenté au sein de ces protocoles.**

Quelques exemples de faiblesses de ces protocoles

•**Absence d'authentification des émetteurs et récepteurs** d'un datagramme : usurpation d'adresse IP possible ;

•**Absence de chiffrement des données**, celles-ci sont donc transmises en clair. Un hacker positionné sur un réseau peut donc écouter les connexions et accéder aux données ;

•**Le routage des datagrammes peut être modifié** de façon à rediriger les datagrammes vers un autre destinataire ;

•Note : l'exploitation de ces faiblesses nécessite des prérequis techniques, i.e. elles ne sont pas systématiquement applicables à tous les réseaux.

Les diapositives suivantes illustrent ces faiblesses.

Introduction

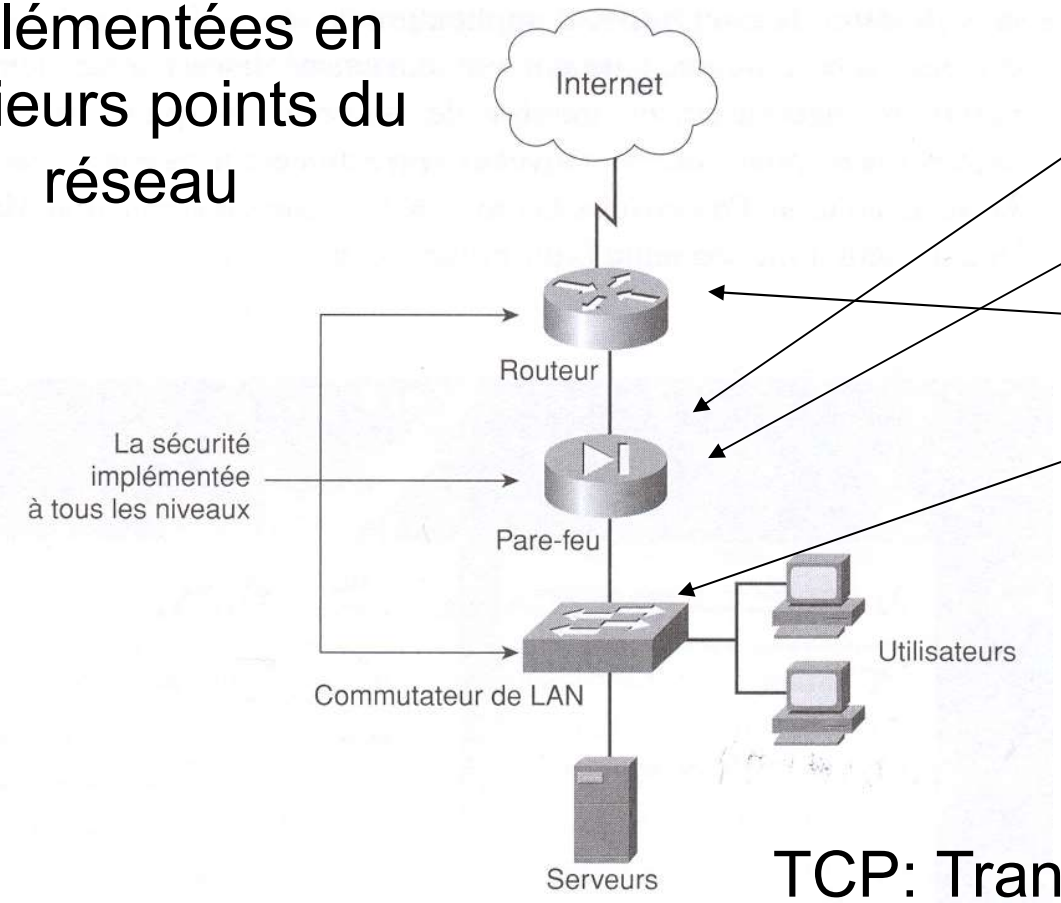
Ainsi, il est nécessaire de **mettre en œuvre des mécanismes de sécurité complémentaires** afin de réduire et maitriser les risques émanant des protocoles historiques régissant les réseaux.

Exemple de mécanismes :

- Chiffrement des communications ;
- Authentification des entités ;
- Cloisonnement réseau ;
- Filtrage ;
- Dimensionnement adapté des infrastructures ;
- Règles de renforcement des configurations des équipements ;
- Supervision des équipements ;
- etc.

Introduction

Sécurité en couches (couches TCP/IP) implémentées en plusieurs points du réseau



7. Application
4. TCP & UDP
3. IP (réseau)
2. Liaison de données
1. Physique

TCP: Transport Control Protocol
UDP: User Datagram Protocol

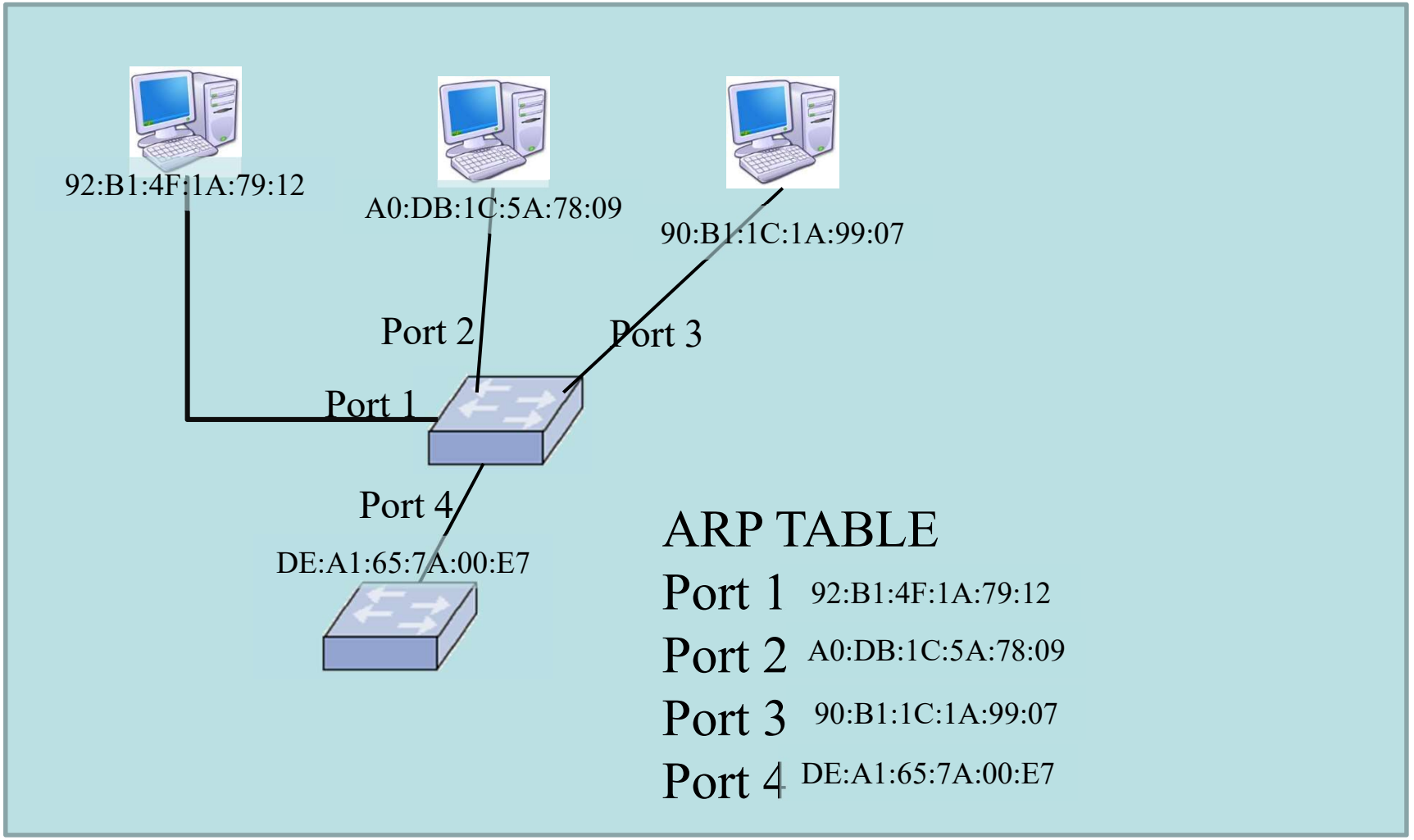
Université Grenoble Alpes

4.1 Les composants simples : commutateurs, ponts et passerelles

4.1.1 Commutateur

4.1.3 Passerelle

4.1.1 Switch


92:B1:4F:1A:79:12
A0:DB:1C:5A:78:09
90:B1:1C:1A:99:07
Port 2
Port 3
Port 1
Port 4
DE:A1:65:7A:00:E7
ARP TABLE
Port 1 92:B1:4F:1A:79:12
Port 2 A0:DB:1C:5A:78:09
Port 3 90:B1:1C:1A:99:07
Port 4 DE:A1:65:7A:00:E7

4.1.1 Commutateur (switch)

- Utilité
  - Couche 2 du modèle OSI
  - Relie les machines entre elles
  - Permet d'augmenter le débit
    - Supprime les collisions
    - Permet d'utiliser le full-duplex
- Fonctionnement
  - Le commutateur apprend les adresses MAC (protocole ARP: Address Resolution Protocol)
    - Note les adresses source des paquets
    - Envoi du paquet directement à la destination (si adresse destination connue)
    - Sinon, envoi sur tous les autres ports

4.1.1 Commutateur (switch) : contournements

- Fausses annonces ARP
- Modification de l'adresse MAC
  - Sous Linux: ifconfig
  - Sous Windows: ipconfig (Propriétés de la carte réseau)
  - Conséquences
    - Tous les paquets arrivent
- Convertir le commutateur en hub
  - Envoi massif d'annonces ARP
  - Saturation de la table, l'apprentissage recommence
  - Conséquences
    - Déni de service
- Obtention d'un contrôle sur tout le réseau
  - Accès à toutes les adresses MAC

4.1.1 Commutateur (switch) : Contre-mesures

Segmenter le réseau physique

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

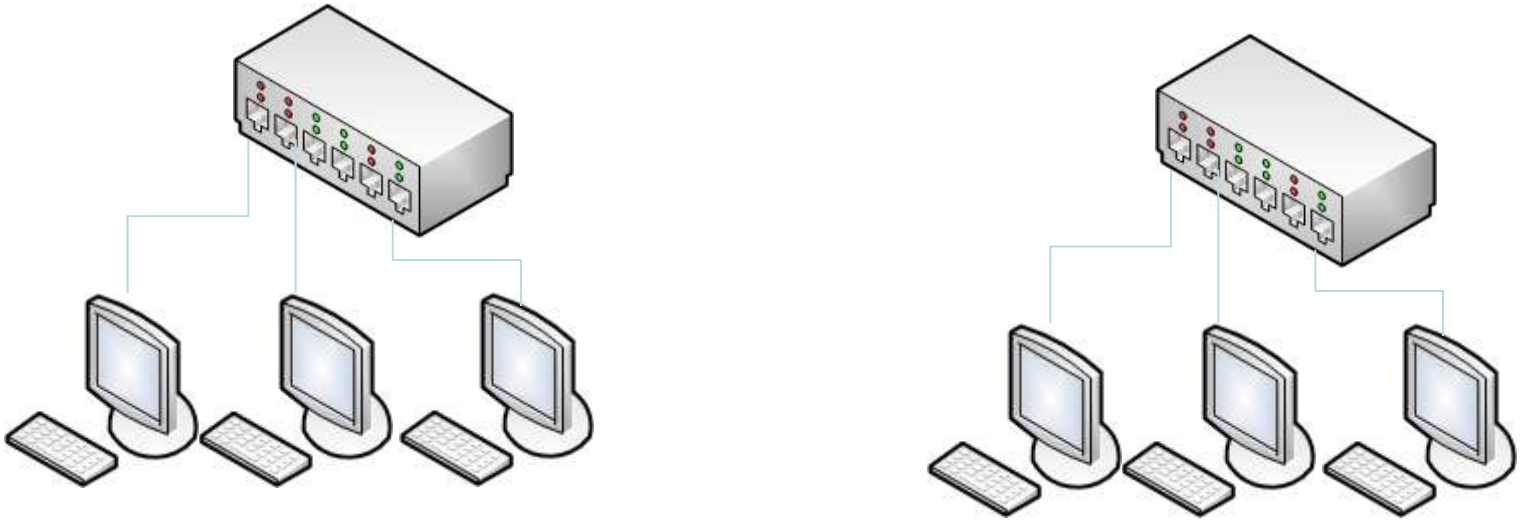
On ne doit donner les droits d'accès à une ressource qu'aux seules personnes/entités ayant un besoin légitime d'y accéder.

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

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

4.1.1 Commutateur (switch) : Contre-mesures

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



Implémentation de deux réseaux physiques différents, non connectés.

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

4.1.1 Commutateur (switch) : Contre-mesures

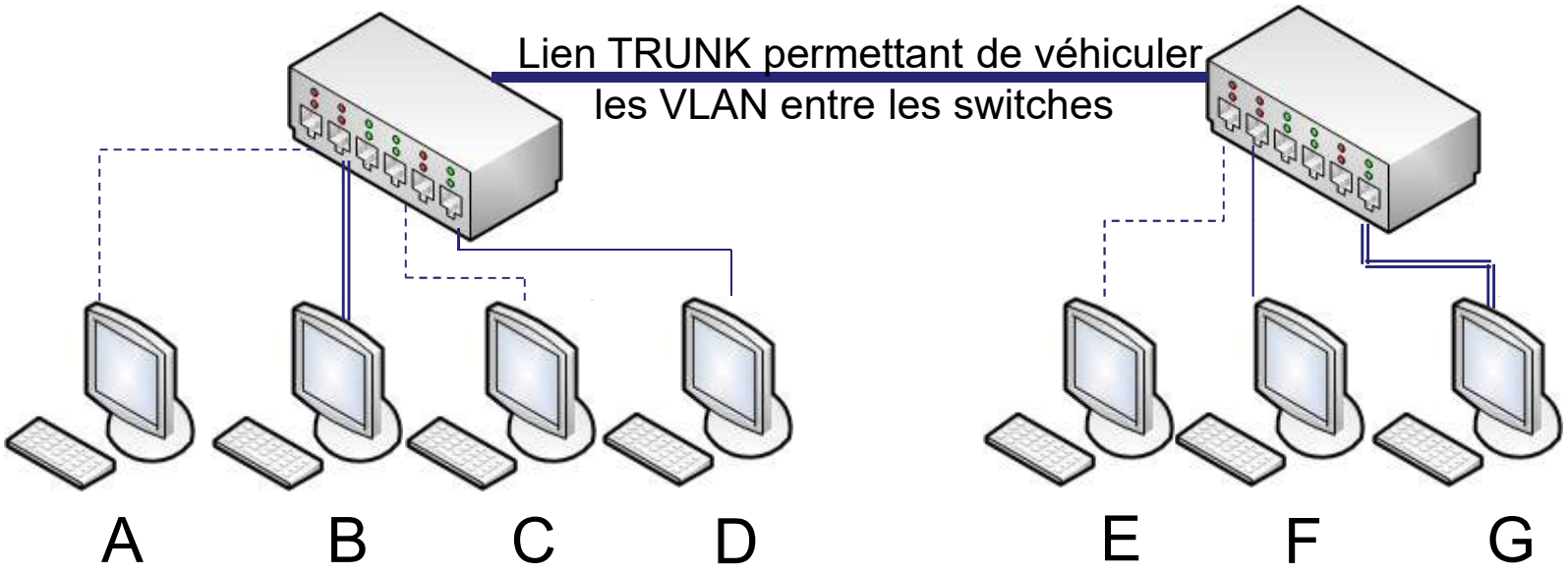
Autre technique de segmentation : **VLAN** (Virtual LAN).

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

- La segmentation peut se faire grâce aux ports Ethernet de chaque switch (on affecte un VLAN particulier à chaque port des switches, les deux switches étant reliés entre eux par un lien TRUNK afin de véhiculer les étiquettes des VLAN) ;
- La segmentation peut aussi se faire grâce aux adresses MAC des systèmes.
  - Attention : les adresses MAC des cartes réseaux pouvant facilement être modifiées par les utilisateurs, le filtrage sur les adresses MAC est à considérer – logiquement – avec précaution car le niveau de sécurité effectif est limité.

Voir exemple sur la diapositive suivante.

4.1.1 Commutateur (switch) : Contre-mesures



Implémentation de 3 VLAN sur des réseaux distants.

VLAN 1. Les machines B et G sont segmentées des autres systèmes et peuvent communiquer entre-elles deux seulement.

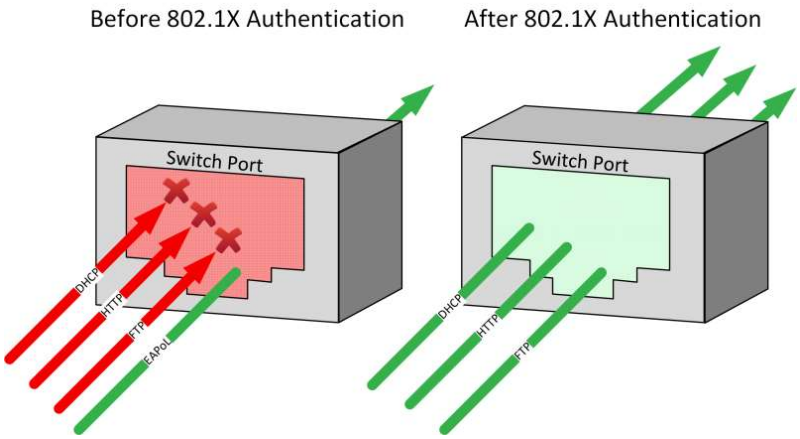
VLAN 2. Les machines A, C et E sont segmentées des autres systèmes et peuvent communiquer entre-elles seulement.

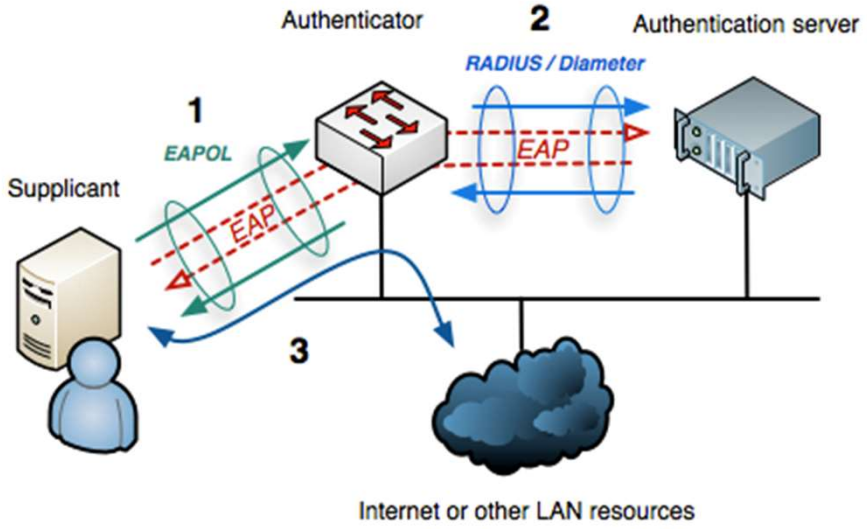
VLAN 3. Les machines D et F sont segmentées des autres systèmes et peuvent communiquer entre-elles deux seulement.

4.1.1 Commutateur (switch) : Contre-mesures

- Utiliser la sécurité des commutateurs
  - Limité aux commutateurs manageables
  - Le standard 802.1X
    - Permet une authentification du matériel connecté
    - Permet une authentification de l'utilisateur
    - Permet une attribution dynamique de VLAN
    - Permet de bloquer l'accès au réseau
- Suivre en temps réel les ports bloqués

4.1.1 Commutateur (switch) : Contre-mesures





4.1.3 Passerelle : son rôle

- Permet de changer de réseau
  - De privé à privé
  - De privé à public
- Utilisation de la translation d'adresse
  - PAT: Port Address **Translation**
  - NAT: Network Address **Translation**
- Filtre entre 2 réseaux (restriction d'utilisation)
  - Niveau MAC
  - Niveau IP
  - Sur les couches supérieures (contenus)

4.1.3 Passerelle : contournement

- Si restriction d'utilisation
  - Usurpation IP
  - Usurpation MAC
- Passage de la passerelle
  - Envoi d'un paquet en utilisant l'autre réseau
    - (si pb de config, la passerelle transmet le paquet)
- Provoquer un déni de service par envoi massif de paquets reset (usurpation d'IP)

4.1.3 Passerelle : contre-mesures

- Configurer correctement
  - Eviter l'envoi de paquets simples
  - Configurer les règles
    - Pour chaque poste
    - Pour chaque service
- Coupler avec un IDS
  - Eviter l'envoi massif de paquet
  - Attention
    - Ne pas interdire la connexion venant du pirate
    - Si l'IP est usurpée, on va interdire le vrai serveur
- La passerelle devient une sonde
  - Informe de l'état du réseau (vers, virus)

Université Grenoble Alpes

4.2 Les routeurs

4.2.1 Les routeurs (rappel)

- Système d'interconnexion de réseaux différents
  - Servent en général de liens entre les réseaux internes (privés) et externes (publics)
- Permet de se connecter à internet
- Obligatoirement nommé et adressé (N° IP)
- Assure des fonctions :
  - de sécurité par
    - filtrage d'adresses
    - filtrage de protocoles
  - d'interconnexion du LAN, WAN et du MAN
  - de routage au niveau des réseaux d'où l'obligation de connaître la topologie internet (niveau OSI 3)
  - d'amélioration et gestion du trafic
- Administrable à distance

4.2.1 Routeur : contournement

- Mêmes problèmes que pour la passerelle
  - Usurpation MAC
  - Usurpation IP
  - Déni de service
- Malformation des paquets
  - Mise en tampon dans le routeur
  - Jusqu'à saturation du tampon
- Gestion du routeur
  - Telnet et WEB
  - SNMP

4.2.1 Routeurs : contre-mesures

- Utiliser les access-lists
  - Mais sensible aux usurpations MAC, IP
- Désactiver les gestions à distance
  - Web, telnet
  - SNMP
  - Privilégier les accès cryptés (HTTPS, SSH)
- Mise à jour impérative de l'IOS et des logs
- Utiliser les logs (attention aux volumes des logs)

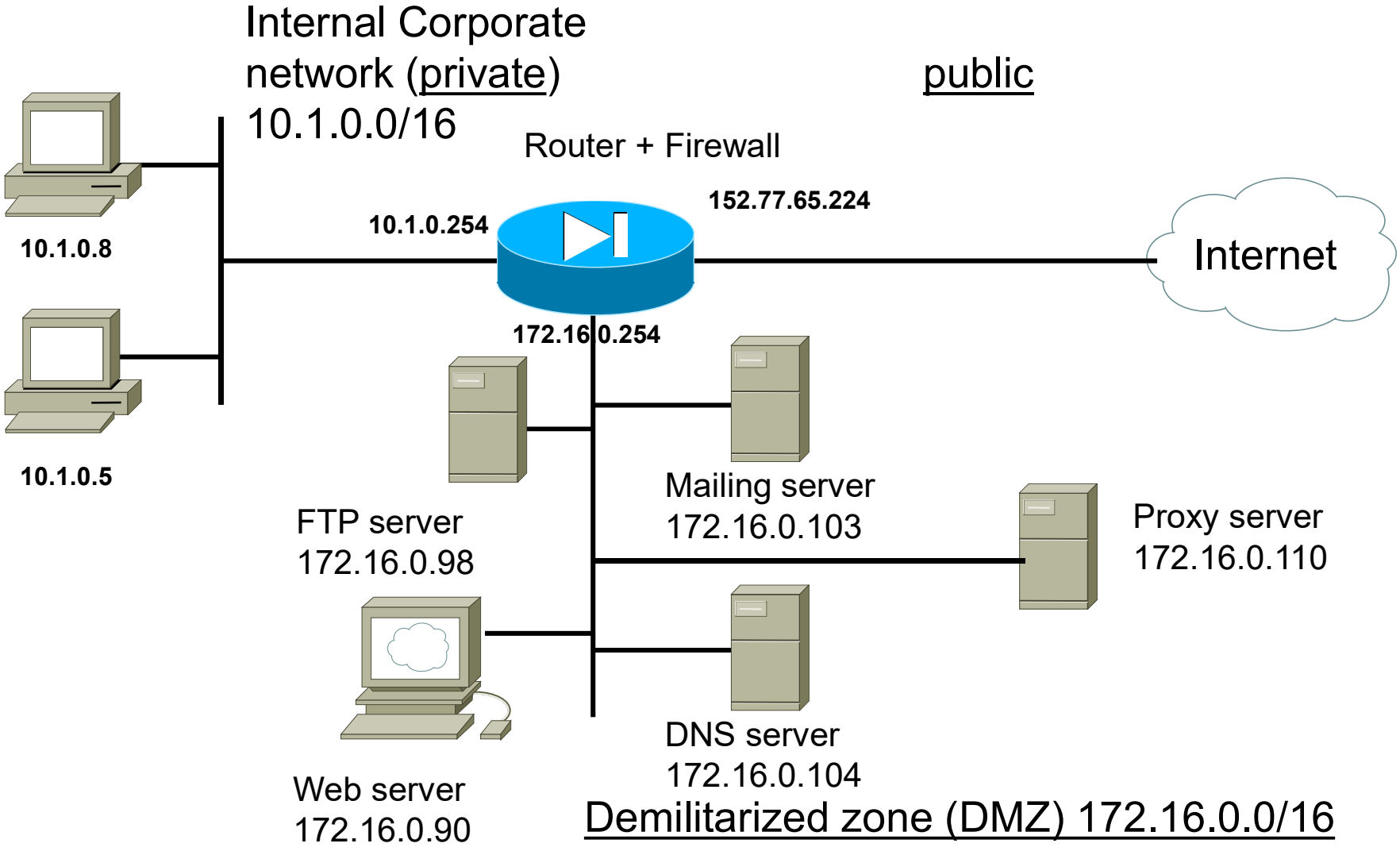
4.2.1 Configuration « sûre » du routeur

- Empêcher le routeur de divulguer sans le vouloir à des attaquants des informations sur le réseau
- Empêcher l'immobilisation du routeur (et du réseau) par des pirates ou des erreurs de configuration
- Empêcher que le routeur serve de tremplin pour attaquer le réseau interne ou d'autres réseaux

Université Grenoble Alpes

Pare-feu

A network…


Internal Corporate
network (private)
10.1.0.0/16
public
Router + Firewall
152.77.65.224
10.1.0.254
Internet
10.1.0.8
10.1.0.5
172.16.0.254
Mailing server
172.16.0.103
FTP server
172.16.0.98
Proxy server
172.16.0.110
DNS server
172.16.0.104
Web server
172.16.0.90
Demilitarized zone (DMZ) 172.16.0.0/16

4.2.2 Filtrage de paquets au moyen de listes ACL (Access Control Lists)

- Les données TCP/IP segmentées en paquets
  - Couche 3 du modèle TCP/IP
- Examen du contenu des paquets et application de certaines règles
  - Transmission du paquet
  - Suppression du paquet
- Technologie très répandue au début d'internet
  - Première ligne de défense
- Très utilisée encore dans les routeurs
- Première ligne de défense, combinée à d'autres technologies de pare-feux

4.2.2 Types d'ACL

- ACL standards
  - Prise en compte de l'adresse source
- ACL étendue
  - Adresses source et destination
  - Optionnellement type de protocole et numéro de port => recherche étendue

4.2.3 Les ACL dynamiques (1/4)

- Filtrage dynamique
  - Entrées dynamiques pour les flux de réponses des connexions TCP, UDP, ICMP
  - Non nécessité de laisser des ports ouverts de manière statique (les ports restent ouverts uniquement le temps de la session)
- Suivi des numéros de séquence TCP
  - Surveillance des numéros de séquence des paquets entrants et sortants pour suivre les flux de communication
  - Protection contre les attaques « man in the middle » et les piratages de session

4.2.2 Fonctionnement : inspection de chaque paquet

  - Adresse source
  - Adresse destination
  - Ports
- La décision d'autoriser ou non dépend de chacun des points inspectés
- Remarque : traitement de l'information rapide
- Exemple d'ACL standard routeur CISCO
  - Autoriser les paquets (permit)
  - Interdire les paquets (deny)

```
access-list 10 permit any 192.168.10.0
access-list 10 permit any 192.168.20.0
access-list 10 deny any 192.168.30.0
```

4.2.2 Types de trafic à filtrer

- Seuls les trafics des services autorisés doivent être permis (explicitement)
- EXEMPLE :

Livraison d'e-mails	Serveur de messagerie SMTP	64.24.14.61
Transferts de fichier	Serveur FTP	64.24.14.60
Trafic DNS (transferts de zones via UDP et requêtes de nom via TCP)	Serveur DNS	64.24.14.61
Trafics TCP et UDP au-delà du port 1023 pour permettre aux connexions en sortie de fonctionner		
Certains types de messages ICMP		

Seules connexions sortantes autorisées :
-SSH (port 22)
-DNS (port 53)
-FTP (ports 20 et 21)
-HTTP (port 80)

4.2.2 Ex : ACL 121 appliquée en entrée du routeur, sens internet => LAN

```
ip address 192.168.254.1/30
ip address group 121 in
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any unreachable
access-list 121 permit icmp any any administratively-
   prohibited
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14.61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```

4.2.2 Ex : ACL 122 appliquée en entrée du routeur, sens LAN => internet

```
ip address 64.24.14.1/24
ip address group 122 in
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq 22
access-list 122 permit udp 64.24.14.1 0.0.0.255 any eq domain
access-list 122 permit icmp 64.24.14.1 0.0.0.255 any echo
access-list 122 permit icmp 64.24.14.1 0.0.0.255 any echo-reply
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq ftp
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq http
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any gt 1023 established
access-list 122 permit udp 64.24.14.1 0.0.0.255 any gt 1023
```

4.2.3 Les ACL dynamiques (2/4)

- Suivi de l'état des sessions
  - Suivi des sessions TCP à demi-ouvertes, ouvertes et fermées pour éviter les attaques SYN Flood
  - Numéros de session et débits de transmission doivent être compris dans des seuils définis par l'administrateur
- Suivi des connexions UDP et ICMP
  - Protocoles difficiles à surveiller
  - Suivi par approximation (filtrage dynamique, temporisateurs)
- Journalisation des sessions
  - Dates et heures
  - Hôtes source et destination
  - Ports
  - Nombre total d'octets transmis

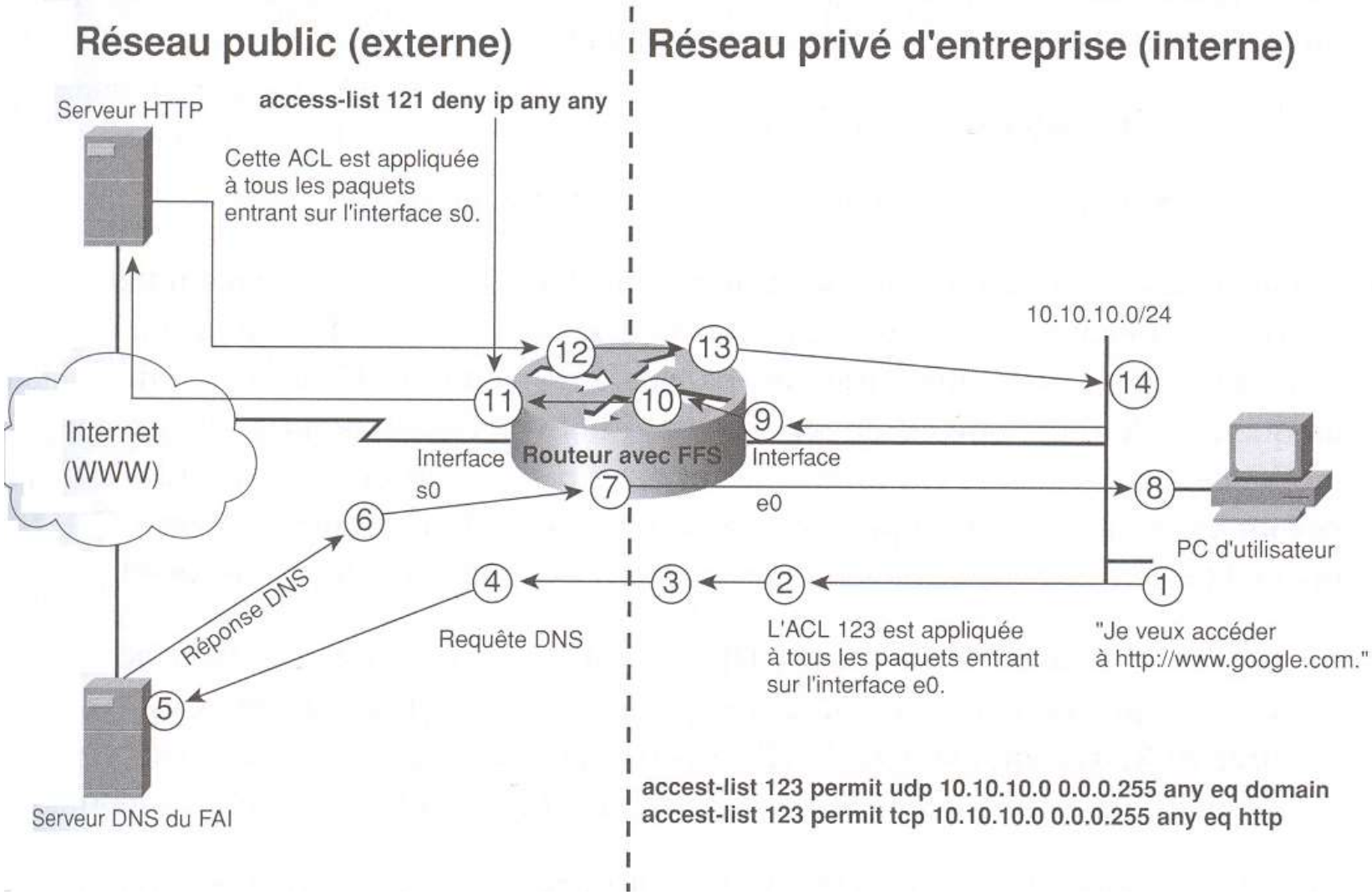
4.2.3 Les ACL dynamiques (3/4)

- Suivi d'applications spécifiques (exemple de protocoles)
  - CU-SeeMe (port 7648): visioconférence PTP
  - FTP (port 21)
  - H.323 (port 1720): communication multimedia (VoIP, vidéo, audio)
  - ICMP: dépannage de problèmes (administrateur) + utilisé par les pirates => ne laisser passer que les messages ICMP générés à l'intérieur du réseau
  - MCGP (Media Control Gateway Protocol, port 2427) : VoIP
  - MSRPC (Microsoft Remote Procedure Call Protocol, port 135) : communication de processus inter-systèmes

4.2.3 Les ACL dynamiques (4/4)

- NetShow (port 1755): streaming Microsoft
- R-EXEC (port 512) : commandes distantes (Unix)
- R-SHELL (port 514): shell distant (Unix)
- RTSP (Real-Time Streaming Protocol, port 544): streaming et VoIP
- SMTP (Simple Mail Transfer Protocol, port 25): courrier
- SQLNet (port 1521): Communications clients-BdD
- Stream Works (port 1558): Streaming de Real Networks
- Real Audio (port 7070): Streaming de Real Networks
- TFTP (Trivial File Transfer Protocol, port 69): transfert de fichiers clients-serveurs
- VDOlive (port 7000) : streaming

4.2.4 Exemple (1/5)



4.2.4 Exemple (2/5)

- 1. L'utilisateur saisit www.google.fr
  - Le PC émet une requête de résolution de nom DNS pour obtenir l'adresse IP de l'URL
- 2. Le paquet de requête DNS (un datagramme UDP) arrive sur l'interface Ethernet interne du routeur
  - Il est comparé à la liste 123 (filtrage)
  - Il est transmis si autorisé ou supprimé
- 3. Le paquet autorisé est soumis au CBAC (Context-Based Access Control => contrôle d'accès contextuel)
  - Inspection
  - Consignation des informations dans la table d'états
    - Adresse IP source et numéro de port
    - Adresse IP destination, numéro de port et protocole
- 4. Création d'une instruction `permit` temporaire sur la liste 121
  - Autorisation du trafic en réponse par l'hôte de destination (serveur DNS)
  - Instruction temporaire placée devant les instructions statiques de l'ACL

4.2.4 Exemple (3/5)

- 5. Le paquet de requête DNS (port UDP 53) est transmis au serveur DNS
  - Réponse du serveur DNS
  - Entrée ACL dynamique maintenue 5 secondes
- 6. Arrivée du paquet de réponse DNS
  - Comparaison à l'ACL 121
  - Autorisé puisqu'appartenant à une session établie
- 7. Inspection du paquet de réponse DNS
  - Conservation des informations d'état jusqu'à expiration du temporisateur par défaut de maintien des sessions UDP
- 8. Arrivée de la réponse DNS sur le PC utilisateur et initiation par le PC d'une session HTTP avec google
  - HTTP s'appuie sur TCP, donc le premier paquet comporte le bit SYN (synchronisation) activé pour entamer le processus de négociation en trois temps de TCP

4.2.4 Exemple (4/5)

- 9. Le paquet HTTP est autorisé
  - liste 123 autorisant le port HTTP 80
- 10. Inspection du paquet sortant et consignation des info dans la table d'états
  - Adresse IP source et port
  - Adresse IP destination, port et protocole
- 11. Création d'une instruction `permit` temporaire sur la liste 121
  - Autorisation du trafic en réponse par l'hôte de destination (serveur HTTP)
  - Instruction temporaire placée devant les instructions statiques de l'ACL
  - Maintien de l'entrée pendant 30 secondes (le temps de recevoir un paquet SYN-ACK, synchronisation-acquittement, de la part du serveur web)
- 12. Réception du paquet provenant du serveur web
  - Autorisé par la liste 121 (car appartenant à une session établie)

4.2.4 Exemple (5/5)

- 13. Inspection du paquet provenant du serveur web
  - Elimination du paquet si violations de protocoles spécifiques
- Dans le cas de HTTP et autres protocoles nécessitant plusieurs sessions
  - Mise à jour continuelle de la table d'états
  - Mise à jour continuelle de l'ACL
- Délais de suppression des entrées ACL temporaires
  - ICMP et UDP, à expiration d'un temporisateur de durée configurable
  - TCP, cinq secondes après l'échange de paquets FIN

Université Grenoble Alpes

4.3 Les pare-feux (firewalls)

4.3.1 Pare-feu : son rôle

- Filtrer les flux
  - Entrant et sortant
- Pare-feu personnel
  - Sur les postes
  - Contrôle couches 1 à 7
- Pare-feu professionnel
  - Equipement réseau
  - Couches 1 à 7

4.3.1 Inspections de paquets avec suivi de l'état de connexion (SPI: Stateful Packet Inspection)

- Couche 4 (couche transport) du modèle TCP/IP
- Implémenté sur un pare-feu derrière le routeur
- Seconde ligne de défense
- Surveille la « connexion » entre deux ordinateurs

4.3.1 Pare-feu : contournement

- Pare-feu personnel
  - Pgm d'amorce en téléchargement, le pirate prend le contrôle en se faisant passer pour un pgm connu (iexplorer.exe)
  - Pas de réaction du pare-feu : pgm connu et port autorisé
- Pare-feu professionnel
  - Usurpation MAC, IP
  - Auto-blocage du pare-feu (envoi d'un flot massif avec usurpation d'IP)
- Saturation des logs

4.3.1 Pare-feu : contre-mesures

- Etre maintenu à jour
- Couplé à un IDS
  - Pour savoir ce qui se passe
- Consultation des logs
  - Et nettoyer les logs

4.3.2 Fonctionnement de l'inspection de paquets avec suivi de l'état de connexion (SPI) (1/2)

- Inspection d'un premier paquet « autorisé » (par le routeur)
- PARE-FEU
  - Une entrée est créée dans une table (nouvelle connexion)
- Paquets reçus => vérification si appartient à une connexion existante

4.3.2 Fonctionnement de l'inspection de paquets avec suivi de l'état de connexion (SPI) (2/2)

- Examen de l'en-tête du paquet
  - Adresse source et destination
  - Type de protocole (TCP, UDP, ICMP…)
  - Ports source et destination
  - Bits indicateurs (SYN, ACK, FIN, RST…)
  - …
- Comparaison aux règles de contrôle du trafic
  - Ex courant : Ne laisser passer que le trafic HTTP
- Généralement, le pare-feu autorise les connexions vers l'extérieur

  => entrée dans la table d'état

  => les paquets entrants (retours de requêtes) appartenant à ces connexions ne sont pas filtrés
- Les règles peuvent être complexes (elles ne sont utilisées qu'une fois par connexion => donc la complexité n'est pas trop synonyme de dégradation des performances)

4.3.3 Règles de filtrage / Pare-feux

- Règles balayées dans l'ordre croissant
  - Nécessité de mettre les règles les plus utilisées au début (performance)
  - Nécessité de mettre les règles les plus restrictives avant les autres (ex.: si une machine a certains droits et le réseau auquel elle appartient ne les a pas)
- Interdire tout trafic vers le pare-feu
- Règle implicite interdisant tout trafic ne correspondant pas à une règle explicite

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	* Any	ip330	* Any	* Any	drop	Log	* Policy Targets	* Any	
2	Lan_privé	* Any	* Any	TCP http	accept	- None	* Policy Targets	* Any	
3	Lan_privé	serveur_dmz	* Any	UDP domain-udp TCP ftp	accept	- None	* Policy Targets	* Any	
4	* Any	Lan_privé	* Any	* Any	reject	Log	* Policy Targets	* Any	
5	serveur_dmz	* Any	* Any	dns	accept	- None	* Policy Targets	* Any	
6	* Any	serveur_dmz	* Any	dns TCP http	accept	- None	* Policy Targets	* Any	
7	* Any	serveur_dmz	* Any	FTP ftp->ftp_get	accept	- None	* Policy Targets	* Any	
8	* Any	* Any	* Any	* Any	drop	Log	* Policy Targets	* Any	

4.3.3 Inconvénients (insuffisances)

- Pas d'inspection au niveau application sur les pare-feu de base
- Pas d'états de connexions de certains protocoles
  - Ex : ICMP, UDP

4.3.4 Fonction NAT, traduction d'adresse (network address translation)

- Adresses de l'internet (IPv4)
  - Théorie, 2^{32} adresses (~4,3 Mds d'adresse)
  - Pratique
    - Adresses publiques : ~3,2 Mds
    - Adresses réservées : test…
    - Adresses privées : réservées pour les réseaux internes (non accessibles de l'extérieur)
      - 10.0.0.0 à 10.255.255.255 (préfixe 10/8)
      - 172.16.0.0 à 172.31.255.255 (préfixe 172.16/12)
      - 192.168.0.0 à 192.168.255.255 (préfixe 192.168/16)
- NAT assure la conversion entre les adresses publiques et privées, entre le réseau interne et des ouvertures sur l'extérieur
  - pare-feu,
  - quelquefois un routeur ou un ordinateur

4.3.4 NAT

- NAT statique
  - Même adresse IP publique à une adresse IP privée donnée
  - Ex : serveur WEB
- NAT dynamique
  - Associe à une adresse IP privée une adresse publique aléatoire tirée d'un groupe
- PAT (Port Address translation)
  - Associe une seule adresse publique à plusieurs adresses privées en utilisant divers ports
  - Rappel : 65 535 ports TCP sont supportés par adresse IP

4.3.4 Sécurité avec NAT

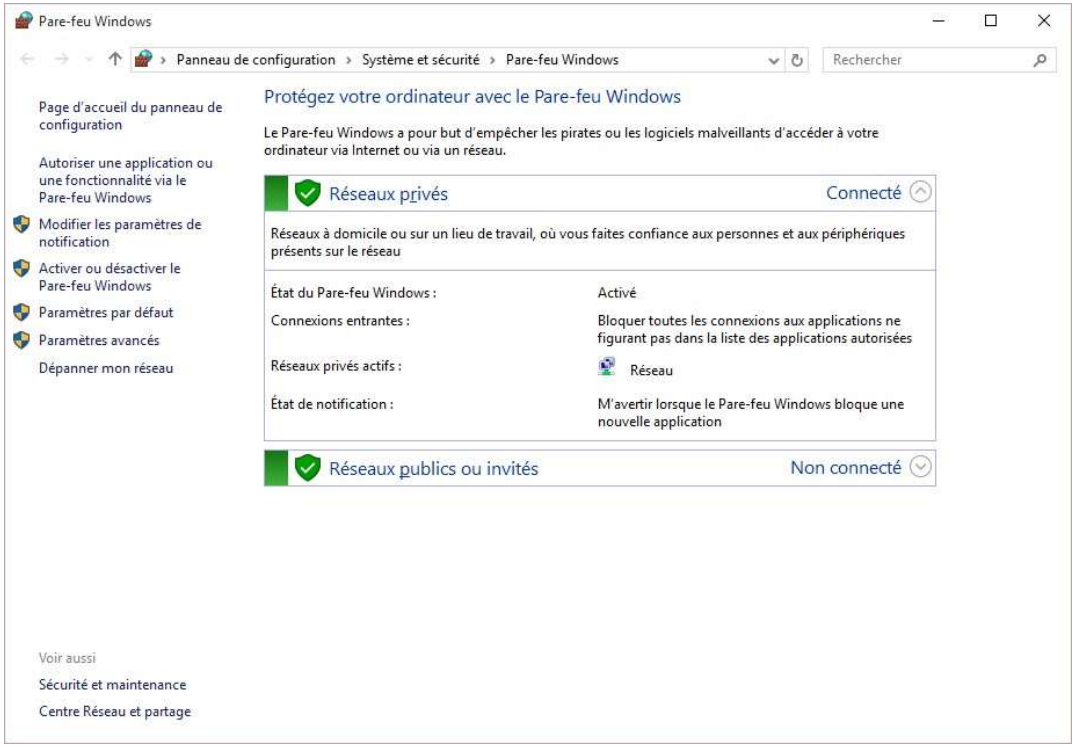
- Plus difficile pour un attaquant de :
  - Déterminer la topologie du réseau et le type de connectivité de l'entreprise cible
  - Identifier le nombre de systèmes qui s'exécutent sur le réseau
  - Identifier le type des machines et leurs systèmes d'exploitation
  - Réaliser des attaques de type déni de service (Ex : SYN Flood, scan de ports, injection de paquets)

4.3.4 Inconvénients de NAT

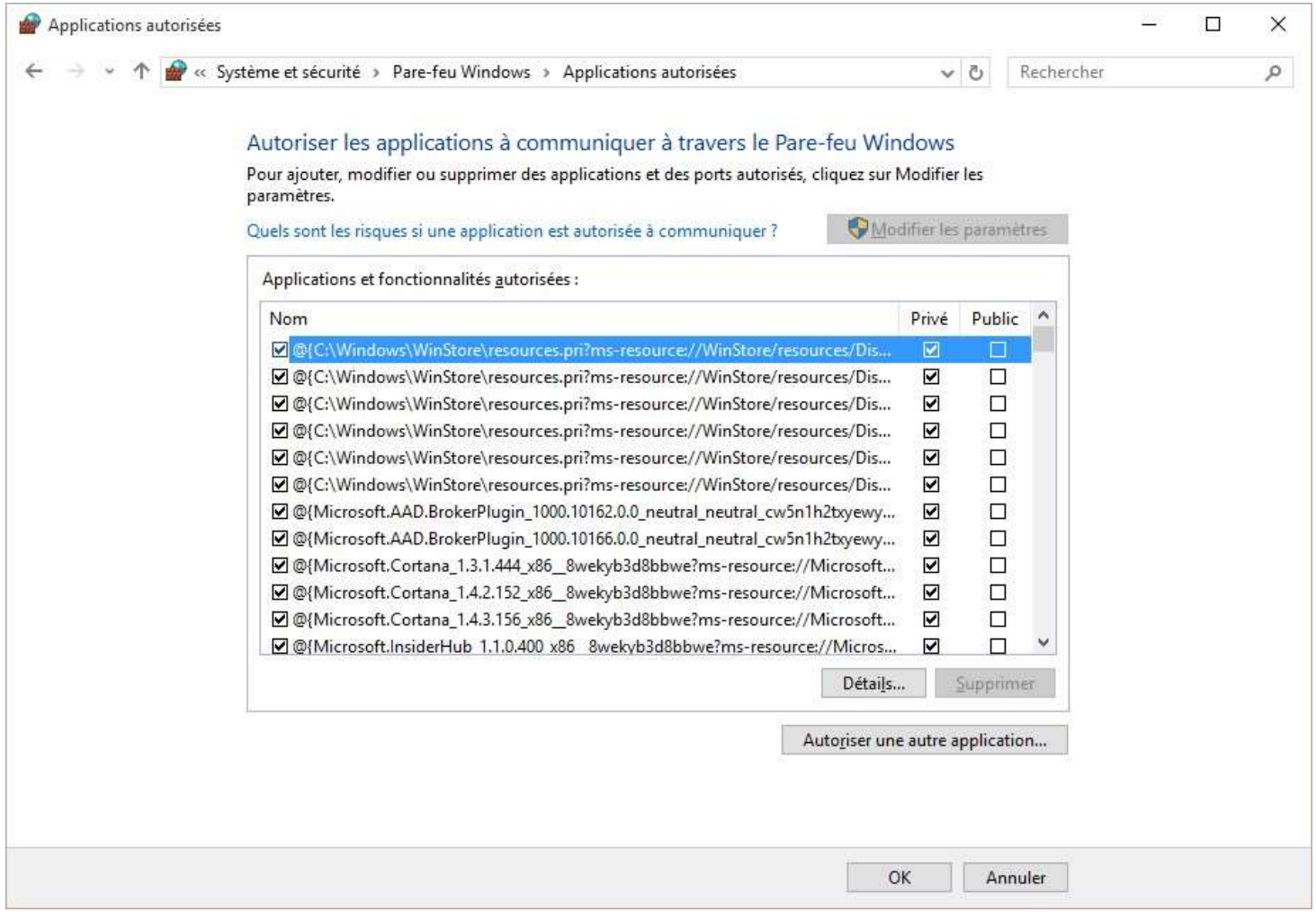
- Connexions UDP mal gérées
  - Estimation du temps où la connexion doit rester ouverte
- D'autres protocoles sont mal gérés
  - Kerberos, X Windows, rsh (remote shell), SIP (Session Initiation Protocol)
- Systèmes de chiffrement et d'authentification
  - Ces systèmes sont basés sur l'intégrité des paquets
  - Or NAT modifie ces paquets
- Journalisation compliquée
  - Mise en corrélation des journaux demande d'intégrer les traductions réalisées par NAT
- Problème de partage d'adresse avec PAT
  - Authentification auprès d'une ressource extérieure protégée (tous les utilisateurs partageant la même adresse risquent de pouvoir utiliser cette ressource)

4.3.5 Types de pare-feux

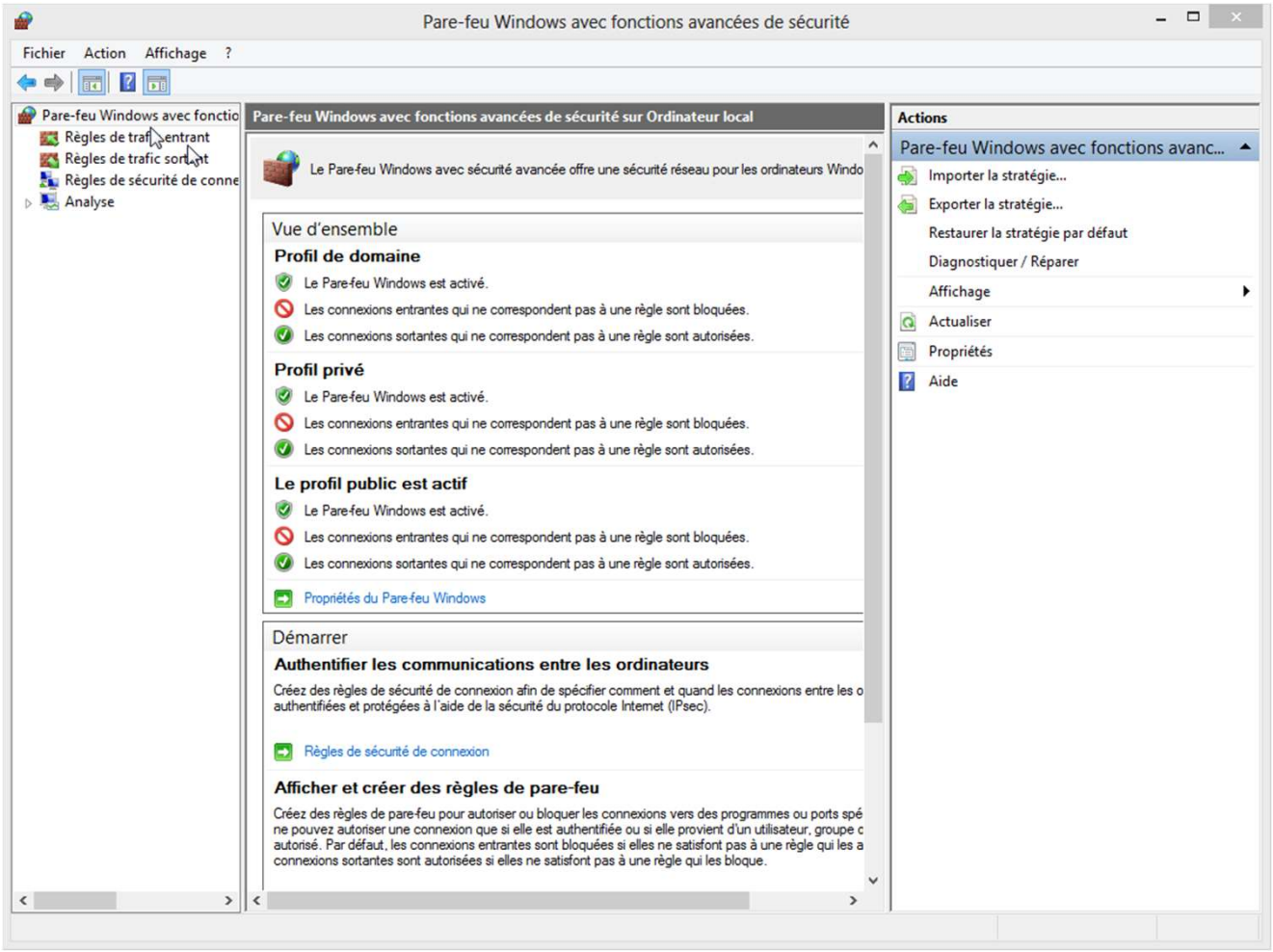
- Pare-feu personnel
  - Peut être intégré au système (Windows, Mac, Linux…)
  - Ex Windows 10 => dans le panneau de configuration



4.3.5 Pare-feu personnel (2/4)



4.3.5 Pare-feu personnel (3/4)



4.3.5 Personal firewalls (4/4)

- Sites connus d'éditeurs de pare-feux personnels
  - www.comodo.com
  - www.zonelabs.com
  - tinywall.pados.hu
  - www.online-armor.com
  - …

4.3.5 Les pare-feu nouvelle génération

- Inspection au niveau applicatif
- Définition de règles au niveau utilisateur
- Analyse de trafic chiffré

- Exemple : Pare-feu Palo Alto

4.3.5 Les pare-feu nouvelle génération

Translation d'adresse

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Afficheur_bureautique	none	Afficheur	Bureautique	ethernet1/2.2	any	any	any	none	none
4	Afficheur_DMZ	none	Afficheur	DMZ1	any	any	any	any	none	none
5	Afficheur_outside	none	Afficheur	Outside	ethernet1/13	192.168.15.50	any	any	static-ip 195.83.29.4 bi-directional: no	none
6	Bureautique-Afficheur	none	Bureautique	Afficheur	ethernet1/4.3	any	any	any	none	none

4.3.5 Les pare-feu nouvelle génération

Règles de filtrage

18	Kali	none	universal	Bureautique	17	any	any	Outside	any	any	any	Allow	none	
19	connect.univ-rouen.fr	none	universal	Bureautique	any	any	any	Outside	193.	any	any	Allow	none	
20	*DMZ_download*	*none*	*universal*	*DMZ1* *DMZ2*	*any*	*any*	*any*	*Outside*	*any*	*any*	*service-http* *service-https*	*Allow*	*none*	
21	VPN_UGA	none	universal	Bureautique Eduroam Wifi_Cermav	any	any	any	Outside	193.	dtls	application-d...	Allow	none	
22	ESRF	none	universal	Bureautique	17	any	any	Outside	193.	any	SSH_ESRF	Allow	none	
23	UPS	none	universal	Bureautique DMZ1 DMZ2 TOIP	17 17 17 17 17 19 19 more...	any	any	IDRAC	192.	any	service-http service-https	Allow	none	
24	Supervision	none	universal	Bureautique	17	any	any	Administra... DMZ1 DMZ2 IDRAC Imprimantes TOIP	any	ping snmp	application-d...	Allow	none	
25	UPS-client	none	universal	IDRAC	19	any	any	Bureautique DMZ1 DMZ2 TOIP	17 17 17 17 17 19 19 more...	apc-powerch...	application-d...	Allow	none	
26	UPS-Ping	none	universal	IDRAC	19	any	any	IDRAC	19	ping	application-d...	Allow	none	
27	Skype	none	universal	Bureautique	any	any	any	Outside	any	ms-lync ms-lync-online skype windows-azure	application-d...	Allow	none	
28	Skype-ip	none	universal	Bureautique	17	any	any	Outside	any	skype	application-d...	Allow	none	
29	VPN_Portal	none	universal	Eduroam	any	any	any	Outside	19	any	service-https	Allow	none	

4.3.5 Types de pare-feux

- Pare-feu tout en un
  - Intègrent les fonctionnalités suivantes :
    - Routeur
    - Commutateur Ethernet
    - Point d'accès sans fil
    - Pare-feu
- Pare-feu pour bureau de taille moyenne
- Pare-feu d'entreprise
    - Différences entre les gammes de pare-feu
  - Nombre de connexions supportées
  - Capacité

4.3.5 Positionnement des pare-feu

- Où mettre des pare-feu ?
  - A l'endroit de la connexion réseau interne-internet
  - Entre diverses portions de réseau interne (grandes entreprises)
  - Au niveau de chaque serveur

4.3.6 Limitations des pare-feu

- Ne peut empêcher des utilisateurs ou attaquants utilisant des modems d'accéder à l'intérieur du réseau
- Ne peut empêcher une mauvaise utilisation des mots de passe (nom respect de la stratégie de mots de passe par les utilisateurs)
- Concentration du trafic en un seul point = goulet d'étranglement = source de panne fatale

Principe de base pour la configuration d'un pare-feu

- Moindre privilège : ne pas accorder aux utilisateurs du réseau protégé par le pare-feu des droits dont ils n'ont pas la nécessité ; interdire par exemple le peer-to-peer dans le cadre d'une entreprise
- Interdiction par défaut : interdire par défaut tout transit à travers le pare-feu et ne laisser passer que celui qui est explicitement autorisé, évitant ainsi tout transit involontairement intercepté
- Défense en profondeur : utiliser les moyens de protection à tous les niveaux possibles, par exemple en analysant et filtrant tout ce qui peut l'être au niveau du pare-feu. Ce principe évite de laisser entrer dans le réseau des communications indésirables, même si un autre moyen de contrôle est utilisé plus en profondeur dans le réseau
- Goulet d'étranglement : toutes les communications entrant et sortant du réseau doivent transiter par le pare-feu. Il ne faut pas de points d'entrée ou de sortie du réseau non contrôlés, comme par exemple des modems sauvages
- Simplicité : les règles de filtrage du pare-feu doivent être les plus simples et les plus compréhensibles possibles afin d'éviter toute erreur de la part de l'administrateur ou de ses successeurs
- Participation des utilisateurs : les utilisateurs doivent être impliqués dans la mise en place du pare-feu. Ils doivent en effet exprimer leurs besoins et recevoir en échange les raisons et les objectifs de l'installation d'un tel dispositif ; les contraintes afférentes au pare-feu seront ainsi mieux acceptées.

Université Grenoble Alpes

4.4 Les pare-feux proxy

4.4.1 Proxy : son rôle

- Cache de consultation Web et FTP
- 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

4.4.1 Proxy : contournement

- Si routeur mal configuré
  - Répond aussi aux autres machines
  - Mauvaise configuration des clients (tous les droits)
- Le routeur identifie le proxy
  - Prend sa place sur le réseau

4.4.1 Proxy : contre-mesures

- Configuration correcte du routeur et des clients
- Protection contre l'usurpation du proxy
  - Mise à jour du système
  - Connexion SSL avec le routeur
  - Mise en place d'un réseau privatif (proxy avec deux cartes réseau)
- Utilisations de sondes pour savoir si un tunnel est en place
  - Trafic élevé sur un site unique
  - Attention aux tunnels à cibles multiples

4.4.2 Reverse-proxy (Rproxy) : son rôle

- Même fonction que le proxy mais dans l'autre sens
  - Mise en cache des serveurs internes en vue d'une consultation de l'internet
- But
  - Reçoit toutes les attaques
  - Filtre les demandes HTTP (ou autres services)
  - Protection des serveurs internes

4.4.2 Reverse-proxy (Rproxy) : contournement

- Trouver l'adresse du vrai serveur (si faille du routeur par exemple)
- Saturation du RProxy
  - Envoi d'un flux constant de demande
  - Empêche le Rproxy de répondre aux autres
  - Envoi de paquet reset
- Envoi de commandes HTTP truquées
  - Dépend des fonctions du proxy
- Corruption d'un poste du réseau local
  - Permet d'accéder aux serveurs

4.4.2 Reverse-proxy (Rproxy) : contre-mesures

- Vérifier les configurations
  - Routeurs
  - Postes du réseau local
- Rendre le proxy obligatoire
  - Pour les accès venant de l'extérieur
  - Pour les accès venant du réseau local
  - Exemple à Grenoble: www-cache.ujf-grenoble.fr, port 3128
- Isoler le réseau des serveurs
  - Cacher les serveurs à tout le monde
  - Rproxy avec 2 cartes réseau

4.4.3 Proxy

- Pare-feu au niveau application, ou pare-feu proxy
- Analyse des paquets au niveau des couches hautes
  - Capable de faire la différence entre un e-mail et des données Java, par exemple
- Sert de "barrière" entre l'extérieur et l'intérieur
- Pare-feu proxy standards
  - Transmission des paquets au niveau TCP/IP
  - Aucune connexion depuis l'extérieur vers l'intérieur par des PC
- Pare-feu proxy dynamiques
  - Refond un filtrage des paquets niveau 3 après avoir traité le niveau application
- Rappels sur le fonctionnement du proxy
  - Séparation des en-têtes et des données
  - Inspection des informations
  - Si le paquet est autorisé
    - Stockage des informations de connexion contenues dans l'en-tête
    - Réécriture des en-têtes
    - Transmission du paquet
- Limitations du proxy
  - Dégradation des performances
    - Très sûrs mais lents
  - Actualisation insuffisante

Université Grenoble Alpes

4.5 DMZ, zone démilitarisée (concept de sécurité périmétrique)

4.5 Zone démilitarisée (sécurité périmétrique) (DMZ, Demilitarized Zone)

- Zone du réseau interne isolée (entre la zone publique et la zone privée)
  - Serveur web
  - Serveur de messagerie
  - Serveur FTP
  - ...
- Cela permet au trafic venant d'internet d'aller dans cette zone, mais pas de pénétrer ailleurs sur le réseau interne
- Possibilité d'auditer le trafic échangé avec la DMZ
- Possibilité de placer un système de détection d'intrusion

4.5 DMZ : son rôle

- Proposer une zone
  - Recevant les demandes de l'extérieur
  - Ne communiquant pas avec le réseau local
  - Possédant son propre adressage
- Accès à la zone
  - Par le routeur depuis l'extérieur
  - Par le routeur + NAT depuis l'intérieur
- Réalise une zone tampon
  - Peut être corrompue
  - Ne révèle jamais la présence du réseau local

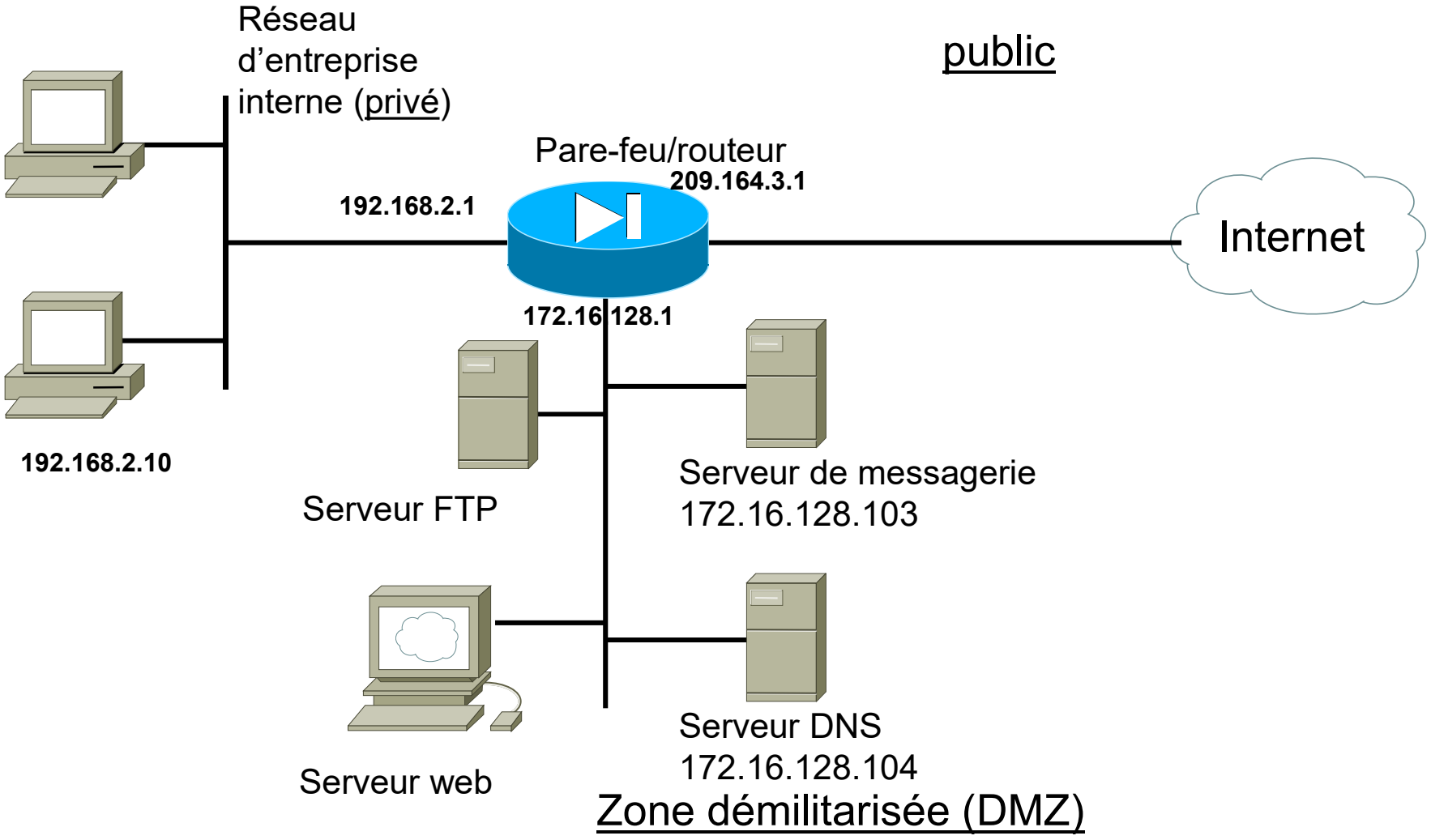
4.5 DMZ : contournement

- Corrompre un serveur de la DMZ
  - Faille de sécurité, injection de code
- Mettre en place un renifleur
  - Décodage des couches supérieures
  - Permet de connaître le réseau local
- Utiliser les techniques de passage de pare-feu
  - Corruption des postes du réseau local
- Utiliser les failles de conception des DMZ
  - => doublement des serveurs de courriers

4.5 DMZ : contre-mesures

- Interdire formellement l'accès
  - DMZ => réseau local
- Accès NAT obligatoire
  - Réseau local => extérieur
  - Réseau local => DMZ
  - Attention piratage interne
- Sonde réseau
  - Voir si DMZ corrompue
- Si 2 serveurs de messagerie
  - Le serveur interne doit demander le courrier au serveur externe

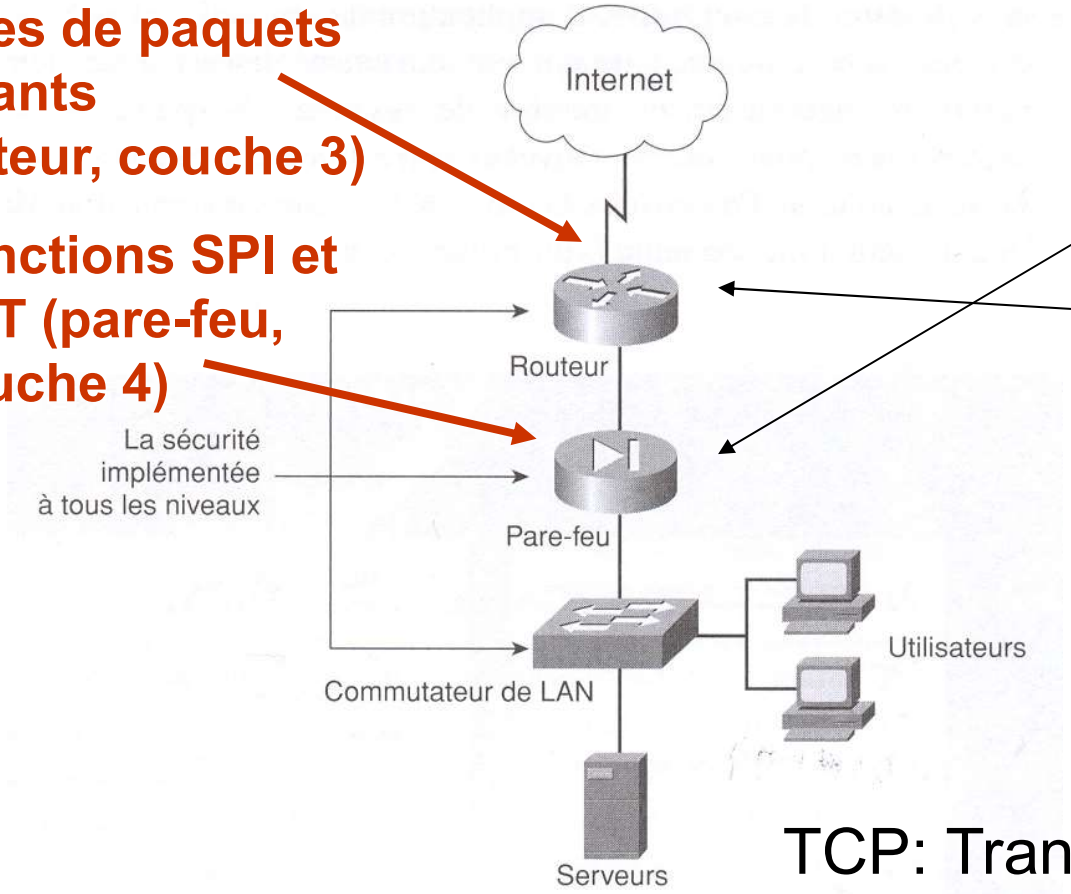
4.5 Localisation et fonction d'une DMZ



Sécurité en couches (couches TCP/IP) implémentées en plusieurs points du réseau

Filtres de paquets entrants (routeur, couche 3)

Fonctions SPI et NAT (pare-feu, couche 4)



7. Application
4. TCP & UDP (transport)
3. IP (réseau)
2. Liaison de données
1. Physique

TCP: Transport Control Protocol
UDP: User Datagram Protocol

4.6 Conclusion

- Couche paquets
  - Filtres de paquets (routeur)
    - Élimine des adresses indésirables
- Couche transport
  - Inspection des paquets SPI (pare-feu)
    - Identifie les connexions autorisées (sollicitées)
  - Translation d'adresse
    - Le réseau interne est invisible de l'extérieur
- Couche application
  - Inspection des données (pare-feu proxy)
- Chaque méthode seule est insuffisante

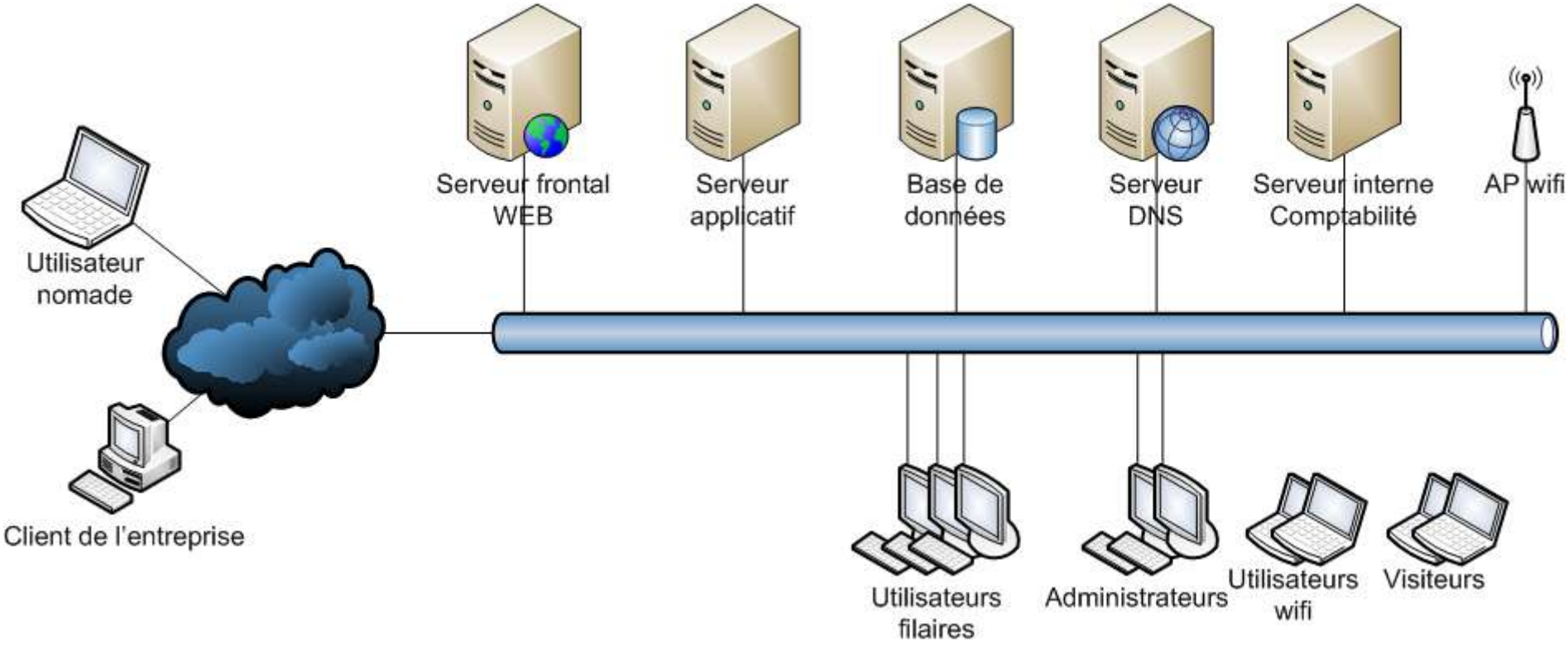
  => Leur combinaison offre un bon niveau de protection

Exemple pratique de sécurisation avec un réseau simple

Prenons l'exemple d'un réseau d'entreprise « à plat ». Caractéristiques de cette entreprise :

- Elle fournit un **site WEB de e-commerce** ;
- Certains employés se connectent sur le **réseau local filaire**, d'autres se connectent en **wifi** ;
- Certains employés sont **nomades** et doivent donc se **connecter à distance** ;
- Il existe deux catégories principales d'utilisateurs : les **utilisateurs « standard »** et les **administrateurs** du S.I. ;
- Afin de fonctionner, l'entreprise possède également des **serveurs internes** (comptabilité, wiki, etc.) ;
- L'entreprise souhaite permettre à ses **visiteurs** de se connecter en **wifi** afin de naviguer sur internet.

Exemple pratique de sécurisation avec un réseau simple



Réseau « à plat », avant sécurisation

Exemple pratique de sécurisation avec un réseau simple

Voyons comment nous allons pouvoir sécuriser ce réseau.

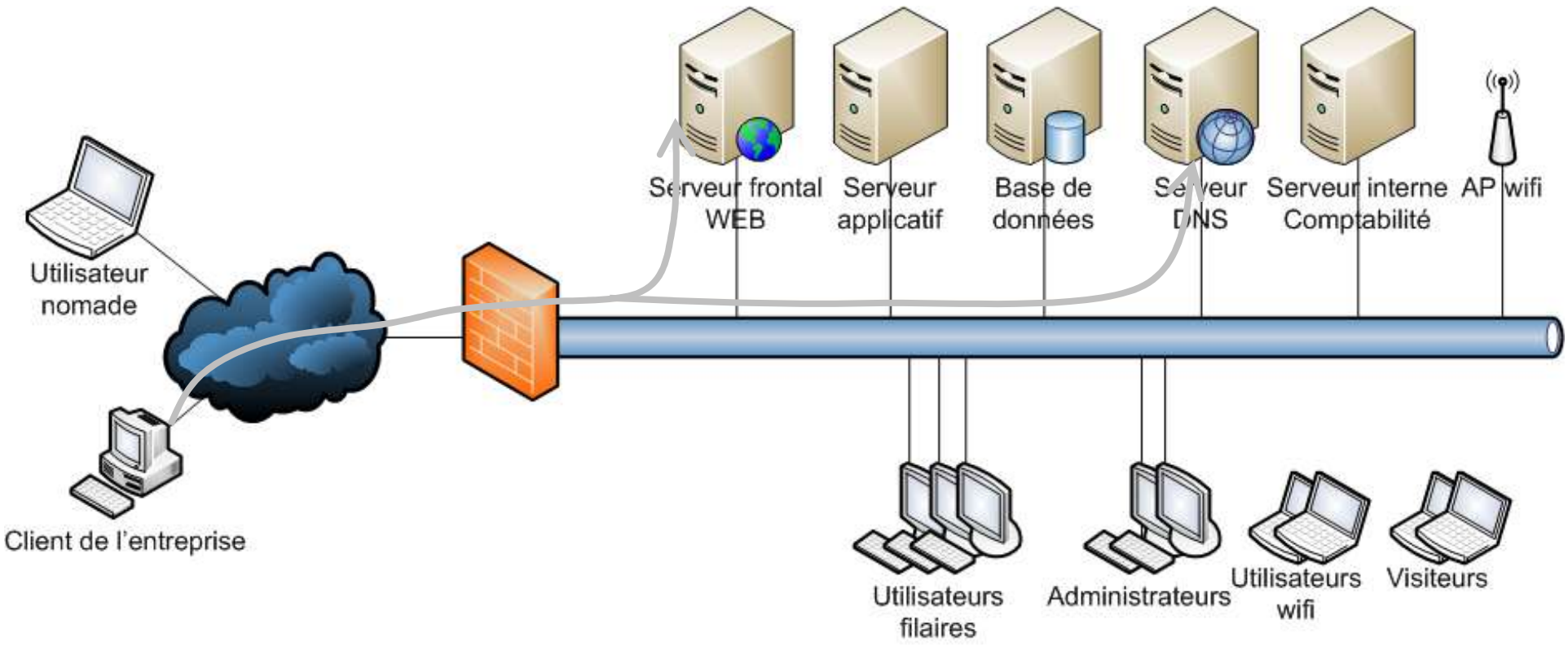
•Note : il existe plusieurs façons d'améliorer la sécurité de ce réseau, nous en présentons ici uniquement les grandes lignes. Cet exercice n'est ni exhaustif ni la seule solution possible.

Parmi les nombreuses faiblesses architecturales de ce réseau, nous pouvons identifier au moins le problème suivant :

•Le réseau est **directement connecté à Internet**, i.e. tous les systèmes et utilisateurs et systèmes peuvent communiquer avec l'extérieur (attention aux **fuites de données !**) et **tout Internet peut se connecter sur notre réseau interne.**

Corrigeons cela en implémentant un **pare-feu** en frontal qui va autoriser uniquement les flux entrants vers le serveur WEB (TCP/80 et TCP/443) et le serveur DNS (UDP/53 et TCP/53). Ainsi, Internet ne pourra plus accéder au reste du réseau interne.

Exemple pratique de sécurisation avec un réseau simple



Réseau « à plat », avec un pare-feu en frontal

Exemple pratique de sécurisation avec un réseau simple

Le pare-feu empêche – certes – la connexion directe entre internet et le réseau interne, mais :

•Au cas où le serveur WEB présente une **vulnérabilité**, un hacker présent sur Internet peut potentiellement **prendre la main sur ce serveur**, puis **rebondir ensuite sur le réseau interne**.

Nous allons donc **segmenter** notre réseau en **différentes zones de criticité**, notamment :

•Une **DMZ (zone démilitarisée)** destinée à héberger tous les serveurs qui doivent être accessibles depuis internet, et uniquement ceux-ci. Ainsi, en cas de faille dans le serveur web, un attaquant aurait plus de difficultés pour rebondir sur le réseau interne ;

•Une zone destinée aux **serveurs internes** de l'entreprise ;

•Une zone pour les **postes de travail filaires des utilisateurs ;**

•Une zone pour les **postes de travail wifi des utilisateurs ;**

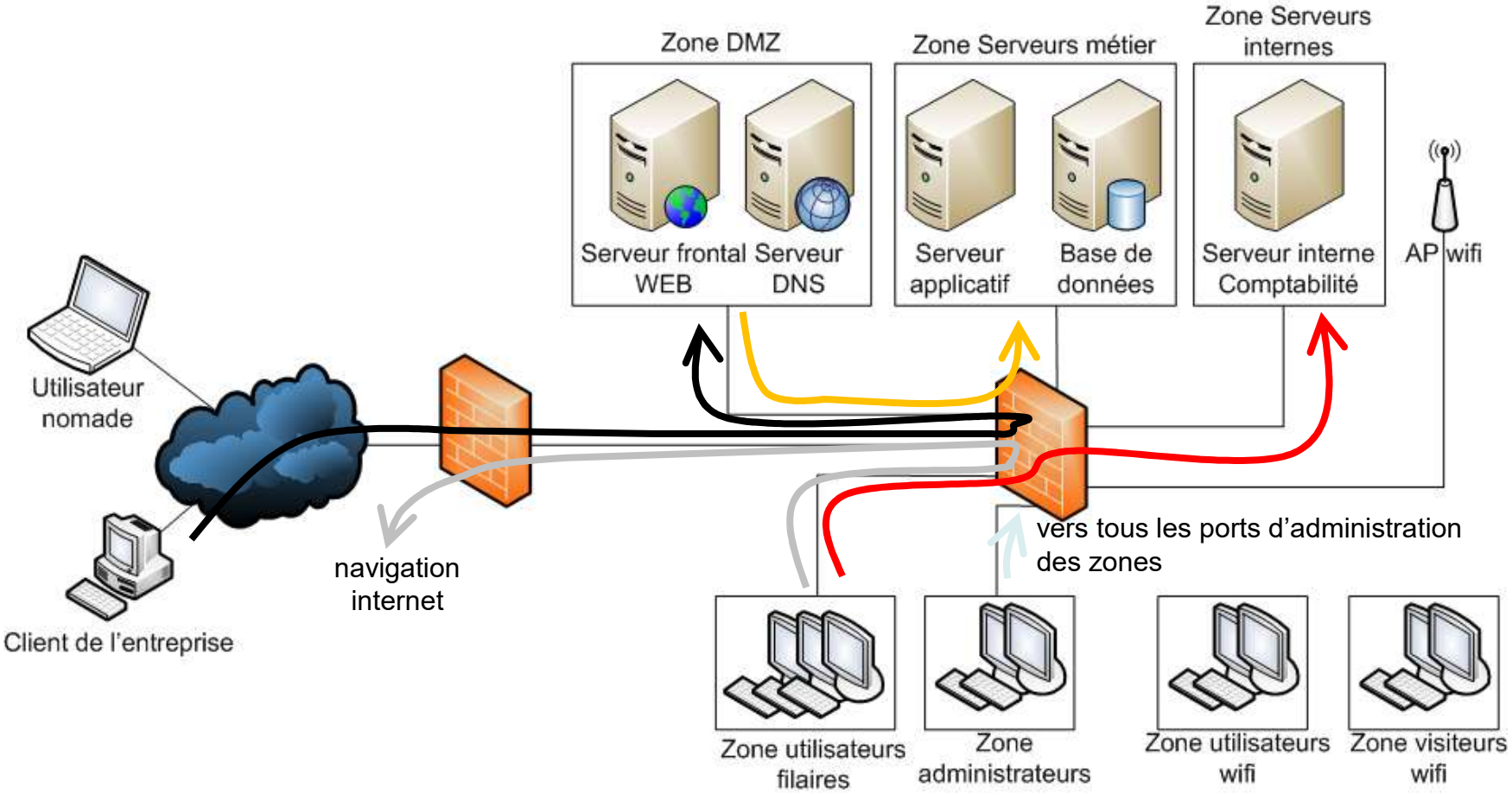
•Une zone pour les **postes wifi des visiteurs ;**

•Une zone pour les **postes de travail des administrateurs**, car ceux-ci ont besoin d'accéder à des interfaces d'administration (RDP, SSH…).

Afin que cette segmentation réseau soit efficace, nous faisons **passer tous les flux** (y compris internes) **par un deuxième pare-feu (interne)** afin que seuls les flux que nous allons configurer soient autorisés.

•Note : on observe malheureusement souvent des réseaux segmentés mais non filtrés. Cela ne sert à rien en terme de sécurité, car toutes les zones peuvent communiquer entre-elles.

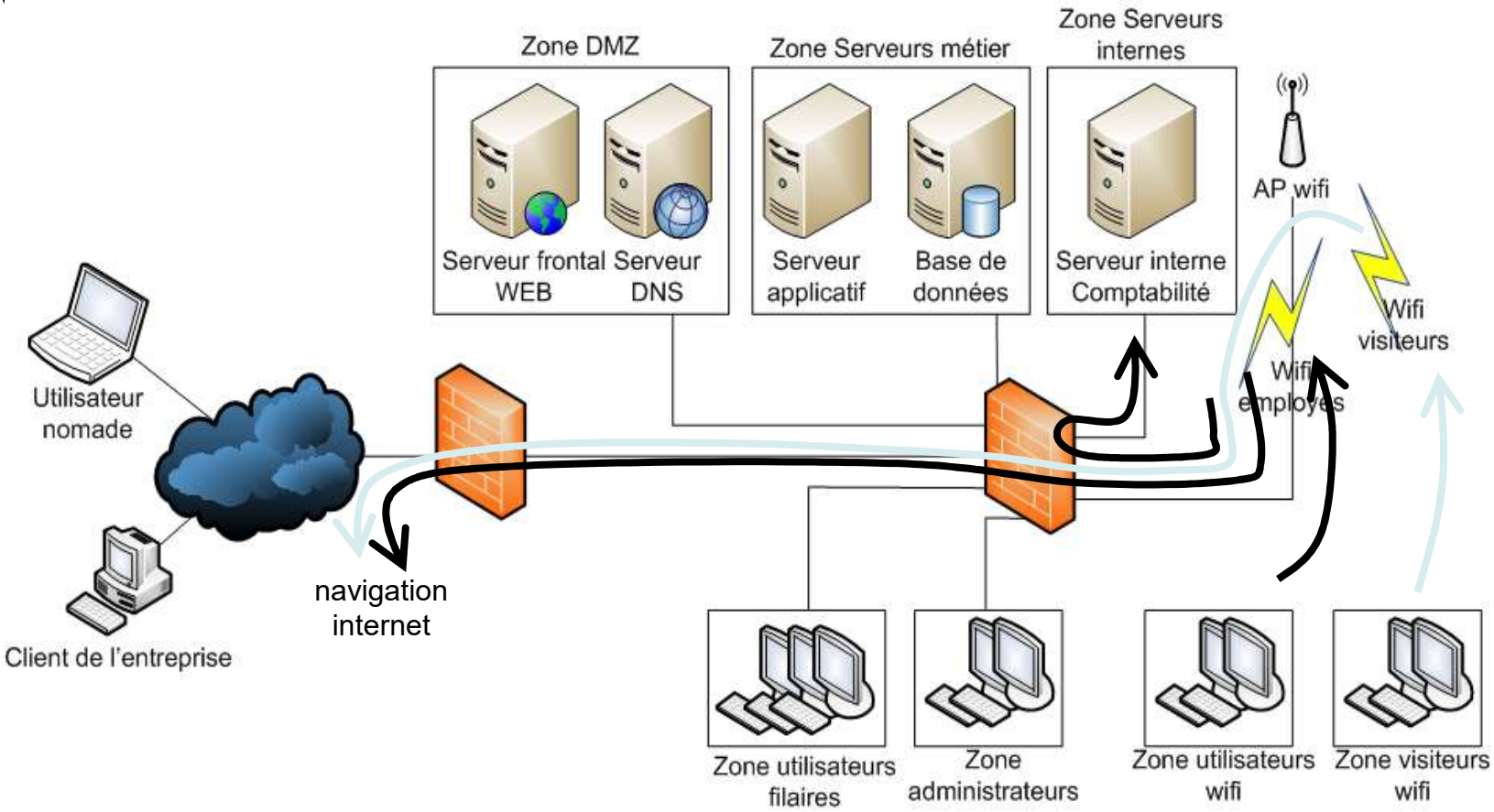
Exemple pratique de sécurisation avec un réseau simple



Réseau avec des zones segmentées, et un filtrage systématique via le pare-feu, y compris pour les flux internes.

Exemple pratique de sécurisation avec un réseau simple

Le point d'accès wifi doit être accessible aux visiteurs et aux employés internes. Puisque le besoin d'accès aux ressources est différent pour ces 2 populations, nous allons donc implémenter deux SSID (**deux réseaux wifi distincts**, portés par le même point d'accès, et dont le pare-feu filtrera les flux).



Deux réseaux wifi, dont les flux sont filtrés différemment.

Exemple pratique de sécurisation avec un réseau simple

Nous devons également permettre aux **utilisateurs nomades de se connecter** au réseau interne depuis internet. Cela se fait via une DMZ spécifique, appelée zone de mise en conformité, dont le rôle est le suivant :

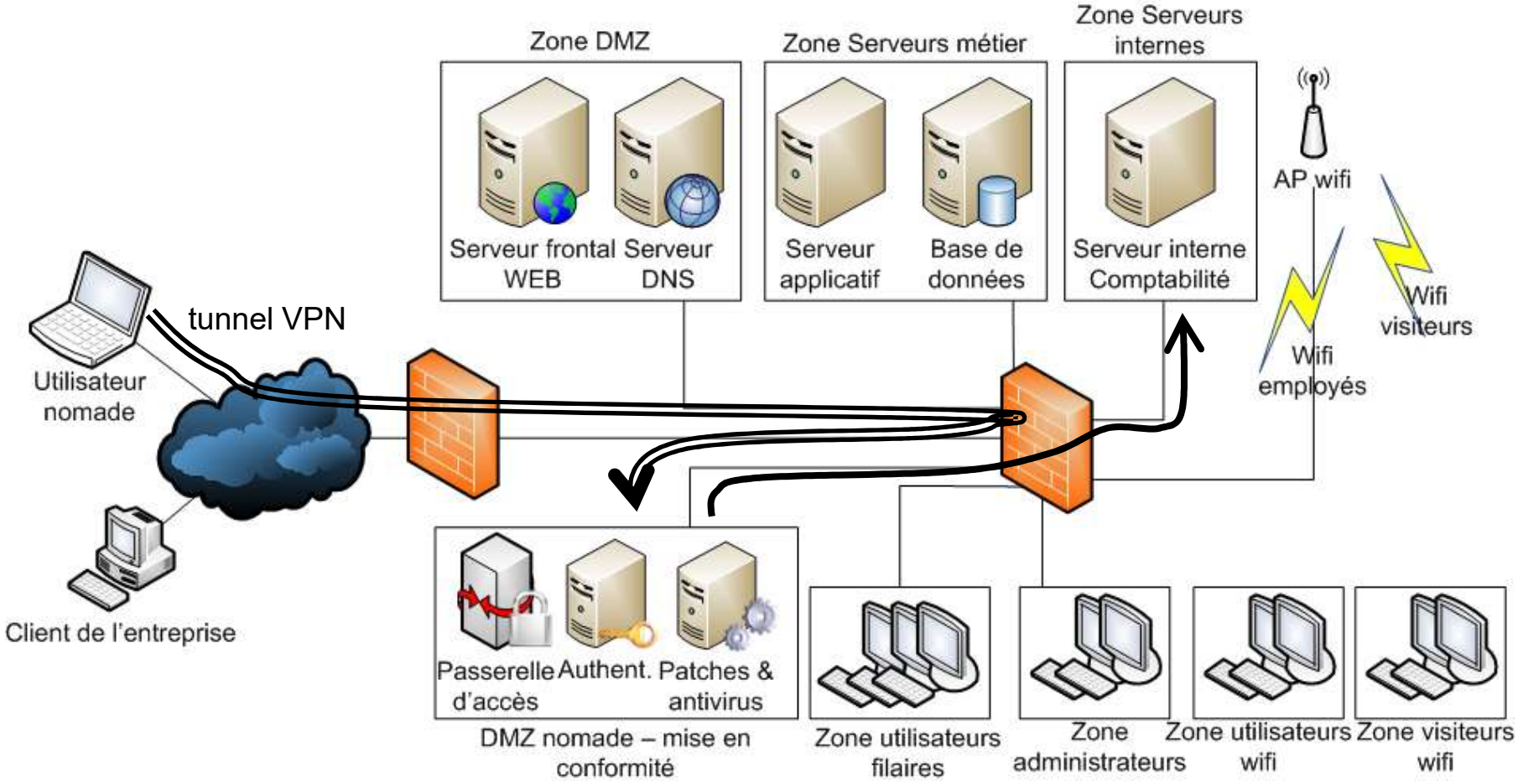
•Fournir l'interface d'accès au réseau interne depuis internet, en général via un **tunnel VPN** ;

•**Vérifier que le poste nomade et son utilisateur sont habilités** pour se connecter à distance ;

•**Vérifier le niveau de sécurité du poste** avant d'autoriser la connexion (**patches et anti-virus à jour** notamment) ;

•Si tout est OK, alors **autoriser les flux vers les zones internes** (et seulement celles qui sont nécessaires pour le métier), toujours en passant par le **pare-feu**.

Exemple pratique de sécurisation avec un réseau simple



Réseau avec DMZ de mise en conformité pour les postes nomades.

Exemple pratique de sécurisation avec un réseau simple

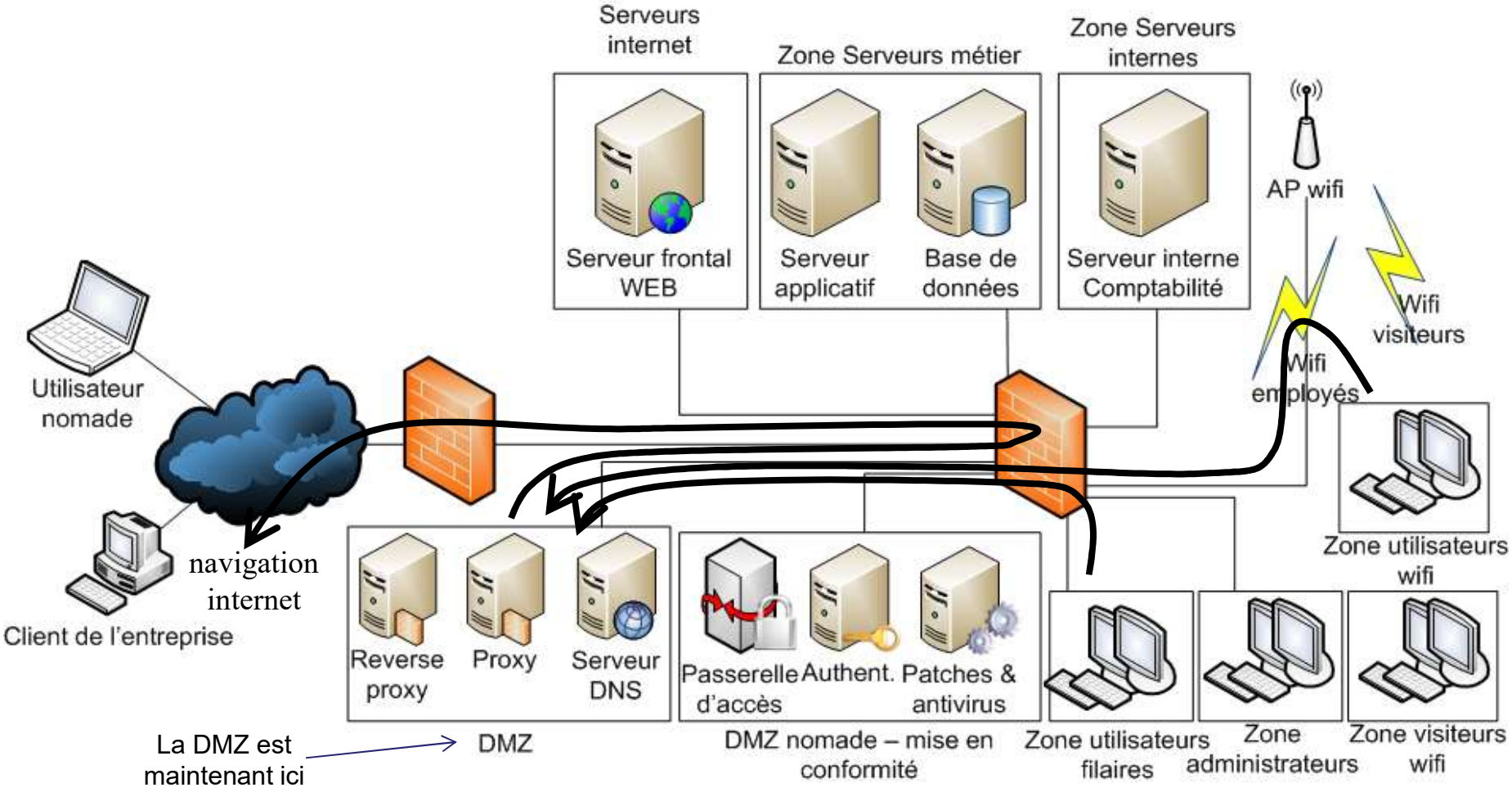
Enfin, il serait souhaitable de **mieux filtrer le trafic WEB** entrant et sortant :

- **Trafic sortant** : définir les catégories de sites WEB que les employés sont autorisés à naviguer, implémenter une liste blanche ou noire de sites autorisés/interdits ;
- **Trafic entrant** : analyser les requêtes WEB d'internet vers le serveur de e-commerce afin d'intercepter les requêtes malveillantes (injection, malware, etc.).

Nous allons donc recourir à un **proxy pour analyser les flux sortants**, et **un reverse-proxy pour analyser les flux entrants**. Ces équipements étant en coupure, ils empêchent donc les postes de travail des utilisateurs d'être connectés directement à Internet tout en leur permettant de naviguer sur les sites autorisés. Même remarque pour le serveur WEB : celui-ci n'est plus connecté directement sur Internet, c'est le reverse-proxy qui est maintenant en frontal.

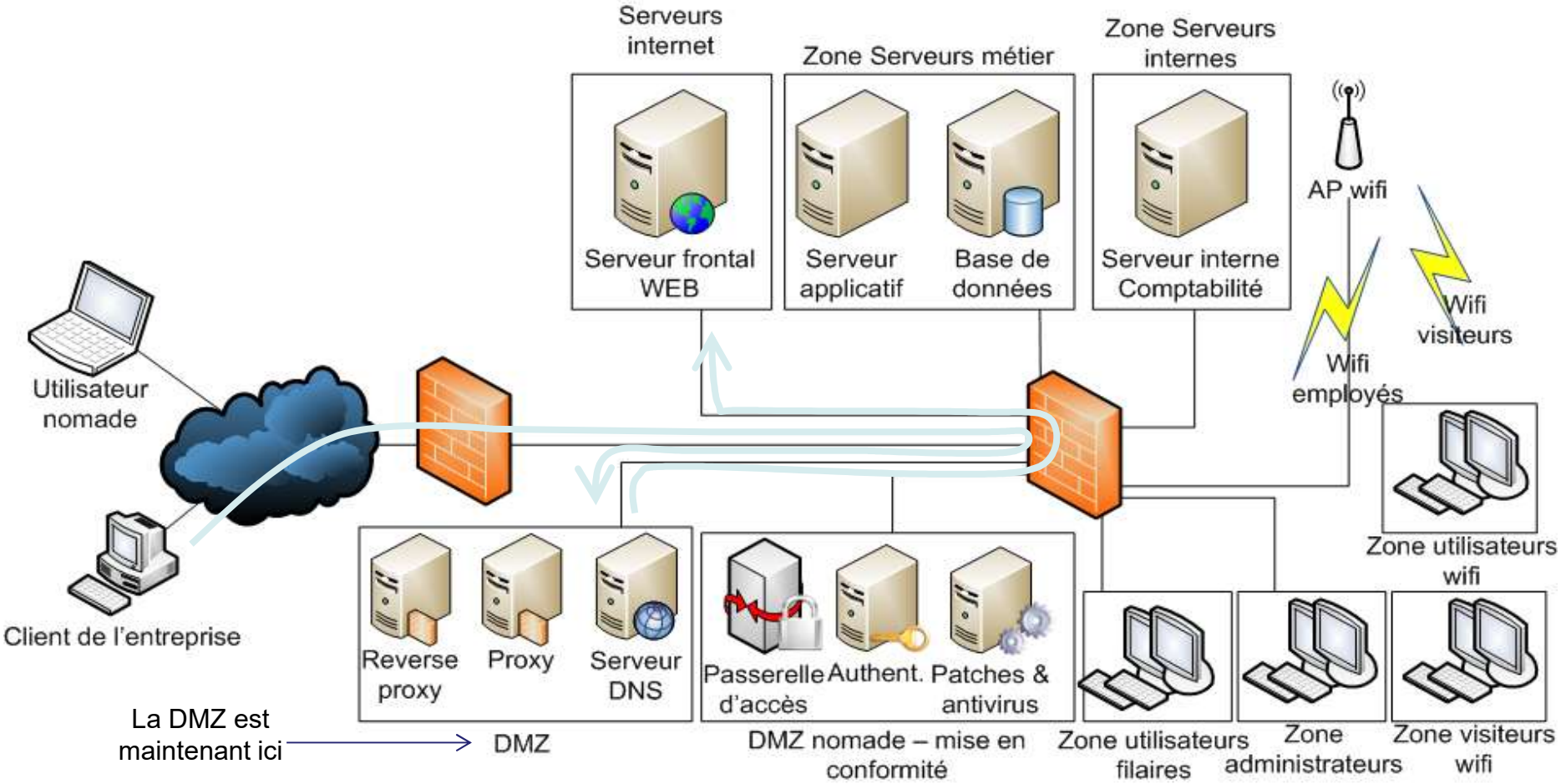
Puisque les proxies et reverse-proxies sont en frontal Internet, ce sont donc eux qu'il faut **placer dans la DMZ** maintenant.

Exemple pratique de sécurisation avec un réseau simple



Réseau avec un proxy et un reverse-proxy en coupure des flux de/vers Internet

Exemple pratique de sécurisation avec un réseau simple



Réseau avec un proxy et un reverse-proxy en coupure des flux de/vers Internet.

Références bibliographiques

- Présentation de Eric WIESS
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Cours de Jean-Luc Noizette, ESSTIN, Nancy, 2005
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux* – Dunod, 2005
- CyberEdu, ANSSI, 2014

TD

- Qu'est-ce qu'un pare-feu ? Quels sont ses rôles et fonctions ?
- Un pare-feu est un outil de sécurité nécessaire mais pas suffisant, pourquoi ?
- Définissez le concept de sécurité périmétrique (zone démilitarisée)
- Etape 4 du rapport de sécurité : quels types de technologies de sécurité allons-nous mettre en place ? Dans quel but ?
  - Comparer avec les résultats de la réflexion à la fin de l'étape 3

Translation d'adresses

- Un mécanisme de translation d'adresses (NAT) permet à un réseau d'utiliser un ensemble d'adresses IP internes différent de celui des adresses IP publiques (c'est-à-dire visibles depuis l'internet)
  - Expliquer en quelques phrases comment fonctionne le NAT
  - Quelle est la différence entre le NAT statique et le NAT dynamique?
  - Quels sont les avantages et les inconvénients du NAT ?

En-tête de courrier électronique

- Ci-dessous l'en-tête d'un pourriel. Comment expliquer les deux adresses IP différentes apparaissant dans l'en-tête ?

```
Received: from
  gw_05[192.168.227.29]
(cust-90-62.as01.chcg.eli.net
  [209.210.90.62]) by
  ns.tsp.co.kr with SMTP id
  LAA29540; Fri, 10 Oct 2008
  11:45:27 +0900
```