Le DNS

- Domain Name System
  - Généralité
  - Espace de noms
  - Implémentation

DNS

- Pourquoi ?
  - les équipements communiquent grâce à leur adresse IP (table de routage,…)
  - Il est plus simple de retenir un nom qu'une suite de chiffre !!!
    - actuellement 4 octets, et mais aussi 16…

Un des rôles du DNS

Convertir les noms en adresse IP et inversement

A une adresse IP peut correspondre à un ou plusieurs noms (alias)

Une adresse IP doit être unique dans le monde

Un nom doit aussi être unique dans le monde

DNS - Généralité

- Objectifs
  - espace de noms mondial, cohérent, indépendant des protocoles et du système de communication sous-jacents
  - gestion décentralisée des informations de la base de données globale
  - usage général indépendant des types d'applications qui l'utilisent

- Avantages - Inconvénients
  - Système distribué / décentralisé
  - utilisation de "cache" pour mémoriser des résolutions précédentes
  - d'où problème de certification (les données changent lentement)
  - priorité à l'accès à l'information, plutôt qu'à la mise à jour et la garantie de cohérence

Espace des noms (1)

- L'espace des noms est arborescent (racine ".")
- Sous la racine, on a des Domaines de niveau supérieur (TLD : Top Level Domains)
- Puis des domaines
- Puis des sous-domaines (optionnels, max 127 niveaux)
- Puis le nom hôte de la machine

Taille maximale d'un domaine : 63 caractères

le nom doit commencer par une lettre (RFC 1032)

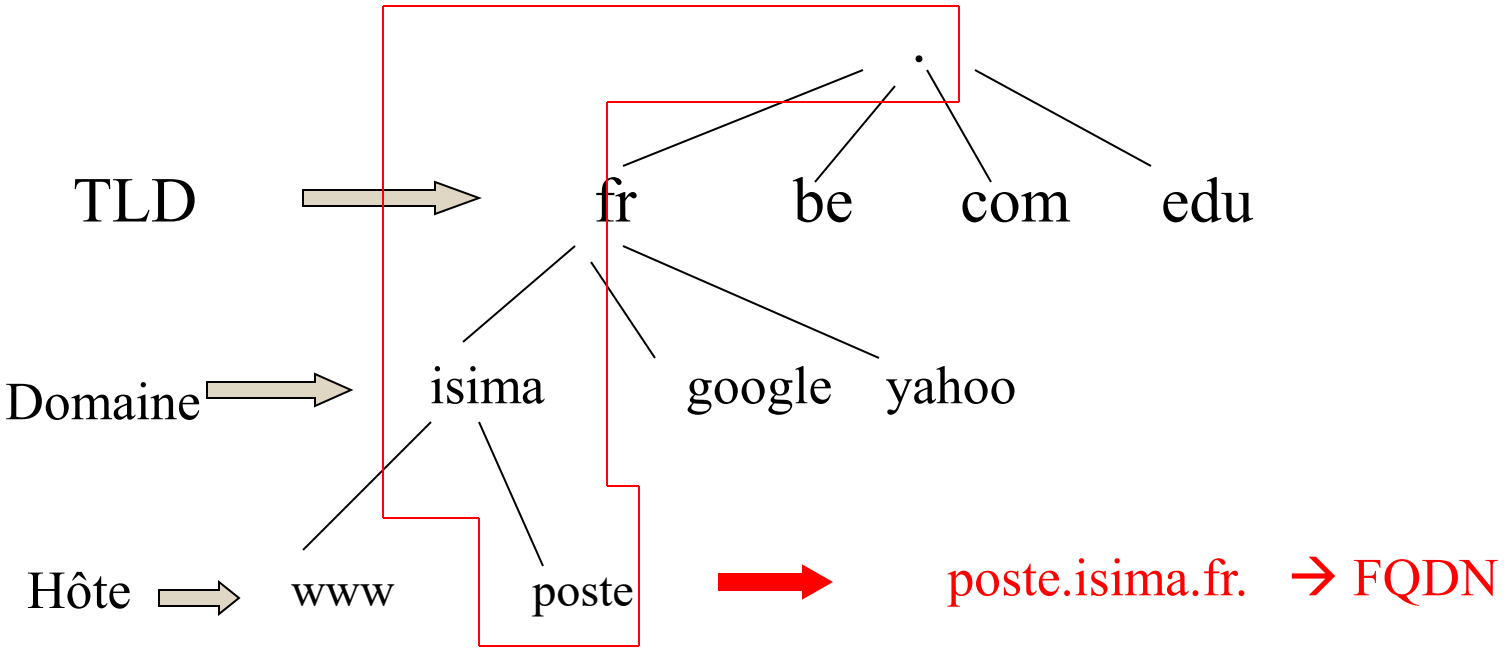
FQDN : Fully Qualified Domain Name

➡ nom complet d'une machine, c'est à dire son nom+ domaine+TLD

chaque domaine est séparé par un "."

exemple : www.isima.fr, ent.uca.fr

Espace des noms (2)



- 2 Sortes de TLD :

- gTLD : generic TLD → réservé à un secteur d'activité

  ex : com, edu, mil, gov, int, net, biz, aero,…

- ccTLD : country code TLD →réservé aux pays

  ex : fr, us, be, nl, tv, zw,…

Les serveurs de nom

- nom usuel : Name Server (NS)

- Implémentation : BIND (Berkley Internet Name Daemon)
  - **Utilisation du port UDP 53**
- Fonctions :
  - Répondre aux requêtes reçues concernant des ressources de sa (ses) zone(s)
  - Eventuellement, répondre à des requêtes concernant d'autres zones (cached data)

Généralement, on a : - un serveur de nom primaire

(SOA : Start of Authority)

- des serveurs secondaires

(copie / sauvegarde du serveur primaire → sur un autre site)

Les RRs

- Composant de la BD du DNS : Ressource Records
- Informations contenues :
- **Type:**
  - A : correspondance nom → @IP
  - CNAME : canonical name : permet l'utilisation des alias
  - HINFO : description de la machine (CPU, mémoire,…)
  - MX : serveur de mail
  - NS : serveur de nom
  - SOA : Start of Authority : le NS maître de la zone
  - PTR : pointeur vers l'espace de nom , correspondance @IP → nom
- **Classe :**
  - IN pour données internet

Fonctionnement

- Lorsqu'un serveur reçoit une requête
  - il répond au client si :
    - il a l'information dans ses tables
    - ou dans son cache
  - sinon
    - soit il construit une requête pour le NS successif, et transmet la réponse à l'auteur de la demande

      → mode récursif (mode habituel)
    - soit il transmet à l'auteur l'@IP du NS à interroger, et c'est l'auteur qui devra aller interroger ce nouveau serveur

      → mode itératif

Les serveurs correspondants aux domaines de plus haut niveau sont appelés "**serveurs de noms racine".**

Il y en a 13 , de a.root-servers.net à m.root-servers.net

Pour finir

un serveur DNS est toujours référencé avec

son @IP

- Il existe des serveurs DNS privés et publics.

La sécurisation d'un réseau

1. Généralité
2. Sécurité d'un système appartenant à un réseau
3. Les Techniques et équipements
4. Le chiffrement

P. Laurençot

Généralité

- 4 mots clés et 1 concepts
  - Authentification
  - Confidentialité
  - Intégrité
  - Disponibilité
  - Non-répudiation

Est-ce que TCP/IP respecte ces critères ?

NON

- Aucune vérification sur l'adresse IP source, ni sur le chemin parcouru
- Buffer de réception de dimension finie…

Objectifs, moyens, techniques

Objectifs de la sécurité

- sécurisation des systèmes
- Sécurisation des accès
  - pour protéger les systèmes
  - pour protéger les informations transmises

Techniques pour la sécurité

- chiffrement
- protocoles sécurisés
- restreindre les accès
- Anti-virus, patches
- etc...

Moyens

- définir une politique de sécurité
  - identifier les entités
  - définir quelle entité a le droit de faire quoi
  - définir ce qui est interdit
- installer la politique définie
- surveiller les systèmes
- participer à la surveillance des réseaux

Pb : les failles de sécurité proviennent à 80% de l'intérieur de l'entreprise

Sécurité d'un système appartenant à un réseau

Rappel : un système ne peut être attaqué que s'il a un processus serveur en attente de demande (*port en état listen* → commande netstat –an).

Configuration des services

- quels services sont nécessaires ? pour quels clients ?
- droits des services (UID, GID, chroot...)
- choix des implémentations

Contrôle des services actifs

- à partir de la configuration du système
- en examinant les services en attente, de l'intérieur (**`netstat`**) ou de l'extérieur du système (**`nmap`**)

Contrôle des demandes de service

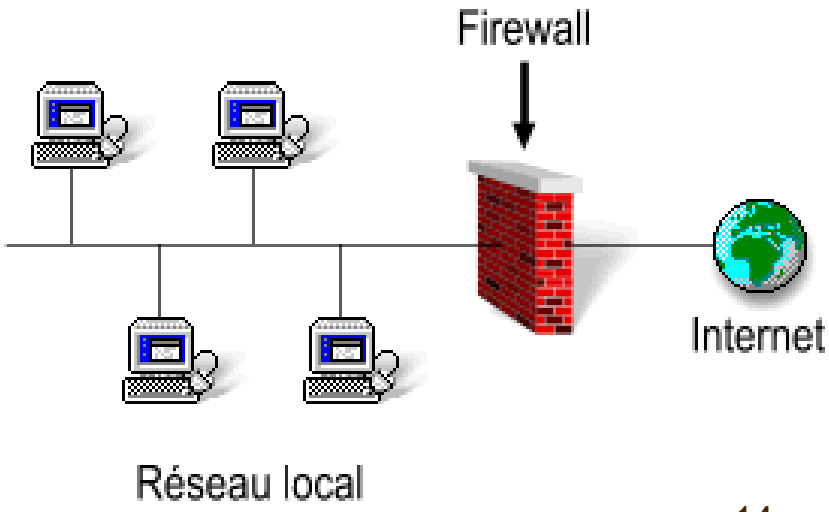
- filtrage des demandes avant de les livrer aux entités serveurs
- journalisation des demandes
- alertes en cas de demandes interdites
- remonter les tentatives malveillantes

Le Pare-feu (1)

- La parefeu (firewall)
  - permet de protéger le réseau interne de l'extérieur
  - utilise des règles définies par la politique de sécurité
  - point de passage obligatoire des données
  - Architecture généralement logicielle

Rôle principal : **FILTRAGE**

- au niveau IP
- au niveau Transport
- quelque fois au niveau applicatif : proxy



Le Pare-feu (2)

- Restriction
  - Ne gère pas les communications sur le réseau interne
  - Ne protège pas contre les virus
  - Ne peut voir que le trafic qui passe par lui
  - Ne peut se configurer tout seul !!!

- Avantage
  - Journalisation du trafic

Actuellement, politique de tout interdire et de n'ouvrir que les services utiles.

Le NAT (1)

- Au niveau Réseau (pour un réseau isolé par un équipement)
  - identification du réseau et des systèmes qui le composent
    - adresses privées (RFC 1918)
      - Classe A : 10.0.0.0
      - Classe B : 172.16.0.0 à 172.31.0.0
      - Classe C : 192.168.0.0 à 192.168.255.0
  - protection par un équipement actif (routeur, pare-feu,…)
    - règles de filtrage sur la source, la destination ou les deux (fonction pare-feu)
    - traduction d'adresses (NAT)
      - **IP-masquerading,**
      - **Network Address Translation (statique ou dynamique),**
      - **Port Address Translation,**

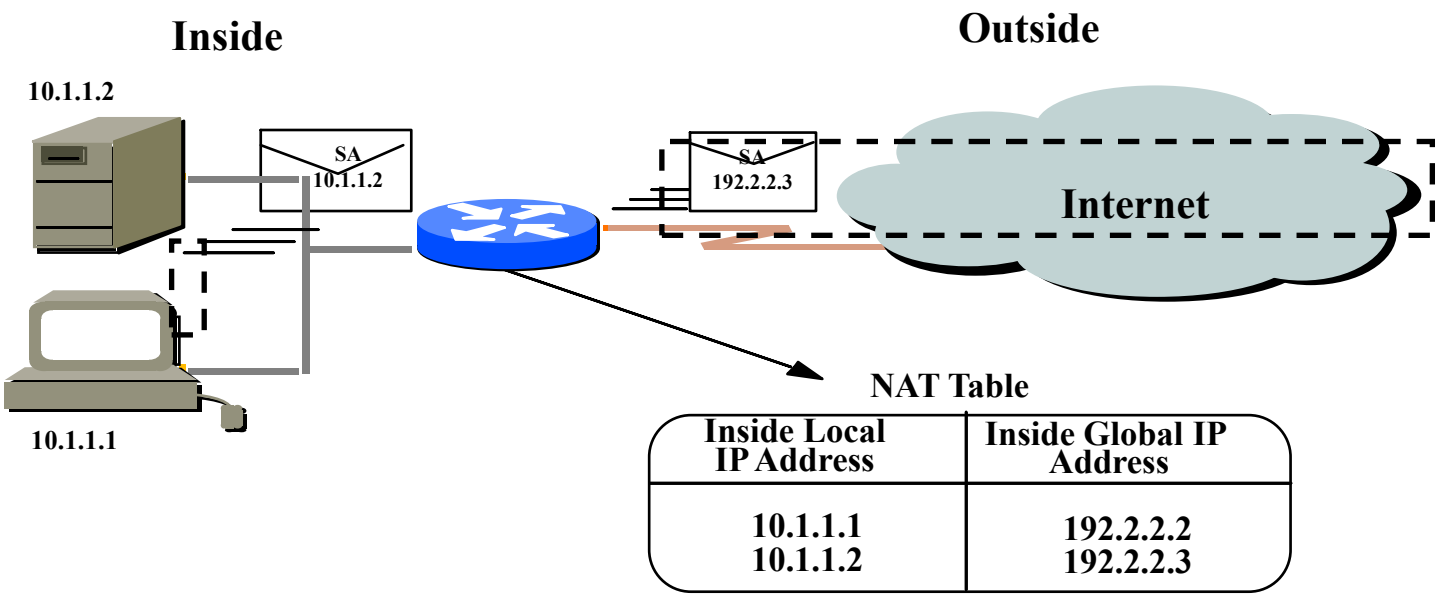
Attention, il peut être nécessaire de réécrire le message du fait du changement d ’@IP.

Le NAT (2)

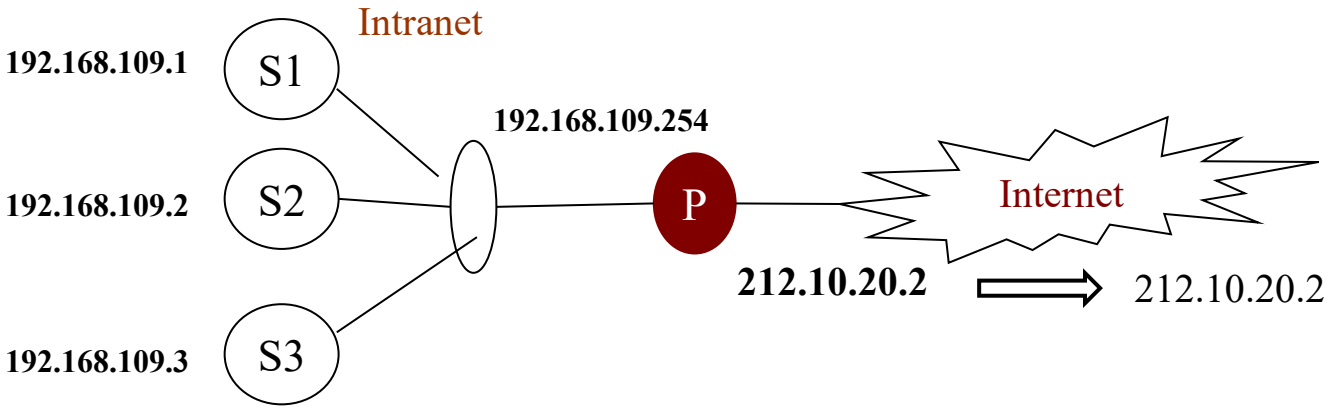
Le NAT statique = association de n adresses avec n adresses.

C'est à dire qu'à une adresse IP interne, on associe une adresse IP externe.

Rôle du système: remplacer l'adresse de la station du réseau par une adresse externe (publique).



Le NAT (3)



1 seule adresse est disponible pour envoyer des paquets IP vers Internet (ex: adsl)

Pb: Si plusieurs stations appartiennent au réseau local, comment peuvent-elles envoyer des PDU-IP vers l'internet et comment les différencier ?

=> Utilisation du NAT dynamique

Le NAT(4)

2 cas possibles :

- **1 seule adresse IP de sortie -> PAT**
- **n adresses de sortie pour m ordinateurs (m > n)**
  -> IP masquerading ou PAT

Fonctionnement :

- *En Masquerading*, traduction automatique de l'adresse IP de la station émettrice avec l'adresse IP de la Passerelle (routeur, proxy)
- *En PAT*, traduction automatique de l'adresse IP de la station émettrice avec l'adresse IP de la Passerelle (routeur, proxy) **et translation du port.**

  La translation du port permet de différencier les stations qui utilisent la même adresse IP Passerelle.

Application possible : mini-réseau derrière un routeur ADSL ➔ pb : adresse IP statique/dynamique

Les sondes (1)

Sonde IPS /IDS

- IDS **I**ntrusion **D**etection **S**ystem
- IPS **I**ntrusion **P**revention **S**ystem

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

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

➢En cas de détection d'une intrusion :

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

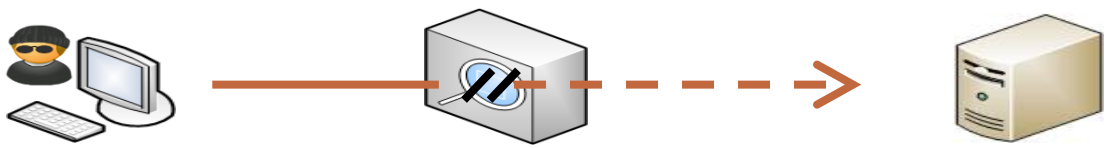
Les sondes (2)

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

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

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

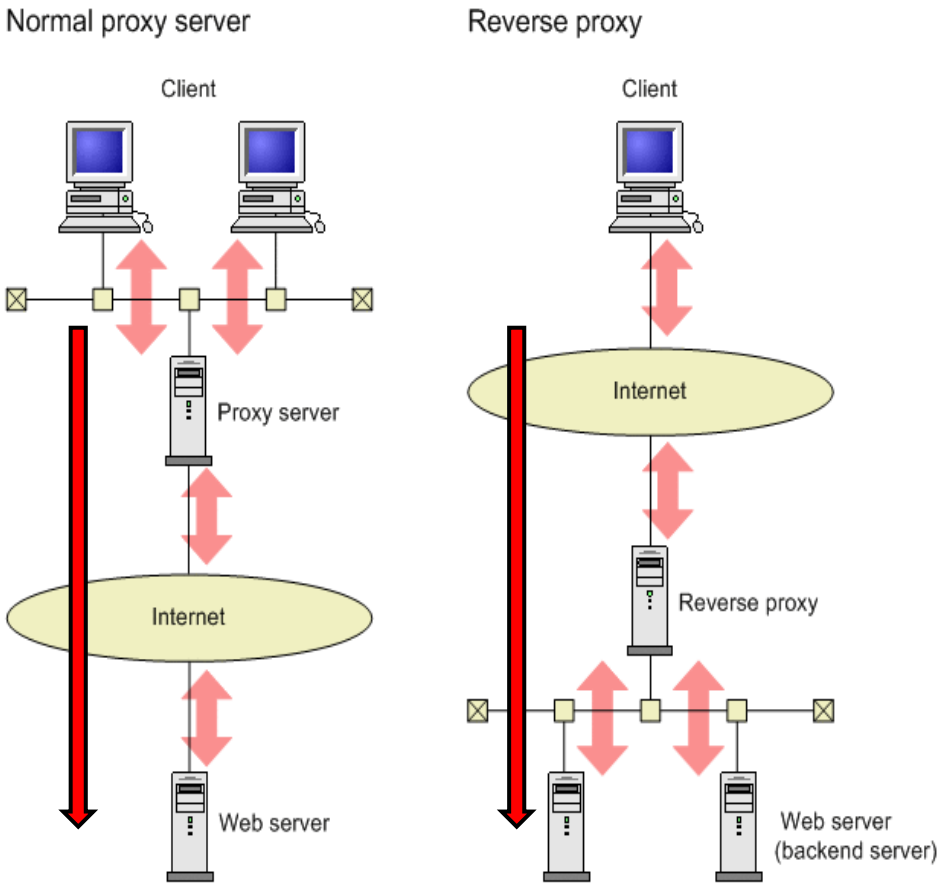
➢Un IPS **doit forcément** être en **coupure du flux** de façon à pourvoir bloquer le trafic lorsque cela est nécessaire.



Proxy et reverse proxy

- Proxy : *composant logiciel servant d'intermédiaire entre la source et la destination*
  - Filtrage
  - Cache
  - Etc…

Le reverse proxy permet de faire aussi:
- load balancer

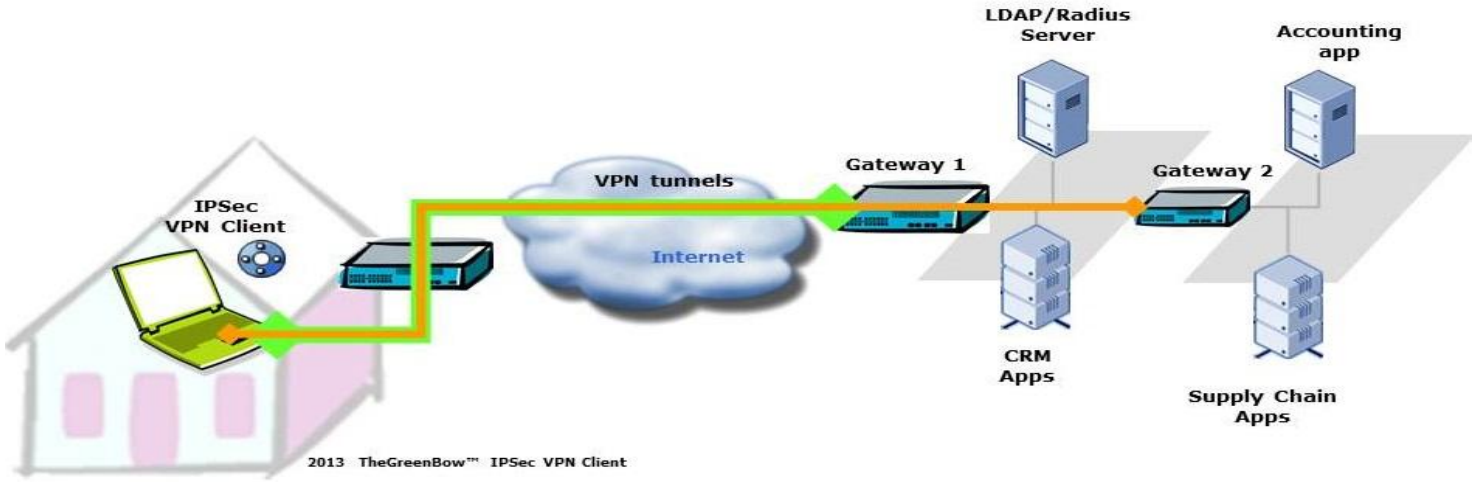


VPN (1)

Virtual Private Network

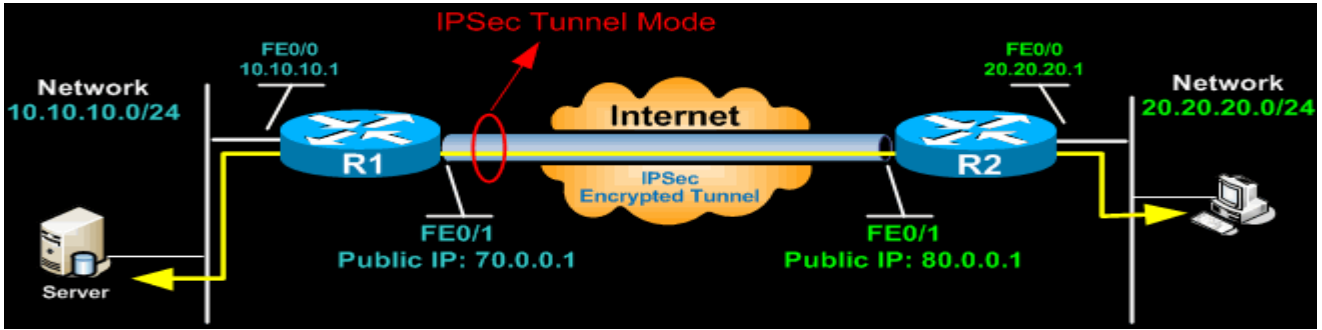
Un VPN est un **réseau virtuel** qui permet à **deux réseaux distants de communiquer en toute sécurité**, y compris si la communication s'effectue via des réseaux inconnus et auxquels nous ne faisons pas confiance.

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



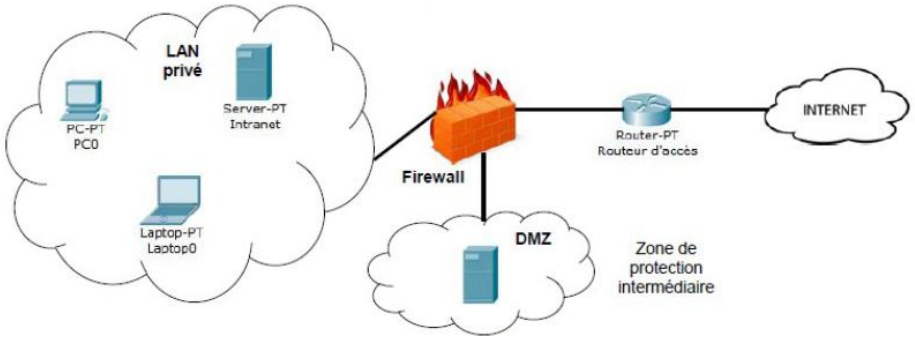
VPN (2)

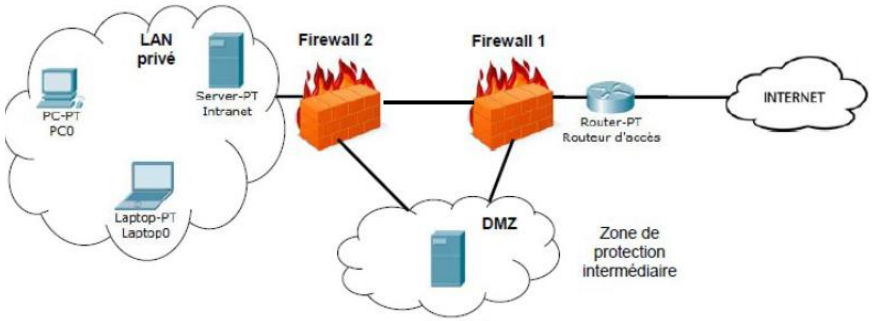
- Nécessite un serveur VPN
  - Le client VPN se connecte sur le serveur VPN et reçoit une nouvelle adresse IP pour communiquer avec ce serveur
  - Les communications passent par ce serveur avant de retourner sur Internet
  - Les communications **sont chiffrées** entre le client VPN et le serveur VPN.
- Plusieurs méthodes pour créer des VPN
  - Poste à entreprise : OpenVPN, winguard, …
  - D'une succursale à une autre
    - Utilisation de IPSEC
      - Protocole Ikev1 ou Ikv2 utilisé



Architecture (1)

- DMZ: est un sous-réseau séparé du réseau local et isolé de celui-ci et d'internet par un parefeu. Ce sous-réseau contient des machines étant susceptibles d'être accédées depuis internet. (wikipédia)
  - Possibilité d'attaques…
  - Plus ou moins de protection suivant l'architecture utilisée





- Utilisation adresse IP privée
  - Mise en place de NAT

Le chiffrement

Chiffrement : principes

- Définitions
  - chiffrement $M \xrightarrow{E_k} C$
  - déchiffrement $C \xrightarrow{D_{k'}} M$

E	algorithme de chiffrement
D	algorithme de déchiffrement
k	clé de chiffrement
k'	clé de déchiffrement

- Propriétés (souhaitées) d'un cryptosystème
  - $D_{k'}(E_k(M)) = M$ où les clés k et k' sont associées
  - $D_{k'}$ et E_k dépendent totalement ou partiellement d'informations secrètes
  - les algorithmes doivent être économiques : processeur, mémoire, taille de code
  - le secret doit reposer sur les clés plutôt que sur les algorithmes
    - algorithme public - > qualité meilleure
  - le calcul de k' doit être très difficile, même si on connaît C et M
  - $D_{b'}(E_a(M))$ doit être une information non valide

Chiffrement : cryptosystèmes

A chiffre symétrique (k = k')

- économique
- problème de la gestion des clés

DES *(Data Encryption Standard –fin en 2001)*
Triple-DES
IDEA *(International Data Encryption Algorithm)*
AES *(Advanced Encryption Standard)*

A chiffre asymétrique (k ≠ k')

- $D_{k'}(E_k(M)) = E_k(D_{k'}(M)) = M$
- peu économique

DH *(Diffie-Hellman)*
RSA *(Rivest, Shamir, Adleman)*

$E_k(M) = M^e$ modulo n k = {e,n}
$D_{k'}(C) = C^d$ modulo n k' = {d,n}

n = p*q
p et q premiers entre eux
e premier avec (p-1)*(q-1)
d*e = 1 modulo ((p-1)*(q-1))

hachage

- pour créer des empreintes d'information (*digest*)
- algorithmes analogues à ceux du chiffrement
- pas de déchiffrement possible

MD5 *(Message Digest)*
SHA-256 *(Secure Hash Algorithm)*

Chiffrement : asymétrique

- **3 éléments essentiels :**
- Nécessité de deux clés -> créer en même temps par la même personne

❑ Clé privée : comme son nom l'indique, cette clé est personnelle et connue de son seul propriétaire

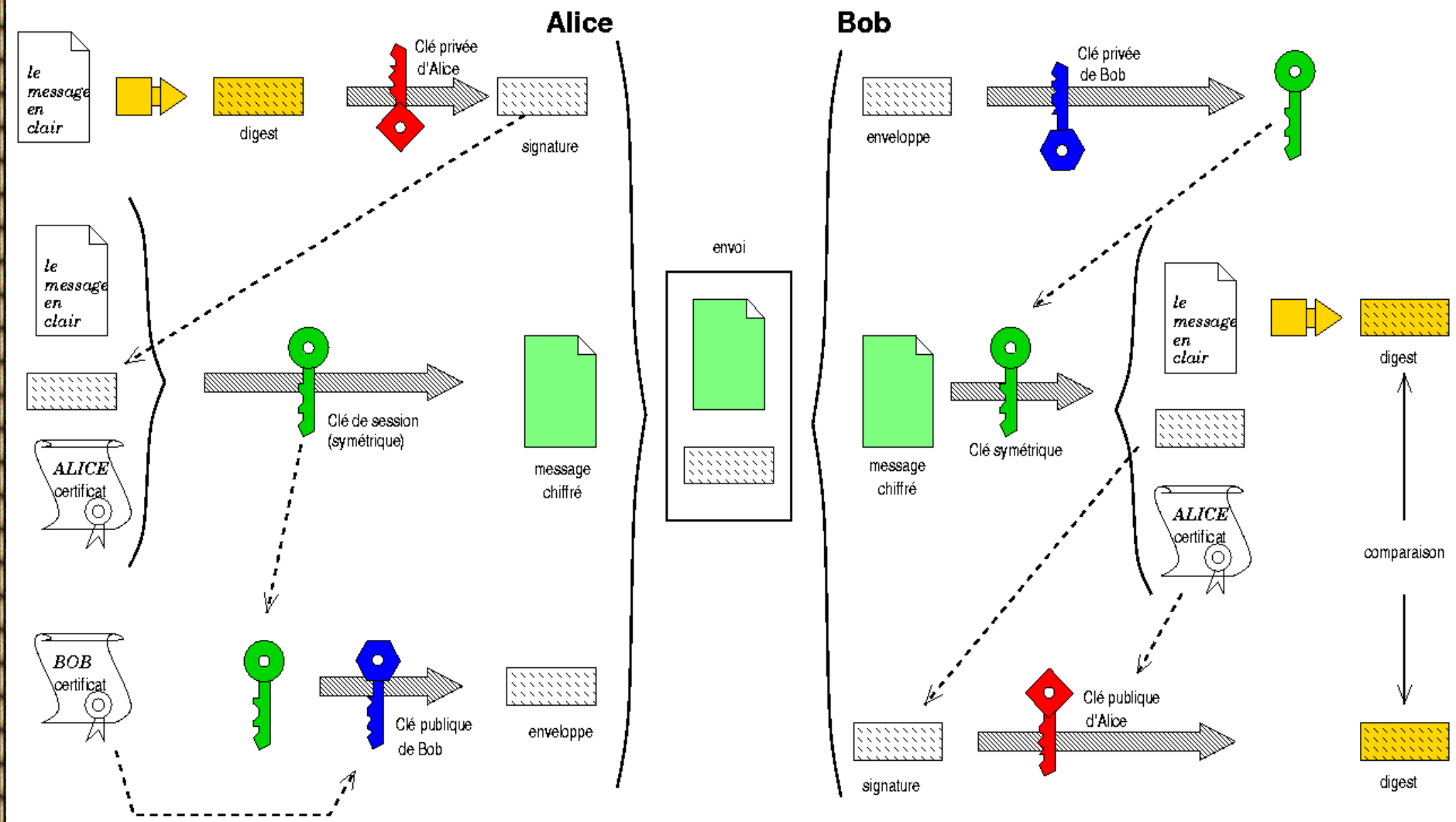
❑ Clé publique : clé distribuée à tout le monde permettant de chiffrer un message

clé privée (clé publique (M)) = clé publique (clé privée ((M)) = M

❑ Certificat : donner par une autorité de certification

-> permet de s'assurer qu'une clé publique appartient bien au propriétaire annoncé.

Chiffrement : exemple résumé



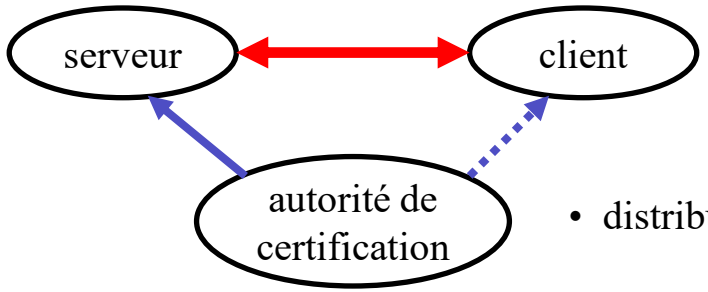
Hachage

- Création d'une empreinte numérique
  - Unique pour un objet
  - Fonction à sens unique
  - Obtention : hash ou condensat ou empreinte sur n bits
  - Problème collision
- Fonctions
  - Md5, sha-1, sha2-256,Sha2-384, sha3-384, sha2-512, …
  - HMAC (Keyed-hash message authentication code)
    - Chiffrement clé secrète + hachage

Protocole sécurisé : SSL/TLS

Secure Socket Layer (Netscape 1994), puis IETF

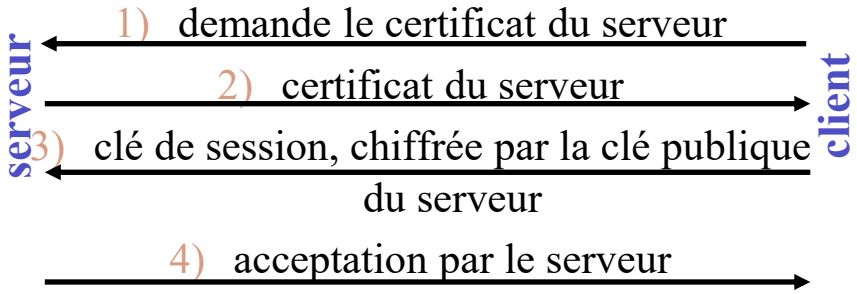
- fournit des services
- possède un certificat



- achète des services
- possède ou non un certificat

- distribue des certificats

établissement de connexion ssl



transmission d'informations

- non chiffrée
- chiffrée avec la clé publique du serveur
- chiffrée avec la clé de session

- compression éventuelle
- Hachage du message envoyé

problèmes

- le client n'est certifié qu'optionnellement ⇒ risque pour le serveur
- si le client est certifié, il ne peut pas être anonyme ⇒ risque pour le client
- pas de contrôle de validité des certificats entre délivrance et fin de validité
- autorités de certification

Protection

Aide

- ANSSI

- Lutte contre le téléchargement illégal : HADOPI

Haute Autorité pour la Diffusion des œuvres et la protection des droits sur Internet.

Comment cela fonctionne-t-il ?

Différent web

TOR

Sécurisation d'un réseau

Sécurisation d'un réseau (1)

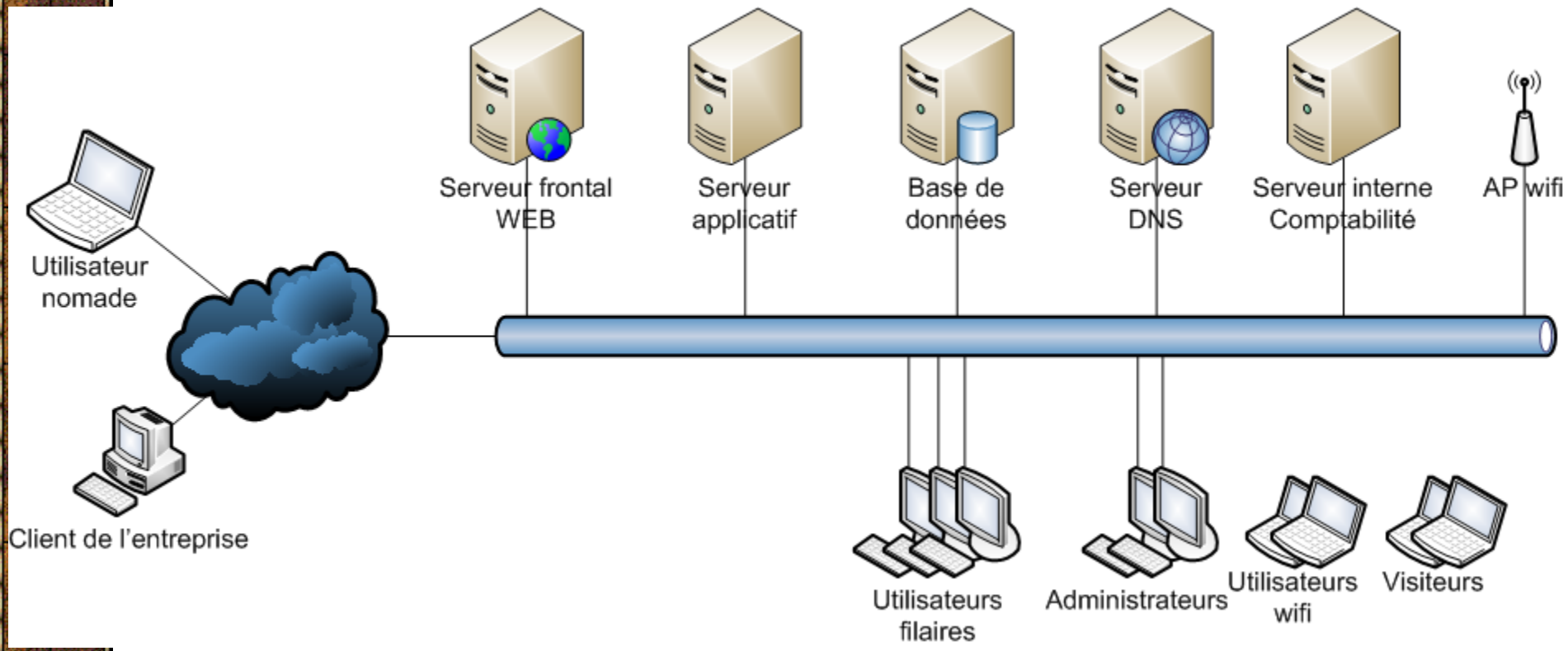
Exemple pratique de sécurisation avec un réseau simple

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.

Sécurisation d'un réseau (2)

Exemple pratique de sécurisation avec un réseau simple



Réseau « à plat », avant sécurisation

Sécurisation d'un réseau (3)

Exemple pratique de sécurisation avec un réseau simple

Comment améliorer la sécurité :

- 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 :

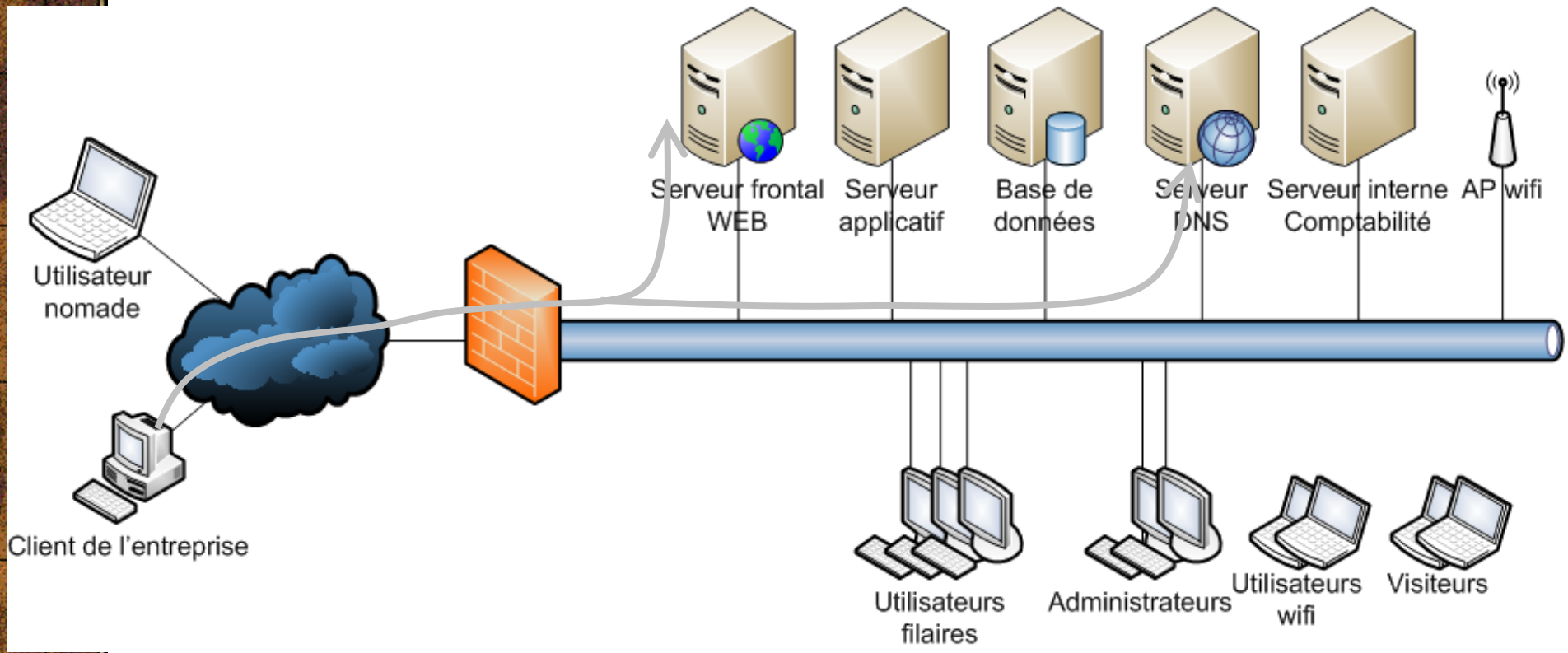
- Le réseau est **directement connecté à Internet**, i.e. tous les systèmes et utilisateurs et systèmes peuvent communiquer avec l'extérieur (attention aux **fuites de données !**) et **tout Internet peut se connecter sur notre réseau interne.**

- *Ajout d'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.

Sécurisation d'un réseau (4)

Exemple pratique de sécurisation avec un réseau simple



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

Sécurisation d'un réseau (5)

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

- Si le serveur WEB présente une **vulnérabilité**, un hacker peut **prendre la main sur ce serveur**, puis **rebondir ensuite sur le réseau interne.**

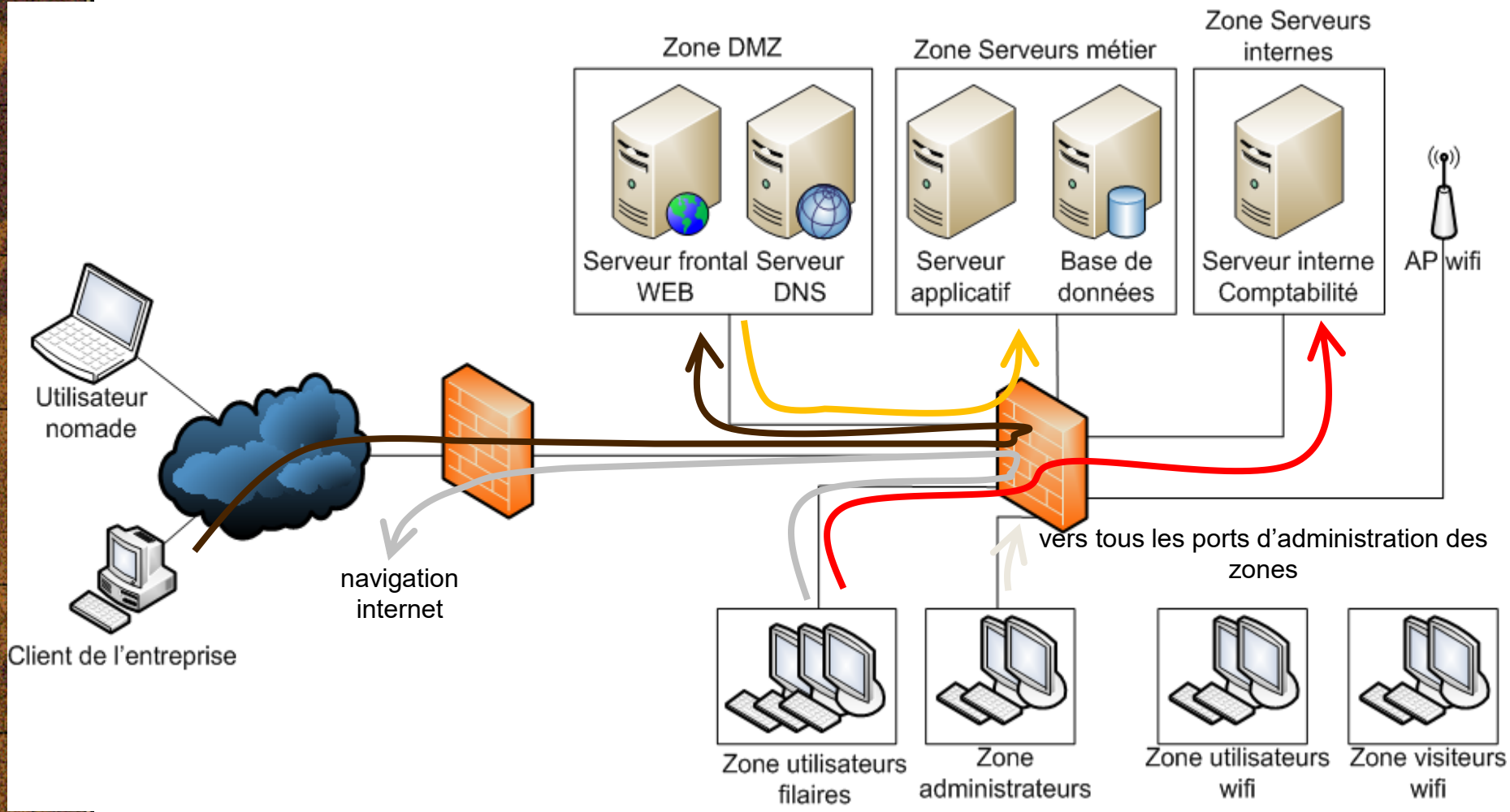
Donc **segmentation** de notre réseau en **différentes zones de criticité** :

- Une **DMZ** destinée à héberger tous les serveurs qui doivent être accessibles depuis internet
- 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…).

Utilisation d'un **un deuxième pare-feu (interne)** afin que seuls les flux que nous allons configurer soient autorisés. *Mise en place d'un filtrage interne.*

Sécurisation d'un réseau (6)

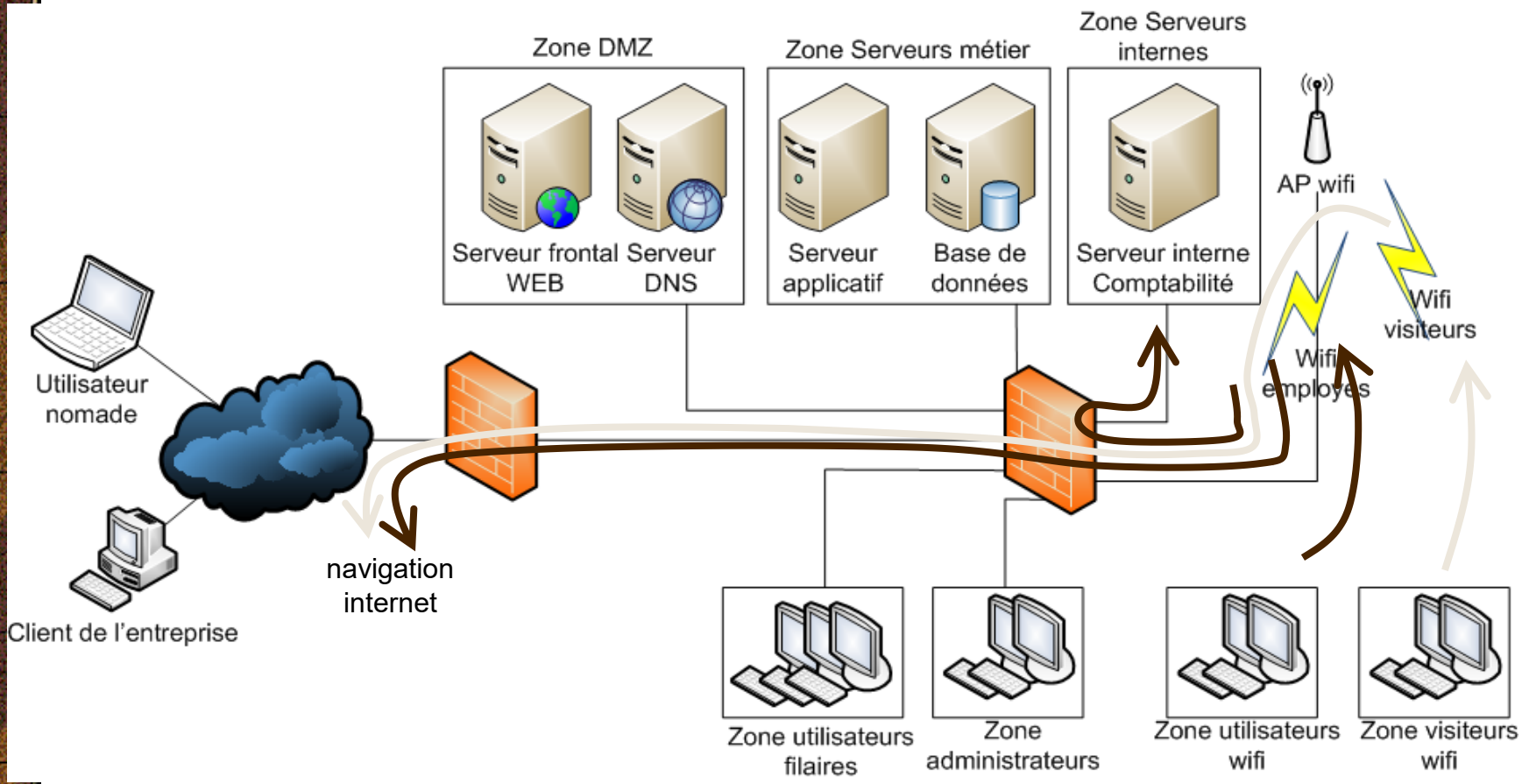
Exemple pratique de sécurisation avec un réseau simple



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

Sécurisation d'un réseau (7)

Le wifi doit être accessible aux visiteurs et aux employés internes. Puisque le besoin d'accès aux ressources est différent pour ces 2 populations, nous implémentons 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.

Sécurisation d'un réseau (8)

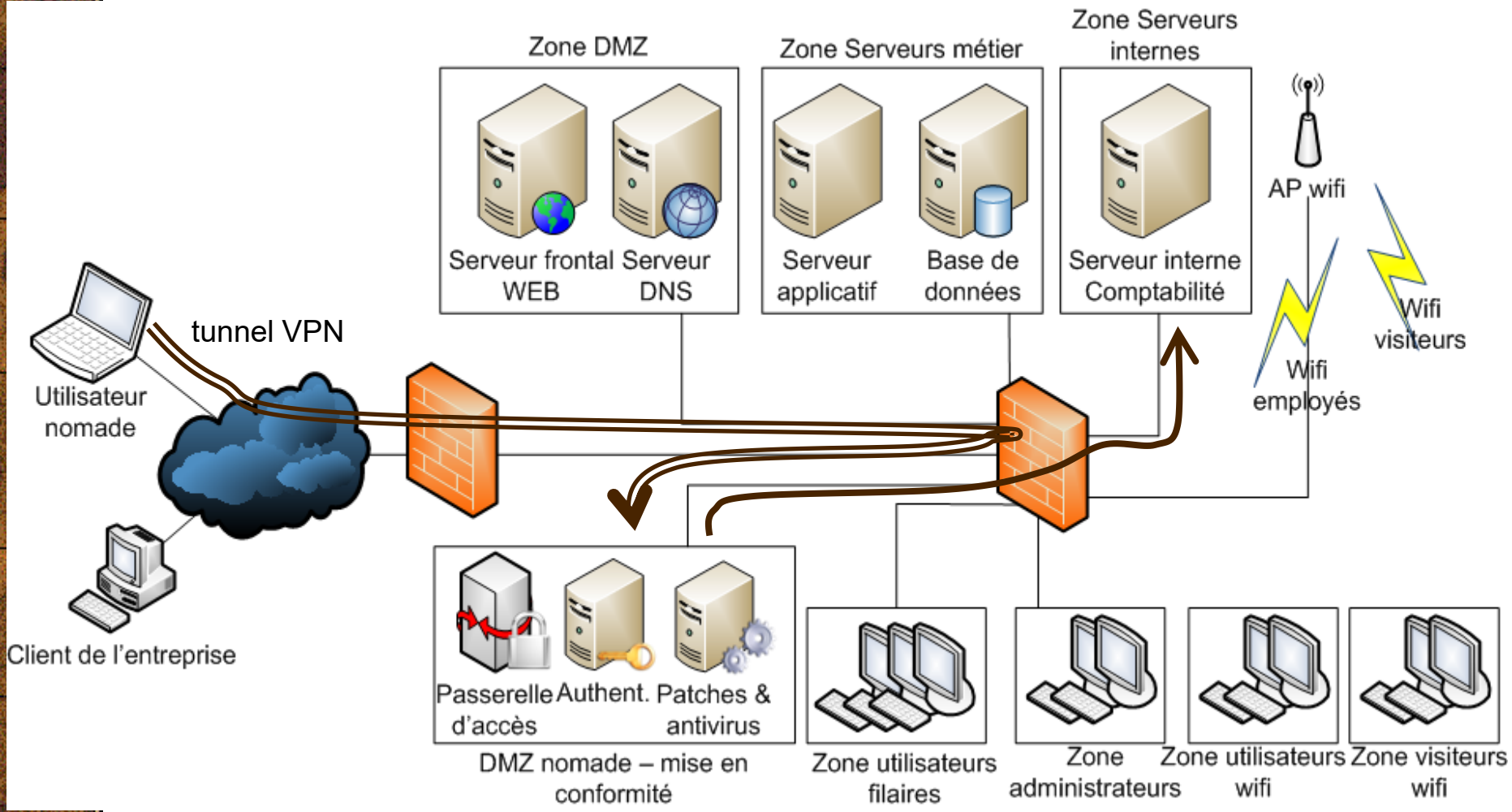
Exemple pratique de sécurisation avec un réseau simple

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**.

Sécurisation d'un réseau (9)

Exemple pratique de sécurisation avec un réseau simple



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

Sécurisation d'un réseau (10)

Exemple pratique de sécurisation avec un réseau simple

- 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.).

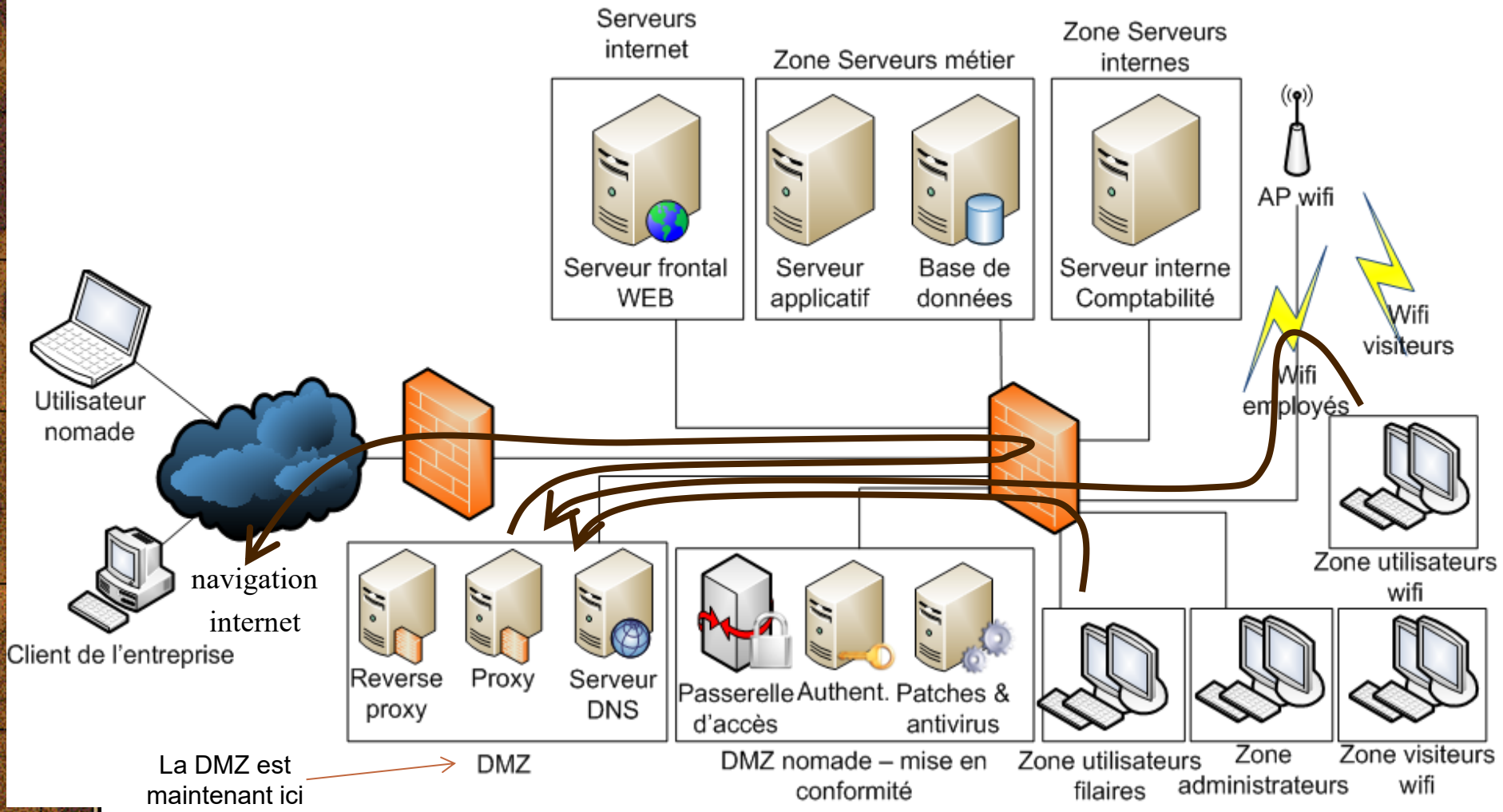
Utilisation d'un **proxy pour analyser les flux sortants**, et **un reverse-proxy pour analyser les flux entrants**.

- équipements en coupure, ils empêchent donc les postes de travail des utilisateurs d'être connectés directement à Internet
- le serveur WEB 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.

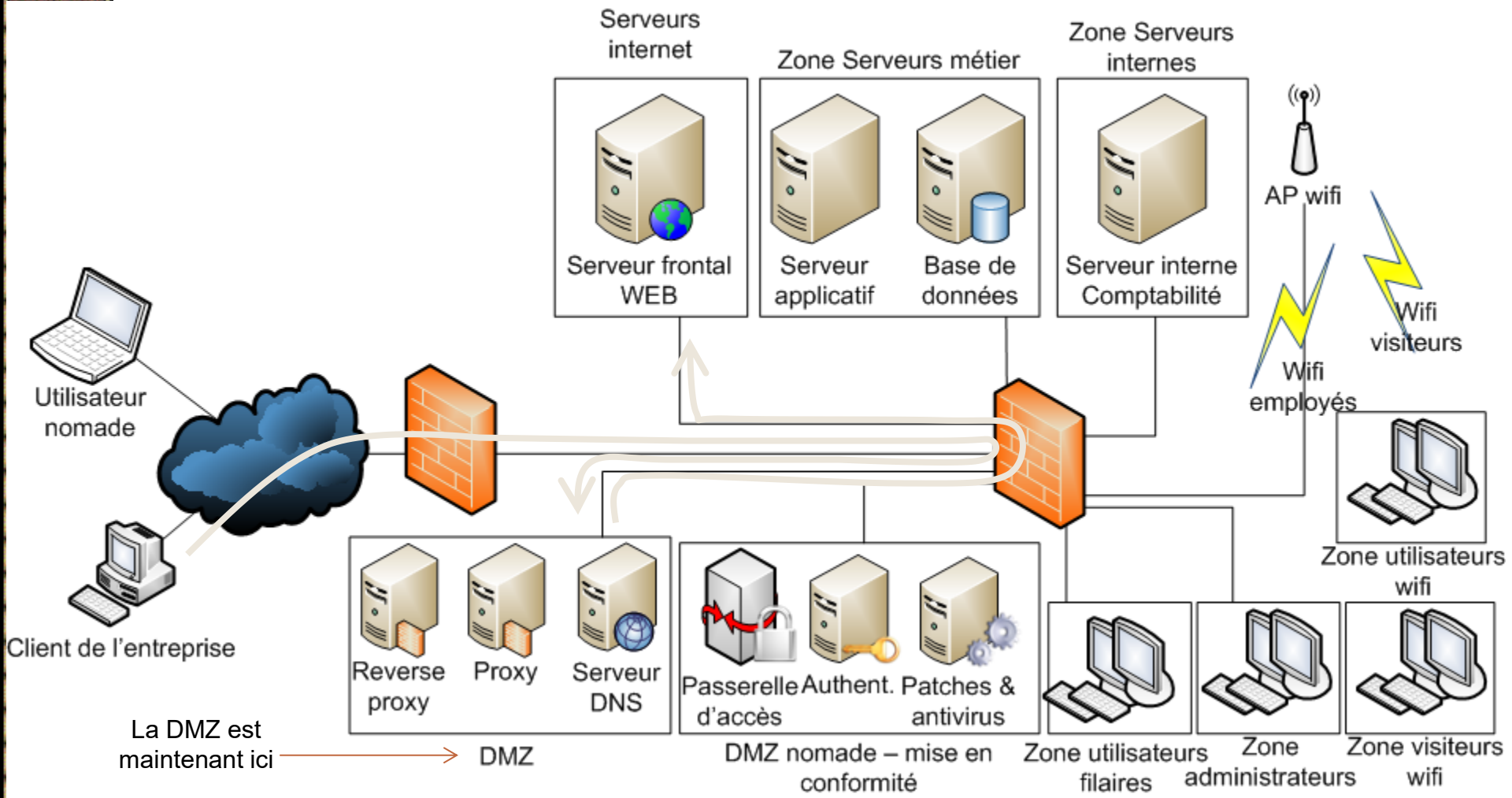
Sécurisation d'un réseau (11)

h. Exemple pratique de sécurisation avec un réseau simple



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

Sécurisation d'un réseau (12)



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