INF4420a: Sécurité Informatique

Sécurité Réseau 2

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de sécurité réseau

- Exercice 1 : Conception d'une architecture de sécurité

- Objectif :
  - Comprendre les risques pour la sécurité réseau
  - Savoir concevoir une architecture de sécurité permettant d'y faire face

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de sécurité réseau

- Exercice 1 : Conception d'une architecture de sécurité
  - Une entreprise vient de créer sa filiale à Montréal
  - Vous venez d'être embauché comme administrateur de sécurité de cette filiale
  - Vous devez proposer une architecture de sécurité pour le réseau informatique de cette entreprise

Exercices de sécurité réseau

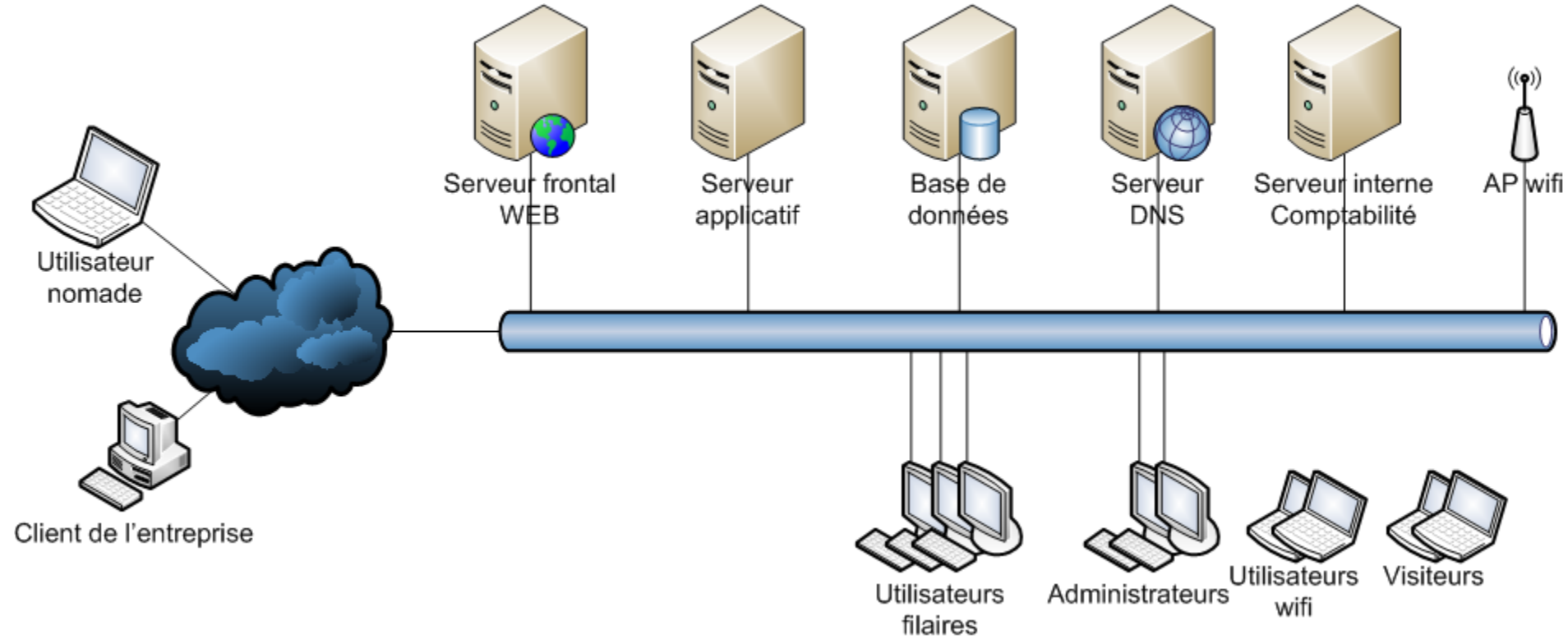
- Cahier des charges (partie 1)
  - L'entreprise fournit un site WEB de e-commerce
  - Afin de fonctionner, l'entreprise possède également des serveurs internes (comptabilité, wiki, etc.)

Exercices de sécurité réseau

- Cahier des charges (partie 2)
  - Certains employés se connectent sur le réseau local filaire, d'autres se connectent en wifi
  - Certains employés sont nomades et doivent pouvoir se connecter à distance
  - Il existe deux catégories principales d'utilisateurs : les utilisateurs « standard » et les administrateurs du S.I.
  - L'entreprise souhaite permettre à ses visiteurs de se connecter en wifi afin de naviguer sur internet

Exercices de sécurité réseau

- Réseau « à plat » de l'entreprise avant sécurisation



POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de sécurité réseau

- Vous devez donc proposer une architecture de sécurité pour ce réseau
- Vous allez procéder par étape
- Note :
  - Il existe plusieurs façons d'améliorer la sécurité de ce réseau
  - Nous présentons ici les grandes lignes
  - Cet exercice n'est pas exhaustif
  - Ce n'est pas non plus la seule solution possible

Exercices de sécurité réseau

- Faiblesse 1
  - Le réseau est directement connecté à Internet
- Conséquence 1
  - Tous les systèmes et utilisateurs et systèmes peuvent communiquer avec l'extérieur
  - Attention aux fuites de données
- Conséquence 2
  - Tout Internet peut se connecter sur notre réseau interne
  - Attention aux attaques

Exercices de sécurité réseau

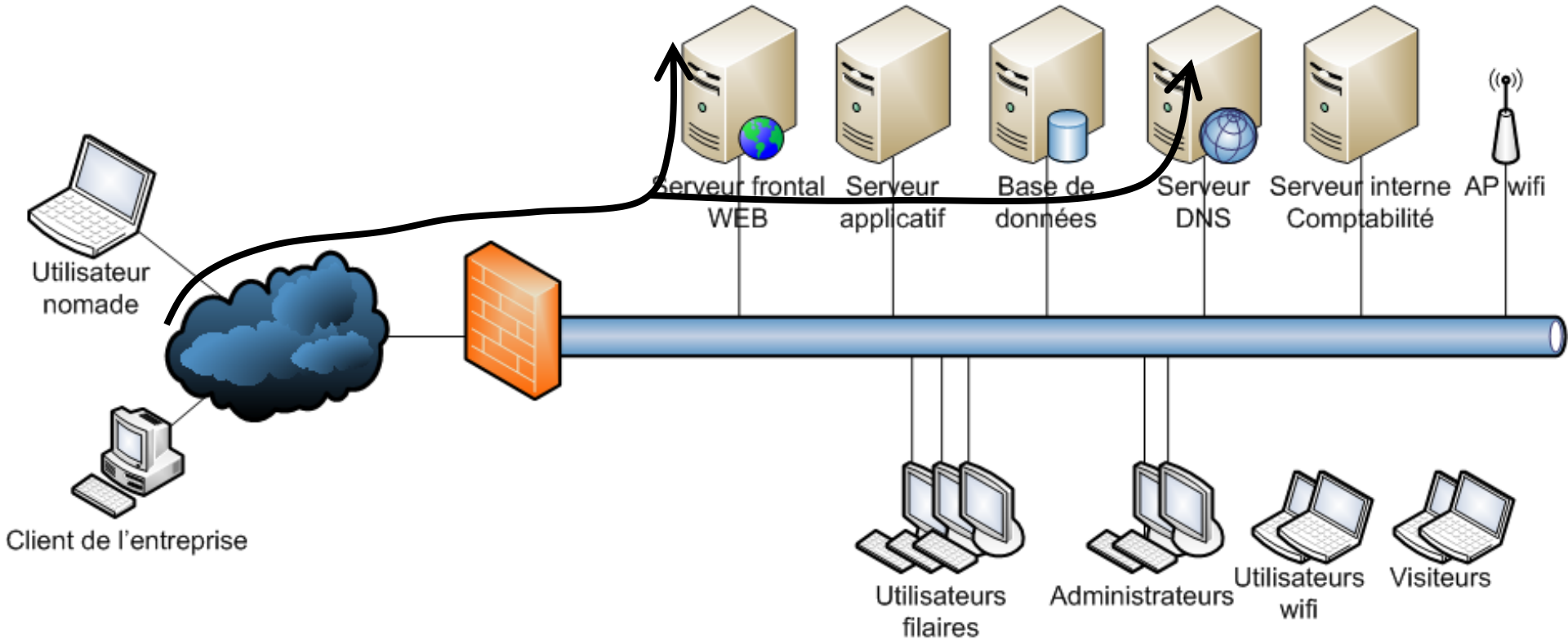
- Question 1 : Comment procédez-vous pour corriger la faiblesse 1 ?

Exercices de sécurité réseau

- Réponse question 1 :
  - En implémentant un pare-feu en frontal
  - Le pare-feu 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

Exercices de sécurité réseau

- Réseau « à plat » de l'entreprise avec un pare-feu en frontal



Exercices de sécurité réseau

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

- Faiblesse 2
  - Au cas où le serveur WEB présente une vulnérabilité, un hacker présent sur Internet peut potentiellement prendre la main sur ce serveur
  - Il pourra ensuite rebondir sur le réseau interne

Exercices de sécurité réseau

- Question 2 : Comment procédez-vous pour corriger la faiblesse 2 ?

Exercices de sécurité réseau

- Réponse Question 2 :
- Vous proposer de segmenter le réseau en différentes zones de criticité :
  - Zone 1 : DMZ (zone démilitarisée) destinée à héberger les serveurs accessibles depuis internet, et uniquement ceux-ci
  - Zone 2 : Zone des serveurs métiers (serveur applicatif et BD)
  - Zone 2 : Zone des serveurs internes de l'entreprise
  - Zone 3 : Zone pour les postes de travail filaires des utilisateurs
  - Zone 4 : Zone pour les postes de travail wifi des utilisateurs
  - Zone 5 : Zone pour les postes wifi des visiteurs
  - Zone 6 : Zone pour les postes de travail des administrateurs,
    - Pour répondre au besoin d'accéder à des interfaces d'administration (RDP, SSH…)

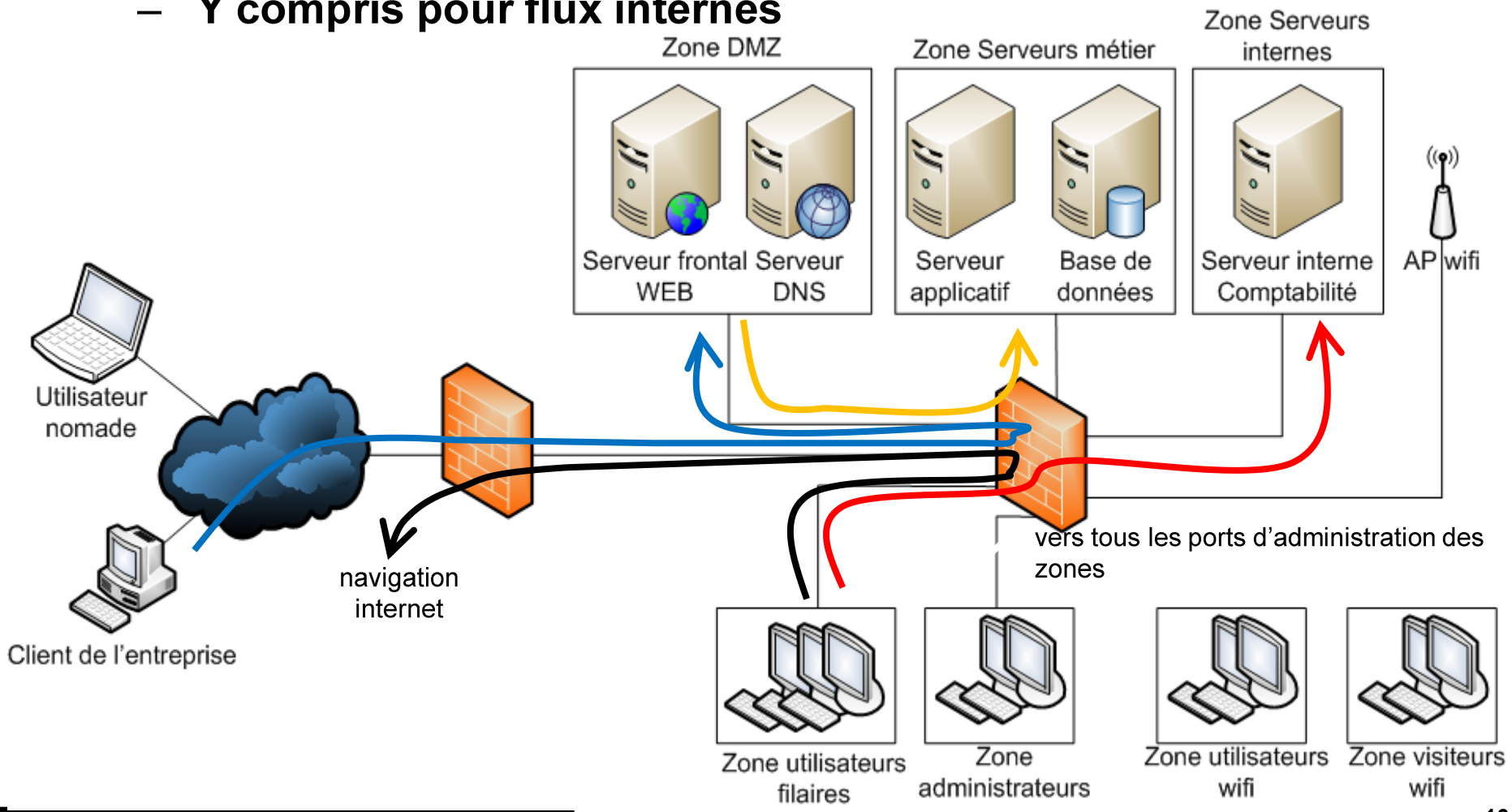
Exercices de sécurité réseau

- Réponse Question 2 (suite) :
- Pour que cette segmentation soit efficace, vous proposez de faire passer tous les flux (y compris internes) par un deuxième pare-feu (interne)
  - En cas de faille dans le serveur web, un attaquant aura plus de difficultés pour rebondir sur le réseau interne
  - Seuls les flux que nous allons configurer seront autorisés

- Remarque
  - Un réseau segmenté non filtré ne sert à rien car toutes les zones peuvent communiquer entre-elles

Exercices de sécurité réseau

- Réseau avec zones segmentées,
  - **Filtrage systématique via le pare-feu**
  - **Y compris pour flux internes**



Exercices de sécurité réseau

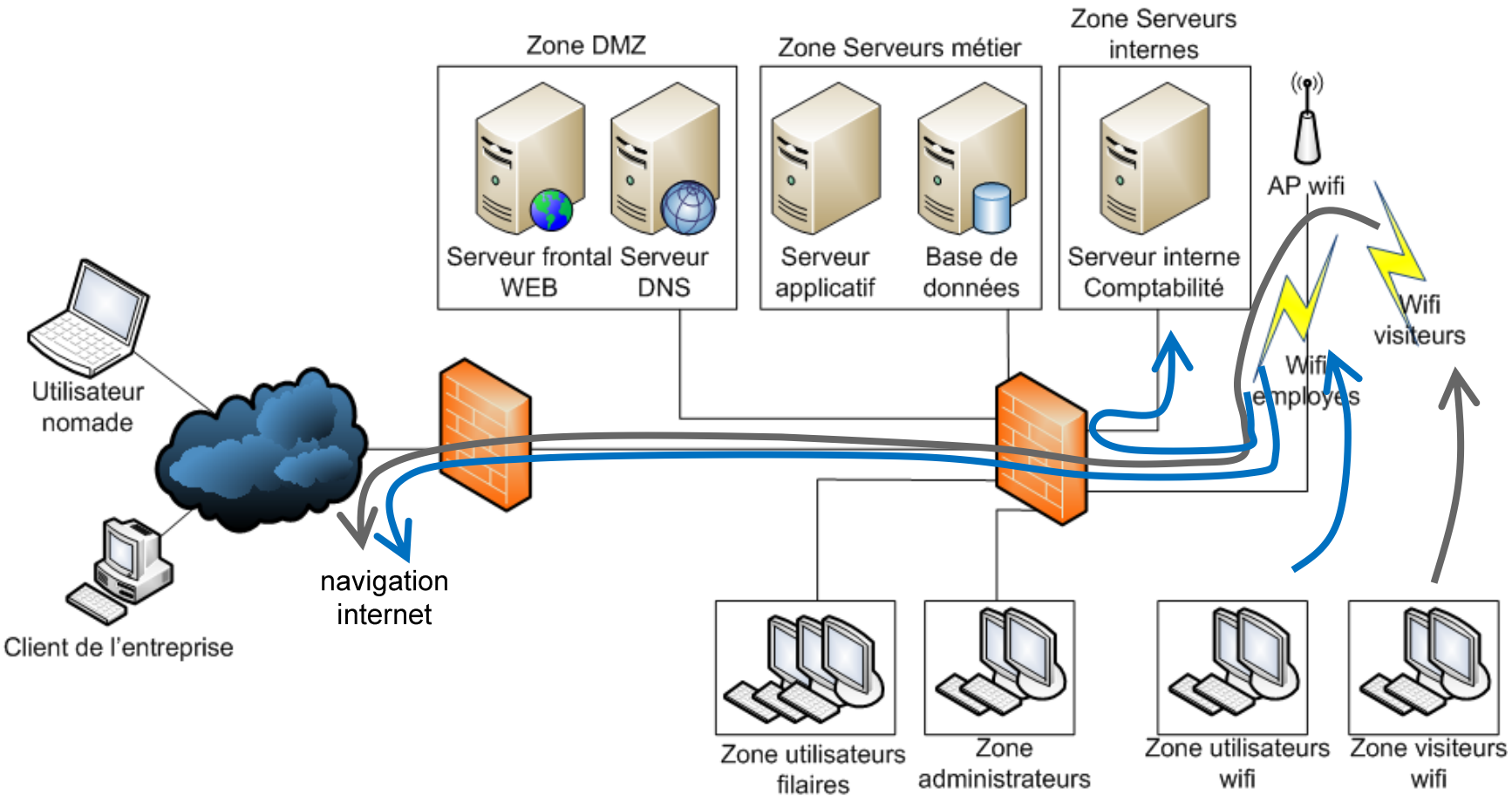
- Question 3 : Comment proposez-vous de gérer les points d'accès Wifi ?

Exercices de sécurité réseau

- Réponse question 3 :
- Le point d'accès wifi doit être accessible aux visiteurs et aux employés internes
  - Le besoin d'accès aux ressources est différent pour ces 2 populations
  - Vous proposez d'implémenter deux SSID (deux réseaux wifi distincts)
  - Ces deux SSID seront portés par le même point d'accès
  - Le pare-feu aura la charge de filtrer les flux

Exercices de sécurité réseau

- Deux réseaux wifi, dont les flux sont filtrés différemment



Exercices de sécurité réseau

- Vous devez également permettre aux utilisateurs nomades de se connecter au réseau interne depuis internet

- Question 4 : Quelle solution proposez vous pour gérer les accès des utilisateurs nomades ?

Exercices de sécurité réseau

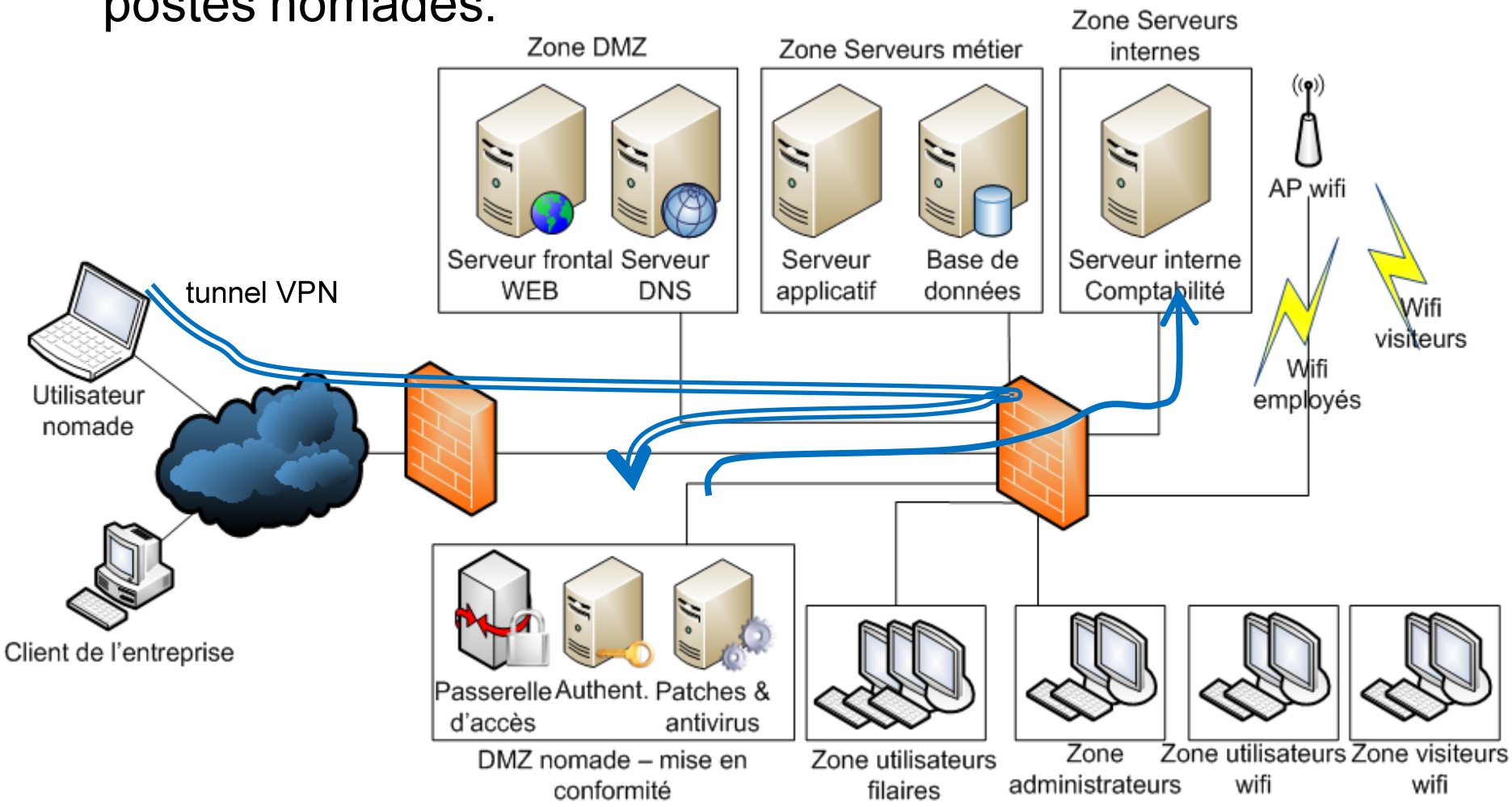
- Réponse question 4 (partie 1) :
- Mise en place d'un tunnel VPN (en général IPSEC) pour permettre aux utilisateurs nomades de se connecter au réseau interne depuis internet
  - Fournit l'interface d'accès au réseau interne depuis internet

Exercices de sécurité réseau

- Réponse question 4 (partie 2) :
- Création d'une DMZ spécifique, appelée zone de mise en conformité, dont le rôle est le suivant :
  - 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

Exercices de sécurité réseau

- Tunnel VPN avec DMZ de mise en conformité pour les postes nomades.



Exercices de sécurité réseau

- Enfin, il reste à filtrer le trafic WEB entrant et sortant

- Question 5 : Quelle solution proposez-vous pour filtrer les connexions des usagers internes lorsqu'ils naviguent sur Internet ?

Exercices de sécurité réseau

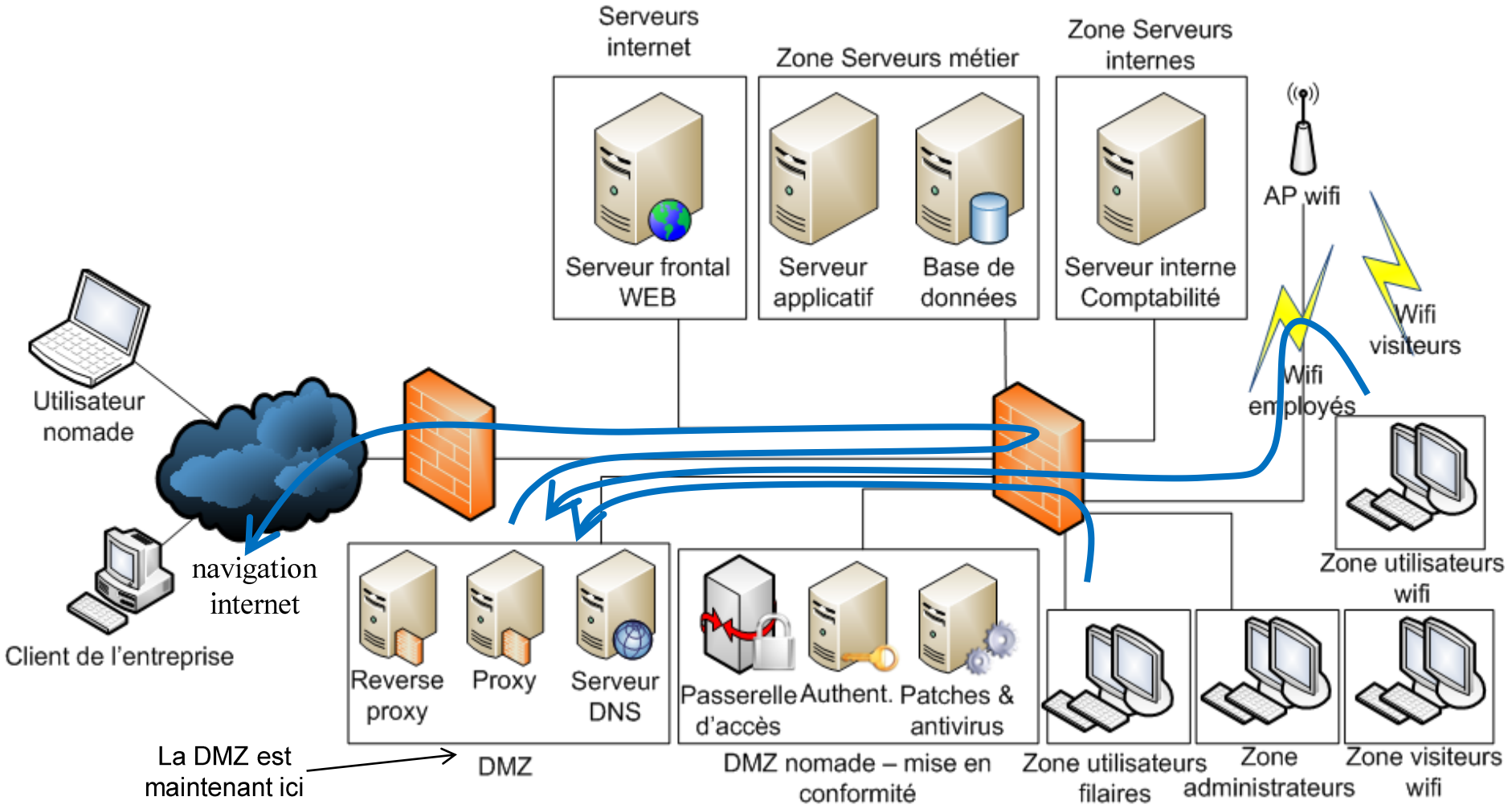
- Réponse question 5 :

- Mise en place d'un proxy pour analyser les flux sortants
  - Le proxy est en frontal d'Internet
  - Le proxy est donc placé dans la DMZ
  - Les postes de travail ne sont plus connectés directement à Internet

- Définition de la politique de filtrage des flux sortants
  - Définir les catégories de sites WEB pour lesquels les employés ont la permission de naviguer
  - Implémenter une liste blanche ou noire de sites autorisés/interdits

Exercices de sécurité réseau

- Réseau avec un proxy en coupure des flux vers Internet



Exercices de sécurité réseau

- Question 6 : Quelle solution proposez-vous pour filtrer les flux entrants ?

Exercices de sécurité réseau

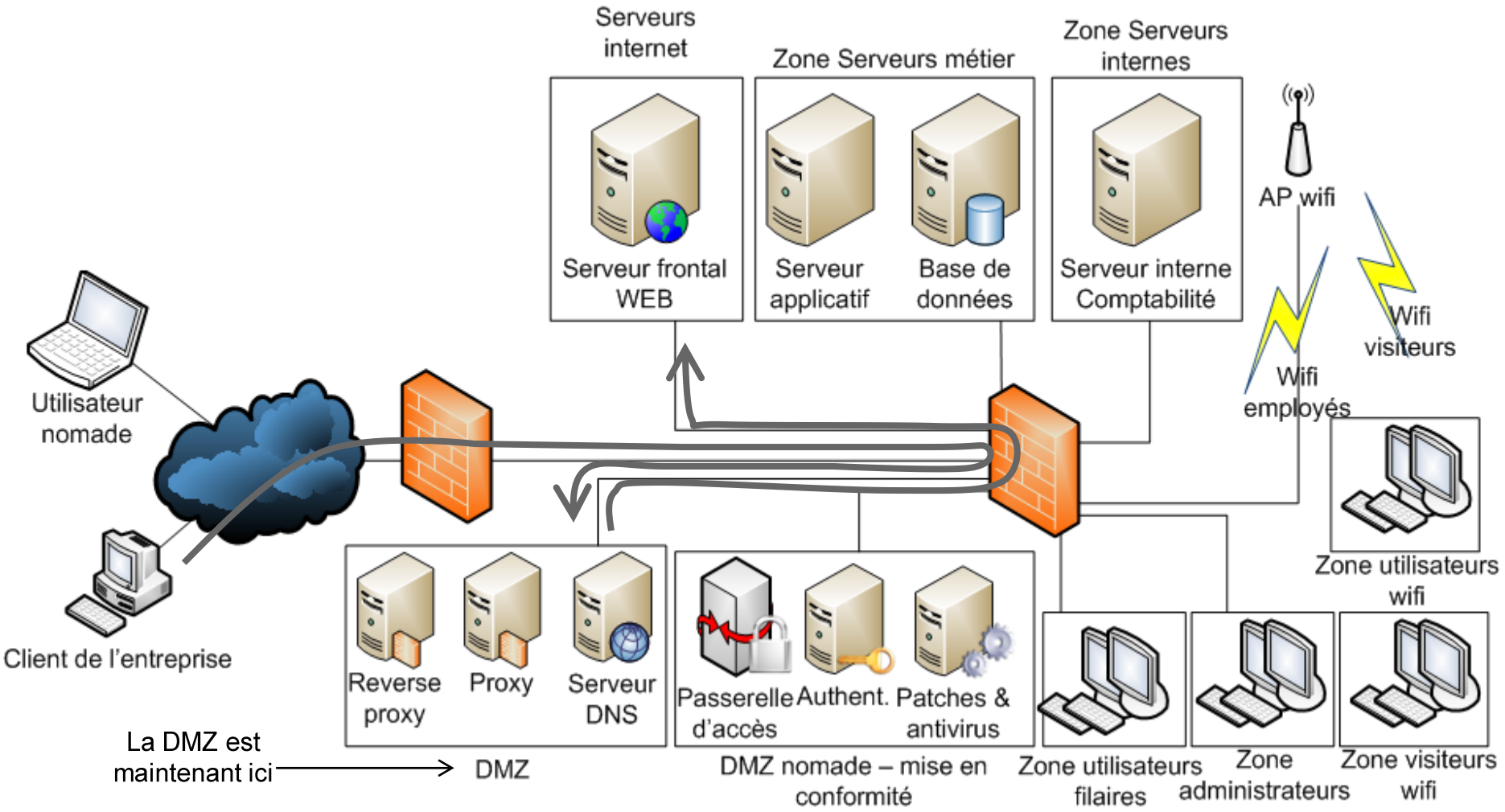
- Réponse question 6 :

- Mise en place d'un reverse-proxy pour analyser les flux entrants
  - Le reverse-proxy est maintenant en frontal
  - Le serveur WEB n'est plus connecté directement sur Internet

- Politique de filtrage des flux entrants
  - Le reverse-proxy analyse les requêtes WEB d'internet vers le serveur de e-commerce
  - Blocage des requêtes non autorisées
  - Deep Packet Inspection pour intercepter les requêtes malveillantes (SQL injection, malware, etc.)

Exercices de sécurité réseau

- Réseau avec un reverse-proxy en coupure des flux entrants



POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

A la semaine prochaine