CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Sensibilisation et initiation à la cybersécurité

Module 3 : les aspects réseau et applicatifs

1. **La sécurité du protocole IP**
2. **Sécurisation d'un réseau**

1. La sécurité du protocole IP

a) Préambule
b) Exemple d’attaque par réflexion
c) Exemples d’écoute de trafic
d) Exemple de modification du routage des datagrammes IP
e) Sécurisation du protocole IP

1. La sécurité du protocole IP

a. Préambule

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.**

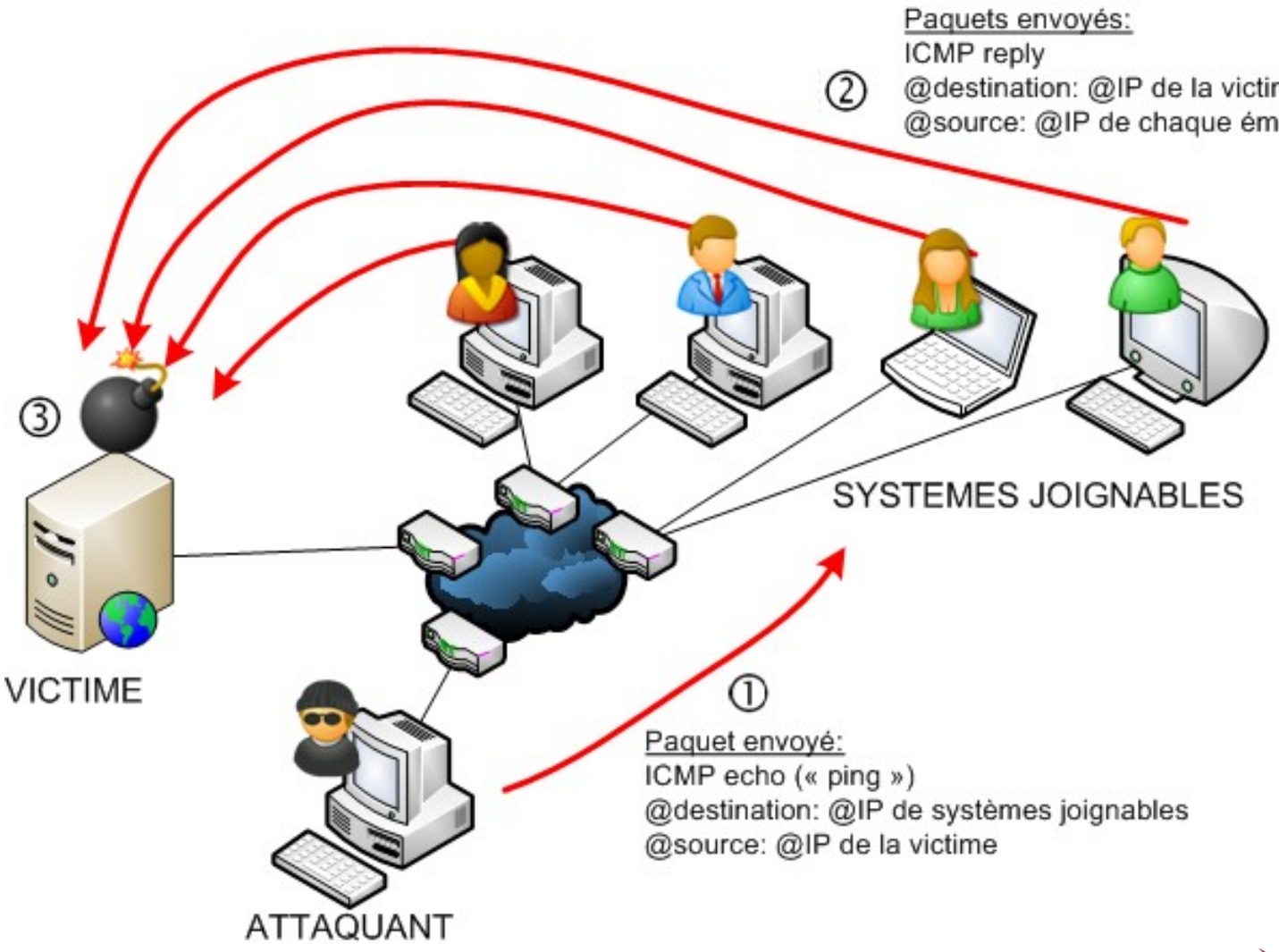
Quelques exemples de faiblesses de ces protocoles

- **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.

1. La sécurité du protocole IP

b. Exemple d'attaque par réflexion



1. La sécurité du protocole IP

b. Exemple d'attaque par réflexion

But de l'attaque

- porter atteinte aux performances d'un système cible (déni de service).

Quelles sont les caractéristiques de l'attaque ?

- usurpation d'adresse IP ;
- réflexion de trafic en ayant recours à des systèmes tiers « innocents ».

Séquences de l'attaque

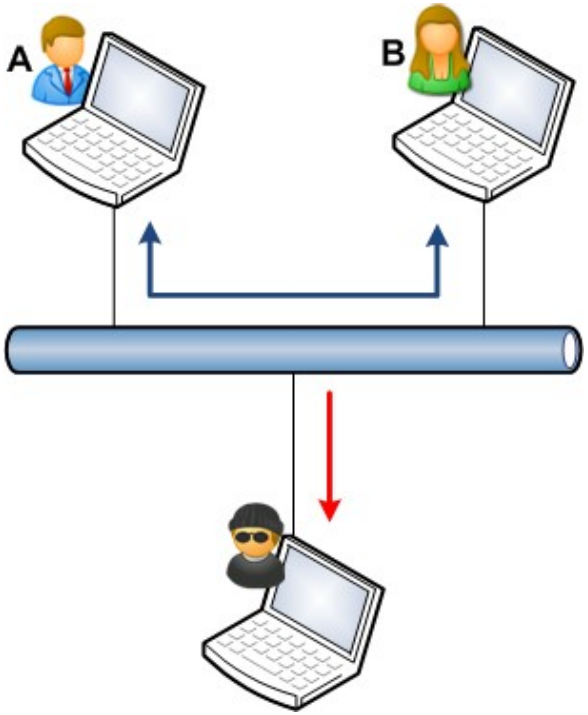
① Un attaquant envoie des paquets PING à des systèmes tiers joignables en indiquant l'@IP de la future victime comme @IP source ;

② Chaque système pense ainsi recevoir un PING de la part d'un système distant, et chacun va répondre à ce PING ;

③ Avec suffisamment de ressources, l'attaquant sera en mesure de faire générer suffisamment de trafic pour affecter les performances de la victime.

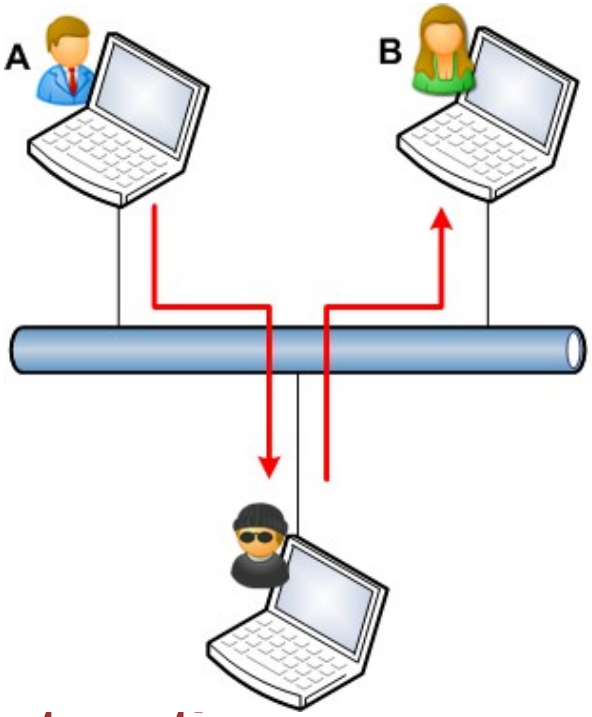
1. La sécurité du protocole IP

c. Exemples d'écoute de trafic



Ecoute passive

L'attaquant est en mesure d'écouter les conversations entre A et B (atteinte à la ***confidentialité*** des échanges).

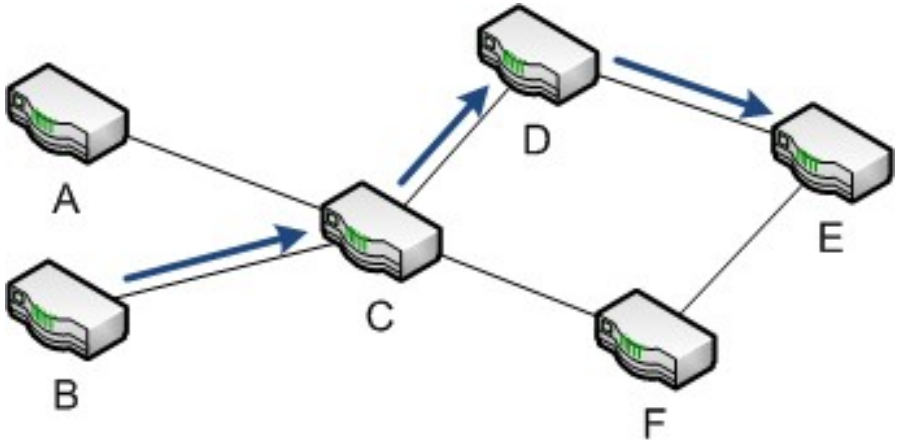


Ecoute active

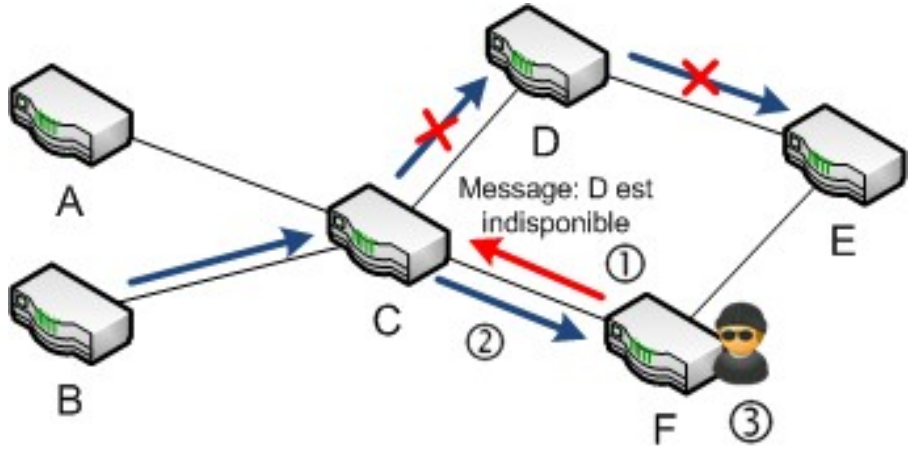
L'attaquant est en mesure de s'insérer dans la conversation entre A et B sans que ceux-ci le sachent (atteinte à la ***confidentialité*** et à l'***intégrité*** des échanges).

1. La sécurité du protocole IP

d. Exemple de modification du routage des datagrammes IP



Chaque routeur possède une table de routage qui indique vers quel routeur voisin transmettre les datagrammes. Cette table peut être mise à jour dynamiquement en fonction des évènements réseaux (protocoles BGP, RIP, OSPF, etc.).



But de l'attaque : **dérouter les paquets** à destination du réseau E, vers le réseau F maitrisé par l'attaquant.

Méthode :

① L'attaquant utilise une faiblesse du protocole de routage pour indiquer au routeur C que le routeur D est indisponible, et que le routeur F peut router les paquets vers E ;

② le routeur C transfère donc à F les paquets pour E, afin qu'ils puissent être routés à destination ;

③ Selon le but visé par l'attaquant, celui-ci peut décider de router ou non les paquets vers E.

1. La sécurité du protocole IP

e. Sécurisation du protocole IP

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.

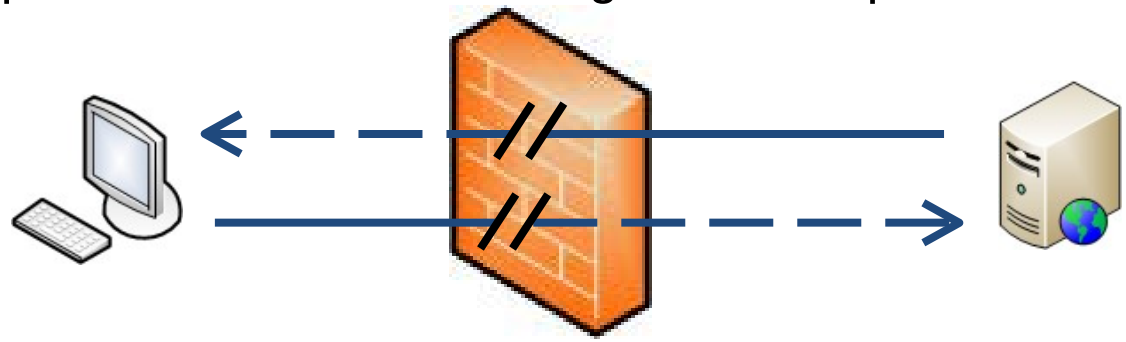
2. Sécurisation d’un réseau

a) Pare-feu
b) Répartiteur de charge
c) Anti-virus
d) IDS et IPS
e) VPN
f) Segmentation
g) Exemple pratique de sécurisation avec un réseau simple

2. Sécurisation d'un réseau

a. Pare-feu

- **Équipement en coupure entre 2 ou plusieurs réseaux ;**
- Inspecte les paquets réseaux entrants et sortants d'un réseau à l'autre ;
- Implémente un **mécanisme de filtrage basé sur des règles :** il ne transmet donc que les paquets réseaux qui respectent les règles de filtrage implémentées dans la configuration du pare-feu.



Pour chaque flux entrant ou sortant, le pare-feu interroge ses règles de filtrage pour déterminer s'il doit laisser le paquet réseau ou non.

2. Sécurisation d'un réseau

a. Pare-feu

Règles de filtrage :

- Historiquement, elles étaient basées sur les couches basses de la pile protocolaire (réseau, transport), et portaient uniquement sur les paramètres comme les adresses IP et les ports TCP/UDP ;
- Les pare-feu sont également capables de filtrer selon les données de la **couche applicative** (protocole et contenu des données). Ex. : HTTP, SMTP, DNS, etc.
  - Les **proxy et reverse-proxy peuvent être vus comme des pare-feu applicatifs dédiés**. Ils permettent **d'analyser finement** les flux applicatifs (par exemple la navigation web des utilisateurs ou les flux web entrants sur un server de e-commerce).
- Un anti-virus ou un mécanisme de détection d'intrusion peuvent également être implémentés sur le pare-feu de façon à détecter un malware en transit ou certaines attaques.

Avantage sécurité :

- L'exploitant d'un réseau peut donc restreindre le trafic entrant et sortant aux seules connexions qu'il estime légitime. Toutes les autres connexions sont donc bloquées.

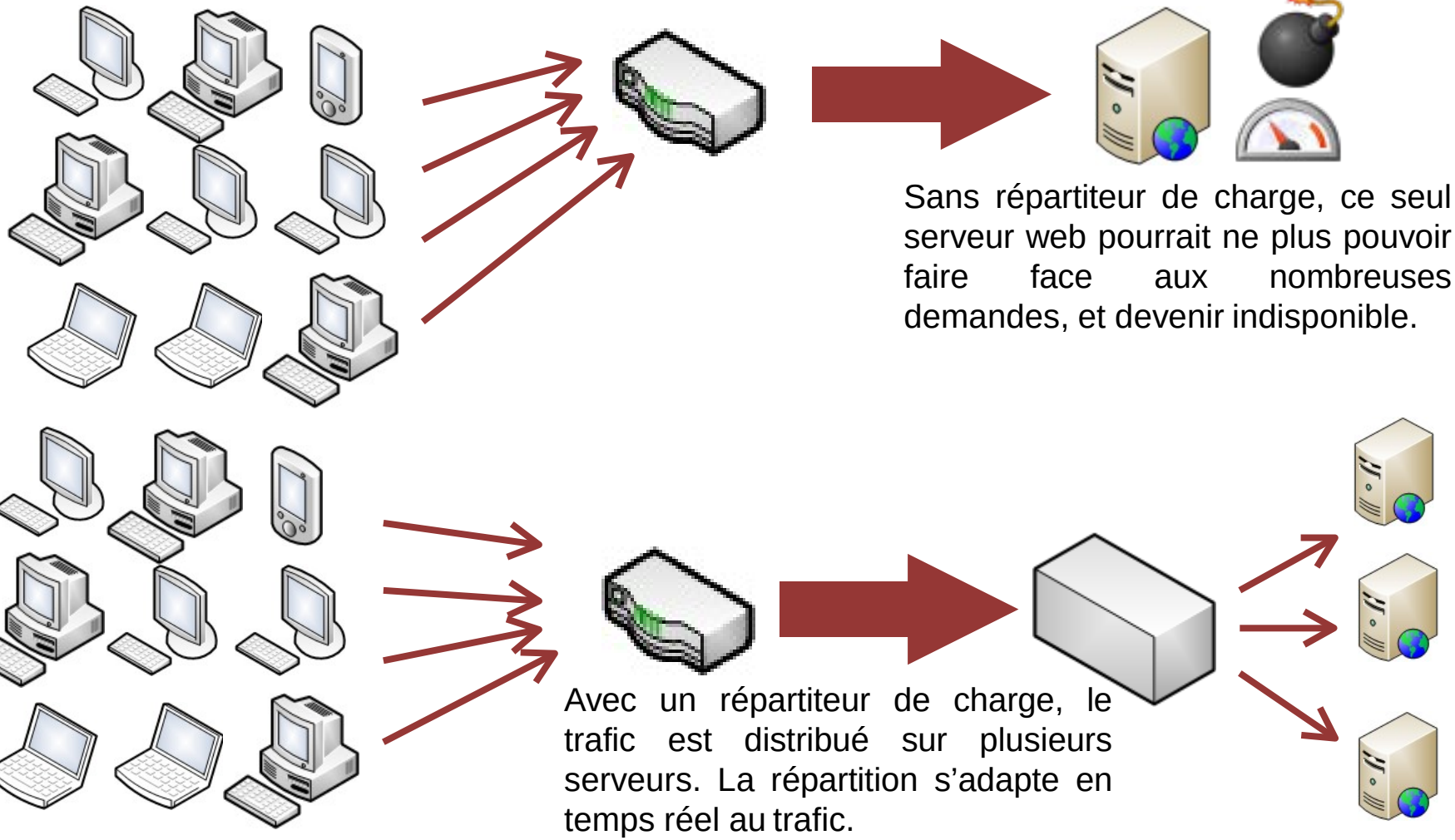
2. Sécurisation d'un réseau

b. Répartiteur de charge

- « Load-balancer » en anglais ;
- Équipement rencontré sur les grosses infrastructures où les serveurs doivent faire face à de très fortes bandes passantes et charges élevées de trafic ;
- Équipement chargé de **répartir/distribuer la charge réseau** en fonction des caractéristiques de celui-ci et de la disponibilité des serveurs ;
- Avantage sécurité : permet de mieux se protéger contre les **dénis de service distribués.**

2. Sécurisation d'un réseau

b. Répartiteur de charge



Sans répartiteur de charge, ce seul serveur web pourrait ne plus pouvoir faire face aux nombreuses demandes, et devenir indisponible.

Avec un répartiteur de charge, le trafic est distribué sur plusieurs serveurs. La répartition s'adapte en temps réel au trafic.

2. Sécurisation d'un réseau

c. Anti-virus

Logiciel chargé de détecter et stopper les **malware connus :**

- Virus, vers, *keylogger* (enregistreur de frappe), chevaux de Troie, etc.

- Ces logiciels fonctionnent en général avec une base de données qui contient les signatures des malware connus. Ils analysent en permanence les fichiers et les exécutables du système hébergeant l'anti-virus ;

- **Limite des anti-virus :** ils ne détectent (en général) que les malware déjà répertoriés par les éditeurs. Ainsi, les nouveaux virus ou les malware ciblés ne sont souvent pas détectés. D'autre part, il est impératif que l'anti-virus soit mis à jour quotidiennement.

2. Sécurisation d'un réseau

d. IDS et IPS

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

Les IDS/IPS demandent un 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) ;
- De plus, les IDS/IPS basés sur des signatures ne peuvent détecter que les intrusions dont les caractéristiques techniques sont déjà connues et référencées.

2. Sécurisation d'un réseau

e. VPN

VPN **V**irtual **P**rivate **N**etwork

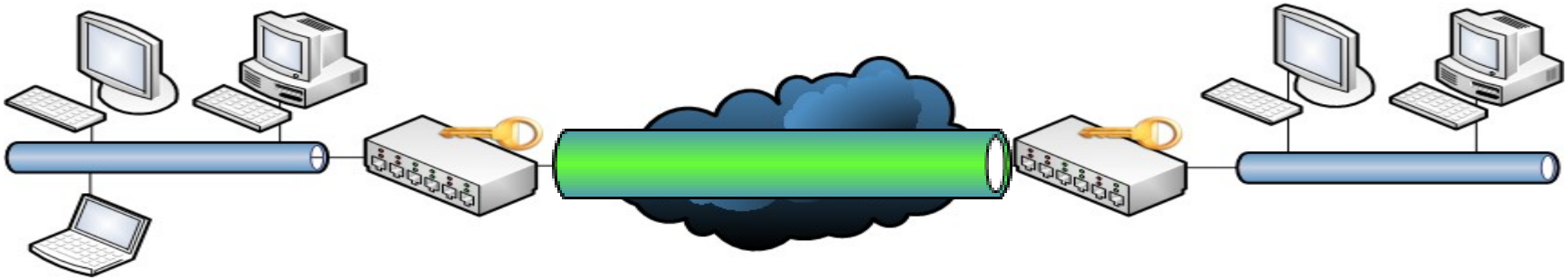
Un VPN est un **réseau virtuel** qui permet à **deux réseaux distants de communiquer en toute sécurité**, y compris si la communication s'effectue via des réseaux inconnus et auxquels nous ne faisons pas confiance.

Solution : grâce à des mécanismes cryptographiques, appliquer un **chiffrement des données, ainsi qu'un motif d'intégrité, à tous les flux entre les 2 sites**. On obtient ainsi un **tunnel virtuel** qui ne contient que des données chiffrées et protégées en intégrité :

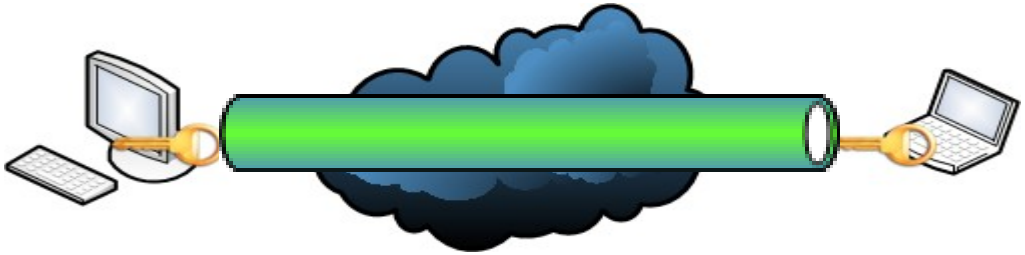
- Les données qui passent sur Internet sont donc chiffrées et non compréhensibles par un attaquant qui écouterait les flux ;
- En cas de modification malveillante des flux, le mécanisme d'intégrité permettra au destinataire de déterminer que les données reçues ne sont pas intègres, et qu'il ne faut donc pas traiter ces données.

2. Sécurisation d'un réseau

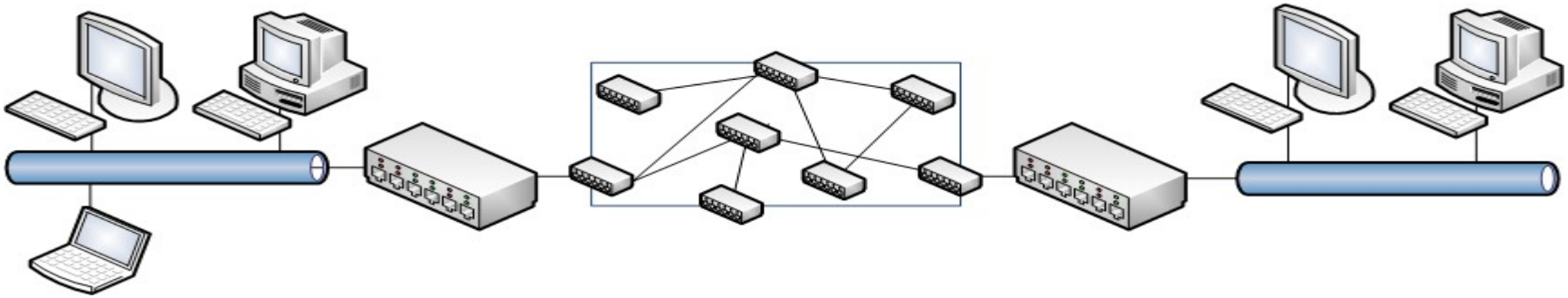
e. VPN



VPN de site à site, dont le tunnel est géré par les routeurs : IPsec – au niveau de la couche Internet



VPN entre systèmes : TLS – au niveau de la couche Transport



Réseau opérateur MPLS, dont le cœur est inaccessible aux clients se connectant sur ce réseau

2. Sécurisation d’un réseau

f. Segmentation

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.

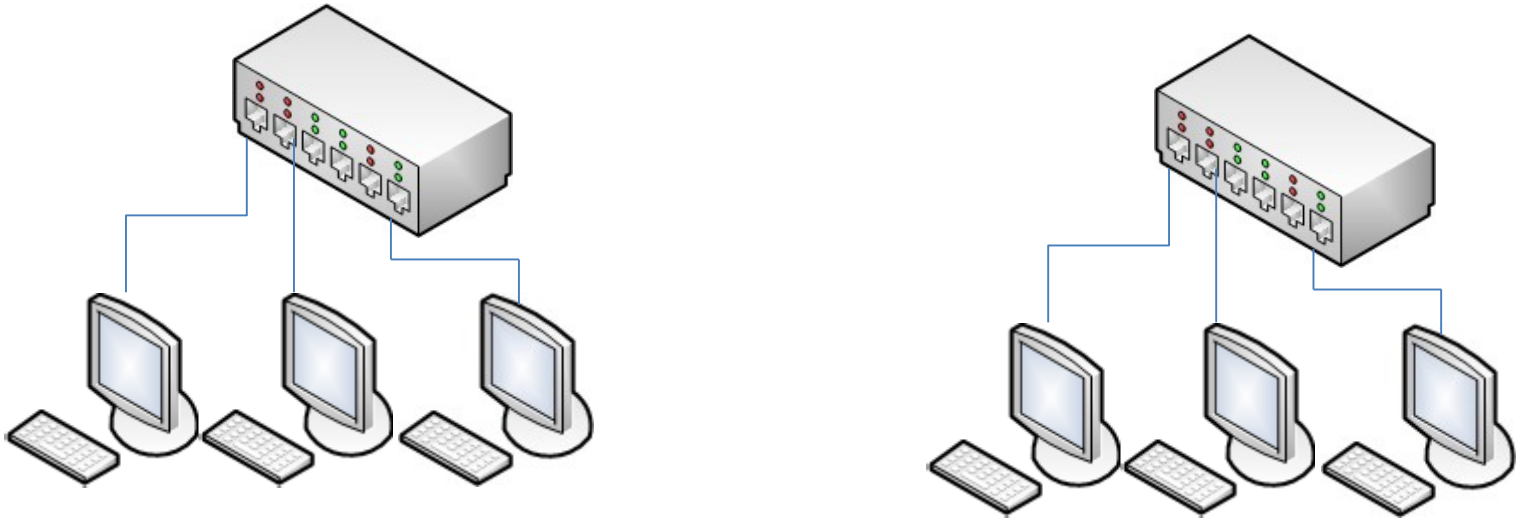
Appliqué au domaine réseau, il est donc fait **recours à de la segmentation** afin de séparer le réseau en différentes zones.

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

2. Sécurisation d'un réseau

f. Segmentation

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.

2. Sécurisation d'un réseau

f. Segmentation

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

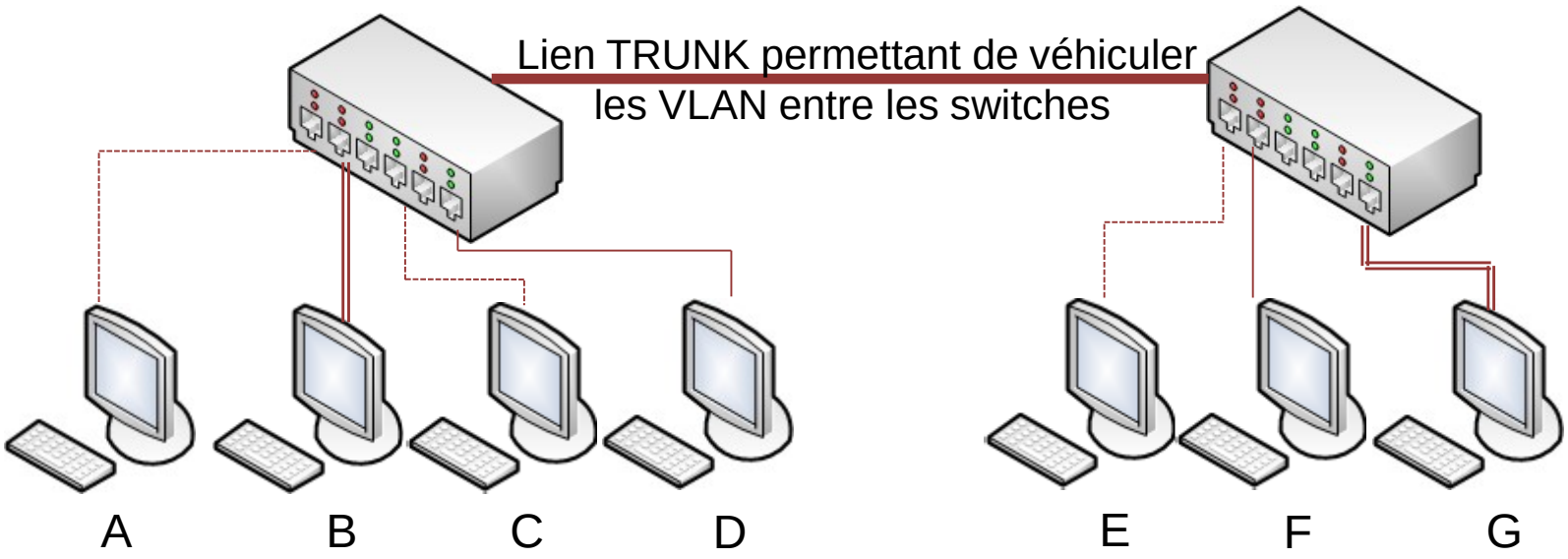
Les VLAN sont des **réseaux virtuels implémentés par les switches**. Ceux-ci **restreignent la communication entre systèmes selon des règles configurées** sur l'équipement réseau :

- 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 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.

2. Sécurisation d'un réseau

f. Segmentation



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.

2. Sécurisation d'un réseau

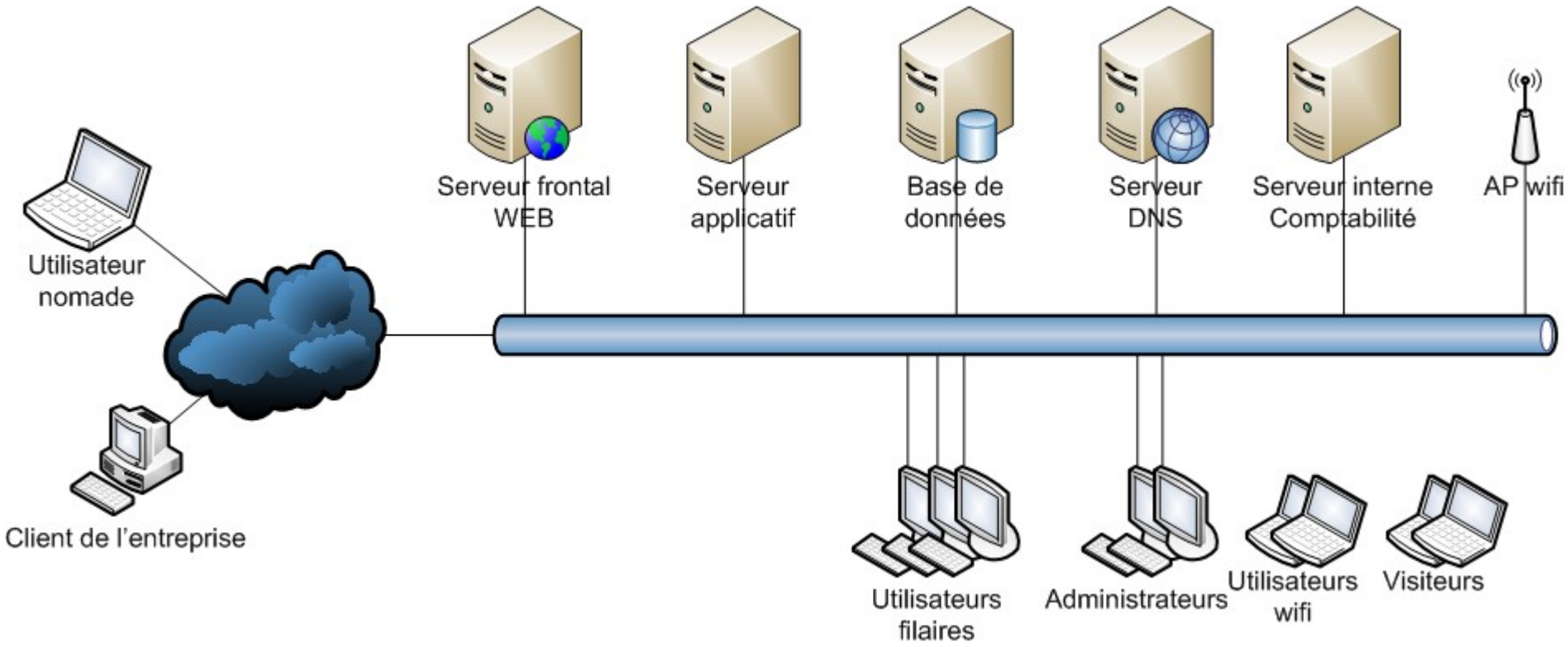
g. Exemple pratique de sécurisation avec un réseau simple

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.

2. Sécurisation d'un réseau

g. Exemple pratique de sécurisation avec un réseau simple



Réseau « à plat », avant sécurisation

2. Sécurisation d'un réseau

g. 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.

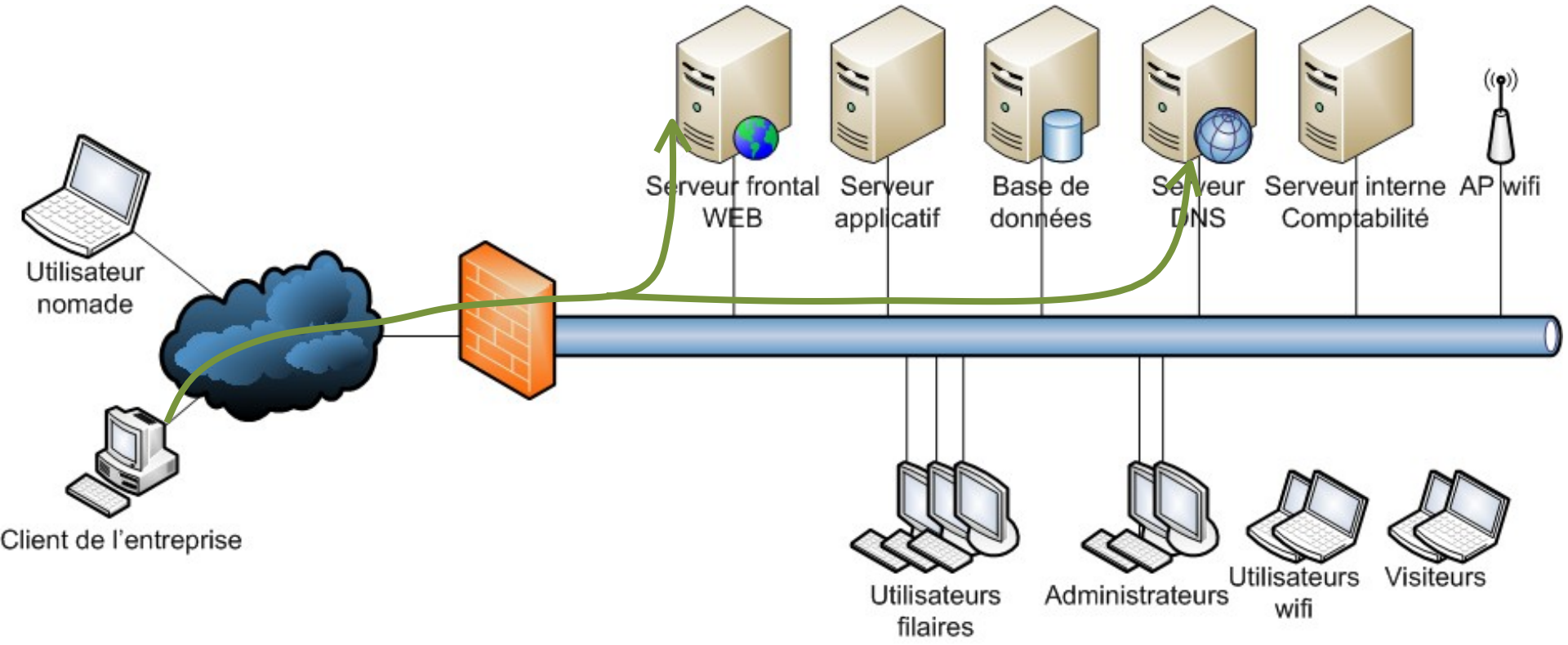
Parmi les nombreuses faiblesses architecturales de ce réseau, nous pouvons identifier au moins le problème suivant :

- 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.

2. Sécurisation d'un réseau

g. Exemple pratique de sécurisation avec un réseau simple



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

2. Sécurisation d'un réseau

g. 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 :

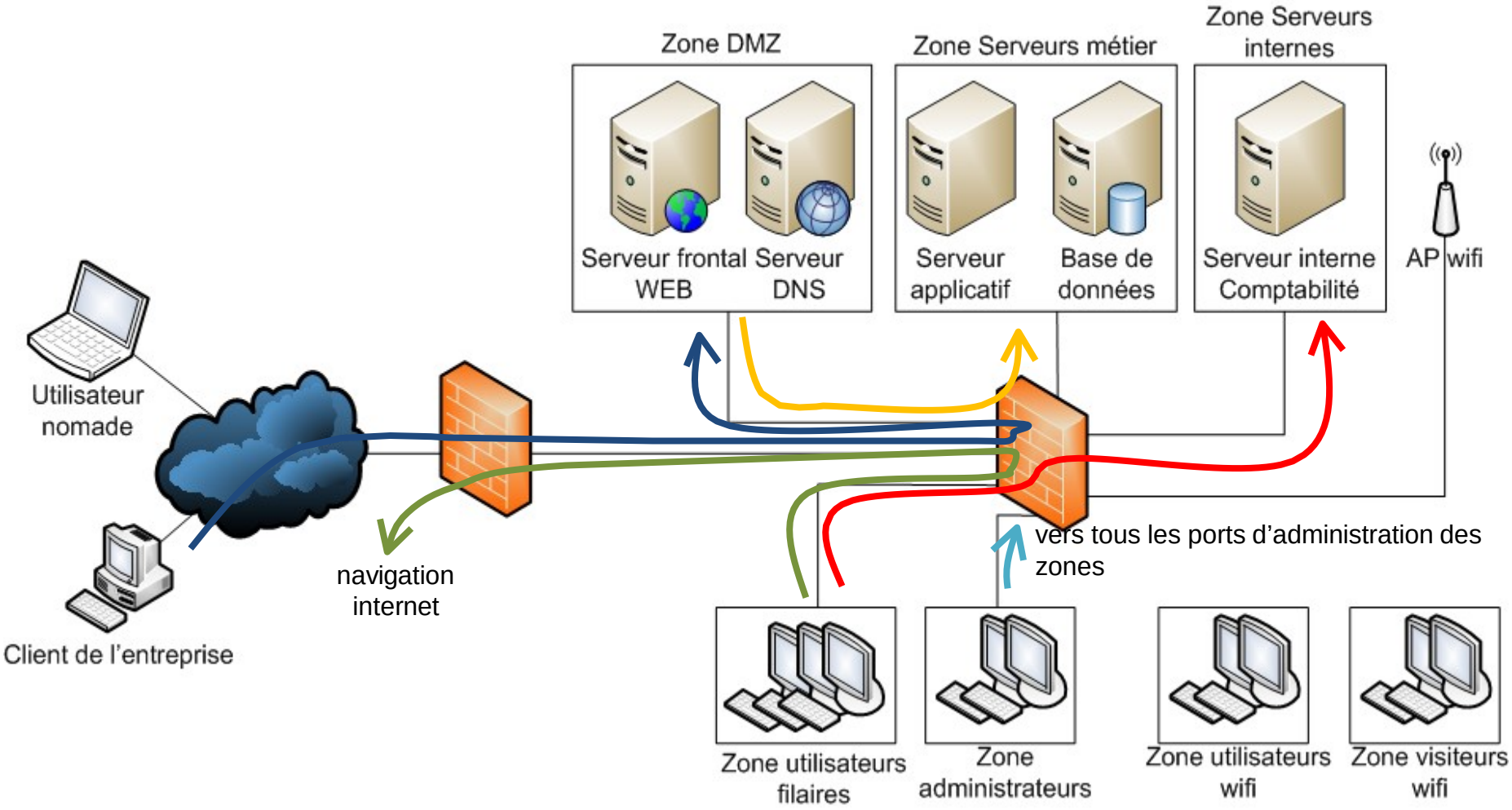
- Une **DMZ (zone démilitarisée)** destinée à héberger tous les serveurs qui doivent être accessibles depuis internet, et uniquement ceux-ci. Ainsi, en cas de faille dans le serveur web, un attaquant aurait plus de difficultés pour rebondir sur le réseau interne ;
- Une zone destinée aux **serveurs internes**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

2. Sécurisation d'un réseau

g. Exemple pratique de sécurisation avec un réseau simple

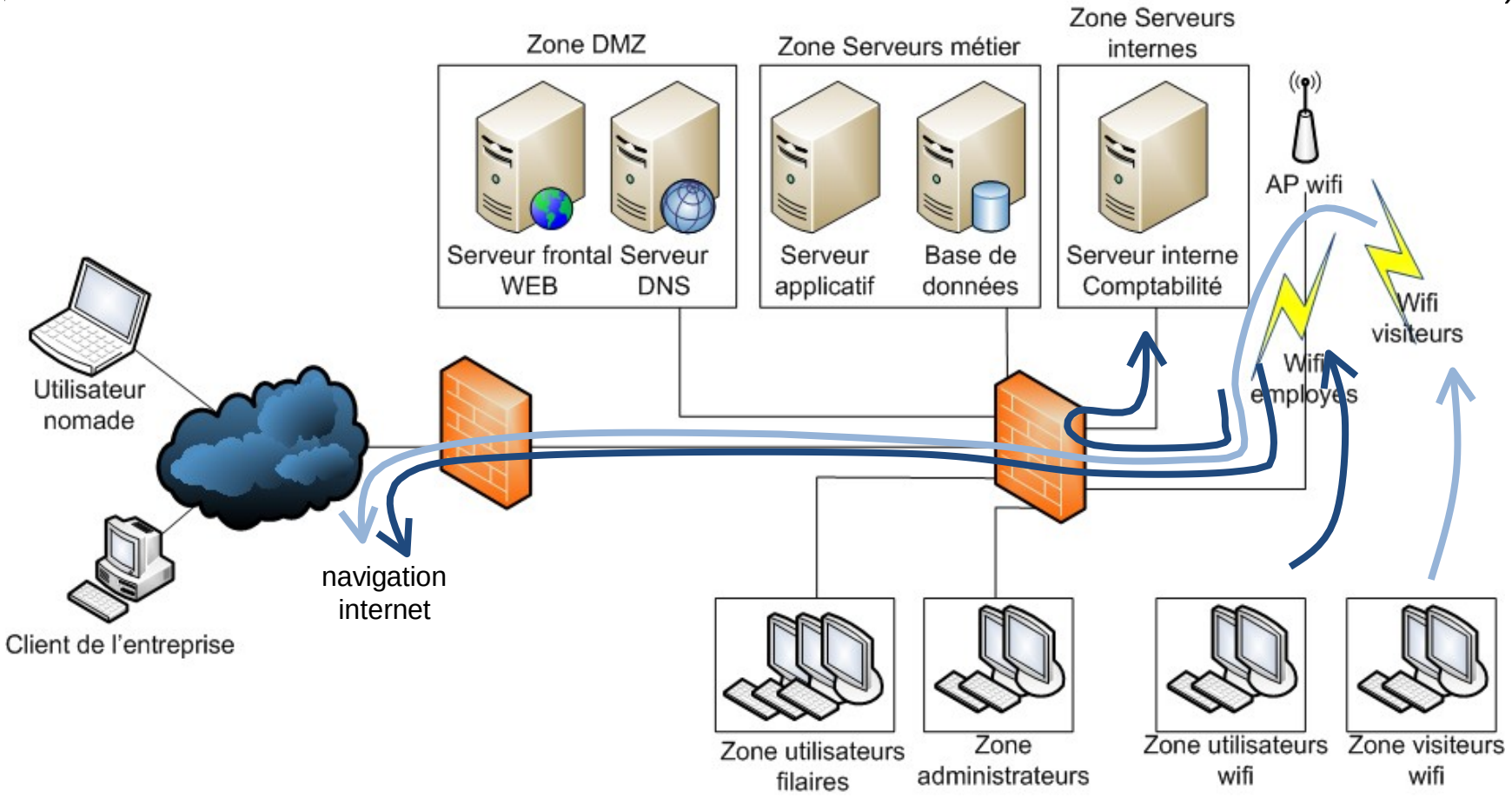


Réseau avec des zones segmentées, et un filtrage systématique via le pare-feu, y compris pour les flux internes.

2. Sécurisation d'un réseau

g. 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.

2. Sécurisation d'un réseau

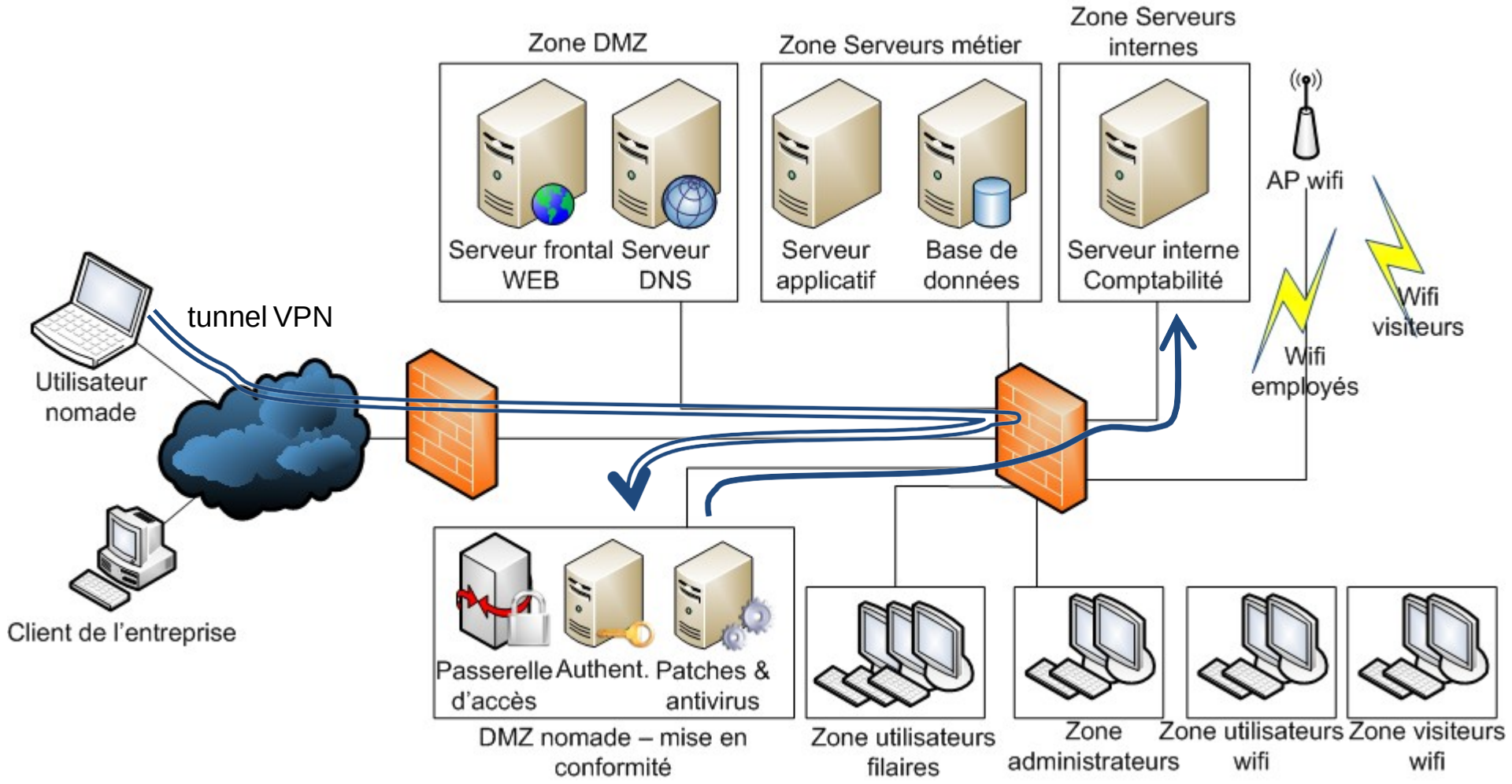
g. Exemple pratique de sécurisation avec un réseau simple

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**.

2. Sécurisation d'un réseau

g. Exemple pratique de sécurisation avec un réseau simple



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

2. Sécurisation d'un réseau

g. Exemple pratique de sécurisation avec un réseau simple

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

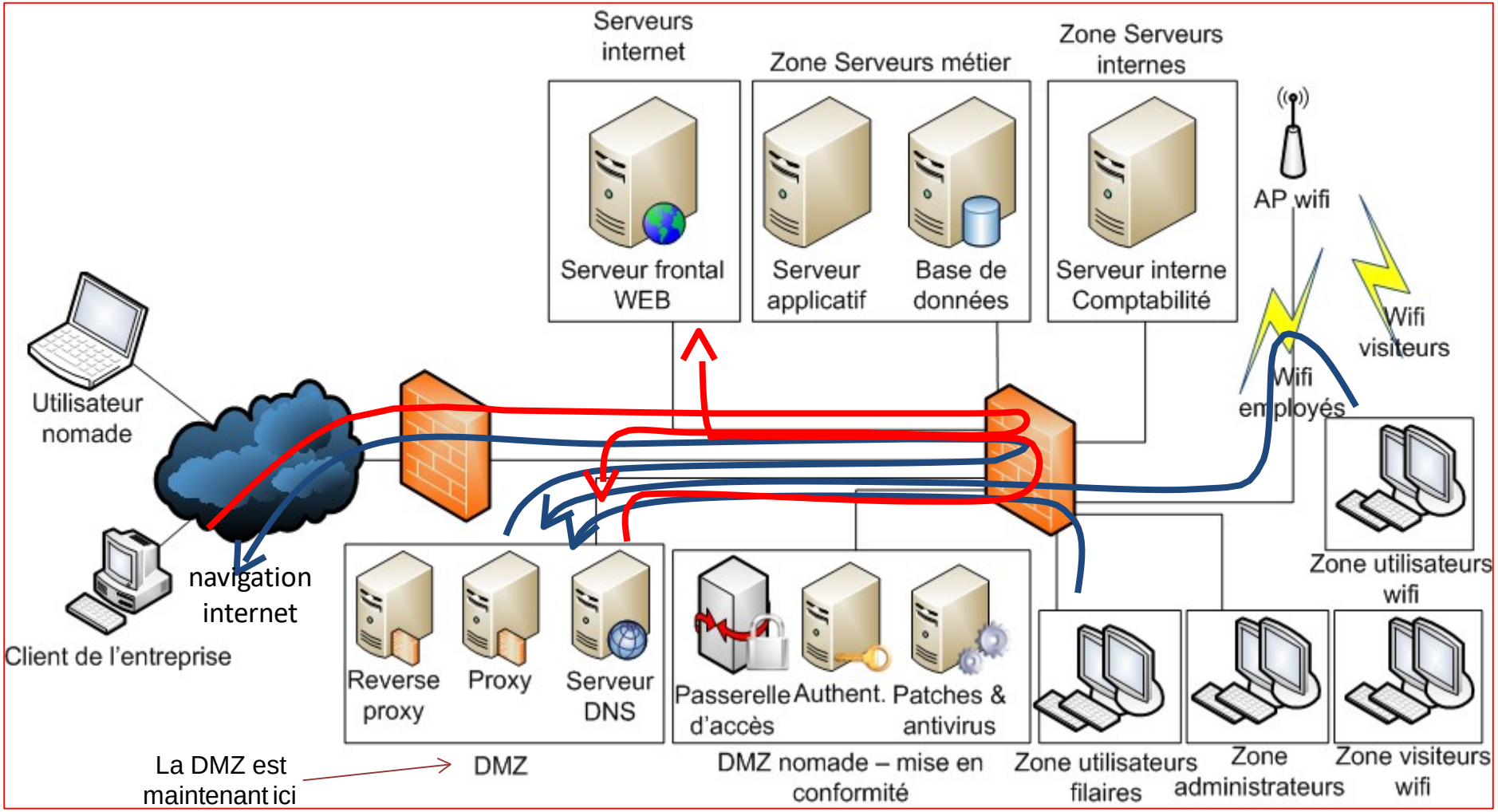
- **Trafic sortant** : définir les catégories de sites WEB que les employés sont autorisés à naviguer, implémenter une liste blanche ou noire de sites autorisés/interdits ;
- **Trafic entrant** : analyser les requêtes WEB d'internet vers le serveur de e-commerce afin d'intercepter les requêtes malveillantes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

2. Sécurisation d'un réseau

g. Exemple pratique de sécurisation avec un réseau simple



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