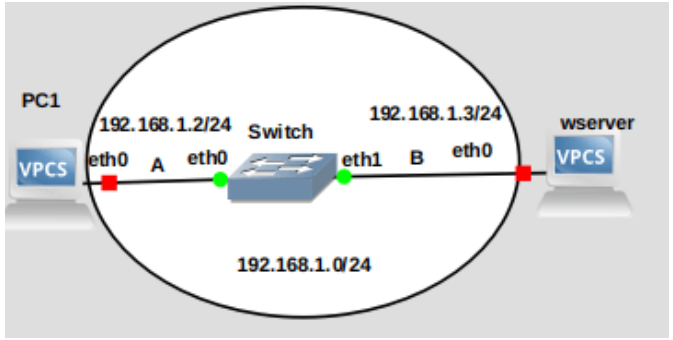
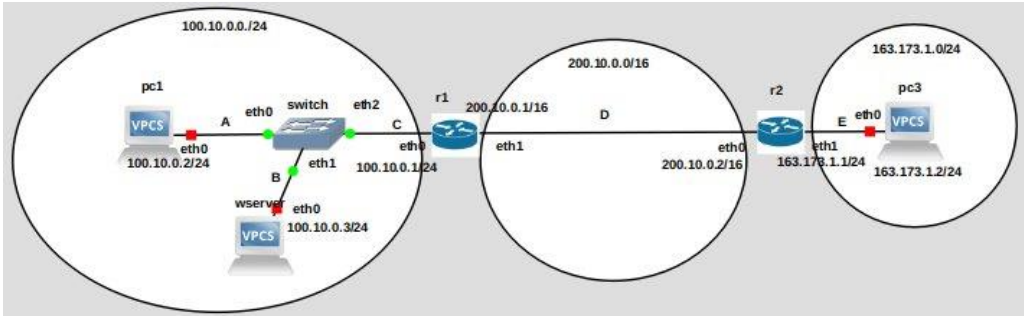
Session 4 – Solution de sécurisation d'un réseau d'entreprise

Bilan de la session 3 – exercice 2



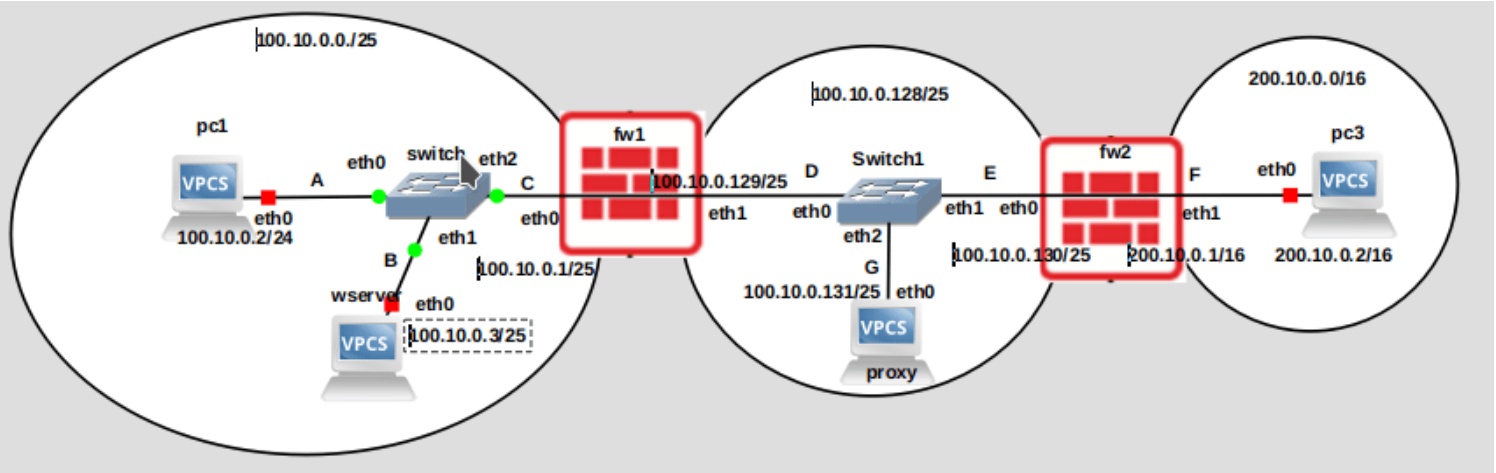
- Vous avez :
  - déployé sur wserver un code python correspondant à un serveur Web
  - déployé sur pc1 un code client correspondant à un client http
  - analysé les tables de commutation du pont entre pc1 et wserver
  - sniffé puis visualisé les communications (paquets http échangés) entre wserver et pc1 grace à wireshark
- **Aucune sécurité particulière pour protéger wserver, pc1, switch et se prémunir d'attaques**

Bilan de la session 3 – exercice 3



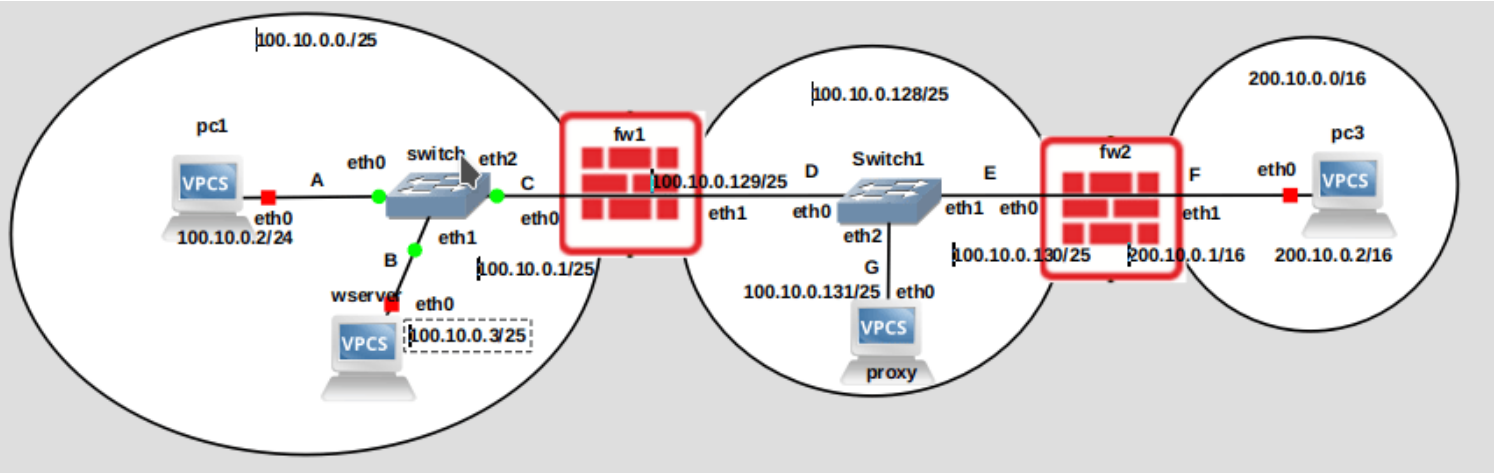
- Vous avez :
  - Interconnecté plusieurs réseau dont le réseau 100.10.0.0/24 qui contenait pc1 et wserver
  - Configuré les tables de routages de r1 et r2 pour que ces derniers fassent suivre le trafic entre les différents réseaux
  - **Aucune sécurité particulière pour protéger wserver, pc1, switch, pc3 et se prémunir d'attaques**
  - **Si le réseau 100.10.0.0/24 était celui d'une entreprise et wserver son serveur Web, comment protégeriez-vous les équipements (PCs de l'entreprise, son serveur web) ?**

Session 4 - Sécuriser le réseau d'une entreprise



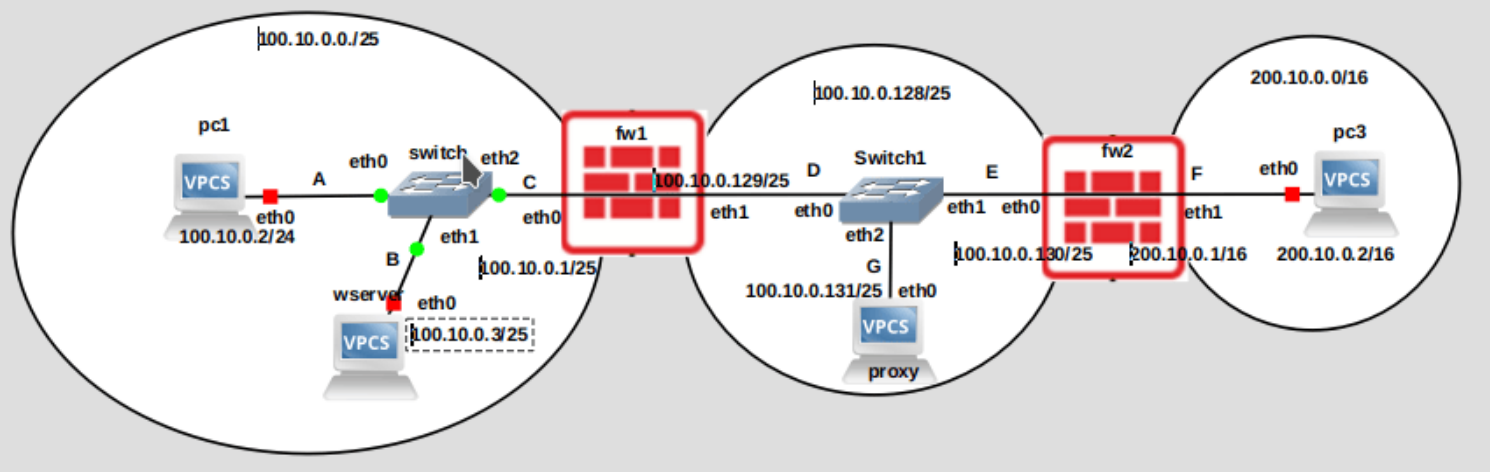
- **Exercice 1 :**
- dans **l'intranet de l'entreprise** (réseau 100.10.0.0/25), vous allez déployer sur wserver un serveur Apache (serveur open source **http**) et y déployer une page web
  - Vous allez configurer fw1 et fw2 qui sont deux routeurs
  - Vous allez par la suite tenter de **protéger l'intranet de l'entreprise** : pc1 et aussi et surtout le **serveur apache wserver** qui est une cible de choix

Session 4 - Sécuriser le réseau d'une entreprise



- Exercice 2 :
  - Dans le sous-réseau 100.10.0.128/25 **de l'entreprise** vous allez déployer un **reverse proxy** nginx qui :
    - reçoit les requêtes des clients et les redirige vers le serveur Web apache (ici wserver), puis, retourne la réponse du serveur Web aux clients comme si elle provenait directement de lui-même
    - wserver ne sera plus visible/directement accessible depuis l'internet où se trouve pc3

Session 4 - Sécuriser le réseau d'une entreprise



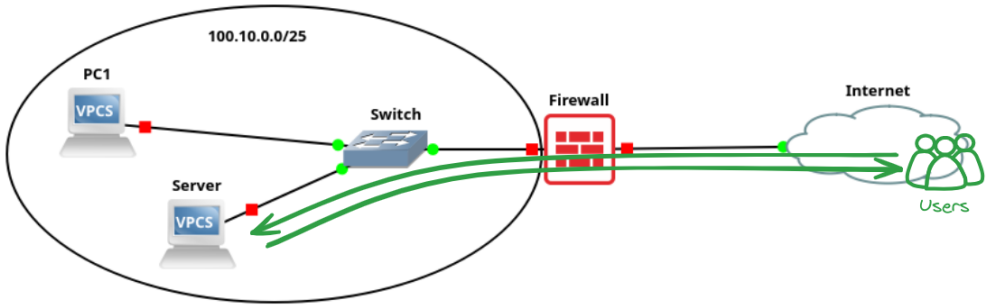
- Exercice 3 : fw1 et fw2 sont deux routeurs jouant le rôle de **firewall qui** ne font pas suivre aveuglement des paquets mais les **filtrent**
  - **Quel est l'intérêt d'avoir deux firewalls ?**

Session 4 - Sécuriser le réseau d'une entreprise

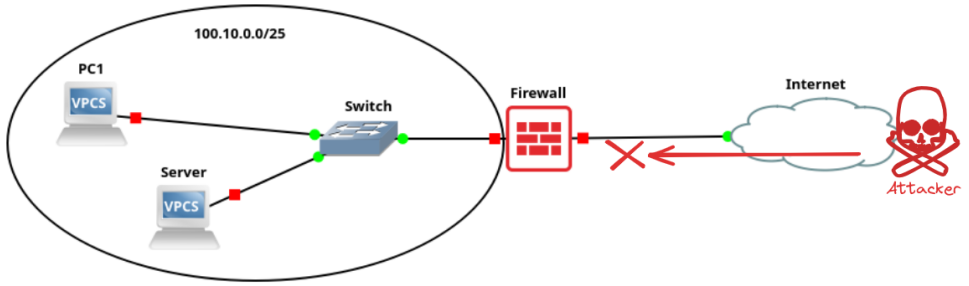
Solution 1 : un seul firewall de niveau 3 applique des règles pour définir quelles sont les communications autorisées en se basant sur :

- Le type de connexion, l'origine et/ou la destination de la connexion, le protocole, le port utilisé, l'« historique » de la connexion...

Connexion acceptée par le firewall



Connexion refusée par le firewall

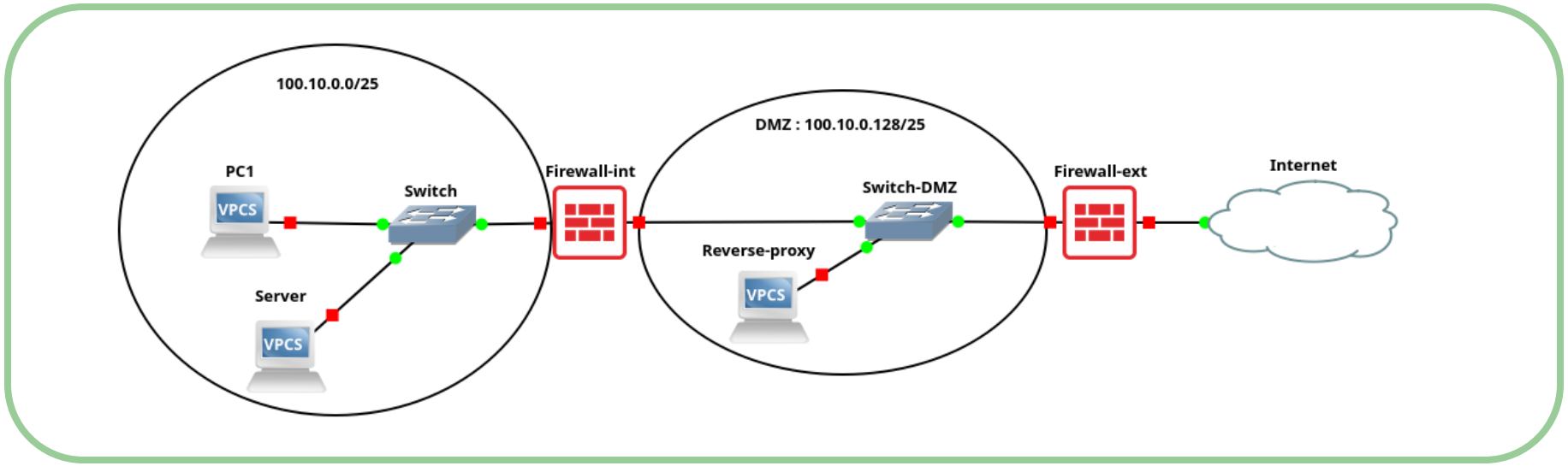


Session 4 - Sécuriser le réseau d'une entreprise

Solution 2 avec une zone démilitarisée ou DMZ = le réseau 100.10.0.128/25 est isolé à l'aide de **deux firewalls** ; la DMZ est destinée à **héberger des serveurs et services** accessibles depuis l'internet :

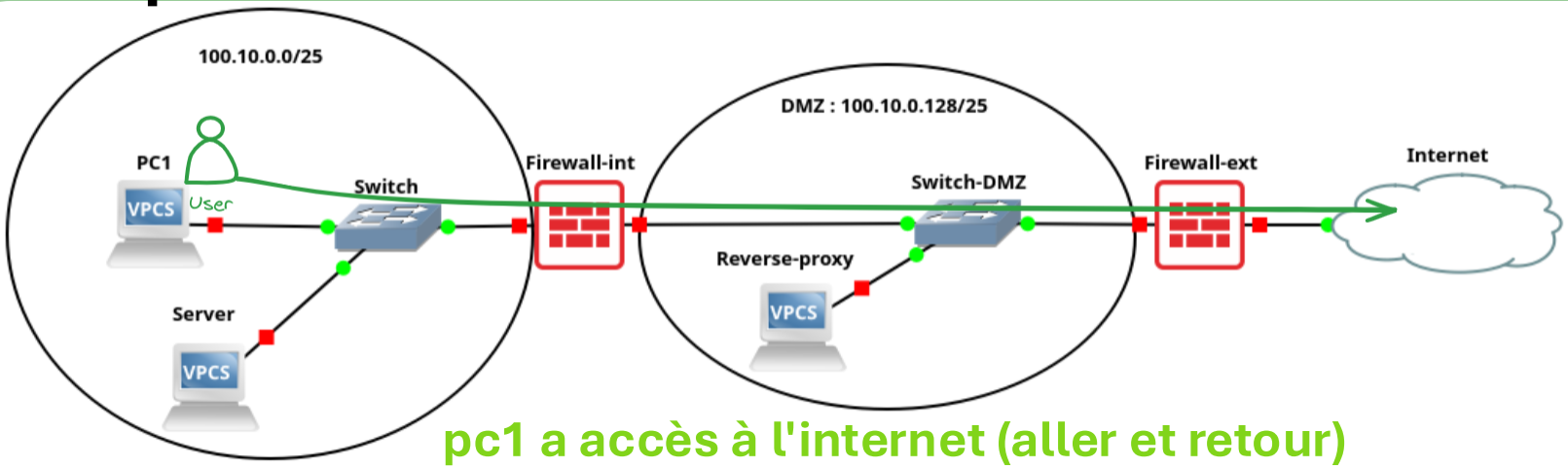
- Exemple : serveurs apache, serveurs DNS, reverse proxy, plus généralement serveur front...

Les serveurs de la DMZ « peu » critiques sont attaqués alors que les serveurs critiques en backend de l'intranet sont épargnés

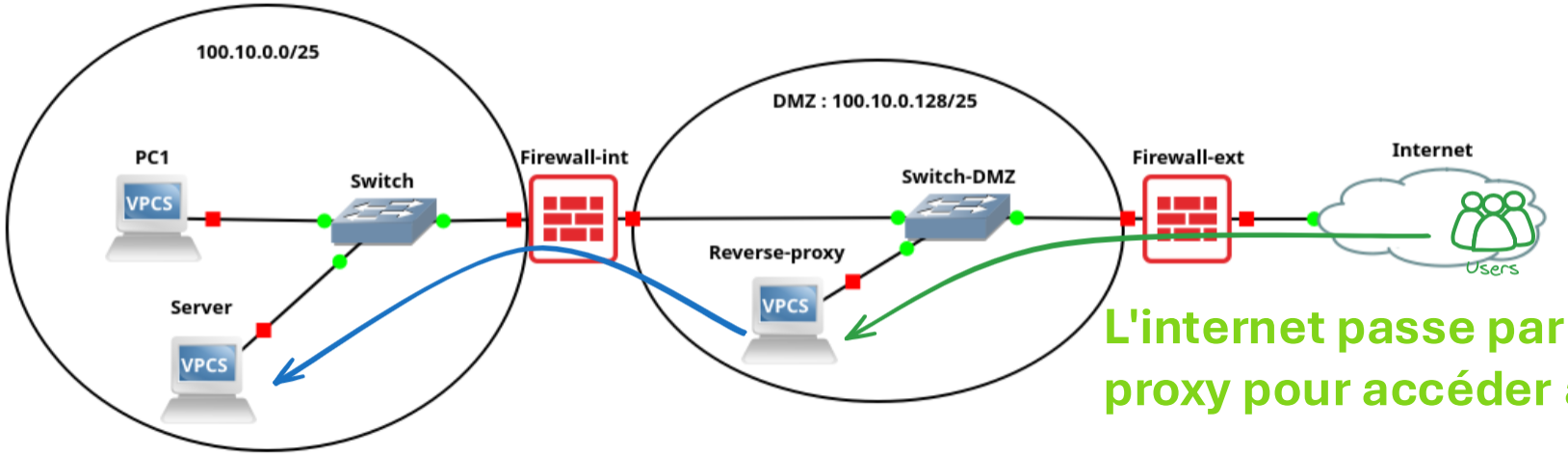


Session 4 - Sécuriser le réseau d'une entreprise

Flux acceptés par les firewalls



pc1 a accès à l'internet (aller et retour)

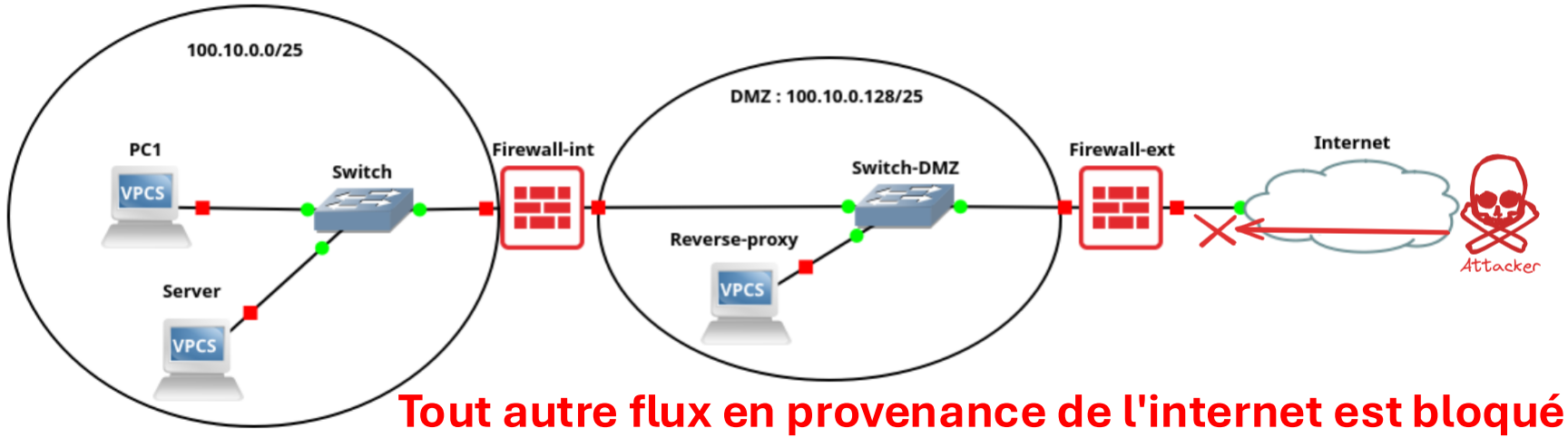


L'internet passe par un reverse proxy pour accéder au serveur

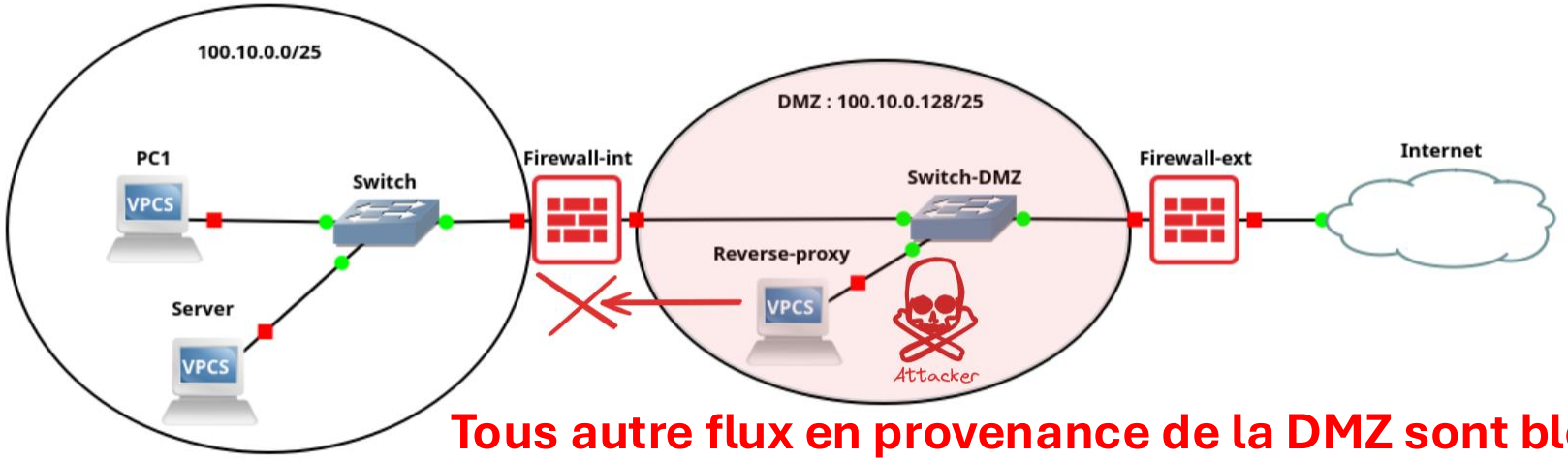
les flux http du reverse proxy vers server (aller retour) sont acceptés

Session 4 - Sécuriser le réseau d'une entreprise

Flux bloqués par les firewalls



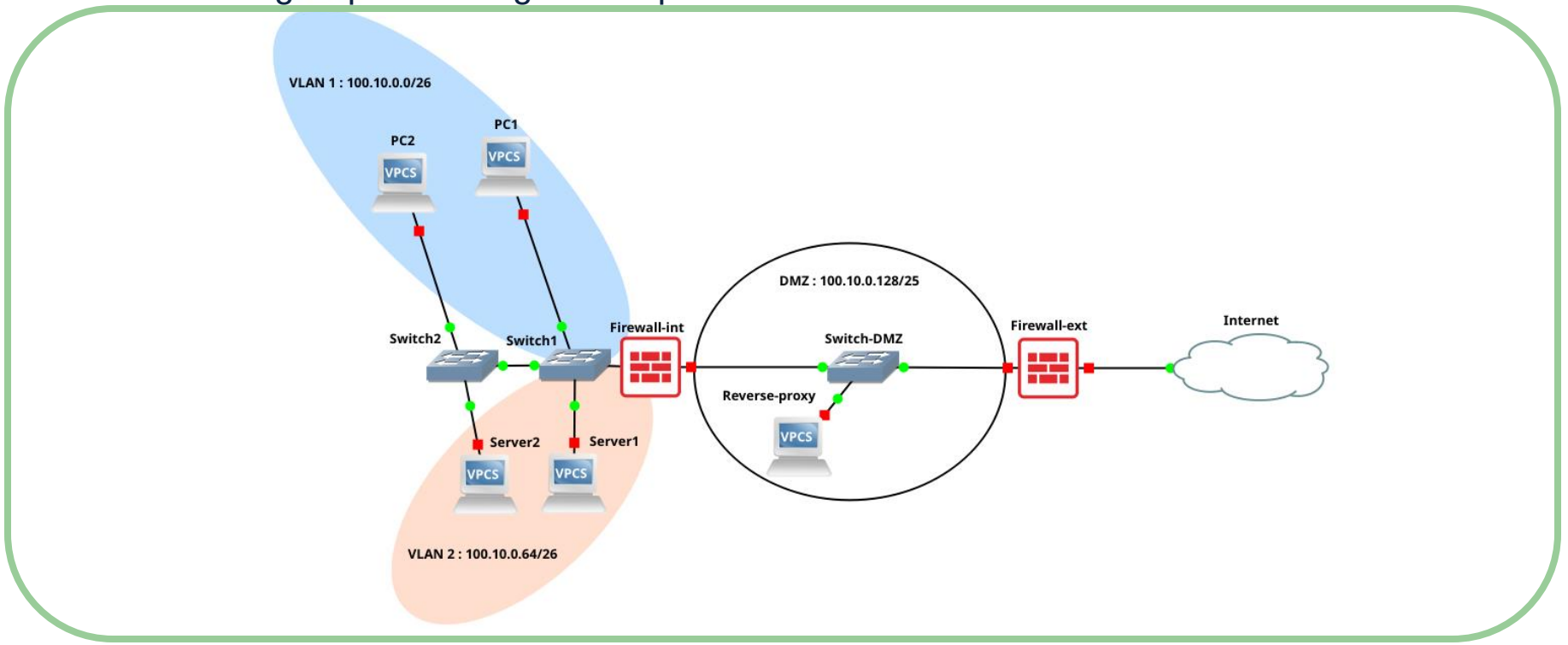
Tout autre flux en provenance de l'internet est bloqué



Tous autre flux en provenance de la DMZ sont bloqués

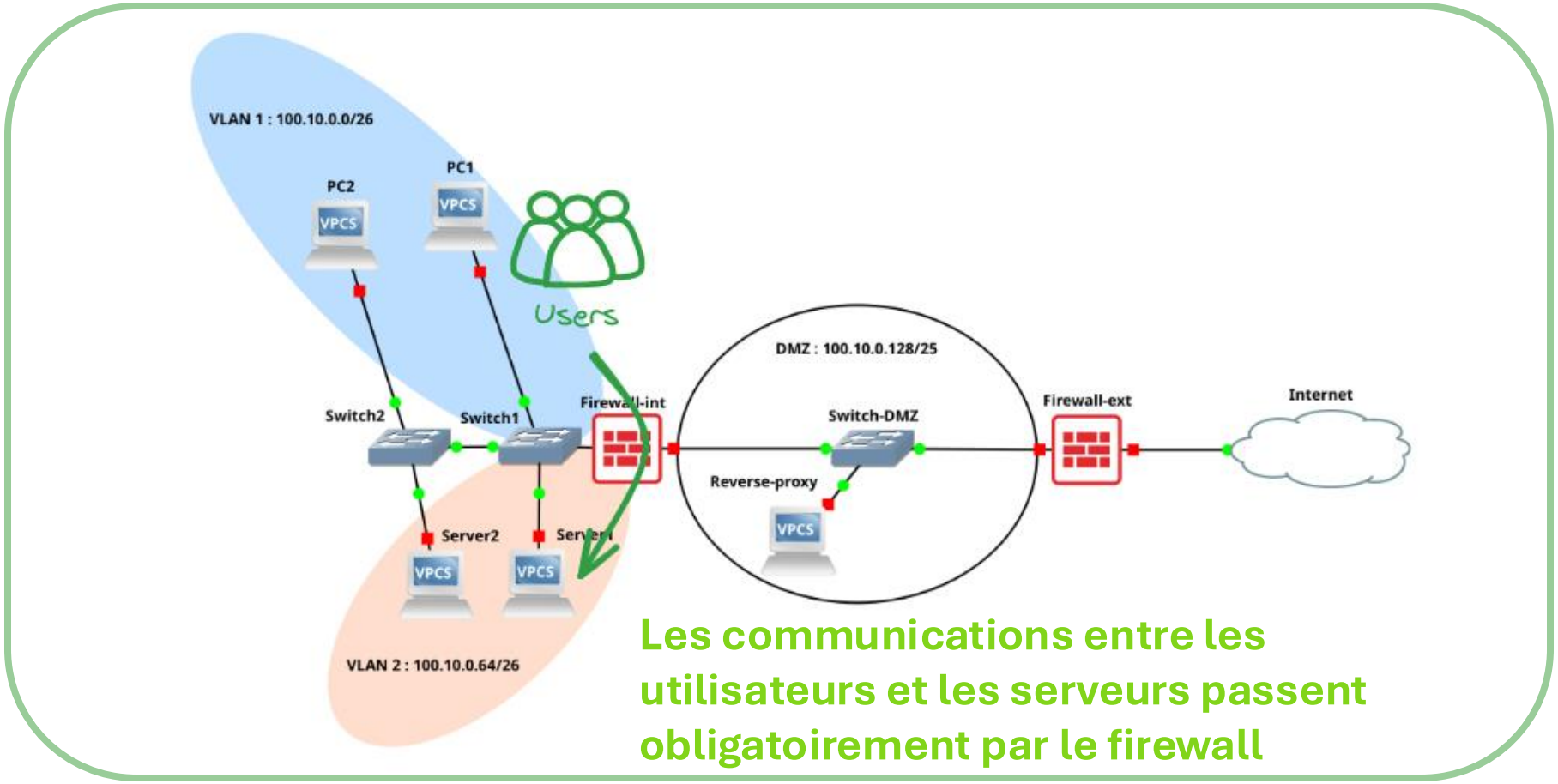
Session 4 - Sécuriser le réseau d'une entreprise

- **Pour aller plus loin :** Virtual Local Area Networks ou VLAN segmente le réseau intranet au niveau 2 pour séparer deux groupes de machines
  - Les PCs des utilisateurs sont séparés des serveurs
  - Les deux groupess sont gérés ici par 2 switchs



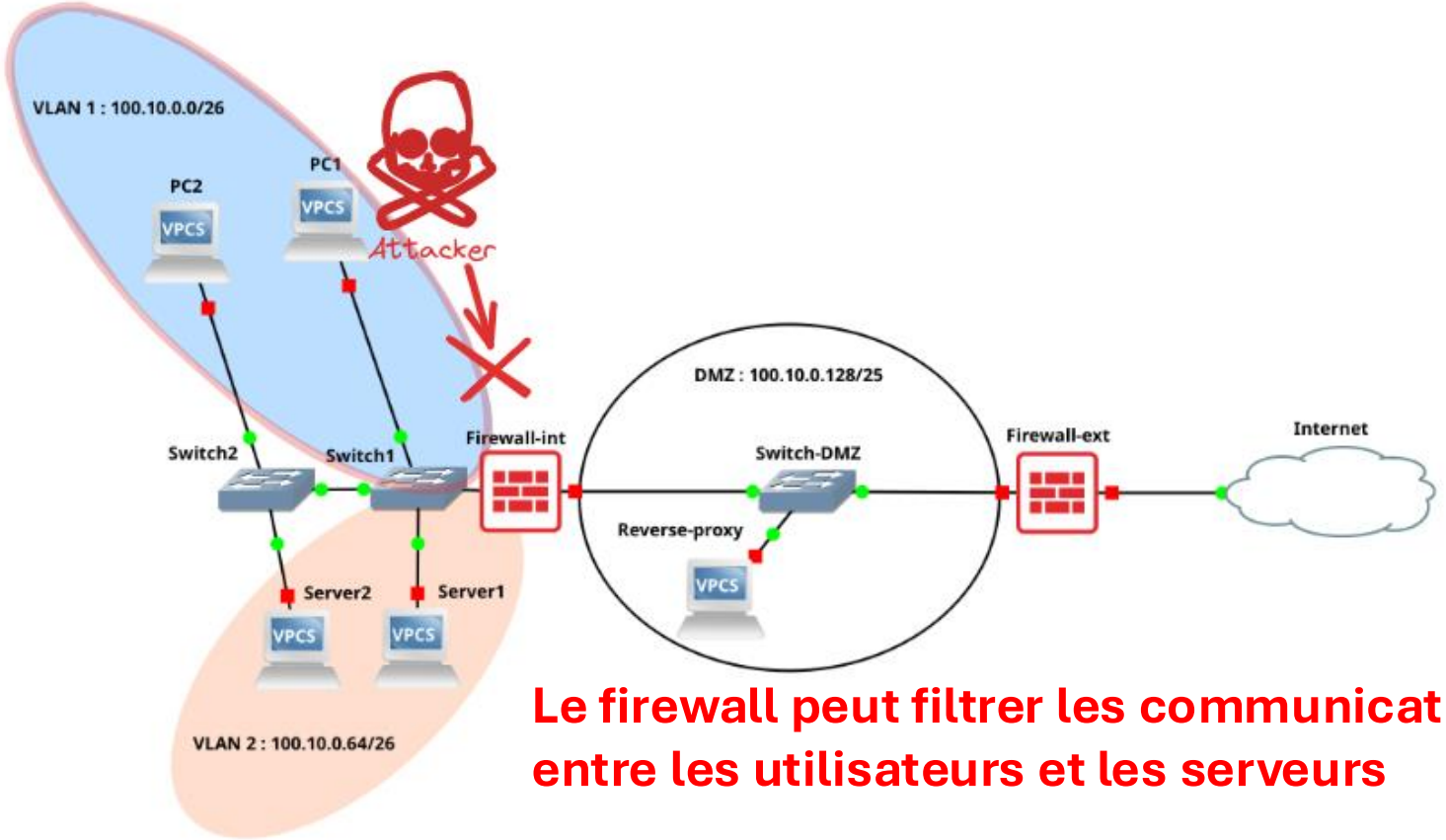
Session 4 - Sécuriser le réseau d'une entreprise

- **Pour aller plus loin : séparation en VLAN avec une partie des flux acceptée par le firewall Firewall-int**

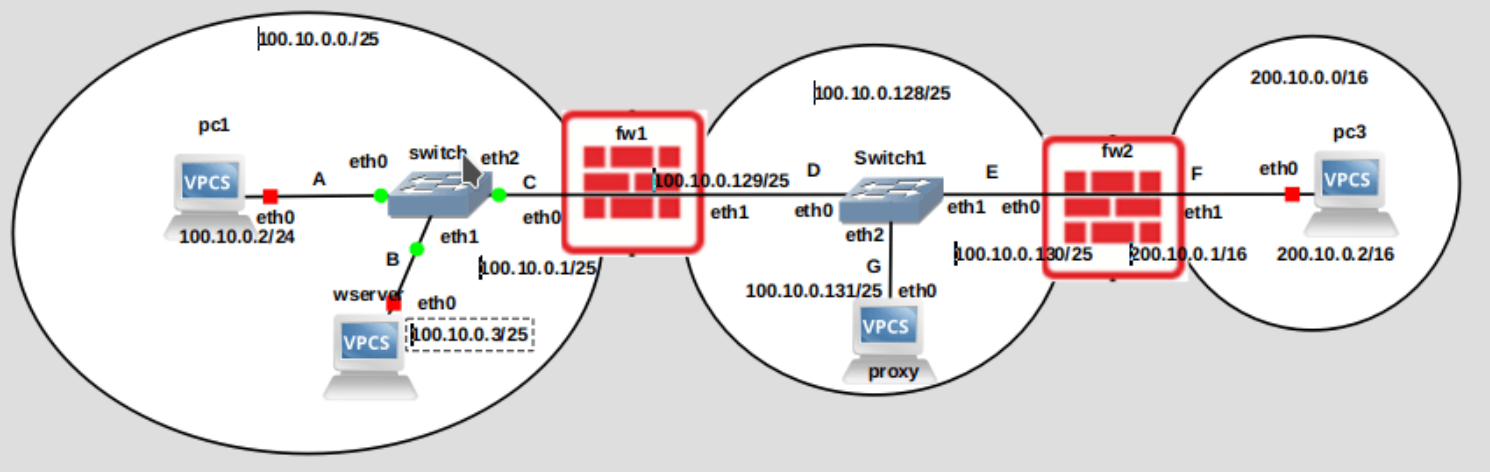


Session 4 - Sécuriser le réseau d'une entreprise

- **Pour aller plus loin : séparation en VLAN avec une partie des flux bloqués par le firewall Firewall-int**

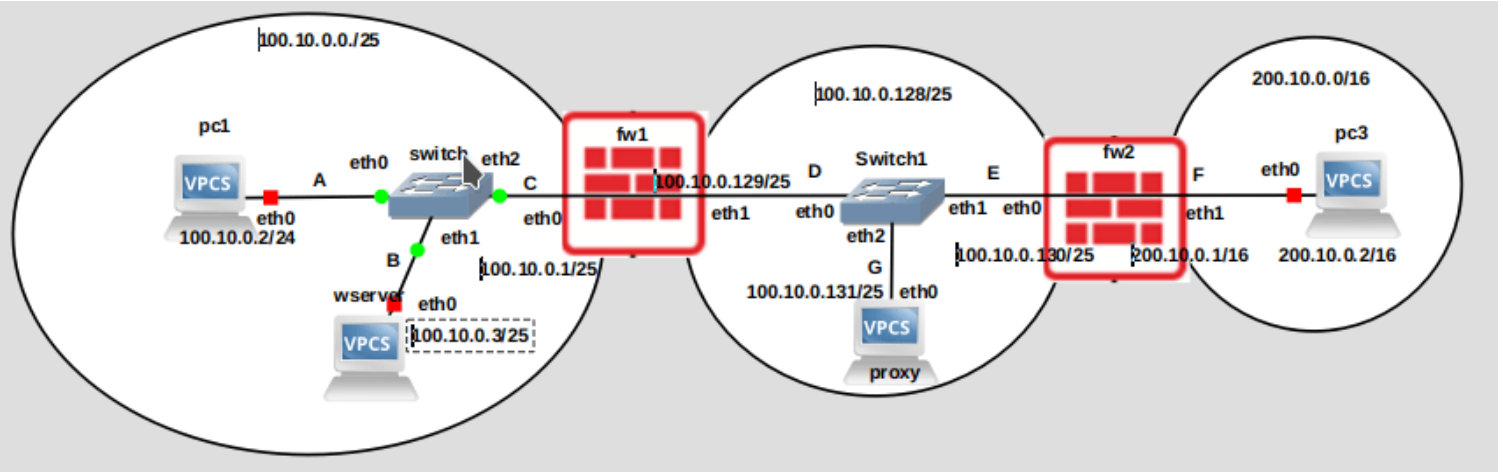


Session 4 - Sécuriser le réseau d'une entreprise



- **Récapitulatif** : vous configurez deux routeurs fw1 et fw2 jouant le rôle de firewall
  - fw2 en front effectue un préfiltrage
  - Proxy joue le rôle de rebond vers le serveur web apache de l'intranet
  - fw1 protège l'intranet

Session 4 - sécuriser le réseau d'une entreprise



- **Quelques dangers restants**
  - **L'espionnage** des communications et du contenu http échangé
    - ***Man in the middle*** intercepte et manipule les communications entre 2 parties (par ex. un client http et un site web http) à leur insu
  - La **réutilisation** des jetons de session http
  - L'échange avec un **site imposteur se faisant** wserver
- **Utiliser un serveur apache https plutôt que http**

Session 4 - sécuriser le réseau d'une entreprise – utiliser https plutôt que http

- **Enjeux** :
  - Assurer la **confidentialité :** garder/ne pas divulger les informations privées (sensibles par ex.), en veillant à ce qu'elles ne soient accessibles qu'aux personnes/entités autorisées
  - Assurer **l'intégrité** en se prémunissant de modification, d'altération ou de destruction non autorisées tout au long du cycle de vie
    - S'il n'est pas possible de s'en prémunir, **se rendre compte lorsque l'intégrité est atteinte**
  - Assurer **l'authenticité** des données/communications/entités en vérifiant l'identité des entités afin de vérifier qu'elle est bien celui celles qu'elles prétendent être, d'éviter l'usurpation d'identité, et, aussi l'accès non autorisé

Chiffrer pour assurer la **confidentialité**

- Le **chiffrement** est un processus de transformation des données (en clair) pour les rendre illisibles/indéchifrable à toute entité non autorisée
  - Pour chiffrer, on utilise un **algorithme de chiffrement** et une **clé de chiffrement** ce qui permet de coder la donnée en clair en un texte chiffré
  - Pour déchiffrer, seule une entité disposant de la **clé de déchiffrement** peut en utilisant l'algorithme de déchiffrement, convertir le texte chiffré en texte clair
- Il existe 2 grandes familles de chiffrement :
  - chiffrement symétrique
  - Chiffrement asymétrique

Chiffrement symétrique

- Le chiffrement symétrique utilise la **même clé pour le chiffrement et le déchiffrement**
  - L'expéditeur et le destinataire doivent **partager une clé secrète** qu'ils utilisent tous deux pour chiffer et déchiffrer les données
  - Le chiffrement symétrique est connu pour être généralement **rapide** et efficace pour traiter de **grandes quantités de données à chiffrer**
  - Le partage sécurisé de la clé secrète est un enjeu majeur

message chiffré = {message clair}$_{Ks}$

Emetteur ----------> Destinataire

Utilise Ks pour Chiffrer le message

utilise Ks pour déchiffer : message clair = {message chiffré }$^{-1}_{Ks}$

Chiffrement symétriques - Exemples simples

- **Chiffrement historique de César : clée secrête = un décalage de n caractères**
  - **Exemple : décalage de 2 caractères : A devient C, B devient D, C devient F, D devient G, …. , O devient Q**
  - Chiffrement (BONJOUR) = DPQLWT avec une clé secrête = déplacement de 2 charactères sur la droite
  - Déchiffrement (dqplpwt) = BONJOUR avec une clé secrête = déplacement de 2 charactères sur la gauche
- **Chiffrement par masque jetable** consiste à appliquer un XOR entre le texte en clair et une **clée secrète** de même longeur que le texte, générée aléatoirement et utilisée une et une seule fois
  - Chiffrement : applique un XOR entre le texte en clair et la clé secrète

    Texte en clair: 0 1 1 0 1 0

    Clé secrête : 1 0 0 1 1 0

    Texte chiffré : 1 1 1 1 0 0
  - Déchiffrement: applique un XOR entre le texte chiffré et la clée secrète

    Texte chiffré : 1 1 1 1 0 0

    Clée utilisée : 1 0 0 1 1 0

    Texte en clair: 0 1 1 0 1 0

Chiffrement asymétrique

- La cryptographie asymétrique utilise 2 clées :
  - **Clé publique pour chiffrer** la donnée ; elle est **partagée** avec n'importe qui en faisant la demande
  - **Clé privée pour déchiffrer** la donnée ; elle est **gardée secrète** (connue que du propriétaire)
- Exemple de chiffrement asymétrique :

Message chiffré = $\{message\}_{K_{bob}^{pub}}$

Alice ----------> Bob

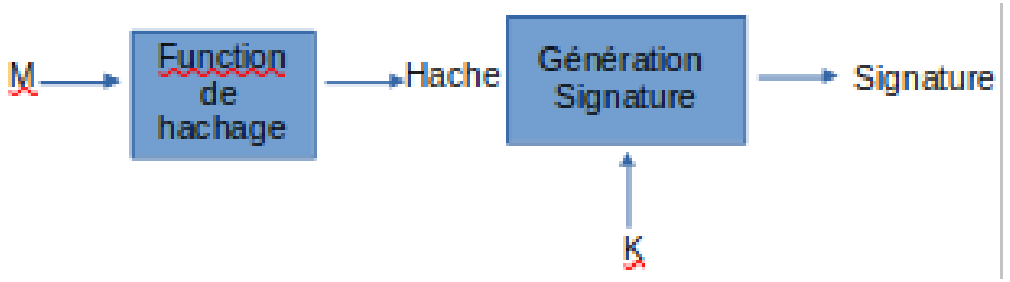
Alice connait K_{bob}^{pub}

Bob a généré K_{bob}^{priv} et K_{bob}^{pub}

Message clair = $\{message\ chiffré\}_{K_{bob}^{priv}}^{-1}$

- La cryptographie asymétrique est couramment utilisée pour
  - **Échanger des clées secrètes** (car le **chiffrement asymétrique est coûteux**)
  - par HTTPS
  - Pour **signer** numériquement une donnée

Signature numérique



- est utile pour vérifier **l'authenticité** et **l'intégrité** et **empêcher la répudiation**
- garantit que la donnée n'a pas été modifiée, vérifie l'identité de l'expéditeur/générateur de la donnée qui ne peut répudier
  - Le document ou message est **haché** avec une fonction de hachage pour créer un hache de longueur fixe du document/message
  - Le hache est ensuite chiffré à l'aide de la clé privée de l'expéditeur, ce qui génère la signature numérique

message en clair , {hash(message)}$_{K\ alice}^{priv}$

Alice ----------> Bob

Alice a généré K_{alice}^{priv} et K_{alice}^{pub}

Bob connait K_{alice}^{pub}

Signature numérique - vérification de l'**authenticité et de l'intégrité**

- Le destinataire déchiffre la signature à l'aide de la clé publique de l'expéditeur et compare le hachage obtenu avec un hachage nouvellement calculé des données reçues. Si les hachages correspondent, les données sont vérifiées comme étant authentiques et inchangées.

message en clair , {hash(message)}

Alice ----------> Bob

K^{priv}_{alice}

Alice a généré K^{priv}_{alice} et K^{pub}_{alice}

Bob extrait message et recalcule hash(message)

Bob déchiffre $\{\{hash(message)\}^{priv}_{K_{alice}}\}^{-1}_{K^{pub}_{alice}}$ = **M**

Bob vérifie que hash(message) que bob a calculé == **M**

Signature numérique - conclusion

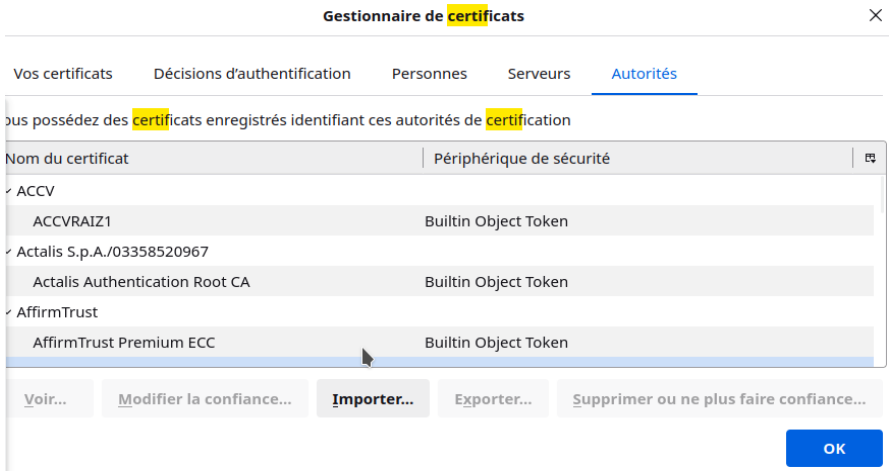
- La clé privée d'Alice est utilisée pour **générer une signature**
  - La génération de la signature ne peut être effectuée que par Alice qui est la seule à avoir accès à sa clé privée
- La clé publique d'Alice est utilisée par Bob pour vérifier la signature
  - Toute personne connaissant la clé publique (dont Bob) peut vérifier la signature en utilisant la clé publique associée
- **Question : comment Alice peut partager avec Bob sa clée publique de manière sécurisée ?**

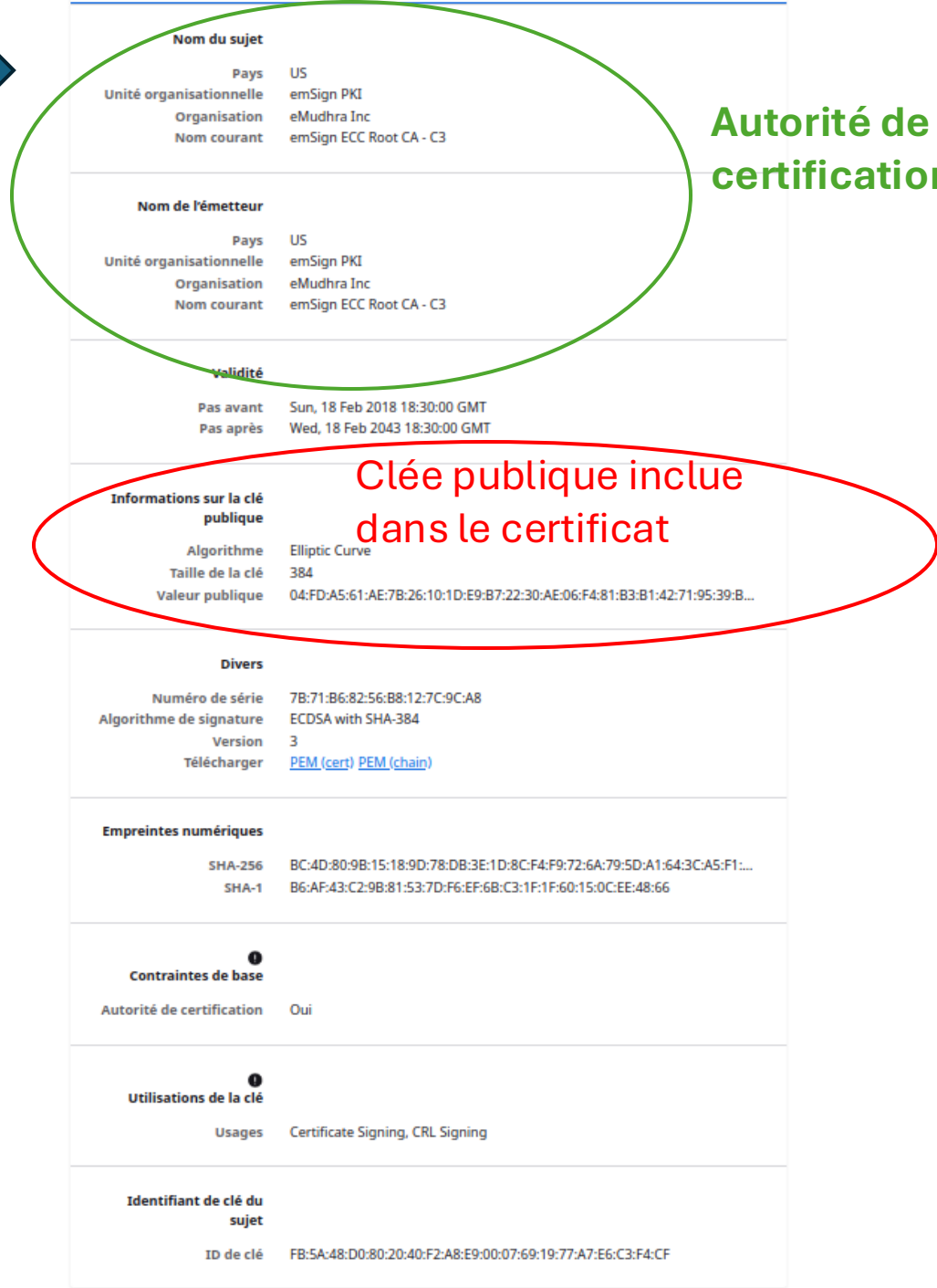
Certificat disponible sur le navigateur mozilla

Partage de clée publique

- Le serveur http dispose d'une **clée publique** et d'une **clée privée**
- Le site web génère un **certificat** contenant sa clée publique signée par une **autorité de certification**
- Le navigateur client dispose de certificats mis à jour

Liste des certificats disponible sur le navigateur mozilla



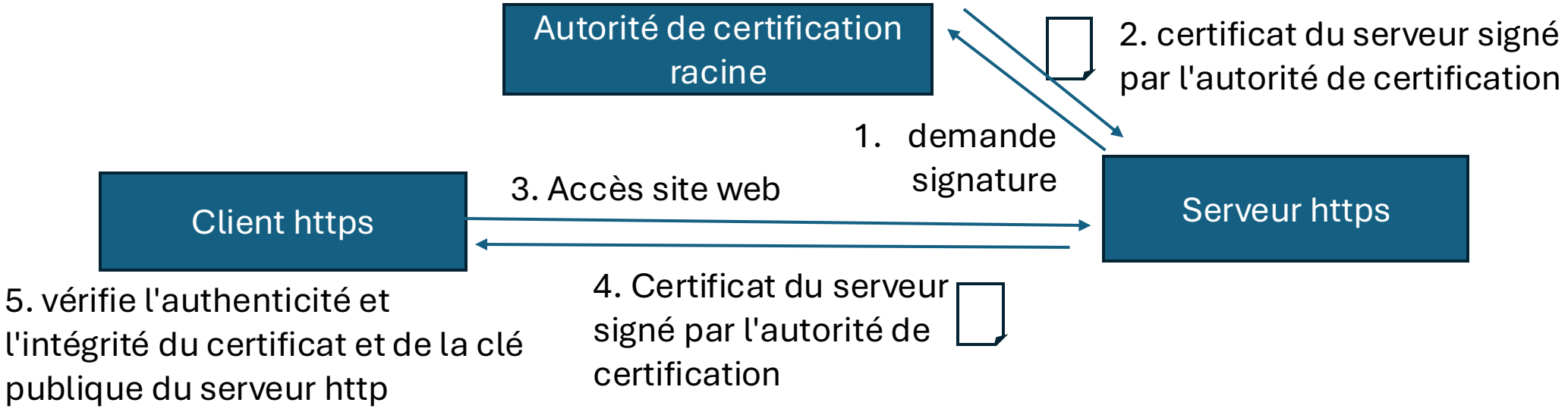


Autorité de certificatio

Clée publique inclue dans le certificat

Partage de clé publique - authorité de certification

- Une autorité de certification
  - est un **tiers de confiance** (dont la confiance n'est pas remise en cause)
  - fait partie d'une **chaine de certification** (l'ami de mes amis est un ami)
  - valide un certificat (applique une signature sur le certificat)
  - Un navigateur peut vérifier l'authenticité/l'intégrité du certificat (et donc de la clé publique) d'un site Web signé par une autorité de certification



Problème lié au partage des clées - solution adoptée lors du TP de la session 4 : https

- Pas d'autorité de certification (kathara n'est pas connecté a l'Internet) :-(
  - Le serveur https auto-signe son certificat :-(
- L'administrateur a échangé avec le client (via une clé usb = répertoire partagé de kathara) son certificat auto-signé
- Le client et le serveurs s'échangent une clé secrête utilisée par la suite pour chiffrer les communications