Sommaire Cours

I. Introduction – problématique de la sécurité – sécurité web
II. Présentation des menaces – vulnérabilités
III. Standards de sécurité utiles pour le web
IV. Architecture du web (infrastructure et applicatif)
V. Sécurisation des services
VI. Sécurisation des applications
VII. Sécurisation de l'infrastructure
    I. Passerelle sécurisée avec Open SSL
    II. Notion de Certificats
    III. Reverse proxy
    IV. Pare-feu : Iptables

Définition d'une architecture sécurisée

- Extrait du livre blanc* ANSSI**
- Menaces principales pour les entreprises :
  - Compromission : fuite de données sensibles depuis le LAN vers internet
  - Défiguration /destruction des serveurs Web internes et bases de données de l'entreprise
  - Eléments des l'architecture typiquement internet
    - LAN : réseau d'entreprise
    - WAN : réseau externe
    - Firewall filtrage et routage des paquets
    - DMZ zone démilitarisée qui est une zone de services (web messagerie, proxy)

* https://www.ssi.gouv.fr/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee

** Agence Nationale de Sécurité des Systèmes d'Informations

Eléments d'architecture sécurisée

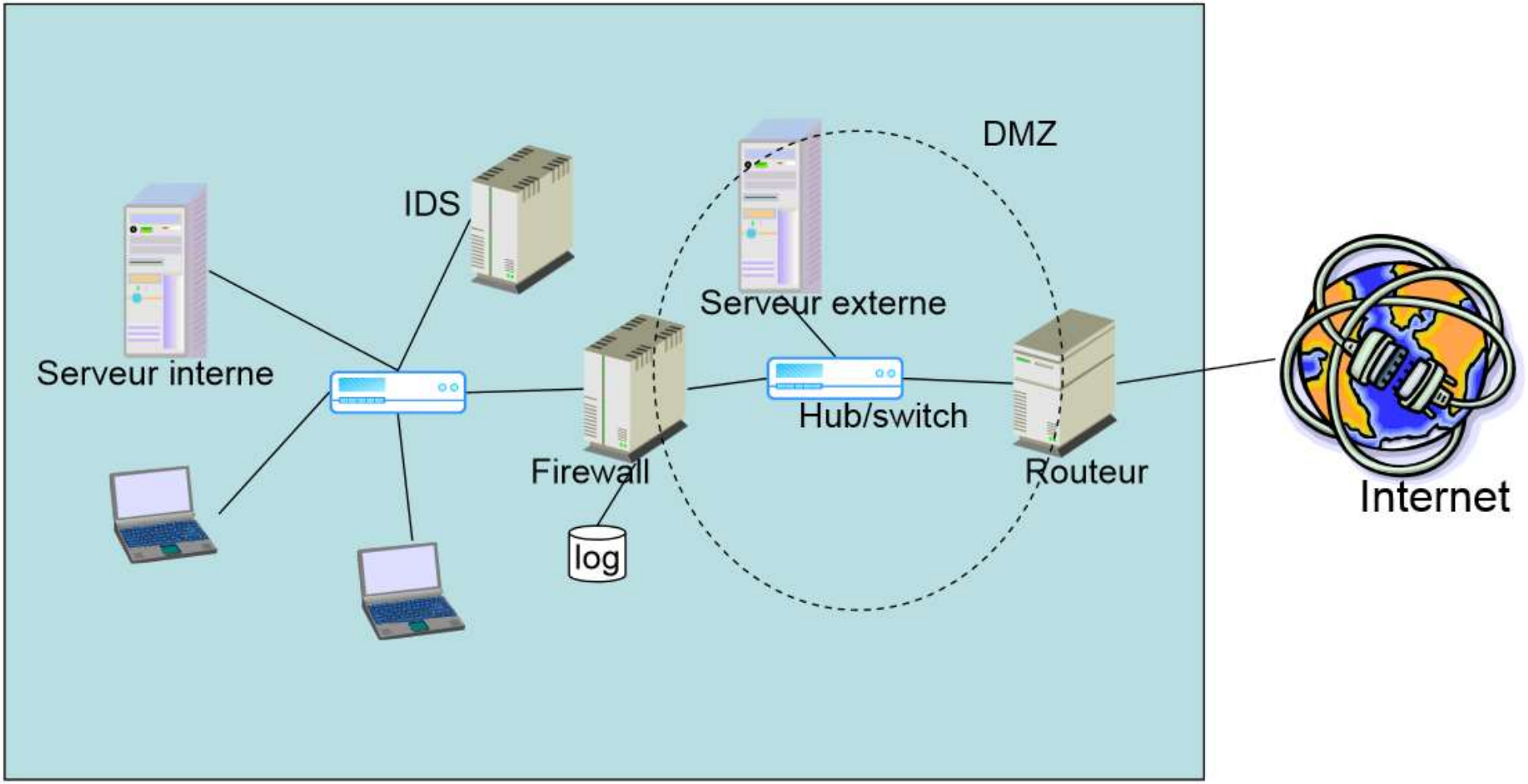
1. Limiter l'accès au réseau à des personnes machines identifiées
   - gère les connexions sortantes à partir du réseau local
   - Protège le réseau interne des intrusions venant de l'extérieur
   - Surveille/trace le trafic entre réseau local et internet
   - -> authentification
2. Pare-feu applicatif : -> intégrité et disponibilité
   - Fonctionne au dessus de TCP
   - Mécanisme de proxy /reverse proxy
   - Possibilité d'interpréter le contenu du trafic

Eléments d'architecture sécurisée

1. Pare-feu niveau réseau (iptables, paquet filter)
   - Fonctionne au niveau TCP
   - Filtrage de paquets
   - Possibilité de filtrer les paquets en fonction de la connexion -> intégrité et disponibilité

3. Pare-feu au niveau des applications (/etc/ftpaccess pour ftp …)
   - Restrictions au niveau des applications -> authentification
   - Cryptage des données -> confidentialité

Eléments d'architecture sécurisée



Eléments d'architecture sécurisée

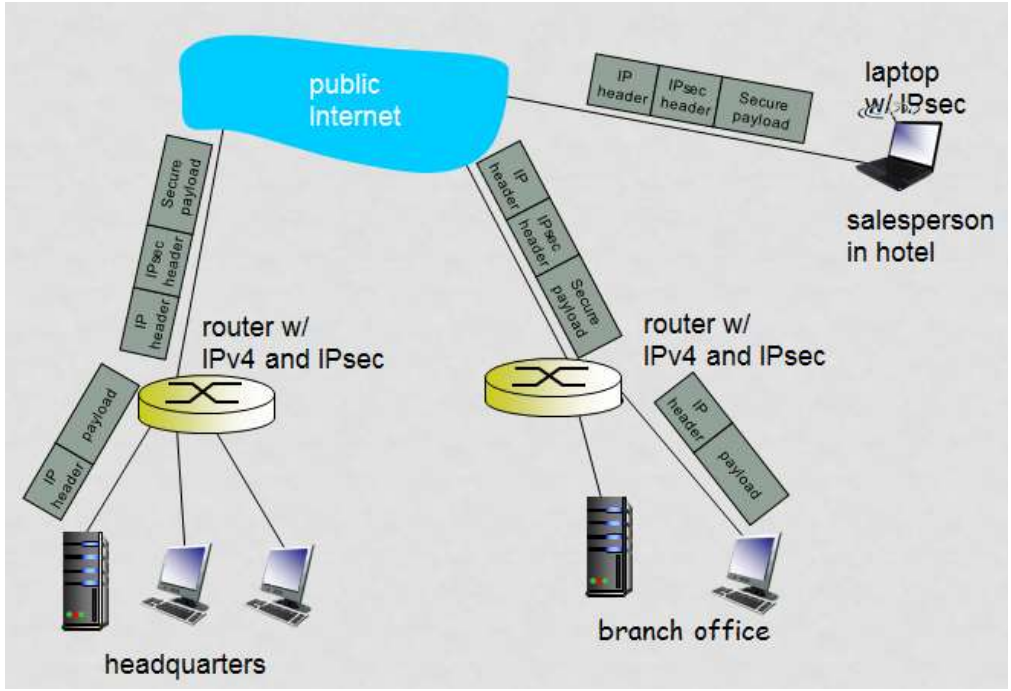
- DMZ: zone démilitarisée
  - Sous réseau entre le réseau extérieur et le réseau local
  - Intérêt :
    - Rendre des machines accessibles depuis l'extérieur (DNS, SMTP, WEB…)
    - Hébergement reverse proxy
    - Zone tampon avant intranet entreprise
  - Propriétés
    - Connexions à la DMZ autorisées de n'importe où
    - Connexions à partir de la DMZ ne sont autorisées que vers l'extérieur

Eléments d’architecture sécurisée

- IDS : (*Intrusion Detection System*) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.
- LOG : enregistrement du trafic au niveau des routeurs/pare-feu et équipements sensibles

Eléments d'architecture sécurisée

- VPN : Virtual Private Network
  - Seuls les agents autorisés ont accès aux réseaux virtuels (authentification, chiffrement des communications)
    - Niveau 2 : VLAN
    - Niveau 3 : IPSEC , SSL



- Autorité de certification (CA)
  - Associe une clef publique à une entité E.
  - E enregistre sa clef publique auprès du CA.
  - CA crée un certificat associé à la clef publique de E .
  - Un certificat contient la clef publique de E avec une signature électronique de CA assurant "c'est la clef publique de E "

Sommaire Cours

I. Introduction – problématique de la sécurité – sécurité web
II. Présentation des menaces – vulnérabilités
III. Standards de sécurité utiles pour le web
IV. Architecture du web (infrastructure et applicatif)
V. Sécurisation des services
VI. Sécurisation des applications
VII. Sécurisation de l'infrastructure
    I. Passerelle sécurisée avec Open SSL
    II. Notion de Certificats
    III. Reverse proxy
    IV. Pare-feu : Iptables

Les transmissions sécurisées (1)
(SSL - Secure Socket Layer ou "https")

- Aucune différence avec consultation de page normale, à part connexion entre serveur et client encryptée et serveur authentifié.

- Le principe basé sur un certificat autentifiant le serveur grâce à un tiers vérificateur.
- Le serveur signe un message avec sa clé privée et
- le client vérifie avec la clé publique du serveur, trouvée sur ce tiers autentificateur.
- Puis ils choisissent une clé pour communiquer.

Les transmissions sécurisées (2) (SSL - Secure Socket Layer ou "https")

Pour un serveur sécurisé sur Internet il faut donc :

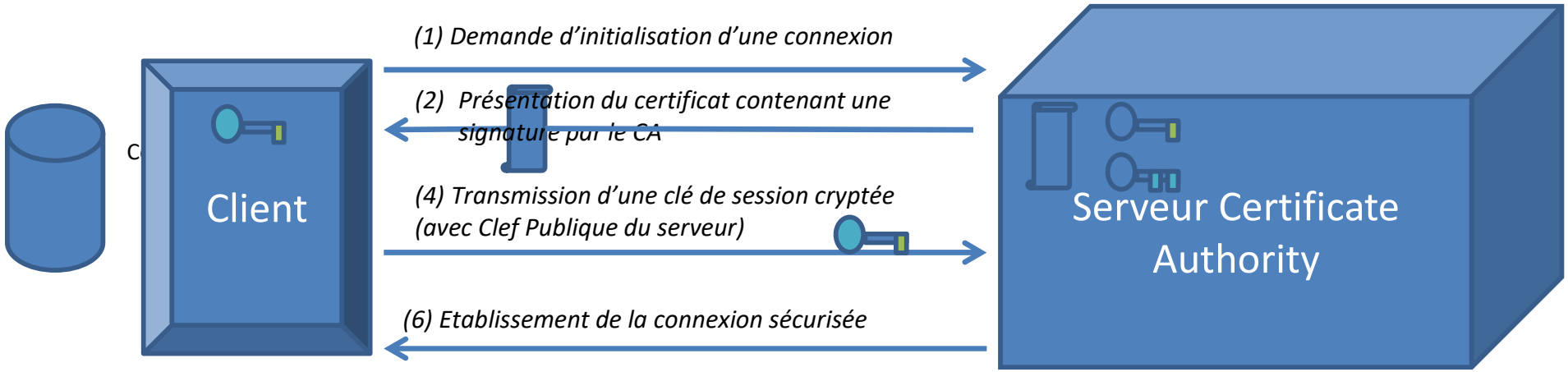
- Se procurer un certificat-serveur chez thawte.com (Europe, moins cher) ou verisign.com (USA, plus cher)

- Créer son propre certificat-serveur et configurer les browsers de tous les visiteurs pour qu'ils l'acceptent. (certificat auto signé)

Demande de certificat

- “Carte d'identité” d'une entité informatique (expl: un serveur ou un équipement ou une personne)

- Est délivré par un tiers de confiance qui atteste du lien entre l'identité physique et l'entité numérique
- Principe d’établissement du certificat :



(3)Vérification du certificat

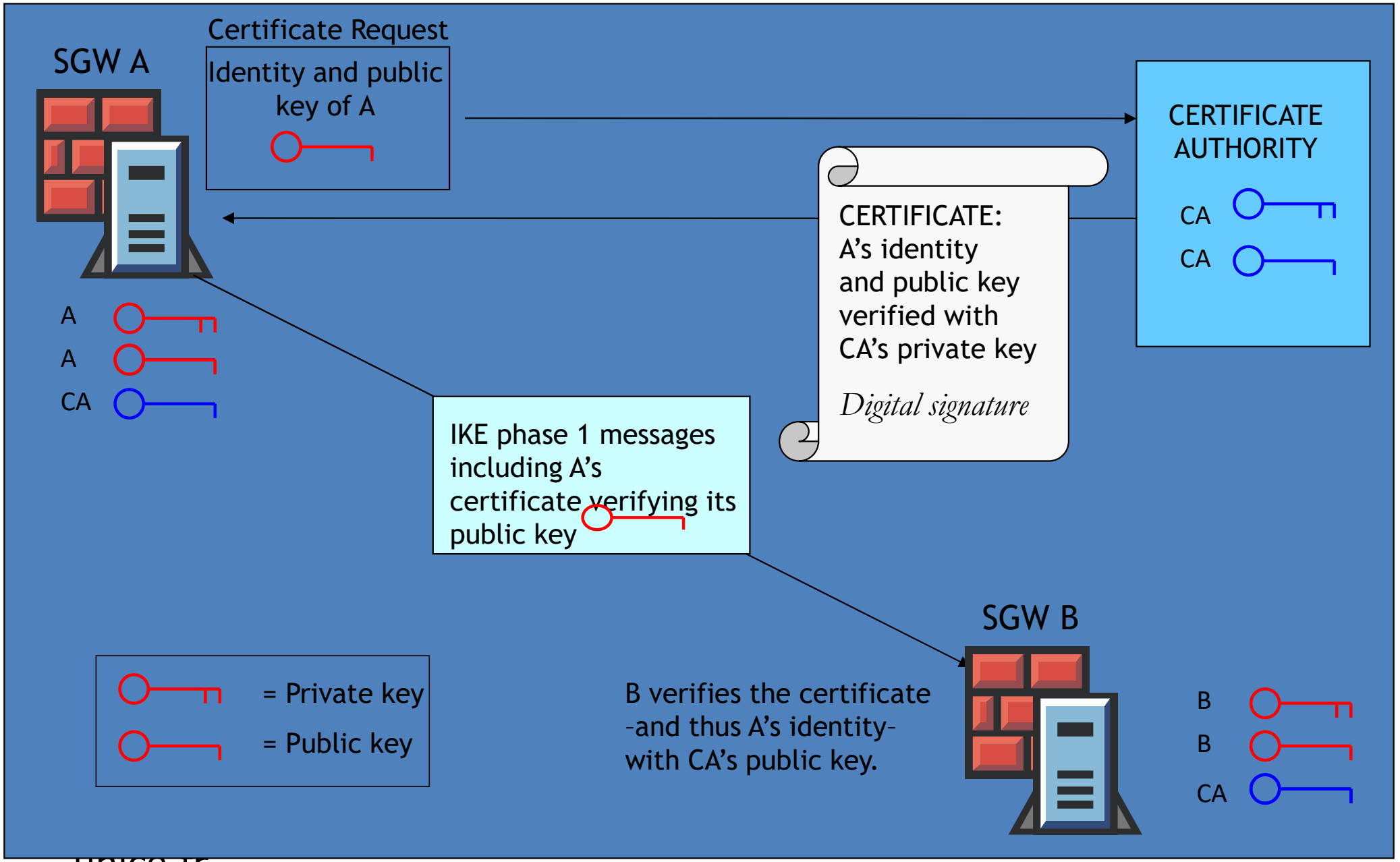
- *validité & CA*
- *Signature par tiers de confiance*
- *Récupération Clef publique*

(5) Décryptage de la clef de session par le serveur

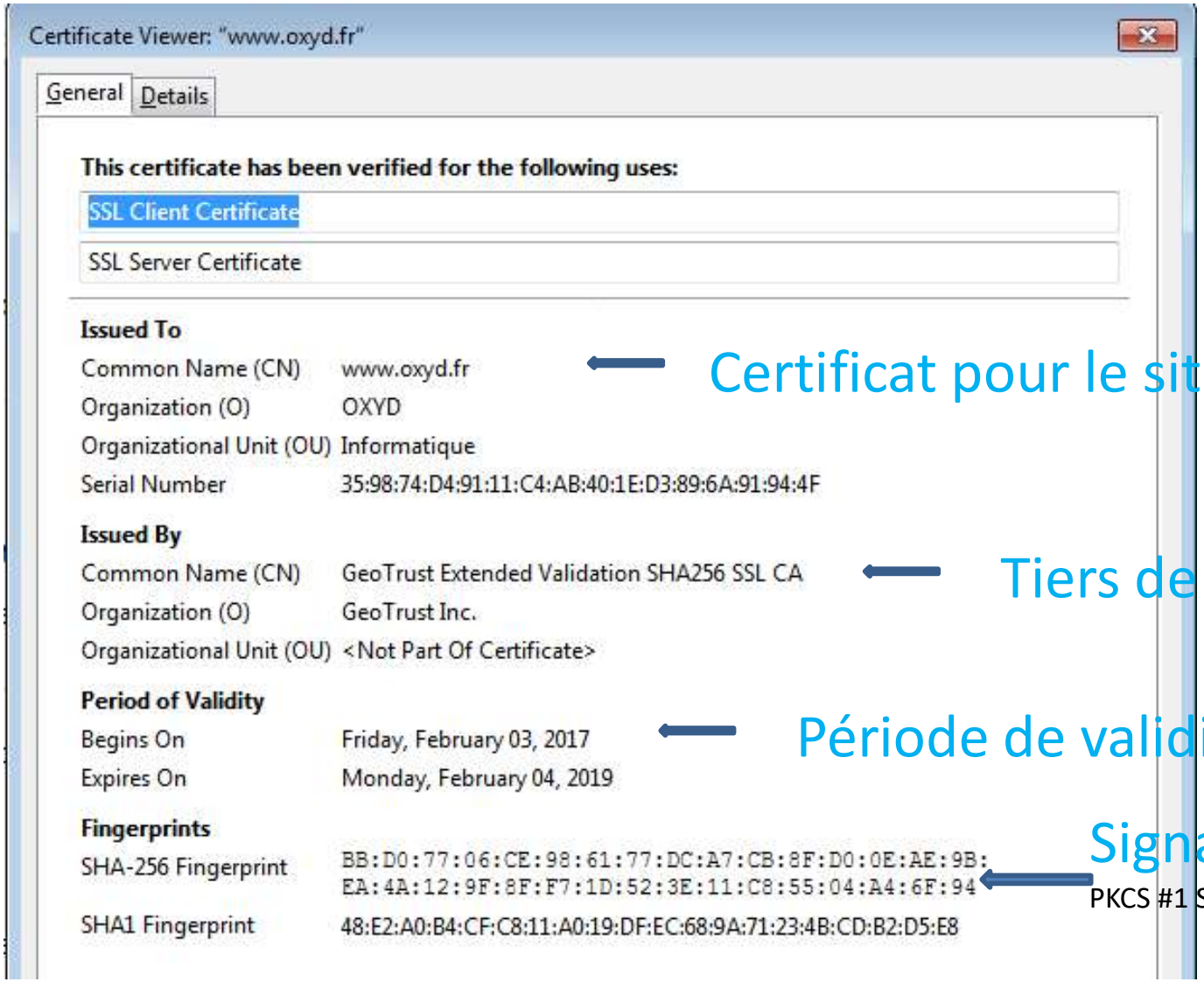
Principe des certificats

- *utilisés* lors du transfert de clefs publiques entre entités
- Les certificats aident à prévenir l'utilisation de fausses clefs publiques pour l'usurpation d'identité.
- une carte qui atteste l'identité d'une clef publique.
- délivrée par une autorité de certification (noté CA). qui peut les révoquer aussi.
- est un fichier qui contient
  - les informations de l'entité(identité + clef publique)
  - La signature du certificat est une fonction de hachage des informations puis ce condensé est signé par la CA (avec sa clef privée)

Authentication avec Certificat



Exemple de certificat



Certificat pour le site

Tiers de confiance

Période de validité

Signature du certificat

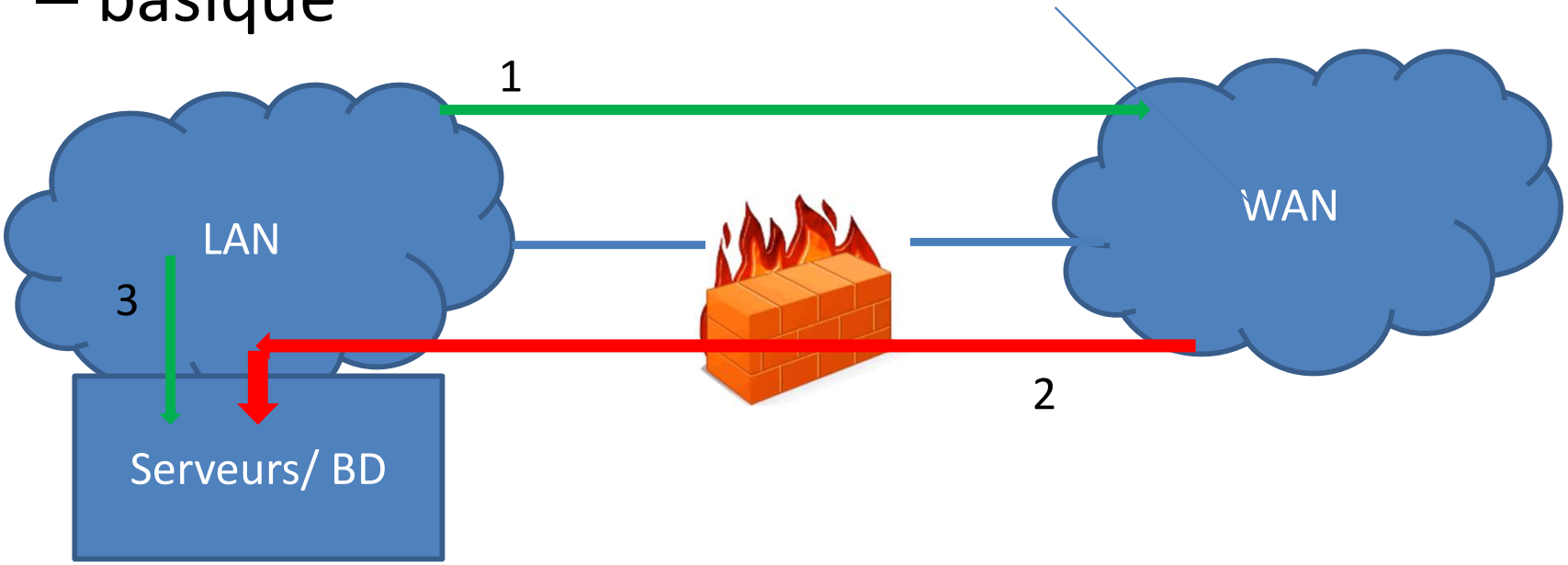
PKCS #1 SHA-256 With RSA Encryption

Sommaire Cours

I. Introduction – problématique de la sécurité – sécurité web
II. Présentation des menaces – vulnérabilités
III. Standards de sécurité utiles pour le web
IV. Architecture du web (infrastructure et applicatif)
V. Sécurisation des services
VI. Sécurisation des applications
VII. Sécurisation de l'infrastructure
    I. Passerelle sécurisée avec Open SSL
    II. Notion de Certificats
    III. Reverse proxy
    IV. Pare-feu : Iptables

Différents types d'Architecture

– basique

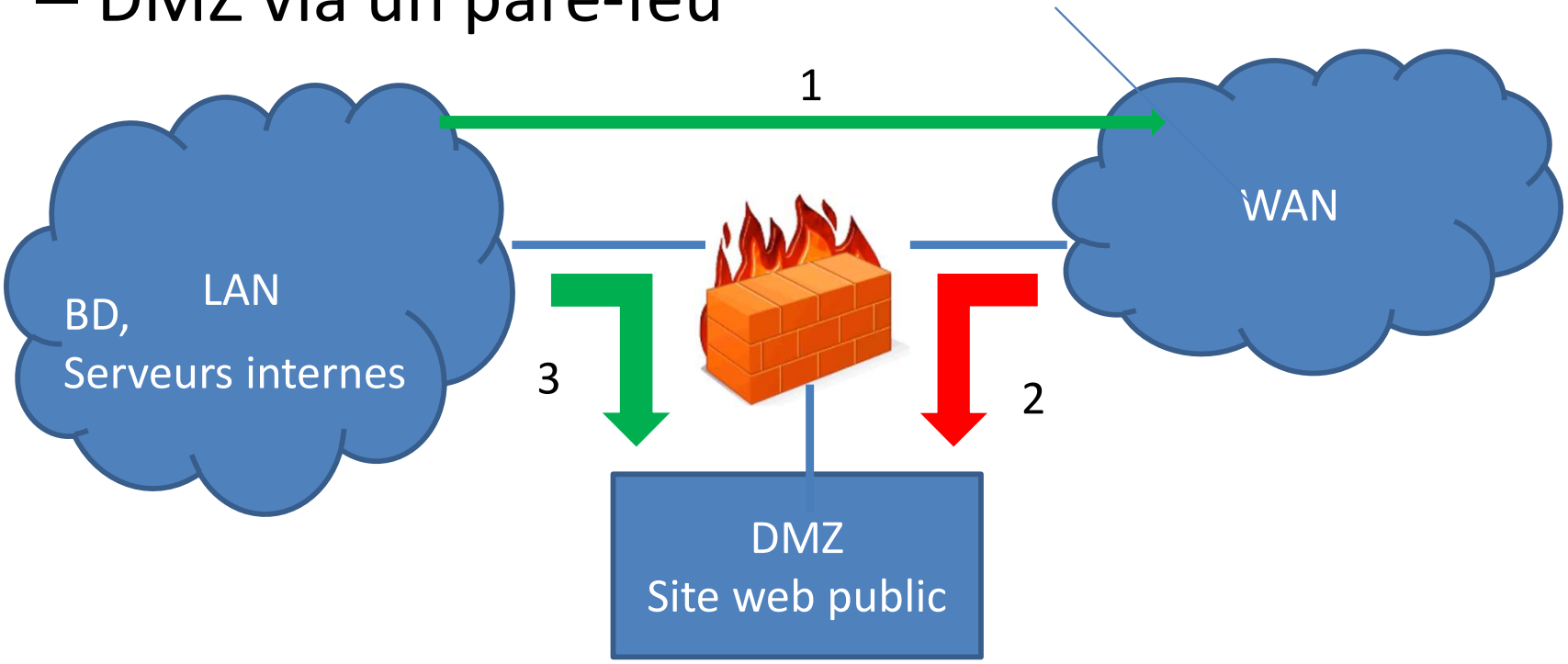


1: flux de consultation internet depuis le LAN
2: flux de consultation du serveur web depuis internet
3: flux de mise à disposition de contenu de serveur web depuis le LAN

PB1: flux depuis internet traversent le LAN => sensible aux erreurs et rebonds
PB2: pare-feu névralgique, si il tombe => accès complet au réseau
PB3 : défiguration du site web/BD si des flux malveillants atteignent le serveur web

Différents types d'Architecture

– DMZ via un pare-feu



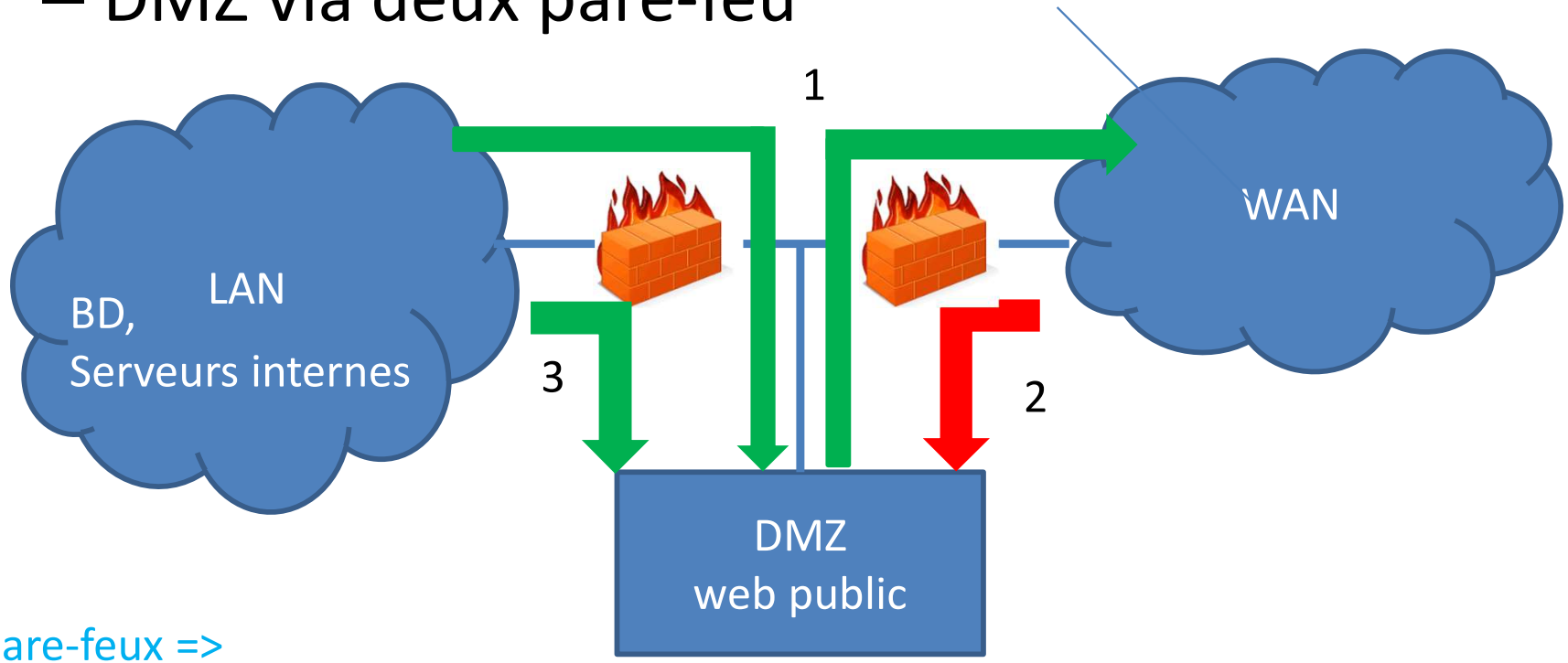
Seuls les serveurs accessibles depuis le WAN sont dans la DMZ

PB2: pare-feu névralgique, si il tombe => accès complet au réseau

PB3 : défiguration du site web/BD si des flux malveillants atteignent le serveur web

Différents types d'Architecture

– DMZ via deux pare-feu



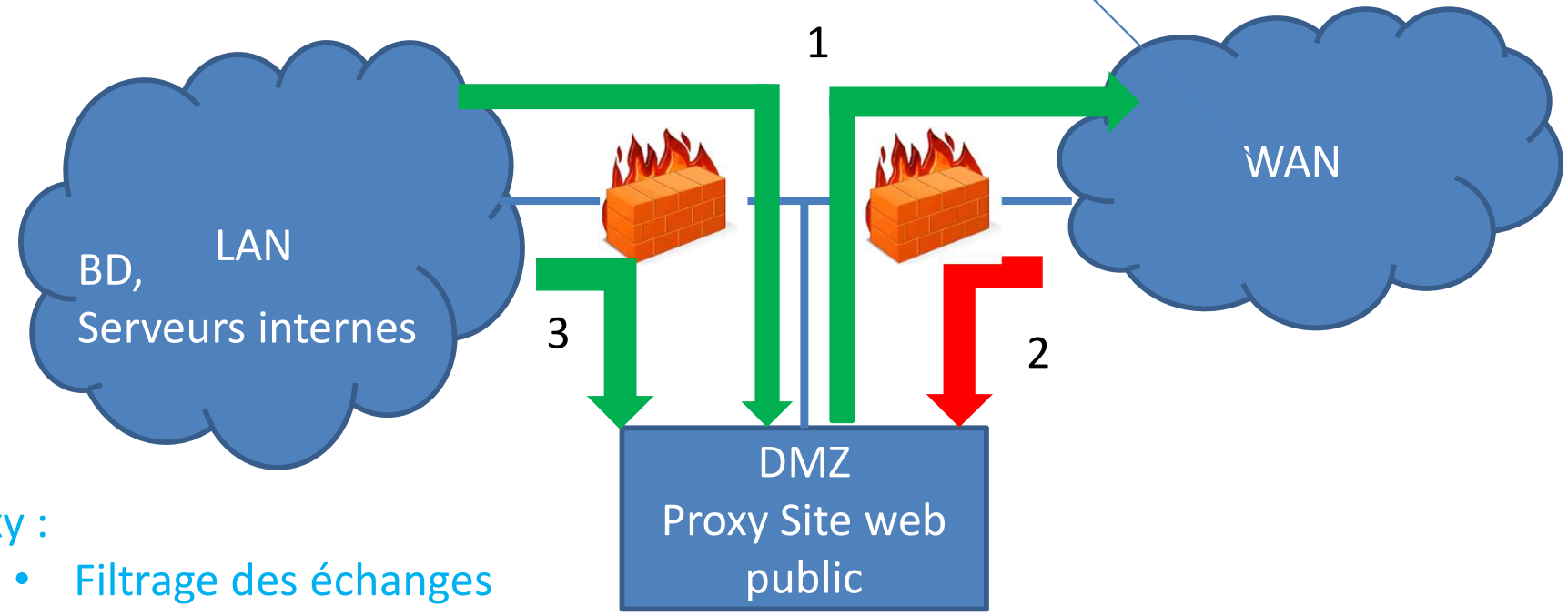
2 pare-feux =>

- un interne et l'autre externe
- équipements deviennent non critiques
- Pare-feu interne en coupure => LAN protégé

PB3 : défiguration du site web/BD si des flux malveillants atteignent le serveur web

Différents types d'Architecture

– DMZ via deux pare-feux et rajout d'un proxy



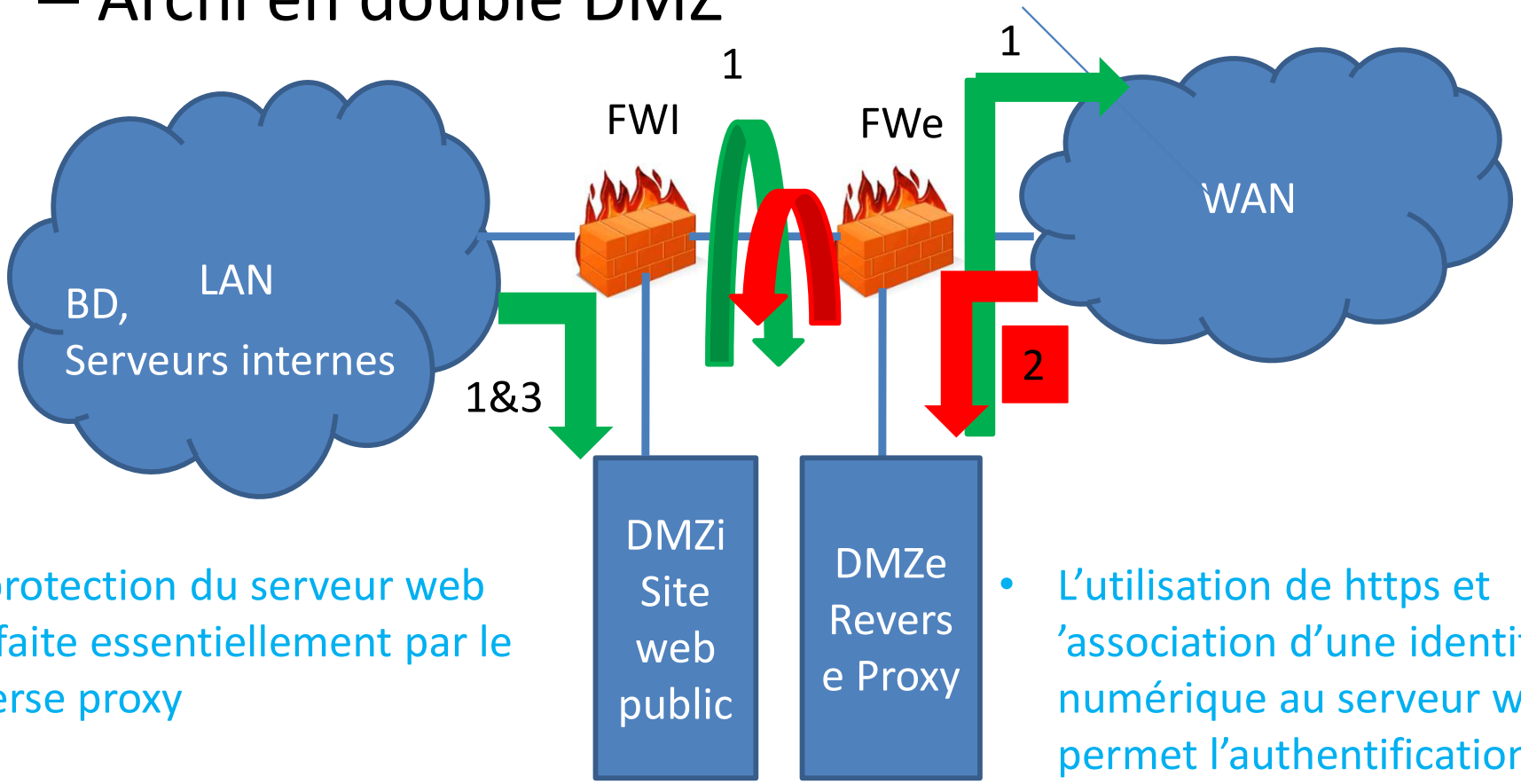
Proxy :

- Filtrage des échanges
- Dépolution ,
- Filtrage de contenus,
- Liste blanche /noire des sites

- la DMZ est en coupure (logique) sur l'ensemble des flux

Différents types d'Architecture

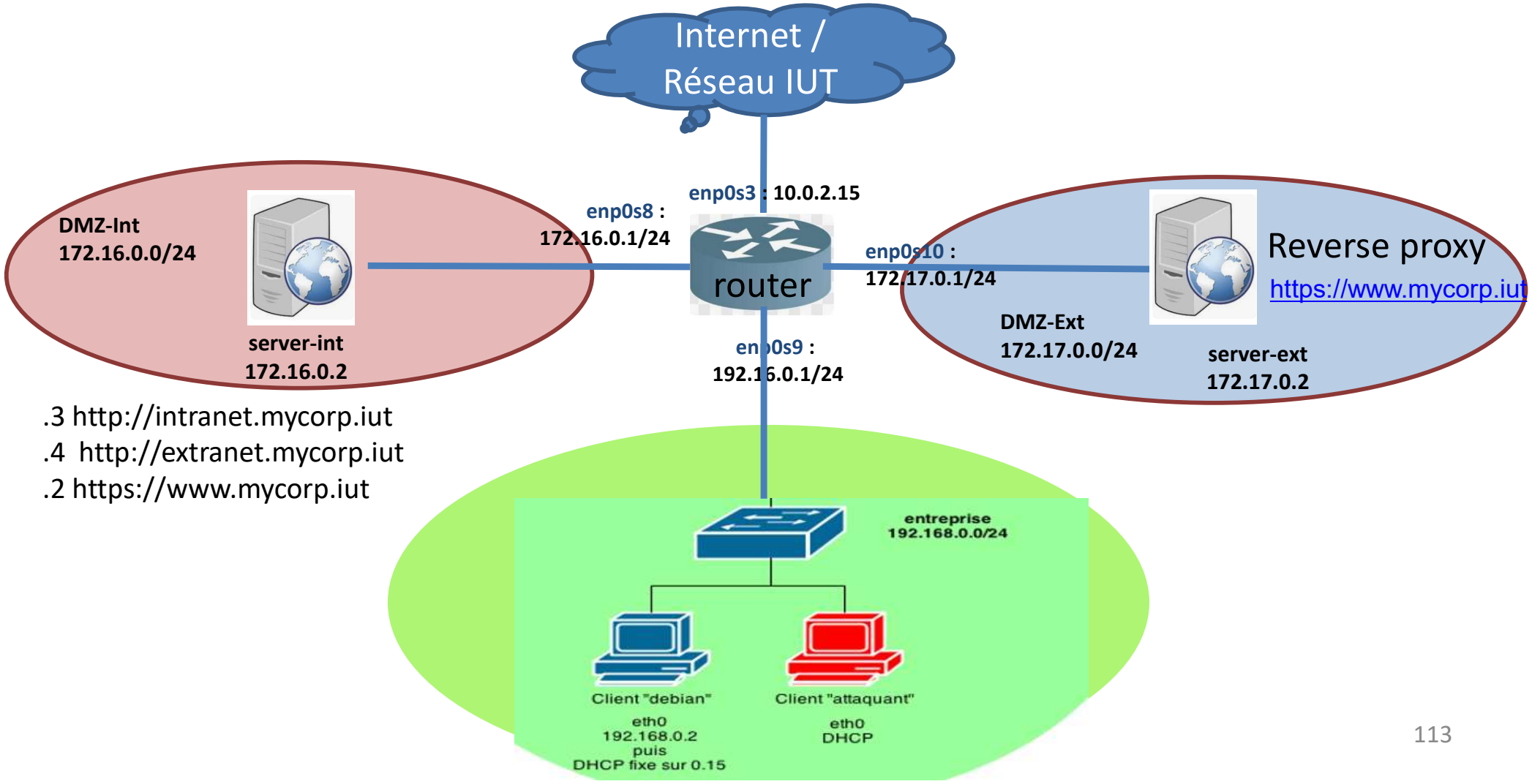
– Archi en double DMZ



- La protection du serveur web est faite essentiellement par le reverse proxy
- L'utilisation de https et 'association d'une identité numérique au serveur web permet l'authentification Et la non compromission du DNS (changement de l'adresse IP des serveurs web)

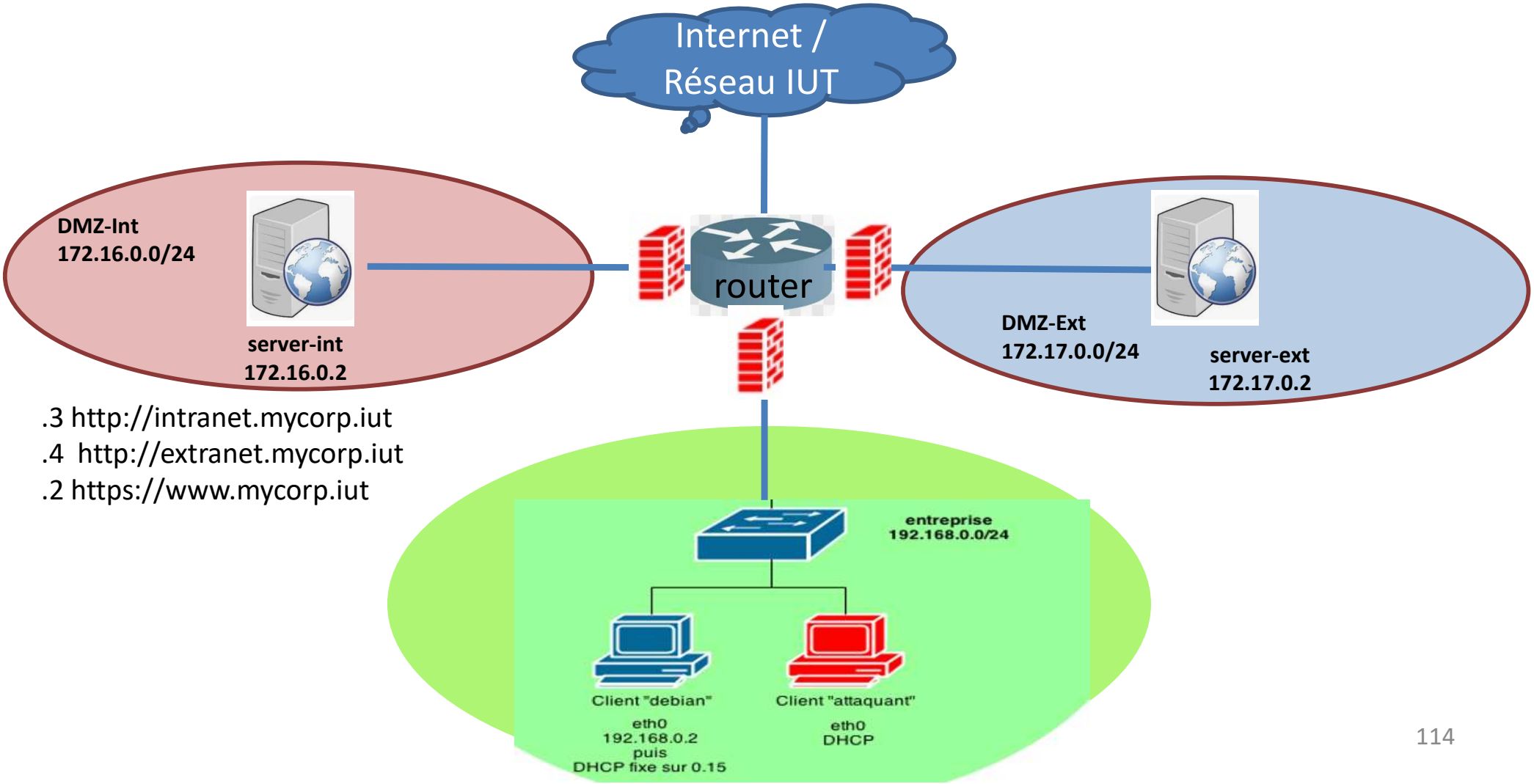
Architecture Use case TP4

Déploiement de l'infrastructure et des services pour mise en place d'une double DMZ



Architecture Use case TP4

Déploiement de l'infrastructure et des services pour mise en place d'une DMZ



Architecture Use case TP4

Architecture virtuelle avec 4 machines :

- 3 réseaux : entreprise, dmz-int dmz-ext
- 1 routeur : routeur linux + couche firewall
- 3 serveur web http et https
- Entreprise: machine cliente