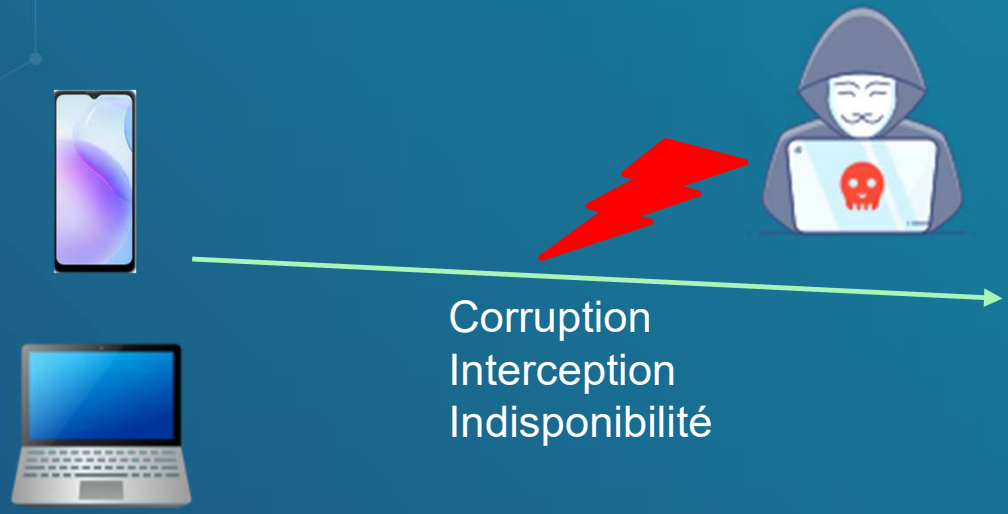
3 SECURITE RESEAU

3

La sécurité réseau

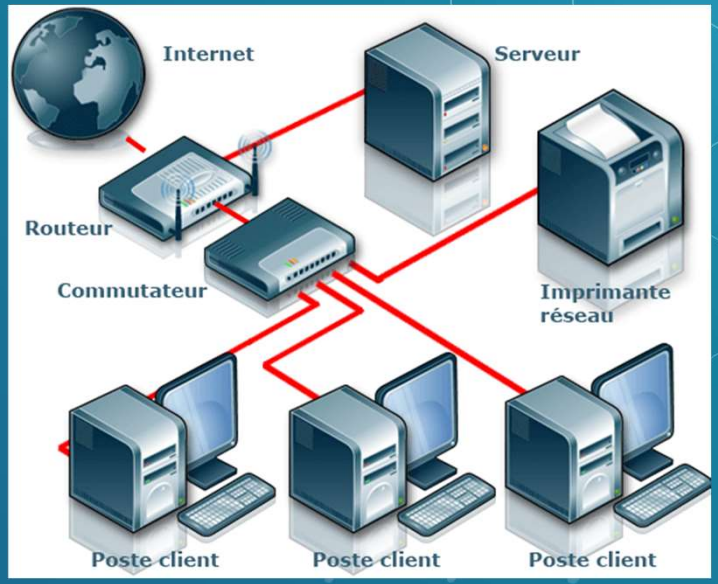
- Les attaques sur les couches réseau.
- La sécurité du LAN.
- Les VLANs.
- Concept AAA & Architectures.
- Le Firewall.
- La DMZ.
- Les Proxy.
- Sécurisation du réseau d'Administration.
- Les UTM
- Modèle d'architecture.
- La sécurité Cloud.

3 Exemples de menaces sur les communications réseaux



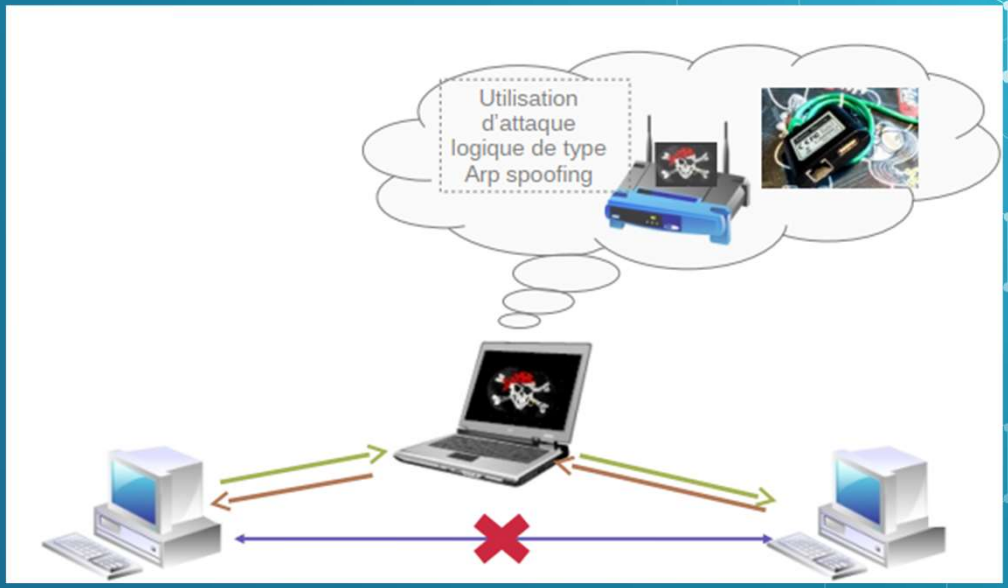
Corruption
Interception
Indisponibilité

Indisponibilité
Accès frauduleux



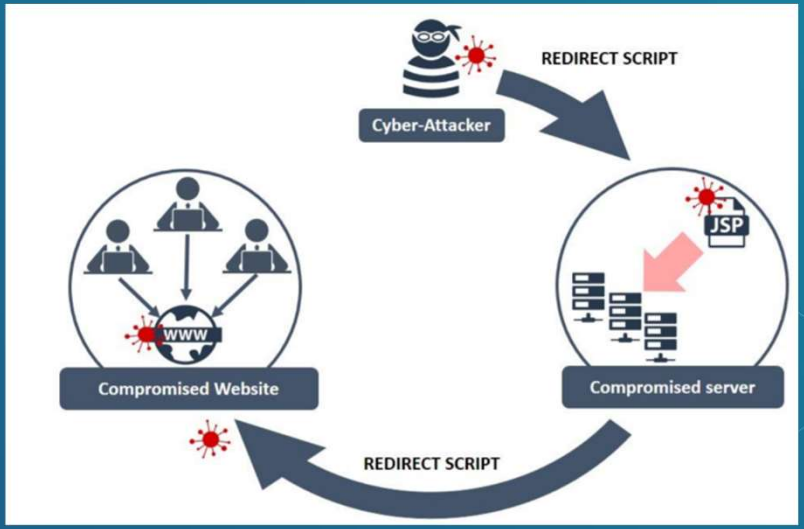
3 Man In The Middle (MITM)

- Ecoute du trafic
  - Récupération de MDP
  - Analyse des centres d'intêrets
  - Interception de communications
- Modification du trafic
  - Modifie les informations envoyés
  - Modifie les informations reçues
- Suppression du trafic
  - Denis de service
  - Réduction de la sécurité (STARTTLS)



3 Attaque du point d'eau

- SaL'attaque dite « du point d'eau » consiste pour l'attaquant à piéger un site web public qu'il sait être visité par la ou les victimes qu'il cible en particulier. Cela lui évite d'entrer en contact direct avec ses victimes (notamment en envoyant un email de phishing, par exemple, qui est facilement repérable). Il s'agit donc d'une attaque indirecte, qui peut faire de nombreuses victimes collatérales (à commencer par le site web infecté pour l'occasion). Afin d'éviter d'être trop vite détectés, certains attaquants avancés n'infectent toutefois que les visiteurs correspondants au profil de leurs victimes (origine de la visite, adresse IP appartenant à l'entreprise ciblée, etc.).



3 Quelques moyens de protection du LAN (Couche 2 & 3)

- **Table ARP** fixe sur certains équipements :
- Segmentation du réseau en VLANs physique (802.1Q) et sous –réseaux logiques.
- Activation du protoole Spanning Tree Protocol avec redondance des switch coeur de réseau.
- Activation des fonctions de sécurité sur les switch:
  - Port Sécurty Mac-LIMITING.
  - Fonction anti “Rogue DHCP” → (DHCP Snooping)
  - Fonction anti-scan
  - Etc .
- Mise en place d’une architecture 802.1x
- Chiffrement des données entre deux swtichs via le protocole MacSec.
- Utilisation IPV4 avec les translations d’adresse (NAT 1 pour N ou PAT)

3 Les principes des vLANs

Un VLAN (Virtual Area Network) Ethernet est un réseua local virtuel.

La communication n'est autorisée qu'entre machines d'un même VLAN.

Les communications Inter-VLAN doivent transiter par un routeur.

Les VLANs servent :

- A **diffénrecier des communications** transitant dans un même réseau physique
- A **maitriser les flux et le cloisonnement** des comunications .

Plusieurs techniques existent, la plis connue et la plus fiable étant la norme **802.1Q**

Les VLANs introduisent la **notion de segmentation virtuelle** selon des critéres prédefinis (Ports, adresses Mac, Etc)

L'affectation peut être introduite manuellement (Statique) ou automatiquement (Dynamique)

3 Cloisonnement de VLANs, Exemple de matrice de Flux

	VLAN 1 Direction	VLAN 2 Compta	VLAN 3 Prod
VLAN 1 Direction	√	√	√
VLAN 2 Compta	X	√	X
VLAN 3 Prod	X	X	√

3 Authentification dans un réseau

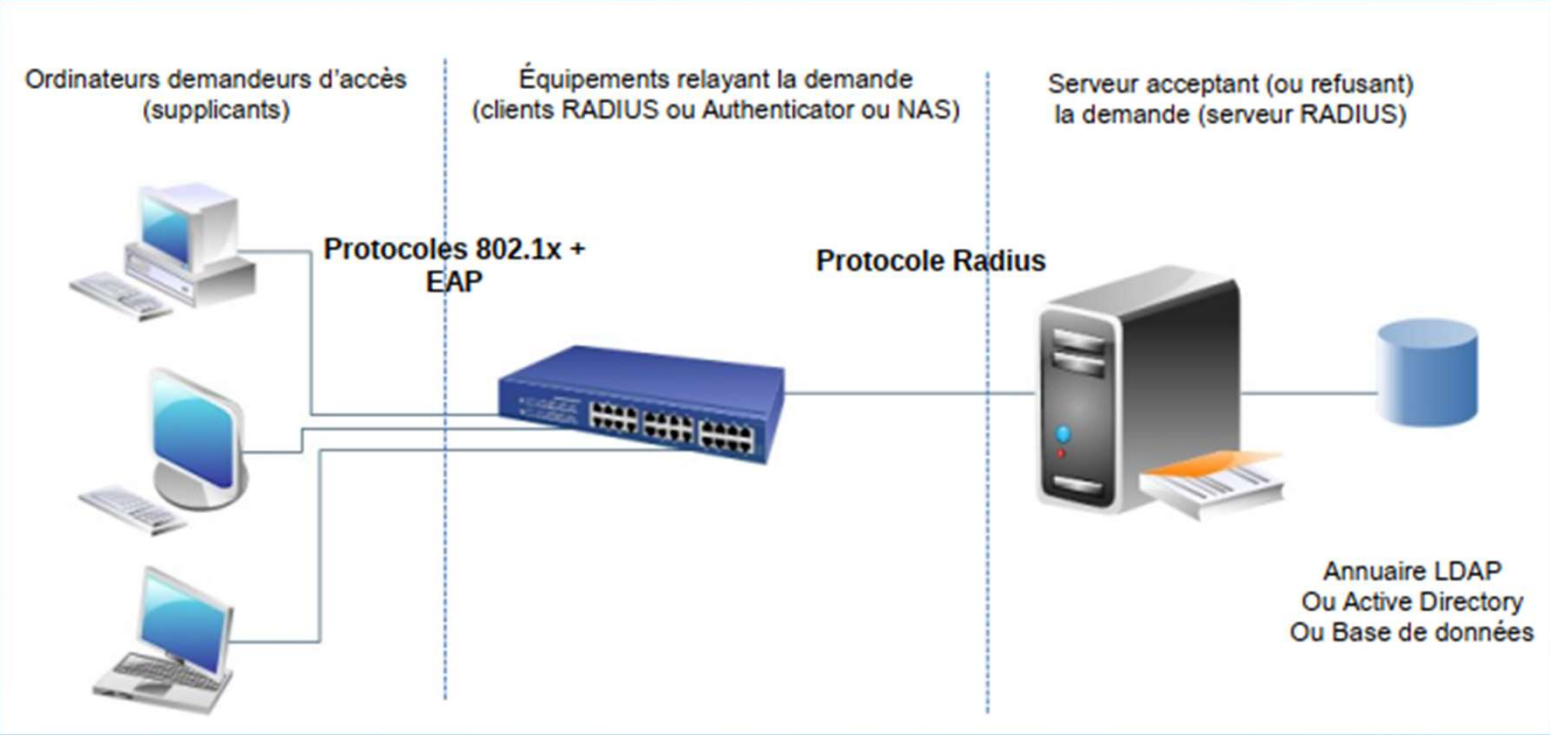
Constats :

- Les intrusions physiques sont les attaques réseau les plus courantes.
- Faiblesse du modèle Ethernet (LAN):
- Pas de contrôle d'accès sur les interfaces physiques réseau
- Faiblesse des protocoles WiFi (familles des normes 802.11) :
- WEP, WPA : un « secret » identique pour tous les accès WiFi

Solution qui permet d'authentifier un utilisateur souhaitant accéder à un réseau :

- filaire : 802.1x + Radius
- Wi-Fi : WPA-Enterprise = WPA2 + 802.1x + Radius

3 Les acteurs d'un authentification Radius / 802.1x



3 Network Admission Control (NAC)

Système **autonome** de **contrôle d'accès avancé** à un réseau qui applique des **règles d'accès ou d'exclusion** à un réseau en fonction de standards de sécurité définis dans un **processus global**

Ses fonctions :

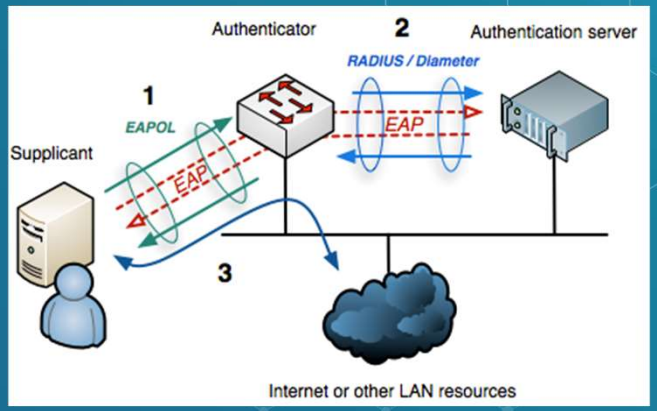
- Vérification de l'état et la légitimité d'un poste à se connecter au réseau
- Unité d'accès réseau : Contrôle, au niveau réseau, l'authentification des postes
- Serveur de politiques : Gère la politique d'accès au réseau (AAA, Radius, etc)
- Système d'administration centralisé

Son rôle :

- Empêcher un système non légitime de se connecter sur le réseau
- Limiter la propagation de malware
- Exclure les machines infectées du réseau

Quelques solutions :

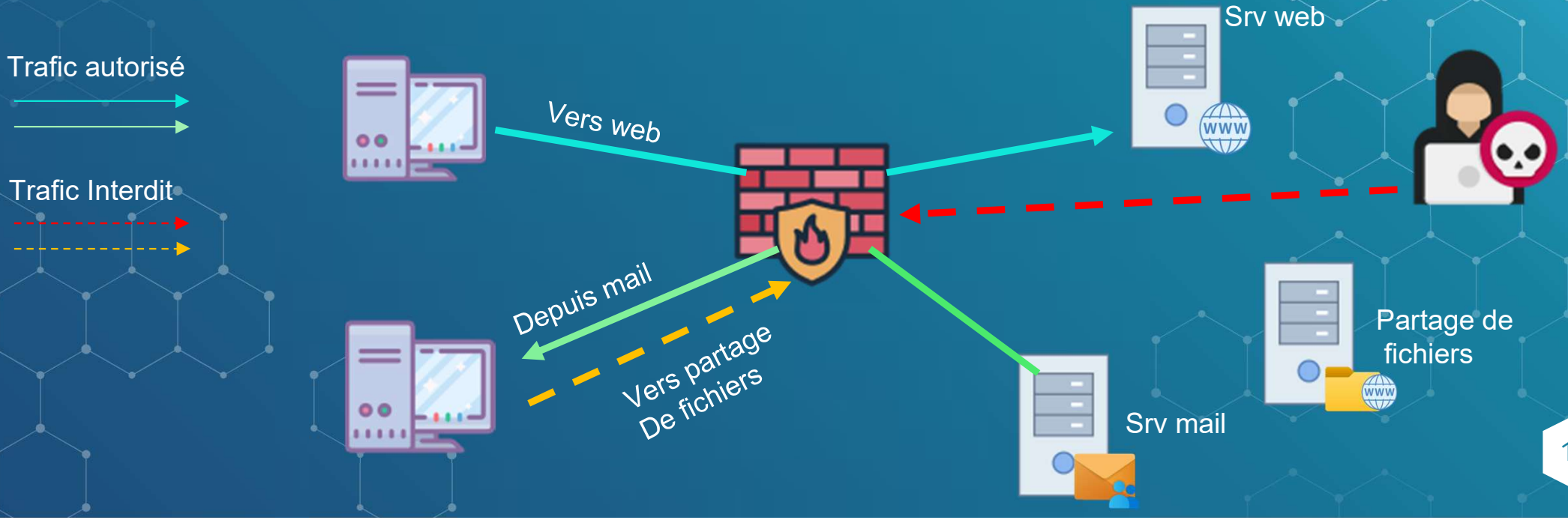
- Cisco ISE
- Aruba ClearPass Policy Manager
- The Forescout Platform
- FortiNAC



3 Le Firewall, la pierre angulaire de la sécurité

- Contrôle les flux pour leur permettre ou non d'accéder à un réseau (Accept, Drop, Deny) avec une **politique de sécurité**

- IP Source + Port source → IP Destination + Port destination = sens du flux associé
- Attention à l'ordre des règles



3 Modèle de filtrage réseau

Ordre	Contenu
Section n°1	Règles d'autorisation des flux à destination du pare-feu (anti-lockout)
Section n°2	Règles d'autorisation des flux émis par le pare-feu (anti-lockin)
Section n°3	Règle de protection du pare-feu (self-defense)
Section n°4	Règles **temporaires** de tests ou de debogage (test)
Section n°5	Règles d'autorisation des flux métiers (production)
Section n°6	Règles « antiparasites » (noise canceling)
Section n°7	Règle d'interdiction finale (clean up)

N.B. : DAT-NT-006/ANSSI/SDE/NP du 30 mars 2013

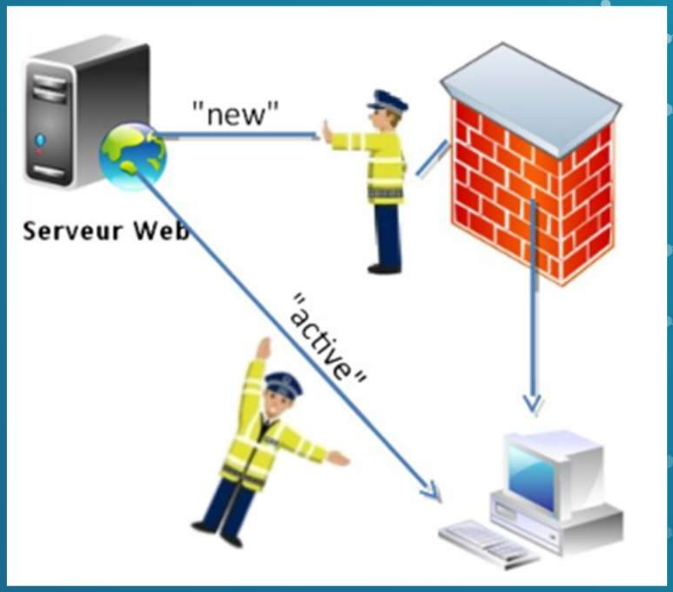
3 Firewalls : les évolutions passées

Firewalls stateless (statiques)

- Filtrage simple de paquets
- Tous les paquets sont inspectés

Firewall stateful et à filtrage dynamique

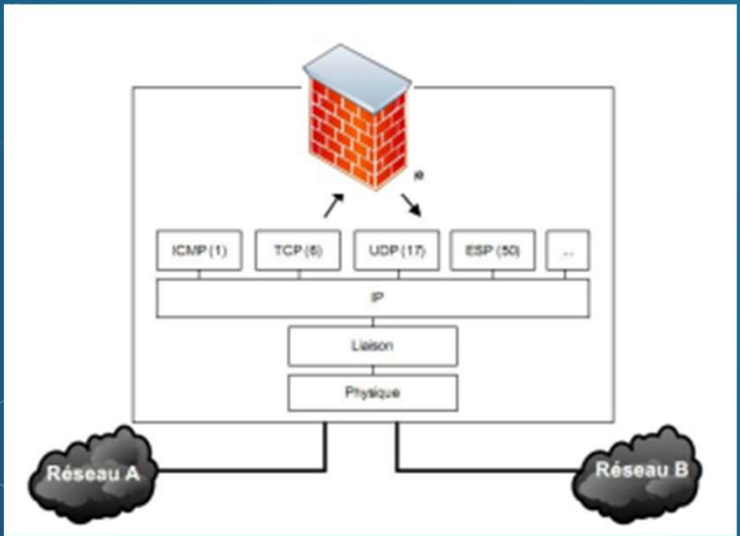
- Utilise « l'état » d'une connexion pour appliquer ou non une règle



3 Firewalls : les évolutions en cours

Firewalls dits « classiques » (SPI)

• Protocoles de niveau 4 utilisés : (TCP, UDP, ICMP) + Ports

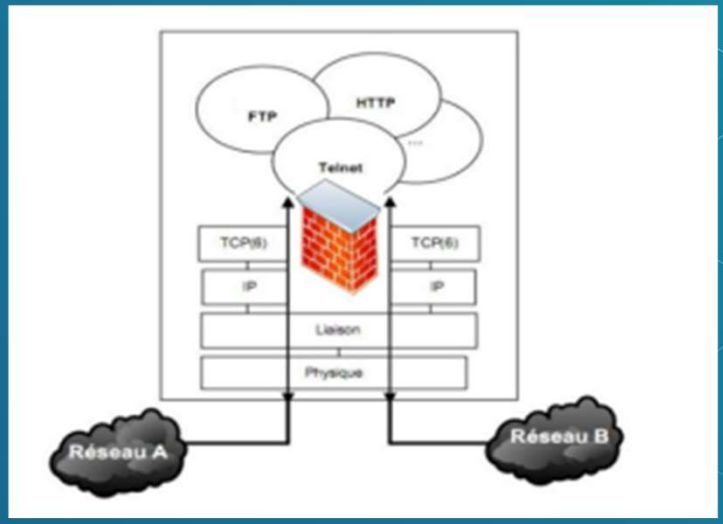


Firewalls applicatifs (ou layer7)

• Analyse de l'entête des données pour reconnaître une application

Firewalls 3ème génération (DPI)

● Analyse tout le contenu du paquet pour vérifier sa conformité



3 Firewall personnel vs Firewall matériel

- Le firewall personnel protège uniquement le système sur lequel il est installé
- Le firewall matériel protège un réseau (donc plusieurs postes)

Avantages du firewall personnel :

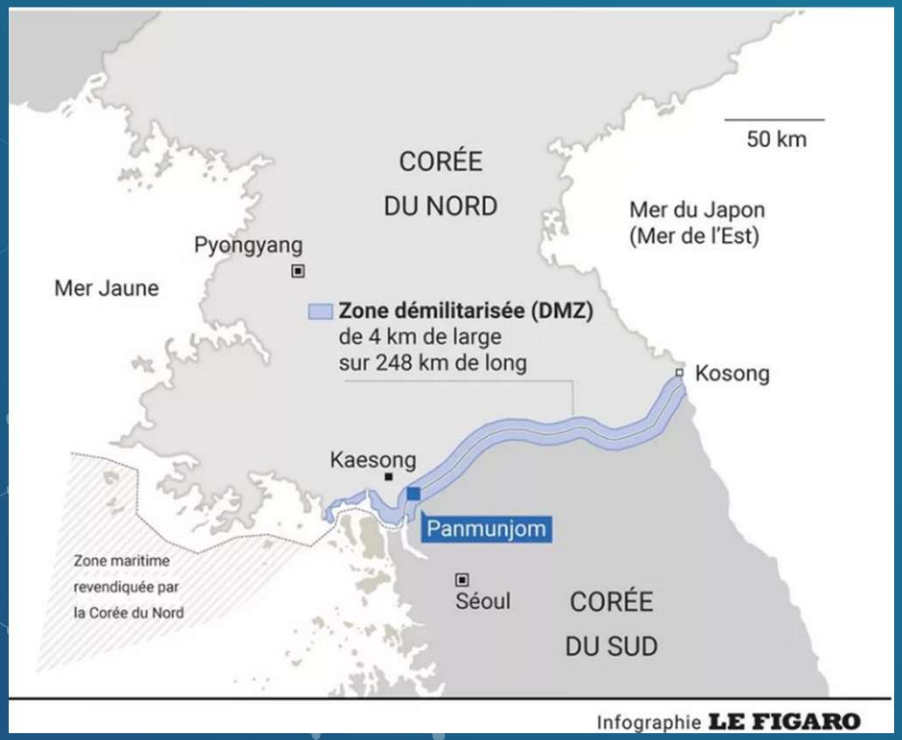
- contrôle efficace des logiciels qui se connectent sur Internet ;
- nativement « Layer7 » ;
- natif dans les OS (iptable pour Unix, le pare-feu de Windows).

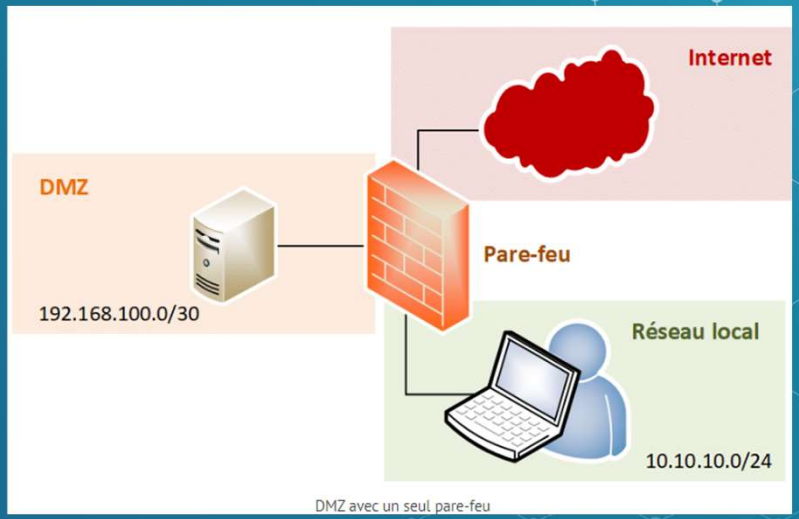
Inconvénients du firewall personnel :

- facilement désactivable ;
- le flux n'est pas bloqué à l'entrée du réseau s'il n'est pas couplé avec un firewall matériel

3 La DMZ

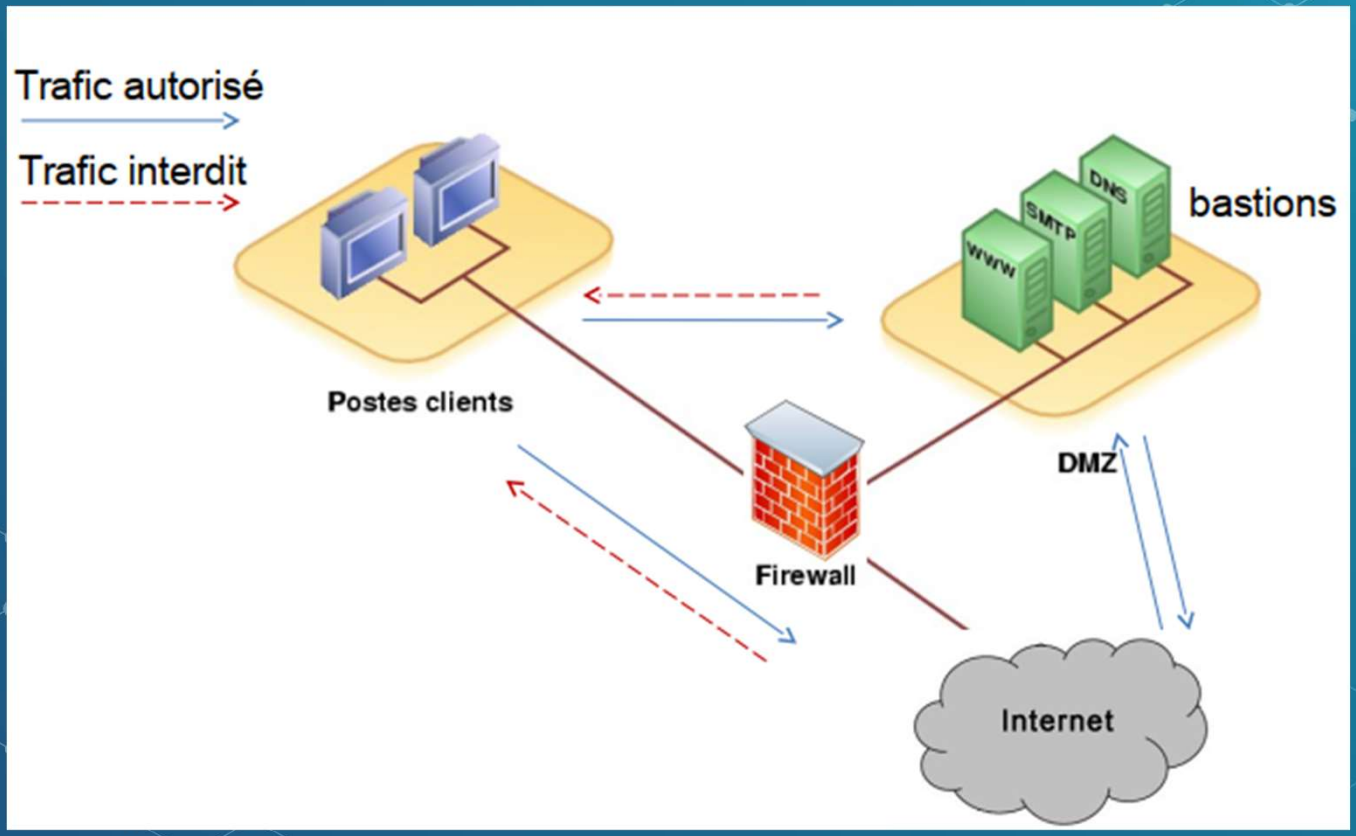
C'est une Zone **Démilitarisée** (DMZ = DeMilitarized Zone) du réseau local dans lequel des **serveurs** sont exposés et **accessible depuis Internet**.





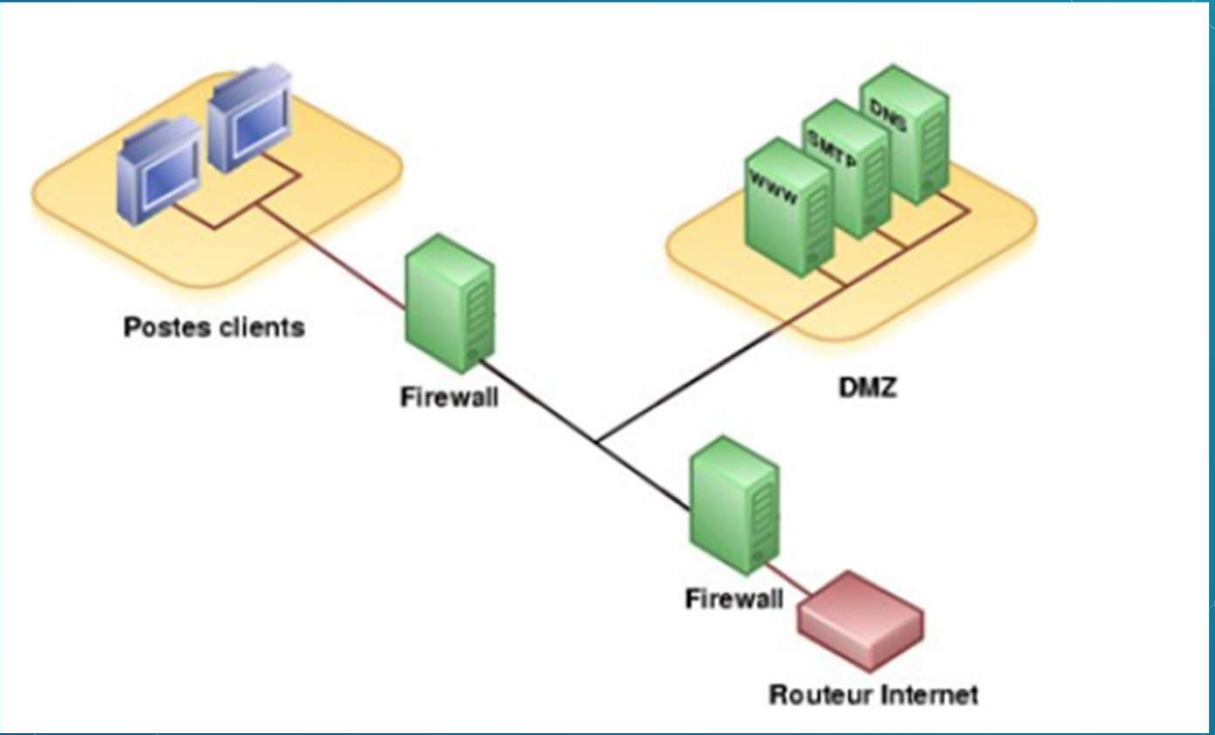
DMZ avec un seul pare-feu

3 Mode « Screened Subnet »



3 Mode « Multi-homed Firewall »

Double cloisonnement : Les zones LAN, DMZ et WAN sont séparées par un pare-feu



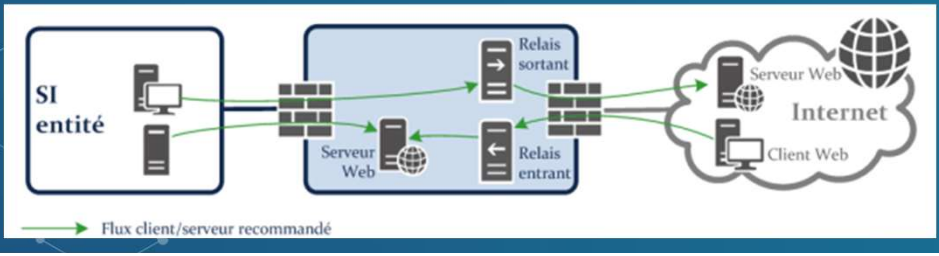
3 Menaces considérées

Pour de nombreuses entités, l'interconnexion de leur SI avec Internet est nécessaire, tant ce dernier offre une richesse de services et d'opportunités numériques. Néanmoins il constitue aussi, de manière incontestable aujourd'hui, une source de menaces. Parmi les plus courantes, il est possible de citer :

- l'exfiltration de données depuis le SI de l'entité vers Internet, portant atteinte à leur confidentialité ;
- l'intrusion pour porter atteinte à l'intégrité ou la disponibilité du SI de l'entité ;
- l'usurpation d'identité en accédant à des ressources de l'entité pour rebondir et mener des attaques vers d'autres cibles ;
- le déni de service pour nuire à la disponibilité de l'accès Internet et donc à la productivité ou à l'image de l'entité ;
- l'accès par les collaborateurs à des sites Web interdits par la charte d'utilisation interne voire par la loi

3 Les recommandations de l'ANSSI 1/2

R1 - Déterminer l'ensemble des services nécessitant l'interconnexion à Internet.
R2 - Déployer un pare-feu maîtrisé entre la DMZ et le routeur d'accès Internet.
R3 - Déployer un pare-feu maîtrisé entre le SI de l'entité et la DMZ.
R4 - Rendre incontournable la passerelle Internet sécurisée
R5 - Déployer si nécessaire des pare-feux intermédiaires dans la passerelle Internet sécurisée
R6 - Cloisonner les flux au sein de chaînes de traitement homogène
R7 - Respecter une cinématique sécurisée des flux
R8 - Procéder à une rupture protocolaire des flux
R9 - Procéder à une analyse des flux en fonction de l'analyse de risque.
R10 - Ne pas exposer d'annuaire du SI de l'entité aux ressources de la passerelle Internet sécurisée.
R11 - Évaluer les risques de mutualisation par virtualisation
R12 - Déployer une passerelle Internet sécurisée à base d'équipements physiques dédiés par zone.
R12* - Déployer une passerelle Internet en acceptant la mutualisation de certains équipements de commutation
R13 - Proscrire toute mutualisation des pare-feux interne et externe
R14 - Homogénéiser les passerelles Internet sécurisées dans le cas d'une architecture multi-zones.
R15 - Utiliser une offre qualifiée par l'ANSSI pour les fonctions relais externalisées 23 .



3 Les recommandations de l'ANSSI 2/2

R15 - Évaluer rigoureusement les risques d'une offre non qualifiée par l'ANSSI pour les fonctions relais externalisées.
R16 - Administrer de manière sécurisée la passerelle Internet sécurisée.
R17 - Garantir la disponibilité attendue grâce à la résilience des accès opérateurs.
R18 - Mettre en œuvre des contre-mesures aux attaques en déni de service.
R19 - Utiliser un routage statique au sein de la passerelle Internet sécurisée.
R20 - Ignorer les paquets refusés par la politique des pare-feux externes .
R21 - Masquer l'architecture interne vis-à-vis d'Internet.
R22 - Mettre en place un serveur mandataire pour l'accès aux contenus Web.
R23 - Authentifier tous les accès aux contenus Web.
R24 - Prévoir des restrictions pour les accès non authentifiables.
R25 - Étudier la mise en place d'une interception TLS maîtrisée.
R26 - Centraliser et sécuriser les journaux liés aux accès Web.
R27* - Déployer des postes de rebond pour la navigation Web.
R28 - Maîtriser le déploiement et l'exploitation du ou des navigateurs Web.
R29 - Configurer le serveur mandataire en mode explicite.
R30 - Empêcher le contournement du serveur mandataire.
R31 - Appliquer une politique de configuration locale du serveur mandataire

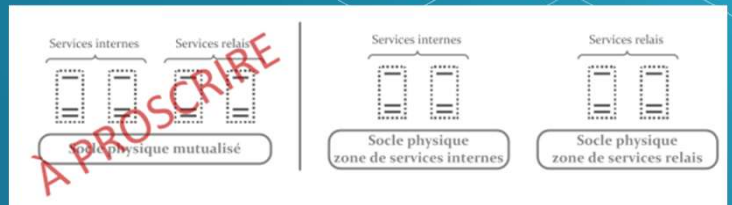
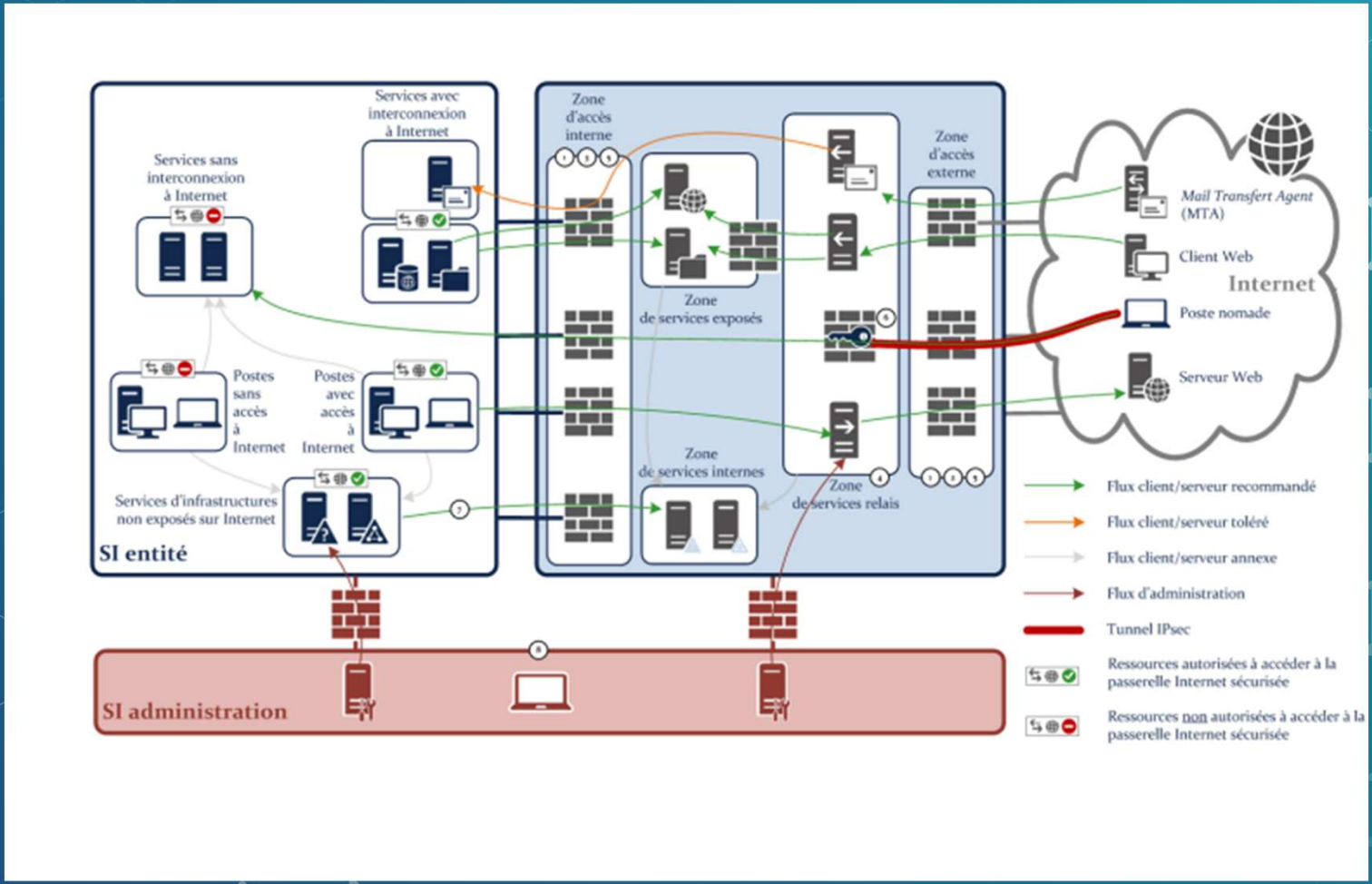


FIGURE 2.11 – Principes de (non) mutualisation par virtualisation

3 Architecture multi-services de la passerelle Internet sécurisée



3 Le proxy ou Mandataire

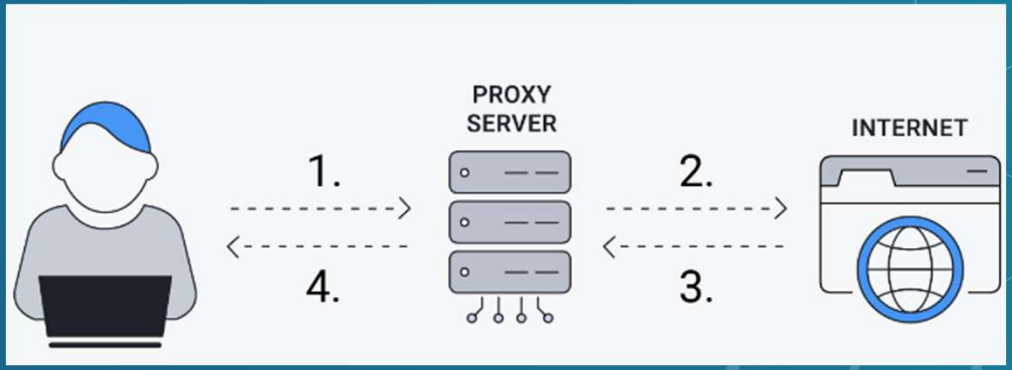
Un serveur proxy (traduction française de «proxy server», appelé aussi «serveur mandataire») est une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet.

Principe de fonctionnement :

1) Le client se connecte au serveur proxy et lui donne sa requête
2) Le serveur proxy se connecte au serveur distant
3) Le serveur distant donne sa réponse au proxy
4) Le proxy transmet la réponse au client

Fonctionnalités :

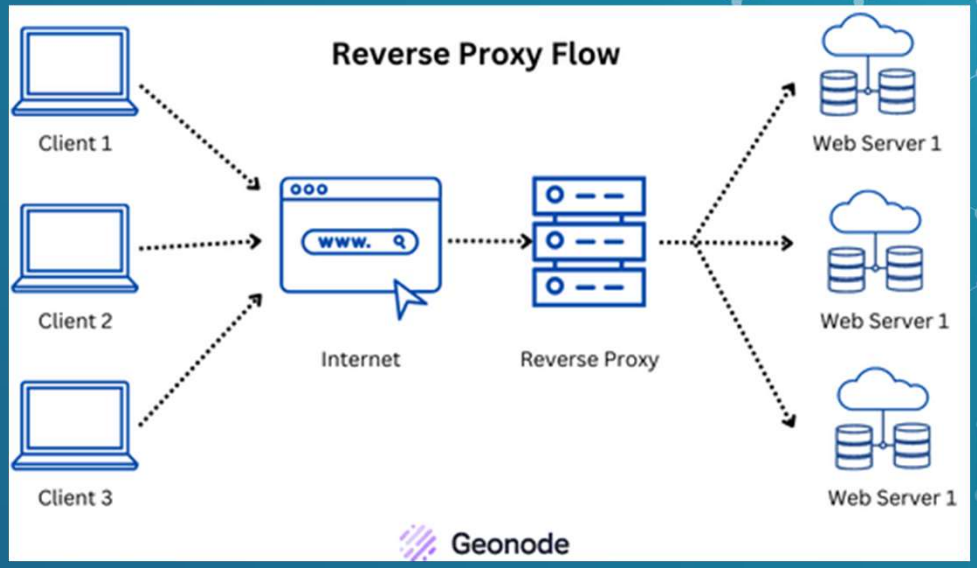
- Cache
- Filtrage d'URL
- Filtrage de contenu
- Authentification



3 Le Proxy inverse, « Reverse Proxy »

Le proxy inverse, « reverse proxys »
Permet aux utilisateurs d'Internet d'accéder **indirectement** à des serveurs internes
• Protection **des attaques directes** de l'extérieur avec la fonction de **WAF** (Web Appliance Firewall) :

- **Contrôle des données envoyées** à l'application web
- **Comparaison** des données envoyées par l'application web et des données retournées à l'utilisateur
- **Sécurité proactive**
- **Cache** qui permet de soulager la charge du serveur
- **Load balancing** qui permet de répartir la charge.



3 Déchiffrement des flux TLS : aspects juridiques

Encadrement par la CNIL :

- **Transparence et loyauté** de l'employeur : information et consentement individuel (charte informatique et sensibilisation)
- Une gestion stricte des **droits d'accès** des administrateurs sur les flux déchiffrés
- Si le flux déchiffré est un **mail noté « Personnel »**, interdiction de le lire

⇒ signifie une sensibilisation du personnel sur l'utilisation des mails professionnels à titre personnel

- Liste blanche de sites dont le flux ne sera pas déchiffré (sites bancaires personnels, webmail perso) sinon, interdiction d'accéder au site (liste noire du proxy).
- Sécurisation des logs conservés à des fins d'analyse
- **Note technique de l'ANSSI de 2014** sur les recommandations de sécurité concernant l'analyse des flux HTTPS :
- Le certificat utilisé pour l'interception des flux TLS doit respecter différentes règles (AC non auto-signé, algorithmes de chiffrement forts ...)

3 Un cloisonnement « fin » et un filtrage entre les composants

- **Table ARP** fixe sur certains équipements :
- Segmentation du réseau en VLANs physique (802.1Q) et sous –réseaux lMettre dans des VLANs différents le réseau de production et supervision/administration ;
- Encore mieux : séparer le réseau d'administration du réseau de supervision.
- Si possible, le réseau de supervision et d'administration doivent être sur un réseau distinct du réseau de production :
  - Nécessite deux cartes réseaux sur chaque équipement.
- Le réseau de supervision et d'administration ne doivent pas accéder à l'Internet (excepté pour les mises à jour système).
- Si un équipement doit être administré à distance, utiliser des canaux sûrs :
  - VPN
  - Bastion/serveur de rebond
  - Règle stricte de sécurité avec le Firewall

3 Serveur de Rebond / Bastion

- Appelé **aussi Privileged account and session management** (PASM)
- Permettent d'autoriser **une seule IP** à se connecter aux équipements (simplification des règles des pares-feux).
- **Multi-protocoles** : SSH, RDP, HTTPS, VNC ...
- Gèrent les comptes de manière nominatives et règlent le problème des comptes génériques (root...).
- Permettent d'enregistrer des log de connexion mais aussi les sessions d'administration des équipements.
- Permettent des contrôles d'accès très fins (plages horaires, groupes d'utilisateurs, par actions ...)

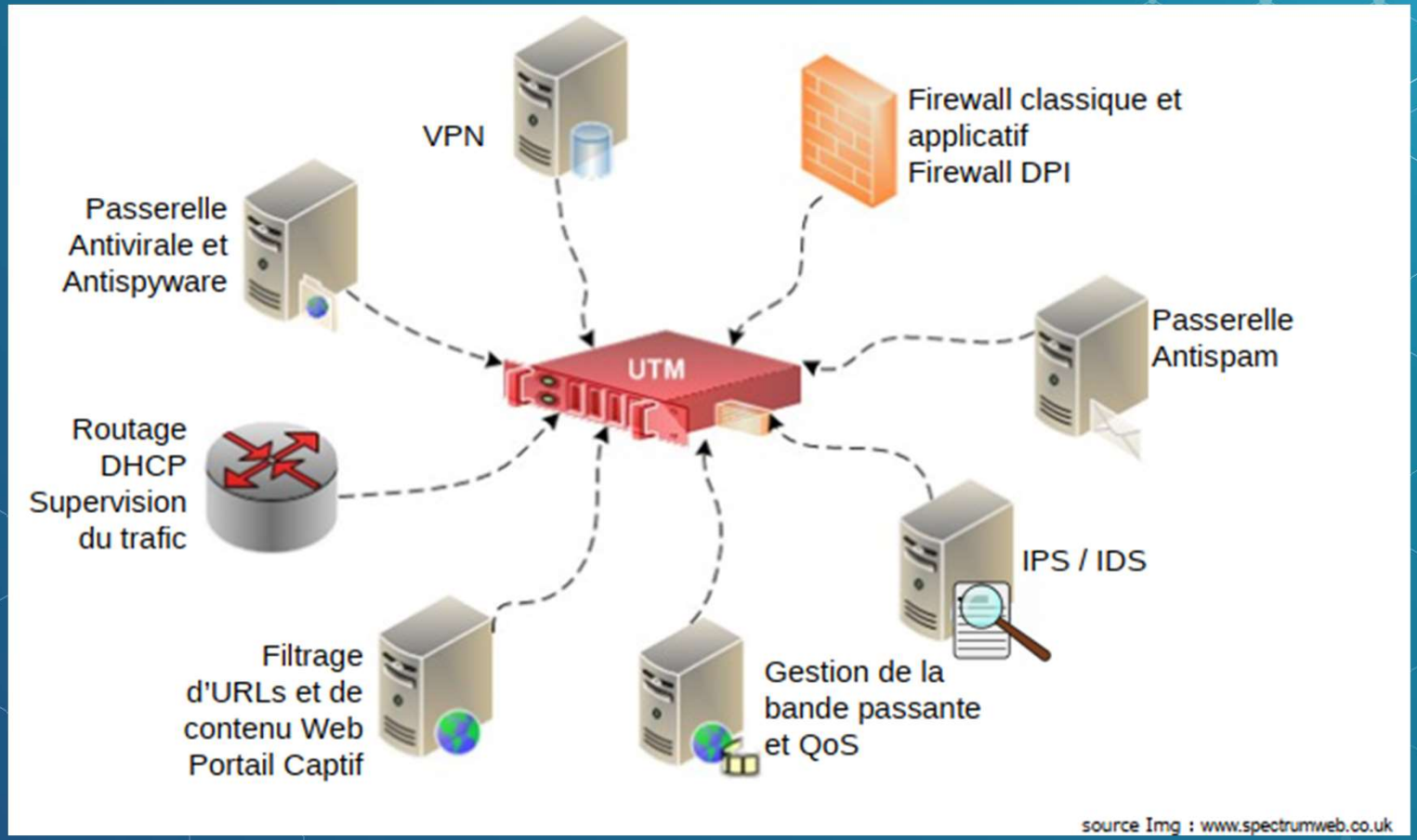
- <u>Quelques solution leader :</u>

CYBERARK

Secure Link

WALLIX
CYBERSECURITY SIMPLIFIED

3 Evolution technologique des firewalls : les pare-feux « Nouvelle Génération »

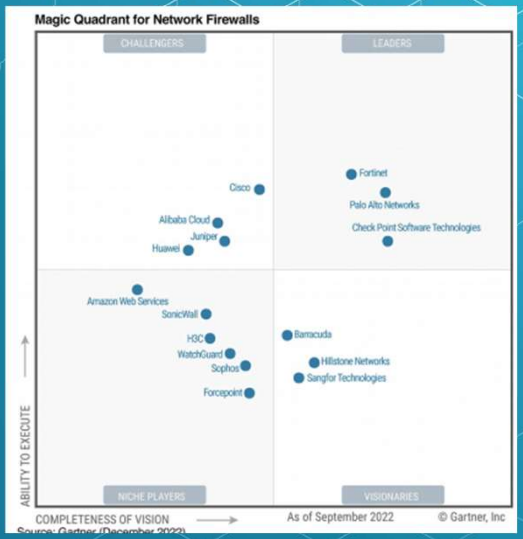


3 Les UTM

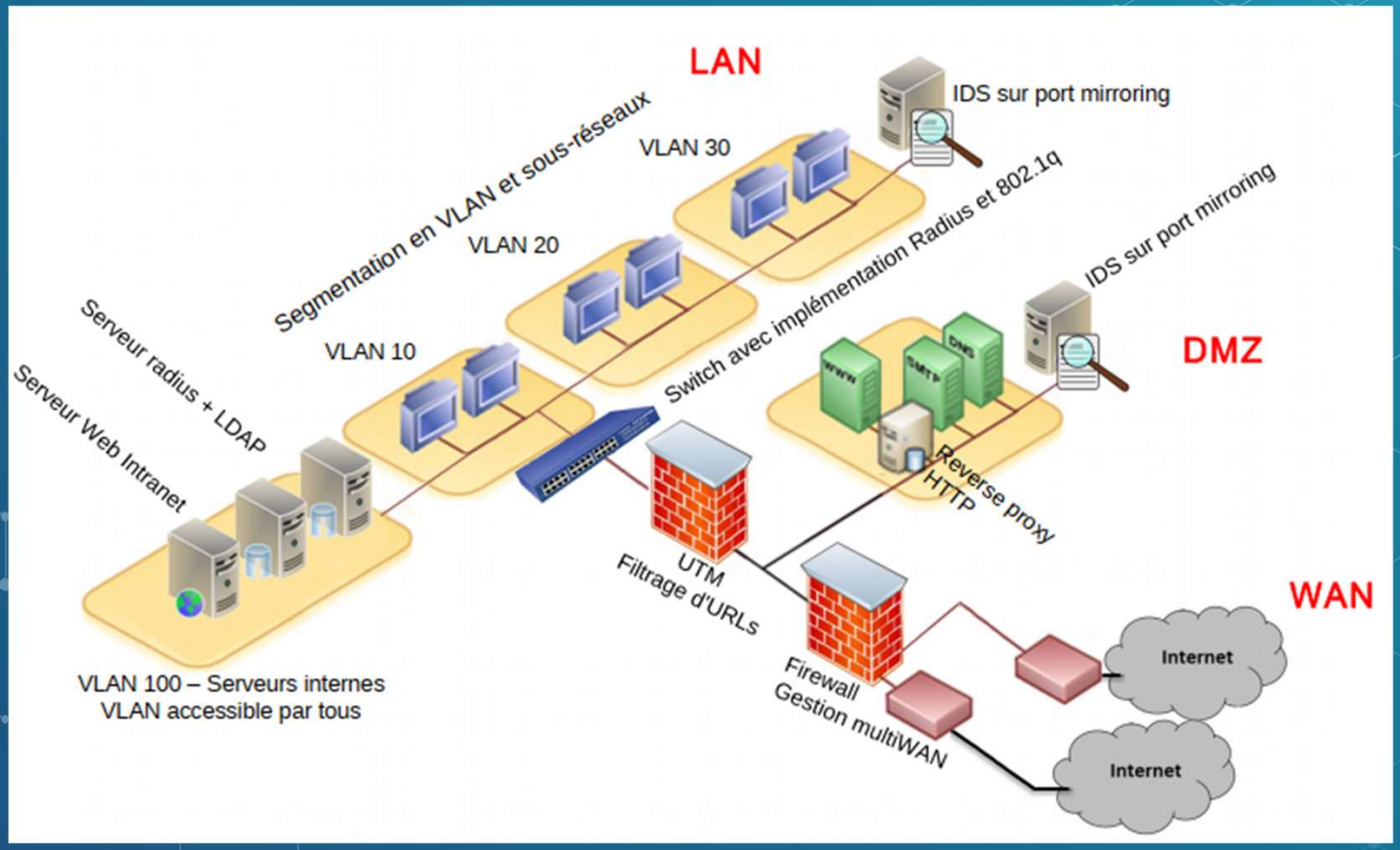
Comment faire son choix ?

10 principales fonctionnalités que doit posséder votre prochaine UTM :

1. Identifier et contrôler les applications sur n'importe quel port (Firewall niveau 7)
2. Identifier et contrôler tous les moyens de contournement (Canaux cachés - IPoICMP, IPoDNS...)
3. Déchiffrer les flux SSL sortants (filtrage d'URLssur SSL) et contrôler les flux SSH (interdire les tunnels)
4. Contrôler les différentes fonctions d'une même application (Ex. Gmail/Gtalk)
5. Gérer systématiquement le trafic inconnu (détection des C&C et bots)
6. Détecter les virus et les logiciels malveillants dans toutes les applications, sur tous les ports
7. Offrir la même visibilité et les mêmes outils de contrôle pour les utilisateurs et équipements
8. Simplifier la sécurité réseau tout en intégrant le contrôle des applications (Gestion des droits, AAA)
9. Fournir le même débit et les mêmes performances une fois le contrôle des applications activé
10. Assurer les mêmes fonctions de pare-feu qu'il s'agisse d'un environnement physique ou virtuel



3 Exemple d'architecture sécurisé



3 La sécurité du Cloud

Les principaux risques

- **Sécurité** des données :
- Qui a accès aux données ?
- Comment sont-elles isolées des autres données ?
- Quels moyens pour détecter une fuite de données ?
- Quels moyens de chiffrement ?
- Quels moyens d'authentification ?
- Récupération des données en cas de perte du service ? Quels délais ?
- Mise au rebut, destruction des données
- Pérennité et **viabilité du fournisseur**
- **Perte de contrôle** des DSI sur les infra et services :
- Quels sont les moyens de supervision mis à disposition ?
- Droit de regard et de contrôle sur les personnels du fournisseur ?
- Quelles garanties pour la correction des vulnérabilités ?
- Quelle gestion des incidents de sécurité ?
- Configuration par défaut, APIs vulnérables …
- Comment faire respecter les process aux utilisateurs finaux ?
- **Localisation** des données et **problématiques juridiques** :
- Sous quel régime juridique local se trouvent les données ?
- Quels moyens de traçabilité de l'accès aux données afin de répondre aux injonctions de la justice (raisons fiscales ou autres d'ordre juridique) ?
- Conformités légales : Audits externes ? Certification de sécurité ?

3 La sécurité du Cloud – Principaux vecteurs d'attaques

- Fuite d'**identifiants**, moyens d'authentification peu sécurisés, usurpation d'identité, non respects des process par les utilisateurs entraînants des vulnérabilités sur l'authentification, bruteforce des mots de passe
- Fuite de **ressources** publiées sur les IaaS **publiques**
- Mauvaises **configurations** des hyperviseurs ou des VM
- Mauvaise **gestion de droits** permettant le stockage de fichiers malveillants (site de phishing, script de minage de crypto-monnaie, ransomware, ouverture de shell sur le serveur ...)
- Exploitation des vulnérabilités applicatives des solutions Cloud et des APIs
- …
- **Principal objectif des attaques :** récupération d'information

3 Cloud de confiance

Stratégie annoncée le 17 Mai 2021

- S'organise autour de **2 piliers**
- Garantir la sécurité des données des citoyens et des entreprises français et garantir la souveraineté numérique
- Accès aux meilleurs services mondiaux

Label Cloud de Confiance

- Qualification délivrée par l'ANSSI
- S'appuie sur 2 dimensions
- Dimension **technique** :

- garantie de protection maximale des données
- conformité aux exigences du **référentiel SecNumCloud** de l'ANSSI

- Dimension **juridique** :

- garantie d'indépendance aux lois extraterritoriales

- Serveurs opérés en France
- Entreprises opérant en Europe et possédées par des européens
- Licences technologiques des *keys players* américains possibles pour les entreprises européennes

3 Autres référenciels

Critical Security Controls ® Cloud Companion Guide

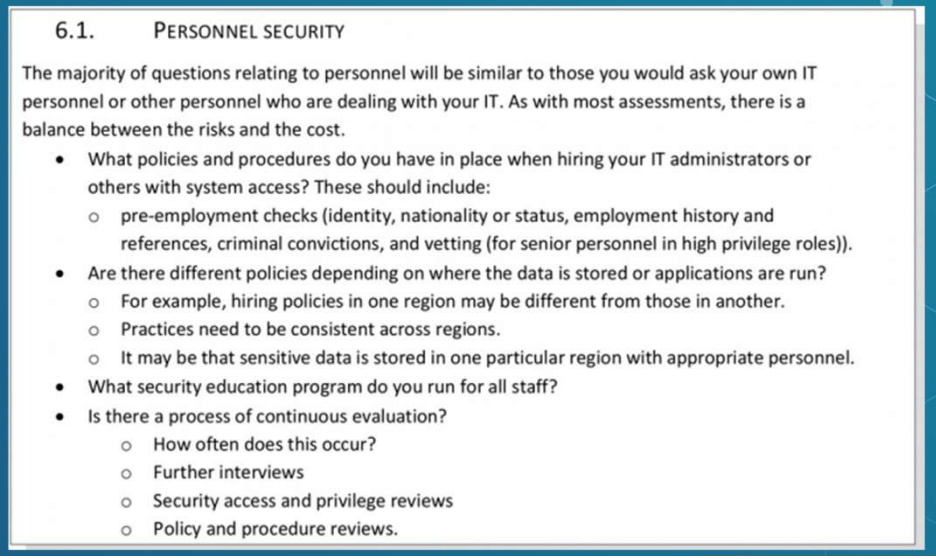
- 20 thèmes principaux eux-même subdivisés en plusieurs points de contrôle.

National Cyber Security Centre ® Cloud security guidance collection

- 14 principes.
- Propose une approche rapide de l'évaluation de la sécurité d'un service avec une série de questions essentielles.

ENISA - Cloud Computing Information Assurance Framework

- Fournit une liste de questions à poser à son fournisseur pour s'assurer de son niveau de sécurité.



6.1. PERSONNEL SECURITY

The majority of questions relating to personnel will be similar to those you would ask your own IT personnel or other personnel who are dealing with your IT. As with most assessments, there is a balance between the risks and the cost.

- What policies and procedures do you have in place when hiring your IT administrators or others with system access? These should include:
  - pre-employment checks (identity, nationality or status, employment history and references, criminal convictions, and vetting (for senior personnel in high privilege roles)).
- Are there different policies depending on where the data is stored or applications are run?
  - For example, hiring policies in one region may be different from those in another.
  - Practices need to be consistent across regions.
  - It may be that sensitive data is stored in one particular region with appropriate personnel.
- What security education program do you run for all staff?
- Is there a process of continuous evaluation?
  - How often does this occur?
  - Further interviews
  - Security access and privilege reviews
  - Policy and procedure reviews.