INTITULÉ : HACKING ET SECURITE - NIVEAU 1

PRÉNOM : ARTHUR

NOM : MENDJANA

Qualification des Services Intellectuels OPQF

Fédération de la Formation Professionnelle

Présentation du Module

❑ **Public concerné** :

Techniciens informatique, gestionnaires de parc, techniciens d'exploitation, techniciens de maintenance…

❑ **Objectifs :**

Pirates et attaques informatiques : savoir les repérer et les contrer

❑ **Modalités pédagogiques :**

Cours magistral / Exercices / Travaux pratiques

❑ **Prérequis**

Connaissance de la structure matérielle et architecturale d'un ordinateur

PROGRAMME

1- ENVIRONNEMENT ET ACTEURS

- Objectif d'une attaque et scénario d'attaque
- Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS, ...
- Rappel de protocole TCP/IP

2- MATÉRIEL DE SÉCURISATION

- Sécurisation des accès physique (802.1X)
- ACL de niveau 2 et 3
- Firewall et règles de filtrage
- La Translation d'adresse NAT et le PAT
- DMZ et multi-DMZ
- Surveillance par IDS/IPS et logs
- Architecture réseau sécurisée

PROGRAMME

3- SÉCURISATION DES ÉCHANGES

- Notion de cryptographie
- Fonctions de hachage
- SSL
- VPN réseau

4- PANORAMA DES TECHNIQUES DE HACKING

- Social Engineering ; Failles physiques (accès aux locaux, BIOS, …)
- Collecte d'information : (footprintig, fingerprinting, découverte réseau, recherche de faille)
- Vol de session (TCP Hijacking) ; Appel à procédures distantes
- Élévation de privilèges et permissions ; Gestion des mots de passe et cracking (brut force)

1- ENVIRONNEMENT ET ACTEURS

1- 1 Présentation, Objectif d'une attaque et scénario d'attaque

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour réduire la vulnérabilité d'un système contre les menaces accidentelles et intentionnelles . La sécurité consiste à assurer :

-La confidentialité : assurer que l'information ne sera lue que par les personnes autorisées.

-L'intégrité : assurer que les informations ne peuvent être modifier ou altérer que par les personnes autorisées.

-La disponibilité : assurer que l'information est disponible pour les personnes autorisées.

-L'authentification : vérifier l'identité d'un utilisateur pour lui associer des droits d'accès.

-La non-répudiation : garantir qu'aucun des correspondants ne pourra nier la transaction (l'envoi ou la réception des données)

1- 1 Présentation, Objectif d'une attaque et scénario d'attaque

Une *attaque* est l'exploitation d'une faille d'un système informatique à des fins non connus par l'exploitant du système et est généralement préjudiciable.

Les objectifs d'un attaquant sont diverses :

- ❑ Vols d'informations.
- ❑ Terrorisme, espionnage, chantage.
- ❑ Attirer l'attention.
- ❑ Avantages concurrentiels et bénéfices financiers.
- ❑ Vérification de la sécurité d'un système. (Pentest)

1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

Dans un monde où le progrès technologique avance à grande vitesse, où les gens, les entreprises, les organismes, les pays et même les objets sont de plus en plus connectés, les attaques informatiques sont de plus en plus fréquentes.

La question de la **cybersécurité** se pose à tous les niveaux et tend à devenir un enjeu essentiel ces prochaines années.
Pour mieux se protéger, il est primordial de savoir à quoi s'attendre, et donc de connaître à minima les attaques informatiques les plus courantes.

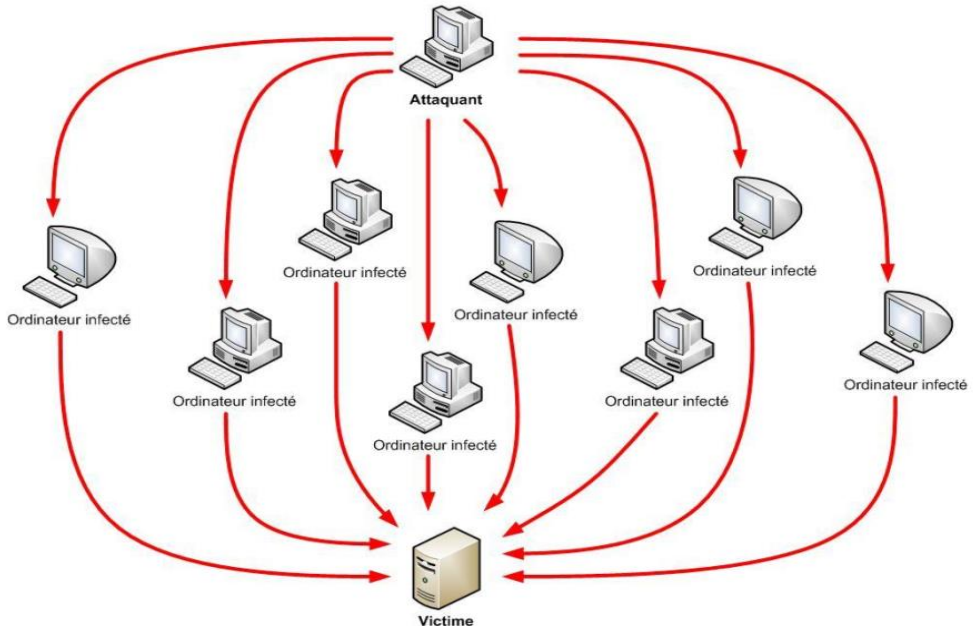
1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

1-2-1 Les attaques DDoS ou attaques par déni de service

Les attaques par **déni de service sont faites pour submerger les ressources d'un système** pour qu'il ne puisse plus répondre aux demandes. Contrairement aux autres attaques qui visent à obtenir ou à faciliter les accès à un système, l'attaque DDoS ne vise qu'à l'empêcher de fonctionner correctement. Cela ne procure pas d'avantages en soi à un pirate, si ce n'est la pure satisfaction personnelle.
Cela est différent si, par exemple, le site victime est celui de votre concurrent. L'avantage pour l'attaquant est alors bien réel.
L'attaque par déni de service peut aussi avoir pour but de lancer un autre type d'attaque.

- *Attaque qui vise à rendre un système ou une ressource indisponible en perturbant temporairement le réseau.*
  (IP bloqués et ports fermés)

- *motif concurrentiel en entreprise*



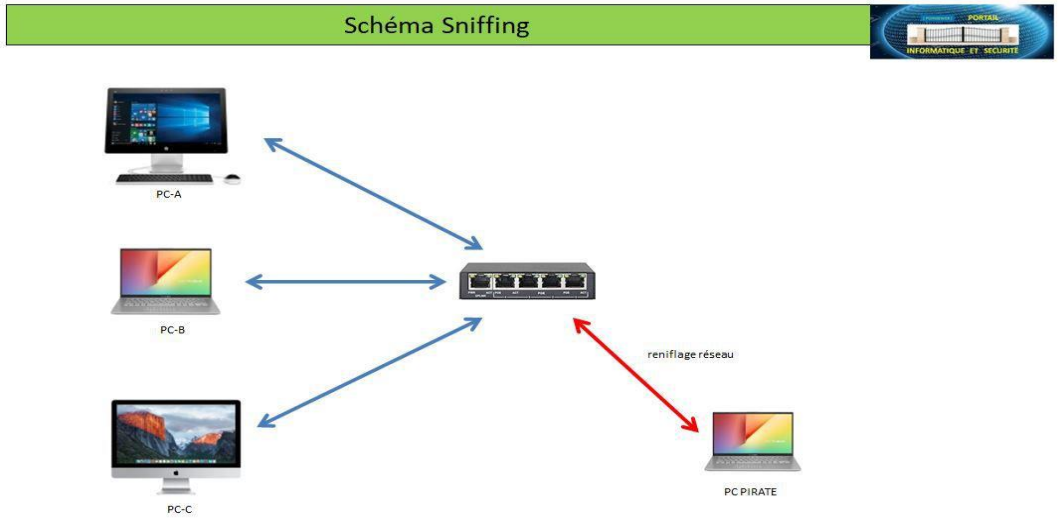
1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

1-2-2 Le Sniffing

Le reniflage (en anglais Sniffing) est une technique qui consiste à analyser le trafic réseau.

Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations (trafic). Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles.

E.g. Soit une entreprise possédant 100 ordinateurs reliés entre eux grâce à un hub. Maintenant, si un pirate écoute le trafic réseau entre 8h et 10h (heure de connexion du personnel), il pourra lire tous les noms d'utilisateurs ainsi que leur mot de passe.



1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

1-2-3 **Scanning**

Le scanning consiste à balayer tous les ports sur une machine en utilisant un outil appelé **scanner**.

Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts.

C'est un outil très utile pour les hackers. Cela leur permet de connaitre les points faibles d'une machine et ainsi de savoir par où ils peuvent attaquer. D'autant plus que les scanners ont évolué. Aujourd'hui, ils peuvent déterminer le système d'exploitation et les applications associées aux ports.

- *Peuvent voir quelle action*

tu es entrain d'effectuer

1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

1-2-4 Social Engineering

Le social engineering est l'art de manipuler les personnes. Il s'agit ainsi d'une technique permettant d'obtenir des informations d'une personne, qu'elle ne devrait pas donner en temps normal, en lui donnant des bonnes raisons de le faire.

Cette technique peut se faire par téléphone, par courrier électronique, par lettre écrite, ... Cette attaque est souvent sous estimée puisqu'elle n'est pas d'ordre informatique. Pourtant, une attaque par social engineering bien menée peut se révéler très efficace. Elle n'est donc pas à prendre à la légère

1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

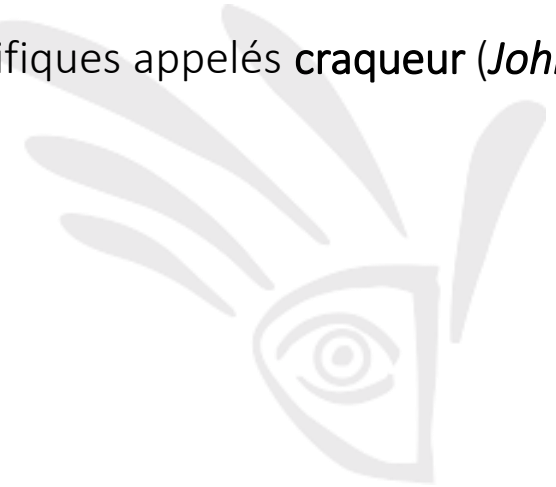
1-2-4 Cracking

Le craquage des mots de passe consiste à deviner le mot de passe de la victime.

Malheureusement, beaucoup d'utilisateurs mal avertis de cette technique mettent des mots de passe évidents comme leur propre prénom ou ceux de leurs enfants.

Ainsi, si un pirate, qui a espionné sa victime auparavant, teste quelques mots de passe comme le prénom des enfants de la victime, il aura accès a l'ordinateur. D'où l'utilité de mettre des bons mots de passe.

Mais même les mots de passe les plus robustes peuvent être trouvés à l'aide de logiciels spécifiques appelés craqueur (*John the ripper, L0phtCrack* pour Windows).



1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

1-2-5 Spoofing

L'usurpation (en anglais spoofing) consiste à se faire passer pour quelqu'un d'autre. Il existe des avantages illégitimes pour un pirate d'usurper une identité. C'est une attaque ou une personne ou un programme s'identifie avec succès comme un autre. Voici quelques exemples d'usurpations, cette liste étant non exhaustive :

- ❑ **Usurpation de l'adresse IP**

Une adresse IP correspond en gros à l'adresse postale d'un ordinateur. Ainsi, en changeant d'adresse IP, on peut se faire passer pour un autre ordinateur et obtenir des informations sensibles qui ne nous sont pas destinées.

- ❑ **Usurpation d'adresse e-mail**

Lors de la réception d'un courrier électronique, nous pouvons lire l'adresse de l'expéditeur. Mais, il est possible de changer l'adresse. Ainsi, un pirate peut vous envoyer un mail en usurpant l'adresse de votre supérieur.

- ❑ **Usurpation WEB**

Ceci est le principe du phishing

Généralement, quand on parle d'usurpation ou de spoofing, on parle de l'usurpation de l'adresse IP.

1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

1-2-6 Man in the Middle

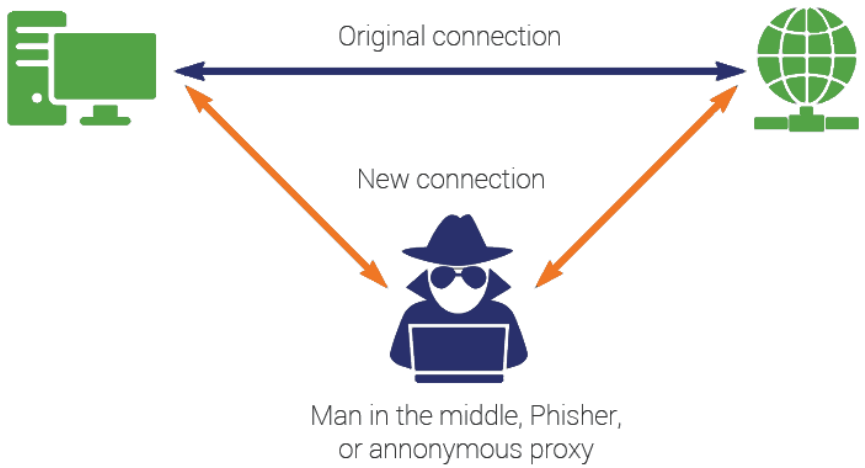
Man in the Middle signifie l'homme du milieu. Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B voulant dialoguer. Maintenant, si un pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, ainsi, toute communication vers A ou B passera par le pirate, l'homme du milieu.

Quels sont les risques ?

Le pirate peut donc intercepter tout le trafic, à savoir les informations sensibles comme les mots de passe. Mais, pire encore, le pirate peut modifier le trafic avant de le renvoyer vers l'autre ordinateur.

MITM a obtenu les privilèges et peut divulguer des informations sensibles.

Ainsi, si vous voulez commander un livre sur internet à 10 euros, et que le pirate change votre commande, vous pouvez très vite vous retrouver à dépenser des milliers d'euros.



1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

1-2-5 Hijacking

Un pirate peut craquer (cible) le mot de passe de la session. Mais si vous choisissez un mot de passe robuste, cela lui prendra beaucoup de temps. Préalablement le pirate a déjà accès à l'ordinateur de A (Elévation de privilège)

Dès que la victime se connecte sur la session il prend sa place. En effet le pirate contourne le processus d'authentification.
C'est le principe du détournement de session (en anglais **hijacking**).
Ensuite, s'il veut pouvoir dialoguer avec le serveur, il doit mettre hors-jeu la victime. Pour cela, il peut lui lancer une attaque par déni de service (cible). Mais, il peut aussi se mettre en écoute et enregistrer tout le trafic en espérant recueillir des informations sensibles comme des mots de passe.

Quels sont les risques ?

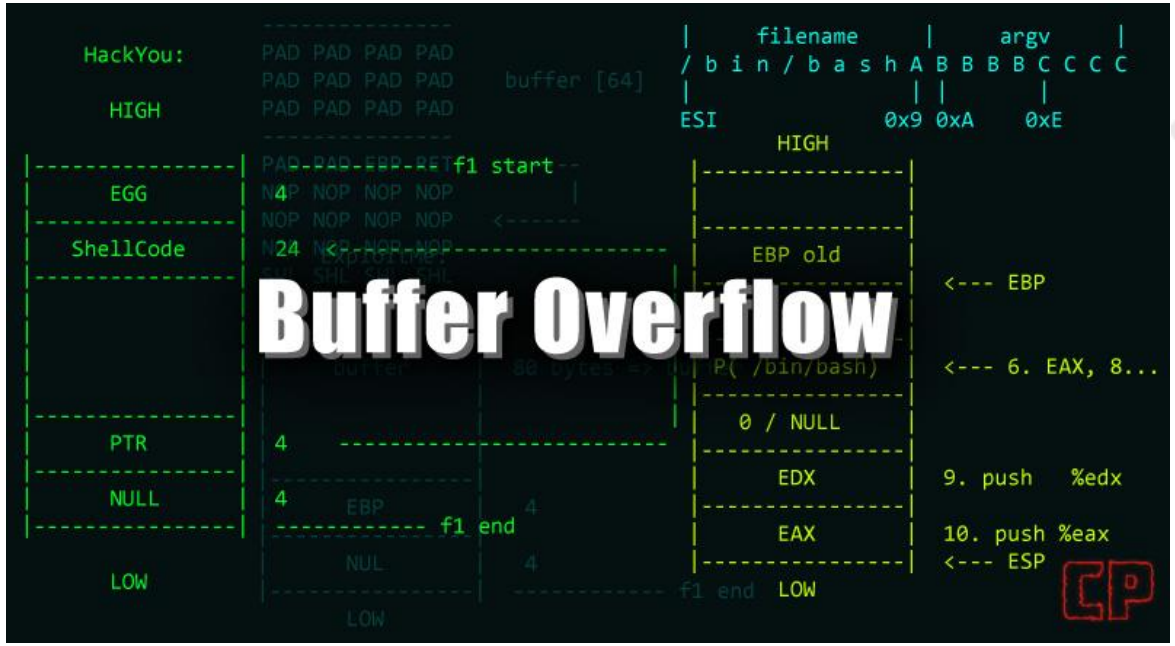
Si le pirate possède des informations sensibles comme un nom d'utilisateur et son mot de passe, il pourra alors revenir sur le système lorsqu'il le souhaitera a l'aide d'une backdoor. Il est donc compliqué d'identifier que le système est compromis puisque le pirate utilise le compte d'une personne autorisée. D'où l'importance de détecter cette attaque. (Il a les privilèges)

1- 2 Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS

1-2-6 Buffer OverFlow

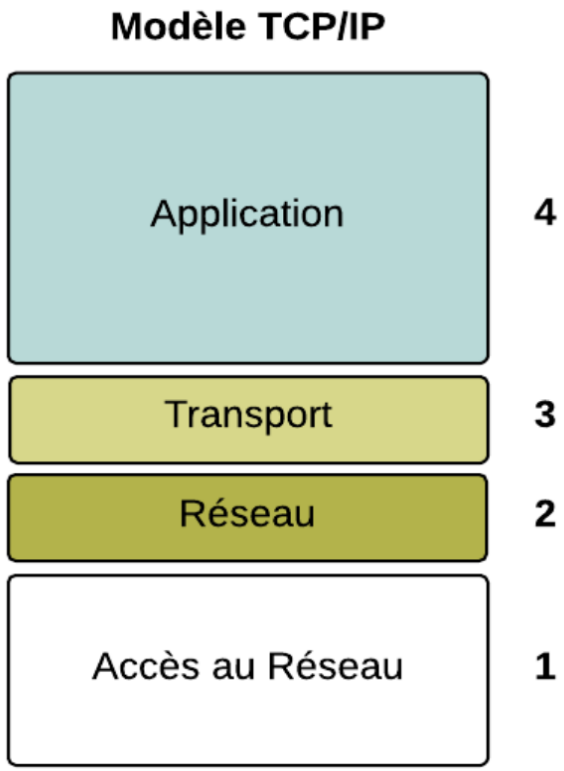
Un débordement de tampon (en anglais Buffer OverFlow ou BoF) est une attaque très utilisée des pirates.
Elle consiste à utiliser un programme résidant sur votre machine en lui envoyant plus de données qu'il n'est censé en recevoir afin que ce dernier exécute un code arbitraire.

Il n'est pas rare qu'un programme accepte des données en paramètre. Ainsi, si le programme ne vérifie pas la longueur de la chaîne passée en paramètre, une personne malintentionnée peut compromettre la machine en entrant une donnée beaucoup trop grande.



1- 2 Rappel de protocole TCP/IP

- TCP-IP (Transmission Control Protocol/Internet Protocol) est la pile protocolaire qui permet aux ordinateurs de communiquer entre eux sans se soucier du système d'exploitation ou du vendeur
- Quand une application envoie des données via TCP/IP, elles passent à travers chaque couche de la 'pile protocolaire' : **Encapsulation**
- A la réception chaque couche extrait et traite l'en-tête de la couche homologue :



2- MATÉRIEL DE SÉCURISATION

2-1 Sécurisation des accès physique (802.1X)

Le 802 .1x est un standard mis en place en juin 2001 par l'IEEE, et fait partie du groupe des protocoles IEEE 802 (802.1).
IEEE (Institute of Electrical and Electronics Engineers) => Institut des ingénieurs électriciens et électroniciens

Ce standard provient du besoin de s'authentifier dès l'accès physique au réseau.
Ce besoin s'est particulièrement fait sentir dans le domaine du WIFI, où les clés de cryptage WEP ne sont pas très efficaces, d'où l'idée d'une authentification physique dès les bornes.

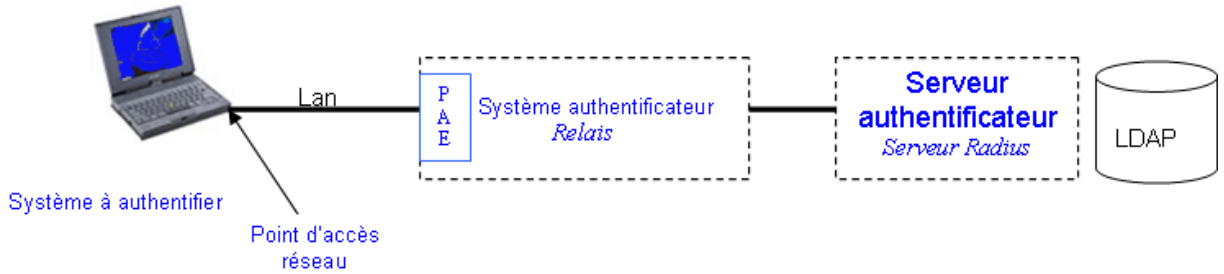
Cette norme 802.1x fut donc développée aussi pour les VLAN et s'appuie sur toutes les normes de niveau 2 comme le 802.5 (Token Ring), le 802.3 (Ethernet), mais également sur le WIFI. L'IEEE souhaitait donc standardiser un mécanisme de relais d'authentification au niveau 2

Objectifs

L'objectif du 802.1x est d'autoriser l'accès physique à un réseau local après une phase d'authentification, peu importe le système de transmission utilisé. Le mécanisme d'authentification de l'accès au réseau se fait lors de la connexion physique (en général connexion sur un réseau Ethernet), avant même tout autre mécanisme d'auto-configuration tel que DHCP pour l'attribution dynamique des adresses IP.
En plus de cela, le 802.1x va apporter des avantages considérables au niveau de l'administration du réseau, notamment par l'affectation dynamique des VLAN en fonction des caractéristiques de cette authentification.

2-1 Sécurisation des accès physique (802.1X)

Le 802.1x s'appuie sur un protocole particulier : l'EAP (Extensible Authentification Protocol) décrit par la suite. Le standard s'appuie sur des mécanismes d'authentification existants.
Il se base sur 3 entités



- **le système à authentifier**

Il s'agit en général d'un poste de travail, éventuellement d'un serveur. Le point d'accès au réseau varie donc selon ce dernier. Le point d'accès physique peut être une prise RJ45. Le point d'accès logique est par exemple le 802.11.

- **le système authentificateur ou Authentificator System**

Ce système sert de relais. Il s'agit d'un équipement réseau, comme une borne sans fil pour le WIFI, un routeur, …
Cet équipement gère un PAE (Port Access Entity) qui sera décrit après, qui permettra au demandeur d'accéder ou non aux ressources du réseau.

- **le système authentificateur ou authentification serveur**

Ce serveur d'authentification est en général un serveur Radius. Selon la requête du demandeur, ce serveur détermine les services auxquels le demandeur a accès.

2-1 Sécurisation des accès physique (802.1X)

Mécanisme Général

Le demandeur souhaite accéder aux ressources du réseau. Mais pour cela il va devoir s'authentifier. Le système authentificateur gère cet accès via le PAE. Il se comporte comme un relais, comme un proxy entre l'entité qui souhaite être sur le réseau et le serveur d'authentification.

Le demandeur va dialoguer avec le serveur via le relais, grâce au protocole EAP. Si l'authentification réussit, le serveur donne au demandeur l'accès aux ressources via le système authentificateur et son PAE.
La structure du 802.1x s'appuie donc sur 4 couches :

- couche média : le Token Ring, l'Ethernet, ..
- couche protocole : l'EAP, protocole d'identification
- couche méthode d'authentification : elle s'appuie sur les mots de passe, les certificats, …
- couche infrastructures qui comporte le matériel d'authentification comme le serveur Radius, …

L'utilisation du 802.1x en Wifi permettra l'authentification du demandeur, le contrôle d'accès aux bornes et la distribution des clés WEP.
Mais attention, il faut que le 802.1x soit bien implémenté sur les différentes machines. Si les implémentations sur les bornes et serveurs sont disponibles, il n'en est pas de même chez les postes clients. Le 802.1x est maintenant de plus en plus intégré avec le système d'exploitation.

2-2 ACL

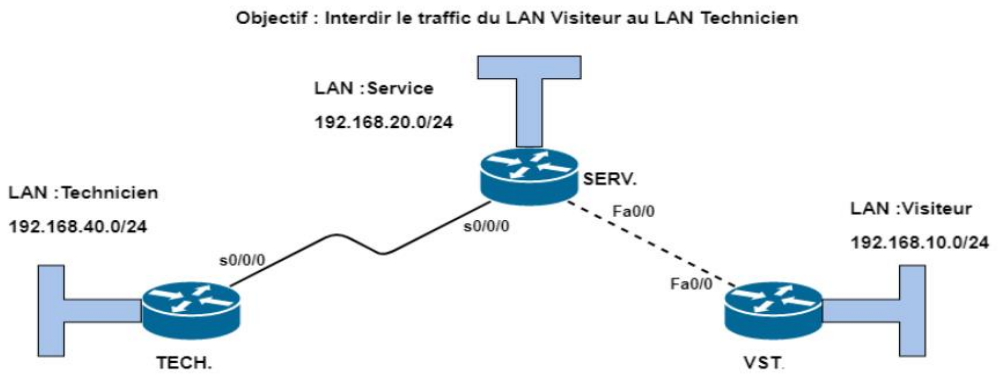
•Une liste de contrôle d'accès est une collection d'instructions ayant comme objectif de permettre ou d'interdire la commutation des paquets en fonction d'un certain nombre de conditions ou de critères, tels que : **Les adresses source et destination et les ports**

•Les ACL opèrent selon un ordre séquentiel et logique, en évaluant les paquets à partir du début de la liste.

•Dès qu'une règle est appliquée, le reste de l'ACL est ignorée. Il faut faire attention lors de la conception des ACL : **tout trafic ne correspondant à aucune règle est rejeté.**

1-Les types d'ACL : Il existe 3 types de liste de contrôle d'accès. Elles sont :

- ❑ les ACLs standards,
- ❑ les ACLs étendues,
- ❑ les ACLs nommées.



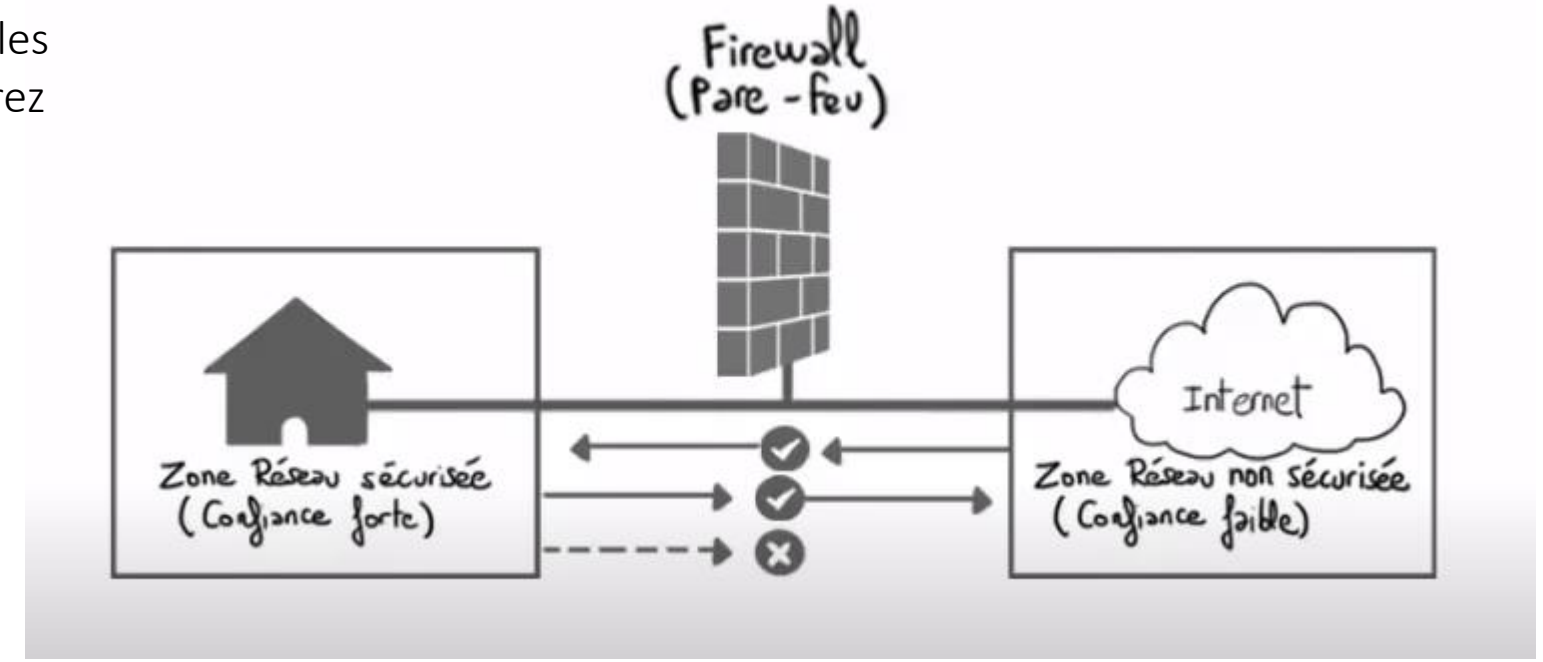
2-3 Firewall et règles de filtrage

Un système pare-feu (firewall) est un dispositif conçu pour examiner et éventuellement bloquer les échanges de données entre réseaux.
C'est donc un élément de sécurité d'un réseau qui peut être : un logiciel, un matériel ou une combinaison des 2
Son rôle est de sécuriser le réseau en définissant les communications autorisées et interdites
Il permet de connecter 2 réseaux ou plus de niveau de sécurité différente

Il permet de :

- Filtrer les communications, les analyser
- Autorise ou rejette les communications selon les règles de sécurité en vigueur; celles que vous aurez prédéfinies
- Protéger le réseau interne et sécurise

Les communications avec internet



2-3 Firewall et règles de filtrage

Les règles de filtrages sont :

- L'origine et/ou la destination des paquets avec l'adresse IP et les ports TCP/UDP notamment
- Les options contenues dans les données (fragmentation et validité)
- Les données en elles-mêmes

Il existe différents types de pare-feu :

❑ Pare-feu SANS ETATS

- Regarde les paquets et le compare à une liste de r

Règles de filtrage (ACL)

- Accorde/Refuse les paquets en fonction de

Adresse IP, port (source/destination)

Couche 3 et 4 modèle OSI (IP =>réseau, transport)

- Paramétrer en fonction N° de port (tout échange avec des port

Non autorisés seront bloqués; port 23 =>connexion serveur/cmd

❑ Filtrage Applicatif

- Se fait en fonction des protocoles utilisés par l'application

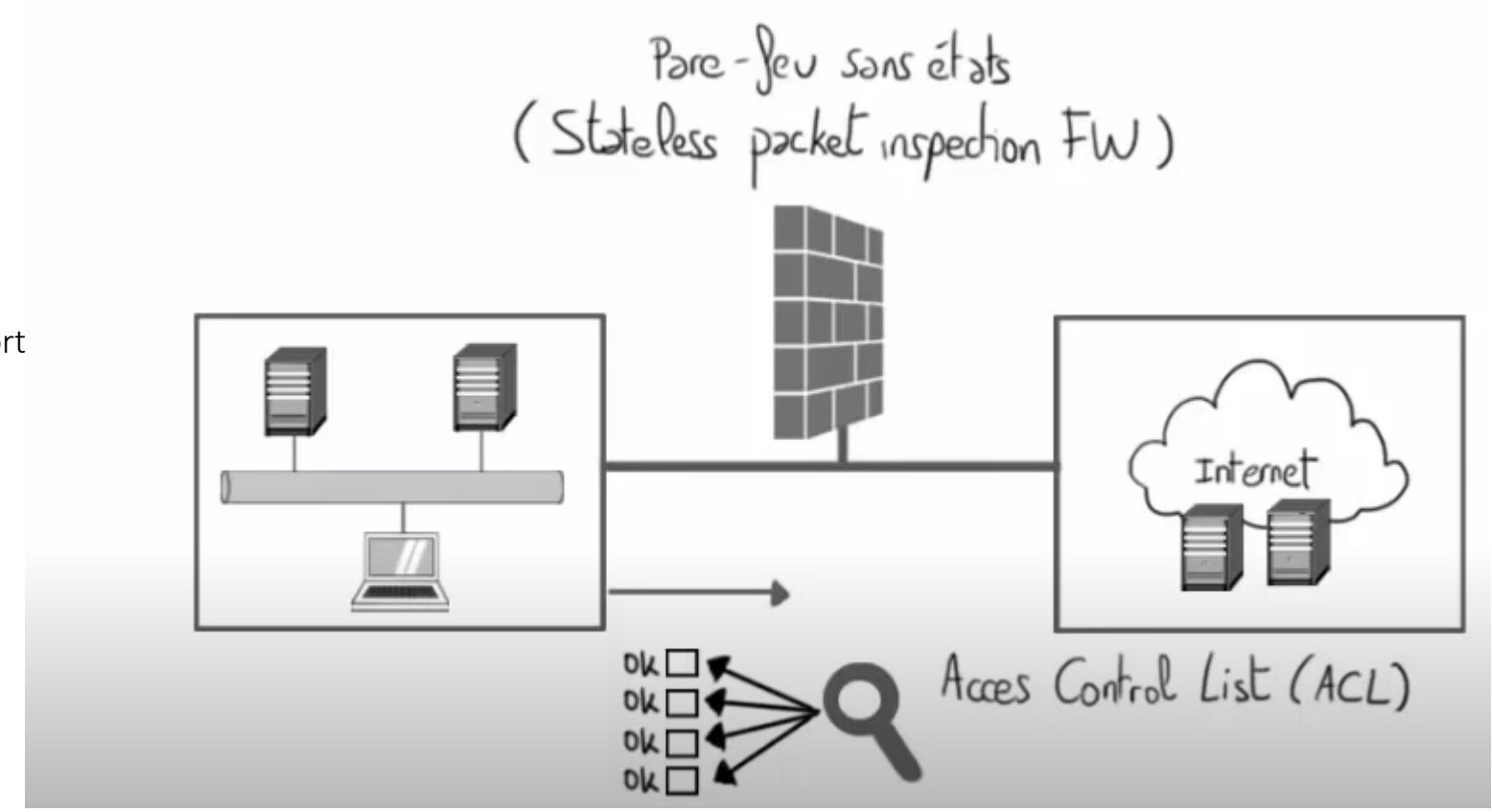
(http, ftp, smtp) => vérifie la conformité des paquets en fonction

Des protocoles attendus

- Suppose donc déjà une connaissance des protocoles déjà

Utilisés par chaque application et rejettera toutes les requêtes

Qui ne sont pas conformes aux spécification du protocole



2-3 Firewall et règles de filtrage

❑ Pare-feu AVEC ETAT (*Firewall Stateful)*

- Vérifie que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet
- Une connexion autorisée => tous les paquets de l'échange sont implicitement acceptés
- Prend ses règles/décisions de filtrage en fonction des informations accumulées lors des connexion précédentes et des paquets précédents appartenant à la même connexion
    - => définie ses règles de filtrage et non celles de l'admin

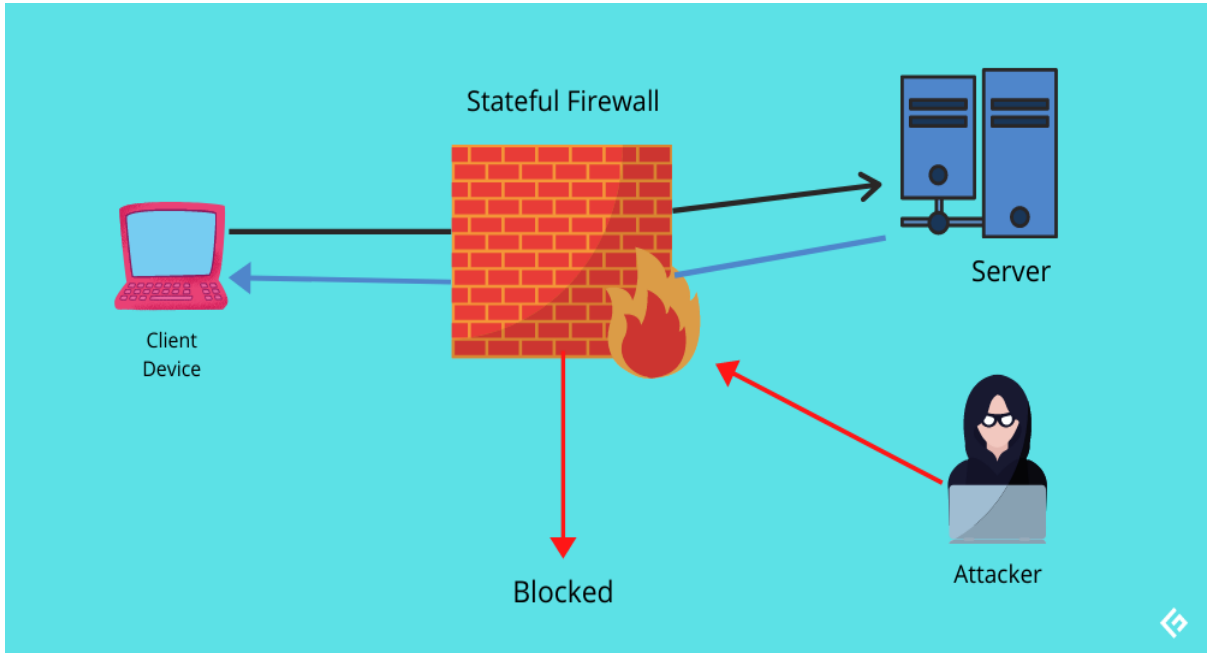
Doit garder un suivi de l'état de connexion, son rôle est donc de vérifier le trafic entrant avec sa table d'état et d'établir la
La correspondance ou pas
Il ne fait donc pas l'inspection approfondie des paquets mais
Filtre en fonction des connexions précédentes.

- Un firewall stateful inclut toutes les fonctionnalités d'un filtrage de paquet, auxquelles il ajoute la capacité de conserver la trace des sessions et des connexions dans des tables d'état interne.

- Tout échange de données est soumis à son approbation et adapte son comportement en fonction des états.

Cette technique convient aux protocoles de type connecté (TCP).

- Le firewall est donc amené à examiner les paquets, et peut seulement gérer des timeout, souvent de l'ordre d'une minute.



2-3 Firewall et règles de filtrage

❑ Proxy

Un **serveur Proxy** =>application qui va permettre à une application d'accéder à Internet.
L'utilisateur se connecte d'abord au serveur proxy et lui envoie sa requête
C'est le serveur proxy qui va à son tour transmettre le message au serveur distant

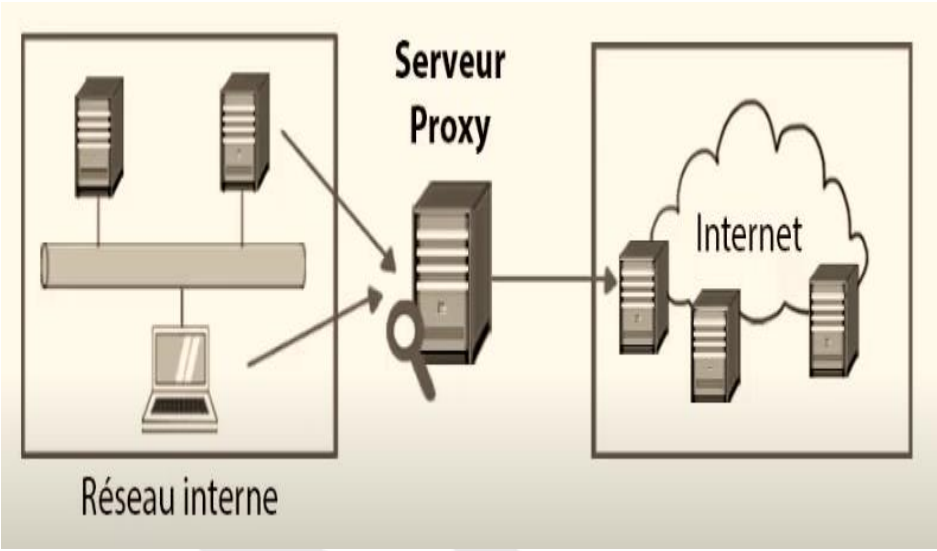
- Permet le filtrage des accès internet au sein d'une entreprise (bloque l'accès

À des sites non conformes à PSSI)

- Permet l'anonymisation de l'internaute via un masquage d'adresse IP client
  - En effet lorsque le proxy transmet la requête c'est l'IP publique et masque

  L'IP client. La réponse également se fait à travers le proxy
- Permet une accélération de la navigation avec des fonctionnalités comme :

Compression des données, filtrage des contenus lourds, la fonction cache la
Capacité de garder en mémoire les pages les plus visitées.



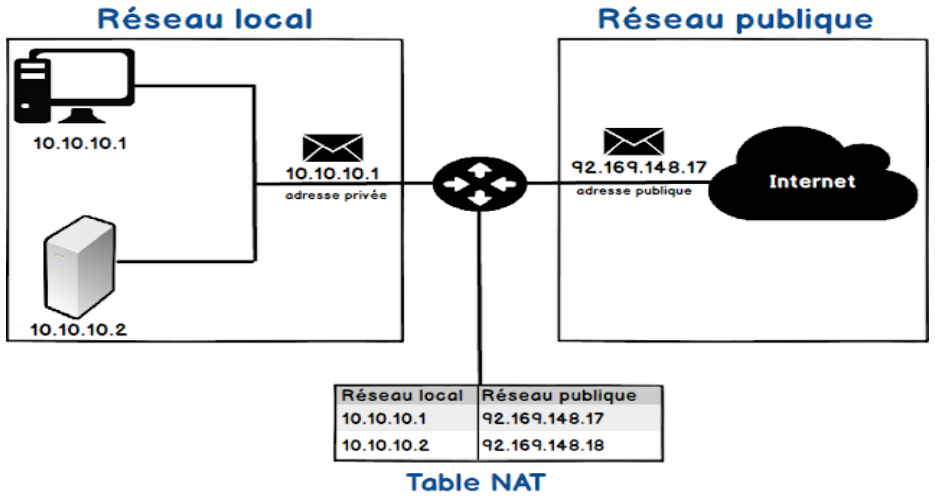
- Permet un suivi de connexion via les logs (enregistre l'ensemble des requête faits via le navigateur internet
  - *White list = filtrage à partir d'une liste de sites autorisés*
  - *Black list = filtrage à partir d'une liste de sites non autorisés*

Un **reverse Proxy** joue le rôle inverse d'un serveur proxy. Il permet lui à un utilisateur d'internet d'accéder au réseau interne

- Joue le rôle d'intermédiaire de sécurité (protège les serveurs web des attaques venant de l'extérieur
- Permet une accélération de la navigation avec des fonctionnalités comme : Compression des données, filtrage des contenus lourds, la fonction cache la capacité de garder en mémoire les pages les plus visitées.
- Répartition des charges des requêtes externes vers les serveurs internes

2-4 La Translation d'adresse NAT et le PAT

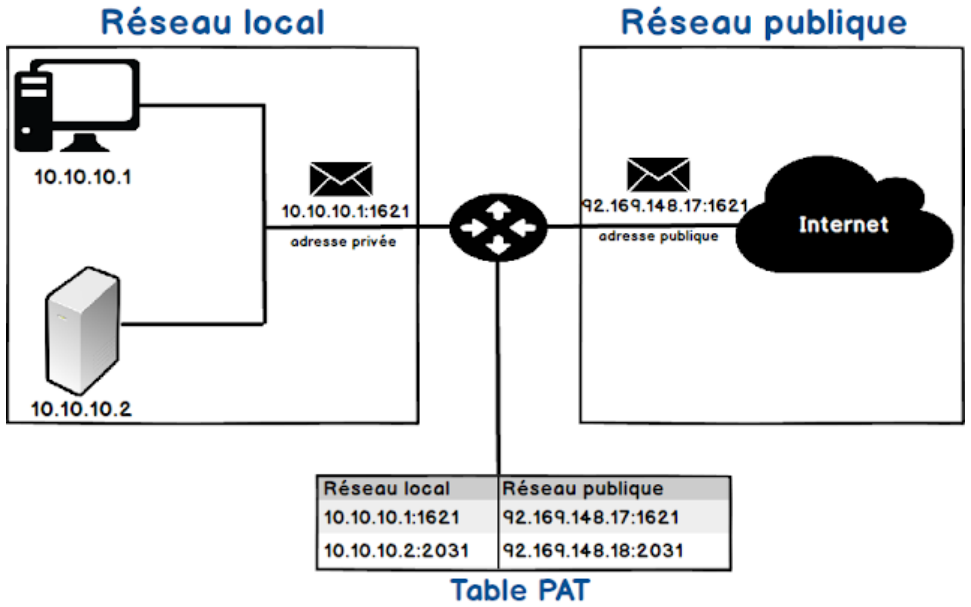
Le NAT est la traduction d'adresses réseau qui relie deux réseaux et mappe les adresses privées en adresses publiques. Ici, le terme adresses privées signifie que l'adresse de l'hôte appartient à un réseau locale et n'est pas assignée par le fournisseur de services. Et l'adresse publique signifie que l'adresse est une adresse assignée par le fournisseur de service et il représente également une ou plusieurs adresses locales internes au monde extérieur.



De plus, une seule adresse peut être configurée en NAT pour représenter l'ensemble du réseau vers le monde extérieur. Par conséquent, il assure la sécurité car le processus de traduction est transparent. Le NAT peut être utilisé comme un outil pour la migration et la fusion de réseaux, le partage de charge de serveur, la création de serveur virtuel, etc.

2-4 La Translation d'adresse NAT et le PAT

Le PAT est la traduction d'adresse de port grâce auquel la traduction d'adresse peut être configurée au niveau du port, et l'utilisation de l'adresse IP est optimisée.
PAT met en correspondance plusieurs adresses locales et ports sources avec une adresse IP publique et un port à partir d'une liste d'adresses IP routables sur le réseau de destination.
Ici, l'adresse IP de l'interface est utilisée en combinaison avec le numéro de port et plusieurs hôtes peuvent avoir la même adresse IP avec un numéro de port unique.
Il utilise une adresse de port source unique sur l'adresse IP globale interne pour identifier des traductions distinctes. Le nombre total de traductions NAT pouvant être exécutées est 65536 car le numéro de port est codé sur 16 bits.



2-4 La Translation d'adresse NAT et le PAT

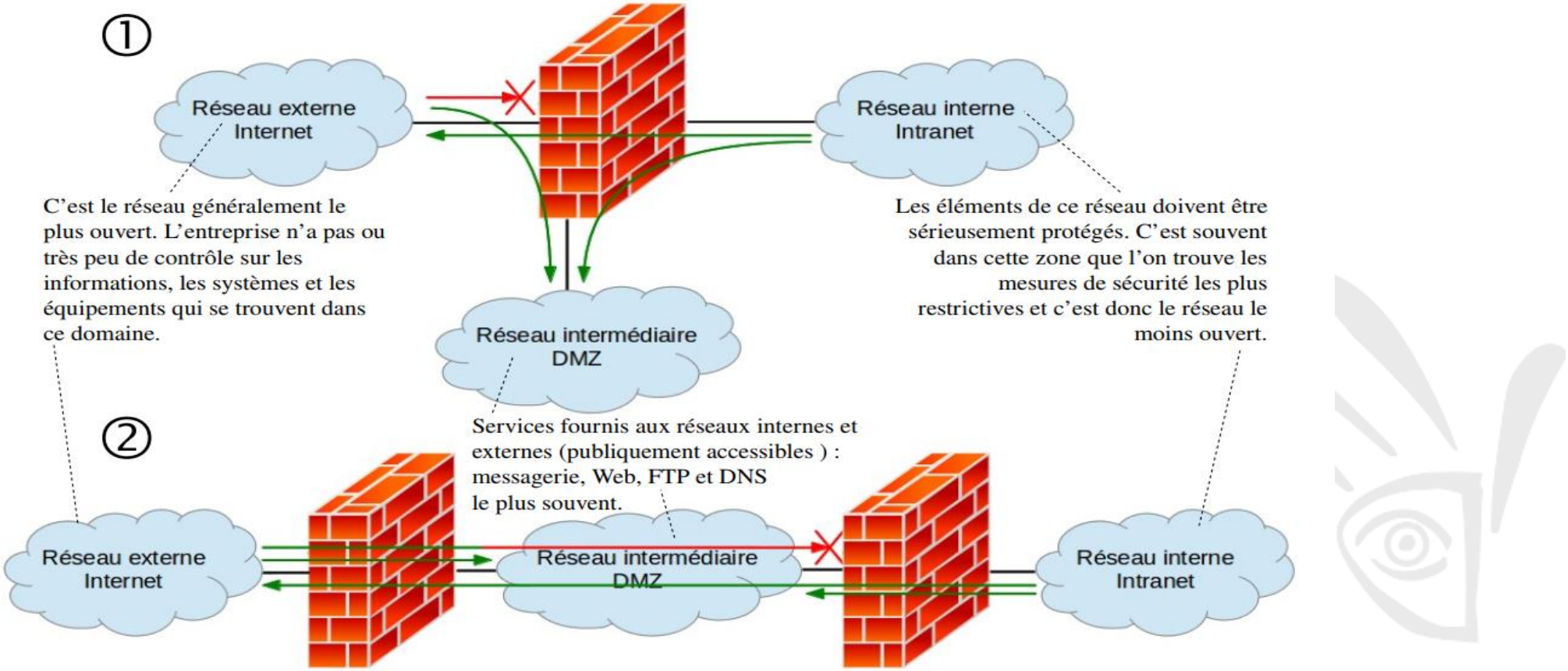
Différences clés entre NAT et PAT

NAT traduit les adresses locales internes en adresses publique similaires, tandis que le PAT convertit les adresses IP non enregistrées privées en adresses IP publiques enregistrées, mais à la différence de NAT, il utilise également des numéros de port source et plusieurs hôtes peuvent être affectés avec la même adresse IP ayant des numéros de port différents.
PAT est une forme de NAT dynamique.
NAT utilise des adresses IP dans le processus de traduction tandis que PAT utilise des adresses IP avec des numéros de port.

2-5 DMZ (*DeMilitarized Zone*)

Une **DMZ** (une zone démilitarisée) est un sous-réseau intermédiaire entre un réseau interne, dit de confiance, et un réseau externe non maîtrisé, donc potentiellement dangereux.
La DMZ isole les machines à accès public (**serveurs**) du réseau interne. La mise en place d'une DMZ est la première étape de la sécurisation d'un réseau. On distingue deux types d'architecture :

.



2-5 Surveillance par IDS/IPS et logs

2. IDS (système de détection d'intrusion)

Un système de détection d'intrusion (**IDS**) est un dispositif ou une application logicielle qui surveille un réseau ou des systèmes pour déceler toute activité malveillante ou toute violation de politique de sécurité.

Toute activité malveillante ou violation est généralement signalée à un administrateur ou est recueillie de façon centralisée au moyen d'un système de gestion des informations et des événements de sécurité (SIEM).

Un système SIEM combine des sorties provenant de sources multiples et utilise des techniques de filtrage des alarmes pour distinguer les activités malveillantes des fausses alarmes.

IPS (systèmes de prévention des intrusions)

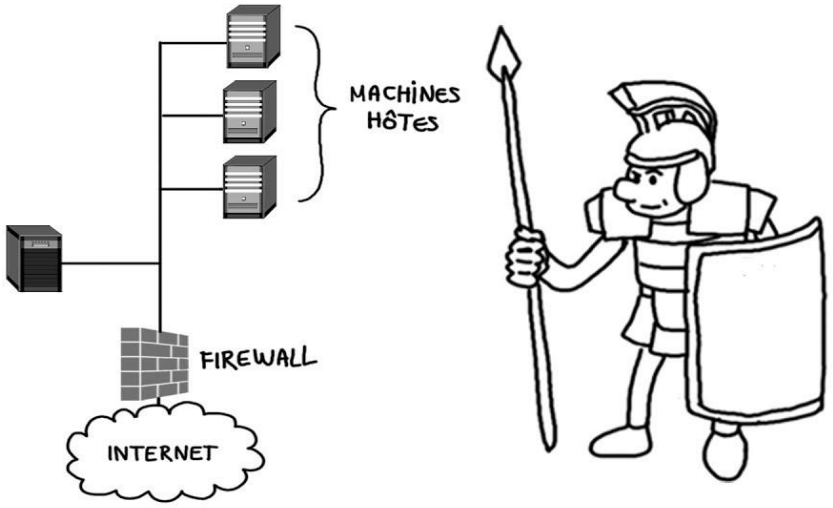
Les systèmes de prévention des intrusions (**IPS**), également connus sous le nom de systèmes de détection et de prévention des intrusions (IDPS), sont des dispositifs de sécurité réseau qui surveillent les activités du réseau ou du système pour détecter toute activité malveillante.

Les principales fonctions des systèmes de prévention des intrusions sont d'identifier les activités malveillantes, d'enregistrer des informations sur ces activités, de les signaler et de **tenter de les bloquer ou de les arrêter**.

2-5 Surveillance par IDS/IPS et logs

Les IDS et les IPS font tous deux partie de l'infrastructure réseau.
Les IDS/IPS comparent les paquets de réseau à une base de données de cybermenaces contenant des signatures connues de cyberattaques et repèrent tous les paquets qui concordent avec ces signatures.

La principale différence entre les deux tient au fait que l'IDS est un système de surveillance, alors que l'IPS est un système de contrôle.
L'IDS ne modifie en aucune façon les paquets réseau, alors que l'IPS empêche la transmission du paquet en fonction de son contenu, tout comme un pare-feu bloque le trafic en se basant sur l'adresse IP.



IDS / IPS