Université Batna 2

Systèmes de filtrage de paquets
Pare-feu (Firewalls)

Chapitre 4

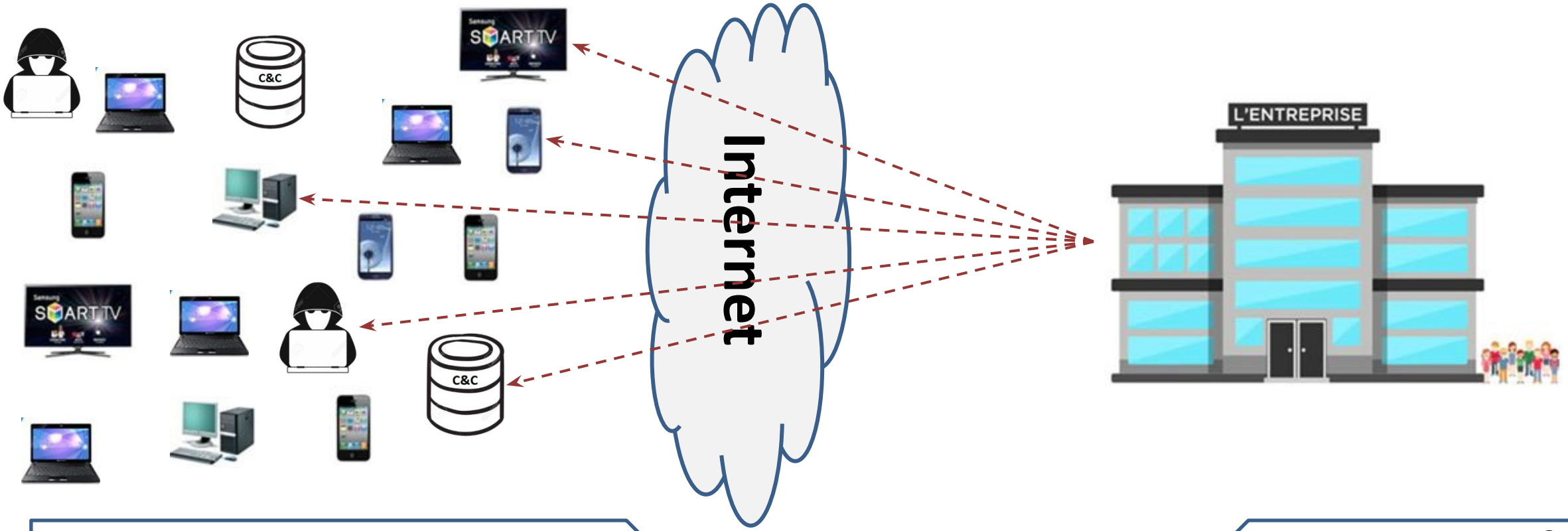
Préambule

Dans ce chapitre, nous allons voir

- Ce que signifie un pare-feu (firewall)
- Pourquoi une entreprise a besoin d'un pare-feu ?
- Différents types de pare-feu
- Ce qu'un pare-feu peut et/ou ne peut pas faire

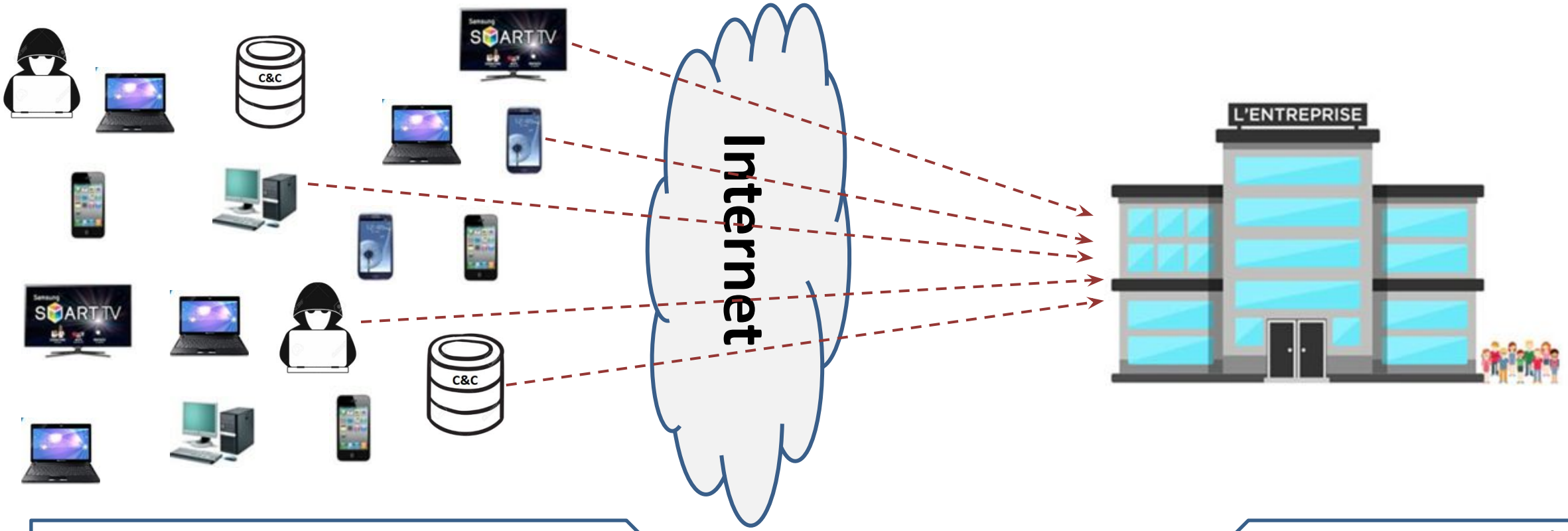
Préambule

Sans le Pare-feu, tous les employés peuvent **se connecter à n'importe** quelle sortie et toutes les personnes connectées à internet peuvent se connecter à votre réseau.



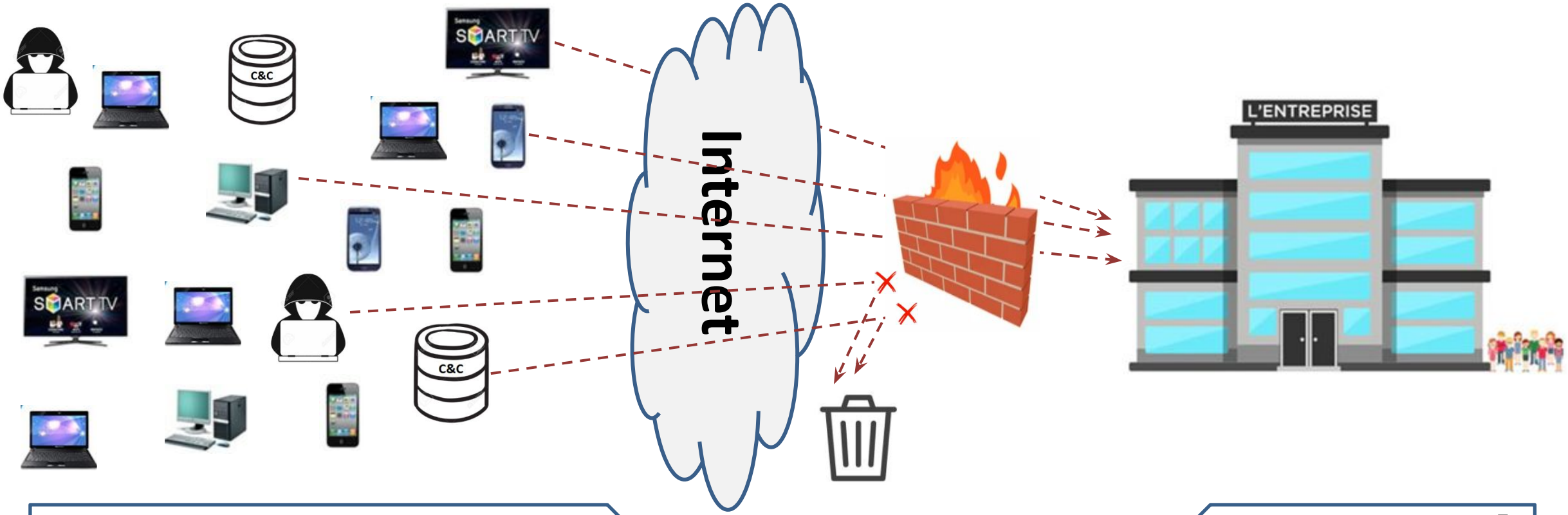
Préambule

Sans le Pare-feu, tous les employés peuvent se connecter à n'importe quelle sortie et **toutes les personnes connectées** à internet peuvent se connecter **à votre réseau**.



Préambule

Avec un Pare-feu les entreprises peuvent **limiter l'accès** de **l'interne vers l'externe et inversement**.



Préambule

Le pare-feu doit être **placé entre deux réseaux** (à coté d'un routeur) et constitue ainsi un **passage obligatoire** entre le réseau de l'entreprise et le reste des réseaux. Il peut aussi être **matériel ou logiciel**.

Dans les entreprises, on installe des Pare-feux physiques (matériels) et on configure des Pare-feux logiciels sur les machines.

Pare-feu physique

Préambule

Fonctionnement d'un Pare-feu

Pour sécuriser le réseau d'une entreprise, le pare-feu peut

- Empêcher des intrus d'accéder au réseau de l'entreprise.
- Empêcher les employés de sortir n'importe où.

et donc Filtrer les entrées et les sorties (adresse IP et port).

Le pare-feu fonctionne sur les **couches 3** (filtrage d'IPs), **4** (filtrage de ports) et **7** (filtrage de protocoles de la couche application) du modèle OSI,

Pour la réalisation de ces filtrages, un pare-feu doit être **configuré en respectant certains règles définies par l'entreprise**. On parle de la **politique de sécurité**.

Préambule

Politique de sécurité (une suite de règles de filtrage**)**

C'est la **première phase avant de créer des règles de filtrage** sur le pare-feu. Elle se base sur les **besoins de l'entreprise en terme de connexions à Internet** et par la suite **transformer ces besoins en règles** tout en assurant non seulement **la sécurité de l'entreprise** mais aussi **son bon fonctionnement**.

Deux méthodes sont possible

- Autoriser tout le trafic et bloquer les services dangereux.
- Bloquer tout le trafic et autoriser que les services nécessaires au bon fonctionnement de l'entreprise.

Question: à votre avis quelle est la méthode la plus recommandée ?

Préambule

Politique de sécurité, Exemples

- Les employés ont besoin d'accéder à Internet =>
- Les utilisateurs ont besoin d'accéder à leurs boite mails =>

Préambule

Politique de sécurité, Exemples

- Les employés ont besoin d'accéder à Internet **=> ouverture des ports HTTP et HTTPs de l'interne vers l'externe.**
- Les utilisateurs ont besoin d'accéder à leurs boite mails **=> ouverture des ports POP et IMAP.**

Préambule

Politique de sécurité, Exemples

- Les employés ont besoin d'accéder à Internet => ouverture des ports HTTP et HTTPs de l'interne vers l'externe.
- Les utilisateurs ont besoin d'accéder à leurs boite mails => ouverture des ports POP et IMAP.

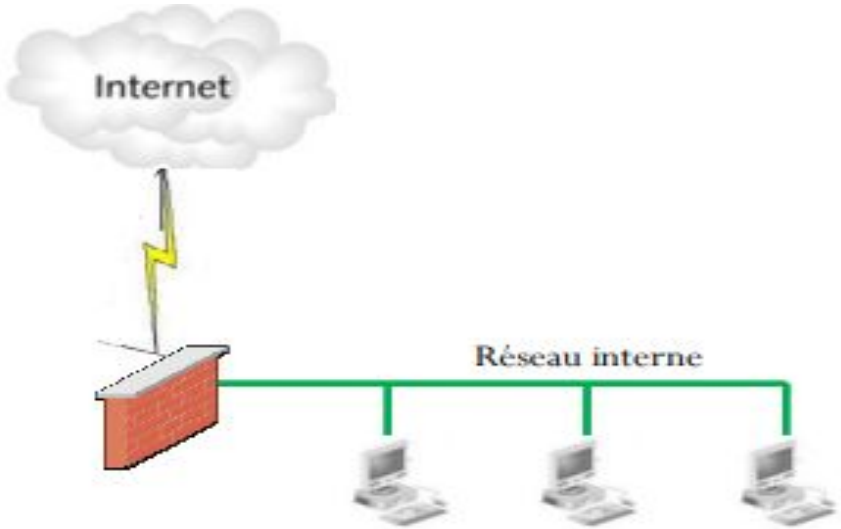
Politique de sécurité, Besoin

- Les règles employées sur un pare-feu sont **spécifiques pour chaque entreprise**.
- Politique de sécurité mal définie **=>** mauvaise configuration sur le pare-feu **=>** exposer l'entreprise à des risques de sécurité.

Différents types d'architecture de Pare-feu

1- Architecture avec un seul pare-feu central

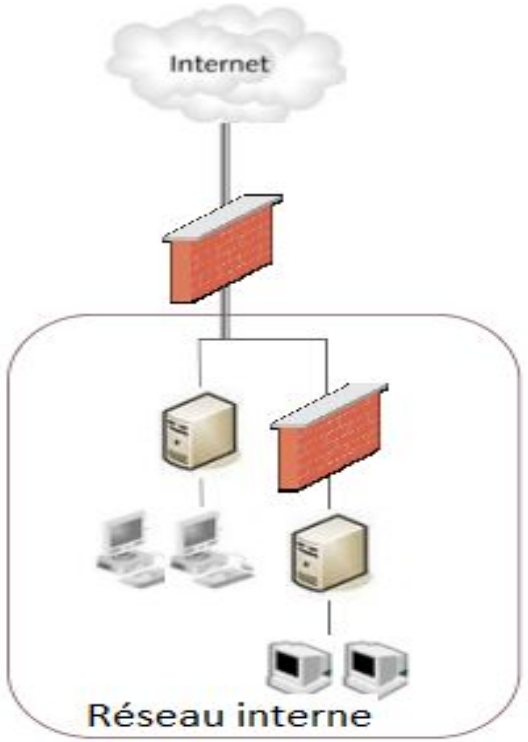
- Le pare-feu est positionné entre le **LAN et le WAN**
- Le filtrage se fait au niveau de la couche **3** et **4**.
- C'est l'architecture **la moins couteuse** et elle est utilisée dans les entreprises **n'ayant pas de serveur interne accessible depuis Internet**



Différents types d'architecture de Pare-feu

2- Architecture avec plusieurs pare-feux

- Un pare-feu est positionné entre le **LAN et le WAN** et un autre pare-feu **entre deux réseaux** internes
- Le filtrage se fait au niveau de la couche **3** et **4**.
- Permet de **protéger un réseau interne sensible** contre des attaques d'un autre réseau interne de l'entreprise.



Différents types d'architecture de Pare-feu

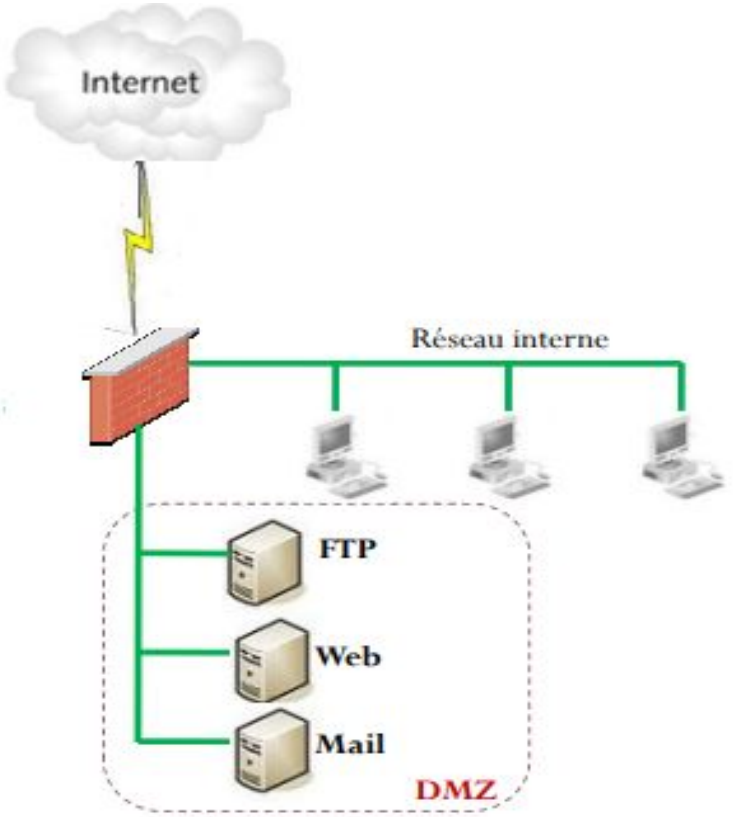
1- Architecture avec une zone démilitarisée (DMZ)

- La DMZ permet de rendre un **serveur accessible depuis Internet** (de l'externe) **mais n'expose pas le réseau interne** en ajoutant un autre pare-feu entre le réseau interne et le(s) serveur(s) exposés.

- Le filtrage se fait **en ouvrant uniquement le port** souhaité selon le besoin.

- Une autre règle doit être mise en place est d'**empêcher le(s) serveur(s) de se rendre sur le réseau interne**

- **Même si un des serveur est attaqué**, ce dernier ne va pas pouvoir contaminer les machines sur réseau interne



Différents types de Pare-feu

1- Pare-feux sans état

- C'est le plus ancien pare-feu.
- Il agit au niveau de la couche réseau et la couche transport.
- Tout échange avec des ports ou adresses IPs non autorisés seront bloqués.

<u>Inconvénients</u>

- Configuration complexe.
- Problème de flexibilité de filtrage.
- Devient de plus en plus obsolète.
- Traite les paquets indépendamment les uns des autres et les compare à une liste de règles appelées ACL (Acces Control List).

Différents types de Pare-feu

1- Pare-feux avec état

- Ce type de pare-feu vérifie que **chaque paquet de connexion est bien la suite du précédent** paquet ou la réponse d'un paquet dans l'autre sens (conformité des paquets).
- Il peut alors **prendre des décisions de filtrage** en fonction des informations récoltées lors des connexions précédentes (appartenant à la même connexion) en **consultant le tableau des états**.
- Il ne se base pas uniquement sur les règles prédéfinies par l'administrateur.
- Cette façon de procéder lui permet de protéger le réseau de certaines attaques DoS.

<u>Inconvénients</u>

- Le tableau des états a une taille limitée.
- Il ne peut pas faire une inspection approfondie des paquets (next-gen: Deep packet inspection (DPI)).

Différents types de Pare-feu

1- Pare-feux applicatifs (Proxy)

- Ce type de pare-feu **permet de filtrer les communications application par application.**
- Les requêtes sont vérifiées par un processus dédié.

Chaque requête doit être conforme aux spécifications du protocole concerné par la requête. Si par exemple, nous avons une requête FTP, cette dernière sera filtrée par un processus proxy FTP.

Dans ce cas le pare-feu va pouvoir filtrer le protocole FTP et non pas le port FTP (21).

- Ce type de pare-feu assure plus de sécurité que les autres pare-feux.
- Ce type de pare-feu peut inspecter le contenu du trafic.

-Il cache efficacement les véritables adresses IP.

<u>Inconvénients</u>

- Plus le débit de connexion est important plus le temps de calcul du proxy est grand.

Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Nous allons prendre le cas des pare-feux utilisant **iptables**. Ces pare-feux se basent sur la couche réseau et la couche transport pour se protéger contre les scan par exemple.

Netfilter: est un pare-feu sous Linux que nous pourrons le configurer à travers plusieurs outils. Cependant, l'outil le plus connu et le plus facile à utiliser est **iptables.**

iptables: peut être alors définit comme une interface (langage) aidant à spécifier les règles de filtrage avec le pare-feu **Netfilter**.

Configuration de Pare-feux

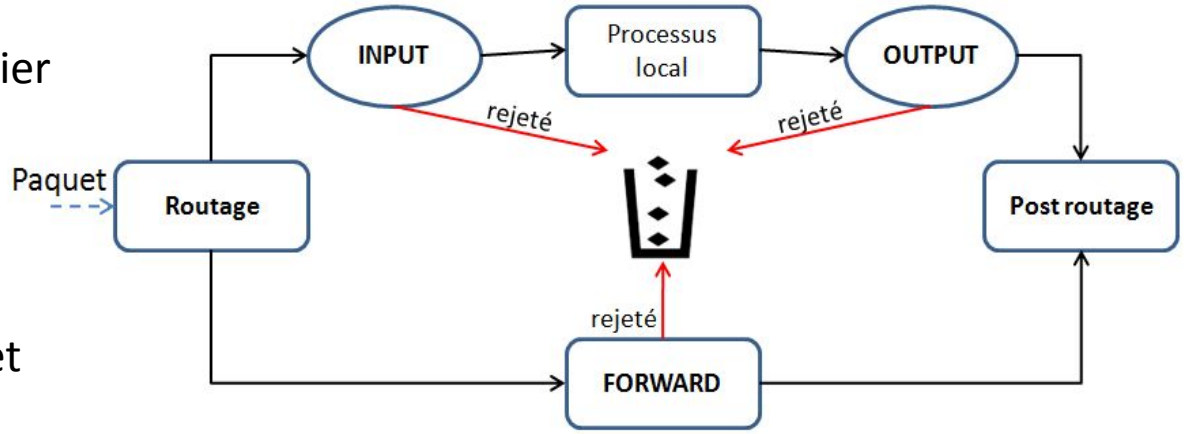
1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Chaque paquet inspecté passe à travers une suite de tables préconstruites, et chaque table est composée de règles. Il existe 3 tables (Filter, NAT et Mangle).
Lors de la réception d'un paquet au niveau du pare-feu ce dernier peut prendre trois chemins appelés chaînes:

INPUT: le paquet est à destination du pare-feu et souhaite accéder au réseau à protéger (chaîne d'entrée). S'il n'est pas rejeté le pare-feu le transmet au processus local.

OUTPUT: le paquet est émis par le pare-feu (chaîne de sortie) et souhaite sortir du réseau.

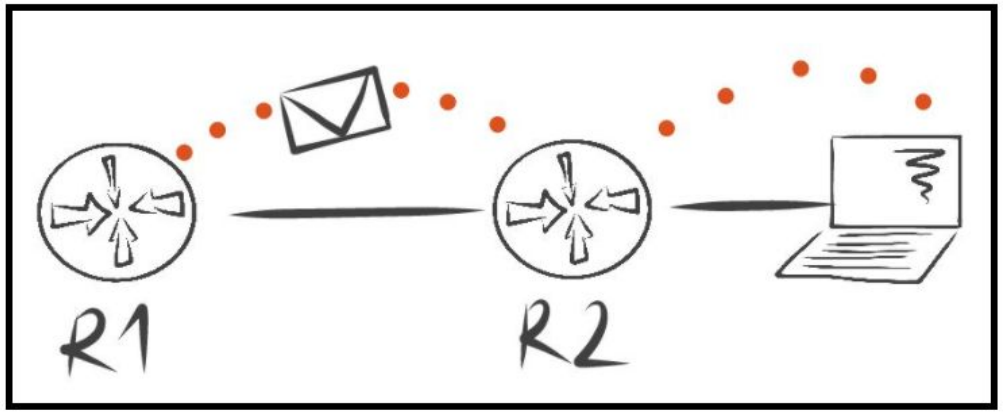
FORWARD: le paquet n'est pas à destination du pare-feu mais passe par ce dernier. S'il n'est pas rejeté le pare-feu le transfert (le forward) vers le terminal destinataire (chaîne de redirection).



Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Nous avons un paquet qui transite par le réseau en passant par deux routeur R1 et R2 à destination du poste de travail.



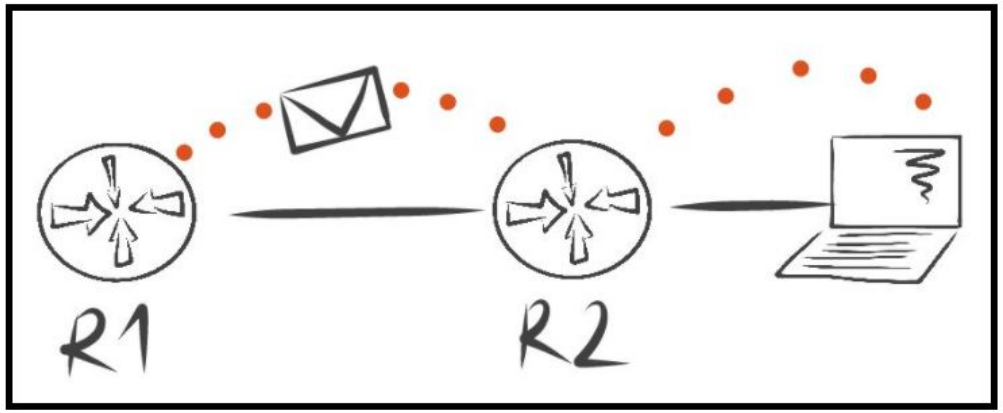
Par quelles chaines va transiter le paquet, pour le routeur R2 et le poste de travail ?

a) Par la chaine INPUT et OUTPUT pour le routeur R2
   et par la chaine INPUT pour le poste de travail.
b) Par la chaine FORWARD pour le routeur R2
   et par la chaine INPUT pour le poste de travail.
c) Par la chaine OUTPUT pour le routeur R2
   et par la chaine INPUT pour le poste de travail.

Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Nous avons un paquet qui transite par le réseau en passant par deux routeur R1 et R2 à destination du poste de travail.



Par quelles chaines va transiter le paquet, pour le routeur R2 et le poste de travail ?

a) Par la chaine INPUT et OUTPUT pour le routeur R2
et par la chaine INPUT pour le poste de travail.

b) Par la chaine FORWARD pour le routeur R2
et par la chaine INPUT pour le poste de travail.

c) Par la chaine OUTPUT pour le routeur R2
et par la chaine INPUT pour le poste de travail.

Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Le filtrage: se base sur l'entête réseau pour les adresses IPs l'entête TCP ou UDP pour les ports.

Syntaxe d'une règle du pare-feu iptables

iptables -A <chaîne> -i <interface d'entrée> -o <interface de sortie> -p <protocole> -s <IP source> -d <IP destination> --sport <port source> --dport <port destination> -j <action>

<chaîne>: chaîne de filtrage (INPUT, OUTPUT, FORWORD)
<interface d'entrée>: interface réseau par laquelle le paquet passe (exp : eth0,eth1, etc.)
<protocole>: le protocole de la couche 3 ou 4 utilisé dans la communication (exp : tcp, icmp, udp)
<IP source>: l'adresse IP source.
<IP destination>: l'adresse IP de destination.
<port source>: numéro de port source identifiant l'application source du paquet.
<port destination>: numéro de port destination identifiant l'application destinataire du paquet.
<action>: action à entreprendre sur le paquet (nous avons deux actions : DROP, REJECT ou ACCEPT).

Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Le filtrage: se base sur l'entête réseau pour les adresses IPs l'entête TCP ou UDP pour les ports.

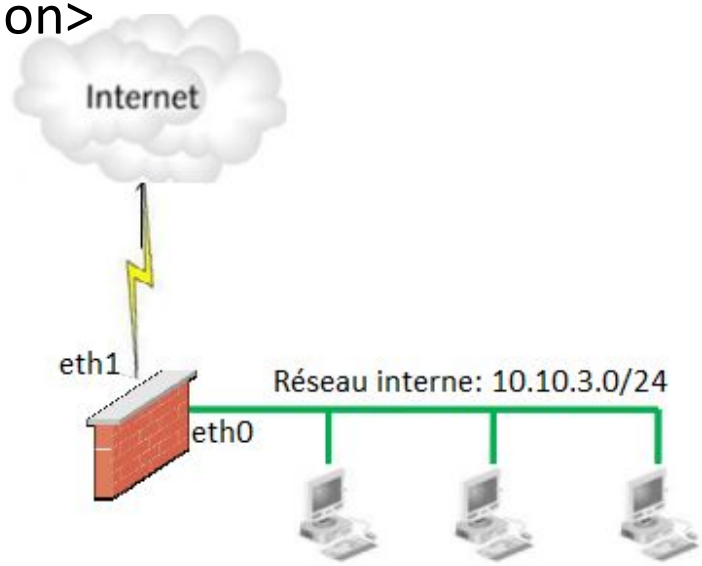
Syntaxe d'une règle du pare-feu iptables

iptables -A <chaîne> -i <interface d'entrée> -o <interface de sortie> -p <protocole> -s <IP source> -d <IP destination> --sport <port source> --dport <port destination> -j <action>

Exemple:

- Supprimez tous les paquets entrant avec le port de destination DNS (53)

- Supprimez tous les paquets sortant excepté celle de HTTPS (443)



Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Le filtrage: se base sur l'entête réseau pour les adresses IPs l'entête TCP ou UDP pour les ports.

Syntaxe d'une règle du pare-feu iptables

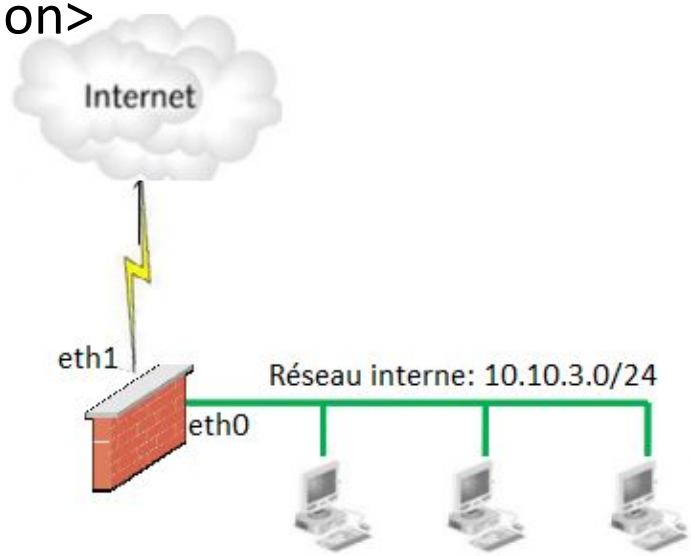
iptables -A <chaîne> -i <interface d'entrée> -o <interface de sortie> -p <protocole> -s <IP source> -d <IP destination> --sport <port source> --dport <port destination> -j <action>

Exemple:

- Supprimez tous les paquets entrant avec le port de destination DNS (53)

iptables -A FORWARD -i eth1 -o eth0 -p TCP -s all -d 10.10.3.0/24 --sport all --dport 53 -j DROP

- Supprimez tous les paquets sortant excepté celle de HTTPS (443)



Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Le filtrage: se base sur l'entête réseau pour les adresses IPs l'entête TCP ou UDP pour les ports.

Syntaxe d'une règle du pare-feu iptables

iptables -A <chaîne> -i <interface d'entrée> -o <interface de sortie> -p <protocole> -s <IP source> -d <IP destination> --sport <port source> --dport <port destination> -j <action>

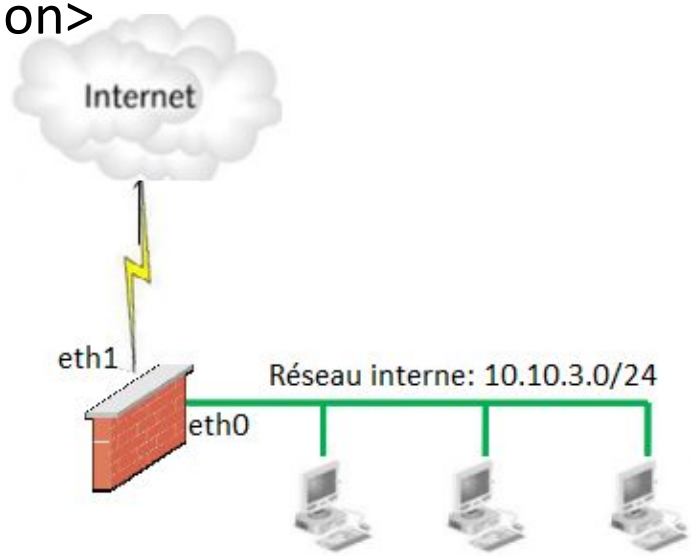
Exemple:

- Supprimez tous les paquets entrant avec le port de destination DNS (53)

iptables -A FORWARD -i eth1 -o eth0 -p TCP -s all -d 10.10.3.0/24 --sport all --dport 53 -j DROP

- Supprimez tous les paquets sortant excepté celle de HTTPS (443)

iptables -A FORWARD -i eth0 -o eth1 -p TCP -s 10.10.3.0/24 -d all --sport all --dport ! 443 -j DROP



Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Définition de la politique par défaut: dans les trois chaines (INPUT, OUTPUT, FORWORD) , tout ce qui n'est pas explicitement autorisé est strictement interdit (Default Policy):
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

Remise à zéro du pare-feu (Flush a chain): effacer toutes les règles sur les trois chaînes (INPUT, OUTPUT, FORWORD)
iptables -F INPUT DROP
iptables -F OUTPUT DROP
iptables -F FORWARD DROP

Flush en informatique signifie vidage d'une mémoire cache.

Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Configuration des règles de filtrage: Les règles doivent être configurées de telle sorte que **les règles les plus génériques doivent être placées à la fin de votre table**, tandis que **les règles les plus spécifiques doivent être placées au début** car le pare-feu va les lire dans l'ordre et de façon séquentielle

Exemple:

- On autorise la réception des Emails sur notre serveur smtp (1.2.3.4)
- On autorise tous les utilisateurs internes à se connecter à tous les services du réseau externe
- On bloque le reste.

Action	IP source	Port Source	IP destination	Port destination
Accept	*	*	1.2.3.4	25
Accept	Utilisateurs internes	*	*	*
Drop	*	*	*	*

Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Configuration des règles de filtrage: Les règles doivent être configurées de telle sorte que les règles les plus génériques doivent être placées à la fin de votre table, tandis que les règles les plus spécifiques doivent être placées au début car le pare-feu va les lire dans l'ordre et de façon séquentielle

Exemple

- On autorise la réception des Emails sur notre serveur smtp (1.2.3.4)
- On autorise tous les utilisateurs internes à se connecter à tous les services du réseau externe
- On bloque le reste.

Action	IP source	Port Source	IP destination	Port destination
Accept	*	*	1.2.3.4	25
Accept	Utilisateurs internes	*	*	*
Drop	*	*	*	*

Problème : les règles de filtrage ne respectent pas la politique définie

Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Exemple

- On autorise la réception des Emails sur notre serveur smtp (1.2.3.4)
- On autorise tous les utilisateurs internes à se connecter à tous les services du réseau externe
- On bloque le reste.

Échec des connexions sortantes

Les hôtes internes ouvrent une connexion TCP sur le port 80 :

-Le paquet initial SYN est autorisé par la règle 2

-Le paquet SYN\ACK de retour est rejeté par la règle 3

Action	IP source	Port Source	IP destination	Port destination
Accept	*	*	1.2.3.4	25
Accept	Utilisateurs internes	*	*	*
Drop	*	*	*	*

Configuration de Pare-feux

1- Filtrage pare-feu au niveau de la couche Réseau et Transport

Exemple

- On autorise la réception des Emails sur notre serveur smtp (1.2.3.4)
- On autorise tous les utilisateurs internes à se connecter à tous les services du réseau externe
- On bloque le reste.

Échec des connexions sortantes

Les hôtes internes ouvrent une connexion TCP sur le port 80 :

-Le paquet initial SYN est autorisé par la règle 2

-Le paquet SYN\ACK de retour est rejeté par la règle 3

-**Solution :** autoriser la réception des paquets associés à une connexion sortante (les paquets avec le flag ACK activé).

Action	IP source	Port Source	IP destination	Port destination	Flag
Accept	*	*	1.2.3.4	25	
Accept	Utilisateurs internes	*	*	*	
Accept	*	*	Utilisateurs internes	*	SYN/ACK
Drop	*	*	*	*	

Configuration de Pare-feux

1- Pare-feu au niveau de la couche Application

- Le filtrage ou le pare-feu au niveau de la couche 3 et 4 permet uniquement de lire les entête IP et TCP/UDP
- Le filtrage ou le pare-feu au niveau de la couche 7 permet de lire le contenu des paquets (les données transmises grâce à un module appelé DPI (Deep Packet Inspection). On peut alors parler de **proxy.**
- Afin que ce dernier fonctionne correctement, les constructeurs de ce type de pare-feu analysent les attaques (virus, spam, etc.) et établissent des signatures (empreintes) pour chaque attaque qui seront enregistrées dans la base de données du pare-feu.
- Le pare-feu (proxy) va donc analyser le trafic et va le comparer aux signatures dans sa base de données, ensuite il accepte ou refuse le trafic.

<u>Inconvénient</u>

- Le constructeur doit maintenir sa base de données à jour car les attaquants changent souvent leurs façon de procéder et donc la signature change aussi.