# Parefeu - Proxy - DMZ

## I) Parefeu :

Un parefeu est un système permettant :

- De protéger un réseau des intrusion provenant d'un réseau tierce (internet)
- De filtrer les données échangés avec le réseau.

Le fonctionnement d'un parefeu repose sur un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).

Il existe 3 types de filtrages.

Le filtrage simple de paquet qui travaille au niveau de la couche 3 du modèle OSI. Le parefeu analyse les en-têtes de chaque paquet de données échangé entre une machine interne et externe afin d' étudier les adresses IP émettrice et réceptrice, les types de paquets et les numéros de port.

Exemples de règles de parefeu :

| Action | IP source | IP destinataire | Protocole | Port source | Port destinataire |
|---|---|---|---|---|---|
| Accept | 192.168.10.20 | 194.154.192.3 | Tcp | Any | 25 |
| Accept | Any | 192.168.1.3 | Tcp | Any | 80 |
| Accept | 192.168.10.0/24 | Any | Tcp | Any | 80 |
| Deny | Any | Any | Any | Any | any |

Le filtrage dynamique travaille au niveau de la couche 3 et 4 du modèle OSI. Le parefeu peut ainsi prévoir les ports à autoriser ou à interdire.

Le filtrage applicatif permet de filtrer les communications application par application au niveau de la couche 7 du modèle OSI. Ce type de filtrage impose la connaissance des protocoles utilisés par chaque application.

## II) Proxy :

Un proxy est un serveur qui fait fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. Le proxy est un serveur mandaté par une application pour effectuer une requête sur internet à sa place.

Le proxy assure une fonction de cache, les pages les plus souvent visitées sont stockées sur le serveur.

Il peut également assurer un suivi des connexions (logs utilisateurs) et filtrer les connexions à internet en analysant les requêtes des clients et les réponses des serveurs pour les comparer à la liste blanche (liste de requête autorisées) ou à la liste noire (liste de requête interdites).

Il peut aussi assurer l'authentification des utilisateurs pour gérer l'accès aux ressources externes.

Il existe 2 types de proxy :
Le proxy web et le proxy applicatif.

Les proxys les plus connus sont Squid (gratuit Linux et Windows) et Wingate (payant).

## III) DMZ :

Une DMZ c'est une zone démilitarisée située derrière un parefeu où l'on place des serveurs devant être accessible de plusieurs réseaux. Cette zone cloisonnée, isolée sert de tampon entre le réseau à protéger et le réseau hostile (internet).

Un serveur situé en DMZ est susceptible d'être corrompu par une attaque. Le cloisonnement et l'isolement rendent plus difficile une attaque du réseau interne depuis le serveur en DMZ.

DMZ publique : C'est une zone accessible depuis l'extérieur (internet) et l'intérieur (réseau interne entreprise).

DMZ privée : Uniquement accessible par les réseaux internes.