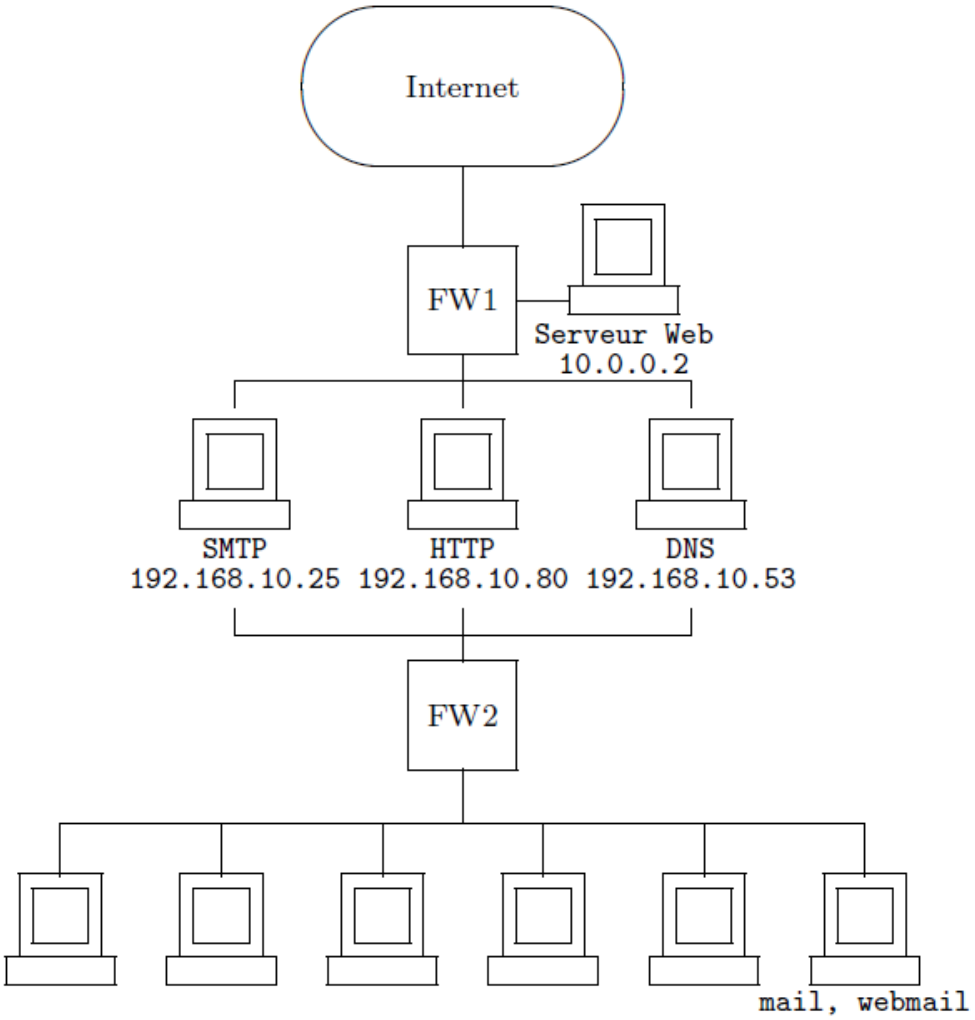
TD PAREFEU

EXERCICE 1:

On considère l'architecture décrite sur la figure ci-dessous. On suppose que l'adresse du serveur web est `10.0.0.2` et que les proxies SMTP, HTTP et DNS possèdent respectivement les adresses `192.168.10.25`, `192.168.10.80` et `192.168.10.53`. Les trois proxies sont utilisés en mode direct (donc vers Internet) et inverse (donc depuis Internet). Le serveur web doit aussi être accessible depuis le réseau interne. On désigne par `dmz_proxy` toutes les adresses de la zone des proxies et par `dmz_web` toutes les adresses de la zone du serveur web.



1. C'est quoi un proxy inverse ? Quels sont les avantages d'un tel proxy?
2. Classer les différentes zones de cette architecture de la zone la plus sécurisée à la zone la moins sécurisée.
3. L'ordre des règles de filtrage dans un pare-feu est-il important ? Justifier votre réponse.
4. En appliquant la démarche d'organisation de règles de filtrage, écrire les règles de filtrage pour le pare-feu externe avec mémoire (FW1).

On veut maintenant placer un IDS entre l'Internet et le pare-feu FW1.

5. Pourquoi placer l'IDS entre l'Internet et le pare-feu? Quel est l'avantage principal ? Quels sont les inconvénients (nommez-en deux)?

EXERCICE 2:

Le NAT est un mécanisme qui limite le problème de la pénurie des adresses IPv4 mais qui a aussi des avantages en termes de sécurité.

1. Quels sont les avantages du NAT du point de vue sécurité, coût et maintenance ?

Les réseaux pair-à-pair rencontrent souvent des problèmes avec le NAT. Les systèmes pair-à-pair (*peer-to-peer ou p2p*) permettent à plusieurs ordinateurs de communiquer via un réseau, de partager simplement des fichiers, mais également des flux multimédia continus (streaming), le calcul réparti, un service (comme la téléphonie avec Skype), etc. sur Internet. Chaque utilisateur dans ce système est à la fois client est serveur.

2. C'est quoi le problème rencontré si les deux utilisateurs (les deux pairs) pratiquent le NAT dynamique ?

La redirection de port ou *port forwarding*, consiste à rediriger automatiquement des paquets réseaux reçus avec un port destination donné (ex. port n°6945) vers une autre adresse IP et avec un numéro de port donné.

3. C'est quoi la différence entre le mécanisme de redirection de port et le mécanisme du NAT ?
4. Comment utiliser le mécanisme de redirection de port pour résoudre le problème du pair-to-pair lorsque les deux pairs sont derrière un NAT dynamique ?