Pare-Feu : Filtrage

TD N°7 Réseaux — R&T2A

19 janvier 2006

Rappel : *Connexions TCP/UDP*

Pour TCP, le schéma d'échange de données : `SYN/SYN+ACK/ACK/.../FIN/ACK/FIN/ACK` définit la "connexion" pourvu que les adresses IP, les numéros de ports, et les numéros de séquences soient cohérents. Dans le cas de UDP la "connexion" est définie par les adresses IP et les numéros de ports.

Exercice 1 : *Règles de filtrage d'un pare-feu sans mémoire*

On considère un pare-feu sans mémoire dont le critère de filtrage est fondé sur les paquets `SYN` (paquets dont le flag `SYN` est 1 et le flag `ACK` est 0). On souhaite que le serveur de messagerie (128.168.1.1) sur le réseau interne puisse recevoir et envoyer des messages vers Internet.

Écrire les règles de filtrage du pare-feu ci-dessous, dans le tableau suivant.

source	port	destination	port	protocole	Paquets SYN (`any`,`no`)	action

1. Toute machine extérieure au réseau doit pouvoir se connecter sur le port 25 du serveur de messagerie.
2. Le serveur de messagerie doit pouvoir répondre à une machine extérieure (`les paquets SYN sont donc rejetés`).
3. Le serveur de messagerie doit pouvoir se connecter sur le port 25 d'une machine extérieure au réseau.
4. Une machine extérieure doit pouvoir répondre à une demande de connexion (`les paquets SYN sont donc rejetés`).
5. Tout autre type de trafic doit être interdit.

Exercice 2 : *Règles de filtrage d'un pare-feu avec mémoire*

On considère l'architecture décrite sur la figure 1. 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 (vers Internet) et inverse (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.

Écrire les règles de filtrage pour le pare-feu externe avec mémoire (`PF1`).

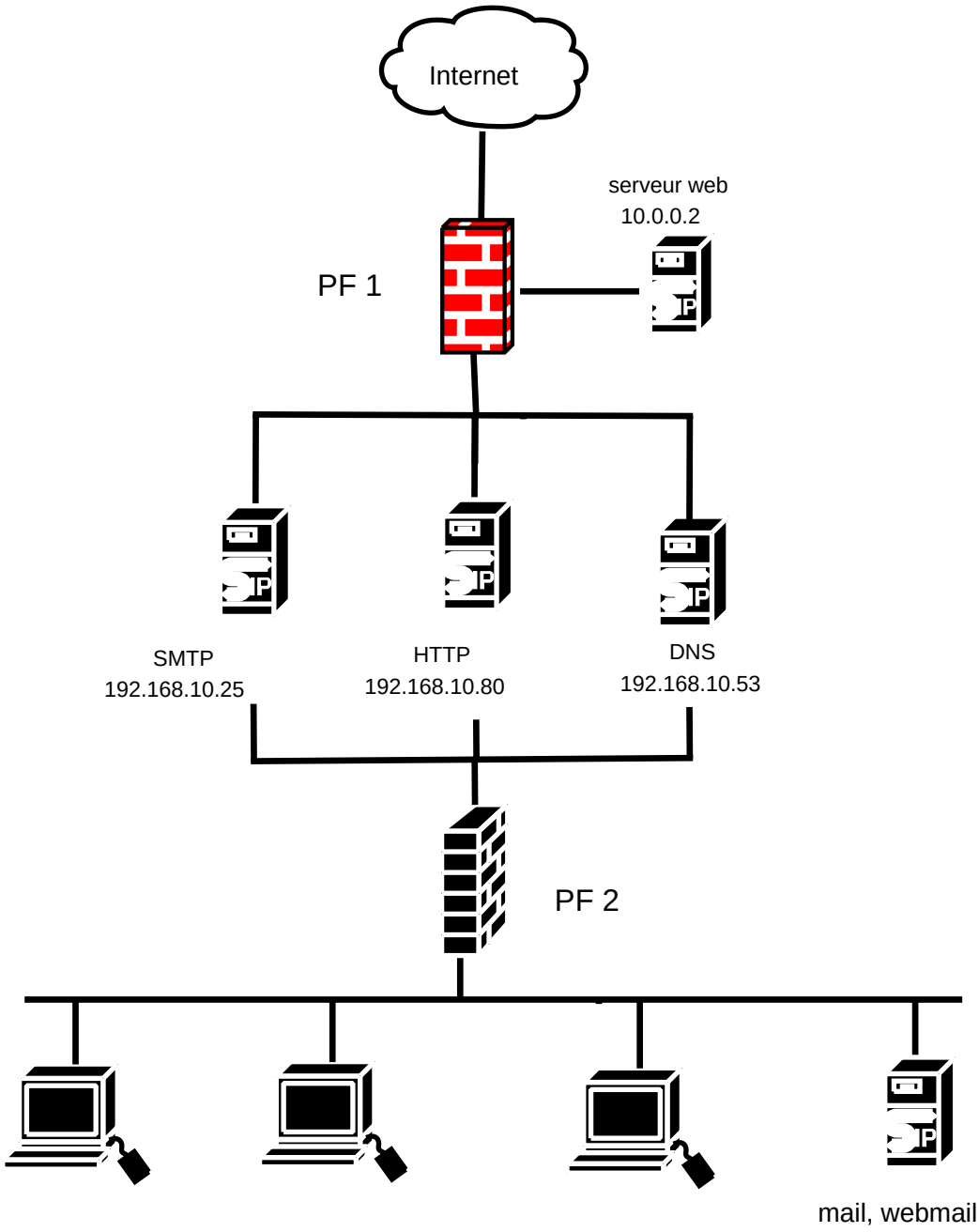

FIG. 1 – Exemple d'une architecture en sandwich.