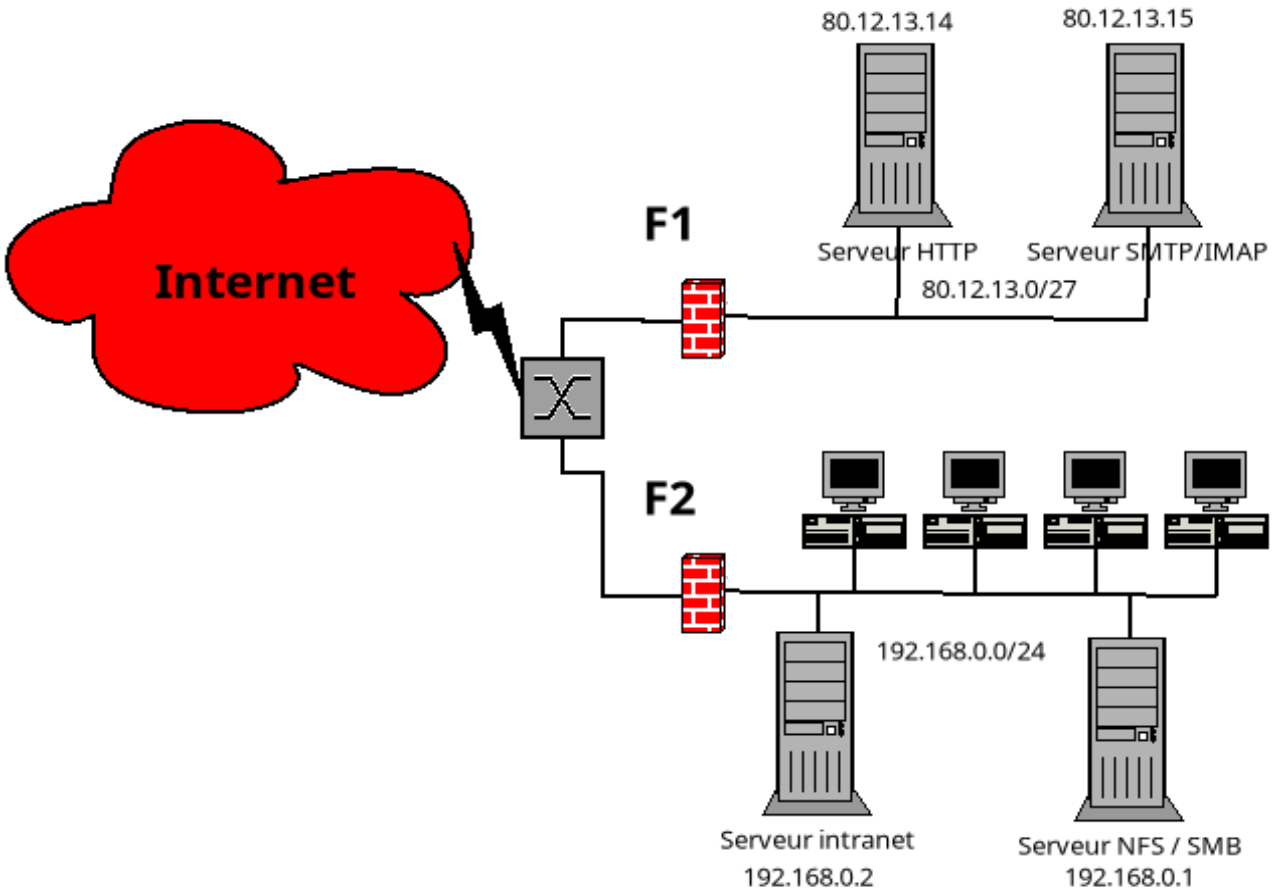
Pare-feu / Firewall

Exercice 1

Soit le réseau suivant :



Pourquoi 2 réseaux et 2 firewall ?

Donnez les services que doivent laisser passer chaque pare-feu, avec leur sens (Internet vers réseau local ou réseau local vers Internet et les éventuelles restrictions.

Comment se fait la mise à jour des données des serveurs ?

Un tel réseau avec ses deux firewall est-il une garantie contre les virus ?

Quels types d'adresses doit-on utiliser pour les machines derrière F1 ?

Exercice 2

Définissez la structure de vos pare-feux, de vos « stratégies » et essayez d'écrire vos règles en utilisant l'état de vos connexions.

- NEW pour la demande de connexion
- ESTABLISHED pour une connexion établie

Pourquoi utiliser l'état de la connexion simplifie l'écriture des règles et sécurise davantage les réseaux ?

Aide iptables :

Cette aide est non exhaustive.

iptables v1.8.10

Commands:

-A chain	Ajoute une chaîne
-L [chain [rulenum]]	Liste les règles d'une ou de toutes les règles
-S [chain [rulenum]]	Affiche comme des commandes les règles d'une ou de toutes les règles
-F [chain]	Supprime une ou toutes les chaînes
-N chain	Crée une nouvelle chaîne définit par l'utilisateur
-X [chain]	Supprime une ou toutes les chaînes définit par l'utilisateur
-P chain target	Définit la politique par défaut

Options:

[!] -p proto	protocole de la couche intermédiaire tcp, udp ou icmp
[!] -s address[/mask][...]	source sous forme d'adresse IP ou de réseau
[!] -d address[/mask][...]	destination sous forme d'adresse IP ou de réseau
[!] -i input name[+]	nom de l'interface d'entrée ([+] avec caractère joker)
[!] -o output name[+]	nom de l'interface de sortie ([+] avec caractère joker)
-j target	définit par cible de la règle (ACCEPT, DROP, …)
-m match	charge une extension
-t table	table à manipuler (par défaut: `filter')
-v	mode verbeux (bavard)
--dport port[:port]	Définit le(s) port(s) destination ([:jusqu'à ce numéro])
--sport port[:port]	Définit le(s) port(s) source ([:jusqu'à ce numéro])

Exemple :

Accepte en entrée sur l'interface eth0 les connexions à destination du service ssh.

iptables -A INPUT -p tcp -i eth0 --dport ssh -j ACCEPT