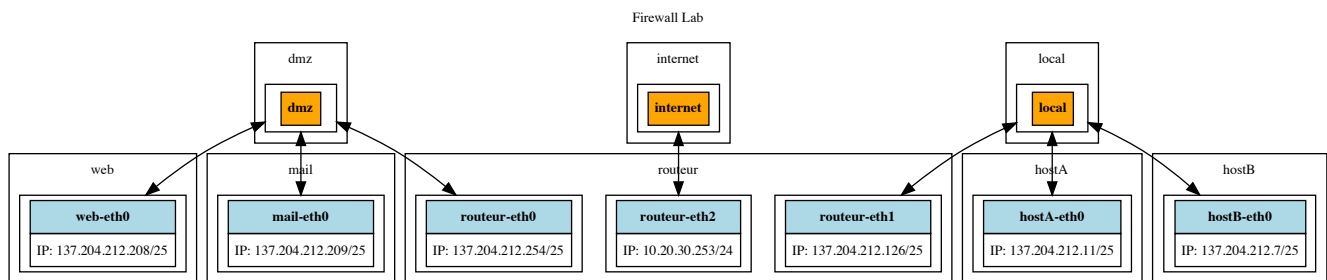


Firewall

■ ■ ■ Firewall

La politique de sécurité de la société requiert deux niveaux de sécurité :

- ★ les hôtes sur le réseau interne, « *internal network* », doivent être protégés d'accès non autorisés depuis Internet ;
- ★ les serveurs de la DMZ, « *demilitarized zone* », doivent être accessibles depuis l'extérieur.



Les fichiers de configuration de ce « *firewall lab* » sont à

https://git.unilim.fr/pierre-francois.bonnefoi/firewall_lab.git

Le firewall doit être configuré de telle manière que :

- ★ chaque connexion initiée de l'extérieur et dirigée vers la DMZ doit être autorisée, si l'adresse IP de destination et le numéro de port correspondent à un serveur accessible publiquement ;
- ★ chaque connexion initiée depuis la DMZ et dirigée vers Internet doit être autorisée ;
- ★ chaque connexion initiée depuis le réseau interne et dirigée vers la DMZ ou Internet doit être autorisée ;
- ★ tout le reste doit être bloqué.

```

1 iptables -t filter -F
2 iptables -t filter -P FORWARD DROP
3 iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
4 iptables -t filter -A FORWARD -i eth1 -d 137.204.212.208 -p tcp --dport 80 -m state --state NEW -j ACCEPT
5 iptables -t filter -A FORWARD -i eth1 -d 137.204.212.209 -p tcp --dport 25 -m state --state NEW -j ACCEPT
6 iptables -t filter -A FORWARD -s 137.204.212.0/24 -o eth1 -m state --state NEW -j ACCEPT
7 iptables -t filter -A FORWARD -s 137.204.212.0/25 -d 137.204.212.128/25 -m state --state NEW -j ACCEPT

```

■ ■ ■ Travail à réaliser

- 1 – Vous mettrez en œuvre la politique de sécurité dans l'environnement simulé avec les « *netns* » :
 - a. Qui joue le rôle du routeur pour l'accès à Internet (le vrai celui qui permet d'aller vers Google par exemple) ?
 - b. Sur qui dois-je configurer le firewall ?
 - c. Configurez le firewall avec les règles indiquées.
- 2 – Testez que les règles de firewall fonctionnent bien à l'aide des commandes :
 - a. « *socat* » en mode TCP, et en mode client et serveur, en les exécutant sur l'un ou l'autre des netns.
 - b. d'audit « *nmap* » ;
 - c. de surveillance de l'activation des règles : `sudo iptables -nvL`

3 – Ajoutez des règles permettant d’offrir l’accès à Internet pour les netns :

- a. hostA uniquement ;
- b. hostA et web ;

Sur quel « routeur » devrez vous les mettre ?

Utilisez la commande « `conntrack -L` » pour voir le SNAT se dérouler.

4 – Testez la différence de comportement observé avec « nmap », lorsque vous rejetez une demande de connexion avec « DROP » et avec « REJECT » (`reject-with icmp` et `reject-with tcp-reset`).

5 – On veut simuler un serveur web sur la machine/netns « Web » avec :

```
xterm
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Indiquez comment avec une **règle de nat** on peut accéder à ce serveur sur le port 80.

Vous utiliserez le *firewall* présent sur la machine **Web**.

6 – Donnez un **accès depuis l’extérieur** (c-à-d votre « netns root ») vers la machine hébergeant le serveur Web.

Attention

Dans ce TP vous utiliserez des adresses **publiques** qui sont utilisées sur Internet.

En cas de « *fuites* » par votre routage, des **paquets** pourraient partir vers ces machines réelles.

Vous devez faire attention à bien **enfermer** le trafic et faire du SNAT quand vous allez vers la sortie sur Internet.