## Wiki Enseignement

admin:tp5

# TP5 (Firewall)

#### Memento

Voici quelques notes concernant l'utilisation d'iptables pour configurer un firewall. La configuration du firewall se base sur la table “filter” et est subdivisée en 3 chaînes (notée <CHAIN>) :

- INPUT : tout ce qui rentre dans la machine ;
- OUTPUT : tout ce qui sort dans la machine ;
- FORWARD : tout ce qui traverse la machine (i.e. lors du routage).

Pour afficher les règles de la table filter :

```
$ iptables -t filter -L -v
```

Pour effacer toutes les règles ajoutées :

```
$ iptables -t filter -F
```

Pour chaque règle que l'on ajoute, trois actions sont possibles (notée <ACTION>) :

- ACCEPT : on accepte ;
- REJECT : on rejette poliment (réponse d'erreur envoyé à l'émetteur) ;
- DROP : on jette à la poubelle (pas de réponse d'erreur).

Pour modifier la politique par défaut du firewall :

```
$ iptables -t filter -P <CHAIN> <ACTION>
```

Pour ajouter une nouvelle règle à une chaîne du firewall (attention à l'ordre des règles) :

```
$ iptables -t filter -A <CHAIN> <SRC> <DST> <...> -j <ACTION>
```

- avec <SRC> des indications sur la provenance des paquets IP, comme par exemple ”-i eth0” ou ”-s 192.168.0.0/24” ou encore ”-s 0/0” ;
- avec <DST> des indications sur la destination des paquets IP, comme par exemple : ”-o eth1” ou ”-d 147.210.0.0/24” ;
- avec <…> des infos complémentaires sur par exemple la nature du protocole ”-p icmp” ou ”-p tcp”, avec éventuellement des precisions spécifiques à ces protocoles (”–dport 80” pour TCP) ou encore sur l'état ”-m state –state NEW”, …

Pour plus d'info, consulter le manuel : man iptables.

##### Accepter le traffic partant du réseau interne vers des serveurs web ou SSH

Soit 192.168.1.0/24 notre réseau interne. On configure le firewall sur *immortal* notre passerelle.

```
$ iptables -F
$ iptables -P FORWARD DROP
$ iptables -P INPUT DROP
$ iptables -P OUTPUT DROP

# traffic sortant
$ iptables -A FORWARD -s 192.168.1.0/24 -m multiport -p tcp --dport 22,80 -j ACCEPT

# traffic retour
$ iptables -A FORWARD -d 192.168.1.0/24 -m multiport -p tcp --sport 22,80 -m state --state ESTABLISHED -j ACCEPT
```

##### Accepter un ping toutes les 10s à destination de nile

Soit *nile* la machine 192.168.0.4. On configure le firewall sur *immortal* notre passerelle.

```
$ iptables -F
$ iptables -P FORWARD DROP
$ iptables -A FORWARD -d 192.168.0.4 -p icmp -m limit --limit 6/mn --limit-burst 1 -j ACCEPT
$ iptables -A FORWARD -s 192.168.0.4 -p icmp -m state --state ESTABLISHED -j ACCEPT
```

Pour faire un test depuis une machine extérieure, on envoie un ping à *nile* toutes les 5 secondes…

```
$ ping -i 5 192.168.0.4
```

admin/tp5.txt · Last modified: 2016/03/11 10:11 by orel