TD: parefeu

1. Expliquez les commandes :

- **a.** `iptables –t filter –P INPUT DROP`
- **b.** `iptables –t filter –P OUTPUT DROP`
- **c.** `iptables –t filter –P FORWARD DROP`

2. Expliquez les commandes – faire un schéma :

- **a.** `iptables –t filter –A INPUT --protocol tcp --destination-port http --jump ACCEPT`
- **b.** `Le poste où la règle` **a** `est installée peut être client HTTP ? Serveur HTTP ?`
- **c.** `iptables –t filter –A OUTPUT --protocol tcp --source-port http --jump ACCEPT`
- **d.** `Le poste où les 2 règles précédentes sont installées peut être client HTTP ? Serveur HTTP ?`

3. Expliquez les commandes – faire un schéma :

- **a.** `iptables –t filter –A FORWARD --protocol ICMP --jump ACCEPT`
- **b.** `iptables –t filter –A INPUT ––in-interface eth0 --protocol ICMP --jump ACCEPT`
- **c.** `iptables –t filter –A OUPUT ––out-interface eth0 --protocol ICMP --jump ACCEPT`

4. Expliquez les commandes :

- **a.** `iptables –t filter -A INPUT --jump LOG --log-prefix local`
- **b.** `iptables –t filter -A FORWARD --jump LOG --log-prefix routage`

5. Expliquez la commande : `iptables –t filter -L`

6. Expliquez les commandes – faire un schéma :

- **a.** `iptables -t nat -A POSTROUTING ––out-interface eth1 --jump MASQUERADE`
- **b.** `iptables -t nat -A POSTROUTING ––source 10.0.0.0/8 --jump SNAT 1.1.1.1`

7. Expliquez les commandes suivantes, faire un schéma et expliquez pourquoi elles ouvrent un trou de sécurité ?

- **a.** `iptables –t filter –A OUTPUT --protocol tcp --destination-port http --jump ACCEPT`
  `Le poste où la règle` **a** `est installée peut être client HTTP ? Serveur HTTP ?`
- **b.** `iptables –t filter –A INPUT --protocol tcp --source-port http --jump ACCEPT`
- **c.** Le poste où les 2 règles précédentes sont installées peut être client HTTP ? Serveur HTTP ?

8. Expliquez pourquoi les commandes suivantes équivalentes aux deux précédentes n'ouvrent pas de trou de sécurité.

- **a.** `iptables –t filter -A OUTPUT --protocol tcp --destination-port http --jump ACCEPT`
- **b.** `iptables –t filter –A INPUT --protocol tcp -m state --state ESTABLISHED --source-port http --jump ACCEPT`

II Configuration d'un parefeu

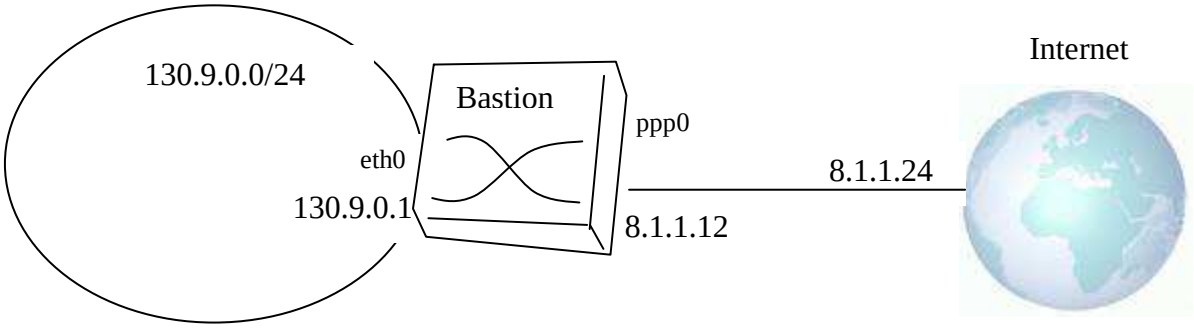

Figure 1 : plan du réseau 130.9.0.0/24

Bastion est routeur qui appartient au réseau 130.9.0.0/24 (voir la figure 1)
Bastion est un poste dont le système d'exploitation est Unix/Linux.
Le poste Bastion est le seul routeur qui connecte le réseau 130.9.0.0/24 à Internet.
Le poste 130.9.0.10 est le serveur DNS du réseau 130.9.0.0/24.
Le poste 130.9.0.20 est le serveur SMTP du réseau 130.9.0.0/24.

Objectif : installation de règles de filtrage des paquets IP sur le routeur Bastion.

a. Politiques par défaut : le rejet des paquets.

b. Acceptez la circulation des paquets ICMP à destination ou émis par le poste Bastion.

c. Acceptez la circulation des paquets ICMP à destination d'un poste du réseau 130.9.0.0/24 et les paquets émis par un poste du réseau 130.9.0.0/24.

d. Acceptez la circulation des requêtes DNS émises par le poste d'adresse IP 130.9.0.10, ainsi que leurs réponses.

e. Acceptez les connexions SMTP sortantes du poste d'adresse IP 130.9.0.20.

f. Acceptez les connexions SMTP entrantes à destination du poste d'adresse IP 130.9.0.20.

Objectif : mascarade d'adresses IP par le routeur Bastion.

a. Mettez en place la commande qui permet de cacher le sous-réseau 130.9.0.0/24 d'Internet. A savoir que tous les paquets venant de 130.9.0.0/24 sembleront venir de 8.1.1.12.

Objectif : détournement des connexions Web - *optionnel* –

Expliquer la commande :

```
iptables -t nat -A PREROUTING –-in-interface eth1 -protocol tcp
 --destination-port 80 --jump DNAT --to-destination 192.168.1.3:8080
```

a. Acceptez les connexions Web à destination d'un poste du réseau 130.9.0.0/24 venant de l'extérieur.

b. Redirigez tous les connexions Web venant de « l'extérieur » vers le poste 130.9.0.30 (port 80). Le poste 130.9.0.30 le serveur WEB du réseau 130.9.0.0/24. Acceptez les connexions Web entrantes à destination du poste d'adresse IP 130.9.0.30.