ROUTAGE / IPTABLES

```
#!/bin/sh

# vider les chaînes au niveau de toutes les tables
iptables -t filter -F
iptables -t nat -F
iptables -t mangle -F

# supprimer d'éventuelles chaînes personnelles au niveau de toutes les tables
iptables -t filter -X
iptables -t nat -X
iptables -t mangle -X


# mise en place de la politique par défaut: ne rien accepter
iptables -P INPUT  DROP
iptables -P OUTPUT  DROP
iptables -P FORWARD DROP

# autoriser le trafic sur l'interface de loopbeck ( 127.0.0.1)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# accepter tout au niveau des tables nat et mangle. Cela ne pose pas de problème parce que tout est$

# table nat
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT
```

```
# table mangle
iptables -t mangle -P PREROUTING ACCEPT
iptables -t mangle -P INPUT ACCEPT
iptables -t mangle -P OUTPUT ACCEPT
iptables -t mangle -P FORWARD ACCEPT
iptables -t mangle -P POSTROUTING ACCEPT

# ACCEPTER TOUT CE QUI VIENT DU RESEAU LOCAL
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A OUTPUT -o eth0 -j ACCEPT

#autoriser le nat uniquement pour le reseau

#AJOUTER le nat pour 192.168.2.0
iptables -t nat -A POSTROUTING -s 192.168.2.0/255.255.255.0 -o eth0 -j MASQUERADE
```

```
#autoriser le transfert du reseau local ..... vers le reseau public eth1

#AJOUTER autoriser le transfert eth1 vers eth0
iptables -A FORWARD -i eth1 -o eth0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT


#autoriser le retour


iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

#autoriser ping
iptables -A INPUT -p icmp -j ACCEPT
iptables -A OUTPUT  -p icmp -j ACCEPT

#autoriser ssh
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

```
#autoriser ftp
iptables -t filter -A INPUT -p tcp --dport 20:22 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 20:22 -j ACCEPT
```

```
#autoriser 80
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 80 -j ACCEPT
```