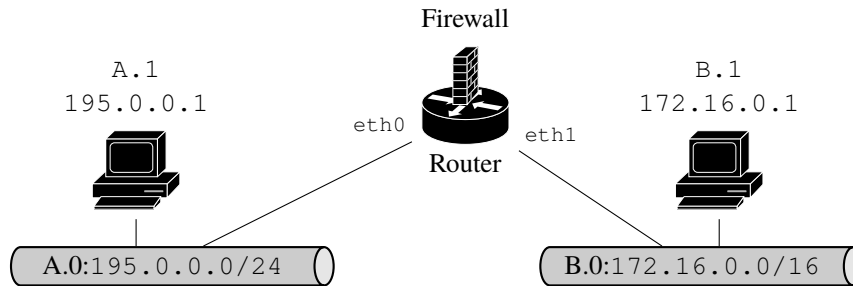


## Firewall

## ■ ■ ■ Firewall &amp; iptables

1 – Soit le réseau suivant :



La configuration du firewall :

int	config	alias
eth0	195.0.0.254/24	A.254
eth1	172.16.255.254/16	B.254

- Interdire tous les paquets de A.0 vers B.0.
- Interdire tous les paquets de A.0 vers B.1.
- Interdire tous les paquets NetBIOS à destination de A.254.  
NetBios correspond à différents protocoles utilisés par les systèmes d'exploitation Microsoft, par exemple pour le partage de ressource (fichier, imprimante, *etc.*) :
  - NetBios over TCP/IP : ports 137 & 138 (UDP) et 139 (TCP) ;
  - SMB, « *Server Message Block* » : port 445 (TCP) ;
- Masquer toutes les adresses de A.0 pour tous les protocoles.
- Masquer toutes les adresses de A.0 pour tous les protocoles uniquement pour les services SMTP et POP3.
- N'autoriser que les paquets de A.1 vers B.1, interdire tout le reste.
- N'autoriser que les paquets ssh de A.1 vers B.1, interdire tout le reste.
- N'autoriser que les paquets TCP de A.0 vers B.0, interdire tout le reste.

## La configuration de base d'iptables :

```
1 #-----Configuration initiale commune aux exercices-----
2 IPTABLES="/sbin/iptables"
3
4 RA="eth0"
5 RB="eth1"
6
7 A1="195.0.0.1"
8 A254="195.0.0.254"
9 B1="172.16.0.1"
10 B254="172.16.255.254"
11
12 sysctl net.ipv4.conf.all.forwarding=1
13
14 # On efface tout
15 $IPTABLES -F
16 $IPTABLES -X
17
18 # On bloque tout
19 $IPTABLES -P INPUT DROP
20 $IPTABLES -P FORWARD DROP
21 $IPTABLES -P OUTPUT DROP
22
23 # Initialisation de la table nat
24 $IPTABLES -t nat -F
25 $IPTABLES -t nat -X
26 $IPTABLES -t nat -P PREROUTING ACCEPT
27 $IPTABLES -t nat -P POSTROUTING ACCEPT
28 $IPTABLES -t nat -P OUTPUT ACCEPT
29
30 # Autorisation de communication pour les protocoles locaux
31 $IPTABLES -A INPUT -i lo -j ACCEPT
32 $IPTABLES -A OUTPUT -o lo -j ACCEPT
33
34 # Création des chaines
35 $IPTABLES -N RA_RB
36 $IPTABLES -N RB_RA
37
38 # Initialisation des chaines
39 $IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
40 $IPTABLES -A FORWARD -i $RA -o $RB -j RA_RB
41 $IPTABLES -A FORWARD -o $RA -i $RB -j RB_RA
42 #-----
```