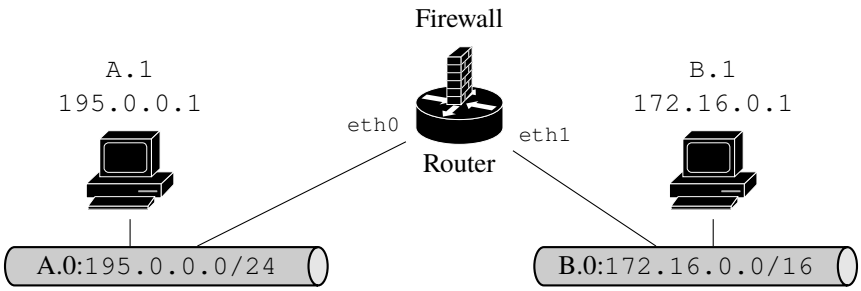
Firewall

Firewall & 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

a. Interdire tous les paquets de A.0 vers B.0.

b. Interdire tous les paquets de A.0 vers B.1.

c. 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) ;

d. Masquer toutes les adresses de A.0 pour tous les protocoles.

e. Masquer toutes les adresses de A.0 pour tous les protocoles uniquement pour les services SMTP et POP3.

f. N'autoriser que les paquets de A.1 vers B.1, interdire tout le reste.

g. N'autoriser que les paquets ssh de A.1 vers B.1, interdire tout le reste.

h. N'autoriser que les paquets TCP de A.0 vers B.0, interdire tout le reste.

La configuration de base d'iptable :

```
#----------------------Configuration initiale commune aux exercices-----
IPTABLES="/sbin/iptables"

RA="eth0"
RB="eth1"

A1="195.0.0.1"
A254="195.0.0.254"
B1="172.16.0.1"
B254="172.16.255.254"

sysctl net.ipv4.conf.all.forwarding=1

# On efface tout
$IPTABLES -F
$IPTABLES -X

# On bloque tout
$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD DROP
$IPTABLES -P OUTPUT DROP

# Initialisation de la table nat
$IPTABLES -t nat -F
$IPTABLES -t nat -X
$IPTABLES -t nat -P PREROUTING ACCEPT
$IPTABLES -t nat -P POSTROUTING ACCEPT
$IPTABLES -t nat -P OUTPUT ACCEPT

# Autorisation de communication pour les protocoles locaux
$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -A OUTPUT -o lo -j ACCEPT

# Création des chaines
$IPTABLES -N RA_RB
$IPTABLES -N RB_RA

# Initialisation des chaines
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -i $RA -o $RB -j RA_RB
$IPTABLES -A FORWARD -o $RA -i $RB -j RB_RA
#-------------------------------------------------------------------------
```