Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

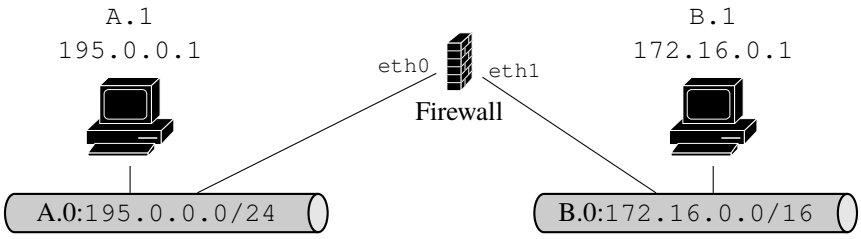
Admin Rés

Corrections TD n°3

Firewall

Firewall & iptables

1 – Soit le réseau suivant :



Attention

Les réponses aux différentes questions sont à insérer, chacunes, dans le fichier de configuration donné en fin de fiche de TD n°3.

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

```
xterm
$IPTABLES -t filter -P RA_RB DROP
```

Si l'on ne se sert pas de la chaîne `RA_RB` pour être plus précis :

```
xterm
$IPTABLES -A FORWARD -s 195.0.0.0/24 -d 172.16.0.0/16 -j DROP
```

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

```
xterm
$IPTABLES -t filter -A RA_RB -d $B1 -j DROP
```

Si l'on ne se sert pas de la chaîne `RA_RB` :

```
xterm
$IPTABLES -A FORWARD -s 195.0.0.0/24 -d 172.16.0.1 -j DROP
```

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) ;

```
xterm
$IPTABLES -A INPUT -p udp --dport 137 -j DROP
$IPTABLES -A INPUT -p udp --dport 138 -j DROP
$IPTABLES -A INPUT -p tcp -m tcp --dport 139 -j DROP
$IPTABLES -A INPUT -p tcp -m tcp --dport 445 -j DROP
```

Ici, on peut également utiliser un intervalle de ports ou une liste, et préciser l'interface d'entrée :

```
xterm
$IPTABLES -A INPUT -i eth0 -p udp -m multiport --dport 137:139 -j DROP
$IPTABLES -A INPUT -i eth0 -p tcp -m multiport --dport 139,445 -j DROP
```

d. Masquer toutes les adresses de A.0 pour tous les protocoles (on réalise l'opération de « MASQUERADING », c-à-d une version de SNAT pour une adresse IP du routeur obtenue dynamiquement) :

xterm
```
$IPTABLES -t nat -A POSTROUTING -s 195.0.0.0/24 -o eth1 -j MASQUERADE
```

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

xterm
```
$IPTABLES -t nat -A POSTROUTING -i $RA -p tcp -m multiport --dport 25,110 -o
eth1 -j MASQUERADE
```

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

xterm
```
$IPTABLES -P RA_RB DROP
$IPTABLEs -P RB_RA DROP
$IPTABLES -A RA_RB -s $A1 -d $B1 -m state --state NEW -j ACCEPT
```

Remarques : les paquets en retour sont autorisés par la règle du fichier de configuration :

xterm
```
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

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

xterm
```
$IPTABLES -P RA_RB DROP
$IPTABLEs -P RB_RA DROP
$IPTABLES -A RA_RB -s $A1 -d $B1 -p tcp --dport 22 -m state --state NEW -j
ACCEPT
```

Remarques : les paquets en retour sont autorisés par la règle du fichier de configuration :

xterm
```
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

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

xterm
```
$IPTABLES -P RA_RB DROP
$IPTABLEs -P RB_RA DROP
$IPTABLES -A RA_RB -s 195.0.0.0/24 -d 172.16.0.1/16 -p TCP -m state --state NEW
-j ACCEPT
```

Remarques : les paquets en retour sont autorisés par la règle du fichier de configuration :

xterm
```
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Remarque

Les numéros de port associés aux services sont indiqués dans le fichier `/etc/services`.