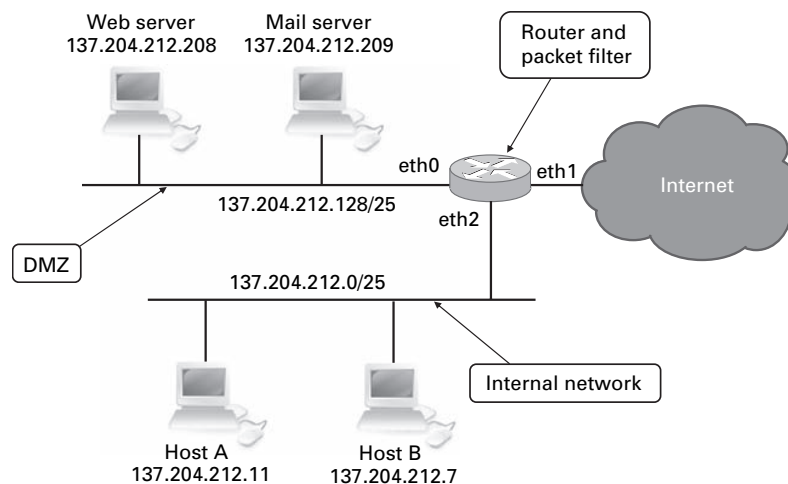


Routing & Firewall

■ ■ ■ Firewall

1 – Une société dispose de 137.204.212.0/24 :



La politique de sécurité de la société requiert deux niveaux de sécurité :

- ▷ les hôtes sur le réseau interne, « *internal network* », doivent être protégés d'accès non autorisés depuis Internet ;
- ▷ les serveurs de la DMZ, « *demilitarized zone* », doivent être accessibles depuis l'extérieur.

Le firewall doit être configuré de telle manière que :

- \* chaque connexion initiée de l'extérieur et dirigée vers la DMZ doit être autorisée, si l'adresse IP de destination et le numéro de port correspondent à un serveur accessible publiquement ;
- \* chaque connexion initiée depuis la DMZ et dirigée vers Internet doit être autorisée ;
- \* chaque connexion initiée depuis le réseau interne et dirigée vers la DMZ ou Internet doit être autorisée ;
- \* tout le reste doit être bloqué.

**Remarque :** pour désigner n'importe quelle adresse on utilise la notation 0.0.0.0/0.

Donnez la configuration du firewall.

La politique de sécurité de la société est la suivante :

```
xterm
sudo iptables -t filter -P FORWARD DROP
sudo iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -t filter -A FORWARD -i eth1 -d 137.204.212.208 -p tcp --dport 80 -m state --state NEW -j ACCEPT
sudo iptables -t filter -A FORWARD -i eth1 -d 137.204.212.209 -p tcp --dport 25 -m state --state NEW -j ACCEPT
sudo iptables -t filter -A FORWARD -s 137.204.212.0/24 -o eth1 -m state --state NEW -j ACCEPT
sudo iptables -t filter -A FORWARD -s 137.204.212.0/25 -d 137.204.212.128/25 -m state --state NEW -j ACCEPT
```

2– Soit la trace suivante :

3pts

Chain FORWARD (policy DROP 345 packets, 23678 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
57	2280	REJECT	tcp	--	eth1	eth2	210.12.56.35	164.81.45.78	tcp dpt:22 reject-with tcp-reset

a. Quelle commande a fourni cette trace ?

```
xterm
iptables -nvL
```

b. Donnez la commande « iptables » qui a défini cette règle.

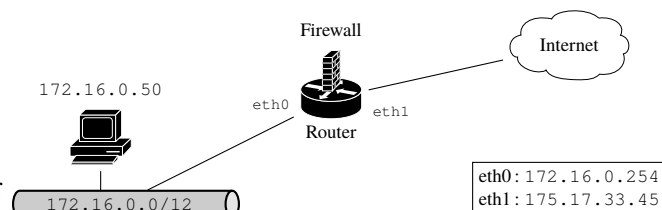
```
xterm
iptables -A FORWARD -i eth1 -o eth2 -s 210.12.56.35 -d 164.81.45.78 -p tcp
--dport 22 -j REJECT --reject-with tcp-reset
```

- c. Cette règle a-t-elle été déjà utilisée ?  
*Oui, le compteur d'activation associé à la règle indique 57 paquets traités.*
- d. La «règle» est-elle bien adaptée à la «policy» ?  
*Si on compare les deux :*
- ◇ la «policy» est DROP, c-à-d que si aucune règle ne «match», correspond, au paquet alors le paquet sera supprimé.
  - ◇ la règle rejette le paquet en informant l'émetteur par un «tcp-reset».
- Dans tous les cas, le paquet est supprimé, par contre avec la règle on choisit d'informer l'émetteur de cette suppression.*  
*Du point de vue strict de l'effet, on peut dire que la règle ne sert à rien.*
- e. Qu'est-ce qu'indiquerait l'outil «nmap», s'il «auditait» ce firewall ?  
*L'outil «nmap» teste successivement différents ports à la recherche de services «sensibles».*  
*Dans le cas d'un rejet avec un «tcp-reset» l'outil interprète le port comme inexistant, comme si le service n'était pas présent sur la cible.*  
*Sans la règle, l'outil «nmap» indiquerait «filtered» ce qui peut trahir la présence du service et de sa protection.*

3 – Une petite PME vous contacte pour configurer le routeur/firewall dans la configuration réseau suivante :

La **politique de sécurité** est la suivante :

- ★ autoriser les communications « intérieur  
 ⇒ extérieur » (l'extérieur correspondant à Internet) ;
- ★ bloquer les communications « extérieur  
 ⇒ intérieur » ;
- ★ autoriser les communications vers la machine 172.16.0.50 depuis l'extérieur vers les services :
  - ◇ web (http) et web sécurisé (https) ;
  - ◇ ssh.



### Questions :

- a. Dans quel type de réseau est installé le serveur 172.16.0.50 ?  
*Dans un réseau privé.*  
 Donnez la configuration du routeur Netfilter à l'aide de commandes «iptables» conformément à cette politique de sécurité.  
*Le réseau de l'entreprise étant privé, il est naturellement protégé contre les accès extérieurs :*
- ◇ pour permettre aux communications de sortir il faut faire du SNAT, ou «masquerading», avec comme @IP source, l'@IP globale du routeur ;
  - ◇ pour permettre les communications entrantes, il faut faire du «port forwarding», c-à-d du DNAT.

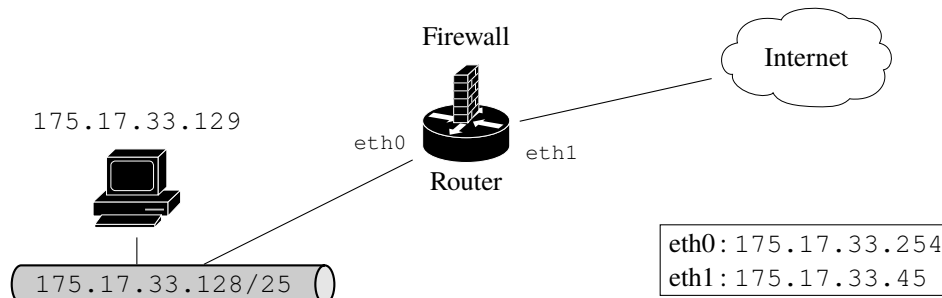
*On choisit de «tout bloquer et d'autoriser seulement le trafic que l'on veut » :*

```
xterm
iptables -t filter -P FORWARD DROP
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A FORWARD -s 172.16.0.0/12 -o eth1 -m state --state NEW -j ACCEPT
iptables -t nat -A POSTROUTING -s 172.16.0.0/12 -o eth1 -j SNAT --to 175.17.33.45
```

Pour l'autorisation des communications de l'extérieur vers la machine 172.16.0.50, on utilise du DNAT et on autorise le passage du trafic :

```
xterm
iptables -t nat -A PREROUTING -d 175.17.33.45 -p tcp --dport 22 -j DNAT --to 172.16.0.50
iptables -t nat -A PREROUTING -d 175.17.33.45 -p tcp --dport 80 -j DNAT --to 172.16.0.50
iptables -t nat -A PREROUTING -d 175.17.33.45 -p tcp --dport 443 -j DNAT --to 172.16.0.50
iptables -t filter -A FORWARD -d 172.16.0.50 -p tcp --dport 22 -d 172.16.0.50 -m state --state NEW -j ACCEPT
iptables -t filter -A FORWARD -d 172.16.0.50 -p tcp --dport 80 -d 172.16.0.50 -m state --state NEW -j ACCEPT
iptables -t filter -A FORWARD -d 172.16.0.50 -p tcp --dport 443 -d 172.16.0.50 -m state --state NEW -j ACCEPT
```

La PME a investi dans l'achat du réseau 175.17.33.128/25 et a reconfiguré son réseau de la manière suivante :



Elle vous contacte pour reconfigurer son routeur/firewall.

- b. Donnez la nouvelle configuration à l'aide de commandes « iptables » du firewall conformément à la politique de sécurité définie précédemment ;

*Le réseau de l'entreprise est un réseau global, il n'y a plus de traduction d'adresses à faire.*

```
xterm
iptables -t filter -P FORWARD DROP
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -d 175.17.33.129 -p tcp --dport 80 -m state --state NEW -j ACCEPT
iptables -A FORWARD -d 175.17.33.129 -p tcp --dport 443 -m state --state NEW -j ACCEPT
iptables -A FORWARD -d 175.17.33.129 -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

- c. le responsable de la PME vous demande de protéger l'accès au serveur SSH de la machine 175.17.33.129 contre les attaques « brute force » :

*On va limiter dans le temps les tentatives de connexion, ce qui ralentira et rendra très difficile les attaques « brute force », en modifiant la règle précédente (autorisant le trafic vers ssh) :*

```
xterm
iptables -A FORWARD -d 175.17.33.129 -p tcp --dport 22 -m state --state NEW -m limit --limit 3/min --limit-burst 1 -j ACCEPT
```

*Seul une demande de connexion toutes les 20s est autorisée, ce qui va ralentir et rendre impossible une attaque « brute force ».*