Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

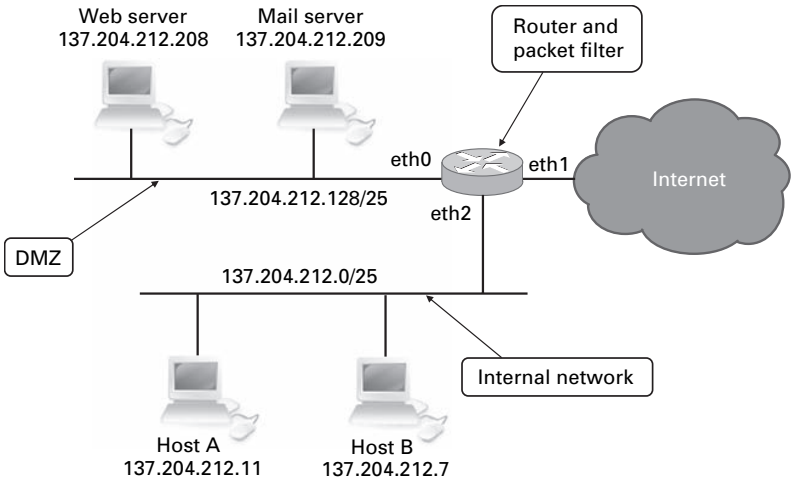
Admin Réseau

TD n°2

Routage & 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.

2 – Soit la trace suivante :

```
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 ?

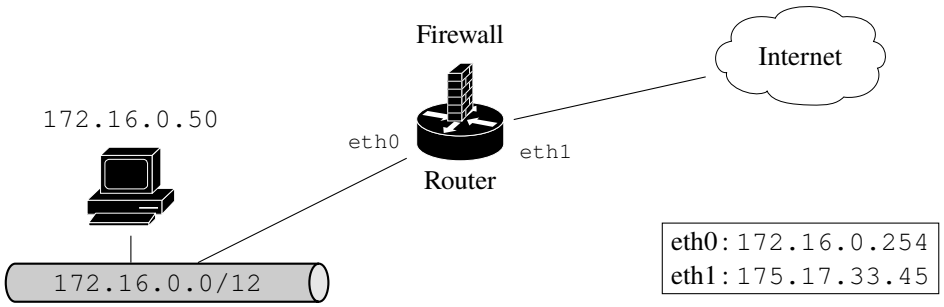
b. Donnez la commande « `iptables` » qui a défini cette règle.

c. Cette règle a-t-elle été déjà utilisée ?

d. La « règle » est-elle bien adaptée à la « *policy* » ?

e. Qu'est-ce qu'indiquerait l'outil « `nmap` », s'il « auditait » ce firewall ?

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



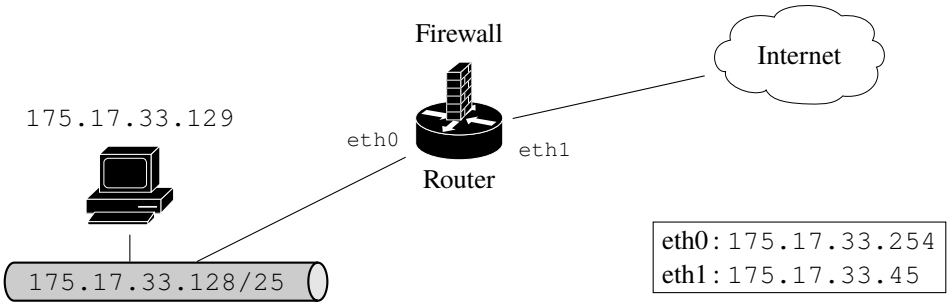
La **politique de sécurité** est la suivante :

- ⋆ 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` ?
Donnez la configuration du routeur Netfilter à l'aide de commandes « `iptables` » conformément à cette politique de sécurité.

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 ;

c. le responsable de la PME vous demandede protéger l'accès au serveur SSH de la machine `175.17.33.129` contre les attaques « brute force ».
Vous indiquerez la ou les commandes « `iptables` » à utiliser.