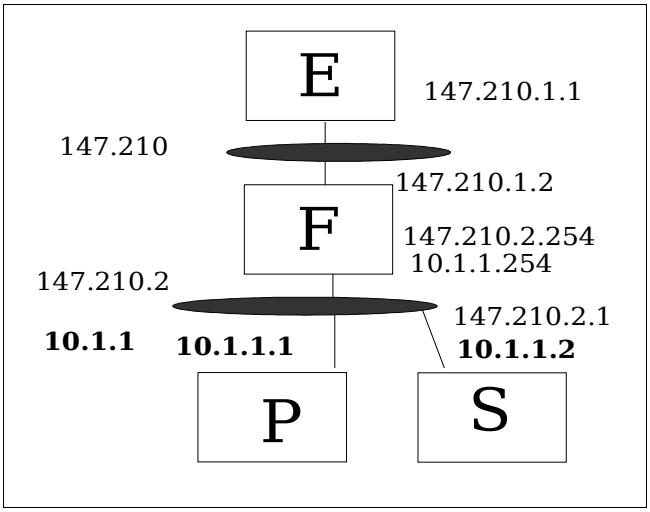
Département Informatique
IUT Bordeaux 1

Mars 2005

IO4 -Travaux dirigés

1.Un poste individuel relié au réseau



Établir et tester les règles de filtrages pour un **poste de travail individuel** relié au réseau. On simulera le réseau extérieur par une seule machine, qui jouera aussi le rôle de serveur de noms.

Politique à respecter:

1. Le poste de travail peut ouvrir des communications librement vers l'extérieur
2. de l'extérieur, on peut y accéder par `ssh` uniquement.

1. mettre en place une simulation de ce réseau, avec les deux réseaux (extérieur et intérieur) et 4 machines (E, F, P et S). On suppose que le réseau extérieur est `147.210`, que le réseau intérieur public est `147.210.2`, et le réseau privé `10.1.1`.
2. Configurer les routages. Sur E, ne pas mettre de route pour le sous-réseau privé. Vérifiez qu'on peut utiliser ssh entre E vers S, entre S et P mais pas entre E et P.
3. Mettre en place les règles de filtrage empêchant les connexions de l'extérieur vers S, à l'exception de SSH.
4. Ajoutez une route par défaut pour les postes clients. Normalement cette route ne permet pas de joindre E depuis P. Contrôlez.

2.Protection d'un sous-réseau

On considère une architecture de type « sous-réseau à écran », dans laquelle le sous-réseau contenant un poste individuel P et un serveur S avec adresse publique) est protégé par un routeur filtrant *F.*

L'objectif est de permettre :

- *des connexions `ssh` depuis P et S vers E, et de E vers S uniquement.*
- *L'interrogation du DNS de E depuis S et (indirectement) depuis P,*

5. Le « *masquerading* » se met en place en ajoutant une règle dans la chaîne POSTROUTING de la table « `nat` »

   ```
   iptables -t nat -A POSTROUTING --source  10.1.1.0/24 -j MASQUERADE
   ```

6. Installer un DNS sur E et S. Configurez celui de S en mandataire pour le réseau privé.

   Vérifiez que depuis P on peut joindre E par `ssh`, mais pas l'inverse.

Memento

Routage

Associer une adresse IP à une interface	**ifconfig** eth0 10.1.2.3 netmask 255.255.255.0
Associer une seconde adresse	**ifconfig** eth0:0 20.30.40.450
Route par défaut	**route** add default gw 10.1.1.254
Route pour sous-réseau local	**route** add -net 10.1.1.0 \ netmask 255.255.255.0 dev eth0

Commandes IPTABLES

Voir les règles	**iptables** -L
Définir politique par défaut	**iptables** -P INPUT DROP
Effacer règles	**iptables** -F
Effacer règles d'une chaîne	**iptables** -F INPUT
Créer une chaîne	**iptables** -N machaîne
Supprimer une chaîne	**iptables** -X machaîne
Ajouter une règle	**iptables** -A machaîne –s 10.1.1.0/24 -j ACCEPT

Conditions IPTABLES

Adresse IP (source, destination)	-s 10.1.1.0/24 -d ! 10.1.1.45
Protocole	-p tcp
Port (avec TCP ou UDP)	--source-port 53 --destination-port 1024:10000
Interface	-i eth0 -o ppp0
Extension	-m state –-state ESTABLISHED,RELATED
Saut vers cible prédéfinie (accept, drop, reject) ou chaîne	-j ACCEPT -j machaîne

Masquerading

```
iptables -t nat -A POSTROUTING \
    --source 10.1.1.0/24 -o eth1 \
    -j MASQUERADE
```