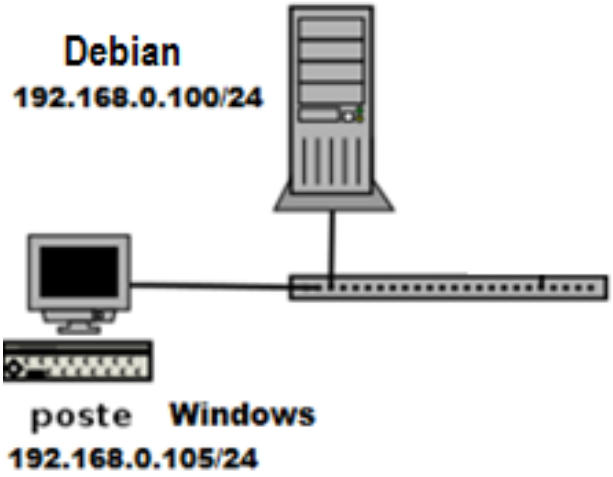
TP Filtrage noyau - iptables/netfilter

Objectif

Mise en œuvre d'un script pare-feu sur une machine à une carte.

Schéma



Configuration : une MV Debian 9 **srviptables (**une seule carte en pont 192.168.0.100 par exemple) et une MV client Window **postewin** pour les tests (en pont 192.168.0.105 par exemple).

Remarque : répartition des adresses ip distinctes dans un même plot afin d'éviter les conflits.

Plan de l'atelier

1. Mise en place de la configuration
2. Création d'un script évolutif regroupant les iptables sur **srviptables**
   a. Stratégie par défaut : tout bloquer
   b. Autoriser DNS client, Web client puis tester. (identifier protocoles et ports utilisés)
   c. N'autoriser que l'accès web (port 80) sur la machine **srviptables** depuis l'extérieur. Tester depuis l'extérieur avec **postewin** et un navigateur.
   d. Autoriser l'accès SSH depuis l'extérieur
   e. Autoriser l'accès SSH depuis l'extérieur sauf pour la machine **postewin**
   f. Autoriser le **ping** depuis la machine **srviptables**

1. Mise en place de la configuration réseau

- Installer sur **srviptables** Apache2 : aptitude install apache2
- Configurer les interfaces en adressage fixe avec passerelle en 192.168.0.1
- Nommer les machines

2. Création d'un script évolutif regroupant les iptables

A chaque étape, on utilisera `iptables -L` et/ou `iptables -L -t nat` pour contrôler l'effet des commandes lancées.

Créer un fichier bash fw (firewall) sous /root pour déclarer les iptables. Le rendre exécutable et l'exécuter ./fw
Mettre un commentaire à chaque étape de la constitution du fichier fw :

```
  GNU nano 2.2.6              Fichier : /root/fw

#!/bin/bash

# Vidage de la table
iptables -F

# Stratégie par défaut : blocage total
```

a. Stratégie par défaut : tout bloquer.
   Tester :

b. Autoriser DNS client, Web client.
   Identifier protocoles et ports utilisés
   Tester :
   - Faire un host d'un site, faire un wget ou curl d'un site.
   - Voir les logs : tail –f /var/log/apache2/access.log

c. N'autoriser que l'accès web sur **srviptables** depuis l'extérieur.
   Tester :
   - Depuis l'extérieur (**postewin**) avec un navigateur

d. Autoriser l'accès SSH depuis l'extérieur
   Identifier protocole et port utilisés
   Tester :
   - Depuis l'extérieur (**postewin**) avec un navigateur

e. Autoriser l'accès SSH depuis l'extérieur sauf pour la machine précédente
   Tester :
   - Depuis l'extérieur (**postewin**) avec un navigateur
   - Depuis l'extérieur avec une autre machine

f. Autoriser le **ping** depuis la machine **srviptables**

   Identifier protocole utilisé. Tester.