Prérequis :

- Avoir pris connaissance du cours Protection 3 sur les commandes **IPTABLES**

- Installation du package ifupdown

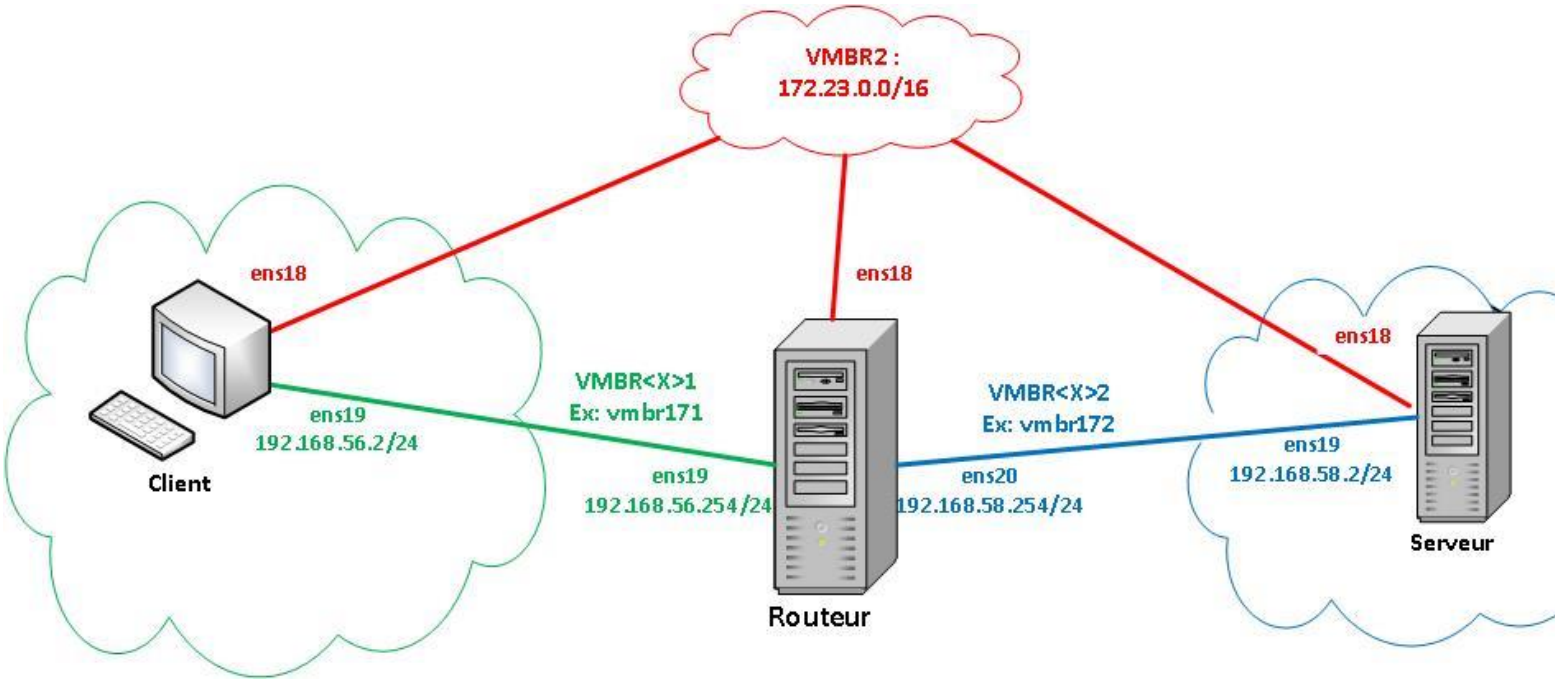
- 1 VM **Client** :
  - Type Ubuntu Serveur, Ubuntu Desktop ou Debian
  - 1 interface connectée à VMBR2 (ex : ens18 => 172.23.3.X/24)
  - 1 interface connectée à VMBR**X**1 (ex : ens19 => à adresser via Netplan sur Ubuntu Server ou /etc/network/interfaces sur Debian)
    - Avec **X** = n° de groupe : pour le groupe 17=> VMBR171
    - Adresse IP d'ens19 : 192.168.56.2/24

- 1 VM **Serveur** :
  - Type Ubuntu Serveur, Ubuntu Desktop ou Debian
  - 1 interface connectée à VMBR2 (ex : ens18 => 172.23.3.X/24)
  - 1 interface connectée à VMBR**X**2 (ex : ens19 => à adresser via Netplan sur Ubuntu Server ou /etc/network/interfaces sur Debian)
    - Avec **X** = n° de groupe : pour le groupe 17=> VMBR172
    - Adresse IP d'ens19 : 192.168.58.2/24

- 1 VM **Routeur** :
  - Type Ubuntu Serveur, Ubuntu Desktop ou Debian
  - 1 interface connectée à VMBR2 (ex : ens18 => 172.23.3.X/24)
  - 1 interface connectée à VMBR**X**1 (ex : ens19 => à adresser via Netplan sur Ubuntu Server ou /etc/network/interfaces sur Debian)
    - Avec **X** = n° de groupe : pour le groupe 17=> VMBR171
    - Adresse IP d'ens19 : 192.168.56.254/24
  - 1 interface connectée à VMBR**X**2 (ex : ens20 => à adresser via Netplan sur Ubuntu Server ou /etc/network/interfaces sur Debian)
    - Avec **X** = n° de groupe : pour le groupe 17=> VMBR172
    - Adresse IP d'ens20 : 192.168.58.254/24

Remarque : Si une interface supplémentaire est connectée sur VMBR0, vous pouvez la laisser telle quelle sans forcément la supprimer.

Schéma de principe :



1. Configuration des interfaces sur les postes :

Dans le fichier /etc/network/interfaces de chaque poste, configurer les interfaces de la manière suivante. ATTENTION, les noms des interfaces sont à adapter en fonction de votre installation.

VM "Client":

Sur Debian :

```
auto ens19
iface ens19 inet static
        address 192.168.56.2
        netmask 255.255.255.0
        up ip route add 192.168.58.0/24 via 192.168.56.254
```

Sur Ubuntu (Netplan) :

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens19:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.56.2/32]
      routes:
      - to: 192.168.58.0/24
        via: 192.168.56.254
        scope: link
```

VM "Serveur":

Sur Debian :

```
auto ens19
iface ens19  inet static
        address 192.168.58.2
        netmask 255.255.255.0
        up ip route add 192.168.56.0/24 via 192.168.58.254
```

Sur Ubuntu (Netplan) :

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens19:
      dhcp4: no
```

```
    dhcp6: no
    addresses: [192.168.58.2/32]
    routes:
    - to: 192.168.56.0/24
      via: 192.168.58.254
      scope: link
```

VM "Routeur":

Sur Debian :

```
auto ens19
iface ens19  inet static
        address 192.168.56.254
        netmask 255.255.255.0

auto ens20
iface ens20  inet static
        address 192.168.58.254
        netmask 255.255.255.0
```

Sur Ubuntu (Netplan) :

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens19:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.56.254/32]
    ens20:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.58.254/32]
```

Pour Activer le Forwarding des paquets sur la VM Routeur et que cette modification soit permanente, éditer le fichier **/etc/sysctl.conf** et décommenter **net.ipv4.ip_forward=1**

Lancer la commande **sysctl -p**

Vérifier la communication entre le Client et le Serveur avec un ping réciproque.

2. Mise en place d'un processus SSHD en écoute sur le Serveur

Installer le package openssh-server. Démarrer
le service ssh :

```
# systemctl restart ssh
```

Sur le Client, tentez de vous connecter sur le daemon ssh du serveur :

```
# ssh toto@192.168.58.2          (depuis le Client)
```

Si le prompt apparaît, cela signifie que vous êtes connecté, et donc inutile d'aller plus loin, faîtes Ctrl-C.

3. Mise en place d'un filtrage IPtables sur le Serveur en INPUT.

Grâce à iptables, activer un filtrage sur la chaîne INPUT du serveur de manière à n'autoriser l'accès au daemon SSH que depuis la machine source 192.168.58.254. Tout le reste du traffic devra être interdit.

```
# ssh toto@192.168.58.2          (depuis le Routeur)
```

4. Mise en place d'un filtrage IPtables sur le routeur en FORWARD.

Toujours avec iptables , filtrer le traffic sur le routeur de manière à ne laisser passer que le traffic SSH du Client vers le Serveur.

```
# ssh toto@192.168.58.2          (depuis le Client)
```

5. Mise en place de redirection de port sur le routeur

Toujours avec iptables mettre en place une translation d'adresse destination avec redirection de port, de manière à ce que , lorsque le client se connecte le port 2222 du Routeur, la requête arrive sur le port 22 du Serveur.

```
# ssh –p 2222 toto@192.168.56.254          (depuis le Client)
```