iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source 172.16.2.254
iptables -A FORWARD -s 172.16.1.0/24 -d 172.16.3.0/24 -j DROP

1)

`iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source 172.16.2.254`

- `-t nat` : indique que la règle appartient à la table NAT, utilisée pour modifier les adresses IP (source ou destination).
- `-A POSTROUTING` : ajoute la règle dans la chaîne POSTROUTING, exécutée après la décision de routage, juste avant que le paquet quitte l'interface.
- `-o eth1` : la règle ne s'applique qu'aux paquets sortant par l'interface eth1.
- `-j SNAT` : l'action consiste à effectuer un Source NAT, c'est-à-dire modifier l'adresse source du paquet.
- `--to-source 172.16.2.254` : nouvelle adresse source à utiliser pour ces paquets.
- Effet global : tous les paquets sortant par eth1 auront pour adresse source 172.16.2.254 ; ceci permet d'assurer que les machines en aval envoient correctement leurs réponses vers la passerelle.

---

2)

`iptables -A FORWARD -s 172.16.1.0/24 -d 172.16.3.0/24 -j DROP`

- `-A FORWARD` : ajoute une règle à la chaîne FORWARD, qui filtre les paquets transitant par la machine lorsqu'elle agit comme routeur.
- `-s 172.16.1.0/24` : condition sur l'adresse source ; la règle s'applique uniquement aux paquets provenant du réseau 172.16.1.0/24.
- `-d 172.16.3.0/24` : condition sur l'adresse de destination ; la règle ne concerne que les paquets visant le réseau 172.16.3.0/24.

- `-j DROP` : le paquet correspondant à ces conditions est supprimé sans notification à l'expéditeur.

- Effet global : tout trafic entre S1 et S3 dans ce sens est bloqué.

1. PREROUTING – DNAT (changer la destination)

C'est ce qu'on vous demande pour : serveur web, serveur FTP, services internes.

- Port forwarding HTTP
  ```
  iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 10.3.2.1:80
  ```

- Port forwarding FTP (TP03 partie II)
  ```
  iptables -t nat -A PREROUTING -p tcp --dport 21 -j DNAT --to 172.16.2.10:21
  ```

- Redirection interne
  ```
  iptables -t nat -A PREROUTING -p tcp --dport 8080 -j REDIRECT --to-port 80
  ```

- Redirection basée sur la source
  ```
  iptables -t nat -A PREROUTING -s 10.0.0.5 -j DNAT --to 192.168.1.10
  ```

port 22: ssh
port 80 : https

Salut les gars alors pour configurer un DHCP:

1. `/etc/dhcp/dhcpd.conf` – Le fichier de configuration principal

C'est le cœur de la configuration du serveur DHCP. Dans ce fichier, tu définis :

- Les **plages d'adresses IP** que le serveur DHCP peut attribuer.

- Les **options** comme les routeurs, les serveurs DNS, la durée du bail, etc.

- Les sous-réseaux que le serveur peut gérer.

- Les **adresses fixes** pour certains clients, comme le routeur ou des équipements spécifiques.

Exemple de `dhcpd.conf` :

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.100; // tu met la range que tu veux
ici
  option subnet-mask 255.255.255.0;
}
```

2.ensuite dans le etc/default/isc-dhcp-server

tu cale :

INTERFACESV4:”eth0”

#INTERFACESV6:””

En résumé, pour la configuration de base de DHCP, les deux fichiers principaux sont :

1. **`/etc/dhcp/dhcpd.conf`** (configuration du serveur DHCP)

exemple du dhcp.conf du tp3:

```
default-lease-time 600;
max-lease-time 7200;

option rfc-3442-classless-static-routes code 121 = array of integer 8;

subnet 192.168.10.0 netmask 255.255.255.0 {
  range 192.168.10.10 192.168.10.40;
  option rfc-3442-classless-static-routes 24,172.16.2.192,168,10,254;
}

host GW-eth0 {
  hardware ethernet 42:00:00:00:00:02;
  fixed-address 172.16.2.254;
}

host GW-eth1 {
```

```
  hardware ethernet 42:00:00:00:00:04;
  fixed-address 192.168.10.254;
}

subnet 172.16.2.0 netmask 255.255.255.0 {
  range 172.16.2.1 172.16.2.254;
  option subnet-mask 255.255.255.0;
}

#option rfc-3442.... : l'adresse 172.16.2.7/24 dans 192.168.10.254 pour que les noeuds 192
connaissent les autres routes.

# SYNTAXE : dhcrelay -i INTERFACE SERVEUR_DHCP
dhcrelay -i eth0 192.168.10.10  # Écoute sur eth0 seulement et évite les doublons
```