Guide complet de `iptables -t nat`

Structure de base

```
iptables -t nat -A CHAINE [CRITÈRES] -j ACTION [OPTIONS]
```

- `-t nat` = table NAT (obligatoire ici)
- `-A` = Append (ajouter à la fin)
- `CHAINE` = `PREROUTING`, `POSTROUTING` ou `OUTPUT`
- `ACTION` = `SNAT`, `DNAT`, `MASQUERADE`, `REDIRECT`

Les 3 chaînes principales de NAT

1. Chaîne `PREROUTING` - Avant le routage

Quand : Paquets qui viennent d'arriver sur la machine
Fonction : Changer la DESTINATION
Typique pour : Port forwarding, redirection

2. Chaîne `POSTROUTING` - Après le routage

Quand : Paquets qui vont sortir de la machine
Fonction : Changer la SOURCE
Typique pour : Masquer l'adresse source, NAT sortant

3. Chaîne `OUTPUT` (nat) - Paquets générés localement

Quand : Paquets créés par la machine elle-même
Fonction : Changer la destination pour le trafic local

Actions NAT principales

A. `SNAT` (Source NAT) - Changer l'adresse source

```
-j SNAT --to-source ADRESSE[:PORT-PORT]
```

Exemples :

```
# Changer la source en IP fixe
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT --to-source
203.0.113.1

# Changer la source avec range de ports
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT --to-source
203.0.113.1:1024-65535

# Dans ton TP
iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j SNAT --to-source
172.16.2.254
```

B. `MASQUERADE` - SNAT avec IP dynamique

```
-j MASQUERADE [--to-ports PORT-PORT]
```

Exemples :

```
# Masquer tout un réseau (typique pour Internet)
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

# Masquer avec ports spécifiques
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j MASQUERADE --to-ports
1024-65535
```

Différence SNAT vs MASQUERADE :

- `SNAT` : IP source fixe (connue à l'avance)

- `MASQUERADE` : IP source = celle de l'interface (dynamique, typique pour connexions Internet)

C. `DNAT` (Destination NAT) - Changer l'adresse destination

```
-j DNAT --to-destination ADRESSE[:PORT]
```

Exemples :

```
# Port forwarding simple
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
192.168.1.100:80

# Rediriger vers un autre port
iptables -t nat -A PREROUTING -p tcp --dport 8080 -j DNAT --to-destination
192.168.1.100:80

# Load balancing entre 2 serveurs
iptables -t nat -A PREROUTING -p tcp --dport 80 -m statistic --mode nth
--every 2 --packet 0 -j DNAT --to-destination 192.168.1.101:80
```

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
192.168.1.102:80
```

D. `REDIRECT` - Rediriger vers un port local

```
-j REDIRECT --to-ports PORT[-PORT]
```

Exemples :

```
# Rediriger le port 80 vers 8080 local
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080

# Rediriger vers un range de ports
```

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports
8080-8090
```

Critères de filtrage (communs avec filter)

Par adresse IP

```
# Source spécifique
iptables -t nat -A POSTROUTING -s 192.168.1.100 -j SNAT --to-source
203.0.113.1

# Destination spécifique
iptables -t nat -A PREROUTING -d 203.0.113.1 -j DNAT --to-destination
192.168.1.100

# Réseau entier
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
```

Par interface

```
# Interface d'entrée (-i)
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT
--to-destination 192.168.1.100

# Interface de sortie (-o)
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

Par protocole et port

```
# TCP
iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to-destination
192.168.1.100:22

# UDP
iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to-destination
192.168.1.100:53
```

```
# Multiple ports
iptables -t nat -A PREROUTING -p tcp -m multiport --dports 80,443 -j DNAT
--to-destination 192.168.1.100
```

Par état de connexion

```
# Seulement les nouvelles connexions
iptables -t nat -A PREROUTING -p tcp --dport 80 -m state --state NEW -j DNAT
--to-destination 192.168.1.100
```

Exemples complets pour ton TP

Exemple 1 : Routeur simple avec Internet

```
# Activer le forwarding IP
echo 1 > /proc/sys/net/ipv4/ip_forward

# NAT pour le réseau local vers Internet
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

# Autoriser le trafic forwardé
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j
ACCEPT
```

Exemple 2 : Serveur avec port forwarding

```
# Forwarding SSH
iptables -t nat -A PREROUTING -d 203.0.113.1 -p tcp --dport 22 -j DNAT
--to-destination 192.168.1.100:22
```

```
# Forwarding HTTP/HTTPS
iptables -t nat -A PREROUTING -d 203.0.113.1 -p tcp --dport 80 -j DNAT
--to-destination 192.168.1.100:80
iptables -t nat -A PREROUTING -d 203.0.113.1 -p tcp --dport 443 -j DNAT
--to-destination 192.168.1.100:443

# NAT de retour (conntrack gère automatiquement normalement)
# Mais parfois besoin de :
iptables -t nat -A POSTROUTING -s 192.168.1.100 -j SNAT --to-source
203.0.113.1
```

Exemple 3 : Dans ton TP02

```
# Sur GW1 : NAT entre S1 et S2
iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -d 172.16.2.0/24 -j SNAT
--to-source 172.16.2.253

# Sur GW2 : NAT vers Internet
iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -o eth2 -j SNAT --to-source
45.45.45.254
iptables -t nat -A POSTROUTING -s 172.16.2.0/24 -o eth2 -j SNAT --to-source
45.45.45.254

# Sur GW2 : DNAT pour le FTP
iptables -t nat -A PREROUTING -d 45.45.45.254 -p tcp --dport 21 -j DNAT
--to-destination 172.16.2.10:21
```

Exemple 4 : Proxy transparent

```
# Rediriger tout le HTTP vers un proxy local
iptables -t nat -A PREROUTING -s 192.168.1.0/24 -p tcp --dport 80 -j REDIRECT
--to-ports 3128

# Rediriger le HTTPS (nécessite proxy SSL)
```

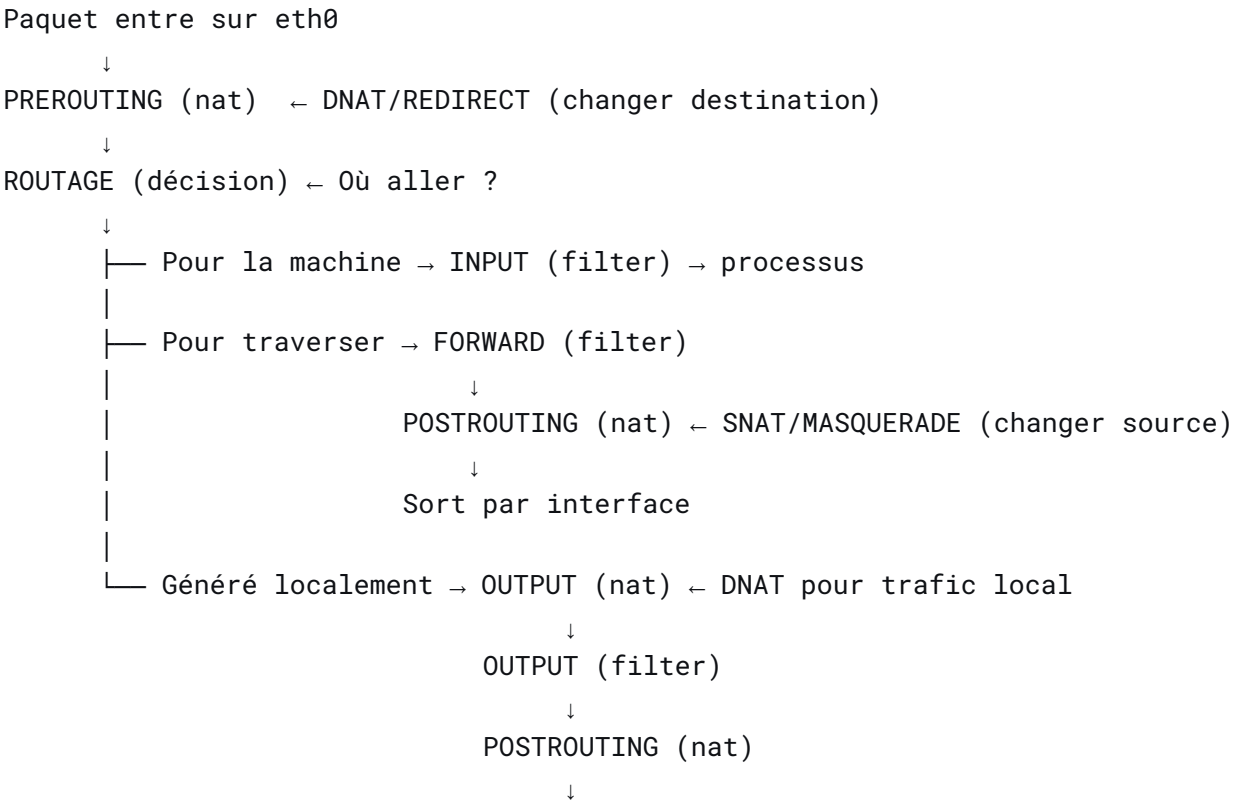
```
iptables -t nat -A PREROUTING -s 192.168.1.0/24 -p tcp --dport 443 -j REDIRECT
--to-ports 3129
```

Exemple 5 : Load balancing

```
# Répartir la charge entre 3 serveurs web
iptables -t nat -A PREROUTING -p tcp --dport 80 -m statistic --mode nth
--every 3 --packet 0 -j DNAT --to-destination 192.168.1.101:80
iptables -t nat -A PREROUTING -p tcp --dport 80 -m statistic --mode nth
--every 3 --packet 1 -j DNAT --to-destination 192.168.1.102:80
```

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
192.168.1.103:80
```

Chemin d'un paquet avec NAT



```
                                Sort par interface
```

Règles importantes avec connection tracking

Le NAT utilise le connection tracking pour gérer les états :

```
# Voir les connexions NAT actives
cat /proc/net/nf_conntrack
# ou
conntrack -L

# Voir le statut d'une connexion spécifique
conntrack -L -s 192.168.1.100

# Effacer les connexions
conntrack -D
```

Exemple de sortie :

```
tcp      6 117 ESTABLISHED src=192.168.1.100 dst=8.8.8.8 sport=54321 dport=53
src=8.8.8.8 dst=203.0.113.1 sport=53 dport=54321 [ASSURED] mark=0 use=1
```

Bonnes pratiques et pièges courants

1. Ordre des règles NAT

```
# Mauvais ordre
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.1.100 -j SNAT --to-source
203.0.113.2
# La règle 2 n'est jamais atteinte !

# Bon ordre (spécifique avant générale)
```

```
iptables -t nat -A POSTROUTING -s 192.168.1.100 -j SNAT --to-source
203.0.113.2
```

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
```

2. NAT et filtrage

```
# IMPORTANT : Les règles filter voient les adresses APRÈS PREROUTING
# Donc pour DNAT :
iptables -t nat -A PREROUTING -d 203.0.113.1 -p tcp --dport 80 -j DNAT
--to-destination 192.168.1.100:80
# Puis en filter :
```

```
iptables -A FORWARD -d 192.168.1.100 -p tcp --dport 80 -j ACCEPT  # Pas
203.0.113.1 !
```

3. FTP avec NAT (cas spécial)

```
# FTP actif nécessite des modules spéciaux
modprobe nf_conntrack_ftp
modprobe nf_nat_ftp

# Puis les règles NAT normales marchent
```

```
iptables -t nat -A PREROUTING -d IP_PUBLIQUE -p tcp --dport 21 -j DNAT
--to-destination IP_FTP:21
```

4. Problèmes courants

```
# Oublier d'activer le forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

# Oublier les règles FORWARD après le NAT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i INTERNE -o EXTERNE -j ACCEPT

# NAT asymétrique (à éviter)
```

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source IP_ETH0
iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source IP_ETH1

# Le mieux : une seule règle MASQUERADE
```

Commandes de débogage

```
# Voir les règles NAT
iptables -t nat -L -v -n

# Voir avec numéros de ligne
iptables -t nat -L --line-numbers

# Voir les compteurs
iptables -t nat -L -v -n -x

# Tracer le chemin d'un paquet
iptables -t nat -L -v -n | grep -A5 -B5 "nom_regle"

# Voir le connection tracking
cat /proc/net/nf_conntrack | grep -i "ton_ip"

# Logguer le NAT
iptables -t nat -A PREROUTING -p tcp --dport 80 -j LOG --log-prefix "DNAT-80:
"

iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
192.168.1.100:80
```

Exemple complet de configuration type

```
#!/bin/bash
# Configuration NAT complète pour un routeur

# Réinitialiser
iptables -t nat -F
```

```
iptables -t nat -X

# Activer le forwarding
sysctl -w net.ipv4.ip_forward=1

# === NAT SORTANT (Internet) ===
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

# === PORT FORWARDING ===
# SSH
iptables -t nat -A PREROUTING -d 203.0.113.1 -p tcp --dport 22 -j DNAT
--to-destination 192.168.1.100:22

# HTTP/HTTPS
iptables -t nat -A PREROUTING -d 203.0.113.1 -p tcp --dport 80 -j DNAT
--to-destination 192.168.1.101:80
iptables -t nat -A PREROUTING -d 203.0.113.1 -p tcp --dport 443 -j DNAT
--to-destination 192.168.1.101:443

# === RÈGLES FILTER CORRESPONDANTES ===
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -d 192.168.1.100 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -d 192.168.1.101 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -d 192.168.1.101 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
iptables -P FORWARD DROP

# === SAUVEGARDE ===

iptables-save > /etc/iptables/rules.v4
```

Ce guide couvre l'essentiel de `iptables -t nat`. La clé est de comprendre que :

- `PREROUTING` = avant routage = changement de DESTINATION
- `POSTROUTING` = après routage = changement de SOURCE
- Le connection tracking gère automatiquement les flux inverses
- Les règles `filter` voient les adresses APRÈS le `PREROUTING` NAT