Firewall

iptables

Syntaxe

Paramètres

-L	Lister les rêgles
-n	Affichage numérique plutôt que substitution
-t nat	Table de NAT
-t filter	Table de filtrage (par défaut)
-F	Vide la table (flush)
-X	Efface une chaîne

Exemples

```
sudo iptables -t nat -L                 # liste les règles de NAT
sudo iptables –t nat –S                # liste les règles de NAT
sudo iptables –t nat –L --line-numbers # liste avec des numéros de ligne
sudo iptables –t nat –D PREROUTING 101 # pour supprimer la ligne 101
sudo iptables -t nat -F                 # supprime les règles de NAT
sudo service iptables save/restore     # sauvegarde/restore dans fichier
/etc/sysconfig/iptables pour prise en compte au redémarrage du service
```

Un utilisateur non root peut obtenir l'erreur « commande introuvable »

Translation d'adresse

IP Forwarding

- Modification temporaire

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Modification persistante avec le fichier /etc/sysctl.conf

```
net.ipv4.ip_forward=1
```

- Prise en compte

```
sudo sysctl -p
```

- Vérification

```
cat /proc/sys/net/ipv4/ip_forward
```

NAT (Network Address Translation)

```
# redirection du port TCP 80 en entrée sur eth0 vers le même port sur 10.10.0.213
sudo iptables -t nat -A PREROUTING  -j DNAT       -i eth0  -p tcp --dport 80 --to-destination 10.10.0.213  # DNAT on substitue à l'adresse destination une adresse du réseau local privé
sudo iptables -t nat -A POSTROUTING -j MASQUERADE -o eth1  -p tcp --dport 80 -d 10.10.0.213  # SNAT on substitue l'adresse source par celle de l'interface
```

NAT / PAT (Port Address Translation)

```
# redirection du port TCP 10010 en entrée sur wlan0 vers le port 22 de 192.168.1.10
sudo iptables -t nat -A PREROUTING  -j DNAT       -i wlan0 -p tcp --dport 10010  --to-destination 192.168.1.10:22
sudo iptables -t nat -A POSTROUTING -j MASQUERADE          -p tcp --dport 22 -d 192.168.1.10
```

Ne pas oublier d'activer l'IP forwarding

From:
https://wiki.iot-acs.fr/ - **Wiki**

Permanent link:
https://wiki.iot-acs.fr/doku.php?id=all:bibles:linux:reseau:firewall

Last update: **2025/02/19 13:53**