Iptables

Iptables est un utilitaire permettant de maniper le firewall natif de linux (netfilter).

Ce guide récapitule les commandes essentielles pour administrer un pare-feu Linux.

Pour changer les policies par défaut on peut utiliser les commandes:

```
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
```

Tout trafic ne s'appliquant pas à une règle présente suivra par défaut la policy.

1. Consultation des règles

Commande	Description
`iptables -L`	Liste les règles de la table **filter** (par défaut).
`iptables -L -n -v`	Liste détaillée (octets, paquets) sans résolution DNS.
`iptables -L --line-numbers`	Affiche les numéros de ligne (utile pour supprimer).
`iptables -S`	Affiche les règles sous forme de commandes brutes.
`iptables -t nat -L -n -v`	Liste les règles de la table **NAT** (redirections).

---

2. Gestion des règles (Ajout/Suppression)

> ⚠ **Note :** L'ordre des règles est crucial, la lecture se fait de haut en bas.

- **Ajouter à la fin (`-A`)** :
  `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
- **Insérer au début ou à une ligne précise (`-I`)** :
  `iptables -I INPUT 1 -i lo -j ACCEPT`
- **Supprimer par numéro de ligne (`-D`)** :
  `iptables -D INPUT 3`

- **Vider toutes les règles d'une table (`-F`)** :
  `iptables -F`

---

3. Configuration du NAT (Table NAT)

Le NAT s'applique toujours avec l'option `-t nat`.

Partage de connexion (Masquerade / SNAT)

Permet aux hôtes internes (LAN) d'accéder à Internet via l'IP du pare-feu.

```
iptables -t nat -A POSTROUTING -o [interface_WAN] -j MASQUERADE
```

Revision #2
Created 5 March 2026 11:04:42 by Bibi
Updated 5 March 2026 14:07:07 by Bibi