# 5. Sécurisation avec un Pare-feu (iptables)  
  
## Objectif  
Configurer un pare-feu pour restreindre les connexions réseau non autorisées sur le Raspberry Pi.  
  
### Commandes pour la configuration du pare-feu :  
sudo iptables -F  
sudo iptables -P INPUT DROP  
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT # SSH  
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # HTTP  
  
### Sauvegarder les règles iptables :  
sudo sh -c 'iptables-save > /etc/iptables/rules.v4'  
  
### Commentaires :  
- Le pare-feu est essentiel pour restreindre les connexions non autorisées.  
- Il protège à la fois les accès SSH et HTTP.  
  
\*\*Importance\*\* : 5/5