# 7. Surveillance et Monitoring avec `Fail2Ban` et `arpwatch`  
  
## Objectif  
Surveiller les tentatives d'accès non autorisées et bannir automatiquement les adresses IP suspectes. Surveiller les adresses MAC connectées au réseau.  
  
### Installation de `Fail2Ban` :  
sudo apt install fail2ban -y  
  
### Configuration de `Fail2Ban` pour SSH et HTTP :  
Ajoutez les lignes suivantes à `/etc/fail2ban/jail.local` :  
[sshd]  
enabled = true  
port = 22  
filter = sshd  
logpath = /var/log/auth.log  
maxretry = 3  
bantime = 600  
  
[http-auth]  
enabled = true  
port = 80  
logpath = /var/log/apache2/access.log  
maxretry = 3  
bantime = 600  
  
Redémarrez Fail2Ban :  
sudo systemctl restart fail2ban  
  
### Installation et configuration de `arpwatch` :  
sudo apt install arpwatch -y  
sudo systemctl enable arpwatch  
sudo systemctl start arpwatch  
  
### Commentaires :  
- Surveille les connexions suspectes et bannit les IP/MAC non autorisées.  
  
\*\*Importance\*\* : 5/5