🔐 Configuration SSH Sécurisée

📃 Tldr

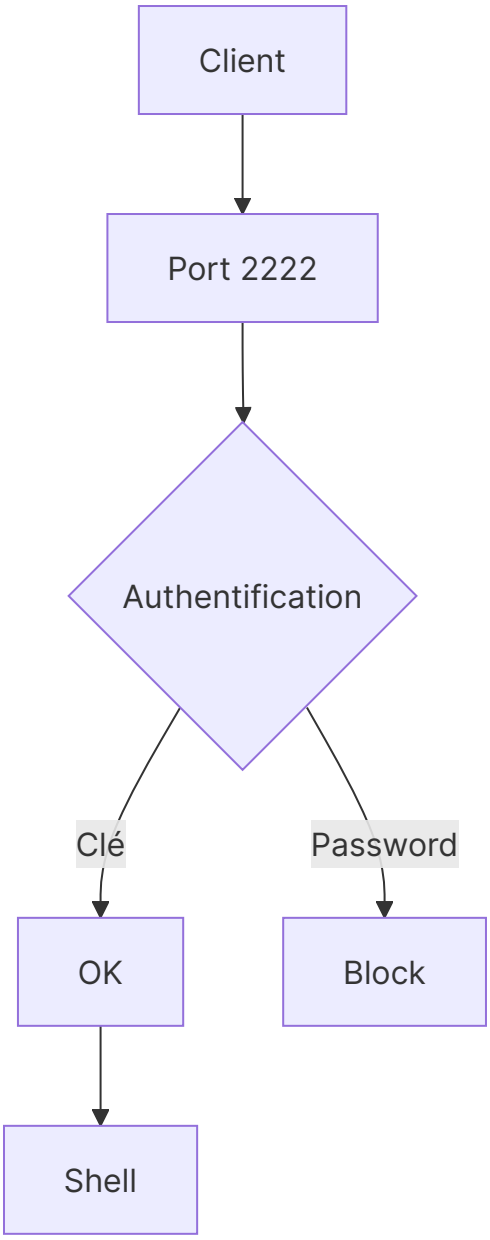
En Bref :
Configuration optimale d'un serveur SSH avec :

- Authentification par clés uniquement
- Chiffrement modernes
- Protection contre les attaques brute-force
- Journalisation renforcée

🌐 Contexte

🖊 Pourquoi sécuriser SSH ?

SSH est la porte d'entrée principale des serveurs - 75% des attaques ciblent SSH (Source: CrowdStrike 2023)



2. Fichier `sshd_config`

```
# /etc/ssh/sshd_config
Port 2222  # ← Changer port par défaut
PermitRootLogin no
PasswordAuthentication no
KexAlgorithms curve25519-sha256@libssh.org
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com
MACs hmac-sha2-512-etm@openssh.com
ClientAliveInterval 300
MaxAuthTries 2
AllowUsers deployer admin
```

> ⚠️ **Attention aux Legacy Clients**
>
> Les algorithmes choisis ne sont pas supportés par les vieilles versions de OpenSSH (<7.4)

3. Outils Complémentaires

- Fail2Ban → Blocage IP après échecs
- Authentification Multi-Facteur
- `ssh-audit` → Vérification configuration

🔍 Vérifications

```
# Test configuration
sshd -t

# Audit sécurité
nmap -sV --script ssh2-enum-algos -p 2222 127.0.0.1

# Monitoring connexions
journalctl -u sshd --since "1 hour ago" -f
```

🛡️ Best Practices

- [x] Rotation clés tous les 6 mois
- [x] Sauvegarde sécurisée des clés
- [x] Mise à jour mensuelle d'OpenSSH

📚 Ressources

- SSH Hardening Guide - Mozilla
- CIS-Benchmark-SSH → Standards de sécurité
- `man sshd_config` → Documentation officielle