






Hardening SSH - Best Practices

 Tldr

En 30 secondes :

Couche de sécurité en 5 étapes :

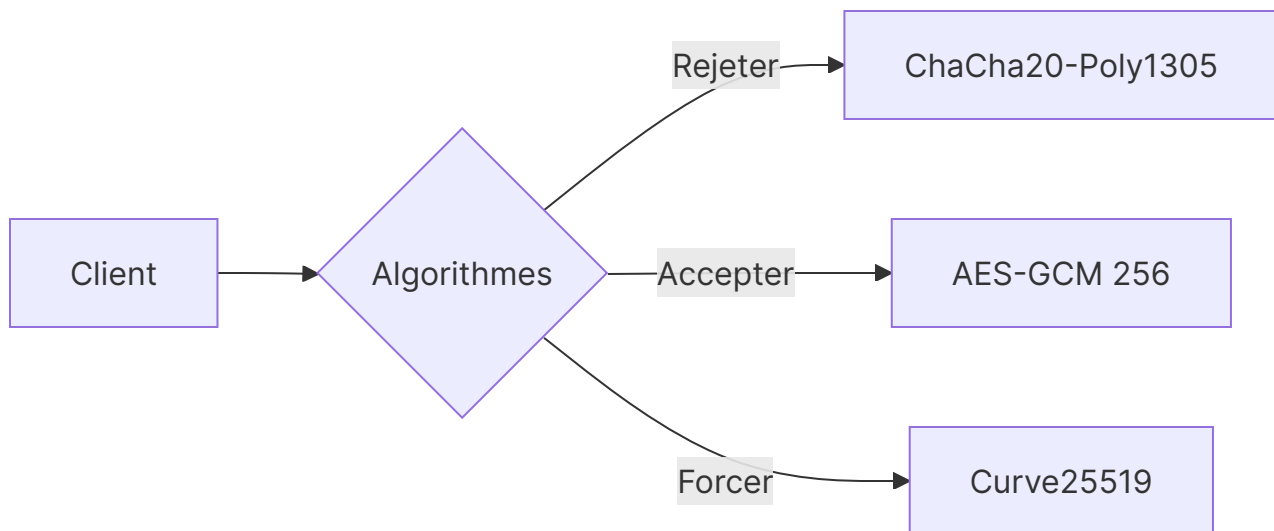
1.  Authentification sans mot de passe
2.  Chiffrement modernes uniquement
3.  Monitoring actif
4.  Restriction réseau
5.  Plan de réponse aux incidents

Configuration de Base

Fichier `sshd_config` Renforcé

```
# /etc/ssh/sshd_config
Port 2222
ListenAddress 192.168.1.100
PermitRootLogin prohibit-password
MaxAuthTries 3
LoginGraceTime 1m
ClientAliveInterval 300
X11Forwarding no
AllowTcpForwarding no
PermitTunnel no
```

Algorithmes Sécurisés (Post-Terrapin CVE-2023-48795)



Authentication

Méthodes Hiérarchisées

```
AuthenticationMethods publickey,keyboard-interactive
PasswordAuthentication no
PermitEmptyPasswords no
KerberosAuthentication no
```

Protection Clés Privées

```
# Verrouillage HSM
pkcs11-tool --login --pin 123456 --keypairgen --key-type EC:secp521r1 --
usage-sign --label "SSH_Key"
```

Restriction d'Accès

Pare-feu (UFW)

```
ufw allow proto tcp from 192.168.1.0/24 to any port 2222
ufw limit 2222/tcp comment 'SSH Brute-Force Protection'
```

Filtrage par Clés

```
# ~/.ssh/authorized_keys
from="192.168.1.*,2001:db8::/32" ssh-ed25519 AAAAC3Nz... user@host
```

Monitoring Avancé

Journalisation Renforcée

```
# Audit des connexions
ausearch -m AVC,USER_AUTH -ts today | aureport

# Détection d'intrusion
grep 'Failed password' /var/log/auth.log | awk '{print $(NF-3)}' | sort |
uniq -c
```


Outils Recommandés

- [Fail2Ban-Config](#) → Blocage automatique
- `ssh-audit` → Vérification config
- [Lynis-Hardening](#) → Audit système

Réponse aux Incidents

Checklist d'Urgence

1. Révoquer les clés compromises
2. Analyser les logs avec `journalctl -u sshd -p warning`
3. Mettre à jour OpenSSH
4. Régénérer les clés hôtes (`ssh-keygen -R`)

 **Attaque Détectée - Procédure**

1. Isoler le serveur
2. Capturer la mémoire (LiME)
3. Préserver les logs
4. Notifier le CERT

Benchmark Sécurité

Contrôle	CIS v8	NIST 800-53
Désactiver root	5.3.4	AC-6(2)
Limite de tentatives	5.3.3	AC-7
Chiffrement fort	5.2.11	SC-13

Ressources

- [SSH-CheatSheet](#) → Commandes utiles
- [Mozilla SSH Guidelines](#) → Référence
- `sshd -T` → Vérifier la config active