Top 19 OpenSSH Server Best Security Practices

- Use TCP wrapper
- Disable root user login
- Use SSH public key based login
- Disable Empty Passwords
- Disable password based login
- Use strong passwords and passphrase for ssh users/keys
- Limit Users' ssh acces
- Change SSH Port and limit IP binding
- Firewall SSH TCP port # 22
- Rate-limit incoming traffic at TCP port # 22
- Thwart SSH crackers/ brute force attacks
- Use port knocking
- Configure idle log out timeout interval
- Disable .rhosts files
- Enable a warning banner for ssh users
- Patch OpenSSH and operating systems
- Disable host-based authentication
- Chroot OpenSSH (Lock down users to their home directories)
- Disable OpenSSH server on client computer

www.kleinhirn.eu