

# configuración

comprobar si hay restricciones en IPTABLES (/etc/sysconfig/iptables)

se puede limitar el uso que se puede hacer de SSH en el siguiente fichero: /etc/ssh/sshd\_config

- *Protocol 2*
- *AllowUsers* solo los usuarios que se pueden conectar vía SSH
- *DenyUsers* a los usuarios que NO se pueden conectar vía SSH
- *PermitRootLogin* {yes|no|forced-commands-only}
- *IgnoreRhosts* {yes|no} evita la lectura de los ficheros ~/.rhosts y ~/.shosts
- *PermitRootLogin* {yes|no}
- *Banner* /etc/fichero
- *Port 22*
- *ListenAddress* 192.168.1.1
- *PermitEmptyPasswords* {yes|no}
- *LogLevel* INFO
- *AllowGroups*
- *DenyGroups*
  
- [Fuente](#)
- [chroot con SSH](#)
- [Port knocking](#)
- [Multiple-port knocking Netfilter/IPTables only implementation](#)

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:ssh:config?rev=1455122504>

Last update: **10/02/2016 08:41**

