configuración ssh server (/etc/ssh/sshd_config)

- 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`
- Opciones destacadas:
  - **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
- curso lpic2: ssh
- Fuente
- chroot con SSH
- Port knocking
- Multiple-port knocking Netfilter/IPtables only implementation

restricciones

agent forwarding

/etc/ssh/sshd_config

```
Match User that-restricted-guy
  AllowTcpForwarding yes
  X11Forwarding no
  AllowAgentForwarding no
  ForceCommand /bin/false
```

/etc/ssh/sshd_config

```
Match User even-more-restricted-guy
  PermitOpen 127.0.0.1:12345
  X11Forwarding no
  AllowAgentForwarding no
  ForceCommand /bin/false
```

- Solo permite forward de conexiones a 127.0.0.1
- para evitar la desconexión y mantener la conexión de reenvio abierta, deberá usar **-N** en su conexión **ssh**:

```
ssh -L 12345:127.0.0.1:12345 -N even-more-restricted-guy@insert-your-machine
```

/etc/ssh/sshd_config

```
Match Group                     nicepeople
    PubkeyAuthentication        yes
    PasswordAuthentication      yes
    PermitEmptyPasswords        no
    GatewayPorts                no
    ChrootDirectory             /opt/dummy_location/%u
    ForceCommand                internal-sftp
    AllowTcpForwarding          yes
        PermitOpen              192.168.0.8:22
        PermitOpen              192.168.0.5:8080
    # Or leave out the PermitOpen to allow forwarding to anywhere.
    HostbasedAuthentication     no
    RhostsRSAAuthentication     no
    AllowAgentForwarding        no
    Banner                      none
```

Restringir acceso a la red:

```
/sbin/iptables -I OUTPUT -m owner --gid-owner 500 -j REJECT
/sbin/iptables -I OUTPUT -m owner --gid-owner 500 -m tcp -p tcp -d 192.168.0.0/24 -
j ACCEPT
```

/via: https://unix.stackexchange.com/questions/14312/how-to-restrict-an-ssh-user-to-only-allow-ssh-tunneling
/more: https://superuser.com/questions/229743/howto-disable-ssh-local-port-forwarding