

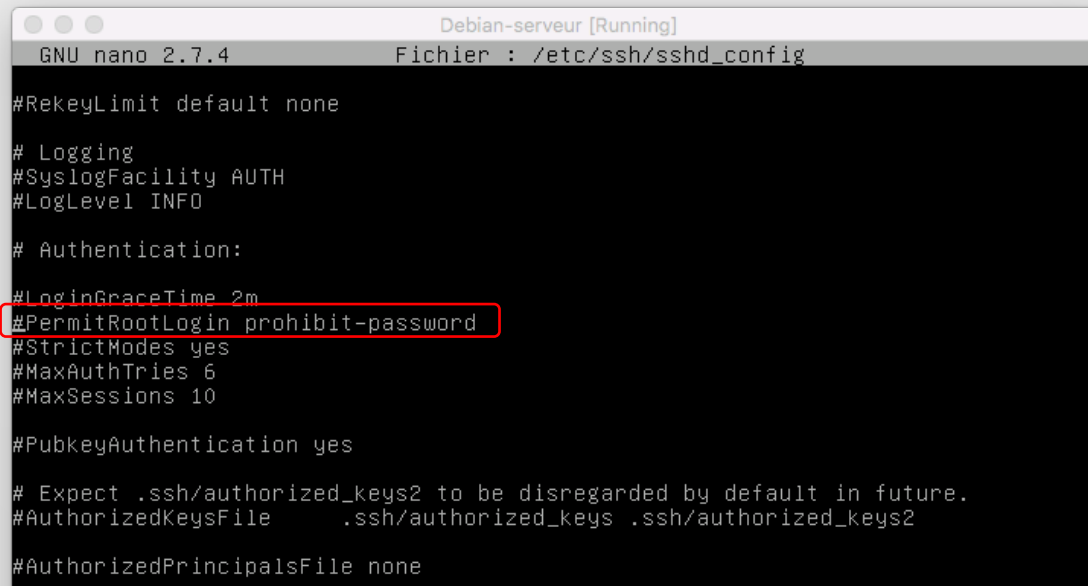
Sécurisé la connexion à distance à son serveur Debian

SÉCURISER SON SERVEUR DEBIAN

- Désactiver l'accès root en SSH
- Modifier le port de connexion SSH
- Restreindre l'accès à des IP autorisés en SSH

L'ACCÈS ROOT EN SSH EST INTERDITE

- Par sécurité, depuis la version Debian 8 Jessie, l'accès en root par SSH est interdite.
- Dans le fichier `/etc/ssh/sshd_config` l'option **PermitRootLogin** est passée de "yes" (autorisée) à "prohibit-password" (interdire le mot de passe).



```
Debian-serveur [Running]
GNU nano 2.7.4      Fichier : /etc/ssh/sshd_config

#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none
```

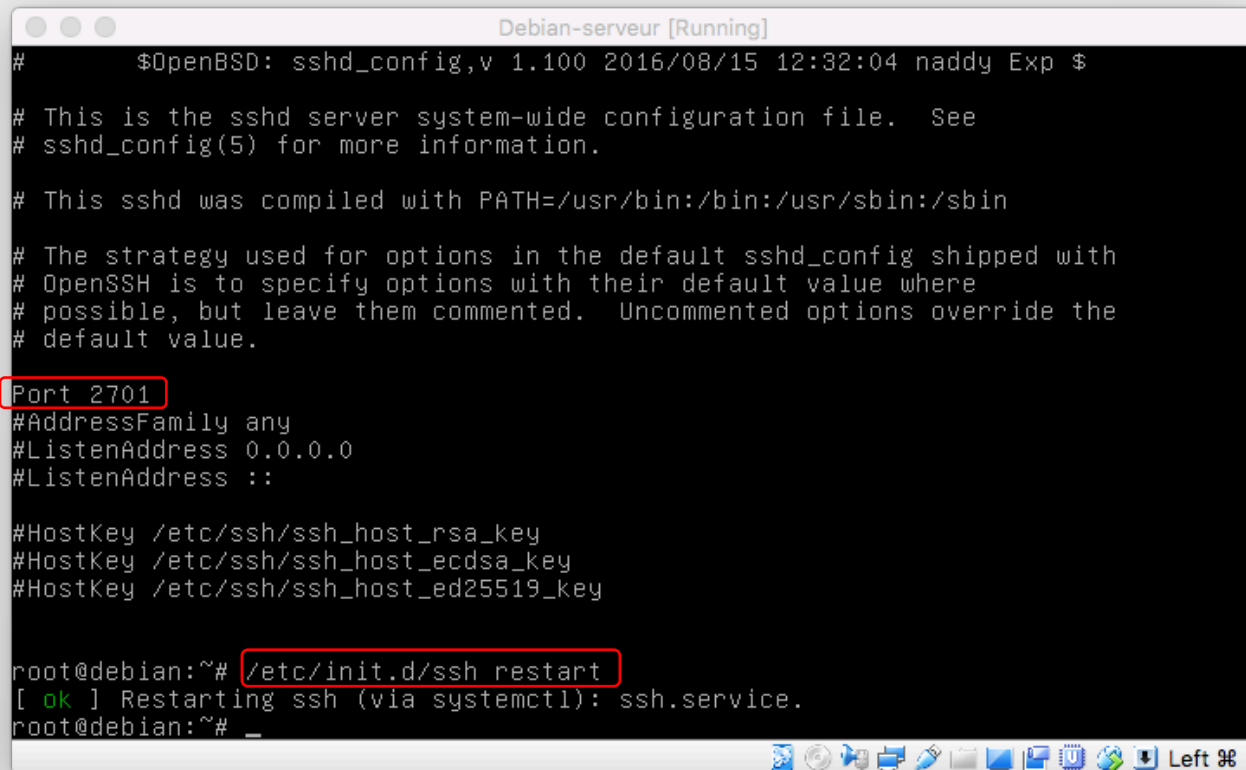
/!\ Par sécurité, il n'est pas conseillé de laisser un accès root par SSH. Il faut se connecter avec un utilisateur puis ensuite passer en root avec un "su root".

CHANGER LE PORT DE CONNEXION

- Le port par défaut est 22.
 - Pour plus de sécurité on change ce numéro de port (vous êtes seule à connaître le port du serveur).
- On tape: `nano /etc/ssh/sshd_config`

On modifie le
port 22 par
défaut. →
On sauvegarde
la modification.

On redémarre
le service ssh →



```
Debian-serveur [Running]
#      $OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

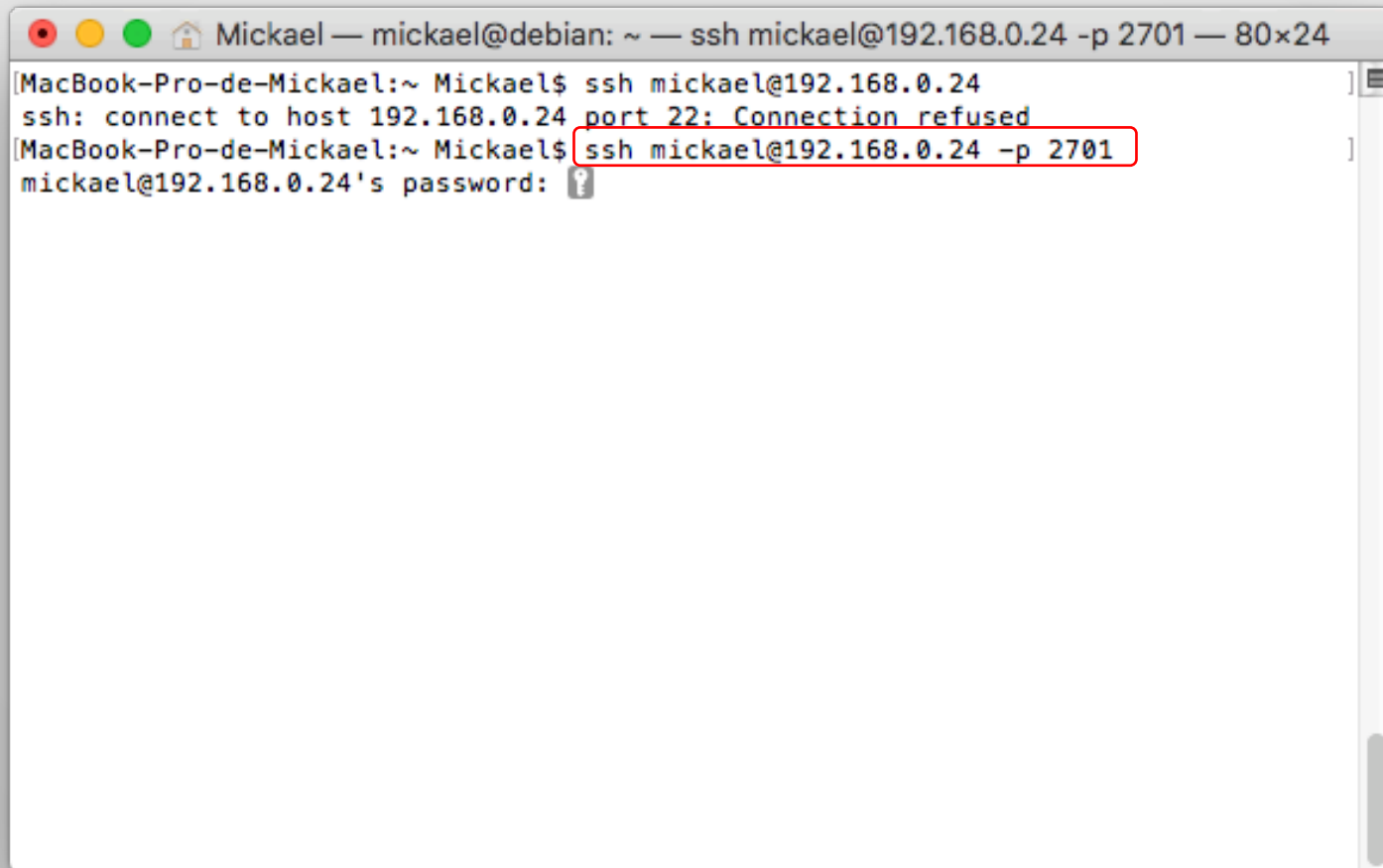
#Port 2701
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

root@debian:~# /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl): ssh.service.
root@debian:~# _
```

SE CONNECTER EN SSH AVEC OPTION -P

- On se connecte a son serveur en précisant le port indiqué.
 - ssh [username@192.168.0.X](#) -p 2701

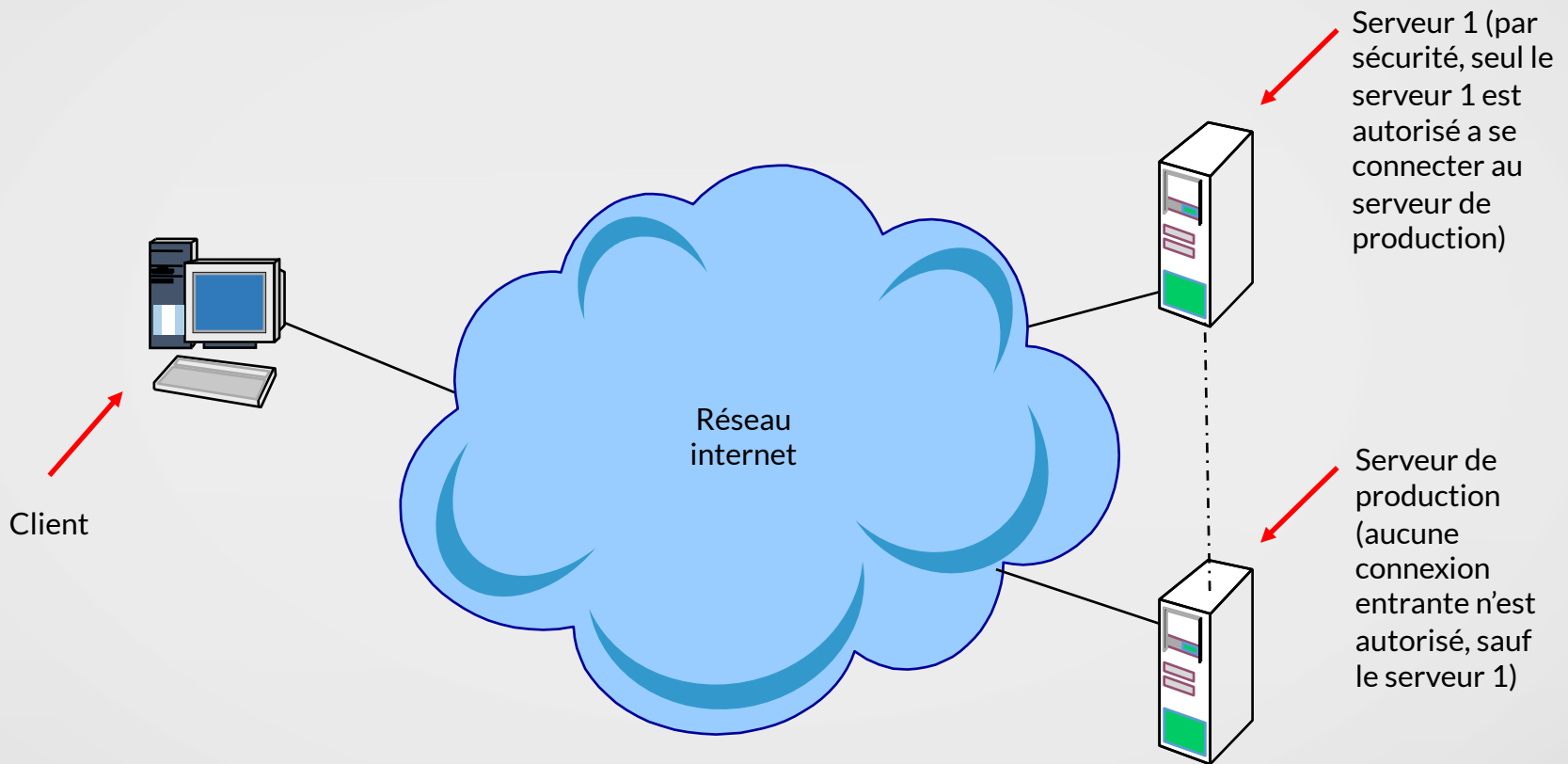


```
Mickael — mickael@debian: ~ — ssh mickael@192.168.0.24 -p 2701 — 80x24
[MacBook-Pro-de-Mickael:~ Mickael$ ssh mickael@192.168.0.24
ssh: connect to host 192.168.0.24 port 22: Connection refused
[MacBook-Pro-de-Mickael:~ Mickael$ ssh mickael@192.168.0.24 -p 2701
mickael@192.168.0.24's password: ]
```

RESTRICTION D'IP SUR SERVEUR

- Pour plus de sécurité

- Le client se connecte au **serveur 1** puis accède ensuite au **serveur de production**.



RESTREINDRE L'ACCES SSH PAR USERNAME / IP

- On peut restreindre l'accès par SSH par nom d'utilisateur et / ou adresse ip avec **AllowUsers**.

On autorise les utilisateurs à se connecter (séparés par un espace).

Tous les utilisateurs avec une ip commençant par 192.168.0.

On redémarre le service **ssh**

```
Debian-serveur [Running]
# $OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Authorisation connexion
AllowUsers jean fabrice arnaud
AllowUsers mickael@192.168.0.*
AllowUsers *@192.168.0.*

Port 2701
#AddressFamily any
#ListenAddress 0.0.0.0

root@debian:~# /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl): ssh.service.
root@debian:~# _
```

L'utilisateur mickael avec une ip commençant par 192.168.0. est autorisé à se connecter.