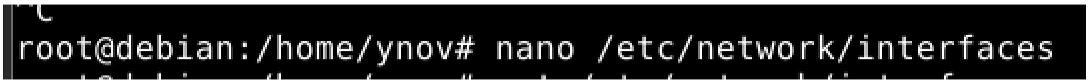
Linux TP

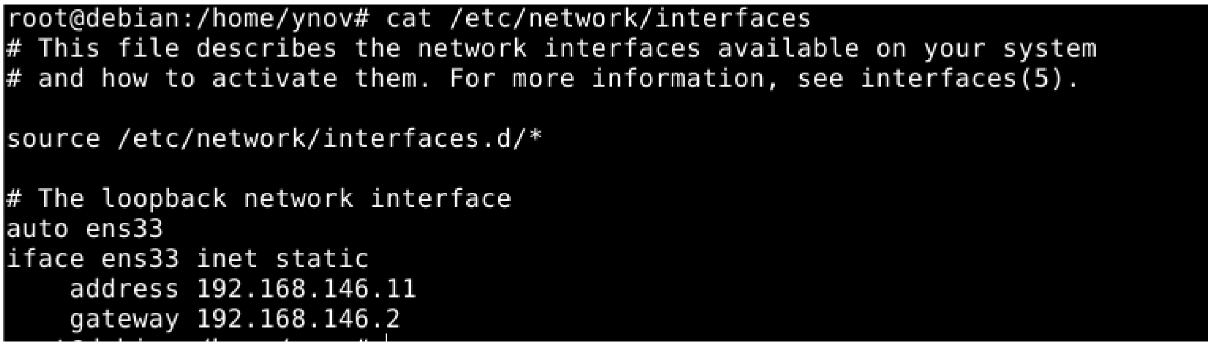
- Configurer IP static :



```
root@debian:/home/ynov# nano /etc/network/interfaces
```

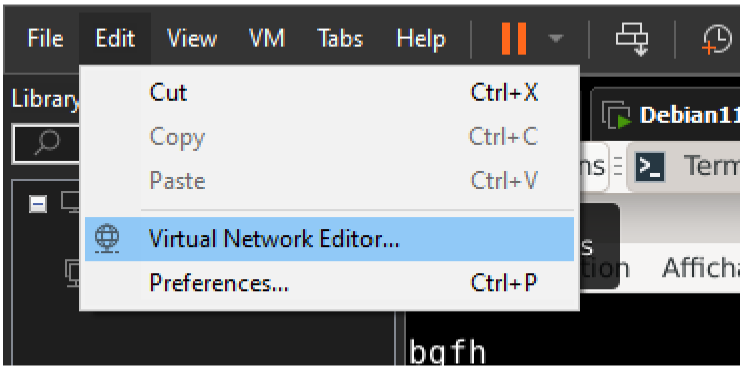
modification du fichier interfaces

Création d’une adresse ip

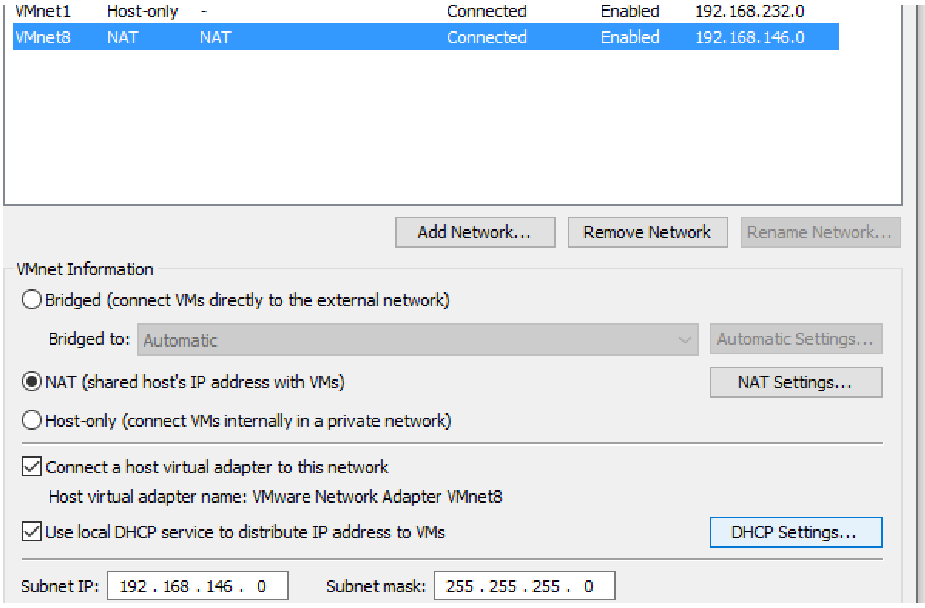


```
root@debian:/home/ynov# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto ens33
iface ens33 inet static
    address 192.168.146.11
    gateway 192.168.146.2
```

Pour vérifier la gateway de vmware



Dans DHCP Settings



```
VMnet1   Host-only   -      Connected   Enabled   192.168.232.0
VMnet8   NAT         NAT    Connected   Enabled   192.168.146.0
```

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

● NAT (shared host's IP address with VMs)

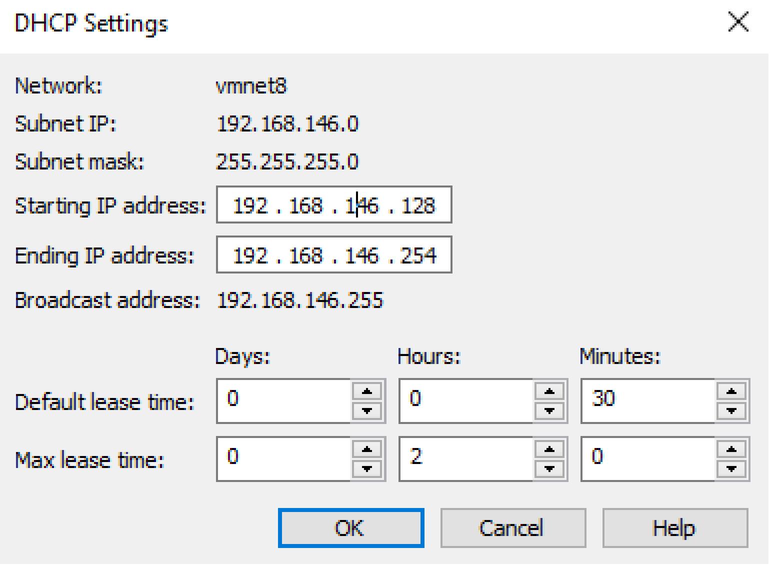
○ Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet8

☑ Use local DHCP service to distribute IP address to VMs

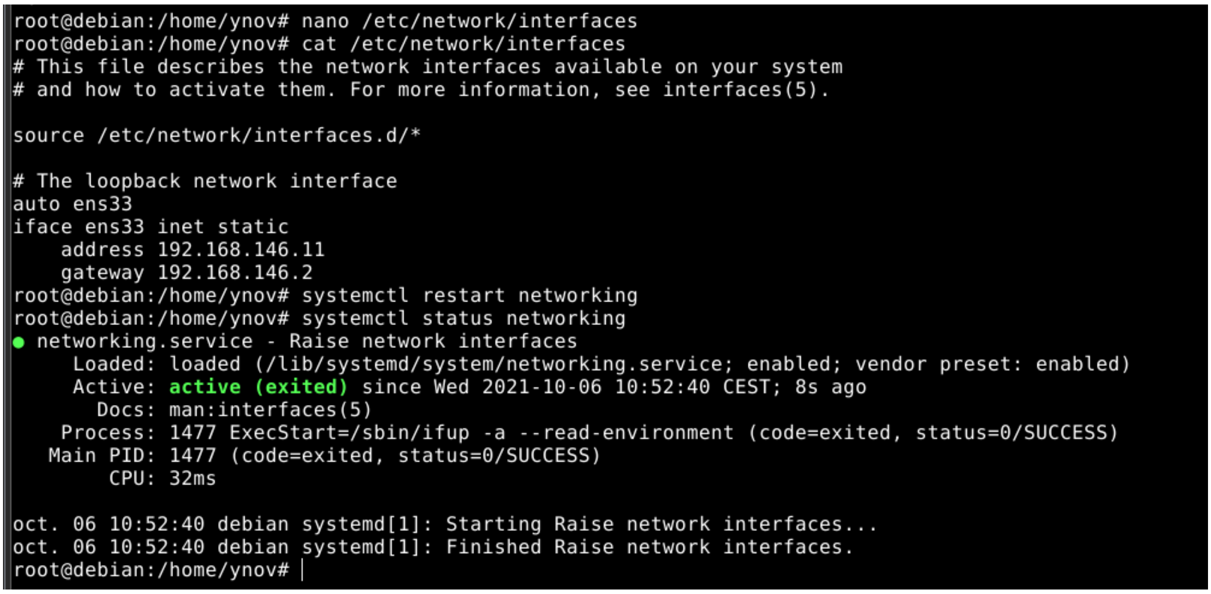
Subnet IP: 192 . 168 . 146 . 0 Subnet mask: 255 . 255 . 255 . 0



Network: vmnet8
Subnet IP: 192.168.146.0
Subnet mask: 255.255.255.0
Starting IP address: 192 . 168 . 146 . 128
Ending IP address: 192 . 168 . 146 . 254
Broadcast address: 192.168.146.255

	Days:	Hours:	Minutes:
Default lease time:	0	0	30
Max lease time:	0	2	0

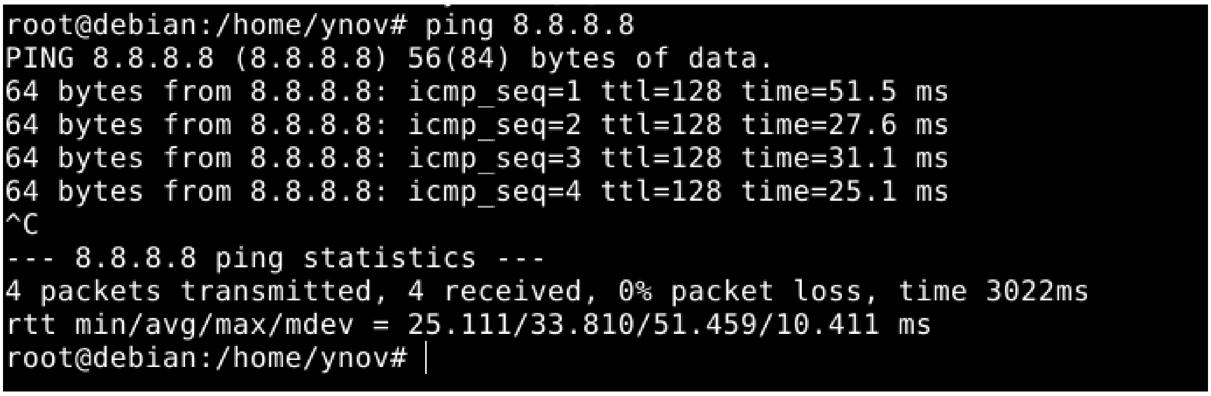
Restart puis on vérifie le status



```
root@debian:/home/ynov# nano /etc/network/interfaces
root@debian:/home/ynov# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto ens33
iface ens33 inet static
    address 192.168.146.11
    gateway 192.168.146.2
root@debian:/home/ynov# systemctl restart networking
root@debian:/home/ynov# systemctl status networking
● networking.service - Raise network interfaces
     Loaded: loaded (/lib/systemd/system/networking.service; enabled; vendor preset: enabled)
     Active: active (exited) since Wed 2021-10-06 10:52:40 CEST; 8s ago
       Docs: man:interfaces(5)
    Process: 1477 ExecStart=/sbin/ifup -a --read-environment (code=exited, status=0/SUCCESS)
   Main PID: 1477 (code=exited, status=0/SUCCESS)
        CPU: 32ms

oct. 06 10:52:40 debian systemd[1]: Starting Raise network interfaces...
oct. 06 10:52:40 debian systemd[1]: Finished Raise network interfaces.
root@debian:/home/ynov#
```

Si l'ancienne adresse ip est resté : systemctl reboot

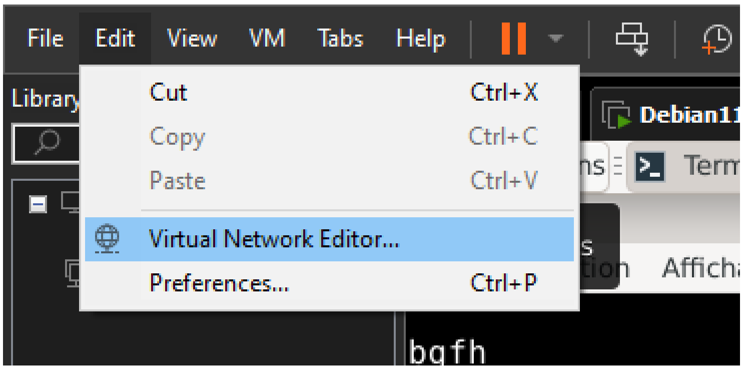
On ping google.com pour vérifier si cela fonctionne



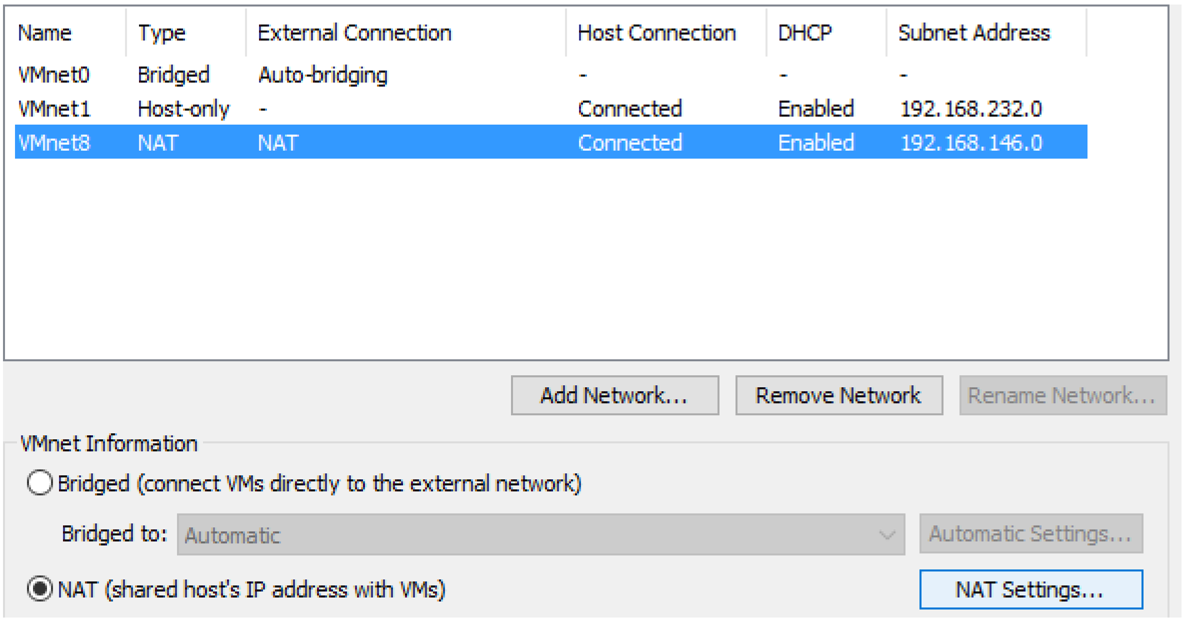
```
root@debian:/home/ynov# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=51.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=27.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=31.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=25.1 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3022ms
rtt min/avg/max/mdev = 25.111/33.810/51.459/10.411 ms
root@debian:/home/ynov#
```

- Contacter un PC distant avec un FQDN

On créer un port pour la machine qui reçoit :



Dans Nat Settings



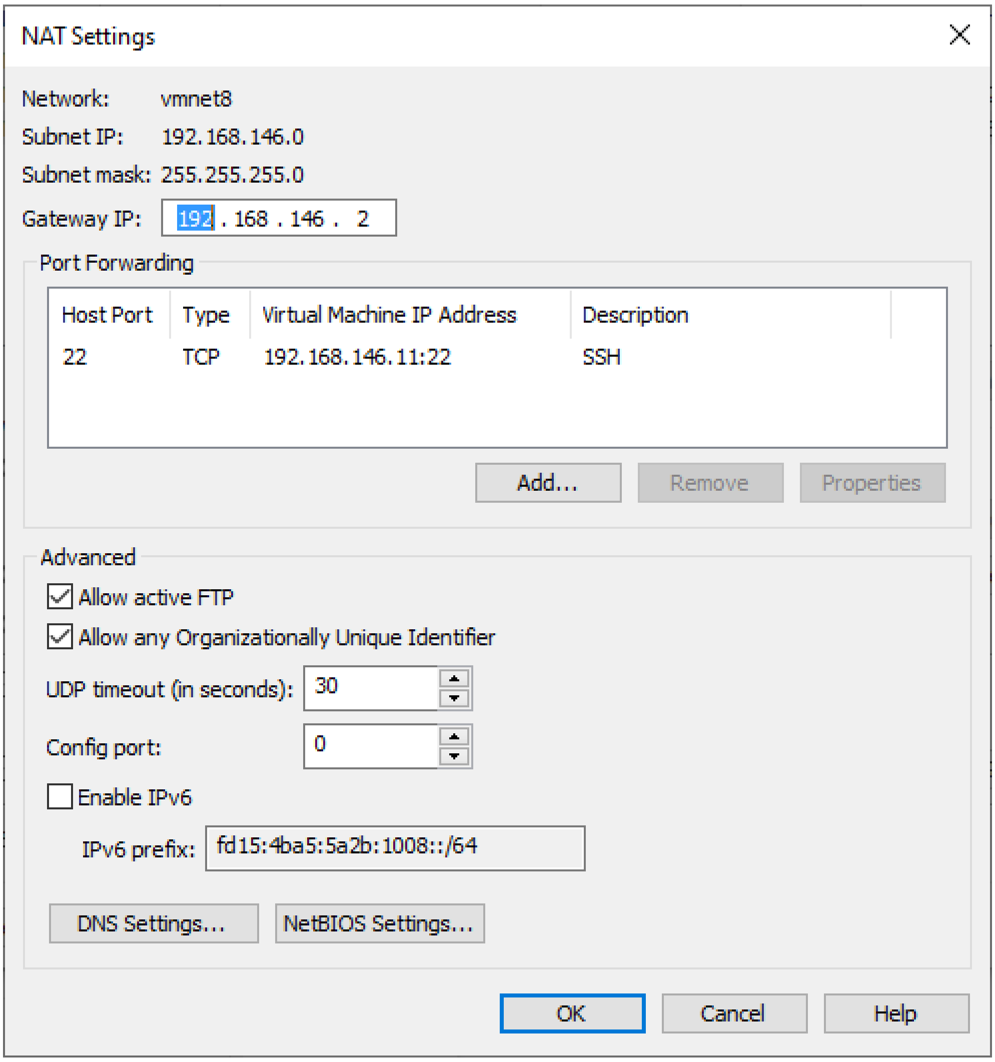
Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.232.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.146.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

● NAT (shared host's IP address with VMs)



NAT Settings

Network: vmnet8

Subnet IP: 192.168.146.0

Subnet mask: 255.255.255.0

Gateway IP: 192 . 168 . 146 . 2

Port Forwarding

Host Port	Type	Virtual Machine IP Address	Description
22	TCP	192.168.146.11:22	SSH

Advanced

☑ Allow active FTP

☑ Allow any Organizationally Unique Identifier

UDP timeout (in seconds): 30

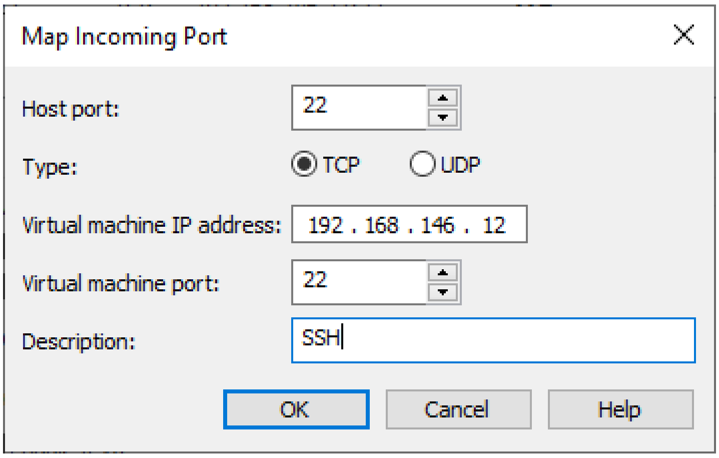
Config port: 0

□ Enable IPv6

IPv6 prefix: fd15:4ba5:5a2b:1008::/64

*

On add un nouveau port



Map Incoming Port

Host port: 22

Type: ● TCP ○ UDP

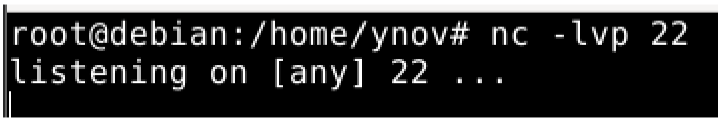
Virtual machine IP address: 192 . 168 . 146 . 12

Virtual machine port: 22

Description: SSH

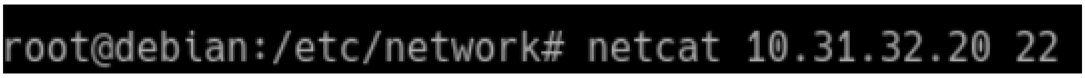
On applique

Pour ouvrir le port sur la vm qui reçoit :



```
root@debian:/home/ynov# nc -lvp 22
listening on [any] 22 ...
```

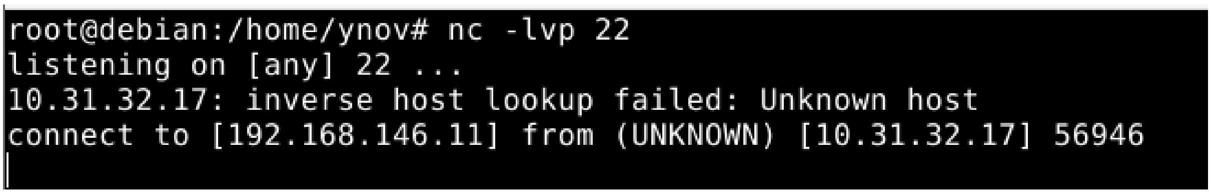
Pour accéder au port sur l’autre vm :



```
root@debian:/etc/network# netcat 10.31.32.20 22
```

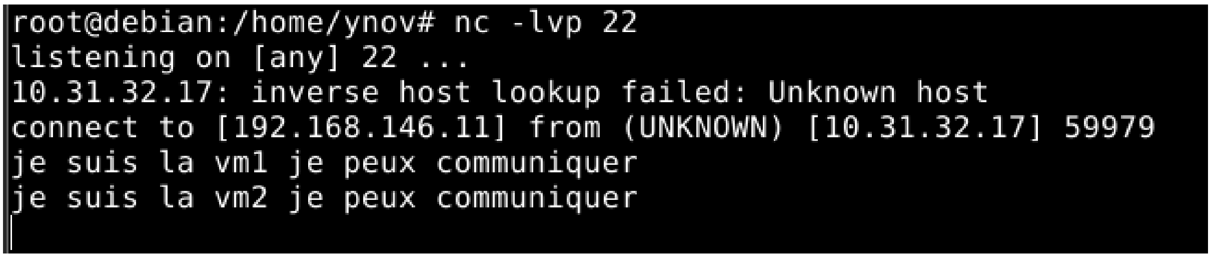
(Addresse ip du pc + port)

La seconde vm s’est connecter :



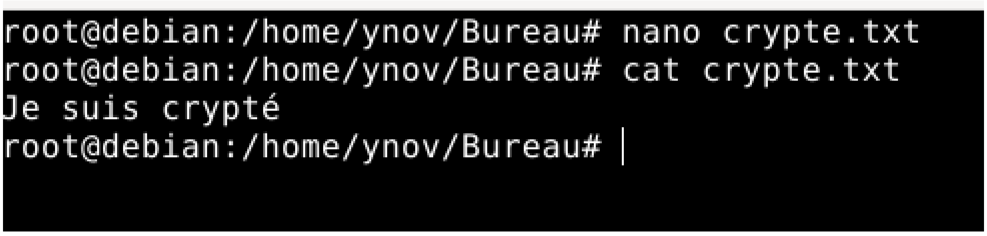
```
root@debian:/home/ynov# nc -lvp 22
listening on [any] 22 ...
10.31.32.17: inverse host lookup failed: Unknown host
connect to [192.168.146.11] from (UNKNOWN) [10.31.32.17] 56946
```

Les 2 vm peuvent communiquer :



```
root@debian:/home/ynov# nc -lvp 22
listening on [any] 22 ...
10.31.32.17: inverse host lookup failed: Unknown host
connect to [192.168.146.11] from (UNKNOWN) [10.31.32.17] 59979
je suis la vm1 je peux communiquer
je suis la vm2 je peux communiquer
```

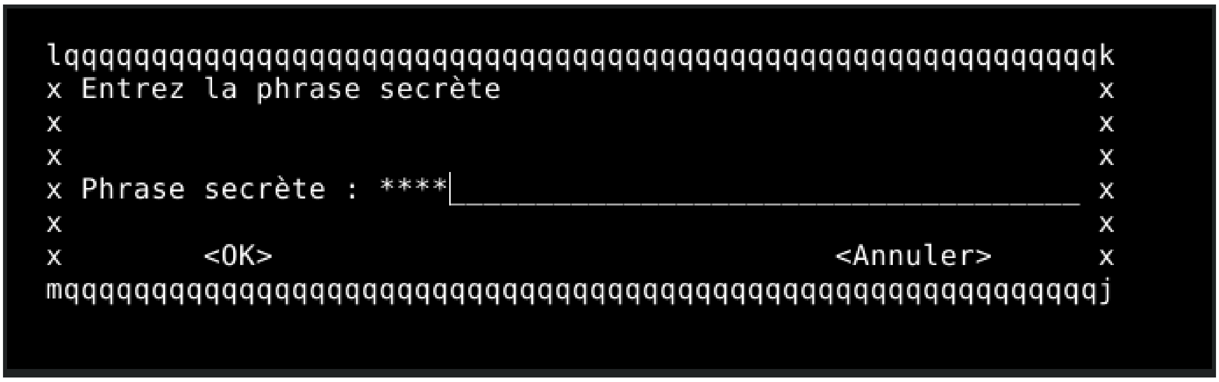
- Chiffrer fichier



```
root@debian:/home/ynov/Bureau# nano crypte.txt
root@debian:/home/ynov/Bureau# cat crypte.txt
Je suis crypté
root@debian:/home/ynov/Bureau# 
```

Utilisation de gnupg :

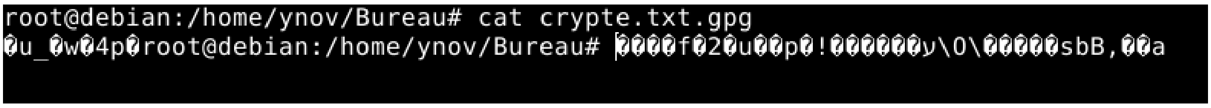
Avec la commande gpg --symmetric fichier.txt



```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Entrez la phrase secrète                                   x
x                                                            x
x                                                            x
x Phrase secrète : ****____________________________________ x
x                                                            x
x        <OK>                                  <Annuler>     x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

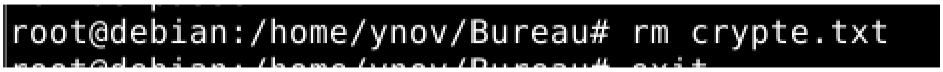
On crée un mot de passe pour avoir accès : ynov

Le fichier crypté devient donc :



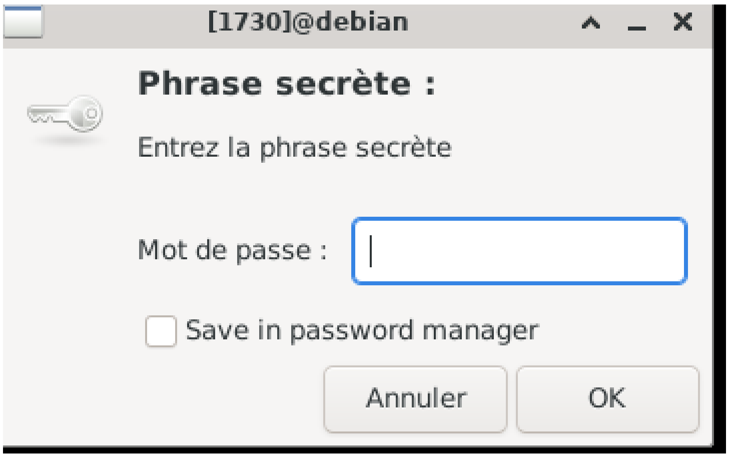
```
root@debian:/home/ynov/Bureau# cat crypte.txt.gpg
�u_�w�4p�root@debian:/home/ynov/Bureau# ����f�2�u��p�!������y\O\�����sbB,��a
```

On peut supprimer le fichier de base :



```
root@debian:/home/ynov/Bureau# rm crypte.txt
```

On le decrypt :

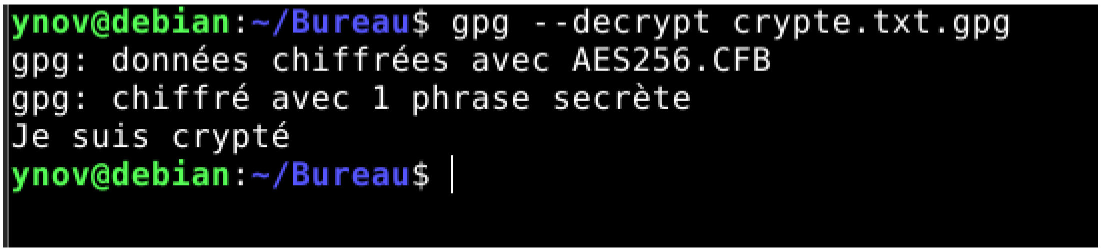


Phrase secrète :

Entrez la phrase secrète

Mot de passe :

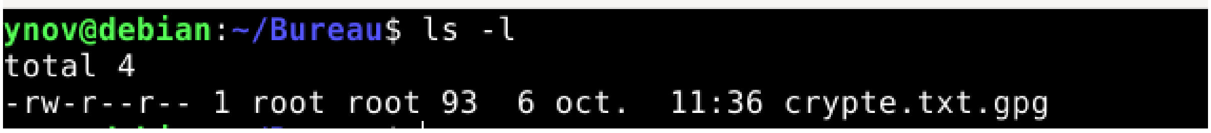
□ Save in password manager



```
ynov@debian:~/Bureau$ gpg --decrypt crypte.txt.gpg
gpg: données chiffrées avec AES256.CFB
gpg: chiffré avec 1 phrase secrète
Je suis crypté
ynov@debian:~/Bureau$ 
```

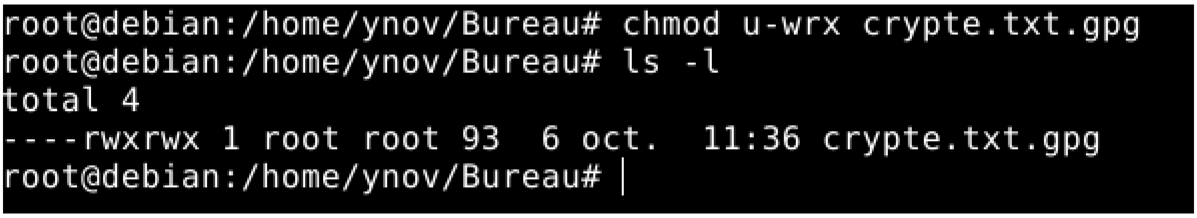
- Limiter les droit d’accès utilisateurs

On vérifie les droit d’accès :



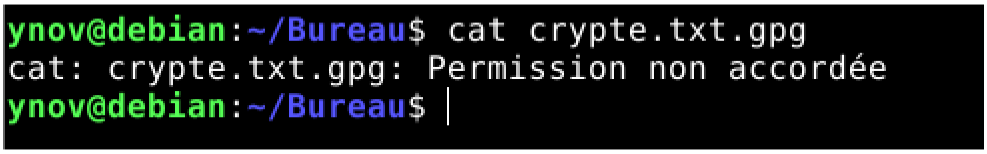
```
ynov@debian:~/Bureau$ ls -l
total 4
-rw-r--r-- 1 root root 93  6 oct.  11:36 crypte.txt.gpg
```

On modifie les droit utilisateur avec chmod



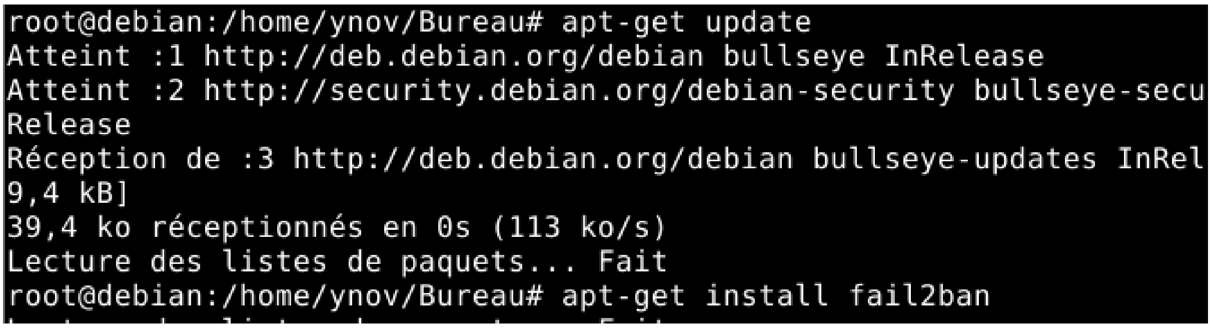
```
root@debian:/home/ynov/Bureau# chmod u-wrx crypte.txt.gpg
root@debian:/home/ynov/Bureau# ls -l
total 4
----rwxrwx 1 root root 93  6 oct.  11:36 crypte.txt.gpg
root@debian:/home/ynov/Bureau# 
```

On retourne sur l’utilisateur

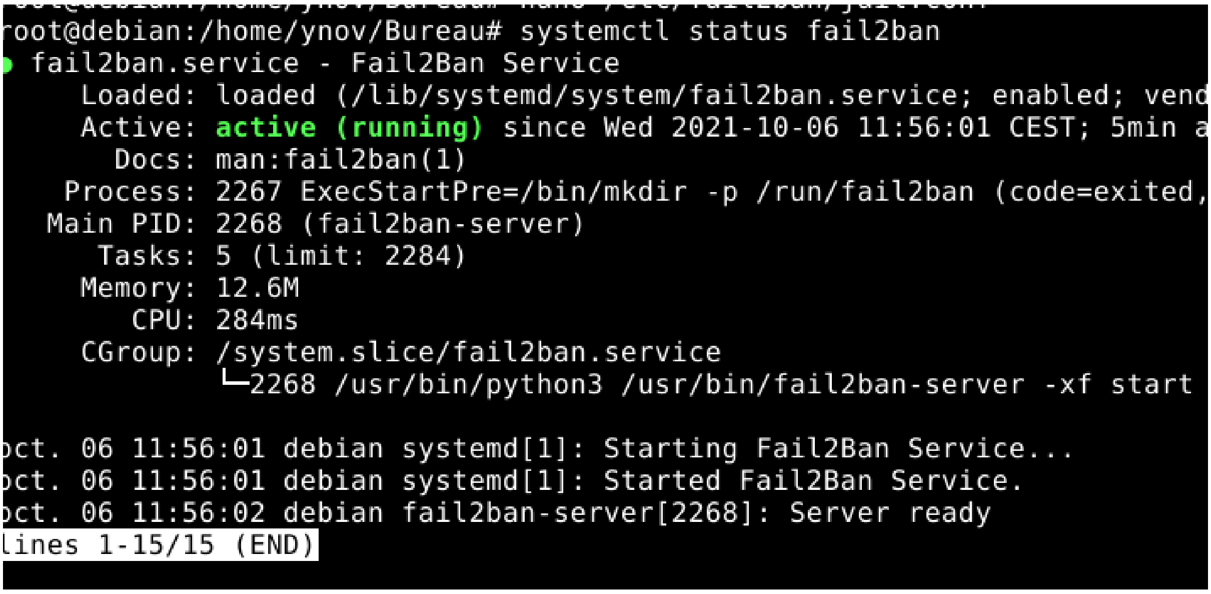


```
ynov@debian:~/Bureau$ cat crypte.txt.gpg
cat: crypte.txt.gpg: Permission non accordée
ynov@debian:~/Bureau$ 
```

- Installer et configurer Fail2Ban

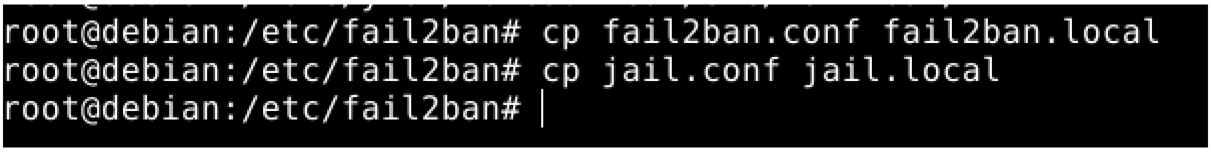


```
root@debian:/home/ynov/Bureau# apt-get update
Atteint :1 http://deb.debian.org/debian bullseye InRelease
Atteint :2 http://security.debian.org/debian-security bullseye-secu
Release
Réception de :3 http://deb.debian.org/debian bullseye-updates InRel
9,4 kB]
39,4 ko réceptionnés en 0s (113 ko/s)
Lecture des listes de paquets... Fait
root@debian:/home/ynov/Bureau# apt-get install fail2ban
```



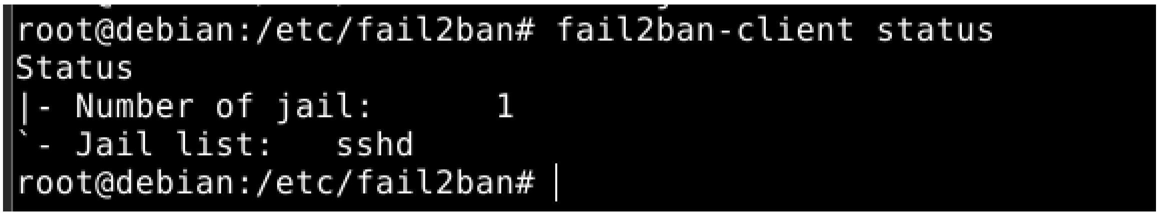
```
root@debian:/home/ynov/Bureau# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vend
     Active: active (running) since Wed 2021-10-06 11:56:01 CEST; 5min a
       Docs: man:fail2ban(1)
    Process: 2267 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited,
   Main PID: 2268 (fail2ban-server)
      Tasks: 5 (limit: 2284)
     Memory: 12.6M
        CPU: 284ms
     CGroup: /system.slice/fail2ban.service
             └─2268 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

oct. 06 11:56:01 debian systemd[1]: Starting Fail2Ban Service...
oct. 06 11:56:01 debian systemd[1]: Started Fail2Ban Service.
oct. 06 11:56:02 debian fail2ban-server[2268]: Server ready
lines 1-15/15 (END)
```

On copie les fichiers que l'on va modifier au cas où il y a une update est que aç overwrite notre fichier:



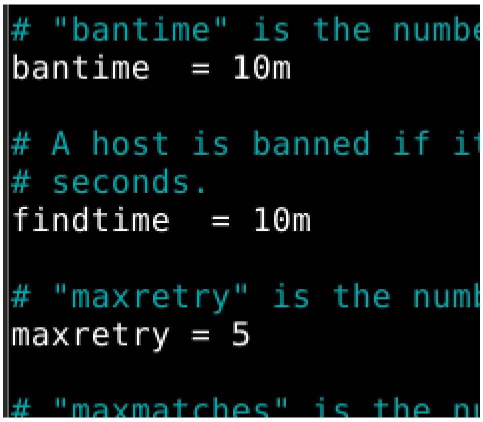
```
root@debian:/etc/fail2ban# cp fail2ban.conf fail2ban.local
root@debian:/etc/fail2ban# cp jail.conf jail.local
root@debian:/etc/fail2ban# 
```

Le sshd est de base bannit :



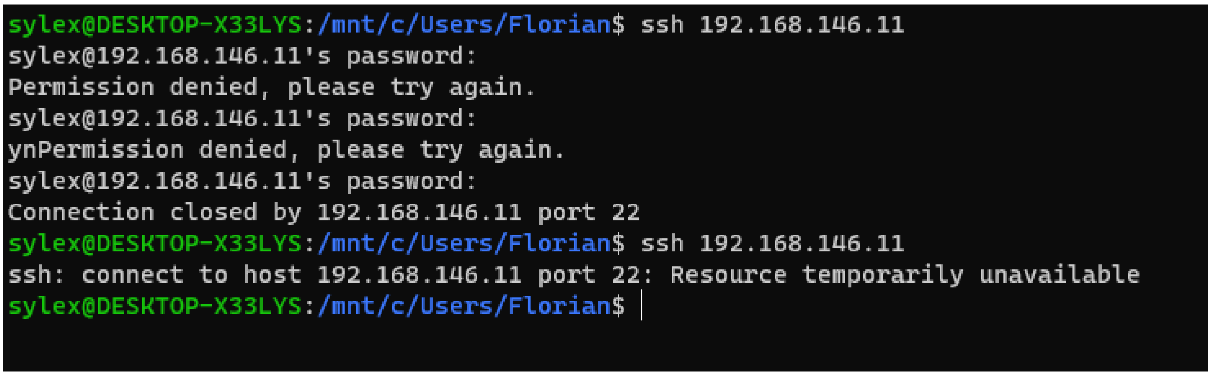
```
root@debian:/etc/fail2ban# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
root@debian:/etc/fail2ban# 
```

La configuration est de pour 5 erreur dans 10 minutes de temps ,l'utilisateur va être bannit 10 minutes



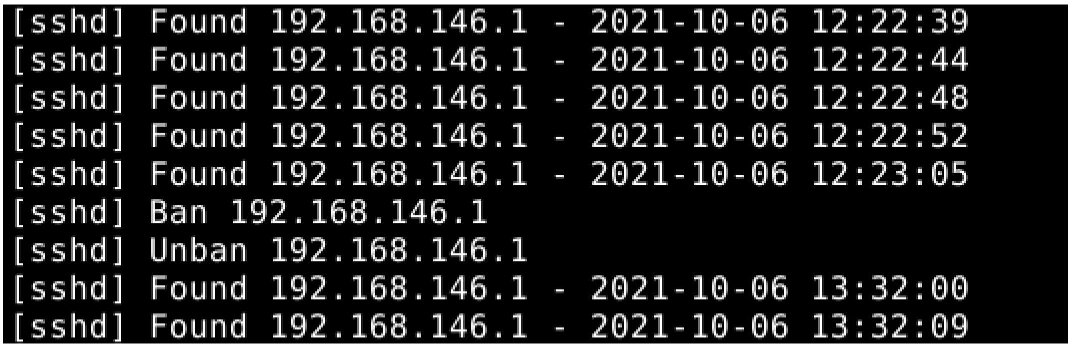
```
# "bantime" is the numbe
bantime  = 10m

# A host is banned if it
# seconds.
findtime  = 10m

# "maxretry" is the numb
maxretry = 5

# "maxmatches" is the nu
```

Après plusieurs essaie infructueux :



```
sylex@DESKTOP-X33LYS:/mnt/c/Users/Florian$ ssh 192.168.146.11
sylex@192.168.146.11's password:
Permission denied, please try again.
sylex@192.168.146.11's password:
ynPermission denied, please try again.
sylex@192.168.146.11's password:
Connection closed by 192.168.146.11 port 22
sylex@DESKTOP-X33LYS:/mnt/c/Users/Florian$ ssh 192.168.146.11
ssh: connect to host 192.168.146.11 port 22: Resource temporarily unavailable
sylex@DESKTOP-X33LYS:/mnt/c/Users/Florian$
```

L’adresse ip se fait ban :



```
[sshd] Found 192.168.146.1 - 2021-10-06 12:22:39
[sshd] Found 192.168.146.1 - 2021-10-06 12:22:44
[sshd] Found 192.168.146.1 - 2021-10-06 12:22:48
[sshd] Found 192.168.146.1 - 2021-10-06 12:22:52
[sshd] Found 192.168.146.1 - 2021-10-06 12:23:05
[sshd] Ban 192.168.146.1
[sshd] Unban 192.168.146.1
[sshd] Found 192.168.146.1 - 2021-10-06 13:32:00
[sshd] Found 192.168.146.1 - 2021-10-06 13:32:09
```