Réseaux: Cours 1

Le groupe des tueurs :

LEJOSNE Florian
MARTY Thomas
DE OLIVEIRA Thomas
ABELLA Alexandre
MANIXAY William
THIEN Anatole

vmware :
réglage de base d'iso
réglage connexion
test iso via win md5
lancer les 2 vm

Vnet 8 et nat :

ping 8.8.8.8 -> ça marche
crtl c

ip a - > 2 machines pour voir l'ip

```
net 192.168.5.129/24
inet 192.168.5.128/24
```

ip 192.168.5.128 -> sur la 129 pour voir la connection

```
ynov@ubuntu:~$ ping 192.168.5.128
PING 192.168.5.128 (192.168.5.128) 56(84) bytes of data.
64 bytes from 192.168.5.128: icmp_seq=1 ttl=64 time=0.066 ms
64 bytes from 192.168.5.128: icmp_seq=2 ttl=64 time=0.227 ms
64 bytes from 192.168.5.128: icmp_seq=3 ttl=64 time=0.060 ms
^C
```

Host Only:

ping 8.8.8.8 -> marche pas
ip a

```
ens33: <BROADCAST,MULTICA
 link/ether 00:50:56:33:1
 inet 192.168.245.128/24
```

```
ens33: <BROADCAST,MULTICA
 link/ether 00:50:56:39:a
 inet 192.168.245.129/24
```

ip a changé

ip pour voir si elles sont connectés : ca marche

```
ynov@ubuntu:~$ ping 192.168.245.129
PING 192.168.245.129 (192.168.245.129) 56(84) bytes of data.
64 bytes from 192.168.245.129: icmp_seq=1 ttl=64 time=1.13 ms
64 bytes from 192.168.245.129: icmp_seq=2 ttl=64 time=1.45 ms
64 bytes from 192.168.245.129: icmp_seq=3 ttl=64 time=0.414 ms
64 bytes from 192.168.245.129: icmp_seq=4 ttl=64 time=0.623 ms
64 bytes from 192.168.245.129: icmp_seq=5 ttl=64 time=0.784 ms
64 bytes from 192.168.245.129: icmp_seq=6 ttl=64 time=0.377 ms
64 bytes from 192.168.245.129: icmp_seq=7 ttl=64 time=0.467 ms
964 bytes from 192.168.245.129: icmp_seq=8 ttl=64 time=0.476 ms
64 bytes from 192.168.245.129: icmp_seq=9 ttl=64 time=0.321 ms
64 bytes from 192.168.245.129: icmp_seq=10 ttl=64 time=0.657 ms
^C
--- 192.168.245.129 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9148ms
rtt min/avg/max/mdev = 0.321/0.671/1.454/0.346 ms
ynov@ubuntu:~$ _
```

bridge

ping 8.8.8.8 -> pas de co

```
ynov2@ubuntu2:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4090ms
```

ip a

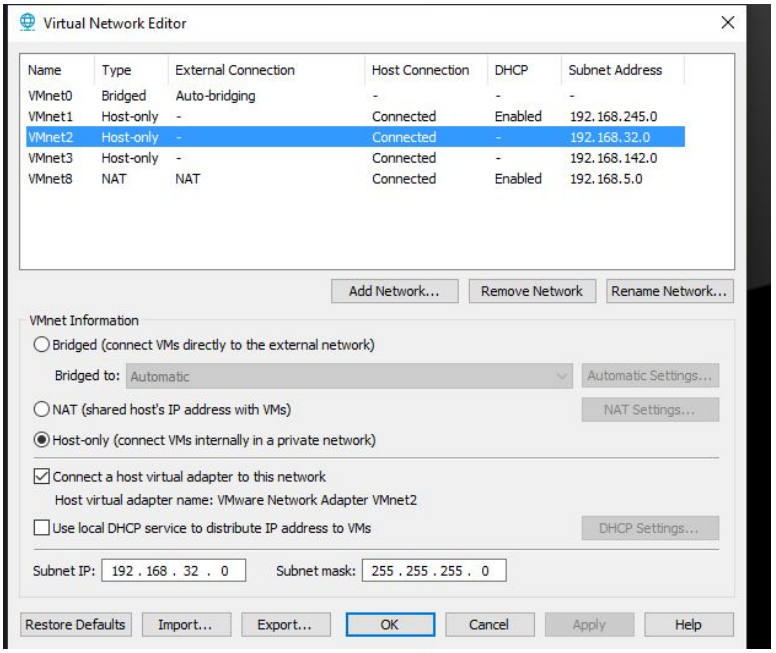
```
ens33: <BROADCAST,MULTICAS
 link/ether 00:50:56:39:aa
 inet 192.168.137.220/24 b
```

```
 link/ether 00:50:56:33:15
 inet 192.168.137.23/24 br
```

ip pour voir la co des 2 -> fonctionne

```
ynov2@ubuntu2:~$ ping 192.168.137.23
PING 192.168.137.23 (192.168.137.23) 56(84) bytes of data.
64 bytes from 192.168.137.23: icmp_seq=1 ttl=64 time=0.699 ms
64 bytes from 192.168.137.23: icmp_seq=2 ttl=64 time=0.394 ms
64 bytes from 192.168.137.23: icmp_seq=3 ttl=64 time=0.821 ms
64 bytes from 192.168.137.23: icmp_seq=4 ttl=64 time=0.542 ms
^C
```

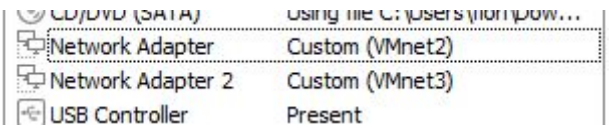
Réseaux: Cours 2



Ubuntu 1 et 2 en vmnet 2
Ubuntu 3 et 4 en vmnet 3

```
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:

   ethernets:
       ens33:

           addresses: [192.168.32.1/24]
           gateway4: 192.168.32.3
           nameservers:
               addresses: [8.8.8.8, 8.8.4.4]
           dhcp4: false
           dhcp6: false
   version: 2
```

Le router :



Réseaux :Cours 3

```
ynov@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4d:ad:5b brd ff:ff:ff:ff:ff:ff
    inet 192.168.32.3/24 brd 192.168.32.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe4d:ad5b/64 scope link
       valid_lft forever preferred_lft forever
3: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4d:ad:65 brd ff:ff:ff:ff:ff:ff
    inet 192.168.142.3/24 brd 192.168.142.255 scope global ens38
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe4d:ad65/64 scope link
       valid_lft forever preferred_lft forever
ynov@ubuntu:~$
```

```
 GNU nano 2.9.3                        /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:

   ethernets:
       ens33:

          addresses: [192.168.32.3/24]
          gateway4: 192.168.32.0
          nameservers:
              addresses: [8.8.8.8, 8.8.4.4]
          dhcp4: false
          dhcp6: false
   version: 2


network:

   ethernets:
       ens38:
            addresses: [192.168.142.3/24]
            gateway4: 192.168.142.0
            nameservers:
                addresses: [8.8.8.8, 8.8.4.4]
            dhcp4: false
            dhcp6: false
   version: 2




                          [ Défilement progressif - marche ]
^G Aide       ^O Écrire     ^W Chercher   ^K Couper     ^J Justifier  ^C Pos. cur.  M-U Annuler
^X Quitter    ^R Lire fich. ^\ Remplacer  ^U Coller     ^T Orthograp. ^_ Aller lig. M-E Refaire
```

ip forward :

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host


ynov@ubuntu:~$ cat /proc/sys/net/ipv4/ip_forward
1
ynov@ubuntu:~$
```

Réseaux: Cours 4

Le groupe des monstres :
PARRIEL Enzo
SENAC--SAVALL Louis
MOIGNE Théo
DE OLIVEIRA Thomas
LEJOSNE Florian

Ubuntu1 = A1
Ubuntu2 = B1
Ubuntu3 = A2
Ubuntu4 = B2

Ubuntu 1:

```
root@ubuntu:/home/ynov# ip route add 192.168.142.2 via 192.168.142.3
Error: Nexthop has invalid gateway.
root@ubuntu:/home/ynov# ip route add 192.168.142.2 via 192.168.32.3
root@ubuntu:/home/ynov# _
```

en gateway la Ubuntu 4
Le ping sur le routeur fonctionne

```
--- 192.168.142.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2019ms
rtt min/avg/max/mdev = 0.420/0.695/1.242/0.387 ms
ynov@ubuntu:~$ ping 192.168.32.2
PING 192.168.32.2 (192.168.32.2) 56(84) bytes of data.
64 bytes from 192.168.32.2: icmp_seq=1 ttl=64 time=1.61 ms
64 bytes from 192.168.32.2: icmp_seq=2 ttl=64 time=0.578 ms
^C
--- 192.168.32.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.578/1.097/1.616/0.519 ms
ynov@ubuntu:~$
```

Le ping sur la Ubuntu 4 à partir de la 1 fonctionne

```
--- 192.168.142.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2019ms
rtt min/avg/max/mdev = 0.420/0.695/1.242/0.387 ms
ynov@ubuntu:~$ ping 192.168.32.2
PING 192.168.32.2 (192.168.32.2) 56(84) bytes of data.
64 bytes from 192.168.32.2: icmp_seq=1 ttl=64 time=1.61 ms
64 bytes from 192.168.32.2: icmp_seq=2 ttl=64 time=0.578 ms
^C
--- 192.168.32.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.578/1.097/1.616/0.519 ms
ynov@ubuntu:~$
```

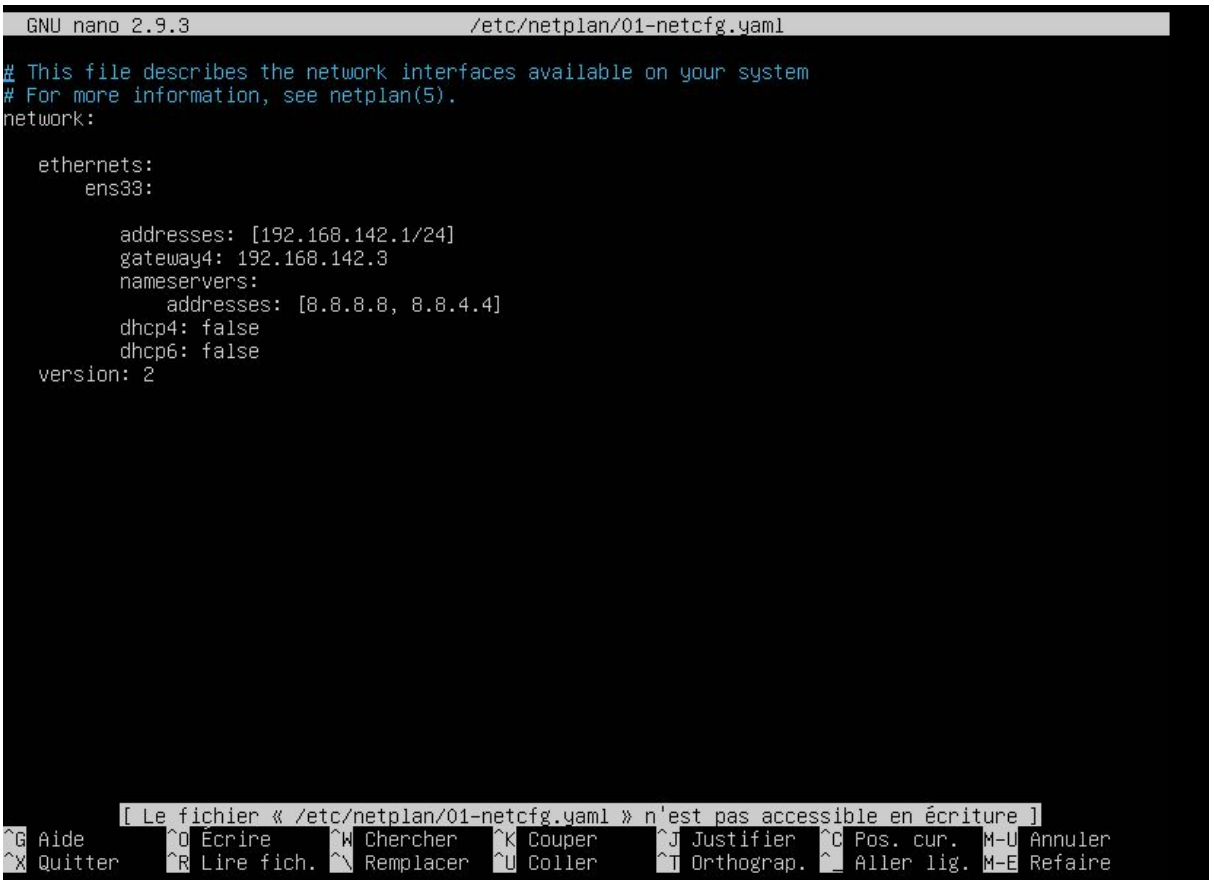
Ubuntu 2:

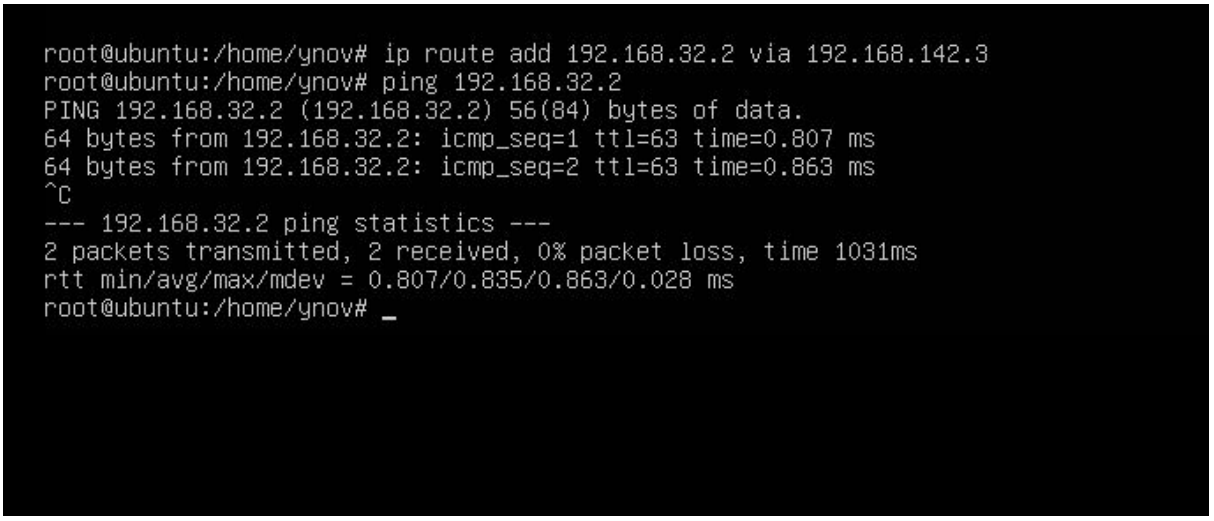
```
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:

   ethernets:
       ens33:

           addresses: [192.168.32.2/24]
           gateway4: 192.168.32.3
           nameservers:
               addresses: [8.8.8.8, 8.8.4.4]
           dhcp4: false
           dhcp6: false
   version: 2
```

gateway sur la Ubuntu 3

```
root@ubuntu:/home/ynov# netplan apply
root@ubuntu:/home/ynov# ip route add 192.168.142.1 via 192.168.32.3
root@ubuntu:/home/ynov# ping 192.168.142.1
PING 192.168.142.1 (192.168.142.1) 56(84) bytes of data.
64 bytes from 192.168.142.1: icmp_seq=1 ttl=63 time=0.875 ms
64 bytes from 192.168.142.1: icmp_seq=2 ttl=63 time=0.741 ms
^C
--- 192.168.142.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.741/0.808/0.875/0.067 ms
root@ubuntu:/home/ynov# _
```

Ubuntu 3:





ping sur router et Ubuntu 2

Ubuntu 4:

```
            addresses: [192.168.142.2/24]
            gateway4: 192.168.142.3
            nameservers:
                addresses: [8.8.8.8, 8.8.4.4]
            dhcp4: false
            dhcp6: false
    version: 2
```

```
rtt min/avg/max/mdev = 0.483/0.968/1.624/0.421 ms
root@ubuntu:/home/ynov# ip route add 192.168.32.1 via 192.168.142.
root@ubuntu:/home/ynov# ping 192.168.32.1
PING 192.168.32.1 (192.168.32.1) 56(84) bytes of data.
64 bytes from 192.168.32.1: icmp_seq=1 ttl=63 time=0.880 ms
64 bytes from 192.168.32.1: icmp_seq=2 ttl=63 time=1.32 ms
64 bytes from 192.168.32.1: icmp_seq=3 ttl=63 time=1.83 ms
64 bytes from 192.168.32.1: icmp_seq=4 ttl=63 time=0.971 ms
64 bytes from 192.168.32.1: icmp_seq=5 ttl=63 time=1.04 ms
64 bytes from 192.168.32.1: icmp_seq=6 ttl=63 time=1.25 ms
^C
--- 192.168.32.1 ping statistics ---
```

ping sur la Ubuntu 1

Ubuntu 5 : Router

```
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:

   ethernets:
       ens33:
          addresses: [192.168.32.3/24]
          nameservers:
              addresses: [8.8.8.8, 8.8.4.4]
          dhcp4: false
          dhcp6: false

   version: 2
   ethernets:
       ens38:
            addresses: [192.168.142.3/24]
            nameservers:
                addresses: [8.8.8.8, 8.8.4.4]
            dhcp4: false
            dhcp6: false
   version: 2









root@ubuntu:/etc/netplan# netplan apply
root@ubuntu:/etc/netplan# _
```

ping sur tous :

```
ynov@ubuntu:~$ ping 192.168.142.1
PING 192.168.142.1 (192.168.142.1) 56(84) bytes of data.
64 bytes from 192.168.142.1: icmp_seq=1 ttl=64 time=0.422 ms
64 bytes from 192.168.142.1: icmp_seq=2 ttl=64 time=0.423 ms
^C
--- 192.168.142.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1029ms
rtt min/avg/max/mdev = 0.422/0.422/0.423/0.020 ms
ynov@ubuntu:~$ ping 192.168.32.2
PING 192.168.32.2 (192.168.32.2) 56(84) bytes of data.
64 bytes from 192.168.32.2: icmp_seq=1 ttl=64 time=0.449 ms
64 bytes from 192.168.32.2: icmp_seq=2 ttl=64 time=0.656 ms
^C
--- 192.168.32.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1038ms
rtt min/avg/max/mdev = 0.449/0.552/0.656/0.106 ms
ynov@ubuntu:~$ ping 192.168.142.1
PING 192.168.142.1 (192.168.142.1) 56(84) bytes of data.
64 bytes from 192.168.142.1: icmp_seq=1 ttl=64 time=0.389 ms
64 bytes from 192.168.142.1: icmp_seq=2 ttl=64 time=0.504 ms
^C
--- 192.168.142.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.389/0.446/0.504/0.061 ms
ynov@ubuntu:~$ ping 192.168.142.2
PING 192.168.142.2 (192.168.142.2) 56(84) bytes of data.
64 bytes from 192.168.142.2: icmp_seq=1 ttl=64 time=0.415 ms
64 bytes from 192.168.142.2: icmp_seq=2 ttl=64 time=0.540 ms
^C
--- 192.168.142.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1029ms
rtt min/avg/max/mdev = 0.415/0.477/0.540/0.066 ms
ynov@ubuntu:~$
```

New iso :

dhcp quand le scope st en global dynamique.

2.1
iptables -L(voir l'état des tables)
2.2
iptables -N chaineName
2.3
nano monscript.sh
iptables -F
iptables -X
pour quitter nano ctrl+x
chmod +x monscript.sh
verification ls -l
exec le fichier bash

apt install netcat
apt install onpenssh-server
nano script.sh
chmod 777 script.sh

```
root@lab-3:~# chmod +x script.sh
root@lab-3:~# ls -l
total 4
-rwxr-xr-x 1 root root 40 déc.   3 10:43 script.sh
root@lab-3:~# iptables -N test
root@lab-3:~# iptables -N
iptables v1.6.1: option "-N" requires an argument
Try `iptables -h' or 'iptables --help' for more information.
root@lab-3:~# iptables -A test -j LOG
root@lab-3:~# iptables - L
Bad argument `-'
Try `iptables -h' or 'iptables --help' for more information.
root@lab-3:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain test (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             LOG level warning
root@lab-3:~#
```


```
root@ubuntu:~# bash script.sh
root@ubuntu:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu:~# chmod 777 script.sh
root@ubuntu:~# ls -l
total 4
-rwxrwxrwx 1 root root 38 déc.   3 12:08 script.sh
root@ubuntu:~# iptables -N test
root@ubuntu:~# iptables -A test -j LOG
```

3.1

iptables -N chainName

iptables -N

iptables -A chainName -j LOG

3.2

trouver l'endroit ou il y a les logs

cat /var/log/messages

```
-rwxrwxrwx 1 root root 38 déc.   3 12:08 script.sh
root@ubuntu:~# iptables -N test
root@ubuntu:~# iptables -A test -j LOG
root@ubuntu:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain test (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             LOG level warning
root@ubuntu:~# _
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain test (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             LOG level warning
root@ubuntu:~# iptables -A test -j LOG --log-prefix "test_DROP    ]"
root@ubuntu:~# iptables -P
iptables v1.6.1: option "-P" requires an argument
Try `iptables -h' or 'iptables --help' for more information.
root@ubuntu:~# iptables -P INPUT DROP
root@ubuntu:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3058ms

root@ubuntu:~# _
```

3.3

iptables -A chainName -j LOG --log-prefix "chainName_DROP   ]"

4.1

iptables -P INPUT DROP

ping 8.8.8.8 pour voir si on est connecter a internet(google)

on ne peux plus joindre internet parce que en iptables INPUT (tous les flux entrant)sont DROP(rejetés)

4.2

On autorise seulement les Flux souhaités , d'où le principe de filtrage et donc de Firewall.

iptables -A OUTPUT -p tcp -i ens33 --dport 80 -j ACCEPT

iptables -A OUTPUT -p tcp -i ens33 --dport 443 -j ACCEPT

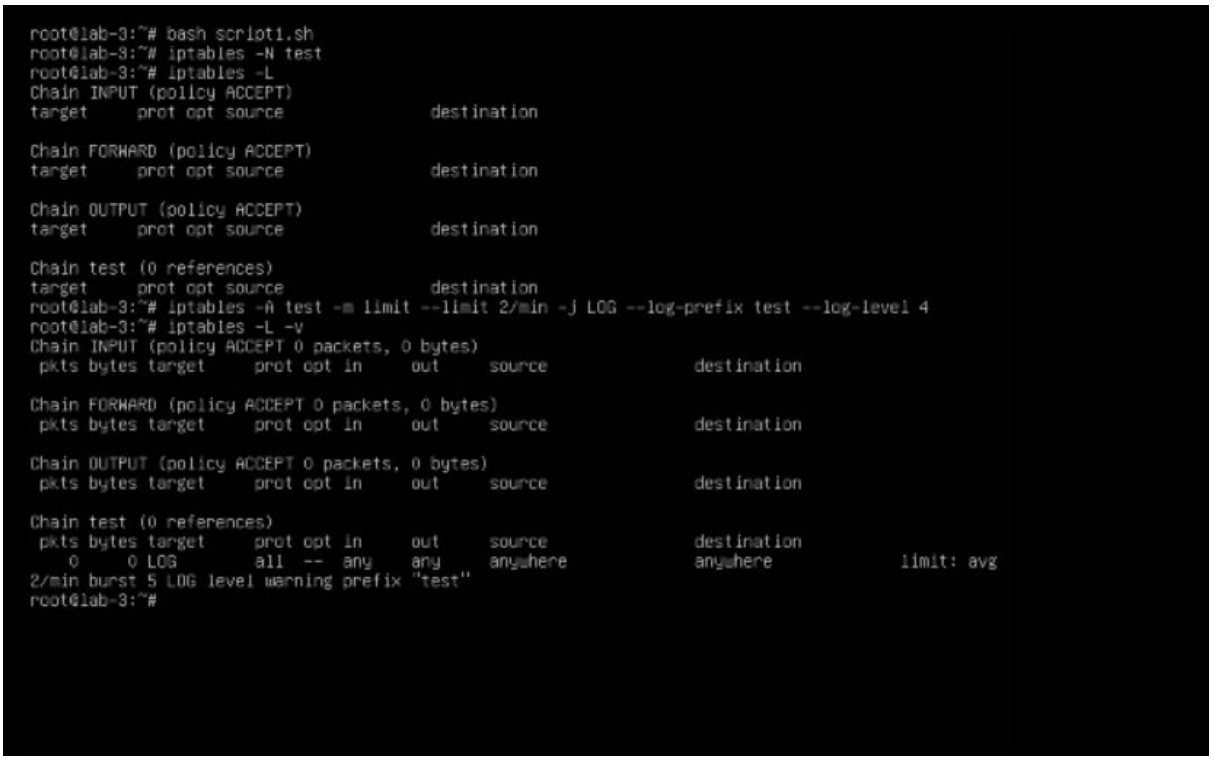
on autorise les ports 80(http), 443(https) et le 53 (DNS)

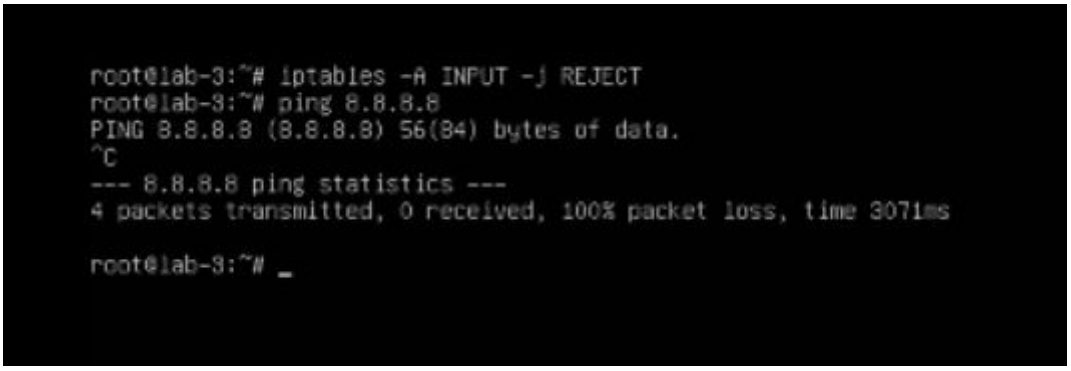
```
root@ubuntu:/script# bash reset.sh
root@ubuntu:/script# iptables -P INPUT DROP
root@ubuntu:/script# iptables -P OUTPUT DROP
root@ubuntu:/script# iptables -P FORWARD DROP
root@ubuntu:/script# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@ubuntu:/script# iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
root@ubuntu:/script# iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
root@ubuntu:/script# iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
root@ubuntu:/script# iptables -A OUTPUT -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
root@ubuntu:/script# iptables -A INPUT -p udp --sport 53 -m state --state ESTABLISHED -j ACCEPT
root@ubuntu:/script# iptables -A OUTPUT -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
root@ubuntu:/script# iptables -A INPUT -p tcp --sport 53 -m state --state ESTABLISHED -j ACCEPT
root@ubuntu:/script# iptables -A INPUT -i lo -j ACCEPT
root@ubuntu:/script# _
```

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain test (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             LOG level warning
root@ubuntu:~# iptables -A test -j LOG --log-prefix "test_DROP    ]"
root@ubuntu:~# iptables -P
iptables v1.6.1: option "-P" requires an argument
Try `iptables -h' or 'iptables --help' for more information.
root@ubuntu:~# iptables -P INPUT DROP
root@ubuntu:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3058ms

root@ubuntu:~# iptables -A INPUT -p tcp -i ens33 --dport 80 -j ACCEPT
root@ubuntu:~# iptables -A INPUT -p tcp -i ens33 --dport 443 -j ACCEPT
root@ubuntu:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain test (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             LOG level warning
LOG        all  --  anywhere             anywhere             LOG level warning prefix "test_DROP
 ]"
root@ubuntu:~# _
```

```
root@ubuntu:/script# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 23 -j REDIRECT --to-port 2
2
root@ubuntu:/script# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 512 -j REDIRECT --to-port
22
```

Avec Louis :


root@lab-3:~# bash script1.sh
root@lab-3:~# iptables -N test
root@lab-3:~# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain test (0 references)
target prot opt source destination
root@lab-3:~# iptables -A test -m limit --limit 2/min -j LOG --log-prefix test --log-level 4
root@lab-3:~# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain test (0 references)
pkts bytes target prot opt in out source destination
0 0 LOG all -- any any anywhere anywhere limit: avg
2/min burst 5 LOG level warning prefix "test"
root@lab-3:~#


root@lab-3:~# iptables -A INPUT -j REJECT
root@lab-3:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3071ms
root@lab-3:~# _