SOMMAIRE

1. Installation du serveur US3

Je mets comme mot de passe Azerty0 à l'utilisateur Root

```
sio@US3:~$ sudo -i
[sudo] password for sio:
root@US3:~# passwd
New password:
Retype new password:
passwd: password updated successfully
root@US3:~# _
```

Je mets le prompte en couleur

```
  GNU nano 6.2                                  /root/.bashrc
    xterm-color) color_prompt=yes;;
esac

# uncomment for a colored prompt, if the terminal has the capability; turned
# off by default to not distract the user: the focus in a terminal window
# should be on the output of commands, not on the prompt
force_color_prompt=yes

if [ -n "$force_color_prompt" ]; then
    if [ -x /usr/bin/tput ] && tput setaf 1 >&/dev/null; then
        # We have color support; assume it's compliant with Ecma-48
        # (ISO/IEC-6429). (Lack of such support is extremely rare, and such
        # a case would tend to support setf rather than setaf.)
        color_prompt=yes
    else
        color_prompt=
    fi
fi

if [ "$color_prompt" = yes ]; then
    PS1='${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033
else
    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
fi
```

j'affiche le contenu du dossier netplan

```
root@US3:~# ls /etc/netplan
00-installer-config.yaml
root@US3:~#
```

Je configure les interfaces réseaux

```
  GNU nano 6.2                    /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses: [192.168.1.101/24]
      dhcp4: no
      routes:
        - to: default
        via: 172.17.250.3
        nameservers:
          addresses: [192.168.1.1]
    enp0s8:
      addresses: [192.168.2.254/24]
      dhcp4: no
    enp0s9:
      addresses: [192.168.3.254/24]
      dhcp4: no
  version: 2
```

J’applique la configuration

```
root@US3:~# netplan apply
```

Je vérifie que les configurations ont bien été prise en compte

```
root@US3:~# 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:fd:c6:4b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fd17:625c:f037:2:a00:27ff:fefd:c64b/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86381sec preferred_lft 14381sec
    inet6 fe80::a00:27ff:fefd:c64b/64 scope link
       valid_lft forever preferred_lft forever
root@US3:~#
```

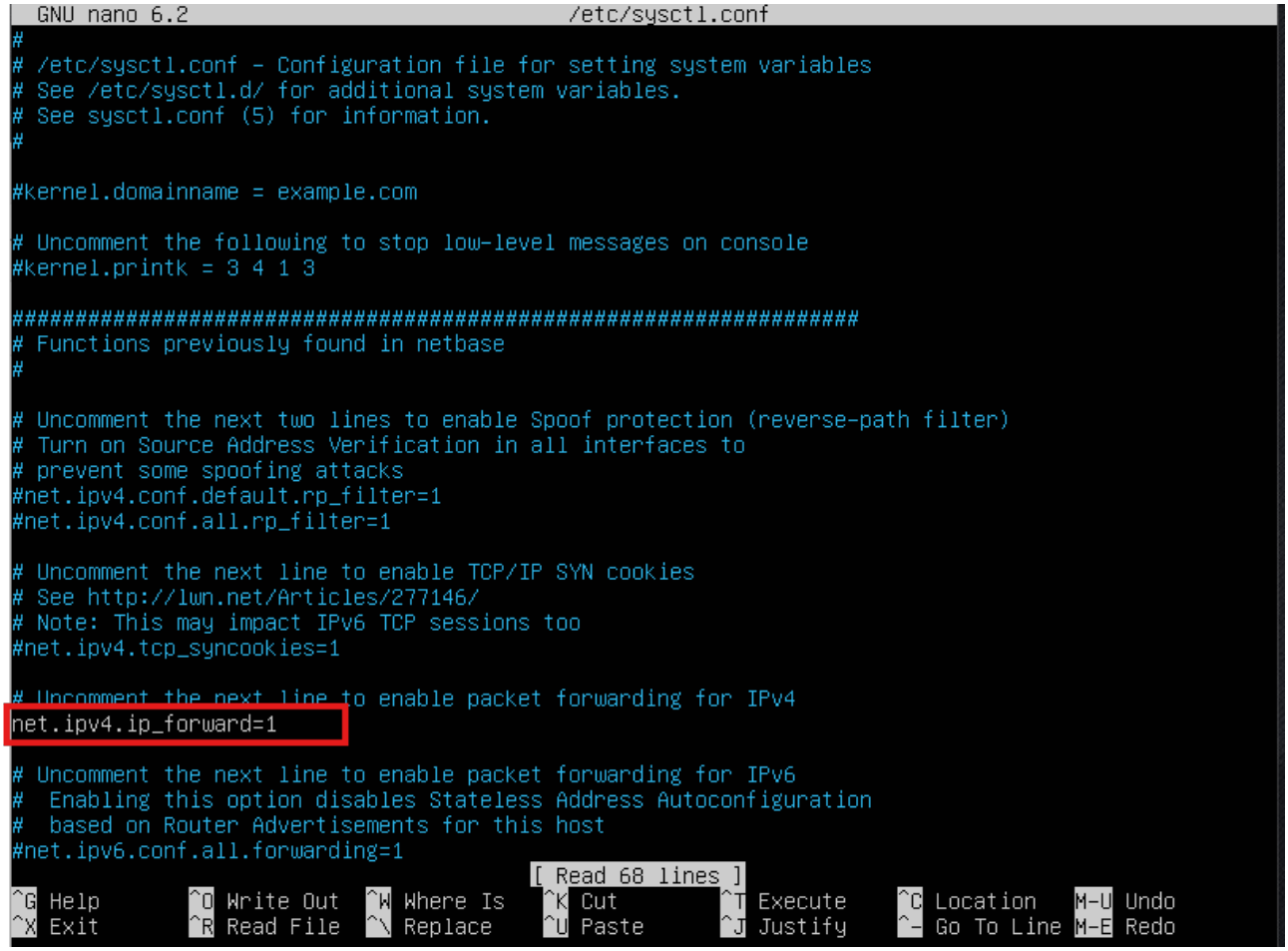
J’affiche la table de routage de US3

```
root@US3:~# ip r
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.101
root@US3:~#
```

Je modifie le fichier hosts

```
  GNU nano 6.2                                  /etc/hosts
127.0.0.1 localhost
192.168.1.101 US3.sio-exupery.local     US3
```

Je décommente la ligne suivante pour que le rouage soit pris en compte au démarrage de la machine



Je mets en place la translation d’adresse

```
root@US3:~# iptables -t nat -A POSTROUTING -o enoOs3 -j MASQUERADE
root@US3:~#
```

Je vérifie que la translation est bien prise en compte

```
root@US3:~# iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (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 POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  all  --  any    enp0s3  anywhere             anywhere
root@US3:~# _
```

Je créer un fichier qui se nomme iptables-service

```
  GNU nano 6.2                  /etc/systemd/system/iptables-rules.service
[Unit]
Desciption=firewall iptables rules

[Service]
Type=oneshot
ExecStart=/root/iptables-rules

[Install]
WantedBy=network-pre.target
```

Je créer le script iptables-rules

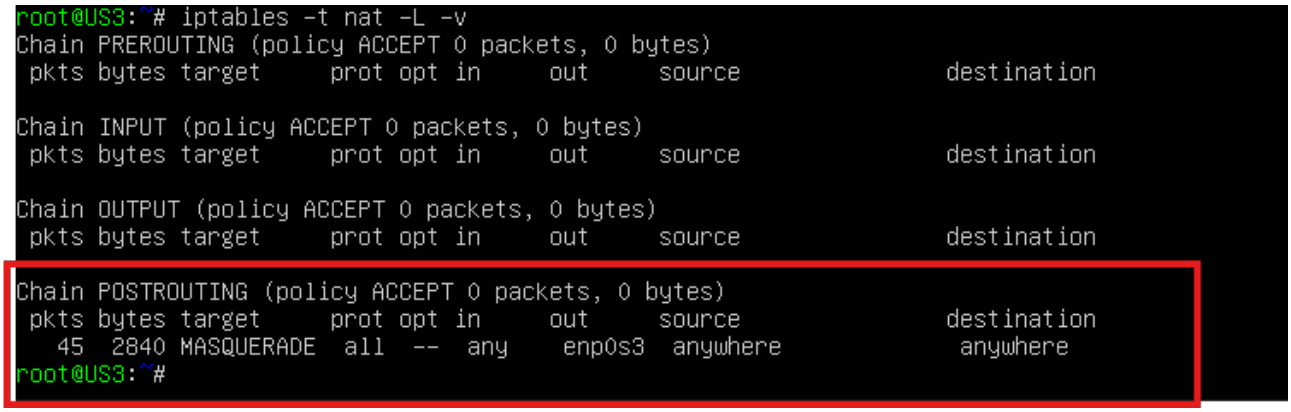
```
  GNU nano 6.2                          /root/iptables-rules
#!/bin/bash
/sbin/iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

```
root@US3:~# chmod 755 /root/iptables-rules
root@US3:~# ls -l iptables-rules
-rwxr-xr-x 1 root root 73 avril  1 17:55 iptables-rules
root@US3:~# _
```

J’active le nouveau service que je viens de créer

```
root@US3:~# systemctl enable iptables-rules.service
Created symlink /etc/systemd/system/network-pre.target.wants/iptables-rules.service → /etc/systemd/s
ystem/iptables-rules.service.
root@US3:~# _
```

Je redémarre la machine et je vérifie la table de routage



2. Modifications sur DS1

Je modifie le mode d’accès réseau pour la carte enp0s3 de DS1

```
 GNU nano 8.4                                                    /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 lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static

#address 172.17.101.218
#netmask 255.255.0.0
#network 172.17.0.0
#gateway 172.17.250.3
#broadcast 172.17.255.255



address 192.168.3.1
netmask 255.255.255.0
network 192.168.3.0
broadcast 192.168.3.255
gateway 192.168.3.254
```

Je vérifie la connectivité avec le serveur ROI

```
root@DS1: ~#ping -c2 172.17.254.11
PING 172.17.254.11 (172.17.254.11) 56(84) bytes of data.
64 bytes from 172.17.254.11: icmp_seq=1 ttl=127 time=2.90 ms
64 bytes from 172.17.254.11: icmp_seq=2 ttl=127 time=0.997 ms

--- 172.17.254.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1021ms
rtt min/avg/max/mdev = 0.997/1.950/2.904/0.953 ms
root@DS1: ~#_
```

3. Mise en place du pare-feu

3.1. Script et règles de base

J’écris le début script du parefeu

```
 GNU nano 6.2                                  /root/parefeu.sh *
#!/bin/bash
# Script pour l'établissement des règles du pare-feu
echo "Script pour le pare-feu"

#Initialisation de quelques variables
echo "--> Initialisation des variables :"

## Interface relié au réseau externe
WAN=enp0s3
## Interface reliée à la DMZ
DMZ=enp0s8
## Interface reliée au réseau interne
LAN=enp0s9
## Pour réduire la longueur des commandes iptables
IPT="/sbin/iptables"

echo"OK."
```

Je donne les droits d’exécution

```
root@US3:~# chmod 755 /root/parefeu.sh
root@US3:~# ls -l
total 12
-rwxr-xr-x 1 root root   73 avril  1 17:55 iptables-rules
-rwxr-xr-x 1 root root  407 avril  3 08:17 parefeu.sh
drwx------ 3 root root 4096 avril  1 15:56 snap
root@US3:~# _
```

Je supprime les règles et les chaînes des tables Filter

```
## Suppression des règles sur les tables FILTER, NAT et MANGLE
## Option -F pour flush
${IPT} -t filter -F
${IPT} -t nat -F
${IPT} -t mangle -F

##Suppression des chaînes sur les tables FILTER, NAT et MANGLE
## Option -X pour delete-chain
${IPT} -t filter -X
${IPT} -t nat -X
${IPT} -t mangle -X

## RAZ du compteur de paquets
## Option -Z pour zero
${IPT} -Z
```

Je créer une fonction qui servira à réinitialiser la politique du parefeu

```
## Interface relié au réseau externe
WAN=enp0s3
## Interface reliée à la DMZ
DMZ=enp0s8
## Interface reliée au réseau interne
LAN=enp0s9
## Pour réduire la longueur des commandes iptables
IPT="/sbin/iptables"

echo "OK."

TableFILTER()
{
${IPT} -t filter -P INPUT $1
${IPT} -t filter -P OUTPUT $1
${IPT} -t filter -P FORWARD $1
}
```

Je fais de sorte que la politique par défaut soit d’accepter les paquets

```
# Table FILTER positionnée en accès ouvert sur ses trois chaînes
TableFILTER ACCEPT


root@US3:~# _
```

J’ajoute une demande de poursuite d’exécution du parefeu

```
# Demande de poursuite du script
echo "--> Voulez-vous continuer loe script (O/n) ?"
read choix
if [ $choix = 'n' ] ; then
echo " Script interrompu. Vous n'avez plus de pare-feu... "
${IPT} -t nat -A POSTROUTING -o ${WAN} -j MASQUERADE
exit 0
fi
```

Je commence à mettre les règles

```
# Ecritures des règles par défaut

## Table NAT : acceptation sur ses trois chaînes
${IPT} -t nat -P PREROUTING ACCEPT
${IPT} -t nat -P OUTPUT ACCEPT
${IPT} -t nat -P POSTROUTING ACCEPT

## Table MANGLE : acceptation sur ses cinq chaînes
${IPT} -t mangle -P PREROUTING ACCEPT
${IPT} -t mangle -P INPUT ACCEPT
${IPT} -t mangle -P FORWARD ACCEPT
${IPT} -t mangle -P OUTPUT ACCEPT
${IPT} -t mangle -P POSTROUTING ACCEPT

## Table FILTER : refus sur ses trois chaînes
TableFILTER DROP

echo " Pare-feu en fonctionnement, blocage maximum. "
```

Je lance le script pour vérifier son fonctionnement

```
root@US3:~# ./parefeu.sh
Script pour le pare-feu
--> Initialisation des variables :
OK.
--> Vidage des règles existantes et verrouillage :
--> Voulez-vous continuer le script (o/n) ?
o
 Pare-feu en fonctionnement, blocage maximum.
root@US3:~#
```

J’affiche les tables Filter et Nat

```
root@US3:~# iptables -t filter -L -v
Chain INPUT (policy DROP 24 packets, 5275 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@US3:~#
```

```
root@US3:~# iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (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 POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@US3:~#
```

Je constate que depuis US3 je ne peux plus faire de ping

```
root@US3:~# ping -c1 192.168.3.254
PING 192.168.3.254 (192.168.3.254) 56(84) bytes of data.

--- 192.168.3.254 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@US3:~# ping -c1 192.168.2.254
PING 192.168.2.254 (192.168.2.254) 56(84) bytes of data.

--- 192.168.2.254 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@US3:~# ping -c1 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.

--- 192.168.3.1 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@US3:~#
```

Je relance le script et je désactive le parefeu

```
root@US3:~# ./parefeu.sh
Script pour le pare-feu
--> Initialisation des variables :
OK.
--> Vidage des règles existantes et verrouillage :
--> Voulez-vous continuer le script (o/n) ?
n
 Script interrompu. Vous n'avez plus de pare-feu...
root@US3:~# _
```

Je vérifie la chaîne POSTROUTING de la table Nat

```
root@US3:~# iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (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 POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   16   988 MASQUERADE  all  --  any    enp0s3  anywhere             anywhere
root@US3:~# _
```

Je vérifie la politique par défaut de chaque chaîne

```
root@US3:~# iptables -t filter -L -v
Chain INPUT (policy ACCEPT 146 packets, 11648 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 203 packets, 15168 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@US3:~# _
```

3.3. Règles concernant les chaînes INPUT/OUTPUT

J’ajoute les règles suivantes :

```
# Règles concernant les chaînes INPUT/OUTPUT
# Autorisation de quelques communications

## Autorisation des connexions locales
${IPT} -A INPUT -i lo -p all -j ACCEPT
${IPT} -A OUTPUT -o ${LAN} -p all -j ACCEPT

## Connexions avec l'extérieur
${IPT} -A INPUT -i ${LAN} -p all -j ACCEPT
${IPT} -A OUTPUT -o ${LAN} -p all -j ACCEPT

## Connexions avec l'extérieur
${IPT} -A INPUT -i ${WAN} -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
${IPT} -A OUTPUT -o ${WAN} -p all -m state ! --state INVALID -j ACCEPT

echo " Communications locales, internes et externes OK."
```

Je relance le script

```
root@US3:~# sh parefeu.sh
Script pour le pare-feu
--> Initialisation des variables :
OK.
--> Vidage des règles existantes et verrouillage :
--> Voulez-vous continuer le script (o/n) ?
o
 Pare-feu en fonctionnement, blocage maximum.
 Communications locales, internes et externes OK.
root@US3:~# _
```

Je vérifie la présence des règles dans la table filter

```
root@US3:~# iptables -t filter -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
    0     0 ACCEPT     all  --  enp0s9 any     anywhere             anywhere
    0     0 ACCEPT     all  --  enp0s3 any     anywhere             anywhere             state RELA
ED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 160 packets, 11360 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    enp0s9  anywhere             anywhere
    0     0 ACCEPT     all  --  any    enp0s9  anywhere             anywhere
    0     0 ACCEPT     all  --  any    enp0s3  anywhere             anywhere             ! state IN
ALID
root@US3:~# _
```

Je vérifie que les ping fonctionnent

```
root@US3:~# ping -c2 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.045 ms

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 0.032/0.038/0.045/0.006 ms
root@US3:~#
```

```
root@US3:~# ping -c2 www.google.fr
PING www.google.fr (142.251.142.67) 56(84) bytes of data.
64 bytes from ncmrsa-al-in-f3.1e100.net (142.251.142.67): icmp_seq=1 ttl=115 time=11.3 ms
64 bytes from ncmrsa-al-in-f3.1e100.net (142.251.142.67): icmp_seq=2 ttl=115 time=9.93 ms

--- www.google.fr ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 9.933/10.641/11.349/0.708 ms
root@US3:~# _
```

3.4. Règles concernant les flux IP traités par la chaîne FORWARD

1. DS1/Clients vers DS2

J’autorise les flux IP pour les requêtes DNS

```
# Autorisation des flux IP pour la châine FORWARD

## DS1/Clients vers DS2 (DNS, HTTP, FTP)
${IPT} -A FORWARD -i ${LAN} -o ${DMZ} -p tcp --dport 53 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${DMZ} -p udp --dport 53 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o $${DMZ} -p tcp --dport 80 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${DMZ} -p tcp --dport 443 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${DMZ} -p tcp --dport 21 -j ACCEPT
```

2. DS2 vers DS1/Clients

J’autorise seulement les connexions initiées par le réseau interne

```
## DS2 vers DS1/clients
${IPT} -A FORWARD -i ${DMZ} -o ${LAN} -m state --state RELATED,ESTABLISHED -j ACCEPT
```

3. DS1/Clients vers Internet

J’autorise seulement les requêtes HTTPS,HTTPS et FTP

```
# DS1/clients vers Internet
${IPT} -A FORWARD -i ${LAN} -o ${WAN} -p tcp --dport 80 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${WAN} -p tcp --dport 443 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${WAN} -p tcp --dport 21 -j ACCEPT
```

4. Internet vers DS1/Clients

J’autorise seulement les réponses qui ont été initiées par le réseau interne

```
## Internet vers Ds1/clients
${IPT} -A FORWARD -i ${WAN} -o ${LAN} -p tcp --sport 80 -m state --state RELATED,ESTABLISHED -j  AC
${IPT} -A FORWARD -i ${WAN} -o ${LAN} -p tcp --sport 443 -m state --state RELATED,ESTABLISHED -j AC
${IPT} -A FORWARD -i ${WAN} -o ${LAN} -p tcp --sport 21 -m state --state RELATED,ESTABLISHED -j ACC
```

5. DS2 vers Internet

J’autorise les flux DNS,HTTP,HTTPS et FTP

```
## DS2 vers Internet
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p tcp --dport 53 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p udp --dport 53 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p tcp --dport 80 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p tcp --dport 443 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p tcp --dport 21 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p tcp --sport 80 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p tcp --sport 53 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p udp --sport 53 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p tcp --sport 443 -j ACCEPT
${IPT} -A FORWARD -i ${DMZ} -o ${WAN} -p tcp --sport 21 -j ACCEPT

                                [ Wrote 129 lines ]
```

6. Internet vers DS2

J'autorise les demandes externes de résolution DNS

```
## Internet vers DS2
${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACC

${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p tcp --sport 53 -m state --state RELATED,ESTABLISHED -j ACC

${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACC

${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p tcp --sport 443 -m state --state RELATED,ESTABLISHED -j AC

${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p tcp --sport 21 -m state --state RELATED,ESTABLISHED -j ACC
PT
${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p tcp --dport 80 -j ACCEPT
${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p tcp --dport 53 -j ACCEPT
${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p udp --dport 53 -j ACCEPT
${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p udp --dport 80 -j ACCEPT
${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p tcp --dport 443 -j ACCEPT
${IPT} -A FORWARD -i ${WAN} -o ${DMZ} -p tcp --dport 21 -j ACCEPT
```

3.5. Fin du script et tests

J'ajoute en fin de script la règle de l'IP MASQUERADING

```
# NAT
${IPT} -t nat -A POSTROUTING -o ${WAN} -j MASQUERADE
```

J'autorise les flux DNS

```
# DS1/clients vers Internet
${IPT} -A FORWARD -i ${LAN} -o ${WAN} -p tcp --dport 80 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${WAN} -p tcp --dport 443 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${WAN} -p tcp --dport 21 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${WAN} -p tcp --dport 53 -j ACCEPT
${IPT} -A FORWARD -i ${LAN} -o ${WAN} -p udp --dport 53 -j ACCEPT


## Internet vers Ds1/clients
${IPT} -A FORWARD -i ${WAN} -o ${LAN} -p tcp --sport 80 -m state --state RELATED,ESTABLISHED -j  AC
${IPT} -A FORWARD -i ${WAN} -o ${LAN} -p tcp --sport 443 -m state --state RELATED,ESTABLISHED -j AC
${IPT} -A FORWARD -i ${WAN} -o ${LAN} -p tcp --sport 21 -m state --state RELATED,ESTABLISHED -j ACC
${IPT} -A FORWARD -i ${WAN} -o ${LAN} -p tcp --sport 53 -m state --state RELATED,ESTABLISHED -j ACC
${IPT} -A FORWARD -i ${WAN} -o ${LAN} -p udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACC
```

J'exécute le script du parefeu

```
root@US3:~# sh parefeu.sh
Script pour le pare-feu
--> Initialisation des variables :
OK.
--> Vidage des règles existantes et verrouillage :
--> Voulez-vous continuer le script (o/n) ?
o
 Pare-feu en fonctionnement, blocage maximum.
 Communications locales, internes et externes OK.
root@US3:~#
```

Depuis DD1 j'accède au site de www.ac-nice.fr