

Práctica SR

05/01/2024

Creado por: Pedro José Riquelme Guerrero



ÍNDICE

1. Configuración del router	3
2. Configuración DHCP	12
3. DHCP Relay	20
4. Failover	28
5. DNS	31
 5.1- DNS2	39
Ahora como en el anterior le cambiaremos el hostname la el interfaces y tendremos que hacer cambios en algunos archivos.	39
6. FTP	46

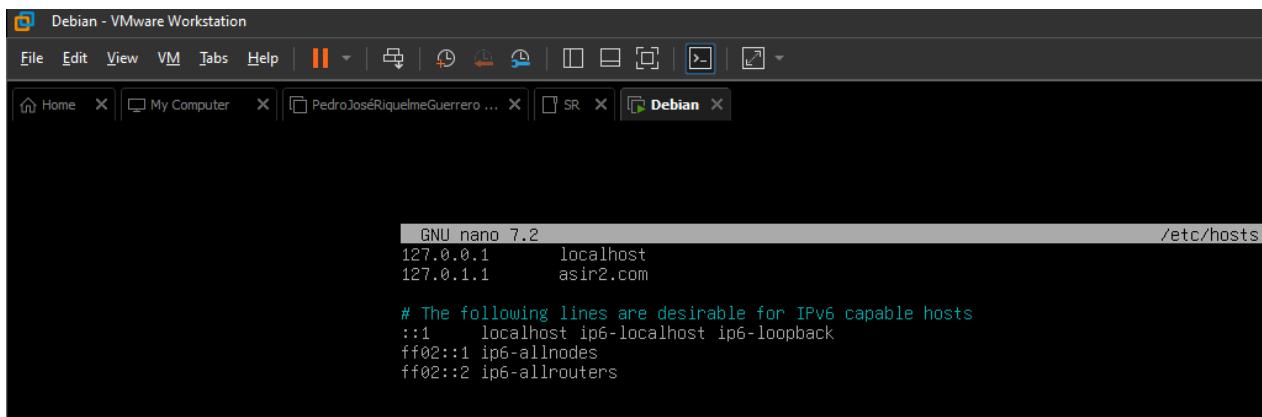
Antes de empezar hay que recalcar que empecé las prácticas con VMWare y por eso alomejor de primeras hay configuraciones que luego están de otra forma y eso es porque VMWare y VirtualBox usan distintos adaptadores

1. Configuración del router

ROUTER1	
Adaptadores	1 Adaptador puente 192.168.35.95 2 Red interna 172.16.95.1

Para configurar el router empezaremos cambiando el hots y el hostname

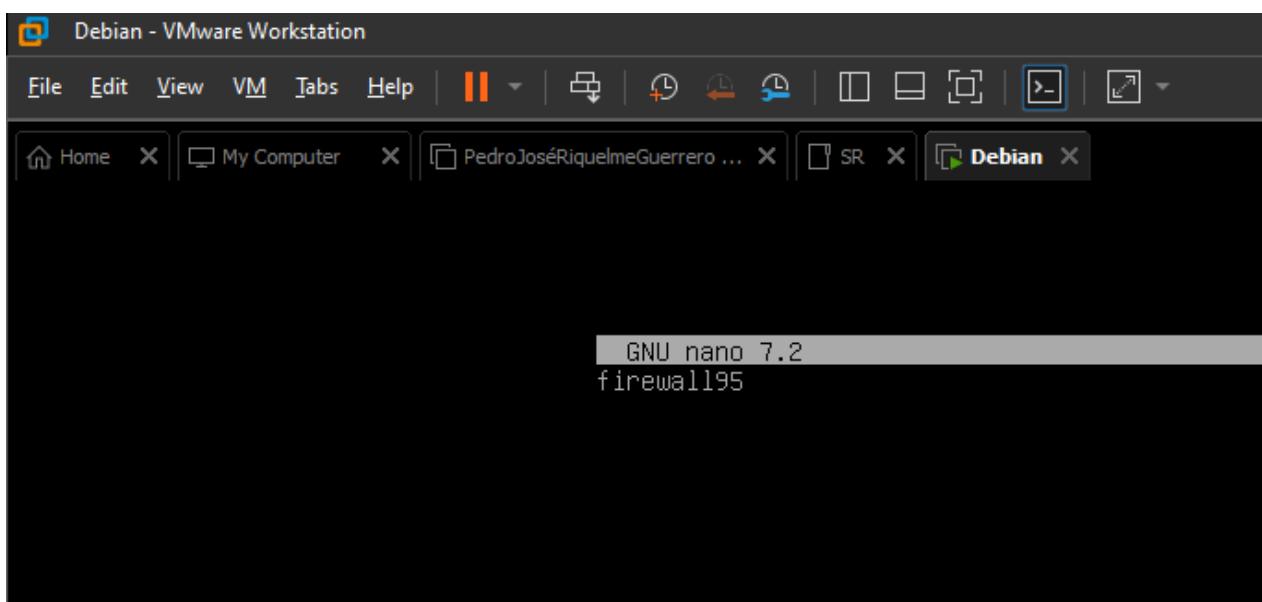
sudo nano /etc/hosts



```
GNU nano 7.2                                     /etc/hosts
127.0.0.1      localhost
127.0.1.1      asir2.com

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

sudo nano /etc/hostname



```
GNU nano 7.2
firewall95
```

Una vez hecho esto reiniciamos el debian y configuramos la ip del router

#Puente

```
auto enp0s3
```

```
iface enp0s3inet static
```

```
    address 192.168.35.95
```

```
    netmask 255.255.255.0
```

```
    network 192.168.35.0
```

```
    gateway 192.168.35.1
```

#redAsir

```
auto enp0s8
```

```
iface enp0s8 inet static
```

```
    address 172.16.95.254
```

```
    netmask 255.255.255.0
```

```
    network 172.16.95.0
```

```
GNU nano 7.2 /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

#Puente
auto ens33
iface ens33 inet static
    address 192.168.35.95
    netmask 255.255.255.0
    network 192.168.35.1
    gateway 192.168.35.1

#redAsir
auto ens37
iface ens37 inet static
    address 172.16.95.254
    netmask 255.255.255.0
    network 172.16.95.0
```

Una vez configurada la ip configuraremos el archivo:

/etc/init.d/reenvioiptables.sh

en el cual vamos a poner lo siguiente:

```
#!/bin/sh
```

```
#Script de inicio
```

```
### BEGIN INIT INFO
```

```
# Provides: reenvioiptables.sh
```

```
# Required-Start: $all
```

```
# Required-Stop: $all
```

```
# Default-Start: 2 3 4 5
```

```
# Default-Stop: 0 1 6
```

```
# Short-Description: Firewall para red interna.
```

```
# Description: Daemon para hacer funcionar la maquina como firewall usando iptables.
```

```
### END INIT INFO
```

```
#BORRA LAS REGLAS QUE HAYA
```

```
iptables -F
```

```
iptables -X
```

```
iptables -Z
```

```
iptables -t nat -F
```

```
#POLITICA POR DEFECTO
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

```
iptables -P FORWARD ACCEPT
```

```
iptables -t nat -P PREROUTING ACCEPT
```

```
iptables -t nat -P POSTROUTING ACCEPT
```

```
#ACEPTAMOS ACCESO LOCALHOST
```

```
iptables -A INPUT -i lo -j ACCEPT
```

```
#PERMITIMOS ACCESO DESDE LA RED LOCAL
```

```
iptables -A INPUT -s 172.16.95.0/24 -j ACCEPT
```

#ENMASCARAMOS RED LOCAL

```
iptables -t nat -A POSTROUTING -s 172.16.95.0/24 -o enp0s3-j MASQUERADE
```

#ACTIVAMOS BIT FORWARD

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

#PERMITIMOS ACCESO AL PUERTO 22 (SSH)

```
iptables -A INPUT -s 0.0.0.0/0 -i enp0s3-p tcp --dport 22 -j ACCEPT
```

#REDIRECCIONAMOS PUERTOS

```
iptables -t nat -A PREROUTING -i enp0s3-p tcp --dport 2201 -j DNAT --to 172.16.95.2:22
```

```
iptables -t nat -A PREROUTING -i enp0s3-p tcp --dport 3389 -j DNAT --to  
172.16.95.3:3389
```

```
iptables -t nat -A PREROUTING -i ens33 -p udp --dport 3389 -j DNAT --to  
172.16.95.3:3389
```

#CERRAMOS LOS PUERTOS BIEN CONOCIDOS

```
iptables -A INPUT -s 0.0.0.0/0 -i enp0s3-p tcp --dport 1:1024 -j DROP
```

```
iptables -A INPUT -s 0.0.0.0/0 -i enp0s3-p udp --dport 1:1024 -j DROP
```

```
pedro@pedro:~  
GNU nano 7.2  
#!/bin/sh  
## Script de inicio  
### BEGIN INIT INFO  
# Provides: reenvioiptables.sh  
# Required-Start: $all  
# Required-Stop: $stop  
# Default-Start: 2 3 4 5  
# Default-Stop: 0 1 6  
# Short-Description: Firewall para red interna.  
# Description: Daemon para hacer funcionar la maquina como firewall usando iptables.  
### END INIT INFO  
  
#BORRA LAS REGLAS QUE HAYA  
iptables -F  
iptables -X  
iptables -Z  
iptables -t nat -F  
  
#POLITICA POR DEFECTO  
iptables -P INPUT ACCEPT  
iptables -P OUTPUT ACCEPT  
iptables -P FORWARD ACCEPT  
iptables -t nat -P PREROUTING ACCEPT  
iptables -t nat -P POSTROUTING ACCEPT  
  
#ACEPTAMOS ACCESO LOCALHOST  
iptables -A INPUT -i lo -j ACCEPT  
  
#PERMITIMOS ACCESO DESDE LA RED LOCAL  
iptables -A INPUT -s 172.16.95.0/24 -j ACCEPT  
  
#ENMASCARAMOS RED LOCAL  
iptables -t nat -A POSTROUTING -s 172.16.95.0/24 -o ens33 -j MASQUERADE  
  
#ACTIVAMOS BIT FORWARD  
echo 1 > /proc/sys/net/ipv4/ip_forward  
  
#PERMITIMOS ACCESO AL PUERTO 22 (SSH)  
iptables -A INPUT -s 0.0.0.0/0 -i ens33 -p tcp --dport 22 -j ACCEPT  
  
#REDIRECCIONAMOS PUERTOS  
iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 2201 -j DNAT --to 172.16.95.2:22  
iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 3389 -j DNAT --to 172.16.95.3:3389  
iptables -t nat -A PREROUTING -i ens33 -p udp --dport 3389 -j DNAT --to 172.16.95.3:3389  
  
#CERRAMOS LOS PUERTOS BIEN CONOCIDOS  
iptables -A INPUT -s 0.0.0.0/0 -i ens33 -p tcp --dport 1:1024 -j DROP  
iptables -A INPUT -s 0.0.0.0/0 -i ens33 -p udp --dport 1:1024 -j DROP
```

Una vez configurado el reenvioiptables y nos iremos a editar el archivo:

/etc/systemd/system/reenvioiptables.service

En el cual le pondremos lo siguiente:

[Unit]

Description=Firewall para red interna

After=network.target

[Service]

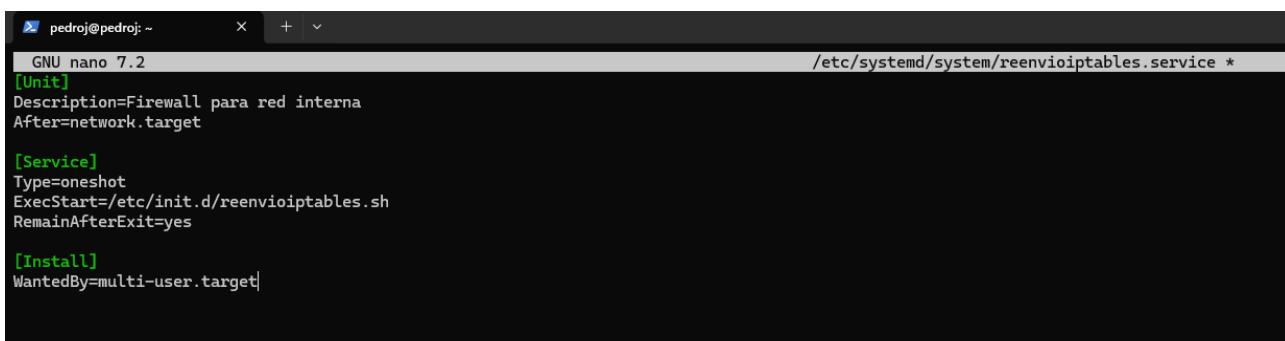
Type=oneshot

ExecStart=/etc/init.d/reenvioiptables.sh

RemainAfterExit=yes

[Install]

WantedBy=multi-user.target



The screenshot shows a terminal window titled "pedroj@pedroj: ~". The command "nano 7.2" is running, and the file "/etc/systemd/system/reenvioiptables.service" is being edited. The content of the file is as follows:

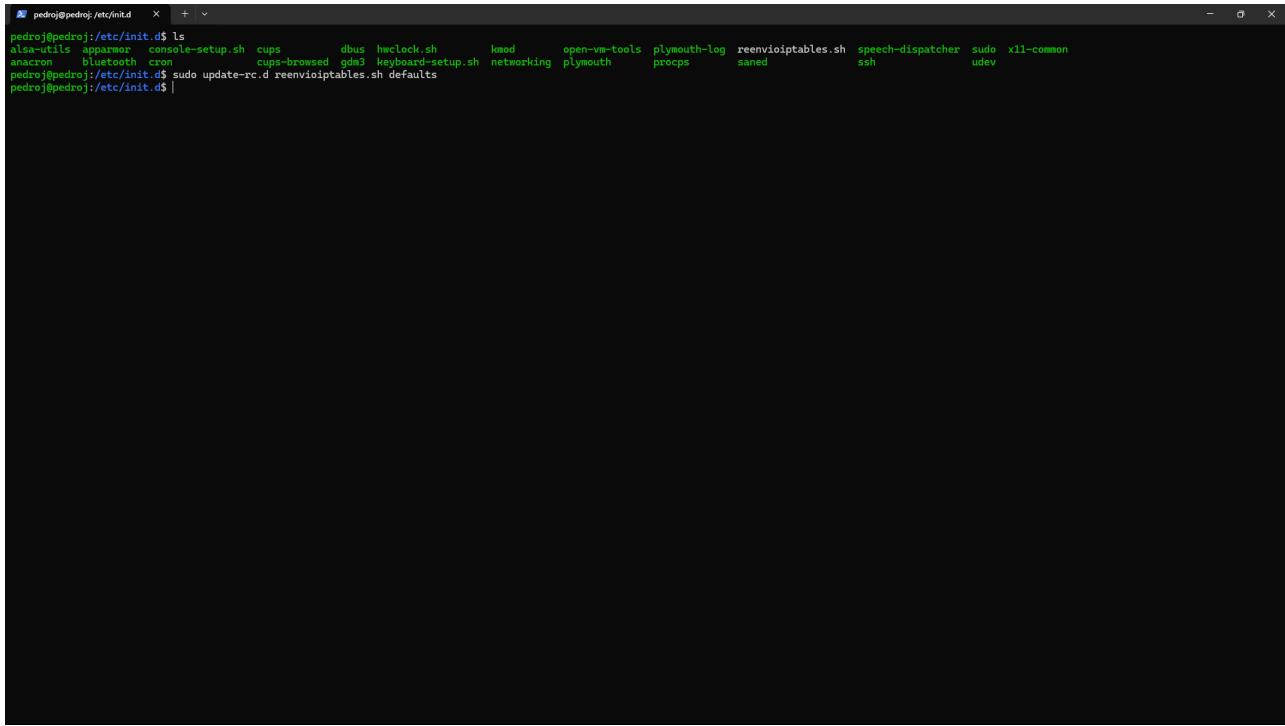
```
[Unit]
Description=Firewall para red interna
After=network.target

[Service]
Type=oneshot
ExecStart=/etc/init.d/reenvioiptables.sh
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

A continuación nos iremos a el repositorio /etc/init.d y ahí dentro ejecutaremos el siguiente comando:

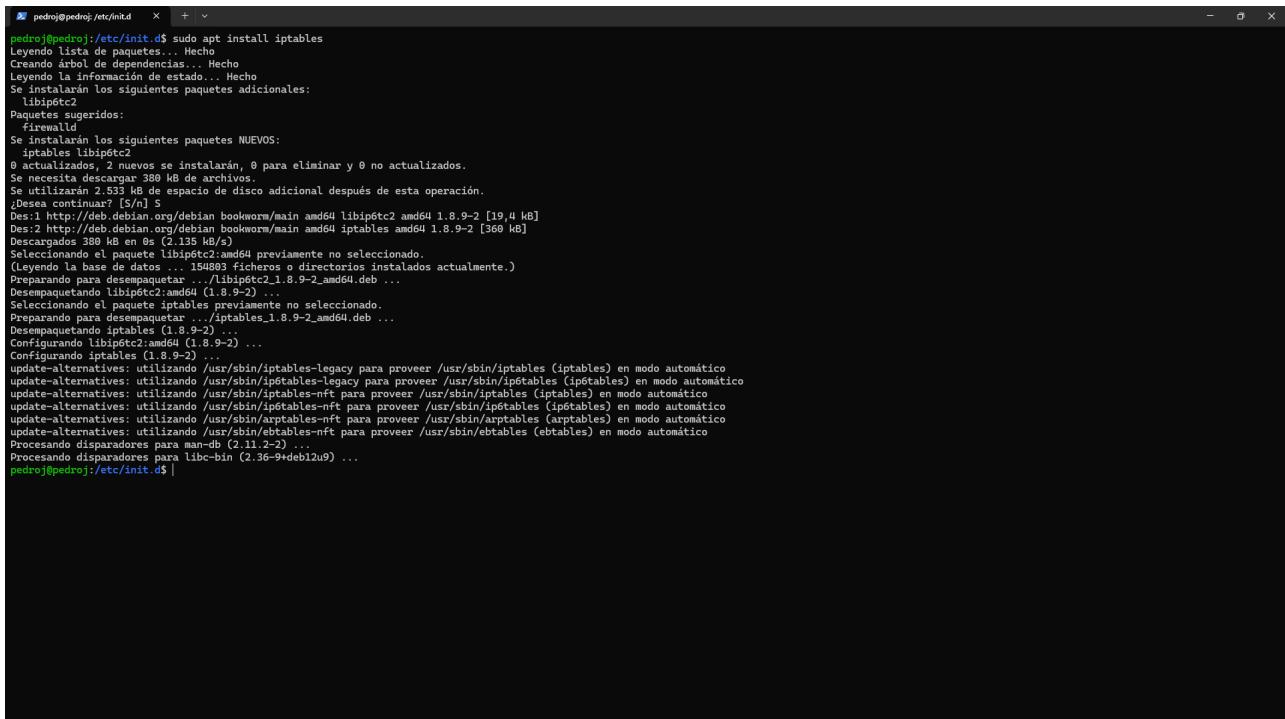
```
sudo update-rc.d reenvioiptables.sh defaults
```



```
pedro@pedroj:/etc/init.d$ ls
alsa-utils apparmor console-setup.sh cups      dbus   hwclock.sh    kmod      open-vm-tools plymouth-log reenvioiptables.sh speech-dispatcher sudo x11-common
anacron bluetooth cron   cups-browsed gdm3   keyboard-setup.sh networking  plymouth   procps    saned    ssh     udev
pedro@pedroj:/etc/init.d$ sudo update-rc.d reenvioiptables.sh defaults
pedro@pedroj:/etc/init.d$ |
```

Una vez hecho instalaremos el iptables

```
sudo apt install iptables
```



```
pedro@pedroj:/etc/init.d$ sudo apt install iptables
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libipipctc2
Paquetes sugeridos:
  firewalld
Se instalarán los siguientes paquetes NUEVOS:
  iptables libipipctc2
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesitarán descargar 300 kB de archivos.
Se utilizarán 2.533 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://deb.debian.org/debian bookworm/main amd64 libipipctc2 amd64 1.8.9-2 [19,4 kB]
Des:2 http://deb.debian.org/debian bookworm/main amd64 iptables amd64 1.8.9-2 [360 kB]
Descargados 388 kB en 0s (2.135 kB/s)
Seleccionando el paquete libipipctc2:amd64 previamente no seleccionado.
(Leyendo la base de datos... 154893 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../libipipctc2_1.8.9-2_amd64.deb ...
Desempaquetando libipipctc2:amd64 (1.8.9-2) ...
Seleccionando el paquete iptables previamente no seleccionado.
Preparando para desempaquetar .../iptables_1.8.9-2_amd64.deb ...
Desempaquetando iptables (1.8.9-2) ...
Configurando libipipctc2:amd64 (1.8.9-2) ...
Configurando iptables (1.8.9-2) ...
update-alternatives: utilizando /usr/sbin/iptables-legacy para proveer /usr/sbin/iptables (iptables) en modo automático
update-alternatives: utilizando /usr/sbin/iptables-legacy para proveer /usr/sbin/iptables (iptables) en modo automático
update-alternatives: utilizando /usr/sbin/iptables-nft para proveer /usr/sbin/iptables (iptables) en modo automático
update-alternatives: utilizando /usr/sbin/iptables-nft para proveer /usr/sbin/p6tables (iptables) en modo automático
update-alternatives: utilizando /usr/sbin/Arptables-nft para proveer /usr/sbin/Arptables (arptables) en modo automático
update-alternatives: utilizando /usr/sbin/eBTables-nft para proveer /usr/sbin/eBTables (ebtables) en modo automático
Procesando disparadores para man-db (2.11.2-2) ...
Procesando disparadores para libc-bin (2.36-9+deb12u9) ...
```

Cuando ya hemos instalado el iptables le daremos permisos a el archivo reenvioiptables.sh y lo ejecutaremos.

```
sudo chmod +x reenvioiptables.sh
```

```
sudo ./reenvioiptables.sh
```

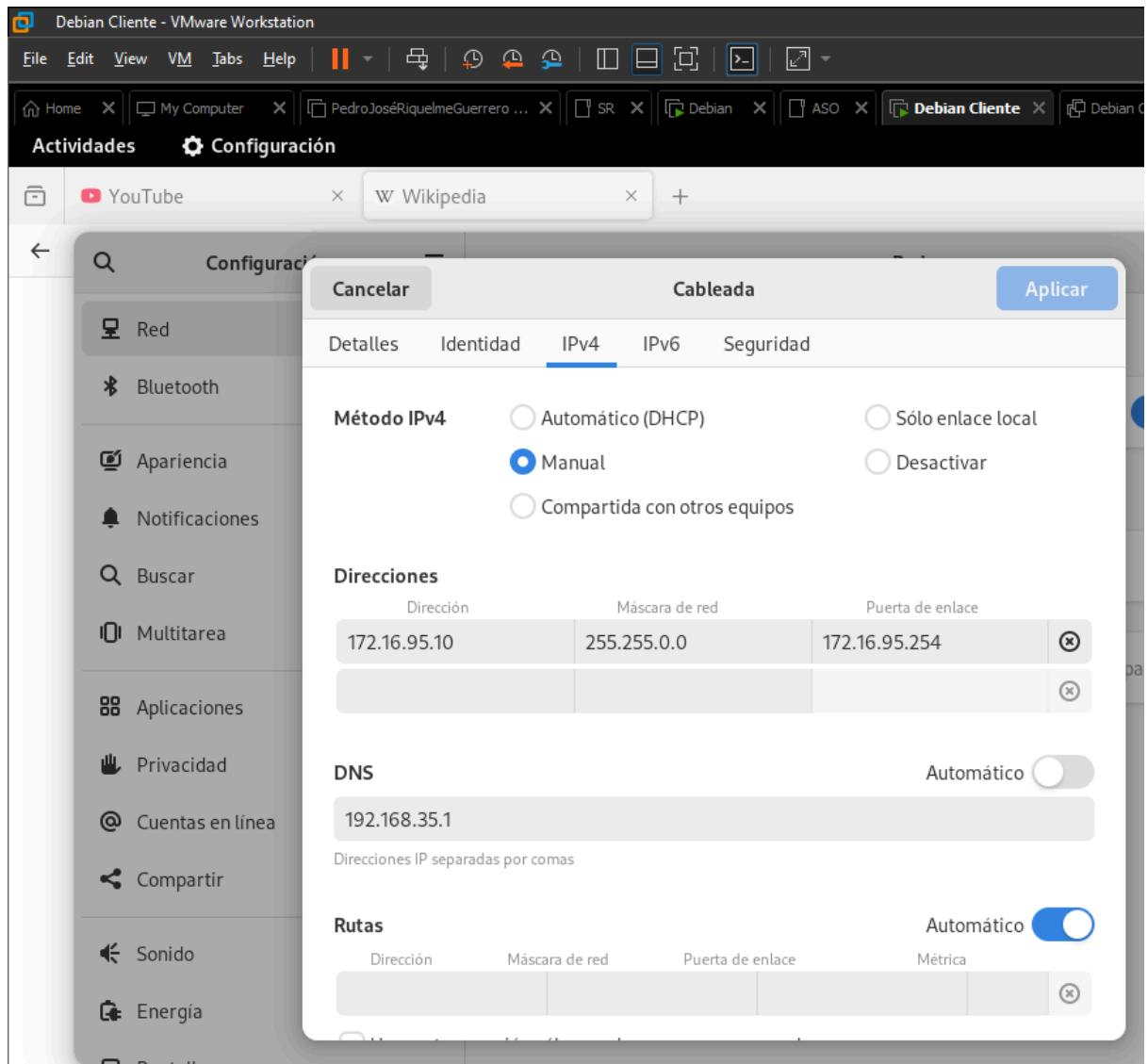
```
sudo iptables -L
```

```
pedroj@pedroj:/etc/init.d      X  +  ~
pedroj@pedroj:/etc/init.d$ sudo chmod +x reenvioiptables.sh
pedroj@pedroj:/etc/init.d$ sudo ./reenvioiptables.sh
pedroj@pedroj:/etc/init.d$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT    all  --  anywhere        anywhere
ACCEPT    all  --  172.16.95.0/24   anywhere
ACCEPT    tcp  --  anywhere        anywhere          tcp dpt:ssh
DROP      tcp  --  anywhere        anywhere          tcp dpts:tcpmux:1024
DROP      udp  --  anywhere        anywhere          udp dpts:1:1024

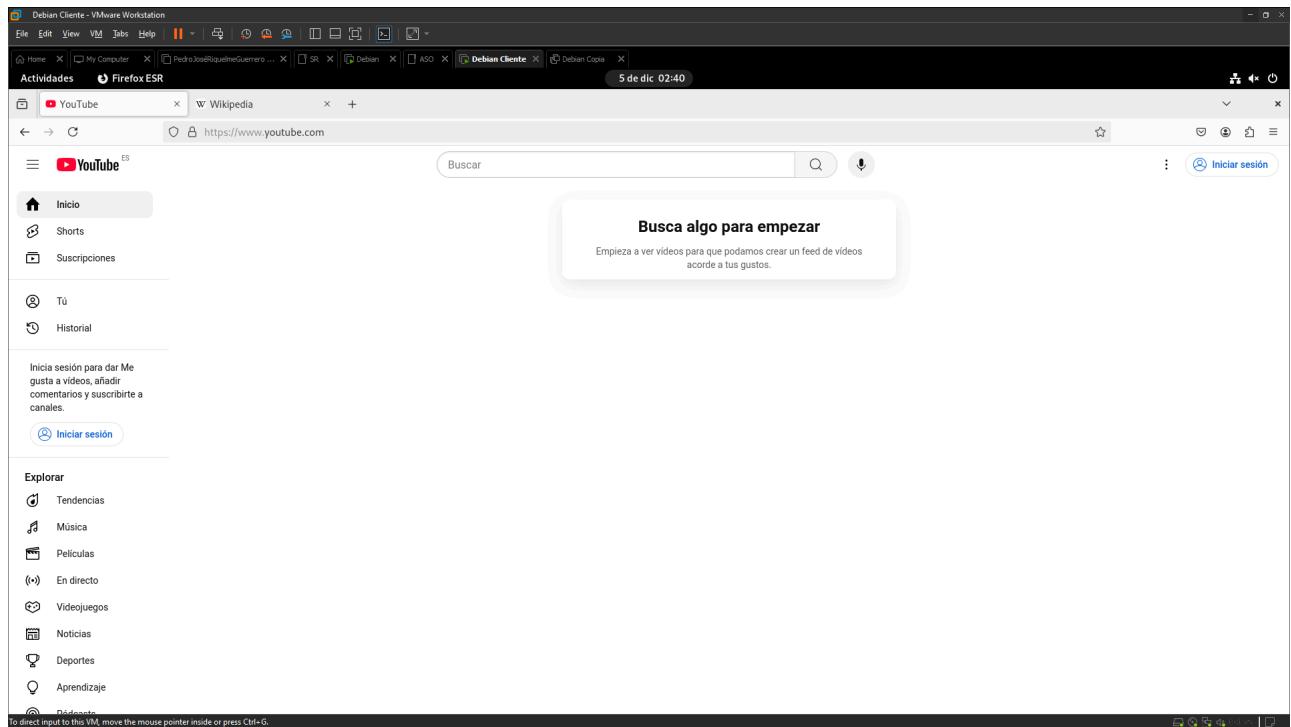
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
pedroj@pedroj:/etc/init.d$ |
```

Una vez hecho todo nos iremos al cliente y le pondremos la ip y la puerta de enlace correspondiente



Para comprobar si todo funciona nos debería de dar internet así que hacemos cualquier búsqueda y nos debería de funcionar

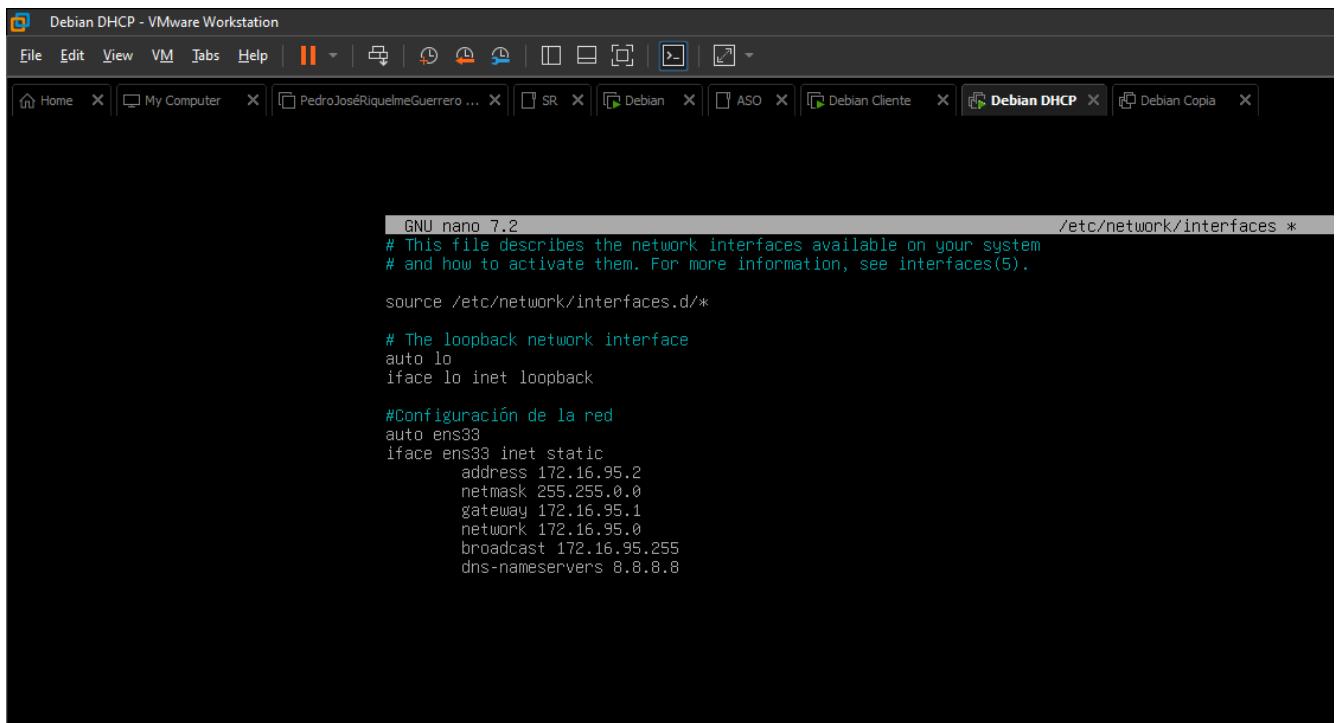


En caso de que no nos funcione podemos probar a ejecutar lo siguiente
`sudo ip route add default via <IP DEL ROUTER>`
`sudo ip route add default via 172.16.95.254`

2. Configuración DHCP

DHCP	
Adaptadores de red	Red Interna 172.16.95.12

Para la configuración del DHCP necesitaremos otra máquina debian la cual le configuraremos la ip



```
GNU nano 7.2                               /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

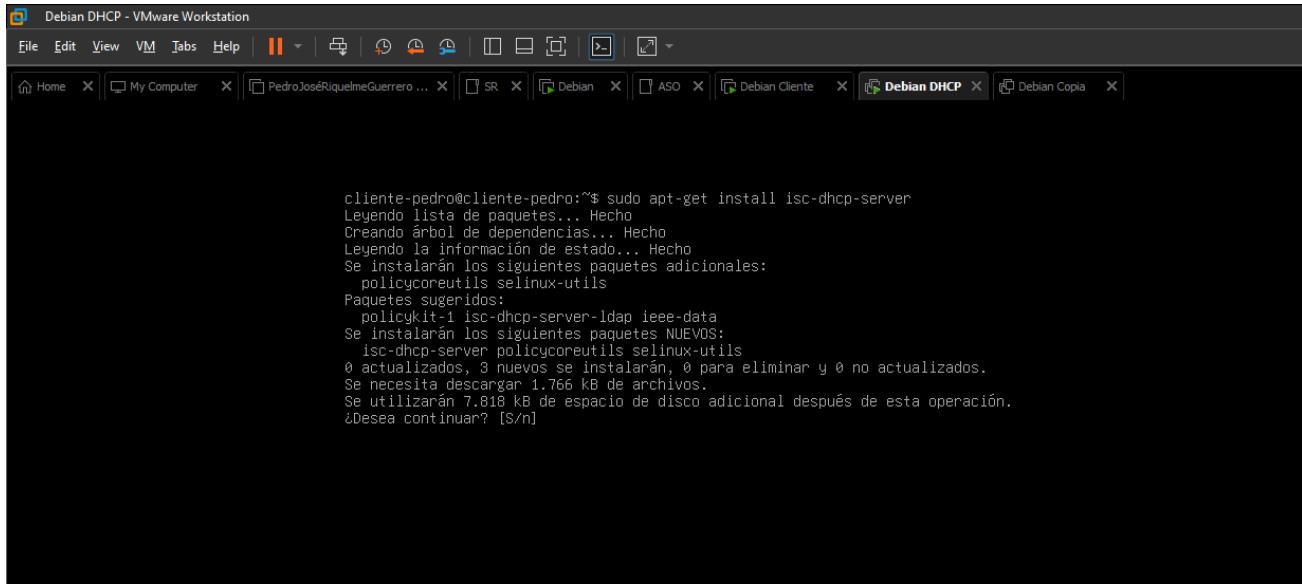
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

#Configuración de la red
auto ens33
iface ens33 inet static
    address 172.16.95.2
    netmask 255.255.0.0
    gateway 172.16.95.1
    network 172.16.95.0
    broadcast 172.16.95.255
    dns-nameservers 8.8.8.8
```

Una vez configurada la ip y comprobar que tenemos internet instalaremos el isc-dhcp-server.

`sudo apt-get install isc-dhcp-server`

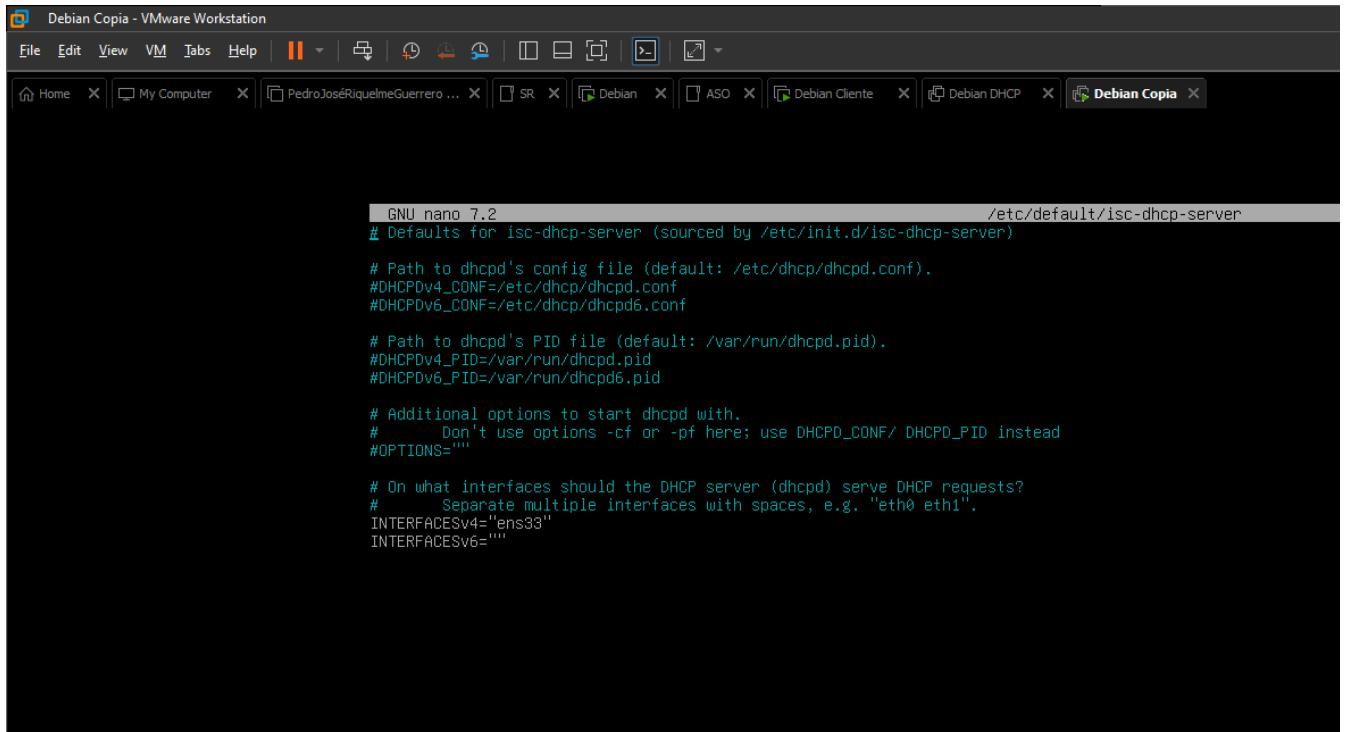


```
cliente-pedro@cliente-pedro:~$ sudo apt-get install isc-dhcp-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Legendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  policycoreutils selinux-utils
Paquetes sugeridos:
  policykit-1 isc-dhcp-server-ldap ieee-data
Se instalarán los siguientes paquetes NUEVOS:
  isc-dhcp-server policycoreutils selinux-utils
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.766 kB de archivos.
Se utilizarán 7.818 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Cambiaremos la configuración del fichero /etc/default/isc-dhcp-server y donde pone INTERFACESv4 se quedará tal que:

INTERFACESv4="ens33"

INTERFACESv6=""



```
GNU nano 7.2 /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpcd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpcd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpcd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDv4_PID=/var/run/dhcpcd.pid
#DHCPDv6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""
```

IMPORTANTE

Comando para verificar errores de sintaxis en el archivo DHCP “dhcpd -t”

Una vez configurado tendremos que modificar el fichero /etc/dhcp/dhcp.conf al cual le tendremos que poner

```
subnet 172.16.95.0 netmask 255.255.255.0 {
```

```
    range 172.16.95.20 172.16.95.30;  
    option subnet-mask 255.255.255.0;  
    option routers 172.16.95.254;  
    option domain-name-servers 8.8.8.8;  
    default-lease-time 86400;  
    max-lease-time 691200;  
    min-lease-time 3600;
```

```
}
```



```
GNU nano 7.2                               /etc/dhcp/dhcpd.conf  
# dhcpcd.conf  
# Sample configuration file for ISC dhcpcd  
  
# option definitions common to all supported networks...  
option domain-name "example.org";  
option domain-name-servers ns1.example.org, ns2.example.org;  
default-lease-time 600;  
max-lease-time 7200;  
  
# The ddns-updates-style parameter controls whether or not the server will  
# attempt to do a DNS update when a lease is confirmed. We default to the  
# behavior of the ISC dhcpcd 2 packages ('none', since dhcpcd vs didn't  
# have support for DDNS).  
ddns-update-style none;  
  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
#authoritative;  
  
# Use this to send dhcpcd log messages to a different log file (you also  
# have to hack sysvinit.conf to complete the redirection).  
#log-facility local;  
  
# No service will be given on this subnet, but declaring it helps the  
# dhcpcd server to understand the network topology.  
subnet 172.16.95.0 netmask 255.255.255.0 {  
    range 172.16.95.20 172.16.95.30;  
    option subnet-mask 255.255.255.0;  
    option routers 172.16.95.254;  
    option domain-name-servers 8.8.8.8;  
    default-lease-time 86400;  
    max-lease-time 691200;  
    min-lease-time 3600;  
}  
#subnet 10.152.107.0 netmask 255.255.255.0 {  
#}  
  
# This is a very basic subnet declaration.  
#subnet 10.254.239.0 netmask 255.255.255.224 {  
#    range 10.254.239.10 10.254.239.20;  
#    option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;  
#}
```

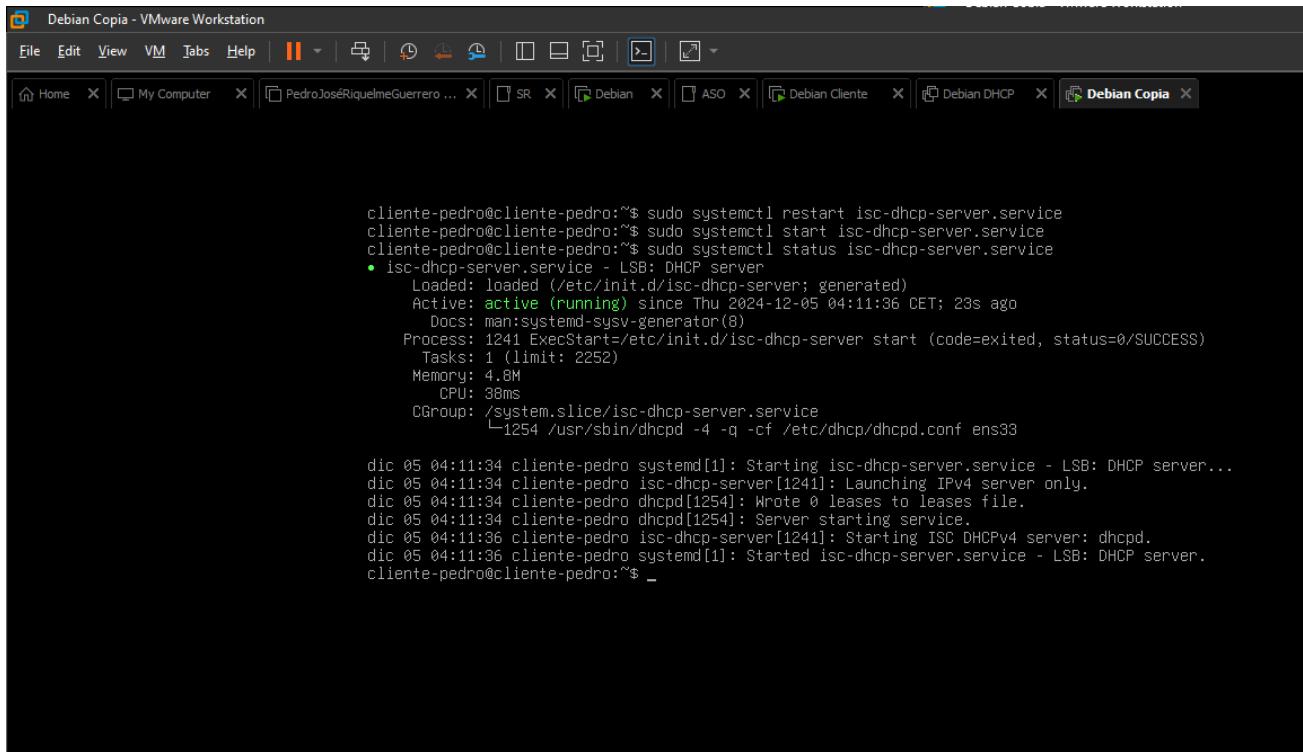
To direct input to this VM, click inside or press Ctrl+G.

Comprobamos que todo funcione correctamente con:

`sudo systemctl restart isc-dhcp-server.service`

`sudo systemctl start isc-dhcp-server.service`

`sudo systemctl status isc-dhcp-server.service`



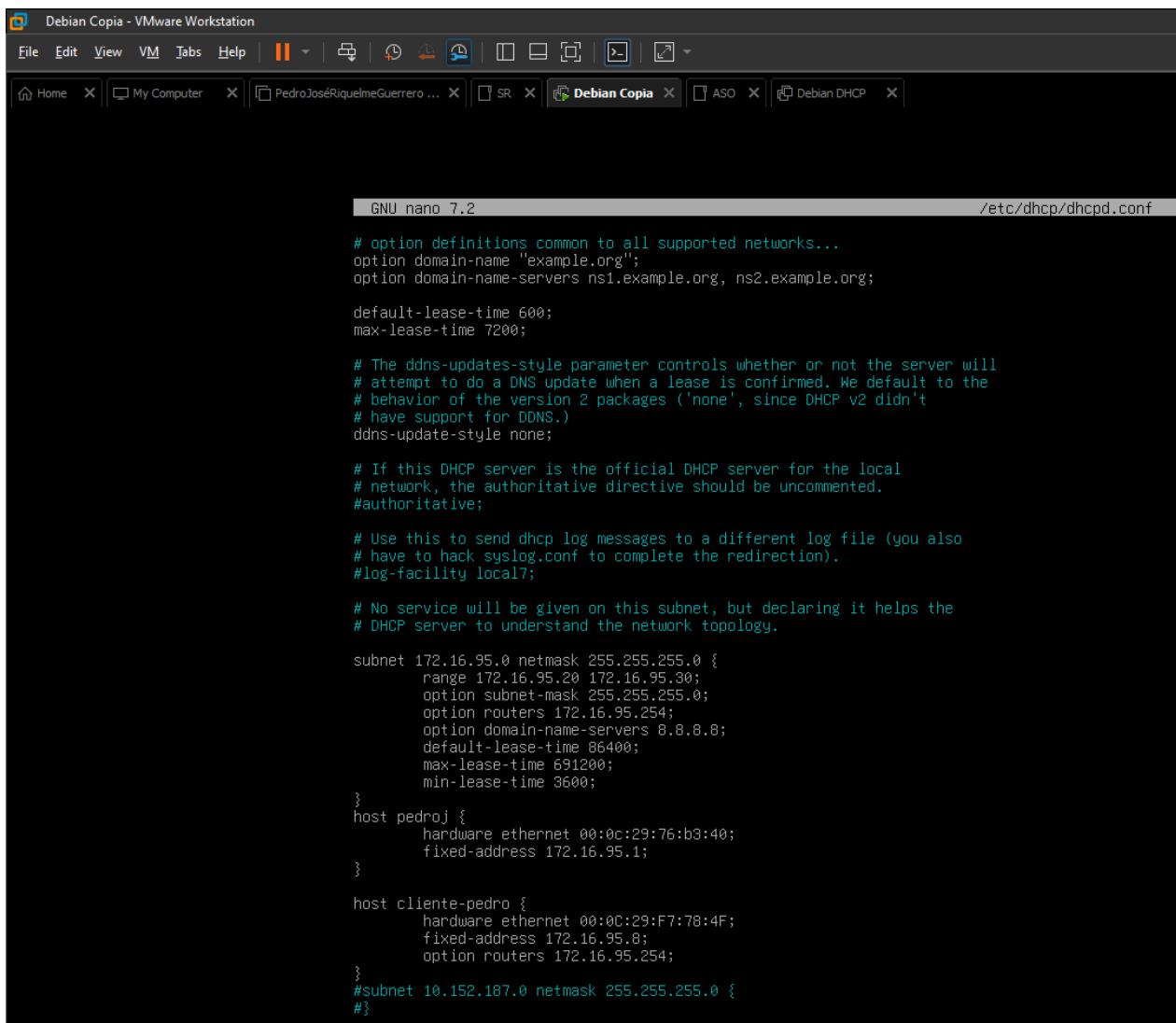
```
cliente-pedro@cliente-pedro:~$ sudo systemctl restart isc-dhcp-server.service
cliente-pedro@cliente-pedro:~$ sudo systemctl start isc-dhcp-server.service
cliente-pedro@cliente-pedro:~$ sudo systemctl status isc-dhcp-server.service
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Thu 2024-12-05 04:11:36 CET; 23s ago
     Docs: man:systemd-sysv-generator(8)
 Process: 1241 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   Tasks: 1 (limit: 2252)
    Memory: 4.8M
      CPU: 38ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─1254 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens33

dic 05 04:11:34 cliente-pedro systemd[1]: Starting isc-dhcp-server.service - LSB: DHCP server...
dic 05 04:11:34 cliente-pedro isc-dhcp-server[1241]: Launching IPv4 server only.
dic 05 04:11:34 cliente-pedro dhcpcd[1254]: Wrote 0 leases to leases file.
dic 05 04:11:34 cliente-pedro dhcpcd[1254]: Server starting service.
dic 05 04:11:36 cliente-pedro isc-dhcp-server[1241]: Starting ISC DHCPv4 server: dhcpd.
dic 05 04:11:36 cliente-pedro systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.
cliente-pedro@cliente-pedro:~$ _
```

Una vez viendo que todo funciona correctamente volveremos a modificar el archivo /etc/dhcp/dhcpd.conf y le meteremos debajo de lo que ya escribimos lo siguiente:

```
host pedroj {  
    hardware ethernet 00:0c:29:76:b3:40;  
    fixed-address 172.16.95.1;  
}
```

```
host cliente-pedro {  
    hardware ethernet 00:0C:29:F7:78:4F;  
    fixed-address 172.16.95.8;  
    option routers 172.16.95.254;  
}
```



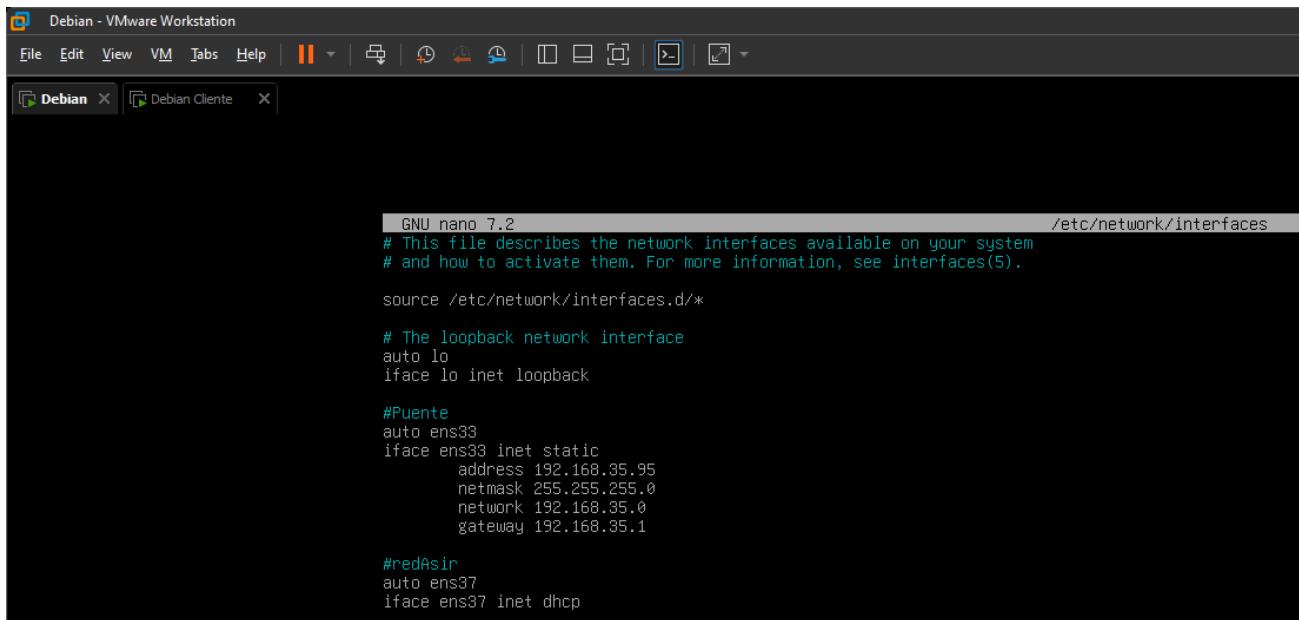
```
GNU nano 7.2 /etc/dhcp/dhcpd.conf  
  
# option definitions common to all supported networks...  
option domain-name "example.org";  
option domain-name-servers ns1.example.org, ns2.example.org;  
  
default-lease-time 600;  
max-lease-time 7200;  
  
# The ddns-updates-style parameter controls whether or not the server will  
# attempt to do a DNS update when a lease is confirmed. We default to the  
# behavior of the version 2 packages ('none', since DHCP v2 didn't  
# have support for DDNS.)  
ddns-update-style none;  
  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
#authoritative;  
  
# Use this to send dhcp log messages to a different log file (you also  
# have to hack syslog.conf to complete the redirection).  
#log-facility local7;  
  
# No service will be given on this subnet, but declaring it helps the  
# DHCP server to understand the network topology.  
  
subnet 172.16.95.0 netmask 255.255.255.0 {  
    range 172.16.95.20 172.16.95.30;  
    option subnet-mask 255.255.255.0;  
    option routers 172.16.95.254;  
    option domain-name-servers 8.8.8.8;  
    default-lease-time 86400;  
    max-lease-time 691200;  
    min-lease-time 3600;  
}  
host pedroj {  
    hardware ethernet 00:0c:29:76:b3:40;  
    fixed-address 172.16.95.1;  
}  
  
host cliente-pedro {  
    hardware ethernet 00:0C:29:F7:78:4F;  
    fixed-address 172.16.95.8;  
    option routers 172.16.95.254;  
}  
#subnet 10.152.187.0 netmask 255.255.255.0 {  
#}
```

Ahora nos iremos tanto al router como al cliente y escribiremos:

auto ens37

iface ens37 inet dhcp

y comprobaremos si nos da la ip que le hemos indicado anteriormente.



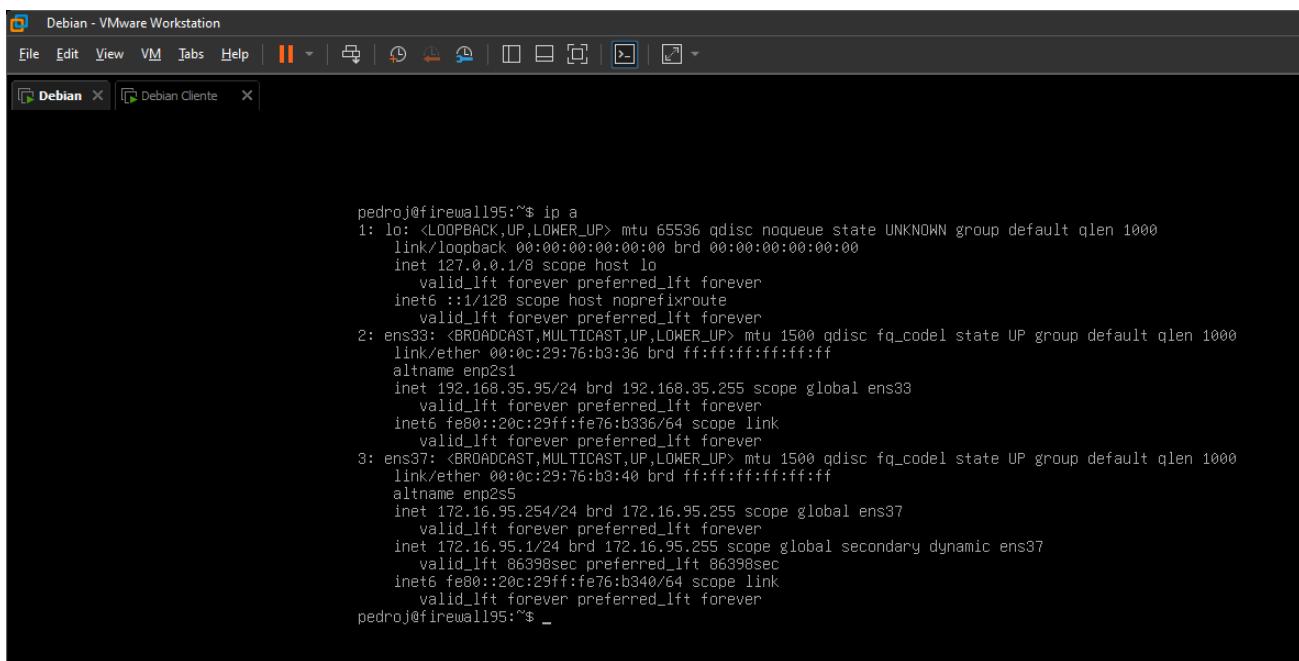
```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

#Puente
auto ens33
iface ens33 inet static
    address 192.168.35.95
    netmask 255.255.255.0
    network 192.168.35.0
    gateway 192.168.35.1

#redAsir
auto ens37
iface ens37 inet dhcp
```



```
pedroj@firewall95:~$ 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 noprefixroute
                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:29:76:b3:36 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.35.95/24 brd 192.168.35.255 scope global ens33
            valid_lft forever preferred_lft forever
            inet6 fe80::20c:29ff:fe76:b336/64 scope link
                valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:76:b3:40 brd ff:ff:ff:ff:ff:ff
        altname enp2s5
        inet 172.16.95.254/24 brd 172.16.95.255 scope global ens37
            valid_lft forever preferred_lft forever
            inet 172.16.95.1/24 brd 172.16.95.255 scope global secondary dynamic ens37
                valid_lft 86398sec preferred_lft 86398sec
                inet6 fe80::20c:29ff:fe76:b340/64 scope link
                    valid_lft forever preferred_lft forever
pedroj@firewall95:~$ _
```

```
GNU nano 7.2 /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

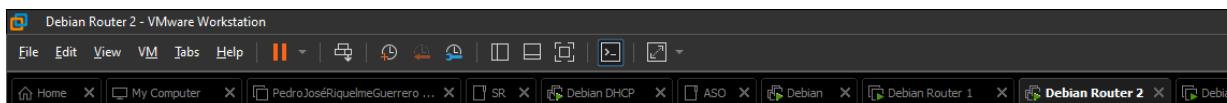
#RedInterna
allow-hotplug ens37
iface ens37 inet dhcp
```

```
cliente-pedro@cliente-pedro:~$ 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f7:78:4f brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 172.16.95.10/16 brd 172.16.255.255 scope global noprefixroute ens37
        valid_lft forever preferred_lft forever
    inet 172.16.95.8/24 brd 172.16.95.255 scope global dynamic ens37
        valid_lft 86350sec preferred_lft 86350sec
    inet6 fe80::20c:29ff:fe7:784f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
cliente-pedro@cliente-pedro:~$
```

3. DHCP Relay

DHCP Relay		
Router	Adaptadores	Red Interna 192.168.35.65 Adaptador Puente 172.16.65.254
DHCP Relay	Adaptadores	Red Interna 172.16.65.13
Cliente	Adaptadores	Red Interna 172.16.65.8

Crearemos un router nuevo para hacer el relay. esta vez la configuración del router va a ser la misma pero con -30 a mi ip así que se quedaría como 192.168.35.65 y la 172.16.65.1



```
GNU nano 7.2                               /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

#Puente
auto ens38
iface ens38 inet static
    address 192.168.35.65
    netmask 255.255.255.0
    network 192.168.35.0
    gateway 192.168.35.1

#redAsir
auto ens37
iface ens37 inet static
    address 172.16.65.254
    netmask 255.255.255.0
    network 172.16.65.0
```

```

pedroj@firewall195:~$ ip link
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 noprefixroute
                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:f5:20:1d brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        altname ens33
        inet 192.168.35.65/24 brd 192.168.35.255 scope global ens33
            valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:feff:1d%ens33 brd ff:ff:ff:ff:ff:ff scope link
            valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f5:20:27 brd ff:ff:ff:ff:ff:ff
        altname enp2s5
        altname ens37
        inet 172.16.65.254/24 brd 172.16.65.255 scope global ens37
            valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:feff:20%ens37 brd ff:ff:ff:ff:ff:ff scope link
            valid_lft forever preferred_lft forever
pedroj@firewall195:~$ _

```

En el iptables tendremos que modificar las ip y poner al que tenemos nosotros actualmente:

```

#!/bin/sh
# Provides: reenvioiptables.sh
# Required-Start: $all
# Required-Stop: $all
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: Firewall para red interna.
# Description: Daemon para hacer funcionar la maquina como firewall usando iptables.
### END INIT INFO

#BORRA LAS REGLAS QUE HAYA
iptables -F
iptables -X
iptables -Z
iptables -t nat -Z
iptables -t mangle -Z

#POLITICA POR DEFECTO
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t mangle -P PREROUTING ACCEPT
iptables -t mangle -P POSTROUTING ACCEPT

#ACEPTAMOS ACCESO LOCALHOST
iptables -A INPUT -i lo -j ACCEPT
#PERMITIMOS ACCESO DESDE LA RED LOCAL
iptables -A INPUT -s 172.16.65.0/24 -j ACCEPT
#ENMASCARAMOS RED LOCAL
iptables -t nat -A POSTROUTING -s 172.16.65.0/24 -o ens33 -j MASQUERADE
#ACTIVAMOS BIT FORWARD
echo 1 > /proc/sys/net/ipv4/ip_forward
#PERMITIMOS ACCESO AL PUERTO 22 (SSH)
iptables -A INPUT -s 0.0.0.0/0 -i ens33 -p tcp --dport 22 -j ACCEPT
#REDIRECCIONAMOS PUERTOS
iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 2201 -j DNAT --to 172.16.65.2:22
iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 3389 -j DNAT --to 172.16.65.3:3389
iptables -t nat -A PREROUTING -i ens33 -p udp --dport 3389 -j DNAT --to 172.16.65.3:3389
#CERRAMOS LOS PUERTOS BIEN CONOCIDOS
iptables -A INPUT -s 0.0.0.0/0 -i ens33 -p tcp --dport 1:1024 -j DROP
iptables -A INPUT -s 0.0.0.0/0 -i ens33 -p udp --dport 1:1024 -j DROP_

```

At the bottom of the terminal window, there is a menu bar with options like Ayuda, Guardar, Buscar, Cortar, Ejecutar, Ubicación, Deshacer, Poner marca, A Llave, Leer fich., Reemplazar, Pegar, Justificar, Ir a línea, Rehacer, Copiar, Buscar atrás, and Siguiente.

```

GNU nano 7.2                               /etc/systemd/system/reenvioiptables.service
[Unit]
Description=firewall para red interna
After=network.target

[Service]
Type=oneshot
ExecStart=/etc/init.d/reenvioiptables.sh
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target

```

To direct input to this VM, click inside or press Ctrl+G.

Una vez configurado tendremos que ejecutarlo todo como hicimos con el primer router

```

pedroj@firewall195:~$ cd /etc/init.d
pedroj@firewall195:/etc/init.d$ sudo chmod +x reenvioiptables.sh
pedroj@firewall195:/etc/init.d$ sudo ./reenvioiptables.sh
pedroj@firewall195:/etc/init.d$

```

Para el DHCP Relay le cambiaremos el hostname y le pondremos dhcp65

```

GNU nano 7.2                               /etc/hostname *
dhcp65

```

Le pondremos la siguiente configuración a el dhcp relay

Debian DHCP 2 [Corriendo] - Oracle VirtualBox

```
Archivo Máquina Ver Entrada Dispositivos Ayuda

GNU nano 7.2 /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

#Configuracion de la red
auto enp0s3
iface enp0s3 inet static
    address 172.16.65.18
    netmask 255.255.255.0
    gateway 172.16.65.1
    network 172.16.65.0
    broadcast 172.16.65.255
    dns-nameservers 192.168.35.1
```

Una vez configurada la ip del dhcp instalaremos el dhcp-relay-server
sudo apt install isc-dhcp-relay

```
cliente-pedro@cliente-pedro:~$ 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 ::/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:dd:58:02 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.35.65/24 brd 192.168.35.255 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fedd:5802/64 scope link
        valid_lft forever preferred_lft forever
cliente-pedro@cliente-pedro:~$ sudo apt install isc-dhcp-relay
Legendando lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Legendando la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  isc-dhcp-relay
0 actualizados, 1 nuevo se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.089 kB de archivos.
Se utilizarán 2.943 kB de espacio de disco adicional después de esta operación.
0% [Conectando a deb.debian.org]_
```

Una vez instalado nos empezará a pedir cosas y le pondremos las siguientes direcciones ip

```
pedroj@firewall95:~$ sudo apt install isc-dhcp-relay
Leyendo lista de paquetes... Hecho
Cargando información de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  isc-dhcp-relay
  o los siguientes se instalarán, o para eliminar y o no actualizados.
  Se necesita descargar 1.089 kB de archivos.
  Se utilizarán 2.943 kB de espacio de disco adicional después de esta operación.
  Descripción http://deb.debian.org/debian/bookworm/main amd64 isc-dhcp-relay amd64 4.4.3-PI-2 [1.089 kB]
  Preconfigurando paquetes ...
  DHCP Relay
  -----
  Se debe especificar el nombre o dirección IP de, al menos, un servidor de DHCP al que se deben redirigir las peticiones DHCP o BOOTP.
  Puede especificar más de un nombre de servidor o dirección IP (en una lista separada con espacios).
  Servidores de DHCP a los que el repetidor de DHCP debería dirigir las peticiones: 192.168.35.95
  Introduzca los nombres de la/s interfaz/es de red en el que el repetidor de DHCP debería intentar configurar. Puede indicar más de un nombre de interfaz con en una lista separada por espacios.
  Si quiere que el repetidor de DHCP realice una detección y configuración automática de las interfaces de red, deje este campo en blanco. En este caso sólo se utilizarán interfaces de difusión (si es posible).
  Interfaces de red en las que debe escuchar el servidor de DHCP: enp0s3
  Especifique cualquier opción adicional que desee utilizar en el demonio repetidor de DHCP.
  Por ejemplo: <-m reemplaza o <-a -D.
  Opciones adicionales para el demonio repetidor de DHCP: -
```

Una vez configurado eso nos iremos a el iptables del router primero que configuramos y añadiremos las dos siguientes líneas:

iptables -t nat -A PREROUTING -i enp0s3 -p udp -- dport 67 - i DNAT -- to 172.

16.95.12:67

ip route add 172.16.65.0/24 via 192.168.35.65 dev enp0s3

```
pedroj@firewall95:~$ /etc/init.d/reenvioiptables.sh
GNU nano 7.2
# Short-Description: Firewall para red interna.
# Description: Daemon para hacer funcionar la maquina como firewall usando iptables.
## END INIT INFO

#BORRA LAS REGLAS QUE HAYA
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

#POLITICA POR DEFECTO
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

#ACEPTAMOS ACCESO LOCALHOST
iptables -A INPUT -i lo -j ACCEPT

#PERMITIMOS ACCESO DESDE LA RED LOCAL
iptables -A INPUT -s 172.16.95.0/24 -j ACCEPT

#ENMASCARAMOS RED LOCAL
iptables -t nat -A POSTROUTING -s 172.16.95.0/24 -o enp0s3 -j MASQUERADE

#ACTIVAMOS BIT FORWARD
echo 1 > /proc/sys/net/ipv4/ip_forward

#PERMITIMOS ACCESO AL PUERTO 22 (SSH)
iptables -A INPUT -s 0.0.0.0/0 -i enp0s3 -p tcp --dport 22 -j ACCEPT

#REDIRECCIONAMOS PUERTOS
iptables -t nat -A PREROUTING -i ens3 -p tcp --dport 2201 -j DNAT --to 172.16.95.2:22
iptables -t nat -A PREROUTING -i ens3 -p tcp --dport 3389 -j DNAT --to 172.16.95.3:3389
iptables -t nat -A PREROUTING -i ens3 -p udp --dport 3389 -j DNAT --to 172.16.95.3:3389
iptables -t nat -A PREROUTING -i enp0s3 -p udp --dport 67 -j DNAT --to 172.16.95.12:67
ip route add 172.16.65.0/24 via 192.168.35.65 dev enp0s3

#CERRAMOS LOS PUERTOS BIEN CONOCIDOS
iptables -A INPUT -s 0.0.0.0/0 -i ens3 -p tcp --dport 1:1024 -j DROP

^C Ayuda      ^Q Guardar      ^N Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación      M-U Deshacer      M-A Poner marca      M-L A llave      M-Q Anterior      ^B Atrás
^X Salir      ^R Leer fich.    ^A Reemplazar   ^U Pegar       ^J Justificar    ^/ Ir a línea     M-E Rehacer      M-C Copiar      M-B Buscar atrás   M-W Siguiente     ^F Adelante
```

Ahora para el router 2 ponemos en el iptables:

ip del dhcp relay:172.16.65.13:67

red del DHCP1:172.16.95.0/24

ip del router (adaptador puente):192.168.35.95

iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 67 -j DNAT --to 172.16.65.13:67

ip route add 172.16.95.0/24 via 192.168.35.95 dev enp0s3

The screenshot shows a terminal window with the following content:

```
GNU nano 7.2
### BEGIN INIT INFO
# Provides: reenvioiptables.sh
# Required-Start: $all
# Required-Stop: $all
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: Firewall para red interna.
# Description: Daemon para hacer funcionar la maquina como firewall usando iptables.
### END INIT INFO

#BORRA LAS REGLAS QUE HAYA
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

#POLITICA POR DEFECTO
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

#ACEPTAMOS ACCESO LOCALHOST
iptables -A INPUT -i lo -j ACCEPT

#PERMITIMOS ACCESO DESDE LA RED LOCAL
iptables -A INPUT -s 172.16.95.0/24 -j ACCEPT

#ENHACERAMOS RED LOCAL
iptables -t nat -A POSTROUTING -s 172.16.95.0/24 -o enp0s3 -j MASQUERADE

#ACTIVAMOS BIT FORWARD
echo 1 > /proc/sys/net/ipv4/ip_forward

#PERMITIMOS ACCESO AL PUERTO 22 (SSH)
iptables -A INPUT -s 0.0.0.0/0 -i enp0s3 -o tcp --dport 22 -j ACCEPT

#REDIRECCIONAMOS PUERTOS
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 2201 -j DNAT --to 172.16.65.2:22
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 3389 -j DNAT --to 172.16.65.3:3389
iptables -t nat -A PREROUTING -i enp0s3 -p udp --dport 3389 -j DNAT --to 172.16.65.3:3389
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 67 -j DNAT --to 172.16.65.13:67

#CERRAMOS LOS PUERTOS BIEN CONOCIDOS
#CERRAMOS LOS PUERTOS BIEN CONOCIDOS
iptables -A INPUT -s 0.0.0.0/0 -i enp0s3 -o tcp --dport 1/1024 -j DROP

#Guardar    Guardar fich.  Buscar  Contar  Ejecutar  Justifican  Ubicación  Deshacer  Poner marca  A Llave  Borrar  Buscar atrás  Siguiente
S Salir  Guardar  Buscar  Contar  Ejecutar  Justifican  Ubicación  Deshacer  Poner marca  A Llave  Borrar  Buscar atrás  Siguiente
```

Comprobamos que está todo bien con route show

The screenshot shows a terminal window with the following content:

```
pedroj@firewall165:/etc/init.d$ sudo chmod +x reenvioiptables.sh
[sudo] contraseña para pedroj:
pedroj@firewall165:/etc/init.d$ sudo ./reenvioiptables.sh
pedroj@firewall165:/etc/init.d$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT    all  --  anywhere        anywhere
ACCEPT    all  --  172.16.95.0/24   anywhere
ACCEPT    tcp  --  anywhere        anywhere          tcp dpt:ssh
DROP      tcp  --  anywhere        anywhere          tcp dpts:tcpmux:1024
DROP      udp  --  anywhere        anywhere          udp dpts:1:1024

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

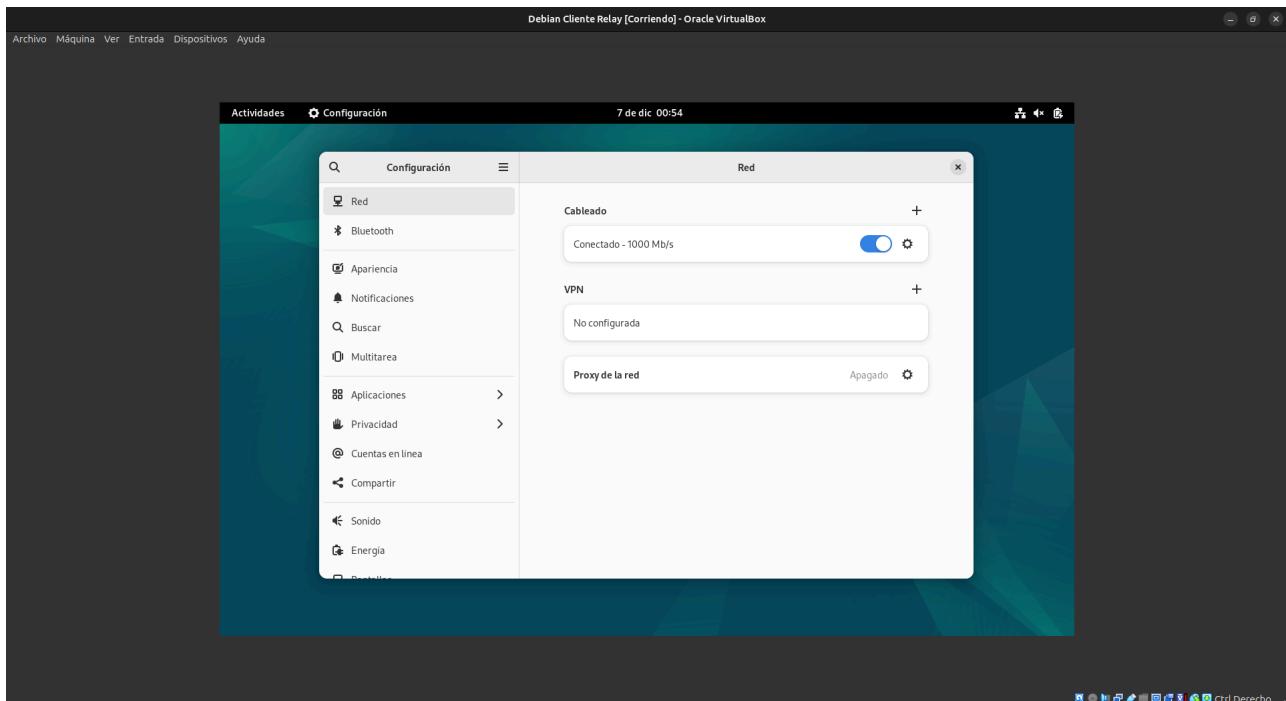
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
pedroj@firewall165:/etc/init.d$ cd
pedroj@firewall165:~$ ip route show
default via 192.168.35.1 dev enp0s8 onlink
169.254.0.0/16 dev enp0s8 scope link metric 1000
172.16.65.0/24 dev enp0s8 proto kernel scope link src 172.16.65.1
172.16.95.0/24 via 192.168.35.95 dev enp0s3
192.168.35.0/24 dev enp0s3 proto kernel scope link src 192.168.35.65
pedroj@firewall165:~$
```

Nos iremos a /etc/dhcp/dhcpd.conf y le pondremos lo siguiente:

```
GNU nano 7.2                                         /etc/dhcp/dhcpd.conf *
```

```
# have support for DDNS.)  
ddns-update-style none;  
  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
#authoritative;  
  
# Use this to send dhcp log messages to a different log file (you also  
# have to hack syslog.conf to complete the redirection).  
#log-facility local7;  
  
# No service will be given on this subnet, but declaring it helps the  
# DHCP server to understand the network topology.  
  
subnet 172.16.95.0 netmask 255.255.255.0 {  
    range 172.16.95.20 172.16.95.30;  
    option subnet-mask 255.255.255.0;  
    option routers 172.16.95.1;  
    option domain-name-servers 8.8.8.8;  
    default-lease-time 86400;  
    max-lease-time 691200;  
    min-lease-time 3600;  
}  
  
#Relay  
subnet 172.16.65.0 netmask 255.255.255.0 {  
    range 172.16.65.20 172.16.65.30;  
    option subnet-mask 255.255.255.0;  
    option routers 172.16.65.1;  
    option domain-name-servers 8.8.8.8;  
    default-lease-time 86400;  
    max-lease-time 691200;  
    min-lease-time 3600;  
}
```

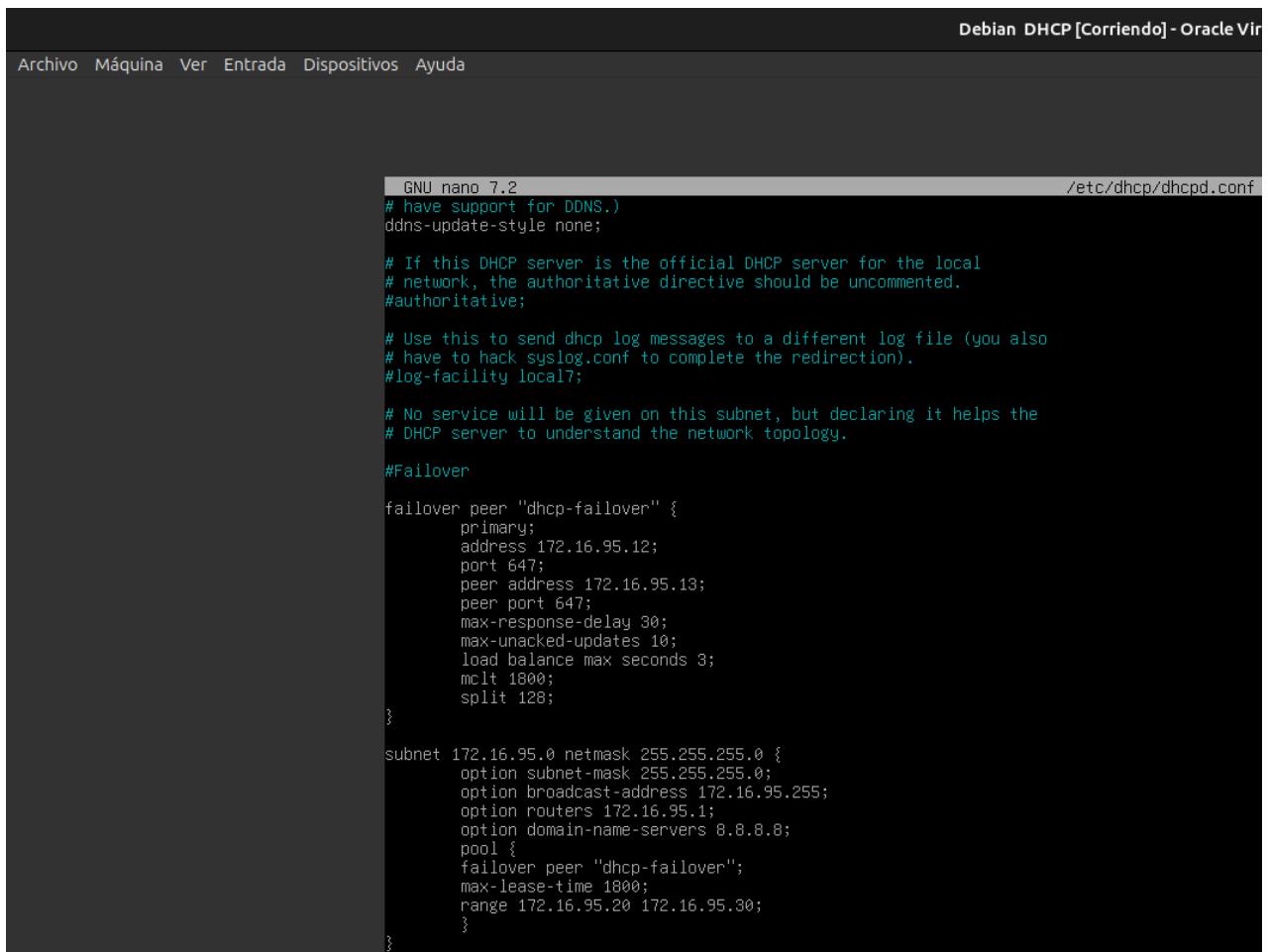
Una vez configurado todo si nos vamos al cliente del relay y todo está bien nos deberá de dar conexión a internet



4. Failover

DHCP Failover	Adaptadores de red	Red Interna 172.16.95.13
Cliente	Adaptadores de red	Red Interna 172.16.95.25

Para configurar el Faylover nos tendremos que ir al primer DHCP que configuramos y nos iremos a su directorio para modificarlo y le tendremos que comentar Relay y añadimos lo siguiente:



The screenshot shows a terminal window titled "Debian DHCP [Corriendo] - Oracle Vir". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The main area displays the contents of the file "/etc/dhcp/dhcpd.conf" using the nano editor. The configuration includes a "Failover" section defining a peer and a subnet declaration.

```
GNU nano 7.2
/etc/dhcp/dhcpd.conf
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#Failover

failover peer "dhcp-failover" {
    primary;
    address 172.16.95.12;
    port 647;
    peer address 172.16.95.13;
    peer port 647;
    max-response-delay 30;
    max-unacked-updates 10;
    load balance max seconds 3;
    mcrlt 1800;
    split 128;
}

subnet 172.16.95.0 netmask 255.255.255.0 {
    option subnet-mask 255.255.255.0;
    option broadcast-address 172.16.95.255;
    option routers 172.16.95.1;
    option domain-name-servers 0.0.0.0;
    pool {
        failover peer "dhcp-failover";
        max-lease-time 1800;
        range 172.16.95.20 172.16.95.30;
    }
}
```

Comprobamos si funciona con un status

```
pedroj@dhcp95:~$ sudo systemctl status isc-dhcp-server.service
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
     Active: active (running) since Sat 2024-12-07 01:24:09 CET; 10s ago
       Docs: man:systemd-sysv-generator(8)
   Process: 1008 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
     Tasks: 1 (limit: 2293)
    Memory: 7.3M
      CPU: 68ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─1021 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf enp0s3

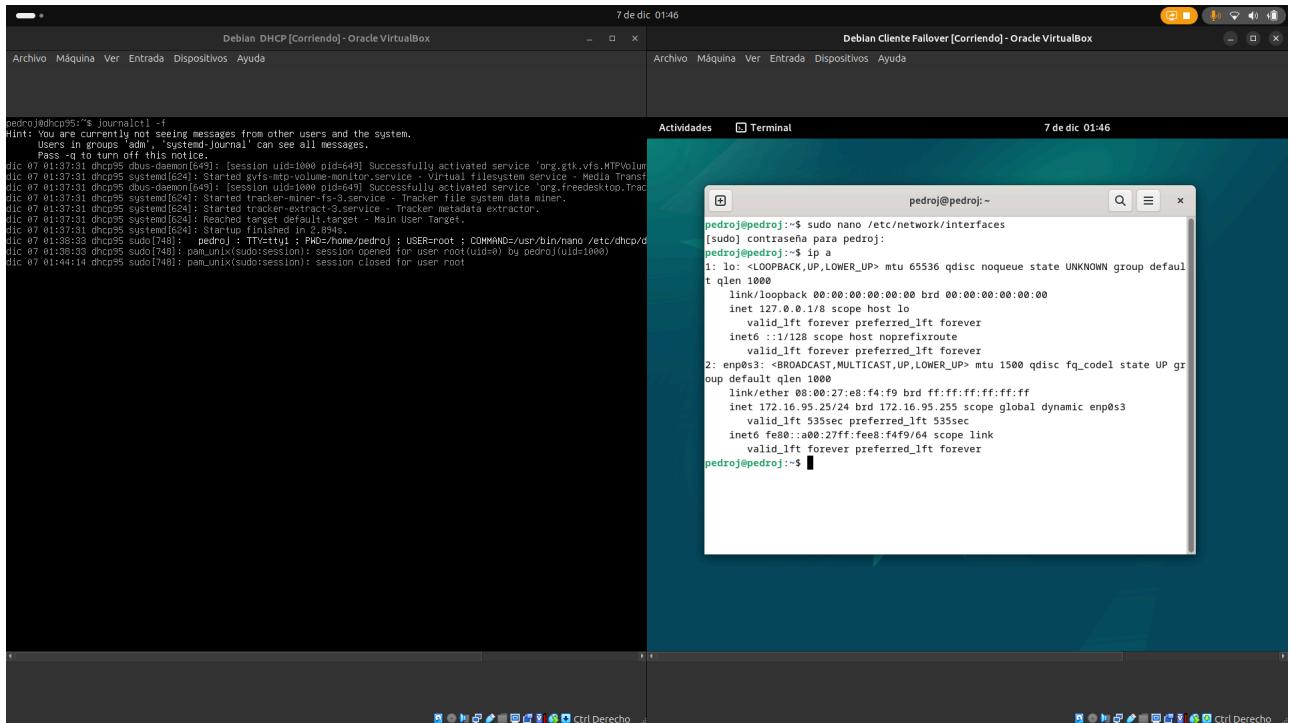
dic 07 01:24:07 dhcp95 systemd[1]: Starting isc-dhcp-server.service - LSB: DHCP server...
dic 07 01:24:07 dhcp95 isc-dhcp-server[1008]: Launching IPv4 server only.
dic 07 01:24:07 dhcp95 dhcpd[1021]: lease 172.16.65.20: no subnet.
dic 07 01:24:07 dhcp95 dhcpd[1021]: Wrote 0 deleted host decls to leases file.
dic 07 01:24:07 dhcp95 dhcpd[1021]: Wrote 0 new dynamic host decls to leases file.
dic 07 01:24:07 dhcp95 dhcpd[1021]: Wrote 1 leases to leases file.
dic 07 01:24:07 dhcp95 dhcpd[1021]: failover peer dhcp-failover: I move from recover to startup
dic 07 01:24:07 dhcp95 dhcpd[1021]: Server starting service.
dic 07 01:24:09 dhcp95 isc-dhcp-server[1008]: Starting ISC DHCPv4 server: dhcpcd.
dic 07 01:24:09 dhcp95 systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.
pedroj@dhcp95:~$ _
```

Ahora nos iremos a la clonación que hicimos del DHCP 1 para poder añadirle lo siguiente:

```
#Failover

failover peer "dhcp-failover" {
    secondary;
    address 172.16.95.13;
    port 647;
    peer address 172.16.95.12;
    peer port 647;
    max-response-delay 30;
    max-unacked-updates 10;
    load balance max seconds 3;
}
```

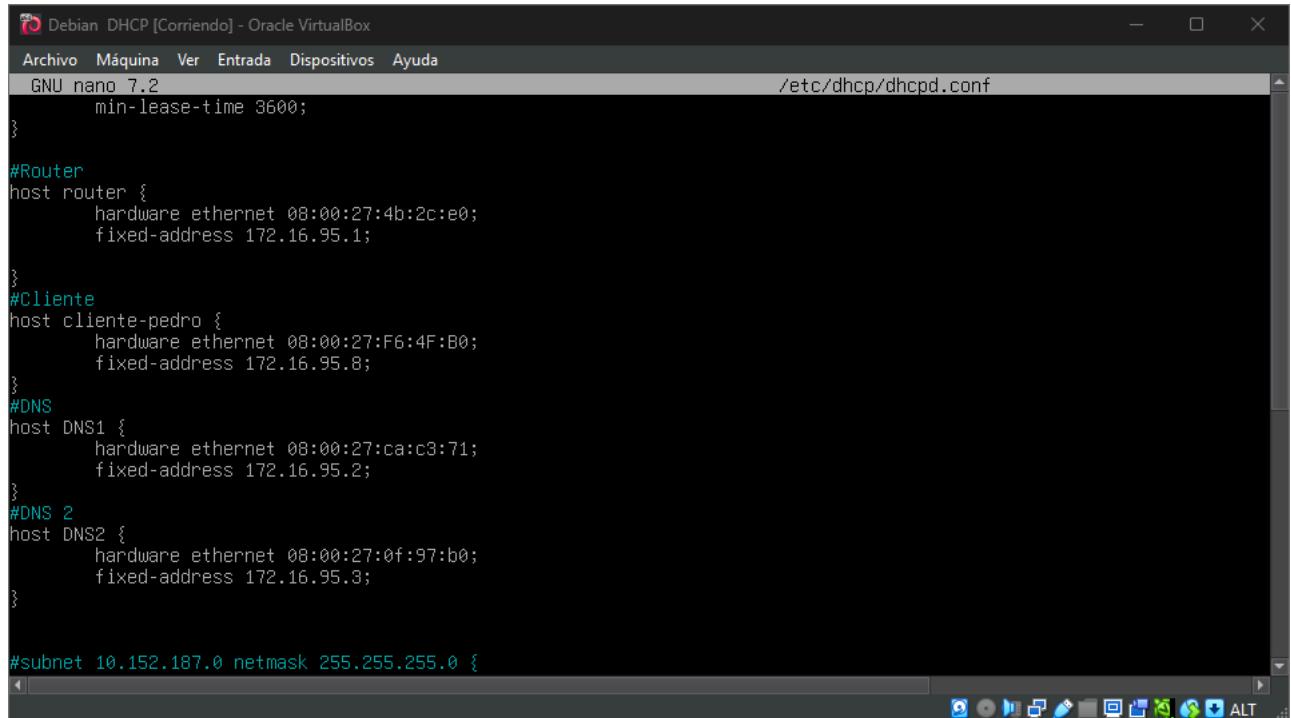
Una vez configuramos todo abriremos el cliente del Failover y vemos si nos da la ip que tenemos dentro del rango establecido, y en mi caso si me la da



5.DNS

DNS1	Adaptadores	172.16.95.2
DNS2	Adaptadores	172.16.95.3

Empezaremos añadiendo en el fichero dhcpd.conf los dns que vamos a usar con las ip que queremos usar



```
Debian DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 7.2                               /etc/dhcp/dhcpd.conf
min-lease-time 3600;
}

#Router
host router {
    hardware ethernet 08:00:27:4b:2c:e0;
    fixed-address 172.16.95.1;
}

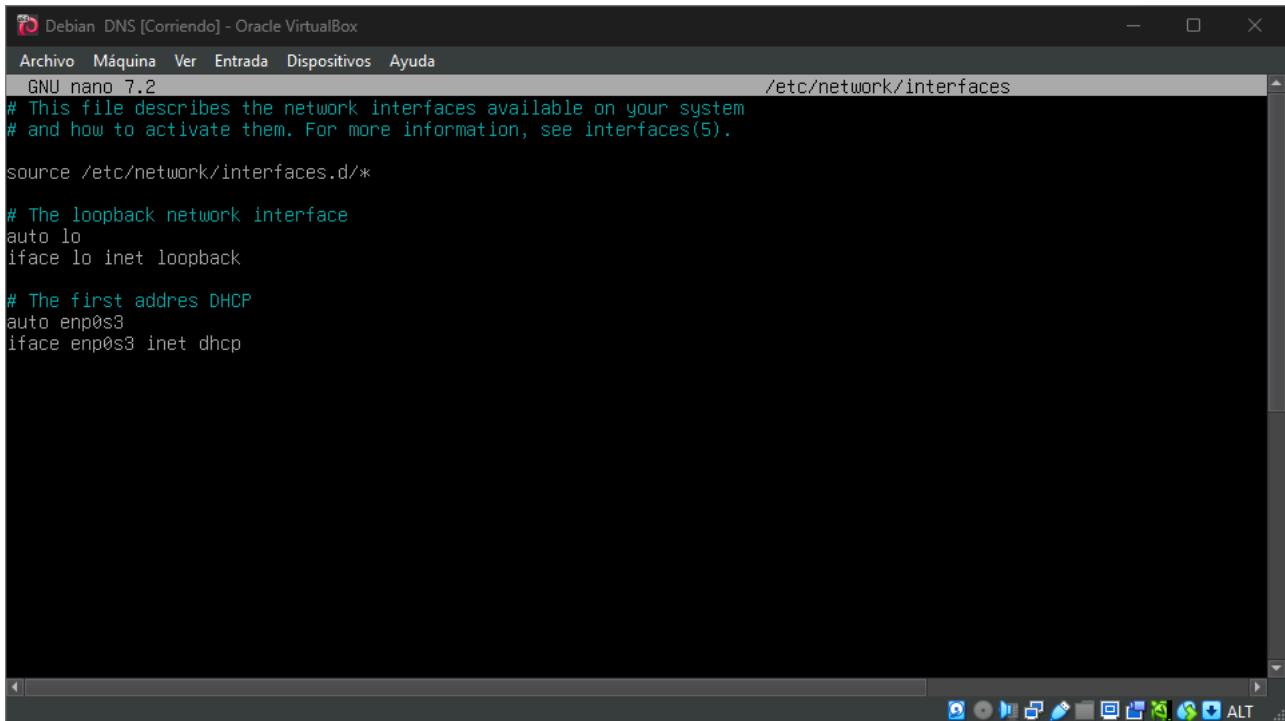
#Cliente
host cliente-pedro {
    hardware ethernet 08:00:27:F6:4F:B0;
    fixed-address 172.16.95.8;
}

#DNS
host DNS1 {
    hardware ethernet 08:00:27:ca:c3:71;
    fixed-address 172.16.95.2;
}

#DNS 2
host DNS2 {
    hardware ethernet 08:00:27:0f:97:b0;
    fixed-address 172.16.95.3;
}

subnet 10.152.187.0 netmask 255.255.255.0 {
```

Cambiaremos la configuración de los adaptadores de red para que coja el dhcp



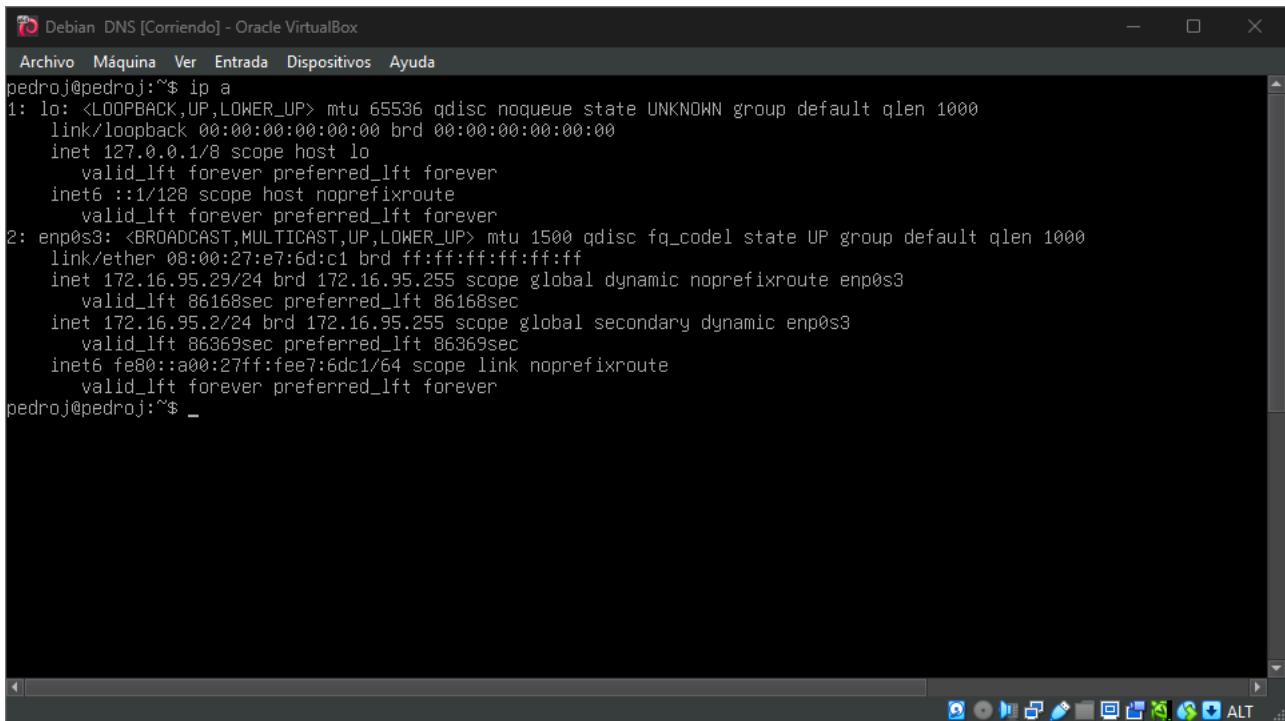
```
Debian DNS [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 7.2
/etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

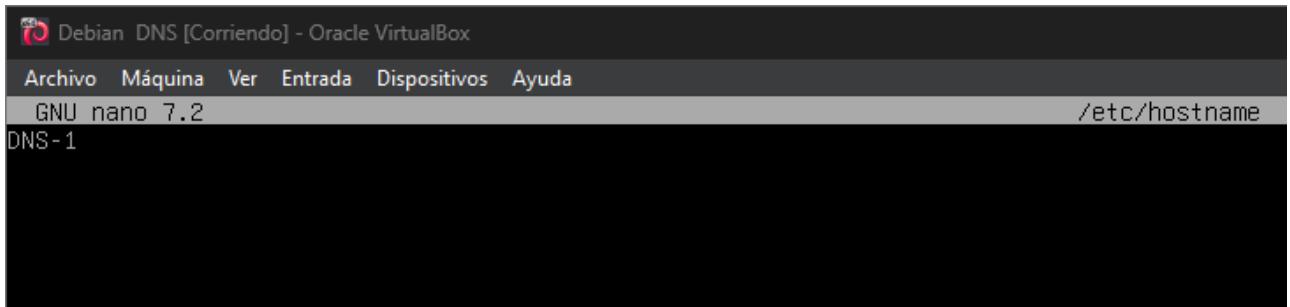
# The first address DHCP
auto enp0s3
iface enp0s3 inet dhcp
```

Si hacemos un ip a nos dará la ip



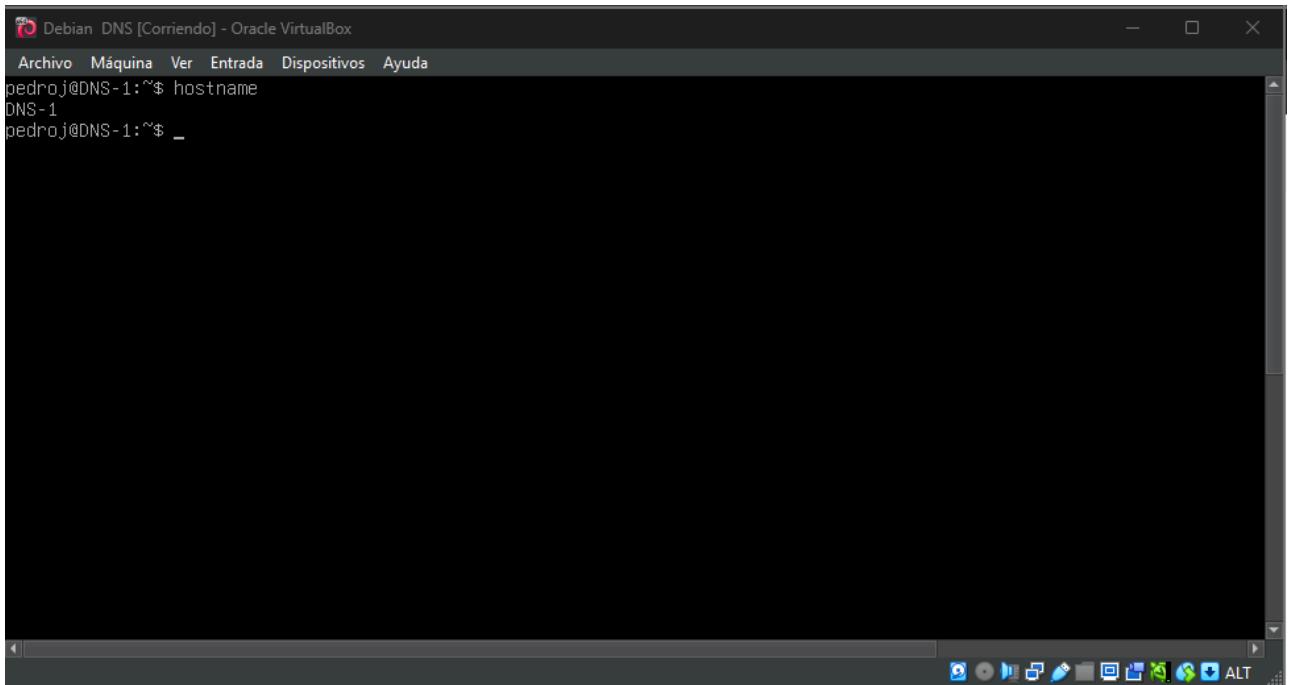
```
Debian DNS [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pedroj@pedroj:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e7:6d:c1 brd ff:ff:ff:ff:ff:ff
        inet 172.16.95.29/24 brd 172.16.95.255 scope global dynamic noprefixroute enp0s3
            valid_lft 86168sec preferred_lft 86168sec
        inet 172.16.95.2/24 brd 172.16.95.255 scope global secondary dynamic enp0s3
            valid_lft 86369sec preferred_lft 86369sec
        inet6 fe80::a00:27ff:fe7e:6dc1/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
pedroj@pedroj:~$ _
```

Cambiamos el hostname de la máquina para aclarar cual es cual.



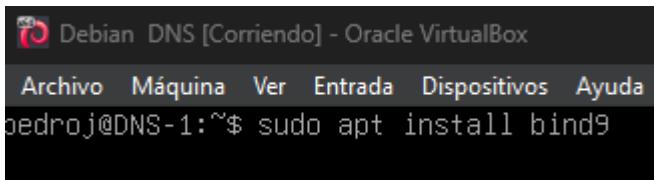
```
Debian DNS [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 7.2 /etc/hostname
DNS-1
```

Comprobamos que nos sale el nombre que hemos puesto



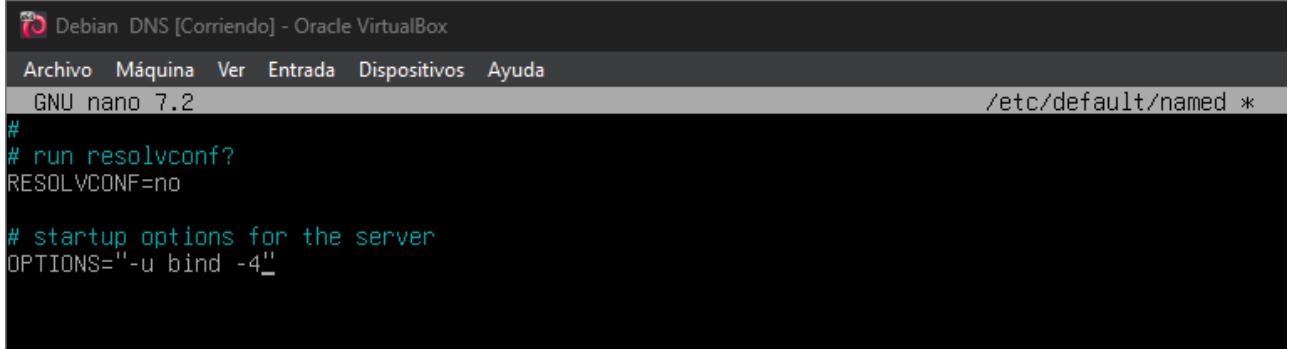
```
Debian DNS [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pedro.j@DNS-1:~$ hostname
DNS-1
pedro.j@DNS-1:~$ _
```

Hacemos un **sudo apt install bind9** para instalar el bind



```
Debian DNS [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pedro.j@DNS-1:~$ sudo apt install bind9
```

sudo apt install bind9-doc dnsutils resolvconf ufw python-ply-doc



```
Debian DNS [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 7.2 /etc/default/named *
#
# run resolvconf?
RESOLVCONF=no

# startup options for the server
OPTIONS="-u bind -4"
```

```

acl "trusted" {
    172.16.95.1; #firewall
    172.16.95.2; # DNS1
    172.16.95.3; # DNS2
    172.16.95.4; # CLIENTE
};

options {
    directory "/var/cache/bind"; # Directorio de caché
    recursion yes; # Habilita la recursividad. Esto significa que en el servidor DNS pu>
    allow-recursion { trusted; }; # Permite que solo los clientes definidos en la ACL "trusted" reali>
    listen-on { 172.16.95.2; }; # Escucha en las IPs de DNS1 Especifica en que direccion IP el
    sefvi> # Privada de tu servidor DNS (en este caso, 'ns1').
    allow-transfer { none; }; # Desactiva las transferencias de zona por defecto. Esto significa >
#Esto significa que otros servidores no podran copias la configuraci>
    forwarders { # Aqui defines servidores DNS a los que se enviaran las consultas qu>
        8.8.8.8; # Servidor DNS de Google
        8.8.4.4; # Otro servidor DNS de Google
    };
    dnssec-validation auto;
};

```

```

GNU nano 7.2                               /etc/bind/named.conf.options
acl "trusted" {
    172.16.95.1; #firewall
    172.16.95.2; # DNS1
    172.16.95.3; # DNS2
    172.16.95.4; # CLIENTE
};

options {
    directory "/var/cache/bind"; # Directorio de caché
    recursion yes; # Habilita la recursividad. Esto significa que en el servidor DNS pu>
    allow-recursion { trusted; }; # Permite que solo los clientes definidos en la ACL "trusted" reali>
    listen-on { 172.16.95.2; }; # Escucha en las IPs de DNS1 Especifica en que direccion IP el
    sefvi> # Privada de tu servidor DNS (en este caso, 'ns1').
    allow-transfer { none; }; # Desactiva las transferencias de zona por defecto. Esto significa >
#Esto significa que otros servidores no podran copias la configuraci>
    forwarders { # Aqui defines servidores DNS a los que se enviaran las consultas qu>
        8.8.8.8; # Servidor DNS de Google
        8.8.4.4; # Otro servidor DNS de Google
    };
    dnssec-validation auto;
};

```

```

//  

// Do any local configuration here  

//  

// Consider adding the 1918 zones here, if they are not used in your  

// organization  

//include "/etc/bind/zones.rfc1918";  

zone "alumno95.com" {  

    type master;  

    file "/etc/bind/zones/db.alumno95.com";  

    allow-transfer {172.16.95.3};  

};  

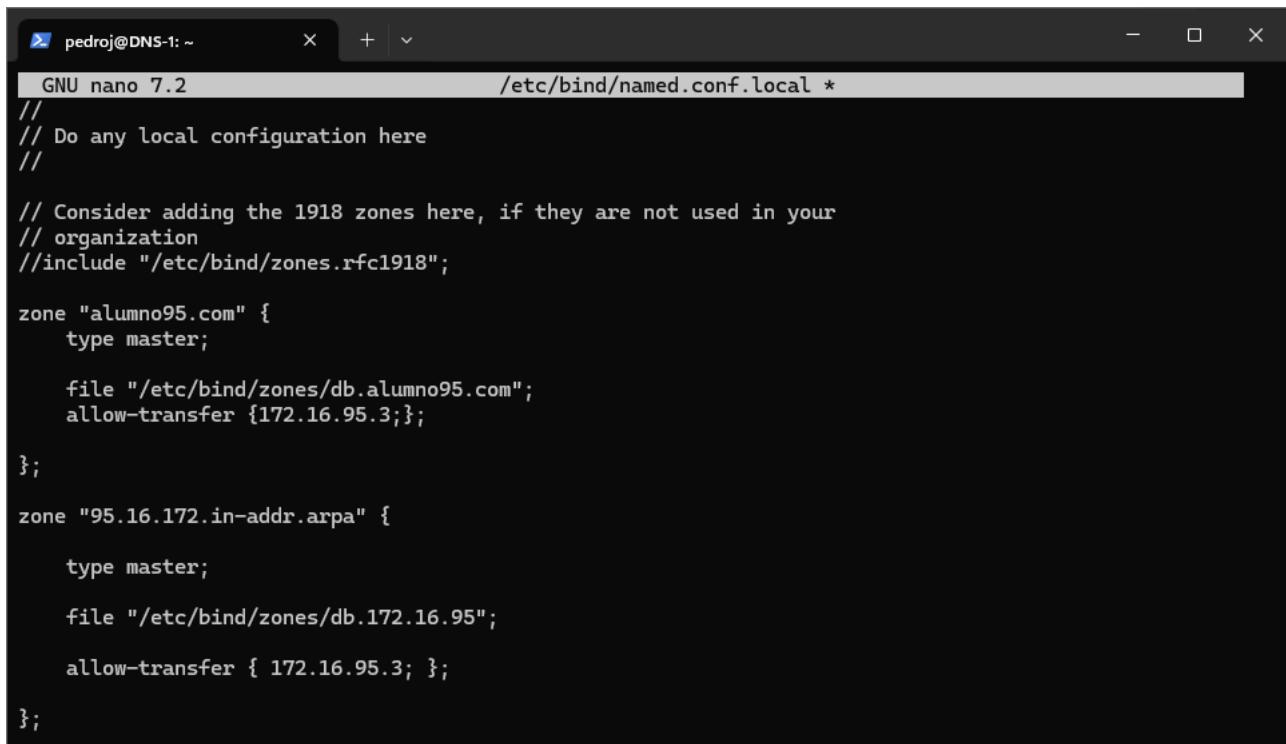
zone "95.16.172.in-addr.arpa" {  

    type master;  

    file "/etc/bind/zones/db.172.16.95";  

    allow-transfer { 172.16.95.3 };  

};
```



The screenshot shows a terminal window titled 'pedroj@DNS-1: ~'. The window contains the contents of the /etc/bind/named.conf.local file, which is being edited in the GNU nano 7.2 text editor. The code is identical to the one shown in the previous code block.

```

GNU nano 7.2          /etc/bind/named.conf.local *
//  

// Do any local configuration here  

//  

// Consider adding the 1918 zones here, if they are not used in your  

// organization  

//include "/etc/bind/zones.rfc1918";  

zone "alumno95.com" {  

    type master;  

    file "/etc/bind/zones/db.alumno95.com";  

    allow-transfer {172.16.95.3};  

};  

zone "95.16.172.in-addr.arpa" {  

    type master;  

    file "/etc/bind/zones/db.172.16.95";  

    allow-transfer { 172.16.95.3 };  

};
```

Para crear la zona deberemos de hacer:

```
sudo mkdir /etc/bind/zones

;

; BIND data file for local loopback interface

;

$TTL 604800

alumno95.com. IN SOA ns1.alumno95.com. admin.alumno95.com. (
    6 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL

;

;

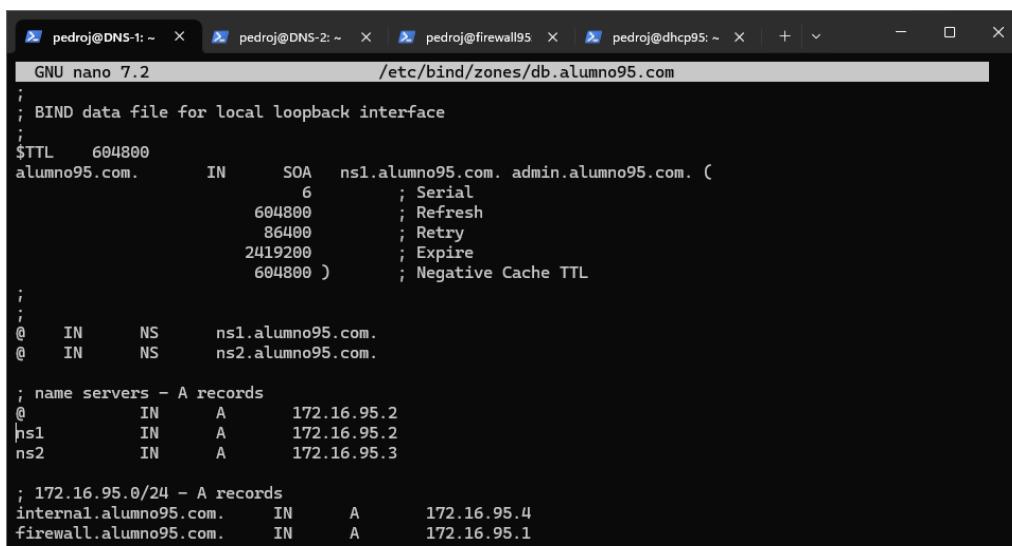
@ IN NS ns1.alumno95.com.
@ IN NS ns2.alumno95.com.

; name servers - A records

@ IN A 172.16.95.2
ns1 IN A 172.16.95.2
ns2 IN A 172.16.95.3

; 172.16.95.0/24 - A records

internal.alumno95.com. IN A 172.16.95.4
firewall.alumno95.com. IN A 172.16.95.1
```



```
GNU nano 7.2 /etc/bind/zones/db.alumno95.com
;

; BIND data file for local loopback interface

;

$TTL 604800

alumno95.com. IN SOA ns1.alumno95.com. admin.alumno95.com. (
    6 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL

;

;

@ IN NS ns1.alumno95.com.
@ IN NS ns2.alumno95.com.

; name servers - A records

@ IN A 172.16.95.2
ns1 IN A 172.16.95.2
ns2 IN A 172.16.95.3

; 172.16.95.0/24 - A records

internal.alumno95.com. IN A 172.16.95.4
firewall.alumno95.com. IN A 172.16.95.1
```

Si hacemos un nslookup a alumno95.com o a pedroj.com nos devolverá la información

```
pedroj@pedroj:~$ nslookup alumno95.com
Server:      172.16.95.2
Address:     172.16.95.2#53

Name:  alumno95.com
Address: 172.16.95.2

pedroj@pedroj:~$ nslookup pedroj.com
Server:      172.16.95.2
Address:     172.16.95.2#53

Non-authoritative answer:
Name:  pedroj.com
Address: 156.226.127.150

pedroj@pedroj:~$ _
```

\$TTL 604800

@ IN SOA ns1.alumno95.com. admin.alumno95.com. (

9 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800) ; Negative Cache TTL

;

; name servers - NS records

IN NS ns1.alumno95.com.

IN NS ns2.alumno95.com.

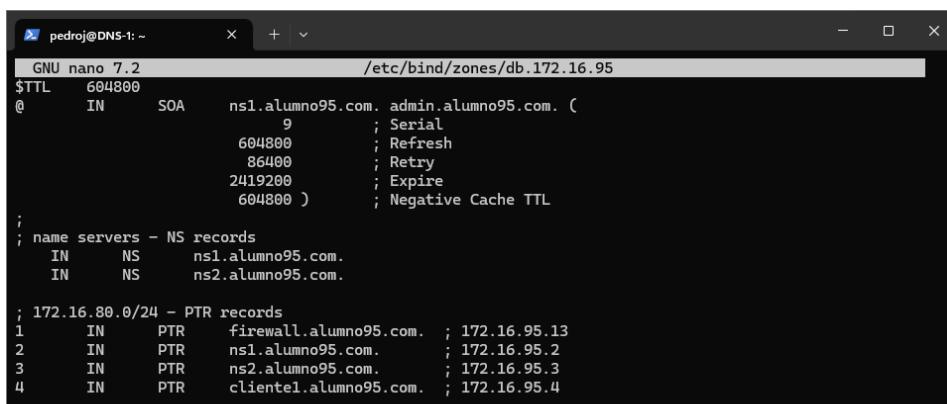
; 172.16.80.0/24 - PTR records

1 IN PTR firewall.alumno95.com. ; 172.16.95.13

2 IN PTR ns1.alumno95.com. ; 172.16.95.2

3 IN PTR ns2.alumno95.com. ; 172.16.95.3

4 IN PTR cliente1.alumno95.com. ; 172.16.95.4



```
GNU nano 7.2          /etc/bind/zones/db.172.16.95
$TTL 604800
@ IN SOA ns1.alumno95.com. admin.alumno95.com. (
        9 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
; name servers - NS records
IN NS ns1.alumno95.com.
IN NS ns2.alumno95.com.

; 172.16.80.0/24 - PTR records
1 IN PTR firewall.alumno95.com. ; 172.16.95.13
2 IN PTR ns1.alumno95.com. ; 172.16.95.2
3 IN PTR ns2.alumno95.com. ; 172.16.95.3
4 IN PTR cliente1.alumno95.com. ; 172.16.95.4
```

Ejecutaremos un check para confirmar que la configuración está bien

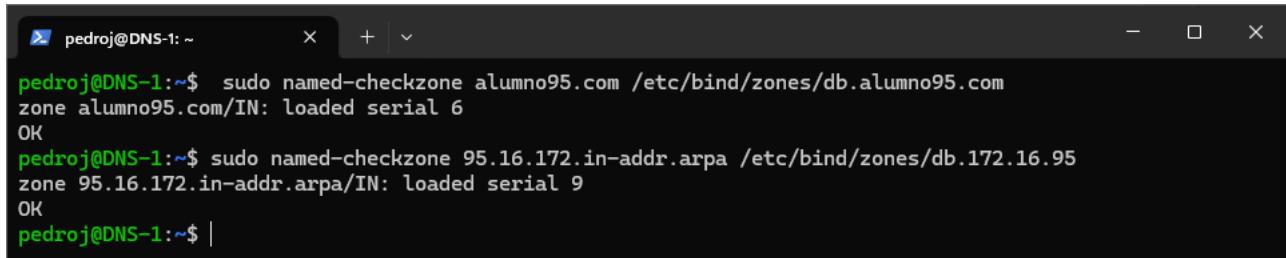
sudo named-checkconf



```
pedroj@DNS-1:~$ sudo named-checkconf
pedroj@DNS-1:~$ |
```

sudo named-checkzone alumno95.com /etc/bind/zones/db.alumno95.com

sudo named-checkzone 95.16.172.in-addr.arpa /etc/bind/zones/db.172.16.95

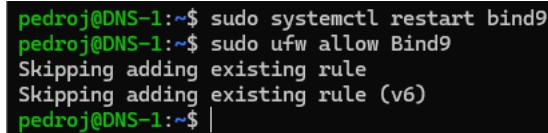


```
pedroj@DNS-1:~$ sudo named-checkzone alumno95.com /etc/bind/zones/db.alumno95.com
zone alumno95.com/IN: loaded serial 6
OK
pedroj@DNS-1:~$ sudo named-checkzone 95.16.172.in-addr.arpa /etc/bind/zones/db.172.16.95
zone 95.16.172.in-addr.arpa/IN: loaded serial 9
OK
pedroj@DNS-1:~$ |
```

Reseteamos el servicio y agregamos las reglas

sudo systemctl restart bind9

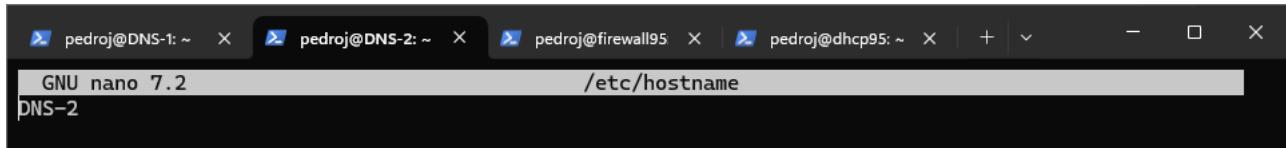
sudo ufw allow Bind9



```
pedroj@DNS-1:~$ sudo systemctl restart bind9
pedroj@DNS-1:~$ sudo ufw allow Bind9
Skipping adding existing rule
Skipping adding existing rule (v6)
pedroj@DNS-1:~$ |
```

5.1. DNS2

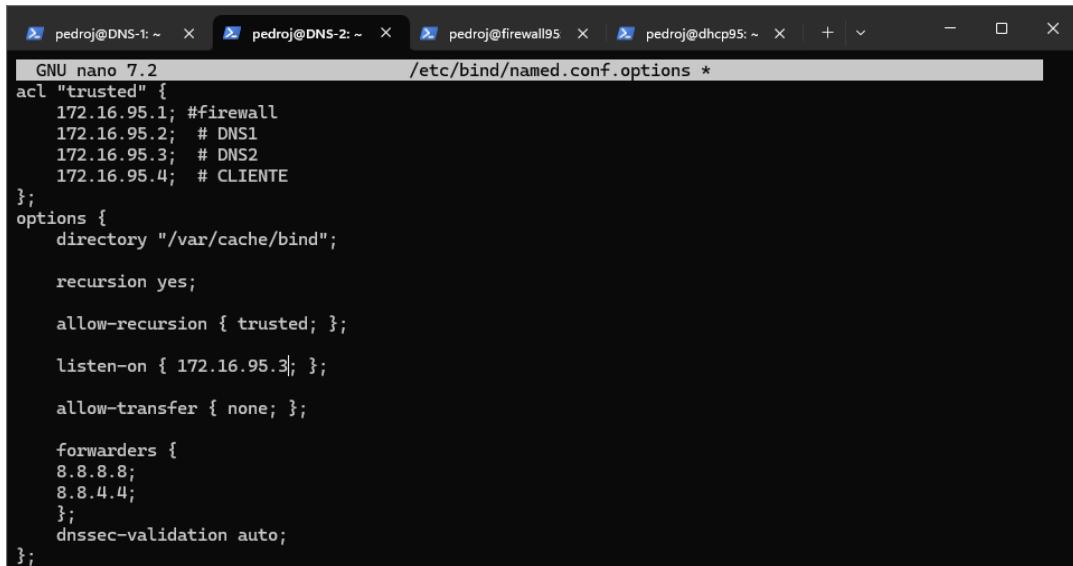
Ahora como en el anterior le cambiaremos el hostname la el interfaces y tendremos que hacer cambios en algunos archivos.



```
GNU nano 7.2          /etc/hostname
DNS-2
```

```
acl "trusted" {
    172.16.95.1; #firewall
    172.16.95.2; # DNS1
    172.16.95.3; # DNS2
    172.16.95.4; # CLIENTE
};

options {
    directory "/var/cache/bind";
    recursion yes;
    allow-recursion { trusted; };
    listen-on { 172.16.95.3; };
    allow-transfer { none; };
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    dnssec-validation auto;
};
```



```
GNU nano 7.2          /etc/bind/named.conf.options *
acl "trusted" {
    172.16.95.1; #firewall
    172.16.95.2; # DNS1
    172.16.95.3; # DNS2
    172.16.95.4; # CLIENTE
};
options {
    directory "/var/cache/bind";
    recursion yes;
    allow-recursion { trusted; };
    listen-on { 172.16.95.3; };
    allow-transfer { none; };
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    dnssec-validation auto;
};
```

```

//  

// Do any local configuration here  

//  

// Consider adding the 1918 zones here, if they are not used in your  

// organization  

//include "/etc/bind/zones.rfc1918";  

zone "alumno95.com" {  

    type slave;  

    file "db.alumno95.com";  

    masters {172.16.95.2};  

};  

zone "95.16.172.in-addr.arpa" {  

    type master;  

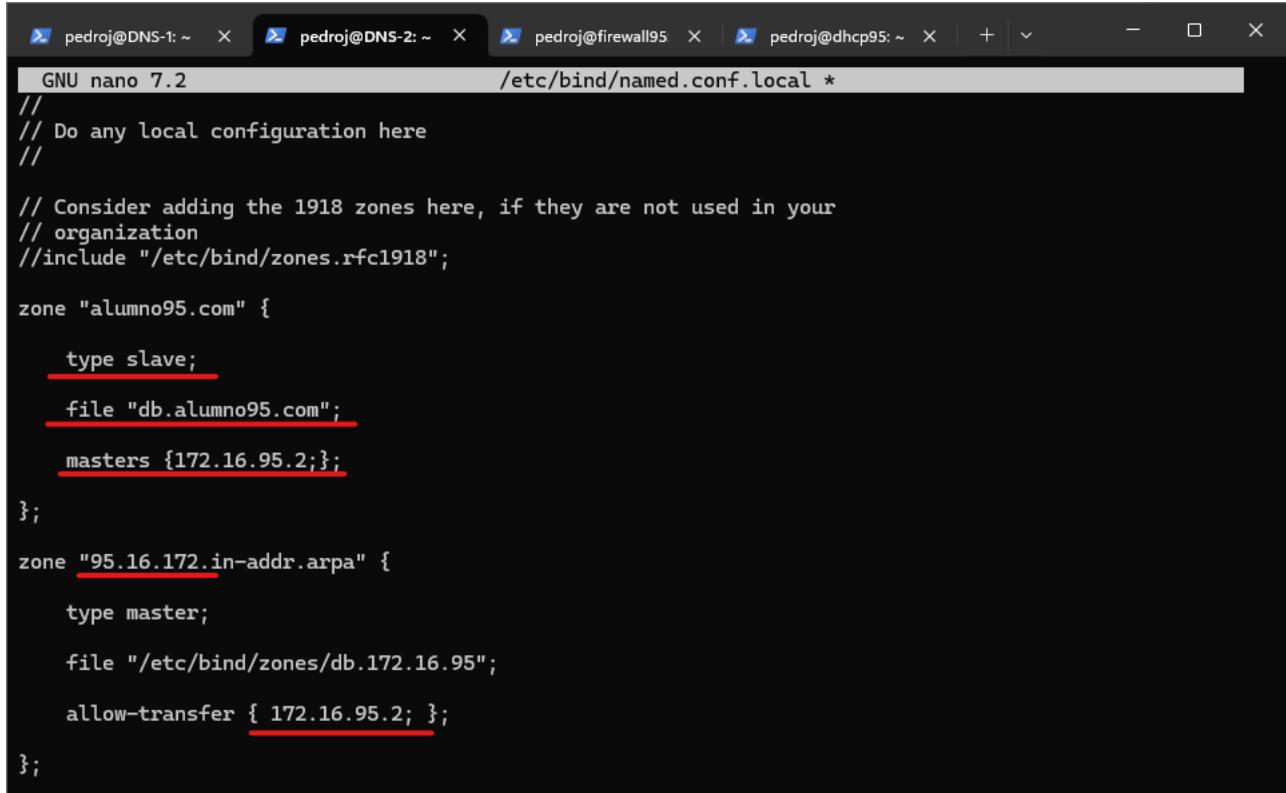
  

    file "/etc/bind/zones/db.172.16.95";  

    allow-transfer { 172.16.95.2; };  

};

```



```

GNU nano 7.2                               /etc/bind/named.conf.local *
//  

// Do any local configuration here  

//  

// Consider adding the 1918 zones here, if they are not used in your  

// organization  

//include "/etc/bind/zones.rfc1918";  

zone "alumno95.com" {  

    type slave;  

    file "db.alumno95.com";  

    masters {172.16.95.2};  

};  

zone "95.16.172.in-addr.arpa" {  

    type master;  

    file "/etc/bind/zones/db.172.16.95";  

    allow-transfer { 172.16.95.2; };  

};

```

Volvemos a hacer un check conf para confirmar que ha funcionado correctamente todo.

```
pedroj@DNS-1: ~ x pedroj@DNS-2: ~ x pedroj@firewall95 x | pedroj@dhcp95: ~ x + v - □ ×
pedroj@DNS-2:~$ sudo named-checkconf
pedroj@DNS-2:~$
```

Aquí añadiremos el apartado de zone.

```
zone "pedroj.com" {
```

```
    type master;
```

```
    file "/etc/bind/zones/db.pedroj.com";
```

```
    allow-transfer { 172.16.95.2; };
```

```
};
```

```
pedroj@DNS-1: ~ x pedroj@DNS-2: ~ x pedroj@firewall95 x | pedroj@dhcp95: ~ x + v - □ ×
GNU nano 7.2 /etc/bind/named.conf.local *
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "alumno95.com" {
    type slave;
    file "db.alumno95.com";
    masters {172.16.95.2;};
};

zone "95.16.172.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.172.16.95";
    allow-transfer { 172.16.95.2; };
};

zone "pedroj.com" {
    type master;
    file "/etc/bind/zones/db.pedroj.com";
    allow-transfer { 172.16.95.2; };
};
```

```
;
; BIND data file for local loopback interface
;

$TTL 604800
pedroj.com. IN SOA ns1.pedroj.com. admin.pedroj.com. (
    6      ; Serial
    604800    ; Refresh
    86400     ; Retry
    2419200   ; Expire
    604800 )  ; Negative Cache TTL
;

;
;

@ IN NS ns1.pedroj.com.
@ IN NS ns2.pedroj.com.

; name servers - A records
@ IN A 172.16.95.3
debian1 IN A 172.16.95.2
debian2 IN A 172.16.95.3
; 172.16.95.0/24 - A records
internal.pedroj.com. IN A 172.16.95.4
firewall.pedroj.com. IN A 172.16.95.1
```

```
GNU nano 7.2 /etc/bind/zones/db.pedroj.com *
;
; BIND data file for local loopback interface
;

$TTL 604800
pedroj.com. IN SOA ns1.pedroj.com. admin.pedroj.com. (
    6      ; Serial
    604800    ; Refresh
    86400     ; Retry
    2419200   ; Expire
    604800 )  ; Negative Cache TTL
;

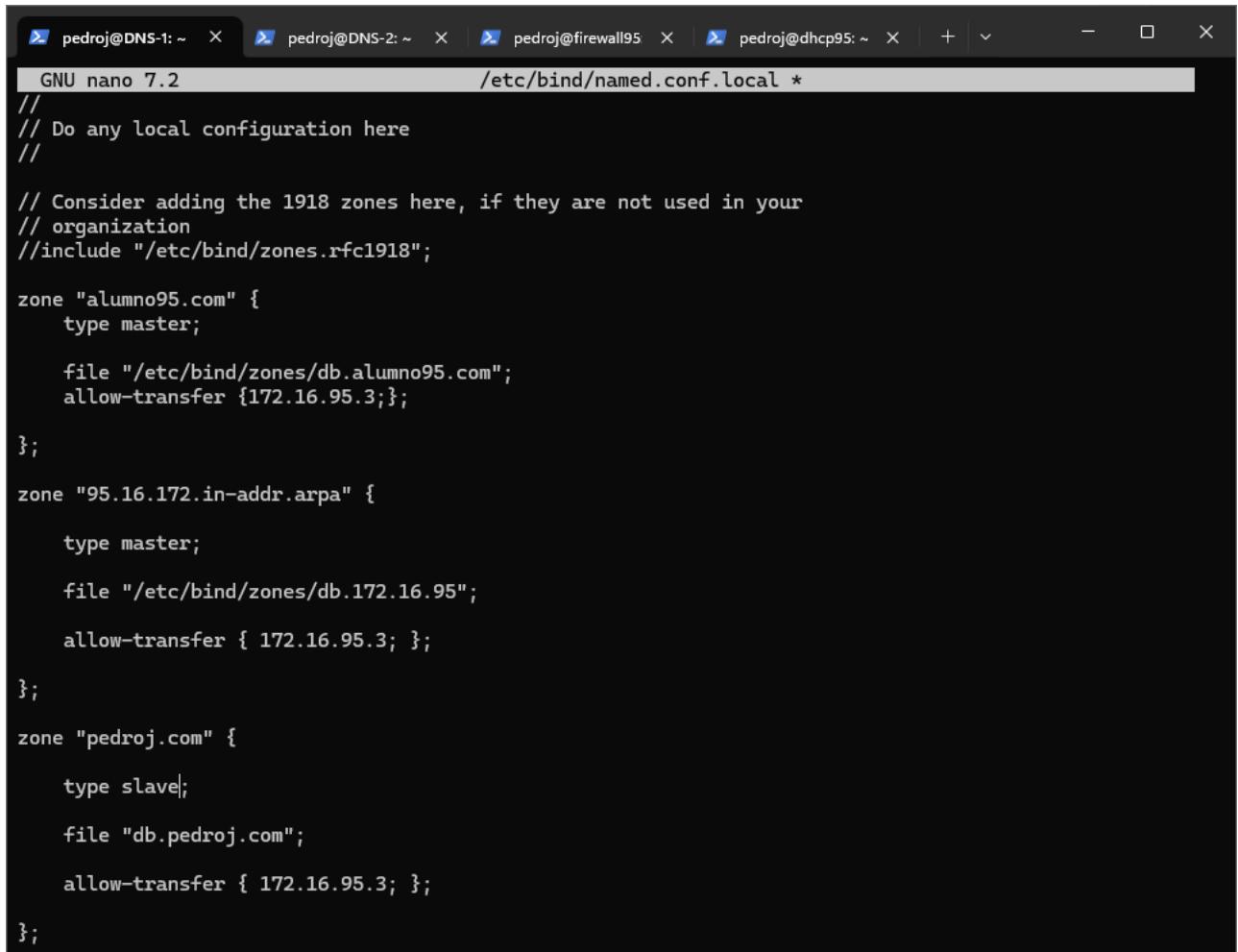
;
;

@ IN NS ns1.pedroj.com.
@ IN NS ns2.pedroj.com.

; name servers - A records
@ IN A 172.16.95.3
debian1 IN A 172.16.95.2
debian2 IN A 172.16.95.3
; 172.16.95.0/24 - A records
internal.pedroj.com. IN A 172.16.95.4
firewall.pedroj.com. IN A 172.16.95.1
```

Nos iremos al DNS1 y le agregaremos el zone que pusimos en el DNS2 pero haciéndolo al contrario.

```
zone "pedroj.com" {  
  
    type slave;  
  
    file "db.pedroj.com";  
  
    allow-transfer { 172.16.95.3; };  
  
};
```



```
GNU nano 7.2                               /etc/bind/named.conf.local *  
//  
// Do any local configuration here  
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
zone "alumno95.com" {  
    type master;  
  
    file "/etc/bind/zones/db.alumno95.com";  
    allow-transfer {172.16.95.3;};  
};  
  
zone "95.16.172.in-addr.arpa" {  
  
    type master;  
  
    file "/etc/bind/zones/db.172.16.95";  
    allow-transfer { 172.16.95.3; };  
};  
  
zone "pedroj.com" {  
    type slave;  
  
    file "db.pedroj.com";  
    allow-transfer { 172.16.95.3; };  
};
```

Agregaremos lo siguiente al fichero del dhcp

```
option domain-name "alumno95.com";  
option domain-search "alumno95.com", "pedroj.com";  
option domain-name-servers 172.16.95.2, 172.16.95.3;
```

#CLIENTE 1

```
host Cliente1 {  
    hardware ethernet 08:00:27:01:b3:cb;  
    fixed-address 172.16.95.4;  
}
```

```
GNU nano 7.2                                         /etc/dhcp/dhcpd.conf *
```

```
# range 172.16.65.20 172.16.65.30;
# option subnet-mask 255.255.255.0;
# option routers 172.16.65.1;
# option domain-name-servers 8.8.8.8;
# default-lease-time 86400;
# max-lease-time 691200;
# min-lease-time 3600;
#}

subnet 172.16.95.0 netmask 255.255.255.0 {
    range 172.16.95.20 172.16.95.30;
    option subnet-mask 255.255.255.0;
    option routers 172.16.95.1;
    option domain-name "alumno95.com";
    option domain-search "alumno95.com", "pedro1.com";
    option domain-name-servers 172.16.95.2, 172.16.95.3;
    default-lease-time 86400;
    max-lease-time 691200;
    min-lease-time 3600;
}

#Router
host router {
    hardware ethernet 08:00:27:4b:2c:e0;
    fixed-address 172.16.95.1;
}

#Cliente
host cliente-pedro {
    hardware ethernet 08:00:27:F6:4F:B0;
    fixed-address 172.16.95.8;
}
#DNS
host DNS1 {
    hardware ethernet 08:00:27:e7:6d:c1;
    fixed-address 172.16.95.2;
}
#DNS 2
host DNS2 {
    hardware ethernet 08:00:27:9f:97:b0;
    fixed-address 172.16.95.3;
}
#CLIENTE 1
host Cliente1 {
    hardware ethernet 08:00:27:81:b3:cb;
    fixed-address 172.16.95.4;
}
```

Y si funciona correctamente si nos vamos al cliente nos hará ping si hacemos

ping ns1

ping ns2

sudo cat /etc/resolv.conf

The screenshot shows a terminal window titled "Debian Cliente [Corriendo] - Oracle VirtualBox". The window contains the following text:

```
pedro@pedro:~$ 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 brd 0.0.0.0 scope host lo
        valid_lifeti...
```

After the configuration, the user runs:

```
pedro@pedro:~$ ping ns1
PING ns1.alumno95.com (172.16.95.2) 56(84) bytes of data.
64 bytes from ns1.alumno95.com (172.16.95.2): icmp_seq=1 ttl=64 time=0.949 ms
64 bytes from ns1.alumno95.com (172.16.95.2): icmp_seq=2 ttl=64 time=1.09 ms
[...]
[1]+ Detenido ping ns1
pedro@pedro:~$ ping ns2
PING ns2.alumno95.com (172.16.95.3) 56(84) bytes of data.
64 bytes from ns2.alumno95.com (172.16.95.3): icmp_seq=1 ttl=64 time=2.00 ms
64 bytes from ns2.alumno95.com (172.16.95.3): icmp_seq=2 ttl=64 time=0.920 ms
[...]
[2]+ Detenido ping ns2
pedro@pedro:~$ ping internal
PING internal.alumno95.com (172.16.95.4) 56(84) bytes of data.
64 bytes from pedro (172.16.95.4): icmp_seq=1 ttl=64 time=0.022 ms
64 bytes from pedro (172.16.95.4): icmp_seq=2 ttl=64 time=0.041 ms
[...]
[3]+ Detenido ping internal
pedro@pedro:~$
```

The terminal window has a dark background and light-colored text. The bottom right corner shows the system tray with icons for battery, signal strength, and date/time.

6. FTP

Agregaremos los valores para darle ip a través del dhcp

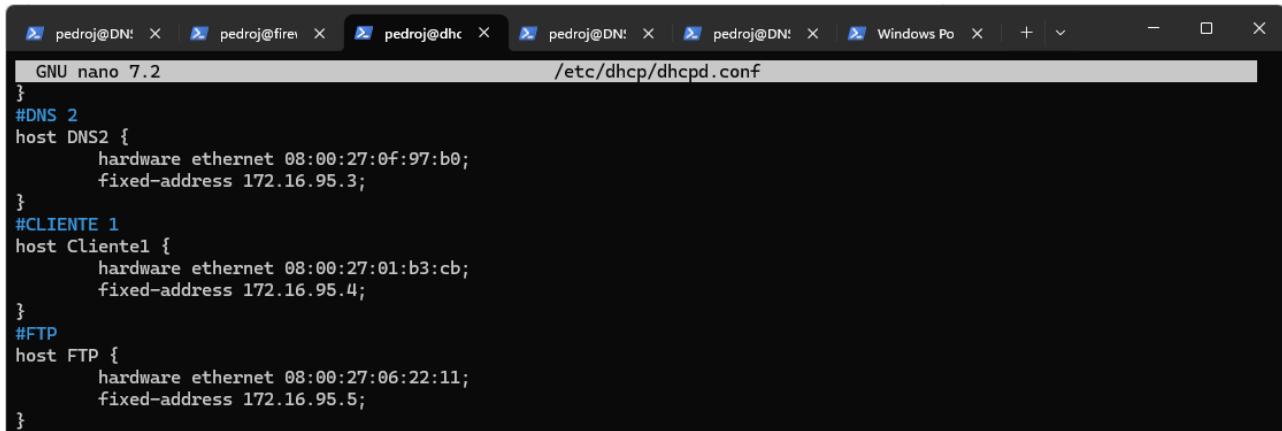
#FTP

```
host FTP {
```

```
    hardware ethernet 08:00:27:06:22:11;
```

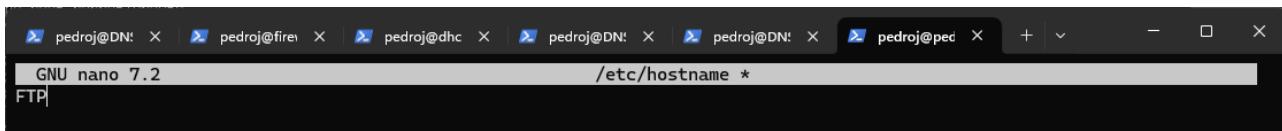
```
    fixed-address 172.16.95.5;
```

```
}
```



```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
}
#DNS 2
host DNS2 {
    hardware ethernet 08:00:27:0f:97:b0;
    fixed-address 172.16.95.3;
}
#CLIENTE 1
host Cliente1 {
    hardware ethernet 08:00:27:01:b3:cb;
    fixed-address 172.16.95.4;
}
#FTP
host FTP {
    hardware ethernet 08:00:27:06:22:11;
    fixed-address 172.16.95.5;
}
```

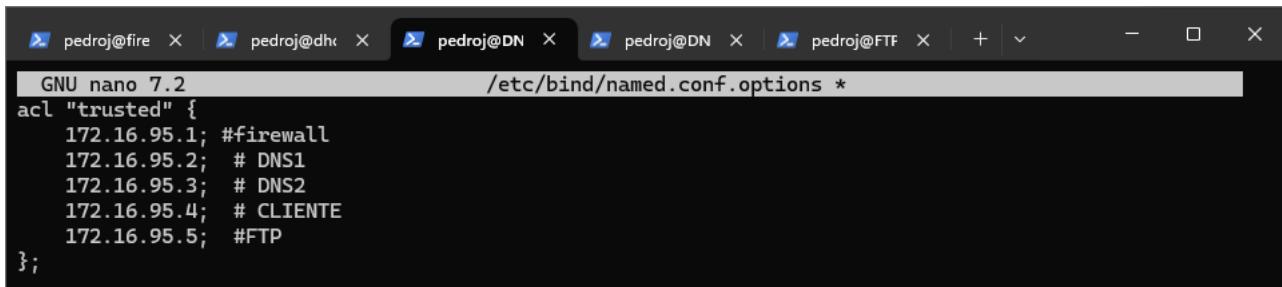
Cambiamos el hostname



```
GNU nano 7.2 /etc/hostname *
FTP
```

En el DNS1 nos iremos al /etc/bind/named.conf.options y añadiremos:

172.16.95.5; #FTP

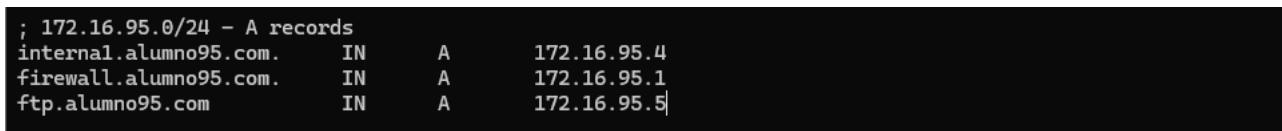


```
GNU nano 7.2 /etc/bind/named.conf.options *
acl "trusted" {
    172.16.95.1; #firewall
    172.16.95.2; # DNS1
    172.16.95.3; # DNS2
    172.16.95.4; # CLIENTE
    172.16.95.5; #FTP
};
```

También añadiremos en la siguiente ruta:

sudo nano /etc/bind/zones/db.alumno95.com

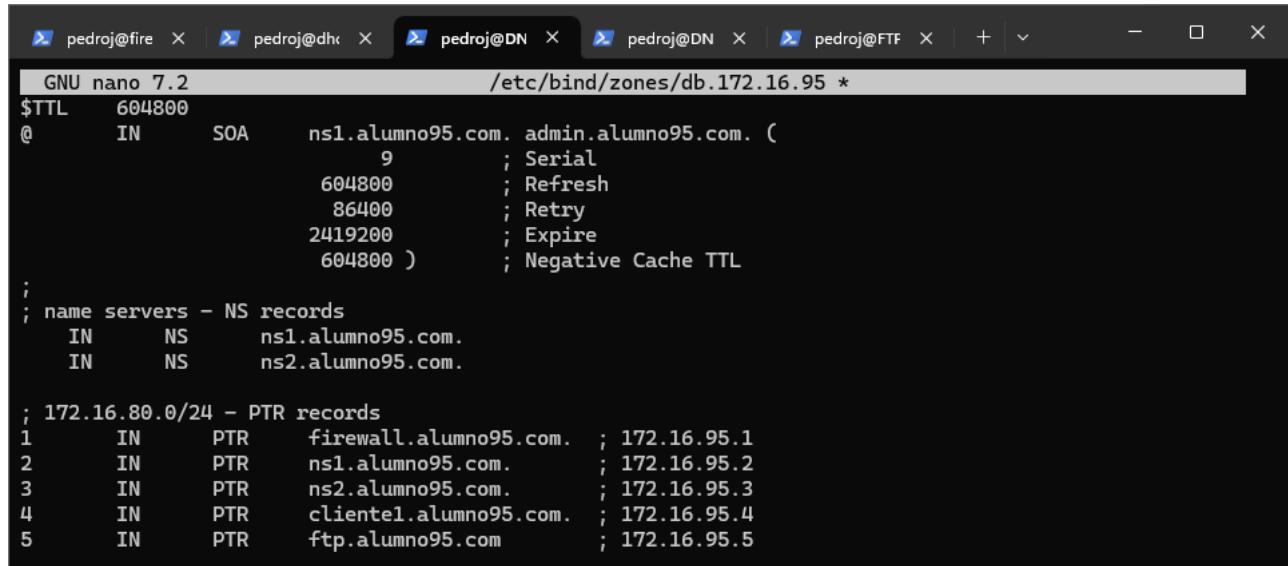
ftp.alumno95.com IN A 172.16.95.5



```
; 172.16.95.0/24 - A records
internal.alumno95.com.      IN      A       172.16.95.4
firewall.alumno95.com.     IN      A       172.16.95.1
ftp.alumno95.com.          IN      A       172.16.95.5
```

En el directorio de la zona inversa tendremos que añadir al final del todo la siguiente línea:

5 IN PTR ftp.alumno95.com ; 172.16.95.5



```
GNU nano 7.2 /etc/bind/zones/db.172.16.95 *
$TTL 604800
@ IN SOA ns1.alumno95.com. admin.alumno95.com. (
    9 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
; name servers - NS records
IN NS ns1.alumno95.com.
IN NS ns2.alumno95.com.

; 172.16.80.0/24 - PTR records
1 IN PTR firewall.alumno95.com. ; 172.16.95.1
2 IN PTR ns1.alumno95.com. ; 172.16.95.2
3 IN PTR ns2.alumno95.com. ; 172.16.95.3
4 IN PTR cliente1.alumno95.com. ; 172.16.95.4
5 IN PTR ftp.alumno95.com ; 172.16.95.5
```

En el DNS2 igual meteremos el **172.16.95.5; #FTP** en el conf.options



```
GNU nano 7.2 /etc/bind/named.conf.options *
acl "trusted" {
    172.16.95.1; #firewall
    172.16.95.2; # DNS1
    172.16.95.3; # DNS2
    172.16.95.4; # CLIENTE
    172.16.95.5; # FTP
};
```

En el DNS2 meteremos en la ruta /etc/bind/zones/db.pedroj.com

ftpdeb.pedroj.com. IN A 172.16.95.5

```
GNU nano 7.2 /etc/bind/zones/db.pedroj.com *
;
; BIND data file for local loopback interface
;
$TTL    604800
pedroj.com.      IN      SOA    ns1.pedroj.com. admin.pedroj.com. (
                      6                   ; Serial
                     604800              ; Refresh
                      86400               ; Retry
                     2419200              ; Expire
                     604800 )            ; Negative Cache TTL
;
;
@      IN      NS      ns1.pedroj.com.
@      IN      NS      ns2.pedroj.com.

; name servers - A records
@      IN      A      172.16.95.3
debian1     IN      A      172.16.95.2
debian2     IN      A      172.16.95.3

; 172.16.95.0/24 - A records
internal1.pedroj.com.   IN      A      172.16.95.4
firewall.pedroj.com.    IN      A      172.16.95.1
ftpdeb.pedroj.com.      IN      A      172.16.95.5
```

Si nos vamos hacemos un cat /etc/hosts nos saldrá todo lo que hemos puesto

```
pedroj@FTP:~$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      FTP

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
pedroj@FTP:~$ cat /etc/hostname
FTP
```

Instalaremos el servicio con: **sudo apt install vsftpd**

```
pedroj@FTP:~$ sudo apt install vsftpd
```

sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig

```
pedroj@FTP:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig
[sudo] contraseña para pedroj:
```

Haremos **sudo ufw allow 20,21,990/tcp** para añadir las reglas

```
pedroj@FTP:~$ sudo ufw allow 20,21,990/tcp
Rules updated
Rules updated (v6)
pedroj@FTP:~$ |
```

```
sudo ufw allow 40000,50000/tcp
```

```
pedroj@FTP:~$ sudo ufw allow 40000:50000/tcp
Rules updated
Rules updated (v6)
pedroj@FTP:~$ |
```

Habilitamos el servicio y si hacemos un status veremos que las rutas que hemos puesto saldrán

```
pedroj@FTP:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
pedroj@FTP:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
20,21,990/tcp              ALLOW      Anywhere
40000:50000/tcp             ALLOW      Anywhere
20,21,990/tcp (v6)          ALLOW      Anywhere (v6)
40000:50000/tcp (v6)        ALLOW      Anywhere (v6)
```

Añadiremos un usuario con una contraseña para poder configurarlo y así luego poder usarlo con el filezilla

```
pedroj@fire  X  pedroj@dhc  X  pedroj@DN  X  pedroj@DN  X  pedroj@FTI  X  +  -  □  ×
pedroj@FTP:~$ sudo adduser krieger
Añadiendo el usuario 'krieger' ...
Añadiendo el nuevo grupo 'krieger' (1002) ...
Adding new user 'krieger' (1002) with group 'krieger' (1002) ...
Creando el directorio personal '/home/krieger' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para krieger
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
  Nombre completo []: krieger
  Número de habitación []:
  Teléfono del trabajo []:
  Teléfono de casa []:
  Otro []:
¿Es correcta la información? [S/n] s
Adding new user 'krieger' to supplemental / extra groups 'users' ...
Añadiendo al usuario 'krieger' al grupo 'users' ...
pedroj@FTP:~$ |
```

```
sudo chown nobody:nogroup /home/krieger/ftp
```

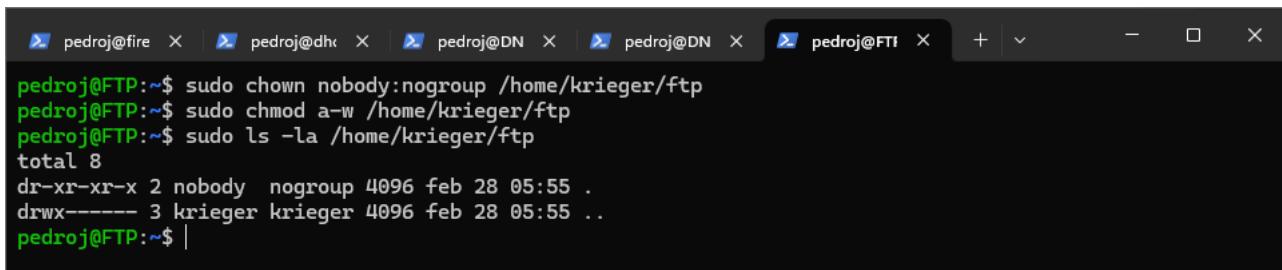
Esto se hace para que el directorio sea accesible solo por un usuario con privilegios limitados, lo que puede ayudar a mejorar la seguridad del servidor FTP.

```
sudo chmod a-w /home/krieger/ftp
```

Este comando quita el permiso de escritura para todos los usuarios en el directorio /home/krieger/ftp. Esto significa que nadie podrá modificar el contenido del directorio, lo que es útil para protegerlo de cambios no autorizados.

```
sudo ls -la /home/krieger/ftp
```

Este comando lista todos los archivos y directorios dentro de /home/krieger/ftp, mostrando detalles como permisos, propietario, grupo, tamaño y fecha de modificación. Se utiliza para verificar que los cambios de propiedad y permisos se hayan aplicado correctamente.



```
pedroj@fire ~ | pedroj@dhc ~ | pedroj@DN ~ | pedroj@DN ~ | pedroj@FTP ~ + | v - □ ×
pedroj@FTP:~$ sudo chown nobody:nogroup /home/krieger/ftp
pedroj@FTP:~$ sudo chmod a-w /home/krieger/ftp
pedroj@FTP:~$ sudo ls -la /home/krieger/ftp
total 8
dr-xr-xr-x 2 nobody nogroup 4096 feb 28 05:55 .
drwx----- 3 krieger krieger 4096 feb 28 05:55 ..
pedroj@FTP:~$ |
```

Crearemos el la carpeta files si no nos la ha creado sola

```
sudo mkdir /home/krieger/ftp/files
```



```
pedroj@FTP:~$ sudo mkdir /home/krieger/ftp/files
```

```
sudo chown krieger:krieger /home/krieger/ftp/files
```

El comando cambia la propiedad y el grupo del directorio /home/krieger/ftp/files a krieger, lo que permite que el usuario krieger y cualquier miembro del grupo krieger gestionen el contenido de ese directorio. Esto es especialmente útil en un entorno de servidor FTP, donde es importante que los usuarios tengan acceso adecuado a sus propios directorios para poder subir, descargar o modificar archivos.

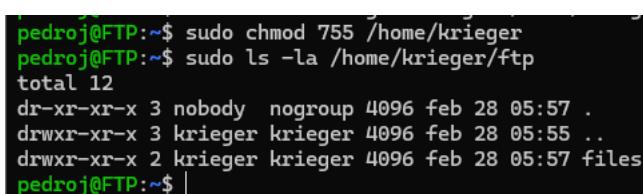


```
pedroj@FTP:~$ sudo chown krieger:krieger /home/krieger/ftp/files
pedroj@FTP:~$ |
```

Le daremos los permisos y si hacemos un ls nos saldrá todo

```
sudo chmod 755 /home/krieger
```

```
sudo ls -la /home/krieger/ftp
```



```
pedroj@FTP:~$ sudo chmod 755 /home/krieger
pedroj@FTP:~$ sudo ls -la /home/krieger/ftp
total 12
dr-xr-xr-x 3 nobody nogroup 4096 feb 28 05:57 .
drwxr-xr-x 3 krieger krieger 4096 feb 28 05:55 ..
drwxr-xr-x 2 krieger krieger 4096 feb 28 05:57 files
pedroj@FTP:~$ |
```

Nos iremos al directorio /etc/vsftpd.conf y tendremos que añadir lo siguiente (lo que no está documentado) y también tendremos que tener la configuración igual que la tengo yo

```
GNU nano 7.2                               /etc/vsftpd.conf *

anonymous_enable=NO

local_enable=YES

write_enable YES

chroot_local_user=YES

user_sub_token=$USER
local_root=/home/$USER/ftp

pasv_enable=YES

connect_from_port_20=YES

pasv_min_port=40000
pasv_max_port=50000
pasv_address=192.168.35.95

userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=NO
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpt's)
#local_umask=022
#
^G Ayuda      ^O Guardar     ^W Buscar     ^K Cortar     ^T Ejecutar     ^C Ubicación   M-U Deshacer
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar      ^J Justificar  ^/ Ir a linea M-E Rehacer
```

```
# Activate logging of uploads/downloads.
xferlog_enable=YES
xferlog_file=/var/log/vsftpd.log
#
```

Luego nos iremos al iptables del router y tendremos que añadir lo siguiente a el, yo lo he puesto al final de la línea:

```
# Redirigir el rango de puertos pasivos al servidor FTP !!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 40000:50000 -j DNAT --to  
172.16.95.5:40000-50000
```

```
iptables -A FORWARD -p tcp --dport 40000:50000 -d 172.16.95.5 -j ACCEPT  
IPTABLES_MODULES="nf_conntrack_ftp ip_nat_ftp"
```

```
# Redirigir puerto 21 al servidor FTP en la red interna !!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 21 -j DNAT --to 172.16.95.5:21  
iptables -A FORWARD -p tcp --dport 21 -d 172.16.95.5 -j ACCEPT
```

```
# Redirigir puerto 20 al servidor FTP en la red interna !!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 20 -j DNAT --to 172.16.95.5:20  
iptables -A FORWARD -p tcp --dport 20 -d 172.16.95.5 -j ACCEPT
```

```
# Redirigir puerto 21 al servidor FTP en la red interna !!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 21 -j DNAT --to 172.16.95.5:21  
iptables -A FORWARD -p tcp --dport 21 -d 172.16.95.5 -j ACCEPT
```

```
# Redirigir puerto 80 al servidor FTP en la red interna!!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j DNAT --to 172.16.95.5:80
```

```
#CERRAMOS LOS PUERTOS BIEN CONOCIDOS
```

```
iptables -A INPUT -s 0.0.0.0/0 -i enp0s3 -p tcp --dport 1:1024 -j DROP  
iptables -A INPUT -s 0.0.0.0/0 -i enp0s3 -p udp --dport 1:1024 -j DROP
```

```
# Redirigir el rango de puertos pasivos al servidor FTP !!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 40000:50000 -j DNAT --to 172.16.95.5:40000-50000  
iptables -A FORWARD -p tcp --dport 40000:50000 -d 172.16.95.5 -j ACCEPT  
IPTABLES_MODULES="nf_conntrack_ftp ip_nat_ftp"
```

```
# Redirigir puerto 21 al servidor FTP en la red interna !!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 21 -j DNAT --to 172.16.95.5:21  
iptables -A FORWARD -p tcp --dport 21 -d 172.16.95.5 -j ACCEPT
```

```
# Redirigir puerto 20 al servidor FTP en la red interna !!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 20 -j DNAT --to 172.16.95.5:20  
iptables -A FORWARD -p tcp --dport 20 -d 172.16.95.5 -j ACCEPT
```

```
# Redirigir puerto 21 al servidor FTP en la red interna !!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 21 -j DNAT --to 172.16.95.5:21  
iptables -A FORWARD -p tcp --dport 21 -d 172.16.95.5 -j ACCEPT
```

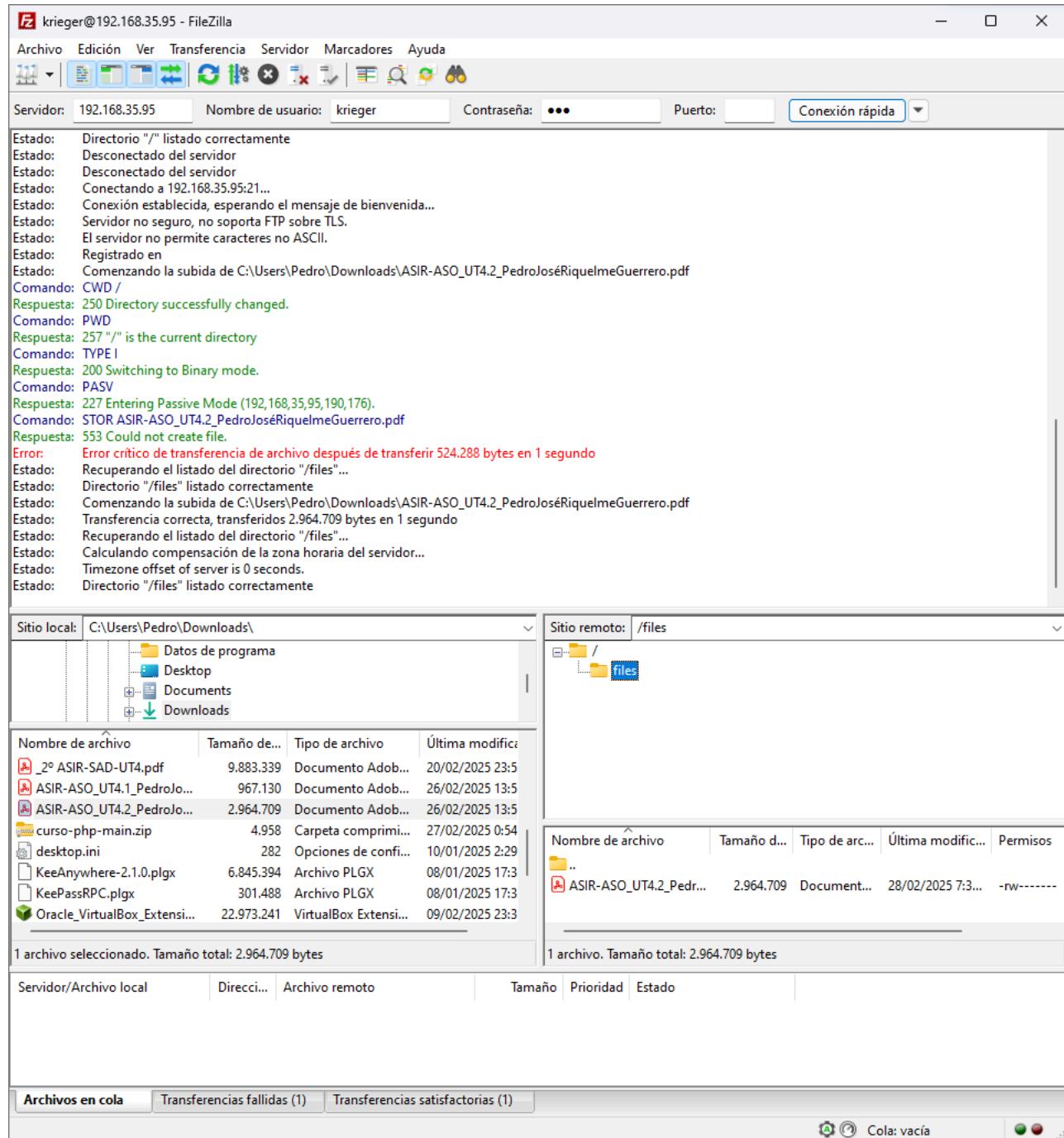
```
# Redirigir puerto 80 al servidor FTP en la red interna!!
```

```
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j DNAT --to 172.16.95.5:80
```

```
|
```

```
^G Ayuda      ^O Guardar     ^W Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación  M-U Deshacer  
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar       ^J Justificar  ^/ Ir a línea M-E Rehacer
```

Luego si nos vamos a nuestra máquina mismamente instalaremos el filezilla cliente. en la barra de arriba tendremos que poner la ip de nuestro router, el usuario y contraseña del usuario que creamos anteriormente. Una vez dado a conexión comprobaremos que efectivamente nos dejará subir archivos.



Luego nos iremos al FTP y si hacemos un ls en /home/krieger/ftp/files veremos que efectivamente nos saldrá el documento que hemos subido.

```
pedroj@FTP:~$ ls
Descargas Documentos Escritorio Imágenes Música Plantillas Público Vídeos
pedroj@FTP:~$ cd /home/krieger/ftp/files/
pedroj@FTP:/home/krieger/ftp/files$ ls
'ASIR-ASO_UT4.2_PedroJos'$'\351''RiquelmeGuerrero.pdf'
pedroj@FTP:/home/krieger/ftp/files$
```

Conclusión