Administración de Sistemas Operativos

Volodimir Yarmash Yarmash

UNIÓN EUROPEA
Fondo Social Europeo
EL FSE invierte en tu futuro

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Junta de Andalucía
Consejería de Educación y Deporte

I.E.S. LA MARISMA

Índice

Para esta nueva unidad didáctica es necesario instalar Ubuntu Server 16.10.

Deben realizar las configuraciones que se han explicado en clase. Como referencia, pueden utilizar los siguientes video tutoriales:

Enrutamiento: http://gofile.me/5ZHr5/tI3QstC2m

Servidor DNS: http://gofile.me/5ZHr5/NAvwJb5w7

Servidor DHCP: http://gofile.me/5ZHr5/LyV41BtjR

Servidor LAMP: https://gofile.me/5ZHr5/siEuaypRV

Firewall Linux: https://gofile.me/5ZHr5/cnmbrKwgf

IPTABLES: https://gofile.me/5ZHr5/XSTdJslMp

NAS IES LA MARISMA: https://nas-marisma.fr4.quickconnect.to/#/signin

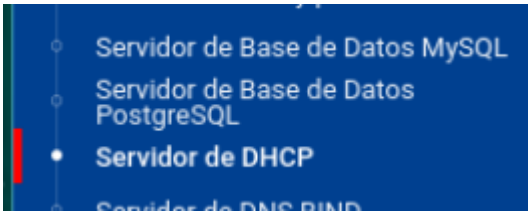
USUARIO: 2asir

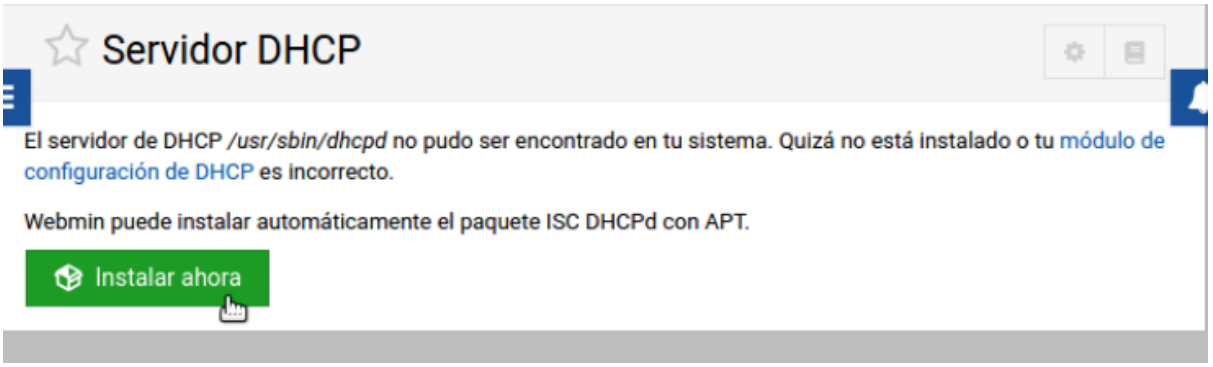
PASSWORD: Asir2marisma

Instala el servicio DHCP.

Antes de nada, necesitamos un equipo sin acceso a internet, conectado a una máquina con webmin.

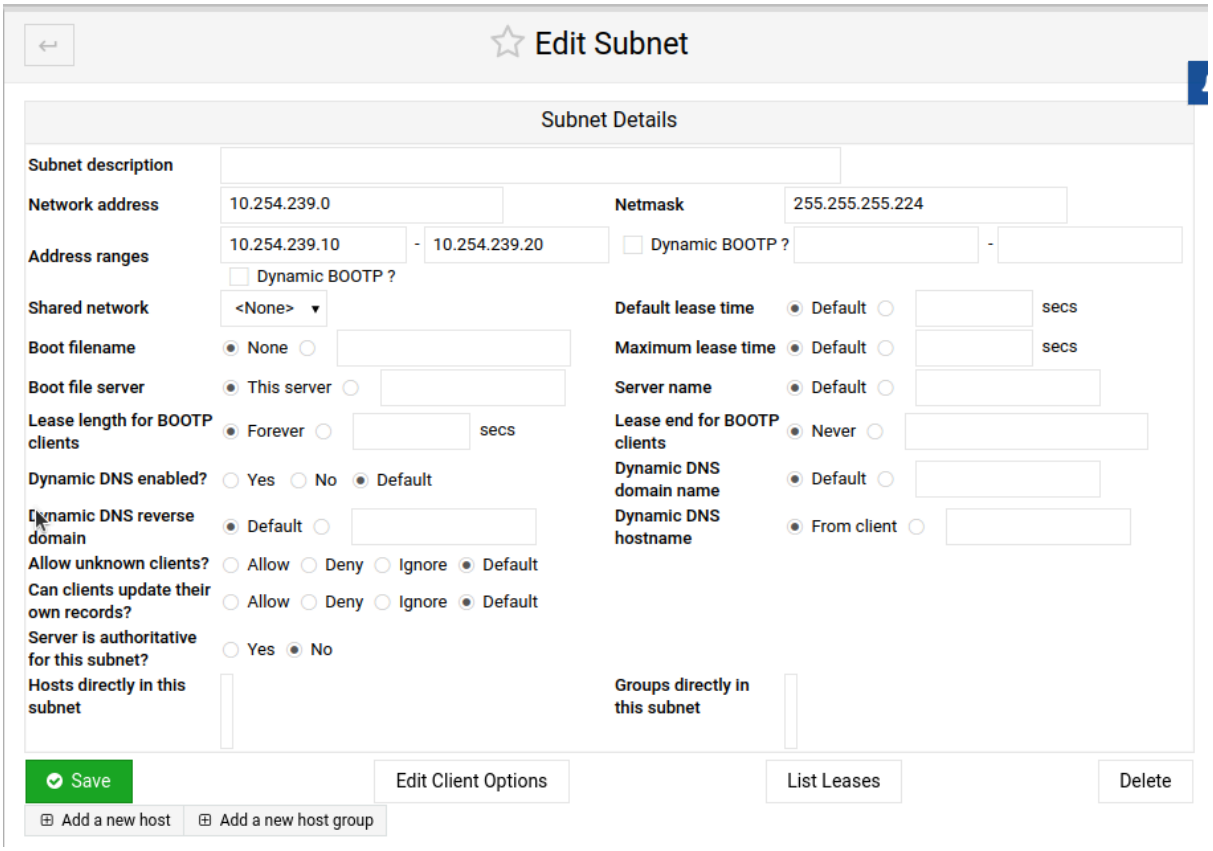
Para instalar el servicio DHCP vamos a utilizar la interfaz de webmin. Desde el panel de webmin accederemos al apartado Módulos sin usar y ahí buscaremos el servidor DHCP. Haremos click en “Instalar ahora”. Una vez se instale, vamos al apartado de Servidor DHCP y nos aparecerá la ventana para configurarlo.





Configura el servicio DHCP para otorgar IP dentro de un rango.

Pulsamos crear Subred y lo configuramos.



Y tenemos nuestra subred lista

Subnets and Shared Networks

Select all | Invert selection | Add a new subnet | Add a new shared network

Select all | Invert selection | Add a new subnet | Add a new shared network

Delete Selected

Hosts and Host Groups

No hosts or groups have been defined.

Add a new host | Add a new host group

DNS Zones

No DNS zones have been defined yet.

Add a new DNS zone

Edit Client Options — Edit DHCP client options that apply to all subnets, shared networks, hosts and groups

Edit TSIG-keys — Edit TSIG-keys (used for authenticating updates to DNS servers)

Hosts and Host Groups

No hosts or groups have been defined.

Add a new host | Add a new host group

DNS Zones

No DNS zones have been defined yet.

Add a new DNS zone

Edit Client Options — Edit DHCP client options that apply to all subnets, shared networks, hosts and groups

Edit TSIG-keys — Edit TSIG-keys (used for authenticating updates to DNS servers)

Manually Edit Configuration — Edit configuration file manually text

Edit Network Interface — Set the network interfaces that the DHCP server listens on when started.

List Active Leases — List leases currently issued by this DHCP server for dynamically assigned IP addresses.

Apply Changes — Click this button to apply the current configuration to the running DHCP server, by stopping and restarting it.

Stop Server — Click this button to stop the running DHCP server on your system. When stopped, DHCP clients will not be able to request IP addresses.

Entramos en el equipo cliente sin acceso a internet, y comprobamos que no se nos ha asignado ninguna ip

```
user@user-Standard-PC-i440FX-PIIX-1996:~/Desktop$ 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: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:ff:4c:85 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
```

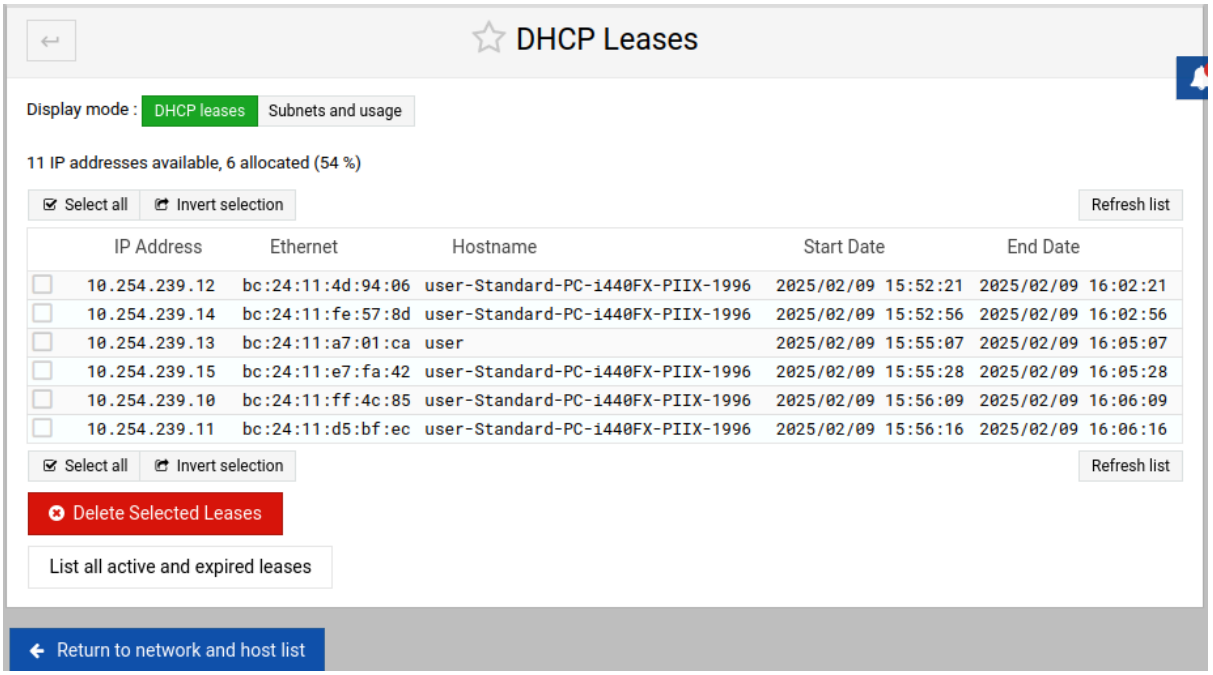
Comprueba el resultado conectando clientes al servidor (configúralos por DHCP apuntando al servidor Ubuntu).

Nos aseguramos de que en los archivos de DHCP estén bien configurados.
Comprobamos sobre todo la configuración de la tarjeta de red con sudo nano /etc/default/isc-dhcp-server

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996: /var/lib/dhcp
 GNU nano 6.2                                /etc/default/isc-dhcp-server
INTERFACESv6=""
INTERFACESv4=ens19
```

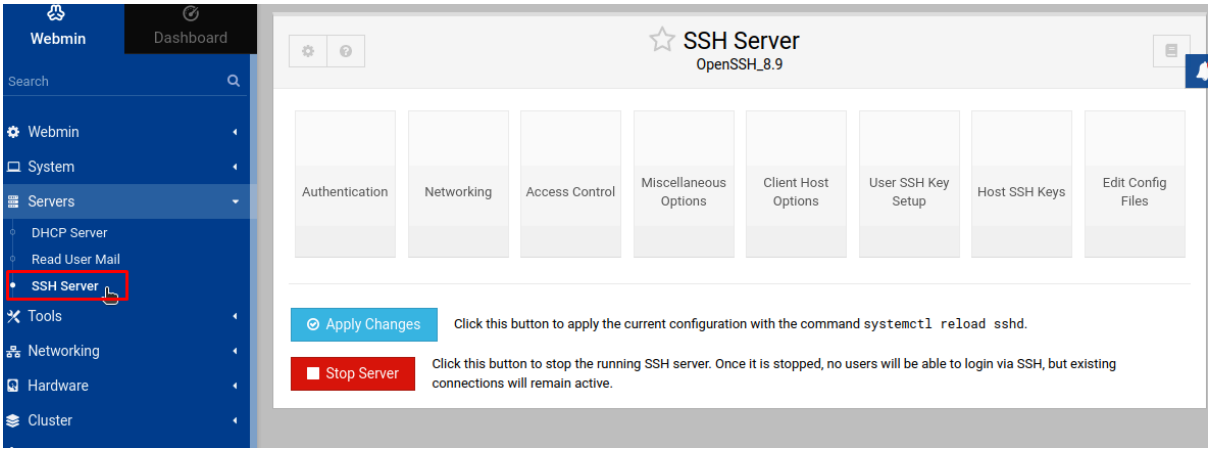
Ahora forzamos la búsqueda de DHCP con sudo dhclient -v
Y listo

```
user@user-Standard-PC-i440FX-PIIX-1996:~/Desktop$ sudo dhclient -v ens19
[sudo] password for user:
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens19/bc:24:11:ff:4c:85
Sending on   LPF/ens19/bc:24:11:ff:4c:85
Sending on   Socket/fallback
DHCPDISCOVER on ens19 to 255.255.255.255 port 67 interval 3 (xid=0x91d41679)
DHCPOFFER of 10.254.239.10 from 10.254.239.1
DHCPREQUEST for 10.254.239.10 on ens19 to 255.255.255.255 port 67 (xid=0x7916d491)
DHCPACK of 10.254.239.10 from 10.254.239.1 (xid=0x91d41679)
bound to 10.254.239.10 -- renewal in 260 seconds.
user@user-Standard-PC-i440FX-PIIX-1996:~/Desktop$ ping 10.254.239.1
PING 10.254.239.1 (10.254.239.1) 56(84) bytes of data.
64 bytes from 10.254.239.1: icmp_seq=1 ttl=64 time=1.17 ms
64 bytes from 10.254.239.1: icmp_seq=2 ttl=64 time=0.655 ms
64 bytes from 10.254.239.1: icmp_seq=3 ttl=64 time=0.530 ms
^C
--- 10.254.239.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2049ms
rtt min/avg/max/mdev = 0.530/0.783/1.165/0.274 ms
user@user-Standard-PC-i440FX-PIIX-1996:~/Desktop$
```



Instala el servicio SSH si no está ya instalado.

Se instala con el comando apt-get install ssh



Realiza una conexión al servidor por SSH.

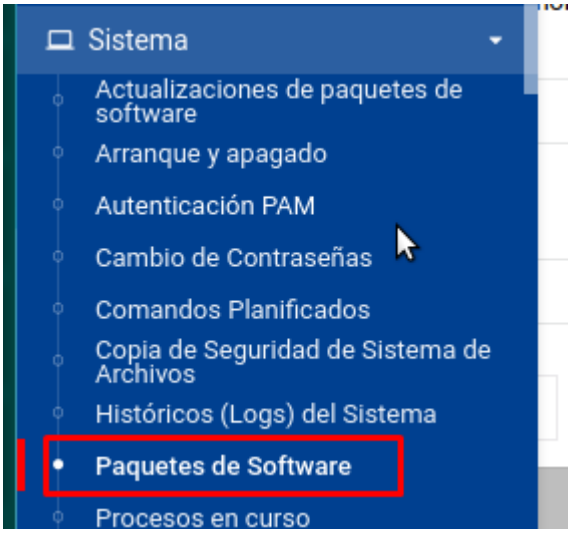
Para hacer una conexión con el servidor usamos el comando “ssh user@192.168.195.21” y acreditamos la contraseña.

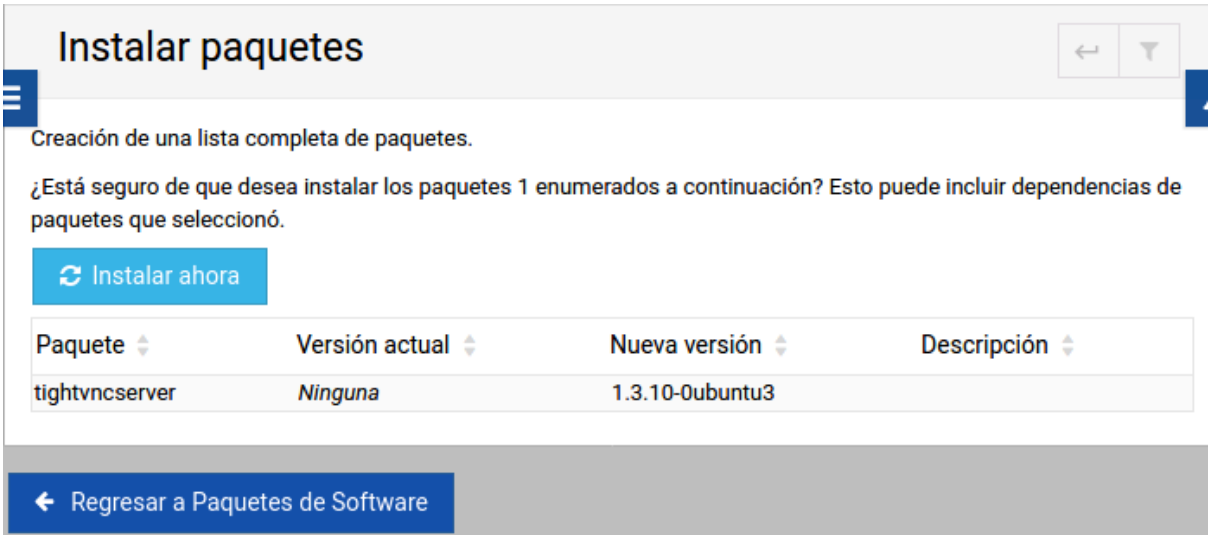
```
user@user-Standard-PC-i440FX-PIIX-1996:~/Desktop$ ssh webmin@10.254.239.1
The authenticity of host '10.254.239.1 (10.254.239.1)' can't be established.
ED25519 key fingerprint is SHA256:dTxX9dQie+n9MRRb4PZYm9DGs94VCdOLjsxXXHBqxDg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.254.239.1' (ED25519) to the list of known hosts.
webmin@10.254.239.1's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

544 updates can be applied immediately.
380 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

webmin@webmin-Standard-PC-i440FX-PIIX-1996:~$
```

comando exit para salir de la sesion del servidor

Instala el servicio VNC.

Para instalar el servicio VNC vamos a usar la característica de paquetes de software integrada en webmin que nos permite descargar e instalar cualquier paquete como si lo hiciéramos desde la consola. Para ello solo tenemos que seleccionar la opción de paquete desde APT y escribir el nombre del paquete.





Comprueba la conexión con un cliente VNC de la red.

Como mi cliente no tiene instalado VNC y además no tiene acceso a internet, lo primero que vamos a hacer es configurar el enrutamiento en nuestro servidor para que nuestro cliente pueda descargarlo. Para ello vamos a habilitar el reenvío de paquetes modificando el archivo sysctl.conf de la siguiente manera.

Habilitamos esta linea

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996: /etc
 GNU nano 6.2                                  /etc/sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

###################################################################
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

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

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

Recargamos la configuración con sudo sysctl -p

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo sysctl -p
net.ipv4.tcp_syncookies = 1
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$
```

Ahora vamos a configurar NAT, creando algunas iptable para permitir el acceso hacia afuera:

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -A FORWARD -i ens19 -o ens18 -m state --state RELATED,ESTABLISHED -j
ACCEPT
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -A FORWARD -i ens19 -o ens18 -j ACCEPT
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$
```

E introducimos en el cliente esta linea

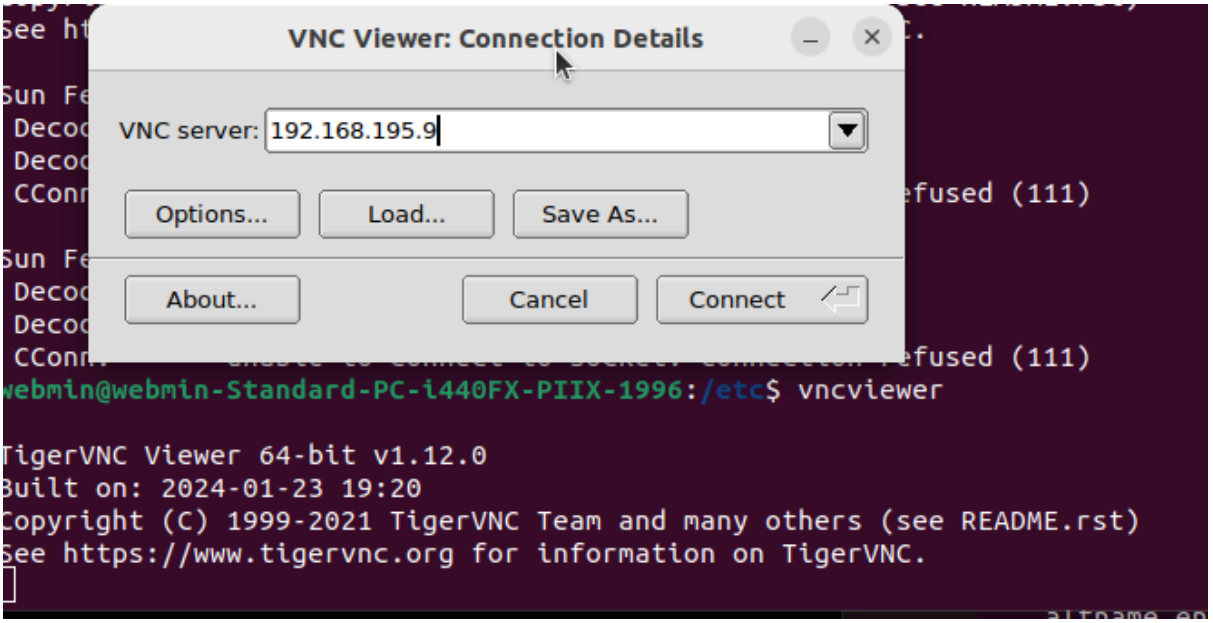
```
user@user-Standard-PC-i440FX-PIIX-1996:~$ sudo ip route add default via 10.254.239.1
```

Y ya tenemos acceso a internet

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ ping 8.8.4.4
PING 8.8.4.4 (8.8.4.4) 56(84) bytes of data.
64 bytes from 8.8.4.4: icmp_seq=1 ttl=113 time=11.6 ms
64 bytes from 8.8.4.4: icmp_seq=2 ttl=113 time=11.4 ms
^C
--- 8.8.4.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 11.356/11.499/11.643/0.143 ms
user@user-Standard-PC-i440FX-PIIX-1996:~$
```

Ahora que tenemos internet, instalaremos VNC en nuestro cliente para poder conectarnos al servidor.

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get install tigervnc-viewer
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libfltk-images1.3 libfltk1.3
Suggested packages:
  tigervnc-tools
The following NEW packages will be installed:
  libfltk-images1.3 libfltk1.3 tigervnc-viewer
0 upgraded, 3 newly installed, 0 to remove and 541 not upgraded.
Need to get 988 kB of archives.
```

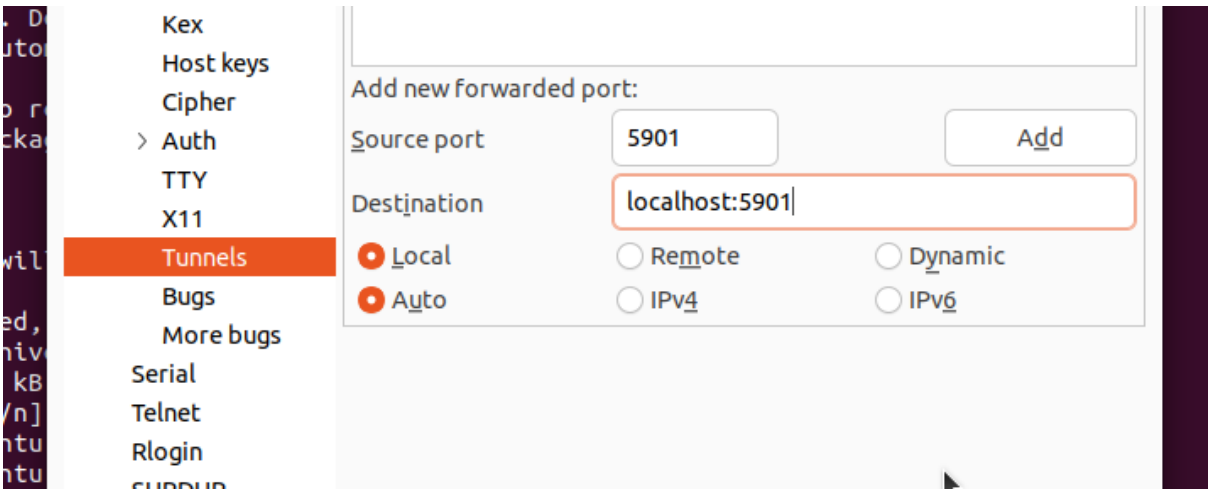


Crea una pasarela SSH y reconfigura el cliente VNC para conectar a través de dicha pasarela.

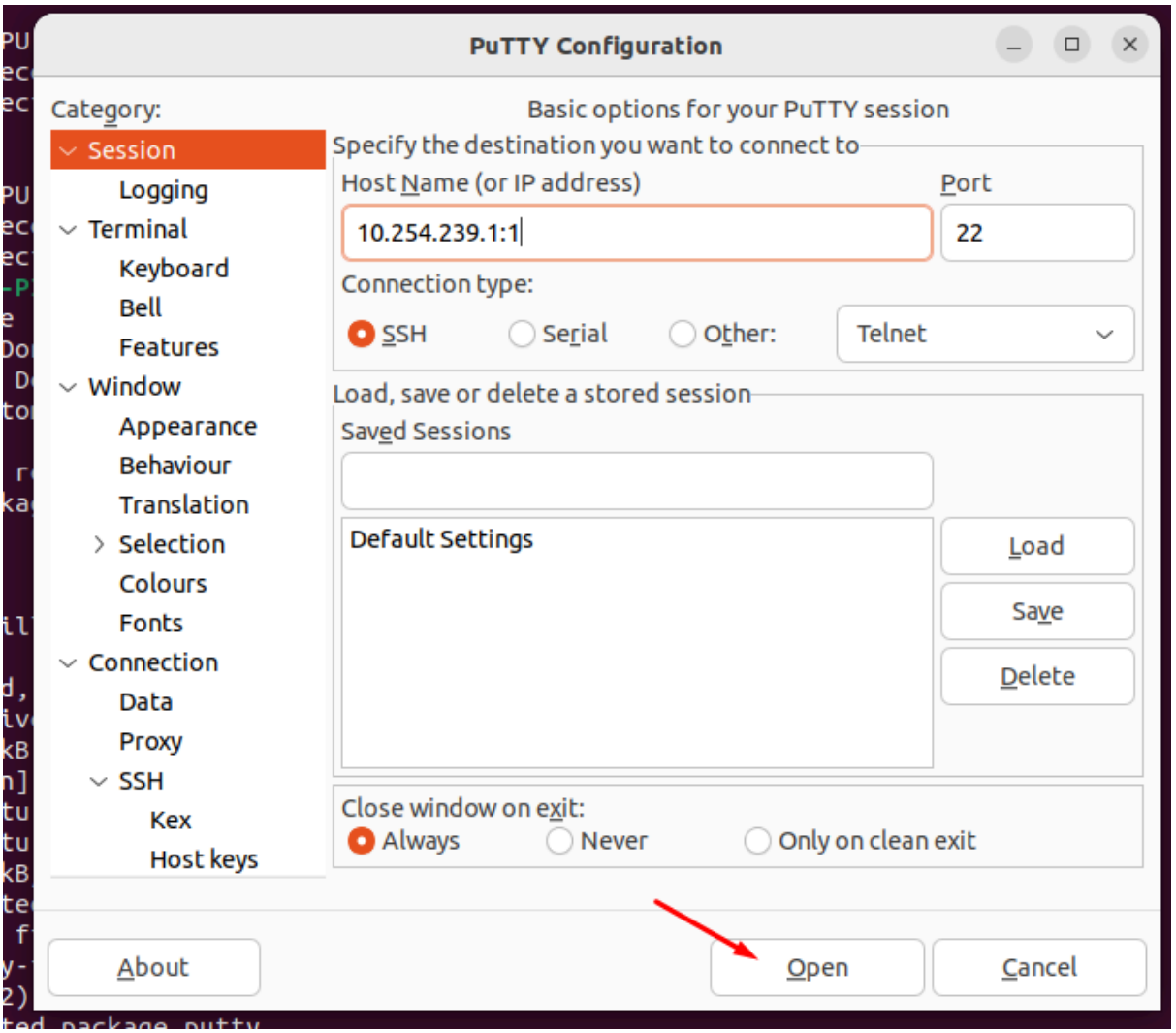
Para conectarse al servidor mediante una pasarela SSH vamos a utilizar PuTTy. Lo descargamos en el cliente con apt-get install putty y una vez instalado lo abrimos con la consola escribiendo “putty”. Ahora vamos a configurar el túnel de la siguiente manera:

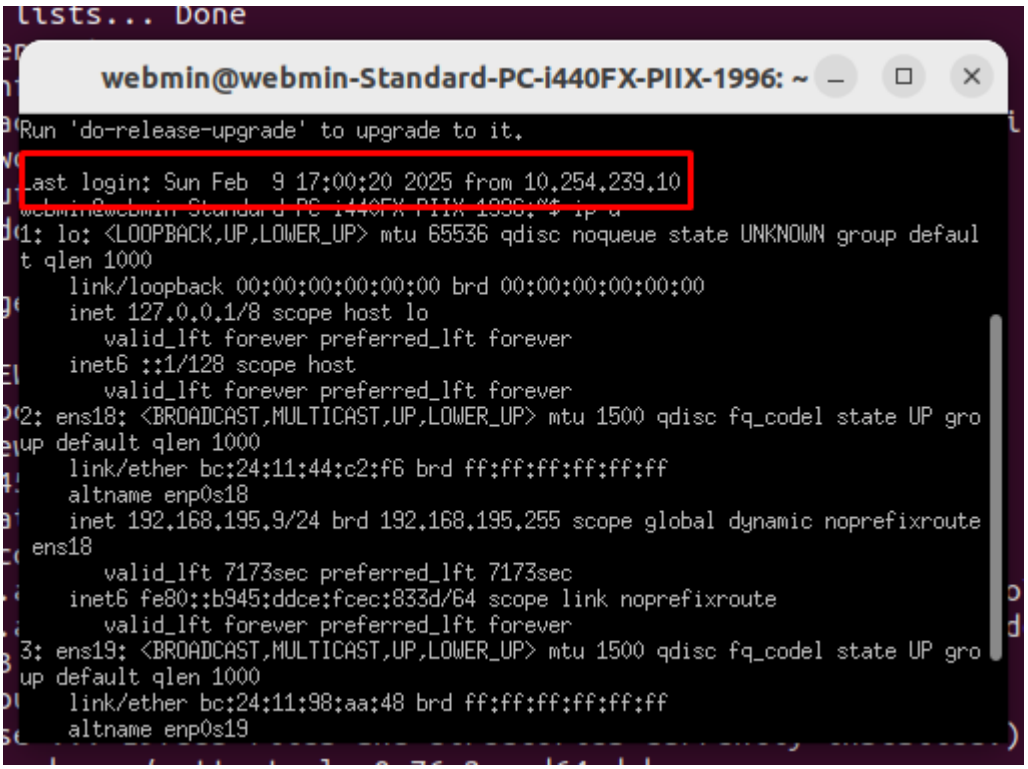
```
user@user-Standard-PC-i440FX-PIIX-1996:~/Desktop$ sudo apt install putty
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  putty-tools
Suggested packages:
```

En el apartado Tunnels introducir estos datos



Vamos al apartado de sesión y ahí introducimos la IP de nuestro servidor seguido de ":" y el número que nos indicaba al momento de instalar tightvnc en nuestro servidor.





Realiza un filtrado de paquetes salientes de forma que ningún equipo de la red tenga acceso al exterior.

Para que ningún equipo pueda salir al exterior tenemos que modificar las iptables que tenemos activas actualmente. Estas son las iptables actuales:

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -S
[sudo] password for webmin:
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A FORWARD -i ens19 -o ens18 -j ACCEPT
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$
```

introducimos iptables -P FORWARD DROP

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -P FORWARD DROP
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD DROP
-P OUTPUT ACCEPT
-A FORWARD -i ens19 -o ens18 -j ACCEPT
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$
```

iptables -F FORWARD y eliminar las de salida
para el servidor con iptables -P OUTPUT DROP

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -F FORWARD
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD DROP
-P OUTPUT ACCEPT
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -P OUTPUT DROP
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD DROP
-P OUTPUT DROP
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$
```

Como podemos comprobar, se ha eliminado la regla que creamos anteriormente que permitía a los equipos clientes salir al exterior y, además, se ha modificado la regla que le permitía al servidor salir al exterior. Si ahora intentamos hacer ping a cualquier sitio web no podremos enviarlo.

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6121ms
```

Y el cliente tampoco

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ ping 8.8.8.8
ping: connect: Network is unreachable
user@user-Standard-PC-i440FX-PIIX-1996:~$ ping 192.168.195.9
ping: connect: Network is unreachable
user@user-Standard-PC-i440FX-PIIX-1996:~$ ping 10.254.239.1
PING 10.254.239.1 (10.254.239.1) 56(84) bytes of data.
^C
--- 10.254.239.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3085ms
```

Realiza un filtrado de paquetes entrantes de forma que ningún equipo del exterior tenga acceso a la red interna.

Para hacer que los paquetes entrantes no lleguen a ningún equipo tenemos que modificar la regla de entrada de nuestras iptables y asignarle el valor DROP. Para ello usamos iptable -P INPUT DROP

```
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD DROP
-P OUTPUT DROP
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -P INPUT DROP
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ sudo iptables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT DROP
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$
```

```
-P OUTPUT DROP
webmin@webmin-Standard-PC-i440FX-PIIX-1996:/etc$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2082ms
```

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ ping 8.8.8.8
ping: connect: Network is unreachable
user@user-Standard-PC-i440FX-PIIX-1996:~$ ping 192.168.195.9
ping: connect: Network is unreachable
user@user-Standard-PC-i440FX-PIIX-1996:~$ ping 10.254.239.1
PING 10.254.239.1 (10.254.239.1) 56(84) bytes of data.
^C
```