

LABRED 2 – Simulación de NAT con pfSense

1. Objetivo. – Implementar y configurar el servicio NAT utilizando pfSense, con el propósito de analizar su funcionamiento en su entorno de red virtual y verificar la conectividad del cliente de forma exitosa.

2. Herramientas. - Para este laboratorio se utilizarán:

- Oracle VirtualBox.
- pfSense (gateway/firewall).
- Cliente Ubuntu (máquina virtual)

3. Procedimiento

3.1 Instalación y configuración pfSense

1. Se realizó la instalación de pfSense a partir de su imagen ISO oficial.
2. Antes de iniciar la máquina virtual, se configuraron dos adaptadores de red en VirtualBox:
 - Adaptador 1 (NAT): proporciona conectividad hacia el host real.
 - Adaptador 2 (Red interna): permite la comunicación entre máquinas virtuales.
3. Al iniciar pfSense, el sistema detectó ambas interfaces de red (ver Figura 1).

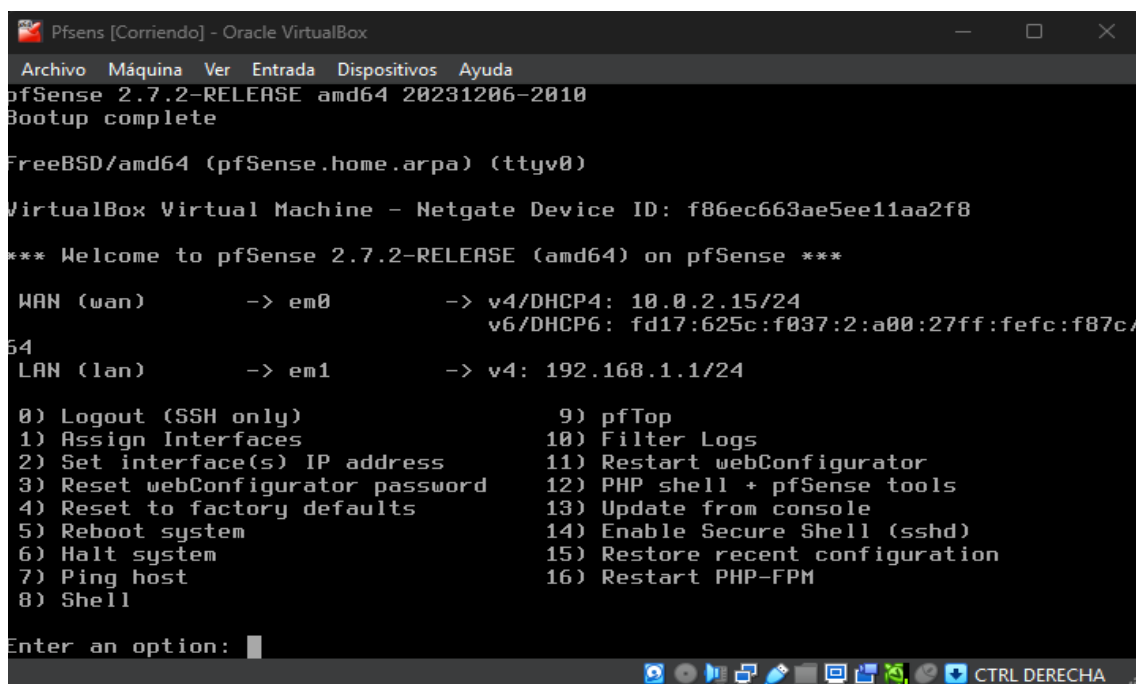
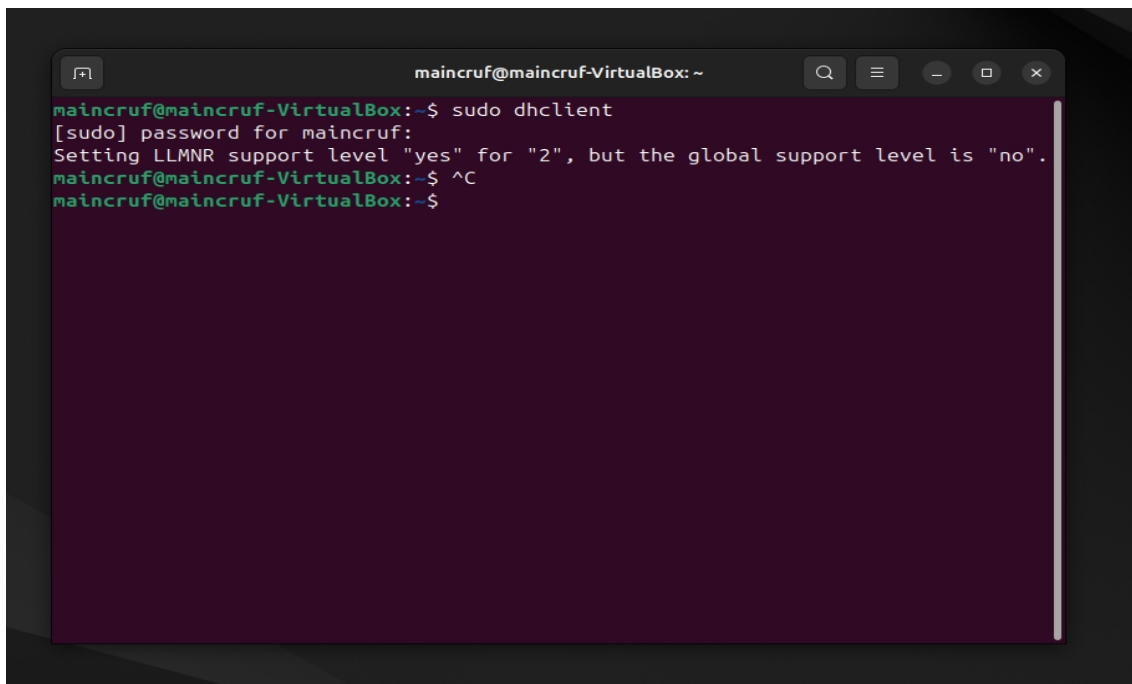


Figura 1. pfSense funcionando correctamente con interfaces WAN y LAN

3.2 Configuración de la red de Ubuntu

Para este laboratorio, previamente se realizó la instalación de la versión mas reciente de Ubuntu 24.04.2 LTS correspondiente a la última actualización disponible hasta el momento hecho este laboratorio, y se procedió con los siguientes pasos para su correcta configuración:

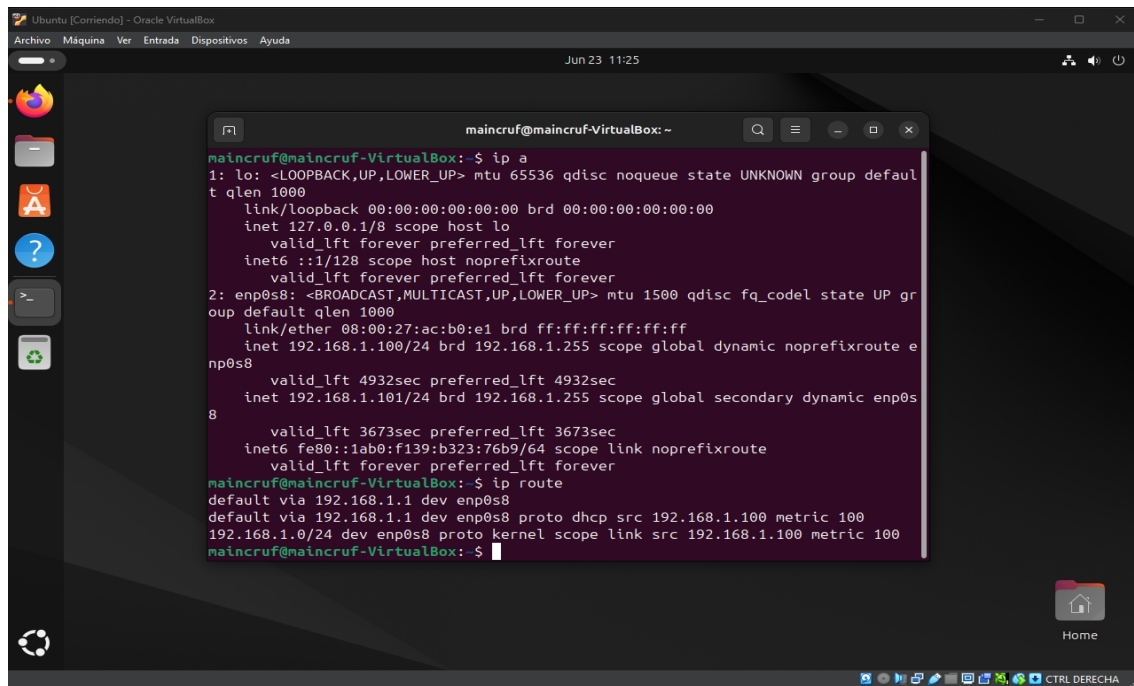
1. Antes de iniciar la máquina virtual, en su configuración de red, se añadió un adaptador de red interna, permitiendo la conexión directa entre el cliente virtual al pfSense.
2. Una vez iniciado el sistema, se accedió a la terminal para solicitar una dirección IP mediante el comando “sudo dhclient”, esto activa la solicitud al servidor DHCP de pfSense, quien asigna una IP dinámica al cliente.



```
maincruf@maincruf-VirtualBox: ~  
maincruf@maincruf-VirtualBox:~$ sudo dhclient  
[sudo] password for maincruf:  
Setting LLMNR support level "yes" for "2", but the global support level is "no".  
maincruf@maincruf-VirtualBox:~$ ^C  
maincruf@maincruf-VirtualBox:~$
```

Figura 2. Solicitando dirección IP al DHCP de pfSense

3. Se validó la asignación correcta de la dirección IP mediante el comando “ip a”, el cual permitió visualizar la IP dinámica asignada y verificar el estado de la red. Posteriormente, se verificó la ruta de salida (gateway) a través del comando “ip route”. La dirección IP identificada como puerta de enlace coincidió con la IP LAN asignada por pfSense (ver Figura 1), lo cual confirmó la correcta conectividad entre el cliente y el gateway.

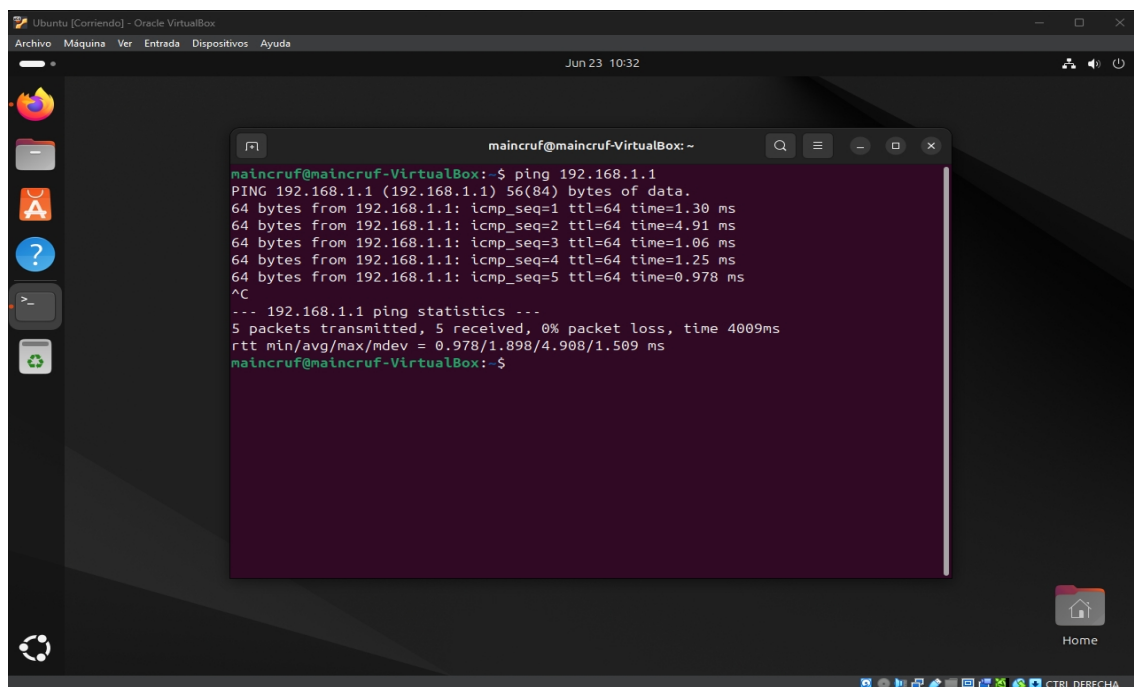


```
maincruf@maincruf-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ac:b0:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s8
        valid_lft 4932sec preferred_lft 4932sec
    inet 192.168.1.101/24 brd 192.168.1.255 scope global secondary dynamic enp0s8
        valid_lft 3673sec preferred_lft 3673sec
    inet6 fe80::1ab0:f139:b323:76b9/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
maincruf@maincruf-VirtualBox:~$ ip route
default via 192.168.1.1 dev enp0s8
default via 192.168.1.1 dev enp0s8 proto dhcp src 192.168.1.100 metric 100
192.168.1.0/24 dev enp0s8 proto kernel scope link src 192.168.1.100 metric 100
maincruf@maincruf-VirtualBox:~$
```

Figura 3. Visualización de la dirección IP asignada por el pfSense y gateway.

3.3 Conectividad y NAT en acción

1. Se comprobó la conectividad de red desde Ubuntu hacia pfSense utilizando el comando ping.



```
maincruf@maincruf-VirtualBox:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=4.91 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.06 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.25 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.978 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 0.978/1.898/4.908/1.509 ms
maincruf@maincruf-VirtualBox:~$
```

Figura 4. Realizando ping hacia el pfSense

2. Posteriormente, se accedió a la interfaz web de pfSense desde el navegador, utilizando la dirección IP del gateway, ingresando las credenciales para visualizar la configuración.

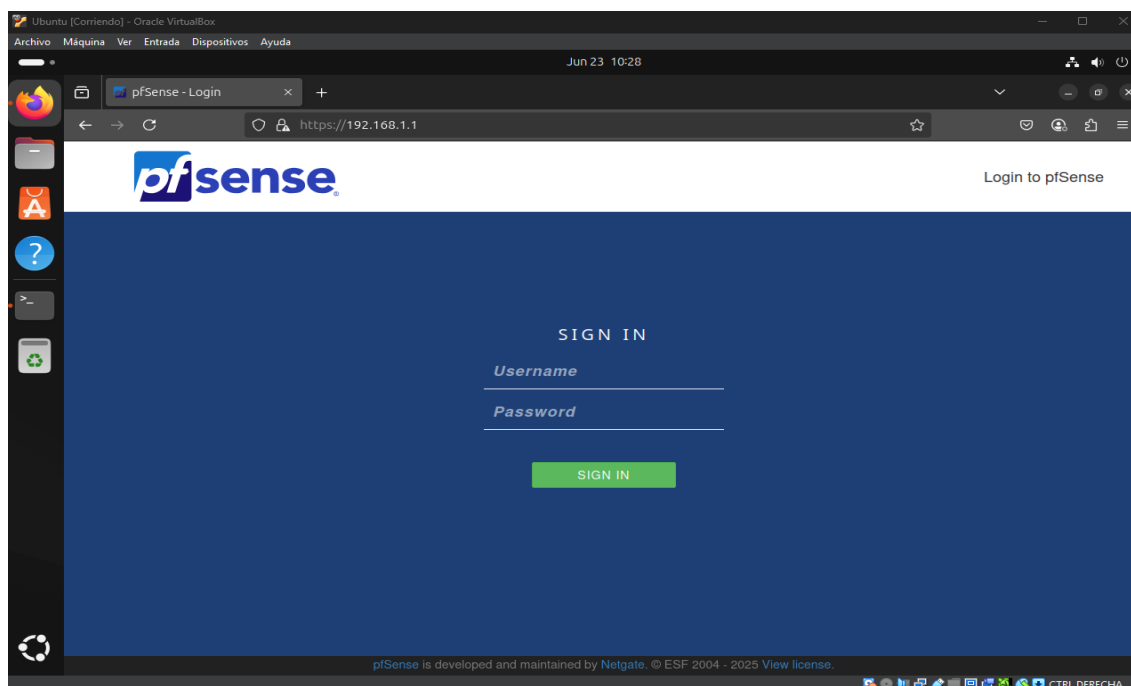


Figura 5. Acceso a la interfaz de administración de pfSense

3. Dentro de la interfaz, se accedió a la ruta Firewall > NAT > Outbound, donde se muestran las reglas automáticas generadas por pfSense para aplicar NAT sobre el tráfico saliente y la red a la que se encuentra.

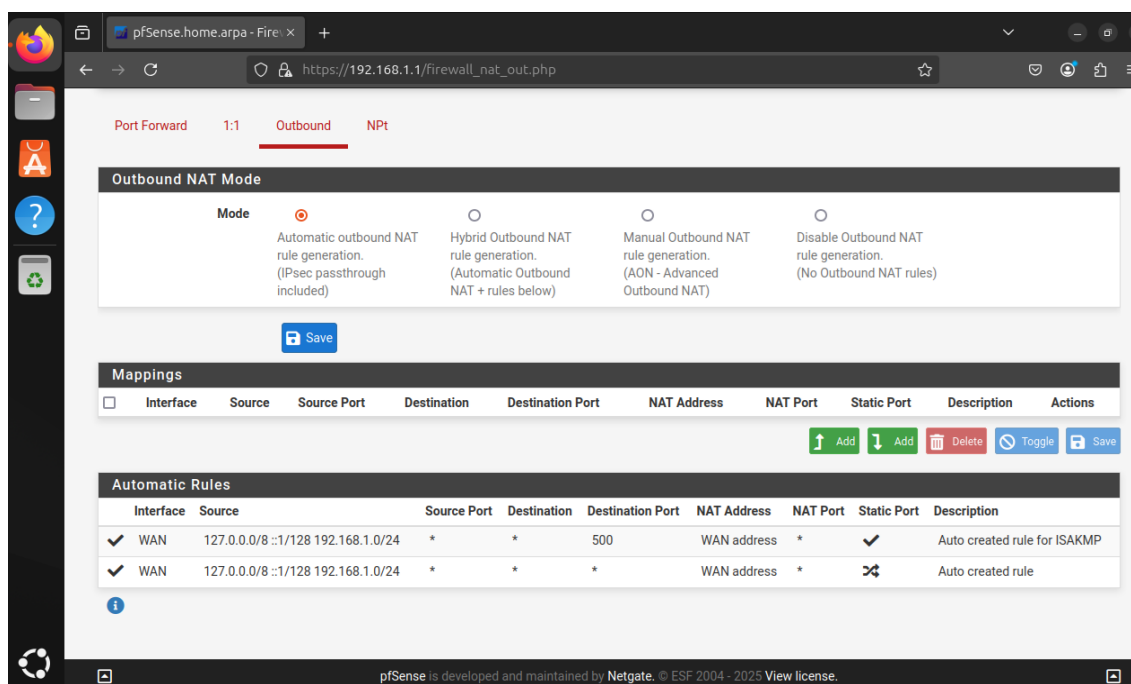


Figura 6. Reglas NAT aplicadas automáticamente en modo Outbound

4. Resultados Obtenidos. - Se evidenció de manera clara el proceso de traducción de direcciones NAT dentro de una red virtual, comprobando su efectividad al permitir que el cliente Ubuntu acceda a servicios a través de una dirección IP diferente a su IP privada original. Además, se observó la presencia de un proceso de doble NAT, ya que la red virtual emplea su propio esquema de traducción, que a su vez es enmascarado por el mecanismo NAT del host real para permitir su salida al internet.

5. Reflexión final. - Este laboratorio permitió comprender el papel fundamental que desempeña el NAT en redes modernas, el cual permite acceso a redes externas desde direcciones privadas, actuando como intermediario que representa toda la red interna, llegando a ser una capa de seguridad al ocultar la estructura de la red y direcciones IP privadas a las redes externas.