Escuela Colombiana de ingeniería Julio Garavito

Seguridad y privacidad de TI

Laboratorio 8

Integrantes

Juan Camargo

Diego Castellanos

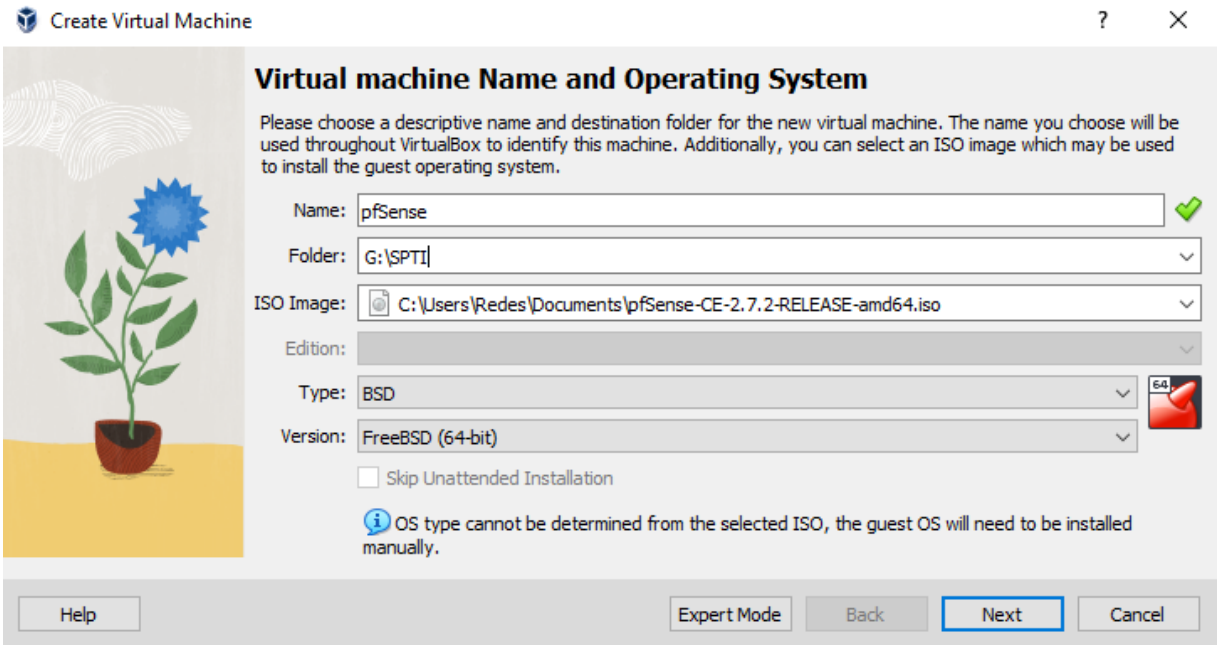
Profesor

Daniel Esteban Vela Lopez

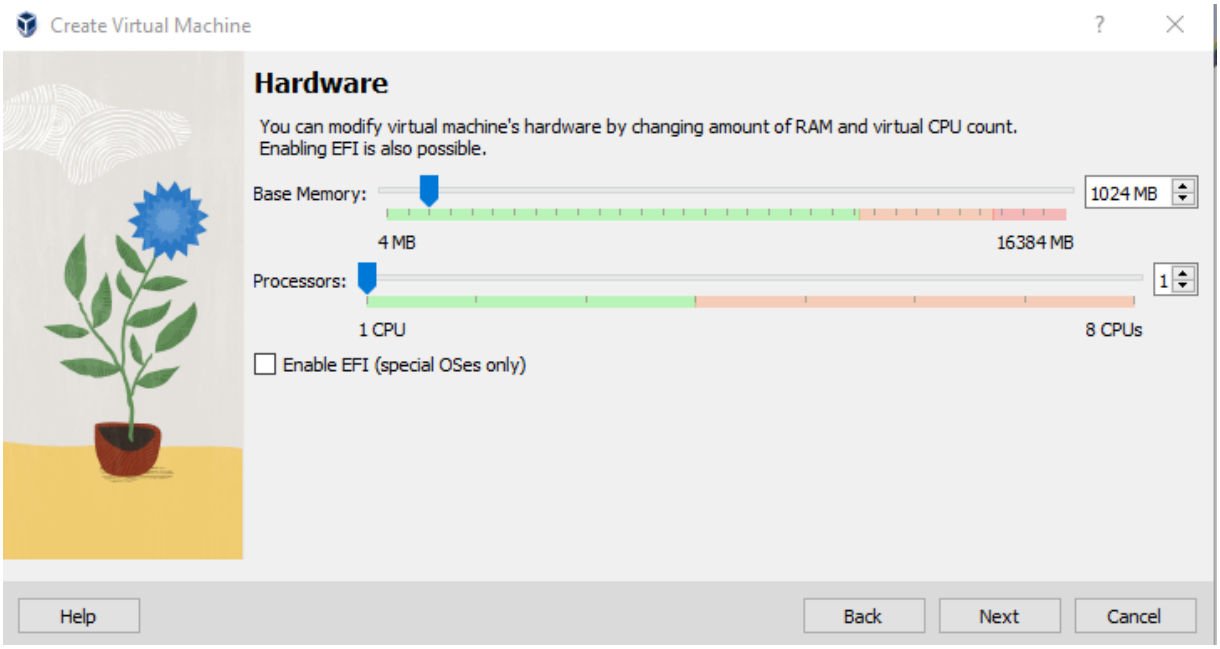
Bogotá 2024

Creación de máquina virtual pfSense

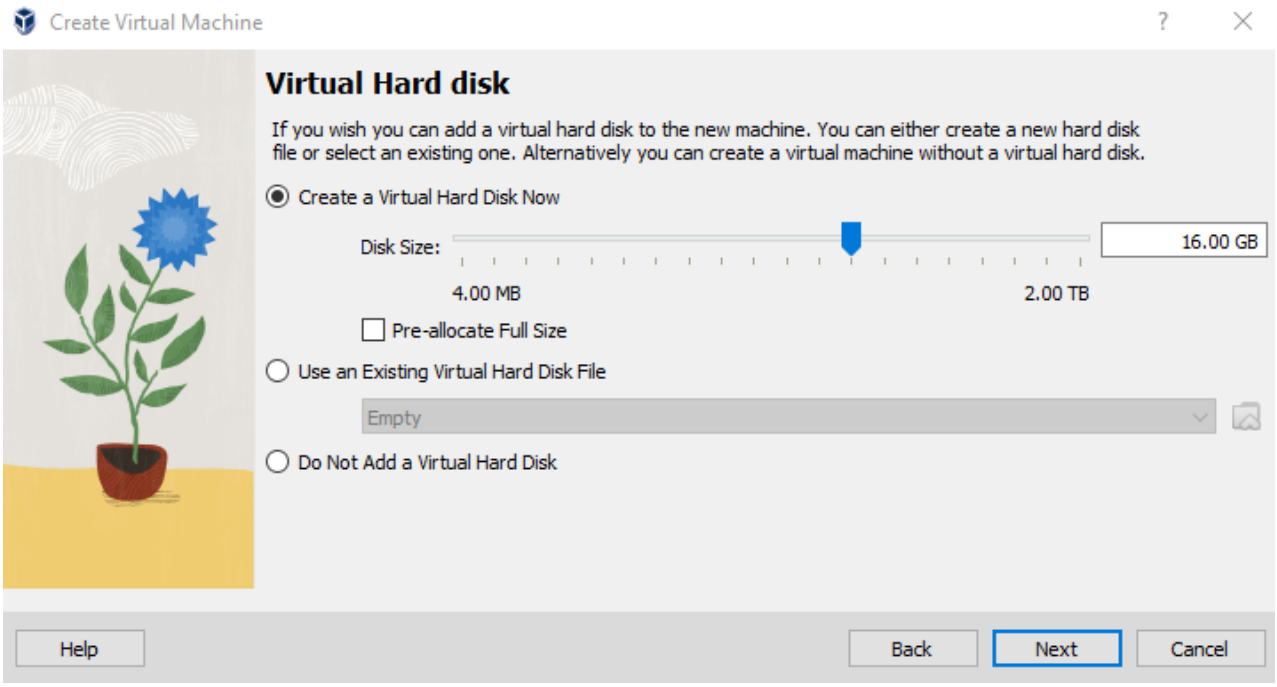
Entramos a virtualBox y creamos una nueva máquina con la imagen ISO de pfSense.

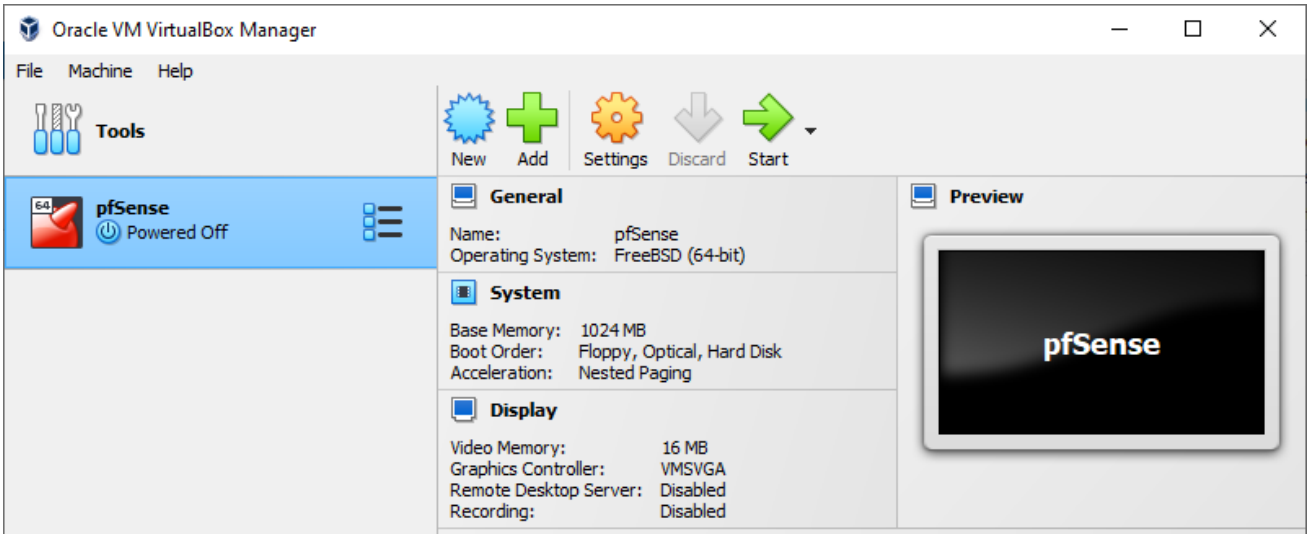


Asignamos una memoria de 1024 MB.



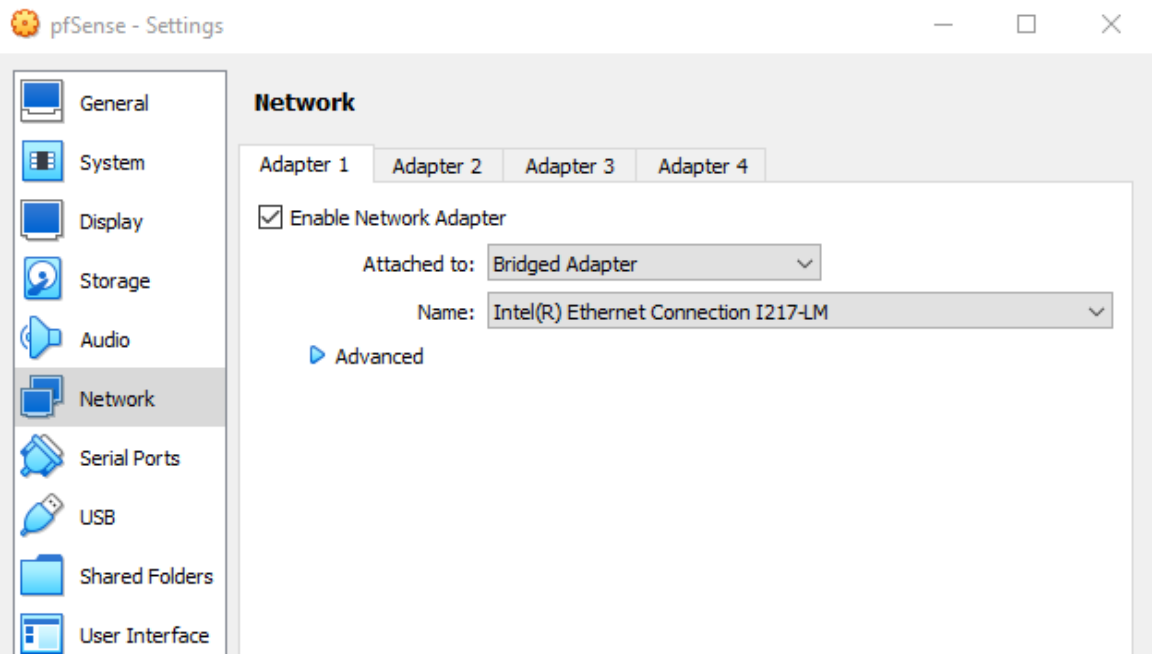
Asignamos un espacio en disco de 16 GB.

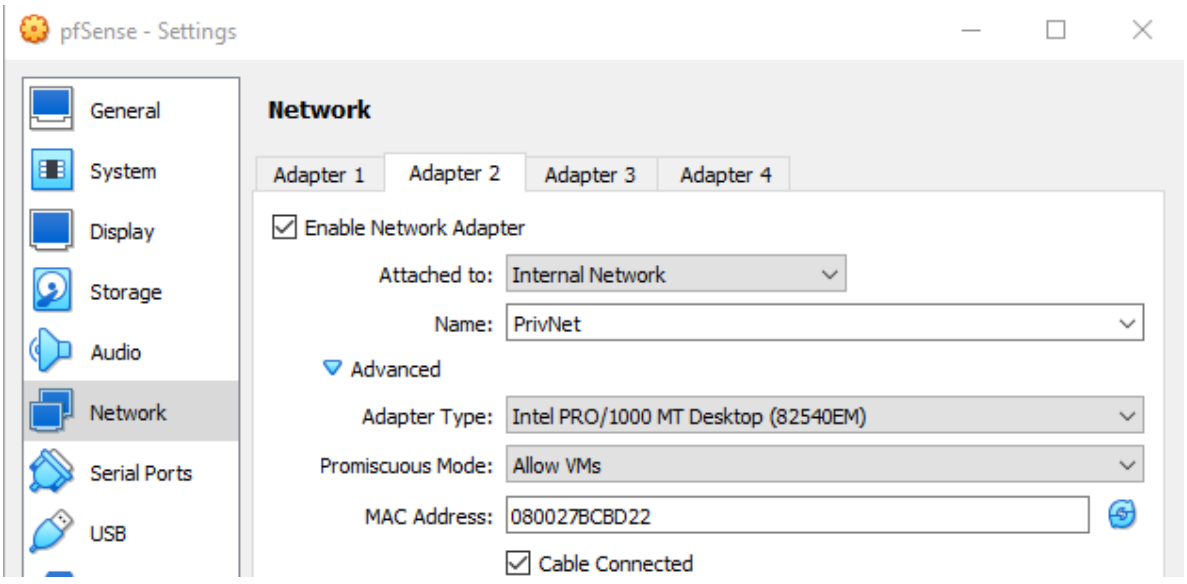




Configurar interfaces de red

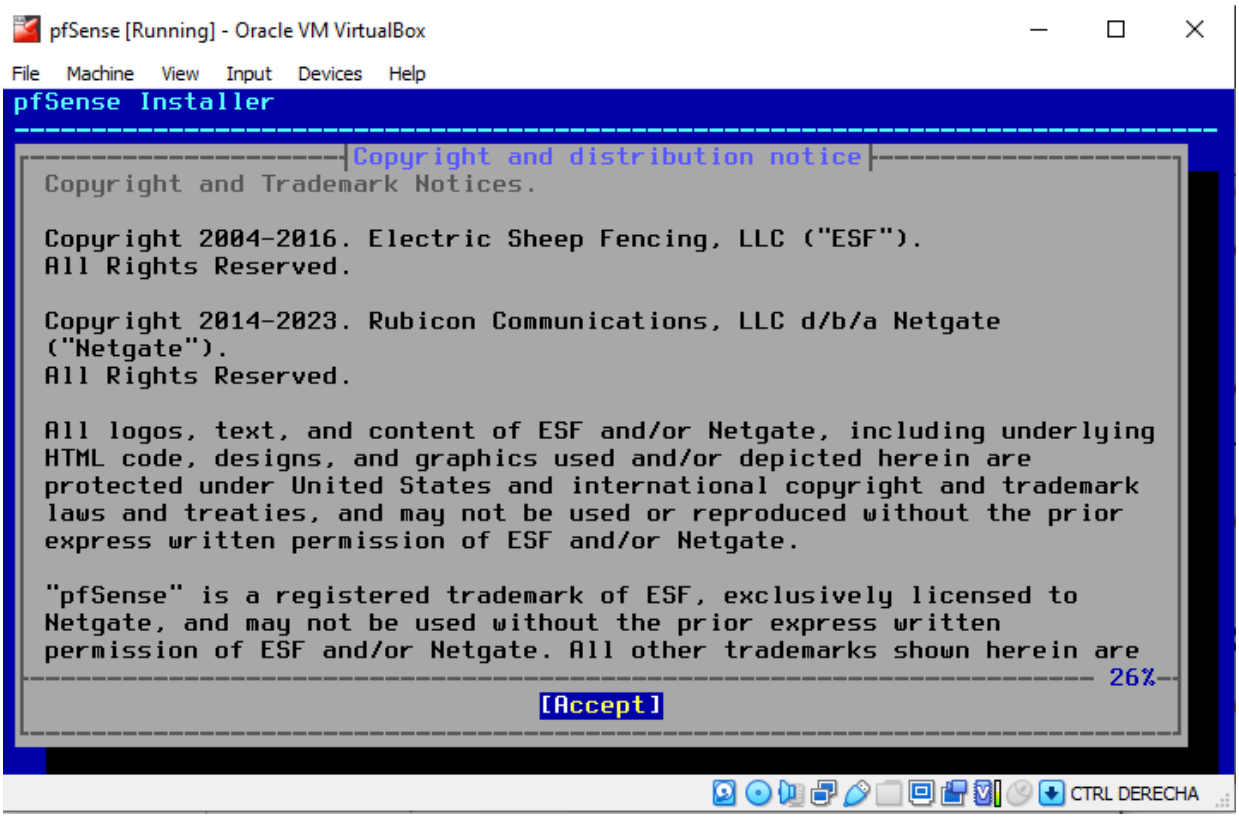
Vamos a las configuraciones de la maquina y nos dirigimos al apartado de red y en el adaptador 1 lo dejamos como puente y el adaptador 2 lo dejamos como red interna y la llamamos PrivNet.

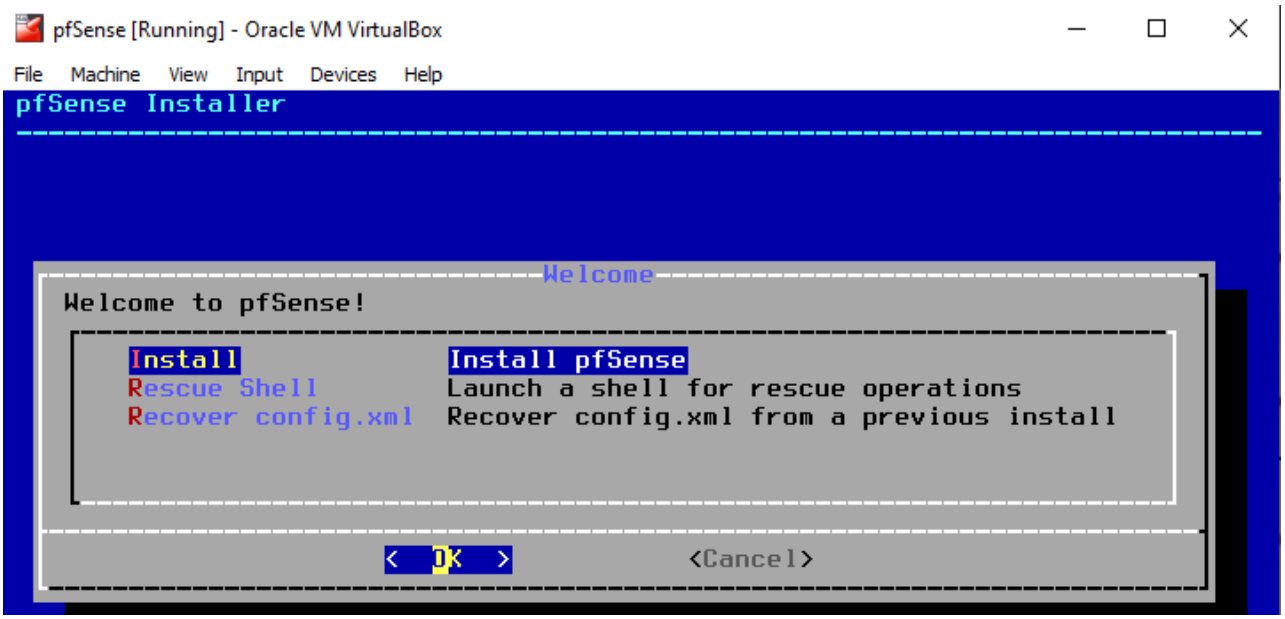




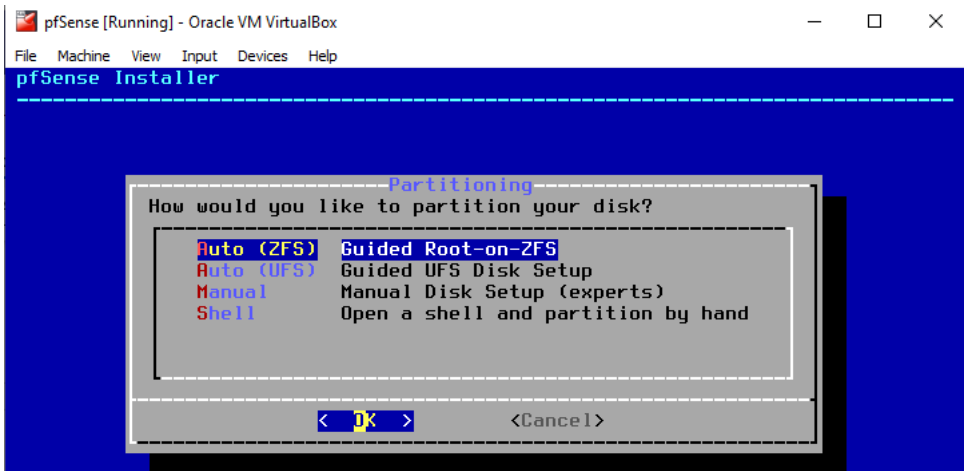
Instalar pfSense

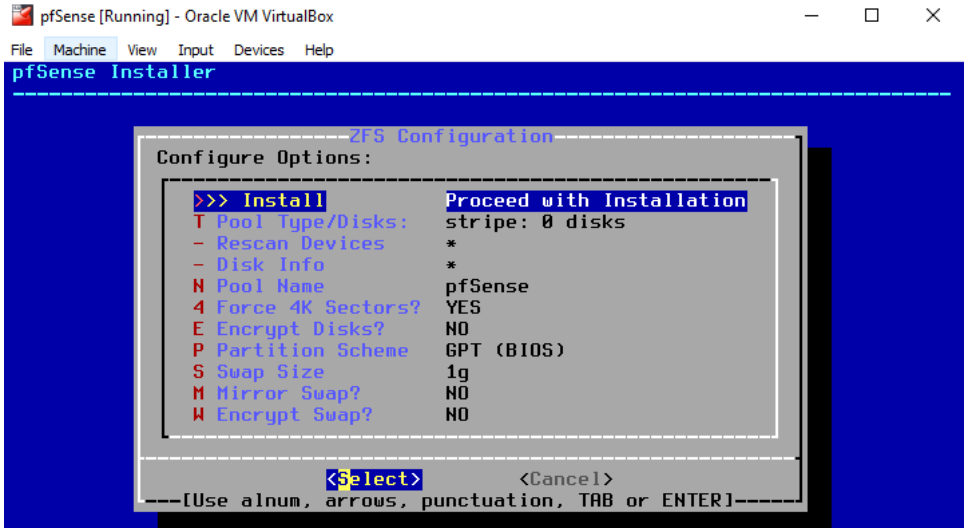
Aceptamos el Copyright y distribución, después, seleccionamos la opción de instalar pfSense.

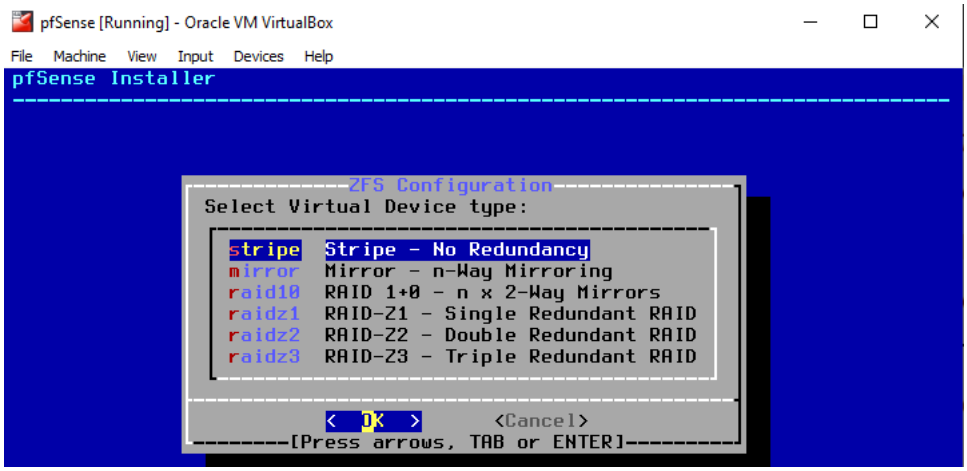


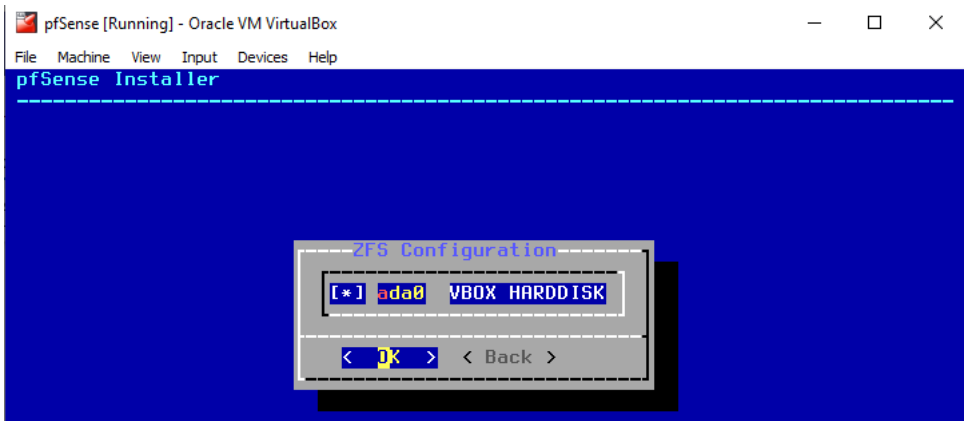


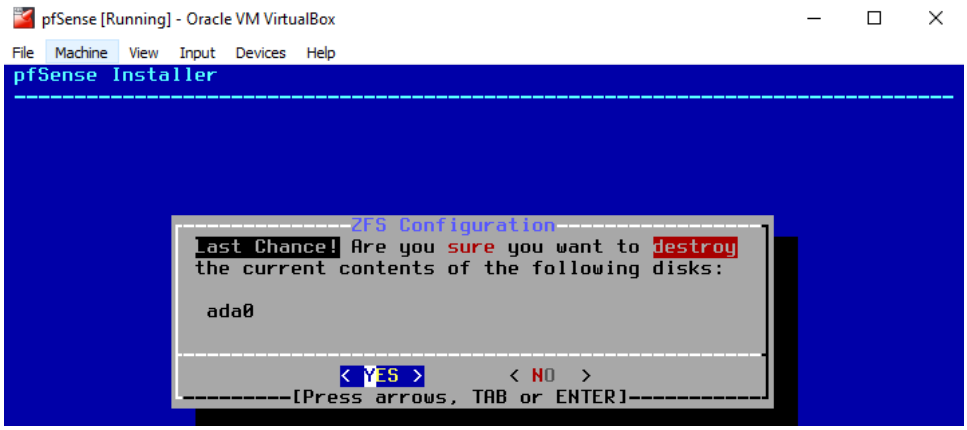
Seguimos los pasos de instalación de pfSense.


pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) Guided UFS Disk Setup
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>

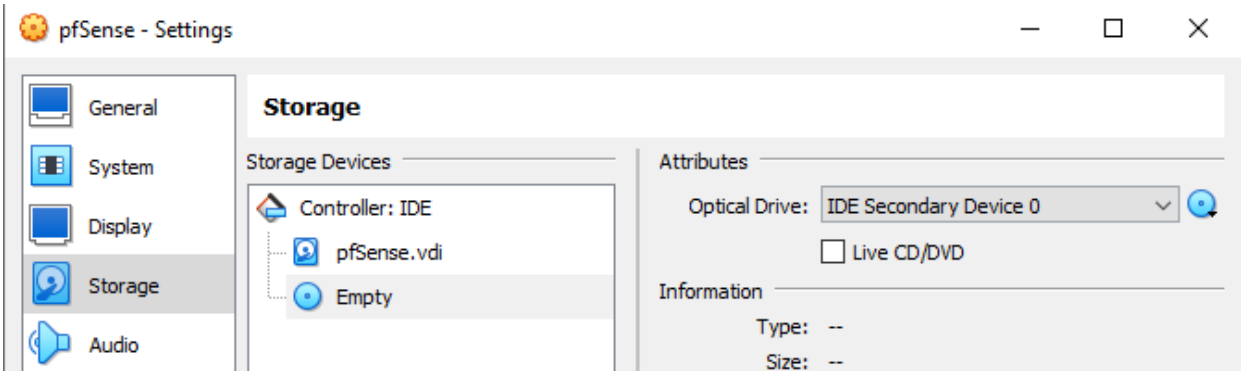

pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>
---[Use alnum, arrows, punctuation, TAB or ENTER]---


pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK > <Cancel>
--------[Press arrows, TAB or ENTER]---------



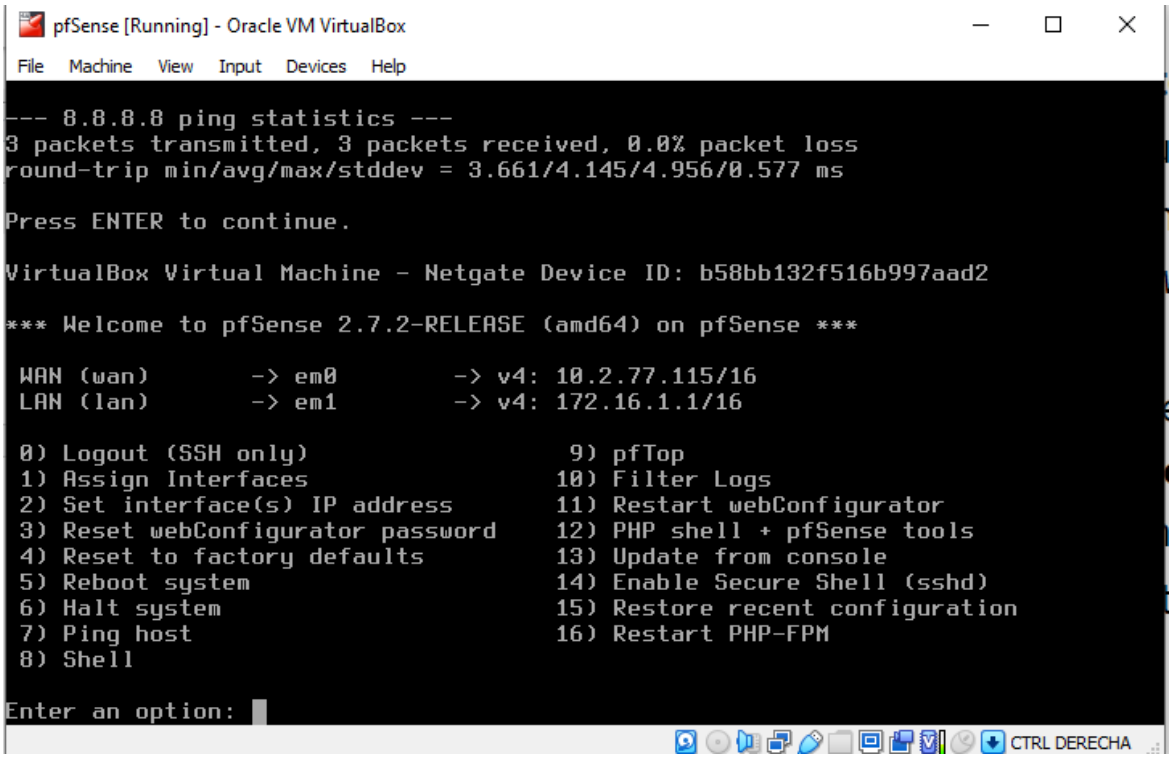


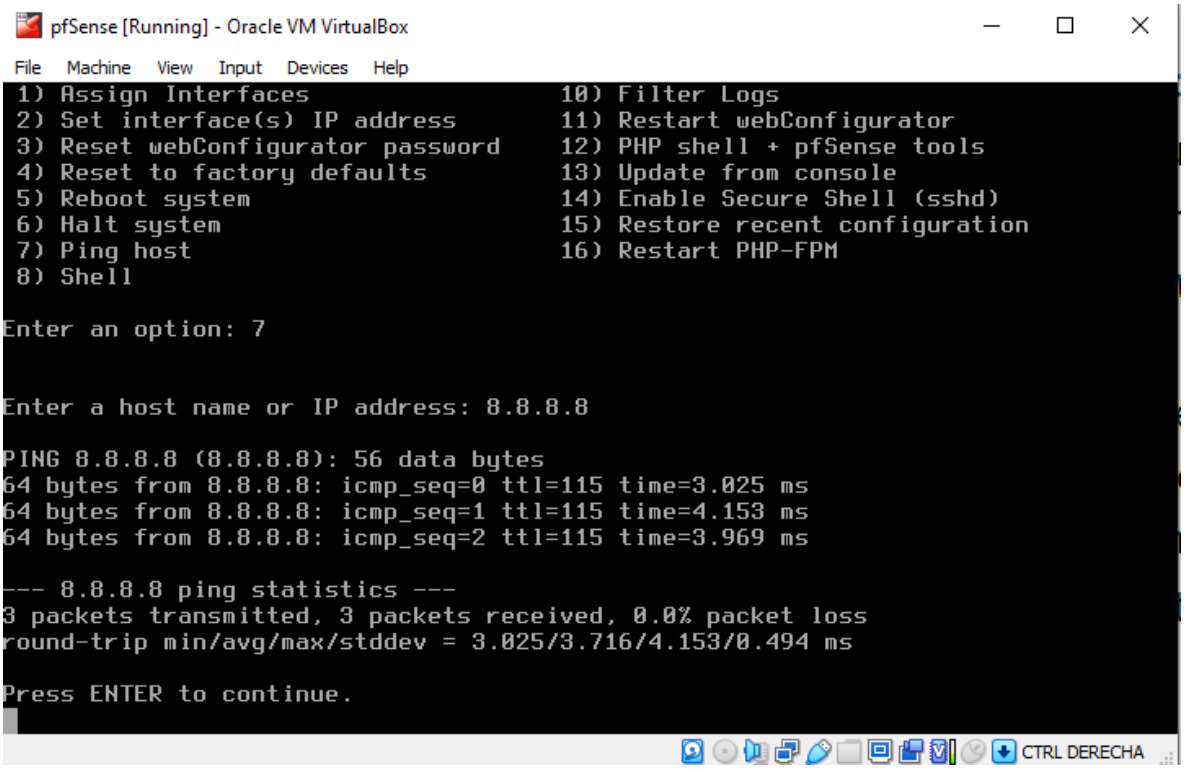
Al finalizar, apagamos la maquina y quitamos la imagen ISO.



Configurar interfaces de red

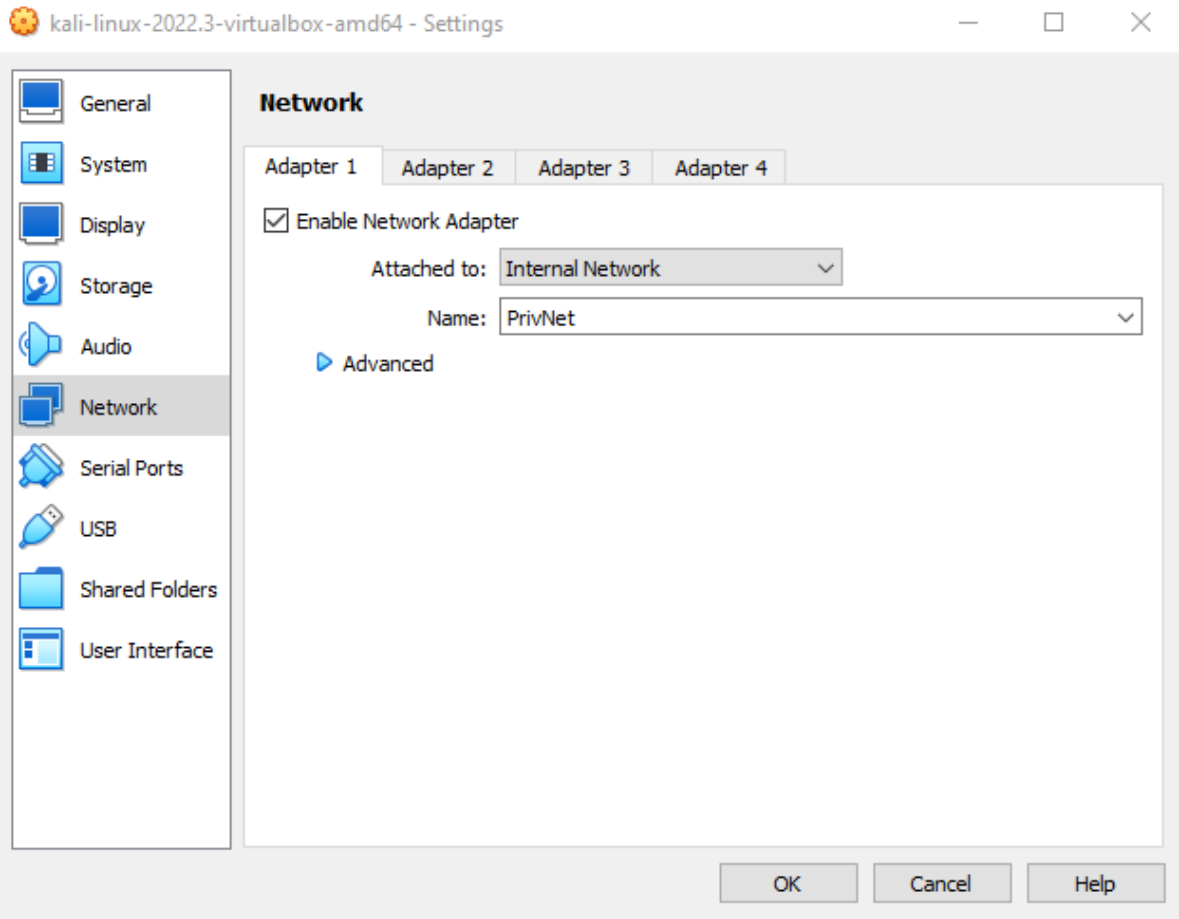
Seleccionamos la opción 2 para configurar las opciones de WAN y LAN y después escogemos la opción 7 para poder revisar que quedó correctamente configurado haciendo ping a 8.8.8.8





Verificar que el servidor DHCP

Abrimos la máquina de kali linux en virtualBox y en configuraciones en el apartado de red, nos dirigimos al adaptador 1 y la hacemos red interna y le colocamos el mismo nombre que a la máquina de pfSense “PrivNet”.

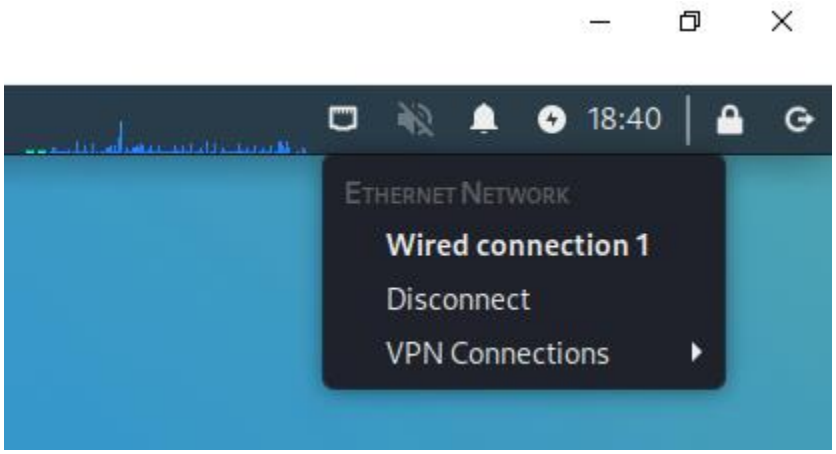


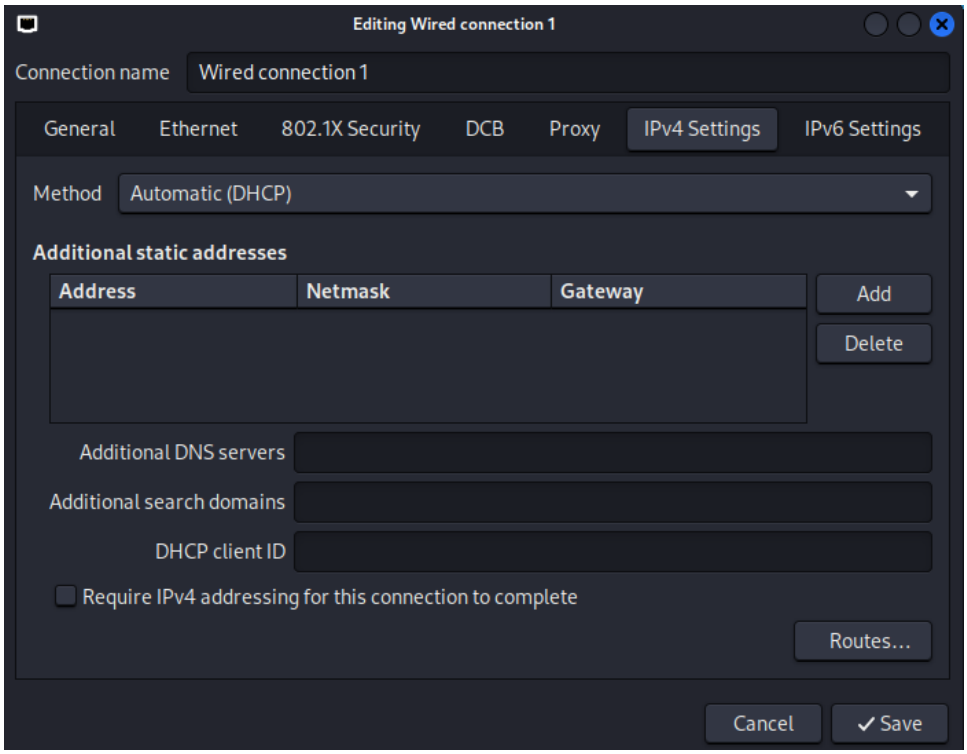
Corremos la máquina y verificamos que la red interna “PrivNet” haya quedada correctamente configurada en la máquina de kali y probamos el ping a la máquina de pfSense para verificar que todo funcione correctamente.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.100  netmask 255.255.0.0  broadcast 172.16.255.255
        inet6 fe80::4e33:2ce:73f0:4bef  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 16  bytes 2810 (2.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54  bytes 6747 (6.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(kali㉿kali)-[~]
└─$ ping 72.16.1.100
PING 72.16.1.100 (72.16.1.100) 56(84) bytes of data.
64 bytes from 72.16.1.100: icmp_seq=1 ttl=47 time=124 ms
64 bytes from 72.16.1.100: icmp_seq=2 ttl=47 time=127 ms
64 bytes from 72.16.1.100: icmp_seq=3 ttl=47 time=114 ms
64 bytes from 72.16.1.100: icmp_seq=4 ttl=47 time=122 ms
```

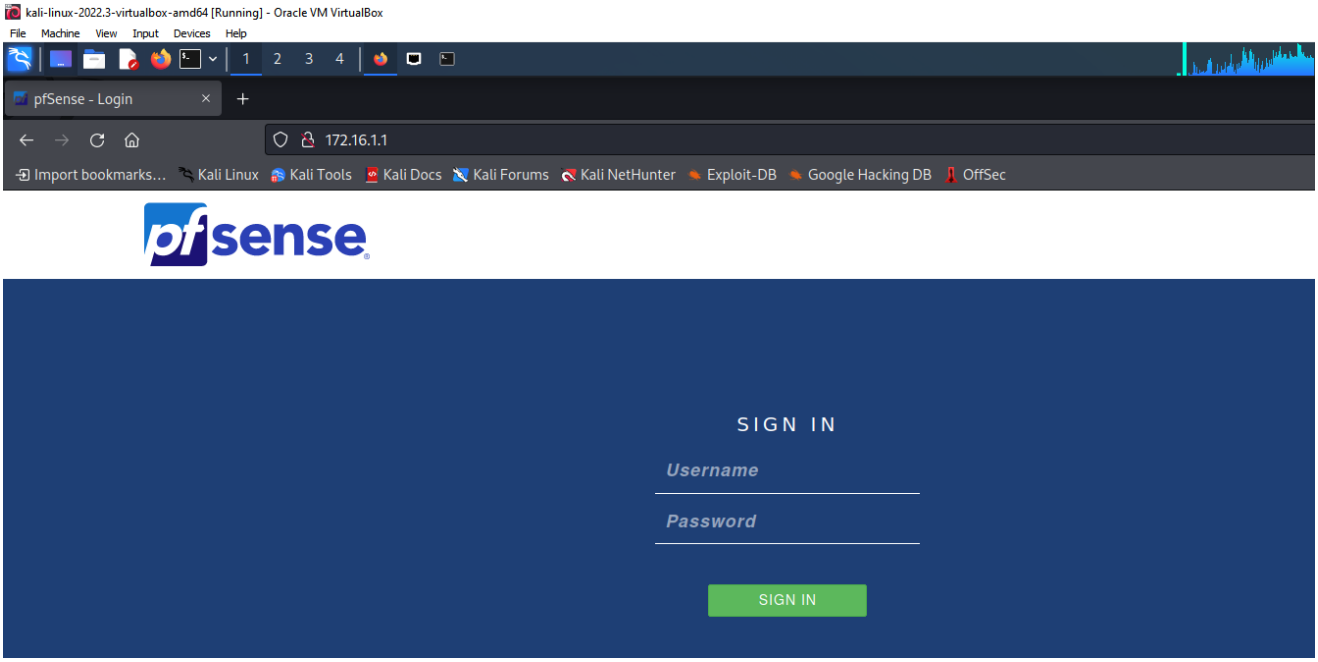
Damos click en el icono de internet y configuramos Wired connection 1 con el IPv4 demo automático y corroboramos que quedó bien haciendo ping a 8.8.8.8



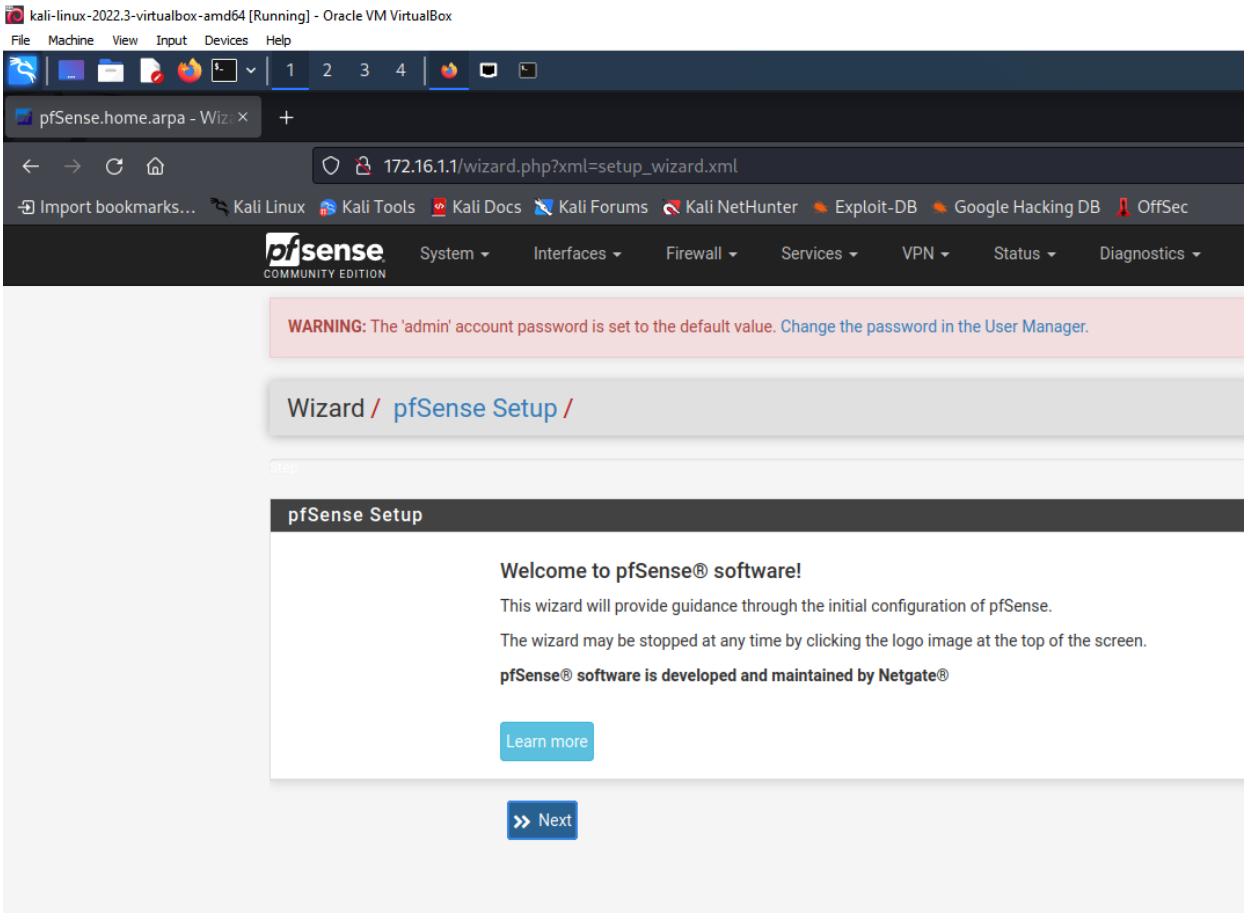


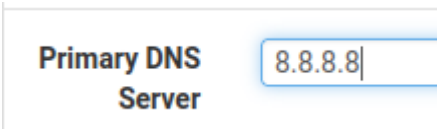
```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=3.55 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=4.30 ms
^Z
zsh: suspended  ping 8.8.8.8
```

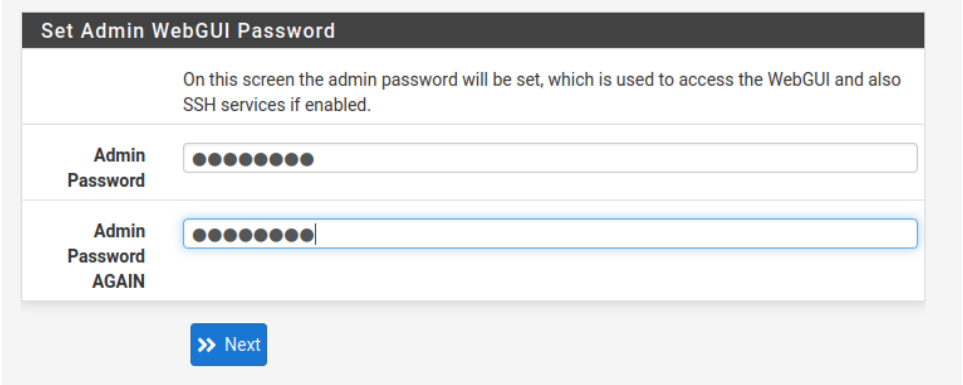
Entramos a mozilla y colocamos en el buscador la IP de la LAN de la maquina pfSense para entrar a su página de configuración.



Seguimos los pasos del asistente asignano el server DNS primario como “8.8.8.8” y cambiando la contraseña del administrador (password).

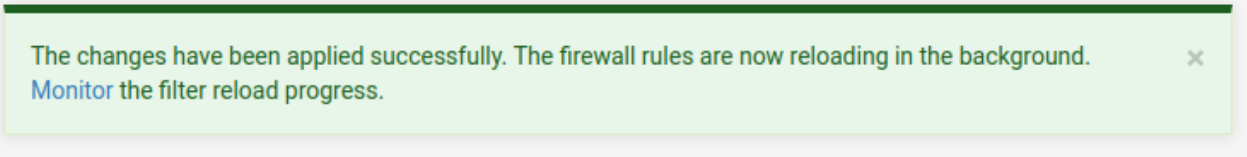


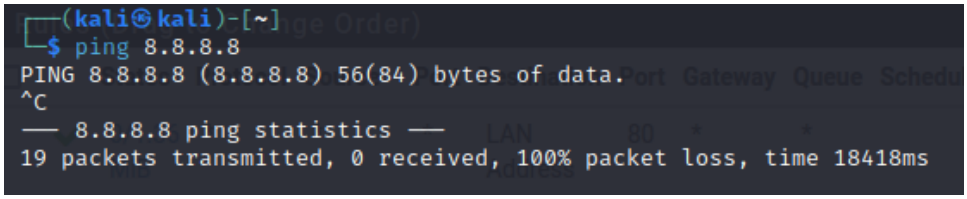




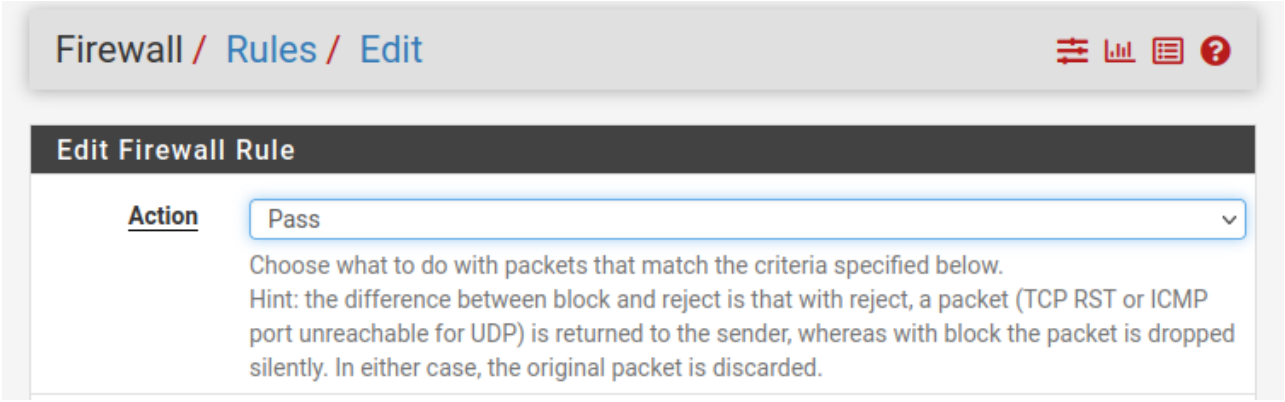
Ahora nos dirigimos a la sección de firewall y editamos las reglas y seguimos los pasos de configuración haciendo que la acción sea de bloqueo, la interfaz sea LAN y el destino de dirección o alias sea el 8.8.8.8

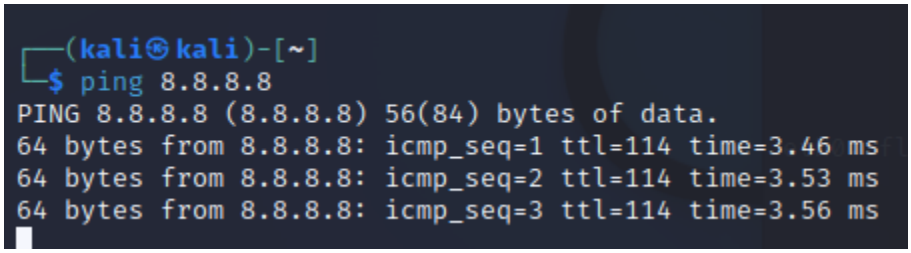
Aplicamos los cambios e intentamos hacer ping a 8.8.8.8 y veremos que no es posible.



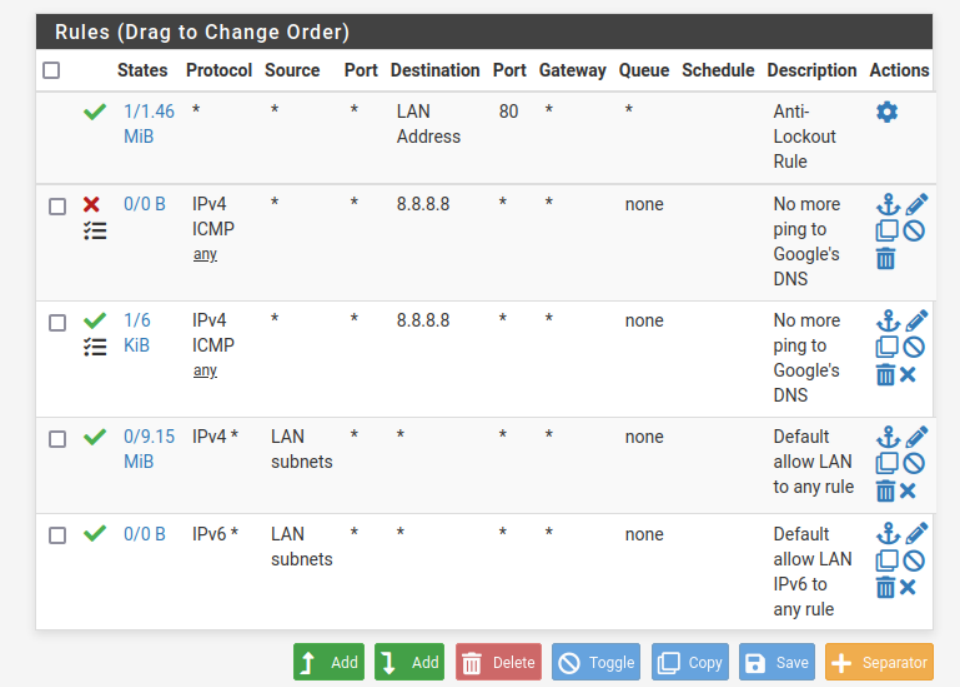


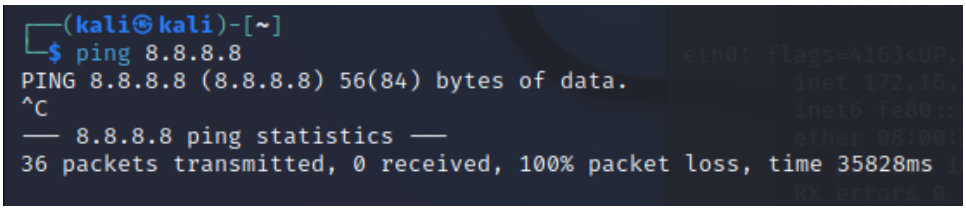
Si volvemos a colocar la acción como de paso y hacemos ping a 8.8.8.8 veremos que si se puede.



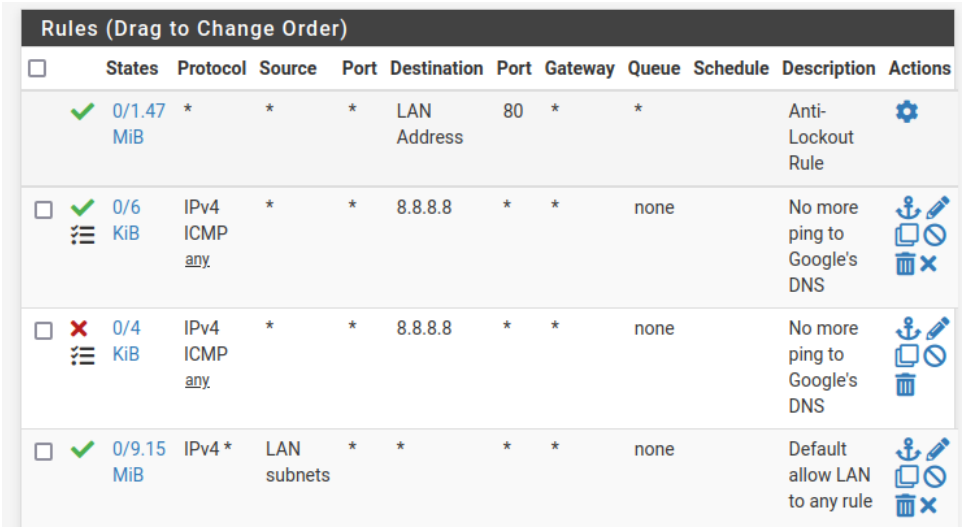


Copiamos la configuración de reglas que creamos anteriormente y la colocamos como de bloqueó y ahora tenemos des reglas, una de paso y una de bloqueo, en este caso, hace efecto la que esté primero en al lista de arriba para abajo, por lo que dejamos la bloqueo antes de la de paso y vemos que hacer ping a 8.8.8.8 no es posible.



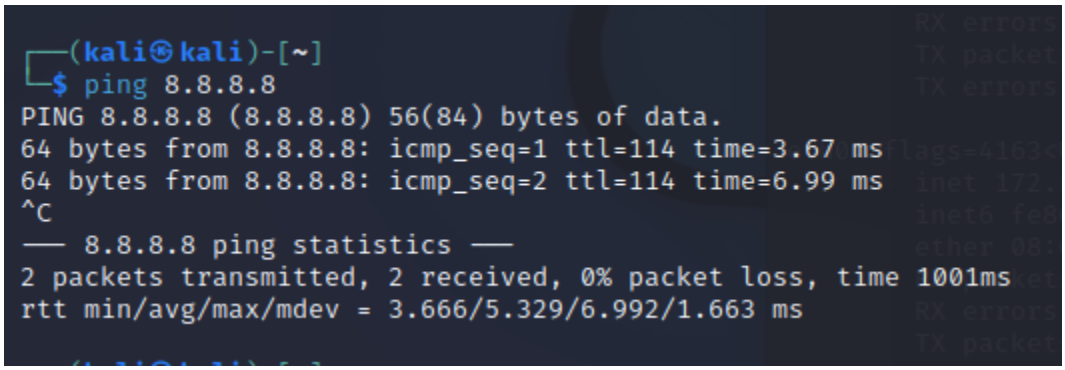


Si dejamos la regla de paso antes que la de bloqueo y hacemos píng a 8.8.8.8 vemos que si es posible.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/1.47 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓	0/6 KiB	IPv4 ICMP any	*	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
✗	0/4 KiB	IPv4 ICMP any	*	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
✓	0/9.15 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	



```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=3.67 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=6.99 ms
^C
── 8.8.8.8 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 3.666/5.329/6.992/1.663 ms
```

Con esto podemos afirmar que hemos configurado satisfactoriamente pfSense para que sea un router, un servidor DHCP y un firewall.