

Escuela Colombiana de ingeniería Julio Garavito

Seguridad y privacidad de TI

Laboratorio 8

Integrantes

Juan Camargo

Diego Castellanos

Profesor

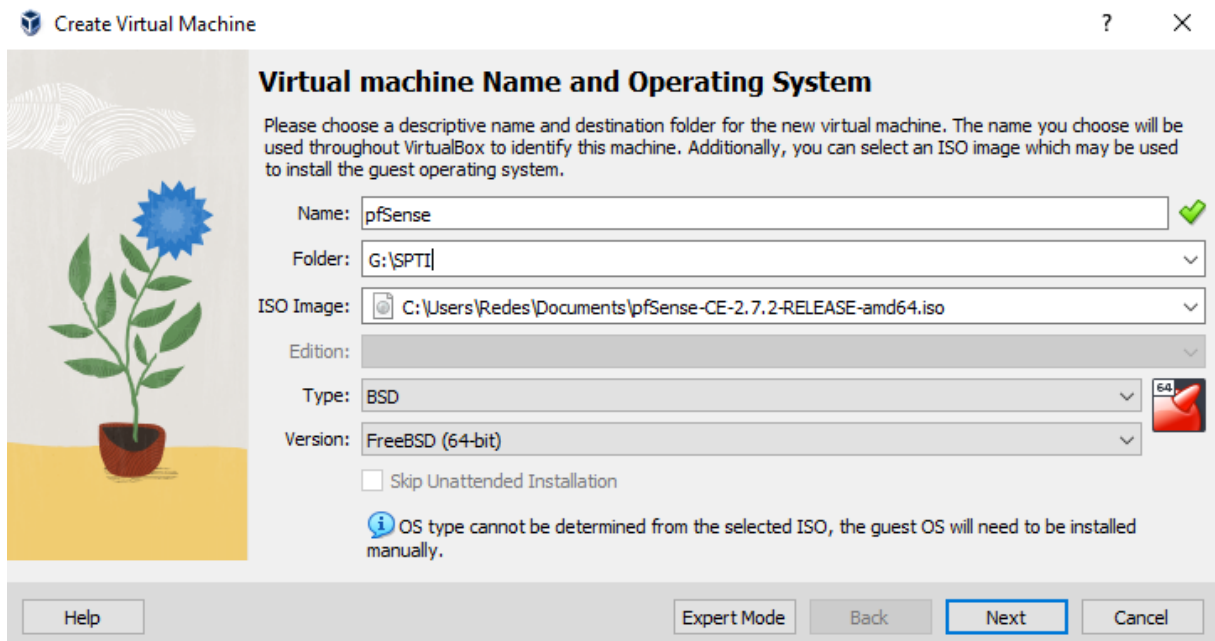
Daniel Esteban Vela Lopez

Bogotá 2024

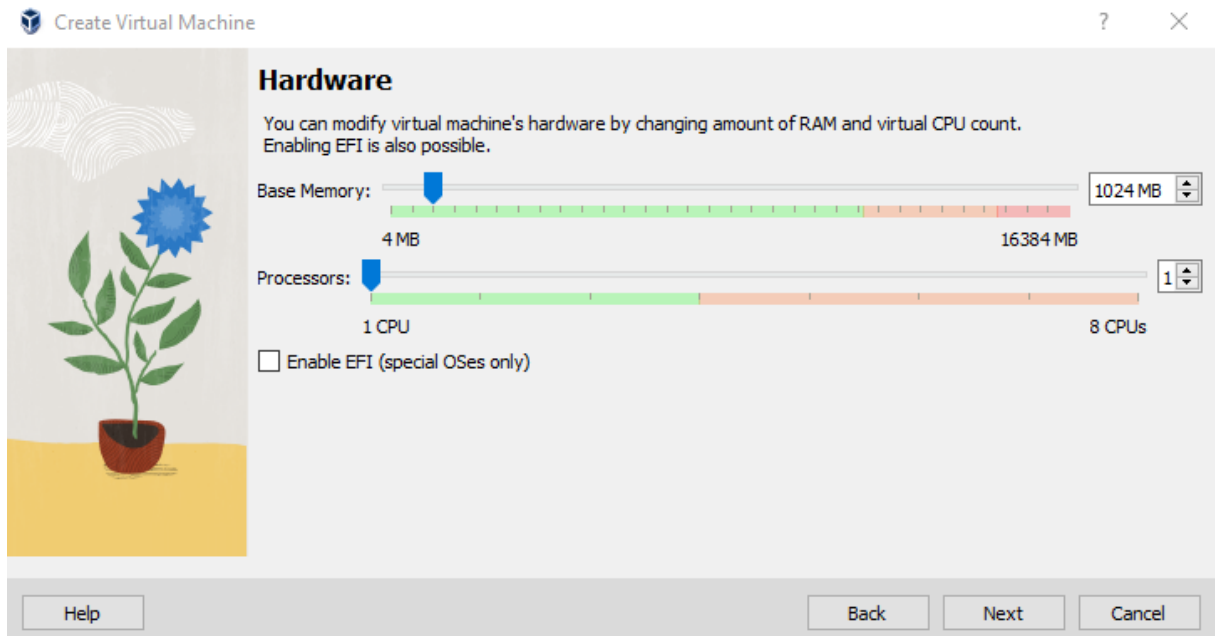


Creación de máquina virtual pfSense

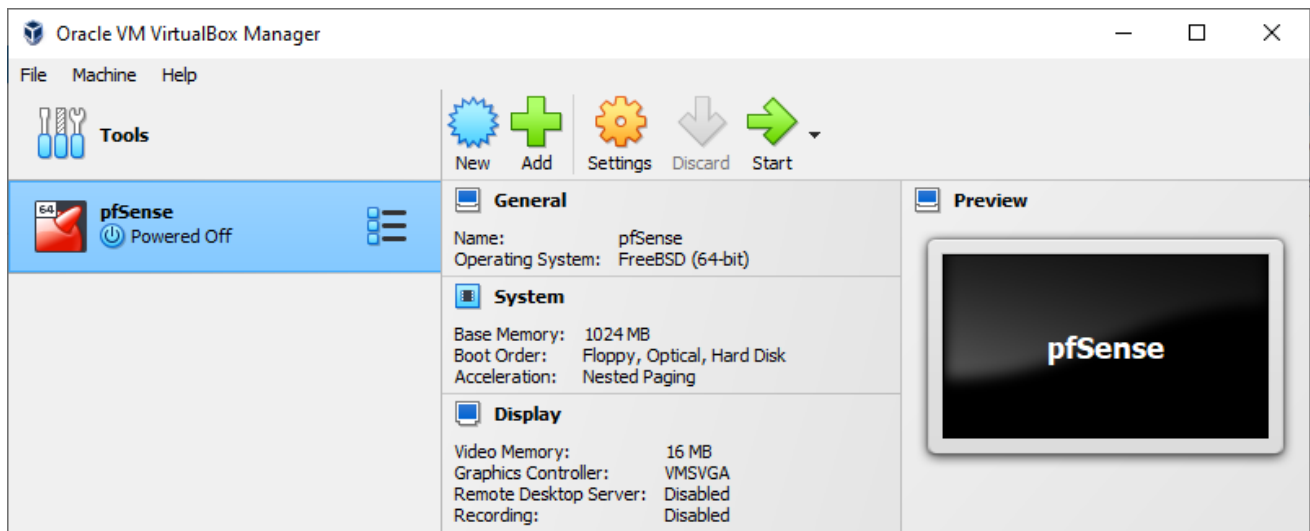
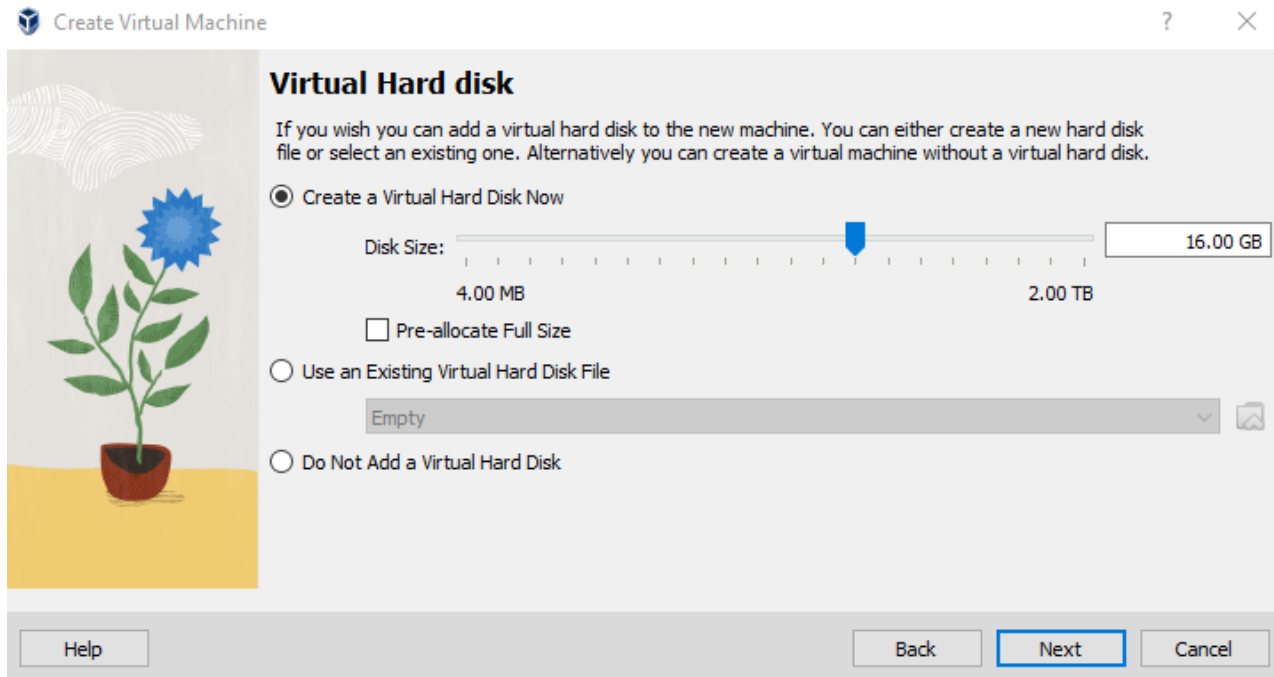
Entramos a virtualBox y creamos una nueva máquina con la imagen ISO de pfSense.



Asignamos una memoria de 1024 MB.

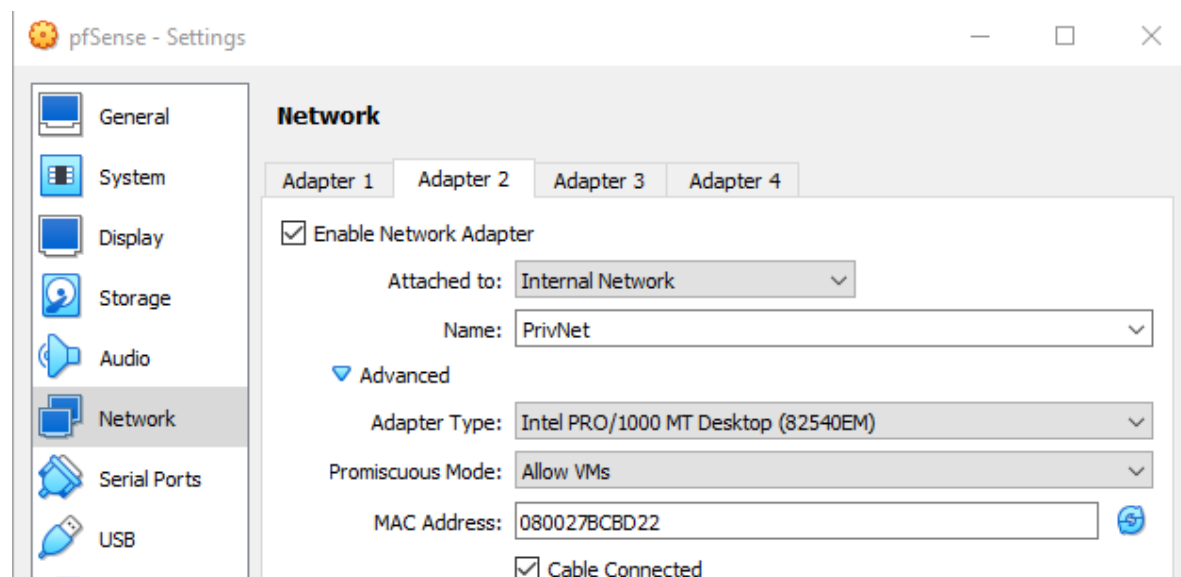
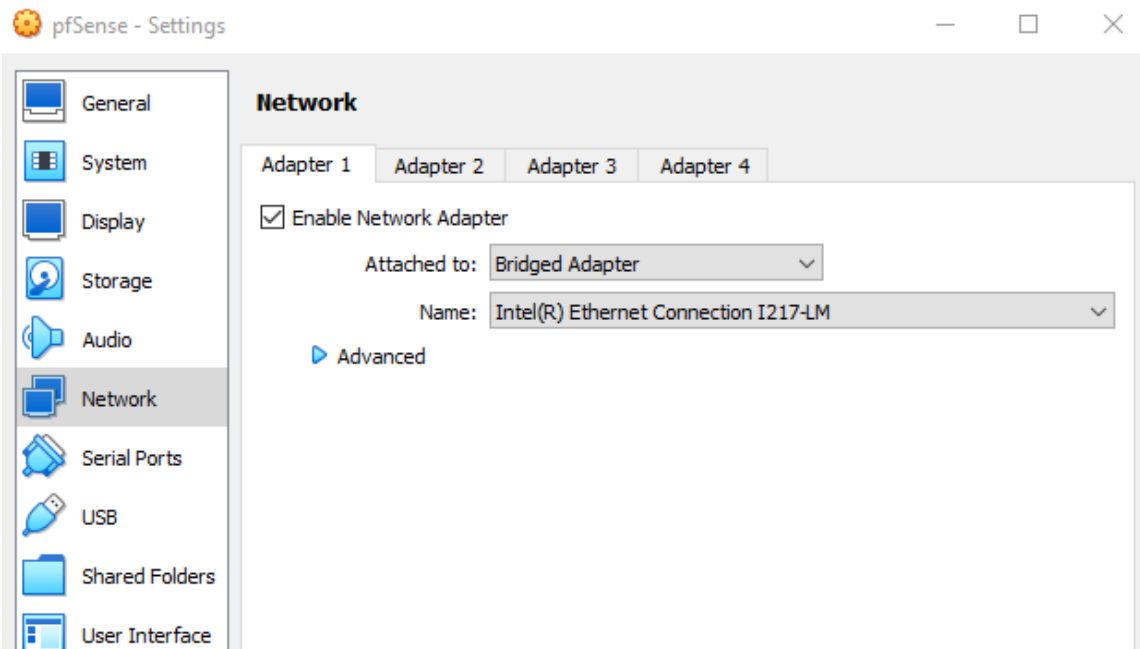


Asignamos un espacio en disco de 16 GB.



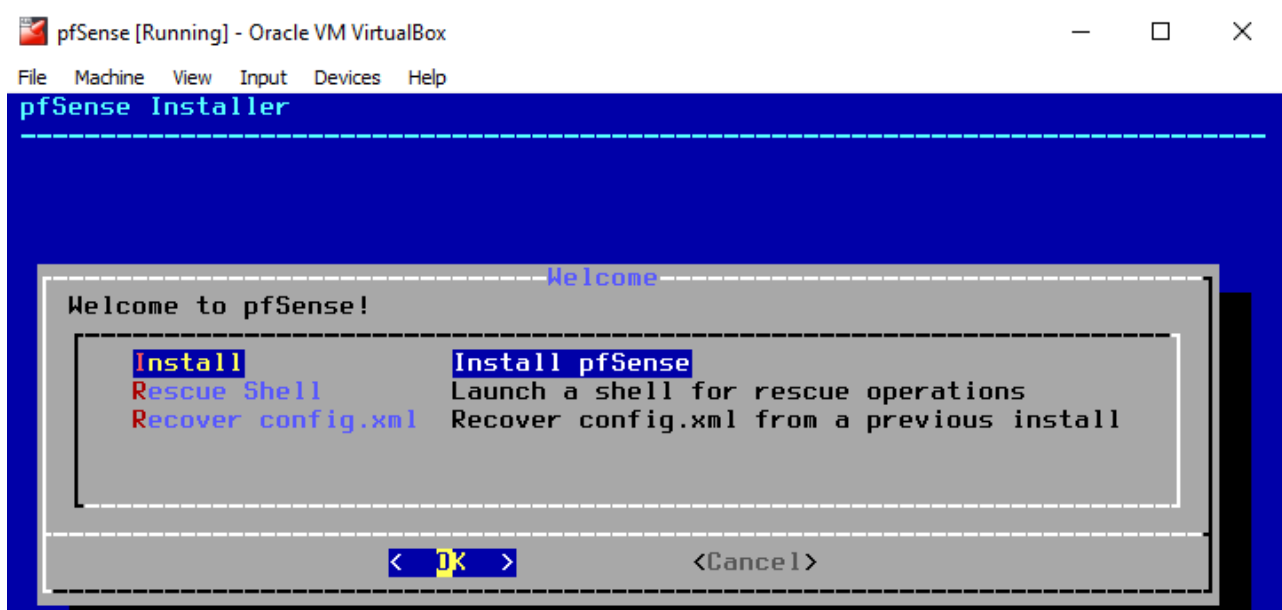
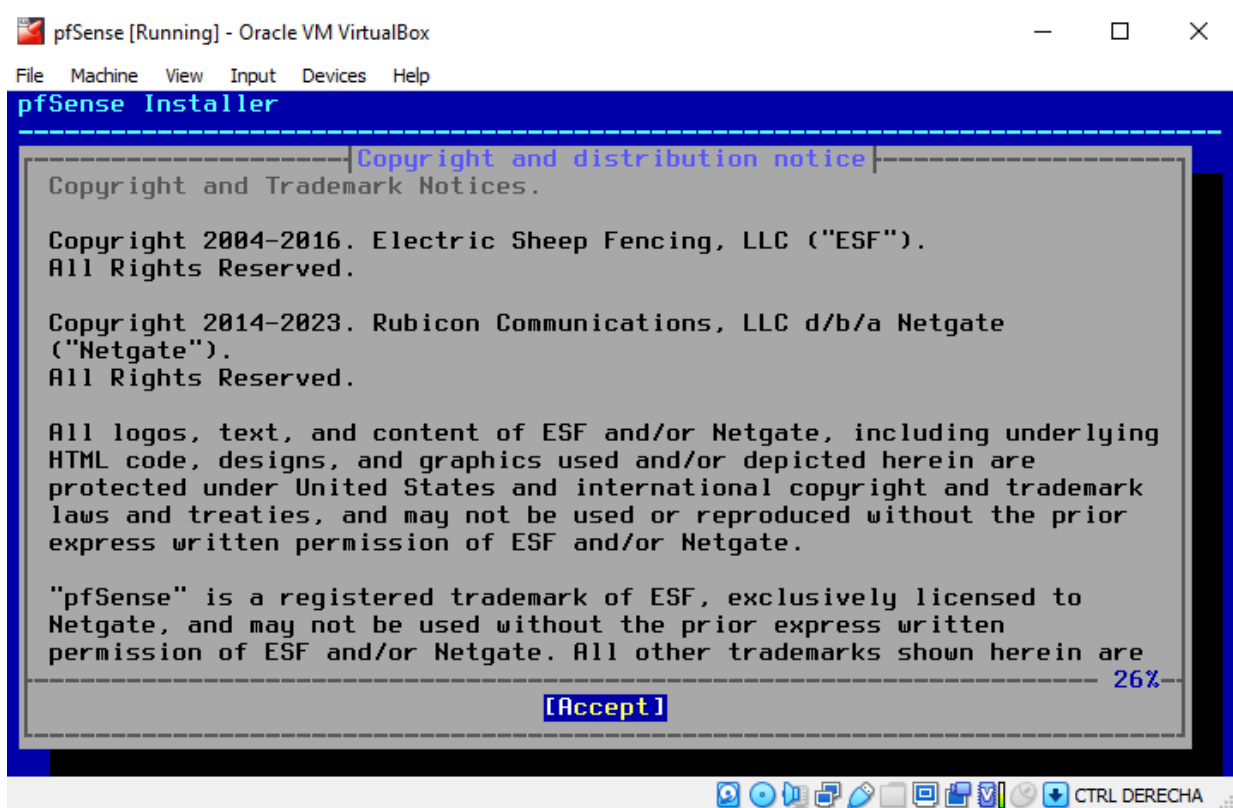
Configurar interfaces de red

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.

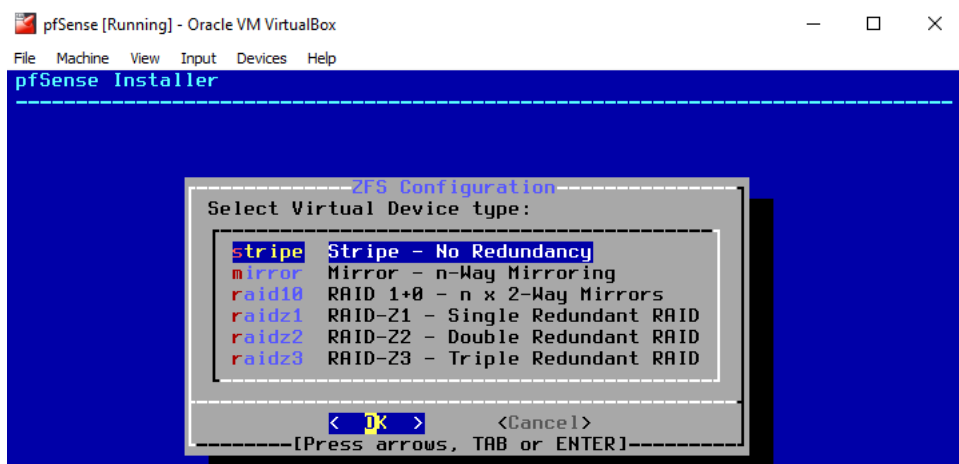
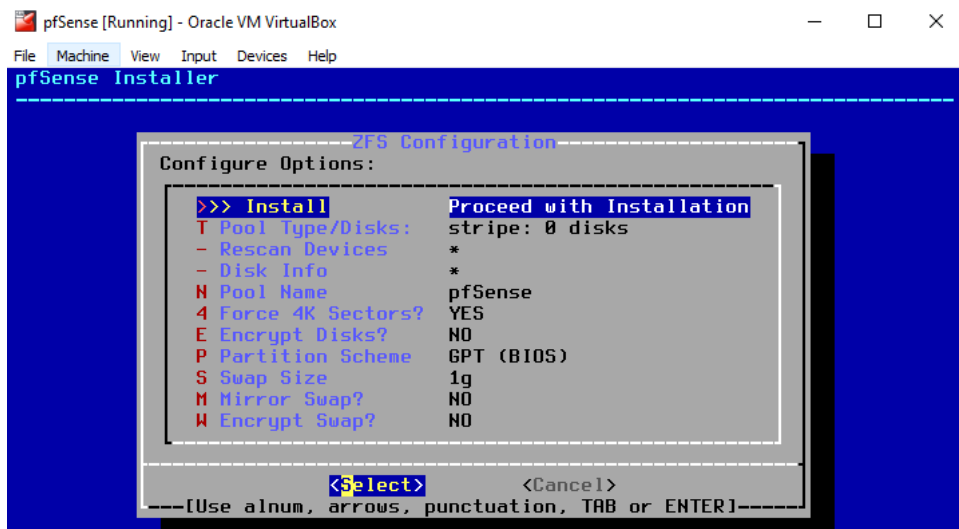
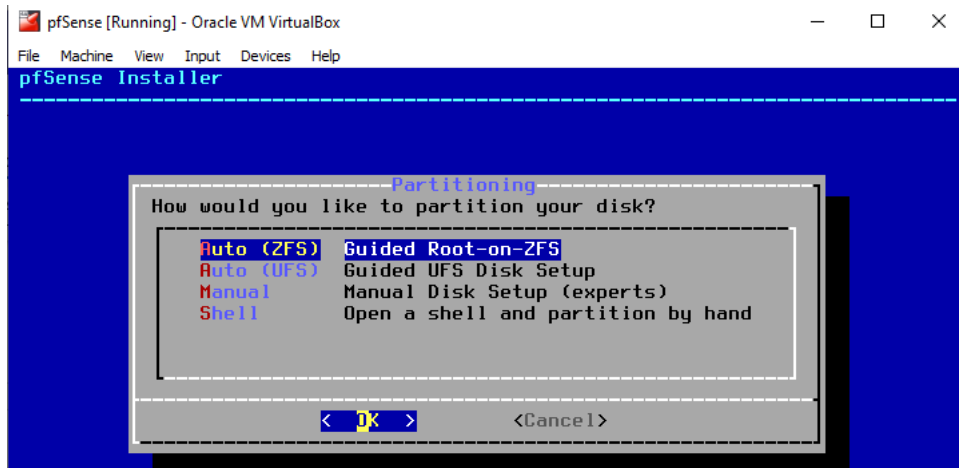


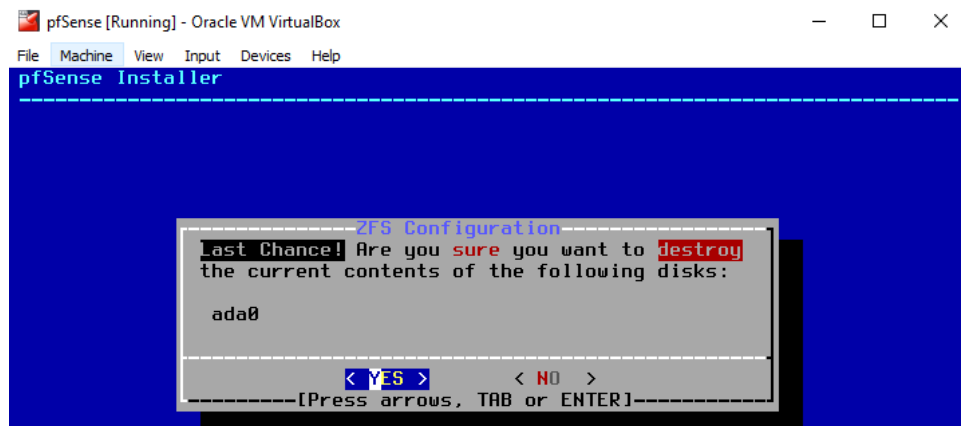
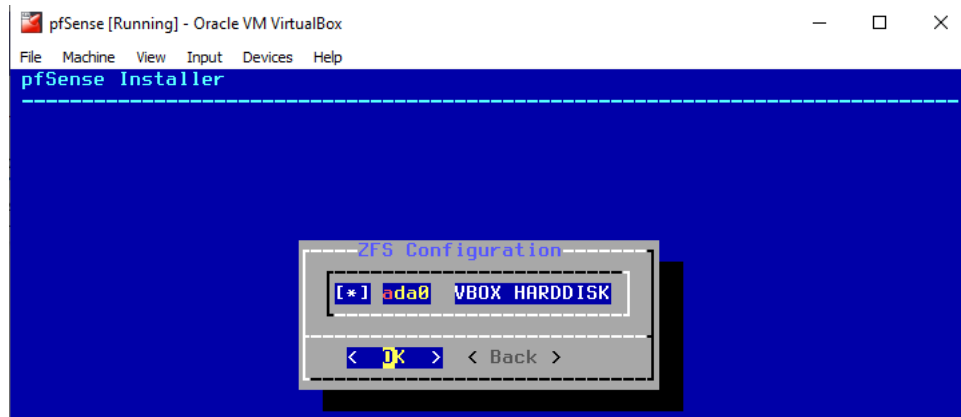
Instalar pfSense

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

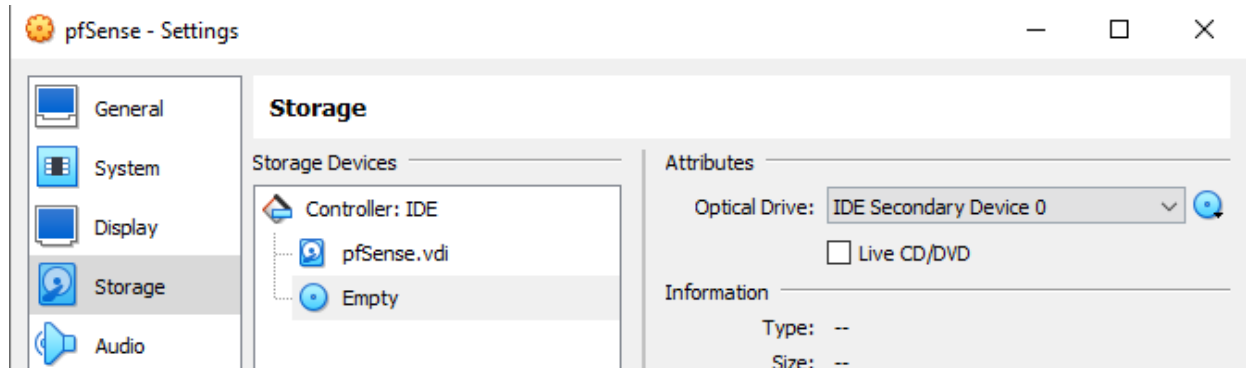


Seguimos los pasos de instalación de pfSense.





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

```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.661/4.145/4.956/0.577 ms

Press ENTER to continue.

VirtualBox Virtual Machine - Netgate Device ID: b58bb132f516b997aad2

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 10.2.77.115/16
LAN (lan)      -> em1      -> v4: 172.16.1.1/16

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 
```

```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 7

Enter a host name or IP address: 8.8.8.8

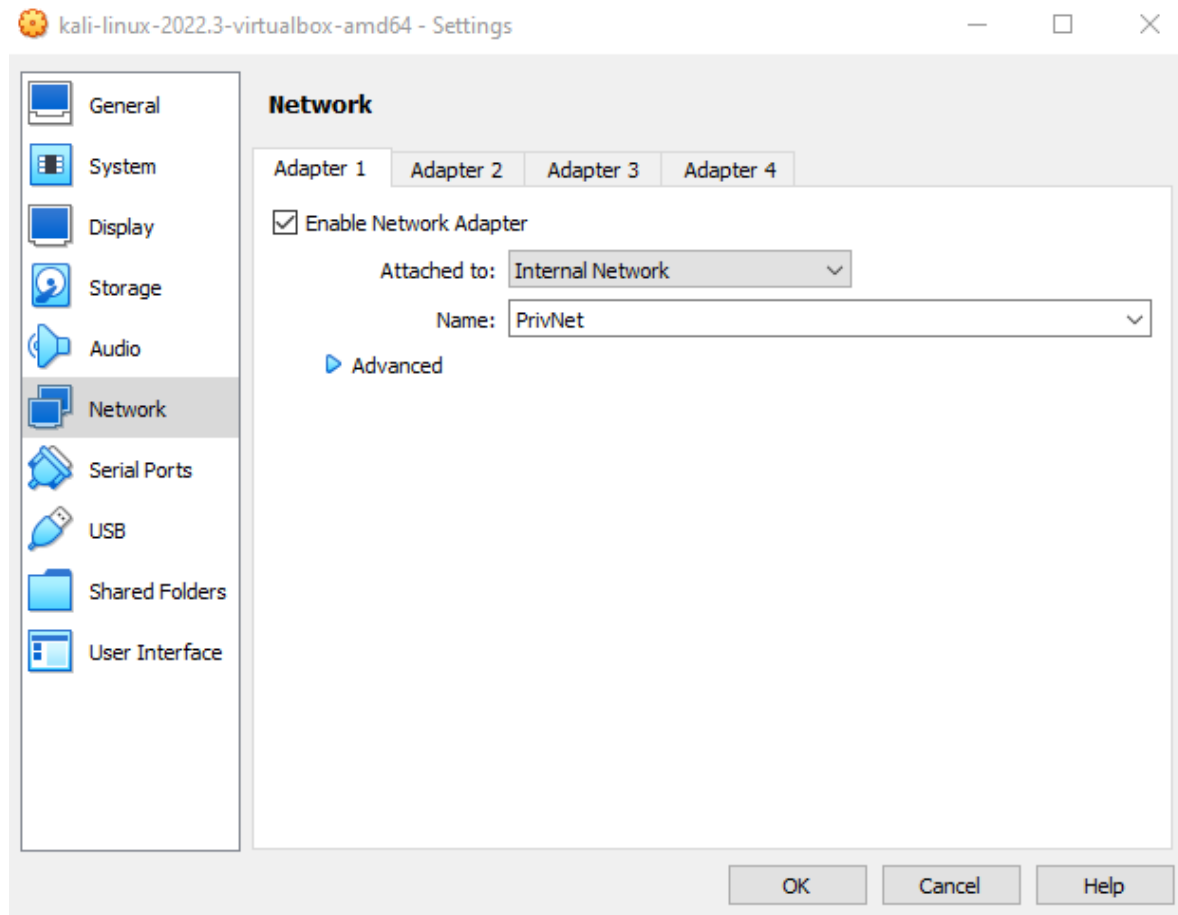
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=115 time=3.025 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=4.153 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=3.969 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.025/3.716/4.153/0.494 ms

Press ENTER to continue.
```


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”.

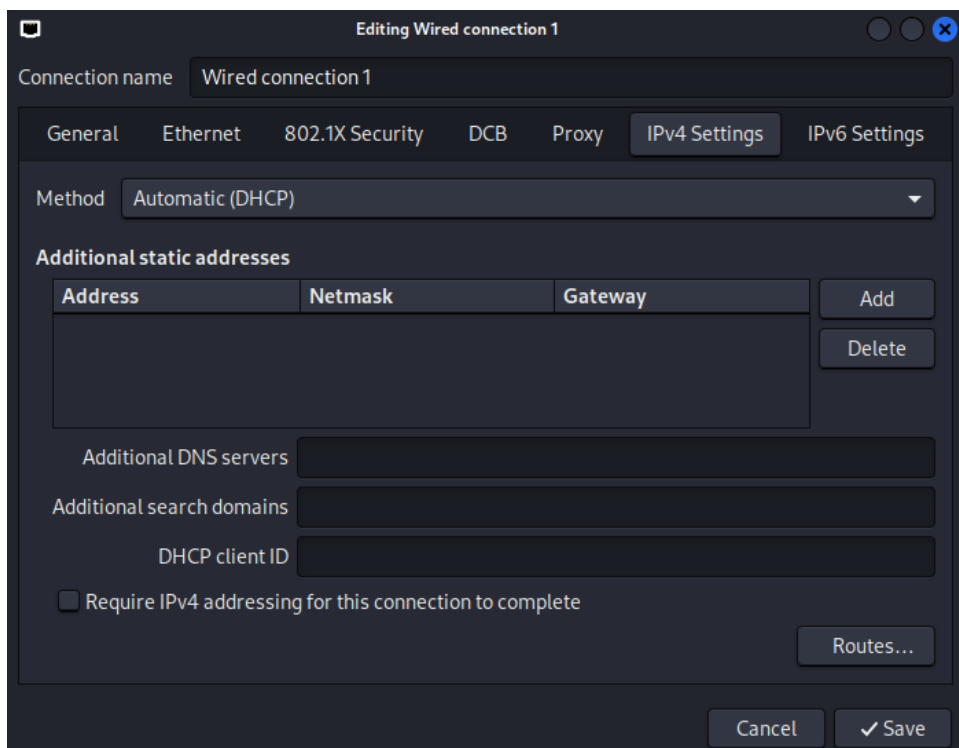
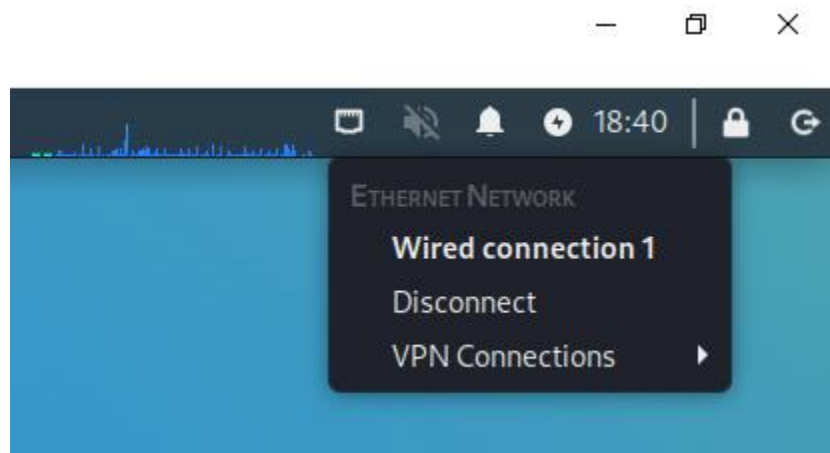


Corremos la máquina y verificamos que la red interna “PrivNet” haya quedado correctamente configurada en la máquina de kali y probamos el ping a la máquina de pfSense para verificar que todo funcione correctamente.

```
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 0x20<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
```

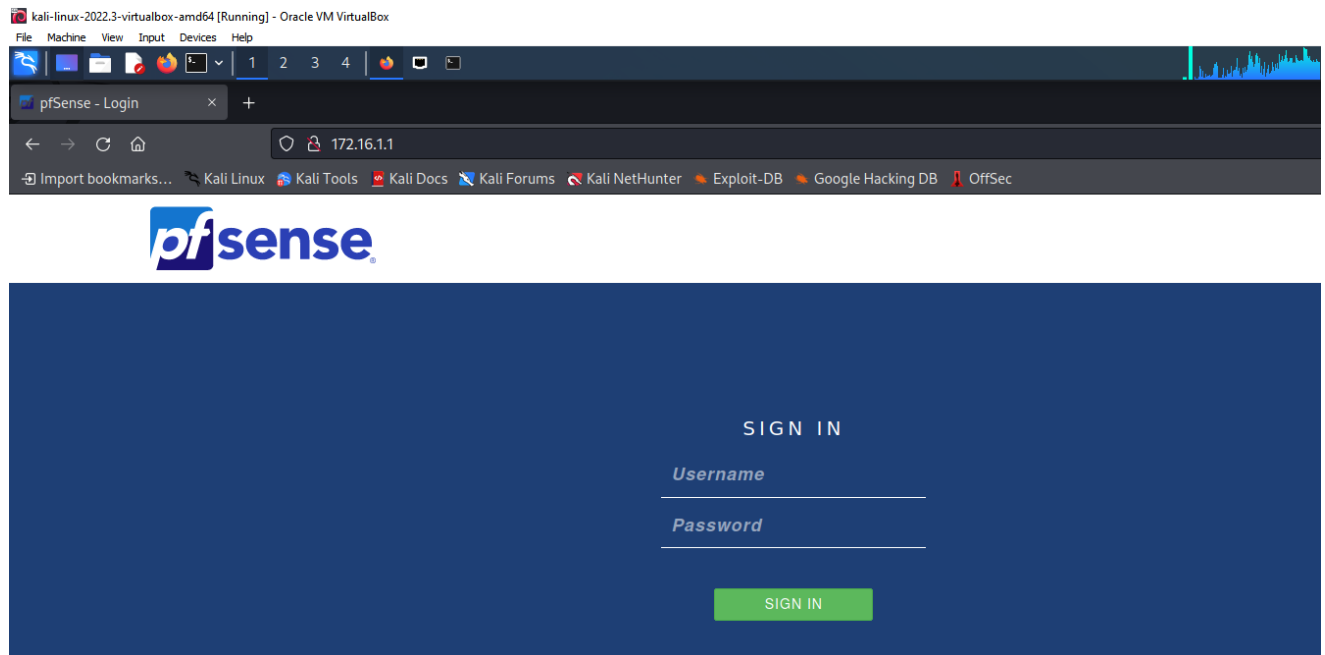
```
(kali㉿kali)-[~]  
$ ping 72.16.1.100  
PING 72.16.1.100 (72.16.1.100) 56(84) bytes of data.  
64 bytes from 72.16.1.100: icmp_seq=1 ttl=47 time=124 ms  
64 bytes from 72.16.1.100: icmp_seq=2 ttl=47 time=127 ms  
64 bytes from 72.16.1.100: icmp_seq=3 ttl=47 time=114 ms  
64 bytes from 72.16.1.100: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

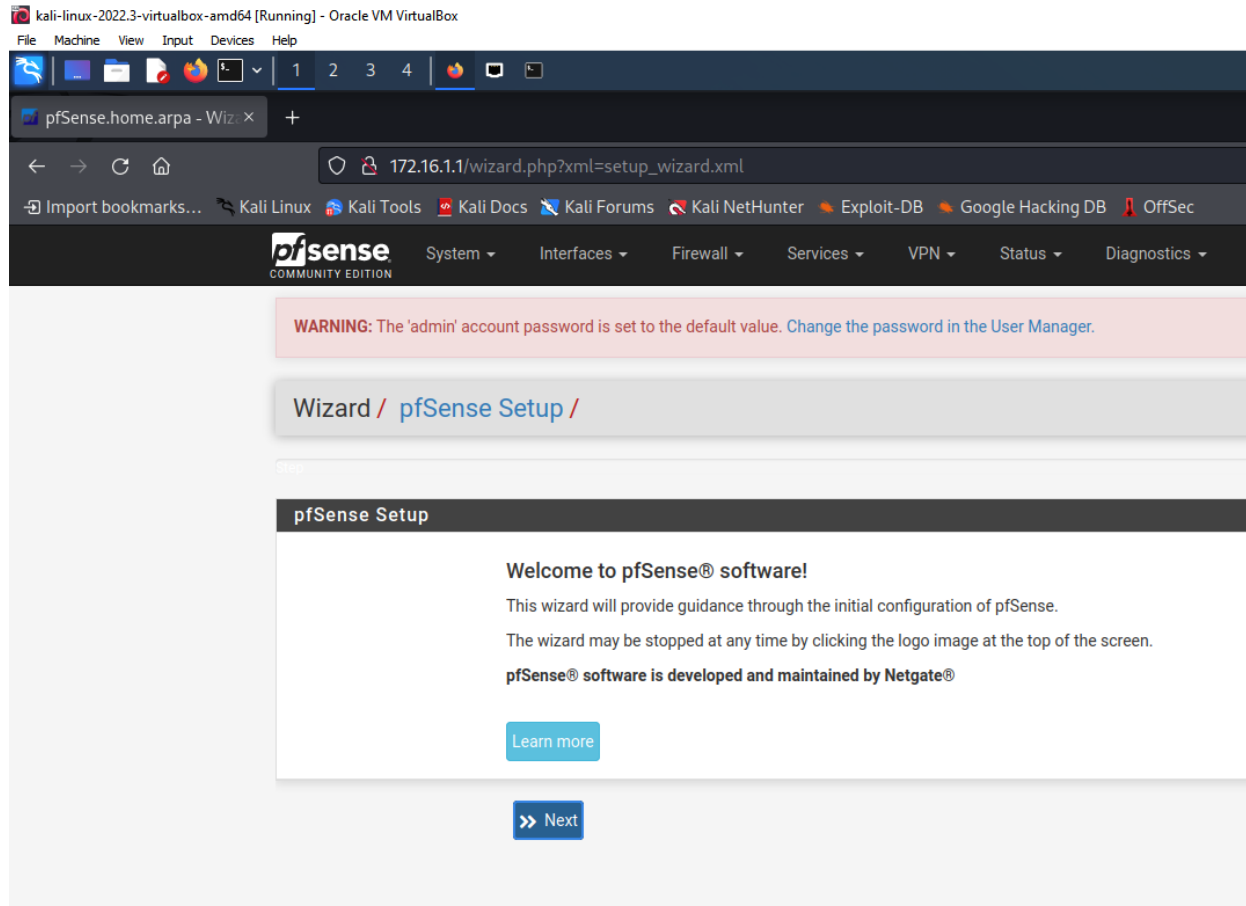


```
(kali@kali)-[~]  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=3.55 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=4.30 ms  
^Z  
zsh: suspended ping 8.8.8.8
```

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 asignando el server DNS primario como “8.8.8.8” y cambiando la contraseña del administrador (password).



Primary DNS Server

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

Next

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

Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

any

Alternate Host

Datagram conversion error

Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source

☐ Invert match

Any

Source Address

/

Destination

Destination

☐ Invert match

Address or Alias

8.8.8.8

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

No more ping to Google's DNS

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

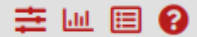
Aplicamos los cambios e intentamos hacer ping a 8.8.8.8 y veremos que no es posible.

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

```
(kali㉿kali)-[~]
└─$ 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 —
19 packets transmitted, 0 received, 100% packet loss, time 18418ms
```

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

Firewall / Rules / Edit



Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

```
(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=3.46 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=3.53 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=3.56 ms
```

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.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	1/1.46 MiB	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗	0/0 B	IPv4 ICMP any	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
<input type="checkbox"/>	✓	1/6 KiB	IPv4 ICMP any	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
<input type="checkbox"/>	✓	0/9.15 MiB	IPv4 *	LAN subnets	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

```

(kali㉿kali)-[~]
└─$ 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 —
36 packets transmitted, 0 received, 100% packet loss, time 35828ms

```

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

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/1.47 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/6 KiB	IPv4 ICMP any	*	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
<input type="checkbox"/>	0/4 KiB	IPv4 ICMP any	*	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
<input type="checkbox"/>	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.