**Escuela Colombiana De Ingeniería**

**Julio Garavito**

**Daniel Esteban Vela Lopez**

**Laura Valentina Rodriguez Ortegon**

**Andres Felipe Montes Ortiz**

**Laboratorio #15**

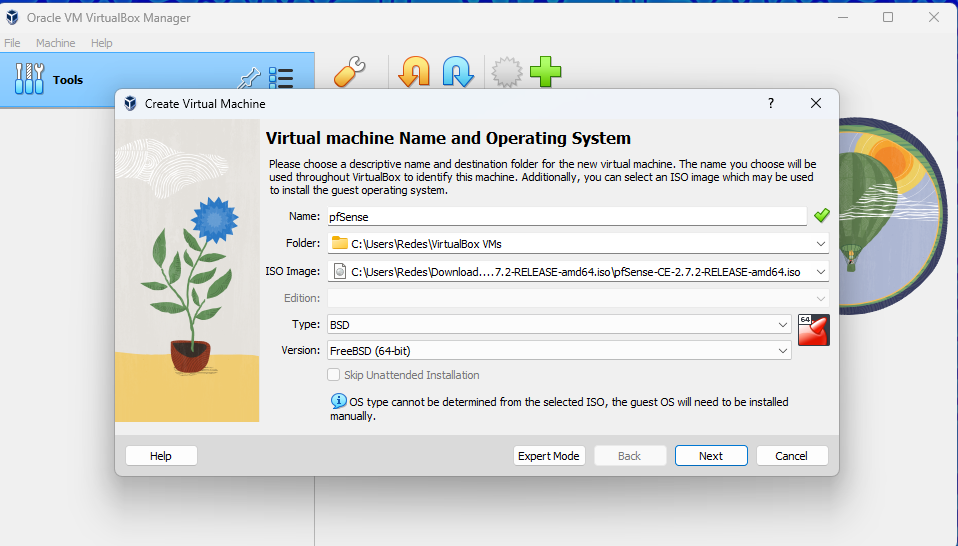
**2024-2**

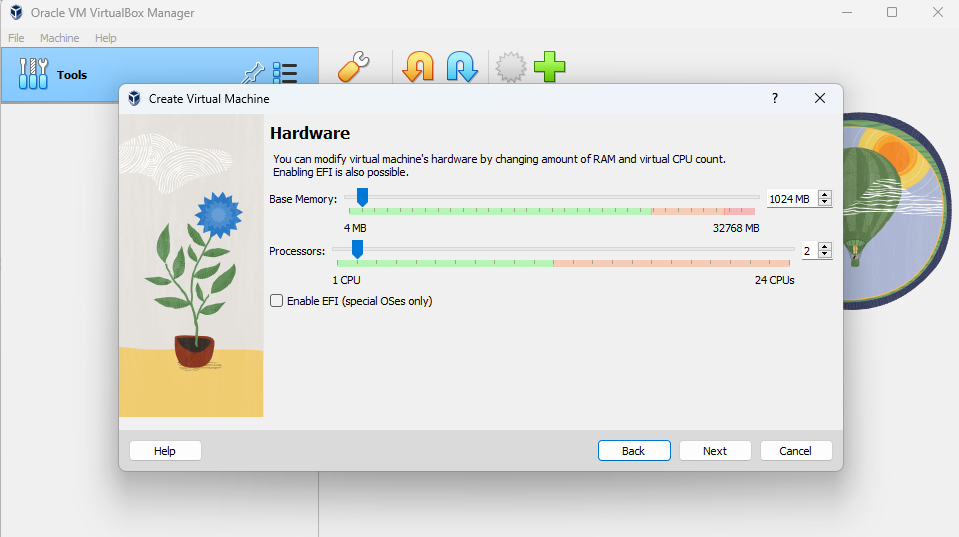
En este laboratorio, se instalará y configurará pfSense, un software de firewall, para restringir que la red 172.16.1.0/16 haga ping a la dirección IP externa 8.8.8.8. Primero, hay que asegurarse de que la máquina virtual pfSense (con dos interfaces de red) y las máquinas Kali estén en ejecución. Acceder a la interfaz web de pfSense desde Kali usando IP LAN (172.16.1.1). Por último, se ajustan las reglas del firewall para bloquear las solicitudes ICMP (ping) a la IP especificada.

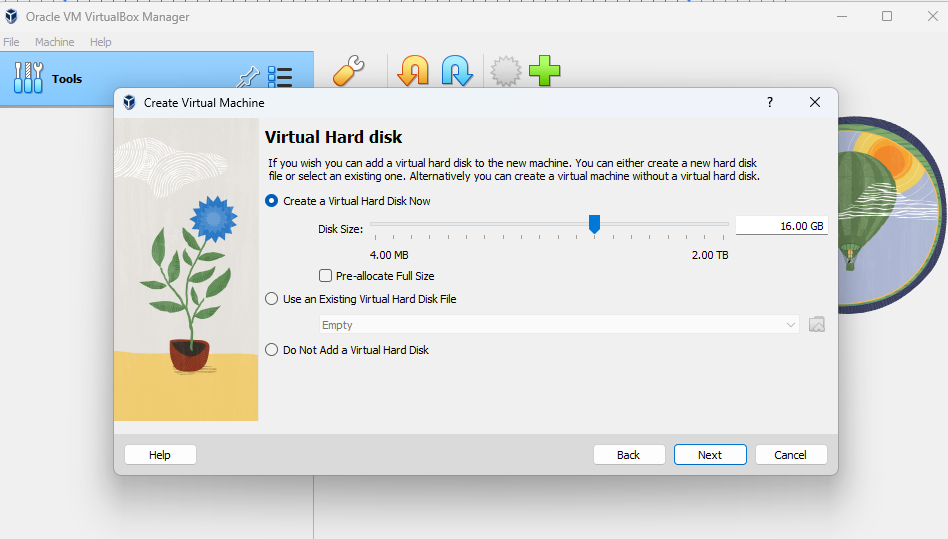
Primero, vamos a crear una nueva máquina virtual en VirtualBox.

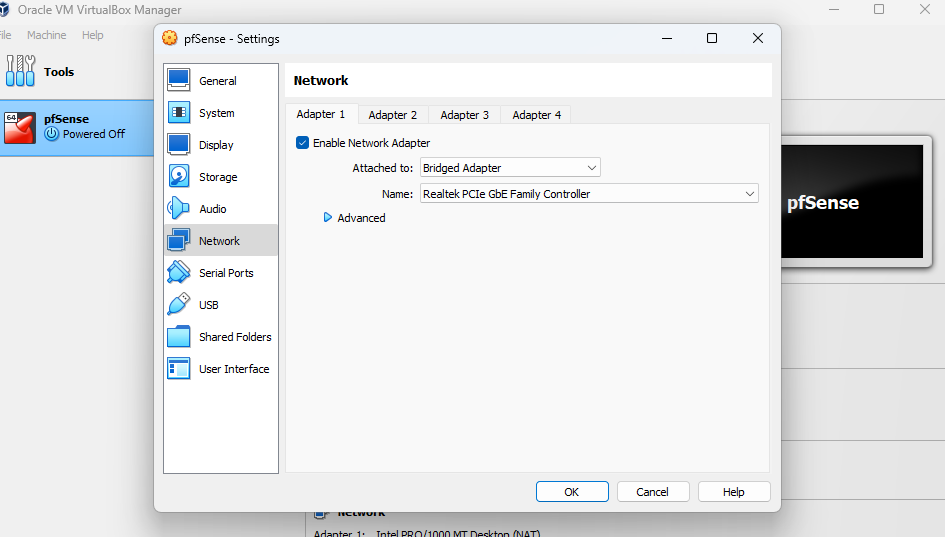
**Seleccionamos la ISO de pfSense:** Las instrucciones para instalar nuestro firewall. La descargamos de la página oficial de pfSense.

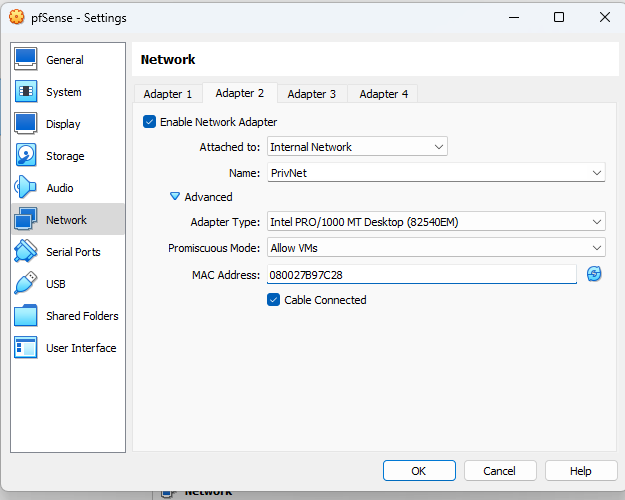
* **Le damos los recursos necesarios:**
  + **Memoria (RAM):** 1024 MB.
  + **Disco Duro:** 16 GB.
* **Configuramos las redes:**
  + **Adaptador 1 (Puenteado):** Este adaptador conectará nuestra máquina virtual directamente a nuestra red real.
  + **Adaptador 2 (Red interna "PrivNet"):** Crearemos una red interna para conectar otros dispositivos virtuales.

****

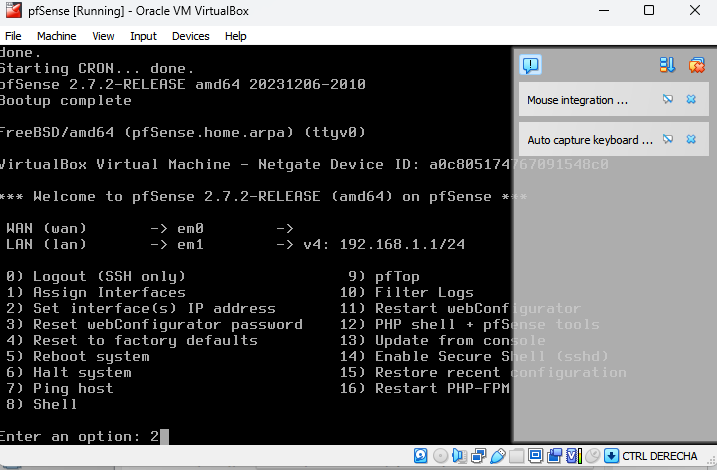
****

****

****

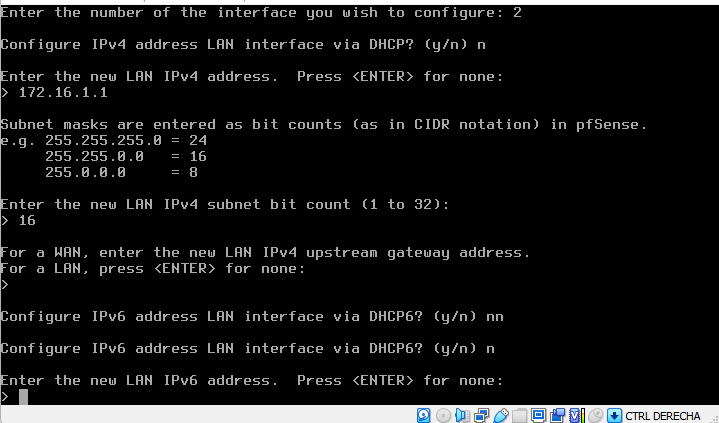
****

Iniciamos nuestra máquina:

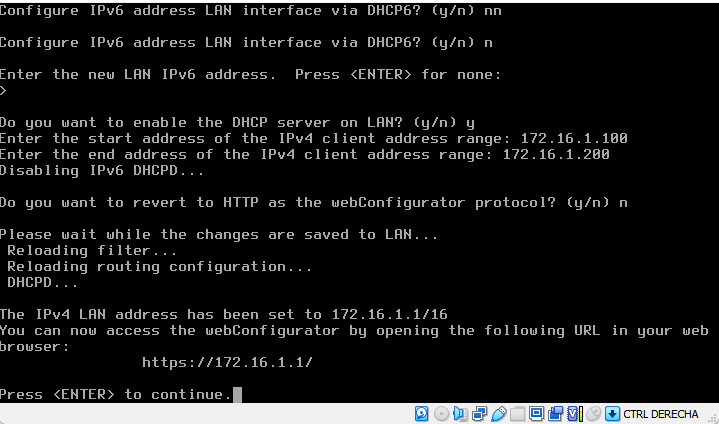
****

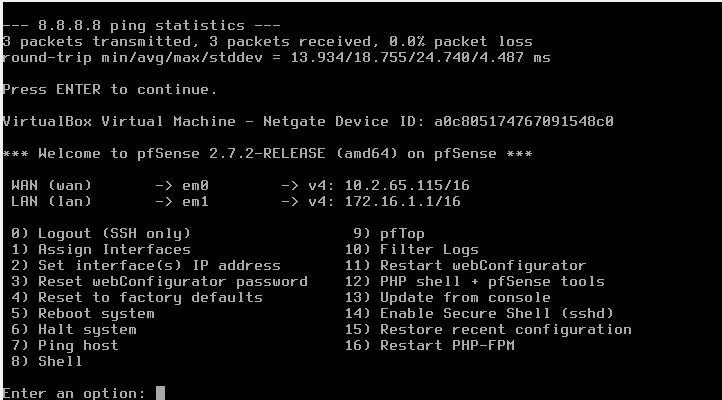
Lo primero que hicimos fue confirmar que queríamos configurar la interfaz número 2, que es justamente nuestra red interna "PrivNet". Luego, decidimos asignarle una dirección IP fija, en lugar de que la obtenga automáticamente. Elegimos la dirección 172.16.1.1, que será como la "dirección postal" de nuestra interfaz.

Después, definimos el tamaño de la red a la que pertenece esta dirección IP. Para eso, utilizamos una máscara de subred. Imagina que la red es una casa y la máscara de subred define el tamaño de cada habitación. En este caso, elegimos una máscara que nos permite tener una red de tamaño mediano.

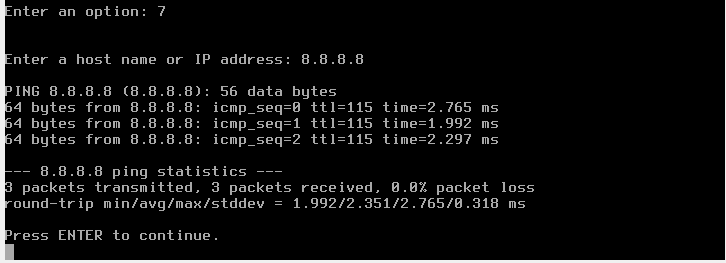
****

Aquí asignamos un rango de IPv4 que podían ser utilizadas, desde 172.16.1.100 a 172.16.1.200

****

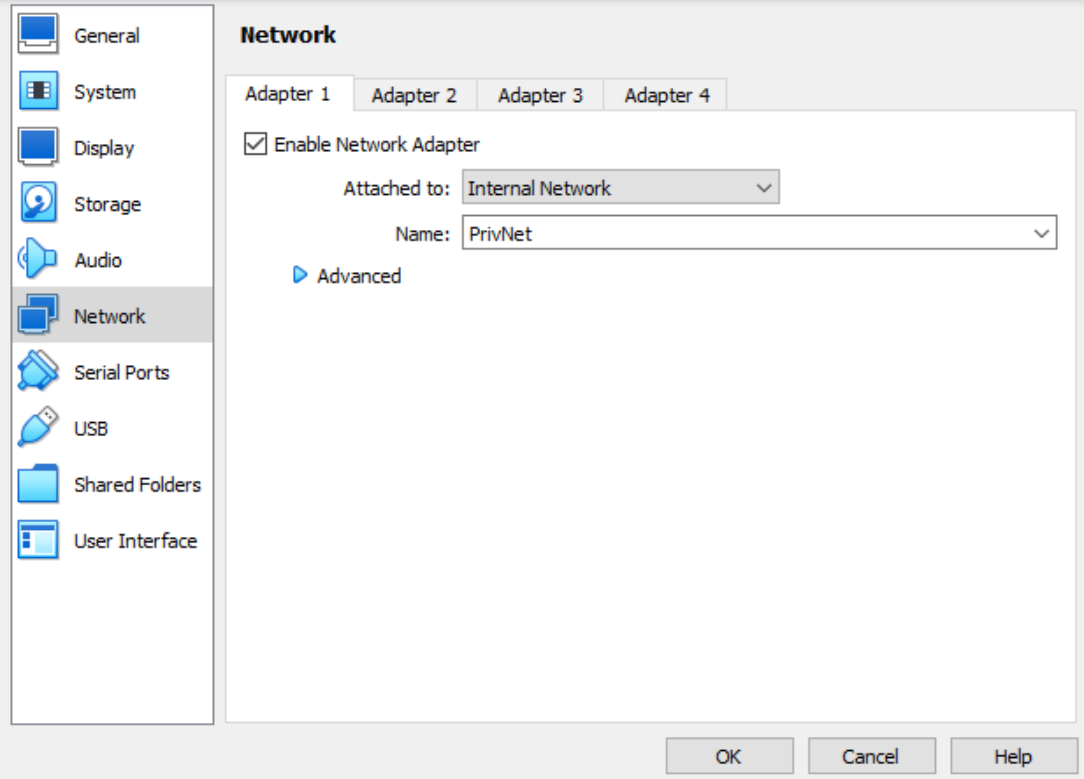
Acá está nuestra configuración final para nuestra WAN y LAN****

Comprobamos que se haga ping en Google 8.8.8.8

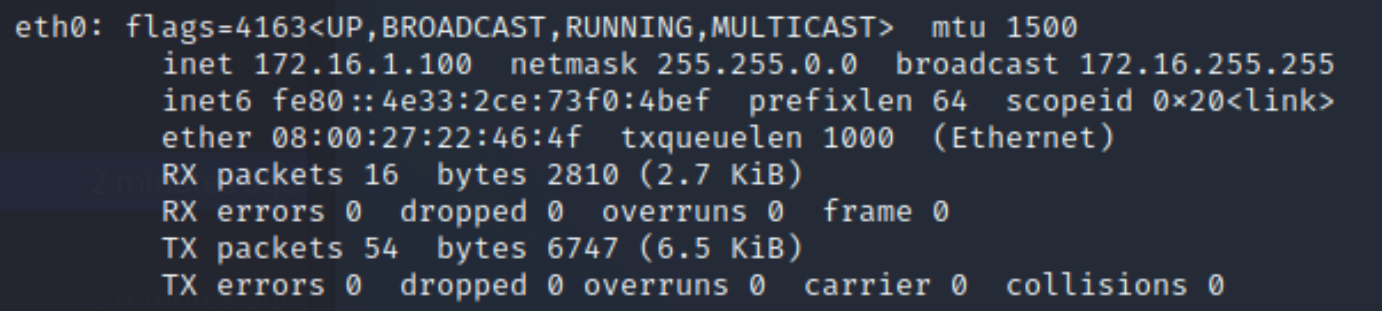
****

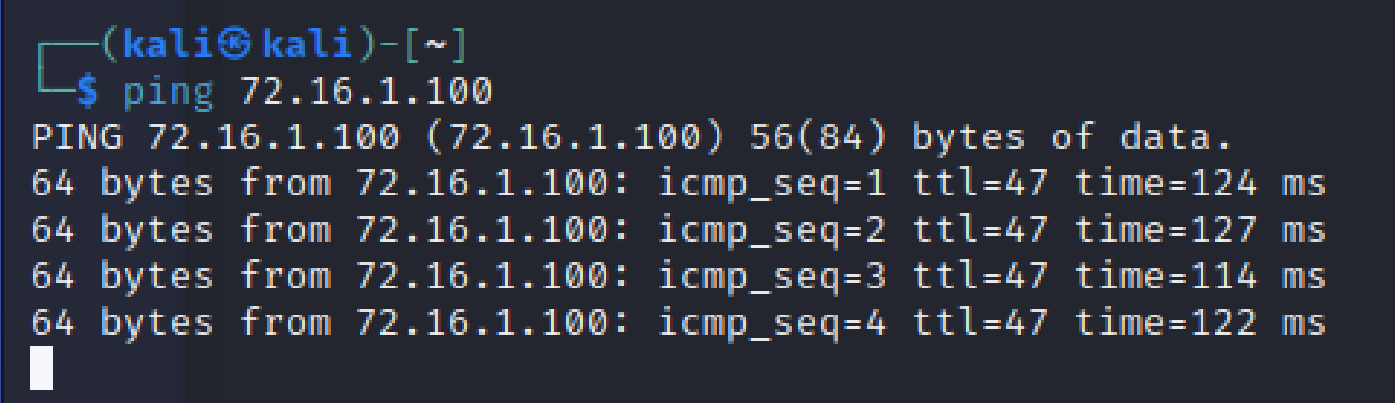
Ahora vamos a verificar el servidor DHCP

Configuramos nuestro Network con una red privada

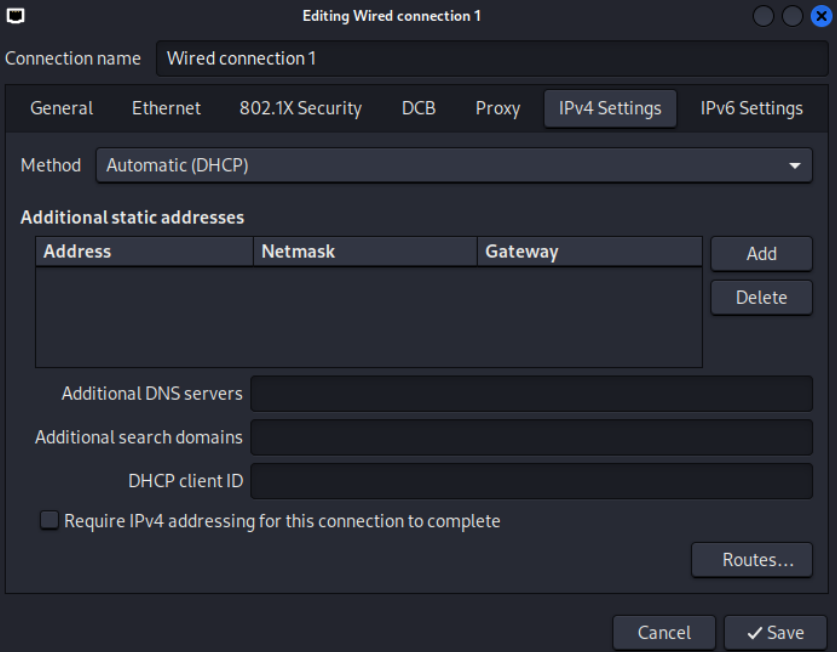
****

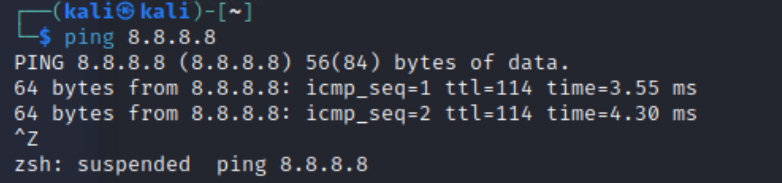
Una vez iniciada la máquina Kali Linux, verificamos la configuración de la interfaz de red 'PrivNet' ejecutando un ping hacia la dirección IP de pfSense. Si la prueba es exitosa, confirmamos que la comunicación entre ambas máquinas se ha establecido correctamente.

****

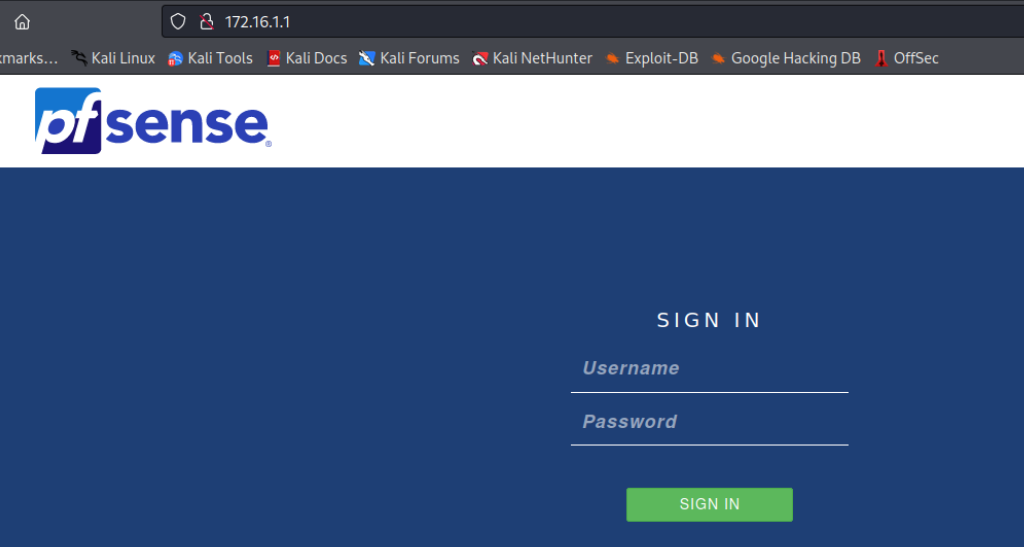
****

Accedemos a la configuración de red del sistema operativo y seleccionamos la conexión por cable (Wired connection 1). A continuación, configuramos la obtención automática de la dirección IPv4. Para verificar la correcta configuración, ejecutamos un comando ping hacia el servidor DNS de Google (8.8.8.8) y comprobamos que se reciben respuestas.

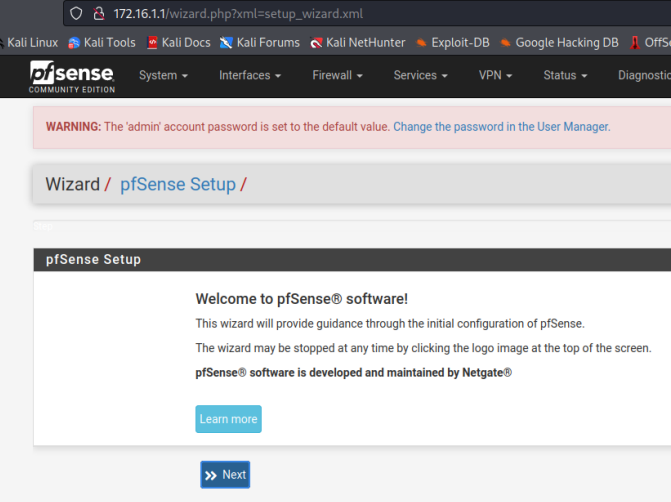
****

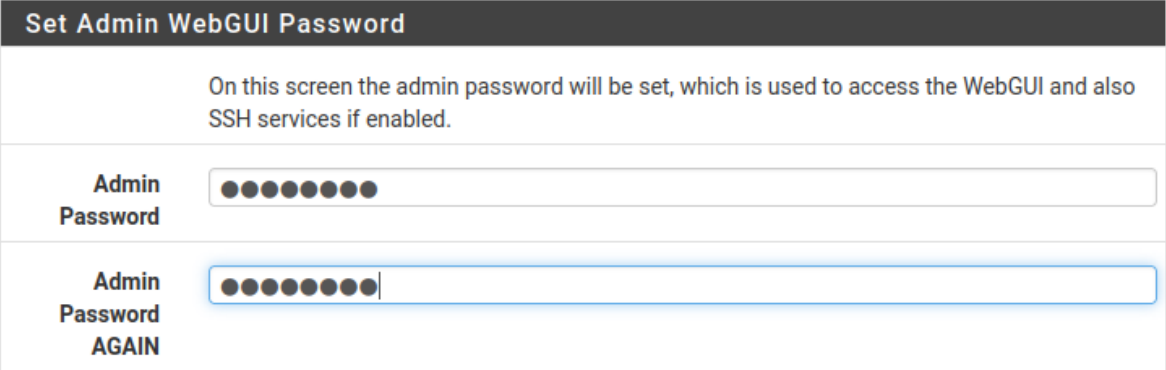
****

Accedemos a un navegador web, e ingresamos en la barra de direcciones la dirección IP de la interfaz de red LAN de pfSense. Esta acción nos permitirá acceder a la interfaz web de administración del firewall.

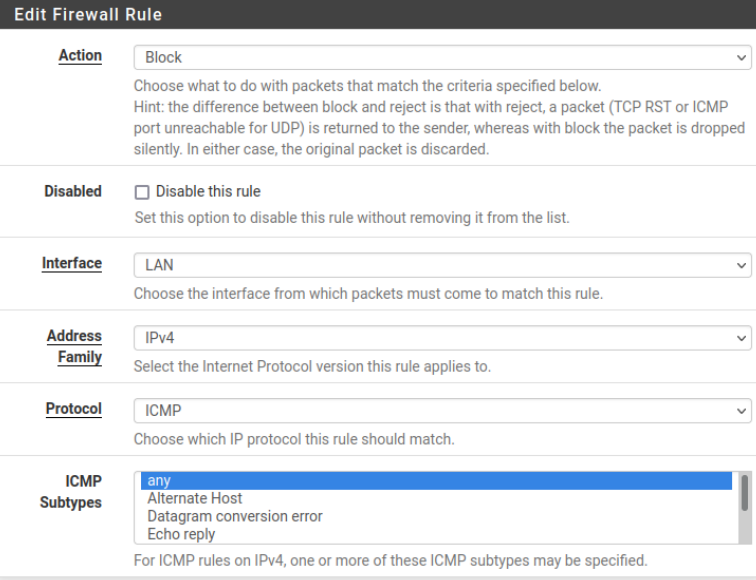
****

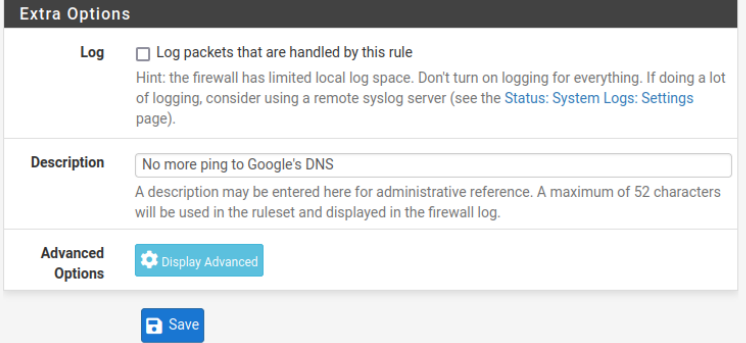
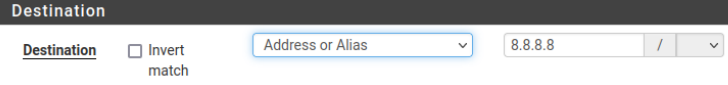
Siguiendo las instrucciones del asistente de configuración, establecemos el servidor DNS primario como '8.8.8.8' y procedemos a modificar la contraseña de administrador, asignándole un valor seguro y complejo.

****

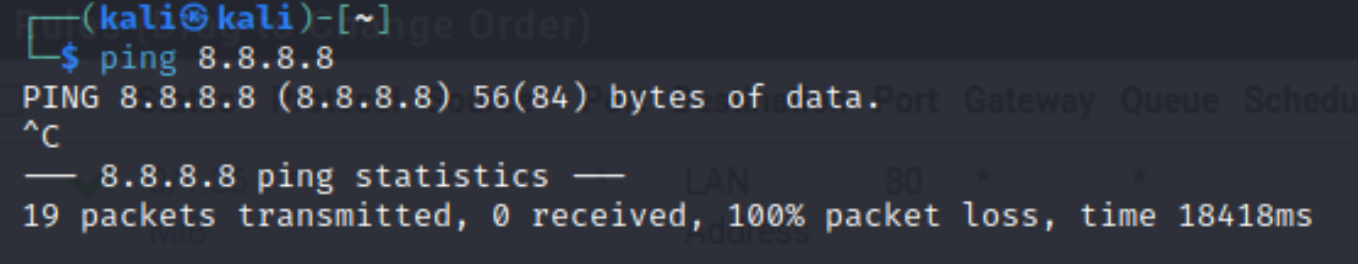
****

A continuación, accedemos a la sección de reglas de firewall y creamos una nueva regla. En esta regla, configuramos la acción como 'bloqueo', la interfaz como 'LAN' y establecemos como destino la dirección IP '8.8.8.8'. De esta manera, impediremos cualquier tipo de comunicación desde nuestra red local hacia el servidor DNS de Google.

****

****

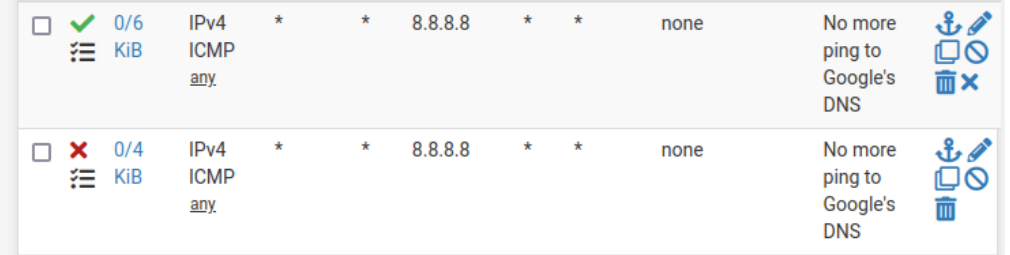
Si nos vamos a nuestra consola, veremos que no es posible la conexión y si cambiamos la conexión, estará activa nuevamente.

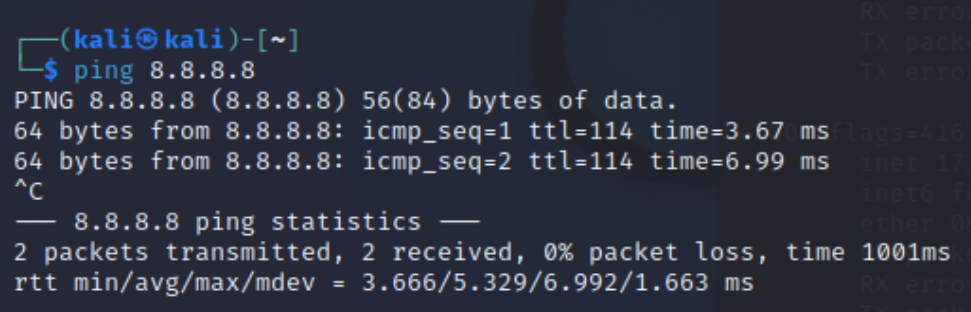
****

Así se verá nuestra configuración cuando no esté permitida:

****

Y la configuración cuando si está disponible se verá:

****

****

Con la configuración realizada, pfSense actúa como un router, asignando direcciones IP a los dispositivos de la red a través de su servidor DHCP, y como un firewall, filtrando el tráfico de red de manera granular. Además, hemos implementado una política de seguridad que bloquea el acceso a servicios no esenciales, como el servidor DNS de Google, y permite el acceso remoto a través de una conexión VPN segura. De esta manera, garantizamos la protección de nuestra red y la privacidad de los datos.