

PfSense - Snort



Carlos Augusto Pinzón Rivera

Tutor:

Joel Carroll

Especialización en Seguridad Informática

Colombia -Bucaramanga

2024

Introducción

“En un entorno de redes modernas, la seguridad informática juega un papel crucial para proteger los datos y garantizar la disponibilidad de los servicios. Este proyecto práctico tiene como propósito diseñar y configurar una topología de red utilizando GNS3, incorporando un firewall (PfSense) y un sistema de detección de intrusos (Snort). Estas herramientas permiten simular un entorno seguro que facilita el análisis de tráfico y la implementación de políticas de seguridad para prevenir accesos no autorizados y ataques cibernéticos.

El trabajo se enfoca en la creación y configuración de reglas específicas para el filtrado de tráfico, como el bloqueo de tráfico ICMP y sitios web no deseados, así como la autorización de servicios esenciales como SSH y HTTP. Esta práctica busca reforzar los conocimientos teóricos mediante la implementación en un entorno virtual que emula una infraestructura de red real.”

Objetivos

Objetivo General

“Diseñar e implementar una topología de red segura utilizando GNS3, incorporando herramientas como PfSense y Snort para aplicar medidas de seguridad avanzadas y evaluar el impacto de reglas de firewall y políticas de control de tráfico.”

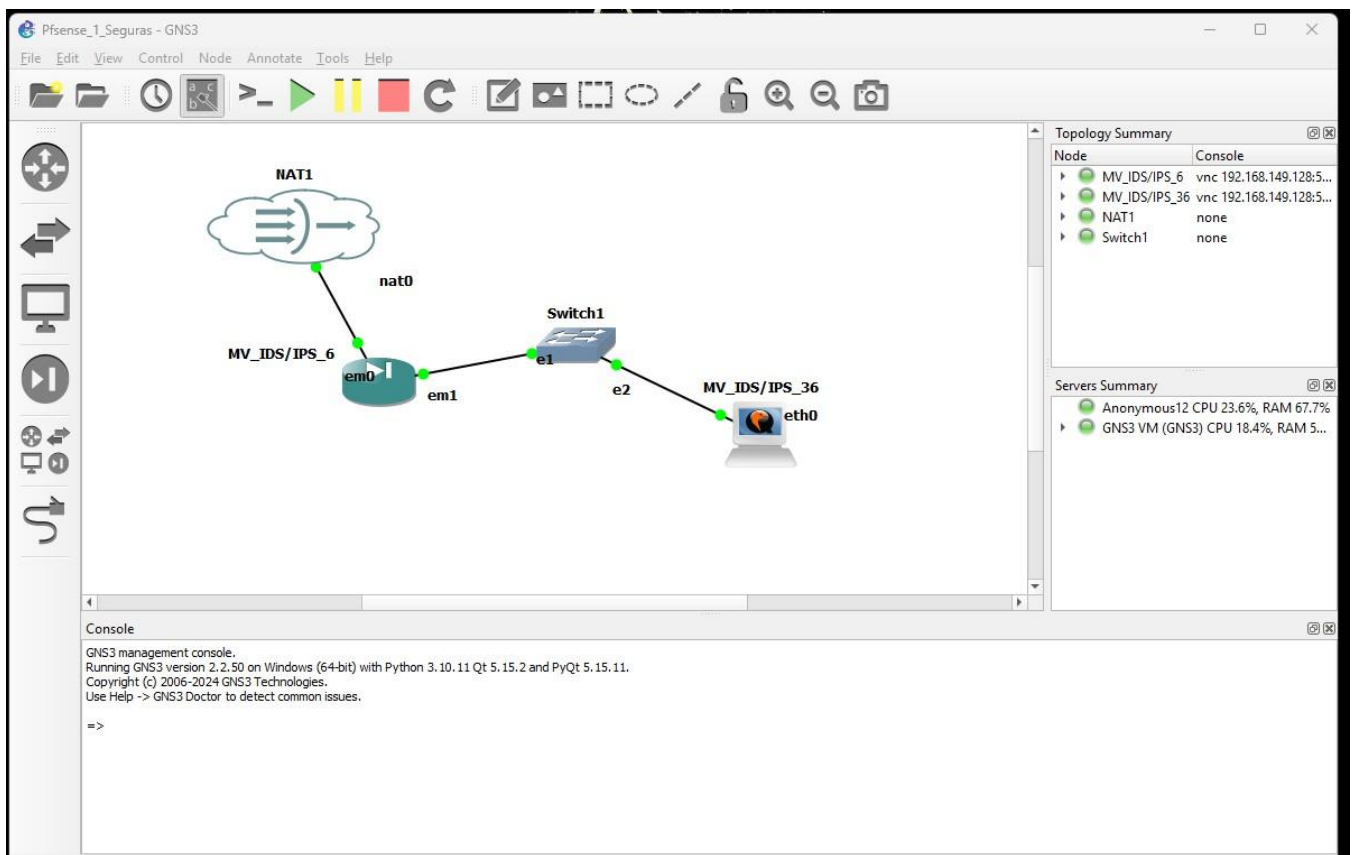
Objetivo Específicos

- Configurar una topología de red básica en GNS3 que integre dispositivos virtuales.
- Implementar un firewall basado en PfSense con reglas de seguridad específicas que incluyan la denegación y aceptación de tráfico.
- Instalar y configurar Snort como sistema de detección de intrusos (IDS) para monitorizar y analizar el tráfico de red.
- Validar la efectividad de las políticas de seguridad mediante pruebas prácticas, incluyendo la verificación de conectividad y el comportamiento ante reglas de filtrado.
- Documentar el proceso de configuración y los resultados obtenidos, destacando las mejores prácticas y lecciones aprendidas.

Desarrollo del trabajo

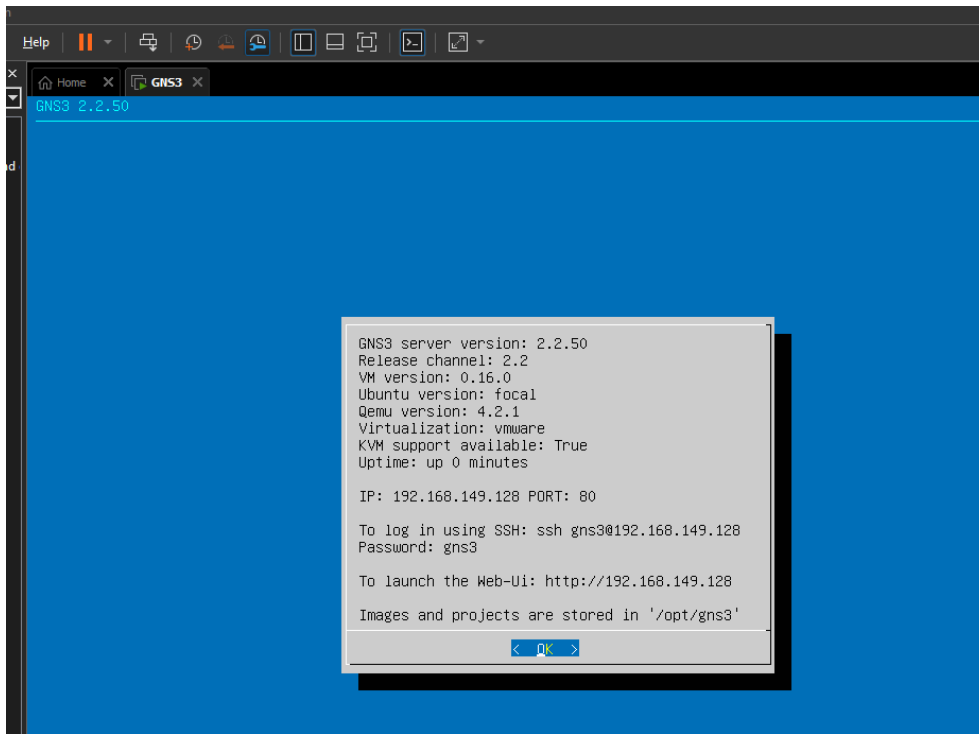
Numero de cedula: 13.715.336

Topología de red en GNS3



Fuente. Autoría propia

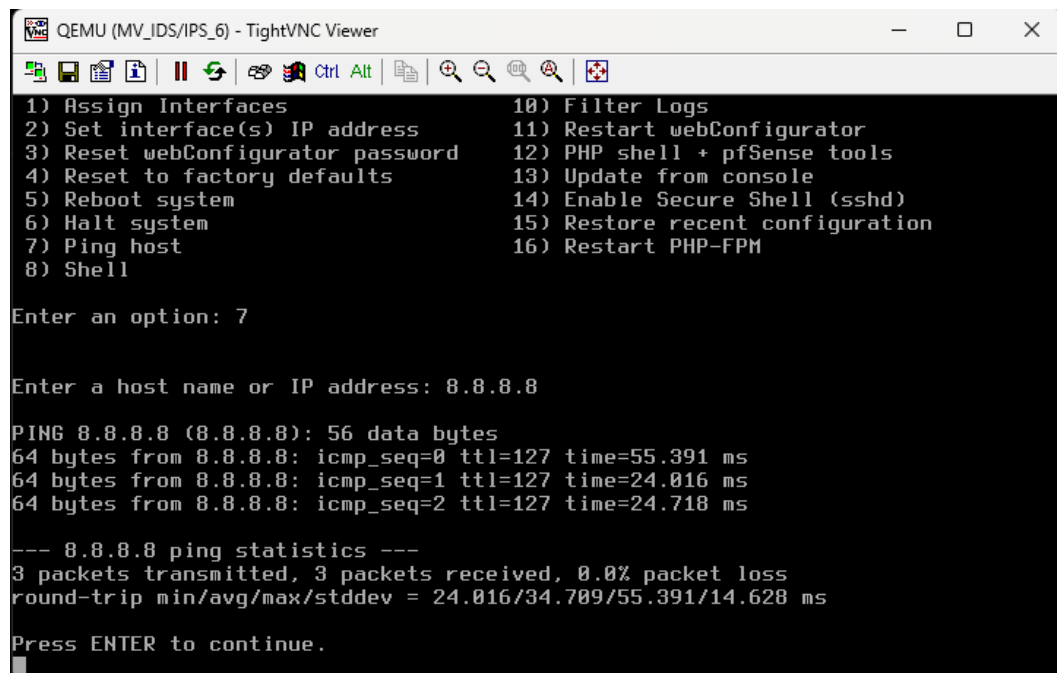
La imagen corresponde a una simulación de red creada utilizando la herramienta GNS3. Esta herramienta es ampliamente utilizada por profesionales y estudiantes de redes para diseñar, configurar y probar topologías de red complejas en un entorno virtual.



Fuente. Autoría propia

Se muestra la ventana inicial del servidor de GNS3, que proporciona información esencial sobre el estado y configuración del servidor virtual. Este paso es crucial para verificar que el entorno de virtualización está correctamente configurado y listo para trabajar.

Conexión internet



```
QEMU (MV_IDS/IPS_6) - TightVNC Viewer
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=127 time=55.391 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=24.016 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=24.718 ms

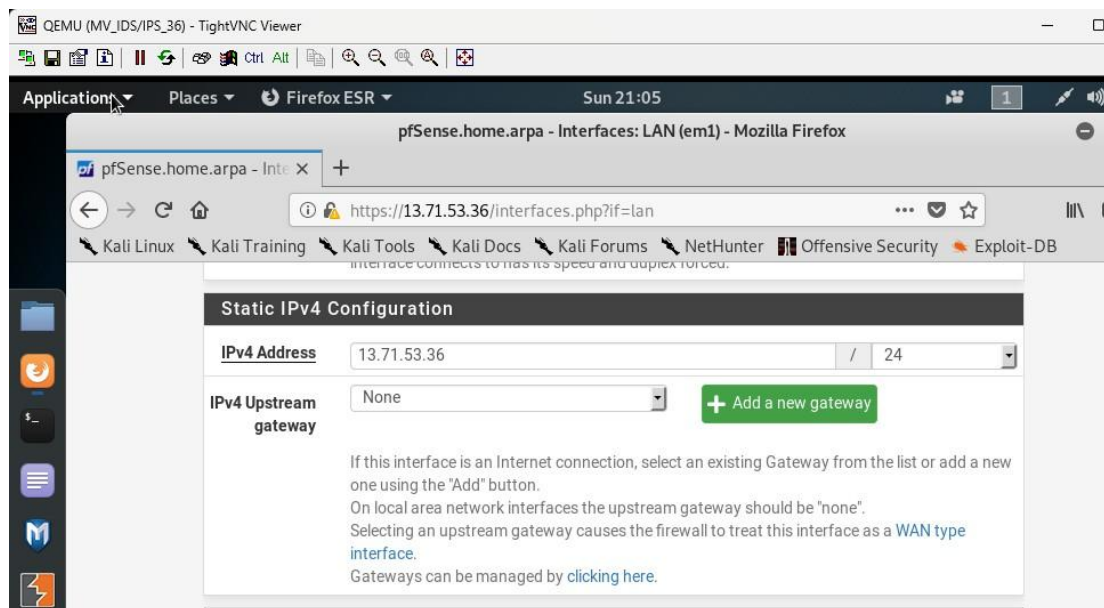
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 24.016/34.709/55.391/14.628 ms

Press ENTER to continue.
```

Fuente. Autoría propia

Después de instalar el Pfsense se selecciona la opción 7 y se ha ingresado la dirección IP 8.8.8.8 (que corresponde a los servidores DNS públicos de Google). Esto significa que se ha ejecutado un comando ping para verificar la conectividad del dispositivo hacia esos servidores.

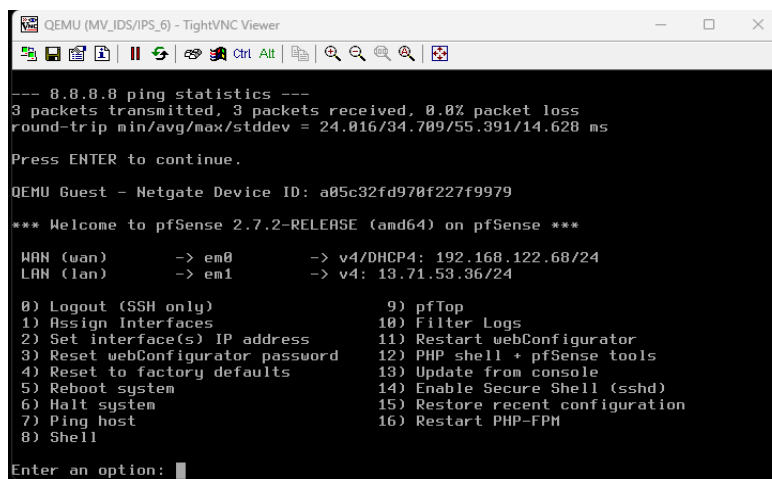
Configuración Direcccionamiento ip con el número de cedula.



Fuente. Autoría propia

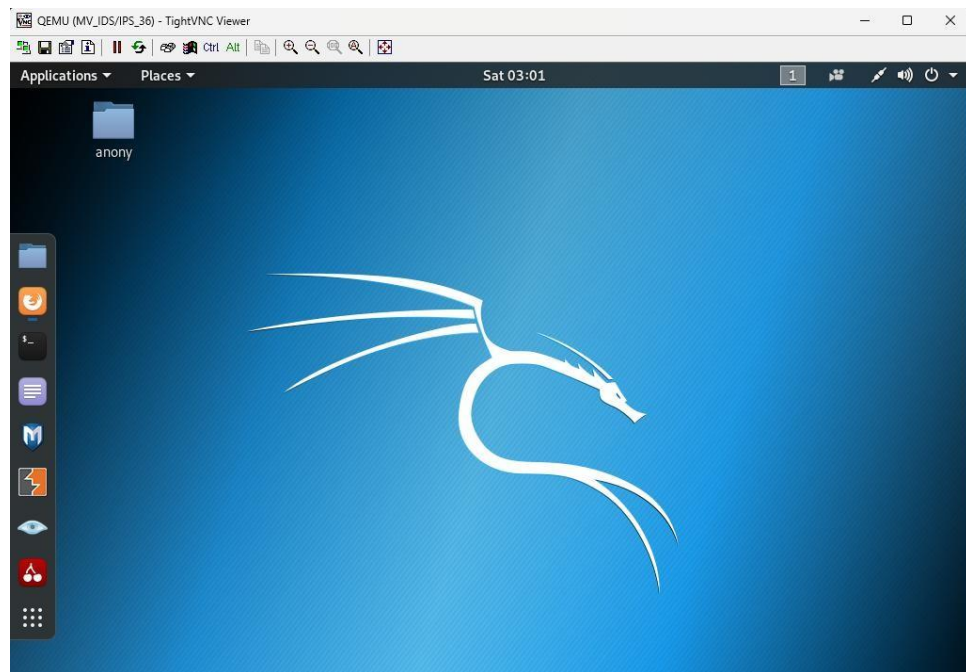
Se utiliza el navegador web Firefox para acceder a una página de configuración de la interfaz de red en Psense Static IPv4.

Se ha asignado la dirección IP a la interfaz LAN.

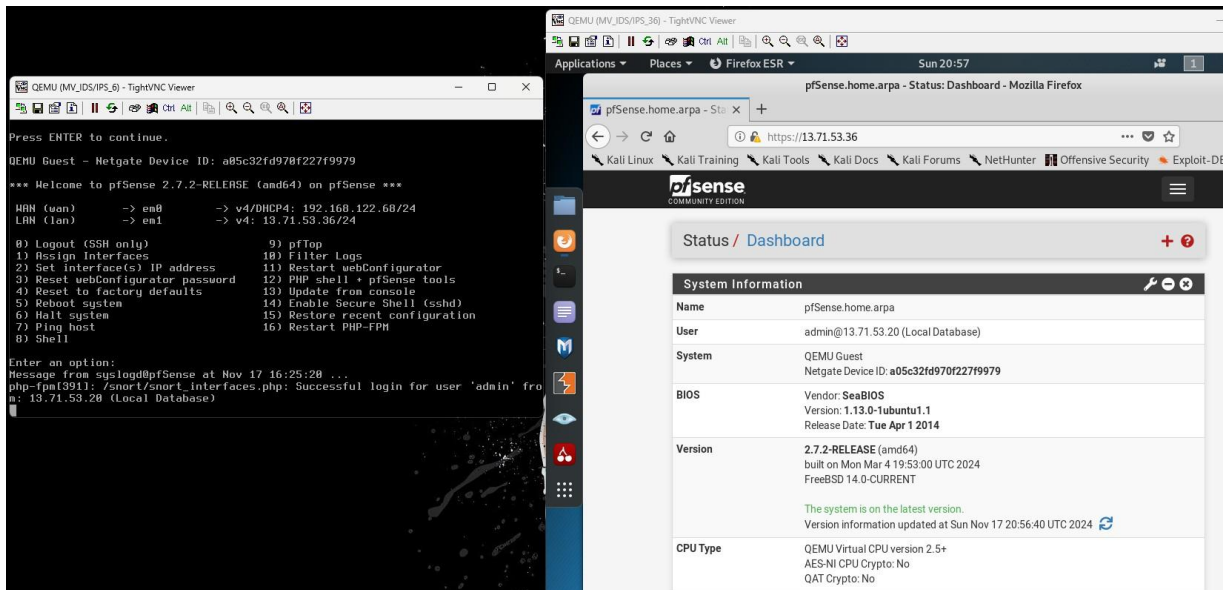


Fuente. Autoría propia

Se abre un navegador web desde la maquina Kali Linux conectada a la misma red que pfSense.



Fuente. Autoría propia



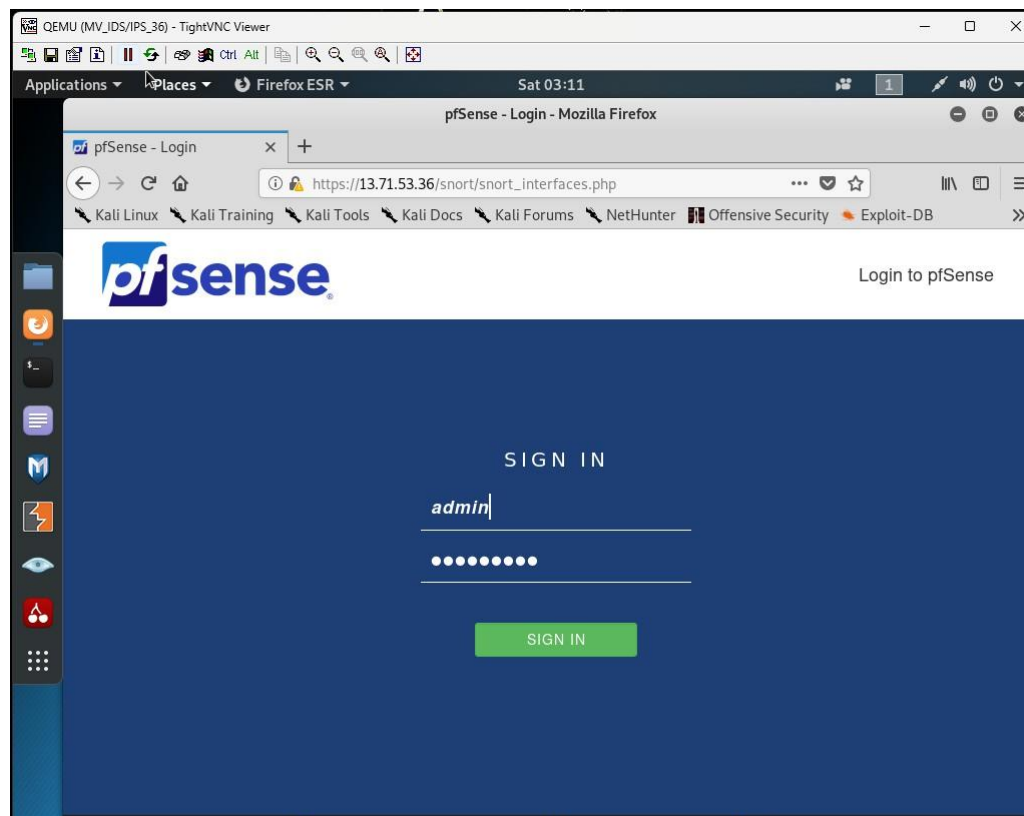
Fuente. Autoría propia

Desde un cliente de red conectado al mismo entorno que pfSense, se accede a la consola del sistema. Se accede a la interfaz de administración de pfSense, con la ip LAN que se configuro de acuerdo con la conversión de mi número de cédula 13.71.53.36. Esta dirección es la que usará para acceder al panel web de administración.

Si es el primer acceso después de la instalación, pfSense iniciará un asistente de configuración para personalizar ajustes como:

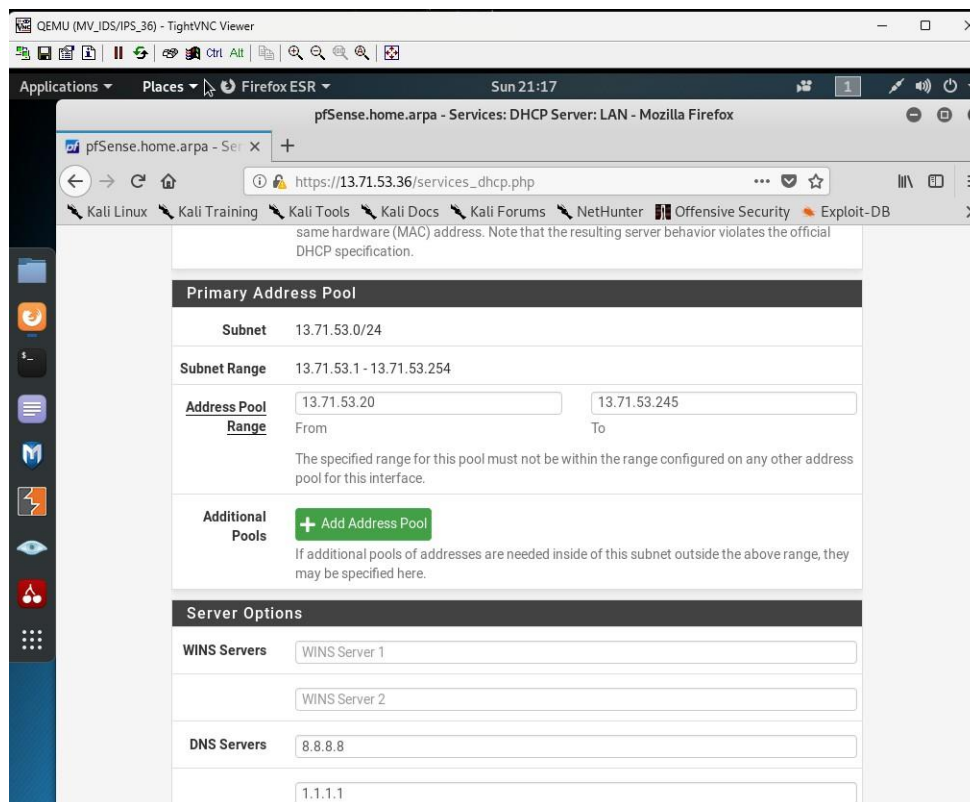
- Configuración de las interfaces de red.
- Contraseña del administrador.
- Configuración de DNS.
- Reglas de firewall básicas.

Pantalla de Inicio de Sesión de PfSense en el Navegador Web firefox



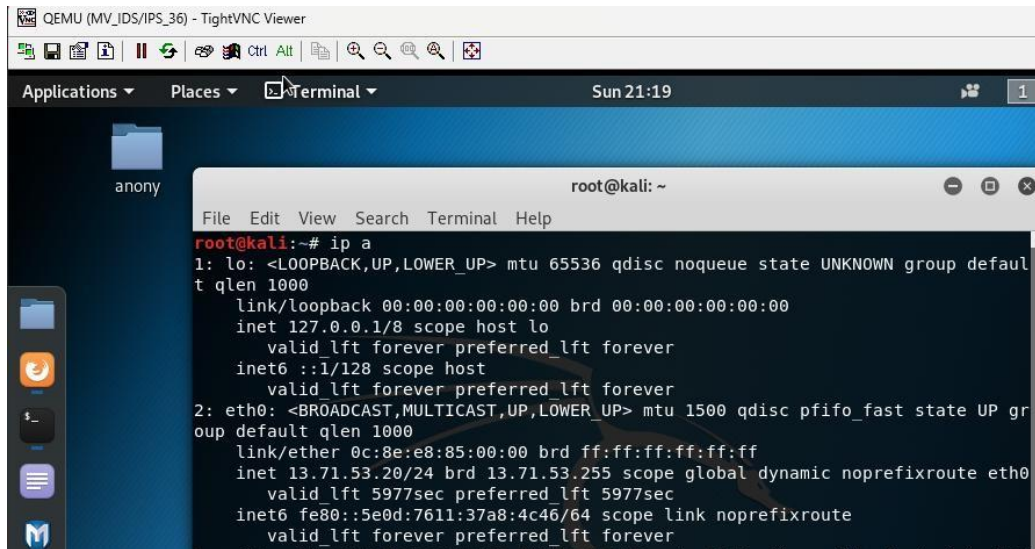
Fuente. Autoría propia

Configuración DHCP server LAN en Pfsense.



Fuente. Autoría propia

Se muestra la configuración de direcciones IP que el servidor DHCP de pfSense asigna a los dispositivos conectados a la interfaz LAN. Luego se configura los DNS.

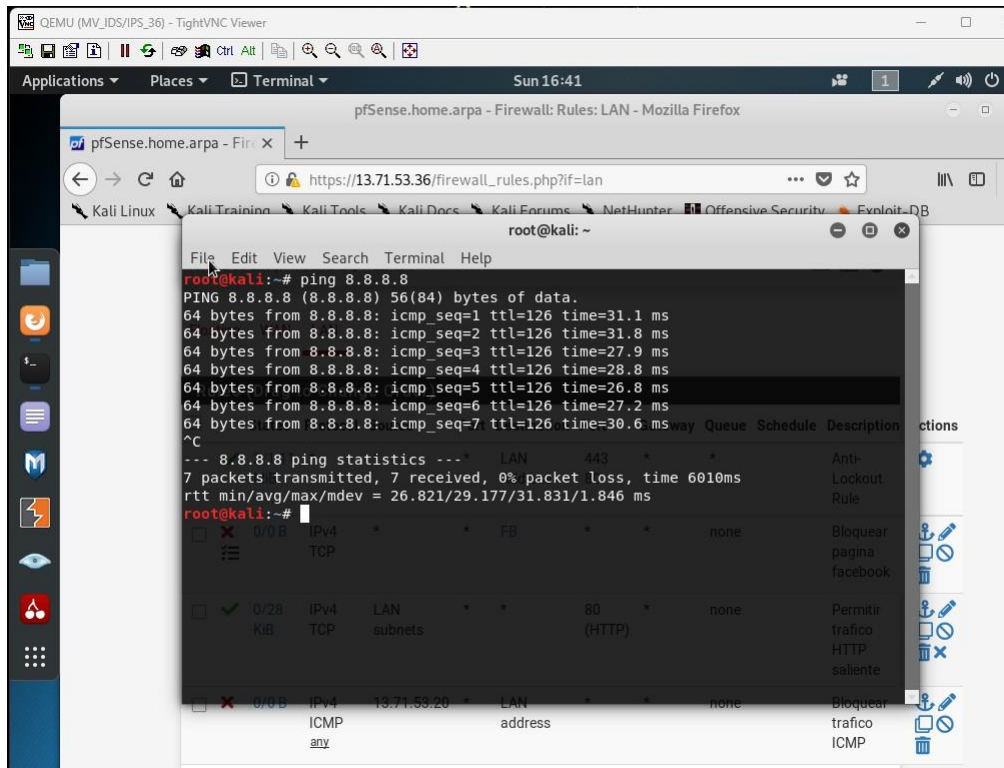


```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0c:8e:e8:85:00:00 brd ff:ff:ff:ff:ff:ff
    inet 13.71.53.20/24 brd 13.71.53.255 scope global dynamic noprefixroute eth0
        valid_lft 5977sec preferred_lft 5977sec
    inet6 fe80::5e0d:7611:37a8:4c46/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Fuente. Autoría propia

La imagen nos muestra una terminal en una máquina con Kali Linux ejecutando el comando `ip a`, que proporciona información sobre las interfaces de red configuradas en el sistema.

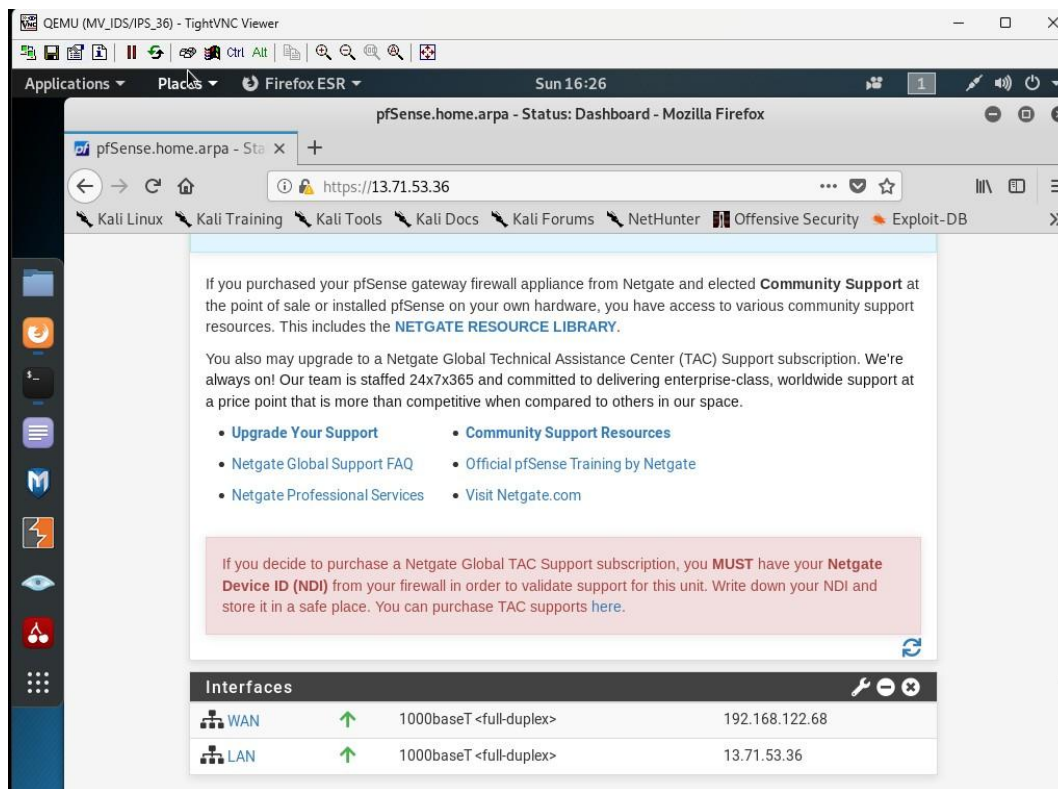
Interfaz eth0 (Ethernet): Dirección IPv4: 13.71.53.20/24, con puerta de enlace en 13.71.53.255



Fuente. Autoría propia

Confirmamos que tenemos internet en nuestra maquina Kali Linux al ejecutar el comando ping a la dirección Ip 8.8.8.8, lo cual indica que se estableció una conexión exitosa con el servidor de Google (8.8.8.8).

Interfaces configuradas



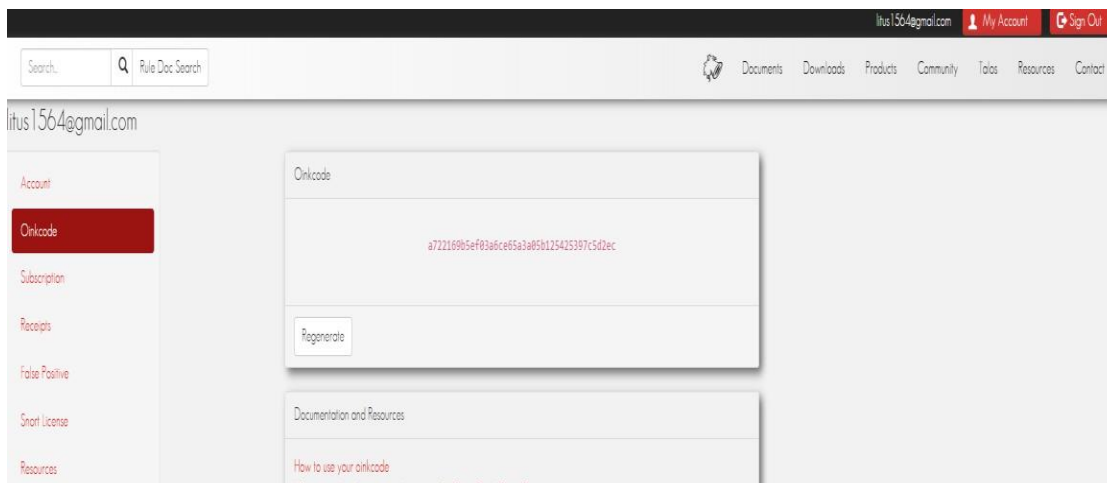
Fuente. Autoría propia

Aquí se muestran las interfaces de red configuradas en pfSense. Tienes dos interfaces:

- **WAN:** La interfaz que conecta el dispositivo a internet.
- **LAN:** La interfaz que conecta el dispositivo a la red local.

Instalación snort

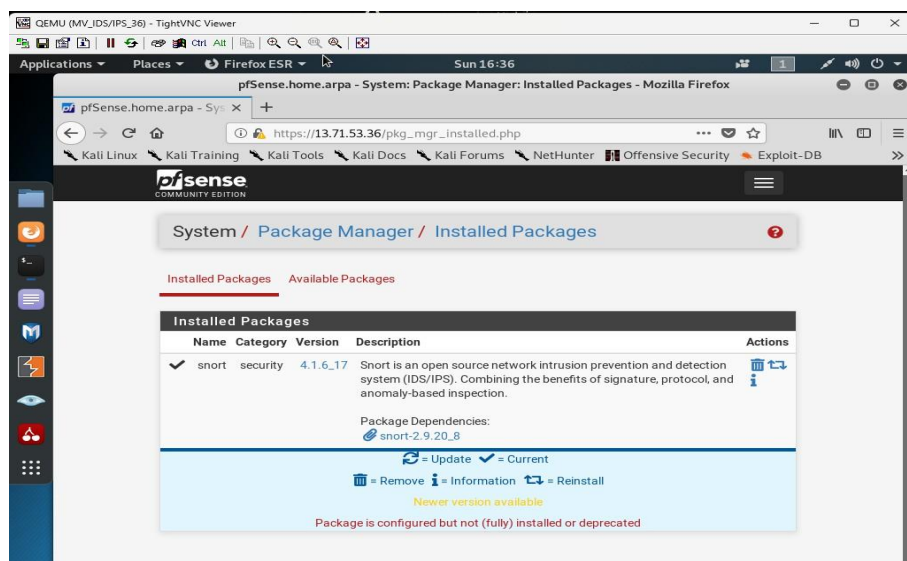
Código OinkCode de Snort



Fuente. Autoría propia

En Package Manager en PfSense se hace la descarga de Snort

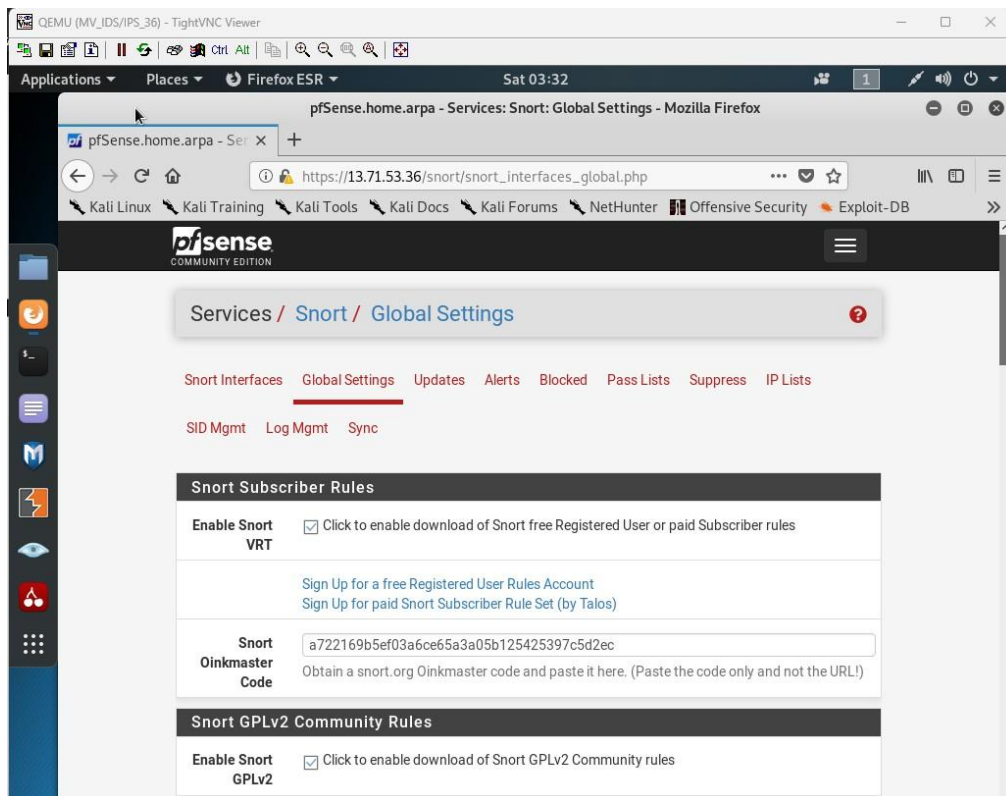
Instalación del Paquete Snort en pfSense



Fuente. Autoría propia

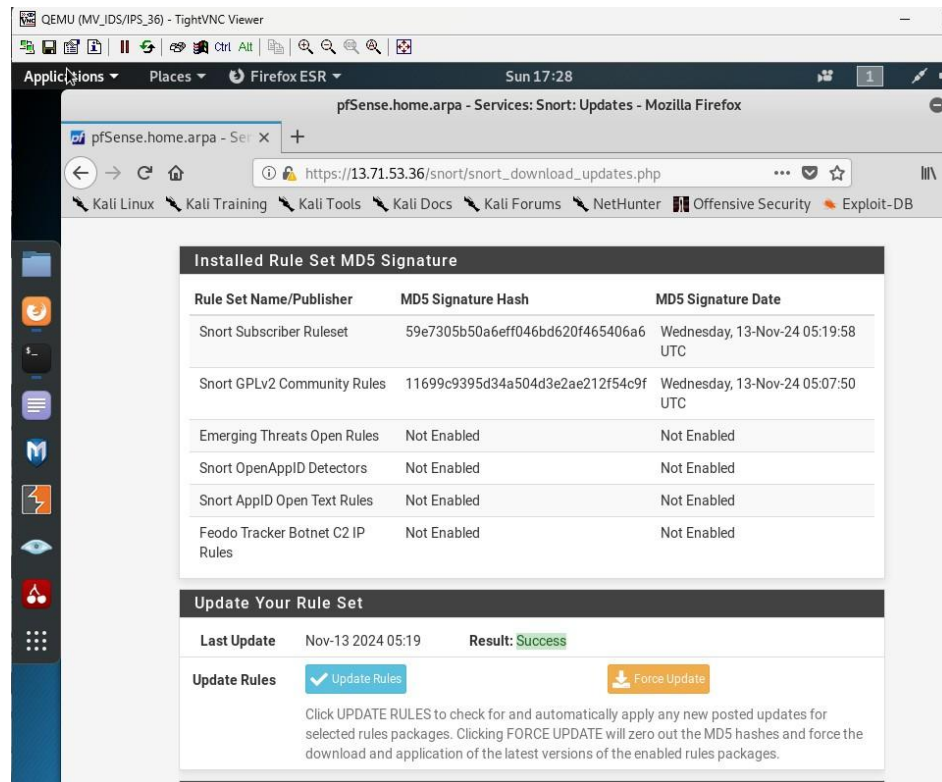
Snort es un sistema de prevención y detección de intrusiones de código abierto muy popular. Se utiliza para monitorear redes y detectar actividades sospechosas, como intentos de intrusión, ataques y otros tipos de amenazas.

Configuración Código OinkCode



Fuente. Autoría propia

Configuración de actualizaciones de reglas de Snort en un sistema basado en pfSense.



Fuente. Autoría propia

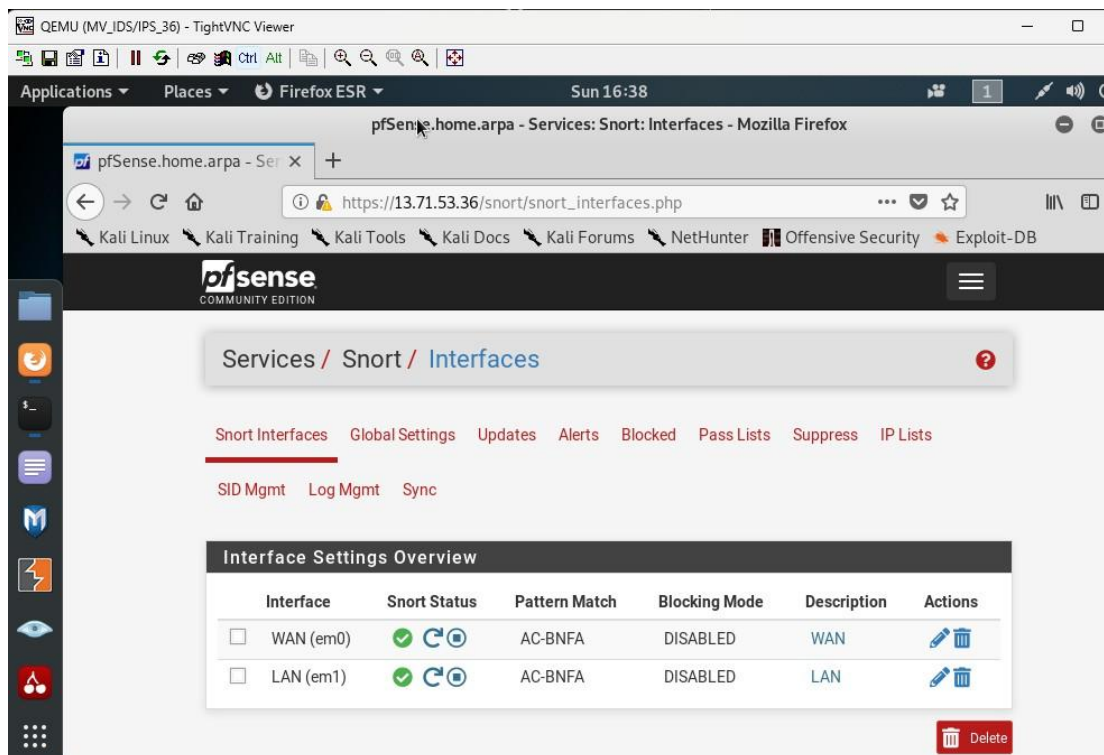
Installed Rule Set MD5 Signature

Snort Subscriber Ruleset: Estado: Activado y actualizado.

Snort GPLv2 Community Rules: Estado: Activado y actualizado.

Update Your Rule Set: **Resultado:** Éxito.

Configuración de Interfaces en Snort



Fuente. Autoría propia

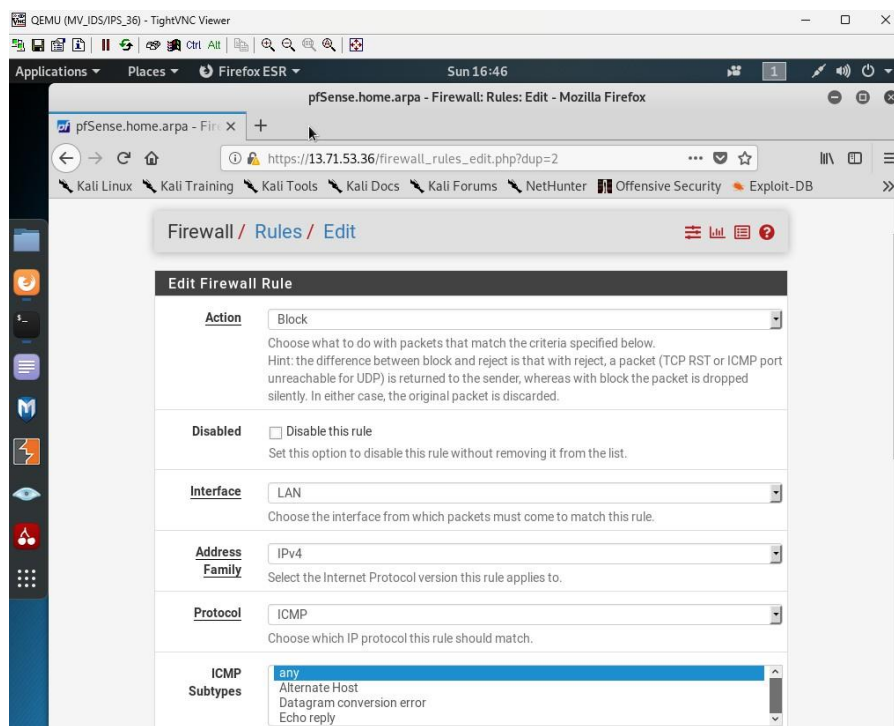
Creación reglas

Reglas de denegación

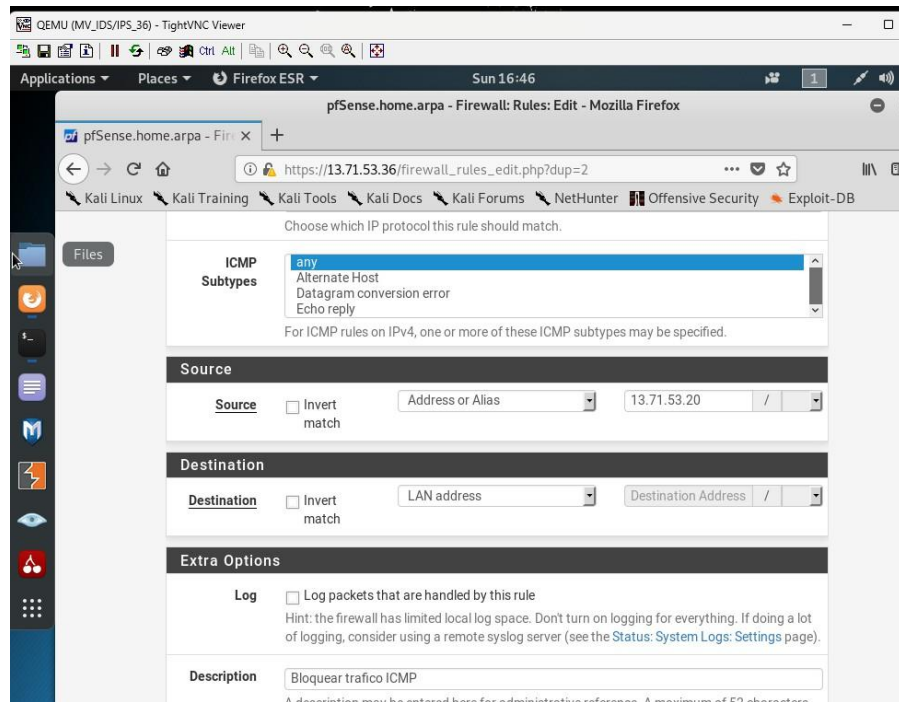
Bloquear tráfico ICMP

ICMP (Internet Control Message Protocol) es un protocolo de red usado principalmente para diagnosticar problemas en las comunicaciones entre dispositivos. Ejemplos de su uso incluyen el comando ping para verificar la conectividad y las notificaciones de error, como

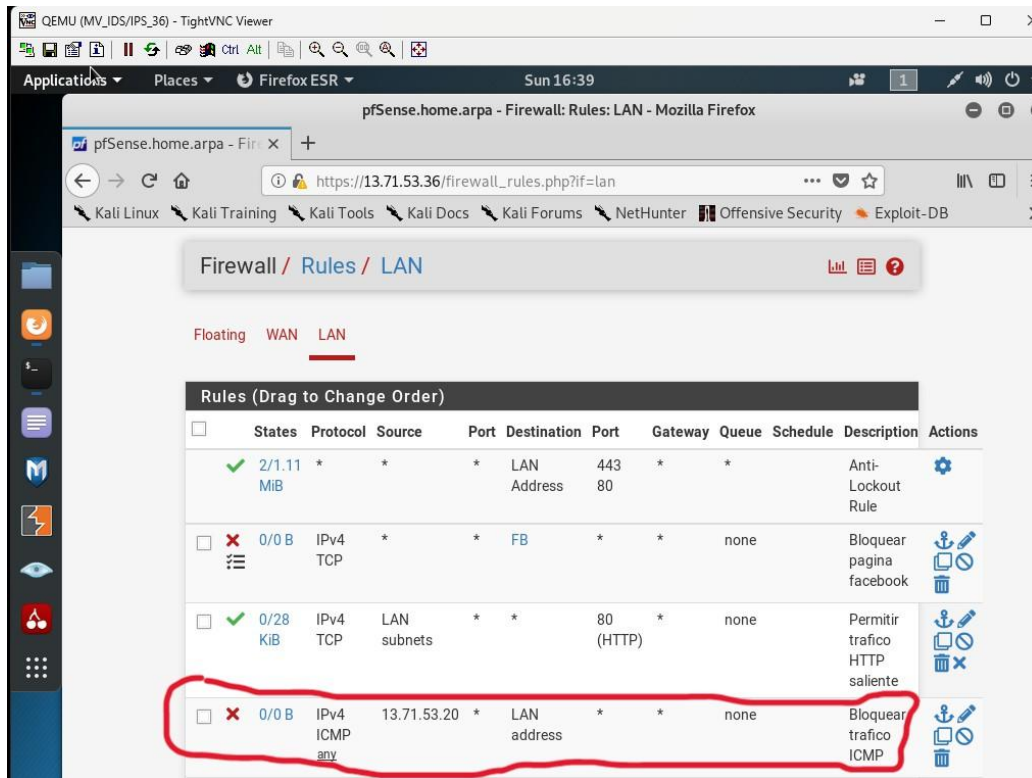
"Host inalcanzable". Bloquear respuestas ICMP evita que usuarios externos recopilen información sobre la infraestructura.



Fuente. Autoría propia

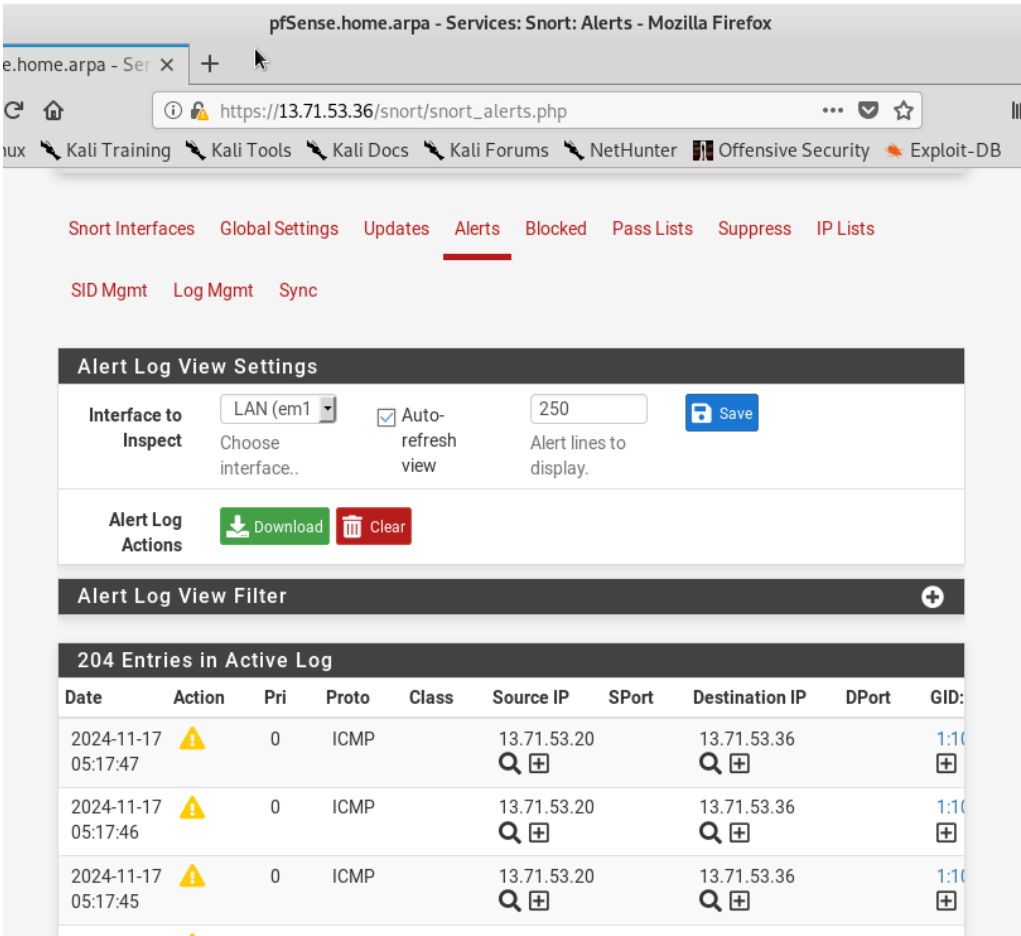


Fuente. Autoría propia



Fuente. Autoría propia

Tráfico ICMP detectado

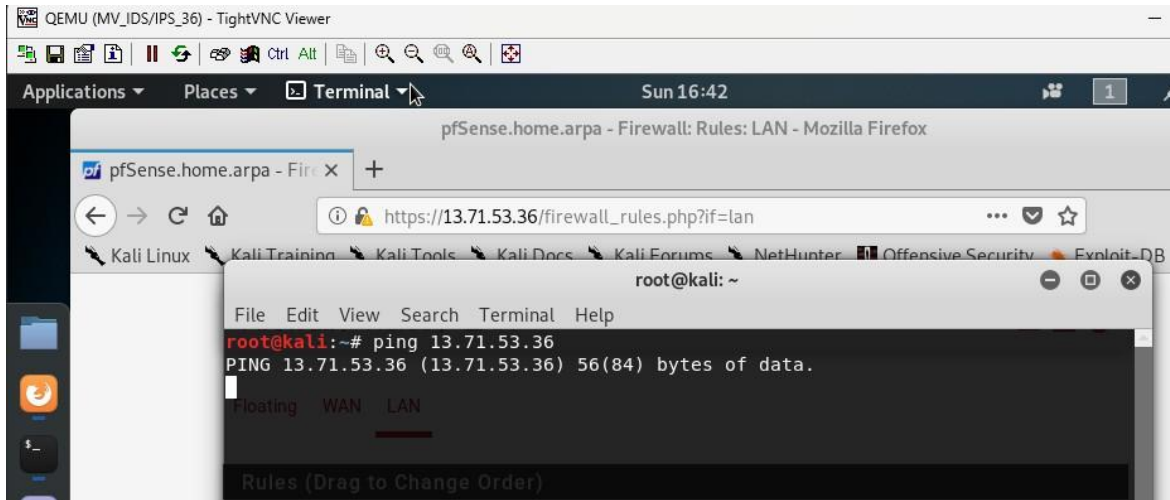


Fuente. Autoría propia

Las alertas muestran paquetes ICMP provenientes de la IP **13.71.53.20** dirigidos a la IP **13.71.53.36**.

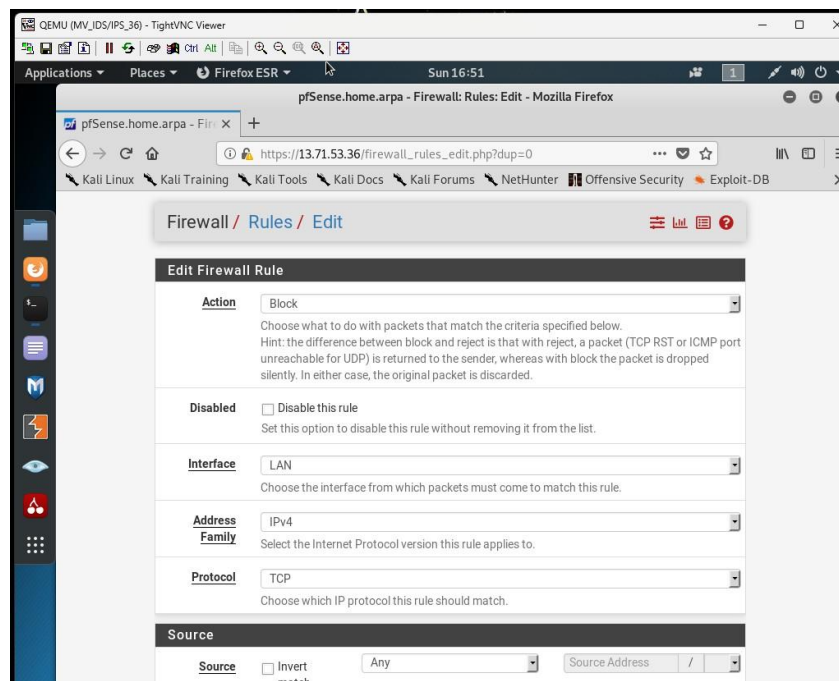
Esto indica que **Snort** está monitoreando y generando alertas para este tipo de tráfico.

Probar tráfico ICMP bloqueado: Ejecuta un comando ping como 8.8.8.8

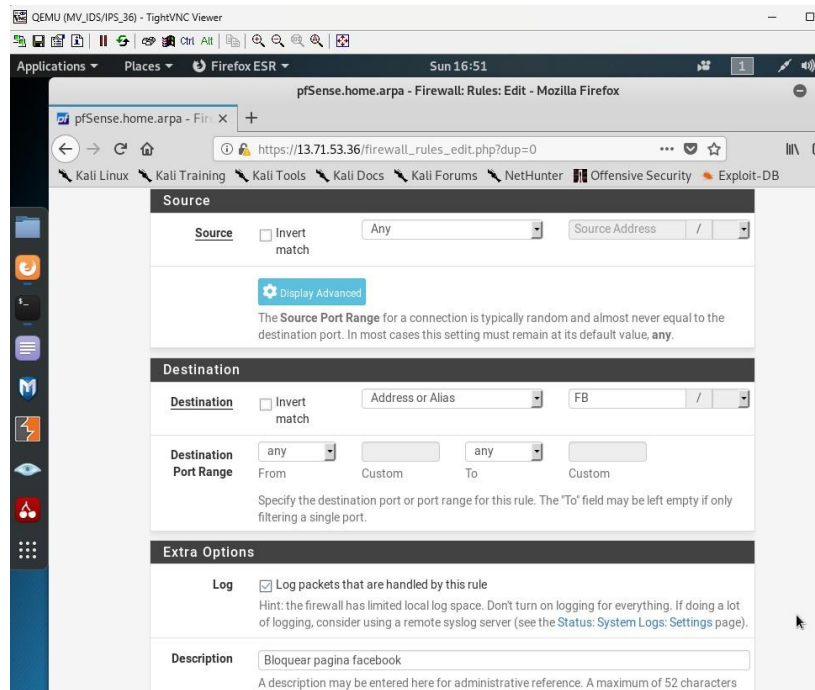


Fuente. Autoría propia

Bloquear página de Facebook

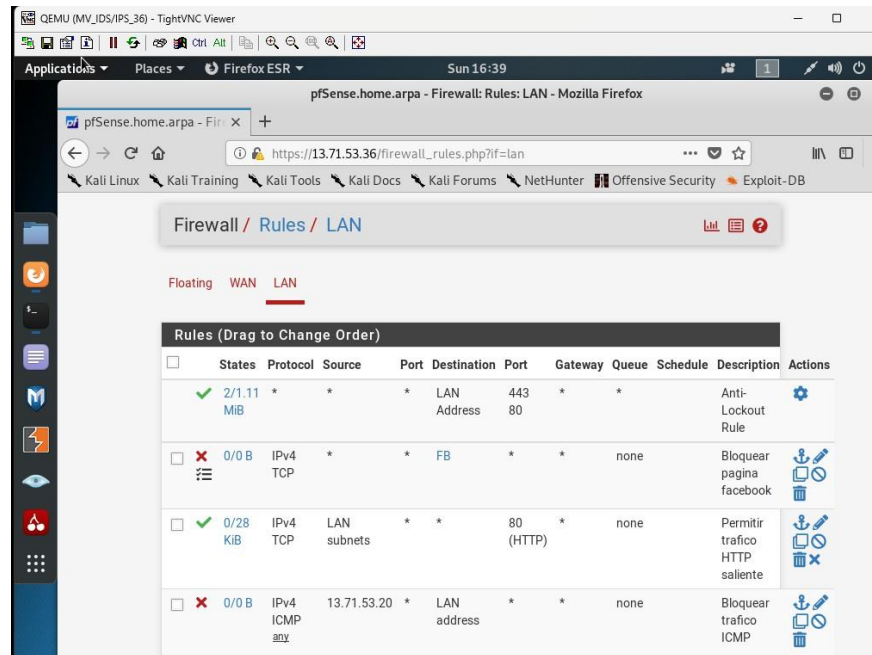


Fuente. Autoría propia



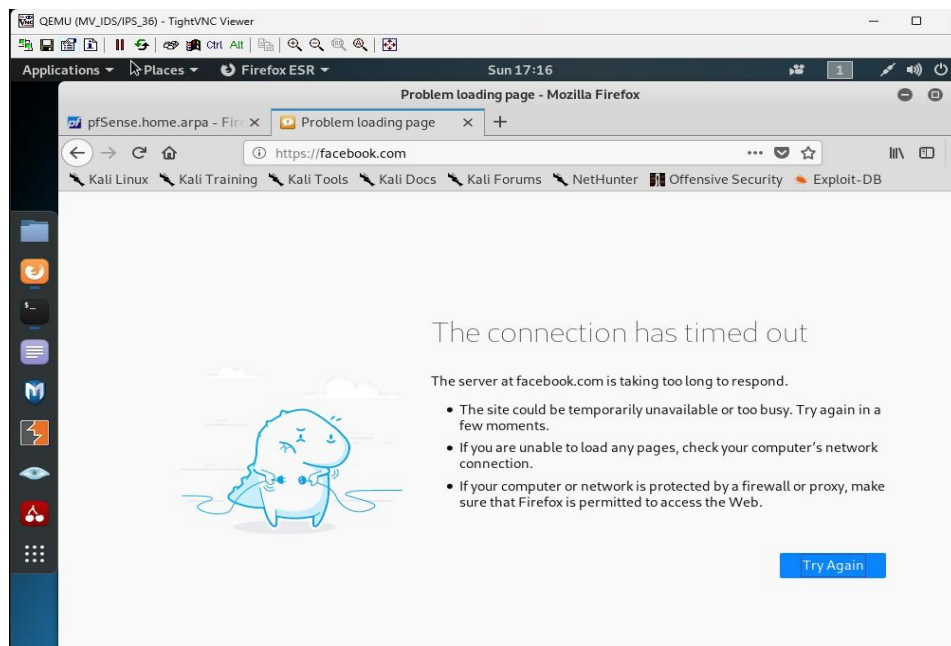
Fuente. Autoría propia

Al configurar una regla que bloquea todo el tráfico hacia “FB” , se está impidiendo que cualquier dispositivo dentro de la red pueda establecer una conexión con los servidores de Facebook.



Fuente. Autoría propia

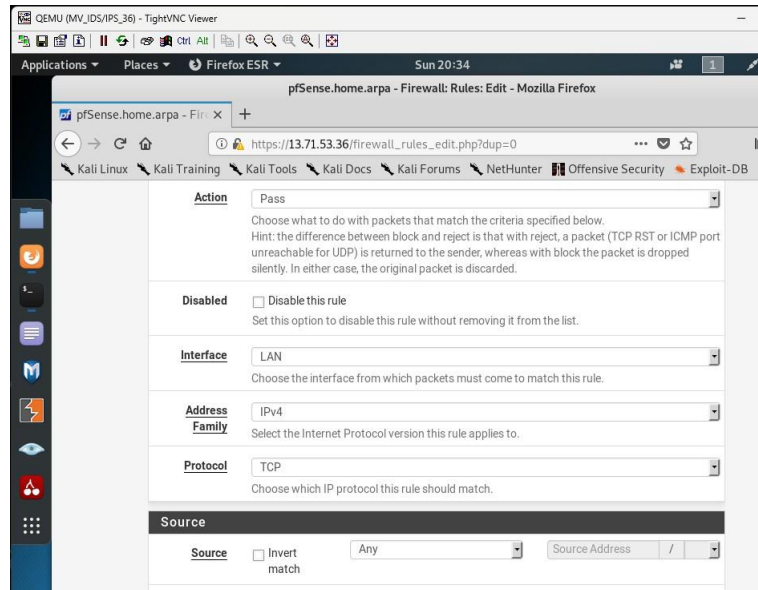
El mensaje de error indica que la conexión ha excedido el tiempo de espera, lo que significa que el servidor de Facebook no ha respondido a la solicitud del navegador.



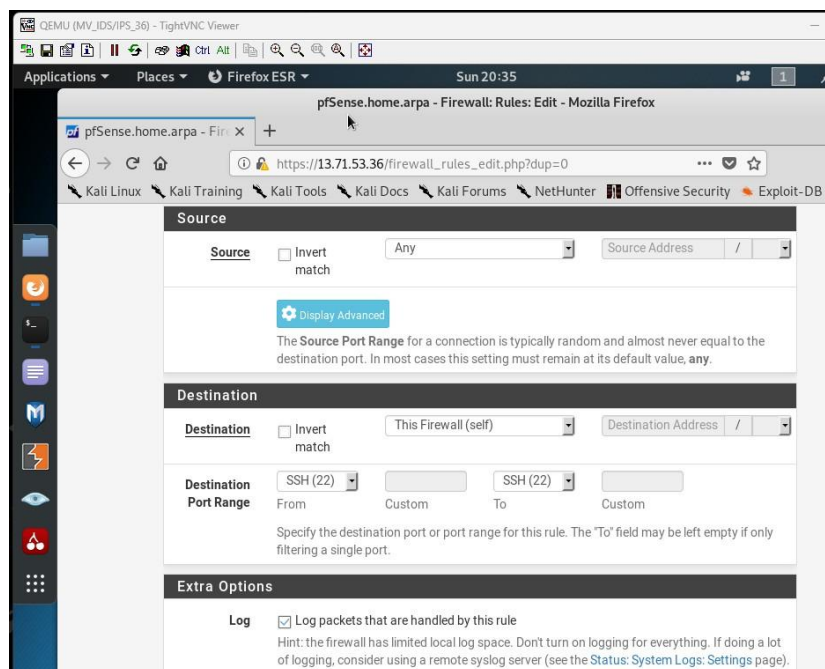
Fuente. Autoría propia

Reglas de aceptación

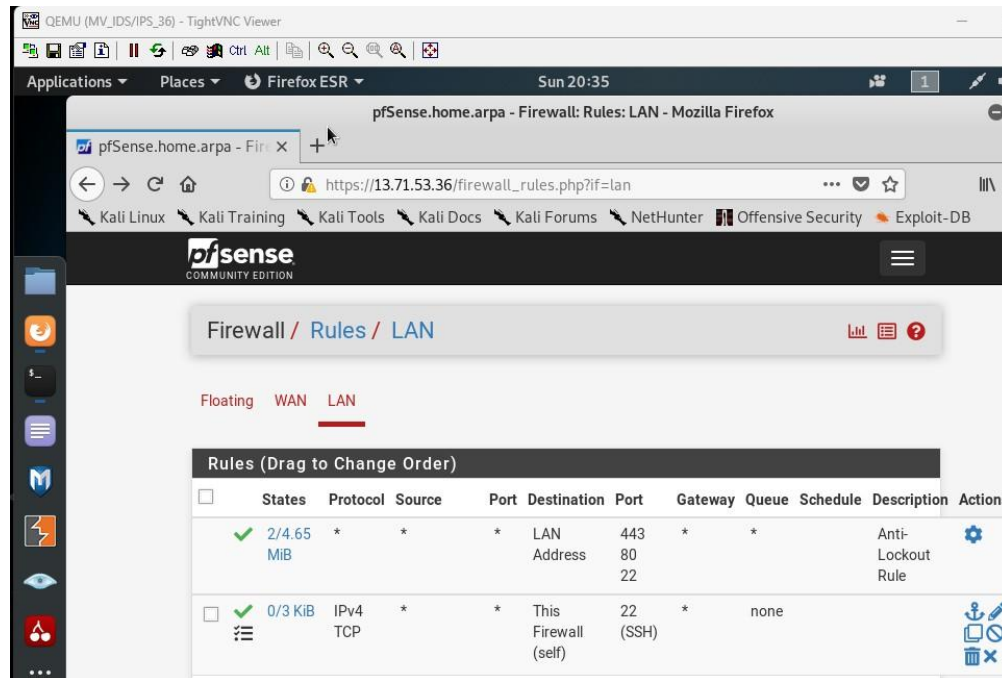
Permitir conexión SSH



Fuente. Autoría propia

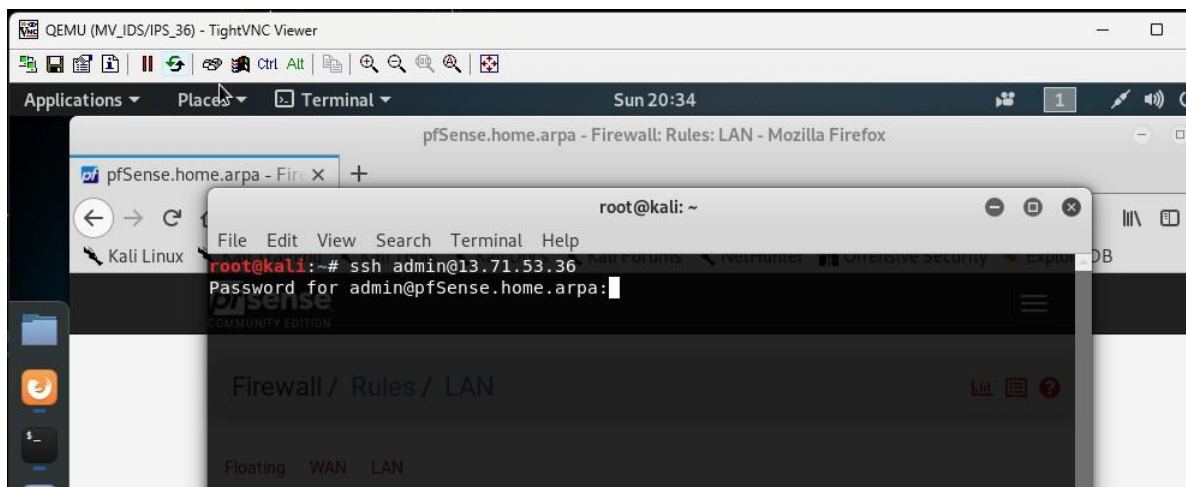


Fuente. Autoría propia



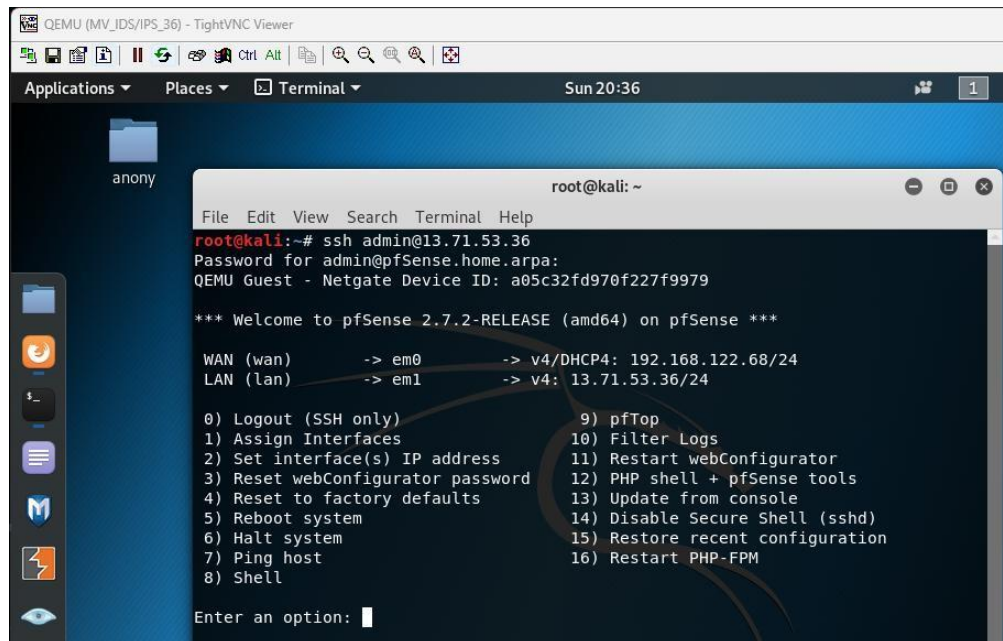
Fuente. Autoría propia

Estableciendo una conexión segura (SSH) con el dispositivo pfSense

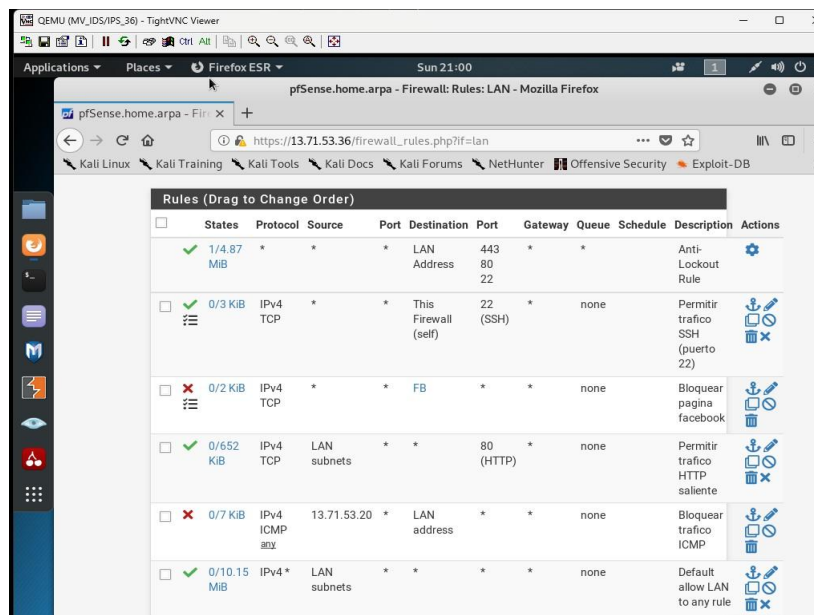


Fuente. Autoría propia

Conexión al servidor SSH

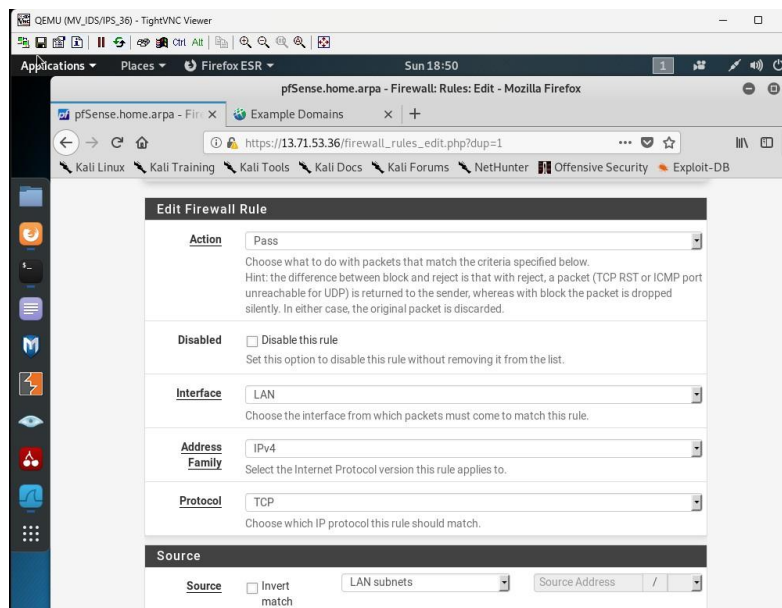


Fuente. Autoría propia

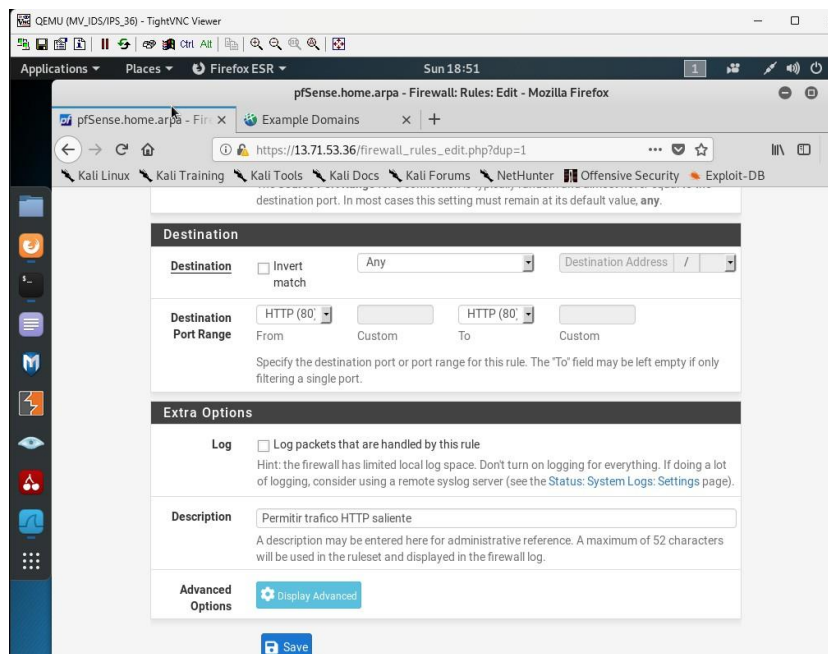


Fuente. Autoría propia

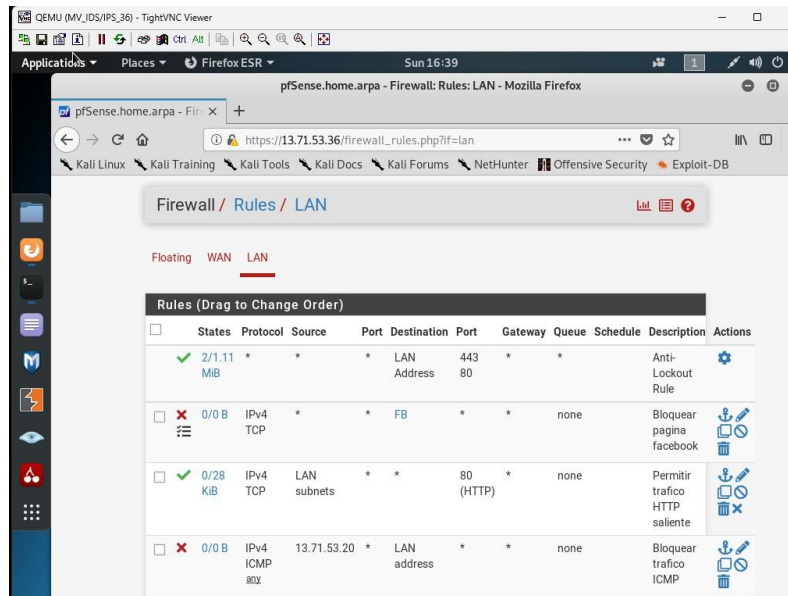
Permitir trafico HTTP saliente



Fuente. Autoría propia

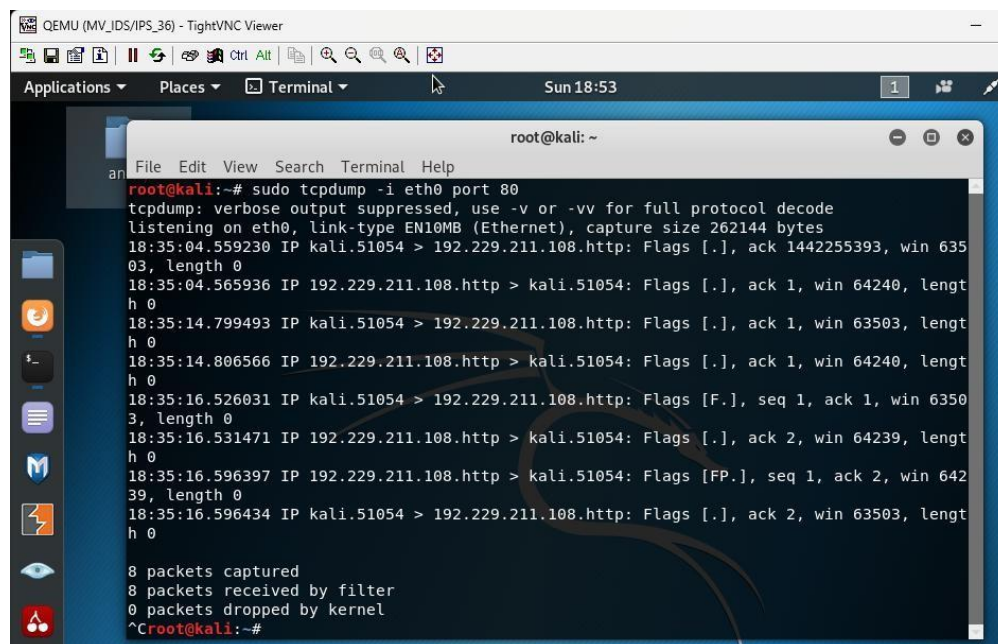


Fuente. Autoría propia



Fuente. Autoría propia

Captura de paquetes



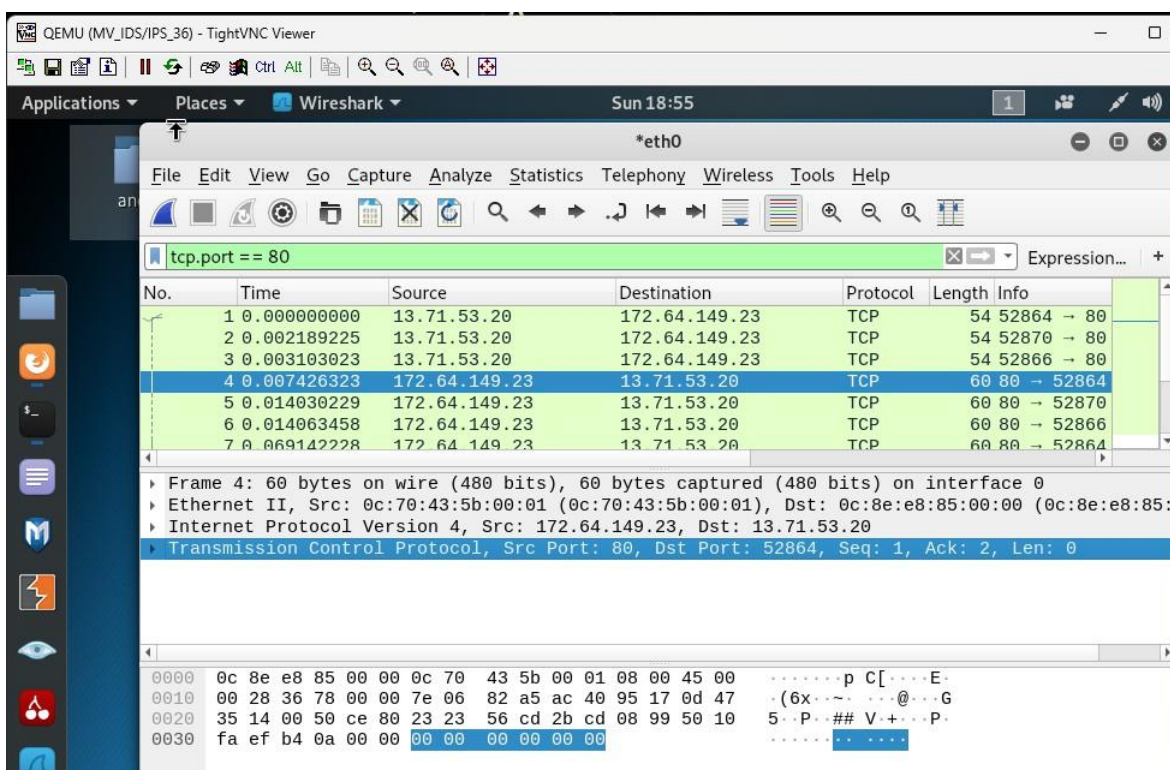
Fuente. Autoría propia

Con el comando tcpdump captura los paquetes de datos que se transmiten a través de la interfaz de red especificada.

Filtra el tráfico: En este caso, se ha utilizado la opción -i eth0 para capturar el tráfico de la interfaz de red eth0 y la opción port 80 para filtrar solo los paquetes que utilizan el puerto 80, el puerto estándar para el tráfico HTTP (el protocolo utilizado para la navegación web).

Los flags en los paquetes indican el tipo de comunicación que se está estableciendo

Captura de paquetes con Wireshark



Fuente. Autoría propia

La captura de pantalla muestra tráfico HTTP (puerto 80) analizado con Wireshark.

El filtro `tcp.port == 80` se utiliza para capturar y mostrar solo tráfico TCP relacionado con el puerto 80, que normalmente corresponde a HTTP.

Conexión cliente-servidor:

- **Dirección IP de origen:** 13.71.53.20.
- **Dirección IP de destino:** 172.64.149.23.
- Esto indica que el host 13.71.53.20 (cliente) se está comunicando con el servidor 172.64.149.23 en el puerto HTTP.

Conclusiones

- La implementación de un firewall con PfSense y la integración de un sistema IDS como Snort permite emular un entorno seguro en el que se pueden aplicar y probar políticas de seguridad de manera efectiva.
- Las reglas de denegación y aceptación configuradas demostraron ser efectivas para controlar el acceso a servicios específicos, garantizando un equilibrio entre seguridad y funcionalidad.
- El uso de GNS3 como herramienta de simulación proporciona un entorno flexible y realista para el aprendizaje y prueba de configuraciones avanzadas de redes y seguridad.
- Este proyecto resalta la importancia de contar con un diseño estructurado y reglas claras para garantizar la protección de los sistemas de información frente a amenazas potenciales.
- La práctica reforzó los conocimientos teóricos y mostró cómo aplicar herramientas profesionales en escenarios reales para resolver problemas de seguridad.

Referencias bibliográficas

Carroll, J. (2022). Infraestructuras seguras. [Objeto_virtual_de_Informacion_OVI].

Repositorio Institucional UNAD.

<https://repository.unad.edu.co/handle/10596/53880>

Carroll, J. (2024). Cipas infraestructuras seguras - 20241105_190548 [Grabación de reunión]. SharePoint UNAD. [https://unadvirtualedu-](https://unadvirtualedu-my.sharepoint.com/personal/joel_carroll_unad_edu_co/_layouts/15/stream.aspx?id=%2Fpersonal%2Fjoel%5Fcarroll%5Funad%5Fedu%5Fco%2FDocuments%2FRecordings%2FCipas%20Infraestructuras%20seguras%2D20241105%5F190548%2DGrabaci%C3%B3n%20de%20la%20reuni%C3%B3n%2Emp4)

[my.sharepoint.com/personal/joel_carroll_unad_edu_co/_layouts/15/stream.aspx?id=%2Fpersonal%2Fjoel%5Fcarroll%5Funad%5Fedu%5Fco%2FDocuments%2FRecordings%2FCipas%20Infraestructuras%20seguras%2D20241105%5F190548%2DGrabaci%C3%B3n%20de%20la%20reuni%C3%B3n%2Emp4](https://unadvirtualedu-my.sharepoint.com/personal/joel_carroll_unad_edu_co/_layouts/15/stream.aspx?id=%2Fpersonal%2Fjoel%5Fcarroll%5Funad%5Fedu%5Fco%2FDocuments%2FRecordings%2FCipas%20Infraestructuras%20seguras%2D20241105%5F190548%2DGrabaci%C3%B3n%20de%20la%20reuni%C3%B3n%2Emp4)

DimensionQuest. (2023, abril, 5). *pfSense 2.7.0 Daily on VMware Workstation 17 Pro*

[Video]. YouTube. <https://www.youtube.com/watch?v=bZYR-ifkx90>

Snort. (2024). *Snort Ruleset Configuration and Updates on pfSense*. Recuperado el 13 de noviembre de 2024, de https://13.71.53.36/snort/snort_download_updates.php

GNS3. (2023). *GNS3 official documentation: Installation and configuration guide*.

Recuperado de <https://docs.gns3.com>

OpenSSH. (2023). *OpenSSH user manual*. OpenBSD Project. Recuperado de <https://www.openssh.com>