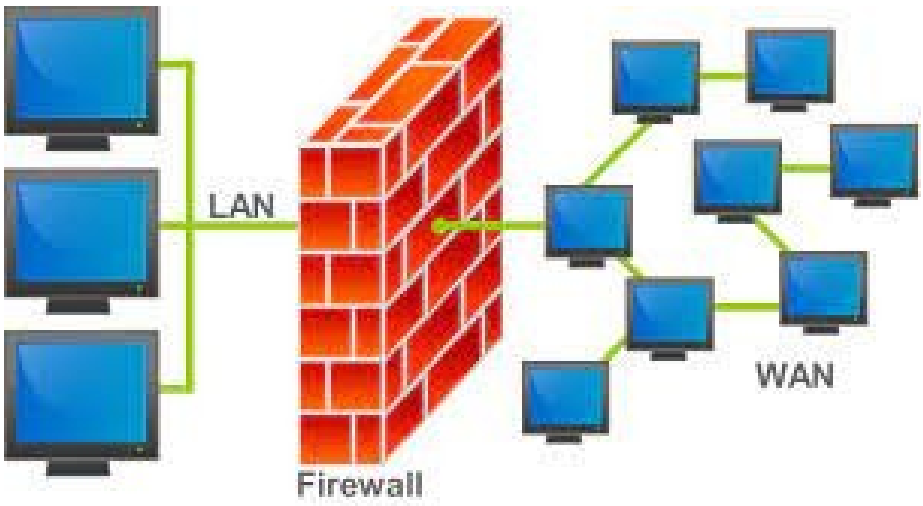
Práctica de Evaluación 12
Conceptos y Practicas con cortafuegos

2ºASIR

DIEGO ACOSTA CABRERA



Actividad 1 – 2p Describe las características, tipos y funciones de los cortafuegos

Un cortafuegos actuá principalmente de forma que trata de **prevenir** todo tipo de ataque que intentas entrar a nuestra red desde el exterior y **controlar** el traspaso de paquetes para mantener la seguridad de nuestra red o equipo personal.

Para poder llevar acabo dicho control estos deben realizar unas funciones especificas como:

- Establecer una protección basada en normas
- Filtrar el tráfico de entrada a través de sistemas más confiables.
- Establecer mecanismos de autenticación más fuertes.
- Ocultar información sobre la red que se quiere proteger.
- Crear registros LOG de información.

Estos tambien se puedes diferenciar según su área de influencia o su tecnología utilizada de forma que se clasifican de la siguiente manera:

Según su **área de influencia** pueden ser:

-**Personales**: estos suelen estar incluidos dentro del software de los sistemas operativos de los dispositivos y se centran principalmente en proteger el trafico que entra y sale de el equipo.

-**Corporativos**: se utilizan en pequeñas redes locales utilizando diferentes extensiones que añades mas funciones al cortafuegos como antivirus, filtrado IP, filtrado de contenidos web, o detección de intrusos.

-**De pequeña oficina**: se encargan de controlar las conexiones de la red de una organización, por lo que deben soportar miles de conexiones. Su potencia y capacidad de proceso deben ser mayores que las de las instalaciones personales o de pequeñas oficinas.

Según sus **tecnologías utilizadas** se clasifican según sus objetivos como:

-**Filtrado de paquetes**: su objetivo es comparar cada paquete recibido con un conjunto de criterios establecidos, como las direcciones IP, tipo de paquete, número de puerto, etc. Los paquetes marcados como sospechosos son desechados y por lo tanto dejan de existir.

-**Circuito a nivel de pasarela**: en este caso la seguridad solo se aplica en la conexión TCP o UDP establecida. Esto hace que nada mas establecida la conexión ya se pueda navegar libremente por la red sin ningún tipo de examen de seguridad lo que hace que solo se use normalmente si se tiene confianza en los usuarios internos

-**Inspección de estado**: este caso es muy parecido al filtrado de paquetes pero con la diferencia de que hace un seguimiento del paquete al completo hasta que se establezca una conexión TCP establecida. Esto también hace que se genere mayor consumo del rendimiento de la red.

-**Capa de aplicación**: también llamado firewall proxy, estos combina algunos de los atributos de los firewalls de filtrado de paquetes con los de las pasarelas de nivel de circuito y filtran los paquetes no solo de acuerdo con el servicio para el que están destinados sino también por otras características

Actividad 2 – 2p Clasifica y describe los distintos niveles en los que se realiza el filtrado de tráfico a través de un cortafuegos

En términos generales se suelen clasificar en:

Firewall de Nivel de Red:

- Trabaja con direcciones IP de origen y destino extraídas de la cabecera de la trama IP.
- Identifica los puertos de origen y destino en la comunicación.
- Analiza la cabecera IP a nivel 3 para los protocolos TCP, UDP e ICMP.
- Reconoce si el paquete es el inicio de una solicitud de conexión.

Firewall de Nivel de Aplicación:

- Capaz de inspeccionar datos utilizados por protocolos como FTP, HTTP y SMTP, abordando transferencias de archivos, páginas web y correos electrónicos.
- Ejecuta software de servidor proxy para facilitar un control más profundo sobre las comunicaciones.

Actividad 3 – 6p

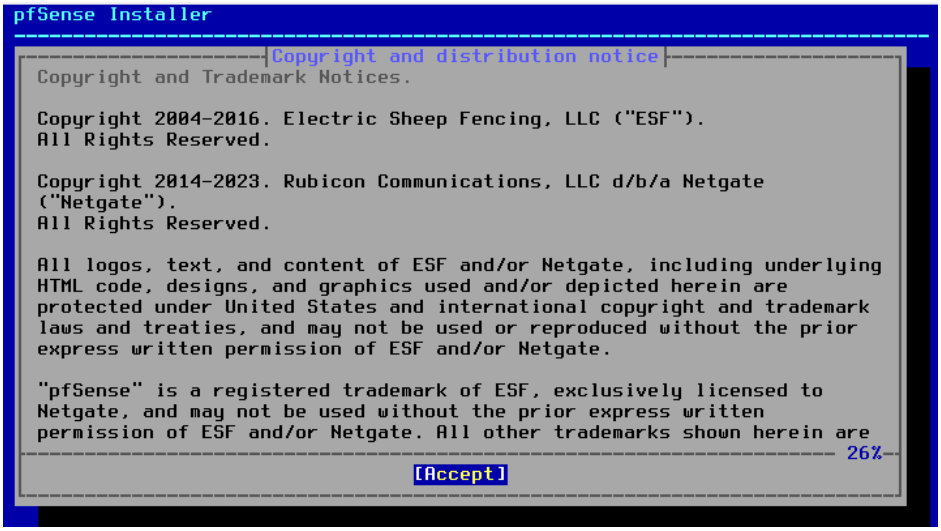
Instala pfsense con 3 tarjetas de red como bastión de tu arquitectura de red. A continuación se describe su configuración.

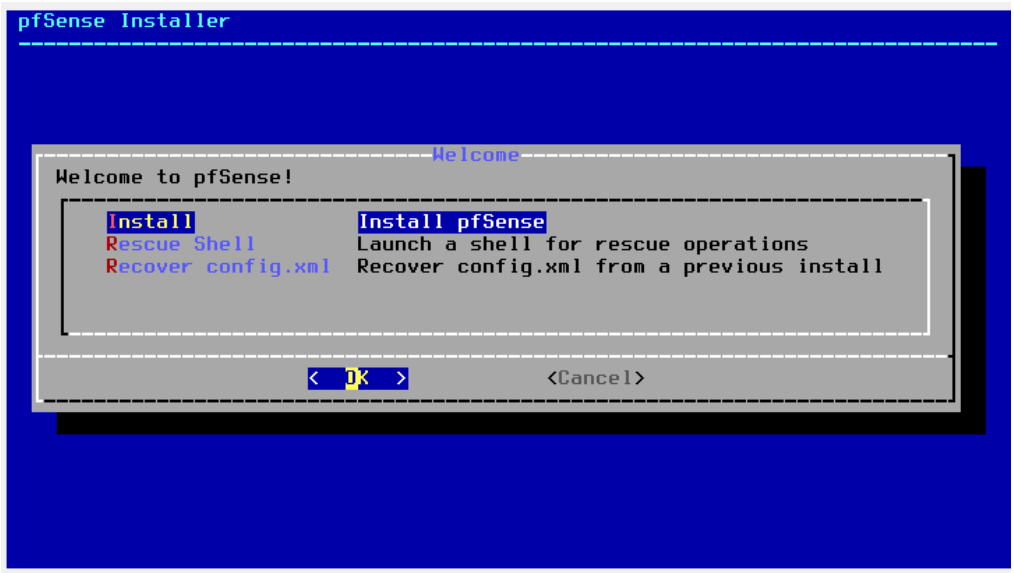
- Tarjeta 1: va a la red WAN
- Tarjeta 2: va a la LAN 192.168.10.0/24
- Tarjeta 3: va a la DMZ 192.168.20.0/24

Realiza los siguientes puntos:

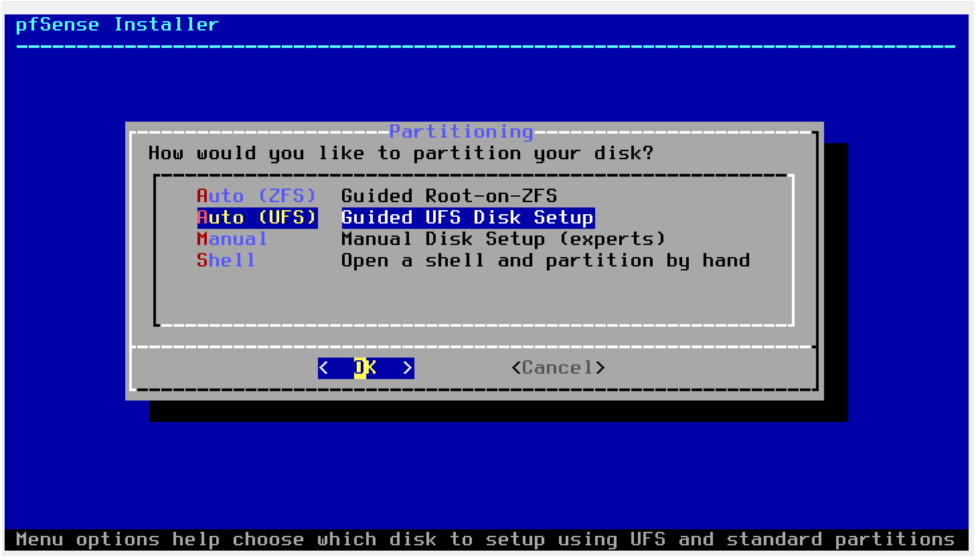
a) muestra la instalación del cortafuegos con la configuración que se dicta

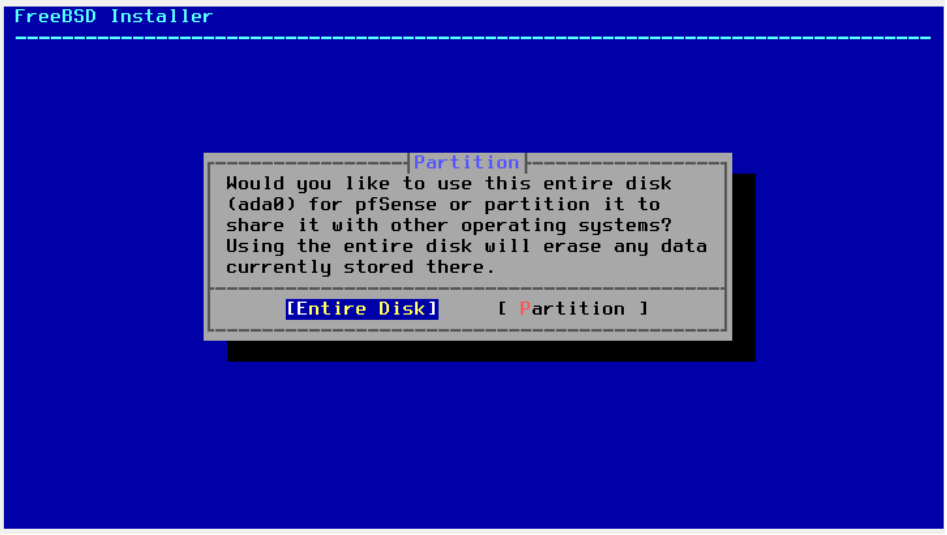
Empezamos la instalación aceptando los términos de copyright y dándole a Instalar pfsense



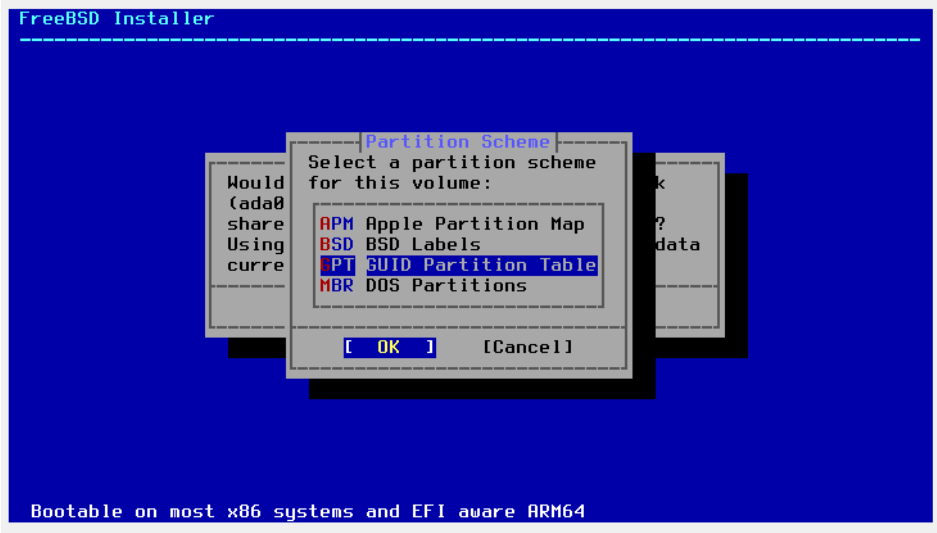


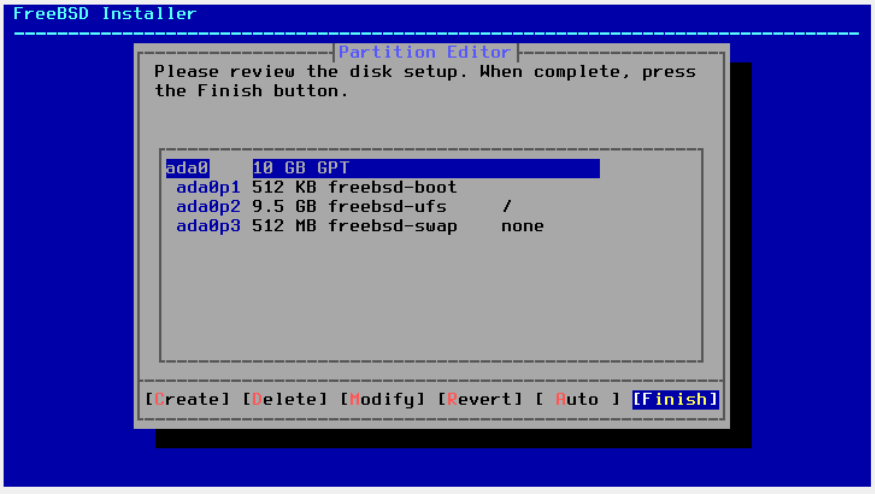
Seleccionamos la opcion de UFS para particionar nuestro disco entero.



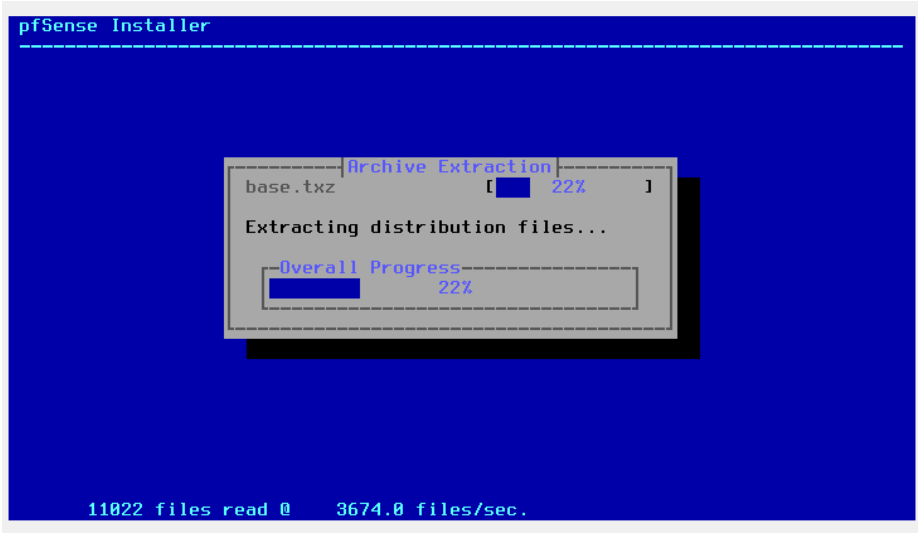


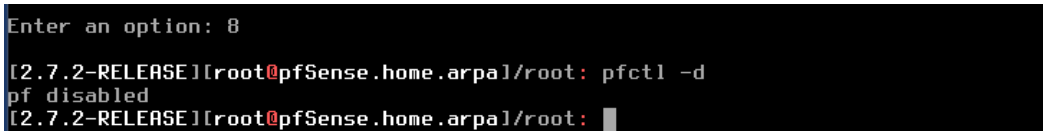
Seleccionamos la versión GUI de la tabla de particiones para verla de forma grafica y le damos a finish.





Esperamos a que termine la instalación y ahora ya podremos ver la interfaz de pfsense con las tres tarjetas que hemos configurado, ademas de aplicar el comando **pfctl -d** que nos dejara abrir la interfaz grafica de pfsense desde nuestra maquina real para mas comodidad.

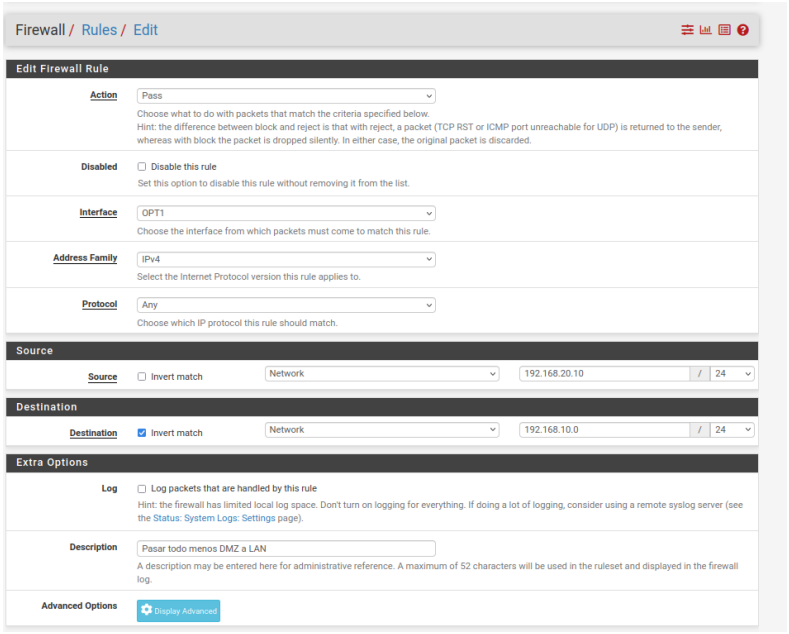




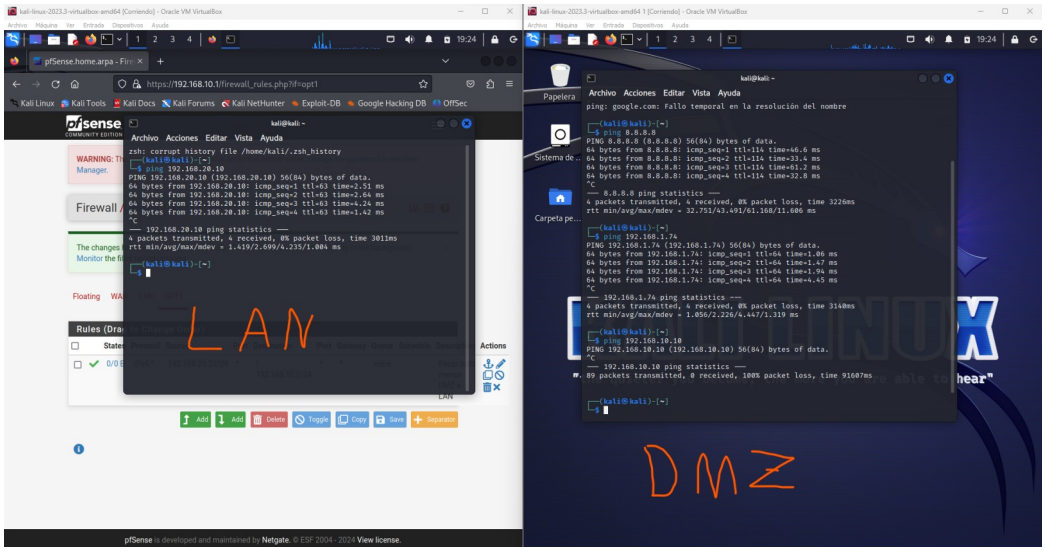
b) Realiza algunos filtros en el cortafuegos, los que tu quieras, por ejemplo, que los nodos de la red DMZ no puedan comunicarse con los nodos de la red LAN, o que los nodos de la LAN no puedan conectarse a internet y los de la DMZ si.

Prohibir conexión de la DMZ a la LAN

En esta regla especifico que toda comunicación IPv4 que salga de la DMZ este permitida menos la entrada a la red 192.168.10.0 (LAN).



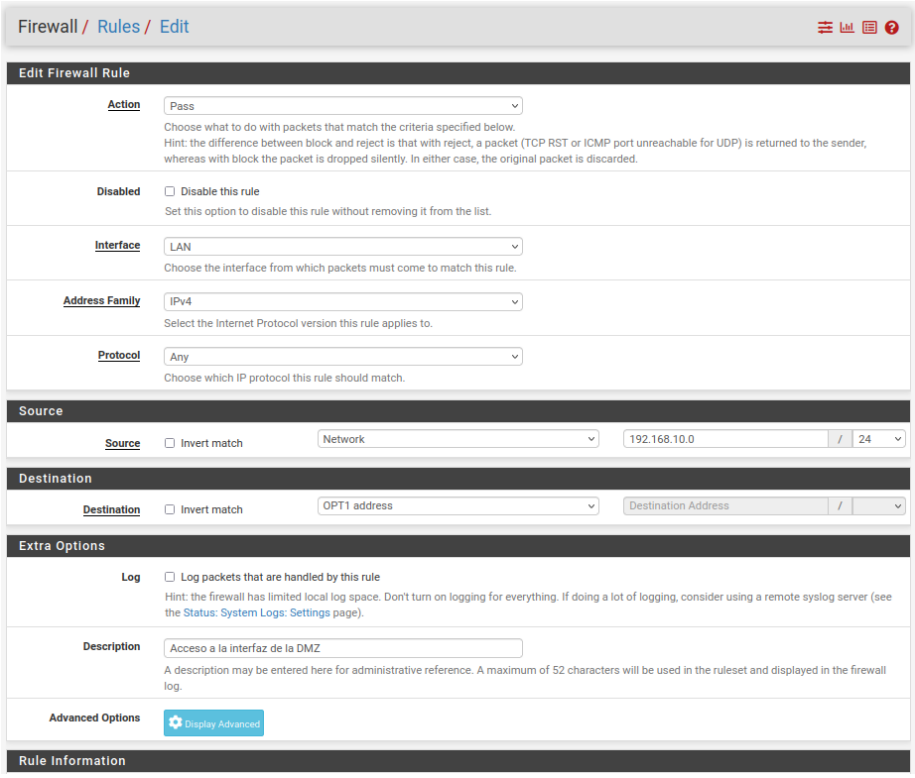
Aqui vemos que en nuestra DMZ tenemos todo tipo de conexión a internet o la interfaz WAN pero al tratar de conectar con la IP de la LAN no nos deja comunicar, en cambio como se ve en la izquierda de la LAN a la DMZ si hay comunicacion



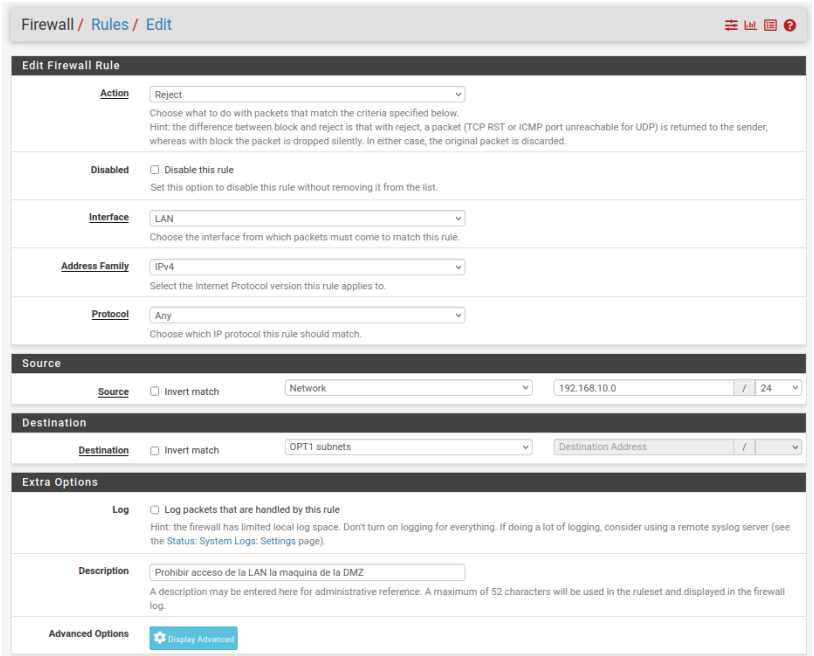
Permitir acceso de la LAN a la interfaz, pero no a la maquina de la DMZ

Aqui implemente 2 reglas:

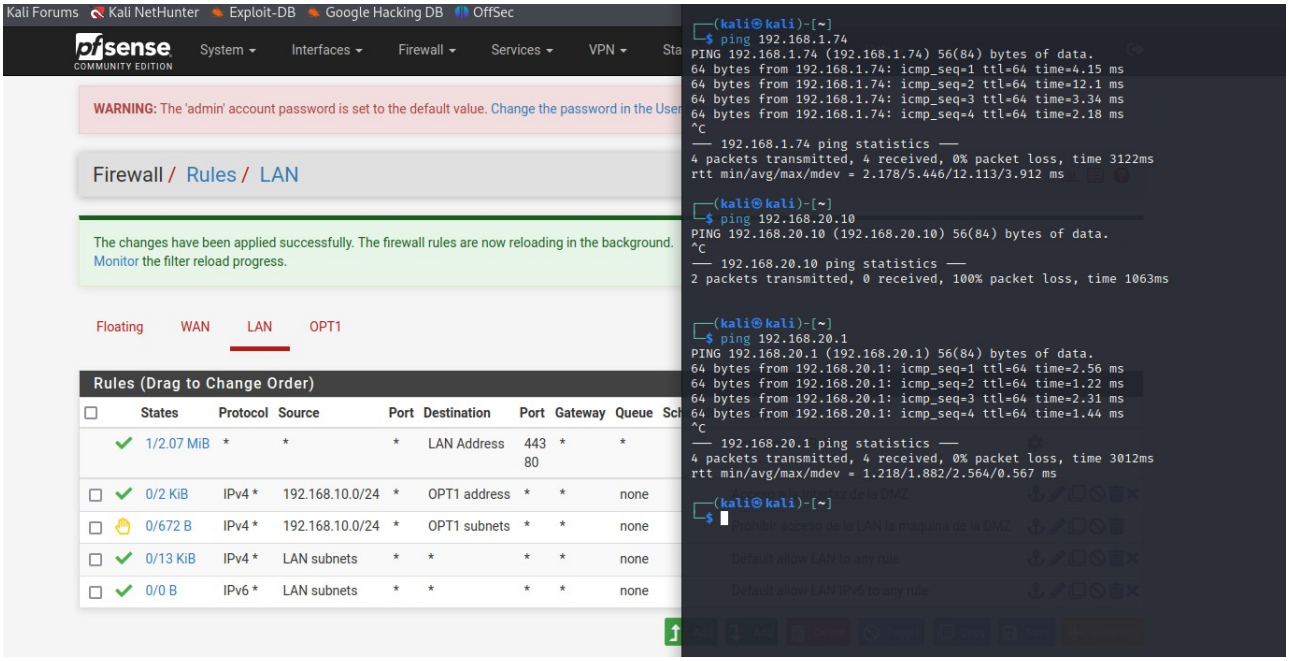
1º. Que la LAN tenga acceso a la interfaz de la DMZ



2º. Que la LAN tenga prohibido comunicarse con toda IP dentro de la red 192.168.20.0 (DMZ)

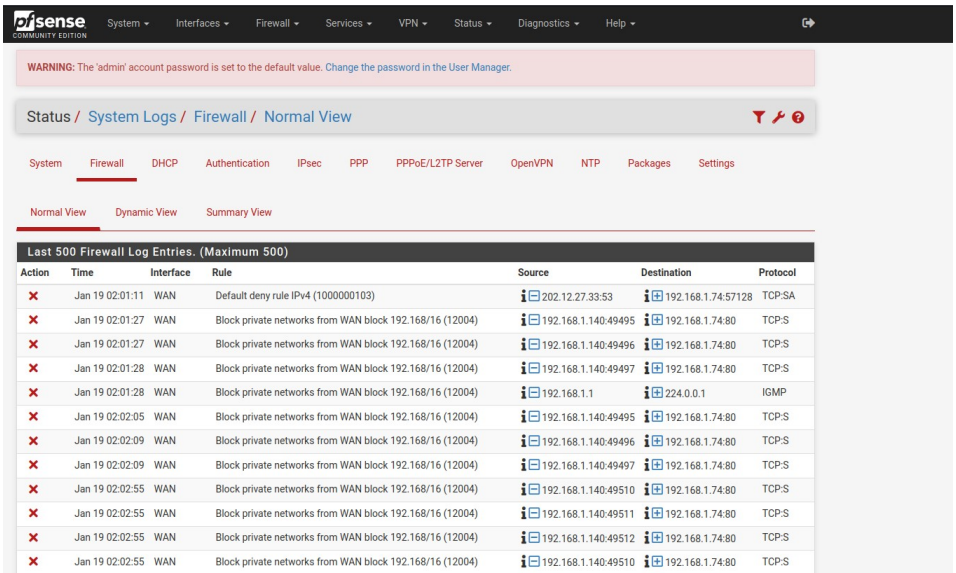


Y al poner por arriba la primera regla podemos ver que como esta tiene prioridad sobre la segunda y aunque la interfaz de la DMZ este dentro del rango de IPs bloqueadas podemos seguir comunicándonos con esta.



c) Verifica los registros de sucesos para comprobar que los filtros que aplicaste en la actividad están funcionan correctamente.

Los registros de Logs los encontraremos en el apartado **STATUS/SYSTEM LOGS/FIREWALL/**



Donde podemos observar como se ven los paquetes que se bloquearon al aplicar la primera regla que hicimos para que la DMZ no conectara con la LAN.

✕	Jan 19 05:19:38	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:19:40	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:19:41	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:19:42	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:19:43	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:19:52	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:06	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:11	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:21	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:31	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:37	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:38	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:39	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:44	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:49	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:20:54	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:21:09	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 05:21:15	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP

✕	Jan 19 03:55:02	WAN	192.168.1.1:138	192.168.1.255:138	UDP
✕	Jan 19 03:59:06	WAN	192.168.1.1	224.0.0.1	IGMP
✕	Jan 19 03:59:45	LAN	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 03:59:55	LAN	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 03:59:58	LAN	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 04:00:07	LAN	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 04:00:33	OPT1	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 04:00:44	OPT1	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 04:00:59	OPT1	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 04:01:28	LAN	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 04:02:04	OPT1	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 04:02:14	OPT1	0.0.0.0:68	255.255.255.255:67	UDP
✕	Jan 19 04:02:51	WAN	192.168.1.1	224.0.0.1	IGMP
✕	Jan 19 04:07:57	WAN	192.168.1.1	224.0.0.1	IGMP
✕	Jan 19 04:12:03	WAN	192.168.1.1	224.0.0.1	IGMP
✕	Jan 19 04:15:05	WAN	192.168.1.1	224.0.0.1	IGMP
✕	Jan 19 04:19:46	WAN	192.168.1.1	224.0.0.1	IGMP
✕	Jan 19 04:24:26	WAN	192.168.1.1	224.0.0.1	IGMP
✕	Jan 19 04:28:23	WAN	192.168.1.1	224.0.0.1	IGMP
✕	Jan 19 04:29:06	OPT1	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 04:29:11	OPT1	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 04:29:16	OPT1	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 04:29:17	OPT1	192.168.20.10	192.168.10.10	ICMP
✕	Jan 19 04:29:23	OPT1	192.168.20.10	192.168.10.10	ICMP