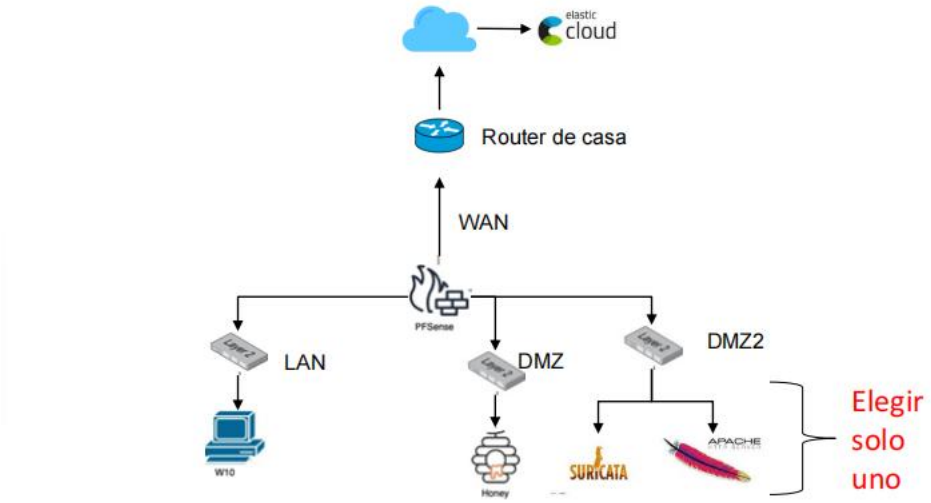
PRACTICA BLUE TEAM

ENRIQUE LOPEZ PACUAL

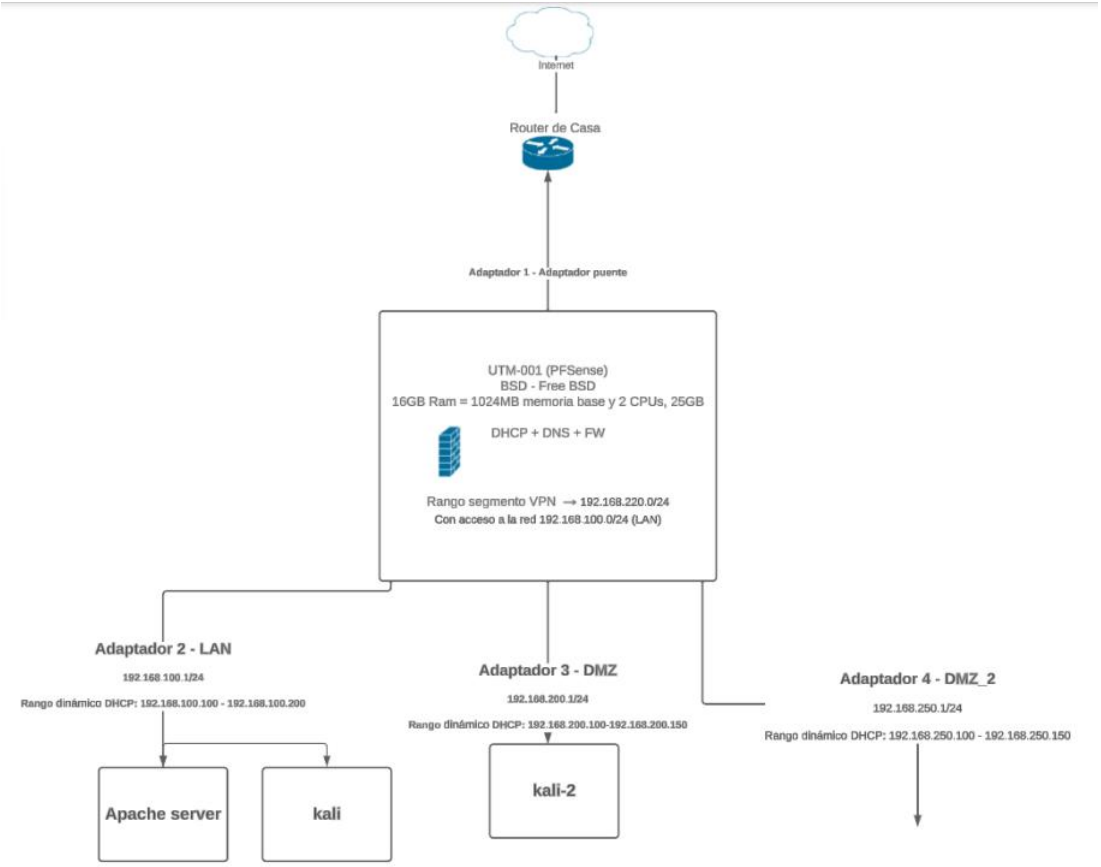
Enunciado

Queremos montar la siguiente infraestructura:



Los requisitos que debe cumplir son los siguientes:

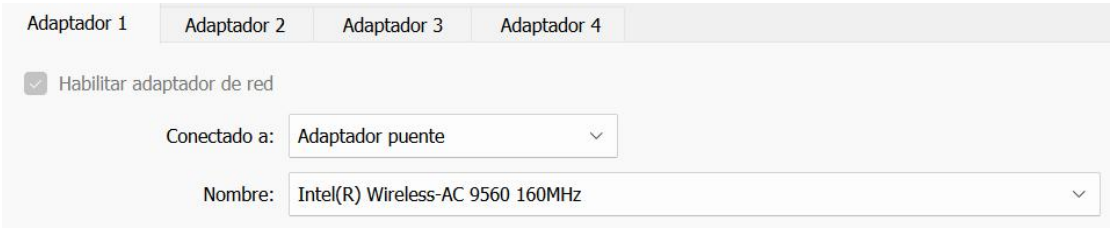
1. Debe tener un Pfsense en que se interconecten las redes LAN, DMZ y DMZ2
2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.
3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.
    1. Este honeypot no debe tener acceso a ninguna red interna (LAN, DMZ2…) y debe ser accesible desde el exterior (red WAN) en ambos sentidos.
4. En la red DMZ2 debe haber otra fuente diferente de logs a las dos mencionadas anteriormente. Se propone Suricata o Apache Server como posibles fuentes pero se deja a elección del alumno.
5. El servidor de Elastic debe recibir, almacenar y poder visualizar los logs del honeypot, el Windows 11 y la fuente elegida ubicada en la DMZ2.



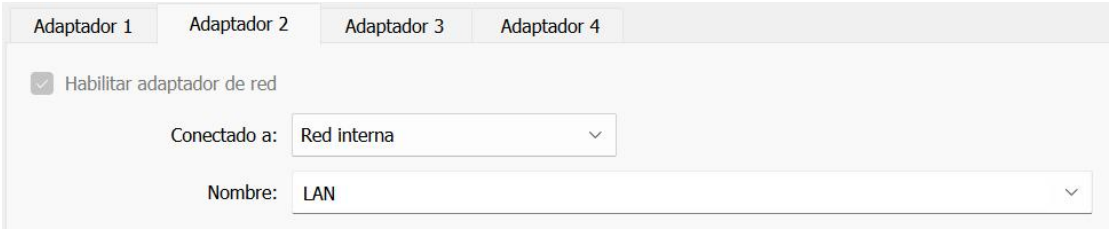
LO PRIMERO QUE VAMOS A HACER ES LA **CONFIGURACION DE LAS REDES DE NUESTRO PFSENSE**.

PARA ELLO, EN VIRTUAL BOX, VAMOS A LA CONFIGURACION DE NUESTRO UTM Y LO CONFIGURAMOS DE LA SIGUIENTE MANERA:

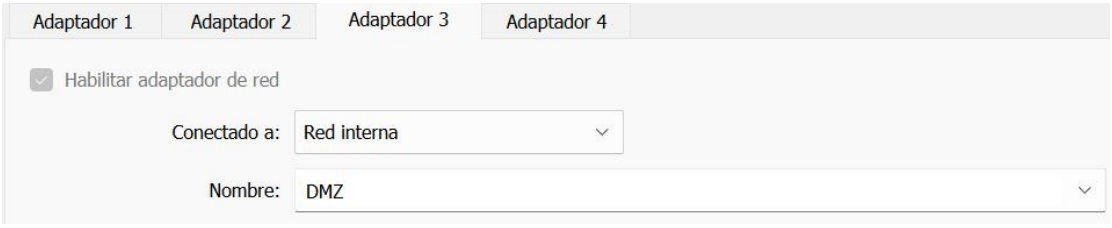
ADAPTADOR 1:



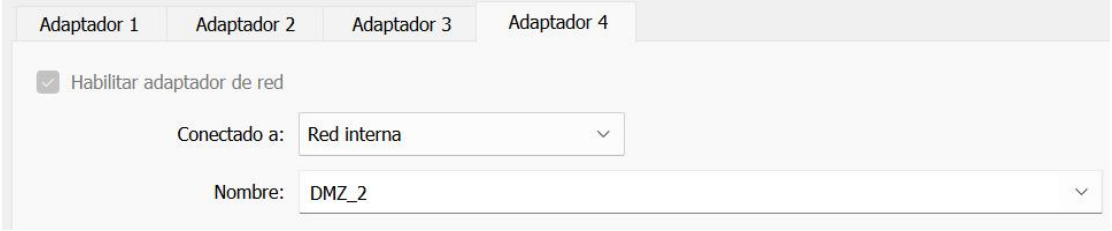
ADAPTADOR 2-LAN:



ADAPTADOR 3-DMZ:

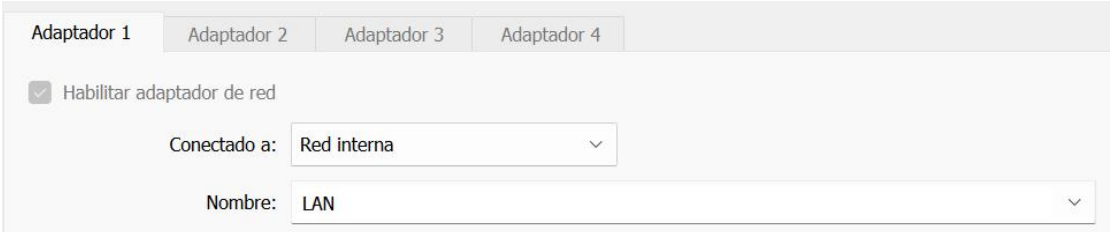


ADAPTADOR 4-DMZ_2:

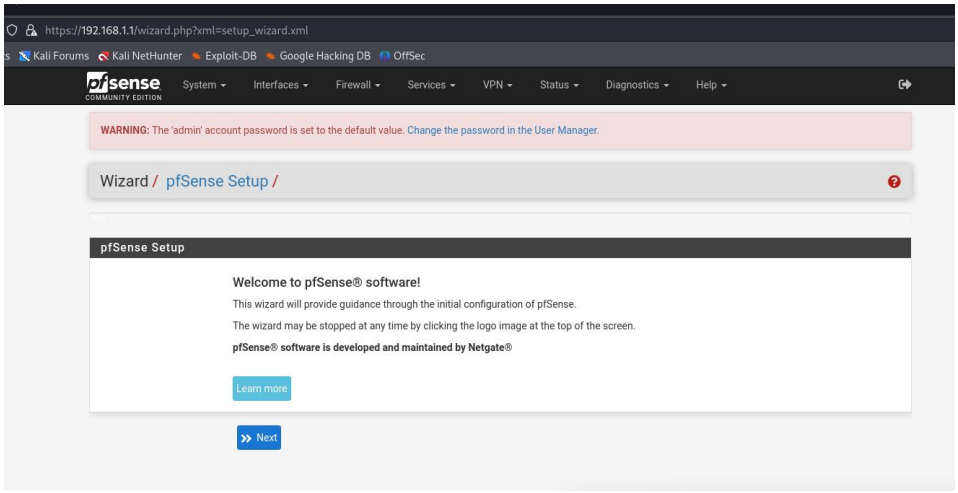


TAMBIEN CONFIGURAMOS LA RED DE NUESTRO KALI LINUX CONECTANDONOS A LA RED INTERNA CON LA LAN.

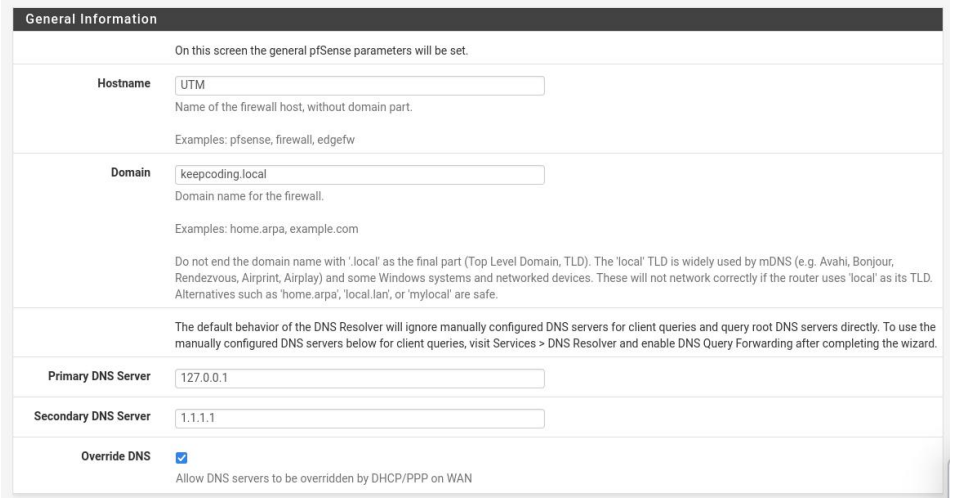
CONFIGURACIÓN DE LA RED DE KALI LINUX:



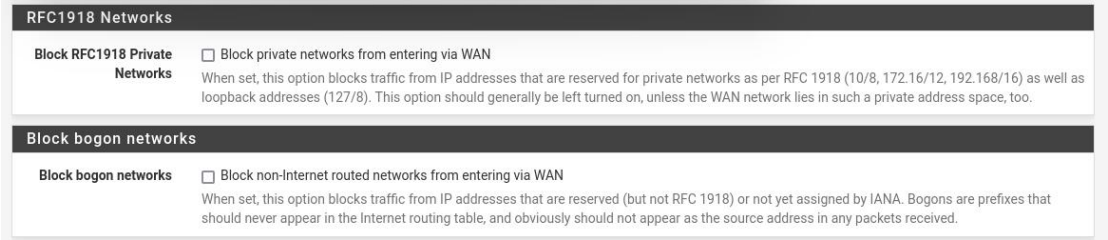
UNA VEZ YA TENEMOS LAS REDES CONFIGURADAS, YA PODEMOS ACCEDER A NUESTRO PFSENSE A TRAVES DE LA DIRECCIÓN IP: 192.168.1.1/24 DESDE EL NAVEGADOR DE NUESTRO KALI LINUX. NOS LOGEAMOS CON EL **NOMBRE**: admin. **CONTRASEÑA**: pfsense



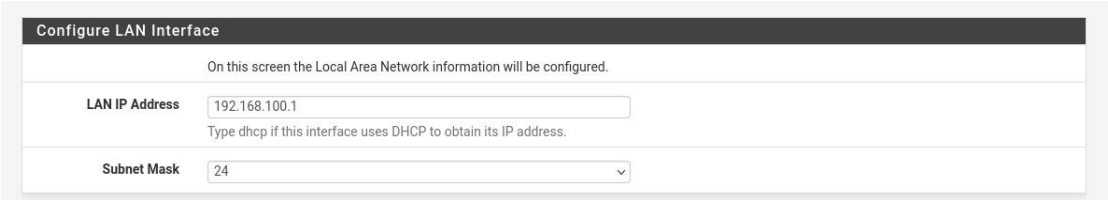
CAMBIAMOS EL **NOMBRE DEL HOST** POR UTM, EN EL **NOMBRE DE DOMINIO** keepcoding.local. EN **SERVIDOR DNS PRIMARIO**: 127.0.0.1 PARA QUE SEA EL PROPIO PFSENSE EL PRIMER SERVIDOR DNS. EN **SERVIDOR DNS SECUNDARIO**: 1.1.1.1. ESTE SERVIDOR DNS SON LOS SERVIDORES DE CLOUDFAIR.



AQUI EN **CONFIGURACION DE LA INTERFAZ WAN**: DHCP (QUE NOS COJA LA IP DE MANERA DINAMICA. EN **BLOCK BOGON NETWORKS** HABILITAMOS LOS BOGON Y LAS REDES PRIVADAS, PARA QUE NO NOS BLOQUEE LAS IPS INTERNAS QUE VAMOS A UTILIZAR.



DENTRO DE LA **CONFIGURACION DE LAN** VAMOS A CAMBIAR EL RANGO DE DIRECCIONES, AHORA MISMO LA DIRECCIONES QUE TENEMOS SON LAS DE IFCONFIG DE NUESTRO KALI LINUX Y LO QUE VAMOS A HACER ES MODIFICARLA Y QUE EN LUGAR DE SER ESTA LA PUERTA DE ENLACE 192.168.1.1 SEA 192.168.100.1 PARA QUE NO ENTRE EN CONFLICTO, POR SI ALGUIEN EN CASA TIENE IP INTERNA. Y EN **MASCARA DE SUBRED** 24



AHORA MISMO SI VAMOS AL UTM DEBERIAMOS VER SI LE DAMOS A INTRO QUE LA DIRECCION DE NUESTRA PUERTA DE ENLACE LAN HA CAMBIADO A LA NUEVA QUE HEMOS ESTABLECIDO

PARA PODER ACCEDER AL PFSENSE, TENEMOS QUE PONER LA NUEVA DIRECCION 192.168.100.1.

AHORA VAMOS A CONFIGURAR TODAS LAS INTERFACES, CONFIGURACION DEL SERVIDOR DHCP, CONFIGURACION DEL DNS

EN PRIMER LUGAR COMPROBAMOS SI TENEMOS ACCESO A INTERNET HACIENDO UN ping 1.1.1.1, Y VEMOS QUE SI RESPONDE.
AHORA VAMOS A HACER POR EJEMPLO ping mercadona.es Y NO RESPONDE, VAMOS A NUESTRO CMD DE WINDOWS Y VAMOS A VER CUAL ES LA IP DE mercadona.es HACEMOS ping mercadona.es Y NOS SALE 35.201.121.112

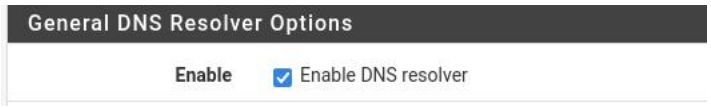
```
(base) C:\Users\Usuario>ping mercadona.es

Haciendo ping a mercadona.es [35.201.121.112] con 32 bytes de datos:
Respuesta desde 35.201.121.112: bytes=32 tiempo=6ms TTL=117
Respuesta desde 35.201.121.112: bytes=32 tiempo=12ms TTL=117
Respuesta desde 35.201.121.112: bytes=32 tiempo=13ms TTL=117
Respuesta desde 35.201.121.112: bytes=32 tiempo=7ms TTL=117

Estadísticas de ping para 35.201.121.112:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 6ms, Máximo = 13ms, Media = 9ms
```

POR LO TANTO, VEMOS QUE POR TEMA DE RESOLUCION DE DOMINIO NO LLEGAMOS, PERO PONIENDO LA IP EN NUESTRA KALI SI LLEGAMOS, POR LO TANTO VEMOS QUE TENEMOS UN PROBLEMA DE RESOLUCION DNS.

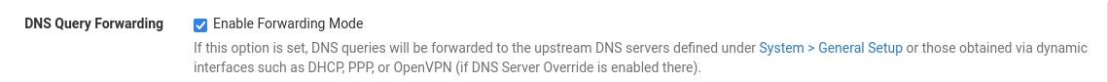
```
┌──(kali㉿kali)-[~]
└─$ ping mercadona.es
^C

┌──(kali㉿kali)-[~]
└─$ ping 35.201.121.112
PING 35.201.121.112 (35.201.121.112) 56(84) bytes of data.
64 bytes from 35.201.121.112: icmp_seq=1 ttl=116 time=7.68 ms
64 bytes from 35.201.121.112: icmp_seq=2 ttl=116 time=10.1 ms
64 bytes from 35.201.121.112: icmp_seq=3 ttl=116 time=7.99 ms
64 bytes from 35.201.121.112: icmp_seq=4 ttl=116 time=8.58 ms
64 bytes from 35.201.121.112: icmp_seq=5 ttl=116 time=6.28 ms
64 bytes from 35.201.121.112: icmp_seq=6 ttl=116 time=9.57 ms
^C
── 35.201.121.112 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 6.276/8.373/10.137/1.265 ms
```

VAMOS A CONFIGURAR EL UTM PARA QUE FUNCIONE DE MANERA CORRECTA

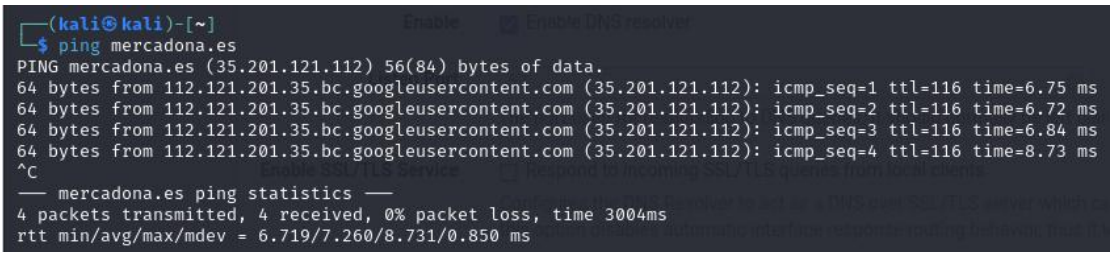
ENTRAMOS EN EL NAVEGADOR DONDE TENEMOS EL PFSENSE, LE DAMOS A SERVICE Y A DNS RESOLVERS, NOS VAMOS AL DNS, QUITAMOS EL DNSSEC (ES UN PROTOCOLO QUE SE UTILIZA PARA EL FIRMADO DE LAS RESPUESTAS DNS, CUANDO HACES UNA CONSULTA DNS LA CONSULTA PUEDE IR FIRMADA PARA QUE SE INDIQUE QUE NADIE TE LA HA MODIFICADO POR EL CAMINO(LA CONSULTA QUE TE DEVUELVA, TE LA ENVIE A TI Y PUEDES CONFIRMAR ESA FIRMA PARA VER QUE NO ES UN DNS FAKE)



Y AHORA HABILITAMOS EL DNS QUERY FORWARDING PARA QUE PUEDA REALIZAR LAS CONSULTAS DNS EN CASO DE QUE PFSENSE NO SEA CAPAZ POR SI MISMO, EN ESTE CASO LO QUE HARIA SERIA FOWARDEARLAS AL DNS SECUNDARIO QUE SERIA EL 1.1.1.1. DE CLOUDFAIR



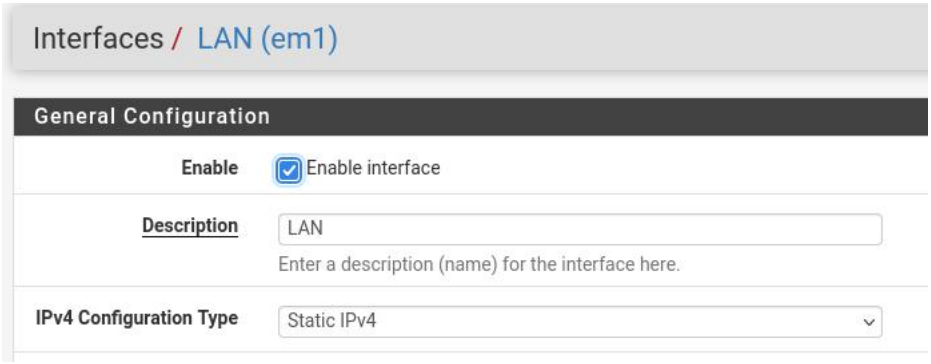
CON ESTO YA TENDRIAMOS LA CONFIGURACIÓN DNS. LANZAMOS OTRA VEZ EL PING A mercadona.es PARA COMPROBARLO.



SI ABRIMOS UN NAVEGADOR, YA NOS DEJA ACCEDER A mercadona.es

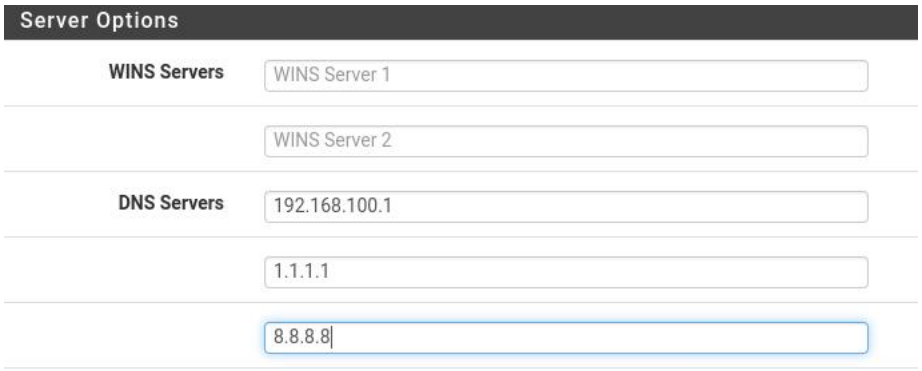
YA TENEMOS NUESTRO DNS FUNCIONANDO Y CONFIGURADO, AHORA QUEREMOS PONER UN RANGO DE DIRECCIONAMIENTO A CADA UNA DE LAS REDES, PARA ELLO NOS VAMOS A CONFIGURAR PARA QUE EL SERVIDOR DHCP DE NUESTRA RED NOS OTORGE ESE RANGO EN LAS MAQUINAS QUE TENEMOS EN ESA SUBRED

PARA ELLO, EN NUESTRA PAGINA DE PFSENSE, VAMOS A INTERFACES Y LE DAMOS A LAN, AQUI DEBERIAMOS TENER LA INTERFAZ HABILITADA Y EN STATIC IPV4.



AHORA NOS VAMOS A SERVICES Y VAMOS A DHCP SERVER, Y AQUI TIENE QUE ESTAR HABILITADA LA INTERFAZ LAN Y ABAJO TENEMOS EL RANGO DE IPs QUE EL DHCP SERVER ESTA CONCEDIENDO A TODOS LOS DIPOSITIVOS QUE SE CONECTAN A LA RED LAN. AHORA MISMO ESTAN DE 192.168.100.10 A 192.168.100.245. LO QUE VAMOS A HACER ES CAMBIARLA A 192.168.100.100 A 192.168.100.200 CON EL FIN DE CONSEGUIR LA SUBRED QUE TENEMOS DEFINIDO EN NUESTRO ESQUEMA DE RED.

EN SERVIDORES DNS PONEMOS EL PROPIO PFSENSE (HAY QUE TENER EN CUENTA QUE HAY QUE PONER LA IP DE PUERTA DE ENLACE, POR LA QUE VAMOS A ACCEDER A NUESTRA MAQUINA KALI, QUE SERÍA 192.168.100.1)
EN LA RED LAN Y COMO SERVIDORES DNS SECUNDARIOS PONEMOS EL 1.1.1.1 (CLOUDFAIR) Y EL 8.8.8.8 (GOOGLE), POR SI EL DNS NO FUESE CAPAZ DE HACER LA RESOLUCION DE NOMBRES.



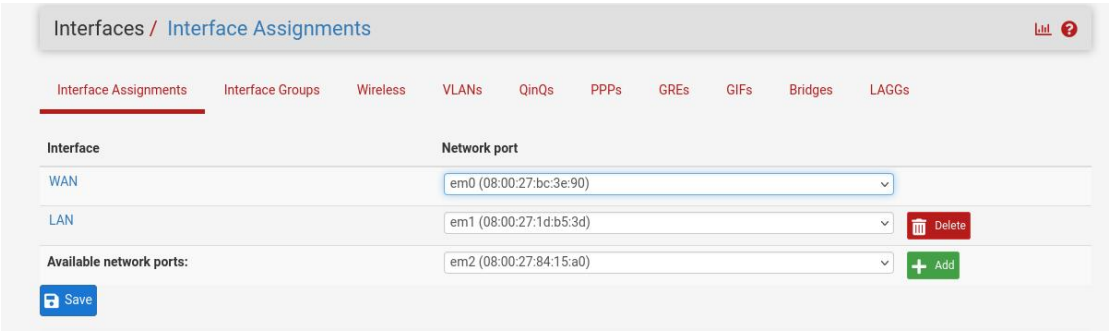
EN LA PUERTA DE ENLACE (GATEWAY), PONEMOS LA MISMA DIRECCIÓN, 192.168.100.1

AHORA EN NUESTRA KALI VEMOS NUESTRA IP CON ifconfig Y ES LA 100.10
VAMOS A DESCONECTARNOS Y CONECTARNOS DE LA RED, PARA QUE NOS ASIGNE UNA NUEVA DIRECCION IP DEL RANGO QUE HEMOS CONFIGURADO EN EL SERVIDOR DHCP, QUE SON LA 100.10.
HACEMOS ifocnfig PARA COMPROBAR.

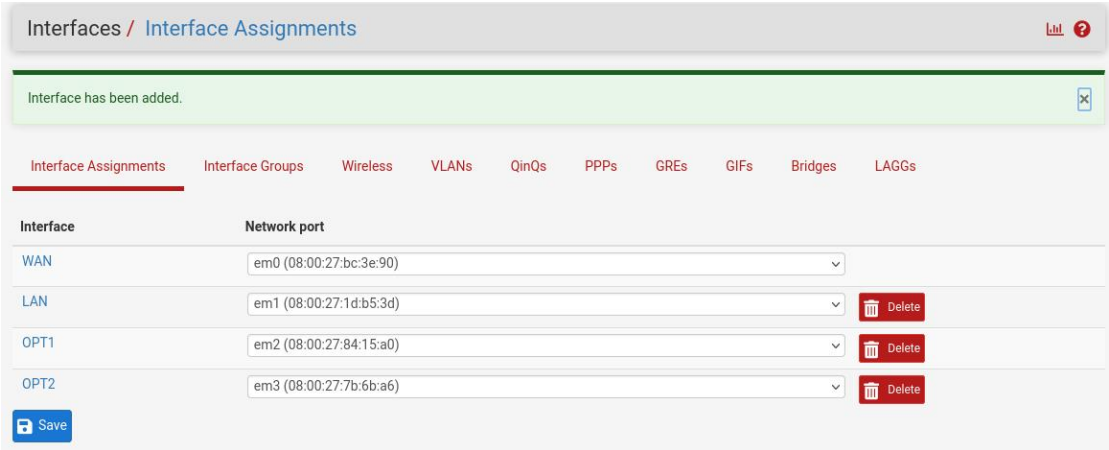
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.10  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::935c:3b70:121a:b502  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 49081  bytes 49165957 (46.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29023  bytes 16494238 (15.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 44464  bytes 4458650 (4.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44464  bytes 4458650 (4.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ifconfig
br-bf5bea264ab3: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:07:76:a6:76  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:bd:4a:1c:03  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.100  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::935c:3b70:121a:b502  prefixlen 64  scopeid 0x20<link>
```

YA TENEMOS DEFINIDA NUESTRA RED, YA TENEMOS EL DIRECCIONAMIENTO QUE QUEREMOS, YA HEMOS CUMPLIDO SIGUIENTE OBJETIVO QUE NUESRA MAQUINA KALI ESTE EN LA RED LAN, NOS FALTARIA **CONFIGURAR LAS DMZ Y DMZ2 DE NUESTRA RED**

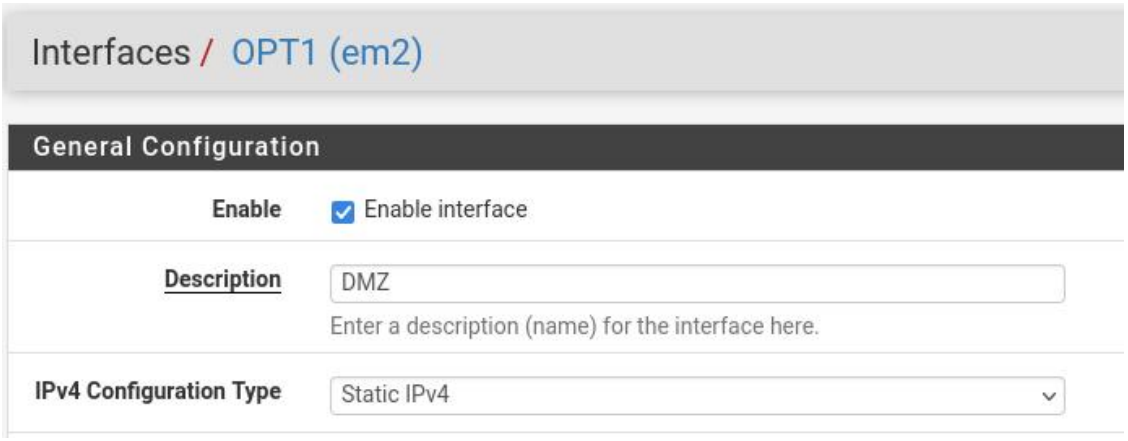
PARA ELLO, EN NUESTRO PFSENSE, NOS VAMOS A LAS INTERFACES ASSIGNMENTS Y AQUI VEMOS QUE PODEMOS AÑADIR MAS INTERFACES DE RED



ESTAS INTERFACES DE RED SON LAS QUE PODEMOS VER EN LA PROPIA MAQUINA DE UTM (SI VAMOS LA CONFIGURACION DE LA MAQUINA, A RED, DONDE DEFINIMOS LAS 4 INTERFACES DE RED, AHORA MISMO SOLO ESTAMOS UTILIZANDO LA 1 QUE SERIA LA INTERFAZ WAN Y LA 2 QUE SERIA LA LAN) ENTONCES VAMOS A AÑADIR LAS QUE NOS FALTAN, LAS DMZ, PARA ELLO LE DAMOS A AÑADIR 2 VECES Y NOS TIENEN QUE SALIR LA em2 Y LA em3

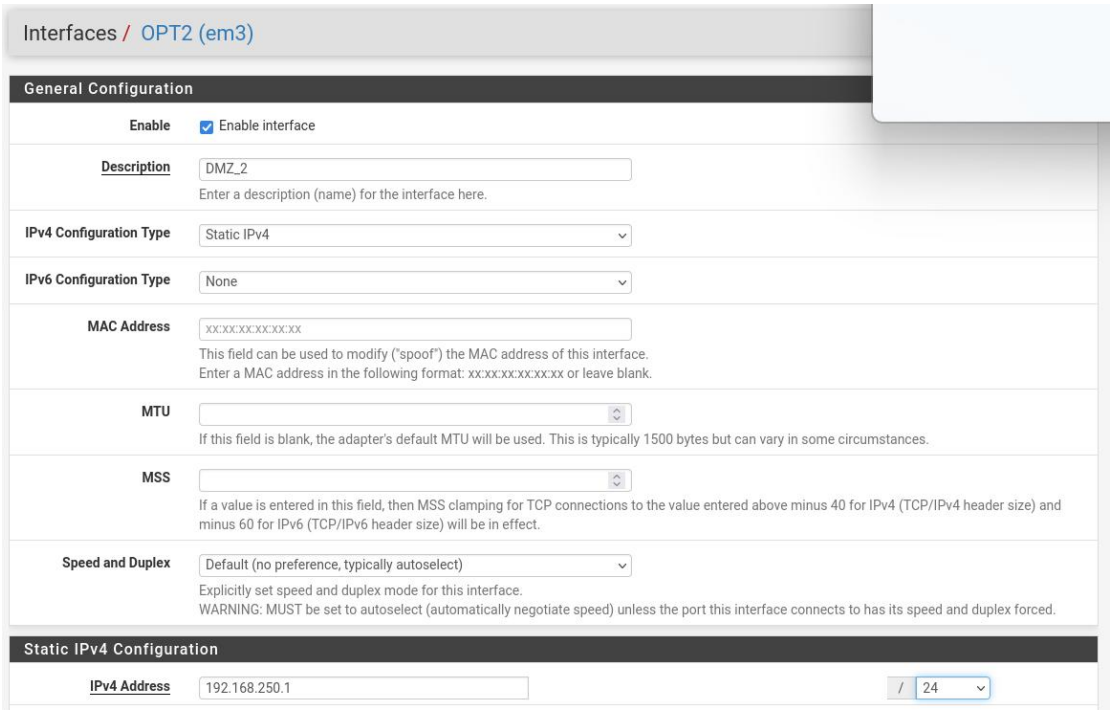


VEMOS QUE AHORA YA NOS APARECE OPT1 Y OPT2, **VAMOS A CONFIGURAR ESTAS INTERFACES DE RED.**
PARA ELLO NOS VAMOS, DENTRO DE INTERFACES, A OPT1 PARA CONFIGURARLA
LO PRIMERO ACTIVAMOS LA INTERFAZ, EN DESCRIPCION LE PONEMOS EL NOMBRE DMZ, EN IPV4 CONFIGURATION TYPE PONEMOS STATIC IPV4 (ESTA DIRECCIÓN ES LA QUE VEMOS EN LA MAQUINA DE LA UTM, ES LA DE LA PUERTA DE ENLACE, PARA QUE NO CAMBIE TIENE QUE SER ESTATICA PARA LAS MAQUINAS QUE HAY EN LA RED SEA SU DIRECCION DE SALIDA DEL ROUTER)

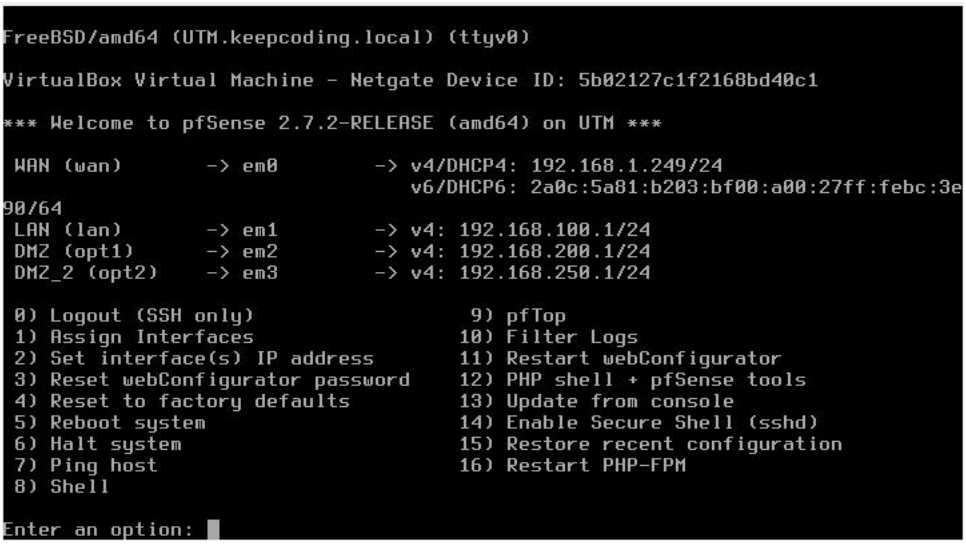


DESPUES, EN IPV4 ADRESS, PONEMOS LA DE LA PRACTICA 192.168.200.1/24 (ESTA SERIA LA PUERTA DE ENLACE)

AHORA VAMOS A OPT2, HACEMOS LO MISMO PERO CAMBIANDO EL NOMBRE A DMZ_2 Y EL RANGO 192.168.250.1/24



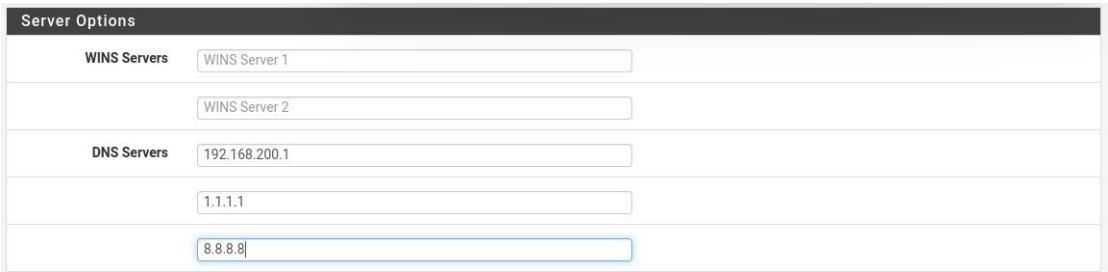
SI NOS VAMOS A LA MAQUINA DE UTM Y LE DAMOS A INTRO YA NOS APARECER NUESTRAS 4 INTERFACES BIEN DEFINIDAS CON LOS RANGOS QUE QUEREMOS.



VAMOS A HABILITAR EL SERVIDOR DHCP. PARA ELLO, EN DHCP SERVER.AQUI VAMOS A CONFIGURAR EL DIRECCIONAMIENTO QUE LE VAMOS A DAR A NUESTROS SEGMENTOS DE RED, QUE HEMOS DEFINIDO EN NUESTRO ESQUEMA, EN NUESTRO DMZ Y DMZ_2, JUNTO CON LA HABILITACION DEL SERVIDOR DHCP.

EN LA PARTE DE DMZ, LO HABILITAMOS Y PONEMOS EN EL RANGO DE DIRECCIONES DE LA 192.168.200.100 A LA 192.168.200.150

EN LOS SERVIDORES DNS PONEMOS, LA PUERTA DE ENLACE QUE SERÍA LA 192.168.200.1, Y COMO SERVIDOR SECUDARIO 1.1.1.1 Y COMO TERCER SERVIDOR 8.8.8.8



POR ULTIMO EN EL GATEWAY(PUERTA DE ENLACE) PONEMOS 192.168.200.1 (LA DEL PFSENSE

AHORA VAMOS A DMZ_2 Y HACEMOS LO MISMO, EL RANGO DE DIRECCIONES IP 192.168.250.100 A 192.168.250.150

EN LOS SERVIDORS DNS 192.168.250.1. LUEGO EL 1.1.1.1 Y EL 8.8.8.8.

EN LA GATEWAY 192.168.250.1

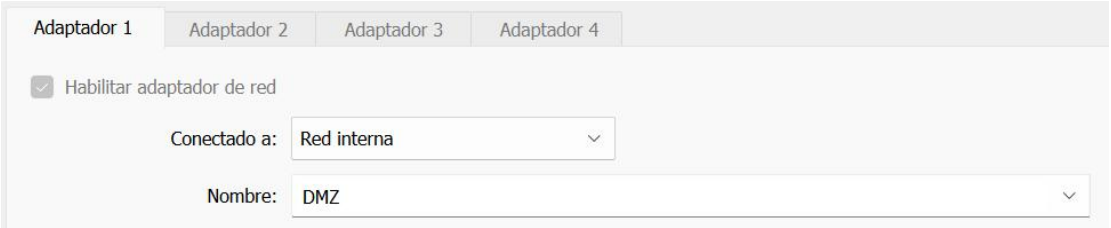
AHORA MISMO TENEMOS CONFIGURADO EL SERVIDOR DHCP Y EL DNS.
YA TENEMOS EN LOS ADAPTADORES LAM, DMZ Y DMZ_2 CONFIGURADOS EL RANGO DE IP Y EL SERVIDOR DHCP.
NOS FALTA CONFIGURAR:
-EN ADAPTADOR 3-DMZ **NO TENEMOS LA KALI 2**
-EN ADAPTADOR 4-DMZ_2 **NO TENEMOS NADA**
-EN ADAPTADOR 2-LAN **SOLO TENEMOS LA KALI**

YA HEMOS ASIGNADO A LAS INTERFACES DE RED DIFERENTES SEGMENTOS DE IP, AHORA VAMOS A COMPROBAR SI LO QUE HEMOS HECHO FUNCIONA.

PARA COMPROBAR QUE SI METEMOS ALGO EN KALI-2 (VER ESQUEMA), NOS DA UN RANGO DINAMICO DE DIRECCIONAMIENTO DE DHCP CORRESPONDIENTE A 192.168.200.100 A 192.168.200.150, LE TENDRIAMOS QUE CAMBIAR LA PUERTA DE ENTRADA AL KALI QUE TENEMOS.

SI AHORA COGEMOS LA KALI, Y EN VEZ DE CONECTARNOS A LA LAN, LA CONECTAMOS A LA DMZ, EL SEVIDOR DHCP NOS DEBERIA DAR AUTOMATICAMENTE UNA NUEVA IP.

PARA COMPROBAR QUE FUNCIONA, NOS VAMOS A LA KALI, CONFIGURACION Y HACEMOS UN CAMBIO DE RED (EN EL ADAPTADOR 1, DONDE ESTÁ LA LAN, PONEMOS DMZ.



SI AHORA HACEMOS UN ifconfig DEBERIAMOS VER QUE NOS DA UNA IP QUE ESTÁ DENTRO DEL RANGO DE LAS DIRECCIONES DE DMZ QUE HEMOS DEFINIDO.

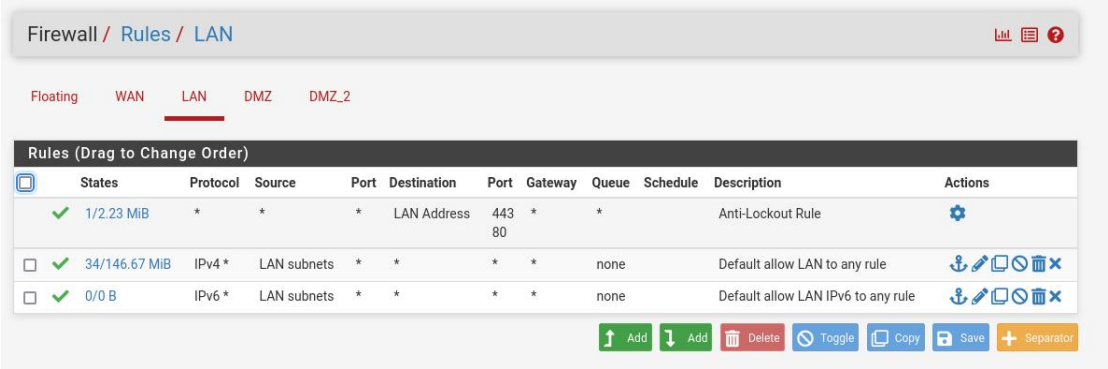
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.200.100  netmask 255.255.255.0  broadcast 192.168.200.255
        inet6 fe80::935c:3b70:121a:b502  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 107550  bytes 112306877 (107.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 65406  bytes 39000328 (37.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

COMPROBAMOS QUE SI ENTRAMOS EN DMZ_2 NOS VUELVE A CAMBIAR LA IP.

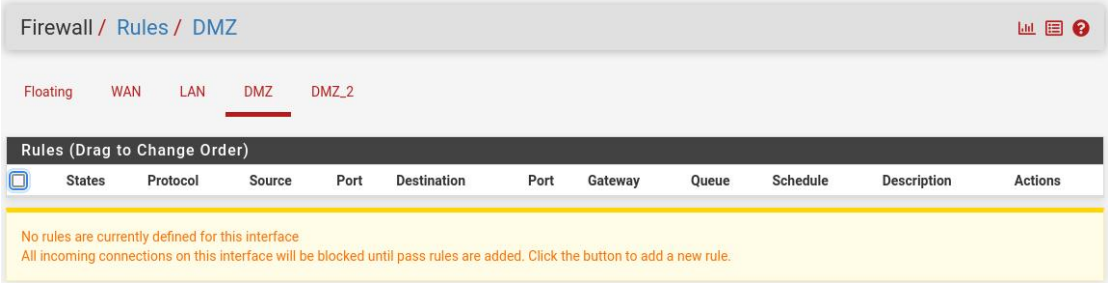
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.250.100  netmask 255.255.255.0  broadcast 192.168.250.255
        inet6 fe80::935c:3b70:121a:b502  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 107562  bytes 112308445 (107.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 66155  bytes 39080573 (37.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

YA TENEMOS CONFIGURADAS LAS REDES Y HEMOS COMPROBADO QUE FUNCIONA.

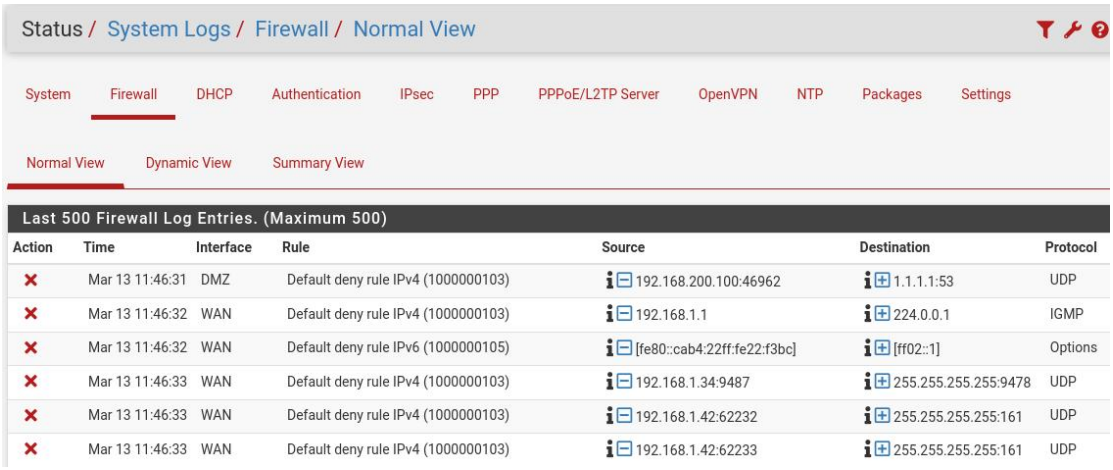
AHORA VAMOS A VOLVER A LA DMZ EN LA RED DE KALI, Y CON ESTAS CONFIGURACIONES VEMOS QUE NO TENEMOS ACCESO A ping NI A INTERNET.
NOS CAMBIAMOS A LA RED LAN PARA PODER ACCEDER TODOS BIEN AL PFSENSE Y PODER VER UN POCO LO QUE NOS ESTA PASANDO AHORA MISMO. UNA VEZ EN PFSENSE, SI NOS VAMOS A FIREWALL Y NOS VAMOS A RULES, VEMOS EN LA LAN POR DEFECTO TENEMOS REGLAS CONFIGURADAS



PERO EN EL RESTO DE DMZ NO TENEMOS NADA.



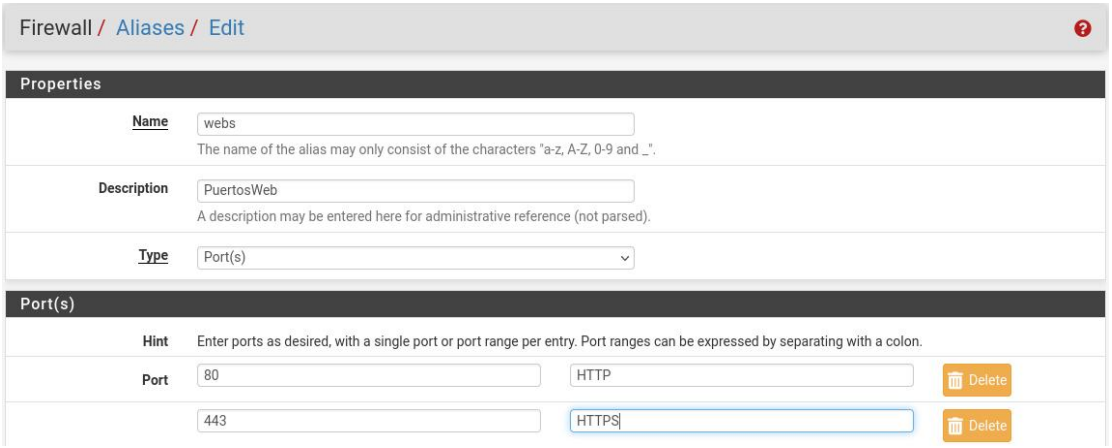
LOS FIREWALLS POR DEFECTO RECHAZAN AUTOMATICAMENTE TODO EL TRAFICO, ENTONCES AL CAMBIARNOS DE RED, SI VAMOS A STATUS, Y LE DAMOS A LOGS DE SISTEMAS Y NOS VAMOS A LOS LOGS DE LOS FIREWALLS VEMOS TODAS LAS PETICIONES DNS QUE HEMOS HECHO ESTÁN BLOQUEADAS.



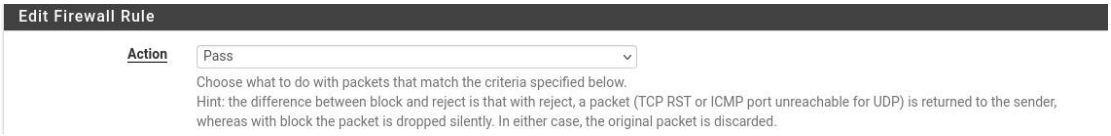
CONFIGURACION DE LOS FIREWALL:

AHORA VAMOS A HACER LA CONFIGURACION DEL FIREWALL, PARA ESO ENTRAMOS EN FIREWALL Y LE DAMOS A RULES. Y ENTRAMOS A DMZ.
PARA NAVEGAR A INTERNET NECESITAMOS HABILITAR EL PROTOCOLO HTTP, PUERTO 4430,80,53 DE DNS PARA QUE SE LLEVE A CABO LA RESOLUCION DE NOMBRE.

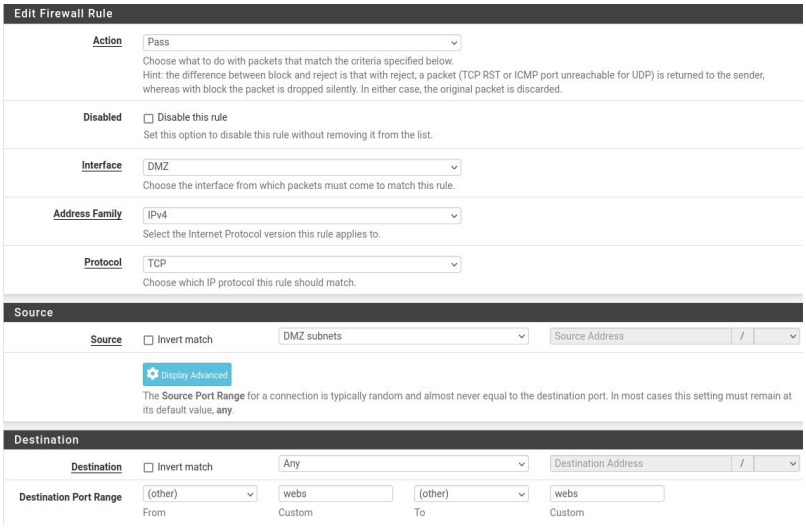
VAMOS A CREAR LAS REGLAS DE LOS FIREWALL, PARA ELLO VAMOS A ENTRAR DENTRO DE FIREWALL, EN ALIASES, Y EN PUERTOS. AQUI VAMOS A PONER EL PUERTO 80 Y EL 443.
ESTO LO HACEMOS PARA CUANDO PONGAMOS EN UNA REGLA DE FIREWALL QUERAMOS HABILITAR EL TRÁFICO HACIA LA WEB, PONIENDO PUERTOS WEB NOS COGE TODO.
NO PONEMOS EL PUERTO DNS PORQUE UTILIZA LO QUE SE DENOMINA **UDP** (CONEXION NO ORIENTADA) Y HTTP Y HTTPS UTILIZA **TCP** (EN TCP SON LAS TRAMAS LO QUE SE TRATA ES QUE NO SE PIERDA NINGUN TIPO DE PAQUETE CUANDO SE ESTABLECE LA CONEXION)



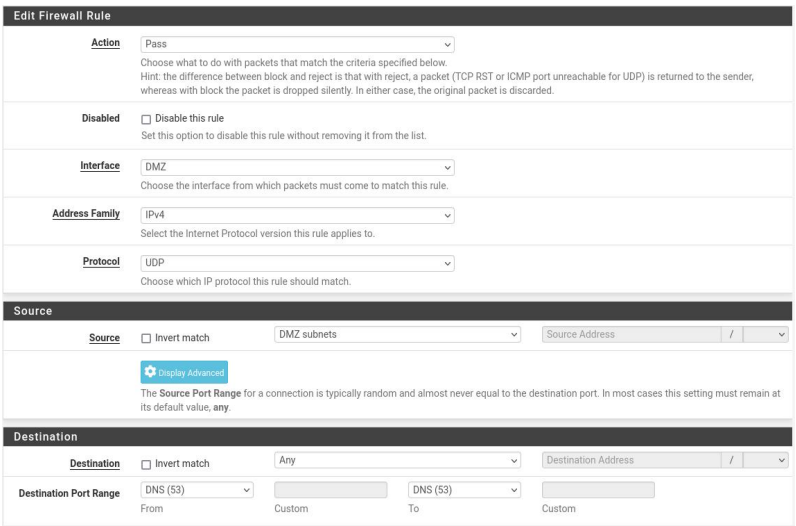
AHORA NOS VAMOS A CREAR LAS REGLAS EN LOS FIREWALLS, NOS METEMOS EN FIREWALL, RULES. Y NOS METEMOS EN DMZ, AÑADIMOS LAS REGLAS.
EN ACTION PONEMOS EN PASS(PORQUE ESTAMOS CREANDO UNA REGLA PARA PERMITIR EL TRAFICO)



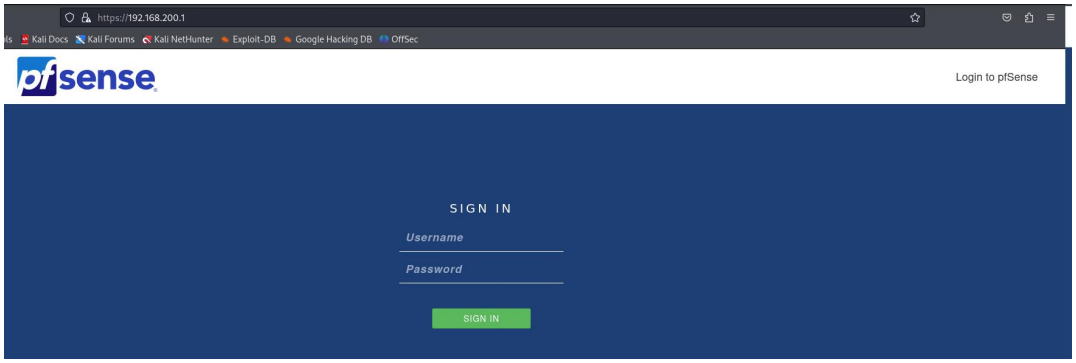
EN INTERFACE PONEMOS DMZ, EN ADRESS FAMILY PONEMOS IPV4, EN PROTOCOL PONEMOS TCP, PARA HACERLO MAS SEGURO, EN SOURCE MARCAMOS DMZ_subnets, EN DESTINATION PONEMOS from (others) EN CUSTOM webs, Y EN TO (other) Y EN CUSTOM webs.(hace referencia a los puertos que hemos definido antes en el alias puerto 443 y 80). EN LA DESCRIPCION PODEMOS PONER Salida tráfico web.
ASI QUEDARÍA NUESTRA CONFIGURACIÓN:



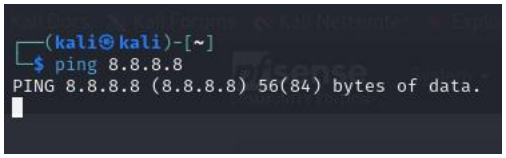
AHORA AÑADIMOS LA REGLA QUE NOS FALTA, QUE SERÍA LA DEL PROTOCOLO DNS, LA DE UDP. NOS METEMOS EN FIREWALL, RULES. Y NOS METEMOS EN DMZ, AÑADIMOS LAS REGLAS.
CAMBIAMOS EL PROTOCOLO PONEMOS udp EN DESTINATIONS PONEMOS from DNS (53) A to DNS (53) Y EN LA DESCRIPTION PONEMOS permitir trafico DNS.



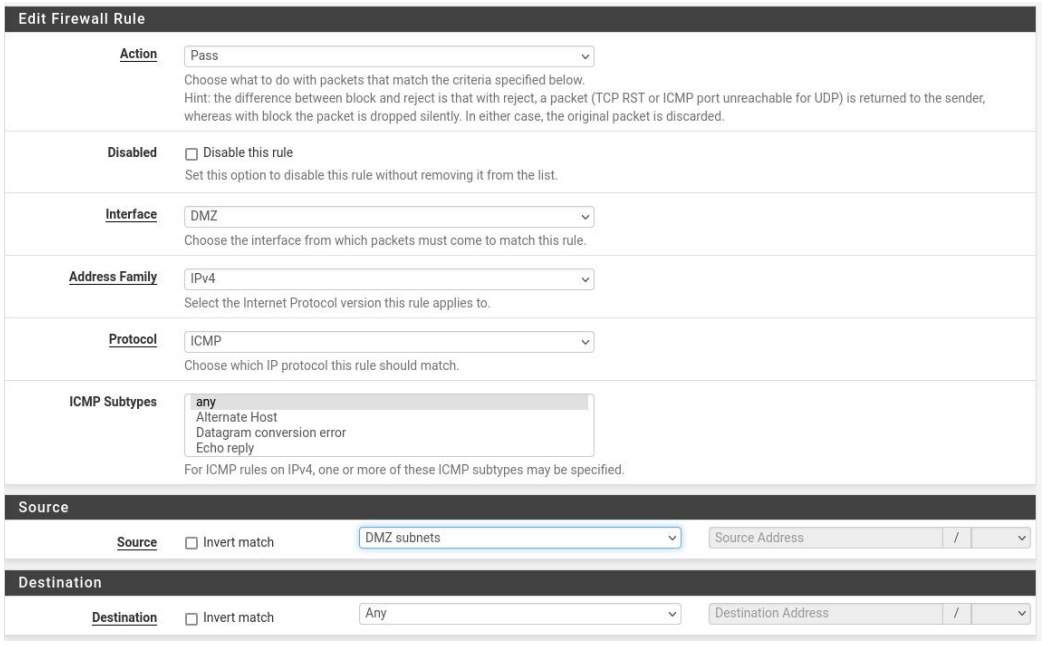
AHORA VAMOS A VER SI LOS CAMBIOS HAN FUNCIONADO, CAMBIAMOS LA MAQUINA DE RED A LA DMZ PARA QUE NOS ASIGNE LA NUEVA IP. AHORA VAMOS A LA CONSOLA Y PONEMOS ip a. NOS METEMOS EN EL NAVEGADOR Y VEMOS QUE FUNCIONA, YA TENEMOS ACCESO. Y SI QUEREMOS ACCEDER AL PFSENSE (192.168.200.1) TAMBIEN TENEMOS ACCESO A LA PAGINA DEL PFSENSE.



AHORA QUE ESTAMOS DENTRO DE LA RED, VAMOS A VER EN LA CONSOLA Y NOS GUSTARIA SABER SI LOS SERVIDORES DE GOOGLE ESTAN BIEN. HACEMOS ping 8.8.8.8 Y VEMOS QUE NO FUNCIONA, PORQUE EL PING NO VA NI POR TCP, NI POR UDP, VA POR LO QUE SE LLAMA ICMP.



PARA QUE NOS FUNCIONE EL PING DEBERIAMOS AÑADIR OTRA REGLA DE PERMITIDO EN LA DMZ DESDE EL PROTOCOLO ICMP. EN ORIGN PONEMOS DESDE LS dmz subnets Y EN DESTINO LO DEJAMOS EN any.

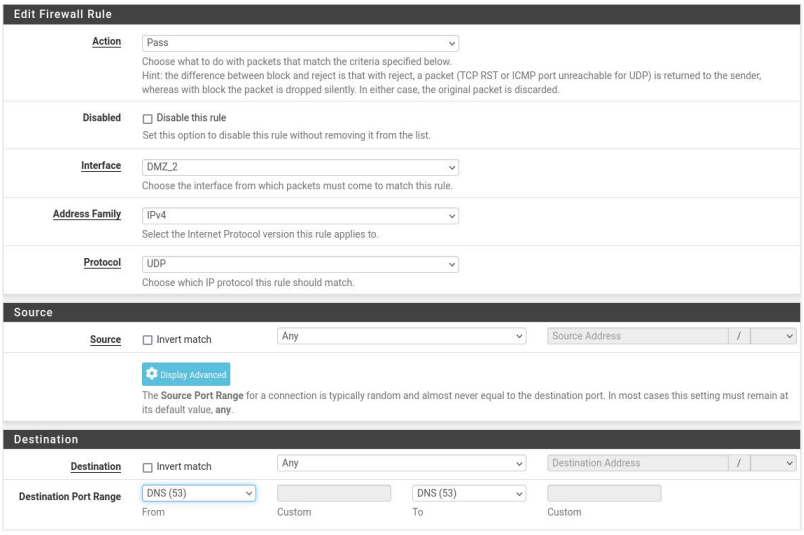


AHORA SI HACEMOS PING, YA NOS RESPONDE

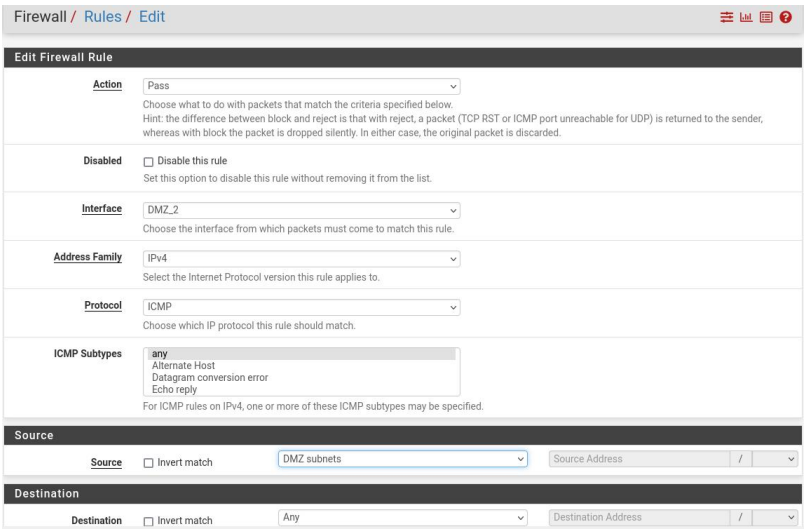
```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=16.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=8.14 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=8.50 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=9.92 ms
^C
── 8.8.8.8 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
```

YA TENEMOS CONFIGURADA LA DMZ, TENEMOS CONFIGURADO YA LA LAN CORRECTAMENTE, NOS FALTARIA CONFIGURAR LA DMZ_2.
PARA ELLO VOLVEMOS A LAS REGLAS DE FIREWALL Y AÑADIMOS UNA NUEVA REGLA CON EL PROTOCOLO: TCP, ORIGEN DMZ_2 subnets, DESTINO: ANY (destination port range: other, custom: webs, to: other, custom: webs).

AHORA AÑADIMOS UNA NUEVA REGLA CON EL PROTOCOL: UDP, ORIGEN: ANY, DESTINO: PORT RANGE: from DNS(53) to DNS (53).



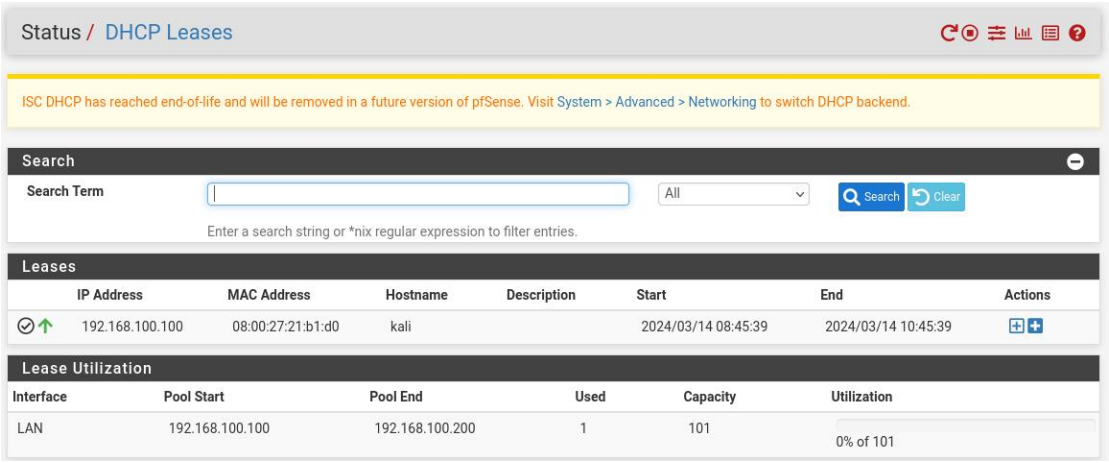
Y POR ULTIMO AÑADIMOS OTRO PARA EL PROTOCOLO ICMP, PROTOCOLO: ICMP, ORIGEN: DMZ_2 subnets Y DESTINO: any



YA HAN QUEDADO MAS O MENOS CONFIGURADAS TODAS LAS INTERFACES.

EL SIGUIENTE APARTADO QUE QUEREMOS CONSEGUIR ES EL KALI

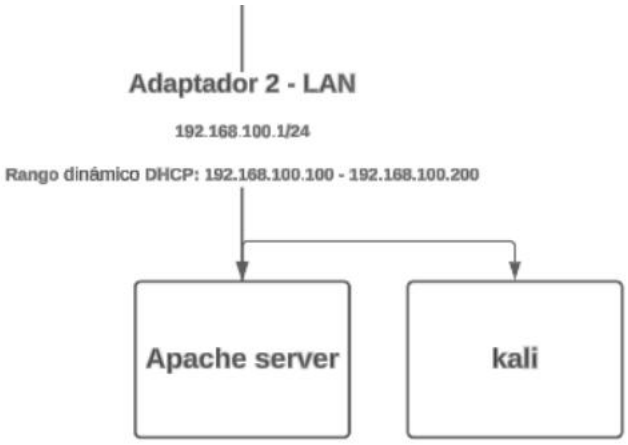
EL APACHE ES UN SERVIDOR QUE VAMOS A TENER DENTRO DE NUESTRA RED, ASI QUE NOS INTERESA QUE SIEMPRE ESTE DENTRO DE LA MISMA IP. SI CAMBIAMOS CONSTANTEMENTE EL SERVDIOR DE IP, AL FINAL NO HAY MANERA DE ENCONTRARLO, POR LO QUE SE SUELEN ASIGNAR IPs FIJAS A ESTE TIPO DE MAQUINAS.
PARA ELLO NOS VAMOS A CONECTAR A LA RED LAN, TENEMOS QUE IR AL PFSENSE, A STATUS-DHCP leases, LE DAMOS A LEAVE, Y AQUI VEMOS LAS MAQUINAS QUE TENEMOS CONECTADAS Y CON IP DENTRO DE NUESTRO PFSENSE, VEMOS LA MAC DE NUESTRA KALI Y LA IP. ESTA IP ESTA ASGINADA DE MANERA DINÁMICA POR NUESTRO SERVIDOR DE DHCP.



PUEDE SER UTIL PARA ADEMAS DE ESTABLECER DIRECCIONES IP FIJAS, TAMBIEN ESTABLECER UN MATCH ENTRE UNA DIRECCION MAC Y UNA IP PARA AÑADIR UNA CAPA EXTRA DE SEGURIDAD.

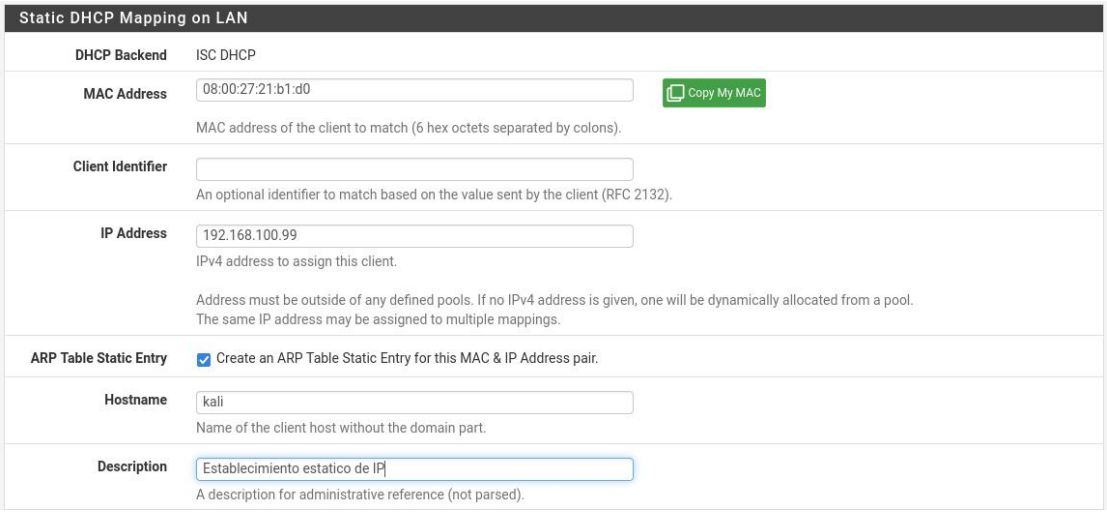
PODEMOS, POR EJEMPLO, CONFIGURAR QUE PARA NUESTRA MAC, ESTA DIRECCION IP ES FIJA, ES LO QUE SE CONOCE COMO UN FILTRO MAC.

AHORA VAMOS A AÑADIR UN MAPEO ESTATICO DE LA DIRECCION DE NUESTRA KALI, PARA QUE NUESTRO SERVIDOR APACHE NO CAMBIE.
PARA ELLO LE DAMOS AL **+ (EL DE FONDO BLANCO**) Y AQUI NOS SALE LA MAC DE NUESTRO SERVIDOR Y LA IP FIJA QUE QUEREMOS AÑADIRLE, EN NUESTRO CASO LE AÑADIMOS LA IP FIJA QUE PERTENEZCA A NUESTRA SUBRED.
LO QUE VAMOS A HACER ES DARLE UNA IP QUE NO ENTRE EN ESE RANGO DINAMICO QUE VEMOS EN LA IMAGEN



PARA QUE NO ENTRE EN CONFLICTO CON EL SERVIDOR DHCP, POR EJEMPLO 192.168.100.99 (QUE ESTA FUERA DEL RANGO DE DHCP PERO ESTA DENTRO DEL RANGO DE NUESTRA RED DMZ)

LE DAMOS A ARP Table Static Entry (LO ACTIVAMOS, RUTA ESTATICA DE NUESTRA TABLA DE ARP, PARA QUE NOS ASOCIE PARA SIEMPRE ESA MAC A ESA IP), PODEMOS PONER UNA DESCRIPCION SI QUEREMOS PARA TENER UNA REFERENCIA Establecimiento estatico de IP



DESCONECTAMOS Y CONECTAMOS Y HACEMOS UN ip a Y VEMOS LA 100.99 COMO DIRECCION ASIGNADA EN eth0.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.99/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
       valid_lft 7176sec preferred_lft 7176sec
    inet6 fe80::935c:3b70:121a:b502/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

APACHE:

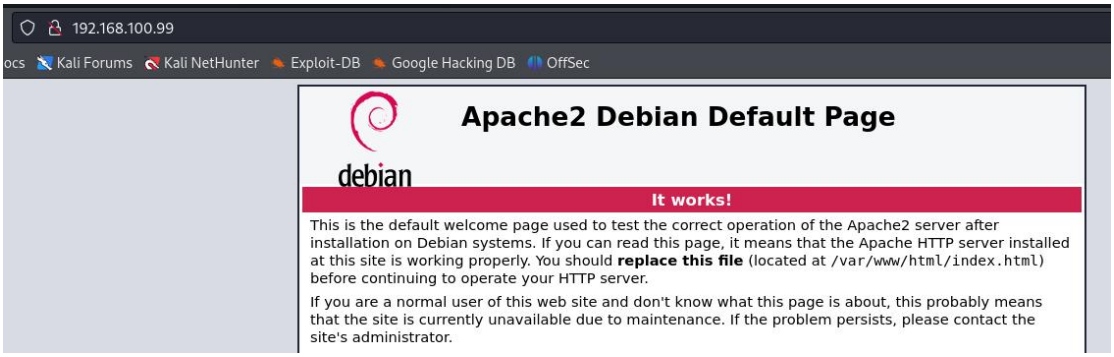
AHORA POR ULTIMO VAMOS A LEVANTAR NUESTO SERVIDOR DE APACHE, PARA ELLO HACEMOS UN sudo service apache2 start

```
┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start
[sudo] password for kali:
```

SI AHORA HACEMOS UN sudo service apache2 status DEBERIAMOS VER QUE ESTA CORRIENDO.

```
┌──(kali㉿kali)-[~]
└─$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Thu 2024-03-14 04:57:28 EDT; 23s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 400875 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 400891 (apache2)
      Tasks: 6 (limit: 6312)
     Memory: 19.8M (peak: 20.3M)
        CPU: 190ms
     CGroup: /system.slice/apache2.service
             ├─400891 /usr/sbin/apache2 -k start
             ├─400894 /usr/sbin/apache2 -k start
             ├─400895 /usr/sbin/apache2 -k start
             ├─400896 /usr/sbin/apache2 -k start
             ├─400897 /usr/sbin/apache2 -k start
             └─400898 /usr/sbin/apache2 -k start

Mar 14 04:57:28 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
```

SI EN EL NAVEGADOR PONEMOS LA IP 192.168.100.99 DEBERIAMOS VER QUE ESTA CORRIENDO EL SERVIDOR DE APACHE EN LA IP QUE LE HEMOS ASIGNADO.



VEMOS QUE YA FUNCIONA NUESTRO SERVIDOR A NIVEL LOCAL, PERO SI ALGUIEN QUIERE ACCEDER DESDE FUERA NO PUEDE.

LO PROXIMO QUE VAMOS A HACER ES CONFIGURAR TODO LO NECESARIO PARA QUE UN DISPOSITIVO QUE SE ENCUENTRE EN NUESTRA RED DE CASA, PERO NO ESTE DENTRO DE LA LAN, PUEDA ACCEDER A ESE SERVIDOR WEB.

A PARTE VAMOS A CONFIGURAR UNA RED VPN PARA QUE PODAMOS ACCEDER A ESE SERVIDOR WEB DESDE UN TERMINAL MOVIL UTILIZANDO POR EJEMPLO LOS DATOS.

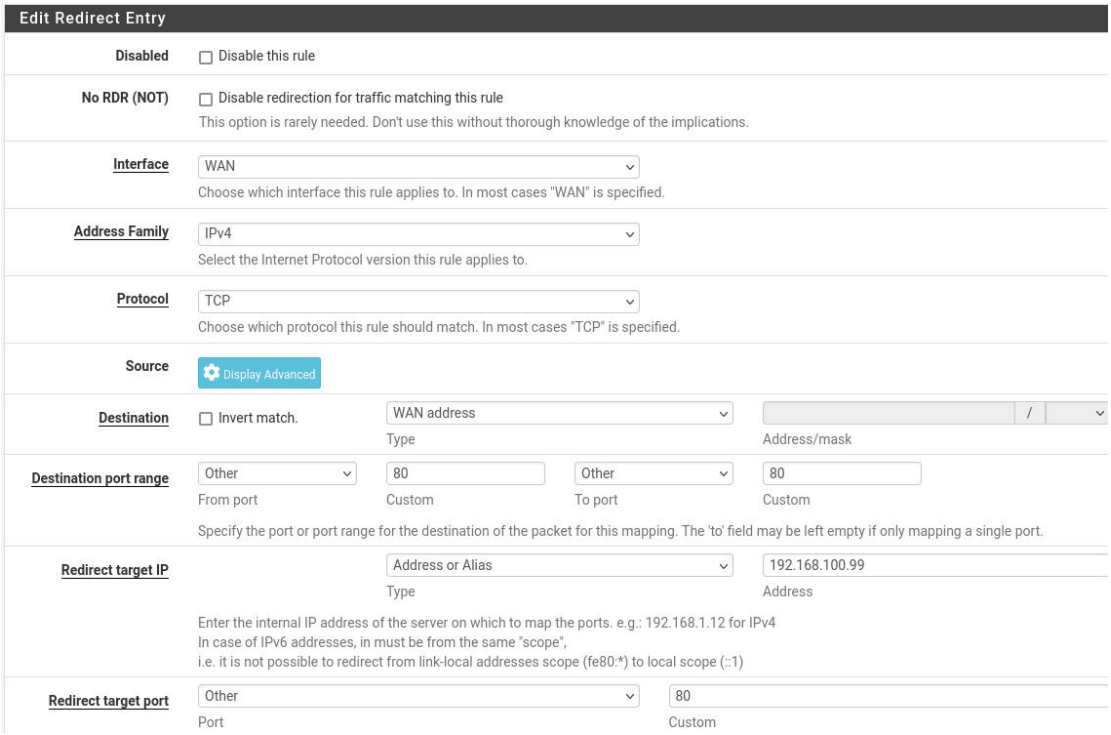
TENEMOS UNA IP FIJA EN LA KALI Y SERVIDOR APACHE (LO TRATAMOS COMO UNA UNICA MAQUINA, VER ESQUEMA), TENEMOS LA KALI ASIGNADA CON UNA IP FIJA QUE ES LA 192.168.100.99, Y SI NOS VAMOS A NUESTRA KALI, PONIENDO ESA IP DEBERIAMOS ACCEDER A NUESTRO PORTAL DEL APACHE.

VAMOS A HACER UNA CONFIGURACIÓN PARA QUE LOS QUE ESTÉN DENTRO DE LA LAN PUEDAN ACCEDER AL SERVIDOR, Y GENTE QUE ESTÉ DETRAS DE NUESTRO UTM TAMBIÉN PUEDAN ACCEDER.

AHORA VAMOS A CONECTARNOS DESDE NUESTRO ORDENADOR.
TENEMOS QUE HACERLE LA PETICION A LA WAN DEL PFSENSE, QUE ES LA QUE TIENE CONTACNO CON EL ROUTER DE NUESTRA CASA, LA PETICION VA A IR AL ROUTER DE NUESTRA CASA Y DE AHI VA A IR AL PFSENSE (LA VA A DERIVAR).

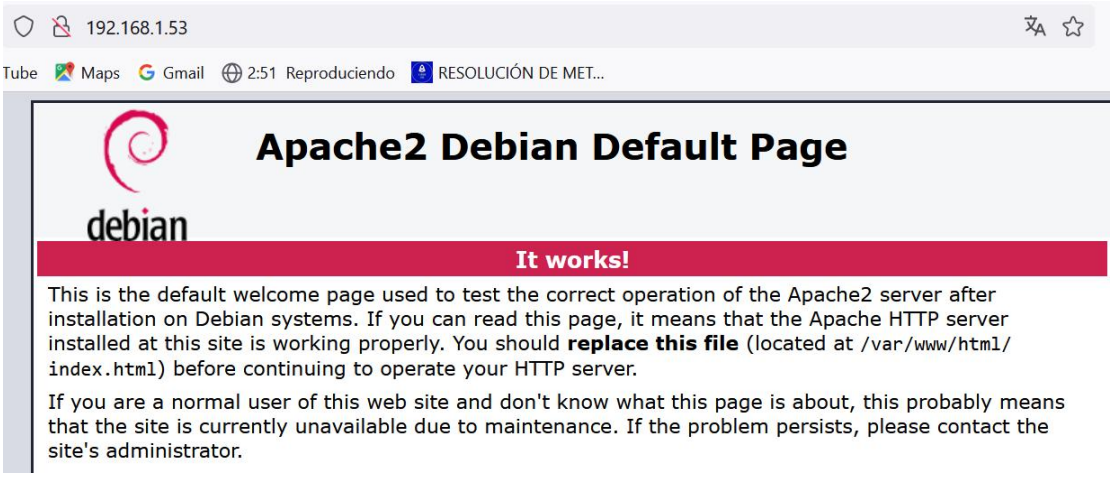
SI PONEMOS LA DIRECCION DE LA WAN EN EL NAVEGADOR, 192.168.1.133, NO NOS LLEGA A LA KALI. ESTO ES PORQUE NO HEMOS CREADO UN TUNEL O UN PASO ENTRE LA WAN DEL PFSENSE Y LA LAN DEL PFSENSE.
AHORA MISMO SOLO TENEMOS REGLAS DE FIREWALL PARA ENTRADA Y SALIDA DE TRAFICO POR EL PUERTO 53, 80 Y 443. COMO NO ESTAMOS HACIENDO PETICIONES Y ESTAMOS YENDO SOLO A UNA UNICA IP EL PFSENSE NO ES CAPAZ DE HACER NADA CON ESO PORQUE LA IP A LA QUE ESTAMOS DIRIGIENDONOS ES HACIA LA WAN DEL PFSENSE.
TENEMOS QUE CREAR UNA REDIRECCION PARA QUE EL TRAFICO QUE ESTAMOS ENVIANDO A LA WAN DEL PFSENSE NOS LO ENCAPSULE Y NOS LO MANDE HACIA LA LAN, LO REDIRIDIJA (LO QUE SERIA UN NATEO).

LO QUE VAMOS A HACER EN PFSENSE ES CREAR UNA REGLA PARA DECIRLE QUE TODO EL TRAFICO QUE NOS LLEGUE AL PUERTO 80 DE NUESTRA INTEFAZ WAN, NOS LO REENVIE HACIA NUESTRA LAN. ENTONCES VAMOS A IR A firewalls-nat Y AÑADIMOS UNA REGLA.
AQUI EN INTERFACE: WAN, PROTOCOLO: TCP, DESTINO: wan address y DESTINATION PORTcustom 80, custom 80, REDIRECCION DE IP: address or alias 192.168.100.99 (NUESTRA KALI), EN REDIRECT TARGET PORT: other, custom: 80 (PARA CREAR LA REDIRECCION), DESCRIPTION: Regla apache server



LO QUE ESTAMOS DICIENDO ES QUE EL TRAFICO QUE ENTRE HACIA LA WAN CON DIRECCION DE LA WAN NOS LO REDIRECCIONE (NATEO) HACIA LA IP DE LA KALI QUE TENEMOS EN NUESTRA LAN Y AL PUERTO WEB DE LA KALI (PUERTO 80, DONDE ESTA NUESTRO SERVIDOR DE APACHE).

SI AHORA NOS VAMOS A NUESTRA MAQUINA HOST Y BUSCAMOS LA IP DE NUESTRA WAN (192.168.1.53), YA ACCEDE A NUESTRO APACHE.



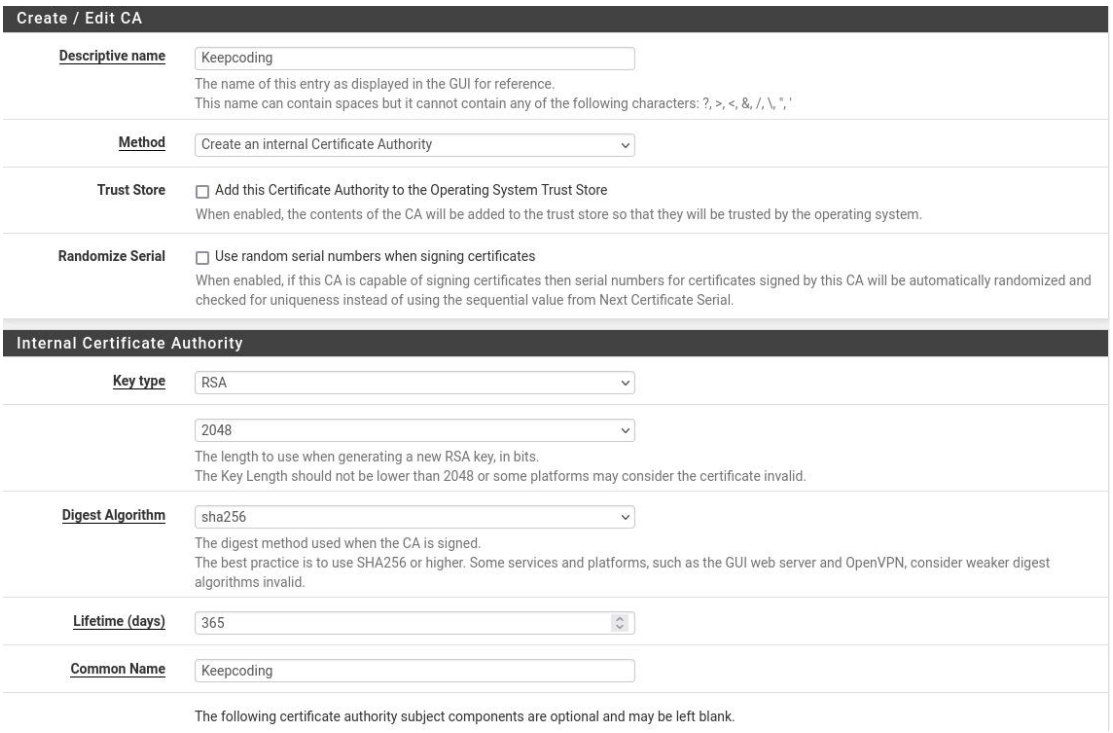
YA TENEMOS ACCESO, YA PODEMOS SERVIR NUESTRA APLICACION WEB AL RESTO DE LA EMPRESA.

CREACION Y CONFIGURACION DE LA VPN:

PARA ELLO TENEMOS QUE INSTALAR UN PAQUETE QUE ES EL DE OPENVPN, VAMOS EN EL PFSENSE A system-package manager-available packages Y BUSCAMOS openvpn-client-export 1.9.2 (PARA PODER EXPORTAR LA CONFIGURACION DEL CLIENTE DE VPN QUE VAMOS A CONFIGURAR) Y LE DAMOS A INSTALAR.

UNA VEZ INSTALADO, VAMOSA IR A LA INSTALACIÓN Y CREACIÓN DE LA VPN, PARA ELLO VAMOS A INSTALAR LOS CERTIFICADOS CON LOS QUE NOS VAMOS A CONECTA A LA VPN, CUANDO NOS CONECTAMOS A LA VPN NECESITAMOS PASARLE UNA SERIE DE CREDENCIALES Y DE CLAVES QUE CONFIRMEN QUE ERES TU.

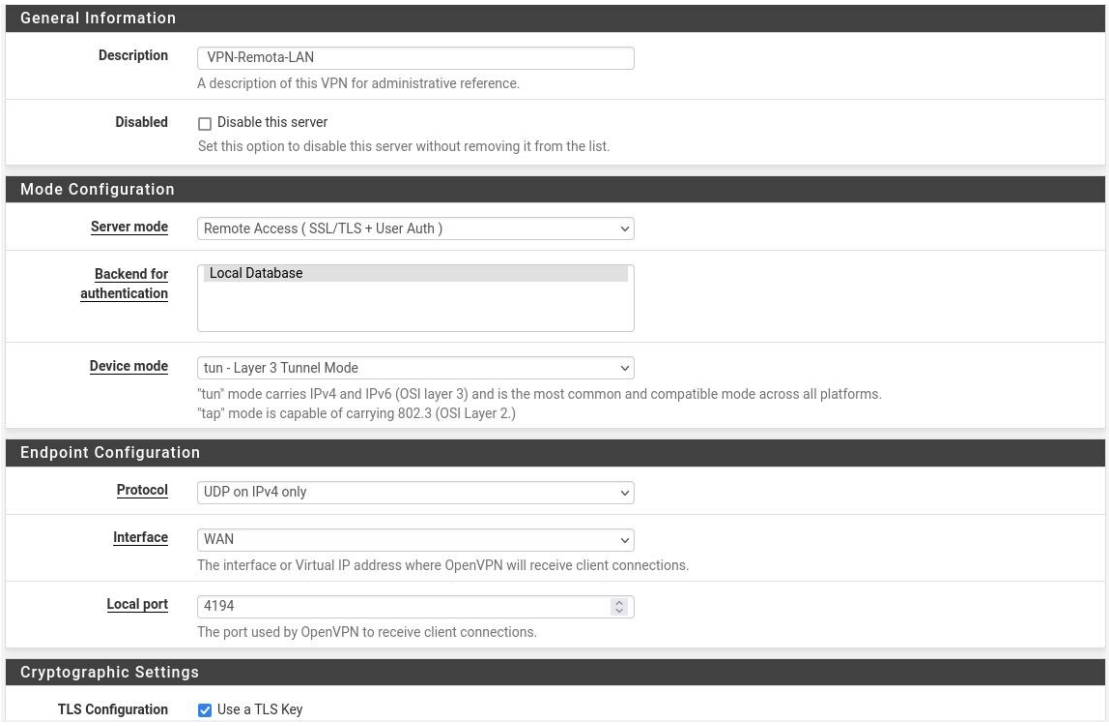
VAMOS A GENERAR LOS CERTIFICADOS PARA LA CONEXION DE LA VPN, PARA ELLO VAMOS A system-certificates Y TENEMOS QUE CREAR UNA ENTIDAD CERTIFICADORA QUE ES LA QUE SE VA A ENCARGAR DE GENERAR Y GESTIONAR LOSCERTIFICADOS DE NUESTRA VPN, LE DAMOS A add Y EN DESCRPTIVE NAME: Keepcoding, METHOD: create an internal Cert Auth, KEY TYPE: rsa 20148, DIGEST ALGORITHM: sha256, LIFETIME: 365, COMMON M¡NAME: Keepcoding, COUNTRY CODE: ES, STATE OR PROVINCE: Madrid, CITU: Madrid, ORGANIZATION: keepcoding, ORGANIZATION UNIT: it



AHORA TENEMOS QUE CREATR EL CERTIFICADO, VAMOS A LA PESTAÑA DE AL LADO, CERTIFICATES Y LE DAMOS add, DESCRIPTIVE NAME: VPN, LIFETIME: 365, CERTIFICATE AUTHORITY: keepcoding (LA QUE HEMOS CREADO ANTES), COMMON NAME: vpn.keepcoding.local, CERTIFICATE TYPE: server certificate (**IMPORTANTE** PORQUE ESTE ES EL CERTIFICADO QUE VAMOS A CREAR PARA NUESTRO PROPIO SERVIDOR DEL PFSENSE Y QUE LUEGO VAMOS A EXPORTAR AL EXTERIOR).

AHORA TENEMOS QUE CREAR EL USUARIO Y LOS RANGOS PARA LA VPN QUE HEMOS DEFINIDO, PORQUE DENTRO DE LA VPN SE VA A CREAR UN TUNEL, Y EN ESE TUNEL TENEMOS QUE ASIGNAR UNA SERIE DE DIRECCIONES IP, PUERTO QUE VA A UTILIZAR LA VPN Y TODA LA CONFIGURACION.

PARA ELLO VAMOS A IR vpn-openvpn Y EN servers LE DAMOS add, DESCRIPTION: VPN-Remota-LAN, EN SERVER MODE: remote access (ssl/tls + use auth), EN PROTOCOL: tcp on ipv4 only, EN DEVICE MODE: tun - layer 3 Tunnel Mode (MODO TUNEL, NIVEL 3 DE LA CAPA PARA CONECTAR REDES A REDES Y NIVEL 2 PARA TENERLO TODO EN EL MISMO FRAGMENTO DE RED), PROTOCOL: udp on ipv4 only, INTRFACE: wan, EN LOCAL PORT(ESTO ES LO QUE VAMOS A CAMBIAR, ES SEGURIDAD POR OSCURIDAD, VIENE POR DEFECTO EL QUE TODO EL MUNDO USA PARA VPN, LE CAMBIAMOS EL PUERTO PARA OCULTARLA): 4194, EN SERVER CERTIFICATE: vpn (server: yes, ca: keepcoding) (EL QUE HEMOS CREADO ANTES), EN HARDWARE CRYPTO: si nos sale el hardware para poder acelerar el proceso criptografico de la vpn lo seleccionamos, EN IPV4 TUNNEL NETWORK (PONEMOS LA DIRECCION IP QUE VA A UTILIZAR NUESTRO TUNEL DE LA VPN): 192.168.220.0/24, EN IPV4 LOCAL NETWORK (LA RED PARA QUE SEA ACCESIBLE DESDE EL EXTERIOR PONEMOS LA DE LA LAN: 192.168.100.0/24 (ESTO SERIA EL PUNTO ACCESIBLE QUE VA A TENER NUESTRA VPN, TODA LA RED QUE CUELGA DE LA PARTE DE LA LAN), EN REDIRECT IPV4 GATEWATY (**NO LO ACTIVAMOS**): SI LO ACTIVAMOS SE REDIRIGE TODO EL TRAFICO DE LA RED DE LOS USUARIOS, SI QUEREMOS TENER CONTROLADO ABSOLUTAMENTE TODO LO QUE HAGAN LOS USUARIOS, LO REDIRECCIONAS, EN CONCURRENT CONECCTIONS (GENTE QUE SE PUEDE CONECTAR A LA VEZ): 10



Automatically generate a TLS Key.

Peer Certificate Authority: Keepcoding

Peer Certificate Revocation list: No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager

OCSP Check: Check client certificates with OCSP

Server certificate: VPN (Server: Yes, CA: Keepcoding)

Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length: 2048 bit

Diffie-Hellman (DH) parameter set used for key exchange.

ECDH Curve: Use Default

The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms

Available Data Encryption Algorithms:
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)

Click to add or remove an algorithm from the list

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list:
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

Fallback Data Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm: SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto: Intel RDRAND engine - RAND

Certificate Depth: One (Client+Server)

When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Strict User-CN Matching: Enforce match

When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

Client Certificate Key Usage Validation: Enforce key usage

Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

Tunnel Settings

IPv4 Tunnel Network: 192.168.220.0/24

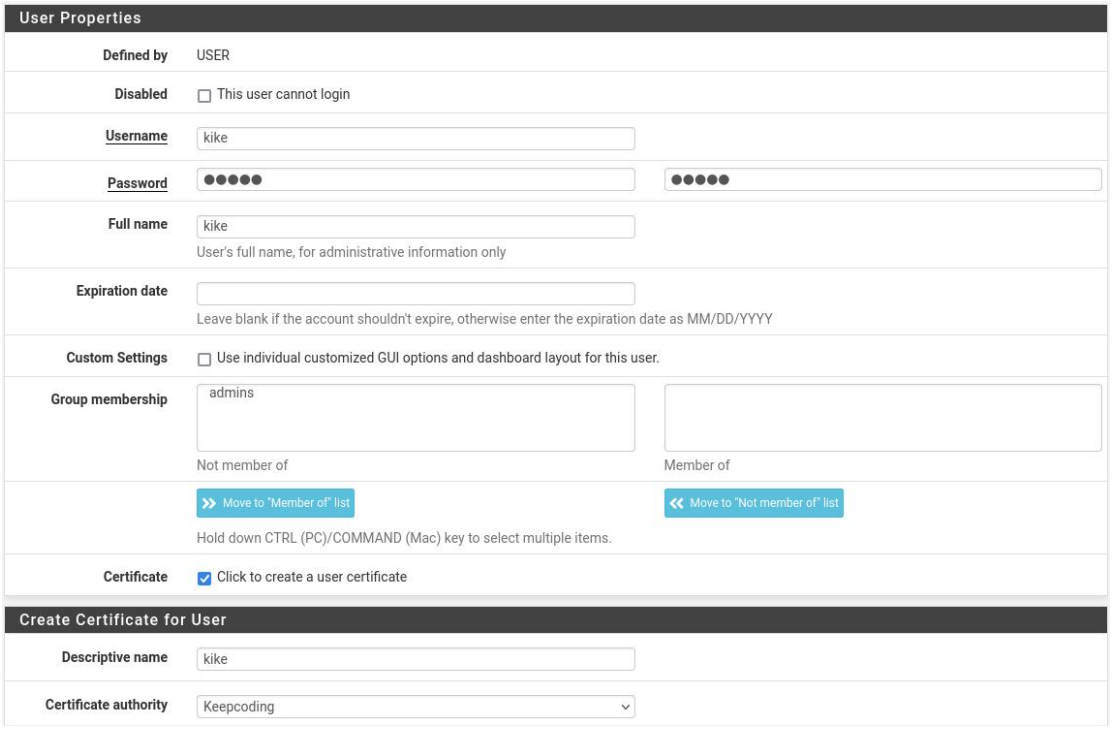
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts

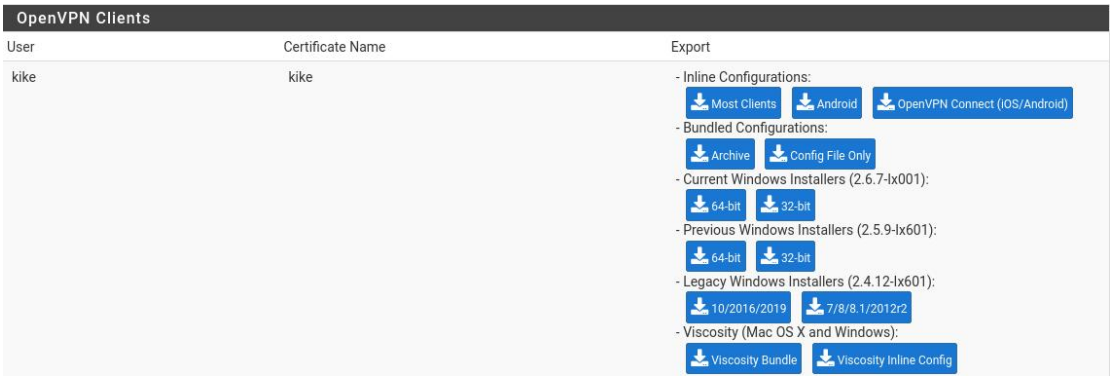
AHORA NOS VAMOS A system-user manager Y AQUI AÑADIMOS UN NUEVO USUARIO QUE ES NUESTRO USUARIO DE LA VPN.
LE DAMOS A add, USERNAME: KIKE, PASSWORD: 12345 (NOS TENEMOS QUE ACORDAR), FULL NAME: KIKE, LE DAMOS A CERTIFICATE: click to create a user certificate, SE NOS DESPLIEGA UN MENU PARA CREAR EL CERTIFICADO DEL USUARIO PARA CONECTARNOS CON NUESTRA ENTIDAD DE CERTIFICACION QUE HEMOS CREADO PARA GENERAR ESTOS CERTIFICADOS (MAQUINAS A PARTE), DESCRIPTIVE NAME: kike, CERTIFICATE AUTHORITY: keepcoding, KEY TYPE: rsa 2048, DIGEST ALGORITHM sha256, LIFETIME: 365, Y LE DAMOS A GUARDAR Y YA TENEMOS NUESTRO USUARIO CREADO



AHORA LO QUE NOS QUEDA SERIA EXPORTAR EL CERTIFICADO DE NUESTRO USUARIO, PARA ELLO NOS VAMOS A vpn-openvpn Y EN LA BARRA ROJA DE ARRIBA A clien export.

SELECCIONAMOS LA VPN QUE HEMOS CREADO CON EL PUERTO QUE HEMOS CONFIGURADO EN REMOTE ACCESS SERVE vpn-remota-lan upd4:4194.

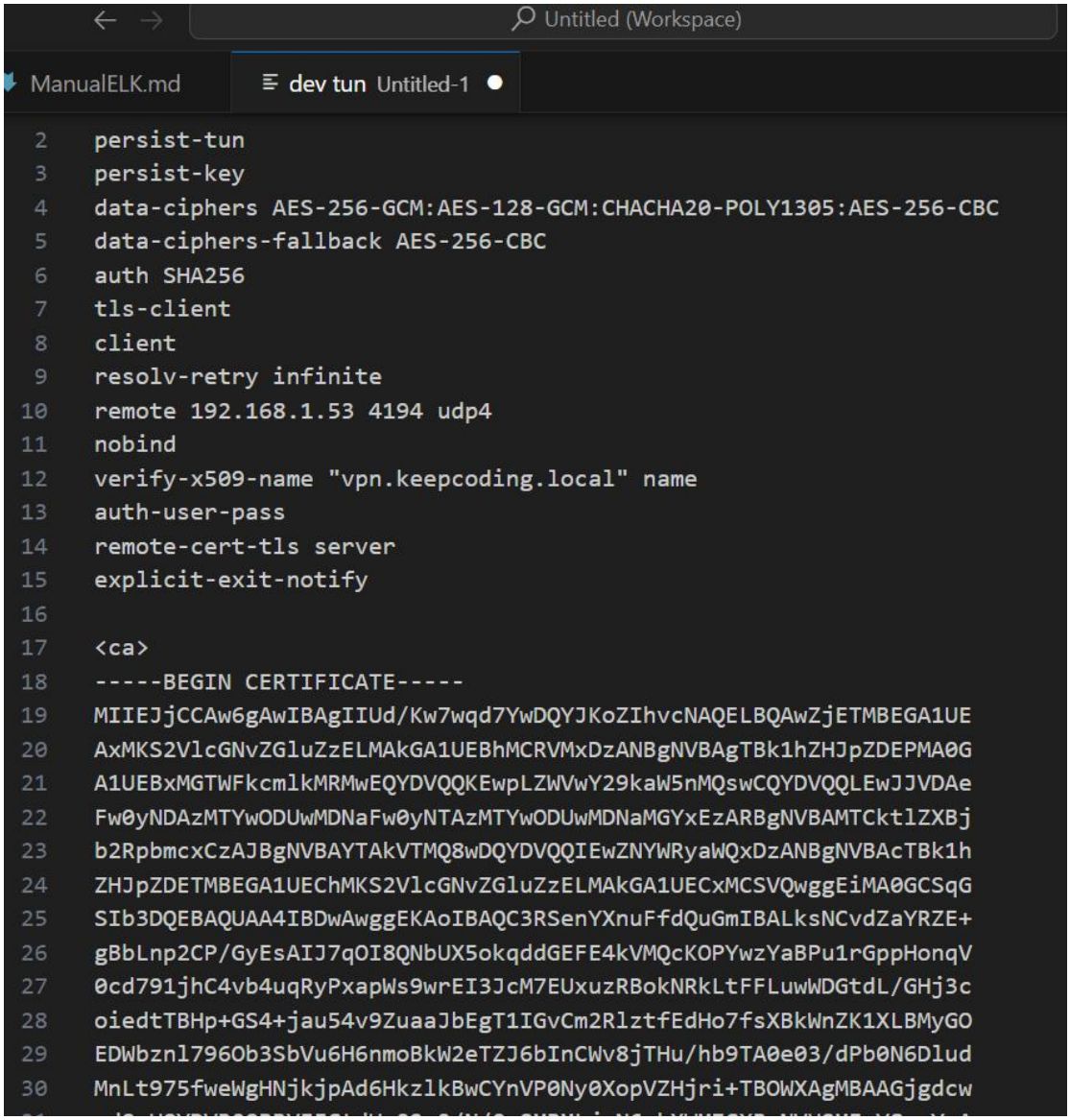
EN OPENVPN CLIENTS NOS TENDRIA QUE SALIR EL USUARIO QUE HEMOS CREADO Y LAS CONFIGURACIONES QUE HEMOS CREADO.



DESCARGAMOS most clients. SE NOS DESCARGA UN ARCHIVO .OVPN. YA TENEMOS EL CERTIFICADO DESCARGADO, LO ABRIMOS CON EL EDITOR DE TEXTO, Y NOS SALE EN LA CONSOLA EL CERTIFICADO.

```
dev tun
persist-tun
persist-key
data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305:AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA256
tls-client
client
resolv-retry infinite
remote 192.168.1.53 4194 udp4
nobind
verify-x509-name "vpn.keepcoding.local" name
auth-user-pass
remote-cert-tls server
explicit-exit-notify

<ca>
-----BEGIN CERTIFICATE-----
MIIEJjCCAw6gAwIBAgIIUd/Kw7wqd7YwDQYJKoZIhvcNAQELBQAwZjETMBEGA1UE
AxMKS2VlcGNvZGluZzELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1hZHJpZDEPMA0G
A1UEBxMGTWFkcmlkMRMwEQYDVQQKEwpLZWVwY29kaW5nMQswCQYDVQQLEwJJVDAe
Fw0yNDAzMTYwODUwMDNaFw0yNTAzMTYwODUwMDNaMGYxEzARBgNVBAMTCktlZXBj
b2RpbmcxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZNYWRyaWQxDzANBgNVBAcTBk1h
ZHJpZDETMBEGA1UEChMKS2VlcGNvZGluZzELMAkGA1UECxMCSVQwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC3RSenYXnuFfdQuGmIBALksNCvdZaYRZE+
gBbLnp2CP/GyEsAIJ7qOI8QNbUX5okqddGEFE4kVMQcKOPYwzYaBPu1rGppHonqV
0cd791jhC4vb4uqRyPxapWs9wrEI3JcM7EUxuzRBokNRkLtFFLuwWDGtdL/GHj3c
oiedtTBHp+GS4+jau54v9ZuaaJbEgT1IGvCm2RlztfEdHo7fsXBkWnZK1XLBMyGO
EDWbznl796Ob3SbVu6H6nmoBkW2eTZJ6bInCWv8jTHu/hb9TA0e03/dPb0N6Dlud
MnLt975fweWgHNjkjpAd6HkzlkBwCYnVP0Ny0XopVZHjri+TBOWXAgMBAAGjgdcw
gdQwHQYDVR0OBBYEFGtdHp02×9/N/0eSMBMLjsN6qkXWMIGXBgNVHSMEgY8wgYyA
FGtdHp02×9/N/0eSMBMLjsN6qkXWoWqkaDBmMRMwEQYDVQQDEwpLZWVwY29kaW5n
MQswCQYDVQQGEwJFUzEPMA0GA1UECBMGTWFkcmlkMQ8wDQYDVQQHEwZNYWRyaWQx
EzARBgNVBAoTCktlZXBjb2RpbmcxCzAJBgNVBAsTAklUgghR38rDvCp3tjAMBgNV
HRMEBTADAQH/MAsGA1UdDwQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAQEALbjWnRvP
7MjblFOTTXIBCLiIx3fIMTafDpBUyViZyta8kfAQy9NVVqr31YE9yjDVjQkEyKdh
KE9y7JvYdUY9PlyDoCxL2P5GFxHA16GiLl9f8ipNNe20hE31lWVVGKGhhLYVsDRV
AetYG5kxPcZZOXLR120eCNPSzcJmjiaS6Lv2kZxXYL5TYJrY1N+RHXAckxi+8VWZ
PmxXZN1owlY77UJTeAMigiJ8iWGmyOkVBBoIVJk3nFPq6gdPC63bH5i4SygN2zjH
h9EXGOx/g+s5pDwJbo59qBACjP88yg1vWKv4eu970I7vNgKqI0gClg15VzR2e19c
ze3Kc+kxlctyQg==
-----END CERTIFICATE-----
```

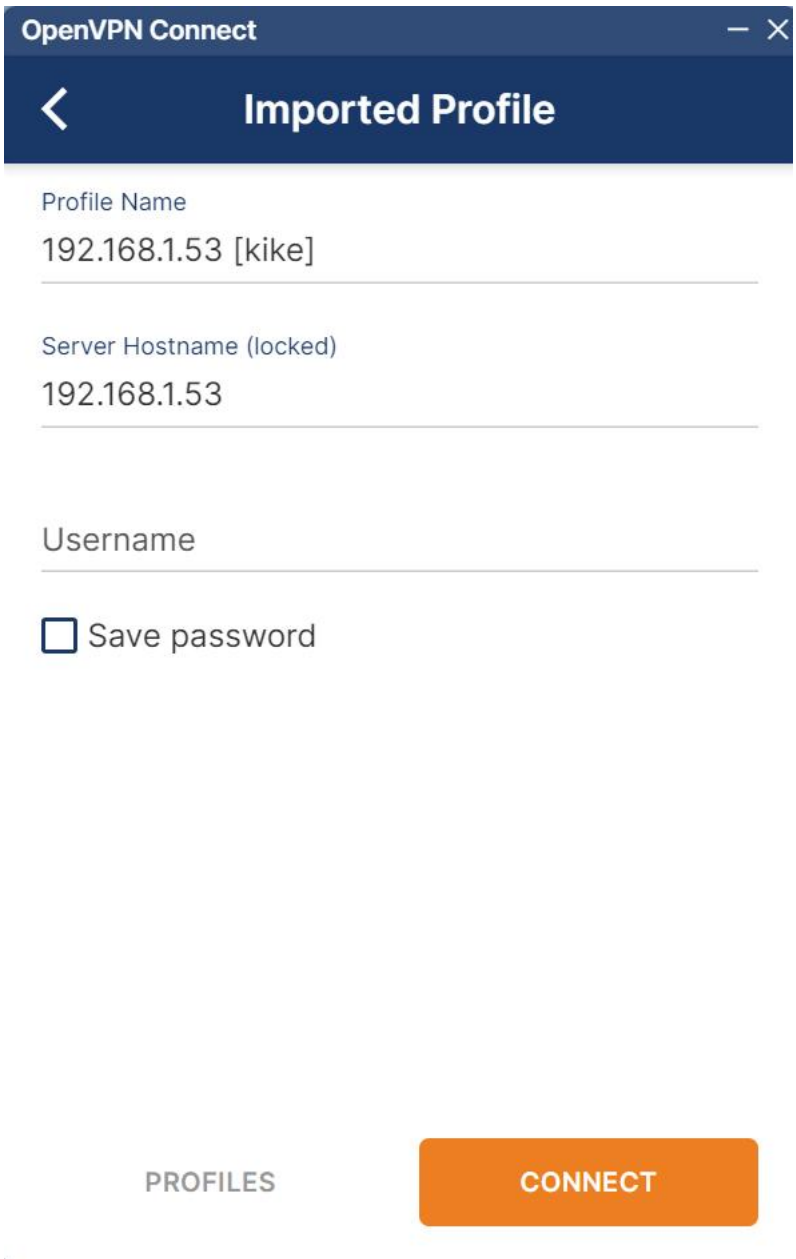
COPIAMOS EL CONTENIDO Y LO TENEMOS QUE TENER EN NUESTRA MAQUINA HOST PARA CONECTARNOS DESDE ELLA. ABRIMOS UN EDITOR, POR EJEMPLO EL VISUAL STUDIO CODE Y LO PEGAMOS.



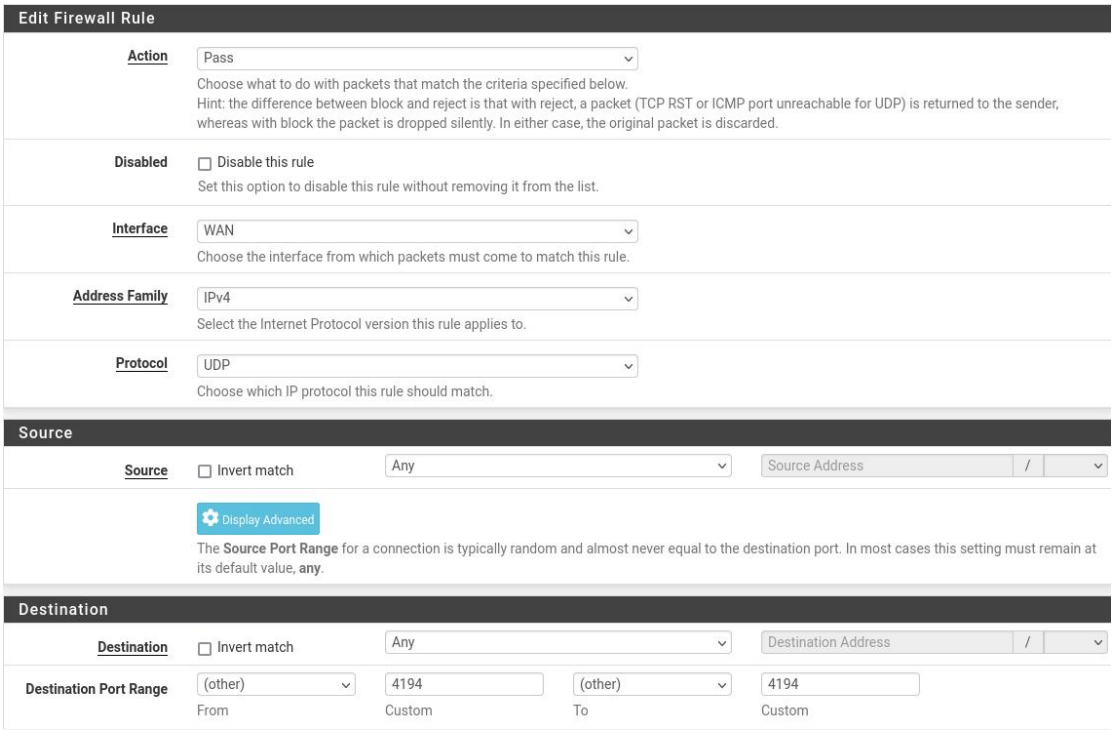
AHORA LE DAMOS A file-save as (lo guardamos en un sitio donde lo veamos, con formato No extension (*,)y con el nombre por ejemplo kike y la extension ovpn: kike.ovpn)

YA CON EL CERTIFICADO EN EL ESCRITORIO DE WINDOWS, NOS TENEMOS QUE DESCARGAR LA APLICACION DE VPNCLIENT Y NOS BAJAMOS EL CLIENTE EN WINDOWS (EN EL HOST EN EL QUE ESTEMOS) (ESTE ES EL CLIENTE DE VPN AL QUE LE VAMOS A SUBIR EL CERTIFICADO DE NUESTRA VPN)

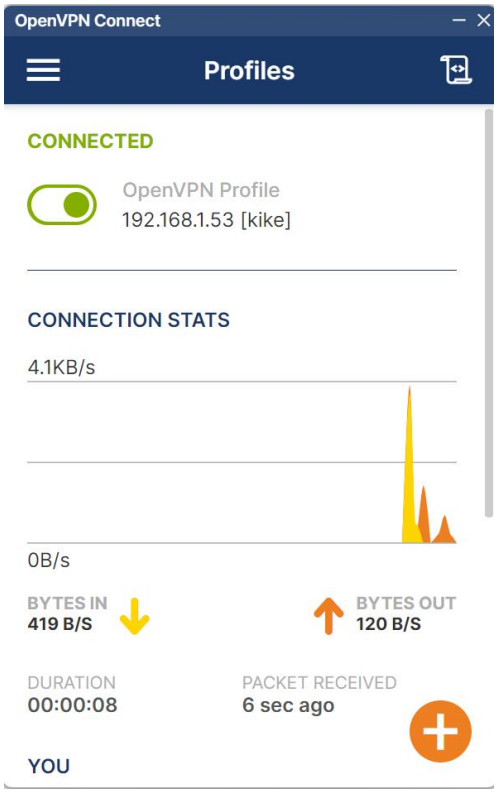
ABRIMOS LA APLICACION DE EL CLIENTE Y EN UPLOAD FILE ARRASTRAMOS EL ARCHIVO CON EL CERTIFICADO QUE HEMOS EXPORTADO, Y NOS DEBERIA SALIR LA DIRECCION DE LA WAN 192.168.1.53 Y EN EL NOMBRE DE USUARIO(EL QUE HEMOS CONFIGURADO): KIKE, Y LE DAMOS A CONNECT Y NOS PIDE LA CONTRASEÑA: 12345, NO SE NOS CONECTA PORQUE NOS FALTA LA REGLA DE FIREWALL PARA HABILITAR EL TRAFICO DE LA VPN



VAMOS AL PFSENSE firewall-rules Y EN LA WAN (BARRA DE ARRIBA) AÑDIMOS UNA NUEVA REGLA DE FIREWALL. ACTION: PASS, INTERFACE: WAN, ADDRESS FAMILY: IPV4, PROTOCOL: UDP, SOURCE(ORIGEN): ANY, DESTINATION: custom 4194 custom 4194(PUERTO QUE HEMOS CONFIGURADO EN NUESTRA VPN), DESCRIPTION: Reagla WAN VPN.



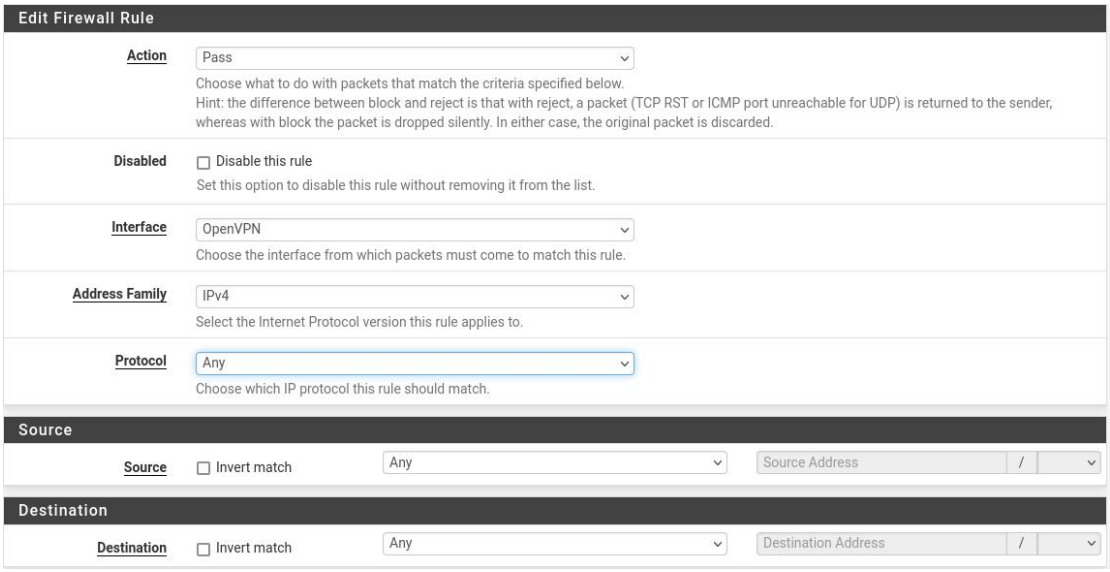
SI VOLVEMOS A VPN YA SE NOS CONECTA

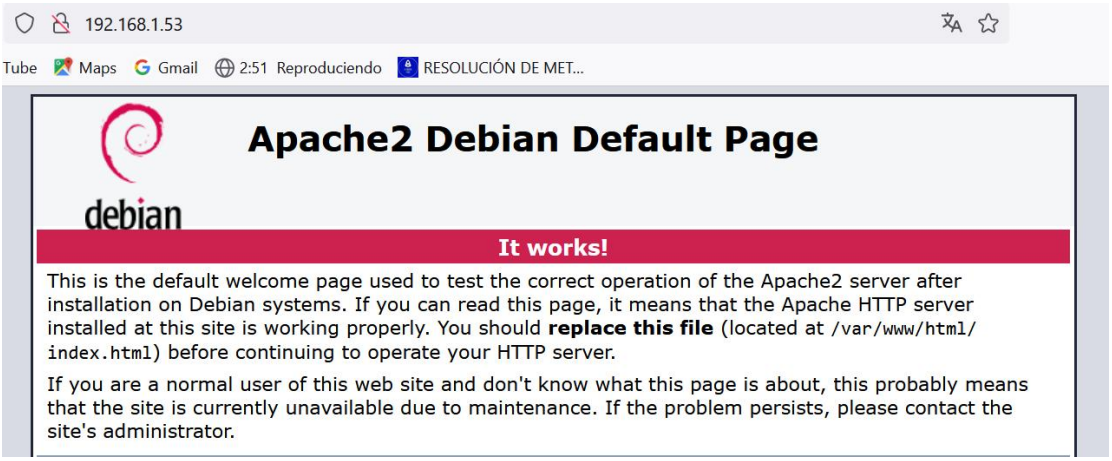


AHORA LA IDEA ES INTENTAR LLEGAR A NUESTRA KALI.

ABRIMOS UN NAVEGADOR EN EL KALI, PONEMOS INCOGNITO Y PONEMOS LA DIRECCION DE LA KALI 192.168.1.53 YNO NOS ENTRA AL APACHE PORQUE NOS FALTA CREAR UNA REGLA MAS.

NOS VAMOS AL PFSENSE, Y EN firewall-rules-openvpn PONEMOS ACTION: PASS, INTERFACE:OPENVPN, ADDRESS FAMILY: IPV4, PROTOCOL: **ANY**, SOURCE: ANY, DESTINATION: ANY. AQUI YA DEBERIAMOS PODR ACCEDER A LA KALI.

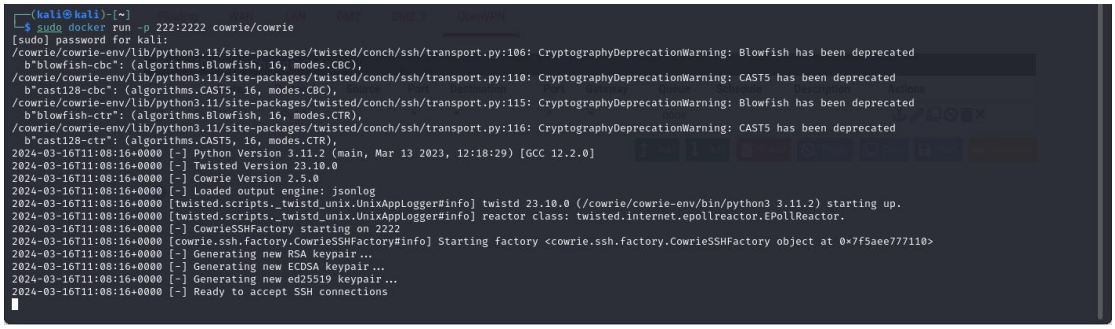




AHORA MISMO TENEMOS CONFIGURADO NUESTRO CLIENTE DE CASA (ORDENADOR) QUE TIENE EL CLIENTE DE LA VPN, HEMOS HECHO UN TUNEL QUE VA DESDE ROUTER DE CASA Y ACCEDE AL SERVIDOR DE APACHE.

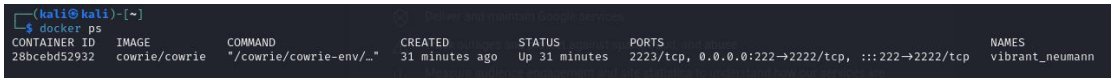
HONEYPOTS-COWRIE:

EL HONEYPOT QUE VAMOS A LANZAR EN DMZ ES EL COWRIE “SSH” A TRAVÉS EL DOCKER



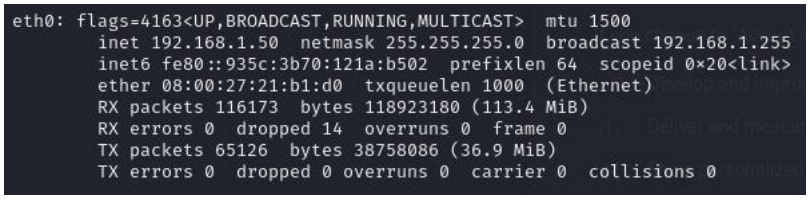
EL PRIMER PASO QUE HEMOS HECHO ES LANZAR EL CONTENEDOR DOCKER PARA QUE ARRANQUE CON ESTE COMANDO: docker run -p 222:2222 cowrie/cowrie. EL PUERTO DE LA IZQUIERDA ES DEL ANFITRIÓN Y EL DE LA DERECHA DEL INVITADO.

CON docker ps VEMOS QUE TENEMOS EL CONTENEDOR CORRIENDO

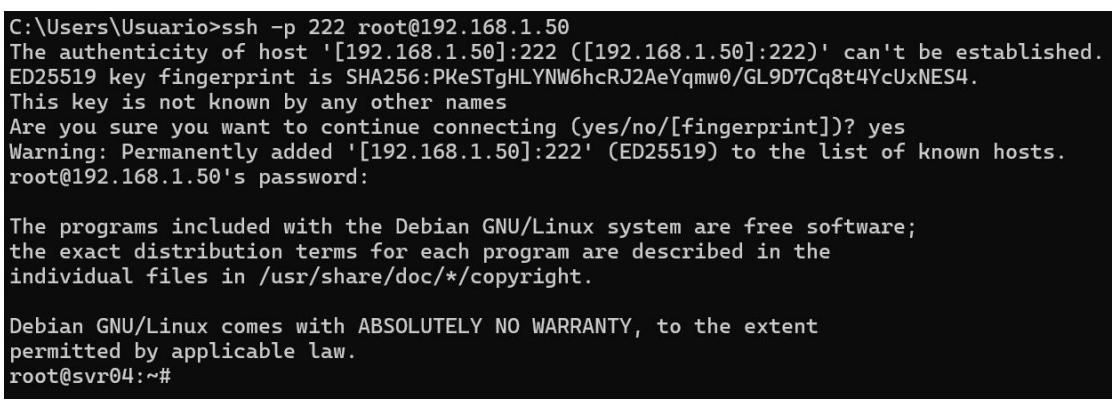


EL QUE TENEMOS CORRIENDO ES EL QUE HEMOS PUESTO QUE SIMULA UN HONEYPOT DE SSH Y LO QUE LE ESTAMOS DICIENDO ES QUE NOS LO ABRA EN EL PUERTO 222

AHORA LO QUE VAMOS A HACER ES A TRAVES DEL CMD DE NUESTRA MAQUINA (WINDOWS), TENEMOS QUE HACER UN SSH AL PUERTO 222 CON EL USUARIO ROOT Y CON LA IP DE NUESTRA MAQUINA.



ABRIMOS CMD Y PONEMOS ssh -p 222 root@192.168.1.50 (PARA CONECTARNOS DESDE LA MAQUINA WINDOWS) Y NOS DEBERIA SALIR LA CLAVE PARA PODER ESTABLECER LA SESION. NOS DICE QUE EL FINGERPRINT NO SE CONOCE, ES NUEVO, Y POR LO TANTO NOS PREGUNTA SI ESTAMOS SEGUROS DE CONECTANOS, LE DAMOS A SI Y EN LA CONTRASEÑA PODEMOS PONER LO QUE SEA Y YA ESTAMOS DENTRO.



ESTE HONEYPOT CONSISTE EN CAPTURAR TODOS LOS COMANDOS QUE SE PRUEBAN DENTRO DEL SERVIDOR, SI HACEMOS UN ls EN EL CMD DE WINDOWS NOS SALE EN LA CONSOLA DEL KALI CONECTADA.

```
root@svr04:~# ls
```

```
2024-03-16T11:49:08+0000 [HoneyPotSSHTransport,0,192.168.1.54] Command found: ls
```

AQUI PODRIAMOS IR RECUPERANDO UN POCO DE INFORMACION DE LO QUE SERIAN LOS COMANDOS QUE LOS ATACANTES ESTAN UTILIZANDO EN NUESTRO HONEPOT. SI POR EJEMPLO LE HACEMOS UN cat AL FICHERO DE PASSWORD cat /etc/passwd Y VEMOS QUE NOS SACA TODA LA INFORMACIÓN, Y QUE EL HONEYPOT NOS LO CAPTURA

```
root@svr04:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
phil:x:1000:1000:Phil California,,,:/home/phil:/bin/bash
root@svr04:~#
```

```
2024-03-16T11:53:30+0000 [HoneyPotSSHTransport,1,192.168.1.54] Command found: cat /etc/passwd
```

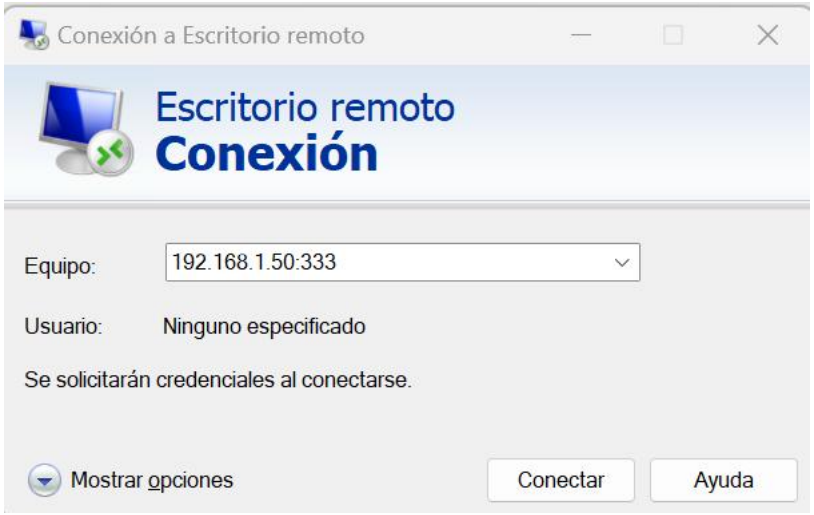
ES COMO SIMULAR UN SISTEMA DE UN SERVIDOR SSH Y POR LO TANTO PODRIAMOS CAPTURAR LOS COMANDOS, HERRAMIENTAS QUE INTENTEN UTILIZAR EN NUESTRO SISTEMA VULNERABLE Y UTILIZAR ESA INFORMACION PARA HACER THREAT HUNTING.

HONEYPOTS-RDPY:

PARA ARRANCARLO HACEMOS docker run -p 333:3389 amazedostrich/rdpy

```
┌──(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE                 COMMAND                  CREATED          STATUS          PORTS                                                  NAMES
74ac3c954ec4   amazedostrich/rdpy    "/bin/sh -c '/usr/bi…"   24 seconds ago   Up 23 seconds   0.0.0.0:333→3389/tcp, :::333→3389/tcp                  competent_cohen
28bcebd52932   cowrie/cowrie         "/cowrie/cowrie-env/…"   54 minutes ago   Up 54 minutes   2223/tcp, 0.0.0.0:222→2222/tcp, :::222→2222/tcp        vibrant_neumann
```

AHORA VAMOS A WINDOWS Y escritorio remoto Y PONEMOS LA IP Y LE DAMOS A CONECTAR



YA ESTAMOS CONECTADOS.

SI DEJAMOS EL CONTENEDOR CORRIENDO Y NOS VAMOS A OTRA TERMINAL Y HACEMOS docker exec -it -u 0 74ac3c954ec4 /bin/bash (PARA QUE NOS ABRA UNA TERMINAL) (74ac3c954ec4:ID DEL CONTENERDOR) CON EL USURARIO ROOT 0, DIRECTAMENTE NOS ABRIRÁ UNA TERMINAL Y ESTA ES LA TERMINAL DE DENTRO DEL DOCKER.

```
┌──(kali㉿kali)-[~]
└─$ sudo docker exec -it -u 0 74ac3c954ec4 /bin/bash
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
bash-4.4#
```

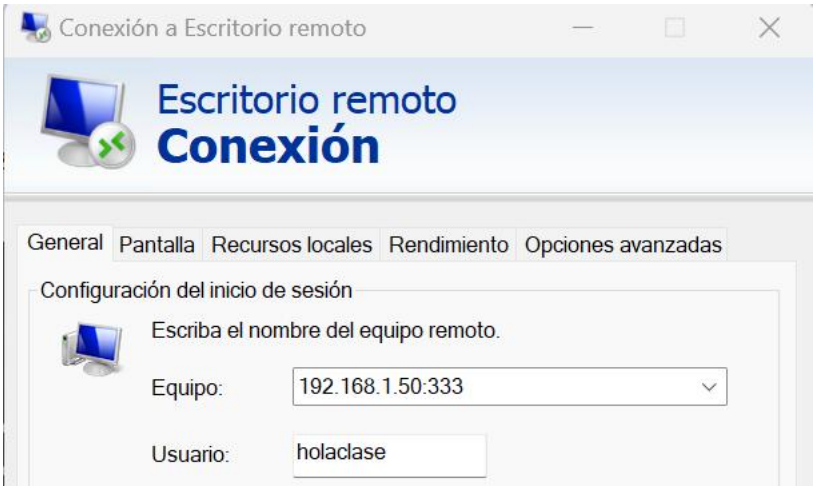
LE DAMOS ls, Y SI NOS VAMOS A cd /var/log, Y LUEGO cd rdpy/ AQUI ESTAN LOS LOGS DEL HONEYPOT.

```
┌──(kali㉿kali)-[~]
└─$ sudo docker exec -it -u 0 74ac3c954ec4 /bin/bash
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
bash-4.4# ls
bin   dev   etc   home  lib   media  mnt   opt   proc  root  run   sbin  srv   sys   tmp   usr   var
bash-4.4# cd /var/log
bash-4.4# ls
rdpy
bash-4.4# cd rdpy
bash-4.4# ls
rdpy.log
bash-4.4#
```

SI HACEMOS UN tail -f AL ARCHIVO tail -f rdpy.log AQUI VEREMOS NOMBRE DE USUARIO, CONTRASEÑA, EL EQUIPO QUE SE CONECTA...

```
bash-4.4#  tail -f rdpy.log
2024-03-16T12:45:20.114236Z,Connection from 192.168.1.54:53680
[*] INFO:
2024-03-16T12:46:02.241518Z,Connection from 192.168.1.54:53690
[*] INFO:
2024-03-16T12:46:04.897123Z,Connection from 192.168.1.54:53691
[*] INFO:       select file (1920, 1080) → /home/rdpy/1
[*] INFO:
2024-03-16T12:46:04.959356Z,domain:,username:,password:,hostname:DESKTOP-GF86LUV
[*] INFO:
2024-03-16T12:46:04.993319Z,domain:,username:,password:,hostname:DESKTOP-GF86LUV
```

SI EN EL ESCRITORIO REMOTO PONEMOS HOLA CLASE Y LE DAMOS A CONECTAR, VEMOS EN LOS LOGS, USUARIO CONECTADO HOLA CLASE.



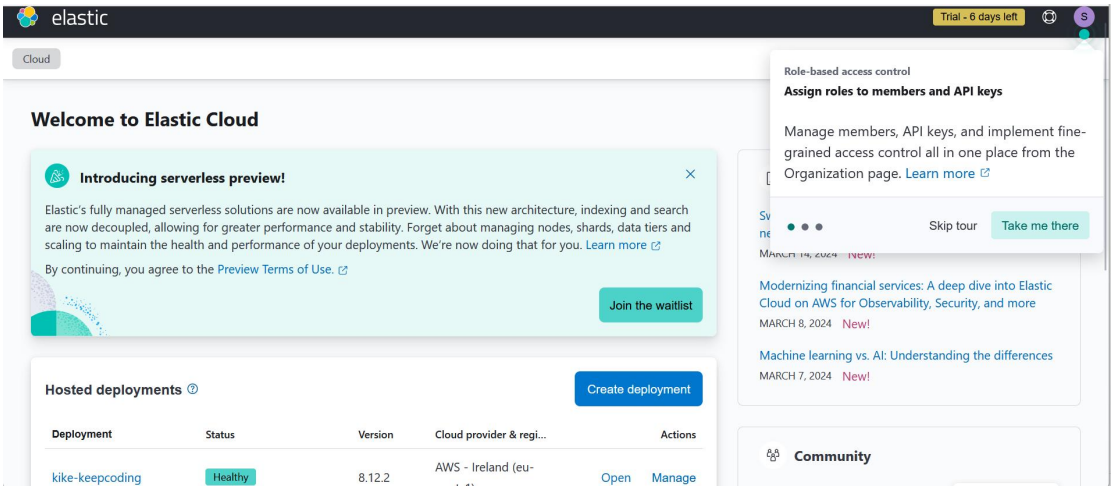

```
2024-03-16T12:56:38.527452Z,domain:,username:holaclase,password:,hostname:DESKTOP-GF86LUV
[*] INFO:
2024-03-16T12:56:38.550014Z,domain:,username:holaclase,password:,hostname:DESKTOP-GF86LUV
```

ASI PODREMOS VER QUIEN SE HA CONECTADO, Y LAS CREDENCIALES QUE HA UTILIZADO Y NOMBRE DE USUARIO,IP DEL ATACANTE... PODEMOS VER ATAQUES DE FUERZA BRUTA POR EJEMPLO.

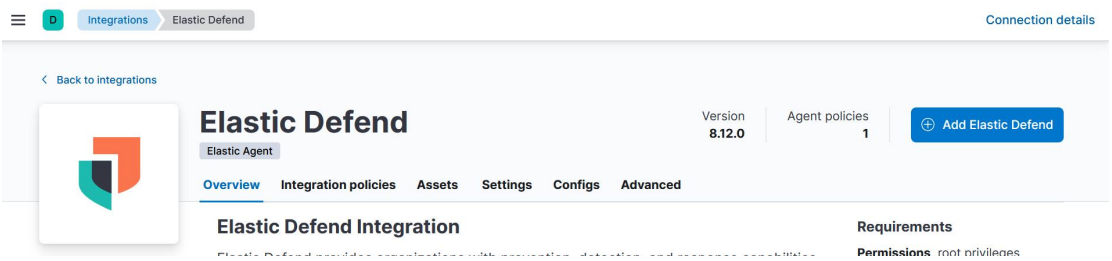
ELASTIC (SIEM):

LA IDEA ES QUE SEPAMOS PODER INTEGRAR FUENTES, Y MIRAR LOS LOGS QUE SE RECOPILAN.

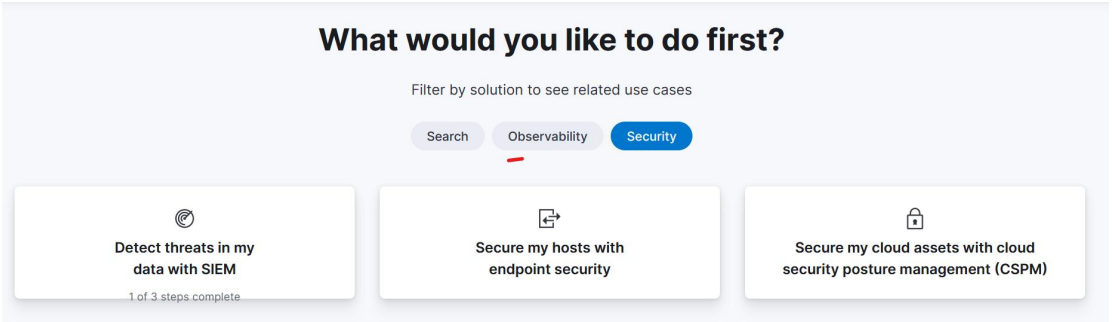
ENTRAMOS EN ELASTIC



VAMOS A AÑADIR ELASTIC DEFEND.
DESPUÉS DEBEREMOS COPIAR LOS COMANDOS QUE NOS DAN SEGÚN EL SISTEMA OPERATIVO EN EL QUE LO VAYAMOS A INSTALAR, EN NUESTRO CASO LO HAREMOS EN WINDOWS Y LINUX.



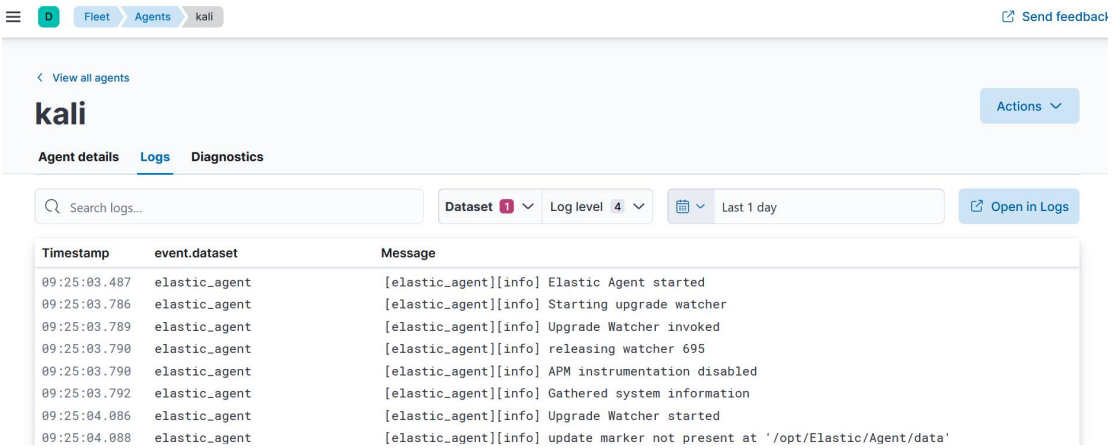
AQUI VAMOS A DETECT THREATS IN MY DATA WITH SIEM



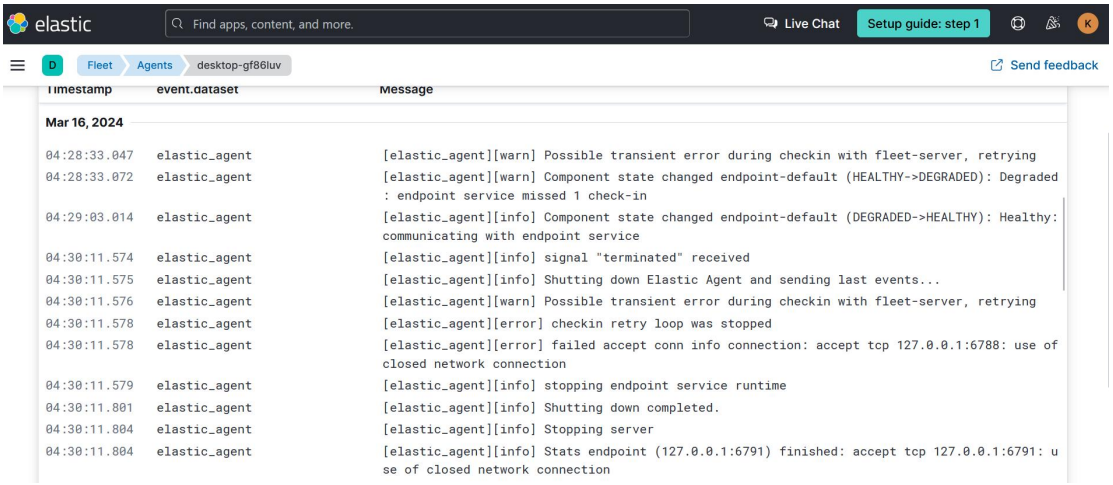
AHORA LE DAMOS A ADD INTEGRATION, AQUI YA LO QUE ESTAMOS HACIENDO ES RECOPILAR TODOS LOS EVENTOS TANTO DE LINUX COMO DE WINDOWS PARA RECOLECTARLOS EN EL SIEM.

LE ESTAMOS DICIENDO QUE COJA TODOS LOS LOGS IMPORTANTES O NECESARIOS PARA EL TEMA DE SEGURIDAD.

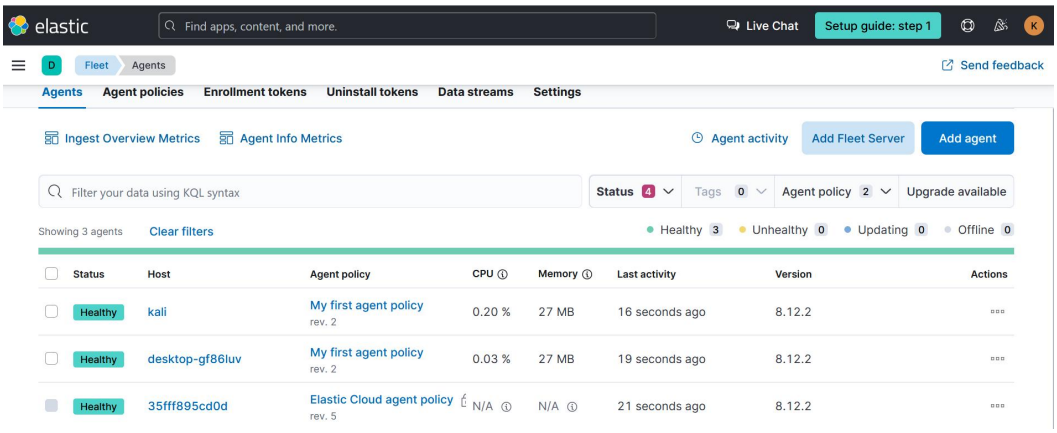
AQUI PODEMOS VER LOS EVENTOS DE KALI:



AQUI PODEMOS VER LOS LOGS DE WINDOWS:

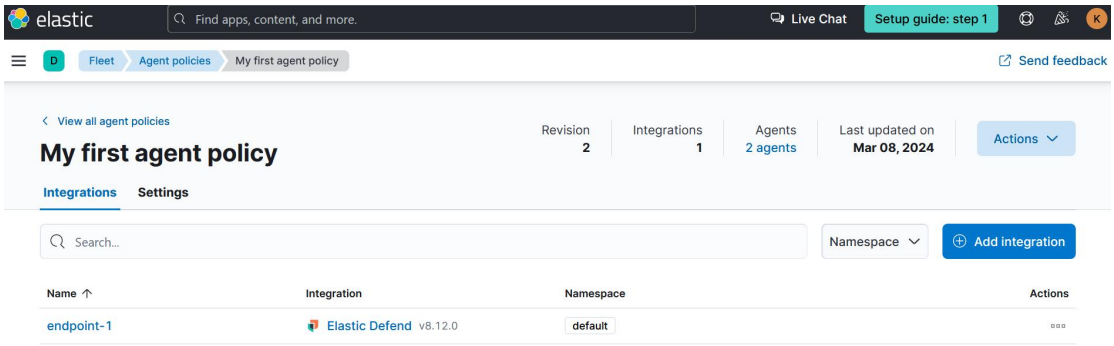


AQUI EN EL FLEET VEMOS LAS POLITICAS QUE TENEMOS:

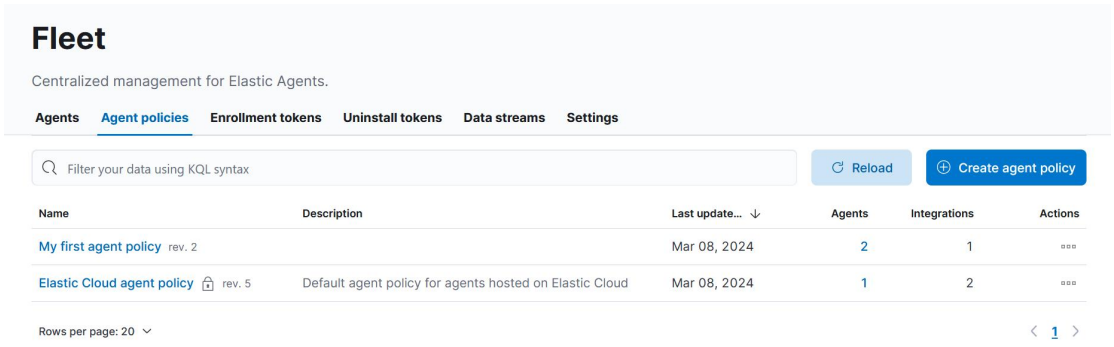


ESTO SON LAS PARTES DE LAS POLITICAS (CONJUNTO DE NORMAS QUE LE VAMOS A PONER EN NUESTROS SISTEMAS)

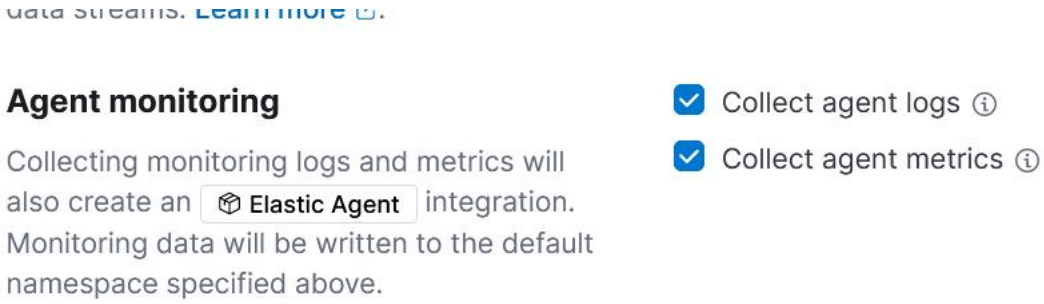
TANTO LA KALI COMO EL WINDOWS LO TENEMOS EN MY FIRST AGENT POLICY (ESTA POLITICA SOLAMENTE TIENEN LA INTEGRACION CON EL ELASTIC DEFEND



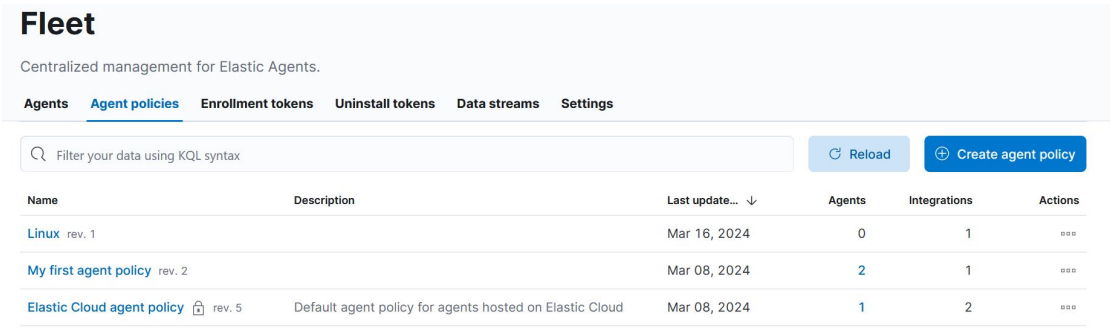
QUEREMOS DIVIDIRLO EN DIFERENTES POLITICAS PARA QUE LOS WINDOWS Y LOS LINUX NOS LO RECOJA CON DIFERENTES PLUGGINS.
PARA ELLO VAMOS A AGENT POLICIES Y CREAMOS UNA NUEVA POLITICA



AQUI VAMOS A PONERLE DE NOMBRE LINUX, Y PODEMOS DAR A COLLECT SYSTEM LOGS AND METRICS PARA QUE NOS RECOJA LOS LOGS DE SISTEMA Y METRICAS DE FUNCIONAMIENTO Y CREAMOS LA POLITICA.



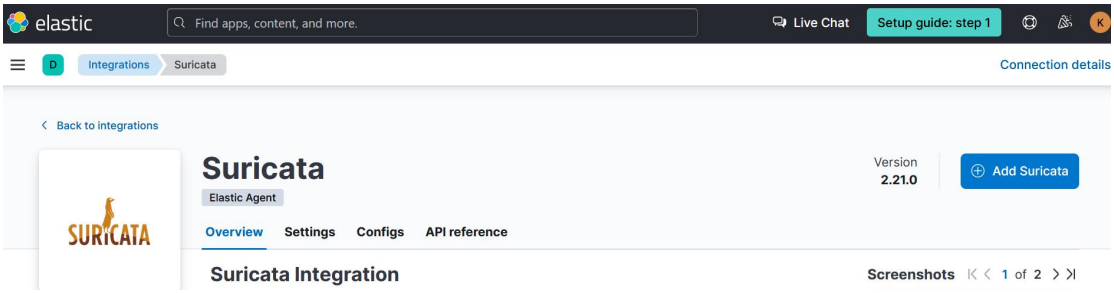
AQUI TENDRIAMOS LA POLITICA LINUX QUE HEMOS CREADO Y LA POLITICA MU FIRST AGENT POLICY



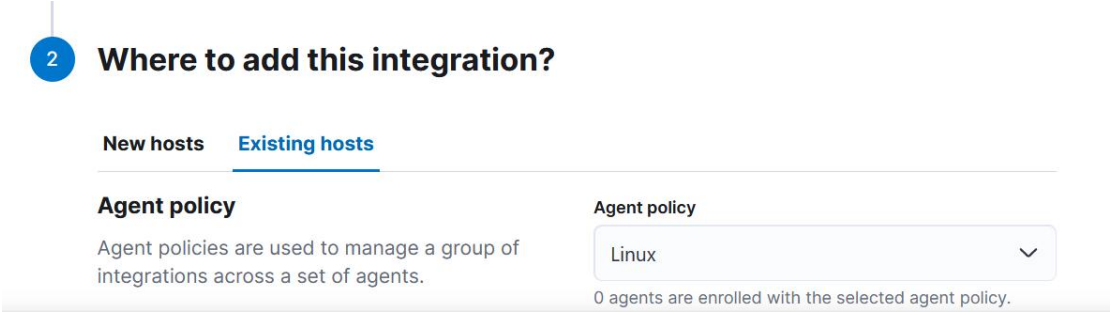
VAMOS A AÑADIRLE UNA INTEGRACION A LA POLITICA DE MY FIRST AGENT POLICY, LE DAMOS A ADD INTEGRATION,

NOSOTROS HEMOS AÑADIDO ANTES LA DE ELASTIC DEFEND, QUE ES PARA PROTEGER NUESTROS HOST Y LA QUE RECOGE LOS EVENTOS DE SEGURIDAD.

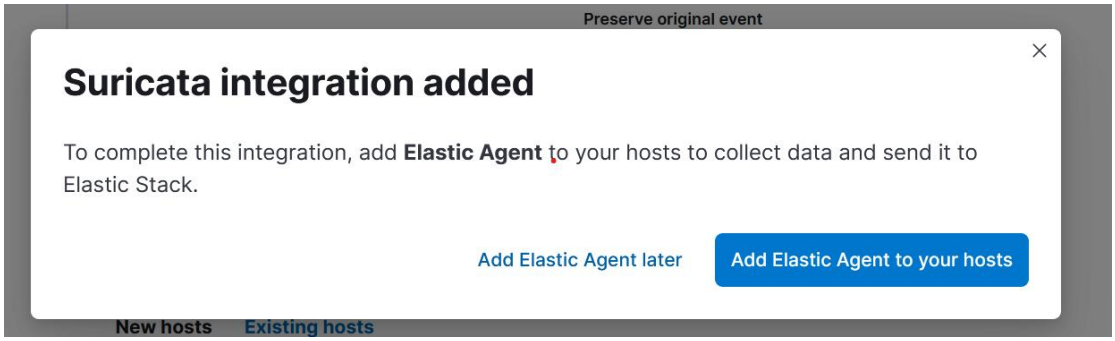
VAMOS A AÑADIRLE LA DE SURICATA PARA QUE RECOJA ESOS LOGS. LE DAMOS A ADD SURICATA.



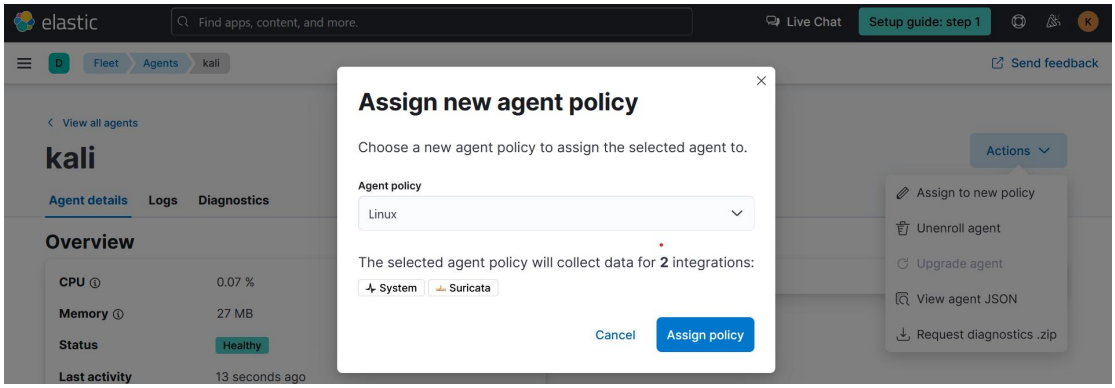
VAMOS A PONERLA EN LA POLITICA DE LINUX



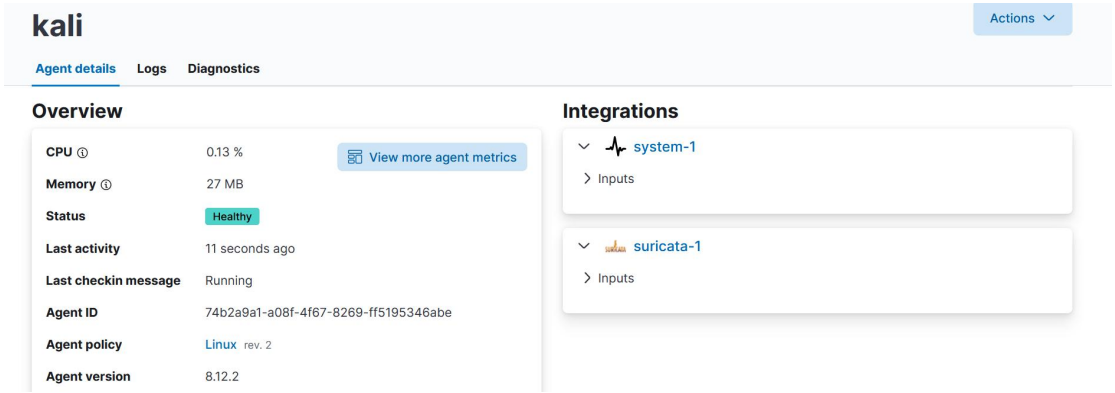
AQUI PODEMOS AÑADIR UN AGENTE, PERO EN PRINCIPIO NO VAMOS A AÑADIR NINGUNO.



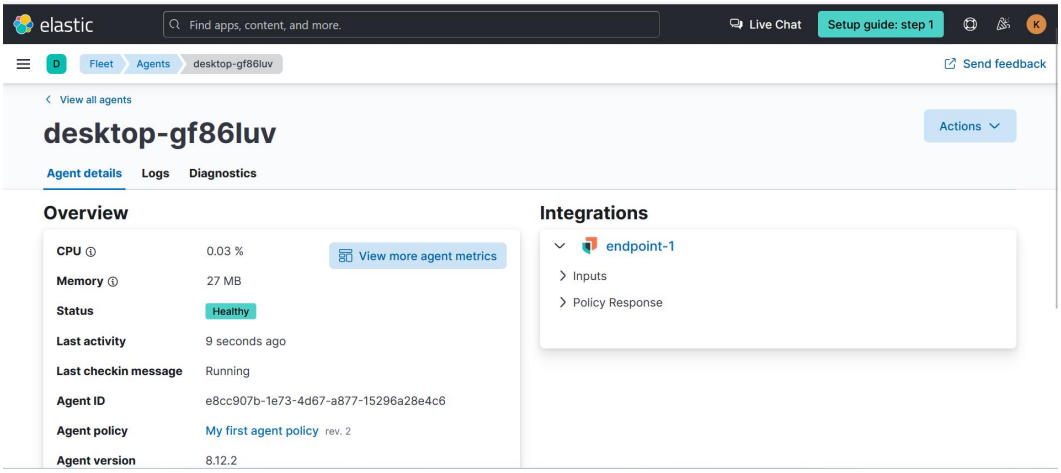
AQUI EN EL KALI, VAMOS A CAMBIARLE A LA POLÍTICA DE LINUX:



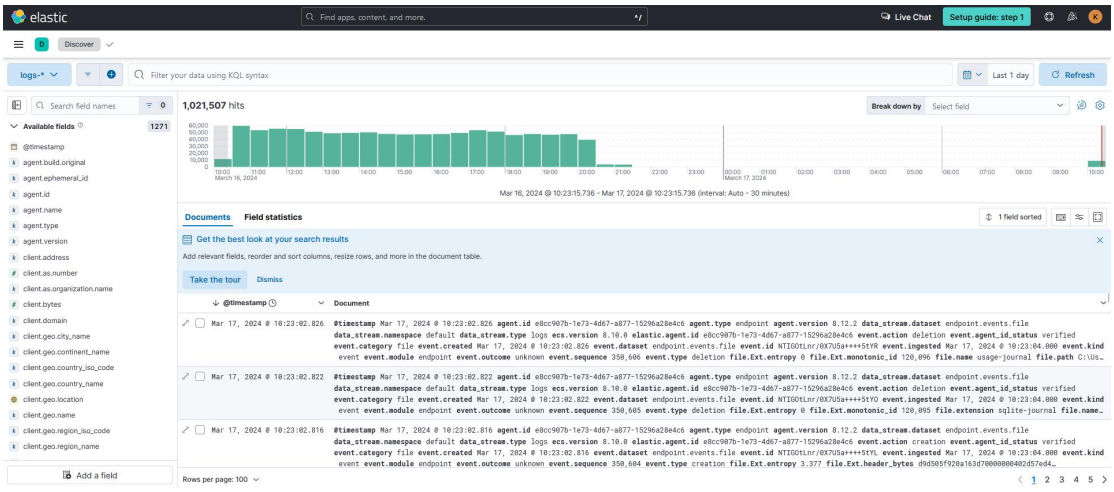
AQUI NOS RECOGE LOS LOGS DE SISTEMA Y LOS DE SURICATA SOLAMENTE PARA EL EQUIPO DE LA KALI



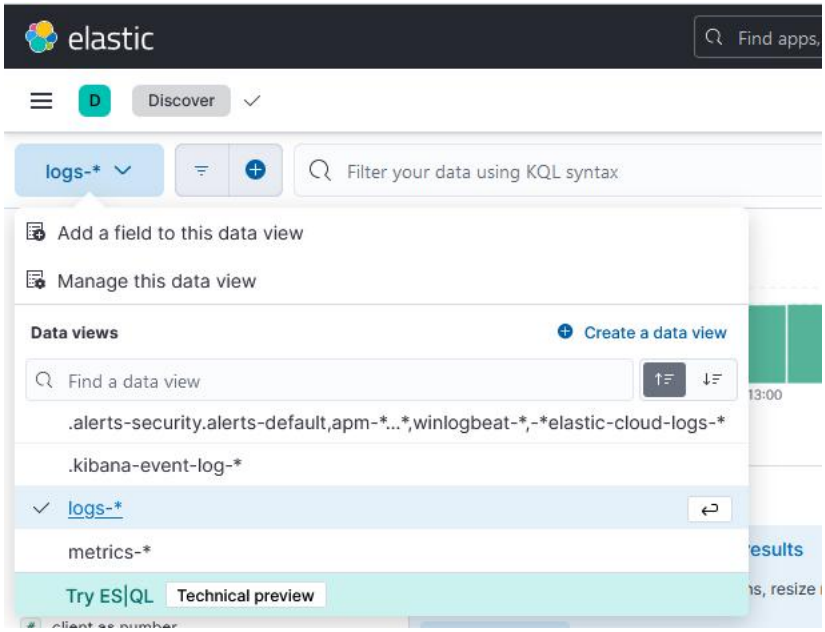
EL WINDOWS NOS ESTÁ RECOGIENDO LOGS DEL END-POINT



UNA VEZ YA TENEMOS CREADAS LAS POLITICAS, EN LA PARTE DE DISCOVER NOS APARECEN LOS LOGS QUE ESTAMOS RECOGIENDO



AQUI PODEMOS CREAR LOS CONJUNTOS DE DATOS QUE QUEREMOS VER



PARA VER LOS LOGS DE SURICATA, BUSCAMOS losgs-suricata*, PONEMOS LOS ULTIMOS 30 DIAS Y YA PODEMOS VER LOS EVENTOS DE SURICATA QUE ESTÁN RECOPILADOS EN EL SISTEMA