



PRACTICA

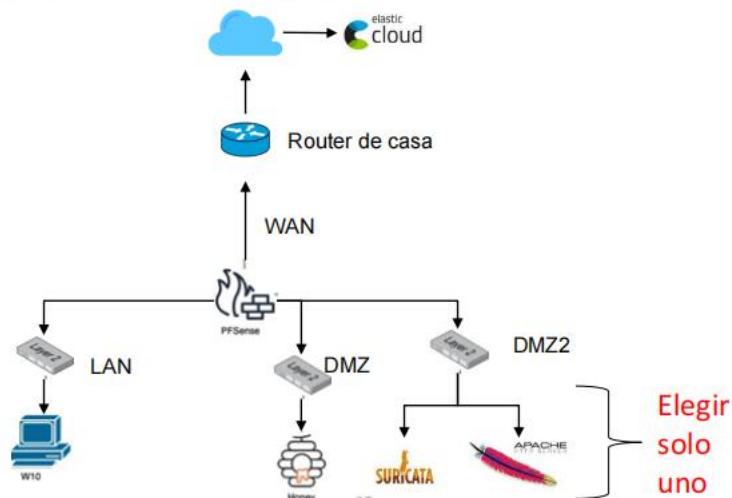
BLUE TEAM

ENRIQUE LOPEZ PACUAL



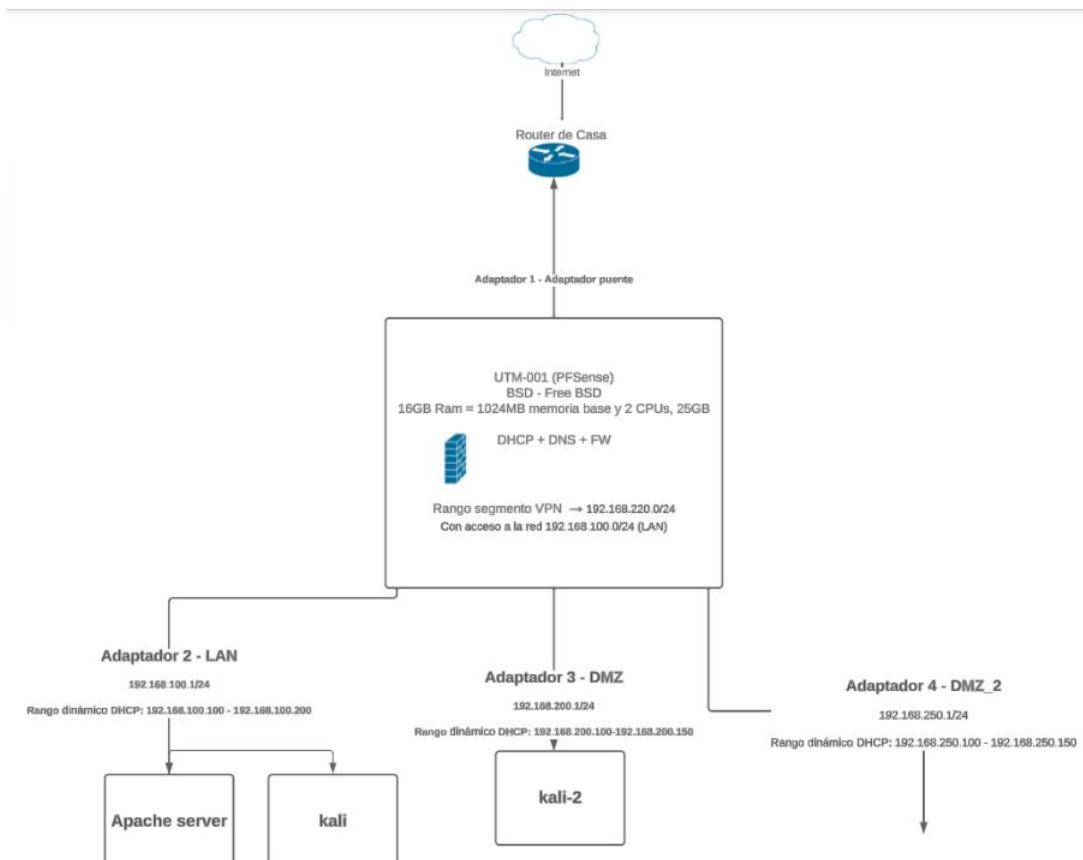
Enunciado

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 1	Adaptador 2	Adaptador 3	Adaptador 4
<input checked="" type="checkbox"/> Habilitar adaptador de red			
Conectado a: Adaptador puente			
Nombre: Intel(R) Wireless-AC 9560 160MHz			

ADAPTADOR 2-LAN:

Adaptador 1	Adaptador 2	Adaptador 3	Adaptador 4
<input checked="" type="checkbox"/> Habilitar adaptador de red			
Conectado a: Red interna			
Nombre: LAN			

ADAPTADOR 3-DMZ:

Adaptador 1	Adaptador 2	Adaptador 3	Adaptador 4
<input checked="" type="checkbox"/> Habilitar adaptador de red			
Conectado a: Red interna			
Nombre: DMZ			

ADAPTADOR 4-DMZ_2:

Adaptador 1	Adaptador 2	Adaptador 3	Adaptador 4
<input checked="" type="checkbox"/> Habilitar adaptador de red			
Conectado a: Red interna			
Nombre: 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:

Adaptador 1	Adaptador 2	Adaptador 3	Adaptador 4
<input checked="" type="checkbox"/> Habilitar adaptador de red			
Conectado a: Red interna			
Nombre: LAN			



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

The screenshot shows the pfSense setup wizard interface. At the top, there's a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title "Wizard / pfSense Setup /" is displayed. The main content area is titled "pfSense Setup" and contains the following text:
Welcome to pfSense® software!
This wizard will provide guidance through the initial configuration of pfSense.
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
pfSense® software is developed and maintained by Netgate®
A "Learn more" button is present, along with a "Next" button at the bottom.

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.

The screenshot shows the "General Information" setup screen. It includes fields for Hostname (UTM), Domain (keepcoding.local), and DNS servers (Primary: 127.0.0.1, Secondary: 1.1.1.1). There is also an "Override DNS" checkbox which is checked.

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.

The screenshot shows two configuration sections. The first section, "RFC1918 Networks", contains a "Block RFC1918 Private Networks" option with a description: "When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too." The second section, "Block bogon networks", contains a "Block bogon networks" option with a description: "When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received."



DENTRO DE LA **CONFIGURACION DE LAN** VAMOS A CAMBIAR EL RANGO DE DIRECCIONES, AHORA MISMO LAS 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

```
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 5b02127c1f2168bd40c1
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***
90/64
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.249/24
                           v6/DHCP6: 2a0c:5a81:b203:bf00:a00:27ff:febc:3e
LAN (lan)      -> em1          -> v4: 192.168.100.1/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
Enter an option: [
```

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)

General DNS Resolver Options

Enable Enable DNS resolver

DNS Query Forwarding Enable Forwarding Mode
If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).

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

```
(kali㉿kali)-[~]
$ ping mercadona.es
PING mercadona.es (35.201.121.112) 56(84) bytes of data.
64 bytes from 112.121.201.35.bc.googleusercontent.com (35.201.121.112): icmp_seq=1 ttl=116 time=6.75 ms
64 bytes from 112.121.201.35.bc.googleusercontent.com (35.201.121.112): icmp_seq=2 ttl=116 time=6.72 ms
64 bytes from 112.121.201.35.bc.googleusercontent.com (35.201.121.112): icmp_seq=3 ttl=116 time=6.84 ms
64 bytes from 112.121.201.35.bc.googleusercontent.com (35.201.121.112): icmp_seq=4 ttl=116 time=8.73 ms
^C
--- mercadona.es ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 6.719/7.260/8.731/0.850 ms
```

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.

Interfaces / LAN (em1)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	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 DISPOSITIVOS 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.

Primary Address Pool

Subnet	192.168.100.0/24
Subnet Range	192.168.100.1 - 192.168.100.254
Address Pool Range	From: 192.168.100.100 To: 192.168.100.200

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 FUERA CAPAZ DE HACER LA RESOLUCIÓN DE NOMBRES.

Server Options

WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.100.1
	1.1.1.1
	8.8.8.8



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

Other DHCP Options

Gateway The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.

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 ifconfig 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 NUESTRAS MAQUINAS KALI ESTAN 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

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (08:00:27:bc:3e:90)
LAN	em1 (08:00:27:1d:b5:3d)
Available network ports:	em2 (08:00:27:84:15:a0) + Add

Save

ESTAS INTERFACES DE RED SON LAS QUE PODEMOS VER EN LA PROPIA MAQUINA DE UTM (SI VAMOS A 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

Interfaces / Interface Assignments

Interface has been added.

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (08:00:27:bc:3e:90)
LAN	em1 (08:00:27:1d:b5:3d)
OPT1	em2 (08:00:27:84:15:a0)
OPT2	em3 (08:00:27:7b:6b:a6)

Save



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)

Interfaces / OPT1 (em2)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	DMZ
Enter a description (name) for the interface here.	
IPv4 Configuration Type	Static IPv4

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

Static IPv4 Configuration

IPv4 Address	192.168.200.1
/ 24	

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

Interfaces / OPT2 (em3)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	DMZ_2
Enter a description (name) for the interface here.	
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XX:XX:XX:XX:XX:XX
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xxxx:xxxx or leave blank.	
MTU	<input type="text"/>
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.	
MSS	<input type="text"/>
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.	
Speed and Duplex	<input type="text"/> Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.	

Static IPv4 Configuration

IPv4 Address	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.

```
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 5b02127c1f2168bd40c1

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

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.249/24
                           v6/DHCP6: 2a0c:5a81:b203:bf00:a00:27ff:febc:3e
90/64
LAN (lan)      -> em1          -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2          -> v4: 192.168.200.1/24
DMZ_2 (opt2)   -> em3          -> v4: 192.168.250.1/24

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

Enter an option: [
```

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

Primary Address Pool	
Subnet	192.168.200.0/24
Subnet Range	192.168.200.1 - 192.168.200.254
Address Pool Range	<input type="text" value="192.168.200.100"/> From <input type="text" value="192.168.200.150"/> To
The specified range for this pool must not be within the range configured on any other address pool for this interface.	

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

Server Options	
WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.200.1"/>
	<input type="text" value="1.1.1.1"/>
	<input type="text" value="8.8.8.8"/>

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

Other DHCP Options	
Gateway	<input type="text" value="192.168.200.1"/>
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.	



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

Primary Address Pool	
Subnet	192.168.250.0/24
Subnet Range	192.168.250.1 - 192.168.250.254
Address Pool Range	<input type="text" value="192.168.250.100"/> <input type="text" value="192.168.250.150"/> From To

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

Server Options	
WINS Servers	<input type="text" value="WINS Server 1"/> <input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.250.1"/> <input type="text" value="1.1.1.1"/> <input type="text" value="8.8.8.8"/>

EN LA GATEWAY 192.168.250.1

Other DHCP Options	
Gateway	<input type="text" value="192.168.250.1"/>

The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.

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 SERVIDOR 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).

Adaptador 1	Adaptador 2	Adaptador 3	Adaptador 4
<input checked="" type="checkbox"/> Habilitar adaptador de red			
Conectado a:	<input type="text" value="Red interna"/>		
Nombre:	<input type="text" value="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

The screenshot shows the Firewall configuration for the LAN interface. There are three rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/2.23 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓ 34/146.67 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom, there are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

PERO EN EL RESTO DE DMZ NO TENEMOS NADA.

The screenshot shows the Firewall configuration for the DMZ_2 interface. A message indicates that no rules are currently defined for this interface, and that all incoming connections will be blocked until pass rules are added. Clicking the 'Add' button will add a new rule.



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.

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Mar 13 11:46:31	DMZ	Default deny rule IPv4 (1000000103)	i 192.168.200.100:46962	i+ 1.1.1.53	UDP
✗	Mar 13 11:46:32	WAN	Default deny rule IPv4 (1000000103)	i 192.168.1.1	i+ 224.0.0.1	IGMP
✗	Mar 13 11:46:32	WAN	Default deny rule IPv6 (1000000105)	i [fe80::cab4:22ff:fe22:f3bc]	i+ [ff02::1]	Options
✗	Mar 13 11:46:33	WAN	Default deny rule IPv4 (1000000103)	i 192.168.1.34:9487	i+ 255.255.255.255:9478	UDP
✗	Mar 13 11:46:33	WAN	Default deny rule IPv4 (1000000103)	i 192.168.1.42:62232	i+ 255.255.255.255:161	UDP
✗	Mar 13 11:46:33	WAN	Default deny rule IPv4 (1000000103)	i 192.168.1.42:62233	i+ 255.255.255.255:161	UDP

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)

Firewall / Aliases / Edit

Properties

Name	webs	The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	PuertosWeb	A description may be entered here for administrative reference (not parsed).
Type	Port(s)	

Port(s)

Hint	Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.		
Port	80	HTTP	Delete
	443	HTTPS	Delete



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)

Edit Firewall Rule

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

EN INTERFACE PONEMOS DMZ, EN ADDRESS 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:

Edit Firewall Rule

Action	Pass			
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.				
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.			
Interface	DMZ			
Choose the interface from which packets must come to match this rule.				
Address Family	IPv4			
Select the Internet Protocol version this rule applies to.				
Protocol	TCP			
Choose which IP protocol this rule should match.				
Source				
Source	<input type="checkbox"/> Invert match	DMZ subnets		
<small>Display Advances</small>				
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.				
Destination				
Destination	<input type="checkbox"/> Invert match	Any		
Destination Address				
Destination Port Range	(other)	webs	(other)	webs
From Custom To Custom				

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.

Edit Firewall Rule

Action	Pass		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	DMZ		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	UDP		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	DMZ subnets	
<small>Display Advances</small>			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.			
Destination			
Destination	<input type="checkbox"/> Invert match	Any	
Destination Address			
Destination Port Range	DNS (53)	DNS (53)	From Custom To Custom



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.

```
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 192.168.200.100/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
    valid_lft 7193sec preferred_lft 7193sec
inet6 fe80::935c:3b70:121a:b502/64 scope link noprefixroute
```

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.

```
(kali㉿kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

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

Edit Firewall Rule

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

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

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

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: ICMP
Choose which IP protocol this rule should match.

ICMP Subtypes: any
Alternate Host
Datagram conversion error
Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source
Source: DMZ subnets
Invert match:

Destination
Destination: Any
Invert match:



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 PROTOCOLO: UDP, ORIGEN: ANY, DESTINO: PORT RANGE: from DNS(53) to DNS (53).

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	DMZ_2
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	UDP
Choose which IP protocol this rule should match.	
Source	
Source	<input type="checkbox"/> Invert match Any Source Address /
<input type="checkbox"/> display Advanced The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.	
Destination	
Destination	<input type="checkbox"/> Invert match Any Destination Address /
Destination Port Range	From: DNS (53) Custom To: DNS (53) Custom

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

[Firewall](#) / [Rules](#) / [Edit](#)

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	DMZ_2
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	ICMP
Choose which IP protocol this rule should match.	
ICMP Subtypes	any Alternate Host Datagram conversion error Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.	
Source	
Source	<input type="checkbox"/> Invert match DMZ subnets Source Address /
Destination	
Destination	<input type="checkbox"/> Invert match Any Destination Address /



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 SERVIDOR 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 ASIGNADA DE MANERA DINAMICA POR NUESTRO SERVIDOR DE DHCP.

IP Address	MAC Address	Hostname	Description	Start	End	Actions
192.168.100.100	08:00:27:21:b1:d0	kali		2024/03/14 08:45:39	2024/03/14 10:45:39	Edit Delete

Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	192.168.100.100	192.168.100.200	1	101	0% of 101

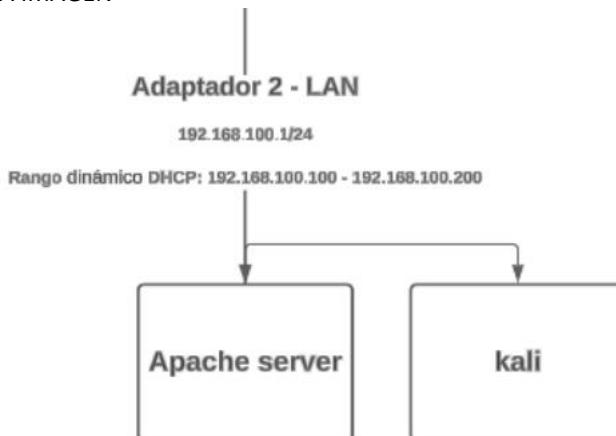
PUEDE SER UTIL PARA ADEMÁS DE ESTABLECER DIRECCIONES IP FIJAS, TAMBIEN ESTABLECER UN MATCH ENTRE UNA DIRECCION MAC Y UNA IP PARA AÑADIR UNA CAPA EXTRA DE SEGURIDAD.

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

Static DHCP Mapping on LAN

DHCP Backend	ISC DHCP
MAC Address	08:00:27:21:b1:d0
MAC address of the client to match (6 hex octets separated by colons).	
Client Identifier	
An optional identifier to match based on the value sent by the client (RFC 2132).	
IP Address	192.168.100.99
IPv4 address to assign this client.	
Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool. The same IP address may be assigned to multiple mappings.	
ARP Table Static Entry	<input checked="" type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair.
Hostname	kali
Name of the client host without the domain part.	
Description	Establecimiento estatico de IP
A description for administrative reference (not parsed).	

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 NUESTRO SERVIDOR DE APACHE, PARA ELLO HACEMOS UN sudo service apache2 start

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

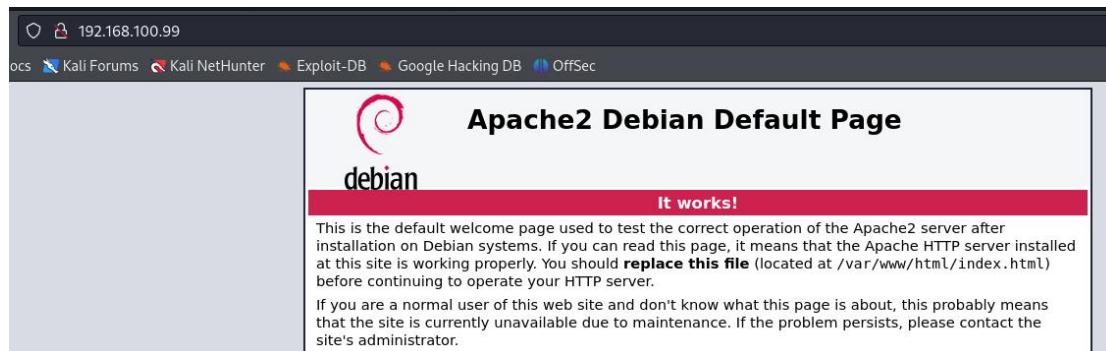
SI AHORA HACEMOS UN sudo service apache2 status DEBERIAMOS VER QUE ESTA CORRIENDO.

```
(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

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 CONTACTO CON EL ROUTER DE NUESTRA CASA, LA PETICION VA A IR AL ROUTER DE NUESTRA CASA Y DE AHÍ 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 INTERFAZ 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 PORT custom 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

Edit Redirect Entry

Disabled	<input type="checkbox"/> Disable this rule
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface	WAN
Address Family	IPv4
Protocol	TCP
Source	Display Advanced
Destination	<input type="checkbox"/> Invert match. WAN address / Address/mask
Destination port range	Other 80 Other 80 From port Custom To port Custom Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP	Address or Alias 192.168.100.99 Type Address Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope (:1)
Redirect target port	Other 80 Port Custom

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.

The screenshot shows a web browser window with the URL 192.168.1.53. The page title is "Apache2 Debian Default Page". It features the Debian logo and the text "It works!". Below this, there is a message about the default welcome page and instructions for maintenance. The browser's address bar and some status icons are visible at the top.

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.



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

VAMOS A GENERAR LOS CERTIFICADOS PARA LA CONEXIÓN 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 LOS CERTIFICADOS DE NUESTRA VPN, LE DAMOS A add Y EN DESCRIPTIVE NAME: Keepcoding, METHOD: create an internal Cert Auth, KEY TYPE: rsa 2048, DIGEST ALGORITHM: sha256, LIFETIME: 365, COMMON NAME: Keepcoding, COUNTRY CODE: ES, STATE OR PROVINCE: Madrid, CITY: 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).

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name VPN
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, '

Internal Certificate

Certificate authority Keepcoding

Key type RSA

Key length 2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 365
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name vpn.keepcoding.local
The following certificate subject components are optional and may be left blank.

Country Code ES

State or Province Madrid

City Madrid

Organization Keepcoding

Organizational Unit IT

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add SAN Row + Add SAN Row



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 OSURIDAD, 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 CONECCCTIONS (GENTE QUE SE PUEDE CONECTAR A LA VEZ): 10

General Information	
Description	<input type="text" value="VPN-Remota-LAN"/> A description of this VPN for administrative reference.
Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.
Mode Configuration	
Server mode	<input type="text" value="Remote Access (SSL/TLS + User Auth)"/>
Backend for authentication	<input type="text" value="Local Database"/>
Device mode	<input type="text" value="tun - Layer 3 Tunnel Mode"/> "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration	
Protocol	<input type="text" value="UDP on IPv4 only"/>
Interface	<input type="text" value="WAN"/> The interface or Virtual IP address where OpenVPN will receive client connections.
Local port	<input type="text" value="4194"/> The port used by OpenVPN to receive client connections.
Cryptographic Settings	
TLS Configuration	<input checked="" type="checkbox"/> Use a TLS Key



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. [i](#)

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
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)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. [i](#)

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



Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	192.168.100.0/24 IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
IPv6 Local network(s)	<input type="checkbox"/> IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent connections	10 Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	Refuse any non-stub compression (Most secure) <input type="checkbox"/> Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.
Asymmetric compression allows an easier transition when connecting with older peers.	
Push Compression	<input type="checkbox"/> Push the selected Compression setting to connecting clients.
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	<input type="checkbox"/> Allow communication between clients connected to this server
Duplicate Connection	<input type="checkbox"/> Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

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

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	kike
Password	●●●●●
Full name	kike User's full name, for administrative information only
Expiration date	<input type="text"/> Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	admins Not member of
<input type="button" value="Move to 'Member of' list"/> <input type="button" value="Move to 'Not member of' list"/> Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate
Create Certificate for User	
Descriptive name	kike
Certificate authority	Keepcoding



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 client export.

The screenshot shows the 'OpenVPN / Client Export Utility' window. At the top, there's a navigation bar with tabs: Server, Client, Client Specific Overrides, Wizards, and Client Export. The 'Client Export' tab is currently active. Below the navigation bar, there's a dropdown menu labeled 'Remote Access Server' with the option 'VPN-Remota-LAN UDP4:4194' selected. The main area of the window is currently empty, indicating no specific configuration or export steps are being performed at this moment.

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

The screenshot shows the 'OpenVPN Server' interface. At the top, there's a header bar with the title 'OpenVPN Server'. Below it, a dropdown menu is open under the heading 'Remote Access Server', showing the option 'VPN-Remota-LAN UDP4:4194'.

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

The screenshot shows the 'OpenVPN Clients' interface. It lists a single user entry: 'User' is 'kike' and 'Certificate Name' is 'kike'. To the right of this entry, there is a large panel titled 'Export' containing several download links:

- Inline Configurations:
 - [Most Clients](#)
 - [Android](#)
 - [OpenVPN Connect \(iOS/Android\)](#)
- Bundled Configurations:
 - [Archive](#)
 - [Config File Only](#)
- Current Windows Installers (2.6.7-ix001):
 - [64-bit](#)
 - [32-bit](#)
- Previous Windows Installers (2.5.9-ix601):
 - [64-bit](#)
 - [32-bit](#)
- Legacy Windows Installers (2.4.12-ix601):
 - [10/2016/2019](#)
 - [7/8/8.1/2012r2](#)
- Viscosity (Mac OS X and Windows):
 - [Viscosity Bundle](#)
 - [Viscosity Inline Config](#)

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.

```
1 dev tun
2 persist-tun
3 persist-key
4 data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305:AES-256-CBC
5 data-ciphers-fallback AES-256-CBC
6 auth SHA256
7 tls-client
8 client
9 resolv-retry infinite
10 remote 192.168.1.53 4194 udp4
11 nobind
12 verify-x509-name "vpn.keepcoding.local" name
13 auth-user-pass
14 remote-cert-tls server
15 explicit-exit-notify
16
17 <ca>
18 -----BEGIN CERTIFICATE-----
19 MIIEjCCAwgAwIBAgIIUdK7wqd7YwDQYJKoZIhvCNQELBQAwZjETMBEGA1UE
20 AxMKS2cLcGhNzGluZzELMAkGA1UEBhMCRVMx0zANBgNVBAgTBk1hZhJpZDEPMA0G
21 A1UEBhxtGTFkcm1kMRMwE0YDVQKewpLZWVwv29kaW5nQswCQYDVQQLejJVDae
22 Fw0yNDAzMjTywDUwMDNaIaMGYxEzARBgNVBAMTClktLXBj
23 b2Rpbmcc2aJBgNVBAYTAkTMQ8wDQYDVQKIEwZNYWRyaWQxDZAnBgNVBacTBk1h
24 ZHJpZDETMBeGA1UEChMkSzVLcGhZGluZzELMAkGA1UECxMSVqggE1MA0GCSqG
25 SIb3DQEBAQUA4IBDwAwggEKAIBAQ3RSenYxufFdQuq1BALksCvdzaYRZE+
26 gBbLnP2CP/GyEsA1J7qI8QnbUX5okqddGEFE4kVQcKOPYwzyabPu1rGppHonV
27 0cd791jh4vbuuRqyXapws9wFE13JcM7EUxuzRBokNRkLTfFLuwWDGtdL/Ghj3c
28 oiedtTBhp+6S4+jau54v9ZuaajbEg1IGVcm2RlztfEdHo7fsXBkWnZ1XLBMg0
29 EDWbznl7960b3SBvU6HomoBkW2eTzJ6bInCW8jThu/bh9TAo0e3/dPbONG6lud
30 MnL975fwgHNjkjpAd6HkzlBuCnVP0Ny0XopZHjri+TOWXAgMBAAGjgdcw
31 gdQWhQDVROOBByFgtDhp02>/N/0eSMBMLjsNgkXW0WqkaDbmMRlwEQYDVOQDewpLZWVwY29kaW5n
32 FGtdhp02>/N/0eSMBMLjsNgkXW0WqkaDbmMRlwEQYDVOQDewpLZWVwY29kaW5n
33 MQswCQYDVQGEmJFUzEPMA0GAI1UECBMTWFkcm1kMQ8wDQYDVQHewZNYWRyaWQx
34 EzARBgNVBAoTCKtlzBjb2Rpbmcc2aJBgNVAsTAKlughR38rDvc3tjAMBgNV
35 HMEBTADQH/MA5GA1UdDwQEAwIBBjANBgqhkiG9w0BAQsfAAOCAGEALdjhWnRp
36 7Mjb1FOTTXIBCL1ix3fIMtaFpbUlyViZta8kfQy9NVqr31YeyjDvjkEyKdh
37 KE9y7JyDUv9PlbyocxL2P5GFxHA16gil19f8ipNNe20hE31lwVVGKhLYvsDR
38 AetYG5kxPcZZ0XLR120eCNPSzCJmjiaS6Lv2kZXYL5TYjy1N+RHxAcxix+8WZ
39 PmxZN1owIy77UJTeMigj8iWgmy0kVBFoIVJk3nPq0gdc63bH5i4SygN2zjH
40 h9EXGox/+5pDwjb59qBACjP88ybg1VWkv4eu970I7vNgkqIoqC1g15VzR2e19c
41 ze3Kc+kx1ctyqg=
42 -----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.

```
2 persist-tun
3 persist-key
4 data-ciphers AES-256-GCM: AES-128-GCM: CHACHA20-POLY1305: AES-256-CBC
5 data-ciphers-fallback AES-256-CBC
6 auth SHA256
7 tls-client
8 client
9 resolv-retry infinite
10 remote 192.168.1.53 4194 udp4
11 nobind
12 verify-x509-name "vpn.keepcoding.local" name
13 auth-user-pass
14 remote-cert-tls server
15 explicit-exit-notify
16
17 <ca>
18 -----BEGIN CERTIFICATE-----
19 MIIEJJCCA...gAwIBAgIIUd/Kw7wqd7YwDQYJKoZIhvcNAQELBQA...ZjETMBEGA1UE
20 AxMKS2V1cGNvZGluZzELMAkGA1UEBhMCRVMx...DzANBgNVBAgTBk1hZHJpZDEPMA0G
21 A1UEBxMGTWFKcm1kMRMwEQYDVQQKEwpLZWVwY29kaW5nMQswCQYDVQQLEwJJVDAe
22 Fw0yNDAzMTYwODUwMDNaFw0yNTAzMTYwODUwMDnaMGYxEzARBgNVBAMTCkt1ZX Bj
23 b2Rp...mcx...CzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZNYWRya...QxDzANBgNVBAcTBk1h
24 ZHJpZDETMBEGA1UEChMKS2V1cGNvZGluZzELMAkGA1UECxMCSVQwggEiMA0GCSqG
25 SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC3RSenYXnuFfdQuGmIBALksNCvdZaYRZE+
26 gBbLnp2CP/GyEsAIJ7qO18QNbUX5okqddGEFE4kVMQcKOPYwzYaBPu1rGppHonqV
27 0cd791jhC4vb4uqRyPxapWs9wrEI3JcM7EUxuzRBokNRkLtFFLuuwWDGtdL/GHj3c
28 oiedtTBH...p+GS4+jau54v9ZuaaJbEgT1IGvCm2RlztfEdHo7fsXBkWnZK1XLBM...yGO
29 EDWbzn17960b3SbVu6H6nm...oBkW2eTZJ6bInCwv8jTHu/hb9TA0e03/dPb0N6Dlud
30 MnLt975fweWgHNjkjpAd6Hkz1kBwCYnVP0Ny0XopVZHjri+TBOWXA...gMBAAGjgd...cw
```

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

OpenVPN Connect — X

< Imported Profile

Profile Name
192.168.1.53 [kike]

Server Hostname (locked)
192.168.1.53

Username

Save password

PROFILES CONNECT

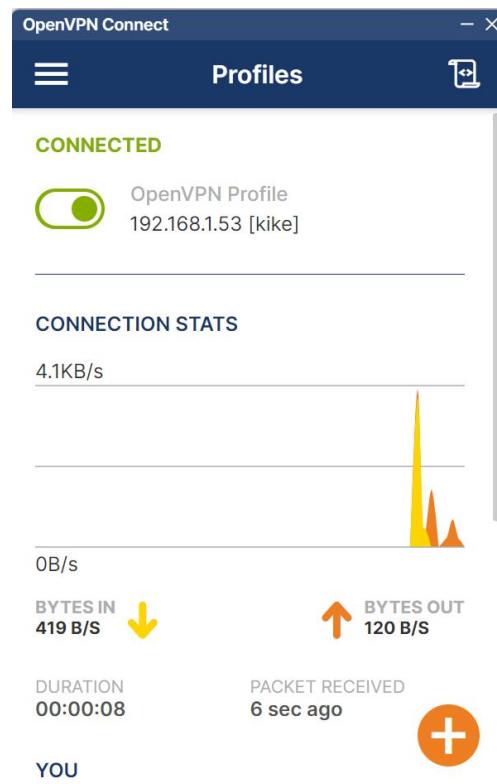


VAMOS AL PFSENSE firewall-rules Y EN LA WAN (BARRA DE ARRIBA) AÑDIMOS UNA NUEVA REGLA DE FIREWALL. ACTION: PASS, INTERFACE: WAN, ADDRESS FAMILY: IPV4, PROTOCOL: UDP, SOURCE(ORIGEN): ANY, DESTINATION: custom 4194 custom 4194(PUERTO QUE HEMOS CONFIGURADO EN NUESTRA VPN), DESCRIPTION: Reagla WAN VPN.

Edit Firewall Rule

Action	Pass				
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.					
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.				
Interface	WAN				
Choose the interface from which packets must come to match this rule.					
Address Family	IPv4				
Select the Internet Protocol version this rule applies to.					
Protocol	UDP				
Choose which IP protocol this rule should match.					
Source					
Source	<input type="checkbox"/> Invert match	Any	Source Address	/	v
Display Advanced The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.					
Destination					
Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	v
Destination Port Range	(other)	4194	(other)	4194	Custom
From	Custom	To	Custom		

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 Y NO 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 PODER ACCEDER A LA KALI.

Edit Firewall Rule

Action	Pass		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	OpenVPN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	Any		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	Any	Source Address /
Destination			
Destination	<input type="checkbox"/> Invert match	Any	Destination Address /

192.168.1.53

Tube Maps Gmail 2:51 Reproduciendo RESOLUCIÓN DE MET...

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

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 HONEYBOT QUE VAMOS A LANZAR EN DMZ ES EL COWRIE "SSH" A TRAVÉS EL DOCKER

```
(kali㉿kali)-[~]
└─$ sudo docker run -p 222:2222 cowrie/cowrie
[sudo] password for kali:
[cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:106: CryptographyDeprecationWarning: Blowfish has been deprecated
  b'blowfish-cbc': (algorithms.Blowfish, 16, modes.CBC),
[cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning: CAST5 has been deprecated
  b'cast128-cbc': (algorithms.CAST5, 16, modes.CBC),
[cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:115: CryptographyDeprecationWarning: Blowfish has been deprecated
  b'blowfish-ctr': (algorithms.Blowfish, 16, modes.CTR),
[cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:116: CryptographyDeprecationWarning: CAST5 has been deprecated
  b'cast128-ctr': (algorithms.CAST5, 16, modes.CTR)
2024-03-16T11:08:16+0000 [-] Python Version 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0]
2024-03-16T11:08:16+0000 [-] Twisted Version 23.10.0
2024-03-16T11:08:16+0000 [-] Cowrie Version 2.5.0
2024-03-16T11:08:16+0000 [-] Loaded output engine: jsonlog
2024-03-16T11:08:16+0000 [twisted.scripts.twistd.unix.UnixAppLogger#info] twistd 23.10.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.
2024-03-16T11:08:16+0000 [twisted.scripts.twistd.unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2024-03-16T11:08:16+0000 [-] CowrieSSHFactory starting on 2222
2024-03-16T11:08:16+0000 [-] CowrieSSHFactory starting on 2222
2024-03-16T11:08:16+0000 [-] Generating new RSA keypair...
2024-03-16T11:08:16+0000 [-] Generating new ECDSA keypair...
2024-03-16T11:08:16+0000 [-] Generating new ed25519 keypair...
2024-03-16T11:08:16+0000 [-] Ready to accept SSH connections
|
```

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 ANFITRÍON Y EL DE LA DERECHA DEL INVITADO.

CON docker ps VEMOS QUE TENEMOS EL CONTENEDOR CORRIENDO

```
(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS               NAMES
28bcebd52932        cowrie/cowrie      "/cowrie/cowrie-env/..."   31 minutes ago    Up 31 minutes   2223/tcp, 0.0.0.0:222→2222/tcp, ::222→2222/tcp   vibrant_neumann
```

EL QUE TENEMOS CORRIENDO ES EL QUE HEMOS PUESTO QUE SIMULA UN HONEYBOT 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.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.1.50  netmask 255.255.255.0  broadcast 192.168.1.255
      inet6 fe80::935c:3b70:121a:b502  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
          RX packets 116173  bytes 118923180 (113.4 MiB)
          RX errors 0  dropped 14  overruns 0  frame 0
          TX packets 65126  bytes 38758086 (36.9 MiB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

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.

```
C:\Users\Usuario>ssh -p 222 root@192.168.1.50
The authenticity of host '[192.168.1.50]:222 ([192.168.1.50]:222)' can't be established.
ED25519 key fingerprint is SHA256:PKeSTgHLNW6hcRJ2AeYqmw0/GL9D7Cq8t4YcUxNES4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.50]:222' (ED25519) to the list of known hosts.
root@192.168.1.50's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~#
```



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:/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/rdp

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

```

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 rdp/** AQUI ESTAN LOS LOGS DEL HONEYBOT.

```
(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.log
bash-4.4# 
```



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

```
bash-4.4# tail -f rdp.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

Welcome to Elastic Cloud

Introducing serverless preview!

Hosted deployments

Deployment	Status	Version	Cloud provider & regi...	Actions
kike-keepcoding	Healthy	8.12.2	AWS - Ireland (eu-...)	Open Manage

Create deployment

Role-based access control

Assign roles to members and API keys

Manage members, API keys, and implement fine-grained access control all in one place from the Organization page. Learn more

Skip tour Take me there

Modernizing financial services: A deep dive into Elastic Cloud on AWS for Observability, Security, and more MARCH 8, 2024 New!

Machine learning vs. AI: Understanding the differences MARCH 7, 2024 New!

Community

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.

Integrations Elastic Defend

Elastic Defend

Elastic Agent

Version 8.12.0 Agent policies 1 Add Elastic Defend

Elastic Defend Integration

Requirements

Permissions root privileges

AQUI VAMOS A DETECT THREATS IN MY DATA WITH SIEM

What would you like to do first?

Filter by solution to see related use cases

Search Observability Security

Detect threats in my data with SIEM 1 of 3 steps complete

Secure my hosts with endpoint security

Secure my cloud assets with cloud security posture management (CSPM)



AHORA LE DAMOS A ADD INTEGRATION, AQUI YA LO QUE ESTAMOS HACIENDO ES RECOLPILAR 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:

The screenshot shows the 'Logs' tab for the 'kali' agent. It includes a search bar, filter options for dataset (1), log level (4), and time (Last 1 day), and a 'Open in Logs' button. The main table lists log entries with columns for Timestamp, event.dataset, and Message. The log entries show the elastic_agent starting up, upgrading, and gathering system information.

Timestamp	event.dataset	Message
09:25:03.487	elastic_agent	[elastic_agent][info] Elastic Agent started
09:25:03.786	elastic_agent	[elastic_agent][info] Starting upgrade watcher
09:25:03.789	elastic_agent	[elastic_agent][info] Upgrade Watcher invoked
09:25:03.790	elastic_agent	[elastic_agent][info] releasing watcher 695
09:25:03.790	elastic_agent	[elastic_agent][info] APM instrumentation disabled
09:25:03.792	elastic_agent	[elastic_agent][info] Gathered system information
09:25:04.086	elastic_agent	[elastic_agent][info] Upgrade Watcher started
09:25:04.088	elastic_agent	[elastic_agent][info] update marker not present at '/opt/Elastic/Agent/data'

AQUI PODEMOS VER LOS LOGS DE WINDOWS:

The screenshot shows the 'Logs' tab for a Windows agent named 'desktop-gf86luv'. It includes a search bar, filter options for dataset (1), log level (4), and time (Last 1 day), and a 'Open in Logs' button. The main table lists log entries with columns for Timestamp, event.dataset, and Message. The log entries show the elastic_agent checking in with the fleet-server and handling transient errors.

Timestamp	event.dataset	Message
Mar 16, 2024		
04:28:33.047	elastic_agent	[elastic_agent][warn] Possible transient error during checkin with fleet-server, retrying
04:28:33.072	elastic_agent	[elastic_agent][warn] Component state changed endpoint-default (HEALTHY->DEGRADED): Degraded : endpoint service missed 1 check-in
04:29:03.014	elastic_agent	[elastic_agent][info] Component state changed endpoint-default (DEGRADED->HEALTHY): Healthy: communicating with endpoint service
04:30:11.574	elastic_agent	[elastic_agent][info] signal "terminated" received
04:30:11.575	elastic_agent	[elastic_agent][info] Shutting down Elastic Agent and sending last events...
04:30:11.576	elastic_agent	[elastic_agent][warn] Possible transient error during checkin with fleet-server, retrying
04:30:11.578	elastic_agent	[elastic_agent][error] checkin retry loop was stopped
04:30:11.578	elastic_agent	[elastic_agent][error] failed accept conn info connection: accept tcp 127.0.0.1:6788: use of closed network connection
04:30:11.579	elastic_agent	[elastic_agent][info] stopping endpoint service runtime
04:30:11.801	elastic_agent	[elastic_agent][info] Shutting down completed.
04:30:11.804	elastic_agent	[elastic_agent][info] Stopping server
04:30:11.804	elastic_agent	[elastic_agent][info] Stats endpoint (127.0.0.1:6791) finished: accept tcp 127.0.0.1:6791: use of closed network connection

AQUI EN EL FLEET VEMOS LAS POLITICAS QUE TENEMOS:

The screenshot shows the 'Agents' tab in the Fleet section. It includes a search bar, filter options for Status (4), Tags (0), Agent policy (2), and Upgrade available, and buttons for 'Agent activity', 'Add Fleet Server', and 'Add agent'. The main table lists agents with columns for Status, Host, Agent policy, CPU, Memory, Last activity, Version, and Actions. Three agents are listed: 'kali' (Healthy, My first agent policy rev. 2), 'desktop-gf86luv' (Healthy, My first agent policy rev. 2), and '35fff895cd0d' (Offline, Elastic Cloud agent policy rev. 5).

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kali	My first agent policy rev. 2	0.20 %	27 MB	16 seconds ago	8.12.2	...
Healthy	desktop-gf86luv	My first agent policy rev. 2	0.03 %	27 MB	19 seconds ago	8.12.2	...
Offline	35fff895cd0d	Elastic Cloud agent policy rev. 5	N/A	N/A	21 seconds ago	8.12.2	...



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

My first agent policy

Name	Integration	Namespace	Actions
endpoint-1	Elastic Defend v8.12.0	default	⋮

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

Fleet

Name	Description	Last update...	Agents	Integrations	Actions
My first agent policy rev. 2		Mar 08, 2024	2	1	⋮
Elastic Cloud agent policy rev. 5	Default agent policy for agents hosted on Elastic Cloud	Mar 08, 2024	1	2	⋮

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.

[View details.](#)

Agent monitoring

Collecting monitoring logs and metrics will also create an **Elastic Agent** integration. Monitoring data will be written to the default namespace specified above.

Collect agent logs

Collect agent metrics



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

Fleet

Centralized management for Elastic Agents.

Agents **Agent policies** Enrollment tokens Uninstall tokens Data streams Settings

Filter your data using KQL syntax		Reload	Create agent policy		
Name	Description	Last update...	Agents	Integrations	Actions
Linux rev. 1		Mar 16, 2024	0	1	...
My first agent policy rev. 2		Mar 08, 2024	2	1	...
Elastic Cloud agent policy rev. 5	Default agent policy for agents hosted on Elastic Cloud	Mar 08, 2024	1	2	...

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

View all agent policies		Revision	Integrations	Agents	Last updated on	Actions
My first agent policy		2	1	2 agents	Mar 08, 2024	...
Integrations Settings						Add integration
Name	Integration	Namespace	Actions			
endpoint-1	Elastic Defend v8.12.0	default	...			

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.

The screenshot shows the Elastic Stack interface with the 'Suricata' integration page. The top navigation bar includes the Elastic logo, a search bar, and various links like 'Live Chat', 'Setup guide: step 1', and 'Connection details'. Below the navigation, there's a breadcrumb trail: 'Back to integrations' → 'Suricata'. The main content area features a large image of a Suricata logo, the title 'Suricata' with a 'Elastic Agent' tag, and a 'Version 2.21.0' badge. There are tabs for 'Overview', 'Settings', 'Configs', and 'API reference', with 'Overview' being the active tab. A 'Suricata Integration' section is shown, along with 'Screenshots' and a '1 of 2' indicator. At the bottom right, there's a 'Add Suricata' button.

VAMOS A PONERLA EN LA POLITICA DE LINUX

The screenshot shows the 'Where to add this integration?' configuration page. It has a step number '2' and the question 'Where to add this integration?'. Below this, there are two tabs: 'New hosts' (disabled) and 'Existing hosts' (selected). Under 'Agent policy', there's a dropdown menu set to 'Linux'. A note below the dropdown states: 'Agent policies are used to manage a group of integrations across a set of agents.' To the right of the dropdown, it says '0 agents are enrolled with the selected agent policy.' At the bottom right of the page, there's a 'Next Step' button.



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

The screenshot shows a modal dialog titled "Suricata integration added". It contains the message: "To complete this integration, add **Elastic Agent** to your hosts to collect data and send it to Elastic Stack." Below the message are two buttons: "Add Elastic Agent later" and "Add Elastic Agent to your hosts". At the bottom of the dialog are tabs for "New hosts" and "Existing hosts".

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

The screenshot shows a modal dialog titled "Assign new agent policy". It asks to choose a new agent policy for the selected agent. The "Agent policy" dropdown is set to "Linux". Below it, it says "The selected agent policy will collect data for 2 integrations: System, Suricata". At the bottom are "Cancel" and "Assign policy" buttons. The background shows the "kali" agent details page in the Fleet interface.

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

The screenshot shows the "kali" agent details page. The "Agent details" tab is selected. The "Overview" section displays metrics like CPU (0.13 %), Memory (27 MB), and Status (Healthy). The "Integrations" section shows two entries: "system-1" and "suricata-1", both with "Inputs" listed under them.



EL WINDOWS NOS ESTÁ RECOGIENDO LOGS DEL END-POINT

The screenshot shows the Elastic Fleet interface. At the top, there's a search bar with the placeholder "Find apps, content, and more." and a "Live Chat" button. Below the header, a breadcrumb navigation shows "Fleet > Agents > desktop-gf86luv". On the right, there are "Send feedback" and "Actions" buttons.

Agent details Logs Diagnostics

Overview

CPU ⓘ	0.03 %
Memory ⓘ	27 MB
Status	Healthy
Last activity	9 seconds ago
Last checkin message	Running
Agent ID	e8cc907b-1e73-4d67-a877-15296a28e4c6
Agent policy	My first agent policy rev. 2
Agent version	8.12.2

Integrations

- endpoint-1
 - Inputs
 - Policy Response

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



AQUI PODEMOS CREAR LOS CONJUNTOS DE DATOS QUE QUEREMOS VER

The screenshot shows the Elastic Stack interface with the 'Discover' tab selected. A search bar at the top right says 'Find apps, content, and more'. Below it, a search bar for 'KQL syntax' is present. A button 'Create a data view' is visible. The main area shows a list of index patterns: '.alerts-security.alerts-default', '.apm-*', '.winlogbeat-*', '.elastic-cloud-logs-*', '.kibana-event-log-*', 'logs-*' (which is selected and highlighted in blue), and 'metrics-*'. A 'Try ES|QL' button is at the bottom left, followed by a 'Technical preview' link.

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

The screenshot shows the Elastic Stack interface with the 'Discover' tab selected. A search bar at the top right says 'Find apps, content, and more'. Below it, a search bar for 'KQL syntax' is present. A button 'Last 30 days' is visible. The main area shows a histogram with '87,075 hits' and a timestamp range from 'Feb 16, 2024 01:00:00:00.000' to 'Mar 17, 2024 01:00:00:00.000'. Below the histogram, there's a 'Field statistics' section with a table showing document counts for various fields like '@timestamp', 'agent.id', etc. The table has columns 'Document' and 'Count'.

ENRIQUE LOPEZ PASCUAL
BLUE TEAM

43

