

PRÁCTICA

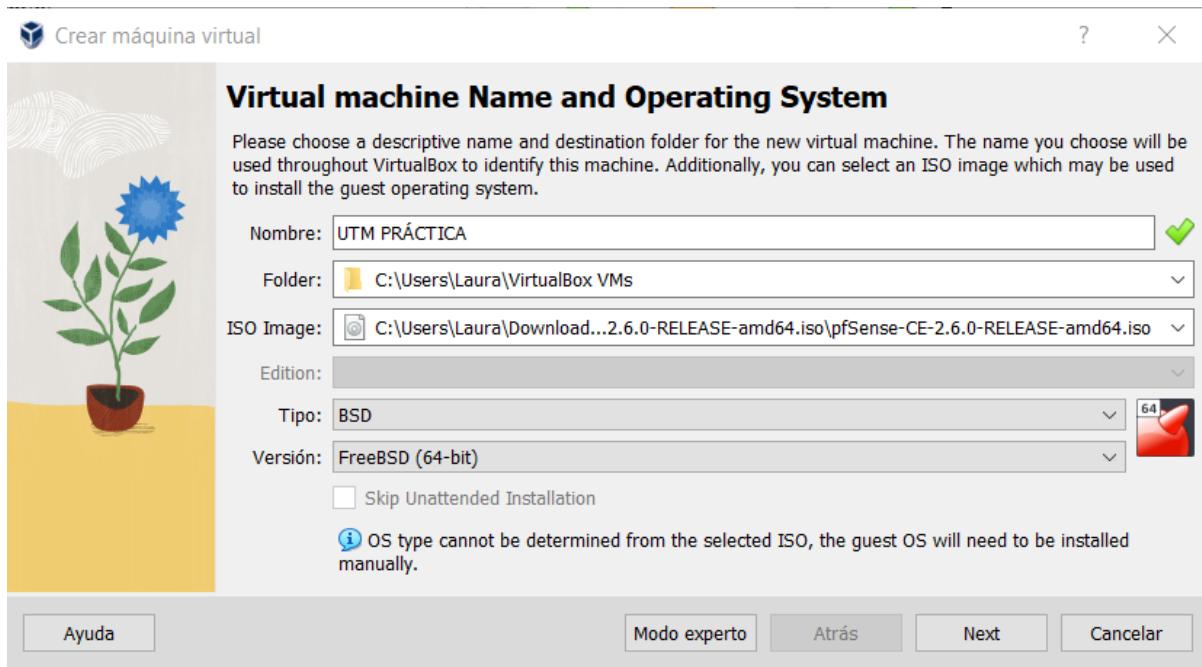
BLUETEAM

Laura Quijorna Velázquez
Abril de 2023

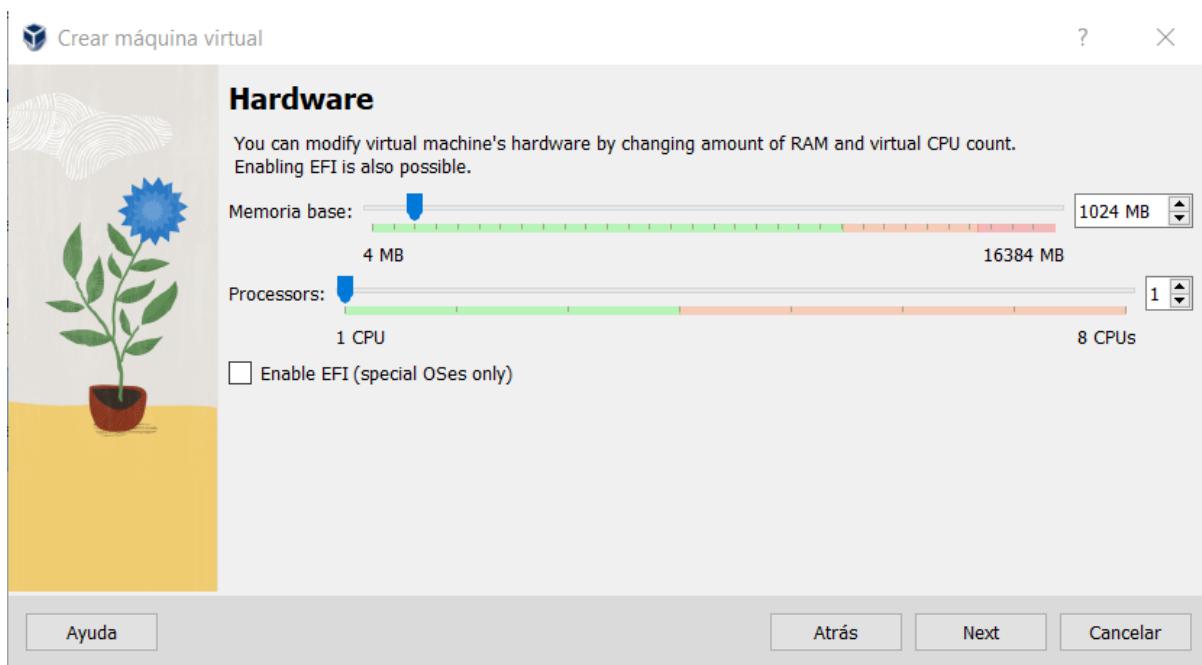
La práctica que se presenta a continuación describe el montaje de una infraestructura de red con PFsense y creación de un servidor VPN para posteriormente a través de un honeypot dar entrada a conexiones de ciberatacantes que serán registradas a través de un suricata y visualizadas a través de un Elastic Agent.

Creación de mi infraestructura en PFSENSE

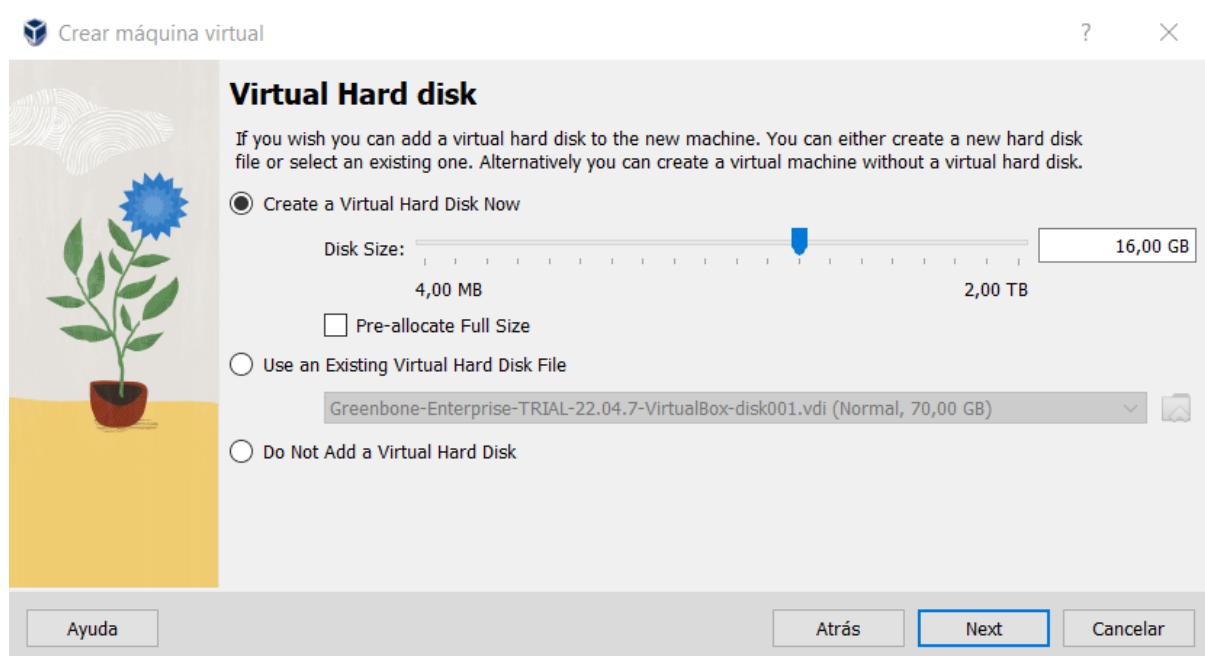
Primero descargo pfsense y creo mi máquina en Virtual Box. Para ello, pincho en “nueva”, pongo el nombre de la máquina, en mi caso la llamaré UTM PRÁCTICA. Despues selecciono donde lo voy a guardar, cargo la iso, selecciono en tipo la opción BSD y en versión la FreeBSD (64-bit). Hago click en Next.



Ahora selecciono cuánto le voy a dar de memoria ram y procesamiento. Lo dejaré como viene por defecto. Pincho Next.

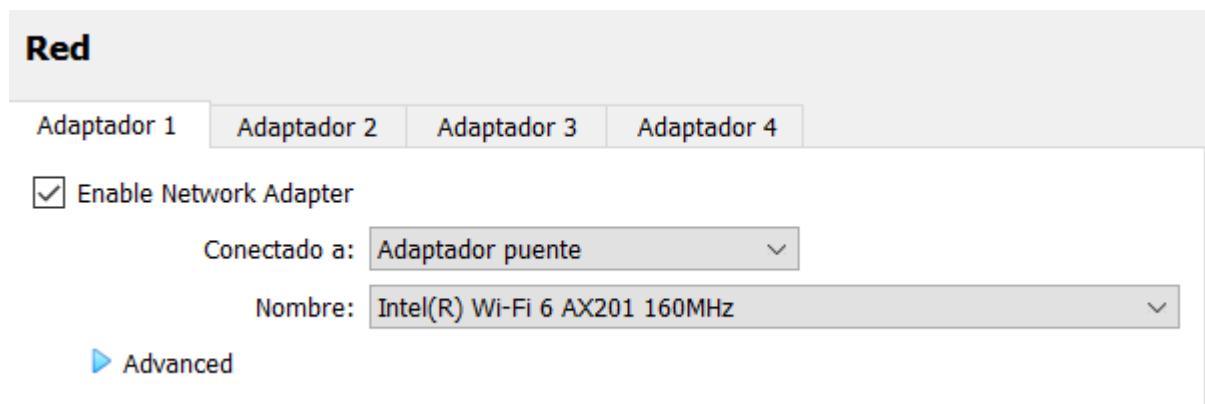


Igualmente selecciono cuánto le voy a dar de disco duro. Lo dejaré tal cual viene por defecto. Click en Next.

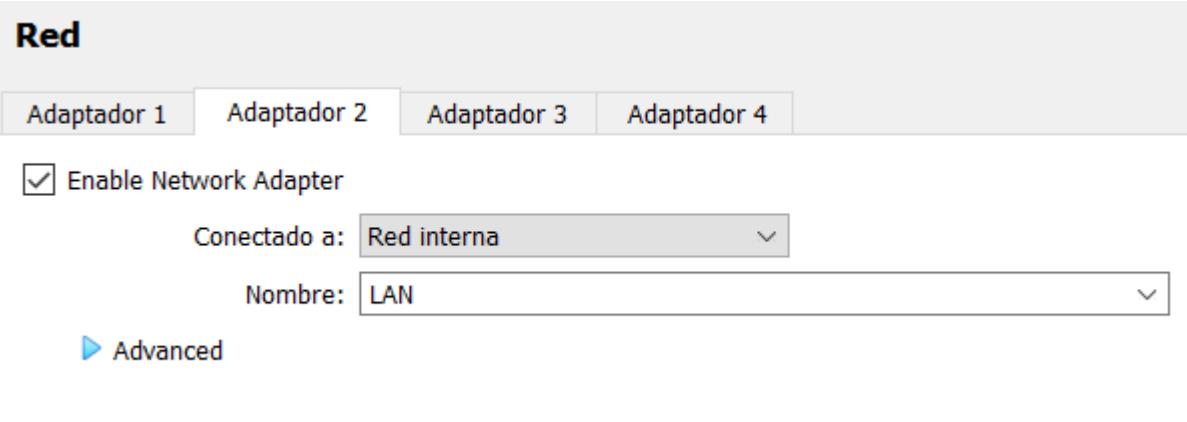


En la siguiente pantalla que aparece pincho en “Terminar” y seguidamente ya aparecerá mi máquina UTM PRÁCTICA en mi Virtual Box.

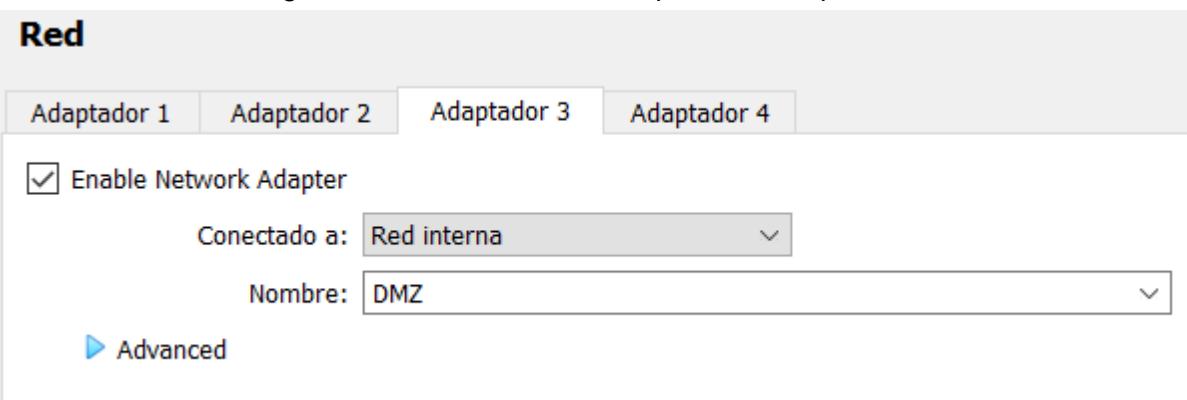
A continuación, procederé a crear las redes WAN (mi red, mi UTM), LAN, DMZ y DMZ_2. Para ello, con mi máquina UTM PRÁCTICA seleccionada, pincho en Configuración y voy al apartado redes. Crearé primero la red WAN en modo bridge (Adaptador puente).



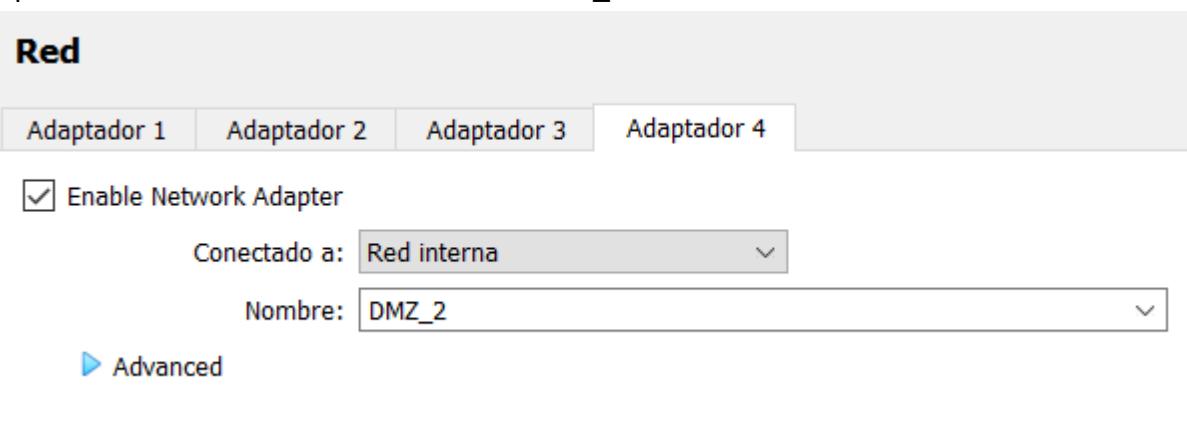
Después me voy a la pestaña de Adaptador 2 y crearé mi red con nombre de etiqueta LAN.



Ahora crearé la DMZ, igualmente red interna, en la pestaña Adaptador 3.



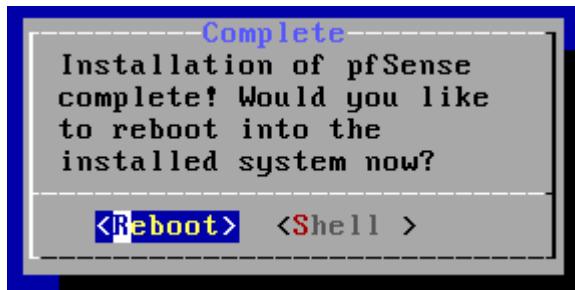
Y para terminar mi infraestructura, añado DMZ_2 como red interna también.



También hay que configurar en “Almacenamiento”, en el discoLA casilla “CD/DVD vivo”

Una vez creada la infraestructura, encenderé la máquina virtual y procederé a seguir los pasos de la instalación de pfSense. Todo lo dejaré como viene por defecto menos el idioma, que seleccionaré Spanish (key accents), el disco duro, que lo seleccionaré en la opción que sale y diré “yes” en cuanto a la destrucción de los datos.

Cuando salga la pantalla que muestro a continuación, daremos en Reboot e inmediatamente iremos a la pestaña de Dispositivo - Unidades Ópticas - Eliminar disco de la unidad virtual. Esto es para que no me arranque con el disco.



Para continuar con la configuración voy a comprobar que las mac de mis redes creadas corresponden con las que salen en la terminal pfsense. Como puedo observar, tengo una lista de acciones enumeradas. Para poner ver las mac por terminal, escribo la opción “1” en la consola, . Después compruebo en el apartado de Configuración de la interfaz gráfica, en Red si coinciden.

- | | |
|-----------------------------------|----------------------------------|
| 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: 1

Valid interfaces are:

em0      08:00:27:42:20:e6  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:5c:2a:29  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:49:5f:79  (down) Intel(R) Legacy PRO/1000 MT 82540EM
em3      08:00:27:c6:c4:5f  (down) Intel(R) Legacy PRO/1000 MT 82540EM
```



He podido comprobar que todas coinciden.

En el siguiente paso, voy a comprobar las ips y las interfaces escribiendo la Opción “2”. Me salen dos interfaces, la LAN y la WAN y esta opción me pregunta que cuál es el número de interfaces que deseo configurar. A ésto respondo 2 y configuro ambas interfaces.

La primera a configurar es la LAN y me dice que le asigne la ip la cual me dará acceso al router y por tanto me servirá como puerta de enlace. Le pondré la 192.168.100.254.

A continuación, me pide la máscara de subred a la cual pondré /24. Después me dice si quiero asignar una puerta de enlace. A esto diré que no ya que la misma ip de la LAN será la puerta de enlace, por lo que no necesito ninguna. También me pide que introduzca la ipv6 la cual tampoco introduciré nada.

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Ahora me pregunta si quiero activar el DHCP en la LAN, a lo que diré que sí y a lo que tendré que introducir el rango de ips que irá de la 192.168.100.100 a la 192.168.100.200

```
For a WAN, enter the new LAN IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>  
Enter the new LAN IPv6 address. Press <ENTER> for none:  
>  
Do you want to enable the DHCP server on LAN? (y/n)  
Do you want to enable the DHCP server on LAN? (y/n) y  
Enter the start address of the IPv4 client address range: 192.168.100.100  
Enter the end address of the IPv4 client address range: 192.168.100.200  
Disabling IPv6 DHCPD...
```

Después me pregunta si quiero activar el panel web en el pfsense, a lo que responderé que Sí.

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y  
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
Restarting webConfigurator...
```

```
The IPv4 LAN address has been set to 192.168.100.254/24  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
http://192.168.100.254/
```

Asignación de interfaces.

Con la opción 1, asignaré las interfaces. Le diré que no a las vpn y a continuación me irá preguntando como aparece en la siguiente imagen.

```

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 a or nothing if finished): em3

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2
OPT2 -> em3

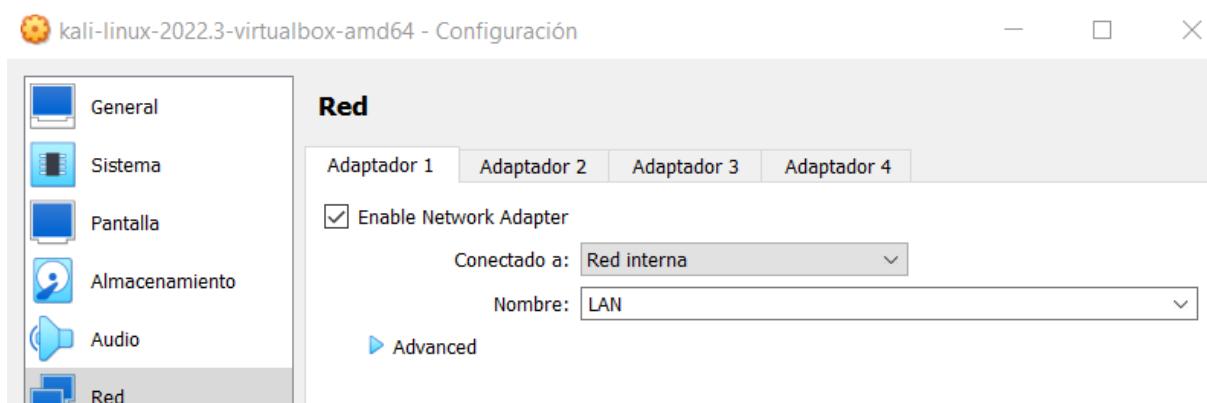
Do you want to proceed [y/n]? y

Writing configuration...done.
One moment while the settings are reloading... done!

```

Configuro Kali Linux en Virtual Box.

Ahora, sin apagar mi máquina de pfsense, iré al Virtual Box y selecciono mi máquina de Kali. Voy a Configuración - Red y selecciono Red interna y LAN. Esto es para que todo el tráfico pase por la red LAN.



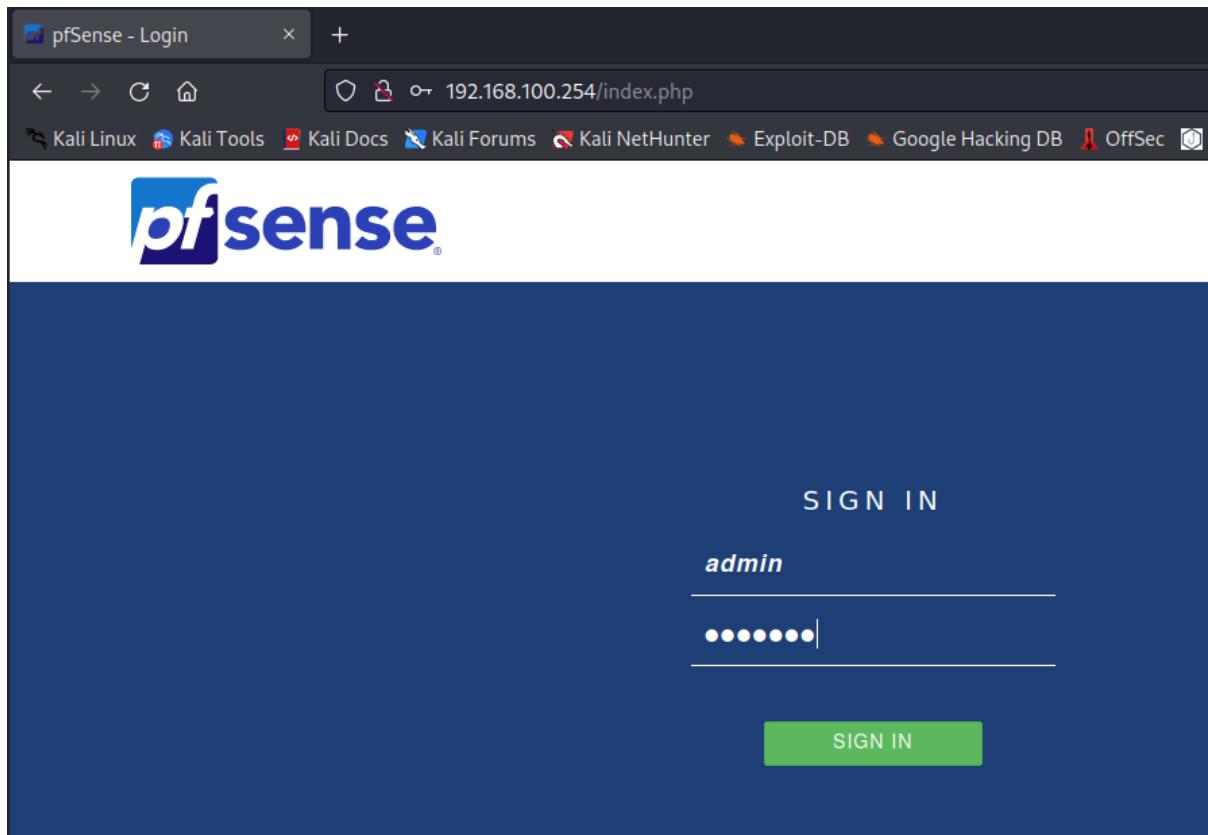
A continuación, inicio mi máquina de Kali y abro mi consola para hacer "ifconfig". Ahí comprobaré que mi ip sea donde comienza mi DHCP.

```

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::c80c:3096:fa1d:101a  prefixlen 64  scopeid 0x20<link>
          ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
            RX packets 1  bytes 342 (342.0 B)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 28  bytes 3434 (3.3 KiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

```

También inicio el pfsense en mi navegador con la dirección ip 192.168.100.254 e introduzco el usuario “admin” y la contraseña “pfsense”.



Configuración inicial en pfsense en web:

Introduzco nombre del hostname, del dominio, las dns y permito que los dns sean anulados por DHCP en Wan. Clic en Next.

General Information

On this screen the general pfSense parameters will be set.

Hostname	utm
EXAMPLE: myserver	
Domain	keepcoding.local
EXAMPLE: mydomain.com	
The default behavior of the DNS Resolver will ignore manually configured DNS servers below for client queries, visit Services > DNS Resolver to change this behavior.	
Primary DNS Server	1.1.1.1
Secondary DNS Server	8.8.8.8
Override DNS	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	

Después ponemos la zona horaria. Clic en Next

Time Server Information

Please enter the time, date and time zone.

Time server hostname Enter the hostname (FQDN) of the time server.

Timezone

Luego configuro la interfaz WAN que la dejaré en DHCP y desbloqueo el tráfico de redes privadas y redes bogon. Lo demás lo dejo como está por defecto. Hago clic en Next.

RFC1918 Networks

Block RFC1918 Private Networks Block private networks from entering via WAN
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.

Block bogon networks

Block bogon networks Block non-Internet routed networks from entering via WAN
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.

La siguiente pantalla que me sale la dejo tal cual. Clic en Next.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

>> Next

La siguiente pantalla me pide cambiar la contraseña, pero no la voy a cambiar, por lo que hago clic en Next.

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the We

Admin Password

Admin Password AGAIN

» Next

A continuación, me saldrá la última pantalla de finalización de la configuración donde haré clic en “Finished”.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey
(anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Una vez finalizado, se iniciará el pfsense y me saldrá una pantalla para aceptar el contrato de condiciones del uso del programa, el cual tendré que aceptar.

Habilitar interfaces

El siguiente paso será habilitar las redes DMZ y DMZ_2. Para ello, me voy a interfaces, a OPT1 primero. Selecciono “Enable interface”, en descripción porque el nombre de DMZ, en configuración Static IPv4 y después le pongo la ip en la configuración de la Static Ipv4, que será la 192.168.90.1 / 24. También quitaré el bloqueo de RFC 1918 y bogons. Despues le damos a guardar y aplicar cambios.

General Configuration

Enable Enable interface

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

IPv4 Address

192.168.90.1

/ 24

Reserved Networks

Block private networks and loopback addresses

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Ahora, realizaré lo mismo para DMZ_2, poniendo el nombre de DMZ_2. Para ello en interfaces me voy a OPT2 y haré el mismo procedimiento.

General Configuration

Enable Enable interface

Description

DMZ_2

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 Configuration

IPv4 Address

192.168.80.1

/ 24

Reserved Networks

Block private networks and loopback addresses

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Habilitamos en DMZ y DMZ_2 el dhcp para tener ips de manera automática. Para ello, voy a Servicios - DHCP Server - DMZ y activo el DHCP server y después asigno el rango de ips que dará (para asignar estas ips concretas tendré que configurarlo con el mac de LAN). También añadiré las dns y la puerta de enlace.

The screenshot shows the 'General Options' configuration for the DMZ interface. The 'Enable' checkbox is checked, and the 'Range' is set from 192.168.90.100 to 192.168.90.200. The 'DNS servers' are listed as 1.1.1.1 and 8.8.8.8. The 'Gateway' is set to 192.168.90.1. A note below the gateway field states: 'The default is to use the IP on this interface of the firewall as the gateway. Specify network. Type "none" for no gateway assignment.'

DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostname	Description
+ Add				

```
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::c80c:3096:fa1d:101a prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)
          RX packets 416 bytes 397625 (388.3 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 1402 bytes 140555 (137.2 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Static DHCP Mapping on DMZ

MAC Address	<u>08:00:27:22:46:4f</u>	Copy My MAC
MAC address (6 hex octets separated by colons)		

Seguiremos llenando datos necesarios.

Client Identifier	kali		
IP Address	192.168.90.225		
If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool.			
The same IP address may be assigned to multiple mappings.			
Hostname	kali		
Name of the host, without domain part.			
Description			
A description may be entered here for administrative reference (not parsed).			
ARP Table Static Entry	<input type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair.		
WINS Servers	WINS 1		
DNS Servers	1.1.1.1	8.8.8.8	DNS 3
Note: leave blank to use the system default DNS servers - this interface's IP is on the General page.			
Gateway	192.168.90.1		

Después daremos a “Guardar” y “Aplicar cambios”. Ahora toca probar si funciona. Me voy Dispositivos - Red - Preferencias de red... y estando conectado a Red Interna, voy a cambiar de LAN a DMZ. Probaré lo mismo con DMZ_2. Haré “ifconfig” en la consola, y me tendrá que salir la ip de DMZ.

```
mito:~ mito$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 192.168.90.225 netmask 255.255.255.0 broadcast 192.168.90.255  
      inet6 fe80::c80c:3096:fa1d:101a prefixlen 64 scopeid 0x20<link>  
        ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)  
          RX packets 4909 bytes 1027915 (1003.8 KiB)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 4987 bytes 486419 (475.0 KiB)  
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Como he podido comprobar, me ha salido la ip de DMZ.

Creación de usuario

System - User Manager - Users - +Add

Añado un nuevo usuario. Pongo el nombre, password, fecha de expiración de la cuenta y selecciono “admins” y lo paso a la lista de “miembros de”. Por último, doy a guardar.

User Properties

Defined by	USER				
Disabled	<input type="checkbox"/> This user cannot login				
Username	laura				
Password	●●●●				
Full name					
User's full name, for administrative information only					
Expiration date	04/13/2023				
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	<table border="1"> <tr> <td>Not member of</td> <td>admins</td> </tr> <tr> <td colspan="2">Member of</td> </tr> </table>	Not member of	admins	Member of	
Not member of	admins				
Member of					
<input style="background-color: #007bff; color: white; border: none; padding: 2px 10px; border-radius: 5px; margin-right: 10px;" type="button" value="» Move to 'Member of' list"/> <input style="background-color: #007bff; color: white; border: none; padding: 2px 10px; border-radius: 5px;" type="button" value="« Move to 'Not member of' list"/>					
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.					
Certificate	No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.				

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	laura		✓	admins	
				Add Delete	

Instalar paquete openvpn-client-export.

Para ello, en “System - Package manager” busco el nombre del paquete y hago clic en install.

Search

Search term	openvpn	Both	<input type="button" value="Search"/>	<input type="button" value="Clear"/>
Enter a search string or *nix regular expression to search package names and descriptions.				

Packages

Name	Version	Description	Actions
openvpn-client-export	1.6.9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	
Package Dependencies:			openvpn-client-export-2.5.8 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
--> NOTICE:
The p7zip port currently does not have a maintainer. As a result, it is
more likely to have unresolved issues, not be up-to-date, or even be removed in
the future. To volunteer to maintain this port, please create an issue at:
https://bugs.freebsd.org/bugzilla

More information about port maintainership is available at:
https://docs.freebsd.org/en/articles/contributing/#ports-contributing
>>> Cleaning up cache... done.
Success
```

Activación de https

En “System - Advanced - Admin Access” activo el protocolo “https” dejando por defecto el certificado SSL/TLS que aparece y añadiendo el puerto 443. Lo demás lo dejamos por defecto como está. Hago clic en “guardar”.

Protocol		<input type="radio"/> HTTP	<input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	webConfigurator default (64287ed99d200)		
Certificates known to be incompatible with use for HTTPS are not included in this list.			
TCP port	443		
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS) after save			

Creación en el servidor dns en un dominio que va a ser la dirección ip. En “Services - DNS Resolver - General Settings” Para añadir un servicio dns, iré a “Host Overrides” y clicaré en “Add”

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'ns.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'someosite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.				
+ Add				

Rellenaremos los datos del nombre del host, del dominio y la ip con la que se corresponde. Despues hago clic en “guardar” y “aplicar cambios”.

Host Override Options

Host	<input type="text" value="blueteam"/>
Name of the host, without the domain part e.g. enter "myhost" if the full domain name is "myhost.example.com"	
Domain	<input type="text" value="keepcoding.local"/>
Parent domain of the host e.g. enter "example.com" for "myhost.example.com"	
IP Address	<input type="text" value="192.168.100.100"/>
IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3	
Description	<input type="text" value="Servidor kali"/>
A description may be entered here for administrative reference (not parsed).	

Luego voy a comprobar que la ip está asociada al dominio indicado. Para ello, en la consola haré “dig @192.168.100.254 blueteam.keepcoding.local” y me debería dar la ip 192.168.100.100.

```
(base) [kali㉿kali] ~ Kali Docs Kali Forums Kali NetHunter Exploit-DB
└─$ dig @192.168.100.254 blueteam.keepcoding.local

; <>> DiG 9.18.4-2-Debian <>> @192.168.100.254 blueteam.keepcoding.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; →HEADER← opcode: QUERY, status: NOERROR, id: 62524
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;blueteam.keepcoding.local. IN A
;ANSWER SECTION:
blueteam.keepcoding.local. 3600 IN A 192.168.100.100
;; Query time: 0 msec
;; SERVER: 192.168.100.254#53(192.168.100.254) (UDP)
;; WHEN: Thu Apr 06 07:56:22 EDT 2023
;; MSG SIZE rcvd: 70
```

Levantar servidor apache

En la consola de Kali, inicio el servidor apache2 con “sudo service apache2 start” y me meto en la ip de apache 127.0.0.1. Después modiflico la página de Apache con “echo Hola Laura

esto es Kali > /var/www/html/index.html” y actualizo la página. Como puedo comprobar, puedo acceder a mi página desde mi ordenador, pero no me puedo conectar con nadie. Para ello hay que abrir los puertos.

(root@kali)-[~/home/kali]
echo Hola Laura esto es Kali > /var/www/html/index.html

Hola Laura esto es Kali

Abrir puertos.

Firewall - NAT - Port Forward. Mi ip pública (wan) en ipv4 por el protocolo TCP. Siempre que vaya alguien con destino WAN (IP pública), por el puerto 9090 al 9090. lo mandaré a un equipo con host 192.168.90.225. Por el puerto 80. Descripción “servidor web kali”.

Interface: WAN
Address Family: IPv4
Protocol: TCP
Source: [Display Advanced](#)
Destination: WAN address: 192.168.90.225 / Address/mask:
Destination port range: From port: 9090 To port: 9090
Redirect target IP: Type: Single host Address: 192.168.90.225
Redirect target port: Port: 80
Description: Servidor web kali

Creación de alias y creación de reglas

Primero crearé un alias para que me ayude en la creación de reglas. Esto me agrupará los puertos en dicho alias que cree, de manera que al tener que introducir estos datos, pondré directamente el alias.

Para ello voy a Firewall - Aliases - Ports - +Add. Después pongo el nombre del alias que será “webs” y añado los puertos que serán el 80 y el 443.

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	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	Description	
	443	Description	

Save Add Port

IP Ports URLs All

Firewall Aliases Ports

Name	Values	Description	Actions
webs	80, 443		

Ahora crearé las reglas. Para ello voy a Firewall - Rules - DMZ - Add. Selecciono en Action la opción “Pass”, en “Interface” dejo “DMZ” que es a la cual estamos haciendo la regla. El protocolo de internet dejo el “ipv4” y con el protocolo “TCP”. En “Source” selecciono “DMZ net” y en los puertos de destino pongo el alias creado, que será de “webs” a “webs”, es decir 80 y 443. También añadiré la descripción a la que he puesto “webs”. Para terminar esta regla, hago clic en “guardar”.

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 (TCI whereas with block the packet is dropped silently. In either case, the original
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 Invert match DMZ net

[Display Advanced](#)

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases the default value, any.

Destination

Destination Invert match any

Destination Port Range webs webs
From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote log server (see the Status: System Logs: Settings page).

Description webs
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and log.

Advanced Options [Display Advanced](#)

Floating WAN LAN DMZ **DMZ_2**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	DMZ net	*	*	webs	*	none		webs	

Seguidamente, creo una nueva regla, que es lo mismo pero en vez de poner “webs”, va a poner “DNS(53)”, que selecciono del listado que me aparece. Para el protocolo selecciono “TCP/UDP” y en descripción “webs dns”.

Protocol Choose which IP protocol this rule should match.

Source

Source	<input type="checkbox"/> Invert match	<input type="text" value="DMZ net"/>
---------------	---------------------------------------	--------------------------------------

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the default value, any.

Destination

Destination	<input type="checkbox"/> Invert match	<input type="text" value="any"/>
Destination Port Range	<input type="text" value="DNS (53)"/> From	<input type="text" value="Custom"/> To <input type="text" value="DNS (53)"/>

Specify the destination port or port range for this rule. The "To" field may be left empty if only one port is needed.

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of traffic, consider using a log collector.
Description	<input type="text" value="webs dns"/> A description may be entered here for administrative reference. A maximum of 52 characters can be used.

Floating WAN LAN **DMZ** DMZ_2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP	DMZ net	*	*	webs	*	none	webs	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	DMZ net	*	*	53 (DNS)	*	none	webs dns	

Add Add Delete Save

Creación de CAs

System - Certificate Manager - CAs - Add

Crearé un certificado de autenticación para poder certificar que soy yo cuando me quiera conectar a LAN, DMZ o DMZ_2.

Create / Edit CA

Descriptive name	<input type="text" value="keepcoding"/>
Method	<input type="text" value="Create an internal Certificate Authority"/>
Trust Store	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

<u>Key type</u>	RSA
	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.	
<u>Digest Algorithm</u>	sha256
The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorit	
<u>Lifetime (days)</u>	365
<u>Common Name</u>	internal-ca
The following certificate authority subject components are optional and may be left blank.	
<u>Country Code</u>	ES
<u>State or Province</u>	Toledo
<u>City</u>	Toledo
<u>Organization</u>	keepcoding
<u>Organizational Unit</u>	it

Creación de certificados

System - Certificate Manager - Certificates - Add

Crearé un certificado de servidor para la conexión a través de las vpn.

Add/Sign a New Certificate

Method	Create an internal Certificate	
Descriptive name	vpn.keepcoding.local	
Internal Certificate		
Certificate authority	keepcoding	
Key type	RSA	
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 an algorithm stronger than SHA1. Some platforms may 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	
Country Code	ES	
State or Province	Toledo	
City	Toledo	
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	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	+ Add	

Creación servidor vpn

VPN - Open VPN - Server - Add

Crearé un servidor VPN que me servirá para conectarme desde mi WAN a LAN, DMZ y DMZ_2. Para ello en descripción pongo VPN to LAN, en “server mode” selecciono “SSL/TLS+User Auth” para que conecte de sede a sede pero con autenticación de usuario,

lo que requerirá un certificado por parte del usuario. En “Device Mode” elijo el modo layer3, que es la entrada al router que nos conecta al tunel y nos dará acceso tanto a LAN como a DMZ y DMZ_2. El protocolo por el que se hará será el TCP. En “server certificate” selecciono el creado de “vpn.keepcoding.local” que fue creado como certificado de servidor. En “Hardware crypto” elijo mi tarjeta “INTEL RDRAND engine - RAND”. Añadiré la ip del tunel y los rangos de ips que serán accesibles como punto remoto. Por último, doy a guardar.

The screenshot shows a web-based configuration interface for a VPN server. At the top, there is a navigation bar with tabs: Servers (highlighted in red), Clients, Client Specific Overrides, Wizards, Client Export, and Shared Key Export. Below the navigation bar, there are two main configuration sections:

- General Information**: This section contains fields for "Description" (set to "VPN to LAN") and "Disabled" (with a checkbox). A note below the "Disabled" field states: "Set this option to disable this server without removing it from the list."
- Mode Configuration**: This section includes dropdown menus for "Server mode" (set to "Remote Access (SSL/TLS + User Auth)"), "Backend for authentication" (set to "Local Database"), and "Device mode" (set to "tun - Layer 3 Tunnel Mode"). A note below the "Device mode" dropdown explains: "'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

<u>Protocol</u>	TCP on IPv4 only
<u>Interface</u>	WAN
The interface or Virtual IP address where OpenVPN will receive client connections.	
<u>Local port</u>	1194
The port used by OpenVPN to receive client connections.	

Cryptographic Settings

<u>TLS Configuration</u>	<input checked="" type="checkbox"/> Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can connect. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peer from unauthorized connections. The TLS Key does not have any effect on tunnel data. <input checked="" type="checkbox"/> Automatically generate a TLS Key.
<u>Peer Certificate Authority</u>	keepcoding
<u>Peer Certificate Revocation list</u>	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
<u>OCSP Check</u>	<input type="checkbox"/> Check client certificates with OCSP
<u>Server certificate</u>	vpn.keepcoding.local (Server: Yes, CA: keepcoding)
<u>DH Parameter Length</u>	2048 bit
Diffie-Hellman (DH) parameter set used for key exchange. i	
<u>ECDH Curve</u>	Use Default
<u>Data Encryption Negotiation</u>	<input checked="" type="checkbox"/> Enable Data Encryption Negotiation This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.
<u>Data Encryption Algorithms</u>	AES-256-CBC (256 bit key, 128 bit block) AES-256-CFB (256 bit key, 128 bit block) AES-256-CFB1 (256 bit key, 128 bit block) AES-256-CFB8 (256 bit key, 128 bit block) AES-256-GCM (256 bit key, 128 bit block) AES-256-OFB (256 bit key, 128 bit block) ARIA-128-CBC (128 bit key, 128 bit block) ARIA-128-CFB (128 bit key, 128 bit block) ARIA-128-CFB1 (128 bit key, 128 bit block) ARIA-128-CFB8 (128 bit key, 128 bit block)
Available Data Encryption Algorithms Click to add or remove an algorithm from the list	
Allowed Data Encryption Algorithms. Click an algorithm from the list i	
The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. i	
<u>Fallback Data Encryption Algorithm</u>	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 negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.	
<u>Auth digest algorithm</u>	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.	
<u>Hardware Crypto</u>	Intel RDRAND engine - RAND
<u>Certificate Depth</u>	One (Client+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate certificates generated from the same CA as the server.	
<u>Strict User-CN Matching</u>	<input type="checkbox"/> Enforce match

Client Certificate Key Usage Validation	<input checked="" type="checkbox"/> Enforce key usage Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").
Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="192.168.225.0/24"/> This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and clients. 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.
IPv6 Tunnel Network	<input type="text"/> This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and clients. Expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
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)	<input type="text" value="192.168.90.0/24, 192.168.80.0/24, 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 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 a LAN network.
IPv6 Local network(s)	<input type="text"/> IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or 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 a global network.
Concurrent connections	<input type="text"/>
Allow Compression	<input type="button" value="Refuse any non-stub compression (Most secure)"/>
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 VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks. 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 one.
Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is considered best security practice but may be necessary in some environments.	
Client Settings	
Dynamic IP	<input type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	<input type="button" value="Subnet -- One IP address per client in a common subnet"/>
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of clients such as Yealink phones may require "net30".	

Ping settings	
Inactive	<input type="text" value="300"/> ▼
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the client to restart.	
Ping method	<input type="text" value="keepalive -- Use keepalive helper to define ping configuration"/> ▼
keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows: ping = interval ping-restart = timeout*2 push ping = interval push ping-restart = timeout	
Interval	<input type="text" value="10"/> ▼
Timeout	<input type="text" value="60"/> ▼
Advanced Client Settings	
DNS Default Domain	<input type="checkbox"/> Provide a default domain name to clients
DNS Server enable	<input type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
Block Outside DNS	<input type="checkbox"/> Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN <small>Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the setting.</small>

Crear usuarios

En “System - User Manager - Users - Add”. Pondré el nombre de usuario y contraseña (vpn:1234). En “Fullname” pondré vpn y después haré clic en “Crear certificado”. Para terminar pondré el “nombre de descripción” que será “vpn” y la información que aparece a continuación la dejaré tal y como sale por defecto. Para terminar la creación de usuario daré a guardar.

User Properties

Defined by **USER****Disabled** This user cannot login**Username** vpn**Password** **Full name** vpn

User's full name, for administrative information only

Expiration date

Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings Use individual customized GUI options and dashboard layout for this user.**Group membership**

admins

Not member of

Member of

>> Move to "Member of" list**<< Move to "Not member of" list**

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

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	vpn
Certificate authority	keepcoding
Key type	RSA
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 an algorithm stronger than SHA1. Some platforms may consider SHA1 invalid.	
Lifetime	3650
Keys	
Authorized SSH Keys	Enter authorized SSH keys for this user
IPsec Pre-Shared Key	

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	 
<input type="checkbox"/>	 laura		✓	admins	 
<input type="checkbox"/>	 vpn	vpn	✓		 

 Add  Delete

Exportar cliente

En “VPN - OpenVPN - Client Export”. Como ya tenemos certificado y usuario y contraseña, ahora hay que exportar el cliente. Con el plugin de “vpn client export” instalado exportaré el cliente.

Una vez dentro de “VPN - OpenVPN - Client Export” primero seleccionaré la vpn que vamos a usar que es la que me sale por defecto. Después seleccionaré la ip de WAN (Interface IP

address). En la parte de “OpenVPN clients” seleccionaré “Most clients” y descargaré el certificado. Lo demás lo dejo por defecto.

The screenshot shows the 'OpenVPN Server' configuration interface. In the 'Client Connection Behavior' section, 'Host Name Resolution' is set to 'Interface IP Address' and 'Verify Server CN' is set to 'Automatic - Use verify-x509-name where possible'. Below this, a note says 'Optionally verify the server certificate Common Name (CN) when the client connects.' In the 'OpenVPN Clients' section, there is one entry for 'User: vpn' with 'Certificate Name: vpn'. To the right of this entry are several download links under 'Export': 'Most Clients' (highlighted with a yellow box), 'Android', 'OpenVPN Connect (iOS/Android)', 'Archive', 'Config File Only', '64-bit', '32-bit', '10/2016/2019', '7/8/8.1/2012r2', 'Viscosity Bundle', and 'Viscosity Inline Config'.

Only OpenVPN-compatible user certificates are shown

Una vez descargado lo copio y pego en mi servidor local, para poder utilizarlo en la conexión con LAN.

Creación de una nueva regla

En “Firewall - Rules - WAN - Add” crearé una nueva regla para que me permita la conexión VPN en WAN. A esta nueva regla le pediré que vaya a WAN por Ipv4, por el protocolo UDP, con origen a cualquier sitio y con destino a nuestro Firewall. Pongo el puerto seleccionado que es el 1194. Para terminar guardo y aplico cambios.

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) 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

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

TCP

Choose which IP protocol this rule should match.

Source

Source

Invert match

any

Source Address

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases its default value, any.

Destination

Destination

Invert match

This firewall (self)

Destination Address

/

Destination Port Range

(other)

1194

(other)

1194

From

Custom

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

VPN to LAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

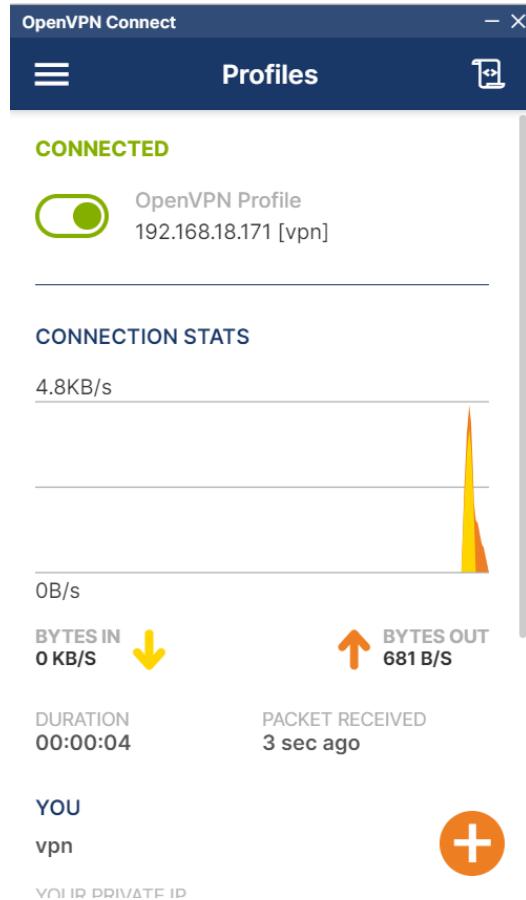
Advanced Options

[Display Advanced](#)

[Save](#)

Compruebo conexión.

Con OpenVPN Connect subiré el certificado descargado previamente y pondré el nombre de usuario y contraseña que asigné en la creación de usuario (vpn:1234). Puedo comprobar que tengo conexión.



Creo nueva regla para acceder al apache desde WAN a través de VPN.

En “Firewall - Rules - OpenVPN - Add” creo regla que permita pasar la interfaz openvpn por cualquier protocolo, a cualquier sitio. En descripción, pondré “Pass all”. Para terminar, guardo y aplico cambios.

Firewall / Rules / Edit

Edit Firewall Rule

Action	<input type="text" value="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) is sent back to the source whereas with block the packet is dropped silently. In either case, the original packet is dropped.	
<hr/>	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
<hr/>	
Interface	<input type="text" value="OpenVPN"/> ▼
Choose the interface from which packets must come to match this rule.	
<hr/>	
Address Family	<input type="text" value="IPv4"/> ▼
Select the Internet Protocol version this rule applies to.	
<hr/>	
Protocol	<input type="text" value="Any"/> ▼
Choose which IP protocol this rule should match.	

Source

Source Invert match Source Add

Destination

Destination Invert match Destination Add

Extra Options

Log Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using the [Status: System Logs: Settings](#) page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used for the log.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 *	*	*	*	*	*	none		Pass all	

ELASTIC SEARCH, HONEYBOT Y SURICATA

Instalación de elastic search y suricata

Me registro en la página web de elastic search (<https://www.elastic.co>) pero en la opción de "Cloud" (<https://cloud.elastic.co>). Una vez registrado, cargo la configuración y una vez finalizado, busco y añado Suricata .

The screenshot shows the 'Suricata' integration page. At the top right, it says 'Version 2.7.0' and has a 'Add Suricata' button. Below that is a navigation bar with 'Overview' (which is underlined), 'Settings', and 'API reference'. The main content area starts with 'Suricata Integration' and a note about reading EVE JSON output files. It includes sections for 'Compatibility' (mentioning v4.0.4) and 'EVE' (with an example event). To the right, there's a 'Screenshots' section showing two monitoring dashboards with various metrics and logs.

Me saldrá una ventanita en la parte inferior para instalar el “Elastic Agent”. Hago clic y aparecerá el instalador, el cual tendré que copiar lo que aparece en la primera parte y pegarlo en mi kali.

Add integration only (skip agent installation) Install Elastic Agent

1 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). For additional guidance, see our [installation docs](#).

[Linux Tar](#) [Mac](#) [Windows](#) [RPM](#) [DEB](#) [Kubernetes](#)

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.7.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.7.0-linux-x86_64.tar.gz
cd elastic-agent-8.7.0-linux-x86_64
sudo ./elastic-agent install --url=https://85e9462904794adcaa179627cb5ef73e.fleet.europe-west1.elastic-cloud.com:443/_internal
```

Copied

2 Confirm agent enrollment

Listening for agent...

After the agent starts up, the Elastic Stack listens for the agent and confirms the enrollment in Fleet. If you're having trouble connecting, check out the [troubleshooting guide](#).

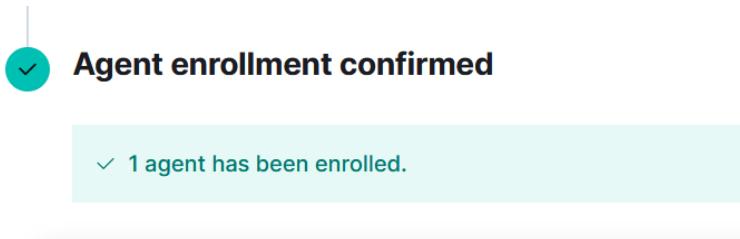
```

[root@kali]~[/var/www/html]
# curl -L -o https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.7.0-linux-x86_64.tar.gz
tar xvzf elastic-agent-8.7.0-linux-x86_64.tar.gz
cd elastic-agent-8.7.0-linux-x86_64
sudo ./elastic-agent install --url=https://85e9462904794adcaa179627cb5ef73e.fleet.europe-west2.gcp.elastic-cloud.co
% Total % Received % Xferd Average Speed Time Time Current
          Dload Upload Total Spent Left Speed
100 407M 100 407M 0 0 11.4M 0 0:00:35 0:00:35 --:--:-- 11.7M [no preference, typically autoselect]
elastic-agent-8.7.0-linux-x86_64/LICENSE.txt Explicitly set speed and duplex mode for this interface
elastic-agent-8.7.0-linux-x86_64/elastic-agent.yml WARNING: MUST be set to autoselect (automatically)
elastic-agent-8.7.0-linux-x86_64/elastic-agent.reference.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/elastic-agent
elastic-agent-8.7.0-linux-x86_64/NOTICE.txt Static IPv4 Configuration
elastic-agent-8.7.0-linux-x86_64/.build_hash.txt
elastic-agent-8.7.0-linux-x86_64/README.md
elastic-agent-8.7.0-linux-x86_64/.elastic-agent.active.commit IP Address 192.168.80.1
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/.build_hash.txt
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/LICENSE.txt
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/NOTICE.txt
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/README.md Interface is an Internet connection, select an ex
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/apm-server ce network interfaces the upstream gateway
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/apm-server.spec.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/apm-server.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/audit.rules.d/
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/audit.rules.d/sample-rules.conf.disabled
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/auditbeat
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/auditbeat.elastic-agent.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/auditbeat.reference.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/auditbeat.spec.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/auditbeat.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/bundle.tar.gz from IP addresses that are reserved for
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/certs/ space, too.
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/certs.pem
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/checksum.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/cloudbeat
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/cloudbeat.spec.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/cloudbeat.yml from reserved IP addresses (but not RF
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/elastic-agent-shipper
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/elastic-agent-shipper.spec.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/elastic-agent-shipper.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/endpoint-security equity can be changed under Sy
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/endpoint-security-resources.zip
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/endpoint-security.spec.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/fields.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/filebeat
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/filebeat.reference.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/filebeat.spec.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/filebeat.yml
elastic-agent-8.7.0-linux-x86_64/data/elastic-agent-fc4a15/components/fleet-server

```

Cuando finalice aparecerá ésto.

En interfaz:



En consola de kali:

```

Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.

```

Después me aparecerá las siguientes ventanas en la parte inferior:

Go back Add the integration

Go back Confirm incoming data

Y ya estaría mi elastic y suricata instalado. Elastic estaría en Cloud, y el Suricata en DMZ_2. De esta manera, cuando el honeypot permita una conexión será registrado por el suricata, y el elastic visualizará los logs. Ahora procederé a la creación de nuevas reglas para que se puedan permitir estas conexiones entrantes.

CREACIÓN DE NUEVAS REGLAS

NAT

En Nat crearé una regla para que las conexiones que entren por la interfaz WAN, por el protocolo TCP, con origen desde cualquier lugar con destino a mi WAN al puerto 22 (ssh), puedan entrar y sean redirigidos al puerto 2222. (Se crea regla del puerto 22, el ssh, para dar paso a aquellos ciberdelincuentes que ataquen a través de ese puerto, y que sean redirigidos al honey de DMZ_2 por el puerto 2222).

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	9090	192.168.90.225	80 (HTTP)	Servidor web kali	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	9091	192.168.80.225	80 (HTTP)	Test	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	22 (SSH)	192.168.80.101	2222	ssh honey	

WAN

En WAN crearé otra regla para que por la interface WAN, por el protocolo TCP, con origen desde WAN con destino a DMZ_2 y en un rango de puertos de 2221-2223 puedan entrar. (Esto es para los atacantes que hayan accedido a mi WAN se redirijan a DMZ_2).

Action	<input type="button" value="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	<input type="button" value="WAN"/>	Choose the interface from which packets must come to match this rule.
Address Family	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.
Protocol	<input type="button" value="TCP"/>	Choose which IP protocol this rule should match.
Source		
Source	<input type="checkbox"/> Invert match	<input type="button" value="WAN net"/> Source Address
<input type="button" value="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	<input type="button" value="DMZ_2 net"/> Destination Address
Destination Port Range	<input type="button" value="From (other)"/> Custom	<input type="button" value="To 2221 (other)"/> Custom
	<input type="button" value="2221"/>	<input type="button" value="2223"/>

DMZ_2

En DMZ_2 crearé dos reglas. La primera será para que por la interface DMZ_2 por el protocolo TCP, con origen DMZ_2 con destino a WAN por cualquier puerto, se les permita pasar. (Esto es para que llegue al elastic los logs de honey).

Edit Firewall Rule		
Action	<input type="button" value="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	<input type="button" value="DMZ_2"/>	Choose the interface from which packets must come to match this rule.
Address Family	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.
Protocol	<input type="button" value="TCP"/>	Choose which IP protocol this rule should match.
Source		
Source	<input type="checkbox"/> Invert match	<input type="button" value="DMZ_2 net"/> Source Address /
<input type="button" value="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	WAN net	Destination Address	/	<input type="button" value="▼"/>
Destination Port Range	(other)	<input type="text" value=""/>	(other)	Custom	Custom
From To					
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.					

Action 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_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 TCP Choose which IP protocol this rule should match.

Source

Source	<input type="checkbox"/> Invert match	any	Source Address	/	<input type="button" value="▼"/>
<input type="button" value="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	DMZ_2 net	Destination Address	/	<input type="button" value="▼"/>
Destination Port Range	(other)	2221	(other)	2223	Custom
From To					
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.					

CREACIÓN DE REGLA EN SURICATA

En el suricata crearé una regla por consola para que puedan registrarse las conexiones entrantes a través del puerto ssh, que serán redirigidos por el puerto 2222, a través del protocolo TCP desde cualquier lugar. Para ello primero creo el fichero de la regla que llamaré “suricata.rules”, lo editaré con “nano” y meteré la regla.

```
[root@kali]~/home/kali/elastic-agent-8.7.0-linux-x86_64]
# cd /etc/suricata/rules

[root@kali]~/etc/suricata/rules]
# ls
app-layer-events.rules    http-events.rules      smb-events.rules
decoder-events.rules      ipsec-events.rules    smtp-events.rules
dhcp-events.rules         kerberos-events.rules ssh-events.rules
dnp3-events.rules         modbus-events.rules   stream-events.rules
dns-events.rules          mqtt-events.rules    tls-events.rules
files.rules               nfs-events.rules
http2-events.rules        ntp-events.rules
```

```
[root@kali]~/etc/suricata/rules]
# nano suricata.rules
```

Añado la regla.

```
GNU nano 7.2                                suricata.rules
alert tcp  any any → any 2222 (msg: "ssh"; sid:100; priority:1;)
```

Ahora ejecuto suricata y después el honeypot con docker.

```
[root@kali]~/etc/suricata]
# suricata -c suricata.yaml -i eth1
8/4/2023 -- 15:37:53 - <Notice> - This is Suricata version 6.0.10 RELEASE run
ning in SYSTEM mode
8/4/2023 -- 15:37:53 - <Notice> - all 2 packet processing threads, 4 manageme
nt threads initialized, engine started.
```

```
[root@kali]~/home/kali]
# docker run -p 2222:2222 cowrie/cowrie
Unable to find image 'cowrie/cowrie:latest' locally
latest: Pulling from cowrie/cowrie
fc251a6e7981: Pull complete
7be4d3667295: Pull complete
a1f1879bb7de: Pull complete
7eb7c5946a58: Pull complete
1817c8a12818: Pull complete
581833d6638a: Pull complete
277414dc2707: Downloading 61.93MB/79.04MB
f8b7231d72a2: Download complete
4f4fb700ef54: Download complete
```

Después simulo ser una ciberatacante desde WAN y soy interceptada por el honeypot de mi DMZ_2.

```
C:\Users\Laura>ssh root@192.168.18.167
The authenticity of host '192.168.18.167 (192.168.18.167)' can't be established.
ECDSA key fingerprint is SHA256:/aDhh9FhgT/Ek3glwEKEXQwiNQJLif/J14qZTG0ook.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.18.167' (ECDSA) to the list of known hosts.
root@192.168.18.167's password:
```

```
C:\Users\Laura>ssh [-46AaCfGgKkNNnqsTtVvXxYy] [-B bind_interface]
[-b bind_address] [-c cipher_spec] [-D [bind_address]:port]
[-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
[-i identity_file] [-J [user@[host[:port]]] [-L address]
[-l login_name] [-m mac_spec] [-O cti_cmd] [-o option] [-p port]
[-Q query_option] [-R address] [-S cti_path] [-W host:port]
[-w local_tun[:remote_tun]] destination [command]

C:\Users\Laura>ssh root@192.168.18.167
ssh: connect to host 192.168.18.167 port 22: Connection timed out

C:\Users\Laura>ssh root@192.168.18.167
The authenticity of host '192.168.18.167 (192.168.18.167)' can't be established.
ECDSA key fingerprint is SHA256:/aDhh9FhgT/Ek3glwEKEXQwiNQJLif/J14qZTG0ook.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.18.167' (ECDSA) to the list of known hosts.
root@192.168.18.167'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:~# hola
-bash: hola: command not found
root@svr04:~#
```

```
root@kali:~/etc/suricata x root@kali:/home/kali x kali@kali:~ x
File Actions Edit View Help
root@kali:/etc/suricata x root@kali:/home/kali x kali@kali:~ x
Starting service b'ssh-userauth'
2023-04-08T19:53:28+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug]
] b'root' trying auth b'none'
2023-04-08T19:55:28+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug]
] b'root' trying auth b'password'
2023-04-08T19:55:28+0000 [HoneyPotSSHTransport,0,192.168.18.223] Could not read etc/userdb.txt, default database activated
2023-04-08T19:55:28+0000 [HoneyPotSSHTransport,0,192.168.18.223] login attempt [b'root'] succeeded
2023-04-08T19:55:28+0000 [HoneyPotSSHTransport,0,192.168.18.223] Initialized emulated server as architecture: linux-x64-1sb
2023-04-08T19:55:28+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug]
] b'root' authenticated with b'password'
2023-04-08T19:55:28+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2023-04-08T19:55:28+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2023-04-08T19:55:28+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2023-04-08T19:55:28+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessionsdopensssh.com' request
2023-04-08T19:55:28+0000 [twisted.conch.ssh.sessioninfo] Handling pty request: b'xterm-256color' (30, 77, 640, 480)
2023-04-08T19:55:28+0000 [SSHChannel session () on SSHService b'ssh-connection' on HoneyPotSSHTransport,0,192.168.18.223] Terminal Size: 77 30
2023-04-08T19:55:28+0000 [twisted.conch.ssh.sessioninfo] Getting shell
2023-04-08T19:55:36+0000 [HoneyPotSSHTransport,0,192.168.18.223] CMD: hola
2023-04-08T19:55:36+0000 [HoneyPotSSHTransport,0,192.168.18.223] Can't find command hola
2023-04-08T19:55:36+0000 [HoneyPotSSHTransport,0,192.168.18.223] Command not found: hola
```

Si me voy a mi elastic search, podré comprobar que se puede visualizar el log y también lo almacena.

	@timestamp	host.name	suricata.eve.flow...	network.transport	source.ip	source.port	destination.ip	destination.port
<input checked="" type="checkbox"/>	Apr 8, 2023 @ 21:55:28,347	-	2096316733333502	tcp	192.168.18.223	60,041	192.168.80.101	2,222

CREACIÓN DE NUEVAS REGLAS. BLOQUEOS.

A continuación, crearé reglas para que DMZ_2 solo tenga salida al elastic search que está en la WAN y entrada de posibles ciberatacantes desde la WAN. De esta manera se bloqueará el acceso de DMZ_2 a DMZ y LAN, tanto desde su interfaz como desde la interfaz de éstas.

En DMZ_2:

- Creo regla para bloquear salida de DMZ_2 con destino DMZ.

Action 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 u 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 Choose the interface from which packets must come to match this rule.

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

Protocol Choose which IP protocol this rule should match.

Source

Source Invert match The **Source Port Range** for a connection is typically random and almost never equal to the destination's default value, any.

Destination

Destination Invert match

- Creo regla para bloquear salida de DMZ_2 con destino LAN.

Action	<input type="button" value="Block"/>	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) 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	<input type="button" value="DMZ_2"/>	Choose the interface from which packets must come to match this rule.																					
Address Family	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.																					
Protocol	<input type="button" value="TCP"/>	Choose which IP protocol this rule should match.																					
Source <hr/> <table border="1"> <tr> <td>Source</td> <td><input type="checkbox"/> Invert match</td> <td><input type="button" value="DMZ_2 net"/></td> <td><input type="button" value="So"/></td> </tr> <tr> <td colspan="4"><input type="button" value="Display Advanced"/></td> </tr> <tr> <td colspan="4">The Source Port Range for a connection is typically random and almost never equal to the destination port. Use its default value, any.</td> </tr> </table> <hr/> Destination <hr/> <table border="1"> <tr> <td>Destination</td> <td><input type="checkbox"/> Invert match</td> <td><input type="button" value="LAN net"/></td> <td><input type="button" value="De"/></td> </tr> <tr> <td>Destination Port Range</td> <td><input type="button" value="(other)"/></td> <td><input type="button" value=""/></td> <td><input type="button" value="(other)"/></td> <td><input type="button" value=""/></td> </tr> </table>			Source	<input type="checkbox"/> Invert match	<input type="button" value="DMZ_2 net"/>	<input type="button" value="So"/>	<input type="button" value="Display Advanced"/>				The Source Port Range for a connection is typically random and almost never equal to the destination port. Use its default value, any .				Destination	<input type="checkbox"/> Invert match	<input type="button" value="LAN net"/>	<input type="button" value="De"/>	Destination Port Range	<input type="button" value="(other)"/>	<input type="button" value=""/>	<input type="button" value="(other)"/>	<input type="button" value=""/>
Source	<input type="checkbox"/> Invert match	<input type="button" value="DMZ_2 net"/>	<input type="button" value="So"/>																				
<input type="button" value="Display Advanced"/>																							
The Source Port Range for a connection is typically random and almost never equal to the destination port. Use its default value, any .																							
Destination	<input type="checkbox"/> Invert match	<input type="button" value="LAN net"/>	<input type="button" value="De"/>																				
Destination Port Range	<input type="button" value="(other)"/>	<input type="button" value=""/>	<input type="button" value="(other)"/>	<input type="button" value=""/>																			

En DMZ:

- Bloqueo la conexión de DMZ_2 a DMZ en la interfaz DMZ.

<u>Action</u>	<input type="button" value="Block"/>	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) is sent back to the source whereas with block the packet is dropped silently. In either case, the original packet is discarded.
<u>Disabled</u>	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
<u>Interface</u>	<input type="button" value="DMZ"/>	Choose the interface from which packets must come to match this rule.
<u>Address Family</u>	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.
<u>Protocol</u>	<input type="button" value="TCP"/>	Choose which IP protocol this rule should match.
Source		
<u>Source</u>	<input type="checkbox"/> Invert match	<input type="button" value="DMZ_2 net"/>
<input type="button" value="Display Advanced"/> <p>The Source Port Range for a connection is typically random and almost never equal to the default value, any.</p>		
Destination		
<u>Destination</u>	<input type="checkbox"/> Invert match	<input type="button" value="DMZ net"/>

En LAN:

Bloqueo salida de DMZ_2 con destino LAN por la interfaz LAN.

Action	<input type="button" value="Block"/>	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) is sent back to the source 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	<input type="button" value="LAN"/>	Choose the interface from which packets must come to match this rule.		
Address Family	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.		
Protocol	<input type="button" value="TCP"/>	Choose which IP protocol this rule should match.		
Source				
Source	<input type="checkbox"/> Invert match	<input type="button" value="DMZ_2 net"/>		
Display Advanced				
The Source Port Range for a connection is typically random and almost never equal to the destination port. Its default value, any .				
Destination				
Destination	<input type="checkbox"/> Invert match	<input type="button" value="LAN net"/>		
Destination Port Range	<input type="button" value="(other)"/>	<input type="button" value=""/>	<input type="button" value="(other)"/>	<input type="button" value=""/>