



**Blue Team**

Fray José Ávila Hernández

# **Índice**

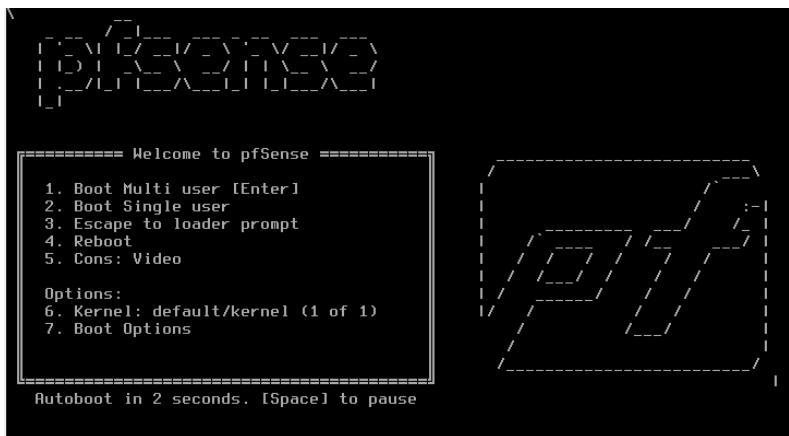
- 1. Creación PFSENSE y Kali Linux**
- 2. Configuración de Redes a través del PFSENSE**
- 3. Exportar VPN desde el PFSENSE**
- 4. HONEYPOTS**

# 1.Creación PFSENSE y Kali Linux

Lo primero que vamos a hacer es crear las redes LAN y DMZ como red interna a través del PFSENSE.

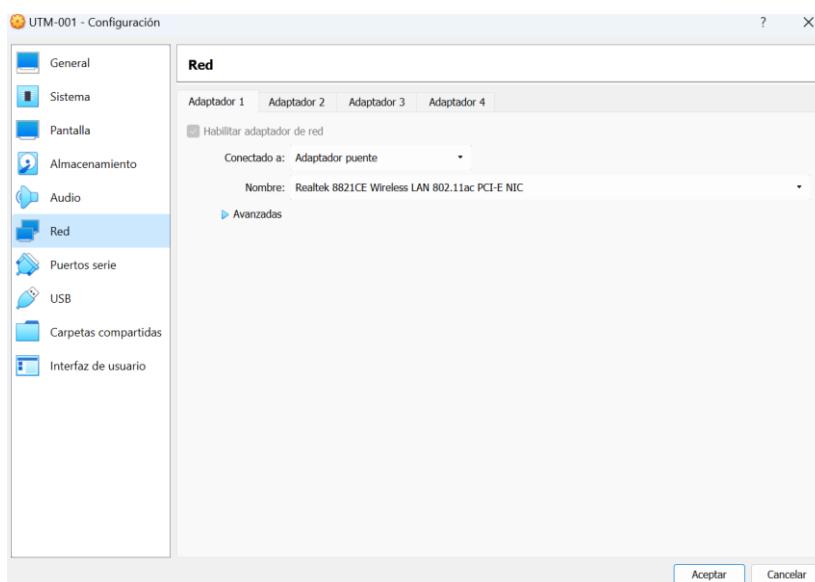
Para ello vamos a levantar dos máquinas virtuales una será UTM que es donde estará montado el PFSENSE y otra será un Kali Linux que estarán conectadas a nuestro ordenador Windows 11 a través de la red WAN.

## 1.1 Máquina Virtual PFSENSE



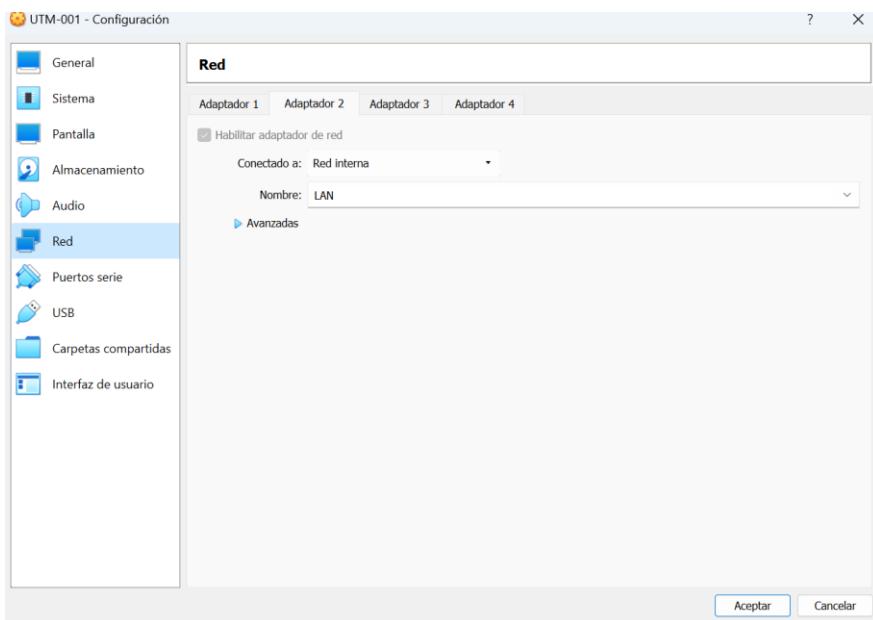
Una vez montado el PFSENSE creamos tres adaptadores red que es como si fuesen switches.

### Adaptador 1 (adaptador puente).

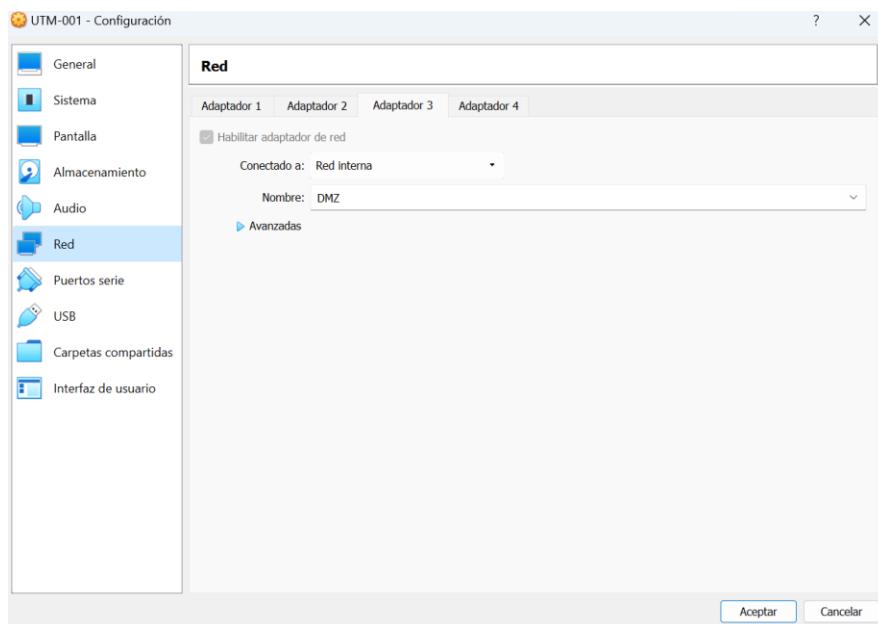


Este primero es el adaptador puente que lo que hace es conectar la máquina virtual a nuestra red.

## Adaptador 2 (LAN).

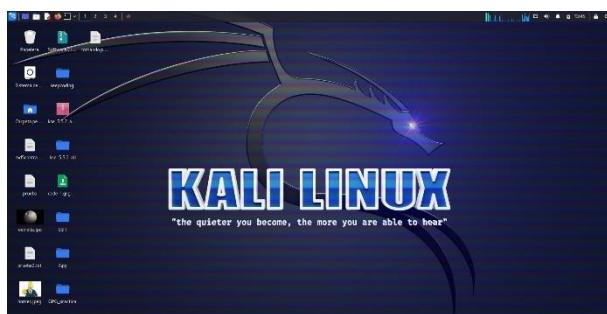


## Adaptador 3 (DMZ).

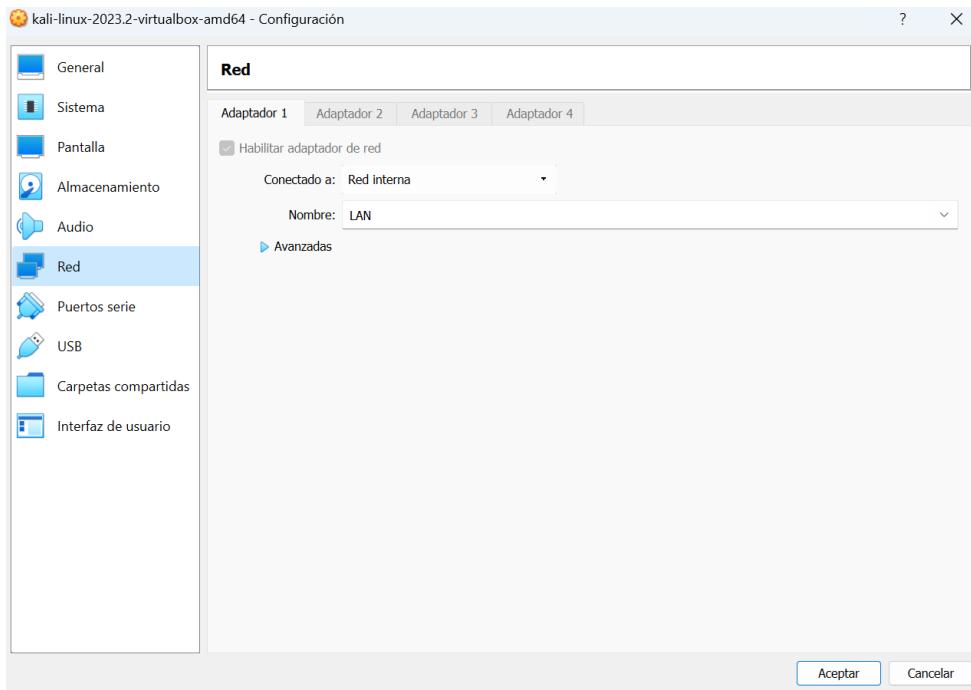


Estos dos adaptadores lo que hacen es crearnos unos switches internos.

## 1.2 Máquina Virtual Kali Linux



Una vez levantado Kali Linux tenemos que ir a configuración red y conectar la maquina a la red interna LAN para que pueda estar conectado al servidor que hemos montado que es el PFSENSE.



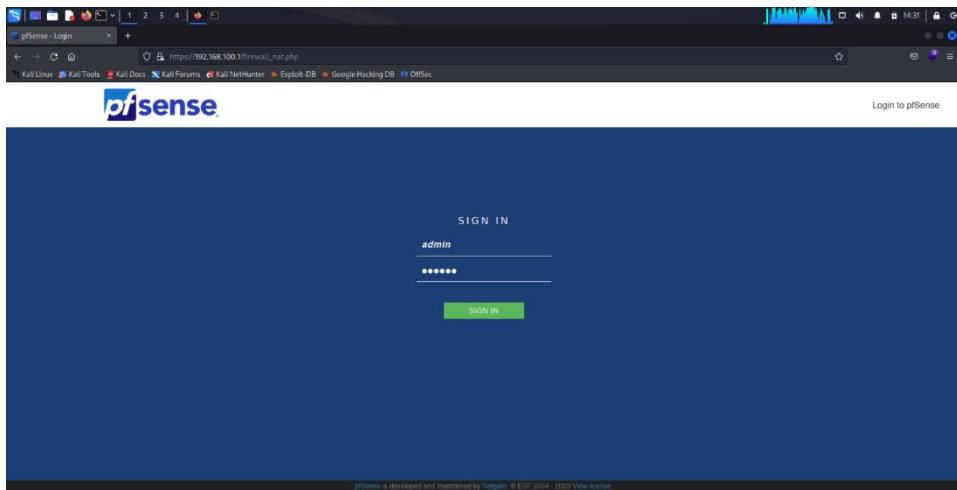
Una vez abrimos la consola de Kali y ponemos el comando ifconfig podemos ver que la IP que nos ha dado es: 192.168.100.

```
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::d5e1:d10d:ab0d:6fb1 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:53:0c:ba txqueuelen 1000 (Ethernet)
          RX packets 13177 bytes 4290379 (4.0 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 13135 bytes 1580186 (1.5 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                                         System VirtualBox Virtual Machine
                                         Netgate Device ID: 3cf63cc4519d5391d8be

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 48669 bytes 3968602 (3.7 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 48669 bytes 3968602 (3.7 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                                         System FreeBSD 14.0-CURRENT
                                         Vendor: Innotek GmbH
                                         Version: VirtualBox
                                         Release Date: Fri Dec 1 2006
                                         OS: 7.0-RELEASE (amd64)
                                         built on Wed Jun 28 03:53:34 UTC 2023
                                         The system is on the latest version.
                                         Version information updated at Tue Sep 12 19:44:29 CEST 2023
```

Ahora que sabemos la IP ponemos en nuestro navegador 192.168.100.1 para entrar al PFSENSE y configurarlo.

## 2. Configuración de Redes a través del PFSENSE



Después de crear el usuario y contraseña nos pondremos a configurar el PFSENSE

System Information	
Name	utm.keepcoding.local
User	admin@192.168.100.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 3cf63cc4519d5391d8be
BIOS	Vendor: innotech GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT
<p>The system is on the latest version. Version information updated at Tue Sep 12 19:44:29 CEST 2023</p>	
CPU Type	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 2 CPUs: 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: No QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 53 Minutes 00 Second
Current date/time	Tue Sep 12 20:41:59 CEST 2023
DNS server(s)	<ul style="list-style-type: none"><li>127.0.0.1</li><li>80.58.61.250</li><li>80.58.61.254</li><li>1.1.1.1</li></ul>
Last config change	Thu Aug 31 22:02:51 CEST 2023

**Netgate Services And Support**

Contract type: Community Support  
Community Support Only

**NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces			
WAN	1000baseT <full-duplex>	192.168.1.34	
LAN	1000baseT <full-duplex>	192.168.100.1	
DMZ	1000baseT <full-duplex>	192.168.200.1	
DMZ_2	1000baseT <full-duplex>	192.168.250.1	

Aquí lo importante es poner en el DNS principal la IP 127.0.0.1 que es la que pertenece al propio PFSENSE y es la que va a resolver.

Como IP secundaria pondremos 1.1.1.1.

## 2.1 Configuración Red WAN

The screenshot shows the 'General Configuration' section of a network interface configuration tool. The interface has several fields:

- Enable:** A checked checkbox labeled "Enable interface".
- Description:** A text input field containing "WAN". A placeholder text below it says "Enter a description (name) for the interface here."
- IPv4 Configuration Type:** A dropdown menu set to "DHCP".
- IPv6 Configuration Type:** A dropdown menu set to "DHCPv6".
- MAC Address:** An input field containing "XXXXXXXXXXXX". A note below it says "This field can be used to modify ("spool") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank."
- MTU:** An input field with a note: "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:** An input field with a note: "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:** A dropdown menu set to "Default (no preference, typically autoselect)". A note below it says "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."

Below this section is a "DHCP Client Configuration" section with the following options:

- Options:** Two checkboxes: "Advanced Configuration" (unchecked) and "Configuration Override" (unchecked). A note below "Advanced Configuration" says "Use advanced DHCP configuration options." A note below "Configuration Override" says "Override the configuration from this file."
- Hostname:** An input field with a note: "The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification)."

Una vez pasamos a la configuración interfaz WAN tendremos que dejar el tipo DHCP que es el que nos da acceso a nuestra red interna.

The screenshot shows the "DHCP6 Client Configuration" section of a network interface configuration tool. It includes the following settings:

- Options:** Two checkboxes: "Advanced Configuration" (unchecked) and "Configuration Override" (unchecked). A note below "Advanced Configuration" says "Use advanced DHCPv6 configuration options." A note below "Configuration Override" says "Override the configuration from this file."
- Use IPv4 connectivity as parent interface:** A checkbox labeled "Request a IPv6 prefix/information through the IPv4 connectivity link".
- Request only an IPv6 prefix:** A checkbox labeled "Only request an IPv6 prefix, do not request an IPv6 address".
- DHCPv6 Prefix Delegation size:** A dropdown menu set to "64". A note below it says "The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP."
- Send IPv6 prefix hint:** A checkbox labeled "Send an IPv6 prefix hint to indicate the desired prefix size for delegation".
- Do not wait for a RA:** A checkbox labeled "Required by some ISPs, especially those not using PPPoE".

Below these settings is a "Reserved Networks" section with two checkboxes:

- Block private networks and loopback addresses:** A checkbox with a note: "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:** A checkbox with a note: "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."

A blue "Save" button is located at the bottom left of the configuration page.

Tendremos que desbloquear las conexiones privadas y los bogon.

## 2.2 Configuración Red LAN

The screenshot shows the 'General Configuration' section for the 'lan' interface. The 'Enable' checkbox is checked. The 'Description' field is set to 'LAN'. The 'IPv4 Configuration Type' is 'Static IPv4'. The 'IPv6 Configuration Type' is 'Track Interface'. The 'MAC Address' field contains 'XXXXXXXXXXXXXX'. The 'MTU' field is blank. The 'MSS' field is also blank. Under 'Speed and Duplex', the dropdown is set to 'Default (no preference, typically autoselect)'. In the 'Static IPv4 Configuration' section, the 'IPv4 Address' is '192.168.100.1'. The 'IPv4 Upstream gateway' is set to 'None'. A note states: 'If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.'

Aquí modificamos la dirección IP 192.168.100.1 para que no coincida con alguna IP de nuestra casa.

## 2.3 Configuración servidores DNS.

El siguiente paso una vez configurada la Red LAN y la WAN, vamos a configurar los servidores DNS, para habilitar que nuestro PFSENSE sea un servidor DNS interno de nuestra infraestructura.

The screenshot shows the 'General Settings' tab for the 'DNS Resolver' service. The 'General Settings' tab is selected. Under 'General DNS Resolver Options', the 'Enable' checkbox is checked. The 'Listen Port' is set to '53'. The 'Enable SSL/TLS Service' checkbox is unchecked. The 'SSL/TLS Certificate' dropdown is set to 'webConfigurator default (64ee2bd7cc6a8)'. The 'SSL/TLS Listen Port' is set to '853'. The 'Network Interfaces' dropdown is set to 'All'. The 'Outgoing Network Interfaces' dropdown is also set to 'All'.

Para ello entramos en la pestaña DNS Resolver, vemos que en los ajustes generales el DNS está habilitado, el puerto que está escuchando es el 53. Tiene que estar habilitado el Network interfaces y el Outgoing Network interfaces.

Por último, comprobamos el DNSSEC esté habilitado y guardamos.

The screenshot shows the pfSense web interface for managing the DNS Resolver. In the 'DNSSEC' section, the checkbox 'Enable DNSSEC Support' is checked. Other sections like 'Python Module' and 'DNS Query Forwarding' have their respective checkboxes unchecked. At the bottom, there is a 'Save' button.

## 2.4 Configuración DHCP Server

### LAN

The screenshot shows the pfSense web interface for configuring the DHCP server on the LAN interface. Under 'General Options', the 'Enable' checkbox is checked, and the 'Allow all clients' dropdown is set to 'Allow all clients'. The 'Range' section shows the IP range from 192.168.100.100 to 192.168.100.200.

Entramos en DHCP Server y la primera red que configuramos es la LAN, vemos que esta habilitada, comprobamos que la IP es la 192.168.100. que es la que hemos modificado anteriormente. Si queremos podemos cambiar el rango en este caso lo hemos puesto desde la 100 hasta la 200.

The screenshot shows a terminal window titled 'dhclient' with the URL ':/192.168.100.1/services\_dhcp.php'. The page displays the configuration of a DHCP server. In the 'Servers' section, WINS servers are set to 'WINS Server 1' and 'WINS Server 2'. DNS servers are set to '192.168.100.1', '1.1.1.1', '8.8.8.8', and 'DNS Server 4'. A note states: 'Leave blank to use the system default DNS servers: The IP address of this firewall interface if DNS Resolver or Forwarder is enabled, otherwise the servers configured in General settings or those obtained dynamically.' In the 'OMAPI' section, the port is set to 'OMAPI Port' and the key is set to 'OMAPI Key'. A checkbox for 'Generate New Key' is available. The 'Key Algorithm' dropdown is set to 'HMAC-SHA256 (current bind9 default)'. At the bottom, there is a 'Other Options' section.

El siguiente paso que haremos es añadir diferentes de servidores DNS.

El primero será 192.168.100.1 (Local)

El segundo será 1.1.1.1 (Cloudflare)

El tercero será 8.8.8.8 (Google)

The screenshot shows a configuration page for a DHCP server on a firewall. The 'Gateway' field is set to 192.168.100.1. Other options like 'Domain name', 'Domain search list', and 'Default lease time' are also present. The 'Failover peer IP' field is empty. Under 'Static ARP', the 'Enable Static ARP entries' checkbox is checked. In 'Time format change', the 'Change DHCP display lease time from UTC to local time' checkbox is checked. The 'Statistics graphs' checkbox is also checked. The 'Ping check' checkbox is checked. A note below it says: 'When enabled dhcpcd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default.'

El último paso que haremos para terminar la configuración será añadir en la puerta de enlace la IP 192.168.100.1 que esto nos va a dar por donde se va a conectar el equipo a internet en este caso PFSENSE.

```

Archivo  Acciones  Editar  Vista  Ayuda
(kali㉿kali)-[~]
└$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 brd 00:00:00:00:00:00 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:00:27:53:0c:ba brd ff:ff:ff:ff:ff:ff
        inet 192.168.100.24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
            valid_lft 7194sec preferred_lft 7194sec
        inet6 fe80::20c:27ff:fe53:0c%eth0/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:9f:9e:26:a0 brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
└$ ping marca.com
PING marca.com (34.147.120.111) 56(84) bytes of data.
64 bytes from 111.120.147.34.bc.googleusercontent.com (34.147.120.111): icmp_seq=1 ttl=54 time=50.9 ms
64 bytes from 111.120.147.34.bc.googleusercontent.com (34.147.120.111): icmp_seq=2 ttl=54 time=75.2 ms
64 bytes from 111.120.147.34.bc.googleusercontent.com (34.147.120.111): icmp_seq=3 ttl=54 time=50.1 ms
^C
--- marca.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 50.105/58.728/75.178/11.636 ms
(kali㉿kali)-[~]
└$ 

```

Comprobamos la conexión IP en la máquina y probamos que tengamos internet.

The screenshot shows the pfSense web interface at [https://192.168.100.1/interfaces\\_assign.php](https://192.168.100.1/interfaces_assign.php). The top navigation bar includes links for Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and the pfSense logo. Below the navigation is a menu bar with System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Interfaces / Interface Assignments". A sub-menu bar below it includes Interface Assignments, Interface Groups, Wireless, VLANs, QinQs, PPPs, GREs, GIFs, Bridges, and LAGGs. The "Interface Assignments" tab is selected. The table lists three entries:

Interface	Network port
WAN	em0 (08:00:27:ae:06:20)
LAN	em1 (08:00:27:4e:eb:96)
DMZ	em2 (08:00:27:ad:ac:8a)

Each entry has a red "Delete" button to its right.

El siguiente paso es irnos a la asignación de interfaz y añadimos una red nueva que en este caso será DMZ y la personalizaremos.

## DMZ

The screenshot shows the pfSense web interface at <https://192.168.100.1/interfaces.php?if=opt1>. The top navigation bar and menu bar are identical to the previous screenshot. The main content area is titled "General Configuration". The configuration fields include:

- Enable:  Enable interface
- Description: DMZ (with placeholder "Enter a description (name) for the interface here")
- IPv4 Configuration Type: Static IPv4
- IPv6 Configuration Type: None
- MAC Address:  (with placeholder "This field can be used to modify ('spoof') the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xxxx:xx:xx:xx or leave blank.")
- MTU:  (with placeholder "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:  (with placeholder "If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IP header size) and minus 60 for IPv6 (TCP/IP header size) will be in effect.")
- Speed and Duplex: Default (no preference, typically autoselect)

Below the General Configuration is the "Static IPv4 Configuration" section:

IPv4 Address	192.168.200.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway

Notes in the Static IPv4 Configuration section:

- If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
- On local area network interfaces the upstream gateway should be "none".
- Selecting an upstream gateway causes the firewall to treat this interface as a [WAN](#) type interface.
- Gateways can be managed by [clicking here](#).

Lo primero que haremos es habilitar la interfaz y en la descripción la nombraremos como DMZ que es el nombre de nuestra red.

El siguiente paso será seleccionar en el tipo de configuración IPv4 el Static IPv4 ya que en VirtualBox no hay DHCP

La IP que añadiremos en este caso será 192.168.200.1 e importante la IP será /24.

Y por último ya guardamos

Una vez creada esta red nos vamos al PFSENSES y vemos como ya están creadas todas las redes.

Podemos observar que tenemos 3 interfaces WAN, LAN y DMZ.

```
VirtualBox Virtual Machine - Netgate Device ID: 3cf63cc4519d5391d8be

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on utm ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.37/24
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:
Message from syslogd@utm at Sep 14 17:34:00 ...
php-fpm[378]: /interfaces_assign.php: Successful login for user 'admin' from: 192.168.100.100 (Local Database)
```

The screenshot shows the pfSense web interface with the URL [https://192.168.100.1/services\\_dhcp.php?f=opt1](https://192.168.100.1/services_dhcp.php?f=opt1). The page title is "Services / DHCP Server / DMZ". The navigation bar includes links for Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and the pfSense logo. The main content area displays the "General Options" for the DMZ interface. The "Enable" checkbox is checked, and the "Ignore BOOTP queries" checkbox is unchecked. Under "Deny unknown clients", the dropdown is set to "Allow all clients". A note explains that if set to "Allow known clients from any interface", any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. Under "Ignore denied clients", the checkbox is unchecked. A note states that this option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured. Under "Ignore client identifiers", the checkbox is unchecked. A note indicates that this option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Under "Subnet", the value is 192.168.200.0. Under "Subnet mask", the value is 255.255.255.0. Under "Available range", the range is 192.168.200.1 - 192.168.200.254. Under "Range", the "From" field contains 192.168.200.100 and the "To" field contains 192.168.200.150. At the bottom, there is a link for "Additional Pools".

Lo siguiente que tenemos que hacer es irnos a DHCP Server para habilitar el DHCP en la red DMZ.

El rango lo pondremos de 100 a 150.

The screenshot shows a configuration interface for a DHCP server. The top navigation bar includes links for Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main form has sections for Servers, OMAPI, and Other Options. In the Servers section, the WINS servers are set to 'WINS Server 1' and 'WINS Server 2'. The DNS servers are set to '192.168.200.1', '1.1.1.1', and '8.8.8.8'. A note below the DNS servers says: 'Leave blank to use the system default DNS servers: The IP address of this firewall interface if DNS Resolver or Forwarder is enabled, otherwise the servers configured in General settings or those obtained dynamically.' In the OMAPI section, the Port is set to 'OMAPI Port'. In the Other Options section, the Gateway is set to '192.168.200.1'.

Ahora añadiremos los servidores DNS:

El primero será 192.168.200.1 (Local)

El segundo será 1.1.1.1 (Cloudflare)

El tercero será 8.8.8.8 (Google)

La puerta de enlace para poder tener internet será la IP 192.168.200.1 (PFSENSE)

Y por último guardamos.

```

Archivo Acciones Editar Vista Ayuda
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:27:53:0c:ba brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.1/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
        valid_lft 7190sec preferred_lft 7190sec
    inet6 fe80::d5e1:1d10:da00:6fb1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:9f:9e:26:a0 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever

```

Comprobamos la conexión IP en la máquina.

Properties	
Name	<input type="text" value="webs"/> The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	<input type="text"/>
Type	<input type="button" value="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	<input type="text" value="443"/> Entry added Tue, 29 Aug 2023 22:26:24 +0200 <input type="button" value="Delete"/> <input type="text" value="80"/> Entry added Tue, 29 Aug 2023 22:26:24 +0200 <input type="button" value="Delete"/>
<input type="button" value="Save"/> <input type="button" value="Export to file"/> <input type="button" value="Add Port"/>	

Ahora una vez configurada la RED DMZ debemos crear una serie de reglas para poder tener acceso a internet.

El primer paso que tenemos que hacer es crear un alias de puerto.

En este caso lo hemos definido como webs y hemos añadido los puertos 443 y 80 que son los que nos dan acceso a internet.

The screenshot shows the 'Edit Firewall Rule' interface on a pfSense system. The 'Action' section is set to 'Pass'. The 'Source' section has 'any' selected under 'Source' and 'any' under 'Source Address'. The 'Destination' section has 'any' selected under 'Destination' and 'any' under 'Destination Address'. Both sections have an 'Invert match' checkbox.

**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**: TCP  
Choose which IP protocol this rule should match.

**Source**

**Destination**

Vamos a crear la primera regla, dejaremos pasar el tráfico y el protocolo será TCP que es el que es orientando a la conexión. El origen y el destino de cualquier sitio.

The screenshot shows the 'Edit Firewall Rule' interface on a pfSense system. The 'Source' section has 'any' selected under 'Source' and 'any' under 'Source Address'. The 'Destination' section has 'any' selected under 'Destination' and 'any' under 'Destination Address'. Both sections have an 'Invert match' checkbox. The 'Destination Port Range' section shows 'From' and 'To' both set to 'Custom' with 'webs' selected in the dropdowns.

**Source**

**Destination**

**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**: habilitar webs  
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

**Rule Information**

Tracking ID	1693340909
Created	8/29/23 22:28:29 by admin@192.168.100.100 (Local Database)
Updated	8/29/23 22:28:29 by admin@192.168.100.100 (Local Database)

Aquí importante el destino de los puertos que es el que creamos anteriormente y definimos como webs (443 y 80) y guardamos.

https://192.168.100.1/firewall\_rules\_edit.php?id=7

Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

### 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** UDP

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 this setting must remain at its default value, any.

### Destination

**Destination**  Invert match any Destination Address /

**Destination Port Range** From DNS (53) Custom To DNS (53) 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

La siguiente regla que debemos crear es para el DNS.

Como en la anterior dejamos pasar el tráfico y el protocolo seleccionamos UDP que no está orientado a la conexión. El origen y el destino de cualquier lugar.

Y lo importante seleccionar el destino del puerto DNS (53) y guardamos.

192.168.100.1/firewall\_rules\_edit.php?id=6

Kali NetHunter Exploit-DB Google Hacking DB OffSec

### 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	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.	
<b>Source</b>	
Source	<input type="checkbox"/> Invert match DMZ net
Source Address /	
<b>Destination</b>	
Destination	<input type="checkbox"/> Invert match any
Destination Address /	
<b>Extra Options</b>	
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 logging, consider using a remote syslog server (see

La última regla que crearemos será con el protocolo ICMP el origen sería desde DMZ net y el destino cualquiera, guardamos y ya tendríamos las 3 reglas creadas que nos darían acceso a internet.

https://192.168.100.1/firewall\_rules.php?f=opt1

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense COMMUNITY EDITION

Firewall / Rules / DMZ

Floating WAN LAN DMZ **DMZ\_2** OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/672 B	IPv4 ICMP any	*	*	*	*	none		habilitar DNS	
<input checked="" type="checkbox"/>	0/6 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none	habilitar webs	
<input checked="" type="checkbox"/>	0/26 KiB	IPv4 TCP	*	*	*	webs	*	none	habilitar webs	

Add Add Delete Toggle Copy Save Separator

Aquí podemos observar las 3 reglas definidas.

```

Archivo  Acciones  Editar  Vista  Ayuda
└──(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:53:0c:ba 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 6979sec preferred_lft 6979sec
    inet6 fe80::d5e1:d10d:ab0d:6fb1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:9f:9e:26:a0 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever

└──(kali㉿kali)-[~]
$ ping marca.com
PING marca.com (34.147.120.111) 56(84) bytes of data.
64 bytes from 111.120.147.34.bc.googleusercontent.com (34.147.120.111): icmp_seq=1 ttl=54 time=49.6 ms
64 bytes from 111.120.147.34.bc.googleusercontent.com (34.147.120.111): icmp_seq=2 ttl=54 time=49.6 ms
64 bytes from 111.120.147.34.bc.googleusercontent.com (34.147.120.111): icmp_seq=3 ttl=54 time=72.3 ms
64 bytes from 111.120.147.34.bc.googleusercontent.com (34.147.120.111): icmp_seq=4 ttl=54 time=64.7 ms
64 bytes from 111.120.147.34.bc.googleusercontent.com (34.147.120.111): icmp_seq=5 ttl=54 time=50.7 ms
^C
--- marca.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4131ms
rtt min/avg/max/mdev = 49.553/57.362/72.277/9.417 ms
└──(kali㉿kali)-[~]
$ 

```

Hacemos la comprobación con PING y vemos que ya tenemos acceso a internet.

## 2.5 Configuración NAT/Port Forward

Vamos a configurar la NAT para poder servir una página web en internet, que es traducir una IP interna y hacer un reenvío de puerto. Con esta configuración podemos conectar la IP del PFSENSE con nuestro ordenador Windows.

### LAN

The screenshot shows the pfSense Firewall / NAT / Port Forward / Edit interface. The configuration details are as follows:

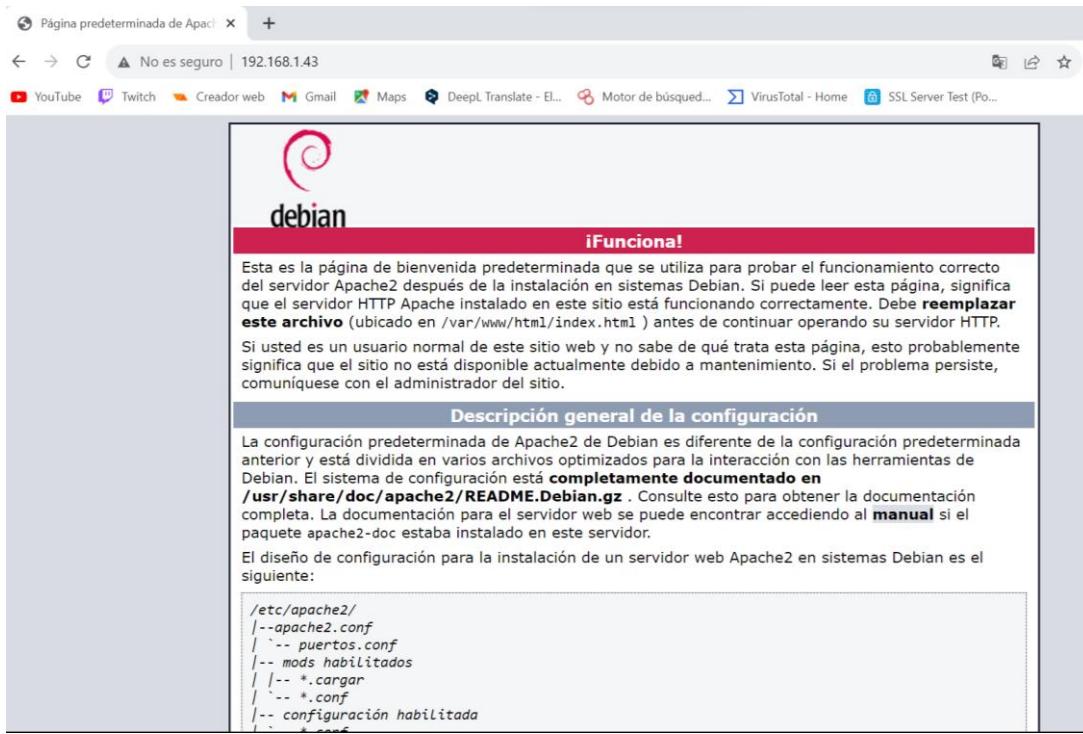
- Edit Redirect Entry**
- Disabled:**  Disable this rule
- No RDR (NOT):**  Disable redirection for traffic matching this rule
- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:**  Display Advanced
- Destination:**  Invert match. **WAN address:** Type: Address/mask /
- Destination port range:** HTTP From port: Custom To port: Custom
- Redirect target IP:** Single host Type: Address: 192.168.100.100

Below the form, there is a note: "Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4". It also states: "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)".

La interfaz por la que se va a acceder es por internet (WAN) y el protocolo que vamos a utilizar es TCP. El destino del puerto será HTTP (80) nos va a redirigir a la IP 192.168.100.100 (RED LAN) y guardamos.

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:53:0c:ba brd ff:ff:ff:ff:ff:ff
        inet 192.168.100.2/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
            valid_lft 4541sec preferred_lft 4541sec
        inet6 fe80::4e01:d10d:ab0d:6fb1/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:25:0e:a7:fc brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ service apache2 start
(kali㉿kali)-[~]
$
```

Para comprobar que funciona vamos a lanzar un apache2.



Aquí podemos observar que utilizando la IP WAN del PFSENSE en nuestro ordenador Windows podemos acceder al apache. Y comprobar que están conectados a través de la red WAN y el puerto 80.

### 3. Exportar VPN desde el PFSENSE

The screenshot shows the pfSense web interface at [https://192.168.100.1/pkg\\_mgr\\_installed.php](https://192.168.100.1/pkg_mgr_installed.php). The navigation bar includes links for Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and the pfSense logo. The main content area is titled "System / Package Manager / Installed Packages". The "Available Packages" tab is currently selected. A table lists the installed package "openvpn-client-export" with details: Name (openvpn-client-export), Category (security), Version (1.9.1), Description (Exports pre-configured OpenVPN Client configurations directly from pfSense software.), and Actions (trash, update, info). Below the table, it says "Package Dependencies: openvpn-client-export-2.6.5, openvpn-2.6.4, zip-3.0\_1, 7-zip-22.01". A note at the bottom states "Newer version available".

El 1º paso que tenemos que hacer es descargar el paquete de `openvpn-client-export` en el PFSENSE. Este paquete, aunque se instale desde Kali el que lo ejecuta es la máquina de UTM.

The screenshot shows the pfSense web interface at [https://192.168.100.1/system\\_cmanager.php?act=new](https://192.168.100.1/system_cmanager.php?act=new). The navigation bar includes links for Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and the pfSense logo. The main content area is titled "System / Certificate / Authorities / Edit". The "Authorities" tab is selected. A form titled "Create / Edit CA" is displayed with the following fields: Descriptive name (Keepcoding), Method (Create an internal Certificate Authority), Trust Store (checkbox for adding to OS trust store), Randomize Serial (checkbox for using random serial numbers), and Internal Certificate Authority (Key type: RSA, Key length: 2048, Digest Algorithm: sha256, Lifetime (days): 365).

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 algorithms invalid	
<u>Lifetime (days)</u>	365
<u>Common Name</u> Keepcoding	
The following certificate authority subject components are optional and may be left blank.	
<u>Country Code</u>	ES
<u>State or Province</u>	Madrid
<u>City</u>	Pozuelo de Alarcon
<u>Organization</u>	Keepcoding
<u>Organizational Unit</u>	IT

**Save**

El 2º paso es crear un certificado de autorización interno lo vamos a denominar Keepcoding, de tipo RSA, tiempo de vida 365 días al año y ponemos los datos de donde nos encontramos y el departamento que queramos. Los demás datos vienen por defecto.

Add/Sign a New Certificate

<u>Method</u>	Create an internal Certificate
<u>Descriptive name</u>	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: ?, >, <, &, /, \, ", '	
<b>Internal Certificate</b>	
<u>Certificate authority</u>	Keepcoding
<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 certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid	
<u>Lifetime (days)</u>	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.	
<u>Common Name</u>	vpn.keepcoding.local
The following certificate subject components are optional and may be left blank.	
<u>Country Code</u>	ES
<u>State or Province</u>	Madrid

4 |

[https://192.168.100.1/system\\_certmanager.php?act=new](https://192.168.100.1/system_certmanager.php?act=new)

Forums Exploit-DB OffSec

The following certificate subject components are optional and may be left blank.	
Country Code	ES
State or Province	Madrid
City	Pozuelo de Alarcon
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 Save

El 3º paso es crear un certificado interno este lo vamos a llamar VPN, importante certificado de autorización seleccionamos el que acabamos de crear al que hemos denominado Keepcoding, tipo RSA, lo nombramos vpn.keepcoding.local, tiempo de vida 365 días, rellenamos los datos de donde nos encontramos y por ultimo y más importante seleccionar, en tipo de certificado, el Server Certificate.

[https://192.168.100.1/vpn\\_openvpn\\_server.php?act=edit&id=0](https://192.168.100.1/vpn_openvpn_server.php?act=edit&id=0)

ms Exploit-DB OffSec

**pfSense COMMUNITY EDITION** System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export

**General Information**

Description VPN-Remota-LAN  
A description of this VPN for administrative reference.

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

Unique VPN ID Server 1 (ovpn1)

**Mode Configuration**

Server mode Remote Access ( SSL/TLS + User Auth )

Backend for authentication Local Database

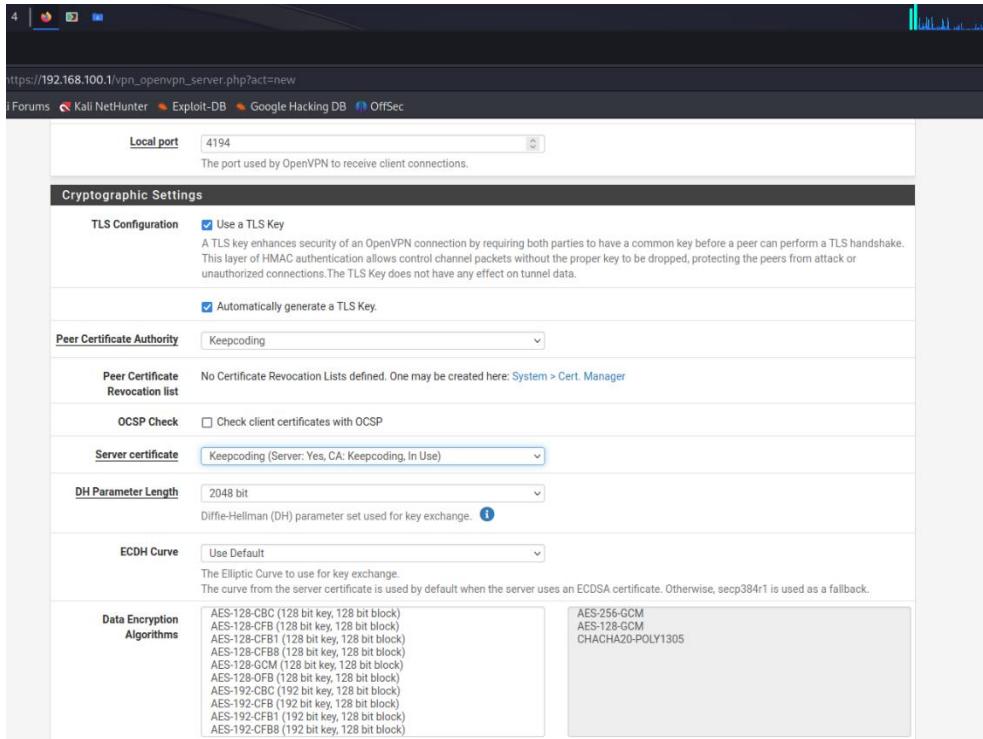
Device mode tun - Layer 3 Tunnel Mode  
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
"tap" mode is capable of carrying 802.3 (OSI Layer 2).

**Endpoint Configuration**

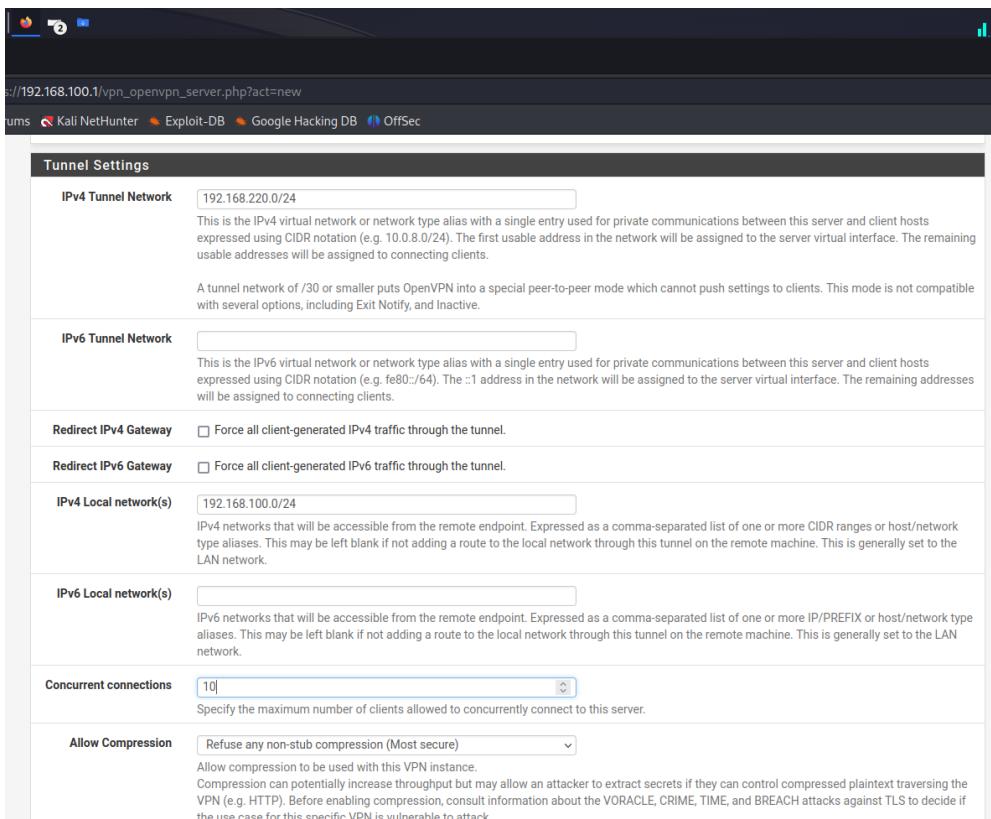
Protocol TCP on IPv4 only

Interface WAN

El 4º paso es irnos a OpenVPN y vamos a crear un servidor al que llamaremos VPN-Remota-LAN ya que estará conectada a nuestra red LAN por lo que estará enlazada a nuestra maquina Windows. El tipo de servidor es muy importante, seleccionaremos acceso remoto con contraseña y certificado, la autenticación por la base de datos local, el tipo de dispositivo tipo Layer 3 Tunnel mode de tipo IP, el protocolo seleccionamos TCP e interfaz WAN (nuestro router) el puerto local podremos 4194.



Aquí importante seleccionar el certificado para el servidor el que hemos creado de VPN.



Como hemos elegido el tipo de dispositivo tipo Layer 3 Tunnel mode vamos a crear un IP nueva que en este caso será 192.168.220.0/24, la IP local a la que accederemos será 192.168.100.0/24 que es la red LAN. Los máximos de usuarios conectados serán 10. Las demás opciones vienen por defecto, por lo que ya guardaríamos toda la configuración.

The screenshot shows the pfSense web interface under the 'VPN / OpenVPN / Servers' section. A single OpenVPN server is listed:

OpenVPN Servers					Description	Actions
Interface	Protocol / Port	Tunnel Network	Mode / Crypto			
WAN	TCP4 / 4194 (TUN)	192.168.220.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits		VPN-Remota-LAN	

A green '+ Add' button is located at the bottom right of the table.

Ya podemos ver como tenemos nuestro servidor VPN creado.

The screenshot shows the pfSense web interface under the 'System / User Manager / Users / Edit' section. A new user account is being created:

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

El 5º paso es crear un usuario, rellenamos los datos, ponemos la contraseña y lo más importante hay que marcar “crea un certificado para este usuario”

The screenshot shows the 'Create Certificate for User' form on a pfSense web interface. The 'Descriptive name' field contains 'fray'. The 'Certificate authority' dropdown is set to 'Keepcoding'. The 'Key type' dropdown is set to 'RSA'. The 'Key Length' dropdown is set to '2048'. The 'Digest Algorithm' dropdown is set to 'sha256'. The 'Lifetime' dropdown is set to '3650'. The 'Keys' section has an empty 'Authorized SSH Keys' input field and an empty 'IPsec Pre-Shared Key' input field. The 'Shell Behavior' section has a checked 'Keep Command History' checkbox with a descriptive note below it.

Lo siguiente es poner la descripción del nombre, el certificado de autorización el que hemos creado de Keepcoding y lo demás viene por defecto, guardamos.

The screenshot shows the 'System / User Manager / Users' page. The 'Users' tab is selected. A table lists two users: 'admin' (Status: ✓, Groups: admins) and 'fray' (Status: ✓, Groups: ). There are 'Add' and 'Delete' buttons at the bottom right.

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	
fray	fray	✓		

Vemos como aparece ya el usuario creado.

The screenshot shows the pfSense OpenVPN Client Export Utility interface. At the top, it displays the URL [https://192.168.100.1/vpn\\_openvpn\\_export.php](https://192.168.100.1/vpn_openvpn_export.php). The navigation bar includes links for Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and the pfSense COMMUNITY EDITION logo. Below the navigation bar, there are tabs for Server, Client, Client Specific Overrides, Wizards, and Client Export. The main content area is titled "OpenVPN / Client Export Utility". It has a sub-section titled "OpenVPN Server" where the "Remote Access Server" is set to "VPN-Remota-LAN TCP4:4194". The "Client Connection Behavior" section contains several configuration options: "Host Name Resolution" (Interface IP Address), "Verify Server CN" (Automatic - Use verify-x509-name where possible), "Block Outside DNS" (unchecked), "Legacy Client" (unchecked), "Silent Installer" (unchecked), and "Bind Mode" (Do not bind to the local port). The "Certificate Export Options" section is also visible.

El último paso será exportar nuestro certificado creado, las opciones ya vienen por defecto.

The screenshot shows the pfSense OpenVPN Client Export Utility interface. The "Advanced" section contains a text input field for "Additional configuration options" with the placeholder text: "Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon." Below this is an example: "EXAMPLE: remote-random;". There is a "Save as default" button. The "Search" section includes a search term input field, a search button, and a clear button. The "OpenVPN Clients" section lists a single client named "fray" with a certificate name of "fray". To the right of the client list is a "Export" section containing various download links for different clients and configurations, such as "Most Clients", "Android", "OpenVPN Connect (iOS/Android)", "Archive", "Config File Only", "Current Windows Installers (2.6.5-1x001)", "Previous Windows Installers (2.5.9-1x601)", "Legacy Windows Installers (2.4.12-1x601)", "Viscosity (Mac OS X and Windows)", "Viscosity Bundle", and "Viscosity Inline Config". A note at the bottom states: "Only OpenVPN-compatible user certificates are shown".

Aquí vemos como está nuestro certificado y la damos al mayor número de clientes para descargarlo.

```
1 dev tun
2 persist-tun
3 tunctl up
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 auth-client
8 client
9 resolve-retry infinite
10 remote 192.168.1.145 4194 tcp
11 nobind
12 resolvconf-x509-name "vpn.keepcoding.local" name
13 auth-user-pass
14 remote-cert-tls server
15
16 <ca>
17 -----BEGIN CERTIFICATE-----
18 MITEIzCAKzAwIBAgIJK0UHPUHgCkxxcQwJcAwQDYJk0ZtHvcNAQELBQAwcJETMBEGAUUE
19 AMXK52VlGvZG1uzL2MAGA1UEBMMCRWVnD2ANBgNVAgTBhIn2j3pZDEm0k
20 A1UEBESKA05G9Wsb3pBZS8BgFyT29uH8wEoDVAQEcwLWwv29uahfR0sw
21 A1UEBESKA05G9Wsb3pBZS8BgFyT29uH8wEoDVAQEcwLWwv29uahfR0sw
22 GbVBAMTCK1Zb0joRjpmc2xAJb2NvBAYAKVYMo8oDy9VQ01EazNyMwAg
23 GzAzbBwNAct1tBewv1t6bgZ0igxhcnvjtBemGE1ueCHMS2V1tGvzolu
24 ZEMLMAGA1UECwQSMC9vQwIwIMAGCgSgQ1JDEBAMQUA1IDBwMEwGKA1BQ0d
25 BgNVBAsTExM5Uk5WTFmfLwLjD21jT2Hwv1tGvzolu
26 T1gLEtHQBBLQ00LjTgF
27 YV0nf1tyu0u0w+e2vbu1wCYQdgFp1j94w8t1wU0u0wPuFoH+U0j0s+Jt8q
28 11BtB7Tgjwv2AXJ0PsYmnu11B91j940191ZzYwLQsOpUcMD0YV1G0rTnw
29 B0rFR1DX0ymwSyRyHnHpsV13XMu0dF0YurAcHrpPSXuN33uageWfM4td
30 B0rFR1DX0ymwSyRyHnHpsV13XMu0dF0YurAcHrpPSXuN33uageWfM4td
31 fo/oxg4cm9bM05Jb9gvuHSIegZsgZL4jW773ubdeZnGf0/oxg4cm9b0ak
32 E2M6N0M0EQYQVOQD0EwpLjWwV2yku5mNsQCD0DQ0QExJ2UEPMACa1UEC0M
33 TWFcmk1LewwQyVQHxExJ2qj1zXvIGR1EfsvXJ2b2wExARBe9wBqTC1t
34 TWFcmk1LewwQyVQHxExJ2qj1zXvIGR1EfsvXJ2b2wExARBe9wBqTC1t
35 A1Ub0dRJ0RJ0BwNqk19t0wB8sfM0ACKAEar1wmbwBtEq-oms3726s480
36 hhsXzJBBP91JbdpFH0DmInwLuTHF5Exu0ZP1M6XV3jBwJ3WwERw0d8uW
37 t9B0CZ526Wb05G05D0x0Gwtw1jp1j2ch08u1D1j01969y193kxBwSL1tFeFaxt+Hd
38 bmrtJ45SVk0dPmAHAXAxASUyQx0l615FmC0L94JhKmfsY3y6y6sdU1J
40 Fd6mJhLkV7vfrqR1ex7zK0MmHMrzu/jeEs0LlVHtJHrJfHstIuLwHwRq0q=
41 -----END CERTIFICATE-----
42 <cert>
43 <cert>
44 -----BEGIN CERTIFICATE-----
45 MITEIzCAKzAwIBAgIJK0UHPUHgCkxxcQwJcAwQDYJk0ZtHvcNAQELBQAwcJETMBEGAUUE
46 Y29uahfR0swEoDVAQEcwLWwv29uahfR0swEoDVAQEcwLWwv29uahfR0sw
```

Certificado descargado.

https://192.168.100.1/firewall\_rules\_edit.php?if=wlan&after=-1

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**pfSense COMMUNITY EDITION**

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / Edit

**Edit Firewall Rule**

<b>Action</b>	<input type="button" value="Pass"/> 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.
<b>Disabled</b>	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
<b>Interface</b>	<input type="button" value="WAN"/> WAN	Choose the interface from which packets must come to match this rule.
<b>Address Family</b>	<input type="button" value="IPv4"/> IPv4	Select the Internet Protocol version this rule applies to.
<b>Protocol</b>	<input type="button" value="TCP"/> TCP	Choose which IP protocol this rule should match.
<b>Source</b>		
<b>Source</b>	<input type="checkbox"/> Invert match	<input type="text" value="any"/> Source Address / <input type="button"/>
<b>Destination</b>		
<b>Destination</b>	<input type="checkbox"/> Invert match	<input type="text" value="This firewall (self)"/> Destination Address / <input type="button"/>

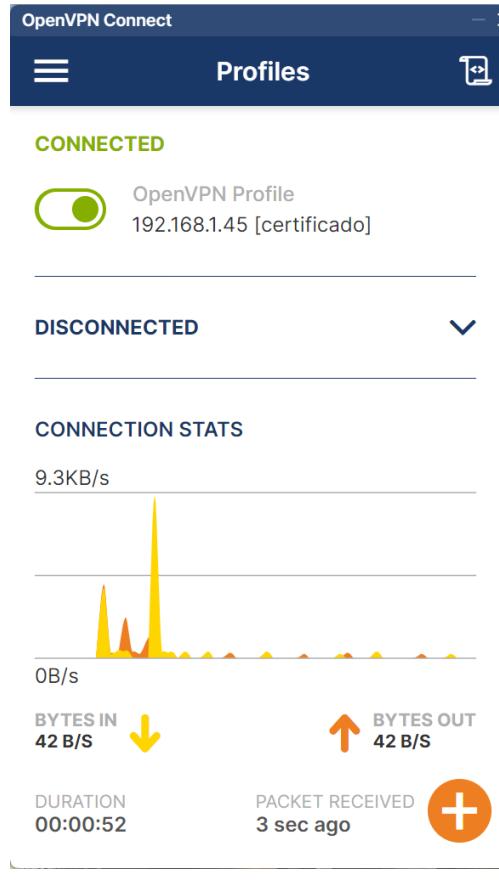
Ahora lo que tenemos que hacer es crear una regla en WAN para permitir pasar el tráfico. El destino tenemos que seleccionar “This firewall”

The screenshot shows the pfSense firewall rules configuration interface. A rule is being edited for TCP port 4194 to 4194. The rule has a source of 'any' and a destination of 'This firewall (self)'. The 'Log' checkbox is checked, and the description is set to 'VPN2'. The 'Save' button is visible at the bottom.

Destino del puerto del 4194 a 4194, la descripción pondremos VPN y guardamos.

The screenshot shows the OpenVPN Connect profile editor. A profile named '192.168.1.45 [certificado]' is being edited. The server hostname is set to '192.168.1.45'. The username is 'fray'. The 'Save' button is visible at the top right.

Para terminar, importamos el certificado al OpenVPN Conenct.



Aquí vemos como ya está conectada la VPN a nuestra red LAN a través de la WAN, en nuestro equipo Windows.

## 4. HONEYPOTS

El Honeypot que vamos a lanzar en DMZ es el Cowrie “SSH” a través el Docker.

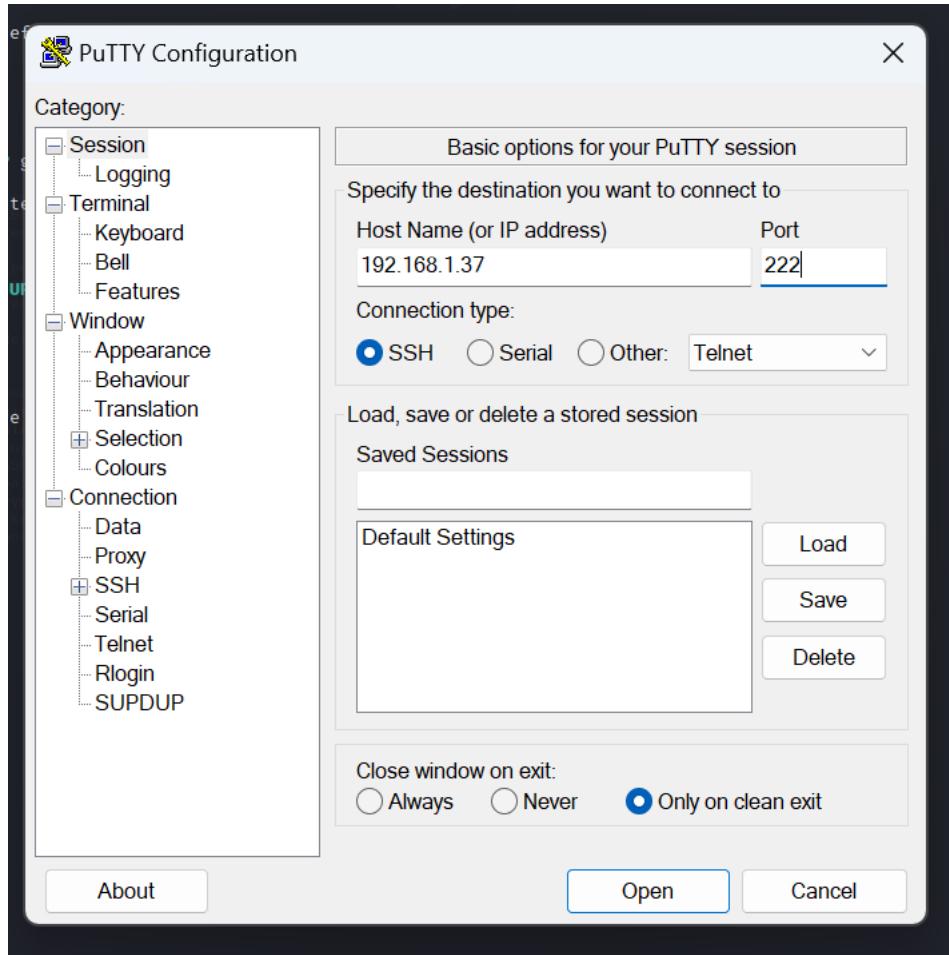
```

root@kali: /home/kali
# docker run -p 222:2222 cowrie/cowrie qdisc noqueue state UNKNOWN proto default qlen 1000
/cowrie/cowrie-env/lib/python3.9/site-packages/twisted/conch/ssh/transport.py:97: CryptographyDeprecationWarning: Blowfish has been deprecated
b"blowfish-cbc": (algorithms.Blowfish, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.9/site-packages/twisted/conch/ssh/transport.py:101: CryptographyDeprecationWarning: CAST5 has been deprecated
b"cast128-cbc": (algorithms.CAST5, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.9/site-packages/twisted/conch/ssh/transport.py:106: CryptographyDeprecationWarning: Blowfish has been deprecated
b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/cowrie/cowrie-env/lib/python3.9/site-packages/twisted/conch/ssh/transport.py:107: CryptographyDeprecationWarning: CAST5 has been deprecated
b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
2023-09-19T17:50:06+0000 [-] Python Version 3.9.2 (default, Feb 28 2021, 17:03:44) [GCC 10.2.1 20210110]
2023-09-19T17:50:06+0000 [-] Twisted Version 23.8.0
2023-09-19T17:50:06+0000 [-] Cowrie Version 2.5.0
2023-09-19T17:50:06+0000 [-] Loaded output engine: jsonlog qdisc noqueue state UP group default
2023-09-19T17:50:06+0000 [twisted.scripts._twisted_unix.UnixAppLogger#info] twisted 23.8.0 (/cowrie/cowrie-env/bin/python3 3.9.2) starting up.
2023-09-19T17:50:06+0000 [twisted.scripts._twisted_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2023-09-19T17:50:06+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f68565d8b50>
2023-09-19T17:50:06+0000 [-] Generating new RSA keypair ...
2023-09-19T17:50:06+0000 [-] Generating new ECDSA keypair ... qdisc noqueue master docker0 state UP group default
2023-09-19T17:50:06+0000 [-] Generating new ed25519 keypair ... tnsid 0
2023-09-19T17:50:06+0000 [-] Ready to accept SSH connections
[valid_ltt forever preferred_ltt forever]

root@kali: /home/kali

```

El primer paso que hemos hecho es lanzar el contenedor Docker para que arranque con este comando: docker run -p 222:2222 cowrie/cowrie. El puerto de la izquierda es del anfitrión y el de la derecha del invitado.



El siguiente paso es abrir la aplicación PuTTY ponemos la IP y el puerto de nuestro Kali. Que en este caso es 192.168.1.37 y 222.

A screenshot of a PuTTY terminal window titled "192.168.1.37 - PuTTY". The session log shows:

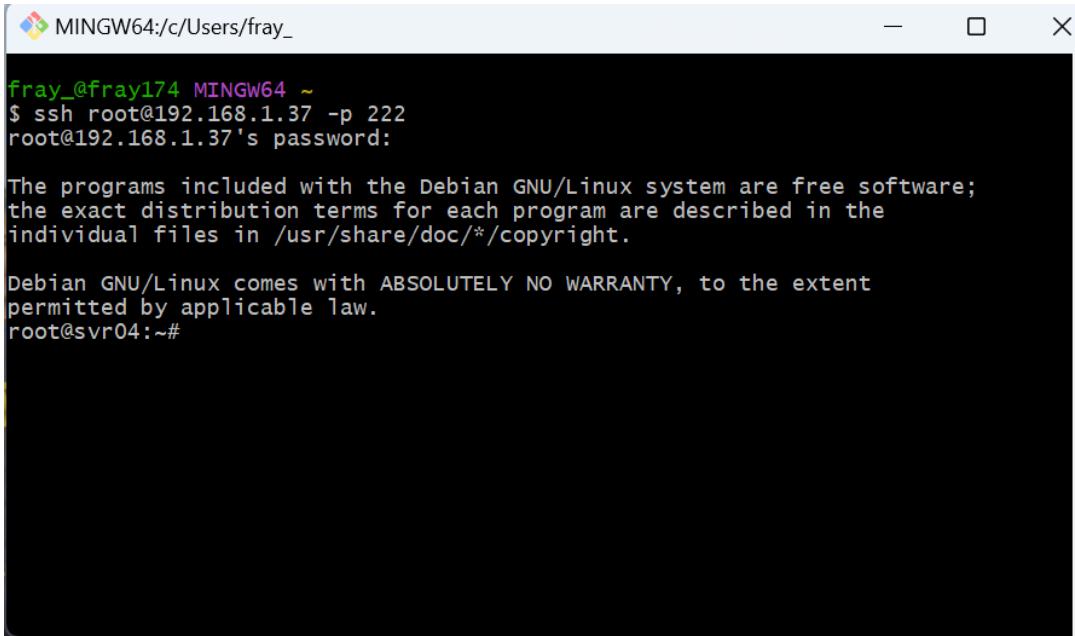
```
login as: root
root@192.168.1.37's password:

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:~#
```

The terminal window has a black background and white text.

Se nos abrirá una consola en PuTTY y tendremos que poner un usuario y contraseña para estar dentro.

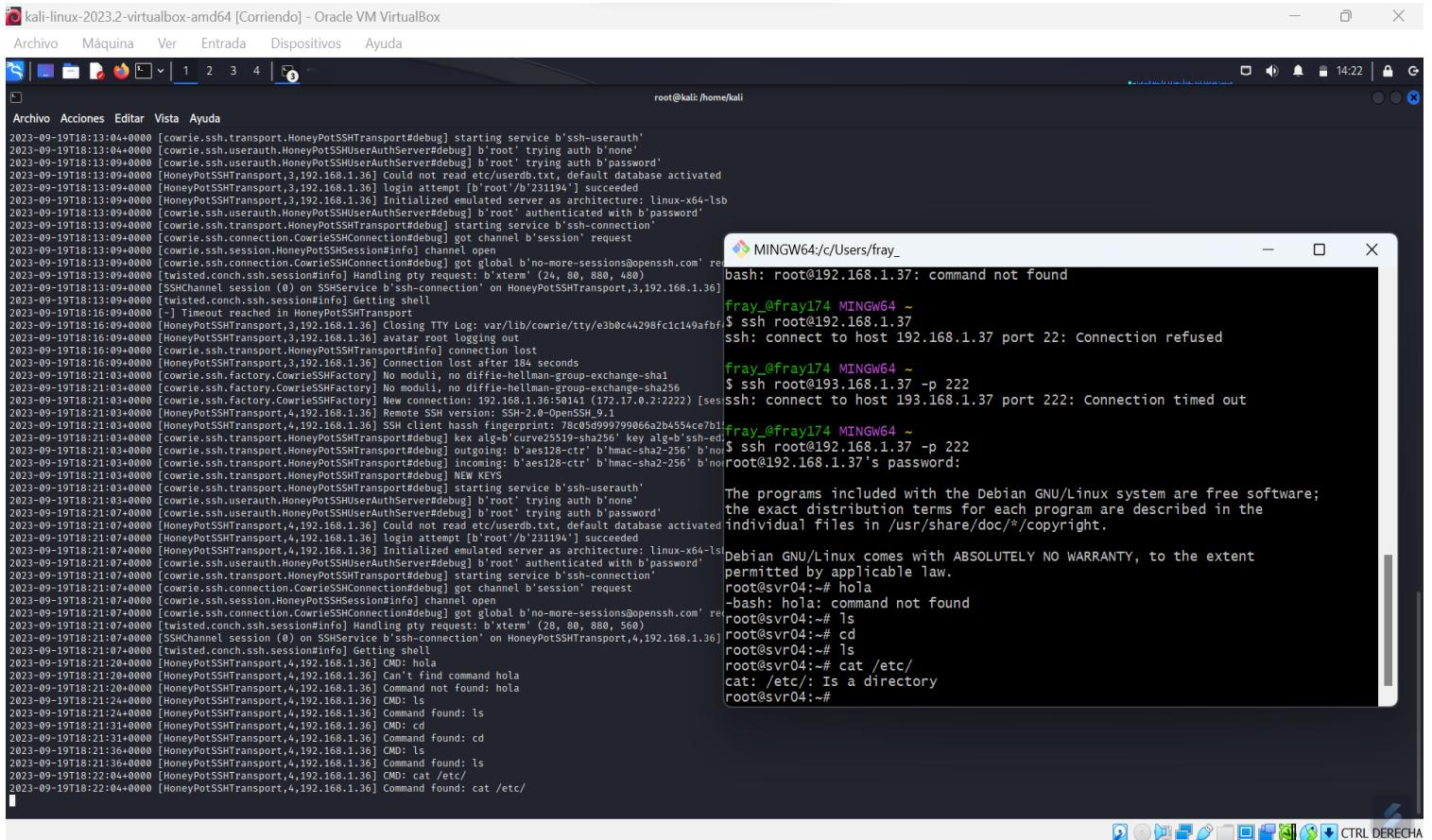


```
MINGW64:/c/Users/fray_
fray_@fray174 MINGW64 ~
$ ssh root@192.168.1.37 -p 222
root@192.168.1.37's password:

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:~#
```

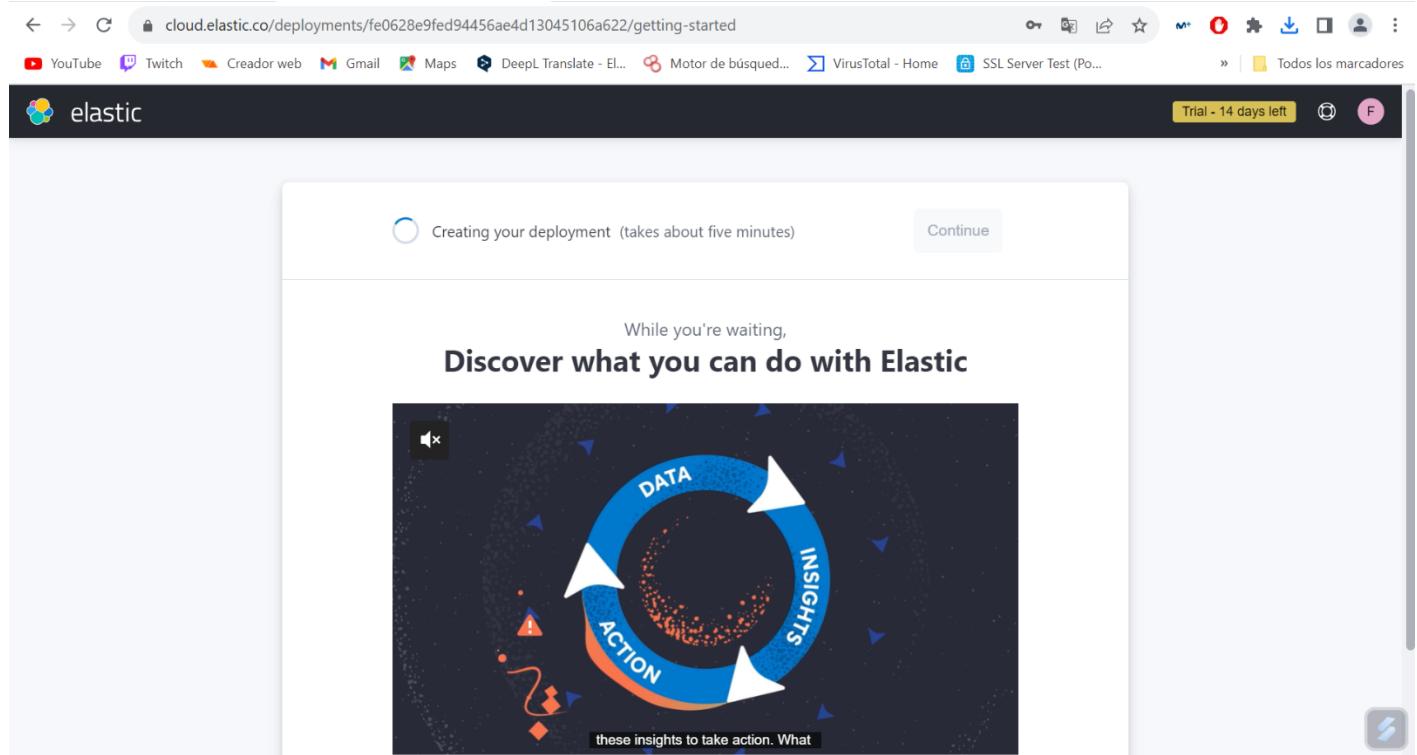
Lo siguiente que debemos hacer es abrir una terminal en Windows y poner el siguiente comando: SSH [root@192.168.1.37](ssh://root@192.168.1.37) -p 222 (en este caso mi IP) y después la contraseña que hemos establecido, una vez hecho esto estamos dentro.



```
kali-linux-2023.2-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali:~/home/kali
Archivo Acciones Editar Vista Ayuda
2023-09-19T18:13:04+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2023-09-19T18:13:04+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2023-09-19T18:13:09+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2023-09-19T18:13:09+0000 [HoneyPotSSHTransport,3,192.168.1.36] Could not read etc/usedb.txt, default database activated
2023-09-19T18:13:09+0000 [HoneyPotSSHTransport,3,192.168.1.36] login attempt [b'root'/b'231194'] succeeded
2023-09-19T18:13:09+0000 [HoneyPotSSHTransport,3,192.168.1.36] Initialized emulated server as architecture: linux-x64-1sb
2023-09-19T18:13:09+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2023-09-19T18:13:09+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2023-09-19T18:13:09+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2023-09-19T18:13:09+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2023-09-19T18:13:09+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' re
2023-09-19T18:13:09+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm' (24, 80, 880, 480)
2023-09-19T18:13:09+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,3,192.168.1.36]
2023-09-19T18:13:09+0000 [twisted.conch.ssh.session#info] Getting shell
2023-09-19T18:13:09+0000 [cowrie.ssh.transport.HoneyPotSSHTransport,3,192.168.1.36] Closing TTY Log: var/lib/cowrie/tty/e3b0c44298fc1c149afbf
2023-09-19T18:13:09+0000 [HoneyPotSSHTransport,3,192.168.1.36] avatar root logging out
2023-09-19T18:16:09+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2023-09-19T18:16:09+0000 [HoneyPotSSHTransport,3,192.168.1.36] Connection lost after 184 seconds
2023-09-19T18:21:03+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2023-09-19T18:21:03+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2023-09-19T18:21:03+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.36:50141 (172.17.0.2:2222) [ses
2023-09-19T18:21:03+0000 [HoneyPotSSHTransport,4,192.168.1.36] Remote SSH version: SSH-2.0-OpenSSH_9.1
2023-09-19T18:21:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] RSA client hash fingerprint: 78c05d999799066a2b4554cc7b1
2023-09-19T18:21:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] key alg=b'ssh-ed25519'
2023-09-19T18:21:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] b'mac-sha2-256' b'no'
2023-09-19T18:21:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] b'mac-sha2-256' b'no'
2023-09-19T18:21:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] b'mac-sha2-256' b'no'
2023-09-19T18:21:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEED KEYS
2023-09-19T18:21:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2023-09-19T18:21:03+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2023-09-19T18:21:07+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2023-09-19T18:21:07+0000 [HoneyPotSSHTransport,4,192.168.1.36] Could not read etc/usedb.txt, default database activated
2023-09-19T18:21:07+0000 [HoneyPotSSHTransport,4,192.168.1.36] login attempt [b'root'/b'231194'] succeeded
2023-09-19T18:21:07+0000 [HoneyPotSSHTransport,4,192.168.1.36] Initialized emulated server as architecture: linux-x64-1sb
2023-09-19T18:21:07+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2023-09-19T18:21:07+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2023-09-19T18:21:07+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2023-09-19T18:21:07+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm' (28, 80, 880, 560)
2023-09-19T18:21:07+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,4,192.168.1.36]
2023-09-19T18:21:07+0000 [twisted.conch.ssh.session#info] Getting shell
2023-09-19T18:21:20+0000 [HoneyPotSSHTransport,4,192.168.1.36] CMD: hola
2023-09-19T18:21:20+0000 [HoneyPotSSHTransport,4,192.168.1.36] Can't find command hola
2023-09-19T18:21:24+0000 [HoneyPotSSHTransport,4,192.168.1.36] Command not found: hola
2023-09-19T18:21:24+0000 [HoneyPotSSHTransport,4,192.168.1.36] CMD: ls
2023-09-19T18:21:31+0000 [HoneyPotSSHTransport,4,192.168.1.36] Command found: cd
2023-09-19T18:21:31+0000 [HoneyPotSSHTransport,4,192.168.1.36] Command found: cd
2023-09-19T18:21:36+0000 [HoneyPotSSHTransport,4,192.168.1.36] CMD: ls
2023-09-19T18:21:36+0000 [HoneyPotSSHTransport,4,192.168.1.36] Command found: ls
2023-09-19T18:22:04+0000 [HoneyPotSSHTransport,4,192.168.1.36] CMD: cat /etc/
2023-09-19T18:22:04+0000 [HoneyPotSSHTransport,4,192.168.1.36] CMD: cat /etc/
2023-09-19T18:22:04+0000 [HoneyPotSSHTransport,4,192.168.1.36] Command found: cat /etc/
```

Por último, podemos ver cómo están conectadas las dos consolas a través de la red WAN, mientras que en la de Windows lanzo diferente comandos la de Kali me va detectando los logs, por lo que ya tendríamos nuestro Honeypot corriendo.

## 5. Elasticsearch en la nube



El primer paso que debemos hacer después de habernos creado una cuenta es crear un “Deployment”

A screenshot of a web browser showing the 'Setup guide: step 1' for Elasticsearch. The URL is 'fray-keepcoding.kb.eu-west-1.aws.found.io:9243/app/home#/getting\_started?useCase=security'. The page has a header with the Elasticsearch logo and a search bar. Below the header, there is a 'Setup guide: step 1' button. The main content area shows six cards under the heading 'Setup guides': 1. 'Set up vector search' (with a vector icon), 2. 'Collect and analyze my logs' (with a log icon), 3. 'Detect threats in my data with SIEM' (with a threat icon), 4. 'Build a semantic search experience' (with a plus icon), 5. 'Monitor my application performance (APM / tracing)' (with a monitor icon), 6. 'Secure my hosts with endpoint security' (with a lock icon). At the bottom, there are three more cards: 7. 'Build an application on' (with a gear icon), 8. 'Monitor my host metrics' (with a chart icon), and 9. 'Secure my cloud assets with cloud' (with a shield icon).

Una vez creado el “deployment” no aparecerá esta ventana con diferentes opciones. La que vamos a seleccionar nosotros es la de “Detect threats in my data with SIEM”

The screenshot shows the 'Elastic Defend' integration page. At the top, there's a navigation bar with tabs for 'Overview', 'Settings', and 'Advanced'. Below the tabs, the 'Elastic Defend Integration' section is displayed. It includes a brief description of what Elastic Defend provides, a list of features (Prevent complex attacks, Alert in high fidelity, Detect threats in high fidelity), and a sidebar with details like Version 8.9.1, Category EDR/XDR, Security, and Elasticsearch assets. A large blue button at the bottom right says '+ Add Elastic Defend'.

Lo siguiente que haremos es añadir el Elastic Defend.

The screenshot shows the 'Add integration - Elastic Defend' page. It displays instructions for installing the Elastic Agent on a host. A step titled 'Install Elastic Agent on your host' is highlighted with a green checkmark. Below it, there's a code snippet for Windows installation:

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/windows/elastic-agent-8.9.2-windows-x86_64.zip -DestinationPath .
Expand-Archive .\elastic-agent-8.9.2-windows-x86_64.zip -DestinationPath .
.\elastic-agent.exe install --url=https://fe0628e9fed94456ae4d13045106a622.fleet.eu-west-1.e
```

A blue button at the bottom of the code block says 'Copied'.

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.

```
Administrator: Windows PowerShell
PS C:\Users\fray_> $ProgressPreference = 'SilentlyContinue'
>> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.9.2-windows-x86_64.zip -OutFile elastic-agent-8.9.2-windows-x86_64.zip
>> Expand-Archive .\elastic-agent-8.9.2-windows-x86_64.zip -DestinationPath .
PS C:\Users\fray_> dir

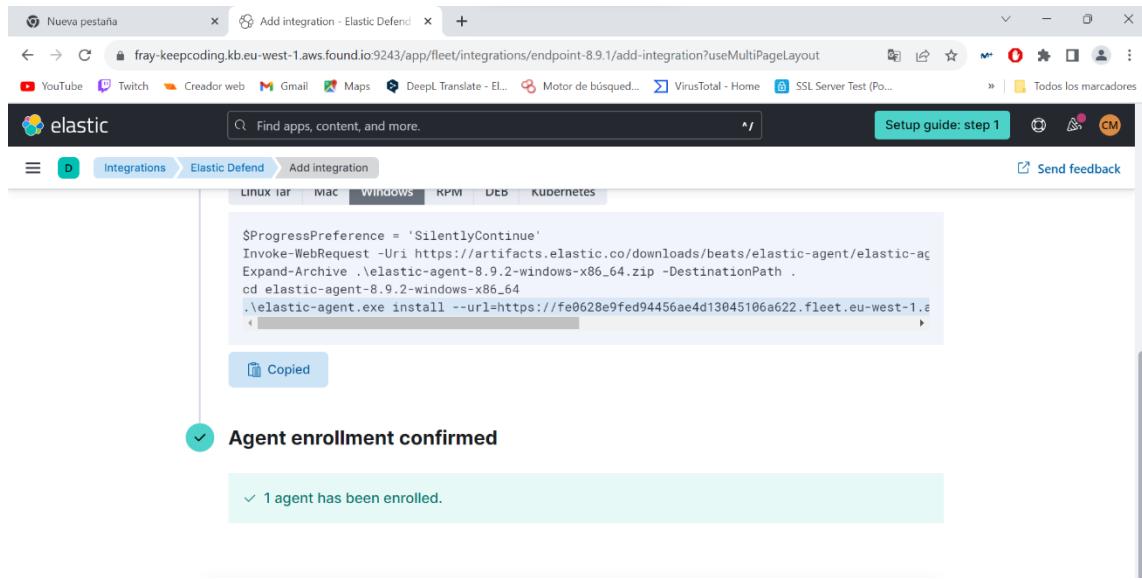
Directorio: C:\Users\fray_


Mode                LastWriteTime       Length Name
----                -----        ---- 
d-----        28/08/2023    22:45          .conda
d-----        24/02/2023    19:47          .config
d-----        03/07/2023    18:33          .continuum
d-----        16/03/2023    20:50          .gem
d-----        03/05/2023    18:26          .jdlrc
d-----        03/07/2023    18:35          .ipython
d-----        03/07/2023    18:35          .matplotlib
d-----        31/01/2023    20:51          .ms-ad
d-----        03/07/2023    18:34          .spyder-py3
d-----        19/09/2023    20:10          .ssh
d-----        17/06/2023    18:07          .vagrant.d
d-----        20/09/2023    19:27          .VirtualBox
d-----        04/07/2023    18:26          .vscode
d-----        06/07/2023    22:57          anaconda3
d-r----        24/11/2022   20:49          Contacts
d-----        24/02/2023    21:49          Documents
d-r----        20/09/2023   20:48          Downloads
d-----        20/09/2023    21:57          elastic-agent-8.9.2-windows-x86_64
d-r----        24/11/2022   20:49          Favorites
d-----        05/09/2023    20:03          Links
d-----        16/03/2023    23:43          metasploitable3-workspace
d-----        24/11/2022   20:49          Music
d-----        16/03/2023    20:23          Nueva carpeta
d-r--1         20/09/2023   19:46          OneDrive
d-r--1         20/09/2023   19:46          OneDrive - Universidad Carlos III de Madrid
d-r---        24/11/2022   20:49          Saved Games
d-r---        24/11/2022   20:49          Searches
d-----        10/07/2023    18:24          source
d-----        03/05/2023    17:55          spiderfoot
d-r---        24/11/2022   20:49          Videos
d-----        01/09/2023    18:17          VirtualBox VMs
d-a---        19/09/2023   20:12          1940 .bash_history
d-----        279352261      elastic-agent-8.9.2-windows-x86_64.zip
```

```
Administrator: Windows PowerShell
PS C:\Users\fray_> cd elastic-agent-8.9.2-windows-x86_64
PS C:\Users\fray_\elastic-agent-8.9.2-windows-x86_64> .\elastic-agent.exe install --url=https://fe0628e9fed94456ae4d13045106a622.fleet.eu-west-1.aws.found.io:443 --enrollme
nt-token=bmVnOHM9b02tLwdahJQtZ3Mtbms5MwI4Y1QtMkhRYU9ajBCb19sU09FQO=
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y
```

```
PS C:\Users\fray_> cd elastic-agent-8.9.2-windows-x86_64
PS C:\Users\fray_\elastic-agent-8.9.2-windows-x86_64> .\elastic-agent.exe install --url=https://fe0628e9fed94456ae4d13045106a622.fleet.eu-west-1.aws.found.io:443 --enrollme
nt-token=bmVnOHM9b02tLwdahJQtZ3Mtbms5MwI4Y1QtMkhRYU9ajBCb19sU09FQO=
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y
{"log.level": "info", "@timestamp": "2023-09-20T22:05:16.599+0200", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": 478}, "message": "Starting enrollment to URL: https://fe0628e9fed94456ae4d13045106a622.fleet.eu-west-1.aws.found.io:443", "ecs.version": "1.6.0"}
{"log.level": "info", "@timestamp": "2023-09-20T22:05:35.281+0200", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": 276}, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0"}
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
PS C:\Users\fray_\elastic-agent-8.9.2-windows-x86_64
```

Lanzamos los distintos comandos en nuestra consola Windows para que corra, le damos a sí y ya lo tendríamos instalado.

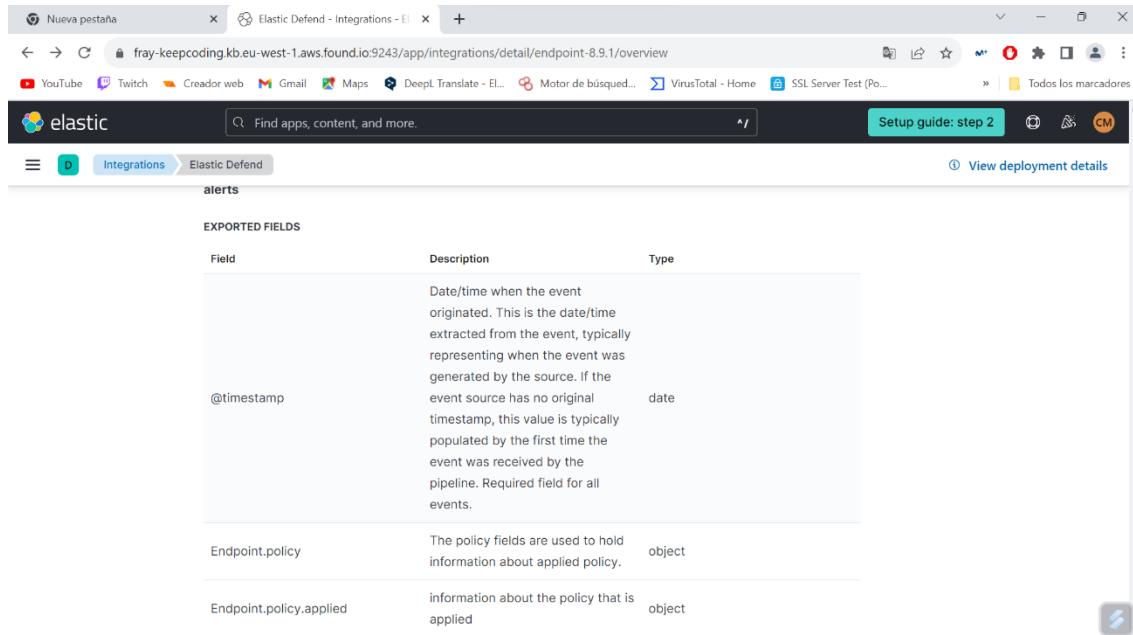


The screenshot shows a browser window with the URL [fray-keepcoding.kb.eu-west-1.aws.found.io:9243/app/fleet/integrations/endpoint-8.9.1/add-integration?useMultiPageLayout](https://fray-keepcoding.kb.eu-west-1.aws.found.io:9243/app/fleet/integrations/endpoint-8.9.1/add-integration?useMultiPageLayout). The tab title is "Add integration - Elastic Defend". The page displays a command for installing the Elastic Agent on Windows:

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.9.2-windows-x86_64.zip -DestinationPath .  
Expand-Archive .\elastic-agent-8.9.2-windows-x86_64  
.\\elastic-agent.exe install --url=https://fe0628e9fed94456ae4d13045106a622.fleet.eu-west-1.e...
```

A blue button labeled "Copied" is visible below the command. A green success message at the bottom left says "Agent enrollment confirmed" with a checkmark icon. Below it, another message states "1 agent has been enrolled.".

Ya vemos como se ha confirmado en la nube. Ahora le daremos añadir y confirmar datos.



The screenshot shows a browser window with the URL [fray-keepcoding.kb.eu-west-1.aws.found.io:9243/app/integrations/detail/endpoint-8.9.1/overview](https://fray-keepcoding.kb.eu-west-1.aws.found.io:9243/app/integrations/detail/endpoint-8.9.1/overview). The tab title is "Elastic Defend - Integrations - [ ]". The page displays a table of exported fields:

Field	Description	Type
@timestamp	Date/time when the event originated. This is the date/time extracted from the event; typically representing when the event was generated by the source. If the event source has no original timestamp, this value is typically populated by the first time the event was received by the pipeline. Required field for all events.	date
Endpoint.policy	The policy fields are used to hold information about applied policy.	object
Endpoint.policy.applied	Information about the policy that is applied	object

Vemos como ya empieza a lanzar distintos logs.

The screenshot shows the Elastic Kibana interface with the 'Endpoints' dashboard selected. The left sidebar has a 'Security' section with various navigation options. The main content area is titled 'Endpoints' and shows a single endpoint named 'fray174'. The table includes columns for Endpoint, Agent status, Policy, Policy stat..., OS, IP address, Version, Last active, and Actions. The endpoint details are: Agent status is 'Healthy', Policy is 'endpoint-1 rev. 1', OS is 'Windows', IP address is '169.254.122.161', Version is '8.9.2', and Last active is 'Sep 20, ...'. There is also a 'Rows per page' dropdown set to 10 and a pagination indicator showing page 1 of 1.

Podemos observar como ya están integrado los “Endpoints” en nuestra maquina Windows.

The screenshot shows the detailed view for the endpoint 'fray174'. The 'Overview' tab is active, displaying the following information:

- OS:** Windows 11 Home 22H2 (10.0.22621.2283)
- Agent Status:** Healthy
- Last Seen:** Sep 20, 2023 @ 22:14:58.113
- Policy:** endpoint-1 rev. 1
- Policy Status:** Success
- Endpoint Version:** 8.9.2
- IP Address:** 169.254.122.161  
fe80::567f:57e2:a848:4913  
192.168.56.1  
fe80::54a0:12c1:3ab8:52e5  
172.28.128.1

At the bottom right, there is a blue button labeled 'Take action' with a gear icon.

Aquí vemos la información que tiene de nuestro equipo.

# Response console

Response actions history

FRAY174 Healthy  
Last seen 26 minutes ago

Help

SYSTEM	144	NzF1NmQ4M2ItZmIxZi00YzdmLT1iMGQtZTNiYz g3NTk3ZDZiTc0NC0xNjk1MjMx0Dc5LjU2NDI1	Registry NTIwMA==
SYSTEM	744	NzF1NmQ4M2ItZmIxZi00YzdmLT1iMGQtZTNiYz g3NTk3ZDZiTc0NC0xNjk1MjMx0Dk0LjM50TkW	C:\Windows\System32\smss.exe

Submit response action ▶

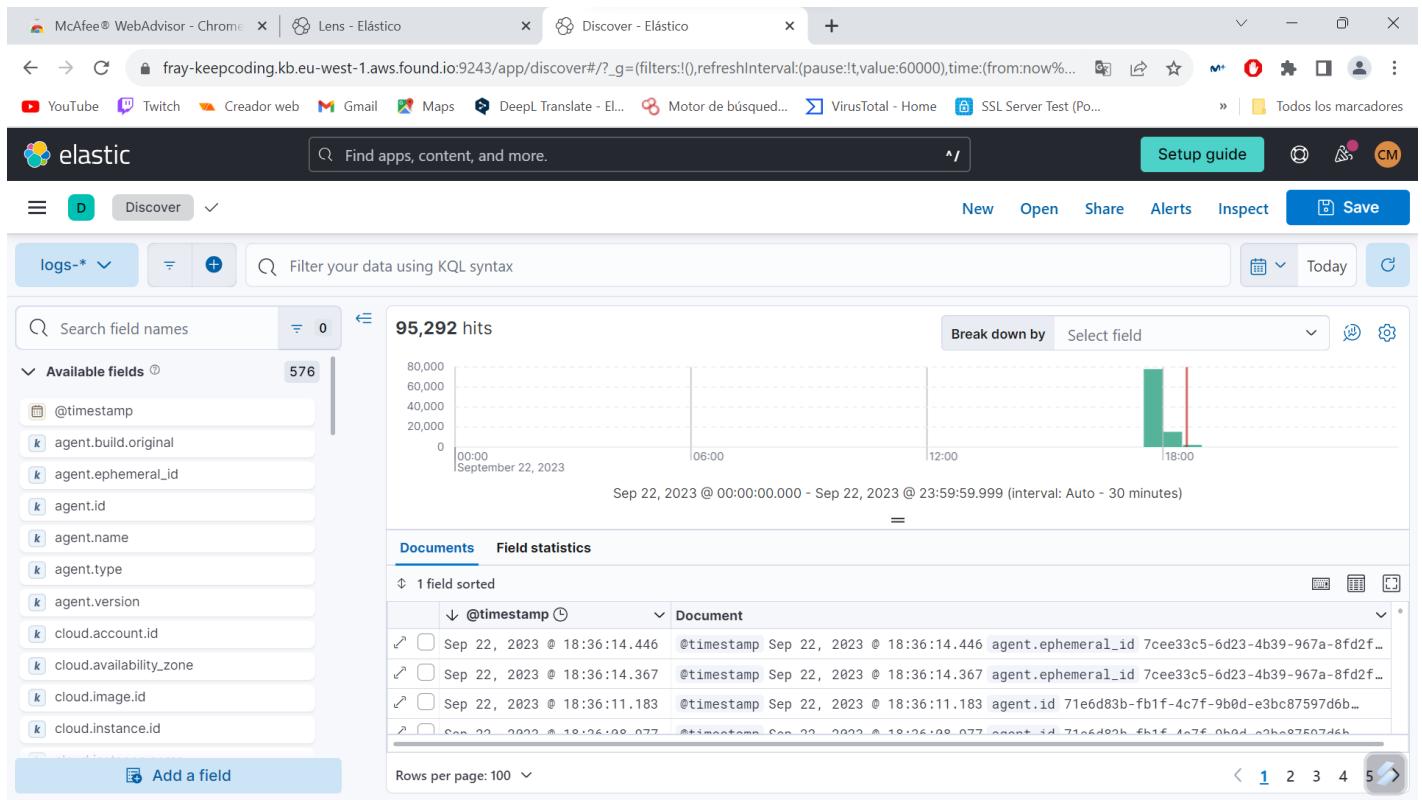
Press the up arrow key to access previously entered commands

⚡

A través del Elastic podemos interactuar con la consola via kibana, en este caso estamos viendo los comportamientos del sistema y podríamos eliminar algún comportamiento anómalo si quisiéramos.

The screenshot shows the Elasticsearch interface with the URL `fray-keepcoding.kb.eu-west-1.aws.found.io:9243/app/integrations/edit-integration/def78c08-8e88-41c0-b1ba-089894787139`. The page title is "Edit Suricata integration". It displays integration settings for "suricata-1" under "Agent policy Agent policy 1". The "Integration name" is set to "suricata-1". The "Description" field is empty. A note says "Choose a name and description to help identify how this integration will be used." Below this, there's a section for collecting Suricata eve logs, with an input field for "Paths" containing "/var/log/suricata/eve.json". There are checkboxes for "Collect Suricata eve logs (input: logfile)" and "Suricata eve logs (log)". At the bottom, there are buttons for "Cancel", "Preview API request", and "Save integration" with a "⚡" icon.

Lo siguiente que haremos es añadir la integración de Suricata y la política que vamos a describir es `/var/log/jsonsuricata/eve`. Para sacar la información.



This screenshot shows the same Elasticsearch Discover interface, but the results table has been expanded to show the full JSON documents. The first few rows are identical to the previous screenshot. The expanded view allows for reading the entire log entries.

_index	_id	_score	_type	_source
...	...	...	...	{@timestamp: Sep 22, 2023 @ 18:36:14.446, agent.ephemeral_id: 7cee33c5-6d23-4b39-967a-8fd2f610dbdd, agent.id: 71e6d83b-fb1f-4c7f-9b0d-e3bc87597d6b, agent.name: fray174, agent.type: endpoint, agent.version: 8.9.2, component.binary.endpoint-security.component.dataset: elastic_ag...
...	...	...	...	{@timestamp: Sep 22, 2023 @ 18:36:14.367, agent.ephemeral_id: 7cee33c5-6d23-4b39-967a-8fd2f610dbdd, agent.id: 71e6d83b-fb1f-4c7f-9b0d-e3bc87597d6b, agent.name: fray174, agent.type: endpoint, agent.version: 8.9.2, component.binary.endpoint-security.component.dataset: elastic_ag...
...	...	...	...	{@timestamp: Sep 22, 2023 @ 18:36:11.183, agent.id: 71e6d83b-fb1f-4c7f-9b0d-e3bc87597d6b, agent.type: endpoint, agent.version: 8.9.2, data_stream.dataset: endpoint.events.file, data_stream.namespace.default: data_stream.type: logs, ecs.version: 1.11.0...}
...	...	...	...	{@timestamp: Sep 22, 2023 @ 18:36:08.977, agent.id: 71e6d83b-fb1f-4c7f-9b0d-e3bc87597d6b, agent.type: endpoint, agent.version: 8.9.2, data_stream.dataset: endpoint.events.network, data_stream.namespace.default: data_stream.type: logs, destination.port: 53... =}
...	...	...	...	{@timestamp: Sep 22, 2023 @ 18:36:08.921, agent.id: 71e6d83b-fb1f-4c7f-9b0d-e3bc87597d6b, agent.type: endpoint, agent.version: 8.9.2, data_stream.dataset: endpoint.events.network, data_stream.namespace.default: data_stream.type: logs, destination.port: 53...}
...	...	...	...	{@timestamp: Sep 22, 2023 @ 18:36:06.164, agent.id: 71e6d83b-fb1f-4c7f-9b0d-e3bc87597d6b, agent.type: endpoint, agent.version: 8.9.2, data_stream.dataset: endpoint.events.file, data_stream.namespace.default: data_stream.type: logs, ecs.version: 1.11.0...}
...	...	...	...	{@timestamp: Sep 22, 2023 @ 18:36:05.828, agent.id: 71e6d83b-fb1f-4c7f-9b0d-e3bc87597d6b, agent.type: endpoint, agent.version: 8.9.2, data_stream.dataset: endpoint.events.file, data_stream.namespace.default: data_stream.type: logs, ecs.version: 1.11.0...}
...	...	...	...	{@timestamp: Sep 22, 2023 @ 18:36:05.819, agent.id: 71e6d83b-fb1f-4c7f-9b0d-e3bc87597d6b, agent.type: endpoint, agent.version: 8.9.2, data_stream.dataset: endpoint.events.file, data_stream.namespace.default: data_stream.type: logs, ecs.version: 1.11.0...}

Ya podemos observar como Jason se integra dentro del Elastic en forma de contenido y nos empieza proporcionar información.

The screenshot shows the Elastic Stack interface with the following details:

- Top Bar:** Shows tabs for "McAfee® WebAdvisor - Chrome", "Lens - Elástico", "Dashboards - Elástico", and several other browser tabs.
- Header:** "elastic" logo, search bar ("Find apps, content, and more."), and navigation buttons ("Setup guide", "Dashboard", "Logs Suricata Alert Overview", "Edit").
- Left Sidebar:** "Navigation [Logs Suricata]" section with a "SURICATA Events | Alerts" heading. Below it are three collapsed sections: "Top Alerting Hosts [Logs Suricata]", "Alerts - Top Source Countries [Logs Su...]", and "Alerts - Top Destination Countries [Logs Su...]".
- Right Main Area:** "Top Alert Signatures [Logs Suricata]" section. It displays a chart titled "1,784 hits" showing event counts from 00:00 to 18:00 on September 22, 2023. The chart shows a fluctuating pattern of hits between 10 and 50. Below the chart is a table titled "Documents" showing log entries. One entry is visible:

Sep 22, 2023 @ 18:45:52.320	@timestamp Sep 22, 2023 @ 18:45:52.320	ecs.version 1.8.0	event.action execute...
-----------------------------	--	-------------------	-------------------------

A través de Suricata en Elastic podríamos ver si tuviéramos alguna alerta en este caso no tenemos ninguna por lo que no se visualizan.

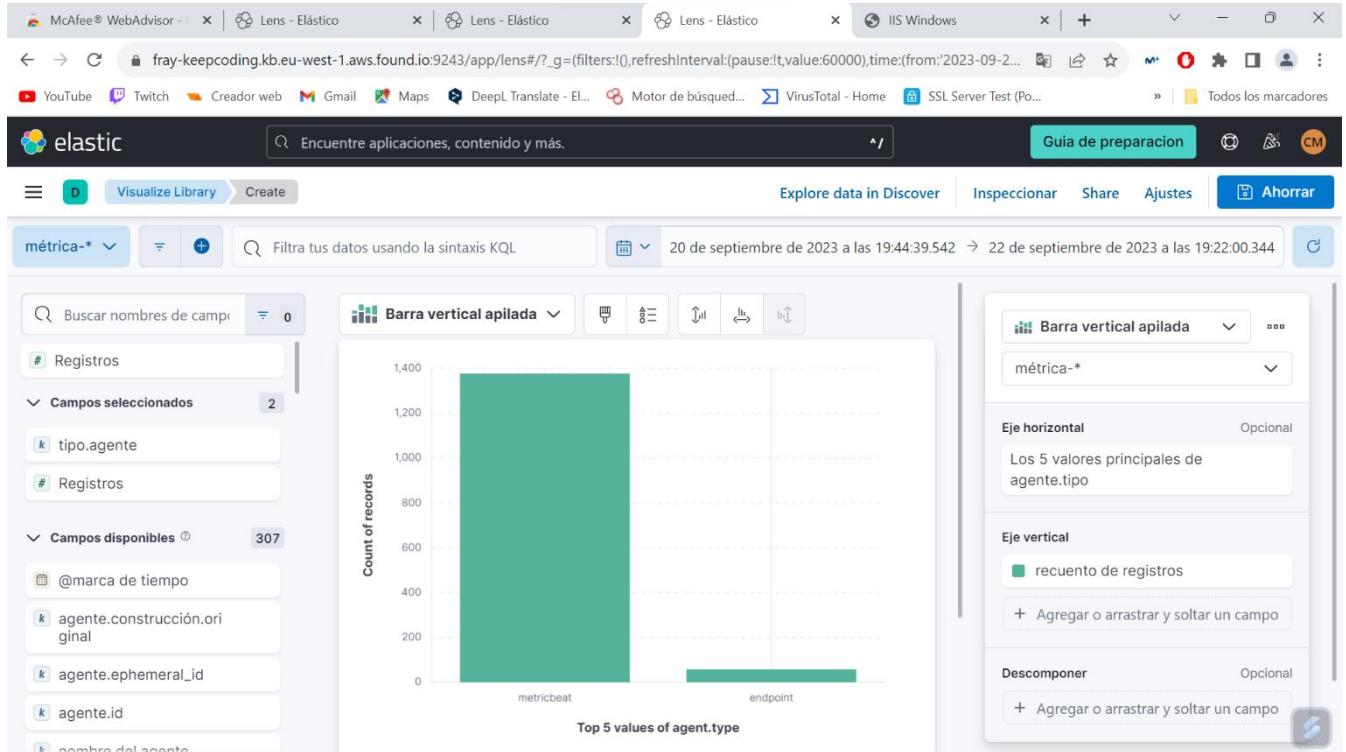
The screenshot shows the Elastic Stack interface with the following details:

- Top Bar:** Shows tabs for "McAfee® WebAdvisor - Chrome", "Lens - Elástico", and "Discover - Elástico".
- Header:** "elastic" logo, search bar ("Find apps, content, and more."), and navigation buttons ("Setup guide", "Discover", "New", "Open", "Share", "Alerts", "Inspect", "Save").
- Left Sidebar:** "Data views" section with a "Create a data view" button. A dropdown menu is open for ".kibana-event-log-\*" showing options like "Add a field to this data view" and "Manage this data view". Other data views listed include "logs-\*", "metrics-\*", "error.type", "event.action", "event.category", "event.code", and "event.created".
- Right Main Area:** A search bar ("Filter your data using KQL syntax") and a histogram titled "1,784 hits" showing event counts from 00:00 to 18:00 on September 22, 2023. Below the histogram is a table titled "Documents" showing log entries. One entry is visible:

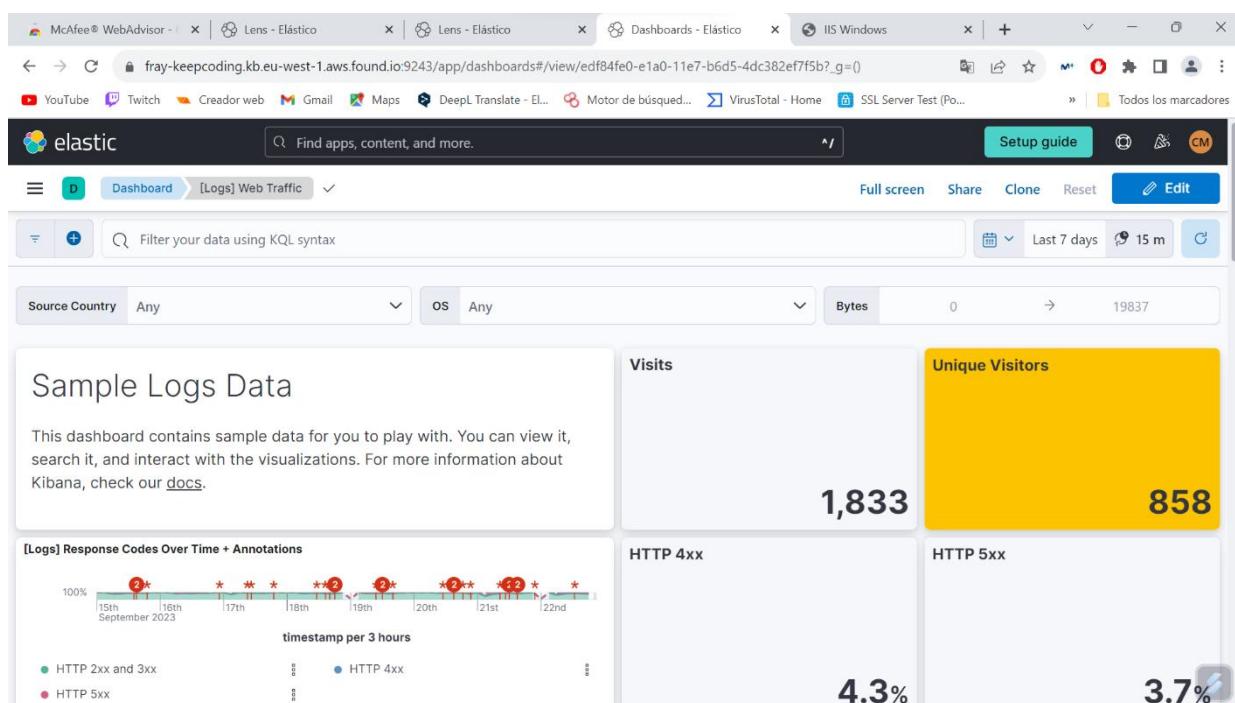
Sep 22, 2023 @ 18:45:52.320	@timestamp Sep 22, 2023 @ 18:45:52.320	ecs.version 1.8.0	event.action execute...
-----------------------------	--	-------------------	-------------------------

Dentro del Elastic podríamos generar mucha información de nuestro equipo, aquí podemos ver otros datos que nos proporciona a través de

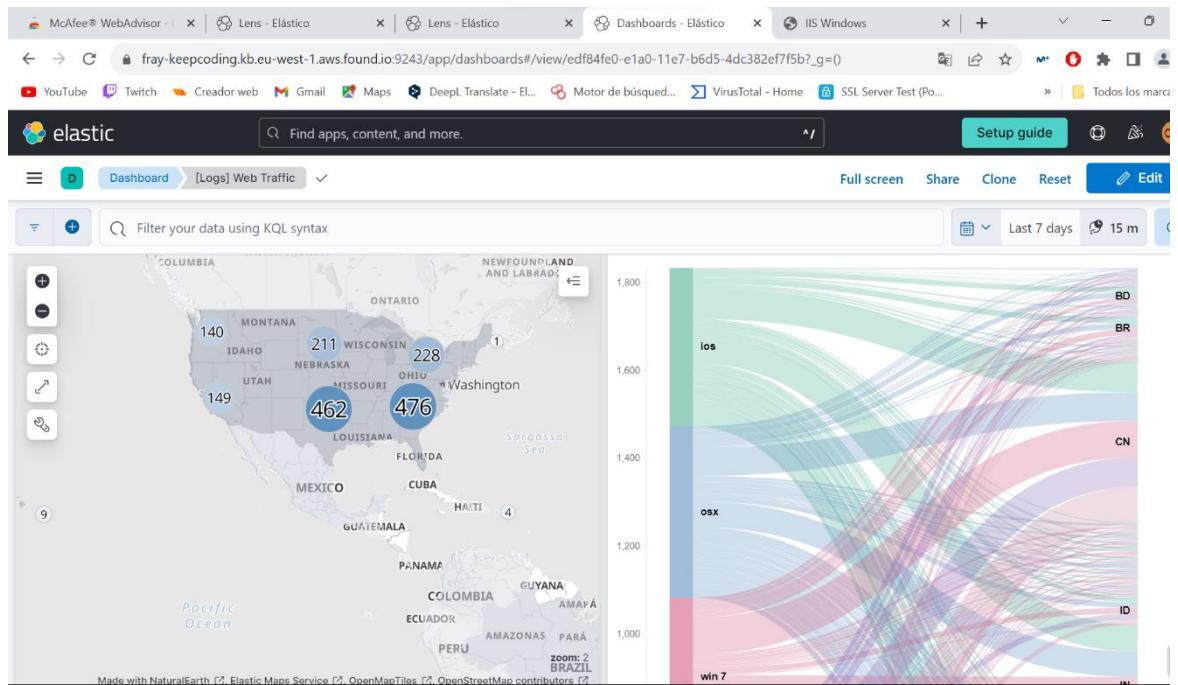
Kibana. Podemos ver también como nos monta un gráfico con todos los hits generados.



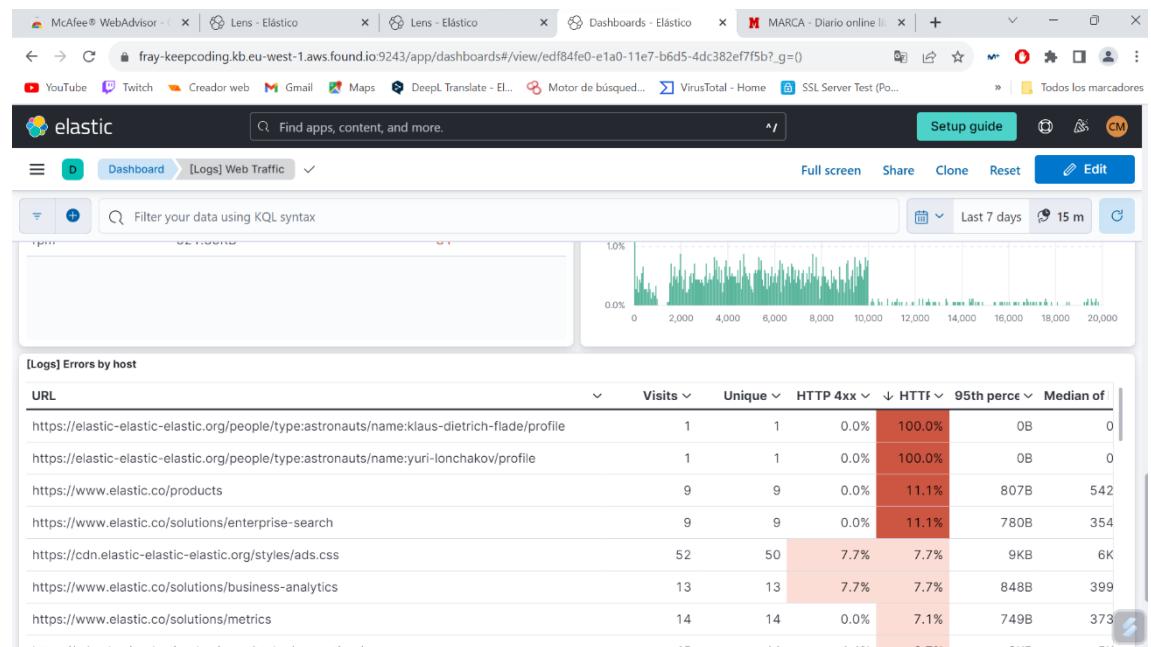
Mas información que nos transmite Elastic son métricas, aquí tenemos un gráfico de los tipos de agentes.



Podemos ver también los Logs del tráfico de web, vemos el nº de visitante, visitantes únicos.



Vemos todas las consultas que se han hecho desde los distintos sitios.



Y por último aquí tenemos la correlación, que nos especifica que hemos descargado, errores que nos da.