



BLUE TEAM | 2022

Alberto Doblado Vera

Primero de todo tenemos que descargar la máquina de **PfSense**. Para ello nos vamos a <https://www.pfsense.org/download/> y descargamos.

The screenshot shows the pfSense download page. At the top, there's a navigation bar with the pfSense logo, 'Get Started', and 'Cloud' options. Below it, a 'Download' button is visible. The main content area is titled 'Latest Stable Version (Community Edition)'. It includes a note about being the most recent stable release and recommended for all. Below this, there are two buttons: 'RELEASE NOTES' and 'SOURCE CODE'. A large central box is titled 'Select Image To Download' and contains fields for 'Version' (2.6.0), 'Architecture' (AMD64 (64-bit)), 'Installer' (DVD Image (ISO) Installer), and 'Mirror' (Frankfurt, Germany). At the bottom of this box is a blue 'DOWNLOAD' button with a hand cursor icon. To the right of the download button, there's a 'Supported by' section featuring the Netgate logo. Below the download button, there's a SHA256 checksum for the compressed (.gz) file: 941a68c7f20c4b635447cceda429a027f816bdb78d54b8252bb87abf1fc22ee3.

Ahora en **VirtualBox** al crear la máquina, es muy importante seleccionar bien el tipo y la versión.



Y luego nos vamos a “Dispositivos de almacenamiento” y seleccionamos “CD/DVD vivo”

The screenshot shows the 'Dispositivos de almacenamiento' (Storage Devices) tab in the VirtualBox settings. Under the 'Controlador:' dropdown, 'IDE' is selected. In the list of devices, 'UTM-Blue-001.vdi' is highlighted. On the right, under 'Atributos' (Attributes), the 'Unidad óptica:' dropdown is set to 'IDE secundario maestro'. Next to it, the 'CD/DVD vivo' checkbox is checked and has a cursor icon over it. Below these, there's an 'Información' (Information) section.

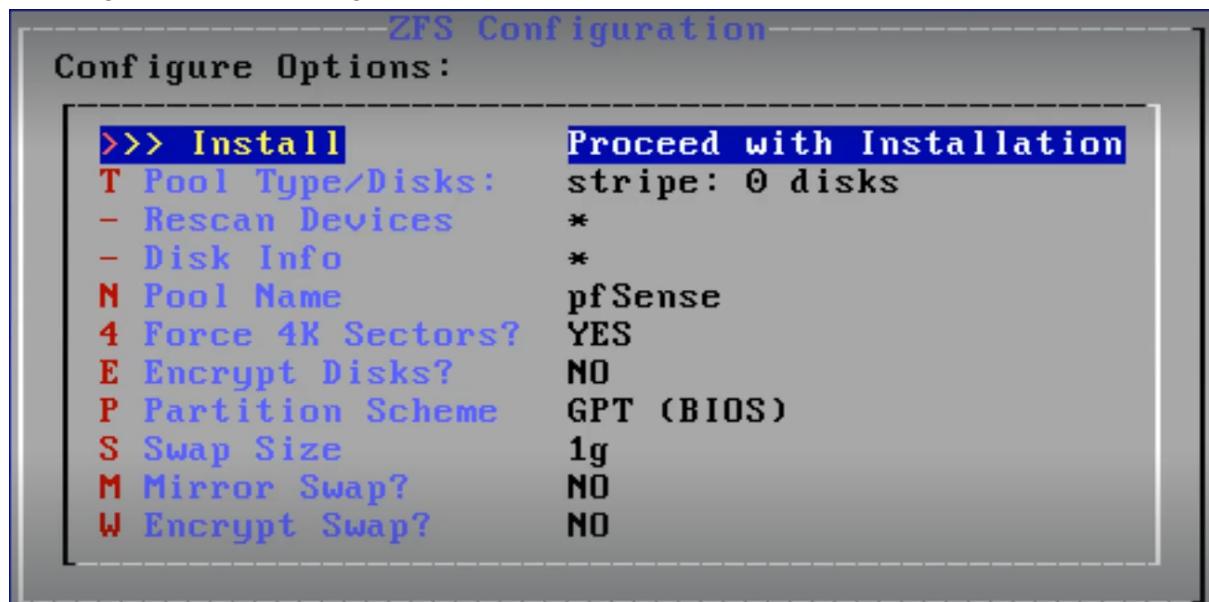
Una vez hecho el paso anterior arrancamos la máquina y seguimos los siguientes pasos en la instalación.

The screenshot shows the pfSense 'Welcome' screen. At the top, it says 'Welcome to pfSense!'. Below that, there are two main buttons: 'Install' and 'Install pfSense'. The 'Install' button is highlighted with a blue border. Underneath these buttons, there are three smaller options: 'Rescue Shell', 'Launch a shell for rescue operations', 'Recover config.xml', and 'Recover config.xml from a previous install'. The 'Recover config.xml' option is partially cut off at the bottom.

Tras este paso tendremos que seleccionar nuestra versión de teclado, y ahora nos pregunta si queremos particionar el disco y seleccionamos lo siguiente.



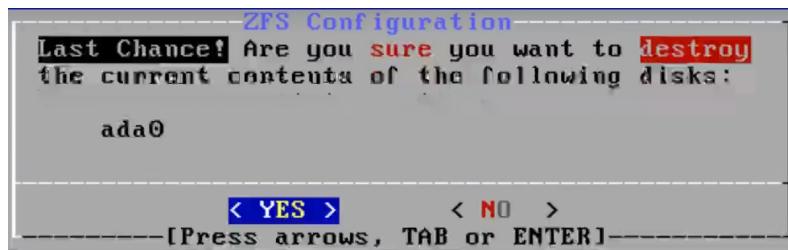
En la siguiente ventana seguimos con la primera opción.



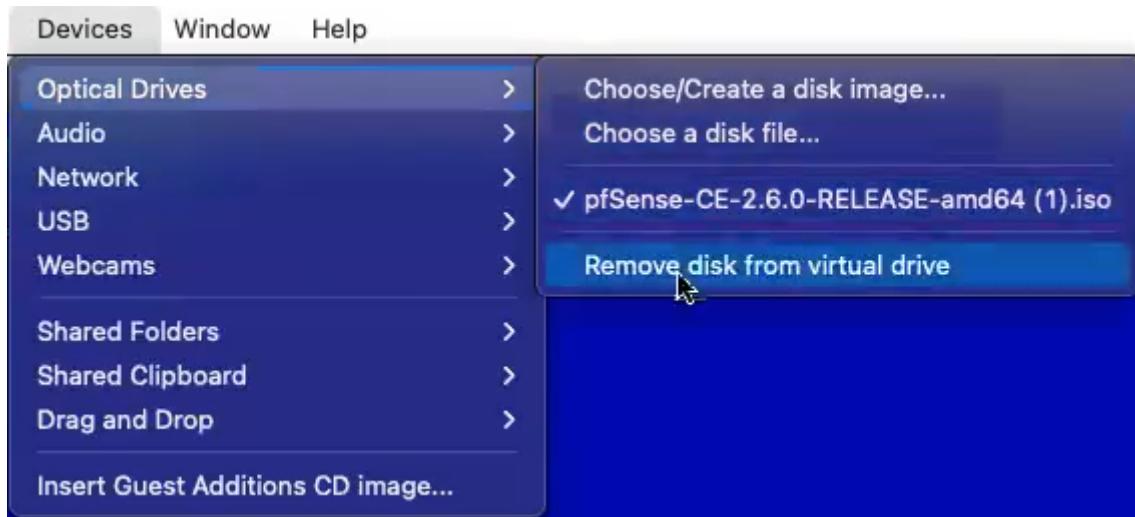
Ahora tenemos que seleccionar el disco, como es el único que hay pulsamos la tecla espacio y lo marcamos.



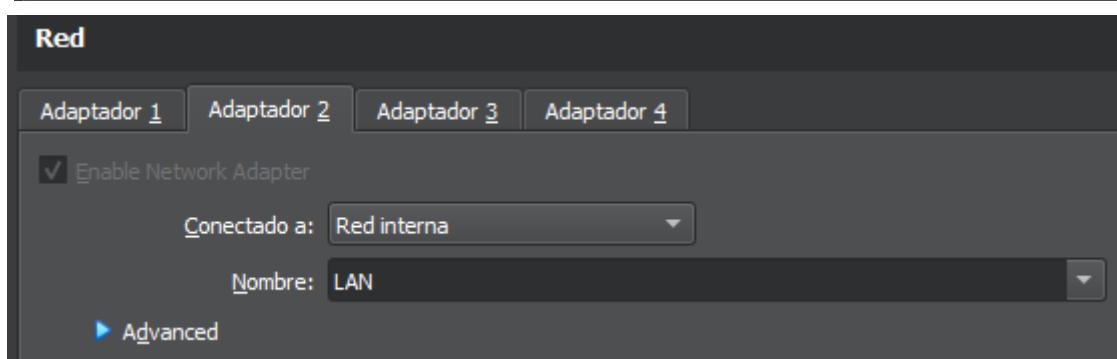
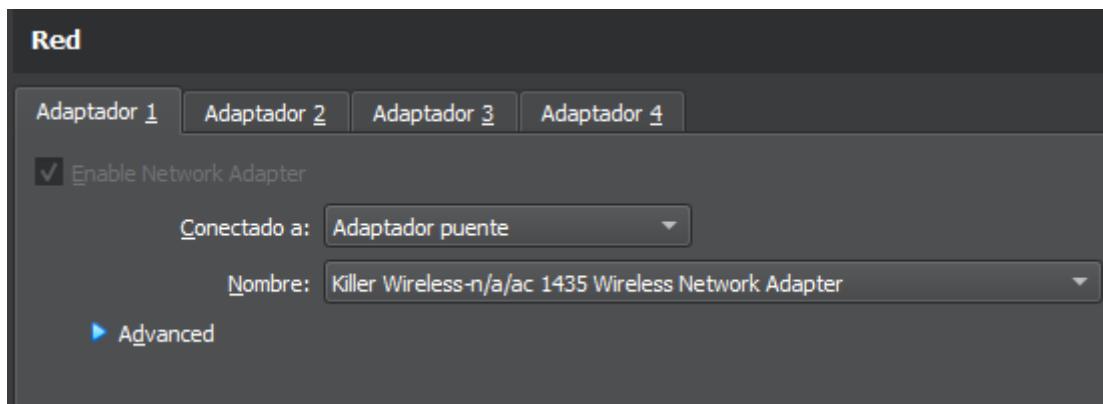
Y marcamos que “YES” para finalizar

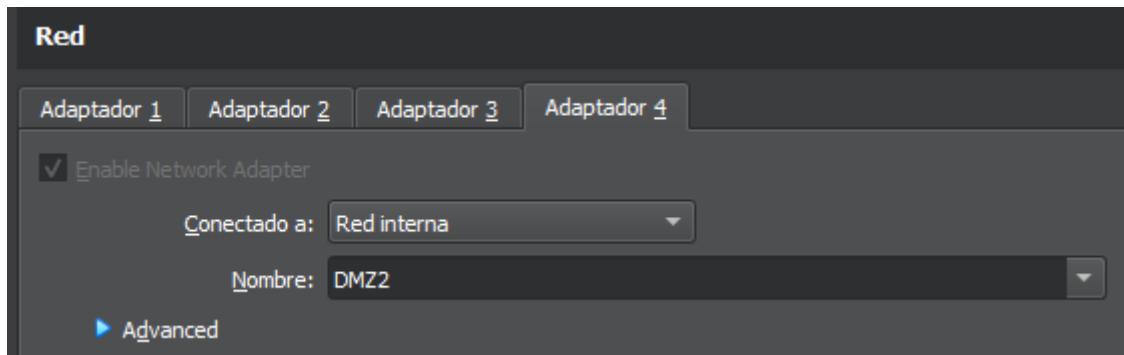
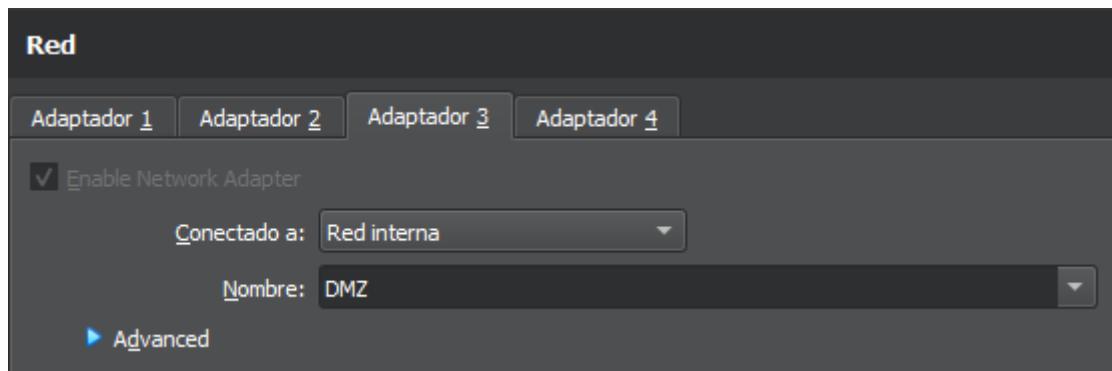


Ahora tenemos que eliminar el disco, ya que de no hacerlo volveríamos al proceso de configuración de nuevo.



Y ahora con la máquina apagada vamos a activar los adaptadores de red de la siguiente manera para crear nuestra red.





Ahora ya podemos arrancar la máquina y configurar las interfaces.

```
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      08:00:27:06:5b:3a  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:89:3e:02  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:0b:f5:1f  (down) Intel(R) Legacy PRO/1000 MT 82540EM
em3      08:00:27:cd:9f:4d  (down) Intel(R) Legacy PRO/1000 MT 82540EM
```

Marcamos que no queremos configurar las VLANs ahora.

```
Should VLANs be set up now [y|n]? n
```

Y vamos asignando el resto de las interfaces.

```
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
```

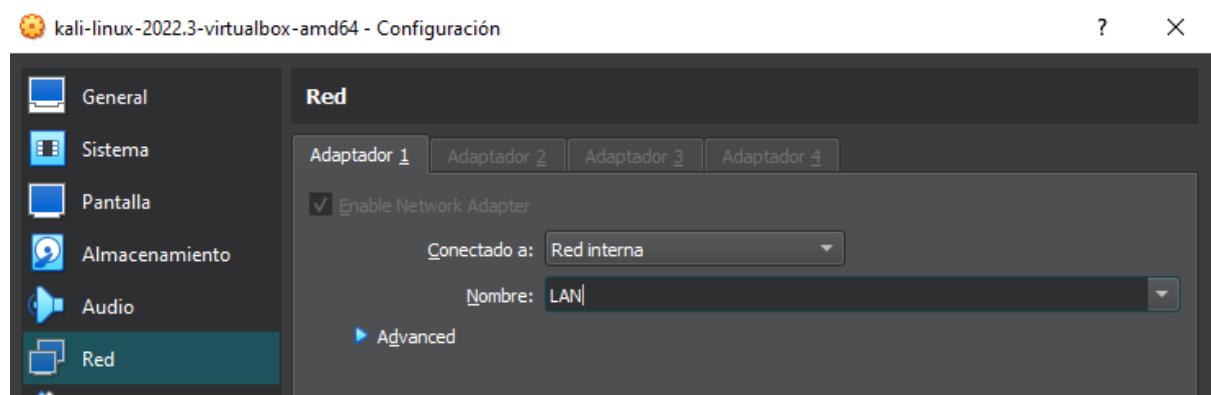
Y le ponemos la IP que nosotros queramos asignarle.

```
Enter the number of the interface you wish to configure: 2  
  
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 192.168.100.1  
  
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  
  
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:  
>
```

Y le decimos que queremos volver a HTTP.

```
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...  
  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Ahora nos vamos con la máquina de Kali, activamos el adaptador de red con la siguiente configuración.

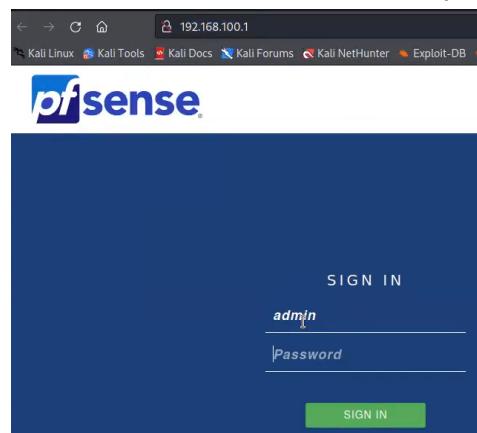


Al arrancar Kali hacemos un “ip a” y vemos que tenemos la IP que habíamos asignado en PfSense.

```
(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
    inetc6 ::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 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.100/24 brd 192.168.100.255 scope global dynamic noprefixroute
        route eth0
            valid_lft 7171sec preferred_lft 7171sec
    inetc6 fe80::ce8e:207f:559e:941d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└─$
```

Ahora si nos vamos al navegador del Kali y escribimos **192.168.100.1** tendremos acceso a PfSense. Para entrar los credenciales son username: **admin** y password: **pfsense**



Y una vez dentro vamos configurando nuestro PfSense del siguiente modo.

Wizard / pfSense Setup / General Information

Step 2 of 9

### 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 for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard. |                                     |
| 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  |                                     |

>> Next

En la zona horaria seleccionamos el país (o uso horario) en el que nos encontramos.

Step 3 of 9

### Time Server Information

Please enter the time, date and time zone.

|   |                        |
|---|------------------------|
| Time server hostname                          | 2.pfsense.pool.ntp.org |
| Enter the hostname (FQDN) of the time server. |                        |
| Timezone                                      | Europe/Madrid          |

>> Next

La interface WAN la ponemos tipo DHCP

Step 4 of 9

### Configure WAN Interface

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

|              |      |
|--------------|------|
| SelectedType | DHCP |
|--------------|------|

En **Reserved Networks** desmarcamos ambas, para que no nos bloquee el acceso de redes privadas.

**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.

Y ahora vamos activando las distintas interfaces.

**Interfaces / WAN (em0)**

**General Configuration**

**Enable**  Enable interface

**Description**  Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**Interfaces / LAN (em1)**

**General Configuration**

**Enable**  Enable interface

**Description**  Enter a description (name) for the interface here.

**IPv4 Configuration Type**

Tenemos que marcar **Static IPv4**

## Interfaces / OPT1 (em2)

### General Configuration

Enable  Enable interface

#### Description

DMZ

Enter a description (name) for the interface here.

## Interfaces / OPT2 (em3)

### General Configuration

Enable  Enable interface

#### Description

DMZ2

Enter a description (name) for the interface here.

En DMZ le ponemos la siguiente dirección IP

### Static IPv4 Configuration

IPv4 Address

/ 24

IPv4 Upstream gateway

+ Add a new gateway

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](#).

### 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 nos vamos a **Services / DHCP Server** y seleccionamos DMZ y activamos el DHCP.

## Services / DHCP Server / DMZ

LAN DMZ

### General Options

Enable  Enable DHCP server on DMZ interface

Le ponemos los siguientes servidores de DNS.

| Servers      |               |
|--------------|---------------|
| WINS servers | WINS Server 1 |
|              | WINS Server 2 |
| DNS servers  | 192.168.90.1  |
|              | 1.1.1.1       |
|              | 8.8.8.8       |
|              | DNS Server 4  |

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

Y la puerta de enlace.

| Other Options |              |
|---------------|--------------|
| Gateway       | 192.168.90.1 |

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

En el siguiente rango.

|       |                |                |
|-------|----------------|----------------|
| Range | 192.168.90.100 | 192.168.90.200 |
| From  |                | To             |

Editamos el mapeo estático de DHCP en DMZ e introducimos nuestra MAC.

Services / DHCP Server / DMZ / Edit Static Mapping

| Static DHCP Mapping on DMZ                     |                   |
|--|-------------------|
| MAC Address                                    | 08:00:27:22:46:4f |
| Copy My MAC                                    |                   |
| MAC address (6 hex octets separated by colons) |                   |

Y rellenamos los campos restantes de la siguiente manera.

|  |  |         |         |       |
|--|--|---------|---------|-------|
| IP Address   | 192.168.90.50  |         |         |       |
| If an IPv4 address is entered, the address must be outside of the pool.<br>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_dmz   |         |         |       |
| Name of the host, without domain part.   |  |         |         |       |
| Description  | Kali para DMZ  |         |         |       |
| A description may be entered here for administrative reference (not parsed).   |  |         |         |       |
| ARP Table Static Entry   | <input checked="" type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair. |         |         |       |
| WINS Servers   | WINS 1   |         |         |       |
| DNS Servers  | 192.168.90.1   | 1.1.1.1 | 8.8.8.8 | DNS 4 |
| Note: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page. |  |         |         |       |
| Gateway  | 192.168.90.1   |         |         |       |
| The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network.         |  |         |         |       |

Una vez finalizado le damos a guardar y aplicamos los cambios. Tras esto nos vamos a **System / General Setup**. Ahí vamos a darle un nombre al firewall y un dominio.

The screenshot shows the 'System' tab selected in the navigation bar. Under the 'System' section, there are two fields: 'Hostname' with the value 'utm' and 'Domain' with the value 'keepcoding.local'. A note below the domain field explains that it should not end with '.local' as it is widely used by mDNS. Alternative TLDs like '.lan' or '.mylocal' are mentioned as safe options.

Tras esto vamos a **Firewall / Aliases** y creamos uno nuevo de tipo **Port(s)** y le metemos los puertos que queremos añadir, en este caso el 80 y el 433.

The screenshot shows the 'Properties' tab selected in the navigation bar. A new alias named 'web' is being created. The 'Type' is set to 'Port(s)'. In the 'Port(s)' section, two ports are listed: 80 and 443. A hint at the top of this section says: 'Enter ports as desired, with a single port or port range per entry. Port ranges can be'.

Y ahora en **Firewall / Rules** seleccionamos **DMZ** y vamos a crear algunas reglas.

**Firewall / Rules / Edit**

**Edit Firewall Rule**

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) 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      
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.

En este caso es una regla de paso utilizando el protocolo TCP y en fuente y destino seleccionamos “any”

**Source**

Source  Invert match

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

Destination Port Range      
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 [Status: System Logs: Settings](#) page).

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

Ahora clonamos la regla anterior y cambiamos el protocolo por TCP/UDP y en el rango del puerto de destino ponemos 53 (El puerto de DNS).

The screenshot shows a configuration page for a firewall rule. At the top, under 'Protocol', 'TCP/UDP' is selected. Below it, a note says 'Choose which IP protocol this rule should match.' In the 'Source' section, 'Source' is set to 'any'. Under 'Destination', 'Destination' is also set to 'any'. 'Destination Port Range' is set to 'DNS (53)' for both 'From' and 'To' fields. A note below says 'Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.'

También creamos una regla para permitir hacer ping.

The screenshot shows a configuration page for a firewall rule. The title bar says 'Firewall / Rules / Edit'. The main section is titled 'Edit Firewall Rule'. Under 'Action', 'Pass' is selected. A note says 'Choose what to do with packets that match the criteria specified below.' and 'Hint: the difference between block and reject is that with reject, a packet (TCP |' followed by text cut off. Under 'Disabled', there is a checkbox 'Disable this rule' with a note 'Set this option to disable this rule without removing it from the list.' Under 'Interface', 'DMZ' is selected. A note says 'Choose the interface from which packets must come to match this rule.' Under 'Address Family', 'IPv4' is selected. A note says 'Select the Internet Protocol version this rule applies to.' Under 'Protocol', 'ICMP' is selected. A note says 'Choose which IP protocol this rule should match.'

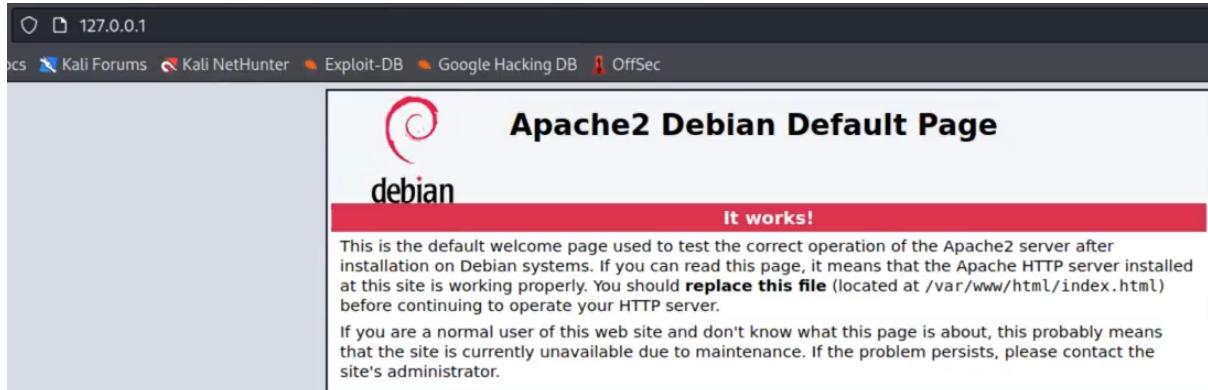
Así quedarían las reglas de nuestro DMZ si hemos seguido los pasos.

| Firewall / Rules / DMZ       |               |              |      |             |         |          |       |          |                |  |
|------------------------------|---------------|--------------|------|-------------|---------|----------|-------|----------|----------------|--|
| Floating                     | WAN           | LAN          | DMZ  | DMZ2        | OpenVPN |          |       |          |                |  |
| Rules (Drag to Change Order) |               |              |      |             |         |          |       |          |                |  |
| States                       | Protocol      | Source       | Port | Destination | Port    | Gateway  | Queue | Schedule | Description    |  |
| <input type="checkbox"/>     | ✓ 0 /1.65 GiB | IPv4 TCP     | *    | *           | *       | web      | *     | none     | Navegacion web |  |
| <input type="checkbox"/>     | ✓ 0 /707 Kib  | IPv4 TCP/UDP | *    | *           | *       | 53 (DNS) | *     | none     | Navegacion web |  |
| Internet                     |               |              |      |             |         |          |       |          |                |  |
| <input type="checkbox"/>     | ✓ 0 /0 B      | IPv4 ICMP    | *    | *           | *       | *        | *     | none     | Navegacion web |  |

Ahora vamos a arrancar el servicio de **Apache** en la terminal de Kali.

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

y probamos a acceder desde nuestro navegador en la IP 127.0.0.1



Nos vamos al dashboard de nuestro PfSense y miramos las IPs que tenemos asignadas.

| Interfaces |      |  |                                       |
|------------|------|--|---------------------------------------|
|            | WAN  |  | 1000baseT <full-duplex> 192.168.1.135 |
|            | LAN  |  | 1000baseT <full-duplex> 192.168.100.1 |
|            | DMZ  |  | 1000baseT <full-duplex> 192.168.90.1  |
|            | DMZ2 |  | 1000baseT <full-duplex> n/a           |

Ahora vamos a **Firewall / NAT / Port Forward** para redireccionar a una IP de nuestra DMZ

Firewall / NAT / Port Forward / Edit

### Edit Redirect Entry

|                        |   |
|------------------------|---|
| Disabled               | <input type="checkbox"/> Disable this rule  |
| No RDR (NOT)           | <input type="checkbox"/> Disable redirection for traffic matching this rule<br>This option is rarely needed. Don't use this without thorough knowledge of the implications. |
| Interface              | WAN   |
| Address Family         | IPv4  |
| Protocol               | TCP   |
| Source                 | <a href="#">Display Advanced</a>  |
| Destination            | <input type="checkbox"/> Invert match.<br>Type: WAN address<br>Address/mask: /  |
| Destination port range | From port: Other, Value: 8080<br>To port: Other, Value: 8080<br>Custom  |
| Redirect target IP     | Type: Single host, Value: 192.168.90.50<br>Address  |

Firewall / NAT / Port Forward

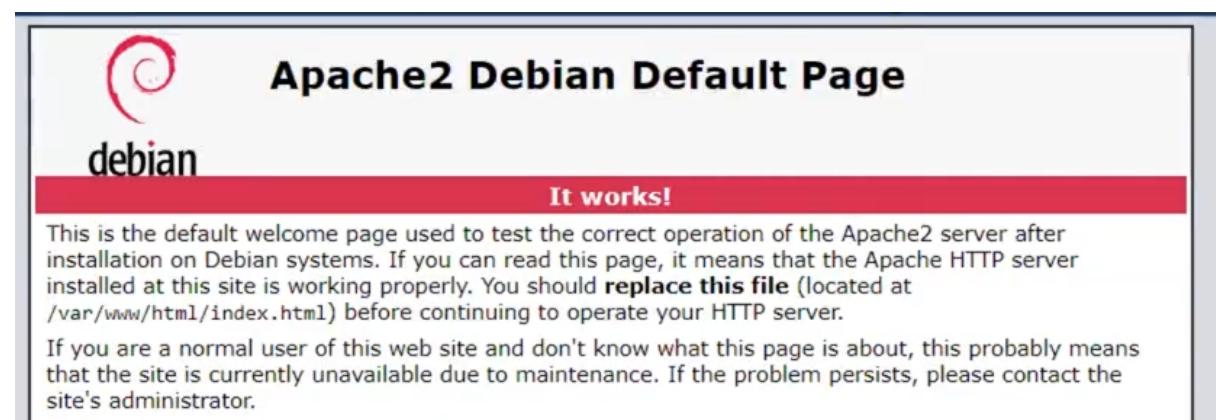
The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor](#) the filter reload progress.

Port Forward    1:1    Outbound    NPt

### Rules

|                                     | Interface | Protocol | Source Address | Source Ports | Dest. Address | Dest. Ports | NAT IP        | NAT Ports | Description  | Actions                                     |
|-------------------------------------|-----------|----------|----------------|--------------|---------------|-------------|---------------|-----------|--------------|---|
| <input checked="" type="checkbox"/> | WAN       | TCP      | *              | *            | WAN address   | 8080        | 192.168.90.50 | 80 (HTTP) | Servidor Web | <a href="#">Edit</a> <a href="#">Delete</a> |

Y ahora podemos acceder a nuestro Apache desde el navegador de nuestro pc escribiendo "IP:8080"



Vamos a configurar nuestro propio **OpenVPN**, para ello primero vamos a **System / Package Manager** (en mi caso ya lo tenía instalado) y vamos a **Available Packages** y escribimos **vpn** y nos aparecerá **openvpn** y lo instalamos.

| Name                    | Category | Version | Description   | Actions |
|-------------------------|----------|---------|---|---------|
| ✓ openvpn-client-export | security | 1.6_4   | 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-2.5.2 openvpn-2.5.4.1 zip-3.0\_1 p7zip-16.02\_3

= Update = Current  
 = Remove = Information = Reinstall

Ahora vamos a crear una entidad certificadora. Para ello nos vamos a **System / Certificate Manager / CAs** y creamos una nueva. (La configuración de la mía)

| Name | Internal | Issuer      | Certificates | Distinguished Name   | In Use         |
|------|----------|-------------|--------------|--|----------------|
| UTM  | ✓        | self-signed | 2            | ST=Malaga, O=keepcoding, L=Malaga, CN=utm.keepcoding.local, C=ES | OpenVPN Server |

Valid From: Thu, 13 Oct 2022 23:04:16 +0200  
Valid Until: Sun, 10 Oct 2032 23:04:16 +0200

Tras tener la CA vamos a crear los certificados, uno de server y otro de usuario.

| Name  | Issuer      | Distinguished Name  | In Use         | Actions |
|---|-------------|---|----------------|---------|
| webConfigurator default<br>(6345cf1d314f3)<br>Server Certificate<br>CA: No<br>Server: Yes | self-signed | O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6345cf1d314f3 |                |         |
| vpn.keepcoding.local<br>Server Certificate<br>CA: No<br>Server: Yes                       | UTM         | ST=Malaga, O=keepcoding, L=Malaga, CN=vpn.keepcoding.local, C=ES            | OpenVPN Server |         |
| alberto<br>User Certificate<br>CA: No<br>Server: No                                       | UTM         | ST=Malaga, O=keepcoding, L=Malaga, CN=alberto, C=ES                         | User Cert      |         |

Y ahora vamos a crear el server, para ello vamos a **VPN / OpenVPN / Servers** y los creamos con los siguientes parámetros.

| OpenVPN Servers |                   |                  |  |             |  |
|-----------------|-------------------|------------------|--|-------------|--|
| Interface       | Protocol / Port   | Tunnel Network   | Mode / Crypto  | Description |  |
| WAN             | TCP4 / 9458 (TUN) | 192.168.210.0/24 | Mode: Remote Access ( SSL/TLS + User Auth )<br>Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC<br>Digest: SHA256<br>D-H Params: 2048 bits | VPN-keep    |  |

Para la creación de usuarios vamos **System / User Manager / Users**.

**User Properties**

|            |   |
|------------|---|
| Defined by | USER  |
| Disabled   | <input type="checkbox"/> This user cannot login |
| Username   | alberto   |
| Password   | ██████████                                      |

**Create Certificate for User**

|                       |   |
|-----------------------|---|
| Descriptive name      | alberto   |
| Certificate authority | UTM   |
| Key type              | RSA   |
| 2048                  | The length to use when generating a new RSA key, in bits.<br>The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid. |

Y ahora nos vamos a **Firewall / Rules / WAN** y creamos una regla de paso con destinos a este firewall.

**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**: 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.

**Destination**

|                               |                                       |                      |                     |         |                        |
|-------------------------------|---------------------------------------|----------------------|---------------------|---------|------------------------|
| <b>Destination</b>            | <input type="checkbox"/> Invert match | This firewall (self) | Destination Address | /       | <input type="button"/> |
| <b>Destination Port Range</b> | (other)                               | From: 9458           | To: 9458            | (other) | 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.keepcoding.local  
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.

Seleccionamos la interface de **OpenVPN** y creamos una regla para que pase todo (no es recomendable crear este tipo de reglas)

**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**: OpenVPN  
Choose the interface from which packets must come to match this rule.

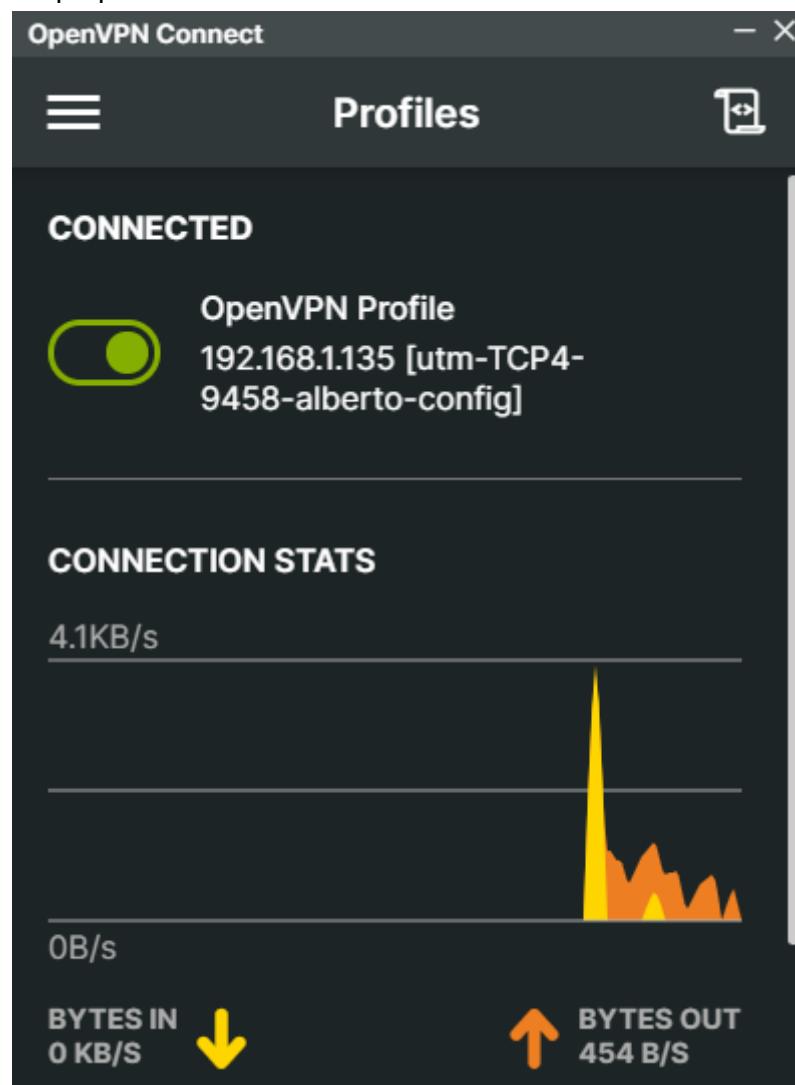
**Address Family**: IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol**: Any  
Choose which IP protocol this rule should match.

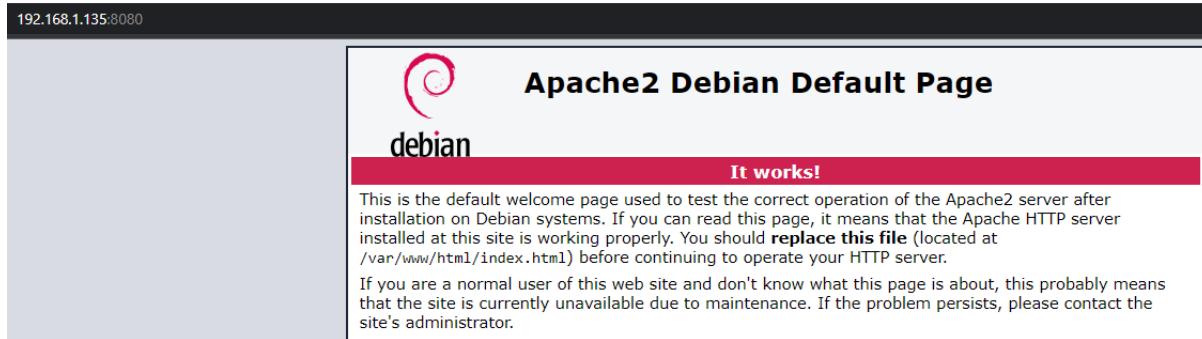
Y ahora nos vamos a **OpenVPN / Client Export Utility** y descargamos nuestro usuario.

The screenshot shows the 'OpenVPN / Client Export Utility' interface. At the top, there are tabs: Server, Client, Client Specific Overrides, Wizards, Client Export, and Shared Key Export. The 'Client' tab is selected. Below the tabs, a section titled 'OpenVPN Server' shows a dropdown menu set to 'Remote Access Server' with the value 'VPN-keep TCP4:9458'. Underneath, a section titled 'OpenVPN Clients' lists a single client named 'alberto' with a certificate name also 'alberto'. There are export options: 'Inline Configurations' (with buttons for 'Most Clients', 'Android', and 'OpenVPN Connect (iOS/Android)').

Nos mandamos el archivo a nuestro PC y lo introducimos en el cliente **OpenVPN Connect** para tener nuestro propio túnel VPN.



Ya podemos acceder a nuestra red desde el PC sin problema.



## ELASTIC

Es el turno de **Elastic**, un potente software de gestión de información y eventos de seguridad. En mi caso voy a instalarlo en home. Para situarnos dentro hacemos el siguiente comando.

```
└─(kali㉿kali)-[~]
  └─$ cd /home
```

Una vez estemos dentro del directorio elegido, descargamos el repositorio (Hay que hacerlo con permiso de root).

```
└─(root㉿kali)-[/home]
  └─# git clone https://github.com/deviantony/docker-elk.git
```

Ahora vamos a la carpeta que nos ha creado y la listamos.

```
└─(kali㉿kali)-[/home]
  └─$ ls
    docker-elk  kali

  └─(kali㉿kali)-[/home]
    └─$ cd docker-elk

  └─(kali㉿kali)-[/home/docker-elk]
    └─$ ls
      docker-compose.yml  extensions  LICENSE  README.md
      elasticsearch        kibana      logstash  setup
```

Ejecutamos el comando **docker-compose up -d**. Para ello también tenemos que ser root.

```
[root@kali]# docker-compose up -d
Creating network "docker-elk_elk" with driver "bridge"
Creating volume "docker-elk_setup" with default driver
Creating volume "docker-elk_elasticsearch" with default driver
Building elasticsearch
Sending build context to Docker daemon 4.608kB
Step 1/2 : ARG ELASTIC_VERSION
Step 2/2 : FROM docker.elastic.co/elasticsearch/elasticsearch:${ELASTIC_VERSION}
8.4.3: Pulling from elasticsearch/elasticsearch
2ec5bc8cf243: Pull complete
e7a52014c641: Pull complete
fe22b900b382: Pull complete
1f95ca3684dd: Pull complete
2d6739673d83: Pull complete
a7ed8e9af4ef: Pull complete
f39cca40e65f: Pull complete
05f4cbbaa0d4a: Pull complete
ce9edbacc81: Pull complete
Digest: sha256:739ec9d428869f16e9e02247d5082849ebb4302c87e0abf9f70971cbb40c3bab
Status: Downloaded newer image for docker.elastic.co/elasticsearch/elasticsearch:8.4.3

```

Ahora vamos a ver los contenedores que nos ha creado.

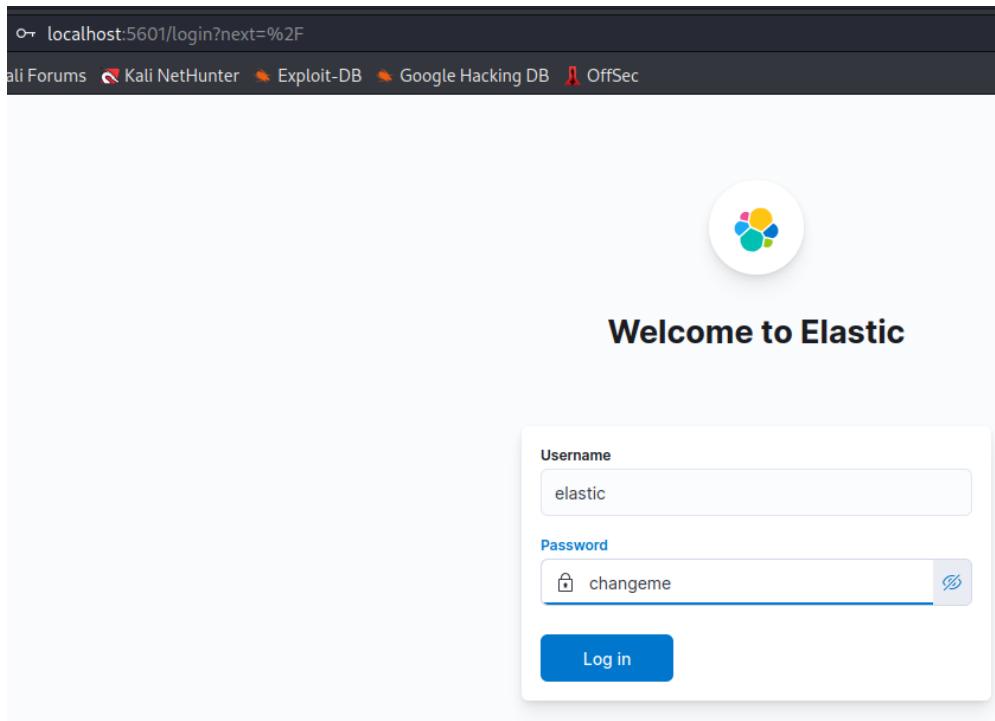
```
[root@kali]# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS
NAMES
06fe2b0c4f9b docker-elk_logstash "/usr/local/bin/docker... About a minute ago Up About a minute 0.0.0.0:5044->5044 /tcp, :::5044->5044/tcp, 0.0.0.0:9600->9600/tcp, :::9600->9600/tcp, 0.0.0.0:50000->50000/tcp, :::50000->50000/tcp, 0.0.0.0:5000->50000/udp, :::50000->50000/udp
6ec42f0e9700 docker-elk_kibana "/bin/tini -- /usr/l... About a minute ago Up About a minute 0.0.0.0:5601->5601 /tcp, :::5601->5601/tcp
411676d5e72b docker-elk_elasticsearch "/bin/tini -- /usr/l... About a minute ago Up About a minute 0.0.0.0:9200->9200 /tcp, :::9200->9200/tcp, 0.0.0.0:9300->9300/tcp, :::9300->9300/tcp

```

```
[root@kali]# docker-compose ps
      Name          Command     State            Ports
docke..._elasticsearch_1   /bin/tini -- /usr/local/bi ...   Up    0.0.0.0:9200->9200/tcp, :::9200->9200/tcp,
                           0.0.0.0:9300->9300/tcp, :::9300->9300/tcp
docke..._kibana_1         /bin/tini -- /usr/local/bi ...   Up    0.0.0.0:5601->5601/tcp, :::5601->5601/tcp
docke..._logstash_1       /usr/local/bin/docker-entr ...   Up    0.0.0.0:50000->50000/tcp, :::50000->50000/tcp,
                           0.0.0.0:50000->50000/udp, :::50000->50000/udp,
                           0.0.0.0:5044->5044/tcp, :::5044->5044/tcp,
                           0.0.0.0:9600->9600/tcp, :::9600->9600/tcp
docke..._setup_1           /entrypoint.sh             Exit 0
```

El último que nos aparece “**docker-elk\_setup\_1**” nos indica que ya ha terminado de crearse. Así que ya podemos entrar en Elastic a través del navegador.

Para acceder tenemos que poner “**localhost:5601**” Username: **elastic** Password: **changeme**



Si hemos seguido todos los pasos estaremos dentro de Elastic.

## Welcome home

A screenshot of the Elastic search home dashboard. It features four main cards: "Enterprise Search" (yellow background, icon of a magnifying glass), "Observability" (pink background, icon of a chart), "Security" (teal background, icon of a shield), and "Analytics" (blue background, icon of a bar chart). Each card has a title, a brief description, and a "Read more" link.

Ahora vamos a añadir una nueva integración. En este caso la de Windows.

## Integrations

Choose an integration to start collecting and analyzing your data.

[Browse integrations](#) [Installed integrations](#)

A screenshot of the Elastic search integrations page. It shows three cards: "Web crawler" (with a magnifying glass icon), "Elastic APM" (with a bar chart icon), and "Endpoint and Cloud Security" (with a shield icon). Below these cards is a search bar with the query "windo" and a dropdown menu showing categories like "All categories" (303), "AWS" (30), "Azure" (25), "Cloud" (59), "Communications" (3), and "Config management" (2).

A screenshot of the search results for "windo". The results show two items: "Custom Windows Event Logs" (with a blue square icon) and "Windows" (with a Windows logo icon). Both items have descriptions below them: "Collect and parse logs from any Windows event log channel with Elastic Agent." and "Collect logs and metrics from Windows OS and services with Elastic Agent." respectively.

Para configurarlo podemos dejar lo primero como estaba o ponerle el nombre que queramos, y luego tenemos que seleccionar **Existing hosts** y “**Fleet Server policy**”

The screenshot shows the 'Add Windows integration' configuration page. At the top right, there are two tabs: 'Agent policy' and 'Fleet Server policy', with 'Fleet Server policy' being selected. Below the tabs, a sub-header reads 'Configure an integration for the selected agent policy.' The main area is divided into two sections: '1 Configure integration' and '2 Where to add this integration?'. In section 1, under 'Integration settings', there is a field for 'Integration name' containing 'windows-1', and a 'Description' field labeled 'Optional'. A link 'Advanced options' is also present. In section 2, under 'Where to add this integration?', there are tabs for 'New hosts' and 'Existing hosts', with 'Existing hosts' being selected. Under 'Agent policy', a dropdown menu shows 'Fleet Server policy'.

1 **Configure integration**

**Integration settings**  
Choose a name and description to help identify how this integration will be used.

Integration name: windows-1  
Description: Optional

Advanced options

2 **Where to add this integration?**

New hosts Existing hosts

**Agent policy**  
Agent policies are used to manage a group of integrations across a set of agents.

Agent policy: Fleet Server policy

Add Elastic Agent later Add Elastic Agent to your hosts

Ahora le damos a añadir a nuestro host

To complete this integration, add **Elastic Agent** to your hosts to collect data and send it to Elastic Stack

[Add Elastic Agent later](#)

[Add Elastic Agent to your hosts](#)

Seleccionamos “Run Standalone” y copiamos en el portapapeles.

## Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

[Enroll in Fleet](#) [Run standalone](#)

Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.

### 1 Configure the agent

Copy this policy to the `elastic-agent.yml` on the host where the Elastic Agent is installed. Modify `ES_USERNAME` and `ES_PASSWORD` in the `outputs` section of `elastic-agent.yml` to use your Elasticsearch credentials.

[Copy to clipboard](#)

[Download Policy](#)

```
id: fleet-server-policy
revision: 5
outputs:
  default:
    type: elasticsearch
    hosts:
      - 'http://elasticsearch:9200'
```

Abrimos algún programa que le podamos pegar texto sin perder el formato, y lo copiamos ahí.

```
<untitled> * ×
1 id: fleet-server-policy
2 revision: 5
3 outputs:
4   default:
5     type: elasticsearch
6     hosts:
7       - 'http://elasticsearch:9200'
8     username: '{ES_USERNAME}'
9     password: '{ES_PASSWORD}'
10 output_permissions:
11   default:
12     _elastic_agent_monitoring:
13       indices:
14         - names:
15           - logs-elastic_agent.apm_server-default
16         privileges:
17           - auto_configure
18           - create_doc
19         - names:
20           - metrics-elastic_agent.apm_server-default
21         privileges:
22           - auto_configure
23           - create_doc
24         - names:
25           - logs-elastic_agent.auditbeat-default
26         privileges:
27           - auto_configure
28           - create_doc
29         - names:
30           - metrics-elastic_agent.auditbeat-default
31           - ..
```

Lanzamos un comando “**ip a**” en nuestra terminal de Kali para ver la IP que tenemos.

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.90.50/24 brd 192.168.90.255 scope global dynamic noprefixroute eth0
      valid_lft 4379sec preferred_lft 4379sec
    inet6 fe80::9f62:3a8c:99a3:cec2/64 scope link noprefixroute
      valid_lft forever preferred_lft forever
```

A continuación sustituimos el fichero anterior con nuestra IP y el usuario y contraseña de Elastic.

```
type: elasticsearch
hosts:
  - 'http://192.168.90.50:9200'
username: 'elastic'
password: 'changeme'
```

En nuestro PC Windows descargamos el agente de Elastic de la siguiente web

<https://www.elastic.co/es/downloads/elastic-agent>

## Download Elastic Agent

### 1 Download Elastic Agent

Download the Elastic Agent for your chosen platform and format. We recommend using the installers (TAR/ZIP) over system packages (RPM/DEB) because they provide the ability to upgrade your agent within Fleet.

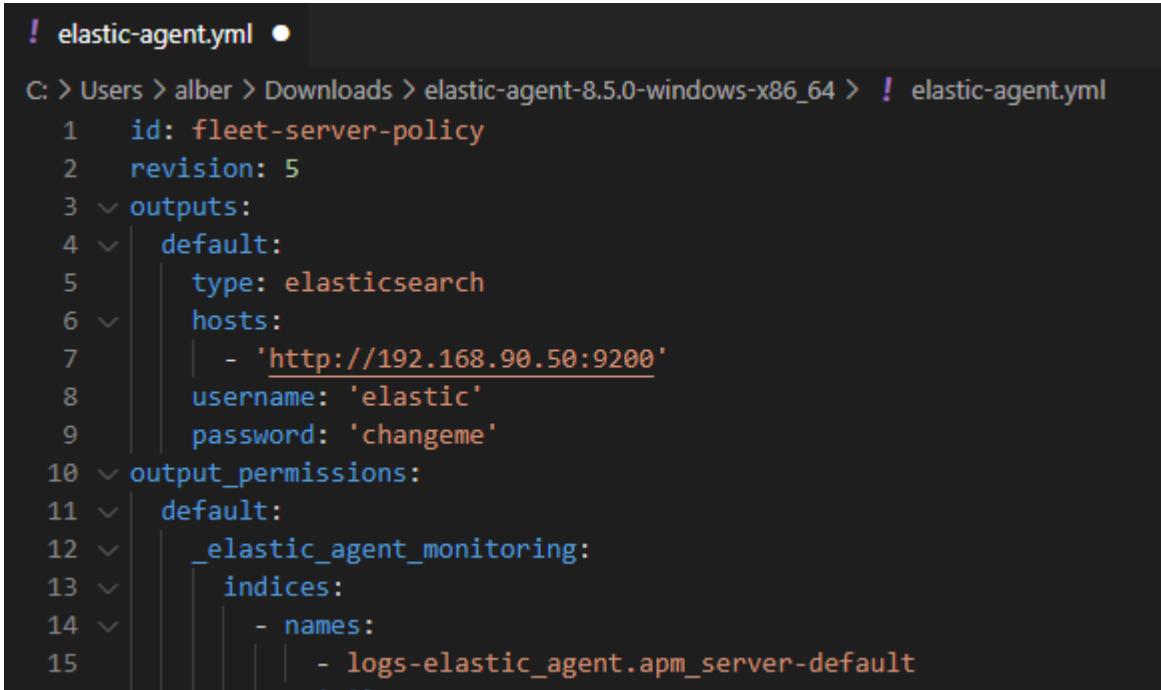
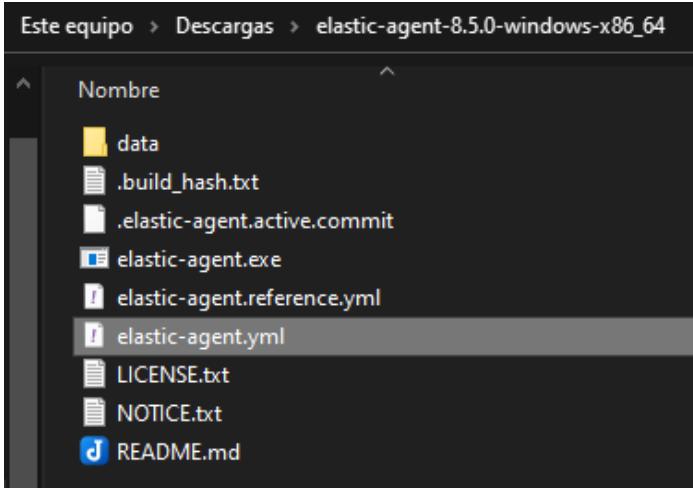
Choose platform:

Windows 64-bit

[Windows 64-bit](#)

[↓ sha](#) [↓ asc](#)

Descomprimimos el archivo, pero no lo ejecutamos. Entramos en la carpeta y abrimos el archivo **elastic-agent.yml** con Visual Studio Code y pegamos el texto que hemos editado.



```
C: > Users > alber > Downloads > elastic-agent-8.5.0-windows-x86_64 > ! elastic-agent.yml
1   id: fleet-server-policy
2   revision: 5
3   outputs:
4     default:
5       type: elasticsearch
6       hosts:
7         - 'http://192.168.90.50:9200'
8       username: 'elastic'
9       password: 'changeme'
10  output_permissions:
11    default:
12      _elastic_agent_monitoring:
13        indices:
14          - names:
15            - logs-elastic_agent.apm_server-default
16            - ...
```

Guardamos y ahora ejecutamos una terminal en Windows con permiso de administrador. Copiamos la ruta donde está el archivo **elastic-agent.yml** y entramos en la ruta mediante terminal. Listamos el directorio, y ejecutamos **elastic-agent.exe**.

```
Administrator: Símbolo del sistema - elastic-agent.exe
Microsoft Windows [Versión 10.0.19045.2193]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd C:\Users\alber\Downloads\elastic-agent-8.5.0-windows-x86_64

C:\Users\alber\Downloads\elastic-agent-8.5.0-windows-x86_64>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 1C47-3F01

Directorio de C:\Users\alber\Downloads\elastic-agent-8.5.0-windows-x86_64

11/01/2022  09:19 PM    <DIR>        .
11/01/2022  09:19 PM    <DIR>        ..
10/24/2022  09:18 PM            41 .build_hash.txt
10/24/2022  09:18 PM            41 .elastic-agent.active.commit
10/24/2022  09:18 PM    <DIR>        data
10/24/2022  09:18 PM        45,205,416 elastic-agent.exe
10/24/2022  09:18 PM            9,164 elastic-agent.reference.yml
11/01/2022  09:27 PM            17,101 elastic-agent.yml
10/24/2022  09:18 PM            13,675 LICENSE.txt
10/24/2022  09:18 PM            929,848 NOTICE.txt
10/24/2022  09:18 PM            864 README.md
                           8 archivos     46,176,150 bytes
                           3 dirs   106,729,312,256 bytes libres

C:\Users\alber\Downloads\elastic-agent-8.5.0-windows-x86_64>elastic-agent.exe
```

Ahora nos vamos a nuestro **Elastic** y abrimos **Dashboards**. Dentro se encuentra **[Metrics Windows] Services**. Pinchamos y lo abrimos para ver las gráficas.

The screenshot shows the Elastic Dashboards interface. At the top, there is a search bar with the placeholder "Search...". Below the search bar is a table with three columns: "Title", "Description", and "Tags". There is one visible row in the table:

| Title                                      | Description                            | Tags |
|--|--|------|
| <a href="#">[Metrics Windows] Services</a> | Overview of the Windows Service States |      |

Pero en mi caso hay un fallo que no he conseguido solucionar y no me muestra las gráficas y estadísticas.

The screenshot shows a dashboard interface with five separate sections, each displaying a red warning icon (triangle with exclamation mark) and an error message. The sections are:

- Startup States [Metrics Windows]**: The field "windows.service.id" associated with this object no longer exists in the data view. Please use another field.
- Unique Services [Metrics Windows]**: The field "windows.service.id" associated with this object no longer exists in the data view. Please use another field.
- Non-zero Service Exit Codes [Metrics Windows]**: The field "windows.service.id" associated with this object no longer exists in the data view. Please use another field.
- Hosts [Metrics Windows]**: The field "host.name" associated with this object no longer exists in the data view. Please use another field.
- Service States [Metrics Windows]**: The field "windows.service.display\_name" associated with this object no longer exists in the data view. Please use another field.