

Blue Team





Archivos necesarios:

- [VirtualBox](#)
- [Windows 11](#) (Se obtiene a través de una aplicación de creación de medios)
- [Pfsense](#)
- [VPN Connect](#)
- [Kali Linux](#) (En este caso se selecciona la opción de VirtualBox)

El primer paso para crear el entorno es instalar VirtualBox. Tras esto se procede a cargar la imagen ISO de Pfsense:

A screenshot of the 'Name and Operating System' tab in the Virtual Machine creation wizard. The 'Nombre' field is set to 'Pfsense_practica'. The 'Folder' is 'C:\Users\dany_\VirtualBox VMs'. The 'ISO Image' is 'C:\Users\dany_\Documentos\Keepcoding\Practicas\Blue Team\pfSense-CE-2.6.0-RELEASE-amd64.iso'. The 'Tipo' is 'BSD' and the 'Versión' is 'FreeBSD (64-bit)'. There is a checkbox for 'Skip Unattended Installation' which is currently unchecked.

Ubicada la imagen, se procede a continuar con los ajustes predeterminados.

Para crear la imagen con el sistema de Windows 11 el procedimiento es exactamente igual que para crear la imagen de PFsense:

A screenshot of the 'Name and Operating System' tab in the Virtual Machine creation wizard for Windows. The 'Nombre' field is set to 'Windows_practica'. The 'Folder' is 'C:\Users\dany_\VirtualBox VMs'. The 'ISO Image' is 'C:\Users\dany_\Documentos\Keepcoding\Pentesting_desde_cero\Instaladores\Windows.iso'. The 'Tipo' is 'Microsoft Windows' and the 'Versión' is 'Other Windows (64-bit)'. There is a checkbox for 'Skip Unattended Installation' which is currently unchecked. Below the settings, there are three blue buttons: '> Unattended Install', '> Hardware', and '> Hard Disk'.



Inicio de configuración:

Se procede a la configuración/creación de redes para Pfsense:

El resultado debe ser el siguiente:



Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Enable Network Adapter

Conectado a: Red interna

Nombre: DMZ_2

Aceptamos y si se ha hecho de forma correcta, el resultado debe ser:

Red

Adaptador 1: Intel PRO/1000 MT Desktop (Adaptador puente, «Intel(R) Wi-Fi 6 AX201 160MHz»)

Adaptador 2: Intel PRO/1000 MT Desktop (Red interna, «LAN»)

Adaptador 3: Intel PRO/1000 MT Desktop (Red interna, «DMZ»)

Adaptador 4: Intel PRO/1000 MT Desktop (Red interna, «DMZ_2»)

Hay que añadir antes de proceder a la configuración la opción de cd vivo:

Almacenamiento

Dispositivos de almacenamiento

Controlador: IDE

Unidad óptica: IDE secundario maestro

☒ CD/DVD vivo

Se procede a ejecutar la configuración interna de Pfsense:

Welcome to pfSense!

Install	Install pfSense
Rescue Shell	Launch a shell for rescue operations
Recover config.xml	Recover config.xml from a previous install

Archivo Máquina Ver Entrada Dispositivos Ayuda

pfSense Installer

Keymap Selection

The system console driver for pfSense defaults to standard "US" keyboard map. Other keymaps can be chosen below.

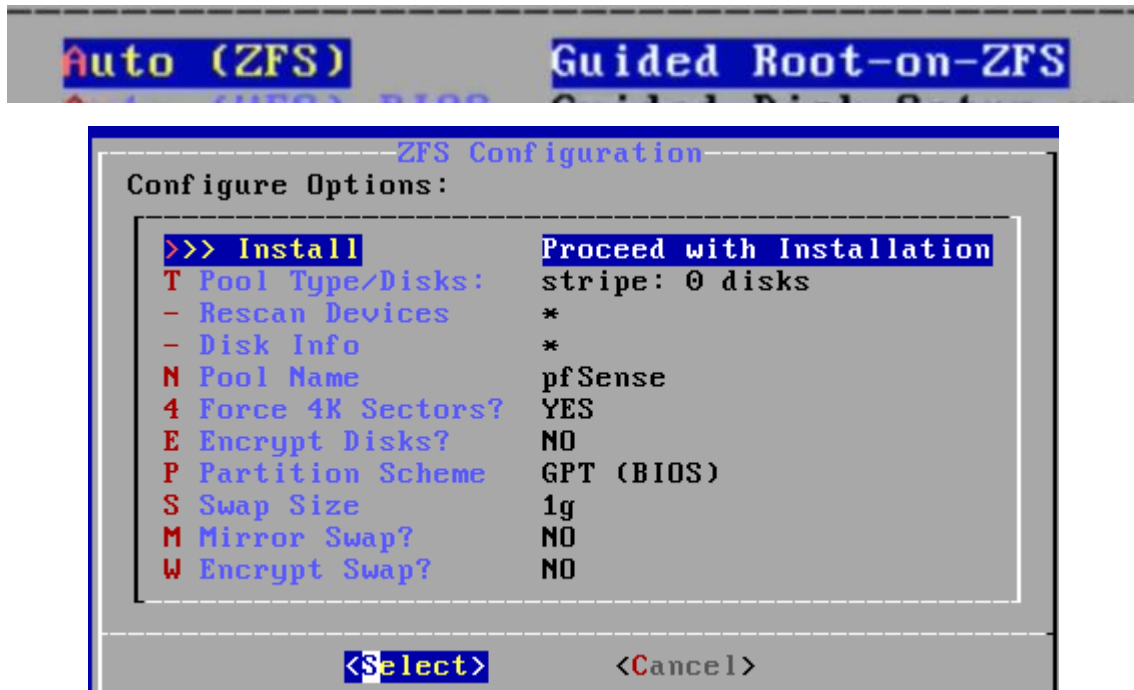
- () Slovenian
- () Spanish
- (*) **Spanish (accent keys)**
- () Spanish Dvorak
- () Swedish
- () Swiss-French
- () Swiss-French (accent keys)
- () Swiss-German
- () Swiss-German (MacBook/MacBook Pro) (accent keys)
- () Swiss-German (accent keys)
- () Turkish (F)
- () Turkish (Q)

80%

<Select> **<Cancel>**

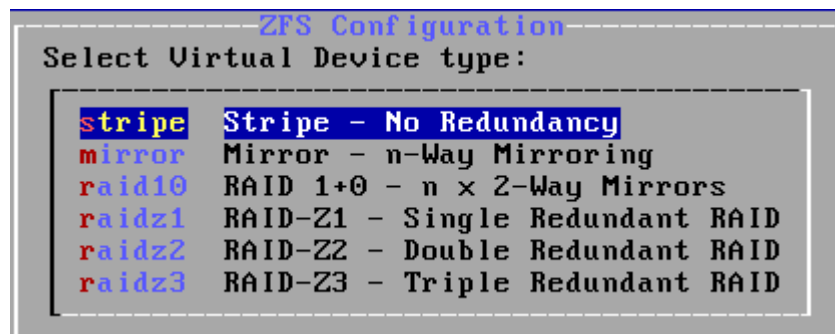


Se procede a la configuración del sistema ZFS (sistema de archivos de próxima generación, diseñado originalmente para proporcionar soluciones NAS con seguridad, confiabilidad y rendimiento mejorados):

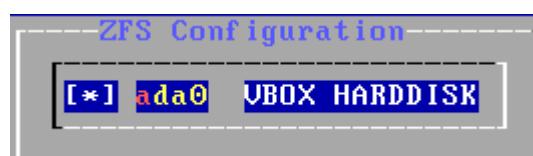


Sin realizar cambio alguno procedemos a instalar.

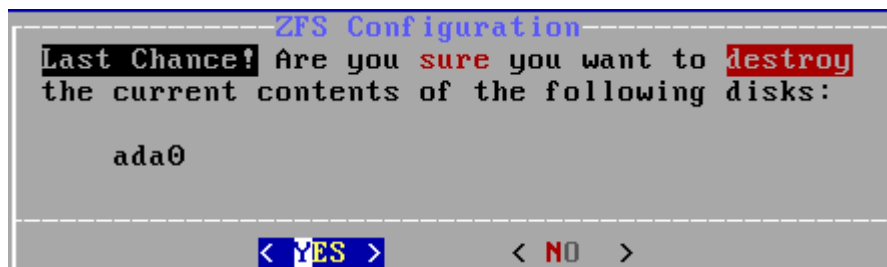
La ventana que aparece es la siguiente:



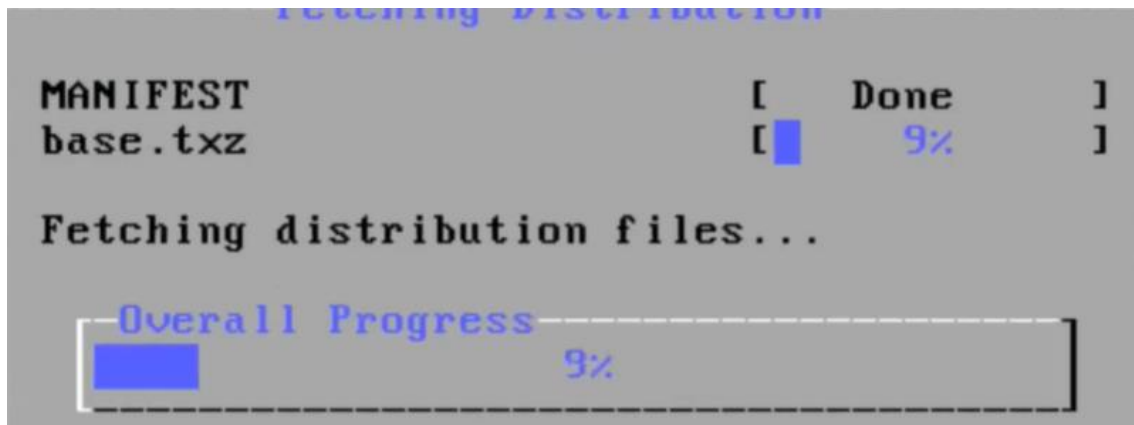
Se selecciona la opción stripe para activar su opción:



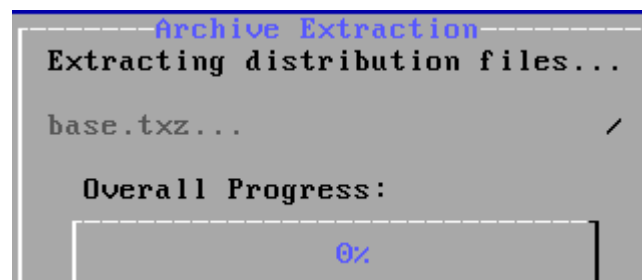
Al aceptar los cambios marcados nos pide confirmar la decisión tomada en la que hay que aceptar los cambios:



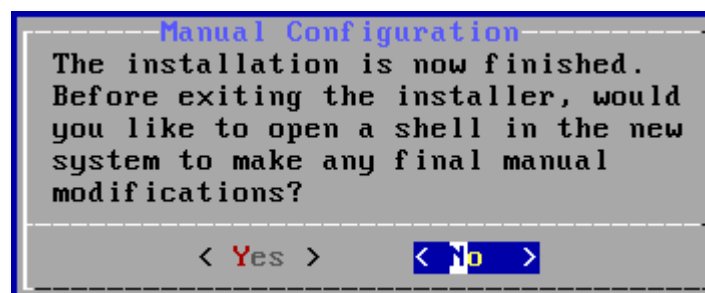
Aparece un proceso de formateo:



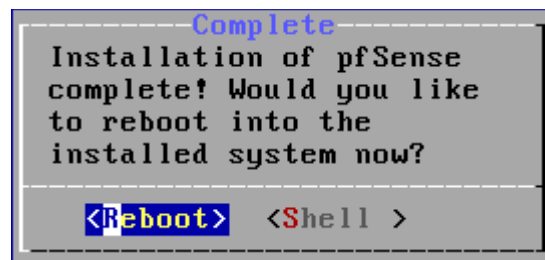
Posteriormente carga/extracción los archivos:



Al finalizar este proceso aparece una nueva ventana en la que se nos pide si deseamos abrir un terminal o no, en este caso no lo queremos por lo que optamos por la opción no:

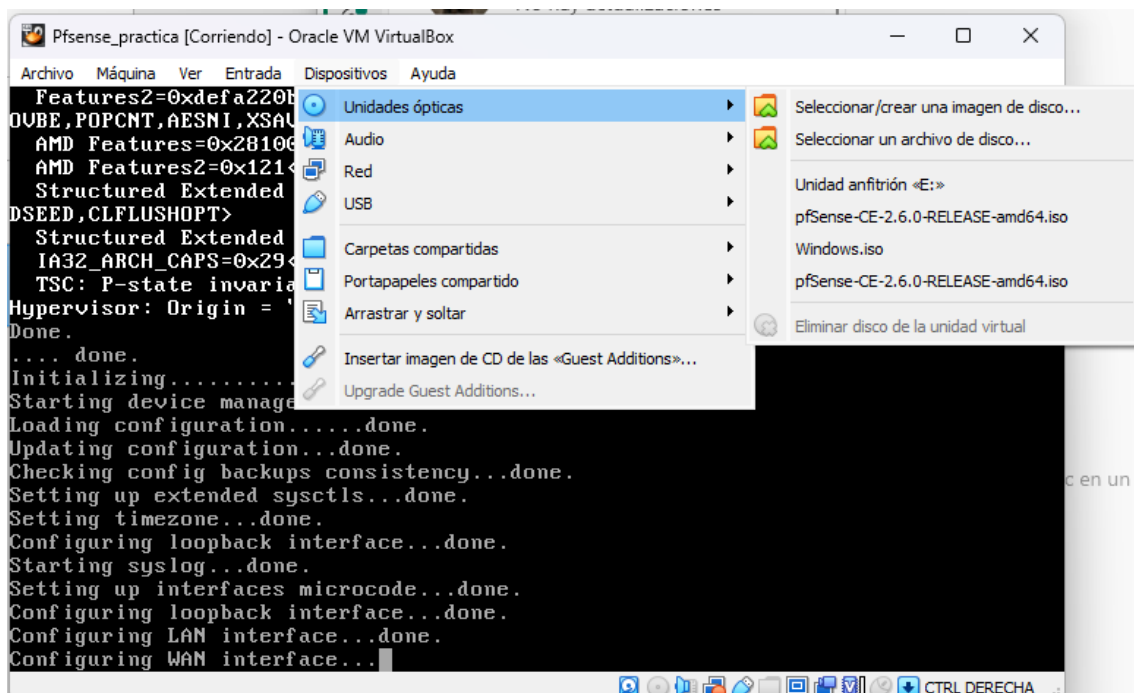


Y, por último, nos pide acceder a un terminal o reiniciar para aplicar cambios:



En este caso aplicamos el reinicio.

IMPORTANTE: Antes de que finalice el reinicio hay que expulsar el cd/dvd vivo que se activo antes de lanzar la aplicación:



Hay que seleccionar la opción de Eliminar disco de la unidad virtual siguiendo la ruta mostrada en la captura de arriba.

Iniciando configuración y asignación de redes dentro de PFsense

Una vez configurado (hasta donde se muestra en las capturas anteriores) aparece una nueva ventana con un menú:



```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.43/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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: 1
```

Se selecciona la opción 1 y se procede a configurar las interfaces.

```
Enter an option: 1

Valid interfaces are:

em0      08:00:27:0a:e2:3e   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:ca:db:08   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:81:de:38   (down) Intel(R) Legacy PRO/1000 MT 82540EM
em3      08:00:27:49:23:6d   (down) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y|n]? n
```

Tras seleccionar la opción 1 nos refleja las 4 redes que previamente hemos creado y se selecciona n de no a la pregunta de si se debería configurar el set up de VLAN.

Acto seguido se va a asignar una de las redes a la conexión WAN (conecta entre sí a las oficinas, los centros de datos, las aplicaciones en la nube y el almacenamiento en la nube):

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

La red Lan se va a asignar a em1 que es el siguiente paso tras asignar em0 a WAN:

```
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
```




La primera red DMZ corresponde a em2:

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

Y, por último, la red DMZ_2 la vamos a asignar a em3:

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

Al finalizar Pfsense muestra un resumen para verificar que la configuración es la correcta, en caso afirmativo aceptamos la configuración marcando “y”:

```
The interfaces will be assigned as follows:

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

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

El resultado de configurar las redes debe ser el siguiente:

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.43/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->
OPT2 (opt2)    -> em3      ->

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
```



El siguiente paso es asignar direcciones IP a cada una de las redes, para ello marcamos la opción 2:

```
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: 2
```

Se comienza por la red em1 o, a partir de ahora, LAN:

```
Enter an option: 2

Available interfaces:

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

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

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

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

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

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) 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: 192.168.100.150
Disabling IPv6 DHCPD...

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



```
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

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

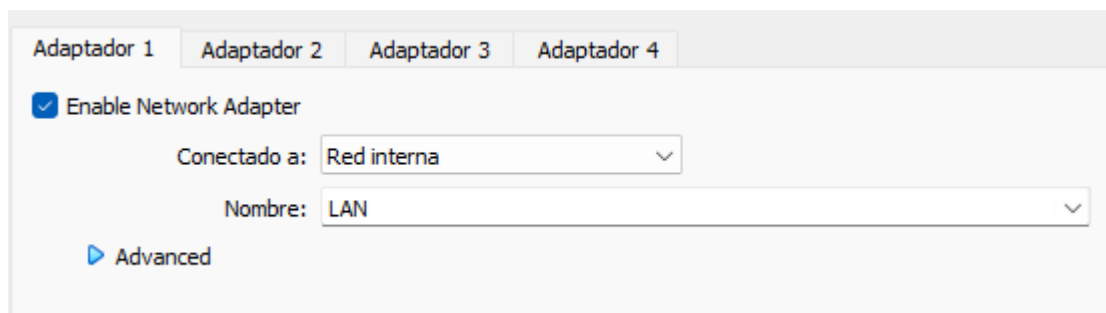
Press <ENTER> to continue.
```

La configuración que se ha escogido es:

- IP estática -> 192.168.100.254, ip por la que accederemos a la configuración vía interfaz gráfica de Pfsense.
- Rango de IP -> 24
- IPv6 -> DHCP NO configurado e IP de v6 sin asignar.
- Rangos de IP -> Red LAN abarca desde 192.168.100.100 a 192.168.100.150

Estos cambios hacen que Pfsense quede establecido en una dirección ip tipo v4 fija y un rango determinado.

Cambiar tipo de red de Windows a LAN:



Con este cambio conseguimos que el tráfico de Windows pase por la configuración LAN creada anteriormente.

IP de Windows:

```
C:\Users\Windows_practica>ipconfig

Configuración IP de Windows

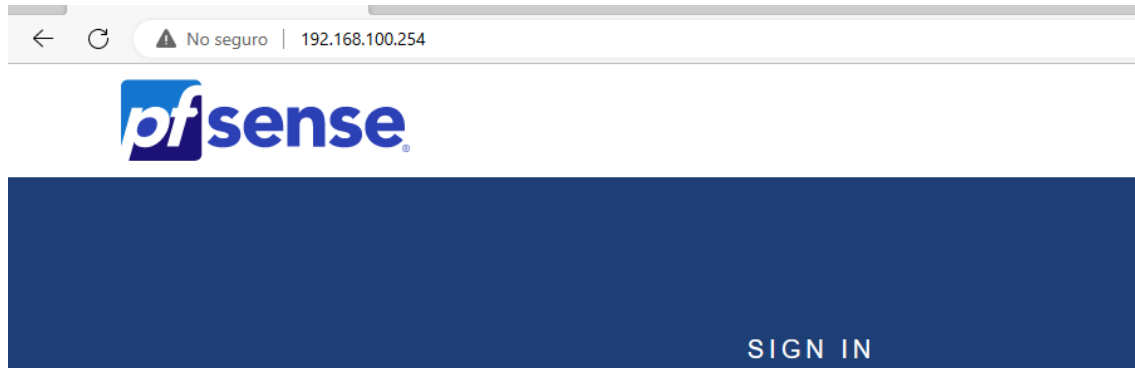
Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . : home.arpa
    Vínculo: dirección IPv6 local. . . . . : fe80::d080:8871:2abb:f6b2%13
    Dirección IPv4. . . . . : 192.168.100.100
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.100.254
```

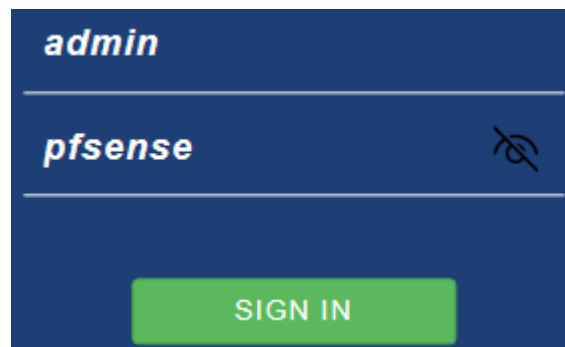


Se puede ver que el cambio ha sido realizado correctamente ya que está configurado dentro del intervalo asignado a LAN.

Si el cambio es correcto, se puede lanzar en cualquier navegador de Windows la dirección de Pfsense (192.168.100.254) y poder acceder a él:



Para acceder a Pfsense los credenciales son: Usuario “admin” y contraseña “pfsense”:



Tras salir dos ventanas en las que aparece una bienvenida y una breve introducción, se comienza la configuración:

Hostname	<input type="text" value="Practica"/> <small>EXAMPLE: myserver</small>
Domain	<input type="text" value="practica.local"/> <small>EXAMPLE: mydomain.com</small>
<small>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.</small>	
Primary DNS Server	<input type="text" value="1.1.1.1"/>
Secondary DNS Server	<input type="text" value="8.8.8.8"/>
Override DNS	<input checked="" type="checkbox"/> <small>Allow DNS servers to be overridden by DHCP/PPP on WAN</small>
» Next	



Es muy importante dejar marcado, o marcar si no lo estuviese, la opción de sobrescribir dns.

Se configura la zona horaria, en este caso se selecciona Madrid:

Please enter the time, date and time zone.

Time server hostname	<input type="text" value="2.pfsense.pool.ntp.org"/>
Enter the hostname (FQDN) of the time server.	
Timezone	<input type="text" value="Europe/Madrid"/>

En el siguiente paso hay varias opciones necesarias para configurar:

Configure WAN Interface

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

SelectedType	<input type="text" value="DHCP"/>
--------------	-----------------------------------

RFC1918 Networks

Block RFC1918 Private Networks ☐ Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks ☐ Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

No es necesario bloquear las redes privadas puesto que se va a proceder a crear una VPN posteriormente.

En el siguiente paso no es necesario modificar nada puesto que ya se configuró previamente en el inicio de Pfsense vía consola de comandos:

Configure LAN Interface

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

LAN IP Address	<input type="text" value="192.168.100.254"/>
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	<input type="text" value="24"/>



Se nos da una oportunidad de modificar la contraseña de acceso a Pfsense (por ahora su contraseña es pfsense). Para esta práctica este paso se omite:

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

A continuación, la interfaz nos solicita una recarga para aplicar los datos hasta ahora configurados:

Reload configuration

Click 'Reload' to reload pfSense with new changes.

[Reload](#)

Por último, aparece una última ventana informando que la configuración se ha modificado correctamente:

Wizard completed.

Congratulations! pfSense is now configured.

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

[Check for updates](#)

Cuando Pfsense está configurado aparece una ventana con fondo de color azul dando la bienvenida:

Copyright and Trademark Notices.

Copyright© 2004-2016. Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved.
Copyright© 2014-2023. Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

pfSense® software is open source and distributed under the Apache 2.0 license. However, no commercial distribution of ESF and/or Netgate

Desde aquí se va a proceder a configurar el resto de funciones y tener al 100% operativo lo necesario.



Configurando DMZ y DMZ_2

En la configuración por terminal o previa no se configuraron estas dos redes, solo se invocaron. Ahora es el momento de su configuración, para ello en el menú superior se procede a ir a Interfaces – OPT1:

Interfaces / OPT1 (em2)

General Configuration

Enable ☒ Enable interface

Description

Enter a description (name) for the interface here.

IPv4 Configuration Type

Esta se procederá a renombrar a DMZ y con un tipo de configuración IPv4 estático. En cuanto a IPv6 se queda en blanco.

Static IPv4 Configuration

IPv4 Address /

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](#).

No es necesario configurar la puerta de enlace ya que la propia dirección asignada va a actuar como si de una se tratase.

Acto seguido se procede a guardar y aplicar cambios.

Se procede de igual forma que en el caso de DMZ:

Interfaces / OPT2 (em3)

General Configuration

Enable ☒ Enable interface

Description

Enter a description (name) for the interface here.

IPv4 Configuration Type



Static IPv4 Configuration

IPv4 Address /

Para DMZ_2 se ha configurado en otro rango de IPs, esta vez ha sido 192.168.80.1/24.

En el terminal se puede comprobar que también se ha configurado de forma correcta:

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.43/24
LAN (lan)      -> em1      -> v4: 192.168.100.254/24
DMZ (opt1)     -> em2      -> v4: 192.168.90.1/24
DMZ_2 (opt2)   -> em3      -> v4: 192.168.80.1/24
```

Para que las redes DMZ y DMZ_2 tengan conexión a internet es necesario configurarlas en el servidor DHCP.

Se procede a su configuración para ambas redes. El primer paso es ir a Services – DHCP Server

LAN **DMZ** DMZ_2

General Options

Enable ☒ Enable DHCP server on DMZ interface

Range
From To

DNS servers

Other Options

Gateway



Se procede a guardar cambios y a continuación en el apartado DHCP Static Mappings for this Interface se añade una nueva:

DHCP Static Mappings for this Interface (total: 1)					
Static ARP	MAC address	Client Id	IP address	Hostname	Description
	08:00:27:96:e7:bc	ELK	192.168.90.220	ELK	

[+ Add](#)

Static DHCP Mapping on DMZ

MAC Address [Copy My MAC](#)
MAC address (6 hex octets separated by colons)

Client Identifier

IP Address
If an IPv4 address is entered, the address must be outside of the pool.
If no IPv4 address is given, one will be dynamically allocated from the pool.
The same IP address may be assigned to multiple mappings.

Hostname
Name of the host, without domain part.

Description
A description may be entered here for administrative reference (not parsed).

ARP Table Static Entry ☐ Create an ARP Table Static Entry for this MAC & IP Address pair.

WINS Servers

DNS Servers
Note: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or R on the General page.

Gateway
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway network.

Los datos insertados son:

- Dirección Mac -> Se puede obtener simplemente haciendo click en Copy My MAC.
- Identificador de cliente -> En este caso se ha llamado ELK ya que en DMZ va a ir alojado este servicio.
- Dirección IP -> Se asigna 192.168.90.220 fuera del rango establecido en la venta anterior.
- Nombre de Host -> ELK también.
- Servidores DNS -> 1.1.1.1 para el primario y 8.8.8.8 para el secundario.
- Puerta de enlace -> 192.168.90.1, sería la dirección de IP que conecta con el resto de servicios externos.



Acto seguido se procede a guardar la configuración y aplicar cambios.

Si se cambia la red de Windows a DMZ se puede comprobar que el cambio es correcto:

```
C:\Users\Windows_practica>IPCONFIG

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . : practica.local
    Vínculo: dirección IPv6 local. . . . . : fe80::d080:8871:2abb:f6b2%13
    Dirección IPv4. . . . . : 192.168.90.220
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.90.1
```

En el caso de DMZ_2 la configuración es la misma, con algunas salvedades:

LAN

DMZ

DMZ_2

General Options

Enable

☒ Enable DHCP server on DMZ_2 interface

Subnet

192.168.80.0

Subnet mask

255.255.255.0

Available range

192.168.80.1 - 192.168.80.254

Range

192.168.80.100

192.168.80.200

FromTo

Other Options

Gateway

192.168.80.1

DHCP Static Mappings for this Interface (total: 1)

Static ARP	MAC address	Client Id	IP address	Hostname	Description
	08:00:27:c5:50:70	HONEYPOT	192.168.80.220	HONEYPOT	



Static DHCP Mapping on DMZ_2

MAC Address	<input type="text" value="08:00:27:c5:50:70"/>	Copy My MAC
MAC address (6 hex octets separated by colons)		
Client Identifier	<input type="text" value="HONEYPOT"/>	
IP Address	<input type="text" value="192.168.80.220"/>	
If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool. The same IP address may be assigned to multiple mappings.		
Hostname	<input type="text" value="HONEYPOT"/>	
Name of the host, without domain part.		
Description	<input type="text"/>	
A description may be entered here for administrative reference (not parsed).		
ARP Table Static Entry	<input type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair.	
WINS Servers	<input type="text" value="WINS 1"/> <input type="text" value="WINS 2"/>	
DNS Servers	<input type="text" value="1.1.1.1"/> <input type="text" value="8.8.8.8"/> <input type="text" value="DNS 3"/> <input type="text" value="DNS 4"/>	
Note: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled on the General page.		
Gateway	<input type="text" value="192.168.80.1"/>	

El resultado se puede ver a continuación:

```
C:\Users\Windows_practica>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . : practica.local
    Vínculo: dirección IPv6 local. . . : fe80::d080:8871:2abb:f6b2%13
    Dirección IPv4. . . . . : 192.168.100.10
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.100.254

C:\Users\Windows_practica>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . : practica.local
    Vínculo: dirección IPv6 local. . . : fe80::d080:8871:2abb:f6b2%13
    Dirección IPv4. . . . . : 192.168.80.220
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.80.1
```

Se aprecia que con la red LAN la IP asignada es 192.168.100.10 y, tras el cambio y configuración a DMZ_2 la dirección IP es 192.168.80.220.



VPN creación

En primer lugar, se va a necesitar instalar un paquete llamado “openvpn-client-export”, el método para obtenerlo es System – Package Manager:

Installed Packages

Available Packages

Search

Search term

OPEN

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
frr	1.1.1_7	FRR routing daemon for BGP, OSPF, and OSPF6 Conflicts with Quagga OSPF and OpenBGPD. These packages cannot be installed at the same time. Package Dependencies: frr7-pythontools-7.5.1_3 frr7-7.5.1_3	+ Install
Open-VM-Tools	10.1.0_5,1	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. Package Dependencies: open-vm-tools-11.3.5_1,2	+ Install
openvpn-client-export	1.6_9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. Package Dependencies: openvpn-client-export-2.5.8 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3	+ Install

Se instala y a continuación toca esperar a que se instale:

Package Installation

All repositories are up to date.
The following 4 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
openvpn-client-export: 2.5.8 [pfSense]

Cuando finalice aparecerá un mensaje similar a este:

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

El siguiente paso es crear un servidor DNS. Se accede desde Services – DNS Resolver:

Host Overrides

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



Habría que crear un perfil nuevo dentro de este apartado:

Host	<input type="text" value="Practica_clase"/>
Name of the host, without the domain part e.g. enter "myhost" if the full domain name is "myhost.example.com"	
Domain	<input type="text" value="practica.local"/>
Parent domain of the host e.g. enter "example.com" for "myhost.example.com"	
IP Address	<input type="text" value="192.168.100.10"/>
IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3	
Description	<input type="text" value="Servidor"/>
A description may be entered here for administrative reference (not parsed).	

Cualquier equipo que se conecte al host se va a conectar a través de la ip fijada. Es necesario guardar y, posteriormente, aplicar los cambios hechos.

A continuación, hay que crear un certificado. La ruta de acceso es System – Certificate Manager:

Se comienza creando una CA (autoridad de certificación):



[System](#) / [Certificate Manager](#) / [CAs](#) / [Edit](#)

[CAs](#) [Certificates](#) [Certificate Revocation](#)

Create / Edit CA

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

Internal Certificate Authority

Key type	<input type="text" value="RSA"/>
	<input type="text" value="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 c
Digest Algorithm	<input type="text" value="sha256"/> The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may co
Lifetime (days)	<input type="text" value="3650"/>
Common Name	<input type="text" value="Certificado_practica"/>





Country Code	<input type="text" value="ES"/>
State or Province	<input type="text" value="Andalucia"/>
City	<input type="text" value="Jaen"/>
Organization	<input type="text" value="Particular"/>



Los datos insertados hacen referencia al tipo de certificado que se desea crear:

- Nombre descriptivo -> Se ha usado uno relacionado con la práctica: Certificado_practica.
- Método -> Interno ya que solo se va a operar de forma interna.
- Tipo de encriptación -> RSA, es el método que viene por defecto.
- Longitud -> 2048 bits, cuanto mayor es el número de bits más difícil de obtener la clave es.
- Logaritmo -> SHA256, es el más común actualmente, es de tipo SHA2. Si se quiere mejorar se puede optar por usar SHA3 o SHA2 de 512 bits.
- Tiempo de vida -> Se ha fijado en 3650 días (la cantidad por defecto), es el tiempo que dura el certificado antes de expirar.
- Nombre común -> Certificado_práctica. Se ha mantenido la misma estructura que con el resto de servicios y configuraciones.
- El resto de información es rellenar campos de ubicación.

Al guardar la configuración expuesta, el resultado queda así:

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Certificado_practica	✓	self-signed	0	ST=Andalucia, O=Particular, L=Jaen, CN=Certificado_practica, C=ES Valid From: Sun, 09 Apr 2023 11:12:47 +0200 Valid Until: Wed, 06 Apr 2033 11:12:47 +0200		   

El siguiente paso es crear un certificado, la ruta es exactamente igual que para hacer un CA -> System – Certificate Manager, pero seleccionando la pestaña certificates:

System / Certificate Manager / Certificates

CAs

Certificates

Certificate Revocation

Search





Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (64319ef6d3090) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-64319ef6d3090 Valid From: Sat, 08 Apr 2023 19:05:58 +0200 Valid Until: Fri, 10 May 2024 19:05:58 +0200		   

+ Add/Sign



Es necesario crear el certificado para el servidor VPN:

CAs	Certificates	Certificate Revocation
-----	---------------------	------------------------

Add/Sign a New Certificate

<u>Method</u>	Create an internal Certificate
---------------	--------------------------------

<u>Descriptive name</u>	vpn.practica.local
-------------------------	--------------------

Internal Certificate

<u>Certificate authority</u>	Certificado_practica
------------------------------	----------------------

<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 algorithms deprecated.

<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.practica.local
--------------------	--------------------



Country Code	ES
State or Province	Andalucia
City	Jaen
Organization	Particular
Organizational Unit	e.g. My Department Name (optional)

Certificate Attributes

Attribute Notes

The following attributes are added to certificates and n
selected mode.

For Internal Certificates, these attributes are added dire

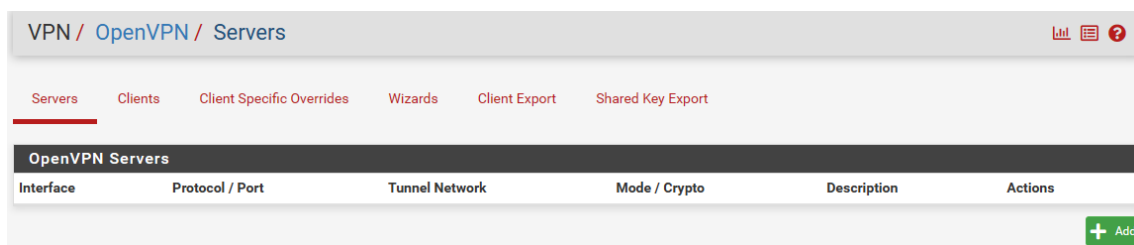
Certificate Type

Server Certificate

Se ha asignado un nombre descriptivo “vpn.practica.local” y se puede apreciar que en el campo CA (certificate authority) ha cogido por defecto el CA que se ha creado previamente.

Acto seguido se procede a guardar y se obtiene el certificado para el servidor.

Con todos estos pasos dados se puede proceder a crear el servidor VPN ya, para ello hay que acudir a VPN – OpenVPN:





Se procede a crear el servidor:

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Ex

General Information

Description

Vpn to 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 (ovpns1)

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 c
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol

TCP on IPv4 only

Inicio

▼

Interface

LAN

▼

The interface or Virtual IP address where OpenVPN will receive client connections.

Local port

1194

The port used by OpenVPN to receive client connections.



Cryptographic Settings	
TLS Configuration	<div><input checked="" type="checkbox"/> Use a TLS Key</div> <p>A TLS key enhances security of an OpenVPN connection by requiring both parties. This layer of HMAC authentication allows control channel packets without the need for encrypted connections. The TLS Key does not have any effect on tunnel data.</p>
<u>TLS Key</u>	<div><pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 60fb5fb898b23642262ba243daf4a327</pre></div> <p>Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication.</p>
<u>TLS Key Usage Mode</u>	<div><div>TLS Authentication</div></div> <p>In Authentication mode the TLS key is used only as HMAC authentication for the control channel. In Encryption and Authentication mode also encrypts control channel communications.</p>
<u>TLS keydir direction</u>	<div><div>Use default direction</div></div> <p>The TLS Key Direction must be set to complementary values on the client and server. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.</p>
<u>Peer Certificate Authority</u>	<div><div>Certificado_practica_mejorado</div></div>
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Certificates
OCSP Check	<div><input type="checkbox"/> Check client certificates with OCSP</div>
<u>Server certificate</u>	<div><div>Certificado_practica1 (Server: Yes, CA: Certificado_practica_mejorado)</div></div>
<u>DH Parameter Length</u>	<div><div>2048 bit</div></div> <p>Diffie-Hellman (DH) parameter set used for key exchange. i</p>



Hardware Crypto	Intel RDRAND engine - RAND
Certificate Depth	One (Client+Server) When a certificate-based client logs in, do not accept certificates below this generated from the same CA as the server.
Strict User-CN Matching	<input type="checkbox"/> Enforce match When authenticating users, enforce a match between the common name of
Client Certificate Key Usage Validation	<input checked="" type="checkbox"/> Enforce key usage Verify that only hosts with a client certificate can connect (EKU: "TLS Web C
Tunnel Settings	
IPv4 Tunnel Network	192.168.225.0/24 This is the IPv4 virtual network or network type alias with a single entry user expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in usable addresses will be assigned to connecting clients.
IPv6 Tunnel Network	 This is the IPv6 virtual network or network type alias with a single entry user expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to connecting clients.
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	192.168.90.0/24, 192.168.100.0/24, 192.168.80.0/24




Los datos usados son:

- Es una VPN que nos da acceso a la Lan creada.
- En el método usado se escoge acceso remoto con acceso por doble factor (pide usuario + contraseña y certificado).
- El modo dispositivo se escoge el método tipo túnel de capa 3 (a nivel IP).
- Protocolo -> TCP on IPv4 only.
- Tipo de interfaz -> LAN.
- En el campo Par Certificate Authority (CA) se selecciona, si no aparece por defecto, el CA creado. Al igual que sucede en el servidor de certificados, si no aparece por defecto el que se ha creado se seleccionar "vpn.practica.local".
- Hardware de encriptación se aplica la opción Intel por ser más rápida y mejor que la opción por defecto.



- Hay que asignar una dirección para el túnel, en este caso se usa: 192.168.225.0/24.
- IPv4 local network indica a qué redes se pueden conectar las peticiones de entrada, se da permiso para acceder a: 192.168.90.0/24, 192.168.100.0/24, 192.168.80.0/24, que son las redes DMZ, LAN y DMZ_2 respectivamente.
- El resto de parámetros se mantiene por defecto.

El resultado tras guardar los cambios es:

Servers	Clients	Client Specific Overrides	Wizards	Client Export	Shared Key Export
OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
LAN	TCP4 / 1194 (TUN)	192.168.225.0/24	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 to Lan	  

Creación de usuarios

Son necesarios para darles acceso a los servicios creados, en este caso por ahora solo hay VPN. La ruta de acceso es System – User Manager:



System / User Manager / Users / Edit

[Users](#)[Groups](#)[Settings](#)[Authentication Servers](#)

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username VPN

Password

Full name vpn

User's full name, for administrative information only

Expiration date 04/24/2023

Leave blank if the account shouldn't expire, otherwise enter the

Custom Settings ☐ Use individual customized GUI options and dashboard layout

Group membership admins



Certificate ☒ Click to create a user certificate

Create Certificate for User

Descriptive name

Certificate authority

Key type

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 it invalid.

Digest Algorithm

The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may not support it.

Lifetime

Es importante activar la opción de crear certificado para usuario.

Los datos empleados para crear el usuario son:

- Nombre de usuario -> VPN.
- Contraseña -> 1234.
- Nombre completo -> vpn.
- Fecha expiración -> 24/04/2023.
- Dentro del certificado para usuario, todo queda completado de forma automática menos el nombre que se asigna "vpn" también.

Acto seguido se procede a guardar los cambios. Este es el resultado tras guardar cambios:

System / [User Manager](#) / [Users](#)

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

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



Configurar Cortafuegos

El primer paso es crear una regla NAT (significa traducción de direcciones IP. Es decir, su trabajo consiste en coger una dirección IP privada y traducirla a una dirección IP pública o viceversa), se accede desde Firewall – NAT:

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
										Add Add Delete Save Separator

Aquí se procede a crear una nueva regla:

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination ☐ Invert match. WAN address
Type Address/mask

Destination port range Other 9090 Other 9090
From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Single host 192.168.90.220
Type Address

Description Servidor web
A description may be entered here for administrative reference (not parsed).



Acto seguido hay que crear una regla. Firewall – Rules:

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) is sent back to the sender, whereas with block the packet is dropped silently. In either case, the original packet is not sent.

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

Source

☐ Invert match

DMZ net

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

(other)

Webs

(other)

Webs

From

Custom

To

Custom

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

Extra Options

Log

☐ Log packets that are handled by this rule

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

Description

Webs

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

Con estas capturas se ve que se ha creado una regla de lista blanca en la que se permite el paso “Pass” en la interfaz DMZ para las IPv4 con el protocolo TCP (bidireccional: recepción y envío), se usa el recurso dmz net con el alias (que se explica más abajo el cómo crearlo) y cuyo nombre se ha establecido como Webs.



Es necesario crear una segunda regla:

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) whereas with block the packet is dropped silently. In either case, the original packet is not sent.

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/UDP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

DMZ net

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 the default value, any.

Destination

Destination

☐ Invert match

any

Destination Address

Destination Port Range

DNS (53)

From

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.

Esta vez se usa un doble protocolo TCP o UDP para el puerto 53 que corresponde al servidor DNS.

Para poder crear las reglas (en Destination Port Range se usan) es necesario tener uno o más alias creados, se accede desde Firewall – Aliases:



Firewall / Aliases / Edit

Properties

Name Webs
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
A description may be entered here for administrative reference (not parsed).

Type Port(s) ▼

Port(s)

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

Port	80	Description	Delete
	443	Description	Delete

Para ello se ha creado un nuevo alias llamado Webs, de tipo puertos que abarcan el 80 y el 443.

Cuando los usuarios accedan a nuestro VPN, será necesario crear una regla adicional para permitirles el paso:

Se accede a Firewall – Rules y vamos a la pestaña WAN (el vpn se configuró para que se accediera a la red WAN y después derive a las demás redes).

Destination

Destination ☐ Invert match This firewall (self) ▼ Destination Address / ▼

Destination Port Range (other) ▼ 1194 (other) ▼ 1194
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

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

Description VPN to Lan

La única configuración que se debe hacer es:

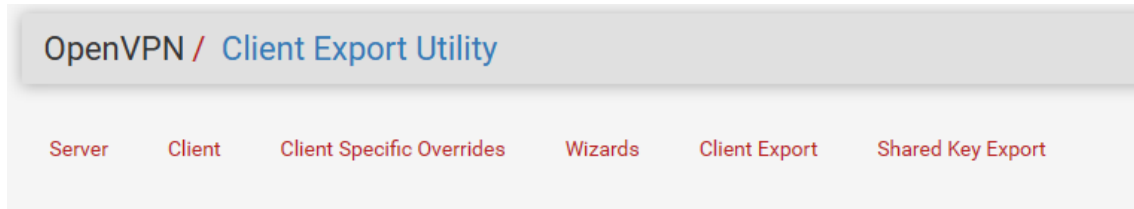
- Destino -> este cortafuegos "This firewall (self)".
- Destino de rangos de puerto -> 1194 fue el que se ha asignado para la VPN.
- Descripción -> VPN to Lan.

Se guardan y aplican los cambios.

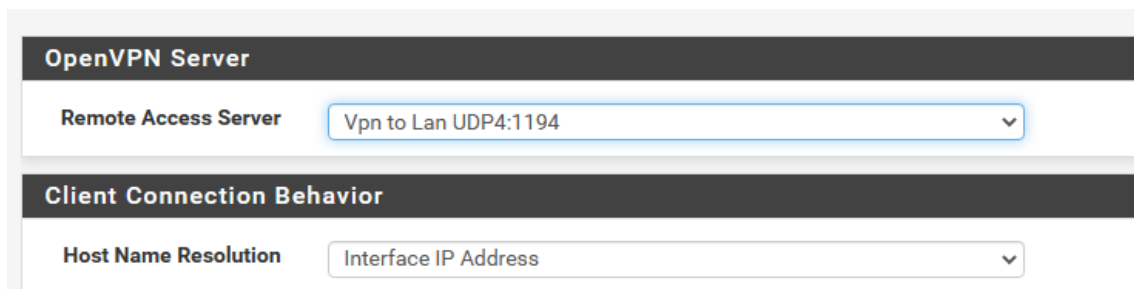


Exportar cliente VPN

Es la llave que cada usuario tiene para poder acceder a todo lo anteriormente creado. Se accede a través de VPN – OpenVPN:



Hay que usar la pestaña llamada Client Export.

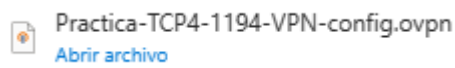


Host name resolution -> hay que seleccionar Interface IP Address que es la red WAN.



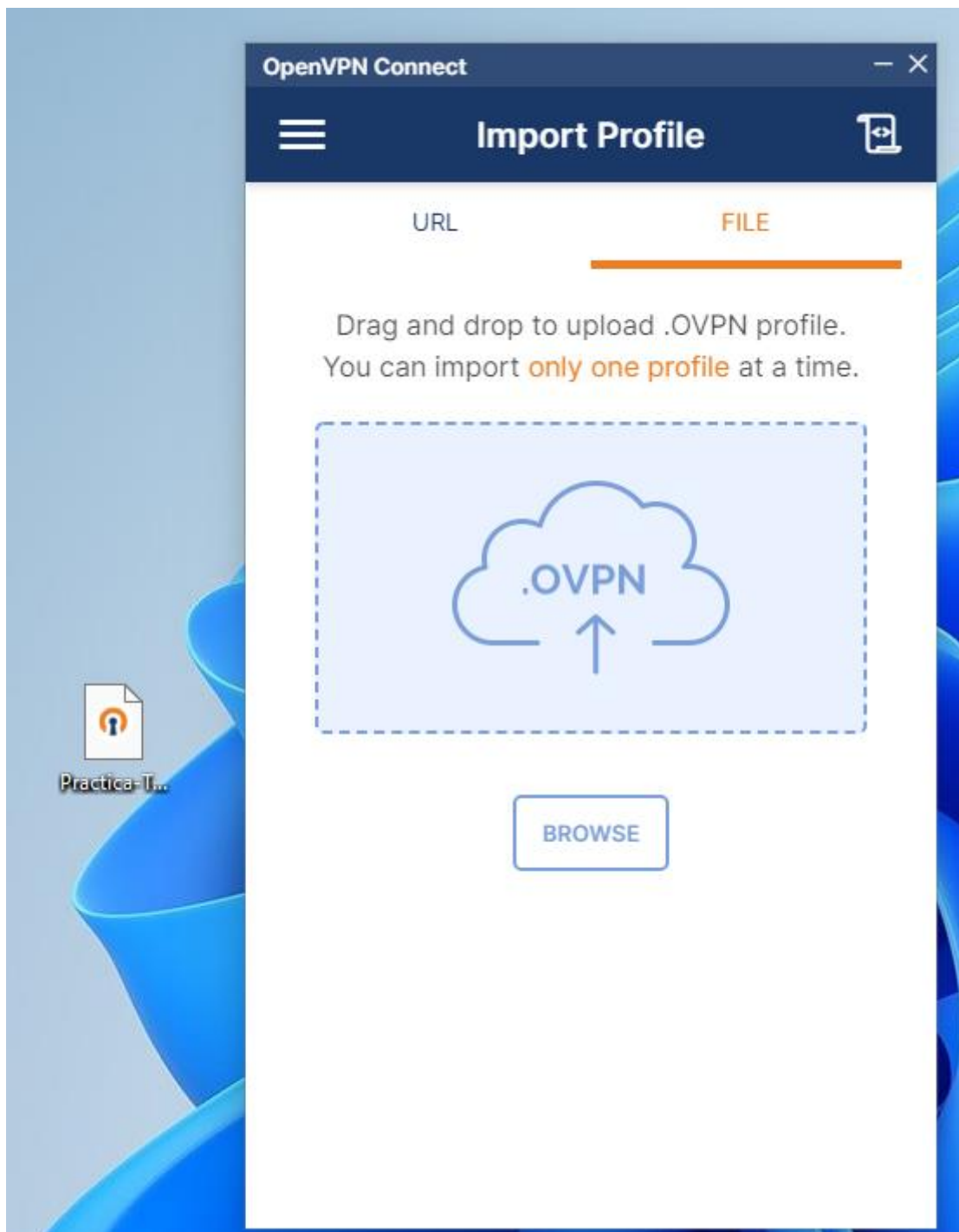
Aparecen los clientes dados de alta, en este caso VPN (creado como usuario, descrito su procedimiento anteriormente).

El último paso es descargar el certificado haciendo click en Most Clients.



Este es el archivo generado con extensión OVPN.

Para usarlo es necesario un cliente VPN, en este caso el elegido es VPN Connect.



Una vez descargado e instalado (instalación estándar). Debemos ir a la pestaña File y arrastrar o buscar el archivo que figura en la imagen de arriba.



Montar Honeypot

Inicialmente hay que usar un entorno basado en Linux, Kali es la distribución elegida. Para ello hay que montar la imagen descargada previamente.

Una vez montada la imagen se procede a actualizar las aplicaciones para preparar la instalación de Docker con el comando:

```
Sudo apt update
```

Acto seguido se procede a instalar Docker con el comando:

```
Sudo install docker.io
```

Hay que aceptar la instalación marcando S cuando se solicite.

A continuación se activa el servicio Docker con el comando:

```
systemctl enable Docker --now
```

```
(root@kali)-[~]
# systemctl enable docker --now
Synchronizing state of docker.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable docker
```

```
(root@kali)-[~]
# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS          NAMES
```

Con docker ps se puede comprobar si el servicio está funcionando, en este caso es afirmativo.

Una vez configurado y comprobado que funciona correctamente lanzamos un honeypot llamado cowrie.

```
(root@kali)-[~]
# docker run -p 2222:2222 cowrie/cowrie
Unable to find image 'cowrie/cowrie:latest' locally
latest: Pulling from cowrie/cowrie
fc251a6e7981: Pull complete
7be4d3667295: Pull complete
a1f1879bb7de: Pull complete
7eb7c5946a58: Pull complete
1817c8a12818: Pull complete
581833d6638a: Pull complete
277414dc2707: Pull complete
f8b7231d72a2: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:91d03265318fc1048f2e79534d6d161524eeae88a134f25d64b42a3b4a8554a3
Status: Downloaded newer image for cowrie/cowrie:latest
```



El comando a usar es:

```
Docker run -p 2222:2222 cowrie/cowrie
```

Con este comando se ejecuta el honeypot en el puerto 2222 y con el puerto interno 2222.

El servicio se pone en escucha y queda activo para recibir ataques/visitas.

```
(root@kali)-[~]
# ssh root@localhost -p 2222
The authenticity of host '[localhost]:2222 ([::1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:19PT0zENZbzVz0yYR9te7IQrbkRe7wWprMKu5GXP+E.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[localhost]:2222' (ED25519) to the list of known hosts.
root@localhost'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:~# timed out waiting for input: auto-logout
Connection to localhost closed by remote host.
Connection to localhost closed.
```

Emulamos un ataque a cowrie usando el puerto en el que se ha abierto 2222. Nos solicita acceder con un usuario y contraseña. Una vez insertados la comunicación termina.

En este momento el honeypot registra el acceso y muestra datos sensibles como la contraseña:

```
2023-04-09T15:48:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2023-04-09T15:48:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2023-04-09T15:48:27+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2023-04-09T15:48:35+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2023-04-09T15:48:35+0000 [HoneyPotSSHTransport,0,172.17.0.1] Could not read etc/userdb.txt, default database activated
2023-04-09T15:48:35+0000 [HoneyPotSSHTransport,0,172.17.0.1] login attempt [b'root'/b'123abc.1'] succeeded
2023-04-09T15:48:35+0000 [HoneyPotSSHTransport,0,172.17.0.1] Initialized emulated server as architecture: linux-x64-lsb
2023-04-09T15:48:35+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2023-04-09T15:48:35+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2023-04-09T15:48:35+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2023-04-09T15:48:35+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2023-04-09T15:48:35+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' req
```

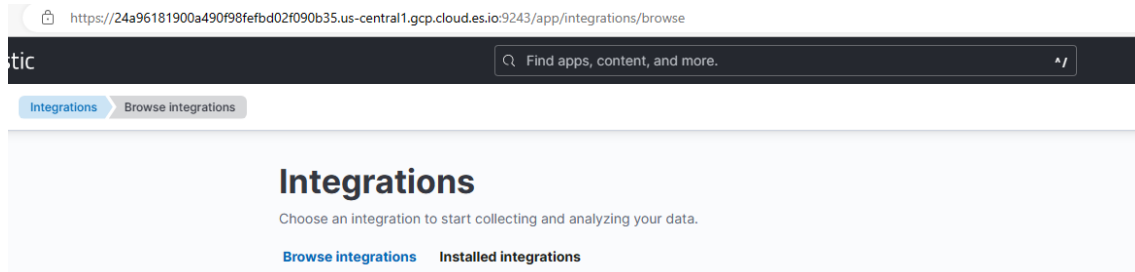


Implementación de Kibana con Windows

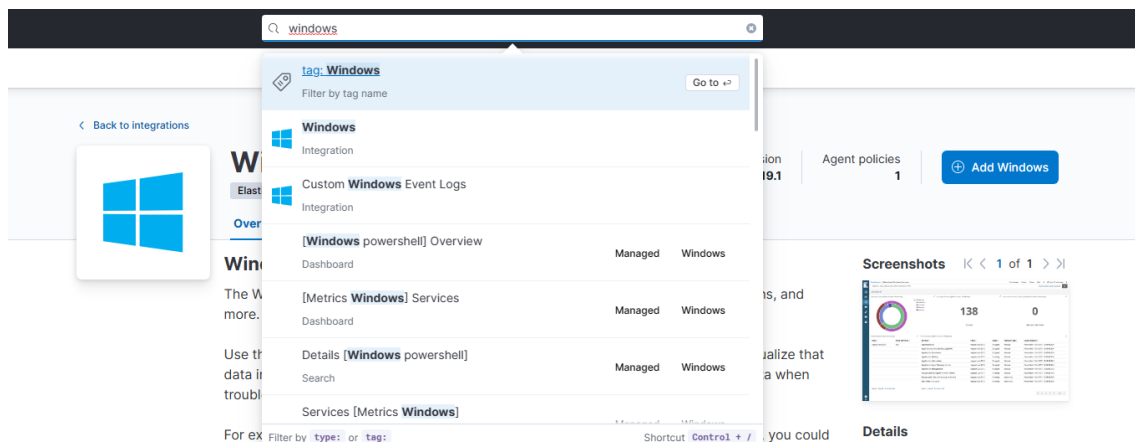
En primer lugar hay que acceder a la web: elastic.co.

Dentro de ella hay que iniciar sesión, en caso de no tener cuenta, crear una.

Una vez dentro, hay que buscar la opción de Windows dentro del siguiente cuadro:



Al escribir Windows, aparece:



Seleccionando la opción Windows “Integration” aparece la pantalla que hay de fondo. Dentro de ella hay que añadir Windows “Add Windows”.

La siguiente ventana nos facilita la instalación para diversas plataformas. En este caso se procede a instalar para Windows. Al pinchar en Windows aparece un comando que hay que ejecutar en la consola de comandos de Windows (se aconseja usar Powershell con privilegios de administrador), es el siguiente:

```
PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'
>> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.7.0-windows-x86_64.zip -OutFile elastic-agent-8.7.0-windows-x86_64.zip
>> Expand-Archive .\elastic-agent-8.7.0-windows-x86_64.zip -DestinationPath .
>> cd elastic-agent-8.7.0-windows-x86_64
```



```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.7.0-windows-x86_64.zip -OutFile elastic-agent-8.7.0-windows-x86_64.zip
Expand-Archive .\elastic-agent-8.7.0-windows-x86_64.zip -DestinationPath .
cd elastic-agent-8.7.0-windows-x86_64
.\elastic-agent.exe install --
url=https://265944c60f334d67af3f9568835d4dfc.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=ZzRHWFPvY0JEU0c3Y0VVMWtpYkM6TUJEZEpnSHBTMlc5ZI9CYk9HMXAyQQ==
```

Al finalizar dicha instalación, el tiempo puede variar según conexión y equipo usado, se verifica el equipo en el que se está usando así como en la versión de Windows.

El resultado es:

