

Proyecto de Diseño y Simulación de una Red Empresarial Segura con pfSense: Segmentación LAN, DMZ y Análisis de Seguridad

INDICE:

INDICE:.....	2
INTRODUCCIÓN:.....	3
Paso 0º Creación del entorno.....	5
Paso 0.2 Creación redes virtuales.....	5
0.3 Creación de vm.....	6
0.3.1.2 Configuración de interfaces.....	13
0.3.1.2. Acceso a internet a la LAN desde Pfsense.....	15
0.3.2 Windows Server y Active Directory.....	16
0.3.2.1 Promover a controlador de dominio.....	18
0.3.2.1.2 Crear servidor DHCP.....	21
0.3.2.2 Unir un cliente Windows al Dominio.....	26
0.4 Máquina Ubuntu.....	29
Paso 1º Aplicación web corporativa.....	35
Paso 1.1 Configuración de LDAP.....	39
Paso 2.1 Uso de Kali Linux.....	41
Paso 2.2 Proceso de detección de servicios.....	41
Paso 2.2.1 Escaneo de red.....	42
Paso 2.3 Ejemplo de servicio vulnerable.....	45
CONCLUSIÓN,.....	47

INTRODUCCIÓN:

En este proyecto se diseña y simula una red empresarial segura basada en una arquitectura de múltiples zonas, utilizando pfSense como cortafuegos principal. El objetivo es crear un entorno virtual que represente una infraestructura de red corporativa segmentada, con separación entre zonas de confianza y zonas expuestas, y aplicar medidas de seguridad reales.

El entorno estará compuesto por los siguientes elementos clave:

- pfSense como firewall perimetral, encargado de controlar el tráfico entre las distintas redes.
- Una zona LAN, que representa la red interna de la empresa, donde estarán ubicados los equipos de usuario y servidores de administración (por ejemplo, un controlador de dominio o un servidor interno).
- Una zona DMZ (Zona Desmilitarizada), donde se desplegarán servicios públicos accesibles desde el exterior, como un servidor web o de aplicaciones.
- Una red WAN simulada, para representar el acceso a Internet desde la empresa y permitir simular ataques externos.
- Estaciones de trabajo, herramientas de administración y auditoría, incluyendo Kali Linux como sistema para pruebas de penetración internas y externas.

Durante el desarrollo del proyecto se llevarán a cabo las siguientes actividades:

- Diseño de la topología de red virtual con VirtualBox (o similar), asignando correctamente las interfaces y redes.
- Instalación y configuración de pfSense, segmentando el tráfico entre LAN, DMZ y WAN, y aplicando reglas de firewall específicas.
- Despliegue de servicios en la DMZ, como un servidor web o una aplicación corporativa.
- Pruebas de conectividad y seguridad, tanto desde dentro de la red (LAN) como desde el exterior (WAN), simulando posibles vectores de ataque.
- Análisis de tráfico y eventos, utilizando herramientas como Wireshark, Snort o Security Onion, para observar el comportamiento de la red ante intentos de acceso o intrusiones.

Este proyecto tiene como finalidad comprender y aplicar los principios de segmentación de red, control de acceso y defensa perimetral, elementos esenciales en cualquier infraestructura empresarial segura.

Cantidad de máquinas a usar.

Nº	Nombre de la Máquina	Sistema Operativo	Red Asignada	IP Estática	Función Principal
1	pfSense Firewall	pfSense CE	WAN / LAN / DMZ	WAN: 192.168.1.2 LAN: 192.168.10.1 DMZ: 192.168.20.1	Firewall, NAT, segmentación, reglas de acceso
2	Servidor Windows	Windows Server 2019/22	LAN	192.168.10.10	Controlador de dominio / servidor interno
3	Cliente Windows	Windows 10 / 11	LAN	192.168.10.20	Estación de trabajo del usuario
4	Servidor Web (DMZ)	Ubuntu Server / Debian	DMZ	192.168.20.10	Aplicación web / servidor público
5	Kali Linux	Kali Linux	WAN / LAN / DMZ	Dinámica o según test	Auditorías de seguridad, escaneo, pentesting
6	Security Onion (opcional)	Security Onion	DMZ o LAN	Según configuración	Monitorización de red, análisis de eventos

Paso 0º Creación del entorno.

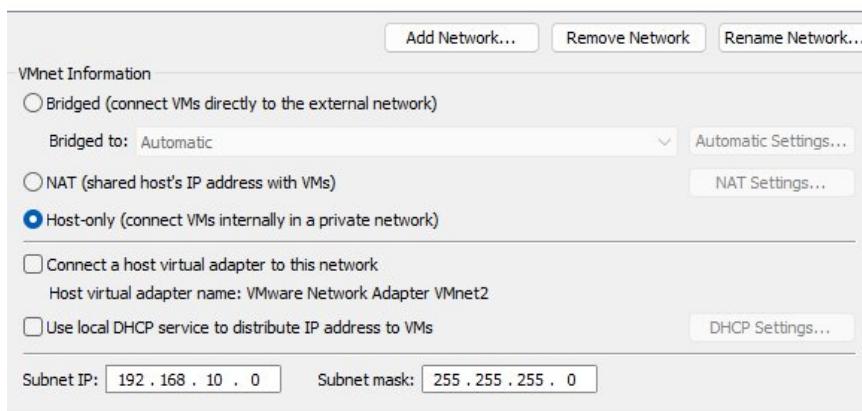
En este proyecto, se ha optado el usar Vmware Pro.

Paso 0.2 Creación redes virtuales.

Se definen varias redes internas para simular los diferentes segmentos de la topología.

Red	Nombre en Vmware	Tipo de Red	Rango de IP	Uso Principal
WAN	Red-WAN	NAT / Interna	192.168.1.0/24	Acceso a Internet simulado
LAN	Red-LAN	Interna	192.168.10.0/24	Red interna empresarial
DMZ	Red-DMZ	Interna	192.168.20.0/24	Zona desmilitarizada (servidores públicos)

Para ello, nos vamos al editor de redes de Vmware.....



Y simplemente la creamos.

Teniendo en cuenta esos parámetros.

0.3 Creación de vm.

Las máquinas virtuales se configurarán para según qué rol vayan a tener en nuestro laboratorio, asignándoles u ip y redes adecuadas.

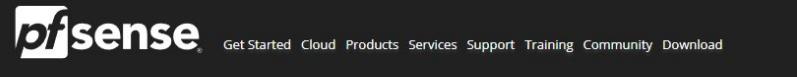
0.3.1 PfSense.

Pfsense, es un firewall open source que nos permite tener un cortafuegos/router para controlar el tráfico qué entra y sale de nuestra infraestructura.

Nos vamos a la página de pfsense....

The screenshot shows the pfSense website homepage. At the top, there is a navigation bar with links: Get Started, Cloud, Products, Services, Support, Training, Community, and Download. The main title "OPEN SOURCE SECURITY" is prominently displayed in the center. Below it, a subtitle reads: "Secure networks start here.™ With thousands of enterprises using pfSense® software, it is rapidly becoming the world's most trusted open source network security solution." A blue "Get Started Now" button is located below the subtitle. The background features a dark blue polygonal geometric pattern. On the right side of the page, there is a section titled "Securely Connect to the Cloud VIRTUAL APPLIANCES". It includes a description of Netgate® virtual appliances and a blue cloud icon with a network graph inside. The text in this section is partially cut off at the bottom.

Damos en download....



Download

Home | Download

Latest Stable Version

pfSense Plus & pfSense CE software downloads are available for installation via the Netgate Installer. Click the "Download" link below to redirect to our online store and download the Netgate Installer package. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#).

[RELEASE NOTES](#) [SOURCE CODE](#)

Version: 2.7.2

Supported by 

[DOWNLOAD](#)

Es gratuito...



The screenshot shows the Netgate website's product page for the Netgate Installer. At the top, there are links for Sign in or Create an Account, a search bar, and a shopping cart icon. Below the header, there are navigation links for ALL PRODUCTS, PFSENSE+ PRODUCTS, TNSR PRODUCTS, ACCESSORIES, SUPPORT, and MORE. The main content area displays the Netgate Installer product, featuring the Netgate logo, a price of \$0.00, and a note that shipping is calculated at checkout. It also mentions that pay over time is available for orders over 35.00\$. There are fields for selecting the image type and quantity, and buttons for ADD TO CART and FIND A PARTNER.

Por lo menos la versión qué usaremos....claro.

NETGATE INSTALLER

\$0⁰⁰

Shipping calculated at checkout.

Pay over time for orders over 35,00 \$ with [Shop Pay](#) Learn more
Customers using Shop Pay Installments might experience a 1-2 day delay in order processing.

Installation Image

AMD64 ISO IPMI/Virtual Machines

Quantity

- 1 +

ADD TO CART FIND A PARTNER

ADD to cart...y luego tendremos qué crearnos una cuenta y luego ya...se nos descarga la iso.
Checkout.....

Payment

All transactions are secure and encrypted.

Your order is free. No payment is required.

P.O. Number (optional)

Order Note (optional)

Aquí vemos qué es gratis....hay otras versiones ya a nivel empresarial qué si..hay que pagar.

Netgate Installer - AMD64 ISO IPMI/Virtual Machines

[netgate-installer-amd64.iso.gz \(302.11 MB\)](#)

Download Now

You will also receive an email with download links for your digital purchases.

Y descargamos.....

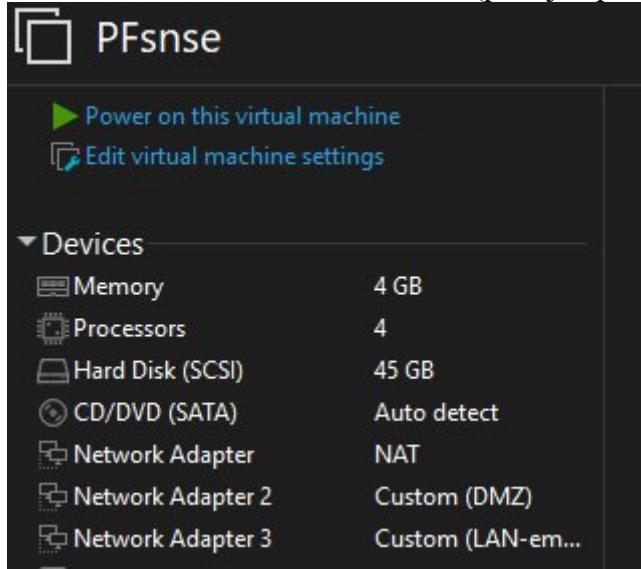
Una vez obtenida y descomprimida la carpeta .zip, tendremos la ISO.

La máquina virtual de pfSense se ajustará a los recursos de hardware disponibles, teniendo en cuenta que se asignarán al menos 2 GB de RAM y 20 GB de espacio en disco. En cuanto a las interfaces de red, se utilizarán tres adaptadores virtuales:

WAN (NAT): Esta interfaz se conectará a la red externa, simulando el acceso a Internet.

LAN: Esta interfaz estará configurada en la red interna de la empresa, proporcionando conectividad a las máquinas dentro de la infraestructura.

DMZ: Esta interfaz estará configurada en la zona desmilitarizada (DMZ), donde se alojarán los servidores accesibles desde Internet (por ejemplo, servidores web).



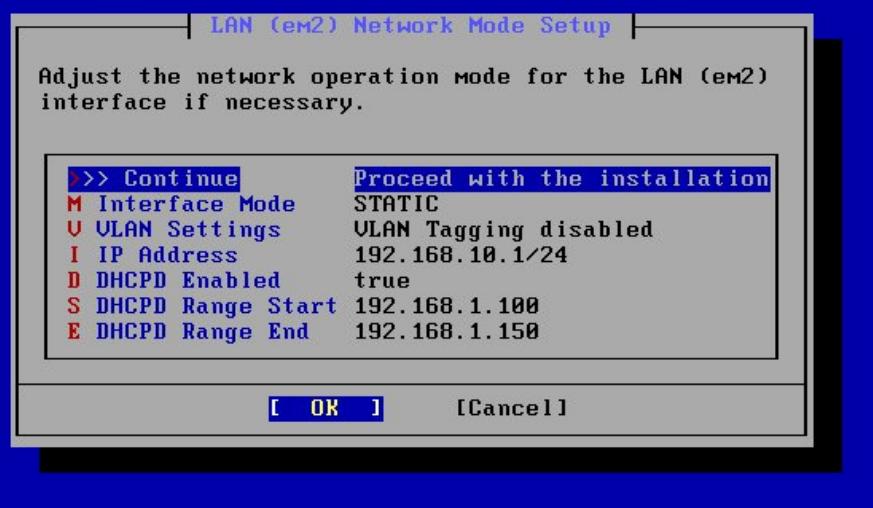
Algo así...

Arrancamos con la iso....

```
Home × PFsnse ×
SRAT: Ignoring local APIC ID 125 (too high)
SRAT: Ignoring local APIC ID 126 (too high)
SRAT: Ignoring local APIC ID 127 (too high)
SRAT: Ignoring memory at addr 0x1400000000
JT(vga): text 80x25
CPU: AMD Ryzen 7 5700X 8-Core Processor (3399.99-MHz K8-class CPU)
  Origin="AuthenticAMD" Id=0xa20f12 Family=0x19 Model=0x21 Stepping=2
  Features=0x1783fbff<FPU, VME, DE, PSE, TSC, MSR, PAE, MCE, CX8, APIC, SEP, MTRR, PGE, MCA,
  MOV, PAT, PSE36, MMX, FXSR, SSE, SSE2, HTT>
  Features2=0xfef83203<SSE3, PCLMULQDQ, SSSE3, FMA, CX16, SSE4.1, SSE4.2, x2APIC, MOVBE,
  POPCNT, AESNI, XSAVE, OSXSAVE, AVX, F16C, RDRand, HU>
  AMD Features=0xe2e500800<SYSCALL, NX, MMX+, FFXSR, Page1GB, RDTSCP, LM>
  AMD Features2=0x4003fb<LAHF, CMP, ExtAPIC, CR8, ABM, SSE4A, MAS, Prefetch, OSUW, Topology>
  Structured Extended Features=0x219c07a9<FGSBASE, BMI1, AVX2, SMEP, BMI2, ERMS, INUD, RDSEED, ADX, SMAP, CLFLUSHOPT, CLWB, SHA>
  Structured Extended Features2=0x40069c<UMIP, PKU, OSPRE, VAES, VPCLMULQDQ, RDPID>
  Structured Extended Features3=0x10<FSRM>
  XSAVE Features=0xf<XSAVEOPT, XSAVEC, XINUSE, XSAVES>
  AMD Extended Feature Extensions ID EBX=0x110c5201<CLZERO, WBNOINVUD, IBPB, IBRS, PEFER_IBRS, SAMEMODE_IBRS, SSBD, PSFD>
  TSC: P-state invariant
Hypervisor: Origin = "VMwareVMware"
real memory = 4294967296 (4096 MB)
```

En primer lugar, endremos que asignar según interfaz, a cómo acua, la primera será WAN, y luego la LAN, la em2.

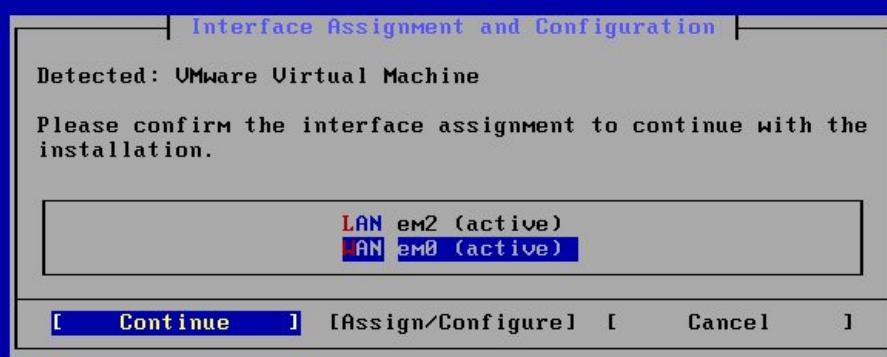
Netgate Installer - v1.0-RC



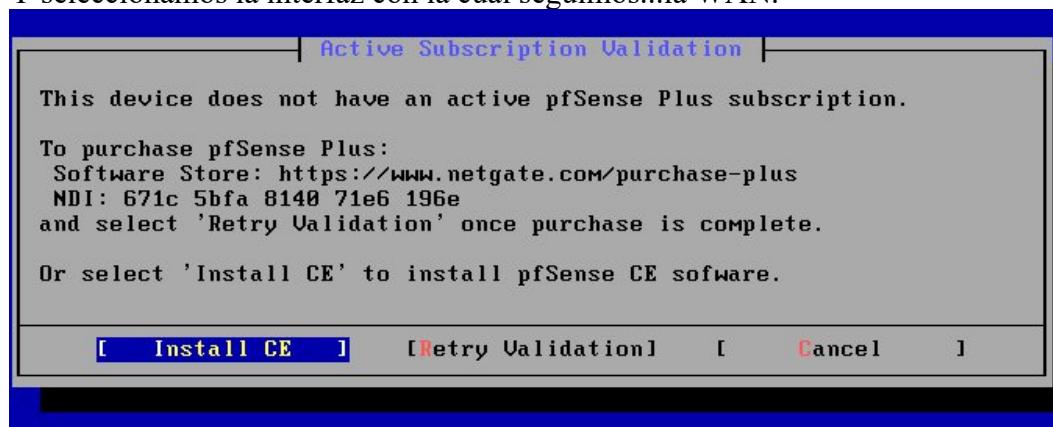
Ojo: Hay que poner la ip address.

El dhcp hay que poner en false.

Netgate Installer - v1.0-RC



Y seleccionamos la interfaz con la cuál seguimos...la WAN.



Le damos en intall CE.



Insalamos esa versión....

```
----- Installation Details -----  
pkg-static: Warning: Major OS version upgrade detected.  Running "pkg boot  
Updating pfSense-core repository catalogue...  
Fetching meta.conf: . done  
Fetching packagesite.pkg: . done  
Processing entries: . done  
pfSense-core repository update completed. 4 packages processed.  
Updating pfSense repository catalogue...  
Fetching meta.conf: . done  
Fetching data.pkg: ..... done  
Processing entries: ..... done  
pfSense repository update completed. 550 packages processed.  
All repositories are up to date.  
The following 1 package(s) will be affected (of 0 checked):  
  
New packages to be INSTALLED:  
    pkg: 1.20.8_3 [pfSense]  
  
Number of packages to be installed: 1  
  
The process will require 39 MiB more space.  
10 MiB to be downloaded.
```

Esperamos.....

Y una vez termine....se iniciará.

```

Home X | PFsense X

Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 671c5bfa814071e6196e

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

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.239.171/24
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: ■

```

Ya lo tendríamos listo.

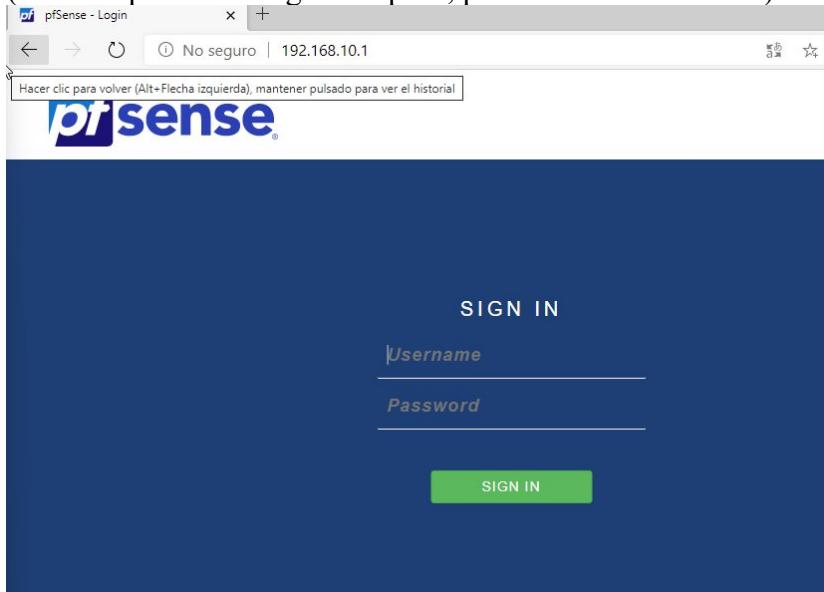
Por ultimo asignaremos la interaz a su tipo...

```

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.239.171/24
LAN (lan)      -> em2          -> v4: 192.168.10.1/24
PT1 (opt1)     -> em1          ->

```

(la red la puse en el siguiente paso, por ello la conectividad).



Accedemos con admin pfSense.

The screenshot shows the pfSense Setup Wizard interface. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title "Wizard / pfSense Setup /" is displayed. The main content area is titled "pfSense Setup" and contains the following text:

Welcome to pfSense® software!
This wizard will provide guidance through the initial configuration of pfSense.
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
pfSense® software is developed and maintained by Netgate®

Learn more

>> Next

Below this, a section titled "General Information" is shown. It says: "On this screen the general pfSense parameters will be set." The configuration fields are:

Hostname: pfSense
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain: empresa.net
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will r network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are saf

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query r servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver enable DNS Query Forwarding after completing the wizard.

Primary DNS Server: 8.8.8.8

Secondary DNS Server: [empty field]

Override DNS: Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

Aquí doy ya el nombre de lo qué será nuestro control domain....empresa.net.

0.3.1.2 Configuración de interfaces.

En ese paso, vamos a configurar las interfaces.

COMMUNITY EDITION

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

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

SelectedType: DHCP

General configuration

MAC Address:

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx or leave blank.

MTU:

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 for connection types will be assumed.

MSS:

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above (in header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for connection types will be assumed.

RFC1918 Networks

Block RFC1918 Block private networks from entering via WAN

Private Networks When set, this option blocks traffic from IP addresses that are reserved for private networks (e.g. 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be selected if your 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). Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear in any packets received.

» Next

Luego, pondremos una nueva contraseña, deberá ser fuerte.

pfSense COMMUNITY EDITION

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

Status / Dashboard

System Information

Name	pfSense.empresa.net
User	admin@192.168.10.54 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 671c5bfa814071e6196e
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Mon Mar 4 20:53:00 CET 2024 FreeBSD 14.0-CURRENT

The system is on the latest version.
Version information updated at Mon May 12 16:08:06 CEST 2025

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

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

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

0.3.1.2. Acceso a internet a la LAN desde Pfsense.

En este apartado, conseguiremos qué pfsense de internet a nuestro windows server. En cuanto a NAT, pfsense tiene activado el NAT automatic, qué por defecto funciona. Nosotros nos preocupamos de poner la regla en la parte de LAN.

The screenshot shows the pfSense Firewall Rules LAN configuration page. The URL in the browser is 192.168.10.1/firewall_rules.php?if=lan. The page displays a list of rules under the 'LAN' tab. There are three rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 3/1.14 MiB	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	
✓ 0/5 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Below the table are several action buttons: Add, Delete, Toggle, Copy, Save, and Separ.

Creo una regla...

A modal dialog box is shown for creating a new rule. The configuration is as follows:

✓ 0/0 B	IPv4 *	LAN subnets	*	*	*	*	none	Internet
---------	--------	-------------	---	---	---	---	------	----------

At the bottom of the dialog are several action buttons: Add, Delete, Toggle, Copy, and Save.

Y ahora nos vamos a DNS resolver, ya que tenemos internet, pero no..resoluciona las peticiones UDP.

Para ello.....nos vamos a Service-DNS-Resolver....

The port used for responding to DNS queries. It should normally be left blank unless another service uses TCP/UDP port 53.

Enable SSL/TLS Service Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients that support DNS over TLS. Activating this option disables automatic interface response routing behavior with specific interface bindings.

SSL/TLS Certificate GUI default (682200bbf15f2)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port 853
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless assigned to TCP/UDP port 853.

Network Interfaces WAN, LAN, WAN IPv6 Link-Local, LAN IPv6 Link-Local, Localhost

Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The resolver responds to queries on every available IPv4 and IPv6 address.

Outgoing Network Interfaces All, WAN, LAN, WAN IPv6 Link-Local, LAN IPv6 Link-Local

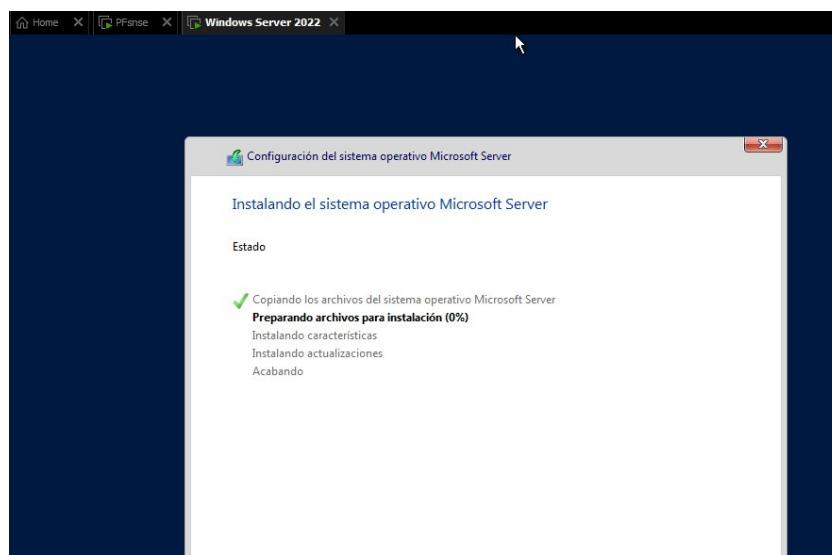
Dejamos seleccionado tal cual viene en la documentación
Y importante....activar el Query Fowarding.

DNS Query Forwarding Enable Forwarding Mode
If this option is set, DNS queries will be forwarded to those obtained via dynamic interfaces.

Y ya tendríamos conectividad.

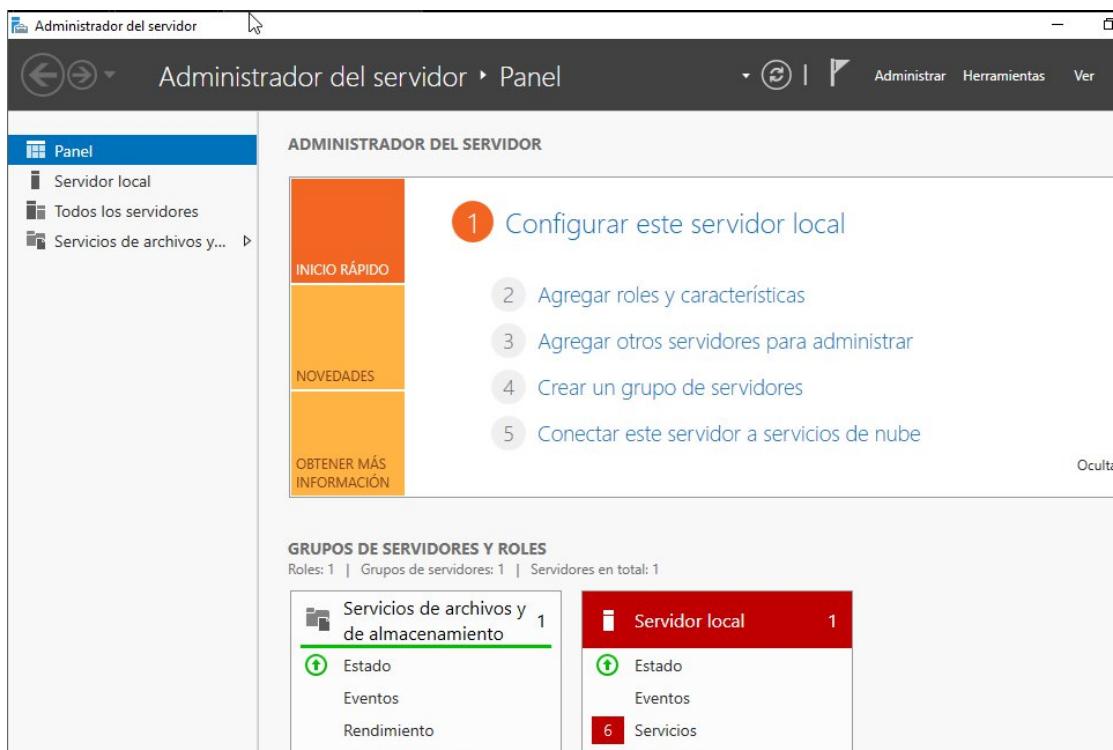
0.3.2 Windows Server y Active Directory.

En este apartado, vamos a crear la máquina virtual de server de Windows, qué actuará de controlador de dominio.

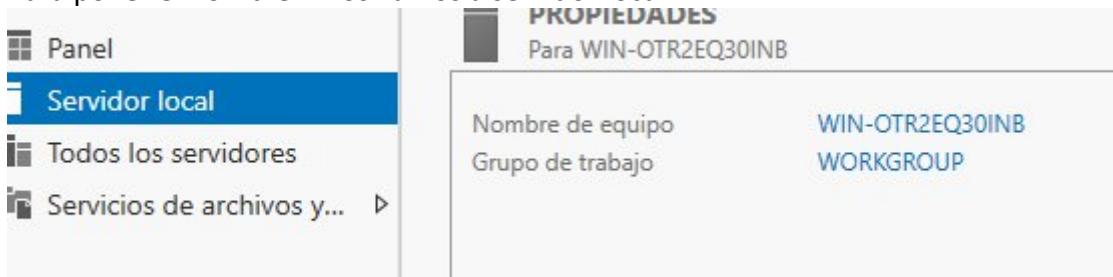


La instalación es trivial.

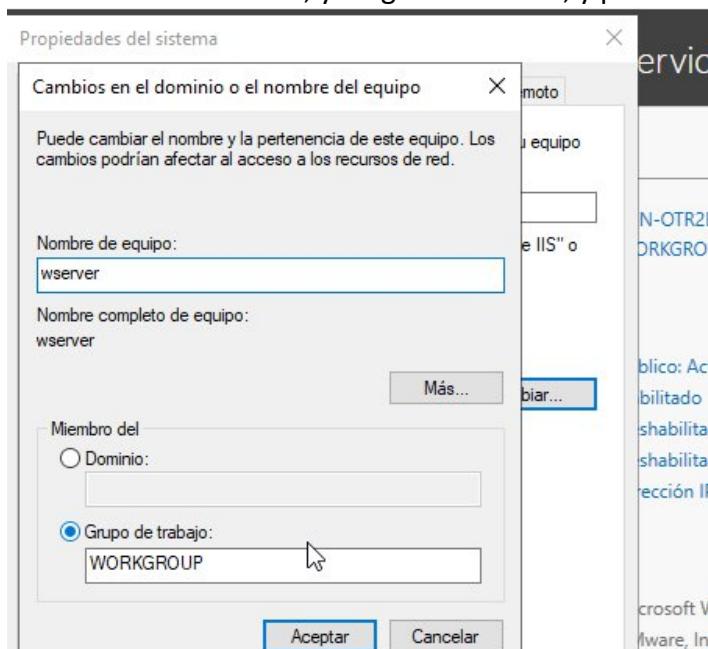
El siguiente paso es poner la ip estatica, cambiar el nombre, y instalar el rol de AD.



Para poner el nombre....nos vamos a servidor local...



Clicamos en el nombre, y luego en nombre, y ponemos el nombre...



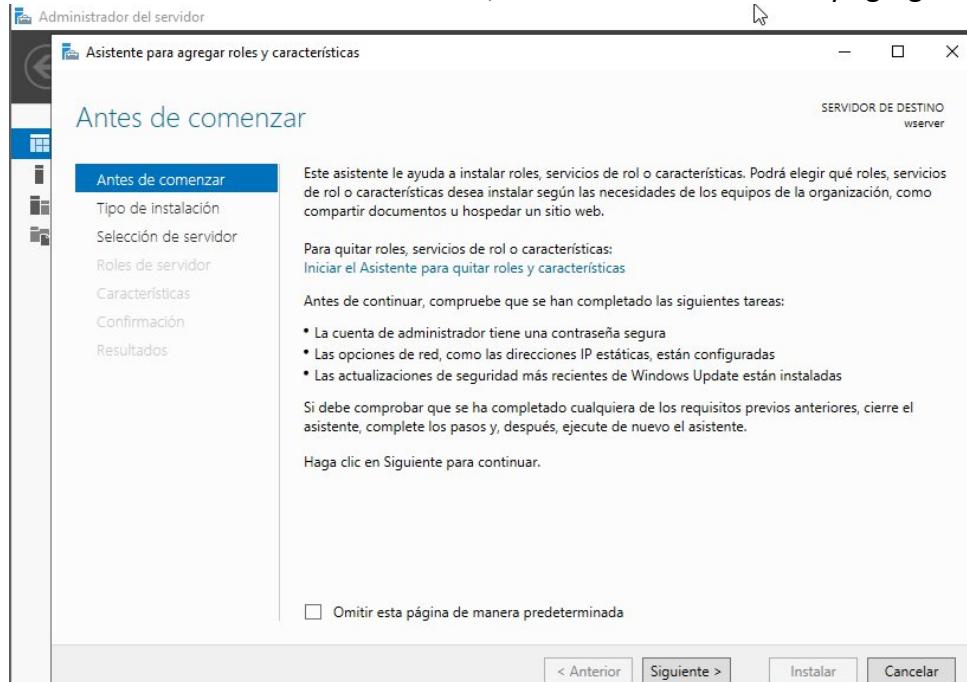
Nos pedirá reiniciar....le damos en reiniciar...

Después de iniciar.....le cambiamos la ip a estática....

0.3.2.1 Promover a controlador de dominio.



Para crear el controlador de dominio, nos vamos a administrar y agregar roles..



Seleccionamos el rol de Dominio..

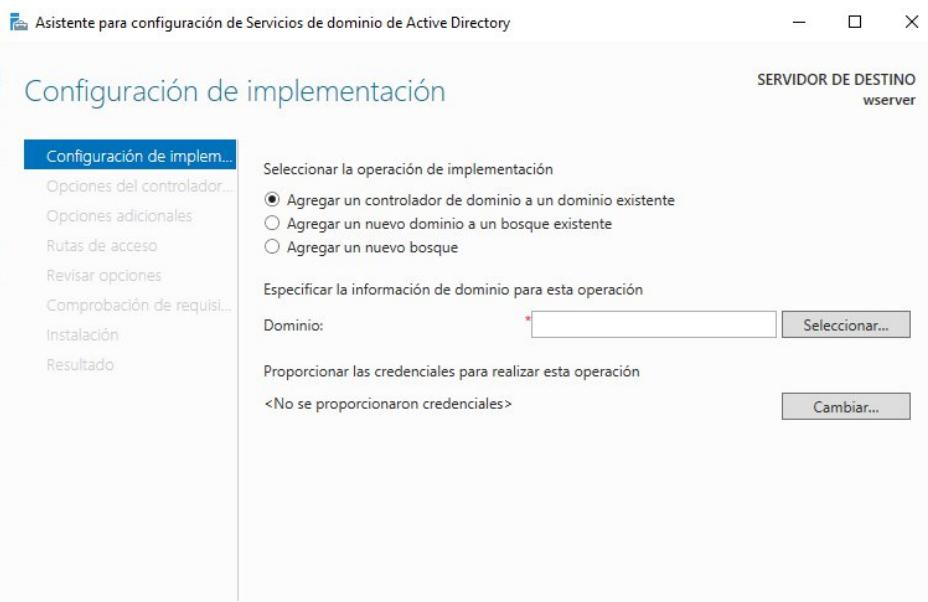
Seleccionar roles de servidor

The screenshot shows the 'Select Server Roles' step of the Server Configuration Wizard. On the left, a sidebar lists steps: 'Antes de comenzar', 'Tipo de instalación', 'Selección de servidor', 'Roles de servidor' (which is selected), 'Características', 'AD DS', 'Servidor DHCP', 'Servidor DNS', 'Confirmación', and 'Resultados'. The main pane title is 'Seleccione uno o varios roles para instalarlos en el servidor sele...'. It has a 'Roles' section with a list of checkboxes. Several checkboxes are checked: 'Servicios de archivos y almacenamiento (1 de 12)', 'Servicios de dominio de Active Directory', 'Servidor DHCP', 'Servidor DNS', and 'Servidor web (IIS)'.

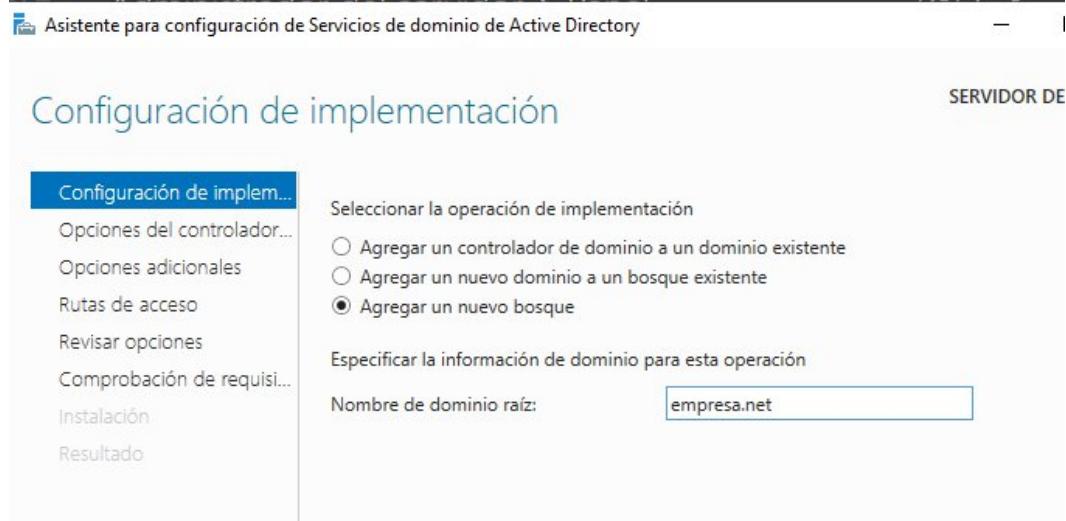
También seleccionaré DHCP y DNS, ya que nos servirá para los clientes de la LAN.
Luego siguiente, y siguiente....e instalar....

The screenshot shows the 'Progresso de la instalación' (Installation Progress) step of the Server Configuration Wizard. The sidebar shows steps: 'Antes de comenzar', 'Tipo de instalación', 'Selección de servidor', 'Roles de servidor' (selected), 'Características', 'AD DS', 'Servidor DHCP', 'Servidor DNS', 'Confirmación', and 'Resultados'. The main pane title is 'Ver progreso de la instalación'. It shows a progress bar for 'Instalación de característica' which is nearly complete. A note says 'Requiere configuración. Instalación correcta en wserver.' Below it, a list of installed features includes 'Servicios de dominio de Active Directory', 'Servidor DHCP', 'Administración de directivas de grupo', and 'Herramientas de administración remota del servidor'. At the bottom, there's a note: 'Este asistente se puede cerrar sin interrumpir la ejecución de las tareas. Para ver el progreso de la tarea o volver a abrir esta página, haga clic en Notificaciones en la barra de comandos y en Detalles de la tarea.' Buttons at the bottom include '< Anterior', 'Siguiente >', 'Cerrar', and 'Cancelar'.

Luego nos vamos a la banderita y le damos al configurador de dominio...

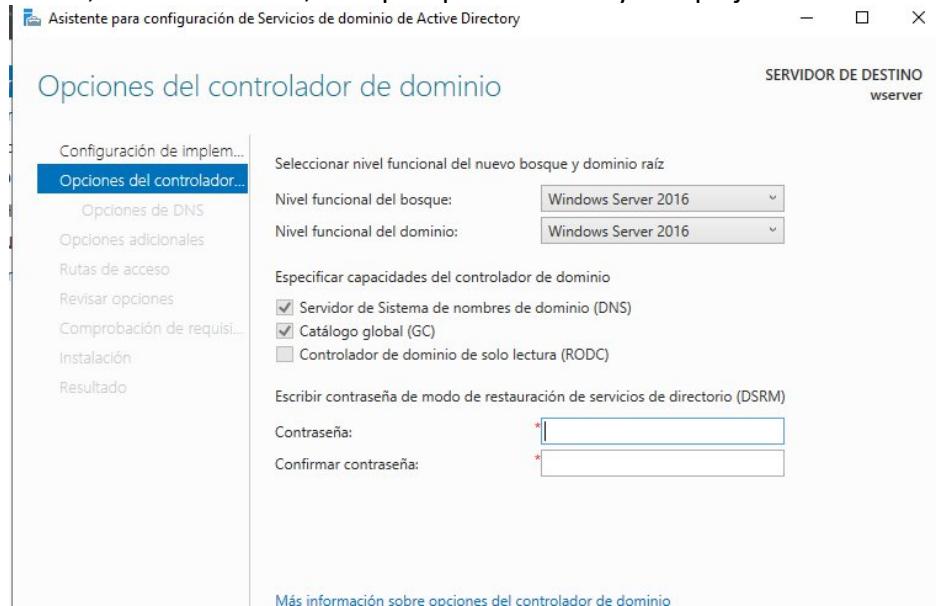


Agregar nuevo bosque en nuestro caso...

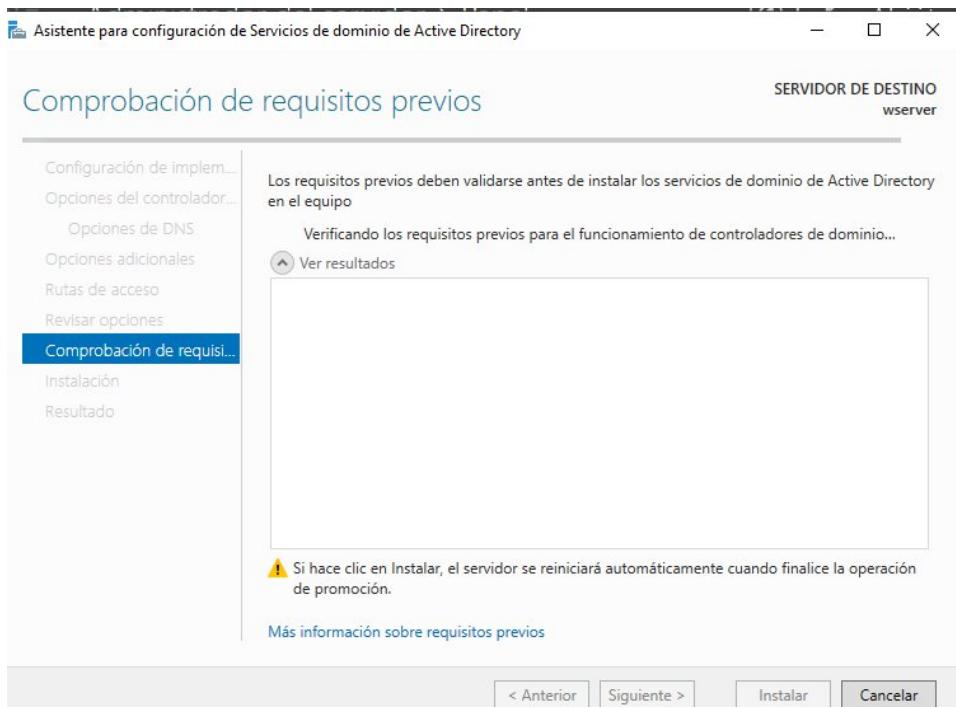


Ponemos un nombre....

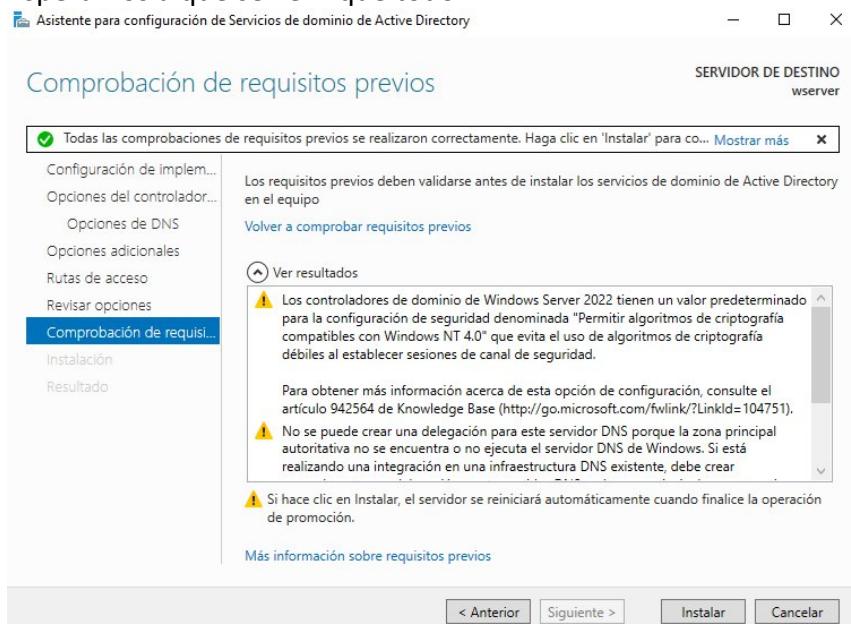
Ahora, una contraseña, siempre que sea difícil y compleja.



En delegación DNS, nada...siguiente....



Esperamos a que se verifique todo....



Y damos en instalar....

Una vez termine, se reiniciará. Y con ello...ya lo tendríamos listo.

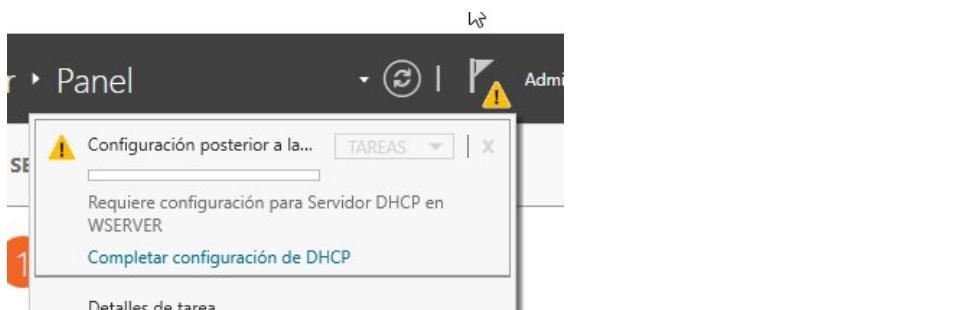
0.3.2.1.2 Crear servidor DHCP.

Cómo bien sabemos, es necesario un servidor DHCP, para que se le asigne automáticamente todos los parámetros a los clientes.

or del servidor



Le damos en la banderita....



Vamos a autorizar el servidor...

Asistente posterior a la instalación de DHCP

Descripción

Se realizarán los siguientes pasos para completar la configuración del servidor DHCP en el equipo de destino:

Cree los siguientes grupos de seguridad para la delegación de la administración de servidores DHCP.

- Administradores de DHCP
- Usuarios de DHCP

Autorizar servidor DHCP en el equipo de destino (si está unido al dominio).

Siguiente...

Usaremos la de administrador, aunque es posible con otro usuario.

Autorización

Descripción

Autorización

Especifique las credenciales que se usarán para autorizar este servidor DHCP en AD DS.

Usar las credenciales del siguiente usuario
Nombre de usuario:

Usar credenciales alternativas
Nombre de usuario:

Omitir autorización de AD

Ya lo tenemos...

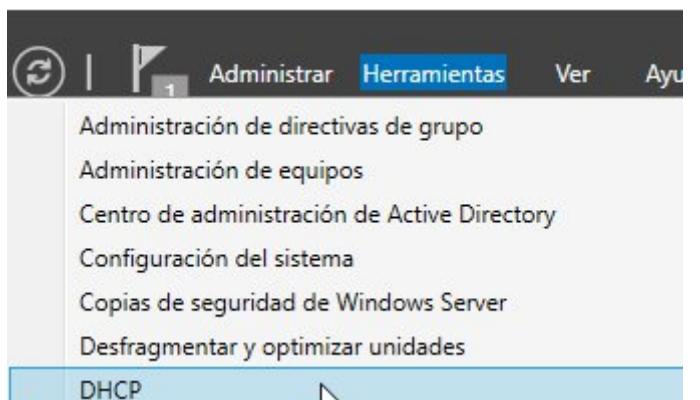
Asistente posterior a la instalación de DHCP

Resumen

A continuación se indica el estado de los pasos de configuración posteriores a la instalación:

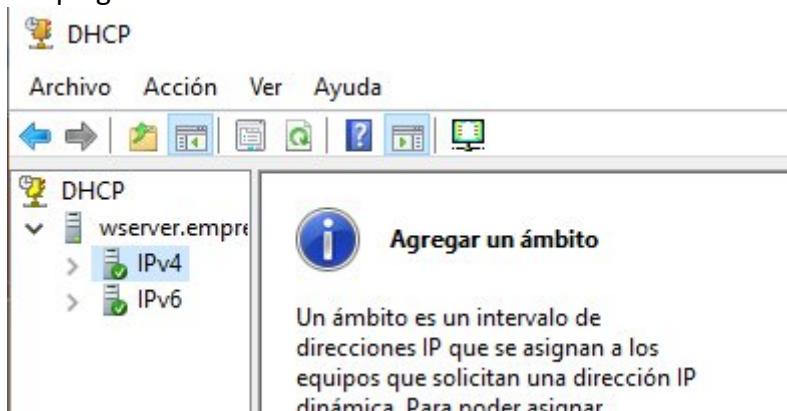
Creando grupos de seguridad	Listo
Reinicie el servicio de servidor DHCP en el equipo de destino para que los grupos de seguridad sean efectivos.		
Autorizando el servidor DHCP	Listo

Ahora, nos vamos a herramientas....

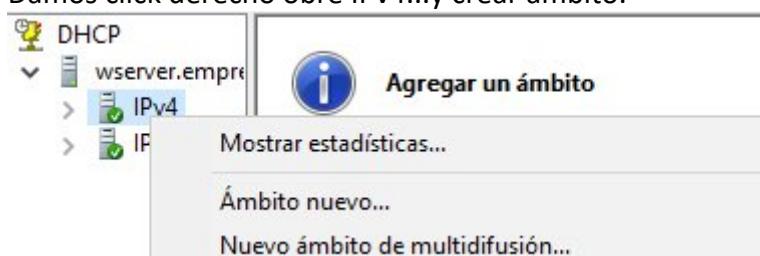


DHCP.....

Desplegamos...



Damos click derecho sobre IPv4...y crear ámbito.



Asistente para ámbito nuevo



Y empezamos a crearlo....

Ponemos un nombre al ámbito.

Asistente para ámbito nuevo

Nombre de ámbito

Debe escribir un nombre identificativo para el ámbito. También puede proporcionar una descripción.

Escriba un nombre y una descripción para este ámbito. Esta información le ayuda a identificar rápidamente cómo se usa el ámbito y su red.

Nombre:

Descripción:

Ponemos un rango de ip...

Asistente para ámbito nuevo

Intervalo de direcciones IP

Para definir el intervalo de direcciones del ámbito debe identificar un conjunto de direcciones IP consecutivas.

Opciones de configuración del servidor DHCP

Escriba el intervalo de direcciones que distribuye el ámbito.

Dirección IP inicial:

Dirección IP final:

Opciones de configuración que se propagan al cliente DHCP

Longitud:

Máscara de subred:

Le damos a siguiente...saltamos tanto el agregar retrasos, y la duración de concesión, la dejamos en 8 dias.

Nos aparecerá si queremos configurar más cosas...le damos a sí...

Asistente para ámbito nuevo

Enrutador (puerta de enlace predeterminada)

Puede especificar los enrutadores, o puertas de enlace predeterminadas, que se distribuirán en el ámbito.



Para agregar una dirección IP para un enrutador usado por clientes, escriba la dirección.

Dirección IP:

.	.	.
<input type="button" value="Agregar"/>		
<input type="button" value="Quitar"/>		
<input type="button" value="Arriba"/>		
<input type="button" value="Abajo"/>		

Ponemos la ip de pfsense...

Asistente para ámbito nuevo

Enrutador (puerta de enlace predeterminada)

Puede especificar los enrutadores, o puertas de enlace que distribuirán en el ámbito.

Para agregar una dirección IP para un enrutador usa

Dirección IP:

Agregar

192.168.10.1

Quitar

Dejamos tal cuál el DNS...

Asistente para ámbito nuevo

Nombre de dominio y servidores DNS

El Sistema de nombres de dominio (DNS) asigna y traduce los nombres de dominio que utilizan los clientes de la red.



Puede especificar el dominio primario que desea que los equipos clientes de su red usen para la resolución de nombres DNS.

Dominio primario:

Para configurar clientes de ámbito para usar servidores DNS en su red, escriba las direcciones IP para esos servidores.

Nombre de servidor:

Resolver

Dirección IP:

< Atrás Siguiente > Cancelar

Servidores WINS, nada....y le damos a activar ámbito y siguiente....

Asistente para ámbito nuevo

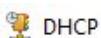
Activar ámbito

Los clientes pueden obtener concesiones de direcciones activado.

¿Desea activar este ámbito ahora?

- Activar este ámbito ahora
 Activar este ámbito más tarde

Ya lo tenemos creado y listo....

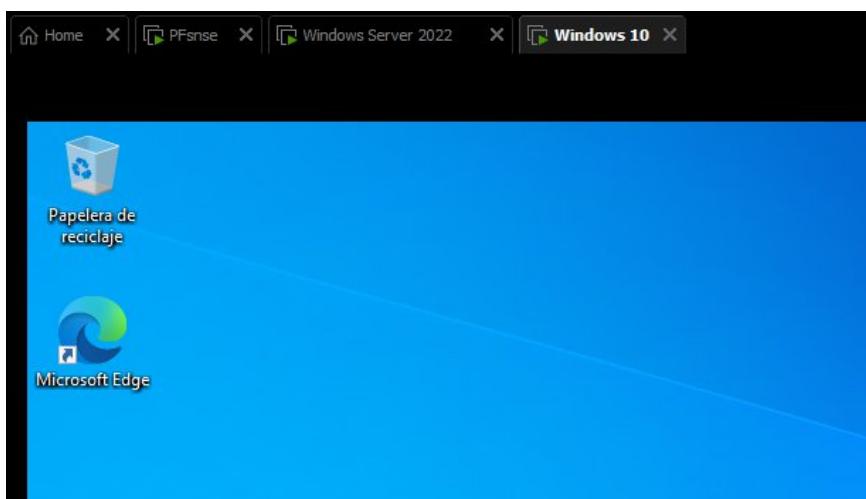


Archivo Acción Ver Ayuda

Sólo falta el cliente y qué funcione realmente....

0.3.2.2 Unir un cliente Windows al Dominio.

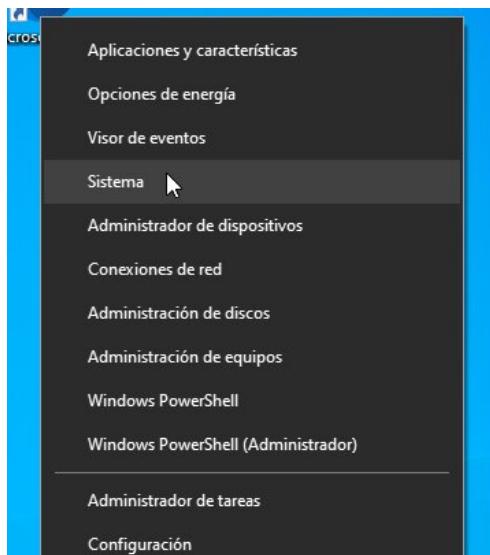
Para ello, creamos una vm nueva, y le instalaremos windows 10 pro.
Ya que la HOME, no admite unirse a dominio.



Nos vamos al icono de Windows...



Click derecho...



Sistema...

Acerca de

[Cambiar la clave de producto o actualizar la edición de Windows](#)

[Lee el contrato de servicios de Microsoft que se aplica a nuestros servicios](#)

[Lee los Términos de licencia del software de Microsoft](#)

Opciones de configuración relacionadas

[Configuración de BitLocker](#)

[Administrador de dispositivos](#)

[Escritorio remoto](#)

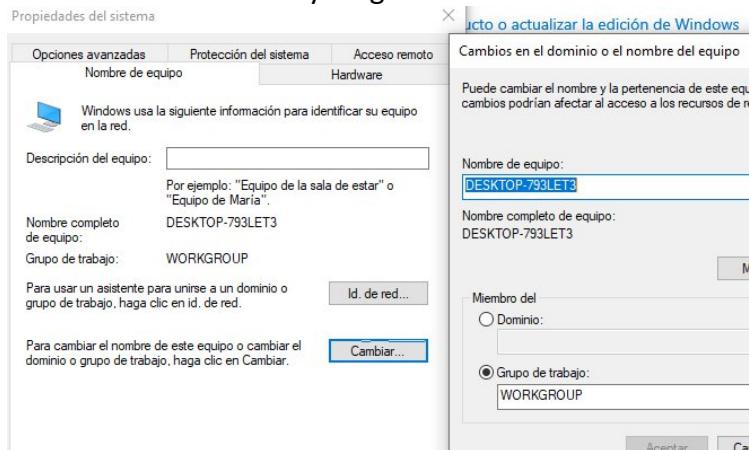
[Protección del sistema](#)

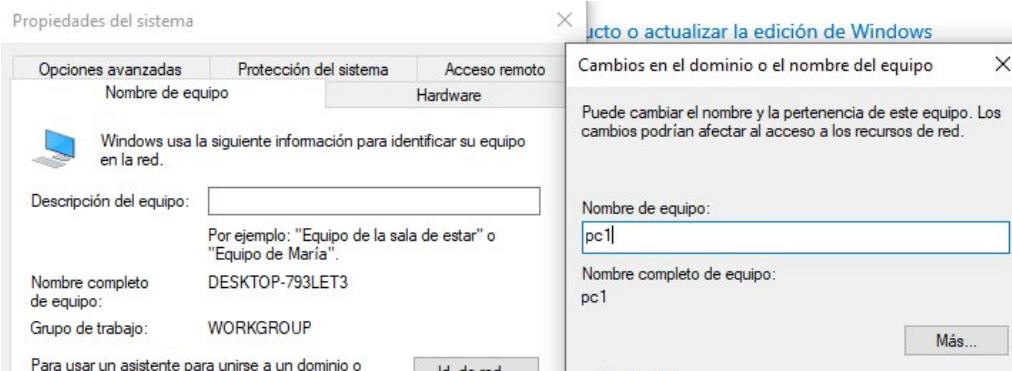
[Configuración avanzada del sistema](#)

[Cambiar el nombre de este equipo \(avanzado\)](#)

Cambiar el nombre de este equipo..

Le damos en cambiar...y luego cambiamos el nombre de este equipo





Debemos reiniciar....

Para qué se apliquen los cambios....

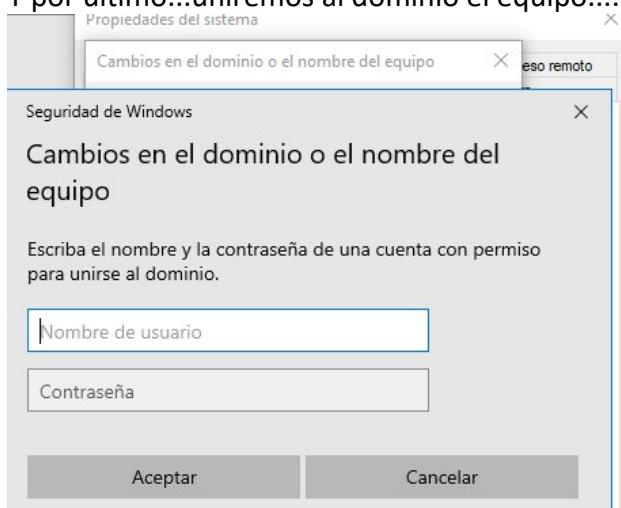
Dicho esto...al estar por defecto por DHCP, nuestro Windows 10 cogerá una ip...

Adaptador de Ethernet Ethernet0:

```
Sufijo DNS específico para la conexión. . . : empresa.net
Vínculo: dirección IPv6 local. . . : fe80::2bf8:bb2:a421:984e%5
Dirección IPv4. . . . . : 192.168.10.3
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.10.1
```

C:\Users\user>.

Y por ultimo...uniremos al dominio el equipo....



Ponemos la credencial de administrador o usuario con privilegios de admin.

Luego...ya directamente se unirá y todo funcionará...



0.4 Máquina Ubuntu.

En el server Ubuntu, vamos a alojar alguna aplicación compatible con LDAP. Pero, además de crear la máquina (omito el paso), deberemos de configurar la interfaz de nuestro firewall, para la DMZ, donde irá esta vm.

```
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 tool
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (ssh)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> ■

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

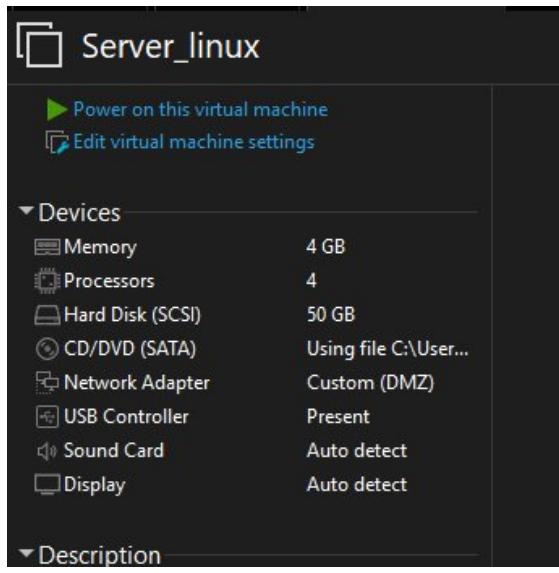
Do you want to enable the DHCP server on OPT1? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to OPT1...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...

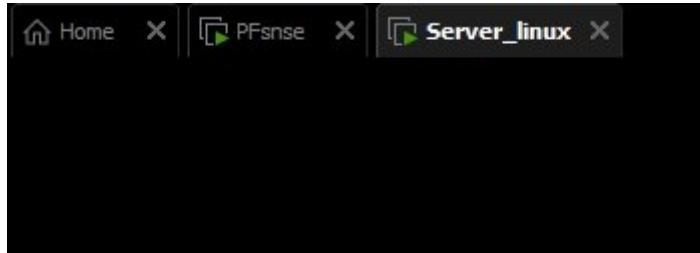
The IPv4 OPT1 address has been set to 192.168.20.1/24
You can now access the webConfigurator by opening the following URL in your browser:
  http://192.168.20.1

Press <ENTER> to continue.■
```

Ya la tendríamos lista....seguimos con el Ubuntu.



Importante, poner la vm en la red DMZ.



Arrancamos...

De mientas, deberemos de poner las reglas en el cortafuego, en la interfaz DMZ.

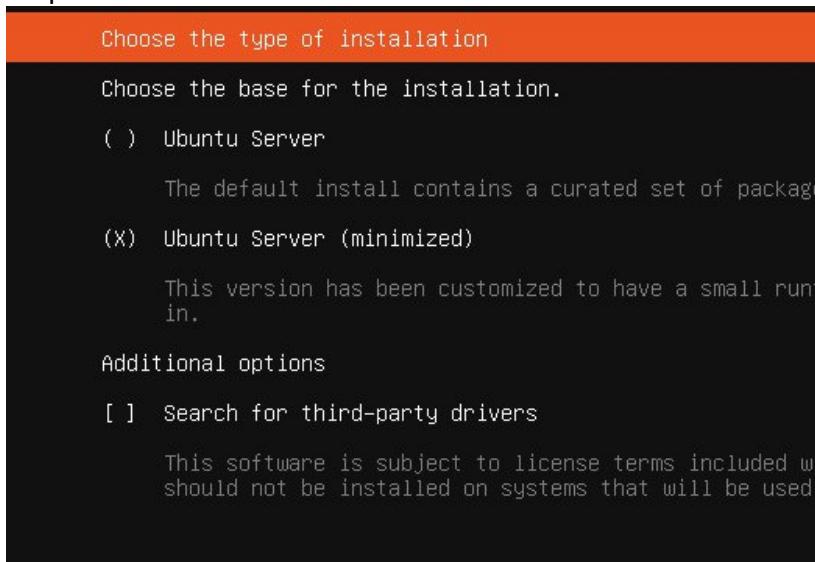
Firewall / Rules / DMZ											Edit	Print	?	
The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.											X			
Floating	WAN	LAN	DMZ	Rules (Drag to Change Order)										
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions			
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	Edit	Delete	Toggle	Copy
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	Edit	Delete	Toggle	Copy
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Internet	Edit	Delete	Toggle	Copy

Después se irá acotando las reglas, para poder reducir y minimizar riesgos.

Esperamos...

```
7.743716] systemd[1]: modprobe@configfs.service: Deactivated successfully.  
7.743955] systemd[1]: Finished modprobe@configfs.service - Load Kernel Module  
e configfs.  
[OK ] Finished modprobe@configfs.service - Load Kernel Module configfs.  
7.744302] systemd[1]: modprobe@dm_mod.service: Deactivated successfully.  
7.744469] systemd[1]: Finished modprobe@dm_mod.service - Load Kernel Module  
dm_mod.  
[OK ] Finished modprobe@dm_mod.service - Load Kernel Module dm_mod.  
7.746621] systemd[1]: modprobe@drm.service: Deactivated successfully.  
7.746782] systemd[1]: Finished modprobe@drm.service - Load Kernel Module dr  
m.  
[OK ] Finished modprobe@drm.service - Load Kernel Module drm.  
7.747098] systemd[1]: modprobe@efi_pstore.service: Deactivated successfully.  
7.747257] systemd[1]: Finished modprobe@efi_pstore.service - Load Kernel Mo  
dule efi_pstore.  
[OK ] Finished modprobe@efi_pstore.service - Load Kernel Module efi_pstore.  
7.747572] systemd[1]: modprobe@fuse.service: Deactivated successfully.  
7.747727] systemd[1]: Finished modprobe@fuse.service - Load Kernel Module f  
use.  
[OK ] Finished modprobe@fuse.service - Load Kernel Module fuse.  
7.748034] systemd[1]: modprobe@loop.service: Deactivated successfully.  
7.748186] systemd[1]: Finished modprobe@loop.service - Load Kernel Module l  
oop.  
[OK ] Finished modprobe@loop.service - Load Kernel Module loop.
```

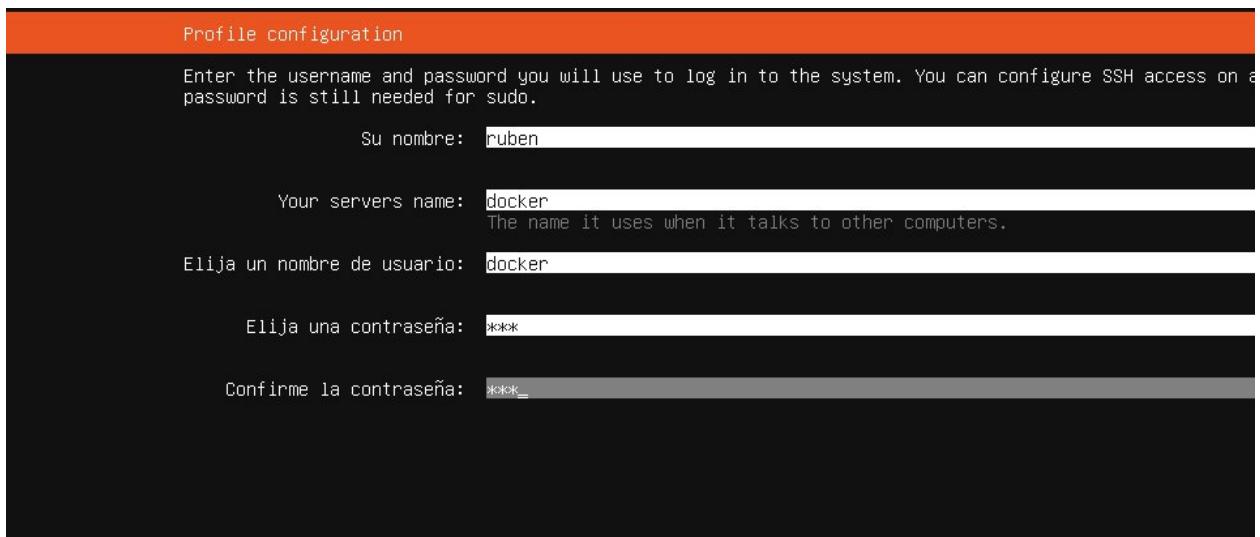
Empezamos la instalación....



*IMPORTANTE: El objetivo, de este laboratorio es ser lo más realista posible a la realidad, pero Ubuntu, debe ser instalado con NAT, y aunque tenemos puesta las reglas....no sabemos si tiene conectividad...a si que, poneis NAT, y luego la quitamos. (antes de empezar la instalación).
En la interfaz, no ponemos nada...seguimos adelante.



Damos en siguiente, luego nos aparecerá lo de la cuenta...y finalmente...se instalará.



Ponemos la información pertinente, esto sólo es para un caso especial, nuestro laboratorio, nunca deberemos de compartir la información, claro está.

```
Instalando el sistema

subiquity/Ad/apply_autoinstall_config:
subiquity/Late/apply_autoinstall_config:
configuring apt
curtin command in-target
installing system
executing curtin install initial step
executing curtin install partitioning step
curtin command install
configuring storage
running 'curtin block-meta simple'
curtin command block-meta
removing previous storage devices
configuring disk: disk-sda
configuring partition: partition-0
configuring partition: partition-1
configuring format: format-0
configuring partition: partition-2
configuring lvm_volumgroup: lvm_volumgroup-0
configuring lvm_partition: lvm_partition-0
configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
executing curtin install extract step
curtin command install
writing install sources to disk
running 'curtin extract'
curtin command extract
acquiring and extracting image from cp://tmp/tmp9uhayh2ix/mount
configuring keyboard
curtin command in-target
executing curtin install curthooks step
curtin command install
configuring installed system
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
Installing packages on target system: ['grub-pc']
configuring lscpu service
configuring raid (mdadm) service
configuring NVMe over TCP
installing Kernel /
```

Esperamos...

Y finalizado....

```

Starting systemd-binfmt.service - Set Up Additional Binary Formats...
Starting systemd-tmpfiles-setup.service Volatile Files and Directories...
Starting ufw.service - Uncomplicated firewall...
OK [ ] Finished console-setup.service - Set console font and keymap.
OK [ ] Finished finalrd.service - Create ...ntime dir for shutdown pivot root.
OK [ ] Finished ldconfig.service - Rebuild Dynamic Linker Cache.
OK [ ] Finished plymouth-read-write.service...Plymouth To Write Out Runtime Data.
OK [ ] Finished ufw.service - Uncomplicated firewall.
Mounting proc-sys-fs-binfmt_misc.m...cutable File Formats File System...
OK [ ] Finished systemd-tmpfiles-setup.service Volatile Files and Directories.
Starting systemd-journal-catalog-u...ervice - Rebuild Journal Catalog...
Starting systemd-resolved.service - Network Name Resolution...
Starting systemd-timesyncd.service - Network Time Synchronization...
Starting systemd-update-utmp.servi...ord System Boot/Shutdown in UTMP...
OK [ ] Mounted proc-sys-fs-binfmt_misc.mo...xecutable File Formats File System.
OK [ ] Finished systemd-journal-catalog-u...service - Rebuild Journal Catalog.
OK [ ] Finished systemd-binfmt.service - Set Up Additional Binary Formats.
Starting systemd-update-done.service - Update is Completed...
OK [ ] Finished systemd-update-utmp.servi...ecord System Boot/Shutdown in UTMP.
OK [ ] Finished systemd-update-done.service - Update is Completed.
OK [ ] Started systemd-timesyncd.service - Network Time Synchronization.
OK [ ] Reached target time-set.target - System Time Set.
OK [ ] Started systemd-resolved.service - Network Name Resolution.
OK [ ] Reached target nss-lookup.target - Host and Network Name Lookups.
OK [ ] Listening on systemd-rfkill.socket - Load/Save RF Kill Switch Status /dev/rfkill Watch
OK [ ] Finished apparmor.service - Load AppArmor profiles.
Starting snapd.apparmor.service - Load AppArmor profiles managed internally by snapd..
OK [ ] Started vauth.service - Authentication service for virtual machines hosted on VMware.
OK [ ] Started open-vm-tools.service - Service for virtual machines hosted on VMware.
Starting cloud-init-local.service - Cloud-init: Local Stage (pre-network)...
OK [ ] Finished snapd.apparmor.service - Load AppArmor profiles managed internally by snapd.

```

Se reinicia...y ya lo tenemos listo.

0.4.1 Configuración de interfaz

Cómo hemos realizado la instalación mínima....ahora vamos a configurar la conectividad a internet.

```

Password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-53-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

docker@docker:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:e7:24:21 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
docker@docker:~$
```

Tenemos la interfaz en down, ahora, con sudo, tendremos qué modificar el archivo de netplan.

```

GNU nano 7.2                                         /etc/netplan/50-cloud-init.yaml
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: true
```

```

network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.20.3/24
      routes:
        - to: default
          via: 192.168.20.1
  nameservers:
    addresses: [8.8.8.8, 1.1.1.1]

```

```

docker@docker:~$ sudo netplan apply
docker@docker:~$ =

```

Ponemos la gateway a la puerta de enlace, qué es el pfSense.

Ahora, desde el windows 10 de la LAN, vamos a poner una regla del lado DMZ.

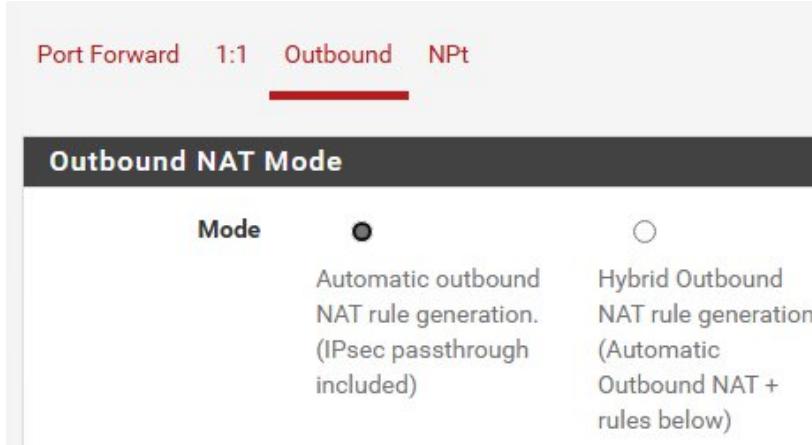
The screenshot shows the pfSense Firewall Rules interface. The top navigation bar has tabs for Firewall / Rules / DMZ. Below the tabs, there are buttons for Floating, WAN, LAN, and DMZ, with DMZ being the active tab. A sub-header "Rules (Drag to Change Order)" is present. The main table lists a single rule:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/4 KiB	IPv4 *	DMZ subnets	*	*	*	*	none		Default allow DMZ to any rule	

At the bottom of the table are buttons for Add, Delete, Toggle, Copy, Save, and Separate.

Aunque, luego haremos todo lo posible por minimizar los riesgos, con reglas más exigentes.
Nos sirve, por ahora...

De NAT, al tener en automático, hace ya las traducciones de paquete de entrada y salida en DMZ.



Dicho esto, ya tendremos el firewall operativo. Ahora, vamos a levantar una aplicación para LDAP.

Paso 1º Aplicación web corporativa.

En este nuevo paso, vamos a ver y cómo levantar una aplicación corporativa opensource.

Para ello, nos apoyaremos de Docker, un software de contenedores.

En este caso, para comodidad, usaré una interfaz más, esta vez Host-only, qué nos permitirá comunicarnos y trabajar por ssh, ya que desde el windows puede ser tedioso.

Tras poner la interfaz, y activar la interfaz.

```
docker@docker:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e7:24:21 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.3/24 brd 192.168.20.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe7:2421/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e7:24:2b brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 192.168.127.131/24 metric 100 brd 192.168.127.255 scope global dynamic ens37
        valid_lft 1800sec preferred_lft 1800sec
    inet6 fe80::20c:29ff:fe7:242b/64 scope link
        valid_lft forever preferred_lft forever
docker@docker:~$ _
```

Instalamos docker y Netplan....

```
docker@docker:~$ sudo apt install docker.io docker-compose -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  bridge-utils containerd dns-root-data dnsmasq-base pigz python3-compose python3-docker python3-dockerrypty
  python3-docopt python3-dotenv python3-texttable python3-websocket runc ubuntu-fan
Paquetes sugeridos:
  ifupdown aufs-tools cgroupfs-mount | cgroup-lite debootstrap docker-buildx docker-compose-v2 docker-doc rinse
  zfs-fuse | zfsutils
Se instalarán los siguientes paquetes NUEVOS:
  bridge-utils containerd dns-root-data dnsmasq-base docker-compose docker.io pigz python3-compose python3-docker
  python3-dockerrypty python3-docopt python3-dotenv python3-texttable python3-websocket runc ubuntu-fan
0 actualizados, 16 nuevos se instalarán, 0 para eliminar y 64 no actualizados.
Se necesita descargar 78,9 MB de archivos.
Se utilizarán 303 MB de espacio de disco adicional después de esta operación.
0% [Esperando las cabeceras]
```

Y activamos docker...

```
root@docker:~$ sudo systemctl enable docker --now
root@docker:~$
```

La app que usaremos será Owncloud, una aplicación suite ofimática que es como un google drive, pero de forma local y privada.

Yo lo he levantado todo gracias a un script, tanto contenedores, como creación de certificados, y archivos....

```
cd proyecto

echo "?? Generando certificados SSL..."
openssl req -x509 -nodes -days 365 \
-newkey rsa:2048 \
-keyout nginx/ssl/server.key \
-out nginx/ssl/server.crt \
-subj "/C=US/ST=Local/L=Dev/O=Dev/CN=localhost"

echo "?? Creando archivo docker-compose.yml..."
cat <<EOF > docker-compose.yml
version: '3.8'

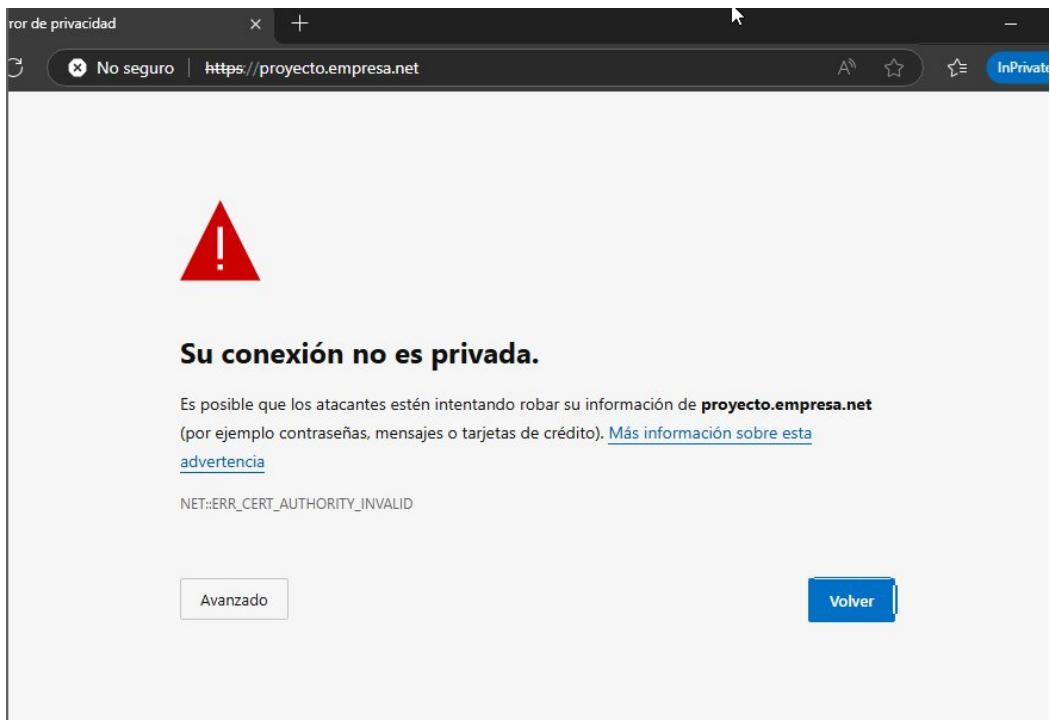
services:
  db:
    image: mariadb:10.6
    container_name: owncloud-db
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: root
      MYSQL_DATABASE: owncloud
      MYSQL_USER: owncloud
      MYSQL_PASSWORD: owncloud
    volumes:
      - ./db:/var/lib/mysql

  owncloud:
    image: owncloud/server:latest
    container_name: owncloud-app
    restart: always
    depends_on:
      - db
    environment:
      - OWNCLLOUD_DOMAIN=proyecto.empresanet
      - OWNCLLOUD_DB_TYPE=mysql
      - OWNCLLOUD_DB_NAME=owncloud
      - OWNCLLOUD_DB_USERNAME=owncloud
      - OWNCLLOUD_DB_PASSWORD=owncloud
      - OWNCLLOUD_DB_HOST=db
      - OWNCLLOUD_ADMIN_USERNAME=admin
      - OWNCLLOUD_ADMIN_PASSWORD=admin
    expose:
      - 80
      - 443

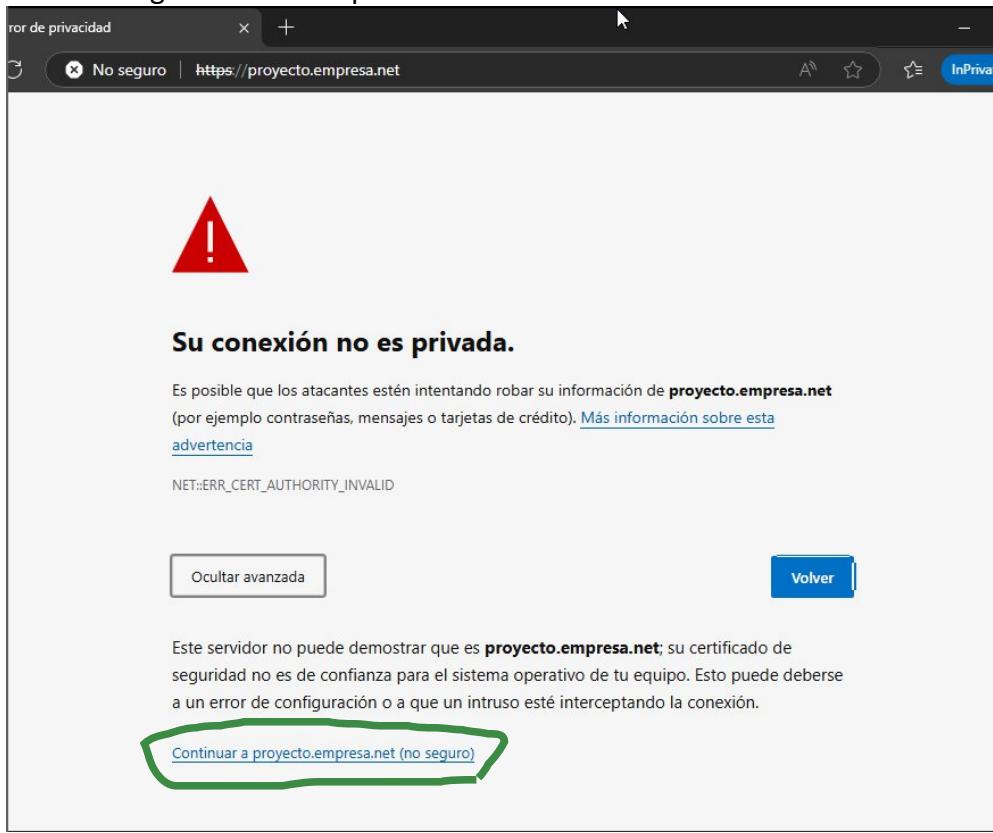
root@docker:/home/docker# docker ps -a
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS
NAMES
25a018b2e5f0        nginx:latest       "/docker-entrypoint..."   7 seconds ago     Up 6 seconds      0.0.0.0:80->80/tcp, ...
::80->80/tcp, 0.0.0.0:443->443/tcp, ::443->443/tcp   owncloud-nginx
1964751875a8        owncloud/server:latest  "/usr/bin/entrypoint..."  7 seconds ago     Up 7 seconds      8080/tcp
owncloud-app
bd833b6862fc        mariadb:10.6       "docker-entrypoint.s..."  8 seconds ago     Up 7 seconds      3306/tcp
owncloud-db
```

Ya lo tenemos levantado.

Cuando accedamos....nos aparecerá la advertencia de “peligro no seguro”, es por el certificado autofirmado.

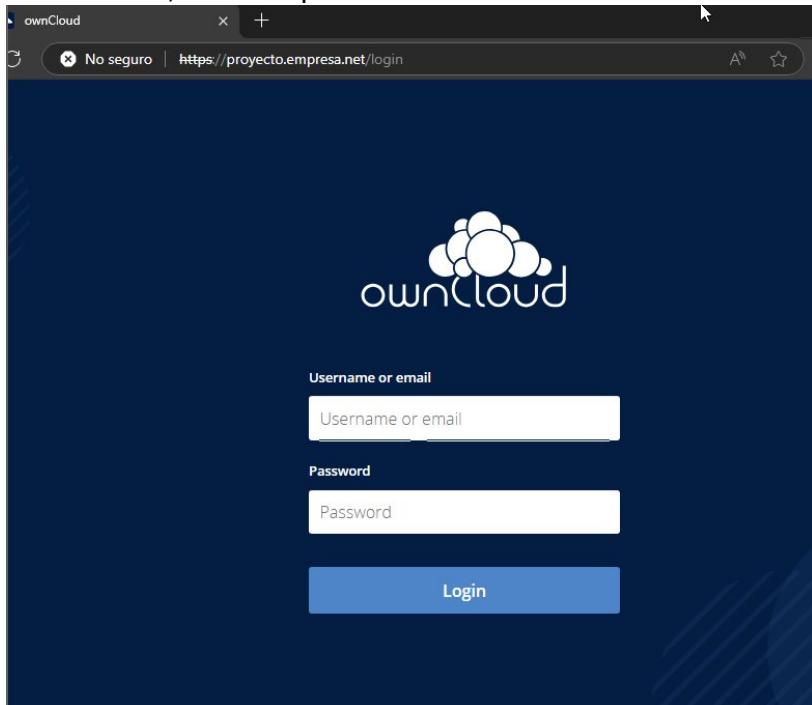


He usado un nombre dns qué apunta a la ip del ubuntu server, todo esto gracias al firewall, qué tiene las reglas necesarias para comunicarse con el dns de la LAN.



Le damos....

Ya estaríamos en el login, las credenciales están en el script, son un mero ejemplo las credenciales, nunca exponerlas****.

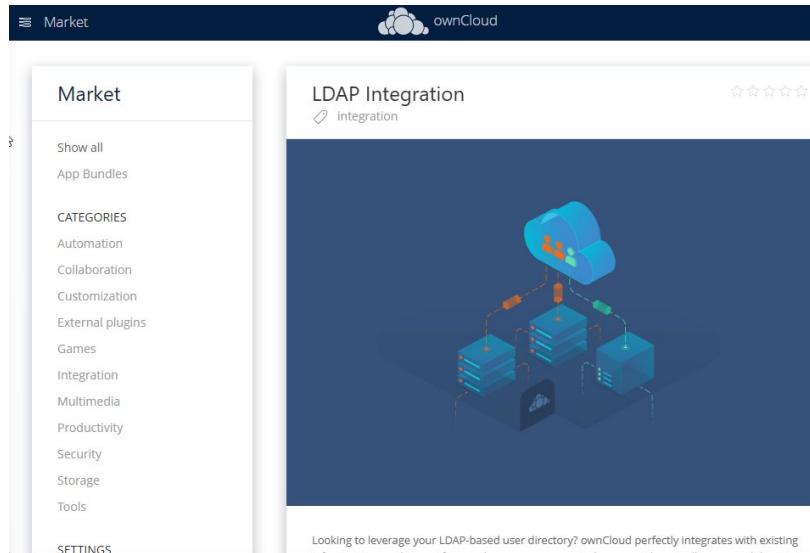
A screenshot of a web browser showing the ownCloud file manager interface. The title bar says 'Files - ownCloud'. The address bar shows 'No seguro | https://proyecto.empresa.net/apps/files/?dir=/&fileid=6'. The page features the ownCloud logo at the top. On the left is a sidebar with a list of files and folders. On the right is a main area showing a list of three folders: 'Documents', 'Learn more about ownCloud', and 'Photos'. Each folder has a preview icon, a share icon, a more options icon, its size (35 KB, 3.5 MB, 988 KB), and its last modified time (5 minutes ago).

Name	Size	Modified
Documents	35 KB	5 minutes ago
Learn more about ownCloud	3.5 MB	5 minutes ago
Photos	988 KB	5 minutes ago

Ya lo tendríamos listo.

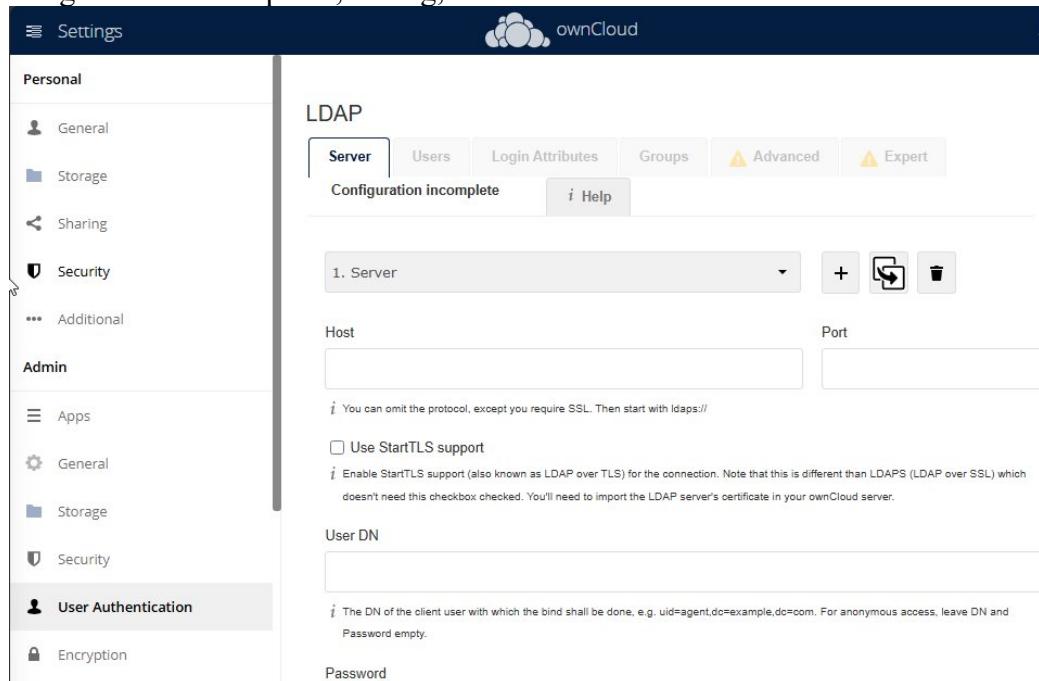
Paso 1.1 Configuración de LDAP.

En este paso vamos a enlazar nuestro Active directory con Owncloud, lo primero es buscar el módulo, plugin en la market....



Bajamos y damos en install...

Luego nos vamos a perfil, setting, user authentication.



En la realidad, deberemos de configurar LDAPs, siempre el protocolo seguro, pero, como es un laboratorio privado y local, luego más adelante haremos pruebas de pentesting.
Por lo cuál simularemos un fallo grave.

The DN of the client user with which the bind shall be done, e.g. uid=agent,dc=example,dc=com. For anonymous access, leave DN and Password empty.

>Password

For anonymous access, leave DN and Password empty.

One Base DN per line

DC=empresa,DC=net

You can specify Base DN for users and groups in the Advanced tab

Detect Base DN Test Base DN 494 entries available within the provided Base DN

Manually enter LDAP filters (recommended for large directories)

Avoids automatic LDAP requests. Better for bigger setups, but requires some LDAP knowledge.

Configuration OK ●
192.168.10.54:389

Continue

Ahí se detectaron los usuarios.... Damos en continue.
Seleccionamos los grupos qué deseemos....

ownCloud access is limited to users meeting these criteria:

Only these object classes: person

The most common object classes for users are organizationalPerson, person, user, and inetOrgPerson. If you are not sure which object class to use, please consult your directory admin.

Only from these groups:

Search groups

Available groups

- Usuarios CORP distribuidos
- Usuarios de DHCP
- Usuarios de administración remota
- Usuarios de escritorio remoto
- Usuarios del dominio
- Usuarios del monitor de sistema
- Usuarios del registro de rendimiento
- accounting

Selected groups

- IT Admins
- Finance Team
- Executives
- Oper. de impresión
- Sales Team
- marketing
- sales

Edit LDAP Query

LDAP Filter:

Damos en continue...hasta el final.
Ya suponemos qué se habrán exportado a owncloud, lo verificamos en perfil y users....

admin ▾

Settings

Users

Una cosa que noto, es que Owncloud no se lleva muy bien con sistemas windows, por lo que, no se exportan muy bien, recomiendo usar Linux.

Paso 2. Parte de Ciberseguridad.

IMPORTANTE:

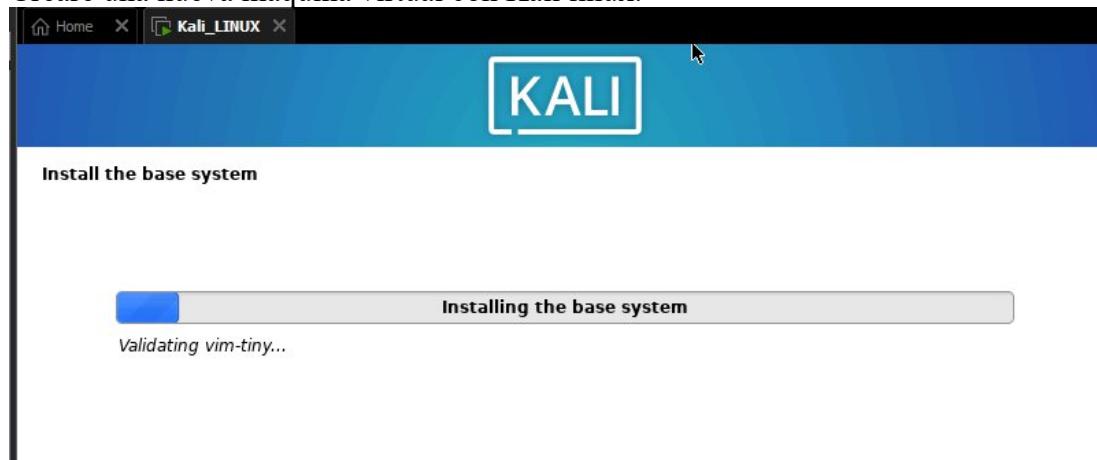
Este entorno está diseñado con fines **educativos, de auditoría y pruebas controladas de ciberseguridad** sobre infraestructura propia. Todas las acciones que se realicen, incluyendo pruebas de intrusión, análisis de vulnerabilidades o simulaciones de ataque, se llevarán a cabo dentro de un **entorno cerrado, controlado y autorizado** por el propietario del sistema.

No está permitido ni se fomenta el uso de estas técnicas en sistemas de terceros, redes públicas o infraestructuras sin permiso explícito.

El autor de este documento y scripts asociados no se hace responsable del mal uso de esta información fuera del entorno previsto. Todo uso debe respetar la legislación vigente en materia de seguridad informática.

Paso 2.1 Uso de Kali Linux.

Crearé una nueva máquina virtual con Kali linux.



El proceso lo omito...lo único importante, es que luego ponerla en la interfaz LAN.

Paso 2.2 Proceso de detección de servicios.

En este paso, lo qué haremos es escanear la red, y ver qué servicios están corriendo y puertos. Montaremos en el ubuntu un FTP totalmente vulnerable para esta prueba.

```
GNU nano 7.2                               docker-compose.yml
version: "3.8"

services:
  vulnerable-ftp:
    image: fauria/vsftpd
    container_name: vulnerable-ftp
    restart: unless-stopped
    ports:
      - "21:21"          # Puerto FTP
      - "21000-21010:21000-21010" # Puertos para modo pasivo FTP
    environment:
      FTP_USER: "vulnuser"
      FTP_PASS: "vulnpass"
      PASV_ADDRESS: "192.168.20.3"   # Cambia por la IP del host o NAT si quiere
      PASV_MIN_PORT: 21000
      PASV_MAX_PORT: 21010
      FILE_OPEN_MODE: 0777
      LOCAL_UMASK: 000
    volumes:
```

```

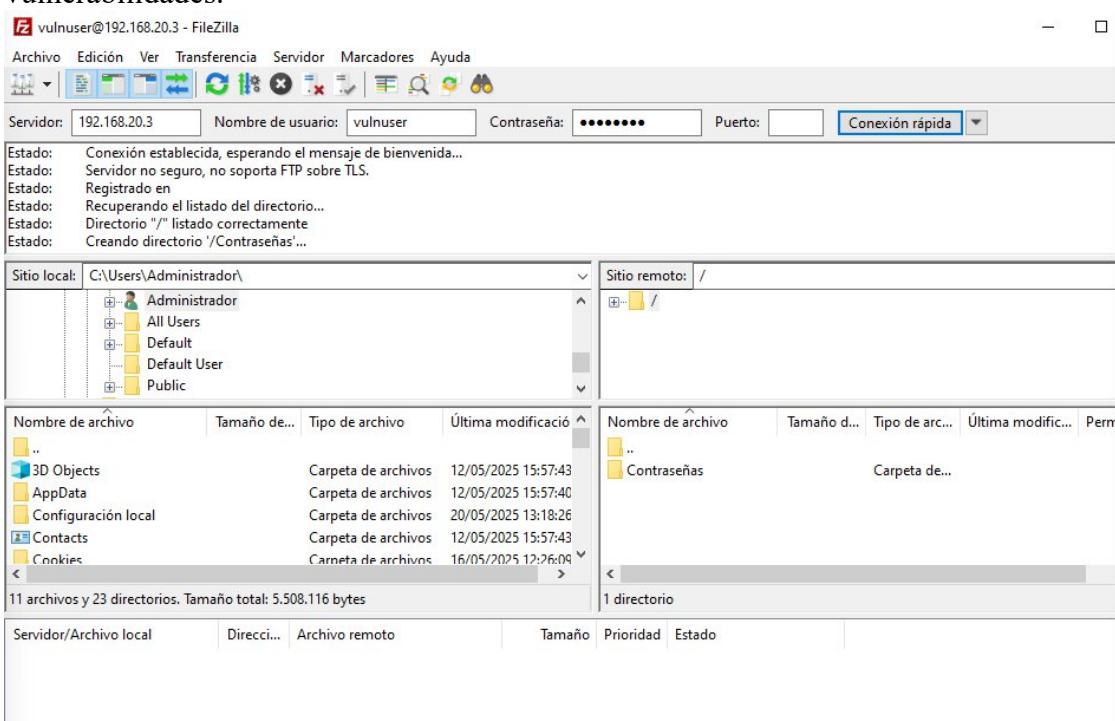
CONTAINER ID   IMAGE      COMMAND   CREATED    STATUS     PORTS      NAMES
docker@docker:~$ docker-compose up -d
Creating network "docker_default" with the default driver
Pulling vulnerable-ftp (fauria/vsftpd:...)
latest: Pulling from fauria/vsftpd
2d473b07cdd5: Downloading [=====] 48.86MB/76.1MB
47.71MB/58.96MB: Download complete
e1871c5d8fc9: Download complete
c17c1255c529: Download complete
ddcbab051542: Download complete
   853B/853B Waiting
dadbb66293c59: Waiting
99a54b7a405b: Waiting
200facf93d0a: Waiting
16ecacf7d0305: Waiting

```

Y montándose....

Esperamos...

Tras poner la regla en el pfSense, tendremos ya levantado el servicio, con ello...podremos ver las vulnerabilidades.



Paso 2.2.1 Escaneo de red.

Cómo tenemos la VM conectada a la red LAN, lo suyo es un IDS, escaneando todo el tráfico, pero en mi caso, es cómo si la infraestructura es muy débil, por presupuesto supongamos, entonces, la mejoraremos poco a poco.

Entonces, para escanear, usaremos nmap, es un software para escaneo de redes....

```

(root㉿kali)-[~/home/usuario]
# nmap 192.168.10.0/24

```

Yo usé root, para evitar poner la contraseña de permiso.

```

(root㉿kali)-[~/home/usuario]
# nmap 192.168.10.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 06:27 CDT

```

El tráfico de un escaneo, arroja esto...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	192.168.10.54	212.230.197.10	TCP	60	6145
2	0.000334210	212.230.197.10	192.168.10.54	TCP	60	443
3	4.297824844	192.168.10.54	49.12.121.47	TCP	60	6146
4	4.298167752	49.12.121.47	192.168.10.54	TCP	60	443
5	16.002206617	192.168.10.3	92.122.144.156	TCP	60	5202
6	16.002605018	92.122.144.156	192.168.10.3	TCP	60	443

Esto es poco, pero, en un caso real, nos pueden detectar, entonces hay formas de “evitar” los ids, aunque estos son muy potentes, y hay qué hacer muy bien el comando, cómo por ejemplo reduciendo la petición o rango de puerto.

Aquí tenemos el informe, en donde podemos ver a primera vista los puertos abiertos...

```
[root@kali)-[/home/usuario]
# nmap 192.168.10.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 06:27 CDT
Nmap scan report for pfSense.empresa.net (192.168.10.1)
Host is up (0.00036s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:0C:29:11:21:81 (VMware)

Nmap scan report for 192.168.10.3
Host is up (0.00033s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
5985/tcp  open  wsmans
MAC Address: 00:0C:29:1D:DD:67 (VMware)

Nmap scan report for 192.168.10.54
Host is up (0.00031s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5357/tcp  open  wsdapi
5985/tcp  open  wsmans
MAC Address: 00:0C:29:3A:0F:A1 (VMware)

Nmap scan report for 192.168.10.4
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.10.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 10.47 seconds
```

Vamos a ir a por la máquina windows server, haber si es posible hacer algo....

```
(root㉿kali)-[~/home/usuario]
└─# nmap --script vuln,vulners -sV 192.168.10.54
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 06:31 CDT
```

Intentaremos escalar en el sistema....., luego tambien haremos un estudio de la estructura AD

```
(root㉿kali)-[~/home/usuario]
└─# nmap --script vuln,vulners -sV 192.168.10.54
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 06:31 CDT
Nmap scan report for 192.168.10.54
Host is up (0.00031s latency).

Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-05-20 11:31:50Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: empresa.net0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: empresa.net0., Site: Default-First-Site-Name)
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: empresa.net0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: empresa.net0., Site: Default-First-Site-Name)
5357/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
5985/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 00:0C:29:3A:0F:A1 (VMware)

Service Info: Host: WSERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 192.00 seconds
```

Aquí tenemos más detallado sobre las versiones de los servicios....

```
(root㉿kali)-[~/home/usuario]
└─# sudo nmap -p 445 --script smb-vuln* 192.168.10.54
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 06:41 CDT
Nmap scan report for 192.168.10.54
Host is up (0.00045s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:3A:0F:A1 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 5.24 seconds
```

Cómo era previsible, el Windows Server, está bien en aspectos de vulnerabilidad, está actualizado y ningún agujero de seguridad....

Paso 2.3 Ejemplo de servicio vulnerable.

Cómo ya vimos antes, montamos un servicio vulnerable en el ubuntu, ese sí qué podremos atacarlo.....

```
—(root@kali)-[/home/usuario]
→# nmap 192.168.20.0/24
```

Vamos a analizar la DMZ....

```
—(root@kali)-[/home/usuario]
→# nmap 192.168.20.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 06:44 CDT
Nmap scan report for 192.168.20.1
Host is up (0.00046s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for proyecto.empresa.net (192.168.20.3)
Host is up (0.00051s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 8.44 seconds
```

Bingo, tenemos servicios expuestos....vamos a ver la de ftp qué versión tiene....

```
—(root@kali)-[/home/usuario]
→# nmap --script vuln,vulners -sV 192.168.20.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 06:45 CDT
```

Esperamos....

```
Host is up (0.00053s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
|_ vulners:
|   vsftpd 3.0.2:
|     CVE-2021-3618  7.4    https://vulners.com/cve/CVE-2021-3618
|     CVE-2015-1419  5.0    https://vulners.com/cve/CVE-2015-1419
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)
|_ vulners:
|   cpe:/a:openbsd:openssh:9.6p1:
|     5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  9.8    https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A *EXPLOIT*
|     33D623F7-98E0-5F75-80FA-81AA666D1340  9.8    https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340 *EXPLOIT*
|     PACKETSTORM:190587  8.1    https://vulners.com/packetstorm/PACKETSTORM:190587 *EXPLOIT*
|     PACKETSTORM:179290  8.1    https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT*
|     FB2E9ED1-43D7-585C-A197-0D6628B20134  8.1    https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B20134 *EXPLOIT*
|     FA3992CE-9C4C-5350-8134-177126E0BD3F  8.1    https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E0BD3F *EXPLOIT*
|     F8981437-1287-5B69-93F1-657DFB1DCE59  8.1    https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59 *EXPLOIT*
|     F58A5CB2-2174-586F-9CA9-4C47F8F38B5E  8.1    https://vulners.com/githubexploit/F58A5CB2-2174-586F-9CA9-4C47F8F38B5E *EXPLOIT*
|     EFD615F0-8F17-5471-AA83-0F491FD497AF  8.1    https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD497AF *EXPLOIT*
|     EC20B9C2-6857-5848-848A-A9F430D13EEB  8.1    https://vulners.com/githubexploit/EC20B9C2-6857-5848-848A-A9F430D13EEB *EXPLOIT*
|     EB13CBD6-BC93-5F14-A210-AC0B5A1D8572  8.1    https://vulners.com/githubexploit/EB13CBD6-BC93-5F14-A210-AC0B5A1D8572 *EXPLOIT*
|     E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD  8.1    https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD *EXPLOIT*
|     E543E274-C20A-582A-8F8E-F8E3F381C345  8.1    https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381C345 *EXPLOIT*
|     E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257  8.1    https://vulners.com/githubexploit/E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257 *EXPLOIT*
|     E24EEC0A-40F7-5BBC-9E4D-7B13522FF915  8.1    https://vulners.com/githubexploit/E24EEC0A-40F7-5BBC-9E4D-7B13522FF915 *EXPLOIT*
|     DC798E98-BA77-5F86-9C16-0CF8CD540EBB  8.1    https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD540EBB *EXPLOIT*
|     DC473885-F54C-5F76-BAFD-0175E4A90C1D  8.1    https://vulners.com/githubexploit/DC473885-F54C-5F76-BAFD-0175E4A90C1D *EXPLOIT*
|     D85F08E9-DB96-55E9-8DD2-22F01980F360  8.1    https://vulners.com/githubexploit/D85F08E9-DB96-55E9-8DD2-22F01980F360 *EXPLOIT*
|     D572250A-BE94-501D-90C4-14A6C9C0AC47  8.1    https://vulners.com/githubexploit/D572250A-BE94-501D-90C4-14A6C9C0AC47 *EXPLOIT*
```

Pues efectivamente....tenemos vulnerabilidades, entonces, podemos continuar hacia adelante...
Con el ejercicio ético.

Vamos a buscar en una base de datos de exploit...el cve....

CVE-2021-3618 7.4 <https://vulners.com/cve/CVE-2021-3618>

└ CVE-2015-1419 5.0 <https://vulners.com/cve/CVE-2015-1419>

Estas vulnerabilidades del contenedor de FTP, no se pueden explotar, pero, se recomendaría actualizar poner siempre a la ultima versión disponible.

CONCLUSIÓN,

En conclusión, aunque sea un poco corto el proyecto personal, hemos visto cosas muy buenas, desde la conectividad a través de un cortafuegos...hasta un poco de hacking ético, pero, puede servir mucho de cara al futuro.

Sobre todo la parte de instalar pfSense.

