

Implementación de conexión WAN mediante pfSense en una infraestructura Windows Server

Objetivo

El alumno deberá instalar y configurar un firewall pfSense para proporcionar salida a Internet a una red privada en la que ya existe:

- Un **Controlador de Dominio (DC1)** Windows Server con Active Directory y DNS.
- Dos clientes Windows Server y Windows11 unidos al dominio.
- Una red privada previamente configurada mediante **VMnet1 (Host-only)**.

El objetivo es que pfSense actúe como **router/firewall**, proporcionando:

- Acceso a Internet a través de **WAN ↳ NAT**.
- Red interna mediante **LAN privada**.
- Reenvío DNS apropiado para que la red resuelva dominios externos.

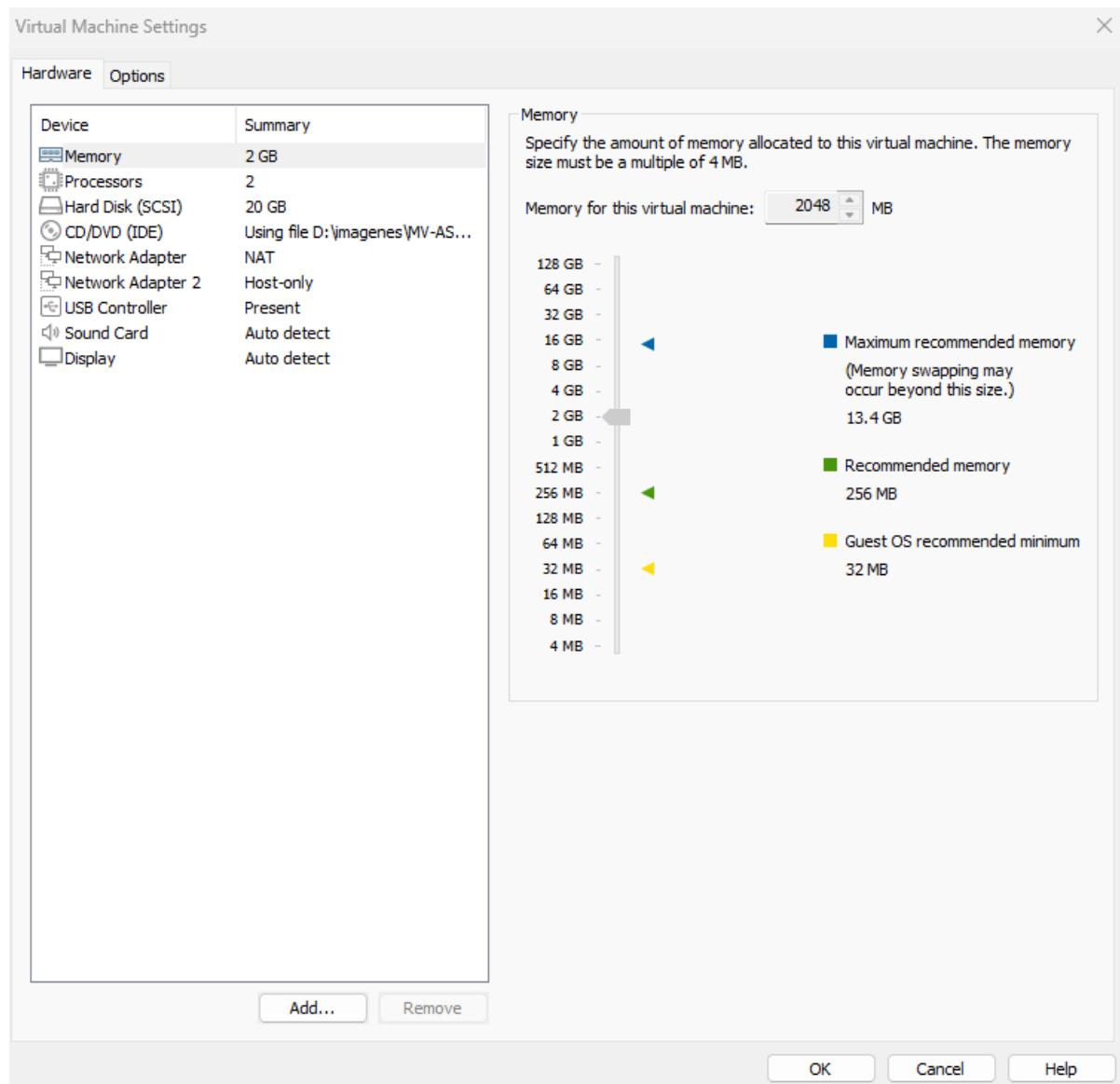
Requisitos Previos

- ISO de pfSense CE 2.8.x (descargada previamente).
- Las máquinas virtuales ya creadas:
- DC1 con IP fija: WS-GU-XXX-DC1
- Cliente1 (WS_GUI_XXX_DC2) y Cliente2 (W11).
- Red privada VMnet1

Tareas por realizar

Crear máquina virtual en VMware para pfSense

1. Crear la máquina virtual:
 - a. Tipo: **FreeBSD 64-bit**
 - b. Disco: **20 GB**
 - c. RAM: **2 GB**
 - d. CPU: **2 vCPU**
2. Añadir **dos adaptadores de red**:
 - a. **Adaptador 1 → NAT** (será la WAN)
 - b. **Adaptador 2 → VMnet1 (Host-only)** (será la LAN)
3. Cargar la ISO de pfSense, arrancar la máquina e instalar.



Esta es la configuración del pfSense

Configurar las interfaces

Durante el arranque de pfSense:

1. Asignar interfaces:
 - a. Se detectarán **em0** y **em1**.
 - b. Elegir:
 - i. **WAN = em0**
 - ii. **LAN = em1**
2. Revisar que la LAN quede con IP por defecto:

a. 192.168.1.1/24

```
LAN (lan) -> em1 -> v4: 192.168.1.1/24
```

Ya esta configurada la LAN

IMPORTANTE:

Esta IP NO sirve para nuestra red de dominio. Debe cambiarse a la red que hayas configurado en la infraestructura del dominio.

Reconfigurar la LAN de pfSense

En el menú de consola (opción 2):

1. Cambiar la IP LAN:

- a. Nueva IP LAN: 192.168.111.1 (es un ejemplo)
- b. Máscara: /24
- c. Habilitar DHCP → **Sí**, pero con rango que no incluya al DC.

Rango ejemplo: **192.168.111.100 – 192.168.111.199**

```
WAN (wan) -> em0 -> v4/DHCP4: 192.168.6.141/24
LAN (lan) -> em1 -> v4: 192.168.179.1/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address     11) Restart GUI
3) Reset admin account and 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: ■
```

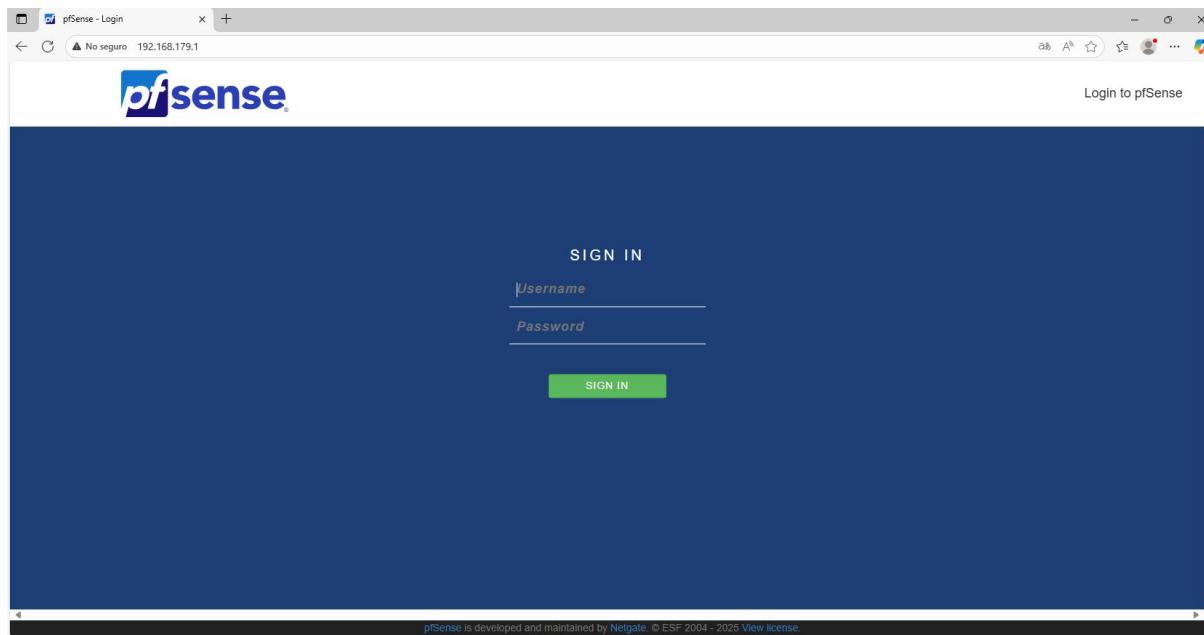
Ya esta configurado con la ip del dominio

2. Acceder desde un navegador a:

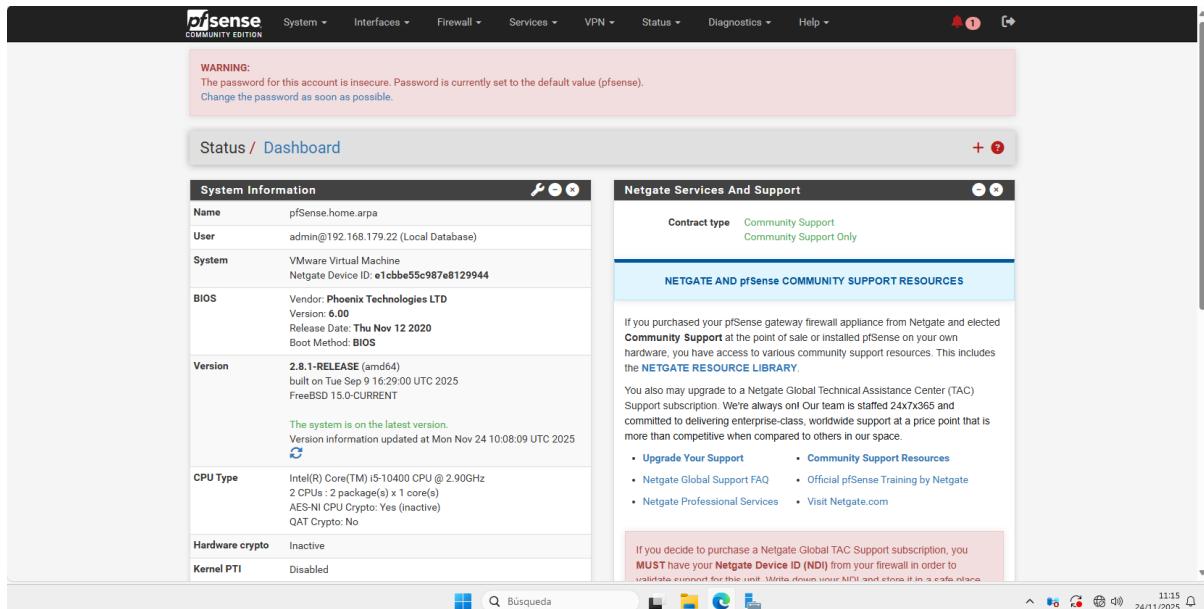
<https://192.168.111.1>

Usuario:**admin**

Contraseña:**pfsense**



The screenshot shows the pfSense Login screen. It features a blue header with the pfSense logo and a "Login to pfSense" link. Below the header is a dark blue background with the word "SIGN IN" in white capital letters. There are two input fields: "Username" and "Password", both with placeholder text. A green "SIGN IN" button is positioned below the password field. At the bottom of the screen, there is a small footer note: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license".



The screenshot shows the pfSense Status / Dashboard page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and a user icon. A red warning message box states: "WARNING: The password for this account is insecure. Password is currently set to the default value (pfSense). Change the password as soon as possible." The main content area is divided into two sections: "System Information" and "Netgate Services And Support". The "System Information" section displays various hardware and software details. The "Netgate Services And Support" section provides information about support contracts and resources. A sidebar on the right contains a "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" section with links to upgrade support, community resources, and professional services.

Y ponemos el usuario y la contraseña

Configuración inicial desde la GUI

En el asistente web:

1. **Hostname:** pfSense
2. **Domain:** el dominio del alumno (ctp.local)
3. **DNS Server 1:** ip del controlador de dominio DC1

System

Hostname	<input type="text" value="pfsense"/>
Name of the firewall host, without domain part.	
Domain	<input type="text" value="srg.local"/>
Domain name for the firewall.	
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.	

DNS Server Settings

DNS Servers	<input type="text" value="192.168.179.22"/>	DNS Hostname
Address		Hostname
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.		Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).
Add DNS Server	+ Add DNS Server	
DNS Server Override	<input checked="" type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server	
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.		

Aquí configuramos en el asistente web

4. Time server: por defecto

5. WAN:

a. Tipo: DHCP

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="WAN"/>
Enter a description (name) for the interface here.	
IPv4 Configuration Type	<input type="text" value="DHCP"/>
IPv6 Configuration Type	<input type="text" value="None"/>

b. Desmarcar checks block

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/>
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.	
Block bogon networks	<input type="checkbox"/>
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.	
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.	
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.	

Desmarcar esas casillas para que no de problemas

6. LAN:

a. Confirmar: puerta de enlace de la red privada (ejemplo: 192.168.111.1)

Static IPv4 Configuration

IPv4 Address	192.168.179.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface . Gateways can be managed by clicking here .		

Reserved Networks

Esta configurada la puerta de enlace

7. Cambiar contraseña del admin.

Change Password

This page changes the password for the current user in the local configuration. This affects all services which utilize the Local Authentication database (User Manager).

This page cannot change passwords for users from other authentication sources such as LDAP or RADIUS.

Database	Local Authentication
Username	admin
Password 
Enter a new password.	
Hints: Current NIST guidelines prioritize password length over complexity. The password cannot be identical to the username.	
Confirmation	<input type="text"/>
Type the new password again for confirmation.	

Cambiamos la contraseña del admin

8. Finalizar.

Integración con el dominio

1. En el Controlador de Dominio (DC1):

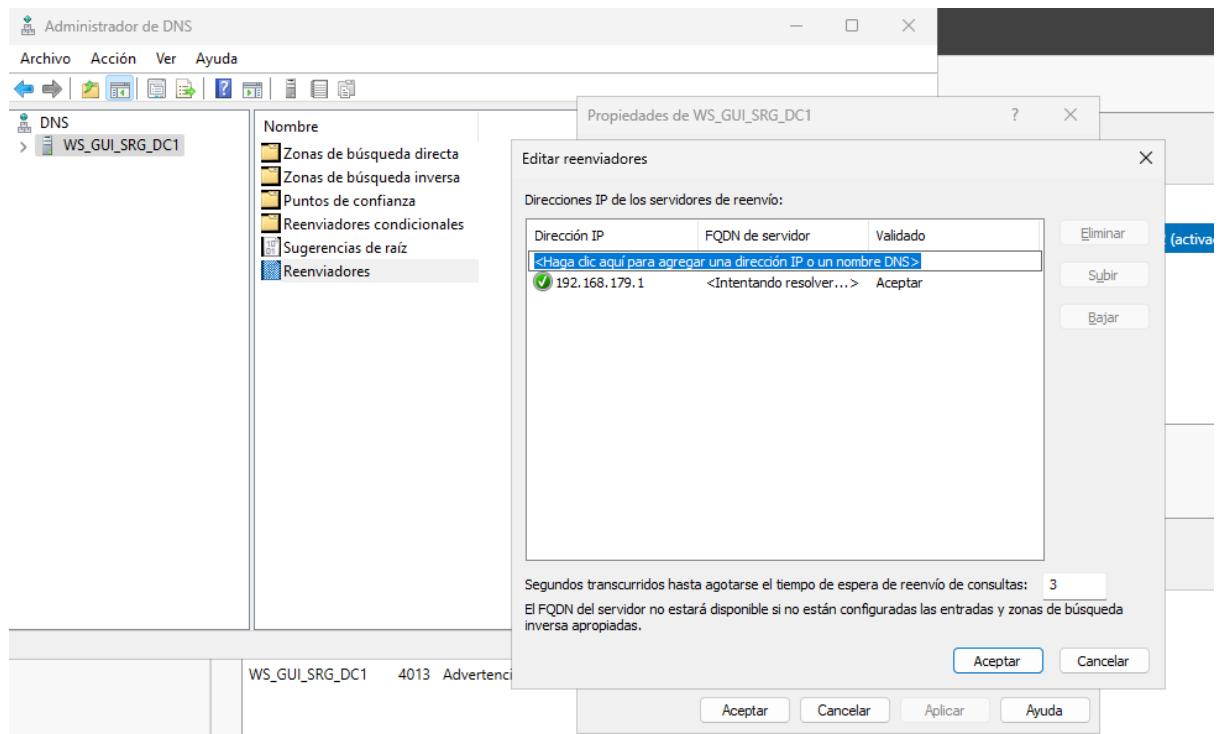
Comprobar que:

- IP fija: por ejemplo 192.168.111.10
- Máscara: 255.255.255.0
- **Puerta de enlace:** la que hayamos configurado en pfSense (ejemplo 192.168.111.1)
- **DNS:** 127.0.0.1

Esta es la configuración del cliente DC1

2. Activar reenviadores DNS:

- Abrir Administrador DNS → Propiedades del servidor.
 - Pestaña **Reenviadores**.
 - Añadir: pfSense



Ya están configurados los reenviadores con la puerta de enlace del pfSense

Pruebas finales

1. Desde DC1:

- Ping: pfsense 8.8.8.8, google.com

```
C:\Users\Administrador>ping 192.168.179.1

Haciendo ping a 192.168.179.1 con 32 bytes de datos:
Respuesta desde 192.168.179.1: bytes=32 tiempo<1ms TTL=64
Respuesta desde 192.168.179.1: bytes=32 tiempo<1ms TTL=64
Respuesta desde 192.168.179.1: bytes=32 tiempo<1ms TTL=64

Estadísticas de ping para 192.168.179.1:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
```

Ping a la pfsense

```
C:\Users\Administrador>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=15ms TTL=127
Respuesta desde 8.8.8.8: bytes=32 tiempo=15ms TTL=127
Respuesta desde 8.8.8.8: bytes=32 tiempo=17ms TTL=127

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 15ms, Máximo = 17ms, Media = 15ms
Control-C
^C
```

Ping 8.8.8.8

```
C:\Users\Administrador>ping google.com

Haciendo ping a google.com [142.250.200.78] con 32 bytes de datos:
Respuesta desde 142.250.200.78: bytes=32 tiempo=27ms TTL=127
Respuesta desde 142.250.200.78: bytes=32 tiempo=22ms TTL=127
Respuesta desde 142.250.200.78: bytes=32 tiempo=15ms TTL=127

Estadísticas de ping para 142.250.200.78:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 15ms, Máximo = 27ms, Media = 21ms
Control-C
^C
```

Ping Google.com

- nslookup google.es

```
C:\Users\Administrador>nslookup google.es
Servidor: Unknown
Address: 192.168.179.22

Respuesta no autoritativa:
Nombre: google.es
Addresses: 2a00:1450:4003:80a::2003
           172.217.168.163
```

Nslookup Google.es esta contestando aunq este mal el nombre del servidor

2. Desde un cliente del dominio:

- ping DC1

```
C:\Users\Administrador>ping 192.168.179.22

Haciendo ping a 192.168.179.22 con 32 bytes de datos:
Respuesta desde 192.168.179.22: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.179.22: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.179.22:
    Paquetes: enviados = 3, recibidos = 2, perdidos = 1
                (33% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
```

Ping al DC1

- ping pfSense

```
C:\Users\Administrador>ping 192.168.179.1

Haciendo ping a 192.168.179.1 con 32 bytes de datos:
Respuesta desde 192.168.179.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.179.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.179.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
```

Ping al pfSense

- ping 8.8.8.8

```
C:\Users\Administrador>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=16ms TTL=127
Respuesta desde 8.8.8.8: bytes=32 tiempo=15ms TTL=127

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 15ms, Máximo = 16ms, Media = 15ms
Control-C
^C
```

Ping 8.8.8.8

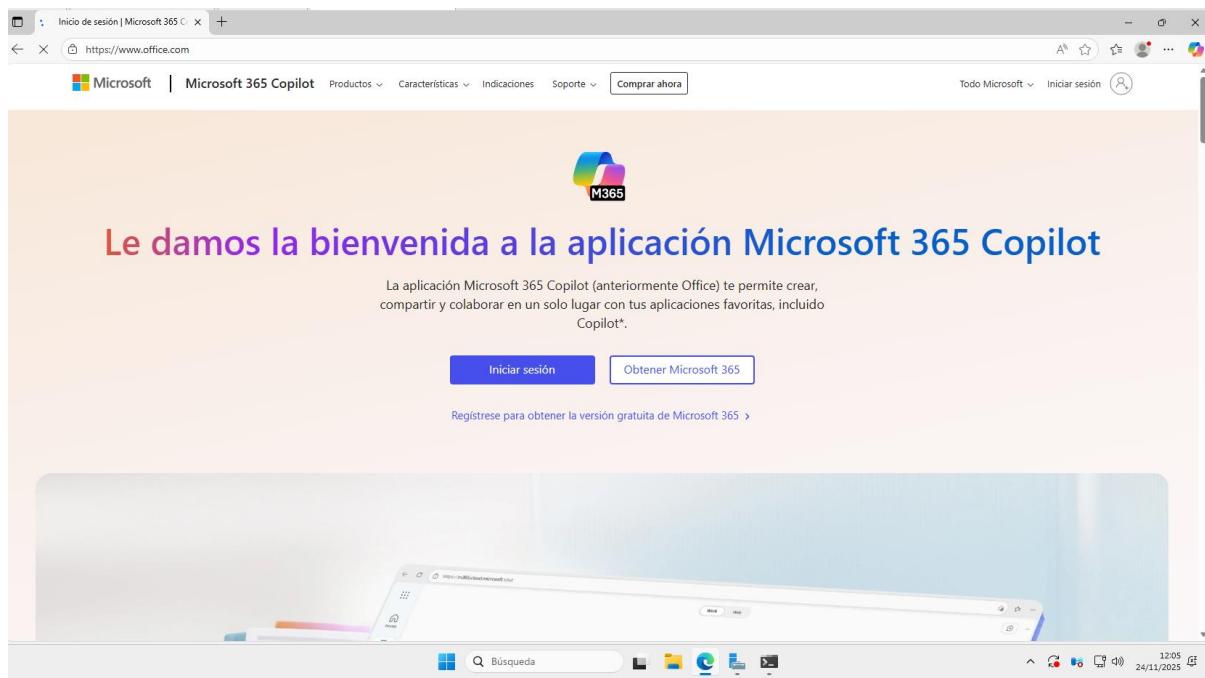
- nslookup google.es

```
C:\Users\Administrador>nslookup google.es
Servidor:  Unknown
Address:  192.168.179.22

Respuesta no autoritativa:
Nombre:  google.es
Addresses:  2a00:1450:4003:80a::2003
                    172.217.168.163
```

Ping a nslookup Google.es

3. Prueba web: abrir un navegador y comprobar que **hay Internet**.



Prueba a internet