



# VPN (WINDOWS SERVER)

Hecho por : Laura Berenguer y Jesús Padilla

## Agregamos el rol de Acceso remoto

Asistente para agregar roles y características

— □ ×

SEVIDOR DE DESTINO  
SERVER2.practica.es

### Seleccionar roles de servidor

Antes de comenzar  
Tipo de instalación  
Selección de servidor  
**Roles de servidor**  
Características  
Acceso remoto  
Servicios de rol  
Confirmación  
Resultados

Seleccione uno o varios roles para instalarlos en el servidor seleccionado.

Roles	Descripción
<input checked="" type="checkbox"/> <b>Acceso remoto</b>	Acceso remoto proporciona conectividad sin problemas a través de DirectAccess, VPN y el proxy de aplicación web. DirectAccess proporciona una experiencia siempre activada y siempre administrada. RAS proporciona servicios VPN tradicionales, incluida la conectividad de sitio a sitio (basada en sucursal o basada en nube). El proxy de aplicación web habilita la publicación de aplicaciones basadas en HTTPS y HTTP desde su red corporativa en dispositivos clientes fuera de dicha red. El enrutamiento proporciona funciones tradicionales de enrutamiento, lo que incluye NAT, así como otras opciones de conectividad. RAS v
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Atestación de mantenimiento del dispositivo	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Servicio de protección de host	
<input type="checkbox"/> Servicios de acceso y directivas de redes	
<input checked="" type="checkbox"/> Servicios de archivos y almacenamiento (2 de 12 in	
<input type="checkbox"/> Servicios de certificados de Active Directory	
<input checked="" type="checkbox"/> Servicios de dominio de Active Directory (Instalado	
<input type="checkbox"/> Servicios de Escritorio remoto	
<input type="checkbox"/> Servicios de federación de Active Directory	
<input type="checkbox"/> Servicios de implementación de Windows	
<input type="checkbox"/> Servicios de impresión y documentos	
<input type="checkbox"/> Servidor de fax	
<input type="checkbox"/> Servidor DHCP	
<input checked="" type="checkbox"/> Servidor DNS (Instalado)	
<input type="checkbox"/> Servidor web (IIS)	
<input type="checkbox"/> Volume Activation Services	

< Anterior **Siguiente >** Instalar Cancelar

Seleccionamos los dos primeros servicios de rol

Asistente para agregar roles y características

— □ ×

SEVIDOR DE DESTINO  
SERVER2.practica.es

### Seleccionar servicios de rol

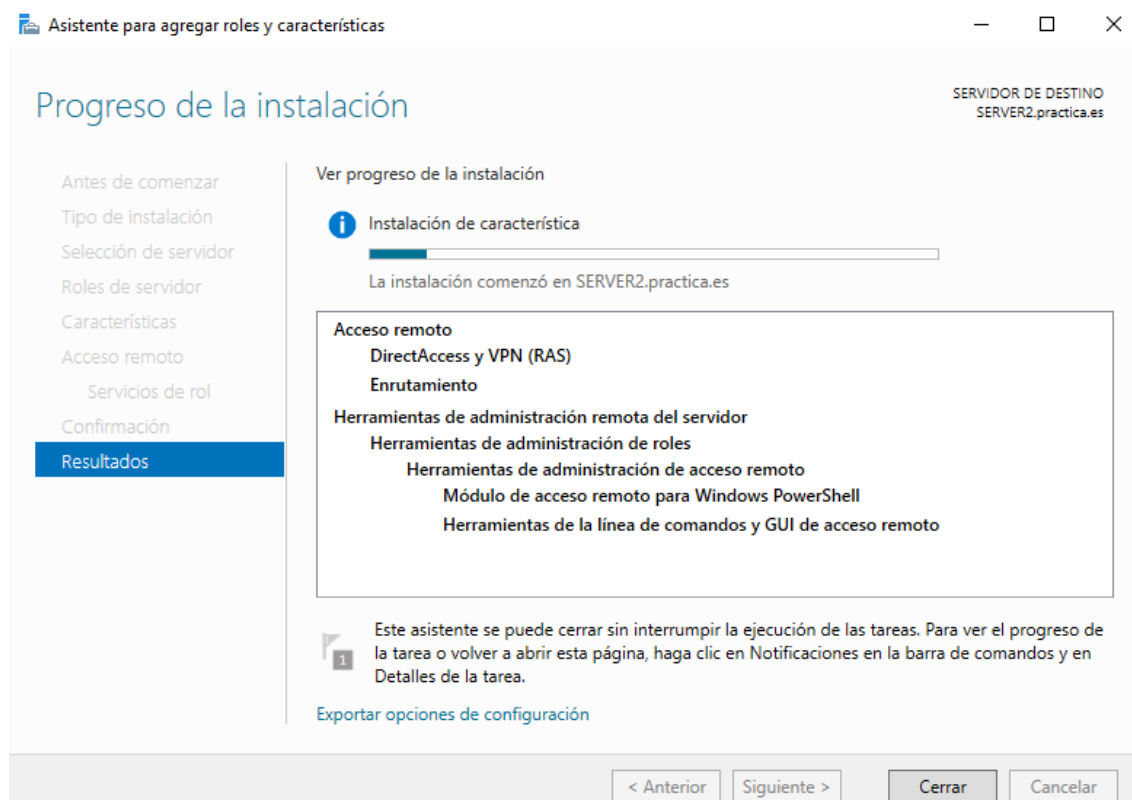
Antes de comenzar  
Tipo de instalación  
Selección de servidor  
Roles de servidor  
Características  
Acceso remoto  
**Servicios de rol**  
Confirmación  
Resultados

Seleccione los servicios de rol que desea instalar para Acceso remoto

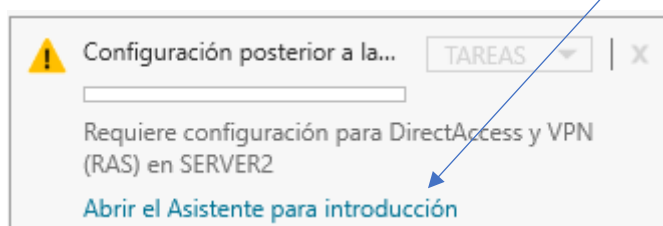
Servicios de rol	Descripción
<input checked="" type="checkbox"/> DirectAccess y VPN (RAS)	El enrutamiento proporciona compatibilidad con enrutadores NAT, enrutadores LAN que ejecutan BGP, RIP y enrutadores compatibles con multidifusión (proxy IGMP).
<input checked="" type="checkbox"/> <b>Enrutamiento</b>	
<input type="checkbox"/> Proxy de aplicación web	

< Anterior **Siguiente >** Instalar Cancelar

Instalamos



Al acabar la instalación nos aparecerá una advertencia en el administrador del servidor, debemos seleccionarla y abrir el asistente para introducción.



## Implementar solo VPN



### Acceso remoto

Use las opciones de esta página para configurar DirectAccess y VPN.

#### → Implementar DirectAccess y VPN (recomendado)

Configure DirectAccess y VPN en el servidor y habilite los equipos cliente de DirectAccess. Permita que los equipos cliente no compatibles con DirectAccess se conecten mediante VPN.

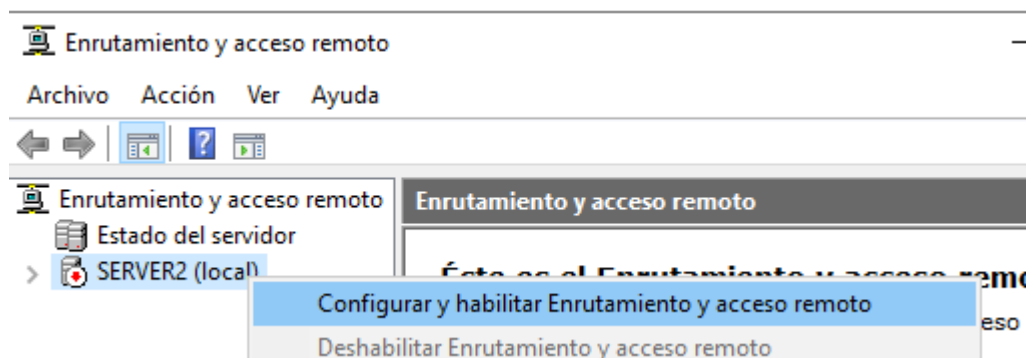
#### → Implementar solo DirectAccess

Configure DirectAccess en el servidor y habilite los equipos cliente de DirectAccess.

#### → Implementar solo VPN

Configure VPN mediante la consola de Enrutamiento y acceso remoto. Los equipos cliente remotos pueden conectarse con VPN y se pueden conectar varios sitios mediante conexiones VPN de sitio a sitio. Los clientes no compatibles con DirectAccess pueden usar VPN.

Se nos abrirá la configuración de enrutamiento y acceso remoto.



Seleccionamos configuración personalizada y elegimos los servicios, en nuestro caso solo acceso a VPN.

#### Asistente para la instalación del servidor de enrutamiento y acceso remoto

##### Configuración

Puede habilitar cualesquiera de las siguientes combinaciones de servicios o puede personalizar este servidor.

- ☐ Acceso remoto (acceso telefónico o red privada virtual)  
Permitir a clientes remotos conectarse a este servidor a través de una conexión de acceso telefónico o una conexión segura a Internet de red privada virtual (VPN).
- ☐ Traducción de direcciones de red (NAT)  
Permitir a clientes internos conectarse a Internet usando una dirección IP pública.
- ☐ Acceso a red privada virtual (VPN) y NAT  
Permitir que los clientes remotos se conecten a este servidor a través de Internet y que los clientes locales se conecten a Internet usando una sola dirección IP pública.
- ☐ Conexión segura entre dos redes privadas  
Conectar esta red a una red remota, como a una oficina sucursal.
- ☒ Configuración personalizada  
Seleccionar cualquier combinación de características disponibles en Enrutamiento y acceso remoto.

< Atrás

Siguiente >

Cancelar

#### Asistente para la instalación del servidor de enrutamiento y acceso remoto

##### Configuración personalizada

Cuando se cierre este asistente, puede configurar los servicios seleccionados en la consola Enrutamiento y acceso remoto.

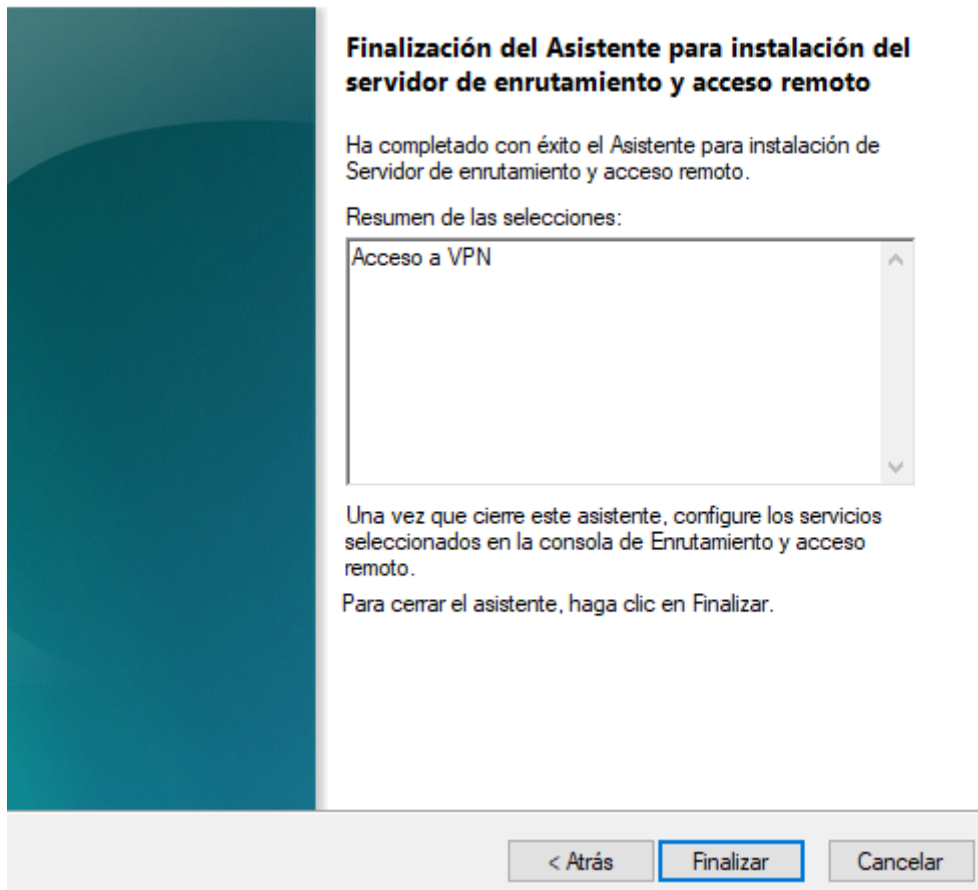
Seleccione los servicios que desea habilitar en este servidor.

- ☒ Acceso a VPN
- ☐ Acceso telefónico
- ☐ Conexiones de marcado a petición (utilizadas para enrutamiento de oficinas sucursales)
- ☐ NAT
- ☐ Enrutamiento LAN

< Atrás

Siguiente >

Cancelar



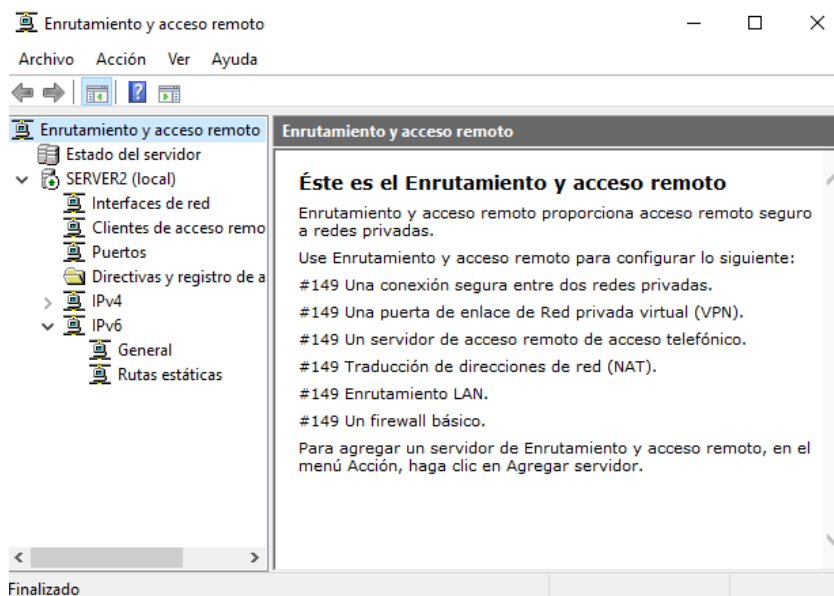
## Enrutamiento y acceso remoto

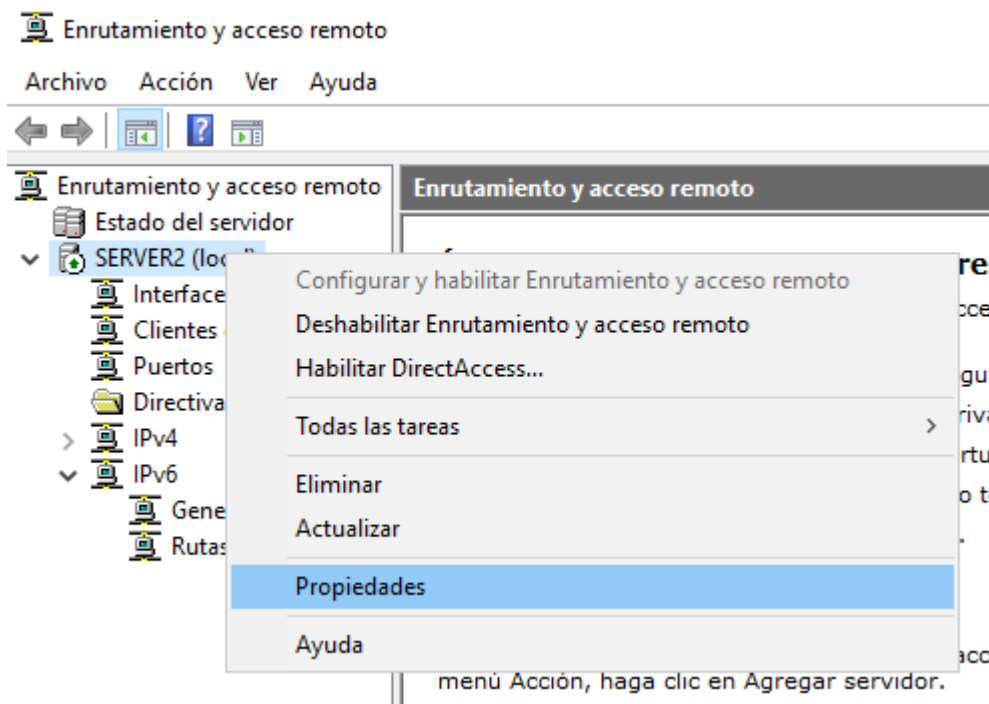
### Iniciar el servicio

El Servicio de enrutamiento y acceso remoto está listo para usarse.

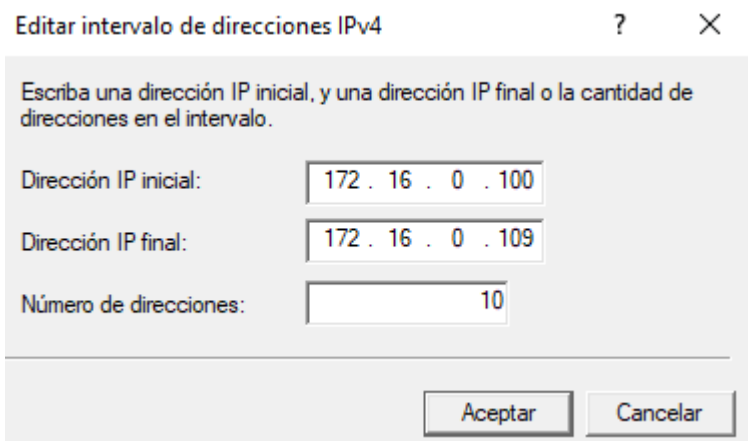
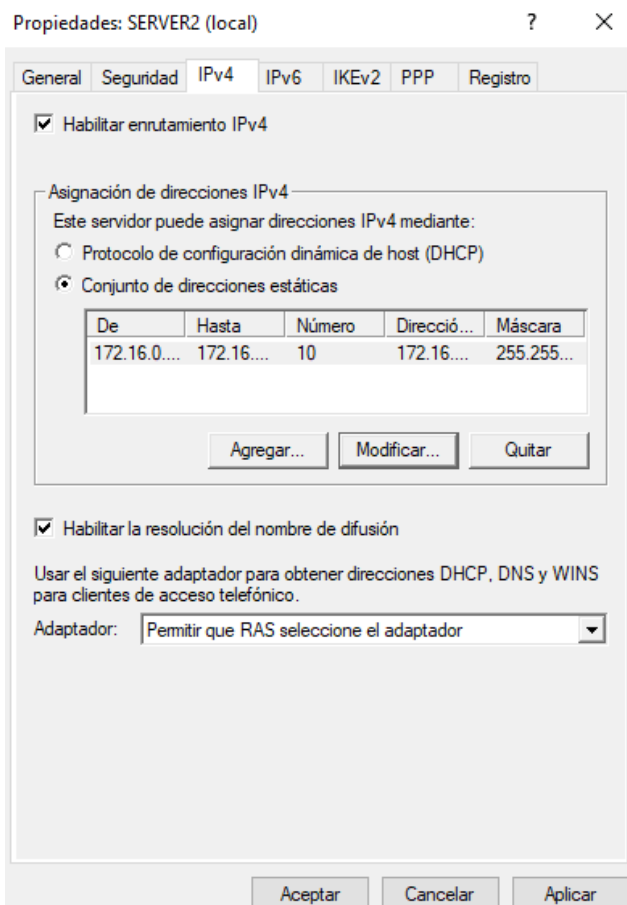
Iniciar servicio

Cancelar

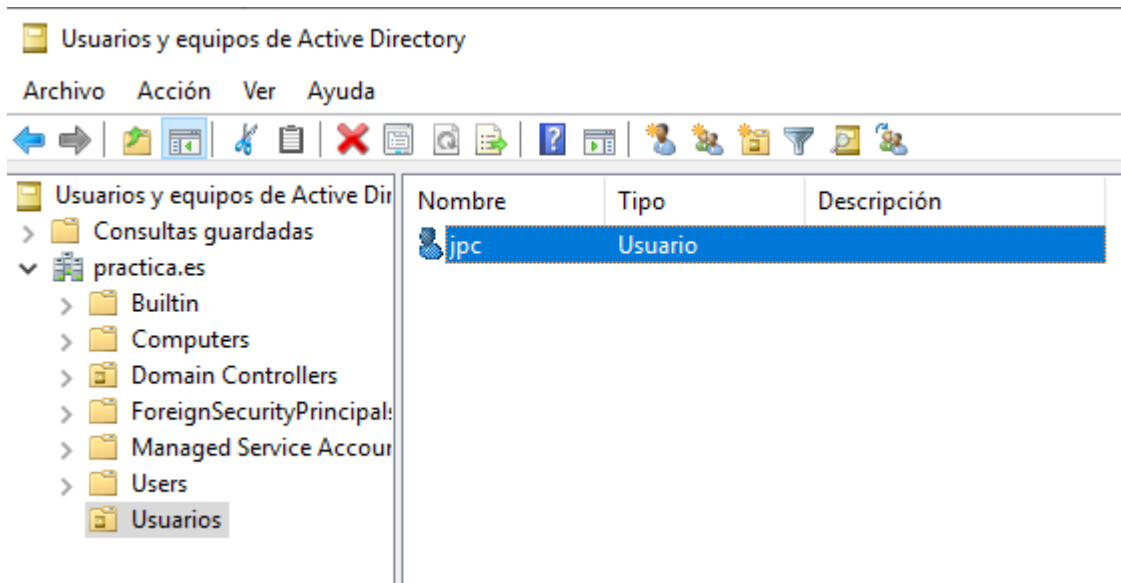




En IPv4 podremos repartir un conjunto de rutas estáticas para limitar el número de usuarios que puedan conectarse a la VPN aumentando así la seguridad. Y estableceremos un rango de IPs deseadas.

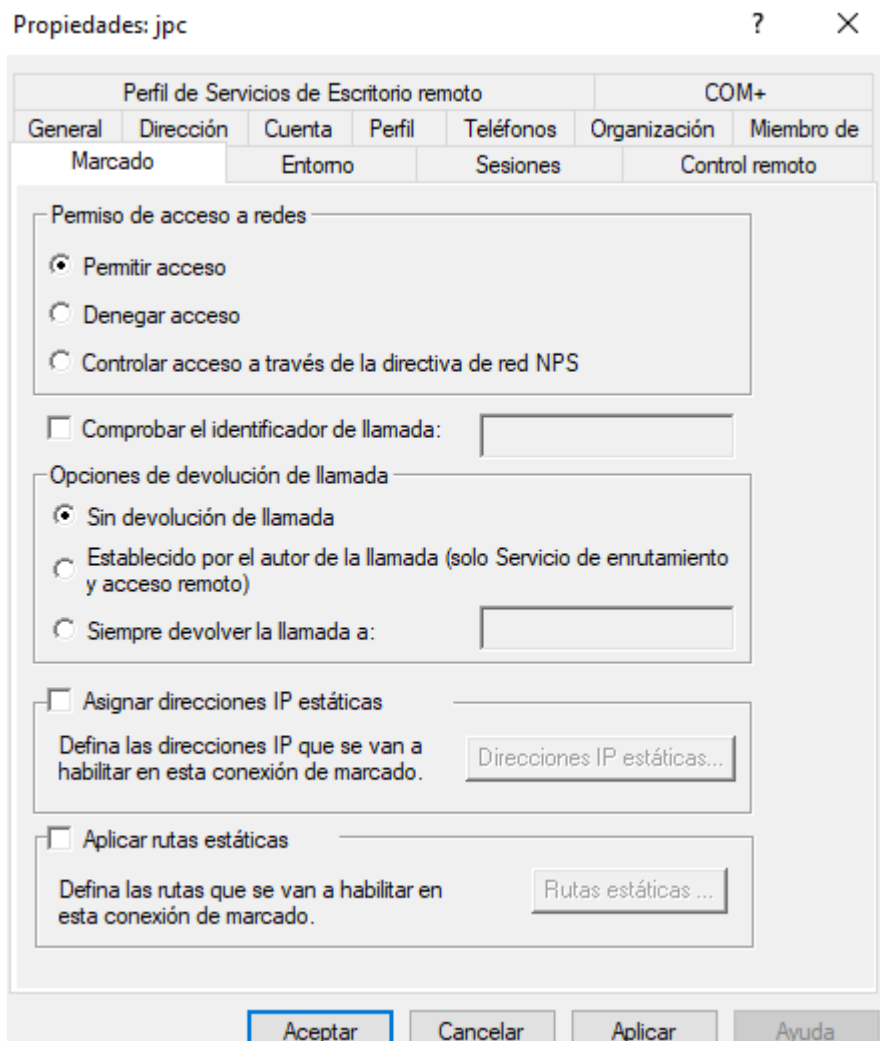


Ahora nos iremos a Herramientas→Usuarios y equipos de ADirectory.



Crearemos un usuario.

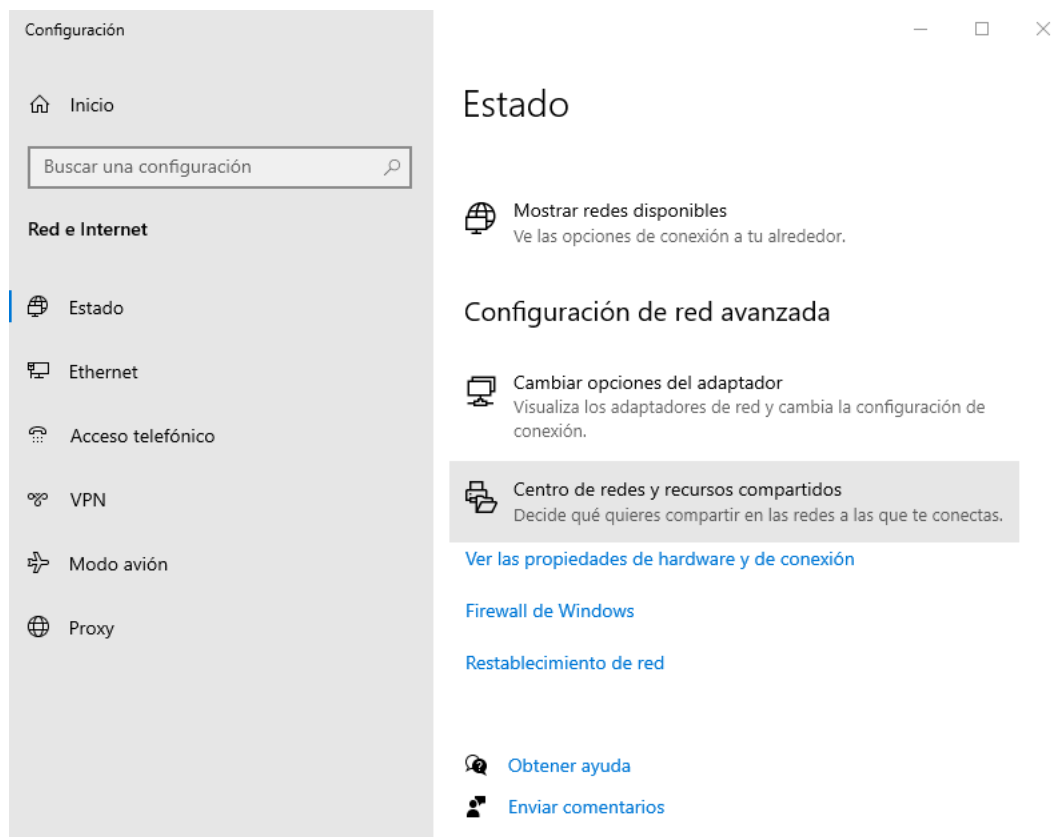
Permitir acceso a redes solo los que vayan a estar conectados por medio de VPN



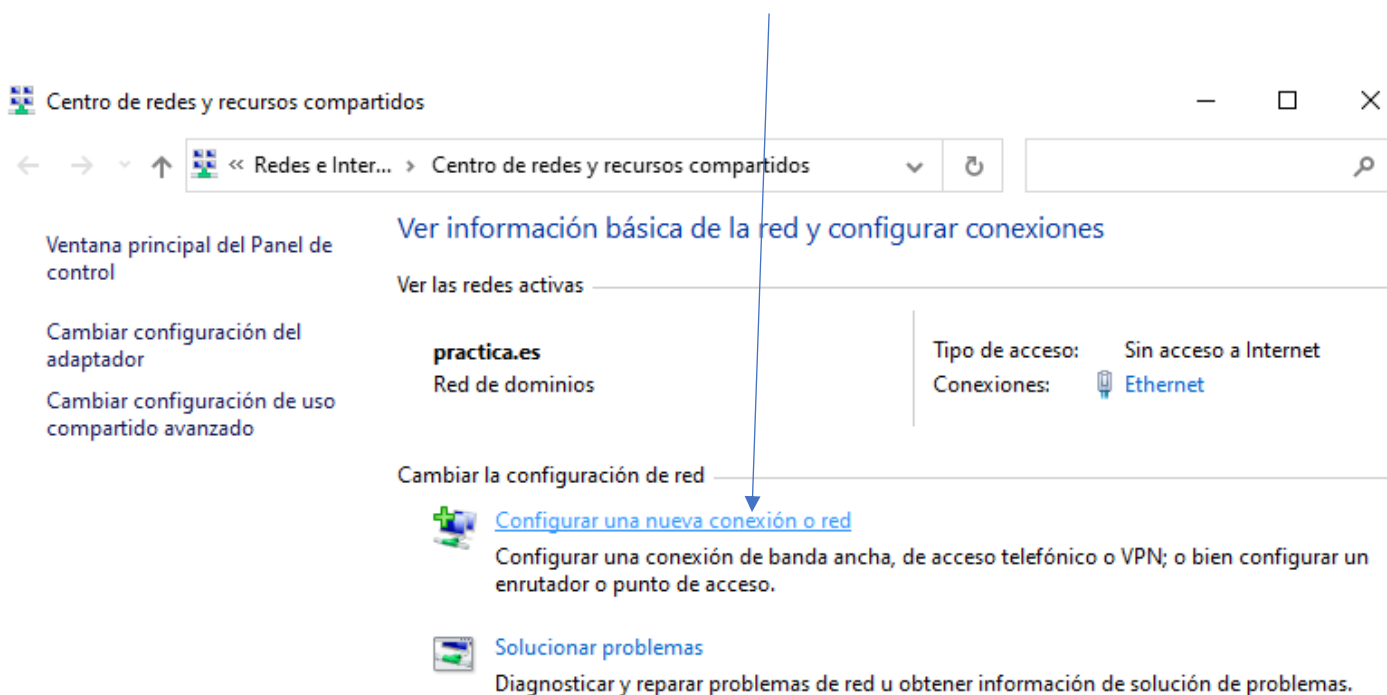


Posteriormente nos dirigiremos al centro de recursos compartidos.

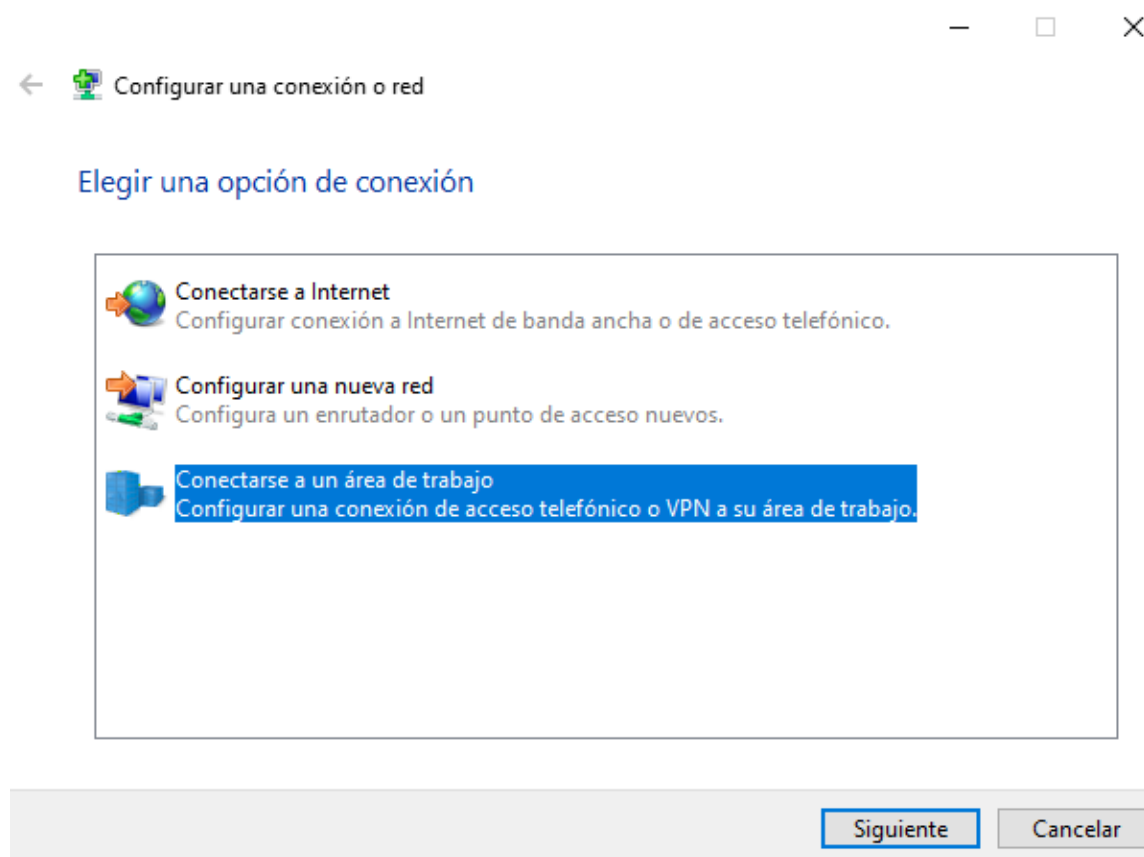
Hay varias vías, pero podemos acceder por ejemplo: Configuración→Red e Internet→Estado→Centro de Redes y Recursos compartidos.



Ahora seleccionamos la opción de configurar una nueva conexión o red.

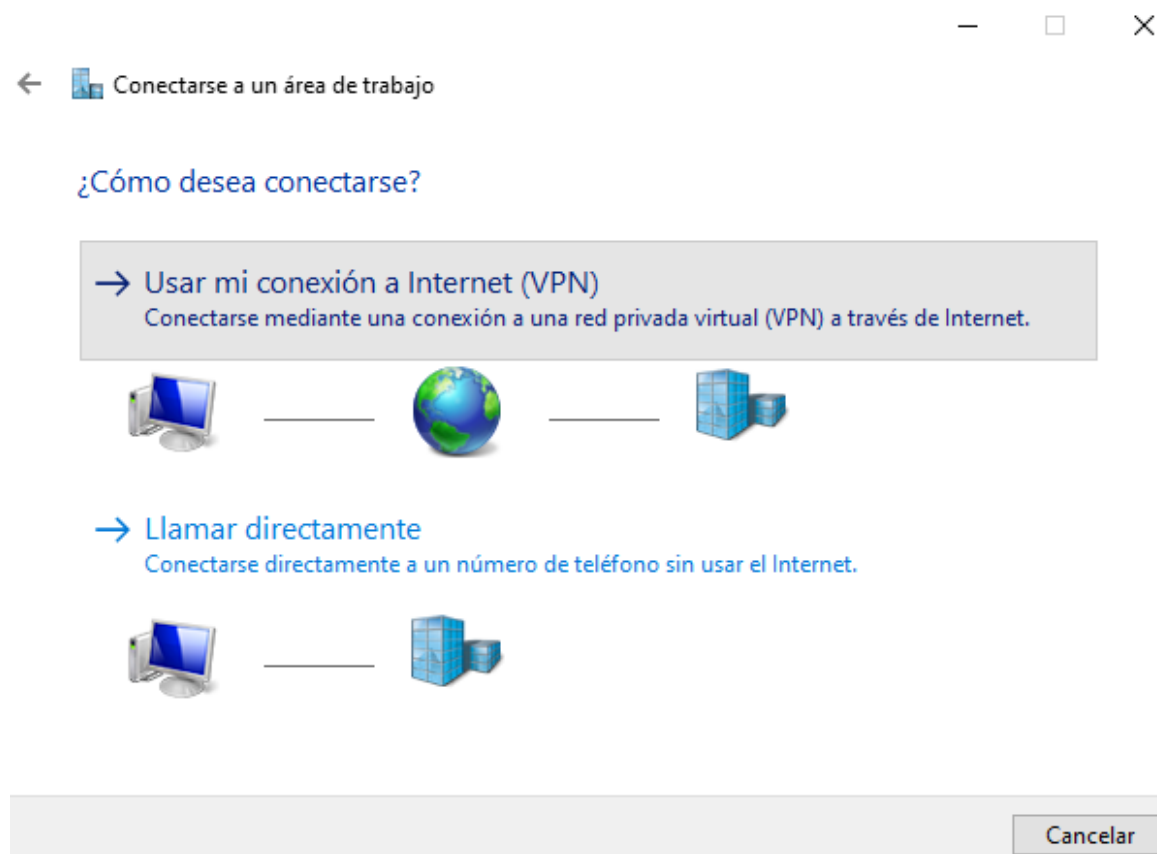


Se nos abrirá una ventana donde seleccionaremos la opción de conectarse a un área de trabajo.




Ahora se nos pregunta que método de conexión queremos utilizar.

En nuestro caso escogeremos Usar mi conexión (VPN).



Debemos introducir la dirección IP de la red externa (adaptador puente) del servidor. Además le estableceremos un nombre a la VPN.

←  Conectarse a un área de trabajo

Escriba la dirección de Internet a la que se conectará

El administrador de red puede darle esta dirección.

Dirección de Internet:

192.168.1.51

Nombre de destino:

practicaVPN

☐ Usar una tarjeta inteligente

☒ Recordar mis credenciales

☐ Permitir que otras personas usen esta conexión

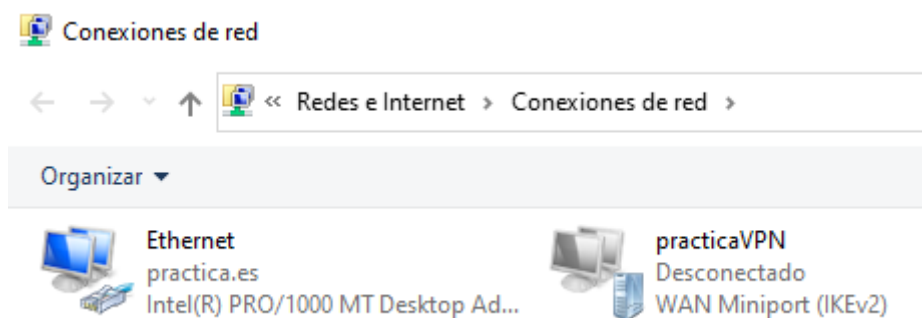
Esta opción permite el uso de esta conexión para cualquier persona con acceso a este equipo.

Crear

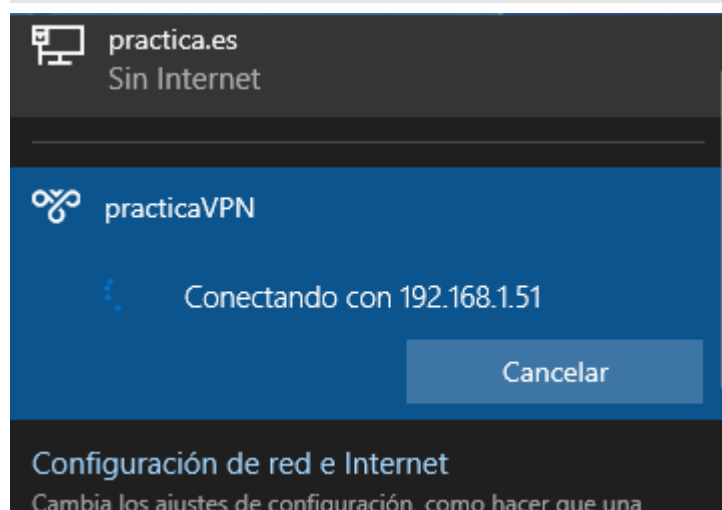
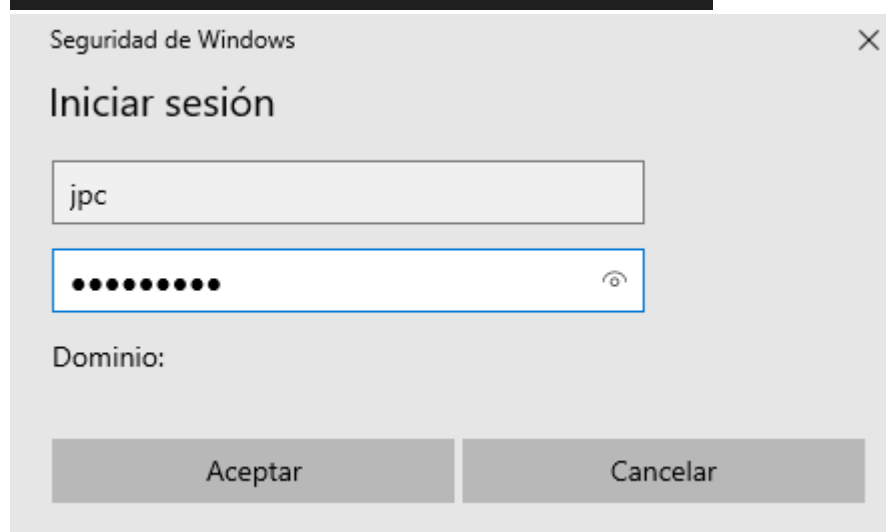
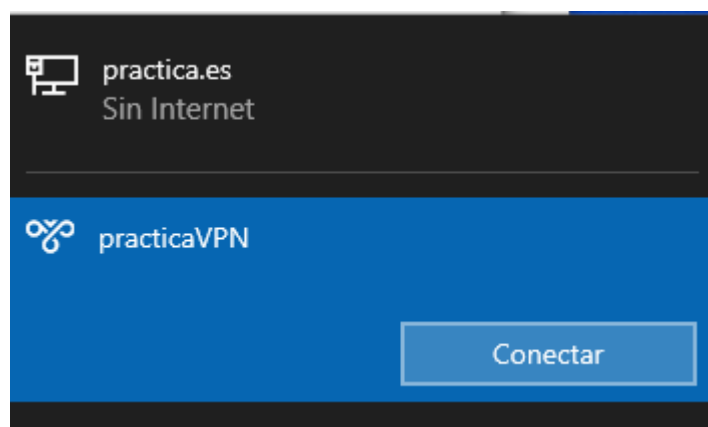
Cancelar

Una vez creada la VPN debemos acceder a la configuración de los adaptadores.

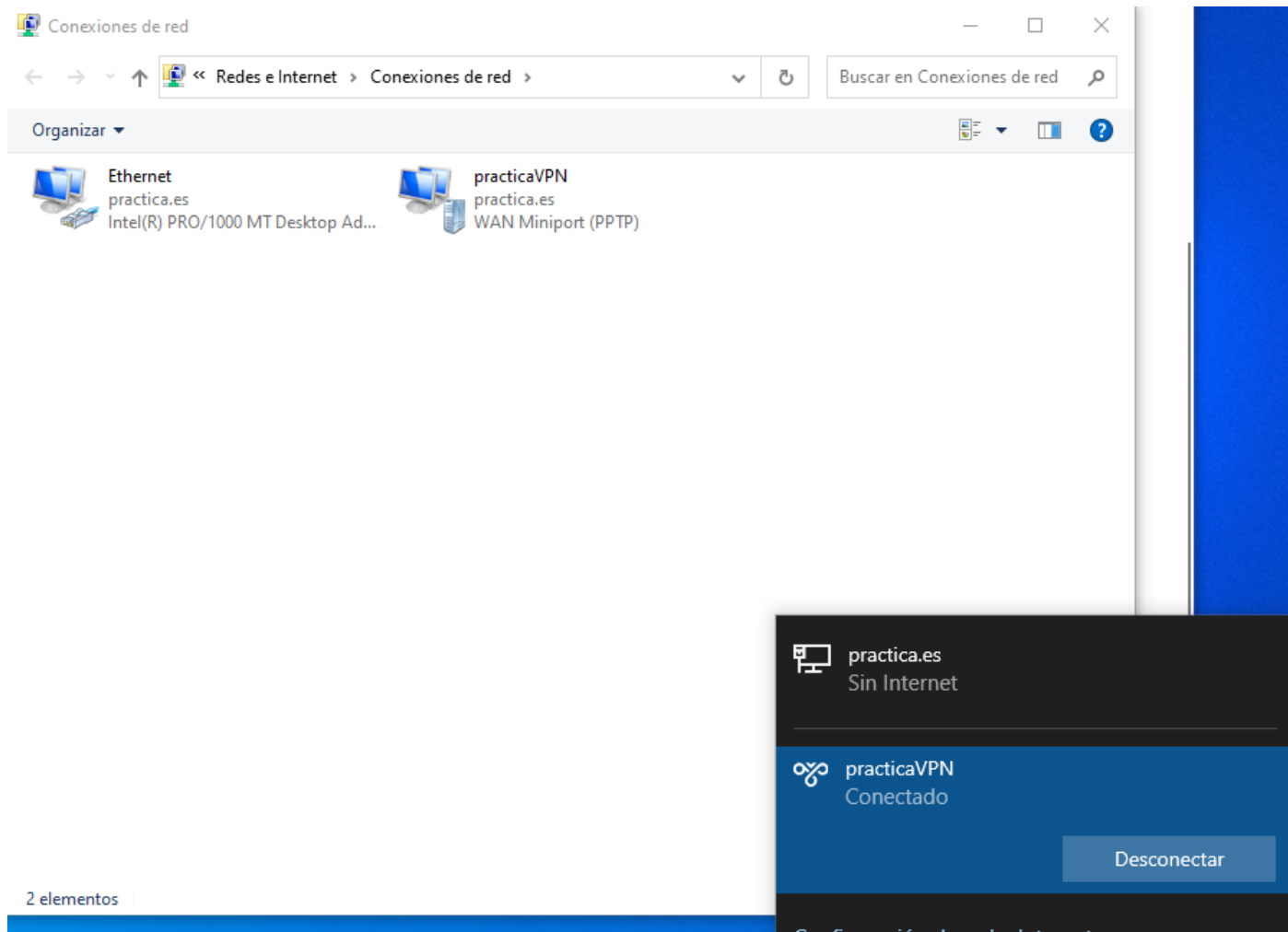
Allí nos aparecerá nuestra VPN pero en estado desconectado.



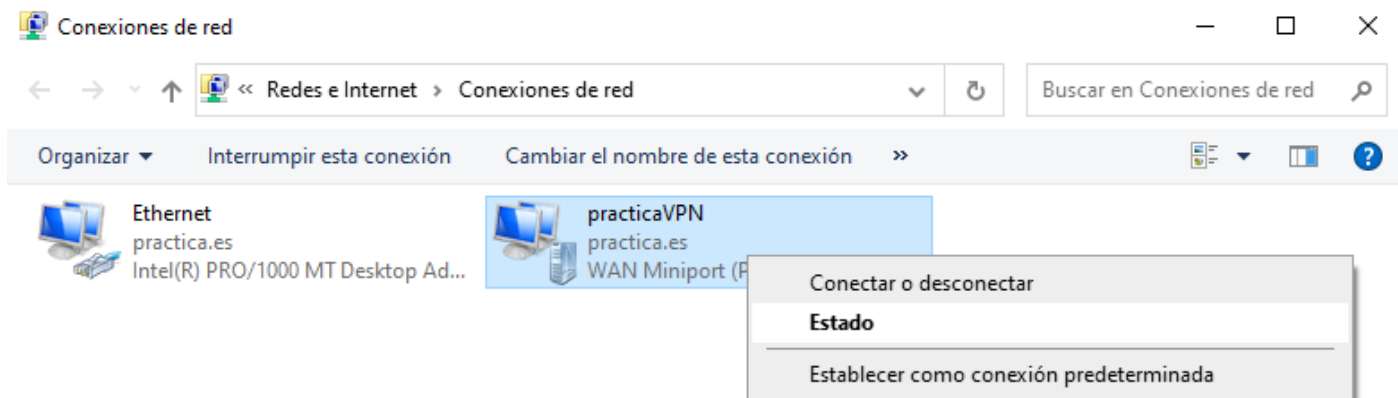
Para solucionarlo debemos acceder en la barra de tareas al icono de redes y clicar en nuestra VPN.  
Allí se nos pedirán unos credenciales los cuales son los del usuario que hemos creado anteriormente.



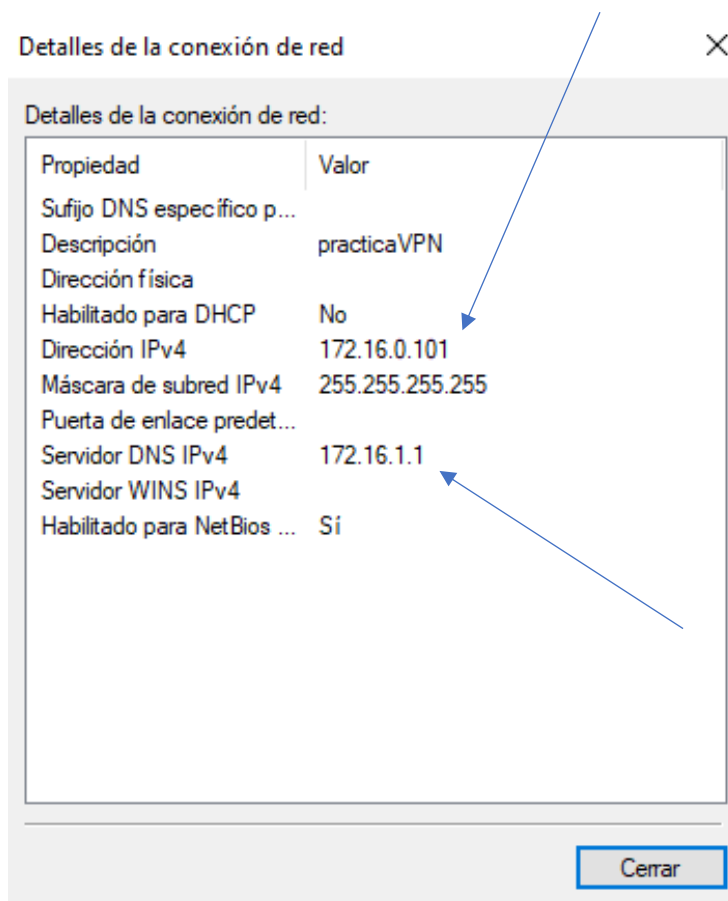
Ya se nos ha conectado como podemos observar.



Ahora comprobaremos si nos ha dado una de las IPs estáticas que hemos establecido en el rango.  
Para ello en las configuraciones de adaptadores clicamos con el botón derecho sobre nuestra VPN.  
Y seleccionamos Estado.



Como podemos observar Nos ha repartido una IP dentro del rango por lo que ha funcionado correctamente.



Además, podremos observar que la dirección IPv4 es distinta a la del servidor DNS.

```
C:\Users\jpc>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::10dc:e5a3:93e:5e0d%14
    Dirección IPv4. . . . . : 172.16.1.2
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 172.16.1.1

Adaptador PPP practicaVPN:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 172.16.0.101
    Máscara de subred . . . . . : 255.255.255.255
    Puerta de enlace predeterminada . . . . . : 0.0.0.0

C:\Users\jpc>ping 172.16.1.1

Haciendo ping a 172.16.1.1 con 32 bytes de datos:
Respuesta desde 172.16.1.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.1.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.1.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.1.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 172.16.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\jpc>
```

Hemos realizado un ping para demostrar que la conexión es real y estable.

