

Índice:

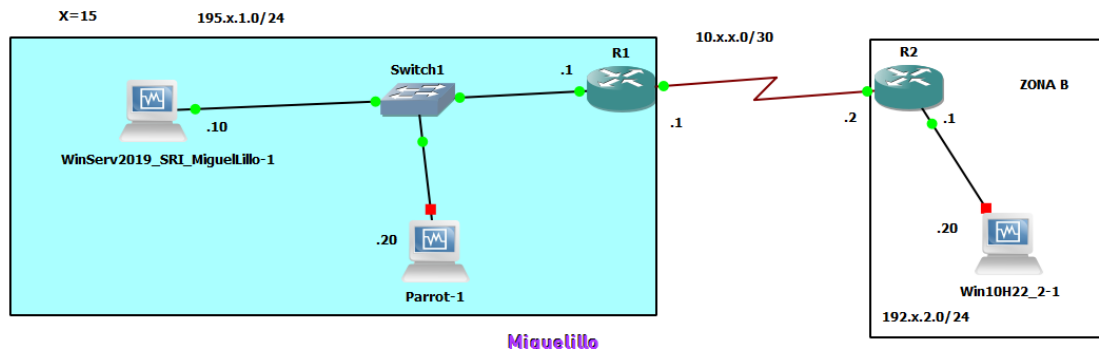
Ejercicio 1	2
a) Protocolo L2TP/IPSEC. Instalación de un servidor VPN en Windows. Acceso desde cliente VPN.....	2

Ejercicio 1

a) Protocolo L2TP/IPSEC. Instalación de un servidor VPN en Windows. Acceso desde cliente VPN.

Solución:

Escenario



Primero configuramos los enrutamientos entre redes y colocamos un NAT con un renvío de puertos, renviaremos los puertos 1701, 500 y 4500 UDP

Configuración **R1**

```

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#router eigrp 1
R1(config-router)#network 195.15.1.0 0.0.0.255
R1(config-router)#network 10.15.15.0 0.0.0.3
R1(config-router)#
R1(config-router)#interface FastEthernet0/0
R1(config-if)#ip address 195.15.1.1 255.255.255.0
R1(config-if)#ip nat inside

R1(config-if)#interface Serial1/0
R1(config-if)#ip address 10.15.15.1 255.255.255.252
R1(config-if)#ip nat outside
R1(config-if)#no shutdown

R1(config)#ip access-list standard ACL_INSIDE_OUT
R1(config-std-nacl)#permit 195.15.1.0 0.0.0.255
R1(config-std-nacl)#exit
R1(config)#ip nat inside source list ACL_INSIDE_OUT interface Se1/0 overload
R1(config)#$de source static udp 195.15.1.10 1701 10.15.15.1 1701 extendable
R1(config)#$de source static udp 195.15.1.10 500 10.15.15.1 500 extendable
R1(config)#$de source static udp 195.15.1.10 4500 10.15.15.1 4500 extendable
R1(config)#
  
```

Configuración R2

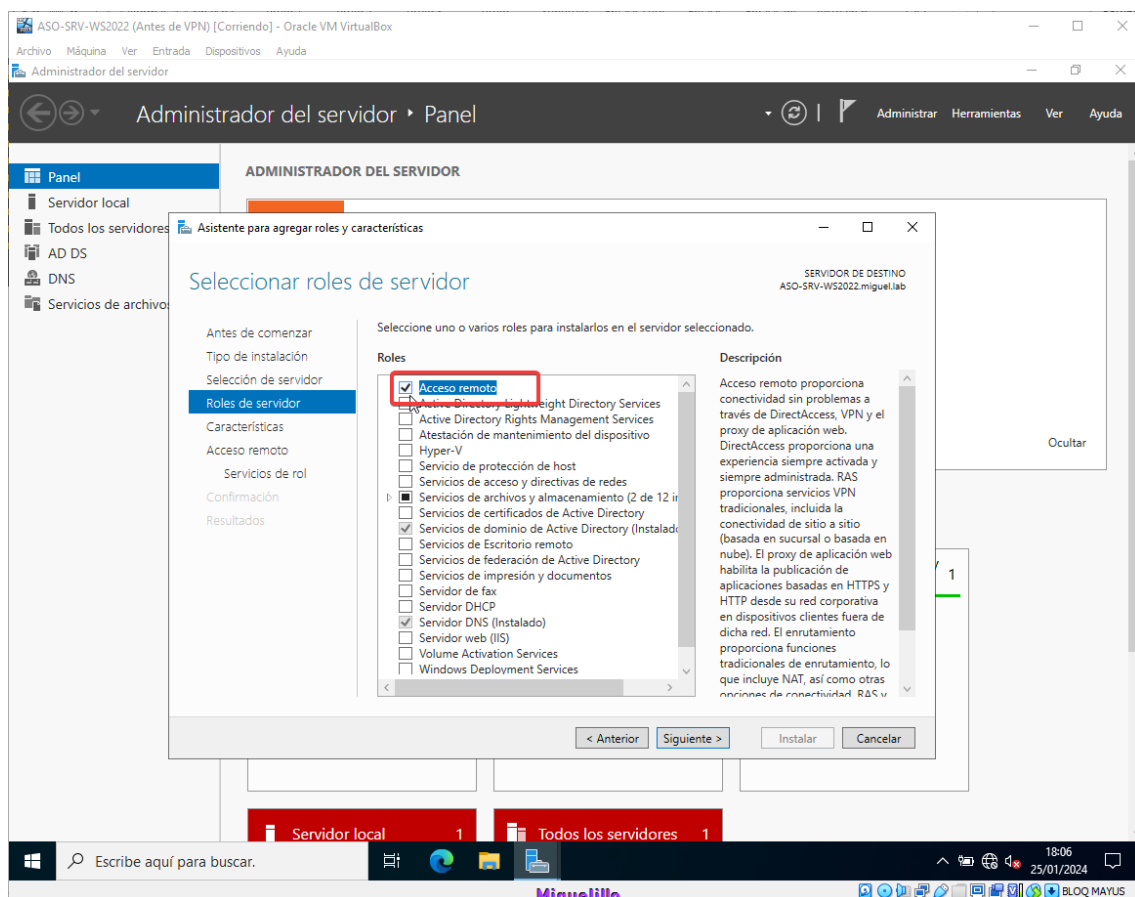
```

R2
R2(config)#router eigrp 1
R2(config-router)#network 192.15.2.0 0.0.0.255
R2(config-router)#network 10.15.15.0 0.0.0.3
R2(config-router)#
R2(config-router)#interface FastEthernet0/0
R2(config-if)#ip address 192.15.2.2 255.255.255.0
R2(config-if)#ip nat inside

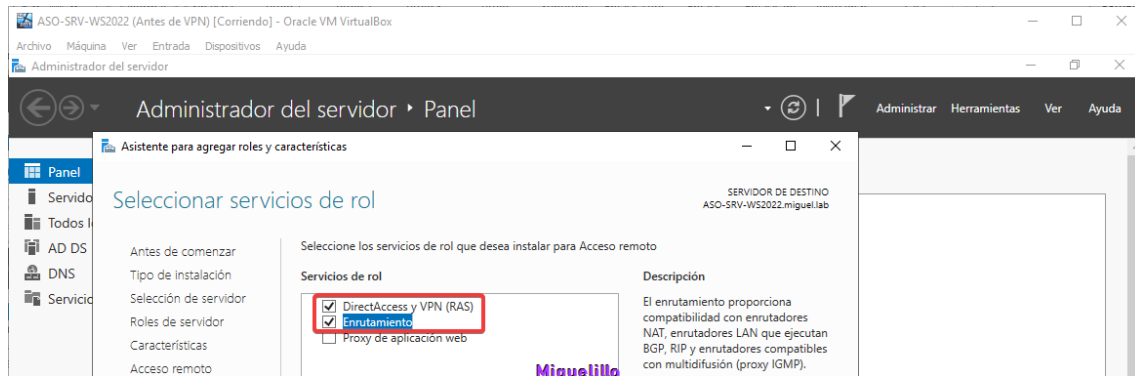
R2(config-if)#no shutdown
R2(config-if)#
R2(config-if)#interface Serial1/0
R2(config-if)#ip address 10.15.15.2 255.255.255.252
R2(config-if)#ip nat outside
R2(config-if)#no shutdown
R2(config-if)#
R2(config-if)#exit
R2(config)#ip access-list standard ACL_INSIDE_OUT
R2(config-std-nacl)#permit 192.15.2.0 0.0.0.255
R2(config-std-nacl)#exit
R2(config)#ip nat inside source list ACL_INSIDE_OUT interface Se1/0 overload
*Mar 1 01:06:51.251: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:06:51.331: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

```

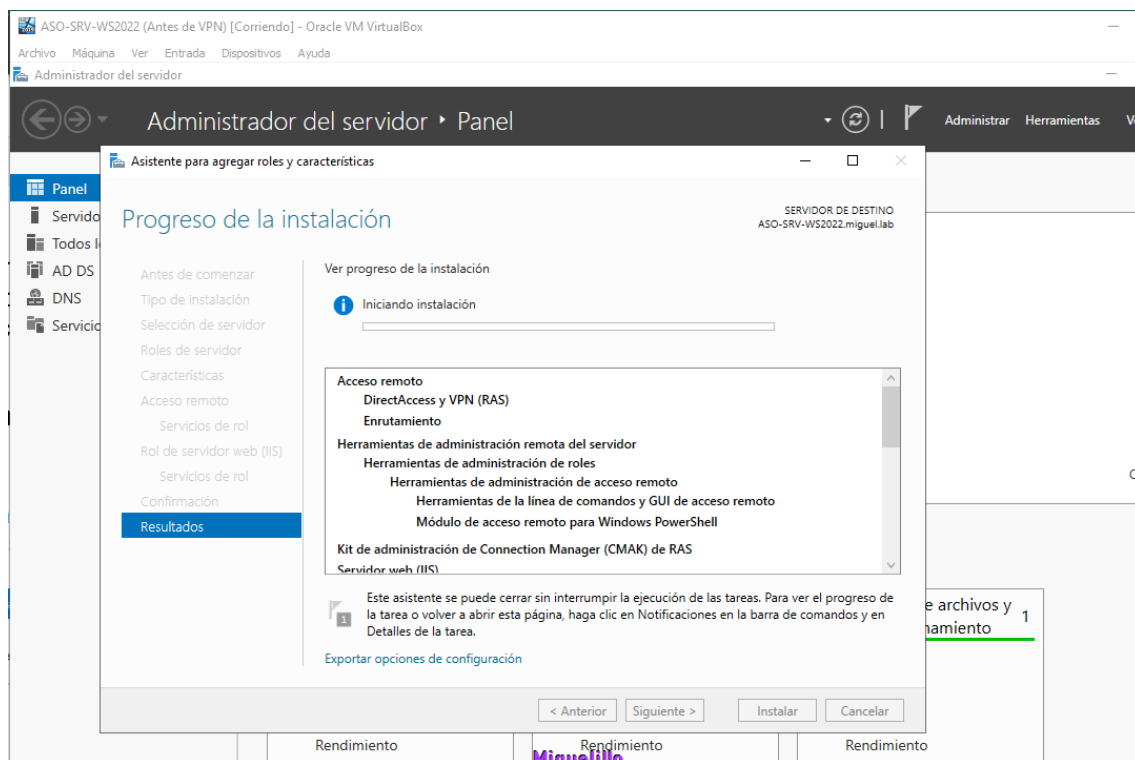
En el servidor vamos a **Administrar** → **Agregar Roles y Características** → **Agregamos el Rol de Acceso Remoto**



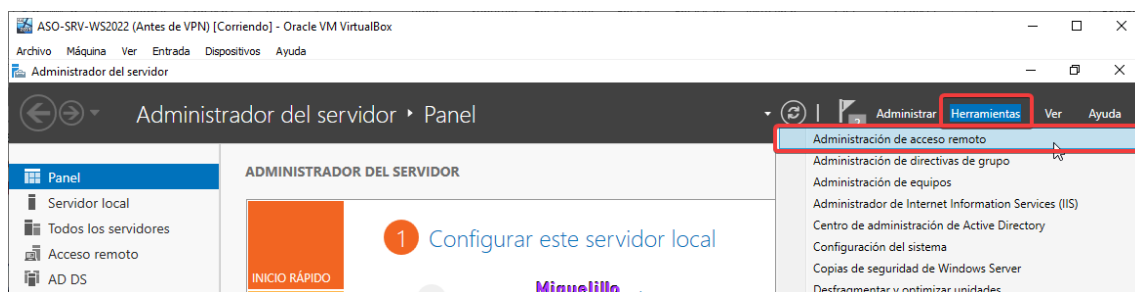
Seleccionamos los servicios del rol



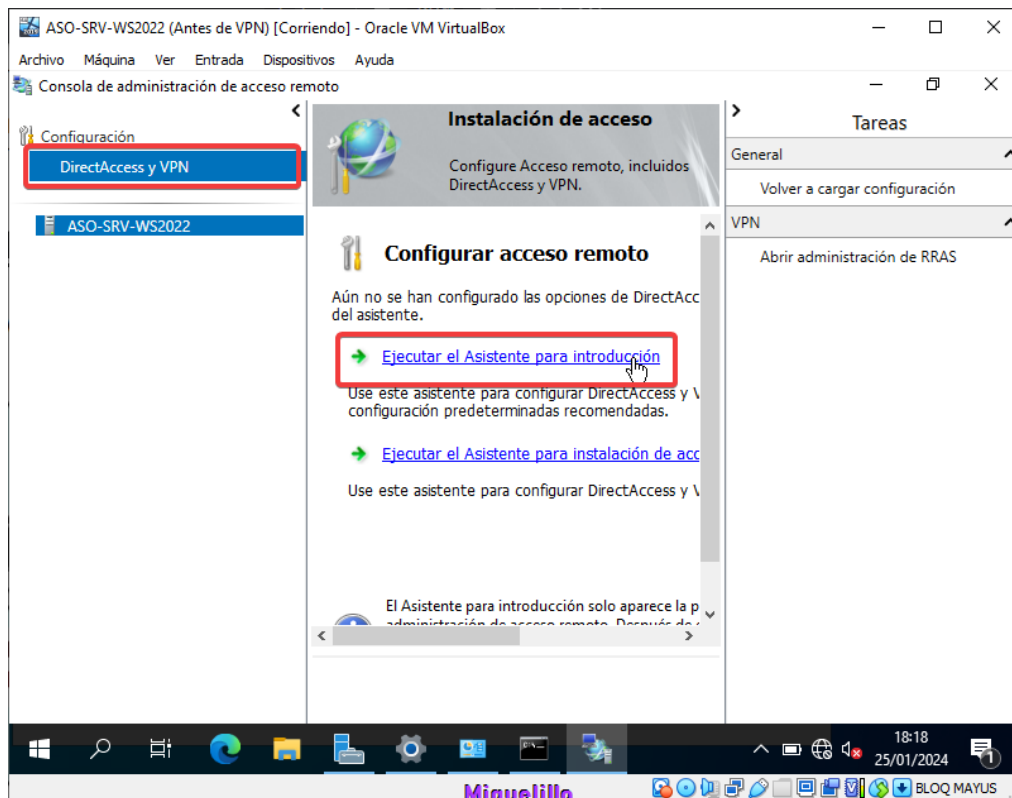
Esperamos a que se instale



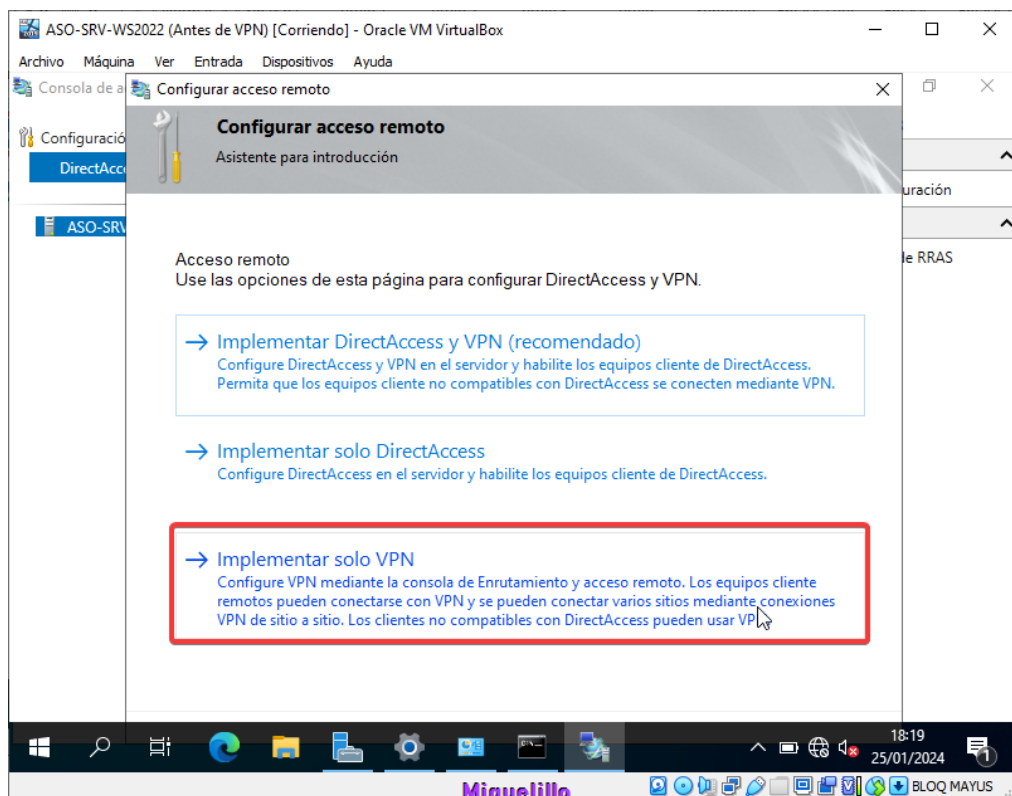
Vamos a Herramientas → Administración de acceso remoto



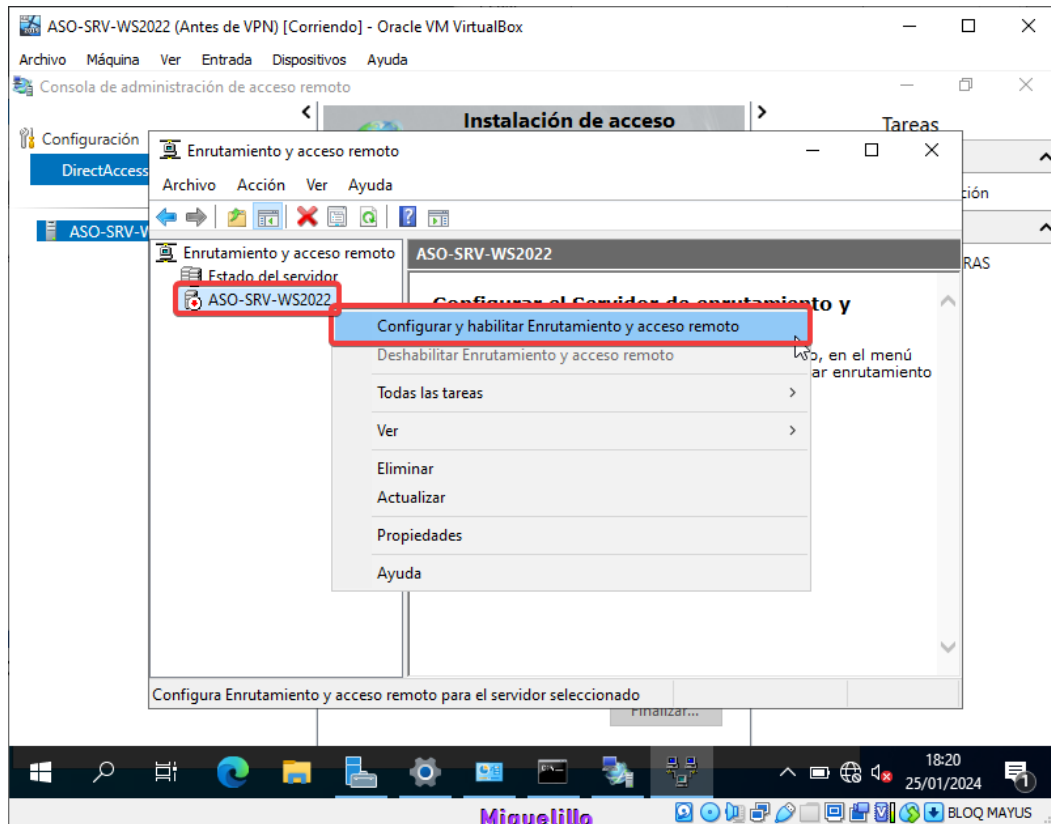
Vamos a DirectAccess y VPN → Ejecutamos el Asistente para introducción



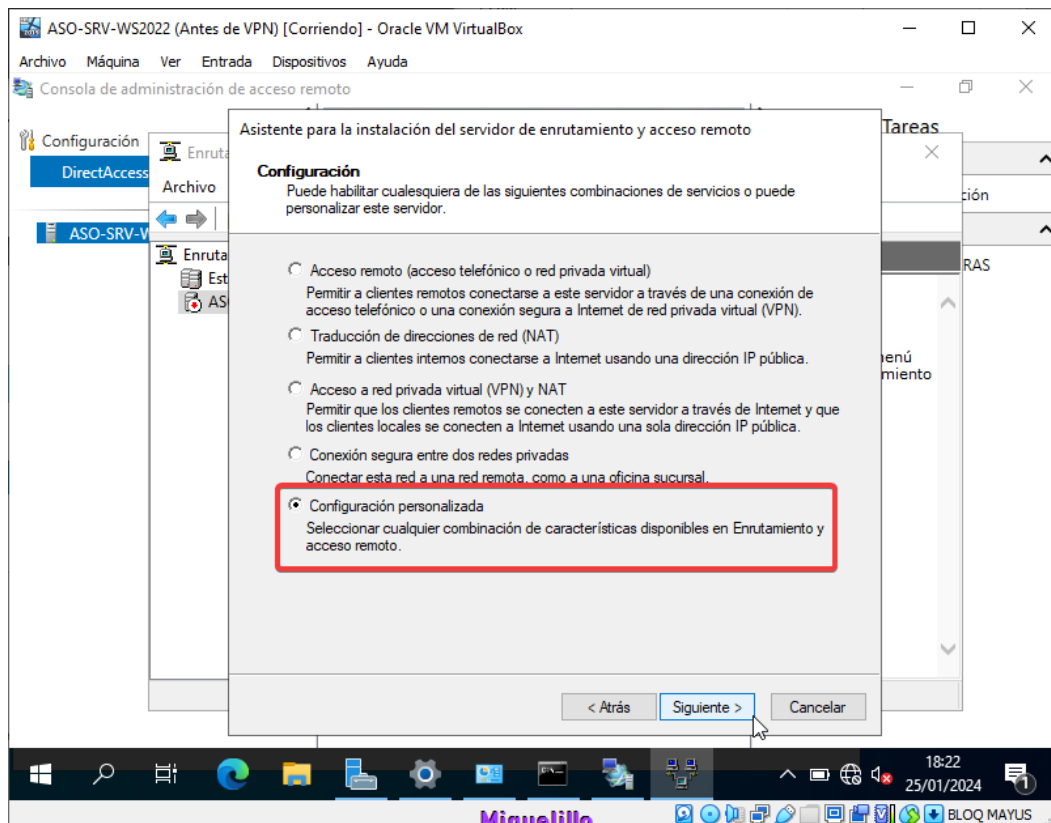
Implementamos solo VPN



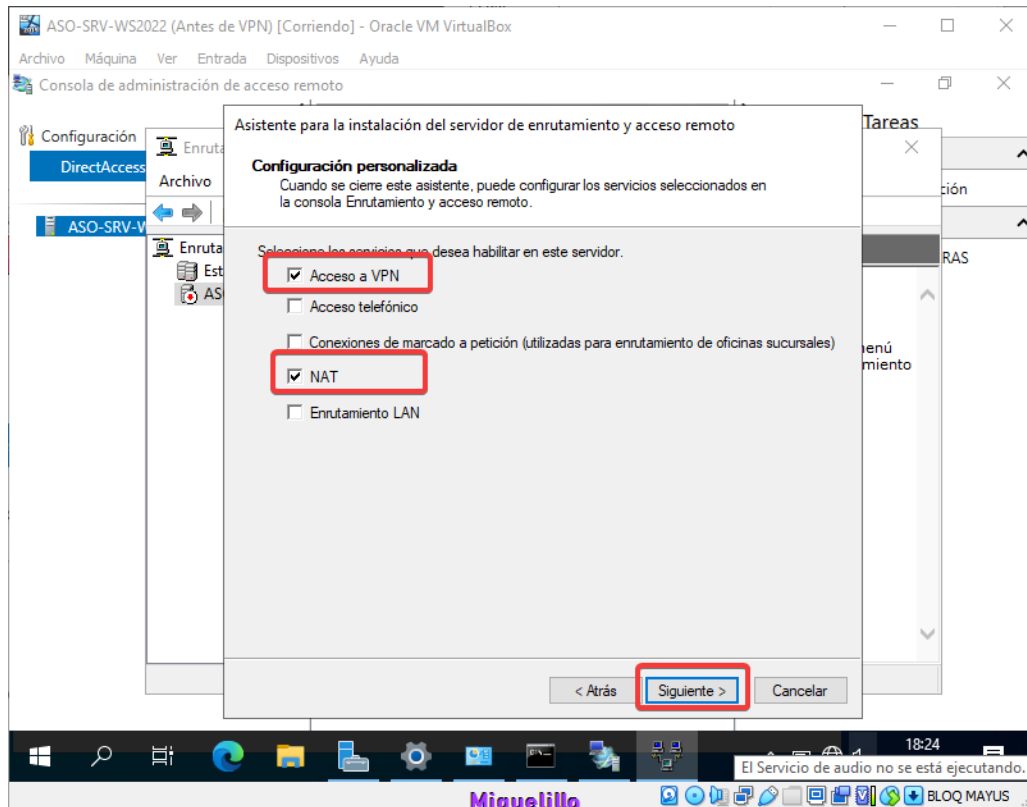
Hacemos clic derecho en el servidor y clicamos en **Configurar y habilitar Enrutamiento y acceso remoto**.



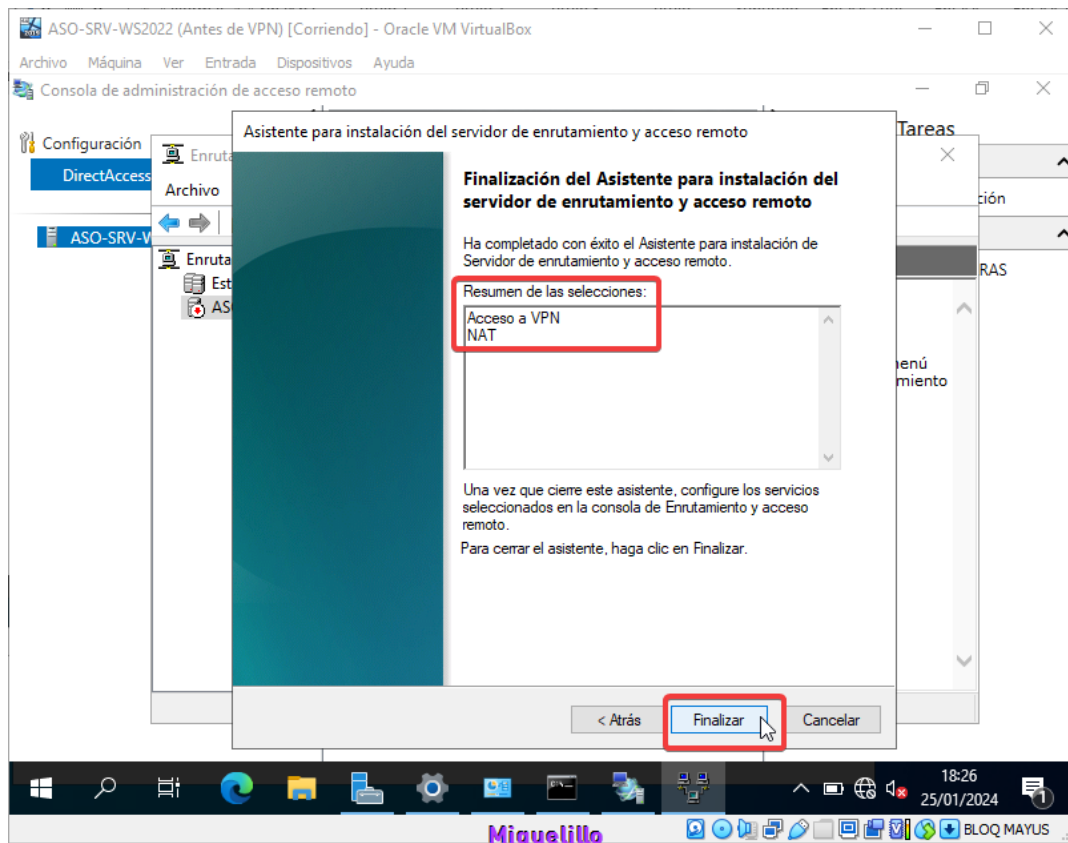
Clicamos en **Configuración personalizada**



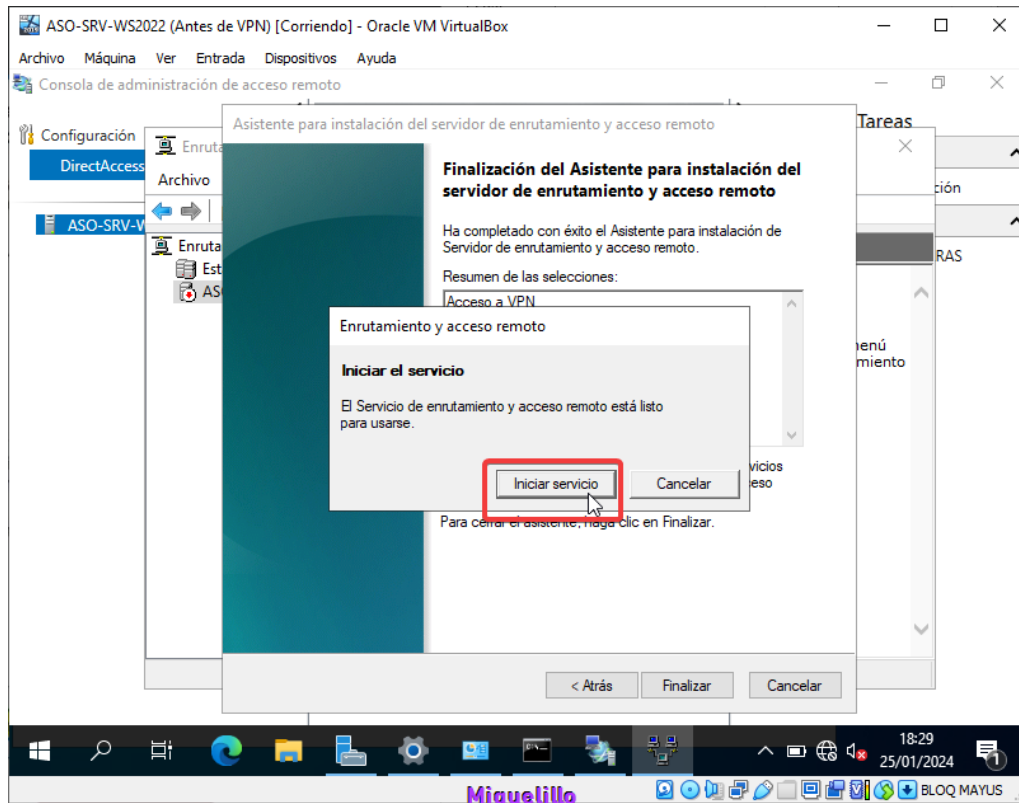
Seleccionamos NAT y Acceso VPN



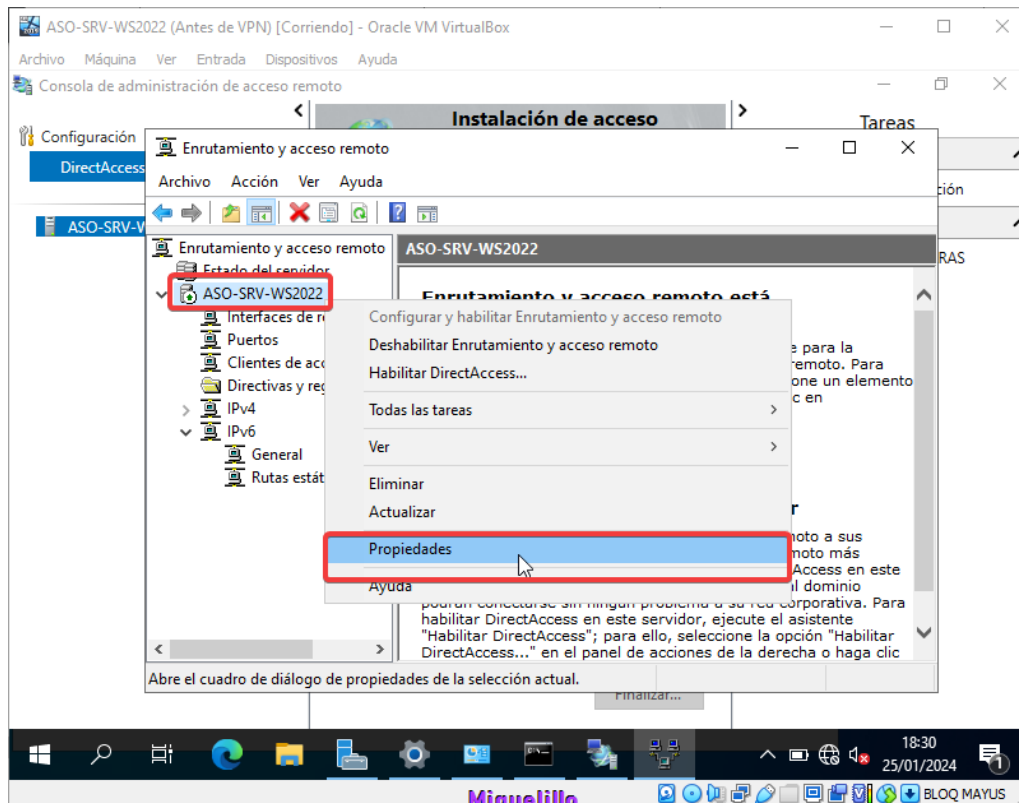
Vemos la configuración y clicamos en Finalizar



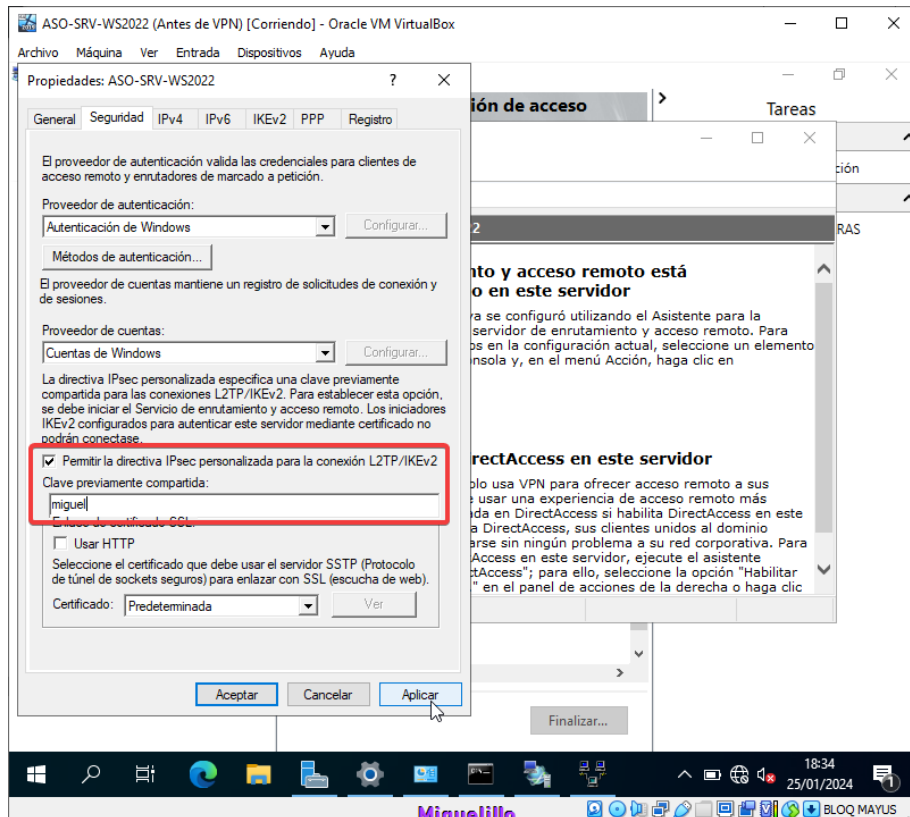
Clicamos en Iniciar el Servicio



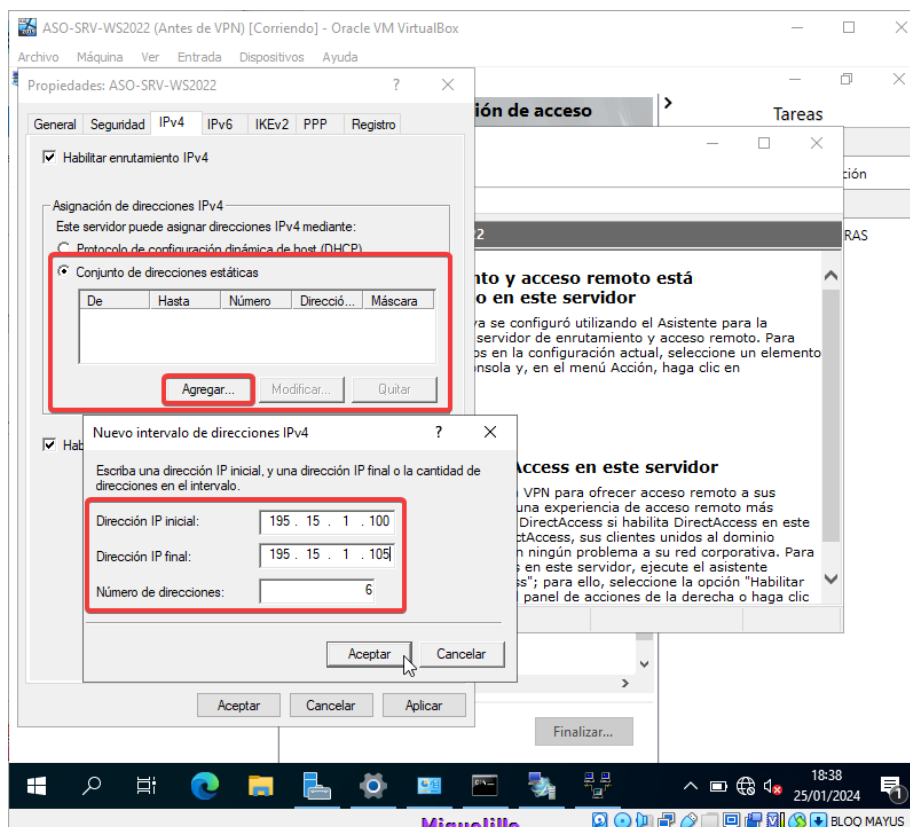
Hacemos clic derecho en el servidor Propiedades



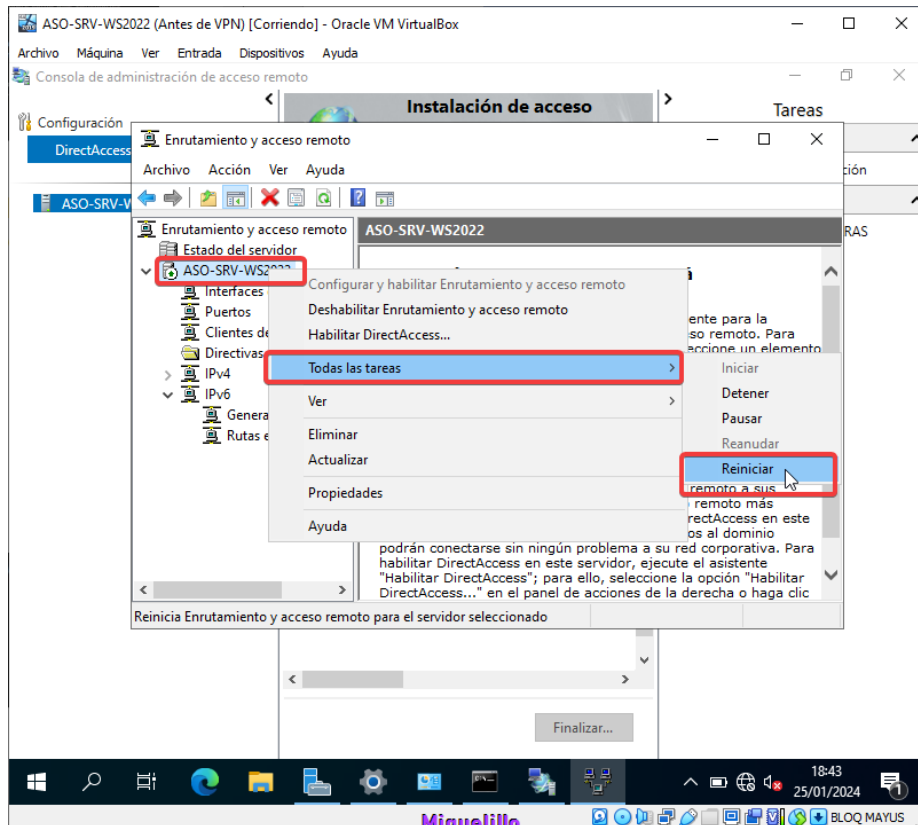
Vamos a **Seguridad** y habilitamos L2TP/IKEv2 y configuramos una clave precompartida



Vamos a IPv4 le asignamos un rango y aplicamos

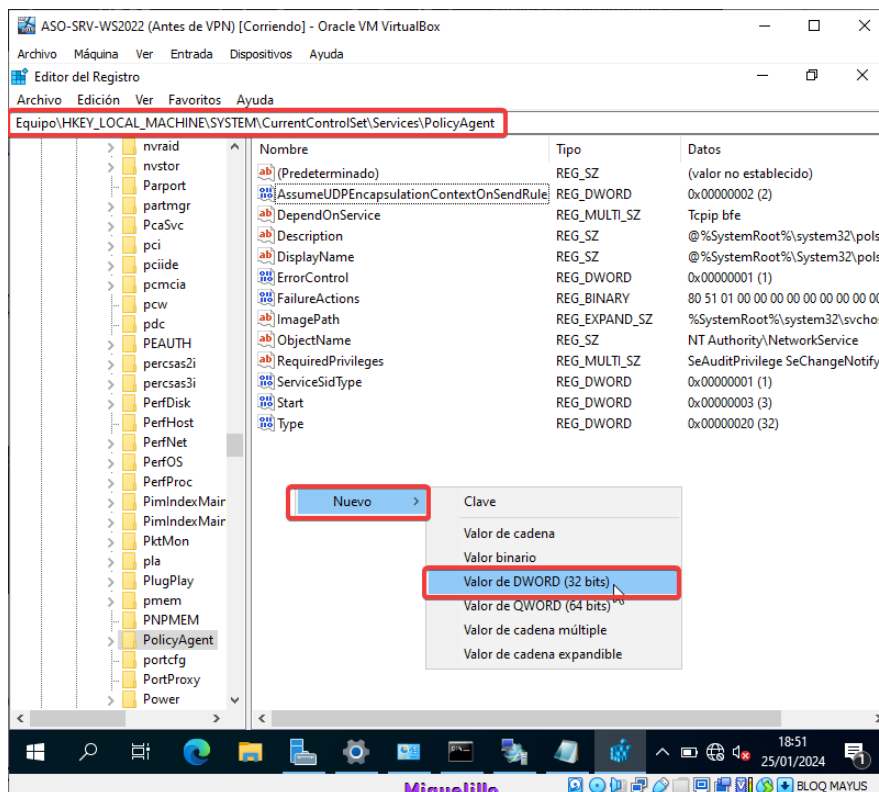


Reiniciamos el servidor

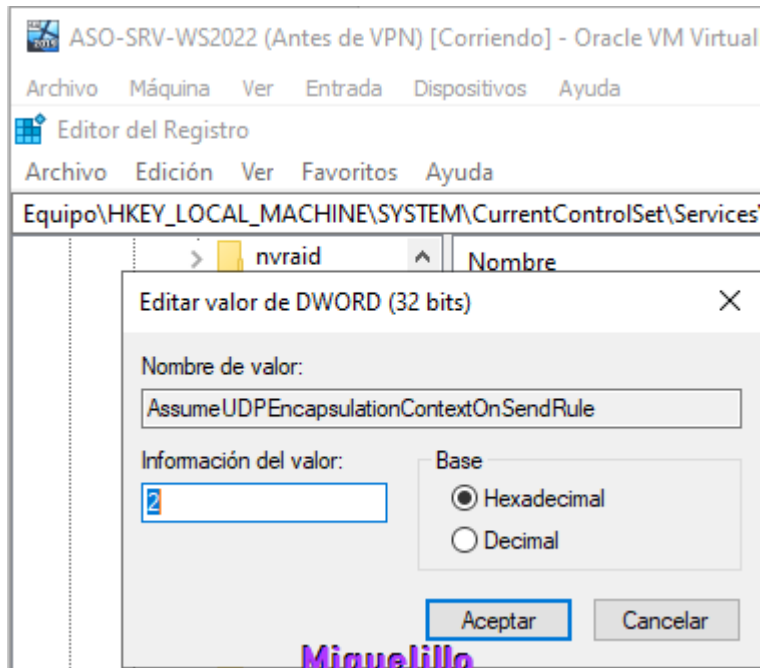


Vamos al Editor del Registro →

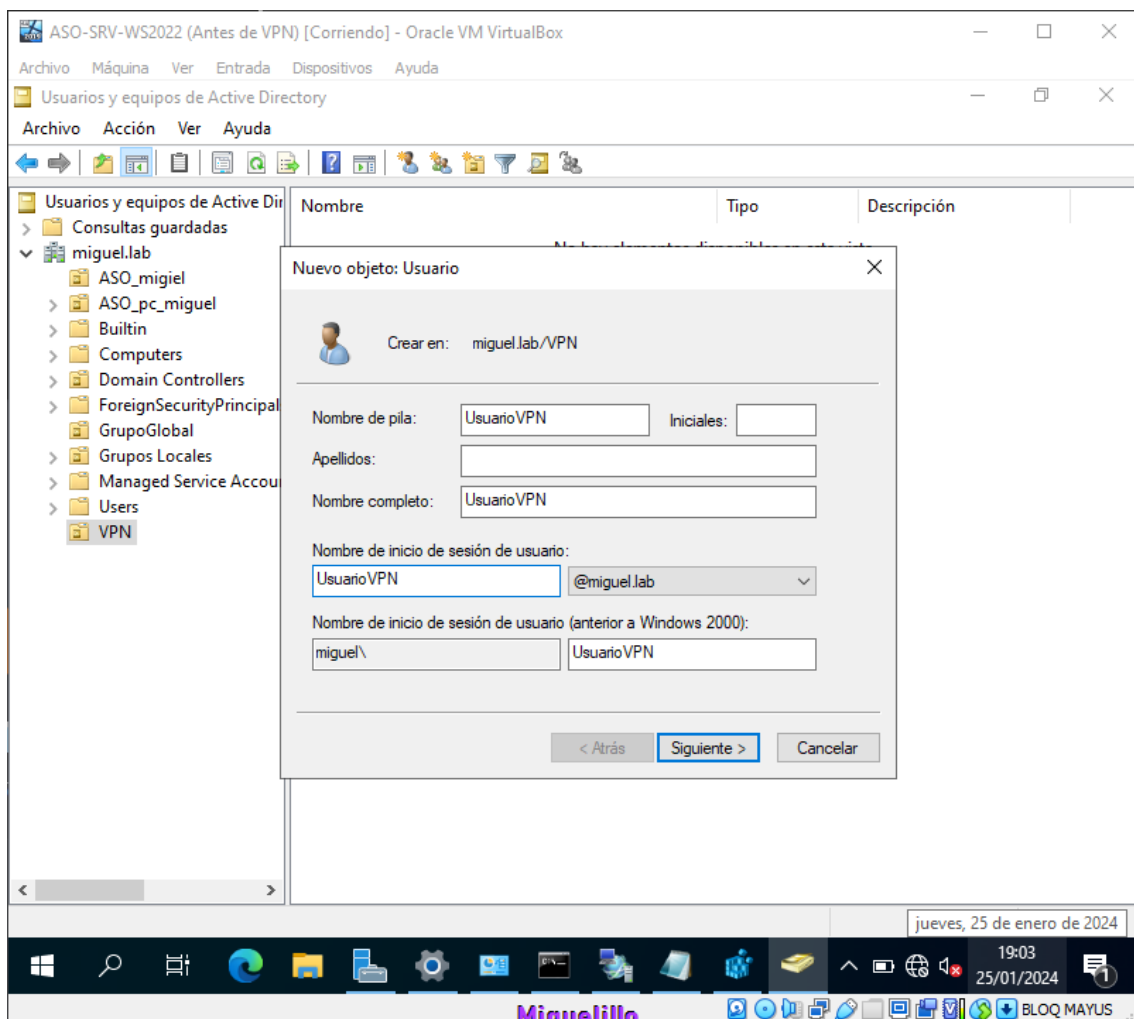
Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent y creamos un Valor DWORD (32 bits)



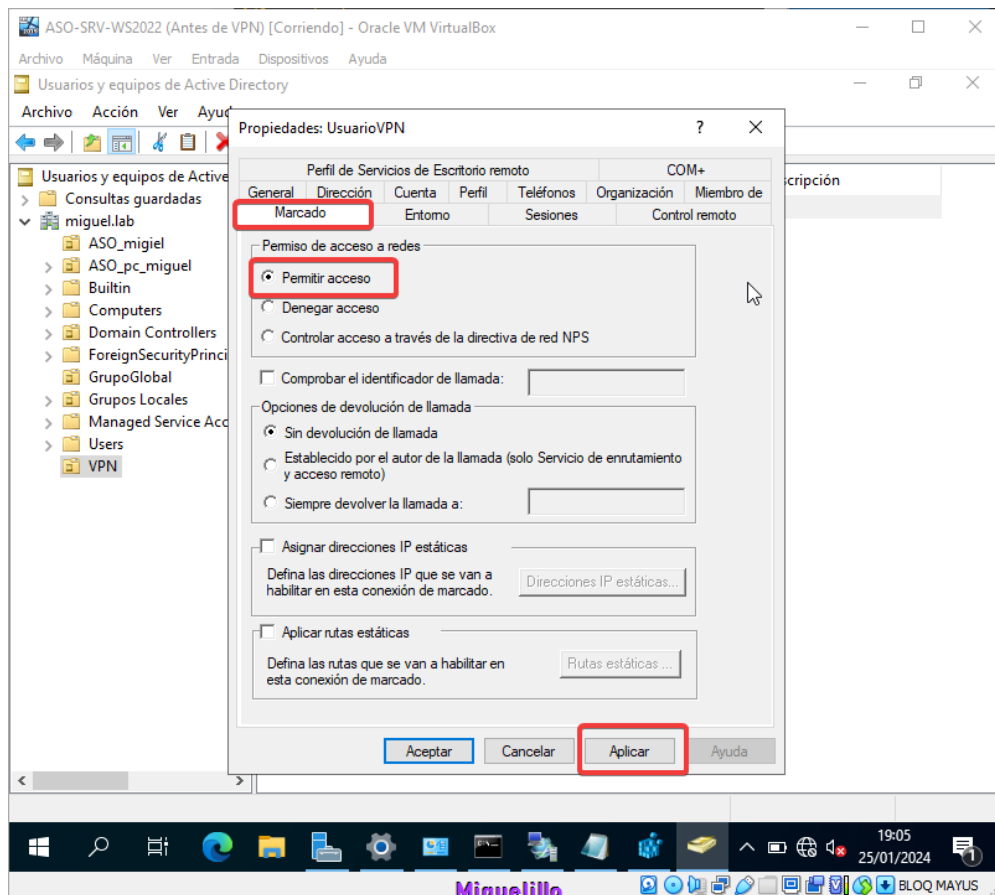
Con esta configuración



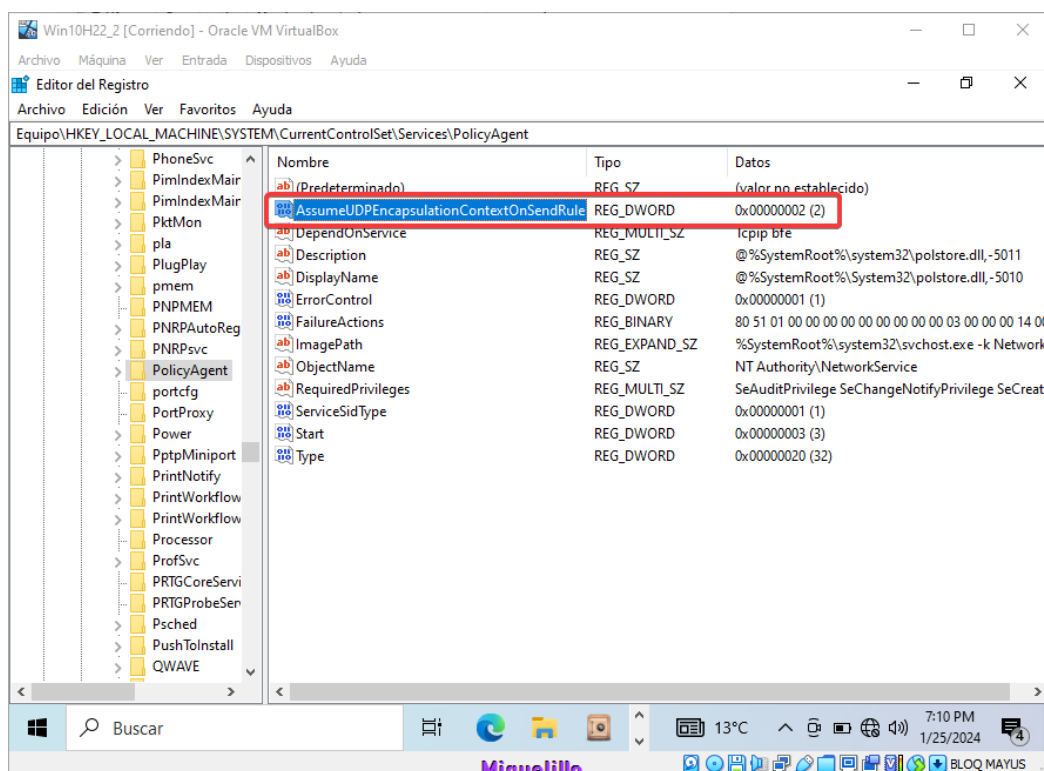
Vamos a **Ususaior y Equipos de Active Directory** y creamos un usuario.



Clicamos en propiedades del usuario **Marcado** → **Permitir acceso** → **Aplicar**



Vamos al cliente y hacemos el registro como el servidor haciendo el editro de registro



```

R1(config)#
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
*Mar 1 00:04:42.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1(config)#
*Mar 1 00:04:56.219: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.15.15.2 (Serial1/0) is up: new adjacency
R1(config)#
*Mar 1 00:05:02.455: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.15.15.2 (Serial1/0) is down: Interface Goodbye received
R1(config)#
*Mar 1 00:05:05.287: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.15.15.2 (Serial1/0) is up: new adjacency
R1(config)#
*Mar 1 00:11:07.491: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.15.15.2 (Serial1/0) is down: holding time expired
R1(config)#
*Mar 1 00:11:22.703: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
R1(config)#
*Mar 1 00:13:22.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1(config)#
*Mar 1 00:13:23.723: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.15.15.2 (Serial1/0) is up: new adjacency
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#exit
R1#
R1#
*Mar 1 00:17:23.715: %SYS-5-CONFIG_I: Configured from console by console
R1#sh
R1#show ip
R1#show ip nat
R1#show ip nat tra
R1#show ip nat translations

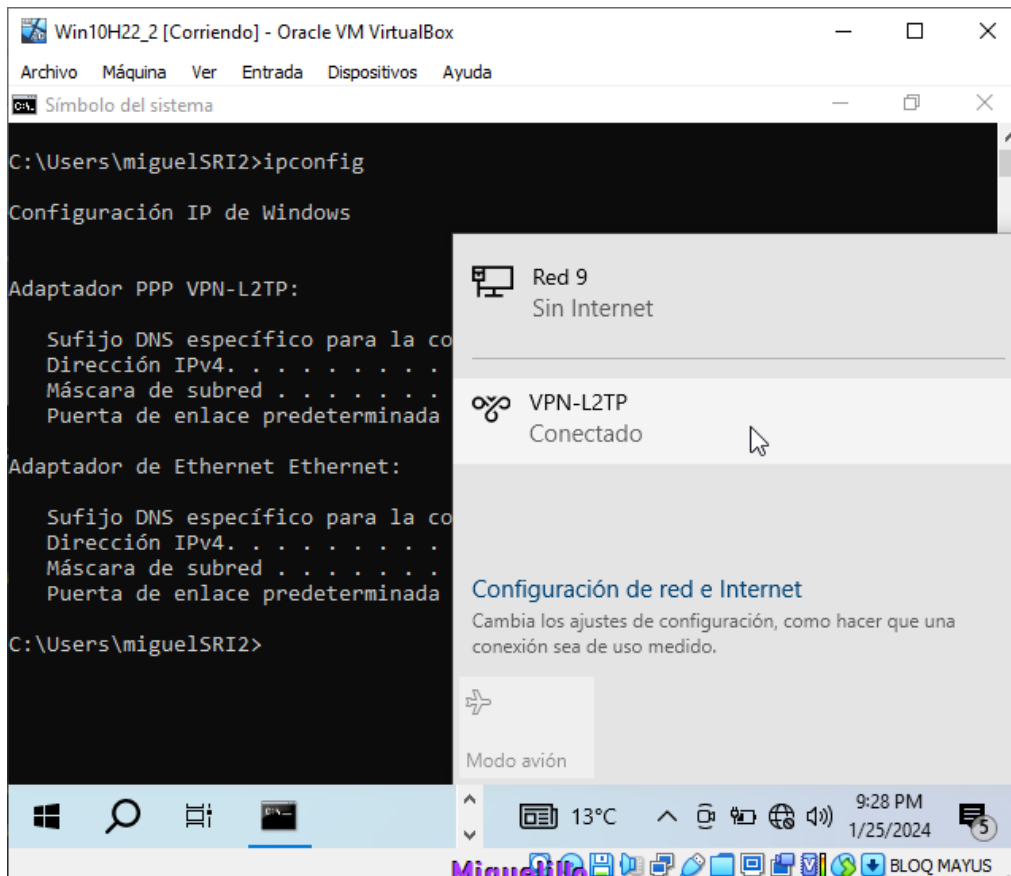
```

Pro	Inside global	Inside local	Outside local	Outside global
udp	10.15.15.1:500	195.15.1.10:500	10.15.15.2:500	10.15.15.2:500
udp	10.15.15.1:500	195.15.1.10:500	---	---
udp	10.15.15.1:1701	195.15.1.10:1701	---	---
udp	10.15.15.1:4500	195.15.1.10:4500	10.15.15.2:4500	10.15.15.2:4500
udp	10.15.15.1:4500	195.15.1.10:4500	---	---

R1#

solarwinds | Solar-PuTTY free tool Miguelillo © 2019-2023 SolarWinds Worldwide, LLC. All rights reserved.

Probamos a conectar



Hacemos un ipconfig y vemos que nos da la Ip correspondiente, y hacemos una prueba de conectividad

```

Win10H22_2 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

C:\Users\miguelSRI2>ipconfig

Configuración IP de Windows

Adaptador PPP VPN-L2TP:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.15.2.101
    Máscara de subred . . . . . : 255.255.255.255
    Puerta de enlace predeterminada . . . . . : 0.0.0.0

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.15.2.10
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.15.2.1

C:\Users\miguelSRI2>ping 195.15.1.10

Haciendo ping a 195.15.1.10 con 32 bytes de datos:
Respuesta desde 195.15.1.10: bytes=32 tiempo=22ms TTL=127
Respuesta desde 195.15.1.10: bytes=32 tiempo=27ms TTL=127
  
```

Miramos los paquetes

Capturando desde - [R1 Serial1/0 to R2 Serial1/0]

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplice un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
43	15.079798	10.15.15.1	10.15.15.2	ISAKMP	260	Identity Protection (Main Mode)
44	15.092721	10.15.15.2	10.15.15.1	ISAKMP	112	Identity Protection (Main Mode)
45	15.110729	10.15.15.1	10.15.15.2	ISAKMP	112	Identity Protection (Main Mode)

> Frame 46: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0

> Cisco HDLC

> Internet Protocol Version 4, Src: 10.15.15.2, Dst: 10.15.15.1

> User Datagram Protocol, Src Port: 4500, Dst Port: 4500

> UDP Encapsulation of IPsec Packets

> Internet Security Association and Key Management Protocol

Initiator SPI: 364f5207c0851887

Responder SPI: 8a5917bbd2425b56

Next payload: Hash (8)

> Version: 1.0

> Exchange type: Quick Mode (32)

> Flags: 0x01

Message ID: 0x00000001

Length: 444

Encrypted Data (416 bytes)