

VPN Windows Server 2016

Práctica 05 SAD y SRI
Gonzalo Tudela Chavero

ÍNDICE DE CONTENIDOS

EUNCIADO	1
ESQUEMA DE RED	1
CREACIÓN DEL SERVIDOR.....	2
CERTIFICADOS	6
INSTALACION DEL SERVICIO VPN	15
PRUEBAS DE FUNCIONAMIENTO.....	17

ÍNDICE DE FIGURAS

Ilustración 1 - Esquema de red.....	1
Ilustración 2 - Roles o servicios instalados mediante Windows Essentials.....	2
Ilustración 3 - Configuración del adaptador que hará las veces de enlace a Internet.....	2
Ilustración 4 - Configuración del adaptador de la parte LAN.	3
Ilustración 5 - Restringir el servicio DNS al ámbito LAN.	3
Ilustración 6 - Configuración de reenviadores para el servicio DNS.....	4
Ilustración 7 - Instalación del servicio DHCP.	4
Ilustración 8 - Configuración de un intervalo de direcciones a servir en nuestro DHCP.	5
Ilustración 9 - El cliente recibe configuración mediante el servicio DHCP correctamente.....	5
Ilustración 10 - Comprobación de que el servicio DNS está funcionando.....	6
Ilustración 11 - Acceso a la ventana de autoridad de certificación.	6
Ilustración 12 - Elegimos una plantilla de certificado sobre la que vamos a crear el nuestro.....	7
Ilustración 13 - Pestaña manejo de solicitudes para la plantilla de certificado.....	7
Ilustración 14 - Pestaña extensiones en las propiedades de la plantilla.	8
Ilustración 15 - Agregando directiva de aplicación para Autenticación del Servidor.	8
Ilustración 16 - Modificación del uso de la clave para firma digital.	9
Ilustración 17 - Configuración de la pestaña seguridad en la plantilla.	9
Ilustración 18 - Agregamos la plantilla a plantillas de certificado.....	10
Ilustración 19 - Microsoft Management Console.....	10
Ilustración 20 - Asignando certificado al servicio VPN.	11
Ilustración 21 - Pasos para lo solicitud de un nuevo certificado.....	12
Ilustración 22 - Nuevo certificado en el equipo local.....	12
Ilustración 23 - Proceso de exportación del certificado.....	13
Ilustración 24 - Asistente para la exportación del certificado.	13
Ilustración 25 - Asistente para importar certificado.	14
Ilustración 26 - Importación del certificado de confianza con éxito.	14
Ilustración 27 - Agregando Roles para VPN.	15
Ilustración 28 - Inicio del asistente para configuración de enrutamiento y acceso remoto.	15
Ilustración 29 - Instalamos el rol de Acceso remoto que contiene también la configuración para VPN.	16
Ilustración 30 - Configuración del servidor de directivas de redes.	16
Ilustración 31 - Configuración de acceso a redes para el usuario "eviladmin".	17
Ilustración 32 - Configuración del adaptador de red VPN en el cliente.	17
Ilustración 33 - Comprobaciones de funcionamiento.....	18

EUNCIADO

Se quiere montar un servidor VPN para una organización sobre Windows Server 2012/2016.

- Crea la infraestructura de red necesaria para que los clientes se puedan autenticar contra el servidor y poder acceder de manera segura a la red de la organización.
- Documenta a modo de manual todos los pasos realizados hasta que el servicio esté disponible y funcione.
- El servidor VPN al menos debe tener dos adaptadores de red, uno de ellos estará conectado a la Internet pública y ésta será la interfaz de red que acepte las conexiones VPN entrantes y deberá de tener una IP estática. El segundo adaptador de red estará conectado a la intranet. Esta interfaz de red redireccionará el tráfico de red entre la VNP y los recursos de red presentes en la Intranet.
- Deberemos de activar el enrutamiento bajo petición en el servidor.

ESQUEMA DE RED

A continuación, se muestra la propuesta del esquema de red para la práctica, debido a pruebas desde el anfitrión del sistema sobre enrutamiento se cambió la red NAT a la red privada de clase A 10.0.0.0.

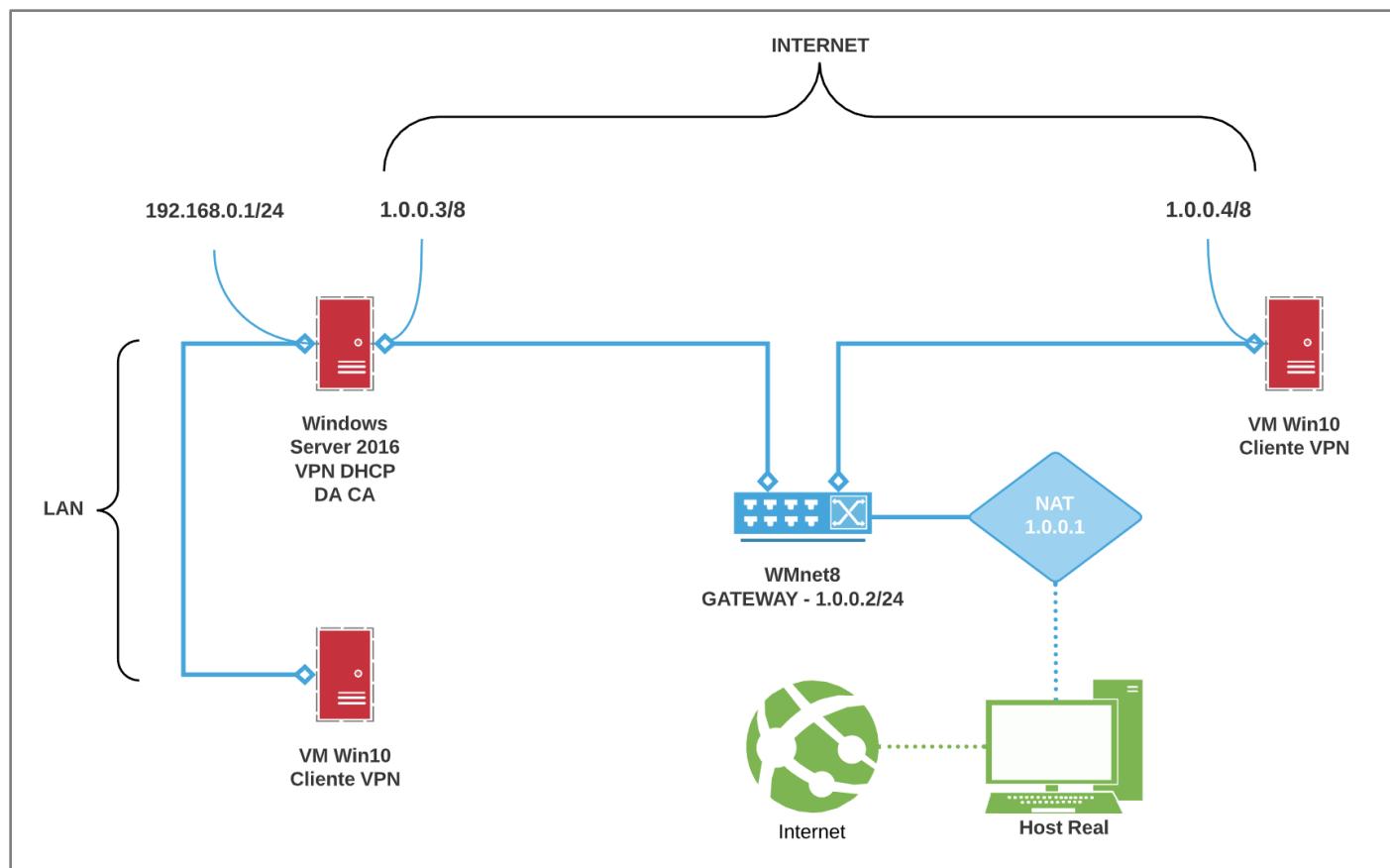


Ilustración 1 - Esquema de red.

CREACIÓN DEL SERVIDOR

Para la creación del servidor realizamos una instalación estándar de Windows Server 2016 en una máquina virtual VMware, tras el primer arranque completamos el asistente de Windows Essentials que nos dejará el servidor con una serie de servicios o roles por defecto como podemos ver en la siguiente imagen.

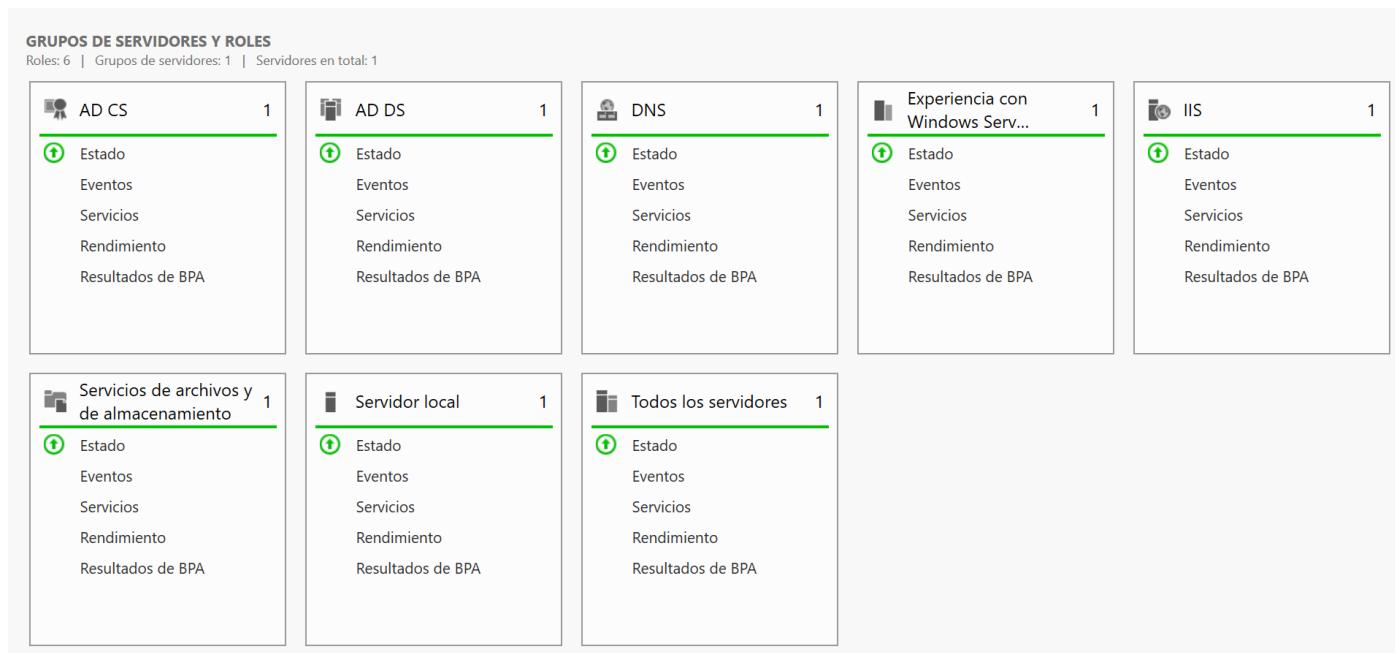


Ilustración 2 – Roles o servicios instalados mediante Windows Essentials.

Configuraremos 2 adaptadores de red uno con el nombre INTERNET en la red de VMnet8 con la IP 1.0.0.3 y el segundo denominado LAN con la IP 192.168.0.1, este último configurado en un segmento LAN ya que no requerimos de ningún servicio DHCP, NAT como ofrecen los otros modos especiales de VMware.

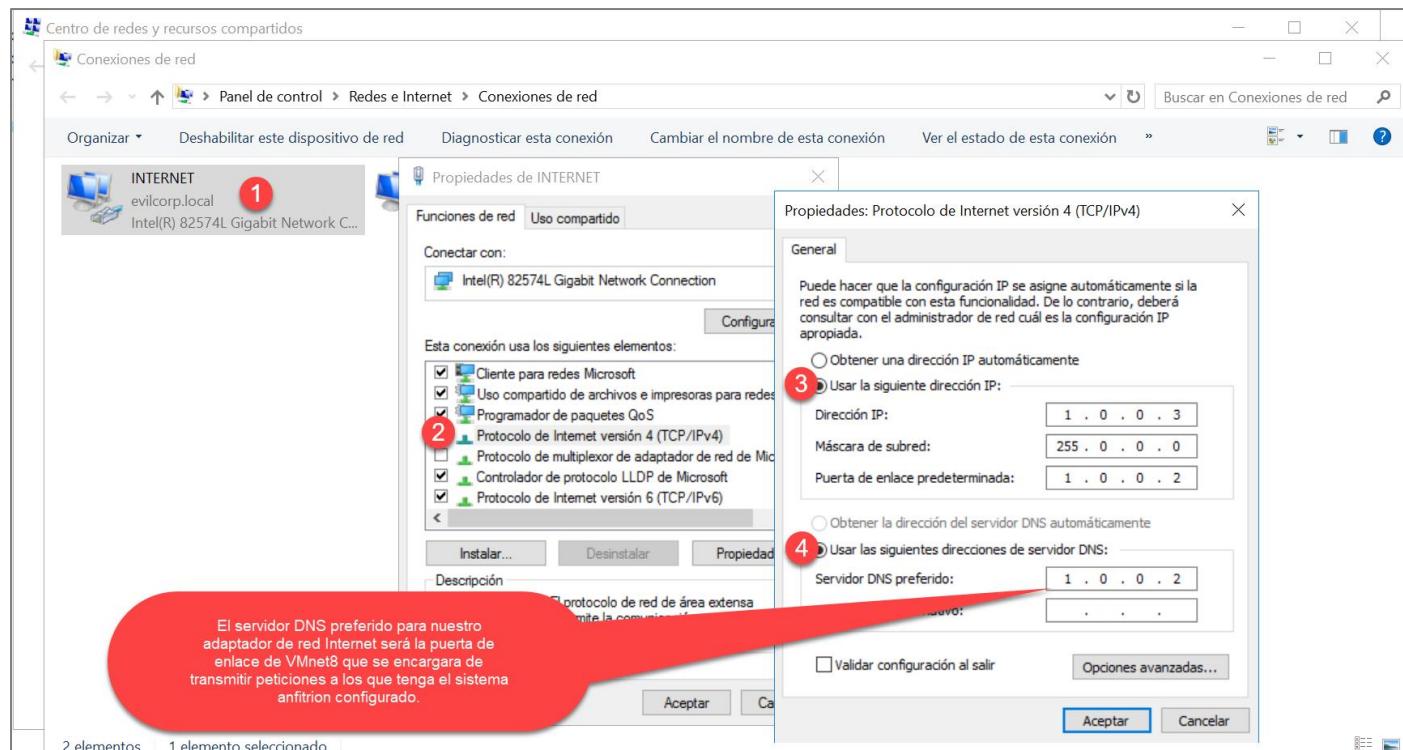


Ilustración 3 – Configuración del adaptador que hará las veces de enlace a Internet.

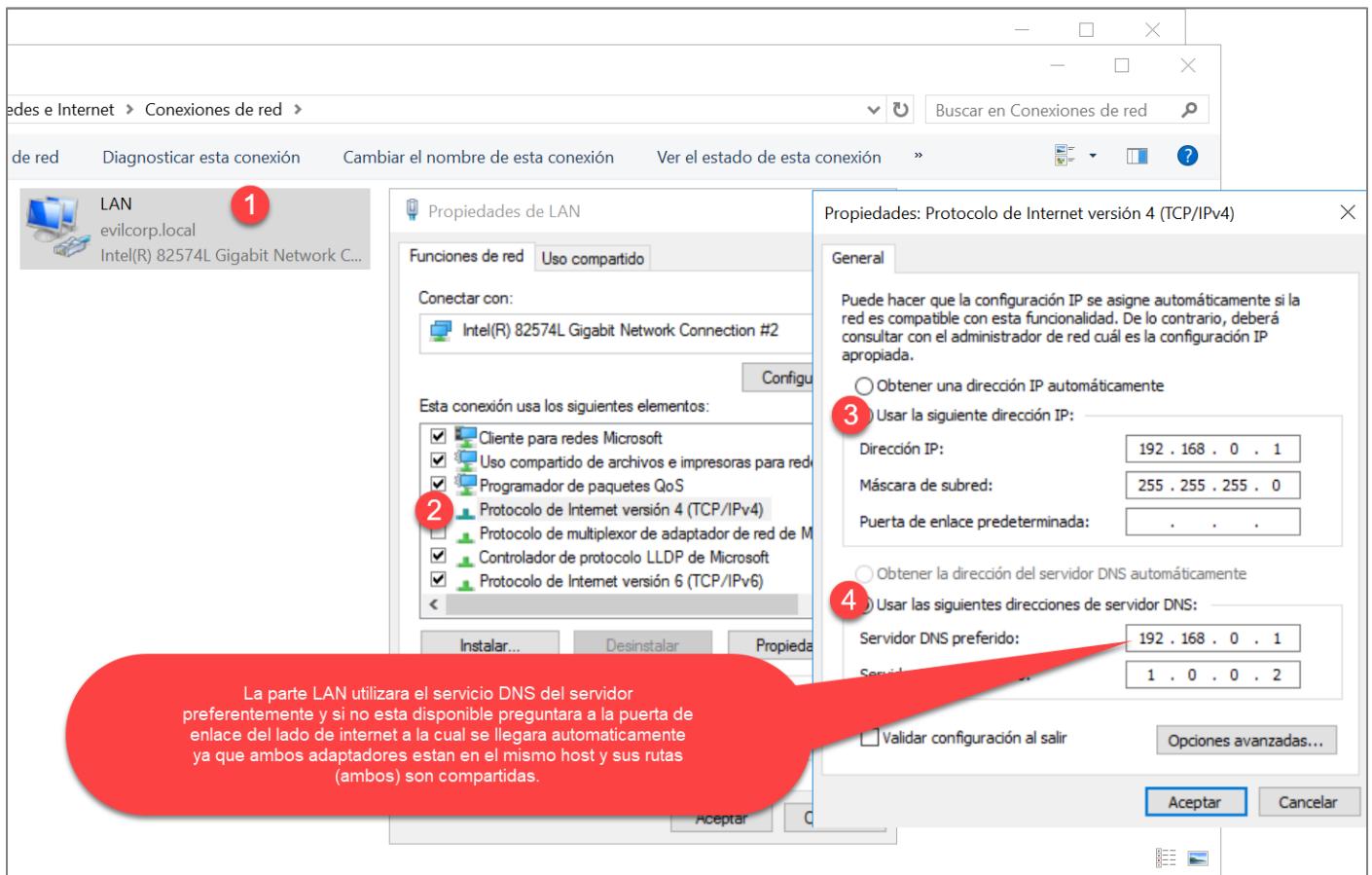


Ilustración 4 - Configuración del adaptador de la parte LAN.

A esta instalación por defecto tenemos que hacer algunas modificaciones, empezaremos por el servicio DNS, en el panel de administración del servicio configuraremos un reenviador que sirva bajo cualquier entorno, ya sea en mi casa o en el aula así como restringir su servicio al ámbito LAN.

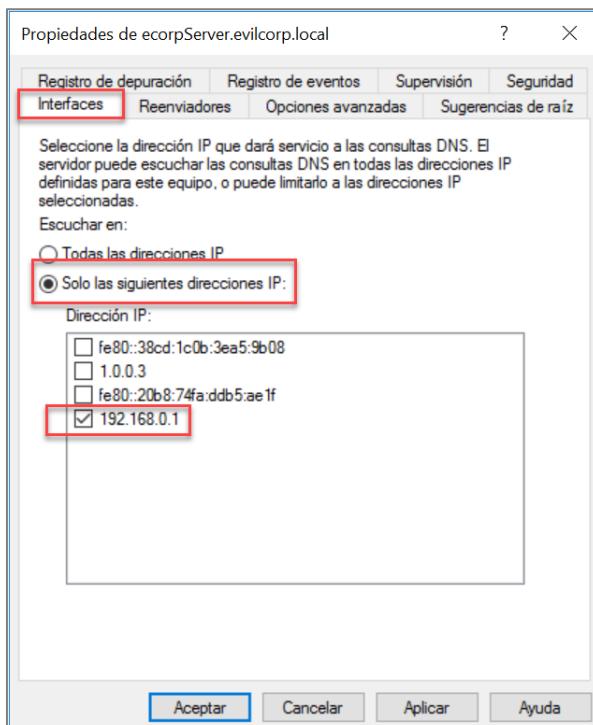


Ilustración 5 - Restringir el servicio DNS al ámbito LAN.

Configuración de los reenviadores para que las máquinas del ámbito LAN puedan resolver nombres o direcciones IP que el servicio DNS no conoce.

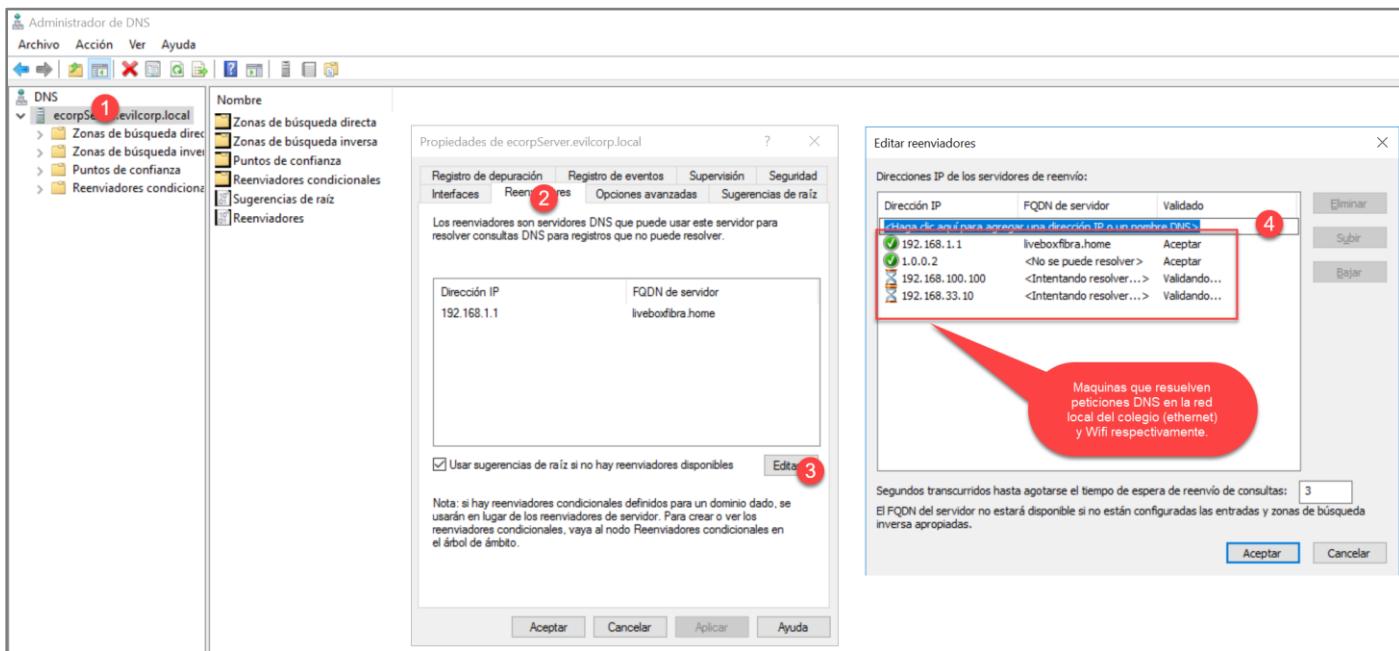


Ilustración 6 - Configuración de reenviadores para el servicio DNS.

Agregamos el ROL o servicio DHCP a nuestro servidor que otorgará configuraciones de red a los miembros de la parte LAN, incluidos los futuros clientes que conecten a través del servicio VPN.

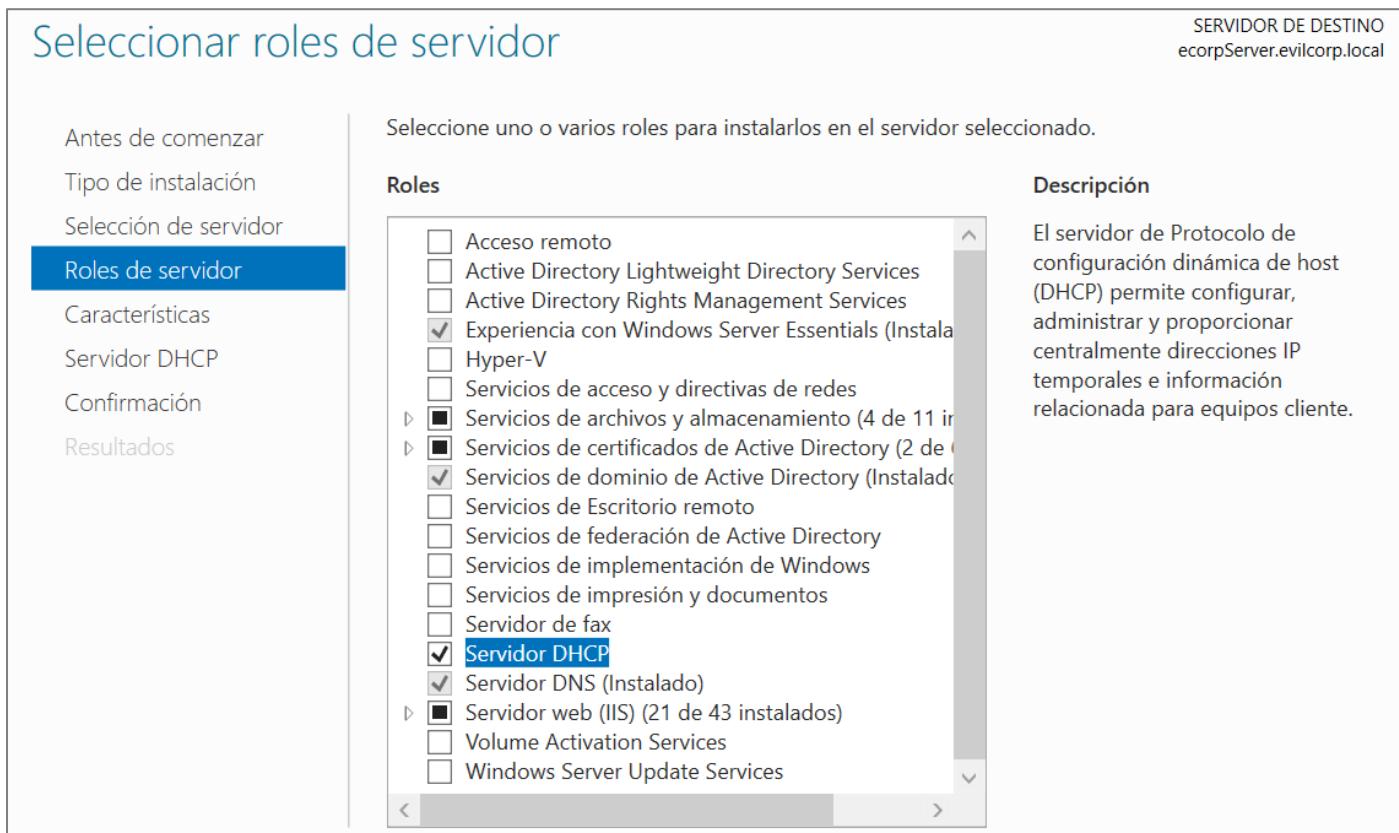


Ilustración 7 – Instalación del servicio DHCP.

Seguimos el asistente hasta que la instalación sea completada y entonces procedemos a su configuración.

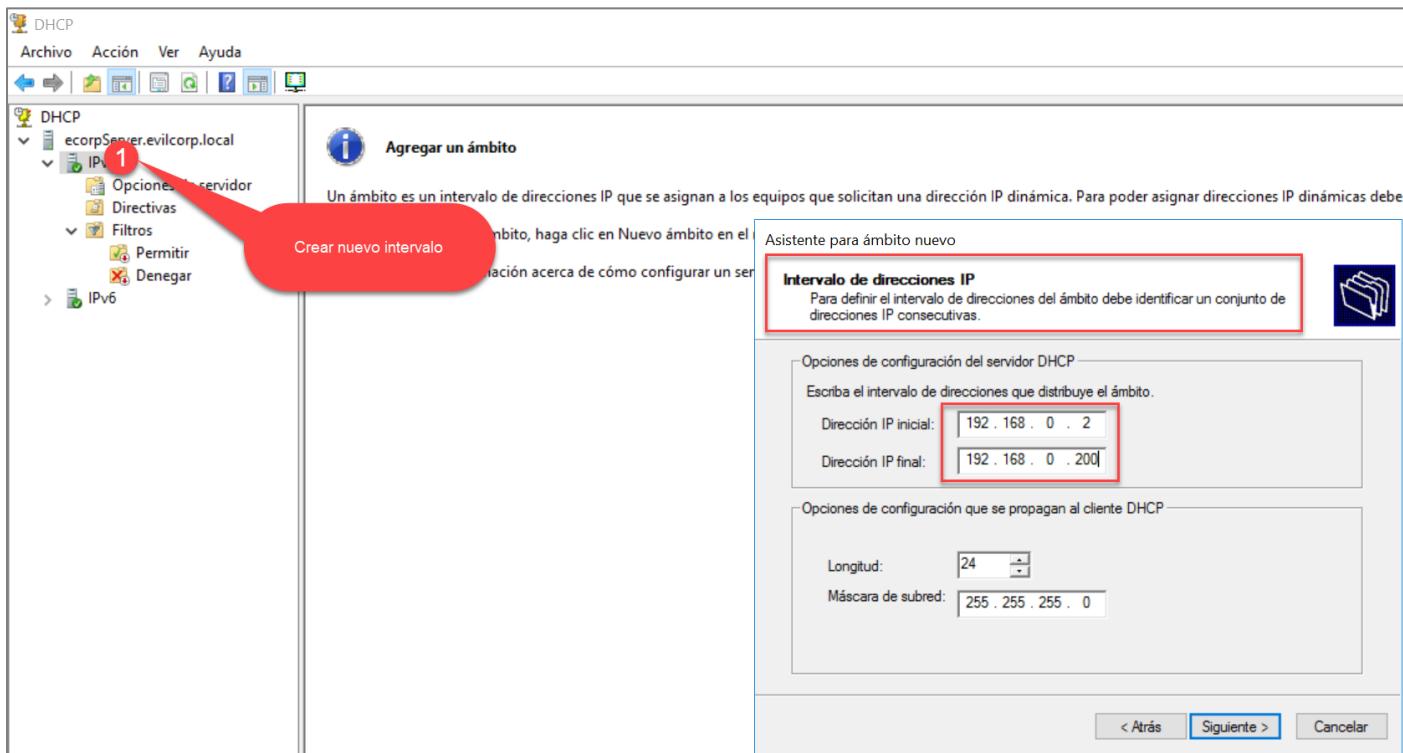


Ilustración 8 - Configuración de un intervalo de direcciones a servir en nuestro DHCP.

Tras finalizar la configuración del ámbito en la que hemos indicado servidor DNS, puerta de enlace... procedemos a meter una VM Windows 10 en el segmento LAN y ver si recibe la configuración automáticamente.

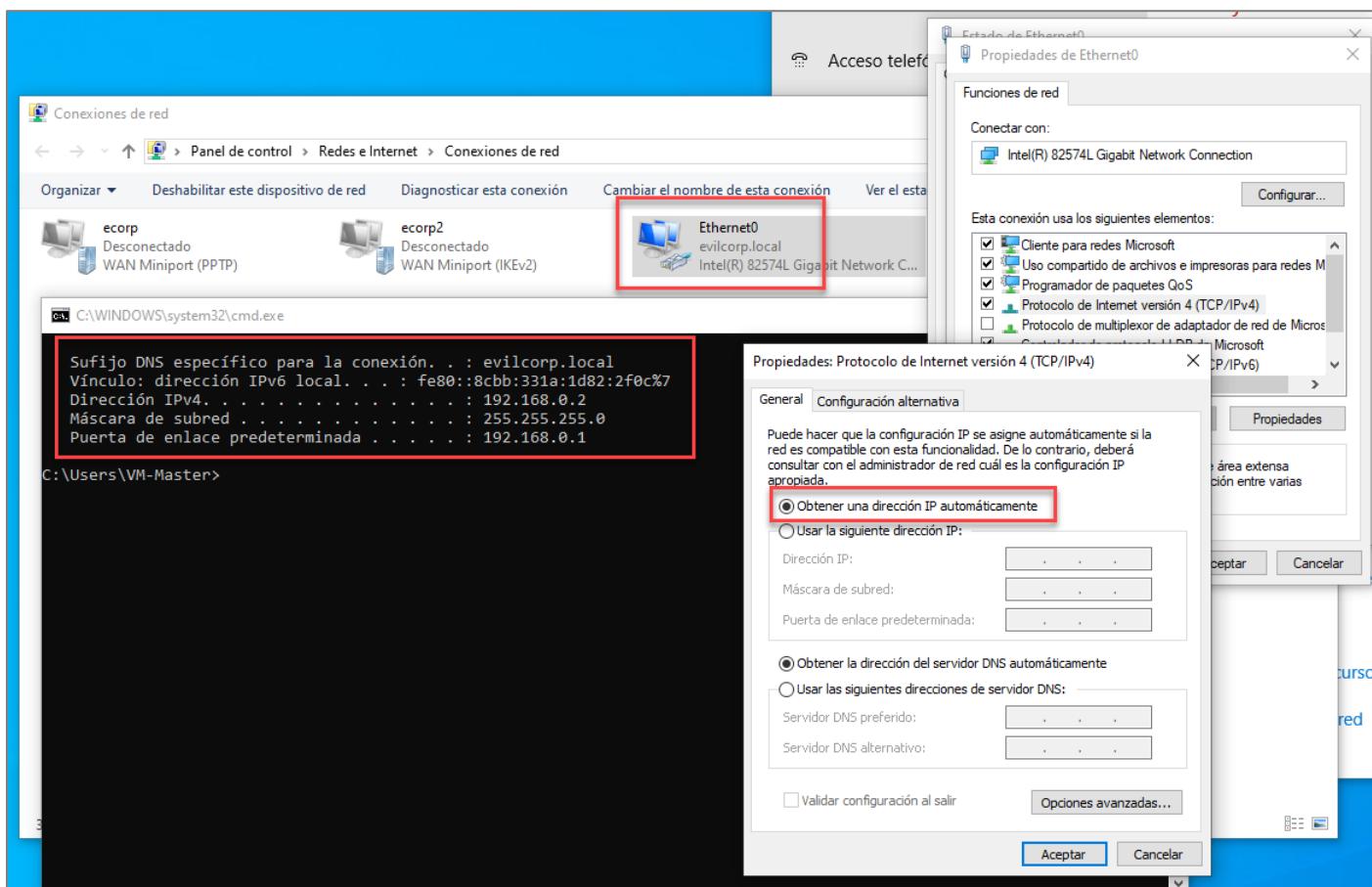


Ilustración 9 - El cliente recibe configuración mediante el servicio DHCP correctamente.

También aprovechamos para comprobar si el servicio DNS resuelve el nombre del servidor.

```
C:\Users\VM-Master>ping ecorpServer.evilcorp.local

Haciendo ping a ecorpServer.evilcorp.local [192.168.0.1] con 32 bytes de datos:
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.1:
    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\VM-Master>
```

Ilustración 10 - Comprobación de que el servicio DNS está funcionando.

CERTIFICADOS

Primero vamos a crear los certificados para ello accedemos a la ventana de administración de Active Directory Certificate Authority (AD CA).

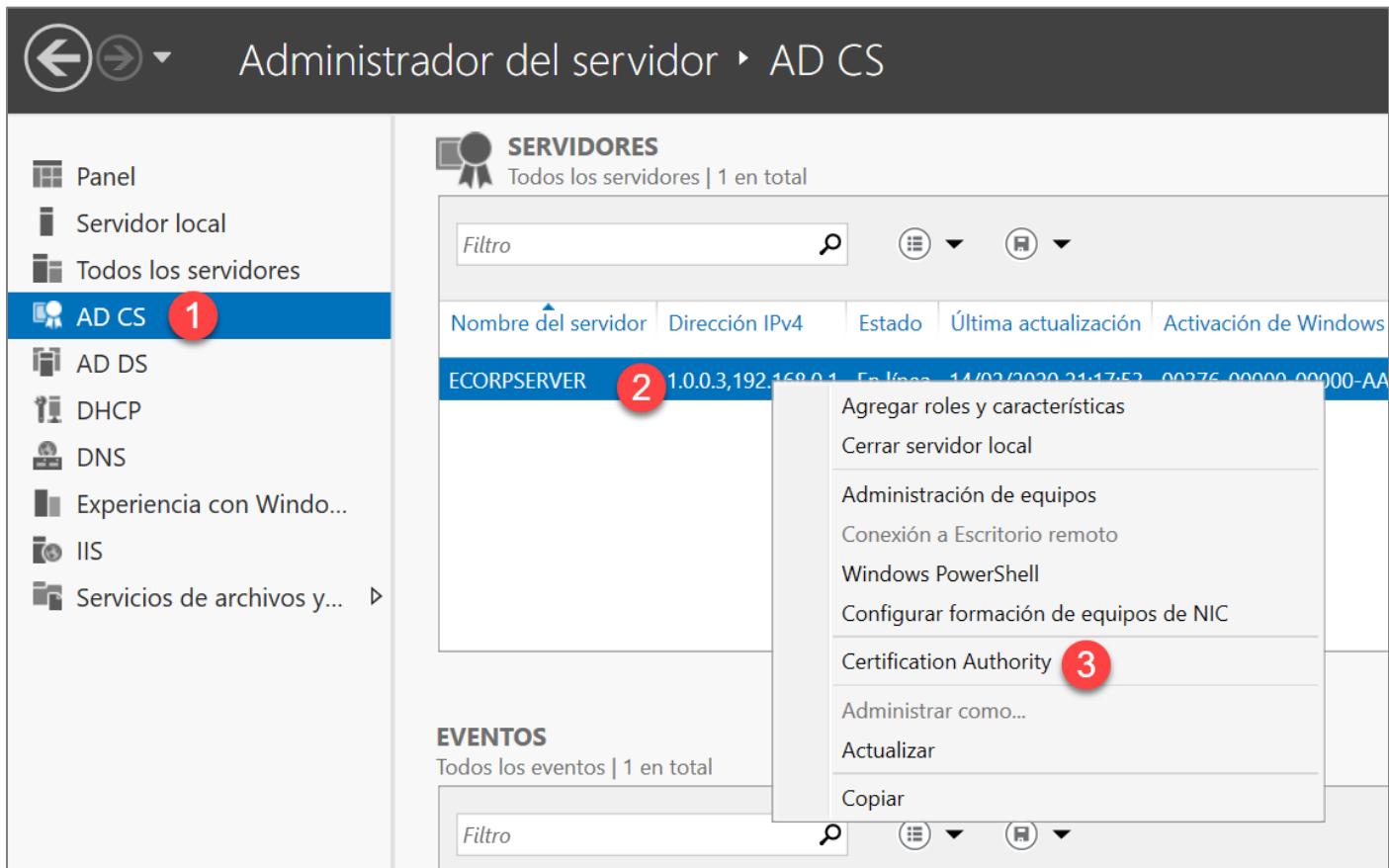


Ilustración 11 - Acceso a la ventana de autoridad de certificación.

Una vez en la ventana de Certificación haciendo click en plantillas de certificados y posteriormente en administrar elegimos la plantilla tipo Ipsec, sobre la que haremos click derecho y seleccionaremos duplicar plantilla.

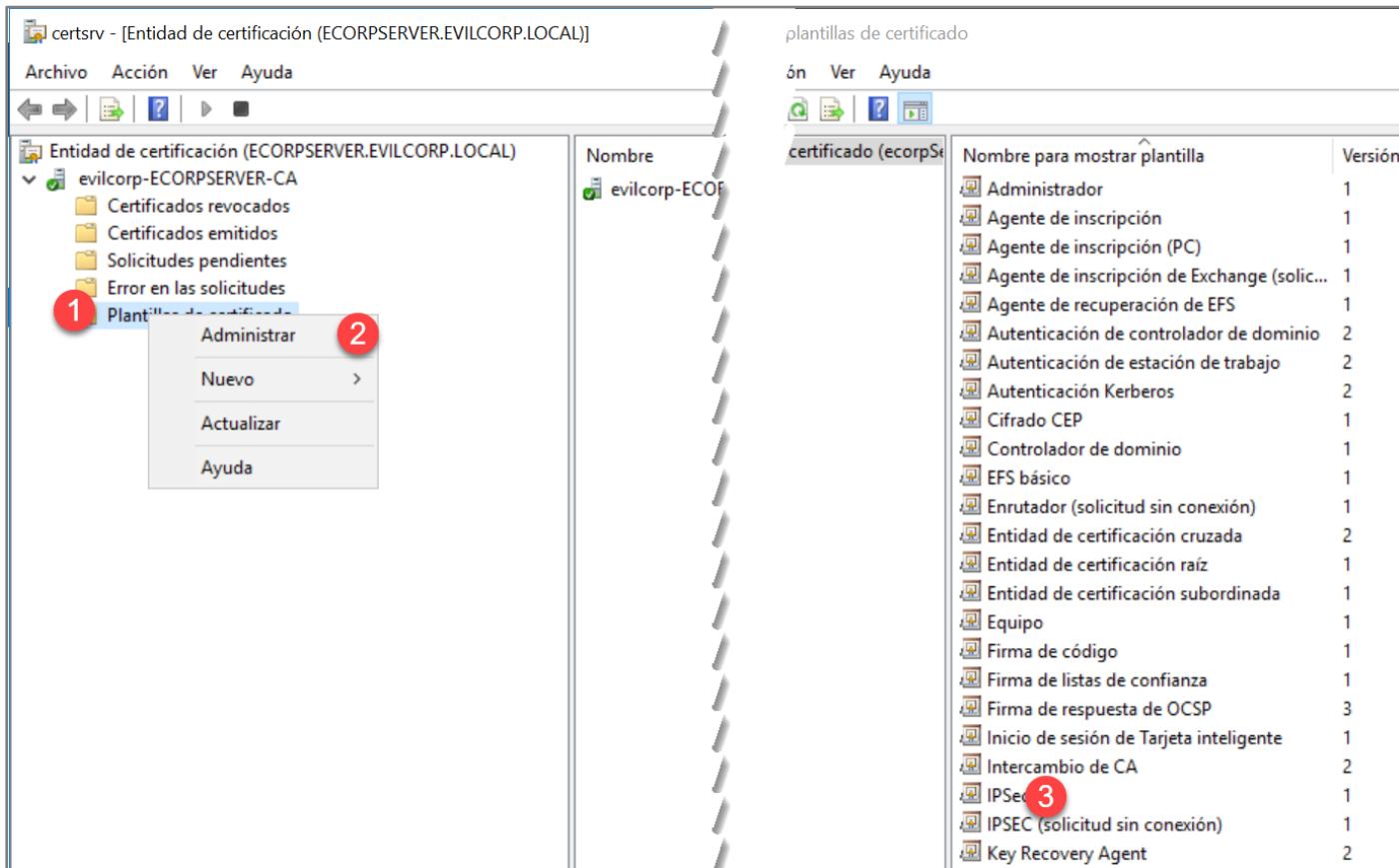


Ilustración 12 – Elegimos una plantilla de certificado sobre la que vamos a crear el nuestro.

Tras pulsar sobre duplicar plantilla aparecerá una ventana con una serie de pestañas, la que nos interesa es la de manejo de solicitudes.

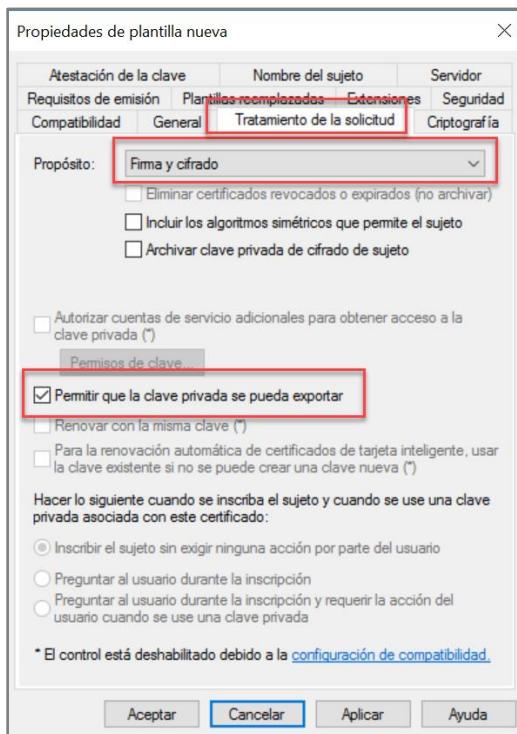


Ilustración 13 – Pestaña manejo de solicitudes para la plantilla de certificado.

Ahora en la pestaña extensiones seleccionamos directivas de aplicación, pulsamos en modificar y en la nueva ventana agregamos Autenticación de Servidor y pulsamos aceptar.

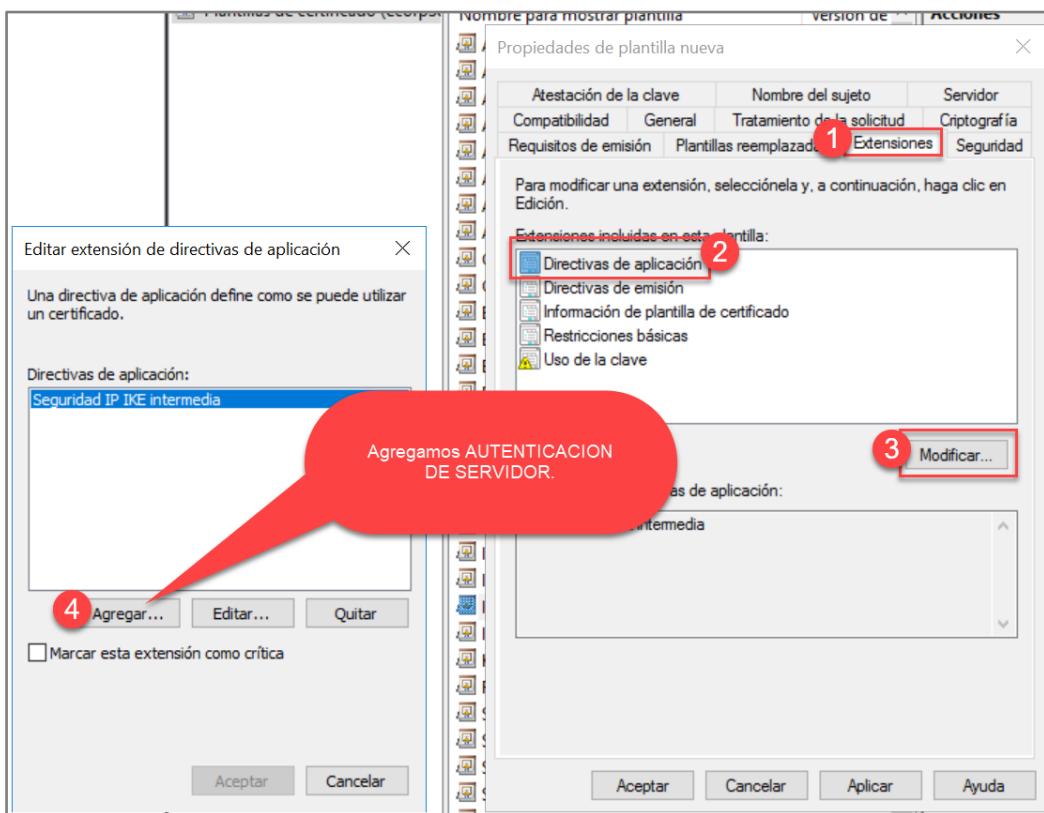


Ilustración 14 - Pestaña extensiones en las propiedades de la plantilla.

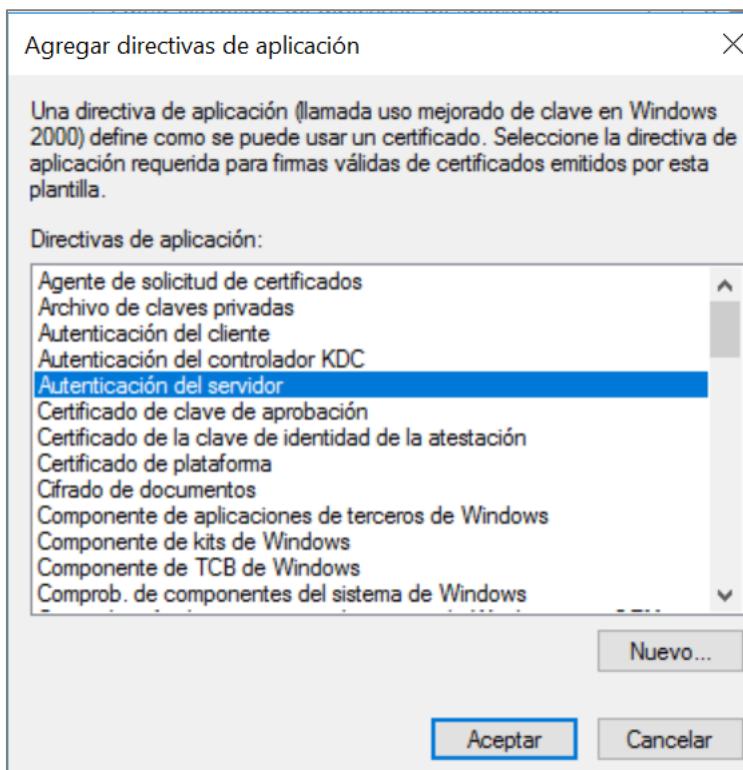


Ilustración 15 - Agregando directiva de aplicación para Autenticación del Servidor.

Ahora seleccionamos la opción Uso de la clave y pulsamos sobre Modificar.

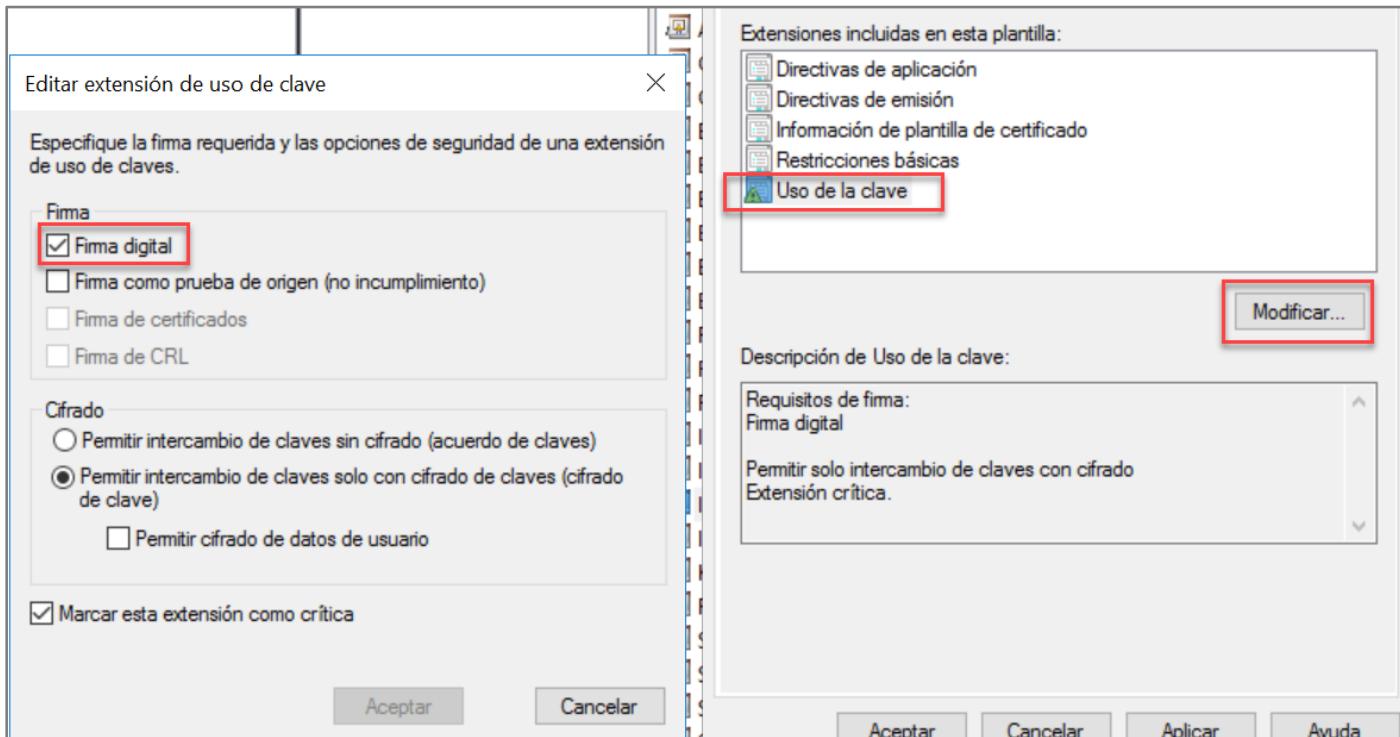


Ilustración 16 – Modificación del uso de la clave para firma digital.

Ahora en la pestaña seguridad en para usuarios autenticados y equipos del dominio vamos a seleccionar las opciones Leer, Inscribirse e Inscripción automática.

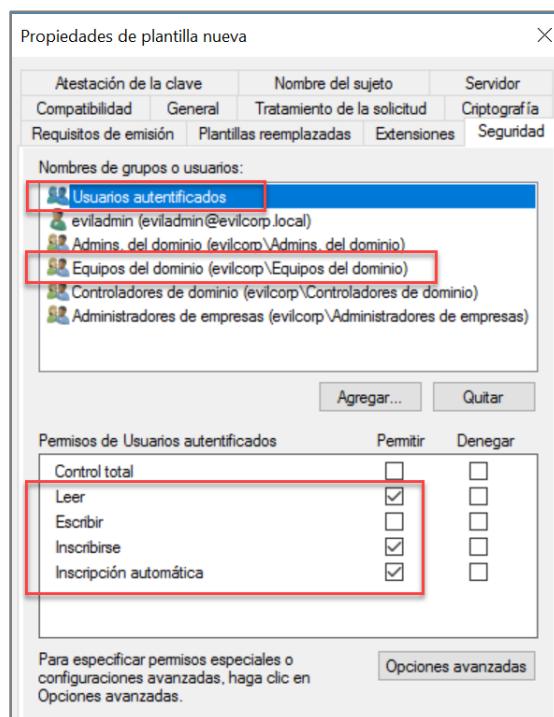


Ilustración 17 – Configuración de la pestaña seguridad en la plantilla.

Una vez finalizada esta configuración nos aseguramos de darle un nombre a esta plantilla mediante click derecho, como se utilizará para certificados en el servicio VPN la llamaremos VPN.

Ahora en la ventana de entidad de certificación hacemos click derecho en plantillas de certificado, nuevo y en la ventana seleccionamos la que acabamos de crear.

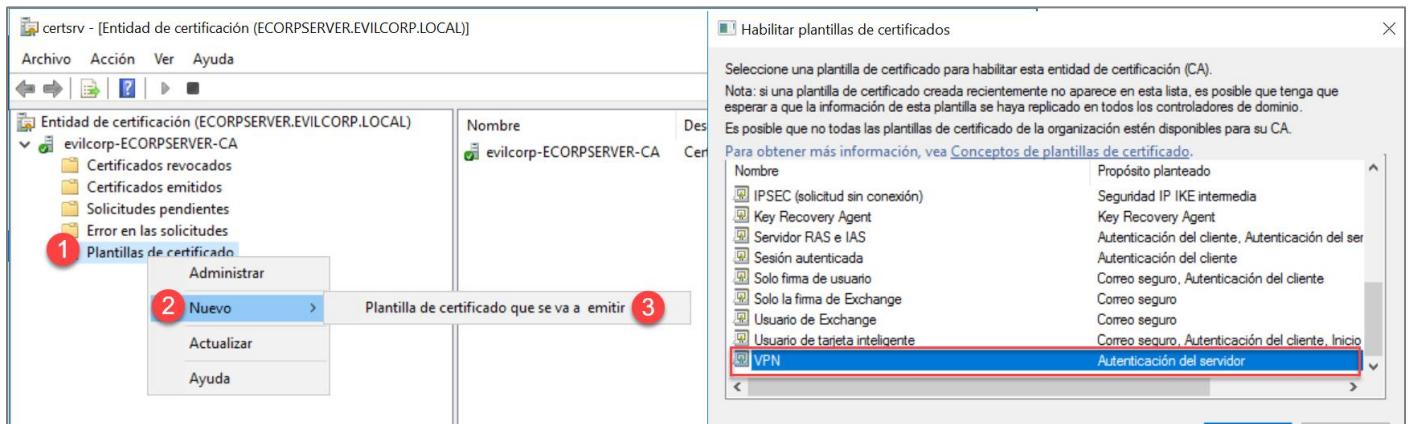


Ilustración 18 - Agregamos la plantilla a plantillas de certificado.

Ahora abrimos una MMC (Microsoft Management Console) ejecutando mmc con la ventana ejecutar (tecla Windows + R).

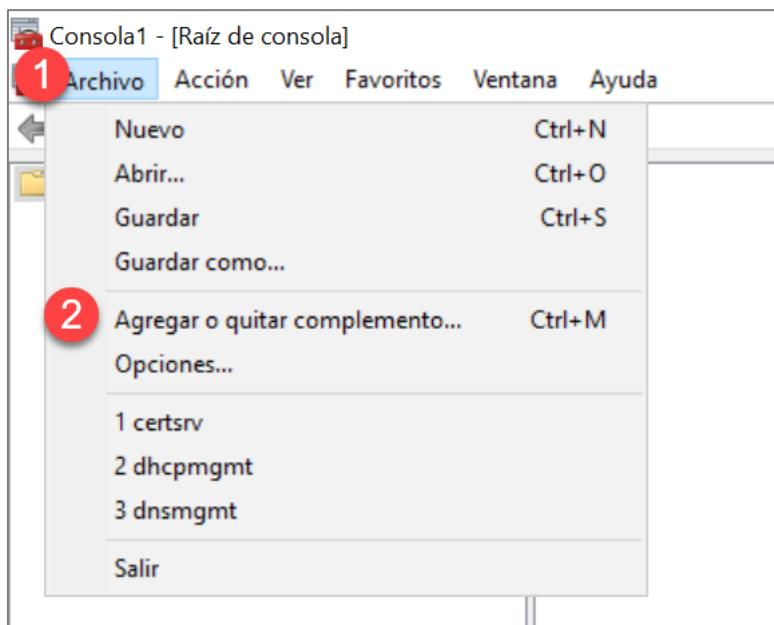


Ilustración 19 - Microsoft Management Console.

En la ventana resultante elegiremos Certificados, lo añadimos y en el nuevo cuadro de dialogo elegiremos cuenta de equipo, en la siguiente ventana no tocaremos nada y aceptaremos para cerrar el dialogo.

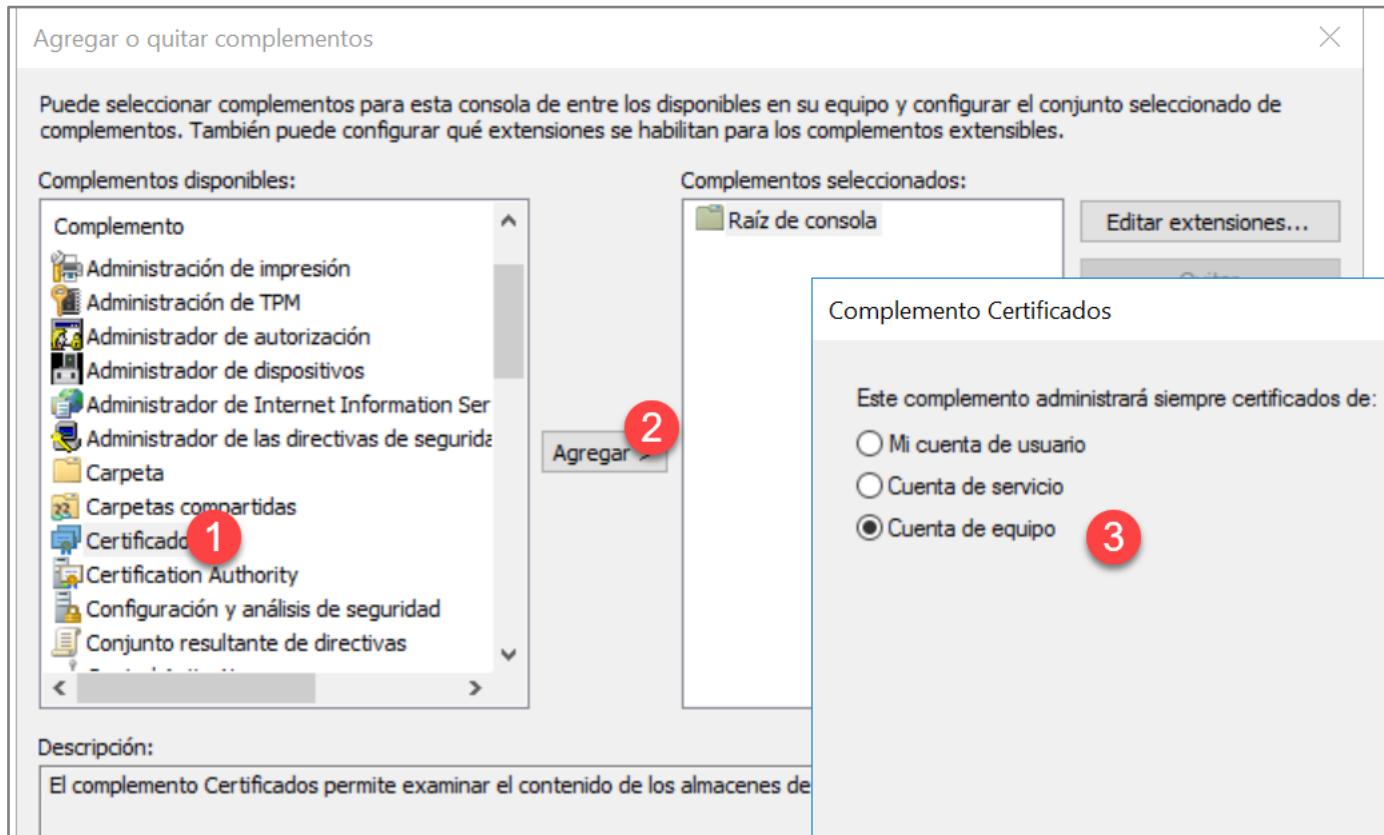


Ilustración 20 - Asignando certificado al servicio VPN.

Ahora en la ventana MMC hacemos click derecho en personal, todas las tareas, solicitar un certificado, aparecerá un nuevo asistente en el que pulsaremos siguiente hasta encontrarnos con la ventana de solicitud del certificado en donde elegiremos el que hemos creado(VPN).

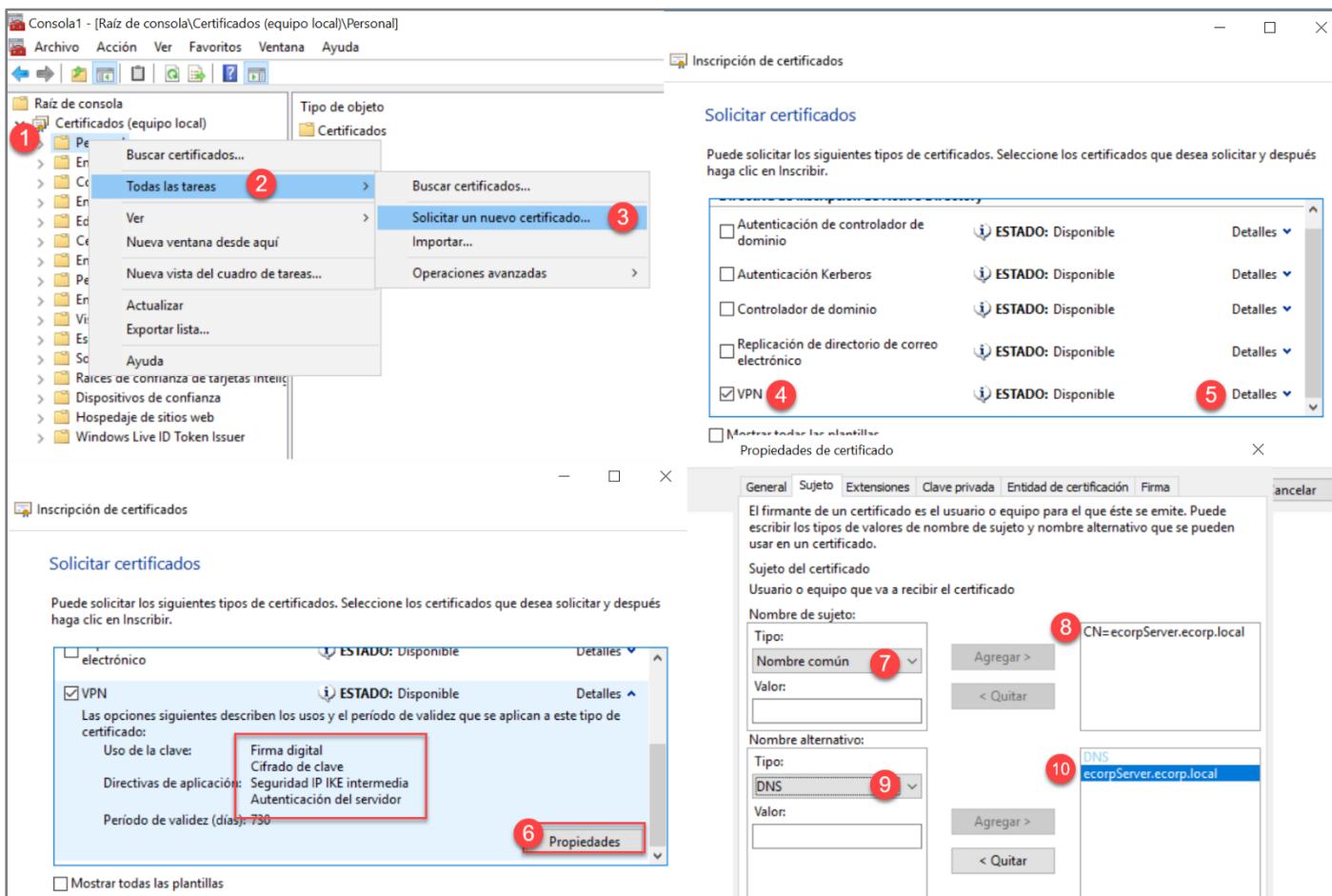


Ilustración 21 – Pasos para lo solicitud de un nuevo certificado.

Si todo ha salido bien nos aparecerá el nuevo certificado.

Consola1 - [Raíz de consola]\Certificados (equipo local)\Personal\Certificados							
Raíz de consola		Emitido para		Emitido por		Fecha de expir...	Propósitos plante...
Certificados (equipo local)	EVILCORP-ECORPSERVER	evilcorp-ECORPSERVER-CA	08/02/2025	Autenticación del c...	<Ninguno>		Windows Server Solutions Computer ...
Personal	ecorpServer.ecorp.local	evilcorp-ECORPSERVER-CA	12/02/2021	Autenticación del c...	<Ninguno>		Controlador de dominio
Certificados	ecorpServer.ecorp.local	evilcorp-ECORPSERVER-CA	12/02/2022	Autenticación del s...	<Ninguno>		VPN
Entidades de certificación raíz de confianza	evilcorp-ECORPSERVER-CA	evilcorp-ECORPSERVER-CA	02/02/2060	<Todos>	<Ninguno>		
Confianza empresarial							

Ilustración 22 – Nuevo certificado en el equipo local.

Ahora este certificado debería ser exportado y entonces importado en la maquina cliente, para esto hacemos click derecho sobre el certificado y seleccionamos exportar.

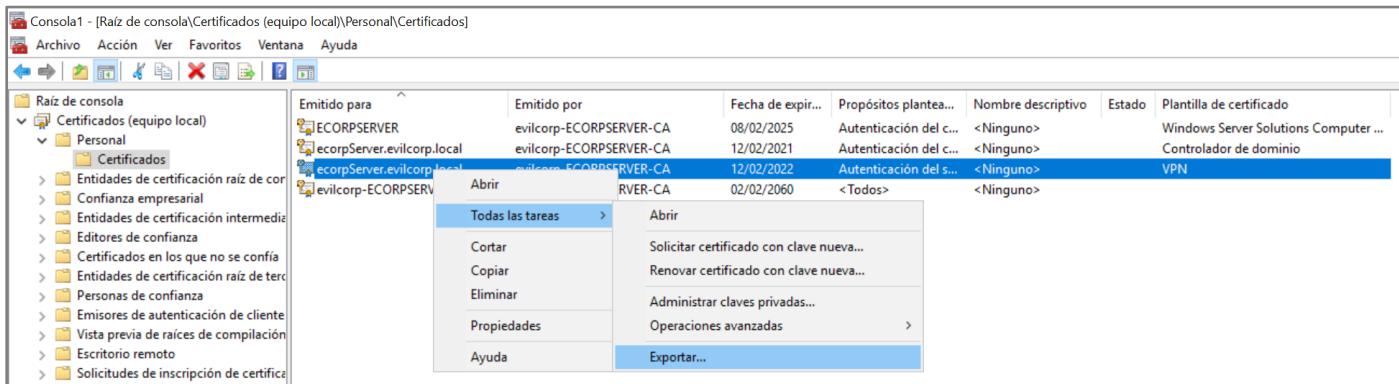


Ilustración 23 - Proceso de exportación del certificado.

Durante el asistente de exportación elegiremos exportar la clave privada.

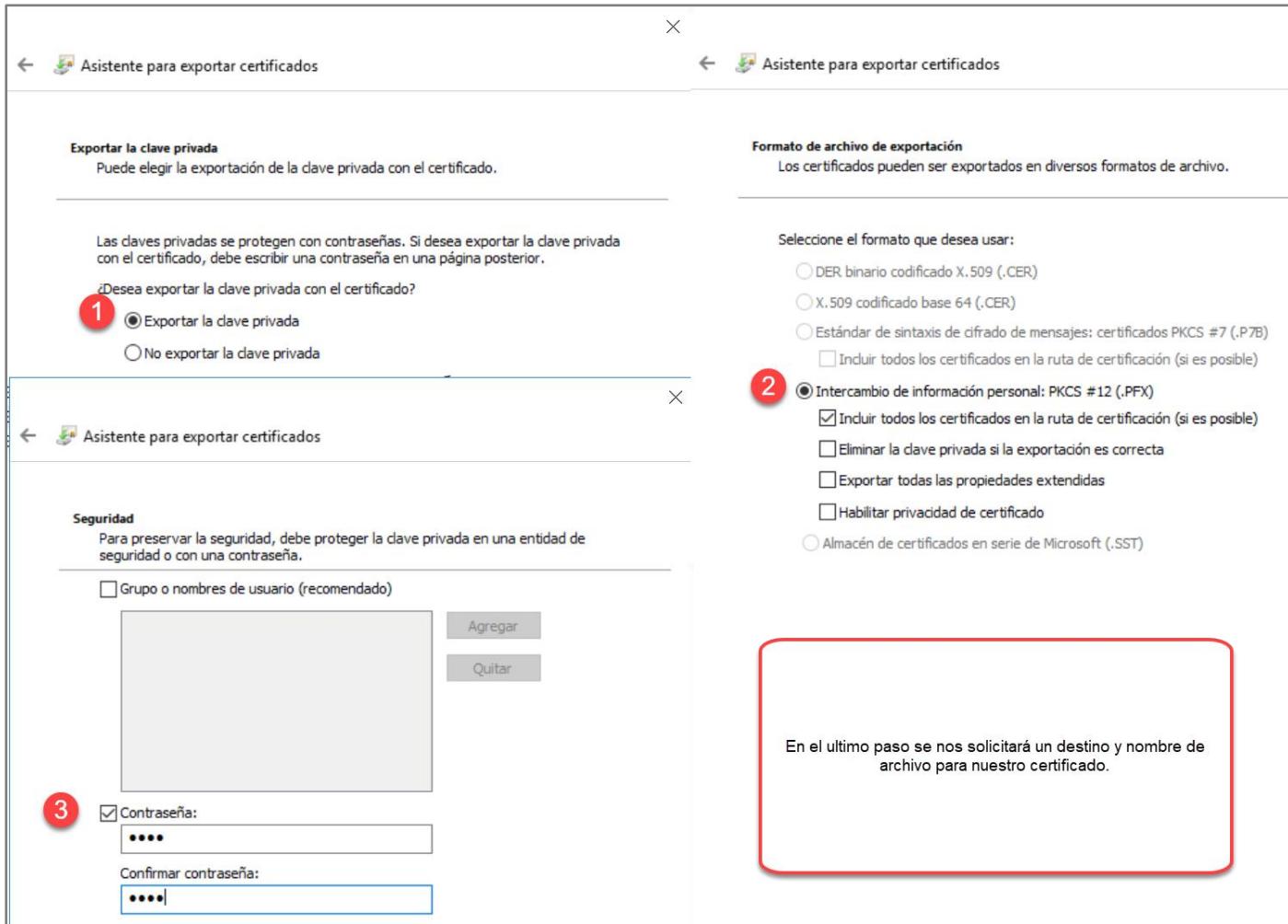


Ilustración 24 - Asistente para la exportación del certificado.

Para importar el certificado en el cliente lanzaremos en la maquina Windows 10 una consola MMC mediante ejecutar como vimos en el servidor, y añadiremos también en esta máquina el complemento certificados configurado para cuenta de equipo, finalmente el certificado será importado en la carpeta "Entidades de certificación de Raíz de confianza".

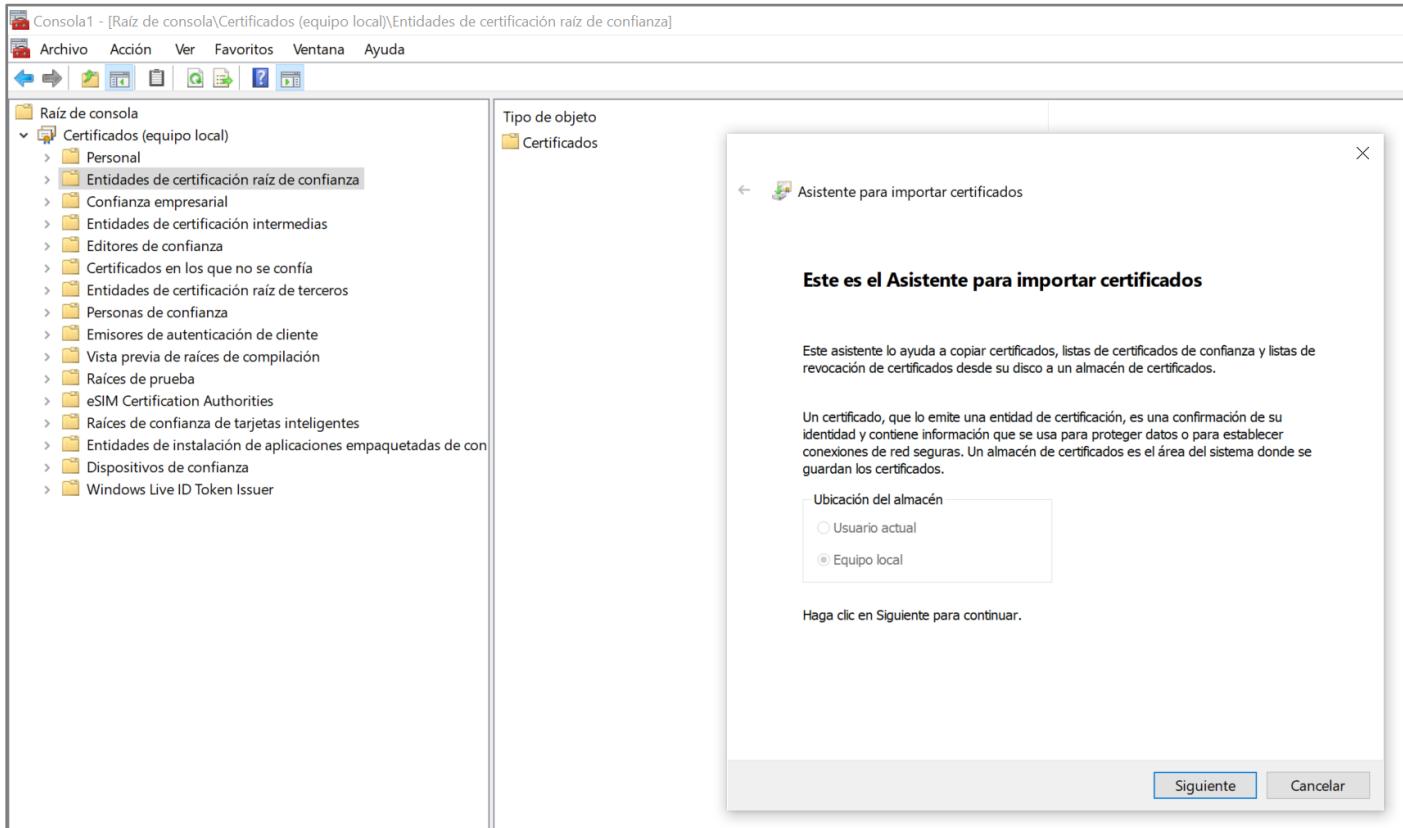


Ilustración 25 - Asistente para importar certificado.

Tras seguir los sencillos pasos del asistente podremos ver como nuestro certificado VPN esta entre el resto de los certificados de confianza.

Emisor para	Emisor por	Fecha de expira...	Propósitos planteado...	Nombre descriptivo	Estado	Plantilla de cert...
AddTrust External CA Root	AddTrust External CA Root	30/05/2020	Autenticación del se...	Sectigo (AddTrust)		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Autenticación del se...	DigiCert Baltimore R...		
Class 3 Public Primary Certificati...	Class 3 Public Primary Certification ...	02/08/2028	Autenticación del se...	VeriSign Class 3 Pub...		
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Impresión de fecha	Microsoft Timestamp...		
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Autenticación del se...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Autenticación del se...	DigiCert Global Roo...		
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	10/11/2031	Autenticación del se...	DigiCert		
DST Root CA X3	DST Root CA X3	30/09/2021	Correo seguro, Aute...	DST Root CA X3		
evilcorp.evilcorp.local	evilcorp-ECORPERVER-CA	12/02/2022	Autenticación del se...	<Ninguno>		13.6.1.4.1311.21...
evilcorp-ECORPERVER-CA	evilcorp-ECORPERVER-CA	02/02/2060	<Todos>	<Ninguno>		
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Autenticación del se...	GlobalSign Root CA ..		
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	08/12/2043	Autenticación del se...	Hotspot 2.0 Trust Ro...		
Microsoft Authenticode(tm) Root...	Microsoft Authenticode(tm) Root ...	01/01/2000	Correo seguro, Firm...	Microsoft Authentic...		
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	27/02/2043	<Todos>	Microsoft ECC Prod...		
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	27/02/2043	<Todos>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certificat...	Microsoft ECC TS Root Certificate ...	27/02/2043	<Todos>	Microsoft ECC TS Ro...		
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<Todos>	Microsoft Root Aut...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	10/05/2021	<Todos>	Microsoft Root Certi...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	23/06/2035	<Todos>	Microsoft Root Certi...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	22/03/2036	<Todos>	Microsoft Root Certi...		
Microsoft Time Stamp Root Certi...	Microsoft Time Stamp Root Certifi...	22/10/2039	<Todos>	Microsoft Time Sta...		
NO LIABILITY ACCEPTED, (c97 Ve...	NO LIABILITY ACCEPTED, (c97 Veris...	08/01/2004	Impresión de fecha	VeriSign Time Stam...		
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	29/06/2034	Autenticación del se...	Starfield Class 2 Cert...		
Symantec Enterprise Mobile Root...	Symantec Enterprise Mobile Root f...	15/03/2032	Firma de código	<Ninguno>		
Thawte Timestamping CA	Thawte Timestamping CA	01/01/2021	Impresión de fecha	Thawte Timestampi...		
UTN-USERFirst-Object	UTN-USERFirst-Object	09/07/2019	Sistema de cifrado d...	Sectigo (UTN Object)		
VeriSign Class 3 Public Primary C...	VeriSign Class 3 Public Primary Cert...	17/07/2036	Autenticación del se...	VeriSign		

Ilustración 26 - Importación del certificado de confianza con éxito.

INSTALACION DEL SERVICIO VPN

Procedemos a agregar el ROL o servicio Acceso Remoto además de Directivas de redes y Servicios de Acceso.

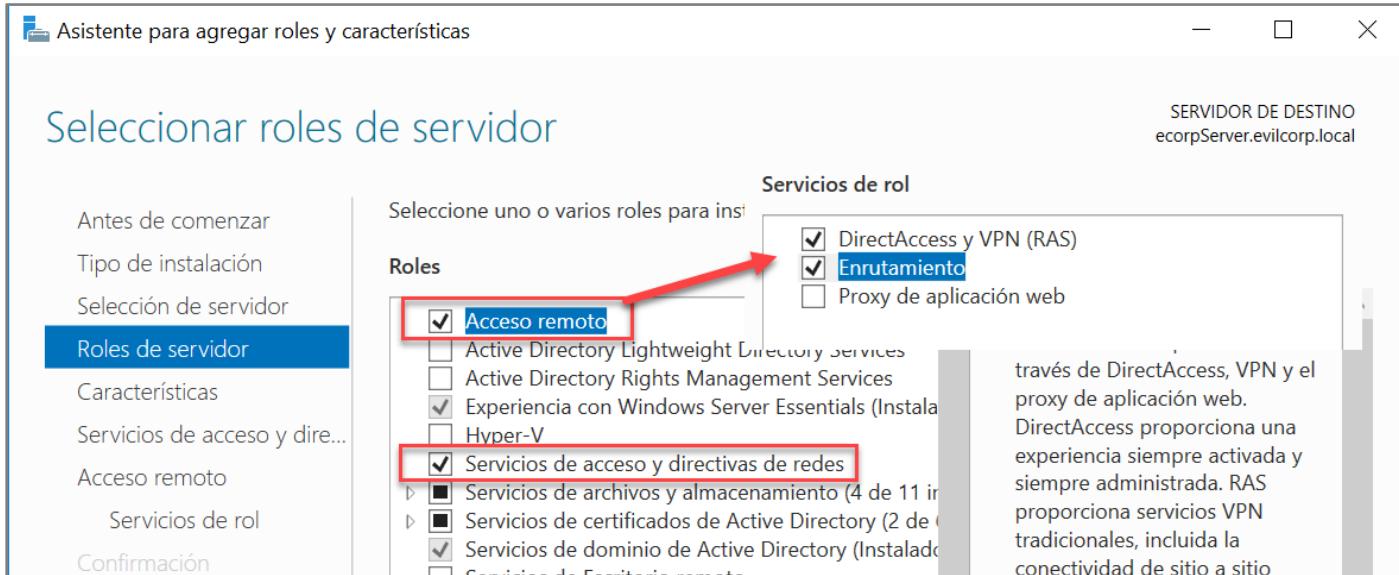


Ilustración 27 - Agregando Roles para VPN.

Una vez instalada la característica de acceso remoto, procedemos a iniciar el asistente de configuración de esta característica.

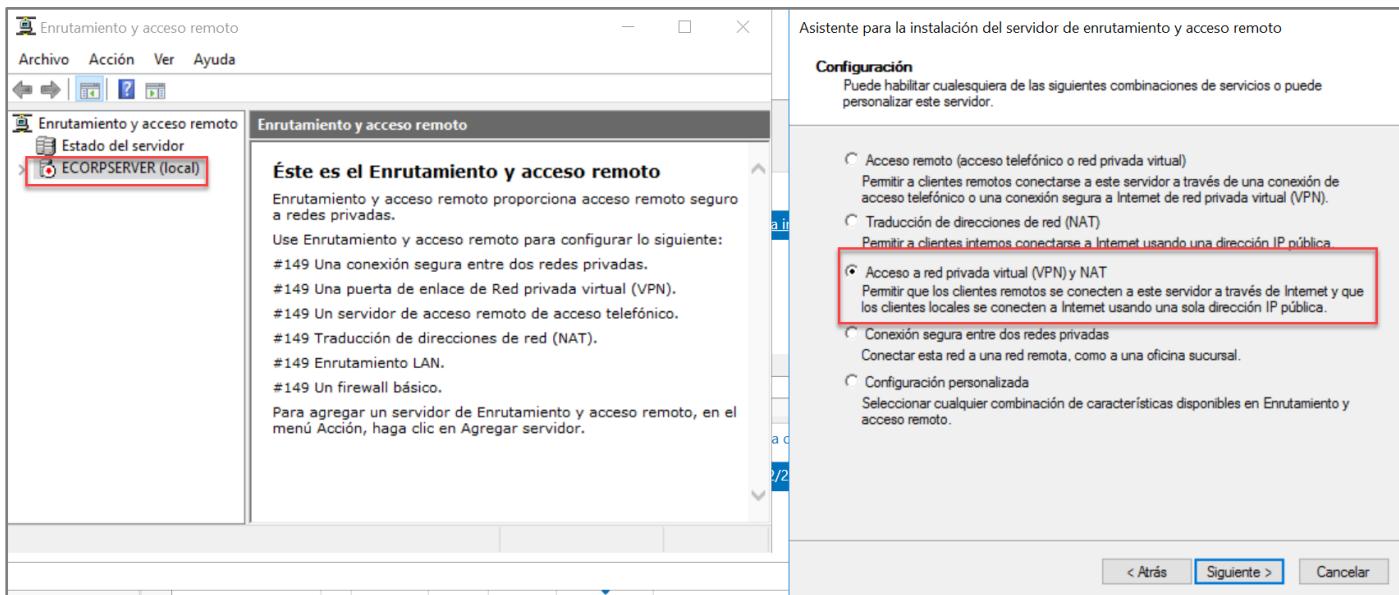


Ilustración 28 - Inicio del asistente para configuración de enrutamiento y acceso remoto.

Configuración del DHCP relay.

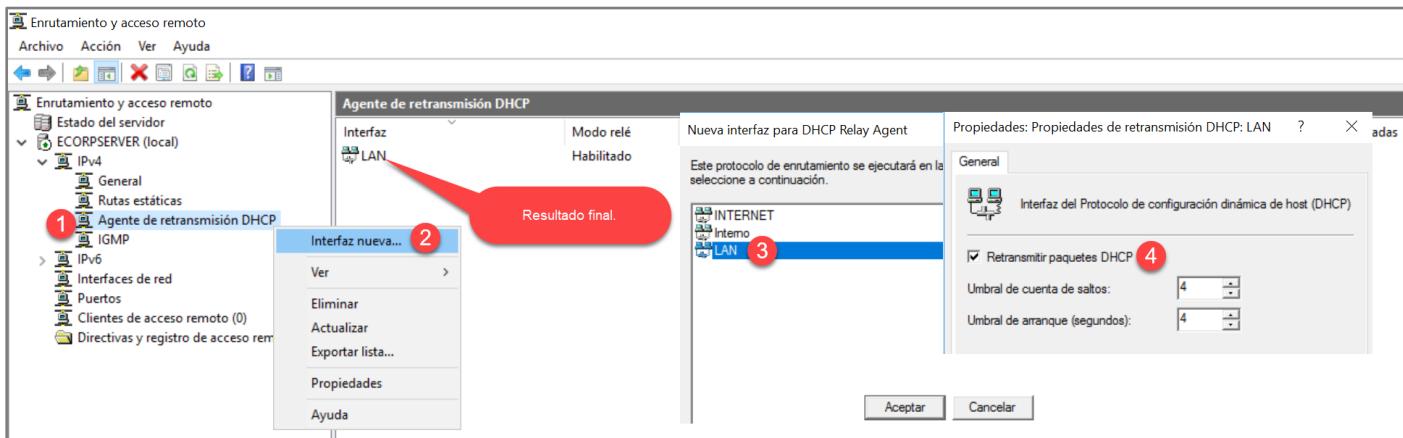


Ilustración 29 - Instalamos el rol de Acceso remoto que contiene también la configuración para VPN.

Ahora hacemos click derecho en directivas y registro de acceso remoto y configuramos las siguientes opciones como vemos en la imagen.

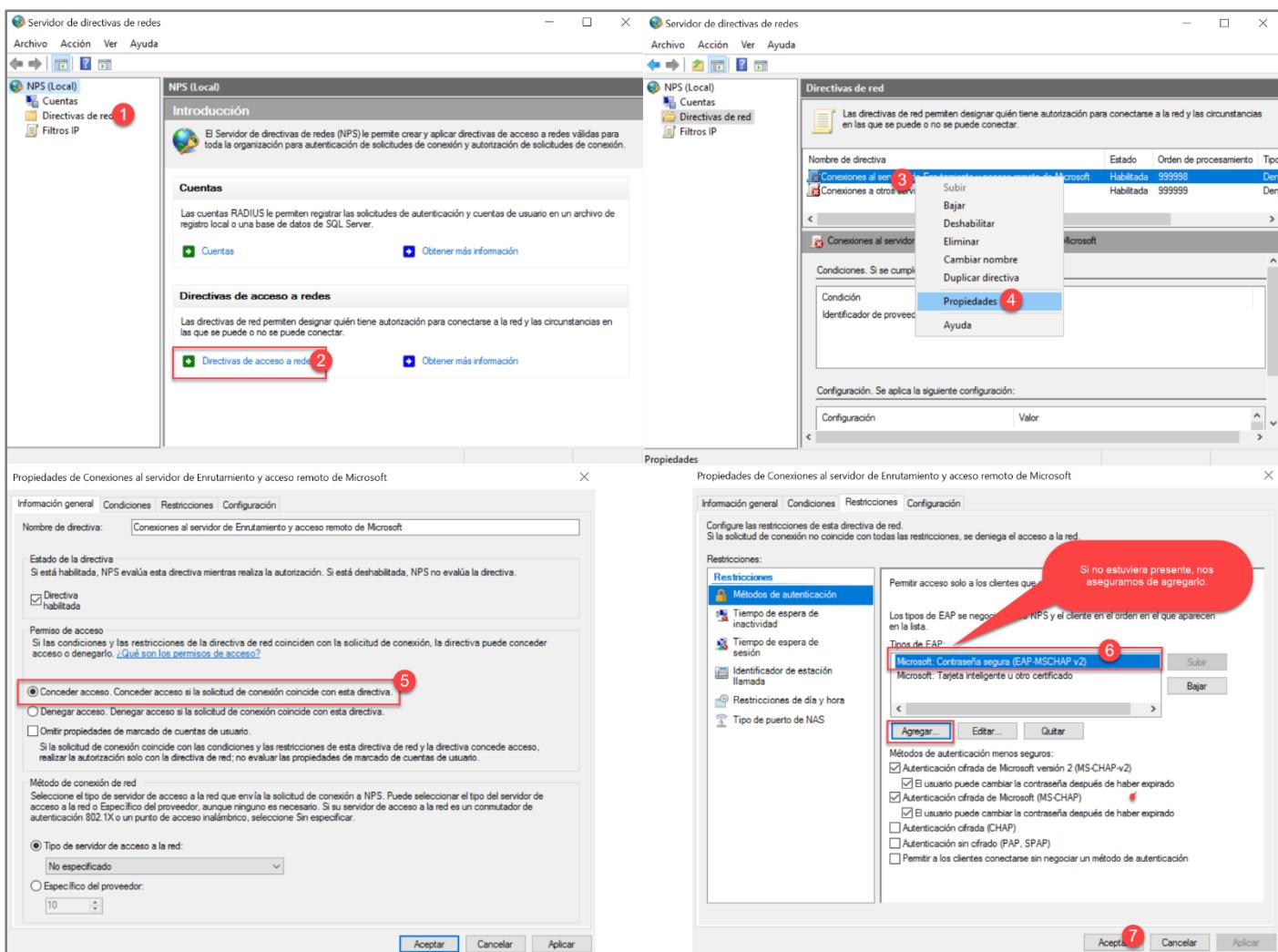


Ilustración 30 - Configuración del servidor de directivas de redes.

Ahora tenemos que dar permiso a los usuarios que podrán acceder remotamente mediante la gestión de usuarios de Active Directory, en el usuario buscamos la pestaña Marcado y seleccionamos Permitir acceso.

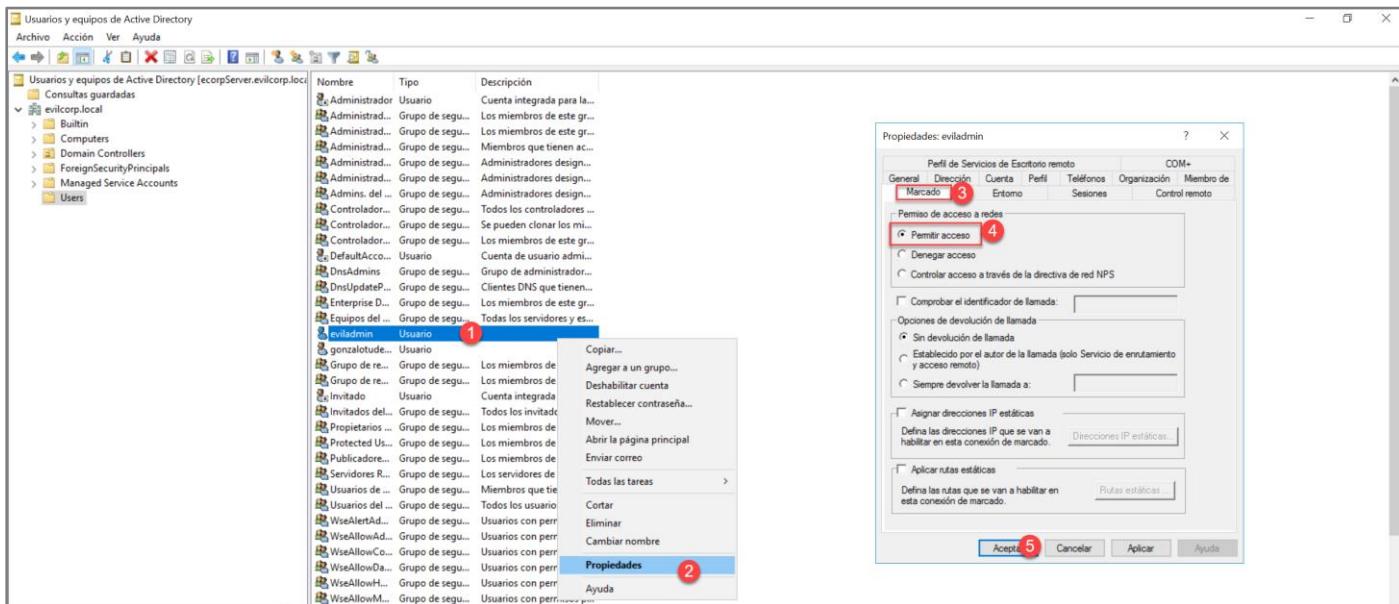


Ilustración 31 – Configuración de acceso a redes para el usuario “eviladmin”.

PRUEBAS DE FUNCIONAMIENTO

Para comprobar el funcionamiento debemos configurar el acceso VPN en el cliente de la siguiente forma, ya que nuestro certificado digital tiene algún error y siempre que intentamos conectar mediante IKEv2 recibimos el error TIPO DE CERTIFICADO NO VÁLIDO, por lo que el túnel VPN deberá utilizar el protocolo PPTP (protocolo de túnel punto a punto).

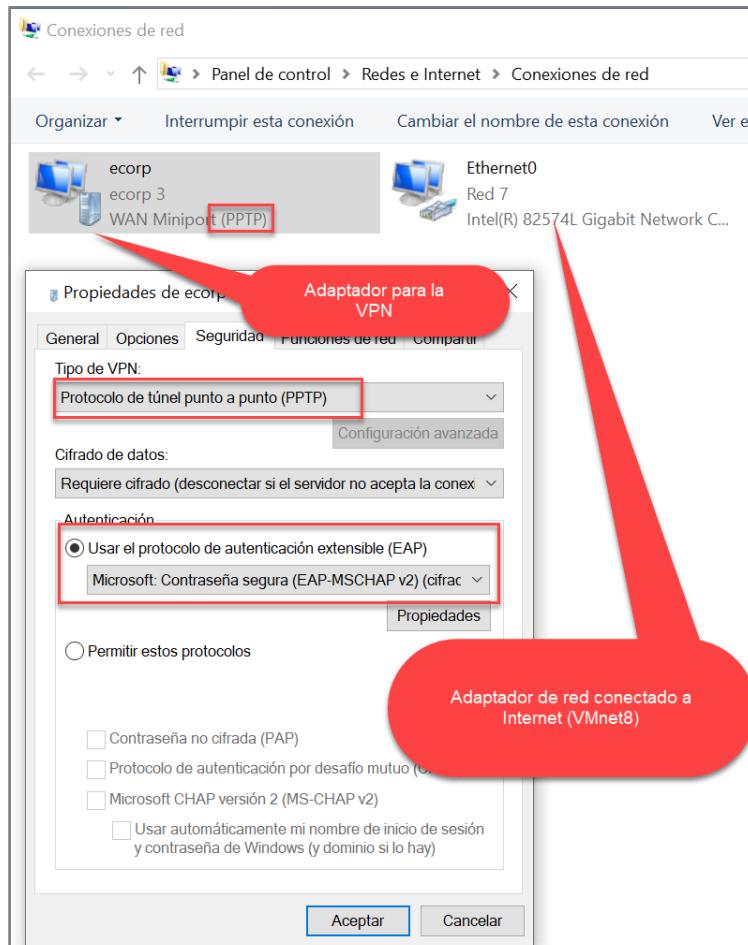


Ilustración 32 – Configuración del adaptador de red VPN en el cliente.

Comprobamos que estamos en la red local que administra el servidor.

```
C:\WINDOWS\system32\cmd.exe

Adaptador de Ethernet Ethernet0:
Sufijo DNS específico para la conexión. . .
Vínculo: dirección IPv6 local. . . : fe80::78db:df99:dbcac%17-%/
Dirección IPv4. . . . . : 10.0.0.4
Máscara de subred . . . . . : 255.0.0.0
Puerta de enlace predeterminada . . . . : 10.0.0.2

Adaptador PPP ecorp:
Sufijo DNS específico para la conexión. . . : evilcorp.local
Dirección IPv4. . . . . : 192.168.0.105
Máscara de subred . . . . . : 255.255.255.255
Puerta de enlace predeterminada . . . . :

C:\Users\VM-Master>ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: bytes=32 tiempo<1ms TTL=127
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=127
Respuesta desde 192.168.0.1: bytes=32 tiempo<1ms TTL=127
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=127

Estadísticas de ping para 192.168.0.1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\VM-Master>ping 192.168.0.101

Haciendo ping a 192.168.0.101 con 32 bytes de datos:
Respuesta desde 192.168.0.101: bytes=32 tiempo=2ms TTL=127
Respuesta desde 192.168.0.101: bytes=32 tiempo=1ms TTL=127
Respuesta desde 192.168.0.101: bytes=32 tiempo=1ms TTL=127
Respuesta desde 192.168.0.101: bytes=32 tiempo=1ms TTL=127

Estadísticas de ping para 192.168.0.101:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

Ilustración 33 - Comprobaciones de funcionamiento.