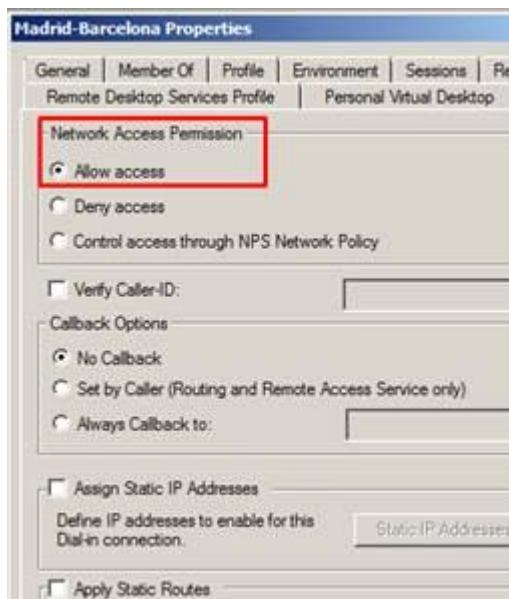
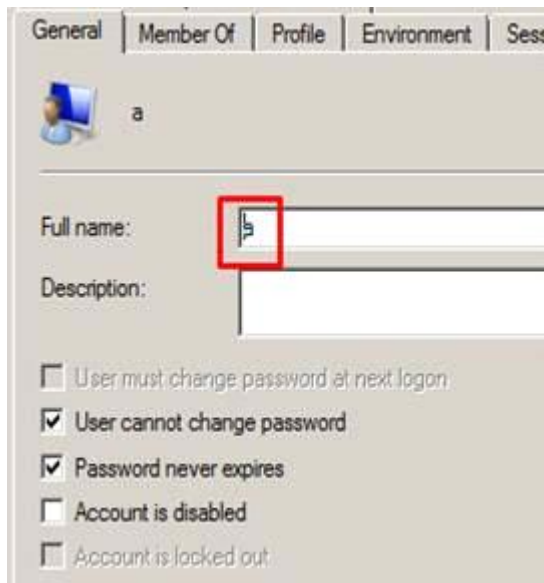


VPN para comunicar dos Forefront

miércoles, 18 de octubre de 2023 12:54

Accedemos al servidor de Madrid

-Primero creamos un usuario que le vamos a llamar A y asignamos permisos totales sobre el apartado Network Access Permission:



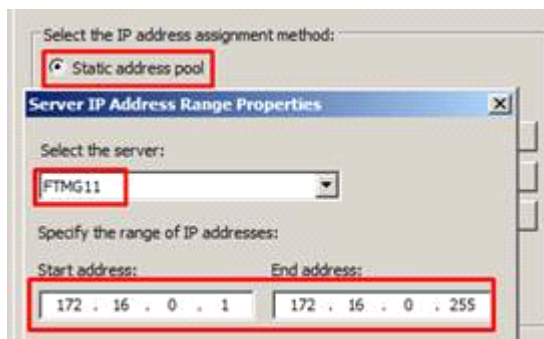
-Para comprobar que la VPN nos funcionará cuando la configuremos, vamos a habilitar la regla para permitir todo el tráfico:

Order	Name	Action
1	Allow All	Allow

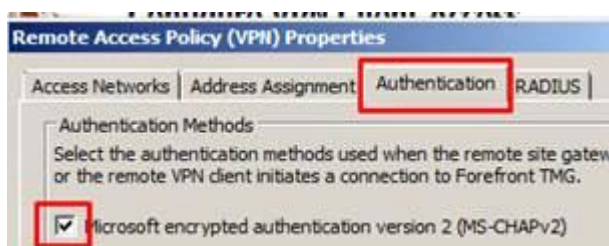
-Accedemos dentro de Remote Access Policy para configurar el método de asignación de IP's para la VPN:



- Marcamos la opción de direcciones estáticas.
- Seleccionamos nuestro servidor de Madrid
- Asignamos el pool de direcciones 172.16.0.1 - 172.16.0.255

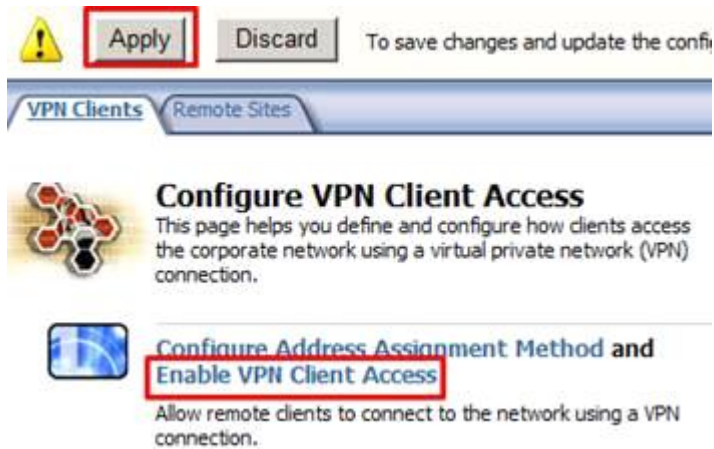


-Aunque viene por defecto, comprobamos que está utilizando como método de autenticación el MS-CHAPv2:

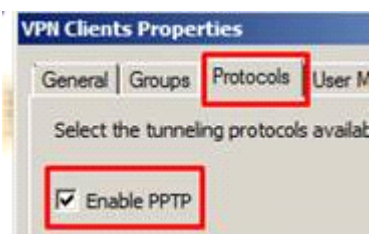
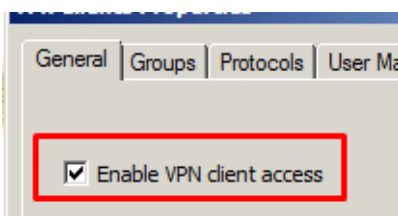


-Aplicamos la configuración

-Ahora habilitamos el acceso de clientes para VPN, simplemente pinchando en el apartado que marcamos en la siguiente foto:

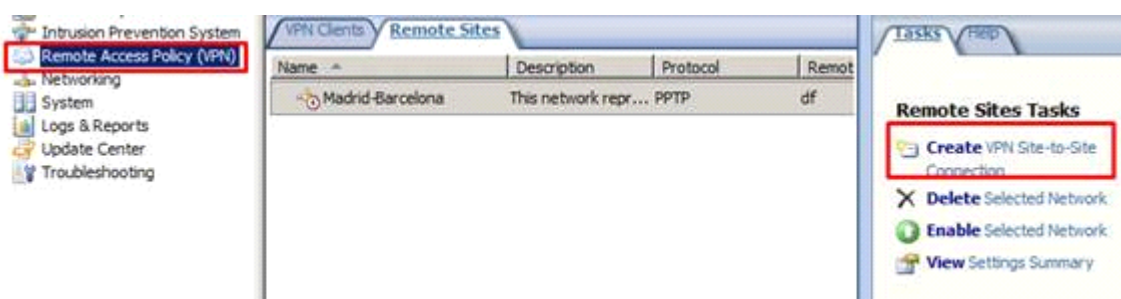


-Entramos en Verify VPN properties para comprobar que se ha habilitado correctamente el acceso de clientes y que además está activado el protocolo PPTP (protocolo que usamos para la configuración de la VPN).



Una vez hecho lo anterior, nos queda configurar el acceso remoto de Madrid.

-Entramos en Create VPN Site-to-Site Connection



-Asignamos como nombre del sitio, el nombre de usuario creado en Madrid:

Site-to-site network name:

a

-Como ya hemos comentado, indicamos que vamos a usar el protocolo PPTP (Protocolo de tunelización punto a punto):



-Registramos como sitio remoto de la VPN, la IP pública del servidor de Barcelona:

Remote site VPN server:

192.168.100.11

-A continuación, nos pregunta sobre la autenticación remota, así que, introducimos un nombre de usuario el cual será utilizado para crearnos el usuario de Barcelona cuando lleguemos a ese punto:

Remote Authentication
For the local site to initiate a connection to the remote site, a user account on the remote site is required for authentication.

☒ Allow the local site to initiate connections to the remote site, using this user account:

 The user account must match the name of the VPN site-to-site connection created on the remote site.

User name:

Domain:

Password:

Confirm password:

-Introducimos la red completa del servidor de Barcelona:

Network Addresses
Specify the IP address ranges of the remote site network. The match the internal ranges at the other end of the tunnel.

Address ranges:

Start Address	End Address
192.168.11.0	192.168.11.255

-Desactivamos el servicio Remote NLB, ya que no es necesario:

Remote NLB
If Network Load Balancing is enabled on the remote site, specify the dedicated IP addresses (DIPs) of the remote site gateway.

☐ The remote site is enabled for Network Load Balancing

Specify the dedicated IP addresses on the remote gateway:

-En este punto nos dice que va a crear una Regla para la VPN en Madrid, nosotros marcamos que queremos todo el tráfico:

Site-to-Site Network Access Rule
An access rule is required to allow traffic to and from the new VPN site-to-site network.

☒ Create an allow access rule. This rule will allow traffic between the Internal network and the new site-to-site network for all users.

Access rule name:

Apply the rule to these protocols:

-Aplicamos la configuración.

Accedemos al servidor de Barcelona

-Creamos un usuario con el nombre que hemos introducido en la autenticación remota de Madrid y asignamos permisos totales sobre el apartado Network Access Permission:



-Para comprobar que la VPN nos funcionará cuando la configuremos, vamos a habilitar la

regla para permitir todo el tráfico:

Order	Name	Action
1	Allow All	Allow

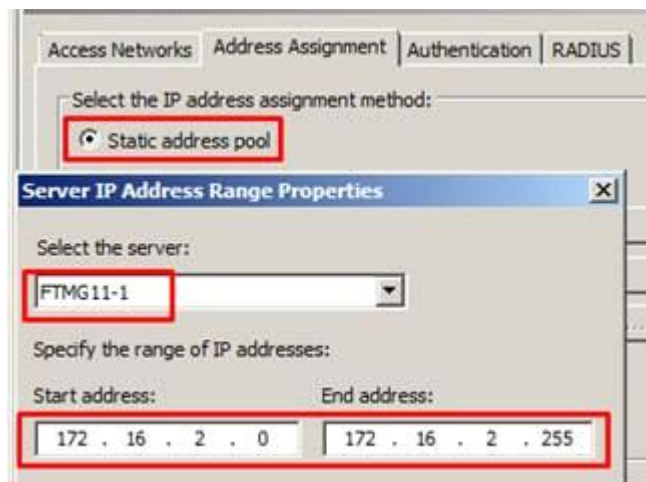
-Accedemos dentro de Remote Access Policy para configurar el método de asignación de IP's para la VPN:



-Marcamos la opción de direcciones estáticas.

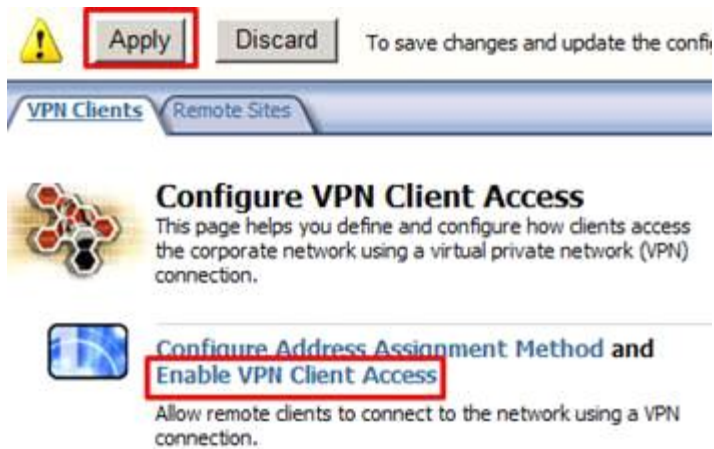
-Seleccionamos nuestro servidor de Madrid.

-Asignamos un pool de direcciones diferente al de Madrid, en este asignamos 172.16.2.0 - 172.16.2.255.

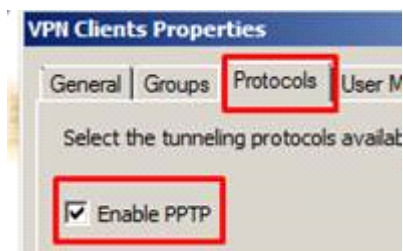
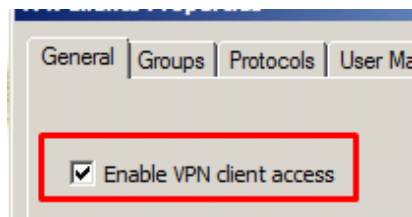
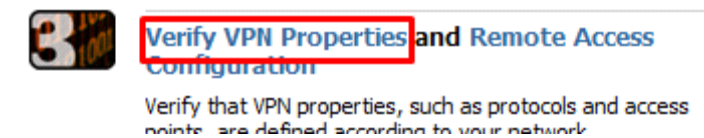


-Aplicamos la configuración

-Ahora habilitamos el acceso de clientes para VPN, simplemente pinchando en el apartado que marcamos en la siguiente foto:

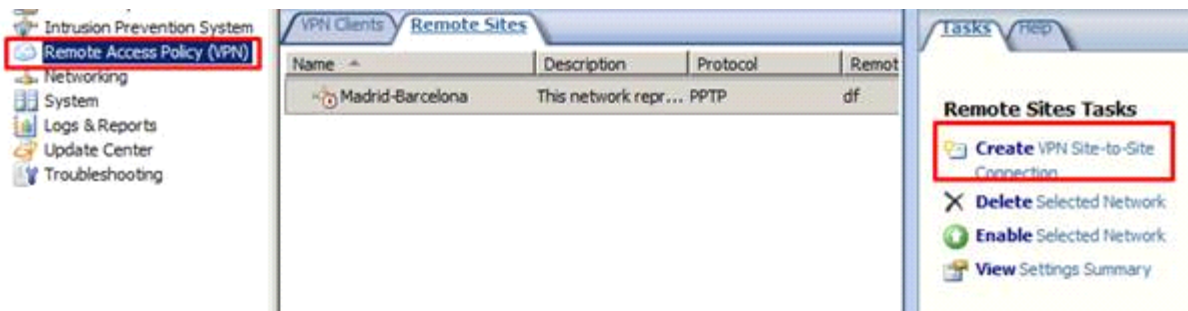


-Entramos en Verify VPN properties para comprobar que se ha habilitado correctamente el acceso de clientes y que además esta activado el protocolo PPTP (protocolo que usamos para la configuración de la VPN).



Una vez hecho lo anterior, nos queda configurar el acceso remoto de Barcelona.

-Entramos en Create VPN Site-to-Site Connection



-Asignamos como nombre del sitio, el nombre de usuario de Barcelona:

Site-to-site network name:

-Indicamos que vamos a usar el protocolo PPTP

VPN Protocol
Select the VPN protocol used to protect traffic sent between the sites.

☐ **IP Security protocol (IPsec) tunnel mode**
Provides high security and interoperability with third party VPN vendors.

☐ **Layer Two Tunneling Protocol (L2TP) over IPsec**
Provides a highly secured connection method.

☒ **Point-to-Point Tunneling Protocol (PPTP)**
Provides a secured connection method.

-Registramos como sitio remoto de la VPN, la IP pública , ahora del servidor de Madrid:

Remote Site Gateway
Enter the IP address or server name (FQDN) of the remote site VPN

Remote site VPN server:

-Nos pregunta sobre la autenticación remota, así que, introducimos el nombre del usuario creado para Madrid:

Remote Authentication
For the local site to initiate a connection to the remote site, a user account on the remote site is required for authentication.

☒ Allow the local site to initiate connections to the remote site, using this user account:

The user account must match the name of the VPN site-to-site connection created on the remote site.

User name:

Domain:

Password:

Confirm password:

-Introducimos la red completa del servidor de Madrid:

Network Addresses
Specify the IP address ranges of the remote site network. They must match the internal ranges at the other end of the tunnel.

Address ranges:

Start Address	End Address
192.168.10.0	192.168.10.255

-Desactivamos el servicio Remote NLB, ya que no es necesario:

Remote NLB
If Network Load Balancing is enabled on the remote site, specify the IP addresses (DIPs) of the remote site gateway.

☐ The remote site is enabled for Network Load Balancing

Specify the dedicated IP addresses on the remote gateway:

-En este punto nos dice que va a crear una Regla para la VPN en Barcelona, nosotros marcamos que queremos todo el tráfico:

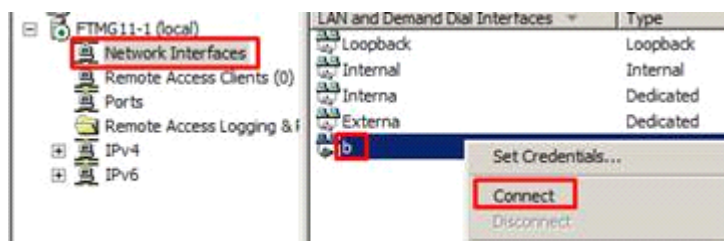
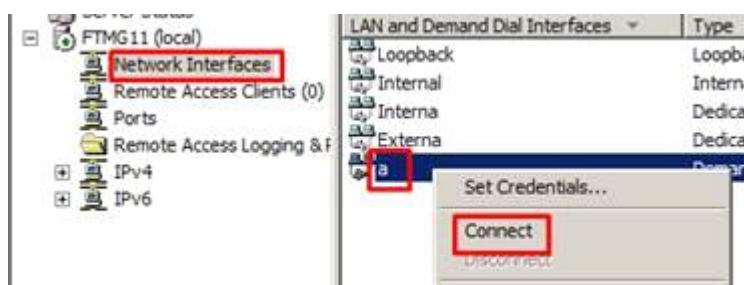
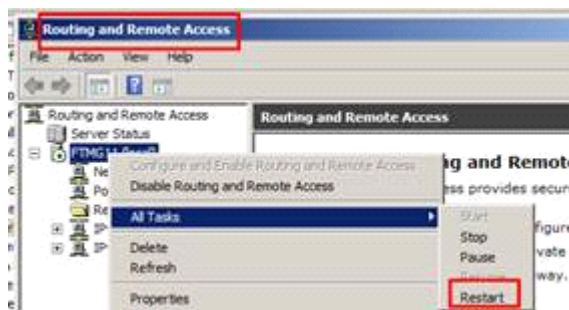
Site-to-Site Network Access Rule

An access rule is required to allow traffic to and from the new VPN site-to-site network.



-Aplicamos la configuración:

Accedemos tanto al servidor de Madrid como al de Barcelona para reiniciar el servicio Routing and Remote Access y conectar la interfaz de cada uno, generada por la VPN:



Comprobación:

-Accedemos al cliente alojado en la red de Madrid, y realizamos un ping hacia el cliente alojado en la red de Barcelona y viceversa:

Madrid - Barcelona:

```
C:\Users\Adrian>ping 192.168.11.104

Haciendo ping a 192.168.11.104 con 32 bytes de datos:
Respuesta desde 192.168.11.104: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.11.104: bytes=32 tiempo<1m TTL=126
Respuesta desde 192.168.11.104: bytes=32 tiempo<1m TTL=126
Respuesta desde 192.168.11.104: bytes=32 tiempo<1m TTL=126

Estadísticas de ping para 192.168.11.104:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Barcelona - Madrid:

```
C:\Users\Adrian>ping 192.168.10.101

Haciendo ping a 192.168.10.101 con 32 bytes de datos:
Respuesta desde 192.168.10.101: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.101: bytes=32 tiempo=18ms TTL=126
Respuesta desde 192.168.10.101: bytes=32 tiempo=205ms TTL=126
Respuesta desde 192.168.10.101: bytes=32 tiempo<1m TTL=126

Estadísticas de ping para 192.168.10.101:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 205ms, Media = 56ms
```

-Realizamos un tracert para comprobar, que utiliza la IP de conexión de la VPN para llegar al destino:

```
C:\Users\Adrian>tracert 192.168.10.101

Traza a 192.168.10.101 sobre caminos de 30 saltos como máximo.

 1  <1 ms    *          <1 ms  FTMG11 [192.168.11.1]
 2  <1 ms    <1 ms     <1 ms  172.16.0.5
 3   1 ms    <1 ms     1 ms   192.168.10.101

Traza completa.
```