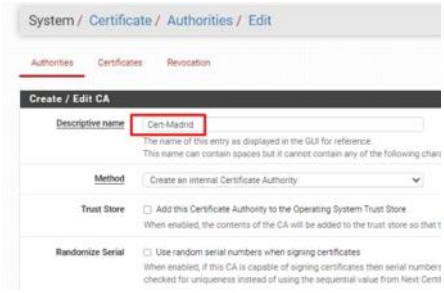
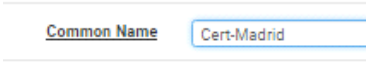
VPN entre 2 PFSENSE con OpenVPN

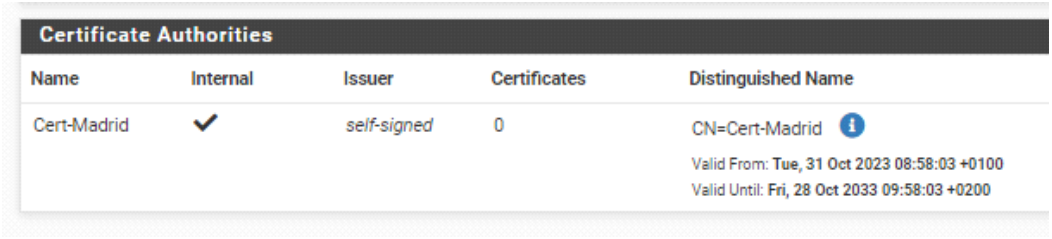
martes, 31 de octubre de 2023 10:57

El objetivo de esta práctica es configurar una VPN en nuestros servidores pfsense, utilizando el protocolo **OpenVPN** utilizando entidades certificadoras.

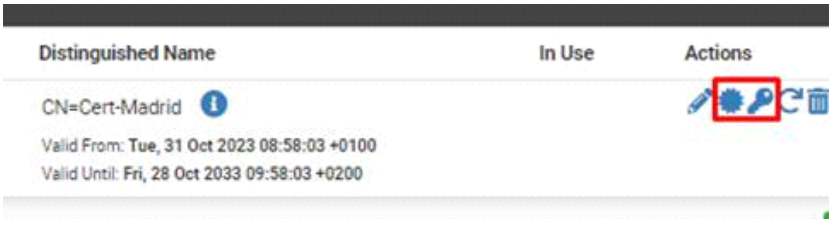
1. El primer paso será crear una entidad certificadora en el servidor de Madrid:



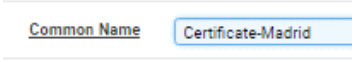




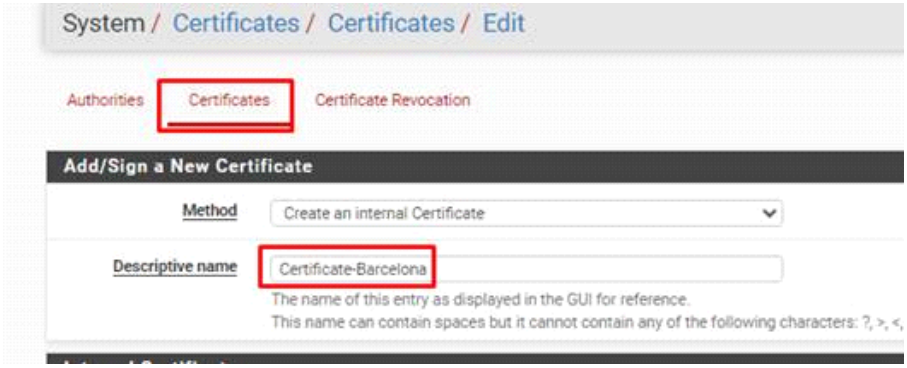
2. Descargamos el certificado y su clave, ya que liego será necesario para exportarlas al servidor de Barcelona:

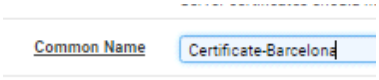


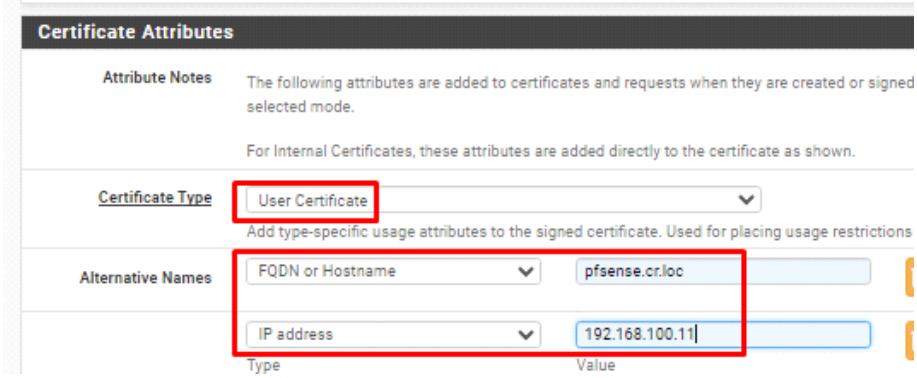
3. A continuación, creamos un certificado de tipo servidor en el servidor de Madrid:



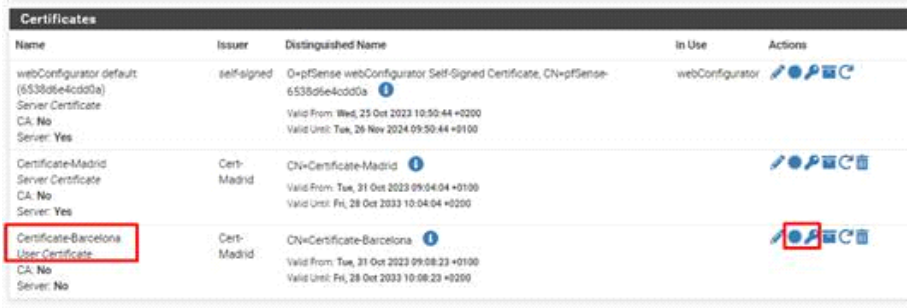
4. Creamos otro certificado en Madrid, pero ahora de tipo usuario para el servidor de Barcelona:





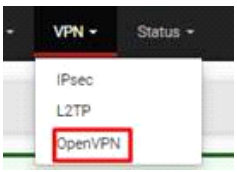


5. Descargamos el certificado y la clave del certificado de tipo usuario creado para Barcelona:

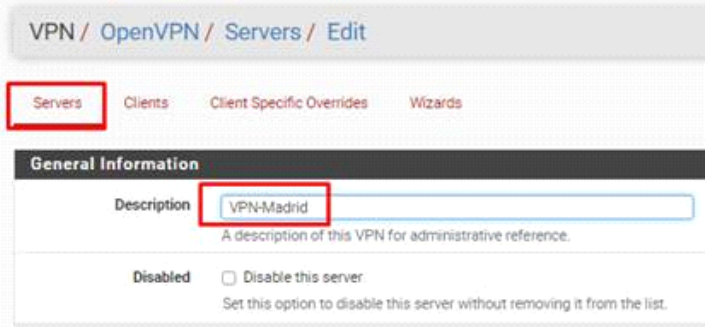


6. Una vez configurado los certificados, configuramos el protocolo OpenVPN:

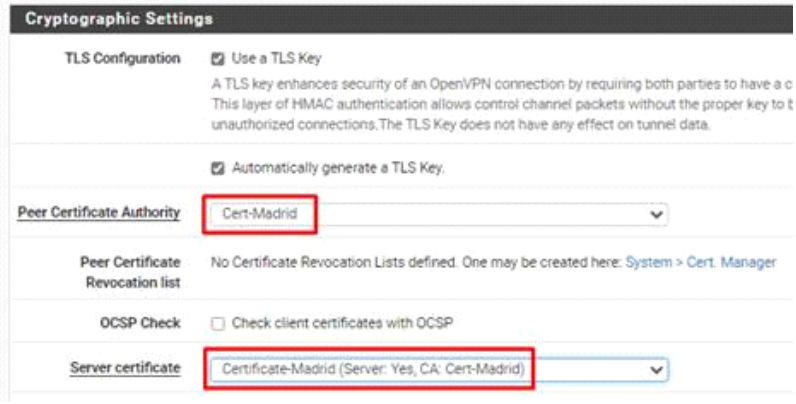
- Accedemos al protocolo:



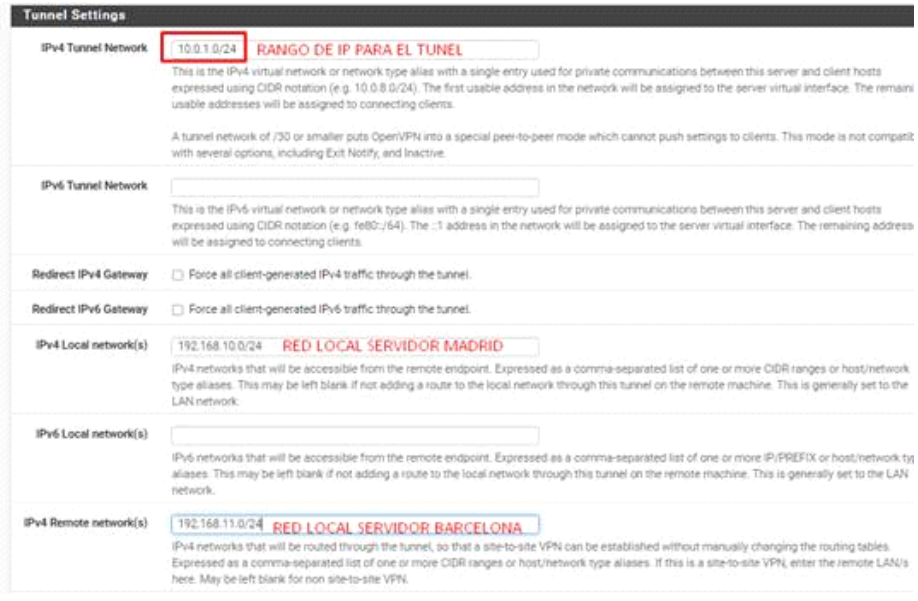
- Dentro de servers pulsamos en ADD…asignamos una descripción para saber que es la configuración de la VPN de Madrid:



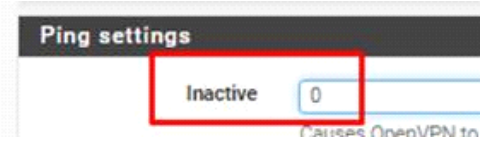
- Indicamos que use el certificado de Madrid creado en el servidor de Madrid:



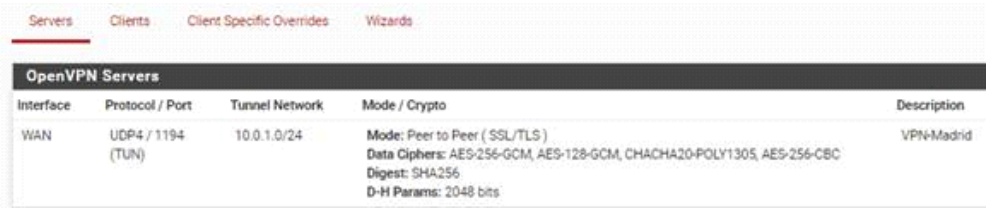
- Asignamos un rango de IP para la configuración del túnel.
- En el apartado IPv4 Local Network utilizamos la Red Local de Madrid.
- Utilizamos la Red Local de Barcelona para la configuración de IPv4 Remote network.



- Tenemos que indicar, que no queremos que se cierre la conexión VPN, esto se hace añadiendo un **0** en el apartado **Inactive**:

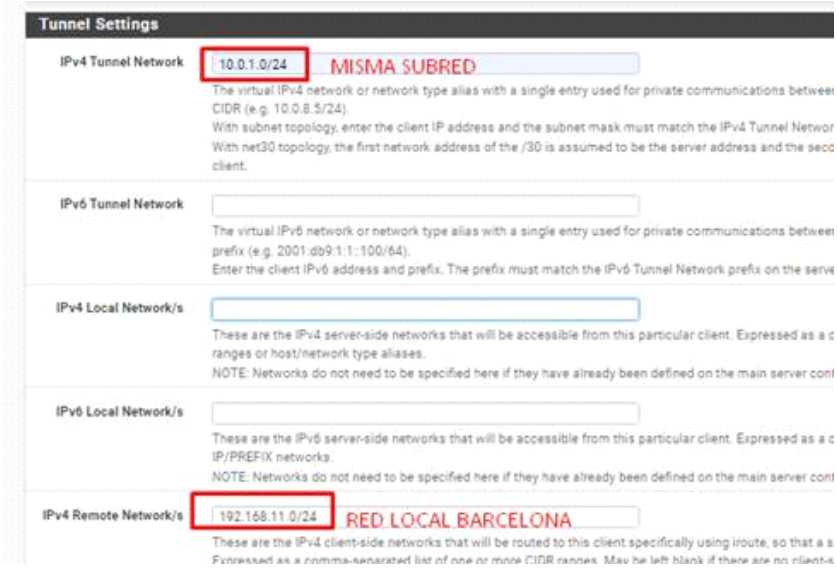


- Guardamos la configuración y vemos que se ha creado correctamente:



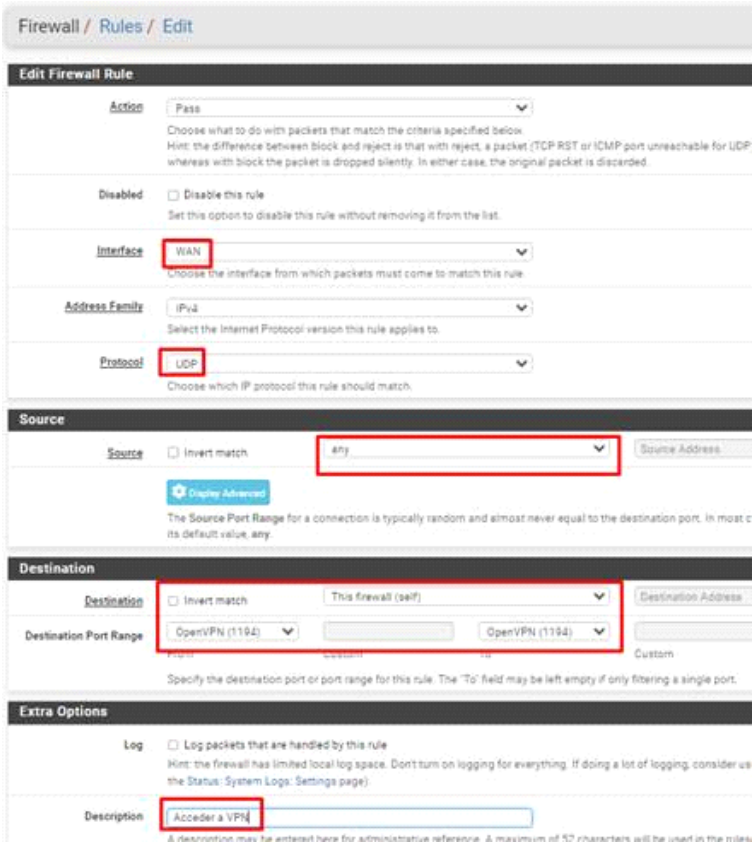
7. Editamos la configuración para copiar su clave TLS y la guardamos en un **archivo.txt**, que será exportada al servidor de Barcelona:

8. A continuación, tenemos que crear un override de clientes para asociar una subred a un certificado, así podremos enrutar**, asignamos el mismo common Name que al certificado creado de Barcelona**:

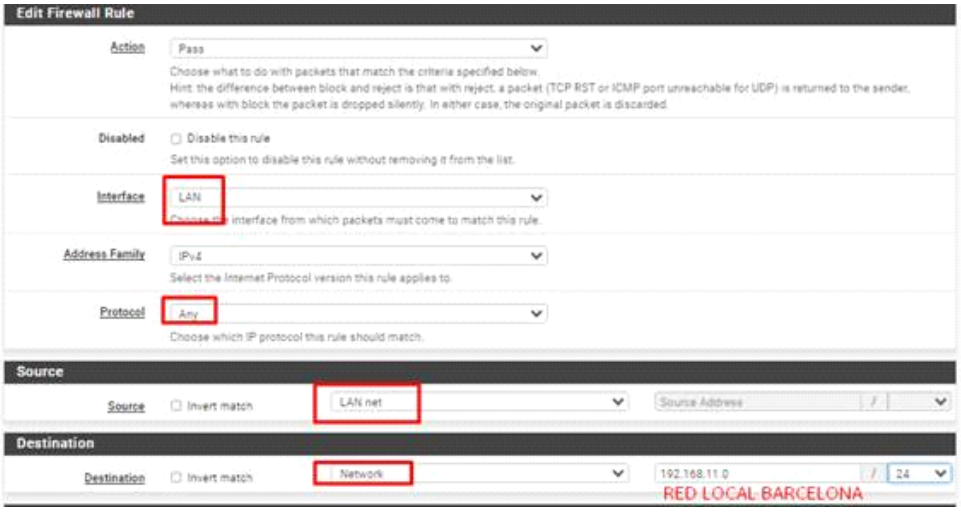


9. Configuramos reglas, para poder permitir la comunicación entre Madrid y Barcelona:

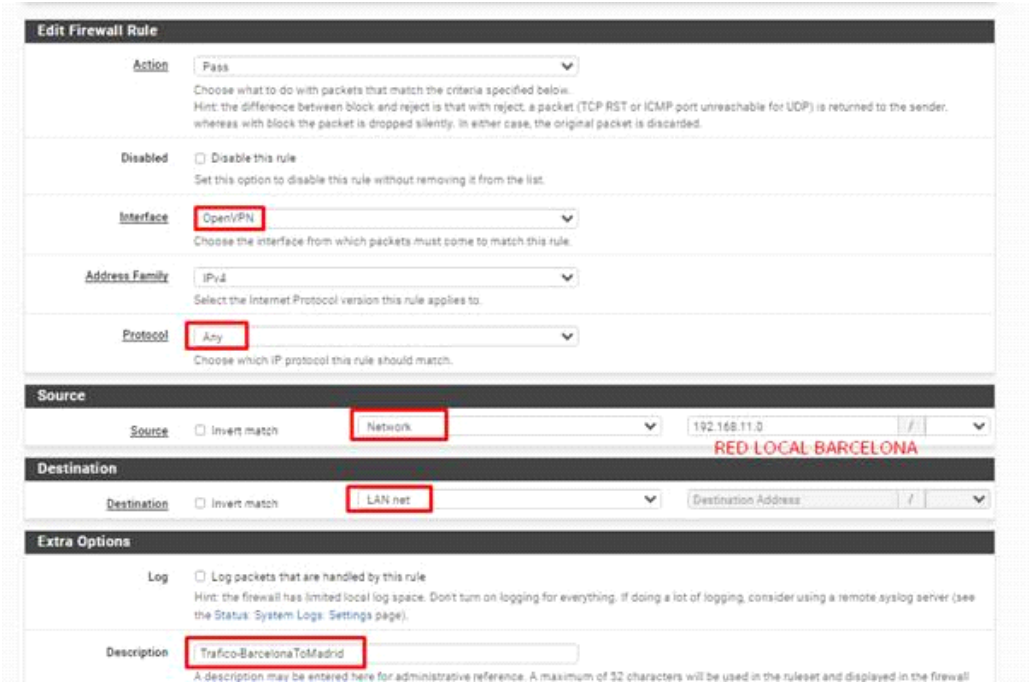
- Primera regla:



- Segunda regla:

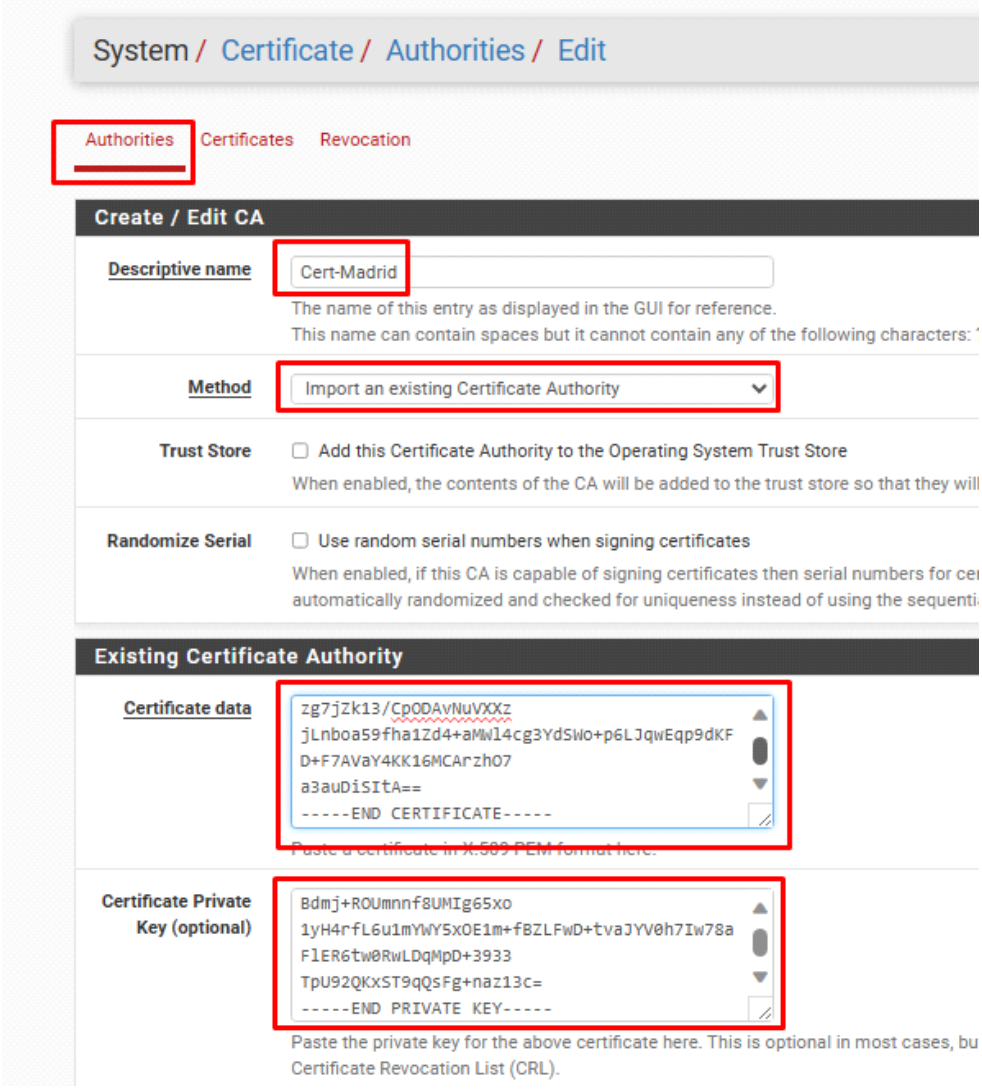


- Tercera regla:

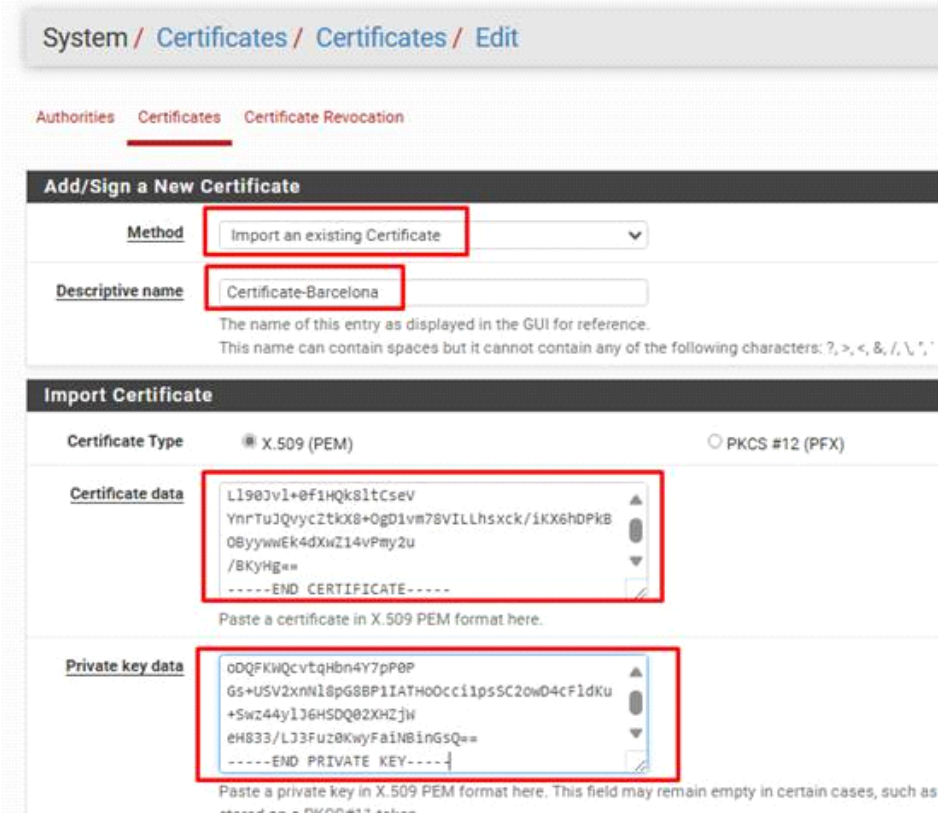


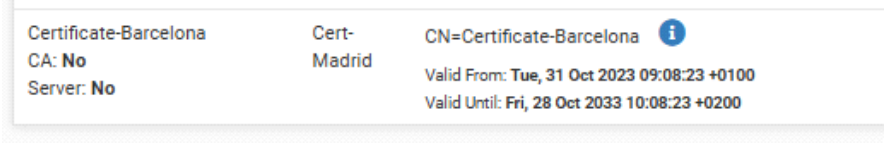
10. Ya hemos terminado la configuración de Madrid, ahora vamos a importar los certificados en el servidor de Barcelona:

- Dentro de **Authorities** asignamos el mismo nombre que al **CA** de Madrid e importamos el **.cert** y el **.key** de Madrid:

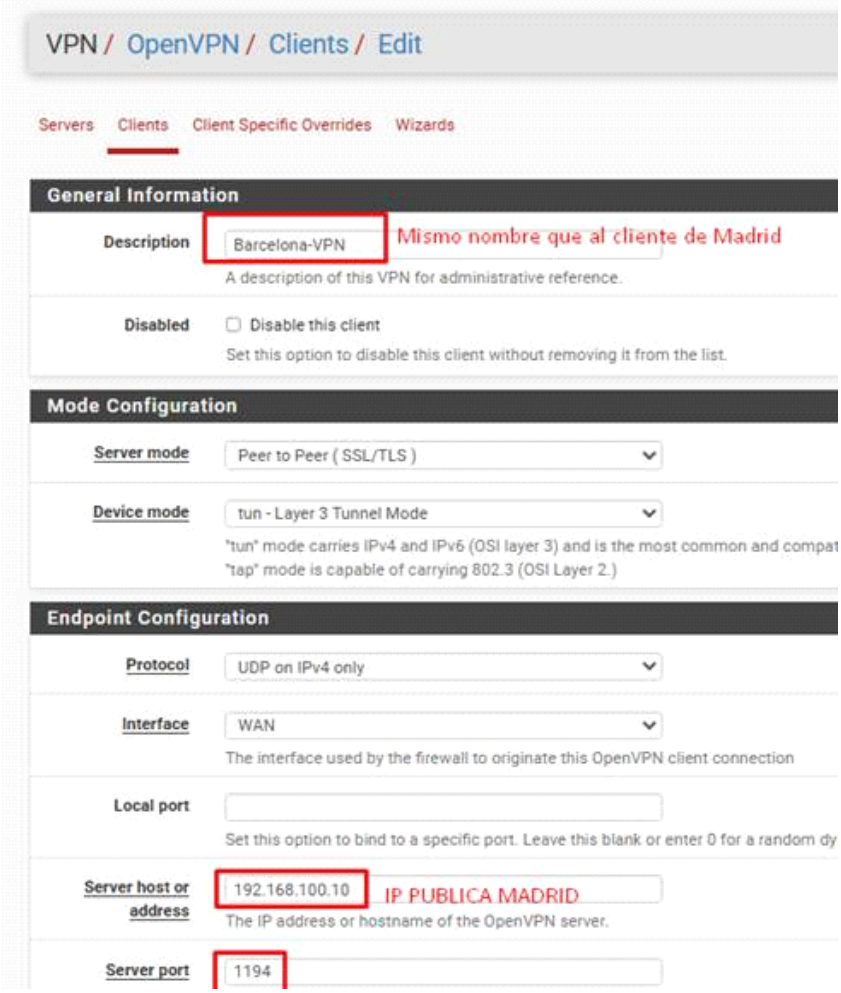


- Dentro de **Certificates** asignamos el mismo nombre que al **cert** de Barcelona e importamos el **.cert** y el **.key** de Barcelona creado en Madrid:

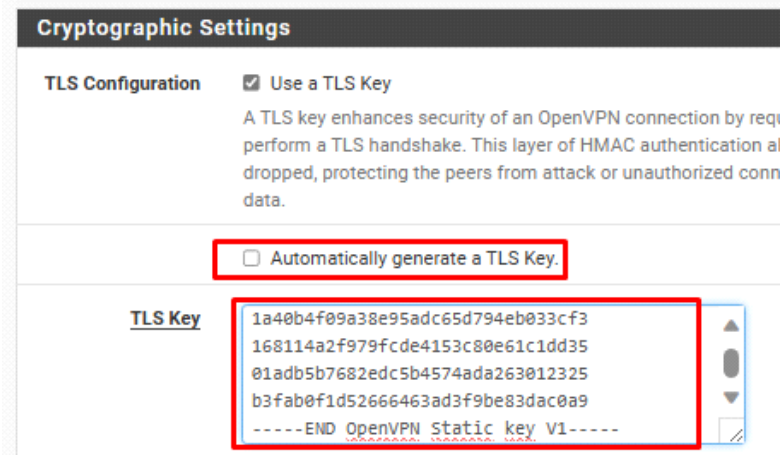


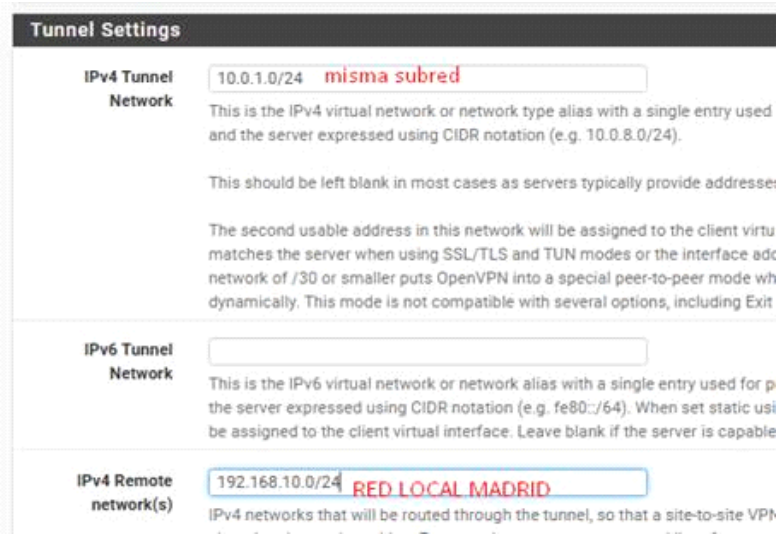


11. Por último, configuramos el cliente VPN en Barcelona:

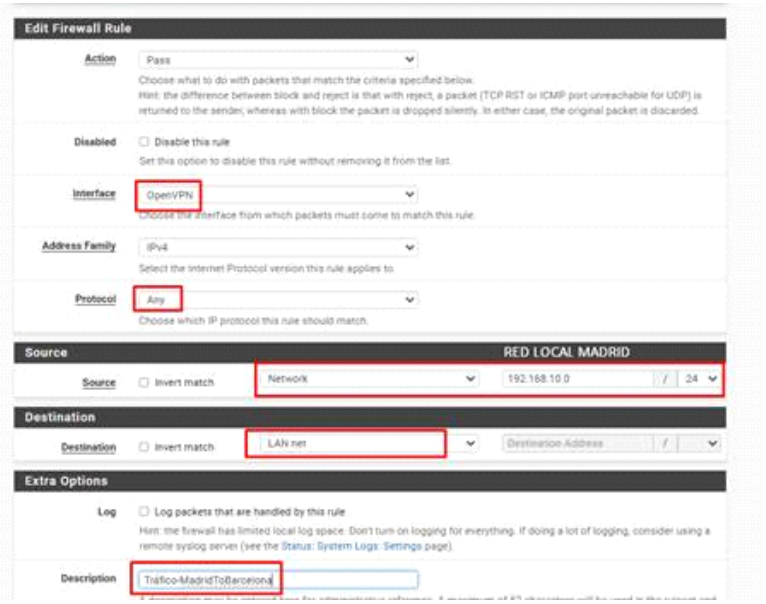


-Pegamos el contenido del fichero TLS, creado anteriormente en Madrid:





12. Creamos una regla para permitir la comunicación entre Madrid y Barcelona mediante la VPN:



Reiniciamos los servicios de las dos oficinas dentro de Status > OpenVPN…
Comprobaciones:

- Realizamos un ping entre un cliente de Madrid hacia uno de Barcelona:

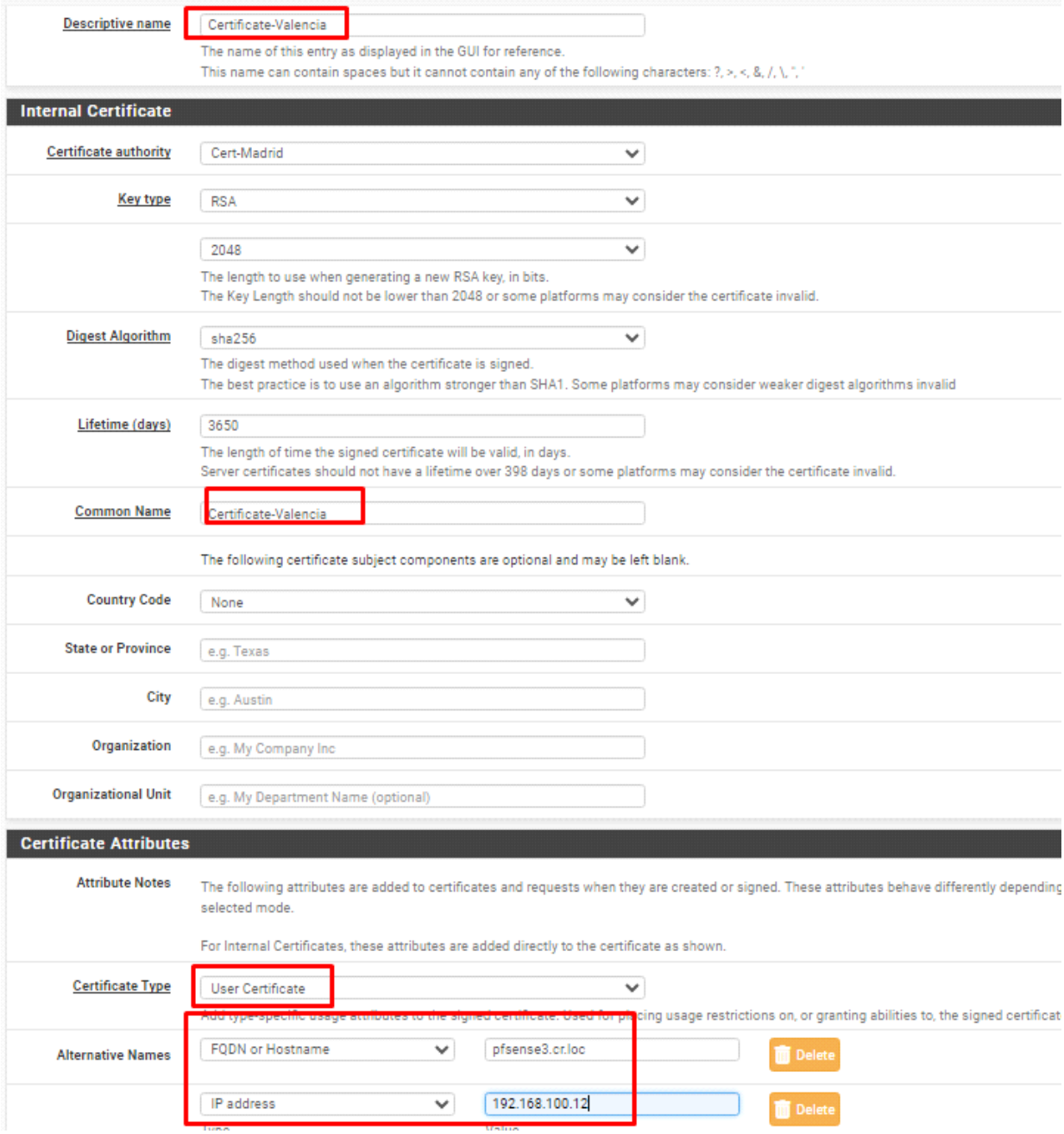
```
C:\Users\User01>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet0:

   Sufijo DNS específico para la conexión. . : cr.loc
   Vínculo: dirección IPv6 local. . . : fe80::ee45:e7cc:fa70:e2d8%13
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.10.201
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.10.1

C:\Users\User01>ping 192.168.11.201

Haciendo ping a 192.168.11.201 con 32 bytes de datos:
Respuesta desde 192.168.11.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.11.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.11.201: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.11.201: bytes=32 tiempo=1ms TTL=126

Estadísticas de ping para 192.168.11.201:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\User01>tracert 192.168.11.201

Traza a 192.168.11.201 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  pfsense.cr.loc [192.168.10.1]
  2     1 ms    <1 ms    <1 ms  10.0.1.0
  3     1 ms     1 ms     1 ms  192.168.11.201

Traza completa.
```

- Realizamos un ping entre un cliente de Barcelona hacia uno de Madrid:

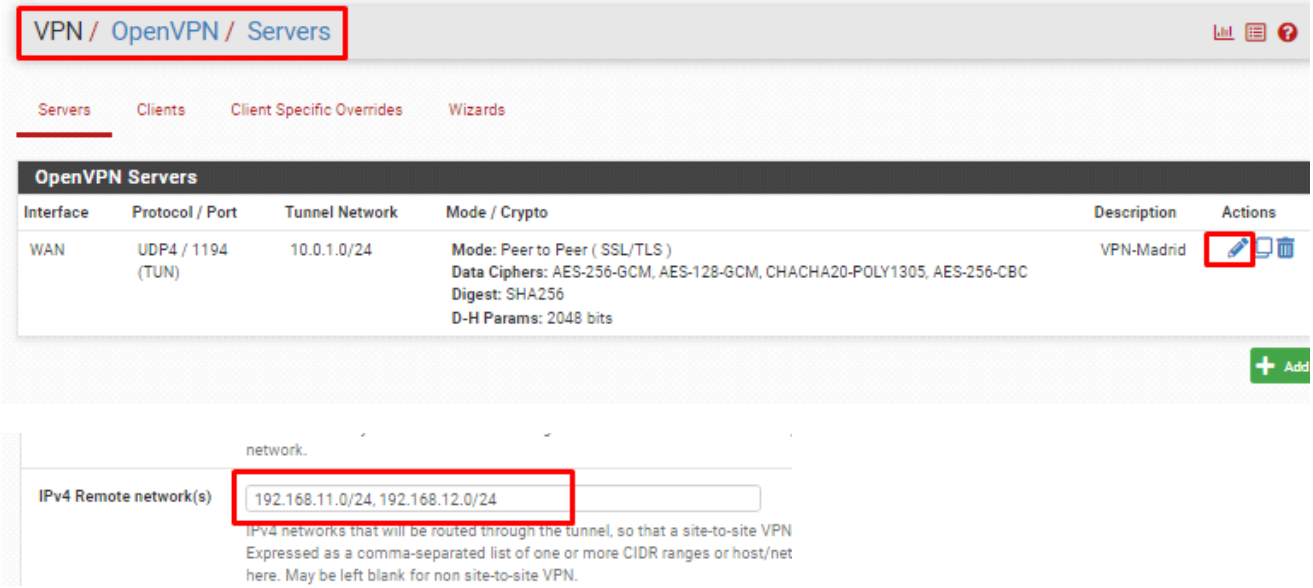
```
C:\Users\Adrian>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet0:

   Sufijo DNS específico para la conexión. . : home.arpa
   Vínculo: dirección IPv6 local. . . : fe80::a3ed:2a87:e038:b82f%13
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.11.201
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.11.1

C:\Users\Adrian>ping 192.168.10.201

Haciendo ping a 192.168.10.201 con 32 bytes de datos:
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=2ms TTL=126

Estadísticas de ping para 192.168.10.201:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\Adrian>tracert 192.168.10.201

Traza a 192.168.10.201 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  pfsense.home.arpa [192.168.11.1]
  2     1 ms     1 ms     1 ms  10.0.1.1
  3     1 ms     1 ms     1 ms  192.168.10.201

Traza completa.
```

-Si queremos configurar valencia, dentro de Madrid tenemos que…

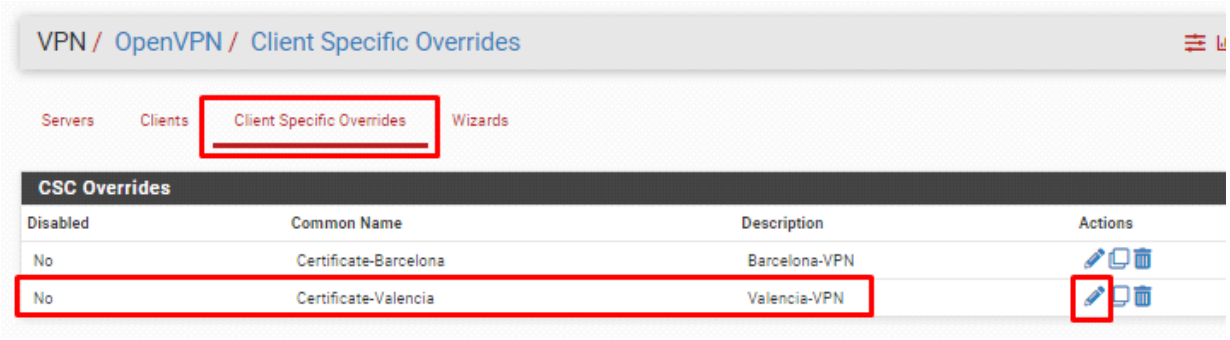
-Crear un certificado para valencia:

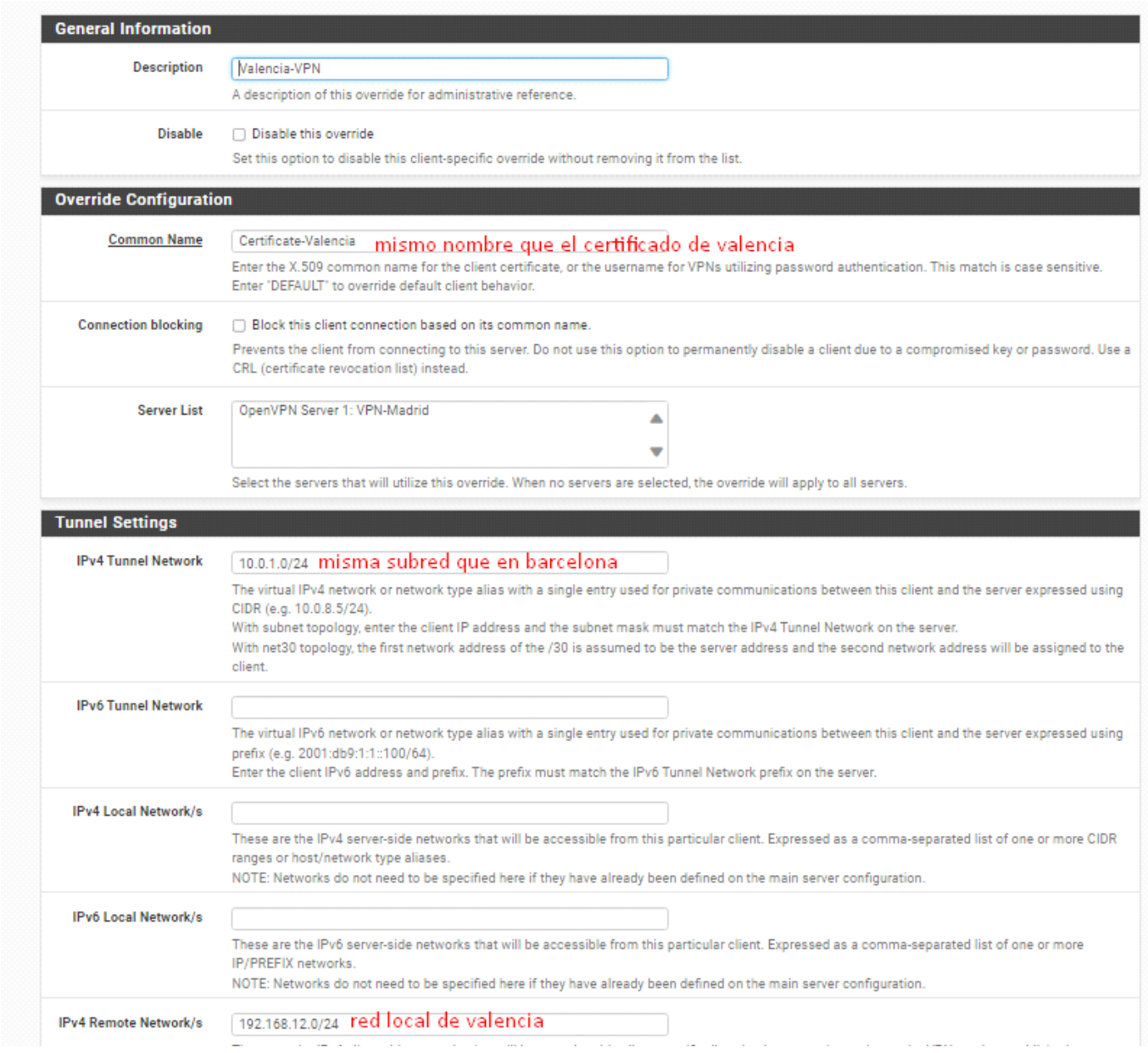


-Añadimos su IP remota en el server:

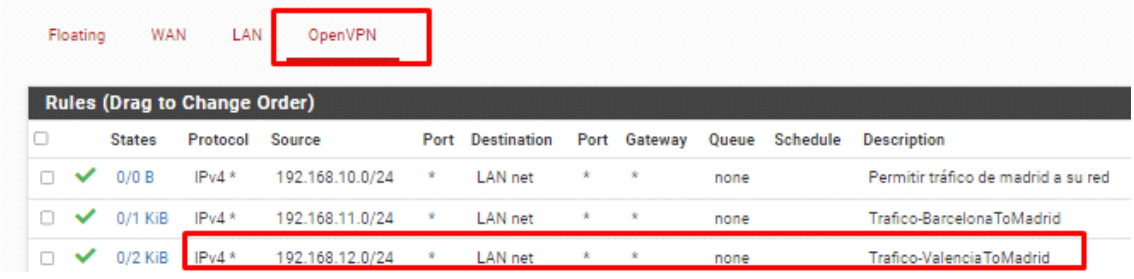


-Creamos un nuevo override:



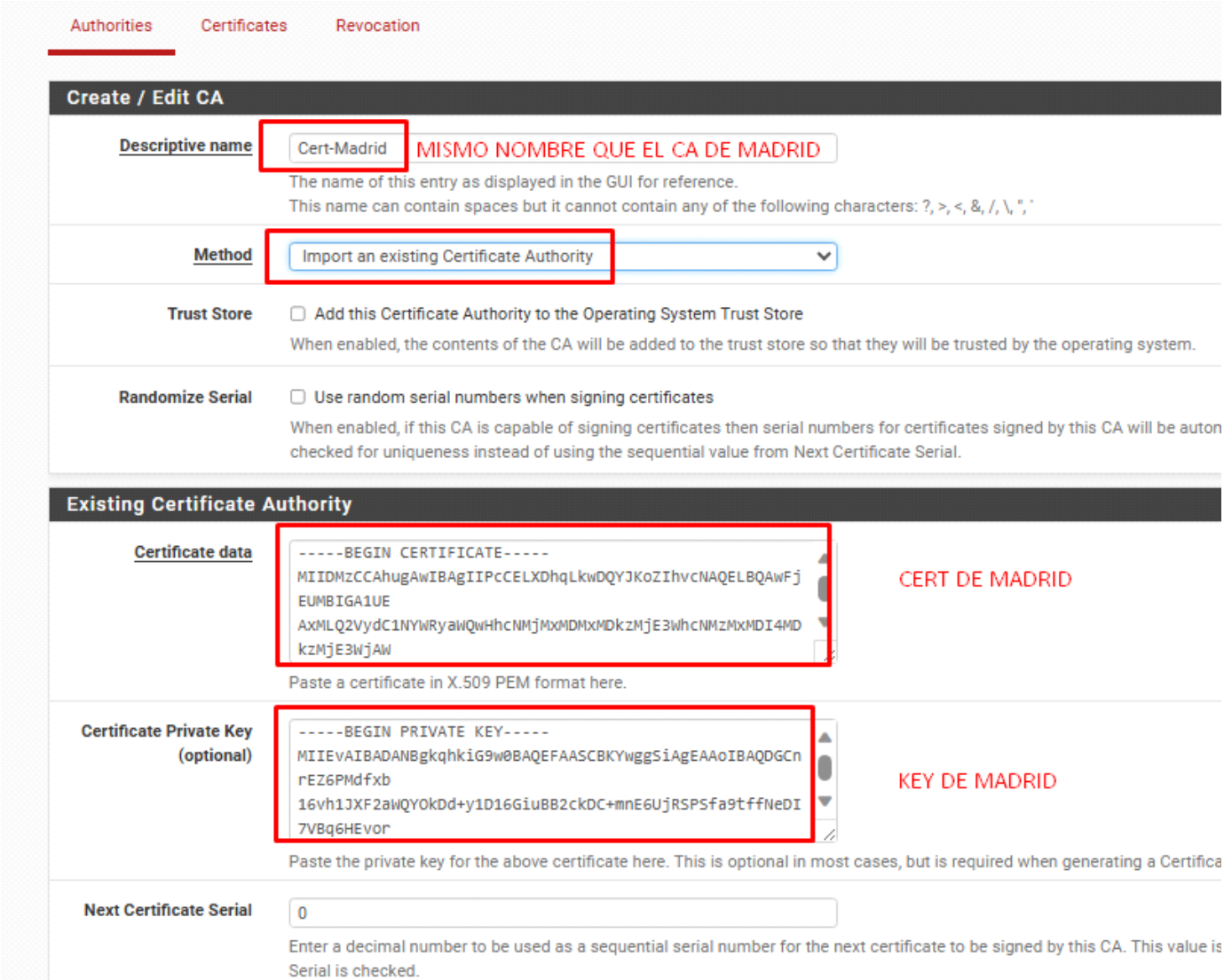


-Añadimos una regla en Madrid, para permitir tráfico de valencia a madrid:



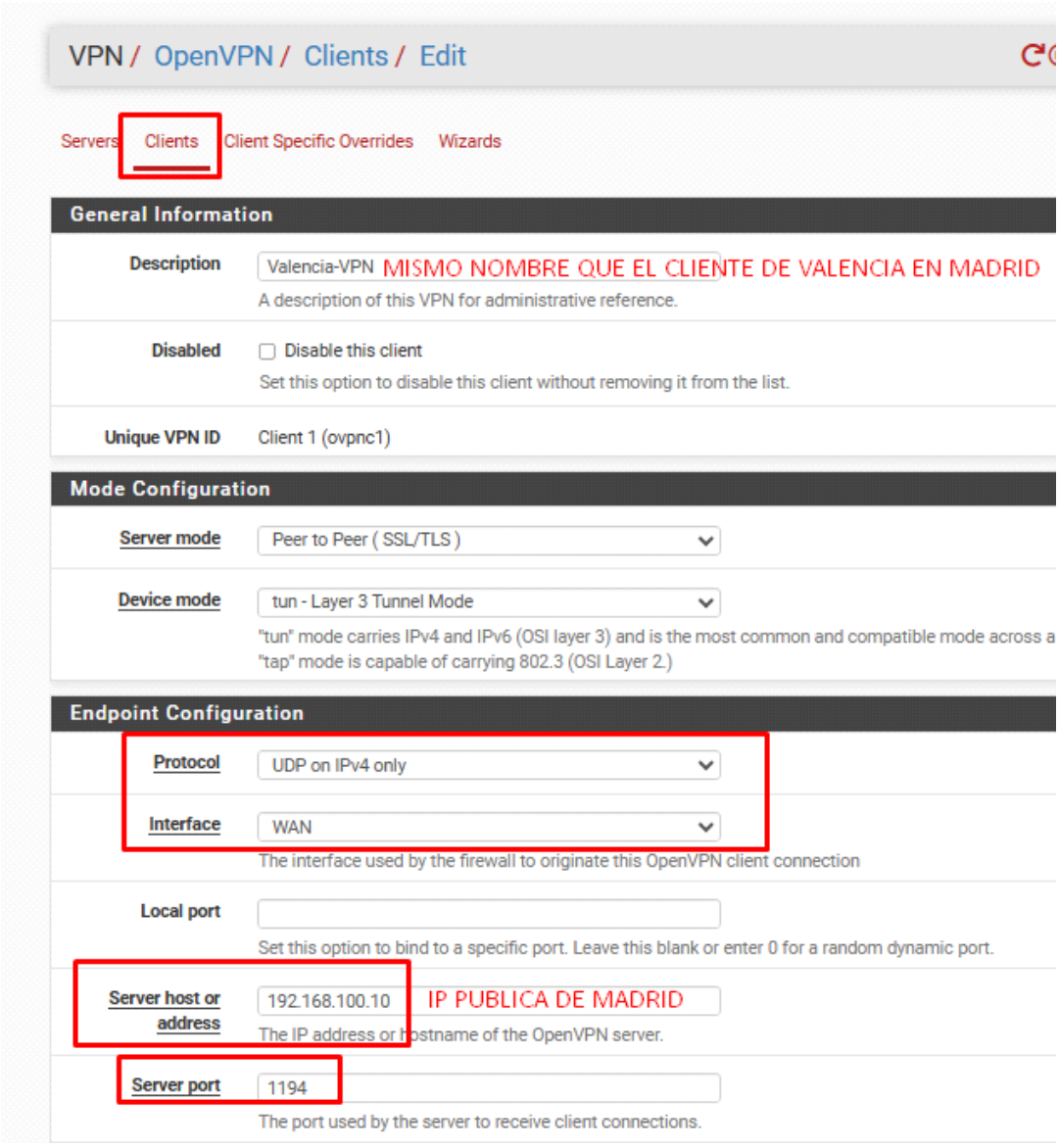
Dentro de valencia…

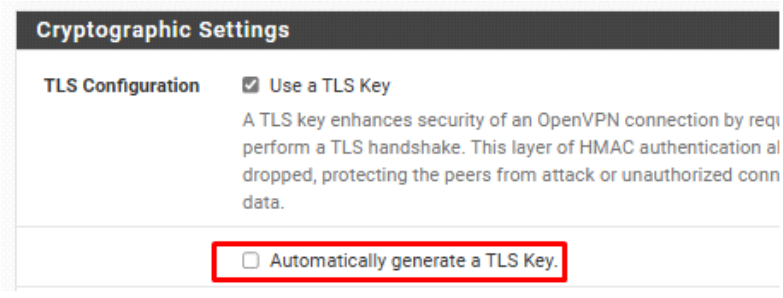
-Importamos el CA de Madrid:

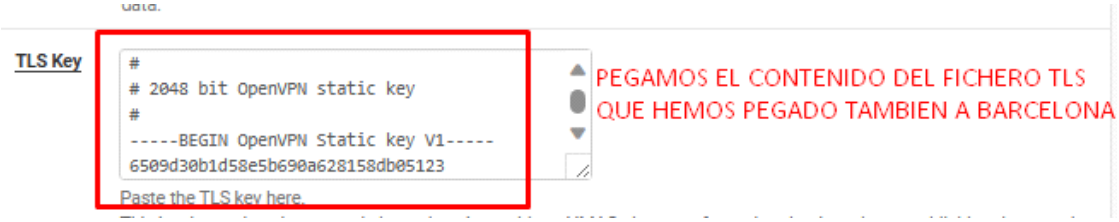


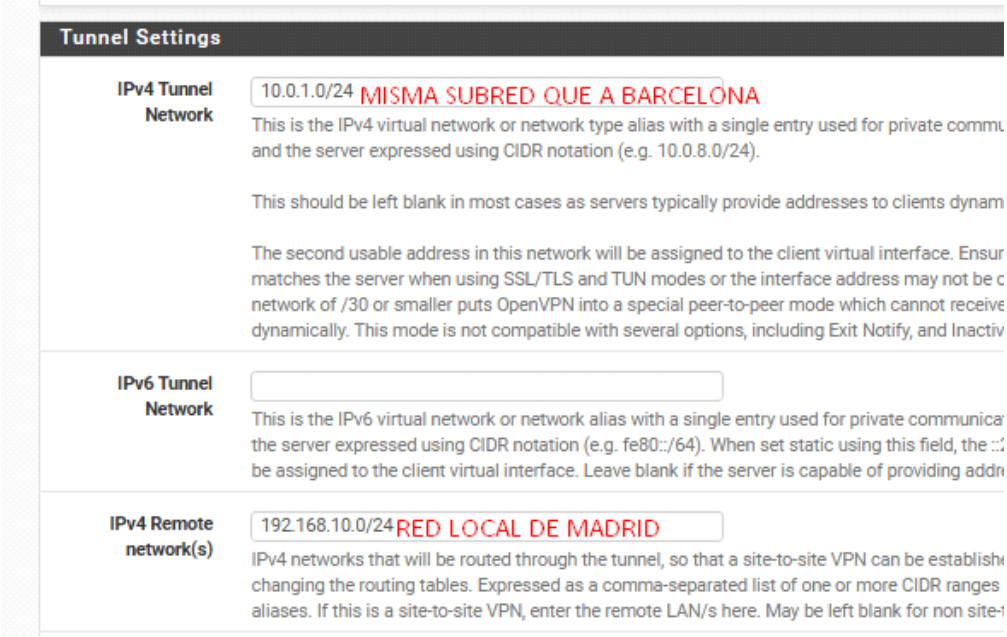
-Importamos el certificado de Valencia que hemos creado en Madrid:

-Configuramos el cliente VPN en Valencia:

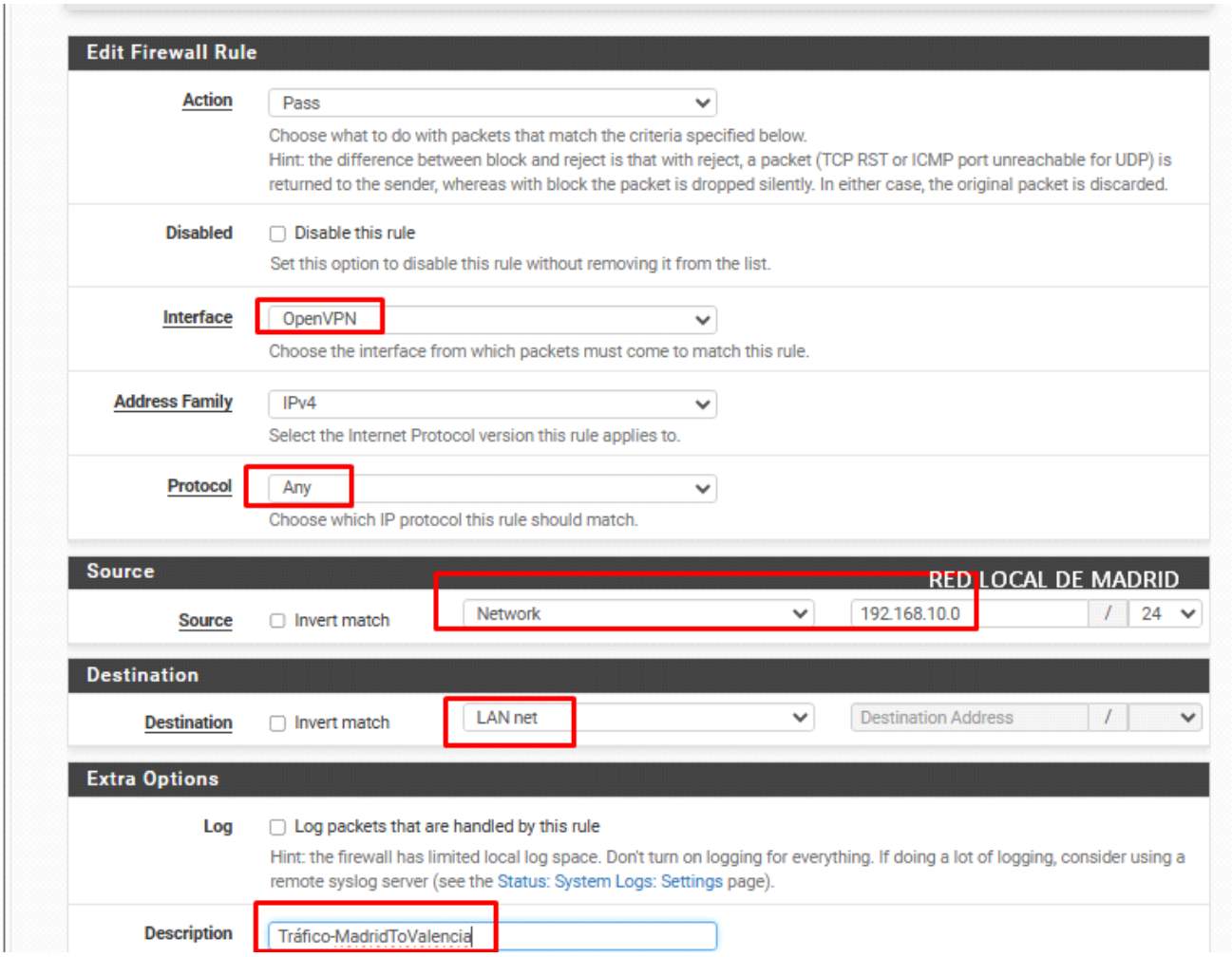

VPN / OpenVPN / Clients / Edit
Servers
Clients
Client Specific Overrides
Wizards
General Information
Description
Valencia-VPN MISMO NOMBRE QUE EL CLIENTE DE VALENCIA EN MADRID
A description of this VPN for administrative reference.
Disabled
Disable this client
Set this option to disable this client without removing it from the list.
Unique VPN ID
Client 1 (ovpnc1)
Mode Configuration
Server mode
Peer to Peer (SSL/TLS)
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across a
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration
Protocol
UDP on IPv4 only
Interface
WAN
The interface used by the firewall to originate this OpenVPN client connection
Local port
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
Server host or address
192.168.100.10
IP PUBLICA DE MADRID
The IP address or hostname of the OpenVPN server.
Server port
1194
The port used by the server to receive client connections.


Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requ
perform a TLS handshake. This layer of HMAC authentication al
dropped, protecting the peers from attack or unauthorized conn
data.
Automatically generate a TLS Key.


TLS Key
#
2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
6509d30b1d58e5b690a628158db05123
Paste the TLS key here.
PEGAMOS EL CONTENIDO DEL FICHERO TLS
QUE HEMOS PEGADO TAMBIEN A BARCELONA



-Creamos una regla para permitir el tráfico entre Madrid y Valencia:



Comprobación:

-Madrid-Valencia:

```
C:\Users\User01>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet0:

   Sufijo DNS específico para la conexión. . : cr.loc
   Vínculo: dirección IPv6 local. . . : fe80::ee45:e7cc:fa70:e2d8%13
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.10.201
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.10.1

C:\Users\User01>ping 192.168.12.202

Haciendo ping a 192.168.12.202 con 32 bytes de datos:
Respuesta desde 192.168.12.202: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.12.202: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.12.202: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.12.202: bytes=32 tiempo=2ms TTL=126

Estadísticas de ping para 192.168.12.202:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\User01>tracert 192.168.12.202

Traza a 192.168.12.202 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  pfsense.cr.loc [192.168.10.1]
  2     1 ms     1 ms    <1 ms  10.0.1.0
  3     1 ms    <1 ms    <1 ms  192.168.12.202

Traza completa.
```

-Valencia-Madrid:

```
C:\Users\Adrian>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet0:

   Sufijo DNS específico para la conexión. . : cr.loc
   Vínculo: dirección IPv6 local. . . : fe80::ec3b:fc37:5b4b:1491%5
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.12.202
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.12.1

C:\Users\Adrian>ping 192.168.10.201

Haciendo ping a 192.168.10.201 con 32 bytes de datos:
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.10.201: bytes=32 tiempo=2ms TTL=126

Estadísticas de ping para 192.168.10.201:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\Adrian>tracert 192.168.10.201

Traza a 192.168.10.201 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  pfsense3.cr.loc [192.168.12.1]
  2     1 ms    <1 ms    <1 ms  10.0.1.1
  3     1 ms     1 ms     1 ms  192.168.10.201

Traza completa.
```