VPN entre 2 PFSENSE con IPSEC

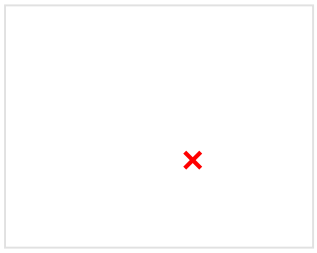
jueves, 26 de octubre de 2023 10:49

Configuración de VPN (IPSEC con clave compartida) mediante Firewalls Pfsense

Vamos a configurar una VPN mediante IPSEC con clave compartida (protocolo para crear túneles cifrados en internet) site-to-site “Sitio a Sitio” utilizando pfsense, esta conexión nos permitirá enlazar 2 ubicaciones, en nuestro caso la oficina de Madrid con la de Barcelona y a la inversa para que los dispositivos de cada oficina se puedan ver entre las ubicaciones.

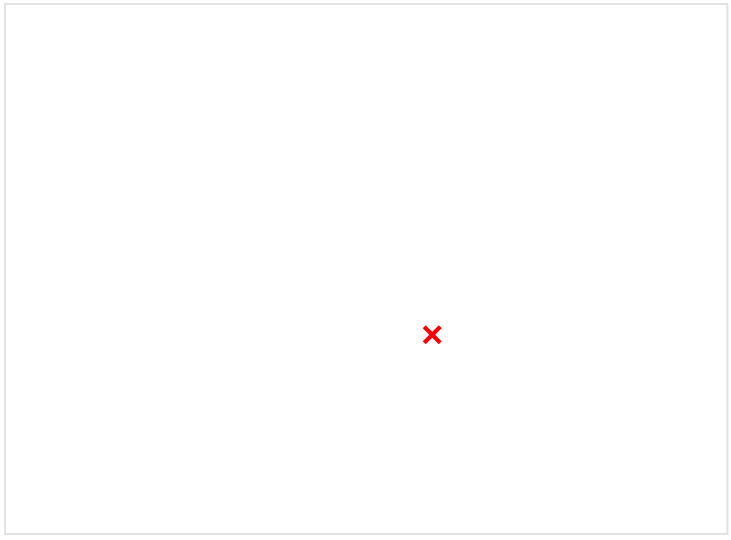
Configuración VPN Oficina Madrid

1. Accedemos al apartado VPN-Ipsec:

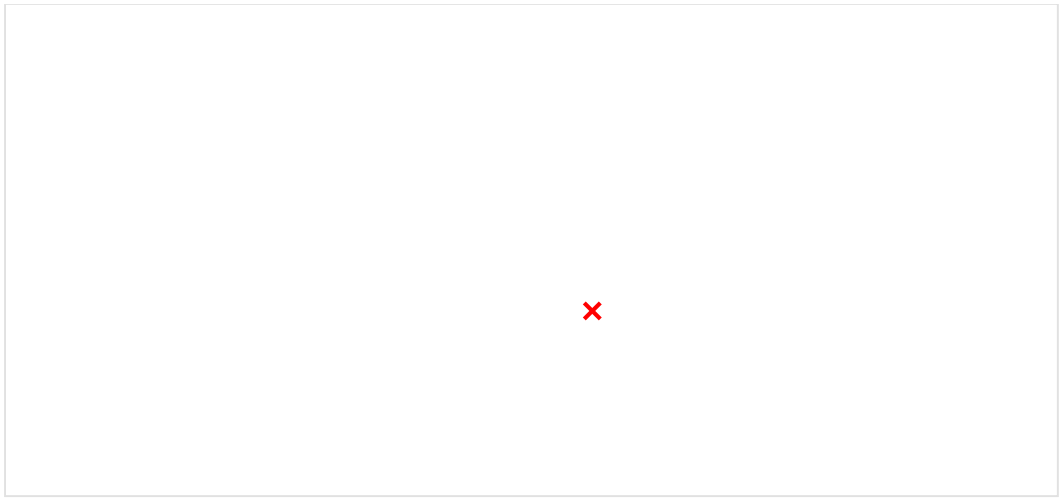


2. Dentro de Tunnels, pulsamos en Add p1 para configurar la primera parte del túnel Ipsec:

3. Indicamos que utilice la versión IKEv2 y que como Remote Gateway utilice la IP pública del pfsense de **Barcelona**:

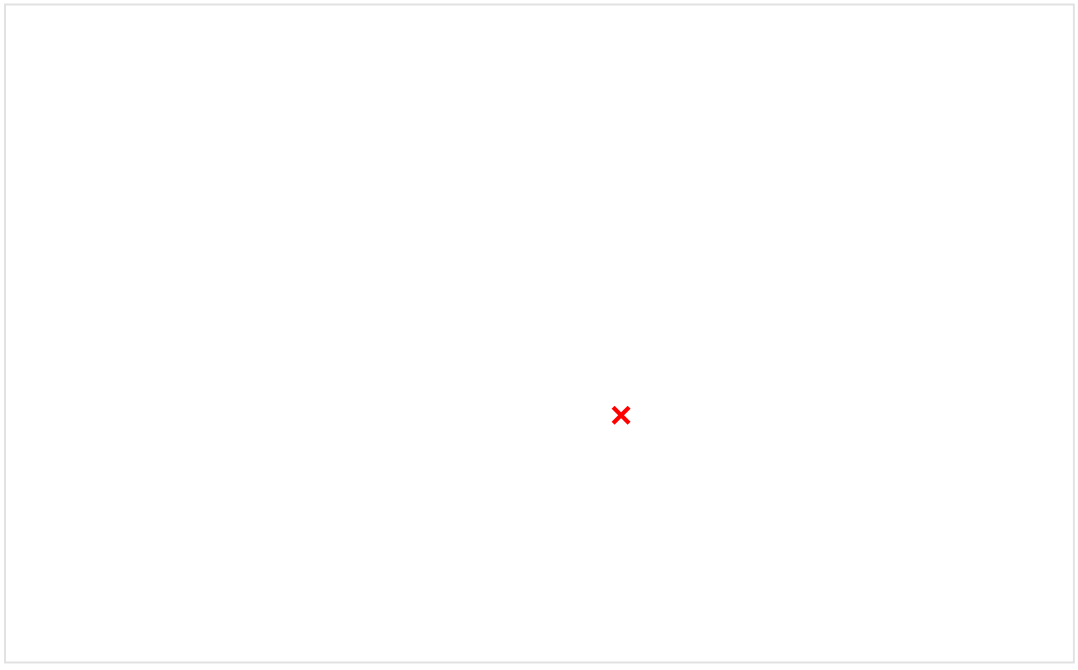


4. Configuramos la autenticación con una clave compartida, que deberá tener el mismo nombre en la configuración de **Barcelona.** En el apartado de algoritmo a utilizar, dejamos el por defecto:

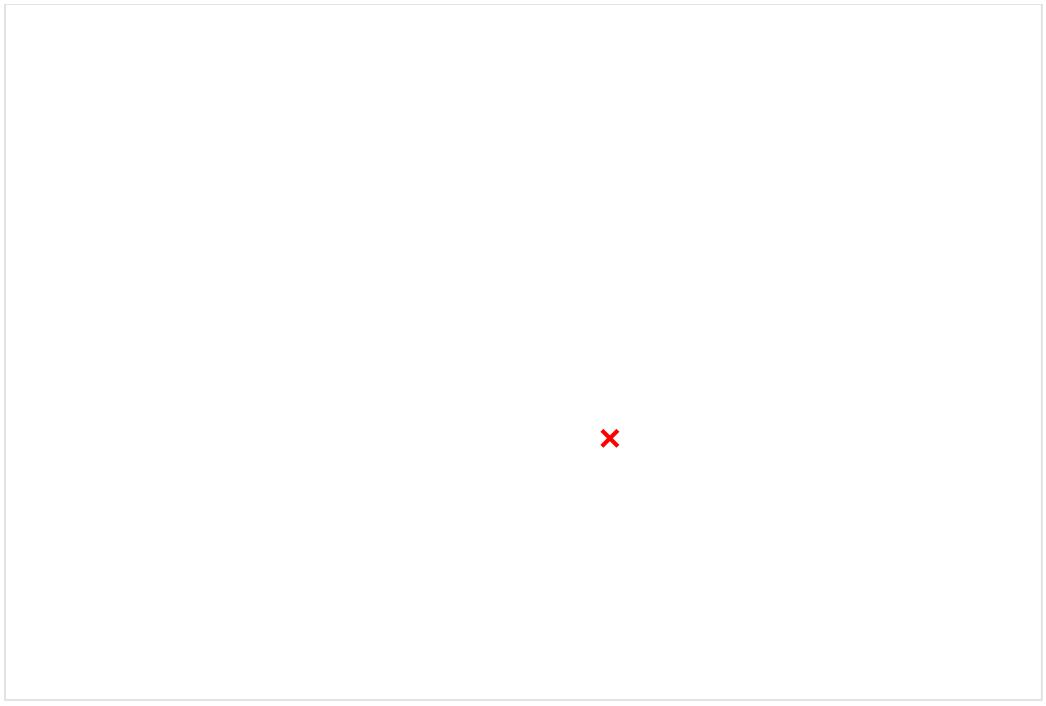


5. Terminada la primera parte, configuramos la segunda entrando en Show Phase 2 Entries – Add p2:

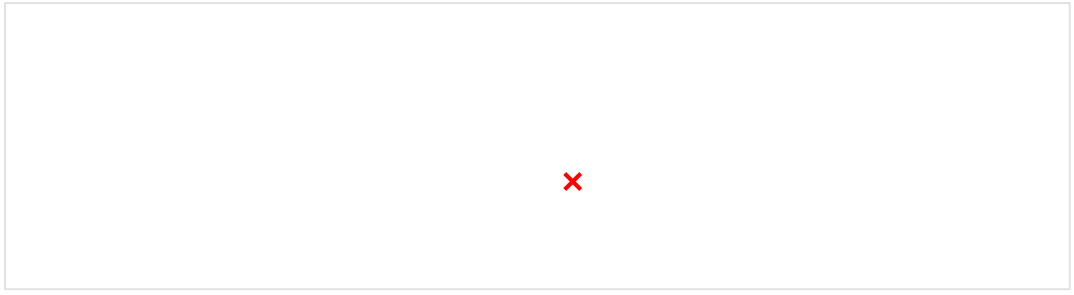
6. Configuramos esta parte 2, indicando que utilizará como Remote Network, la red local del pfsense de **Barcelona**:



7. El algoritmo de encriptación que vamos a utilizar será solo el AES256-GCM de 2048bit:

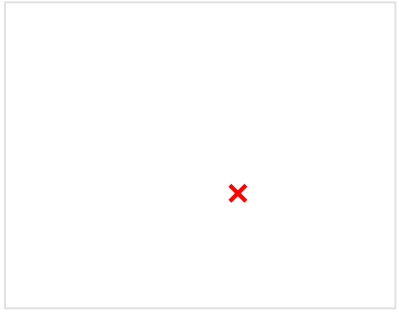


8. Por último, creamos una regla para permitir el tráfico entre Madrid y Barcelona, añadiendo como origen la red de Barcelona y como destino la de Madrid:



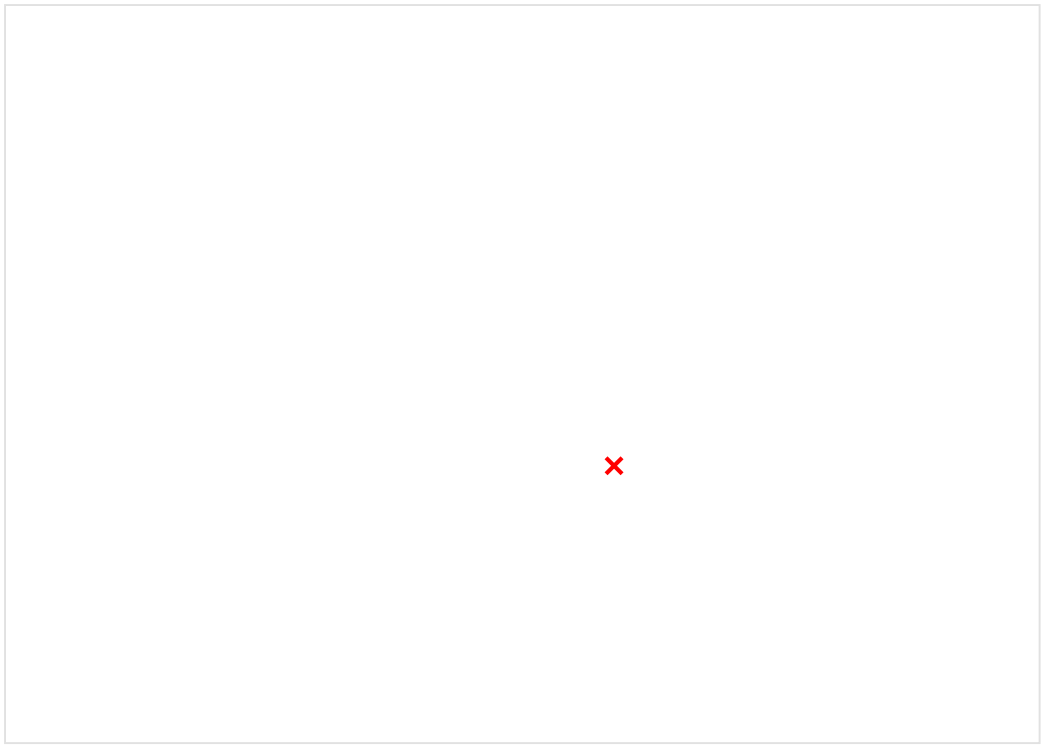
Configuración VPN Oficina Barcelona

1. Accedemos al apartado VPN-Ipsec:

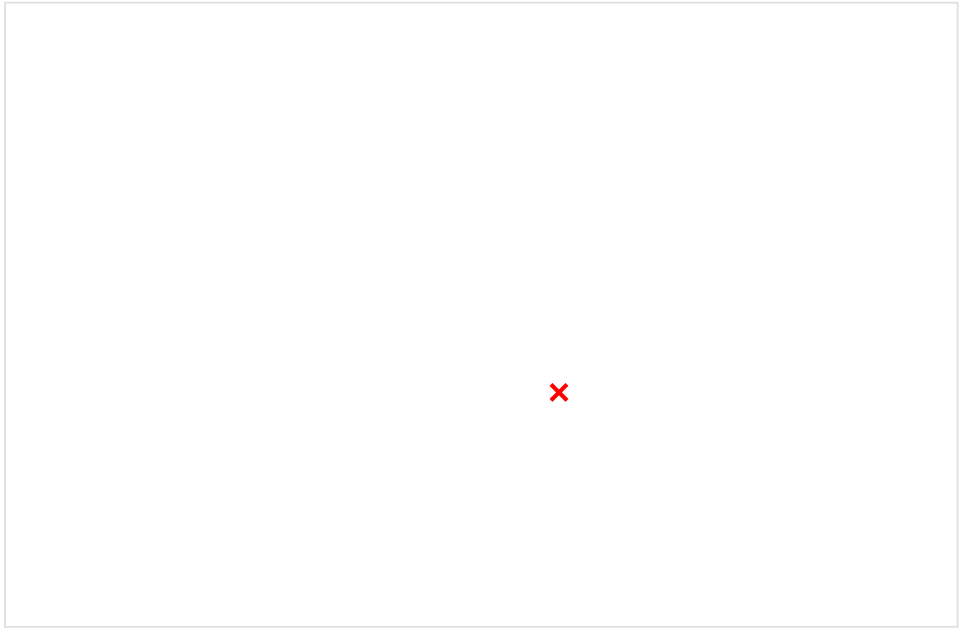


2. Dentro de Tunnels, pulsamos en Add p1 para configurar la primera parte del túnel Ipsec:

3. Indicamos que utilice la versión IKEv2 y que como Remote Gateway utilice la IP pública del pfsense de **Madrid**:

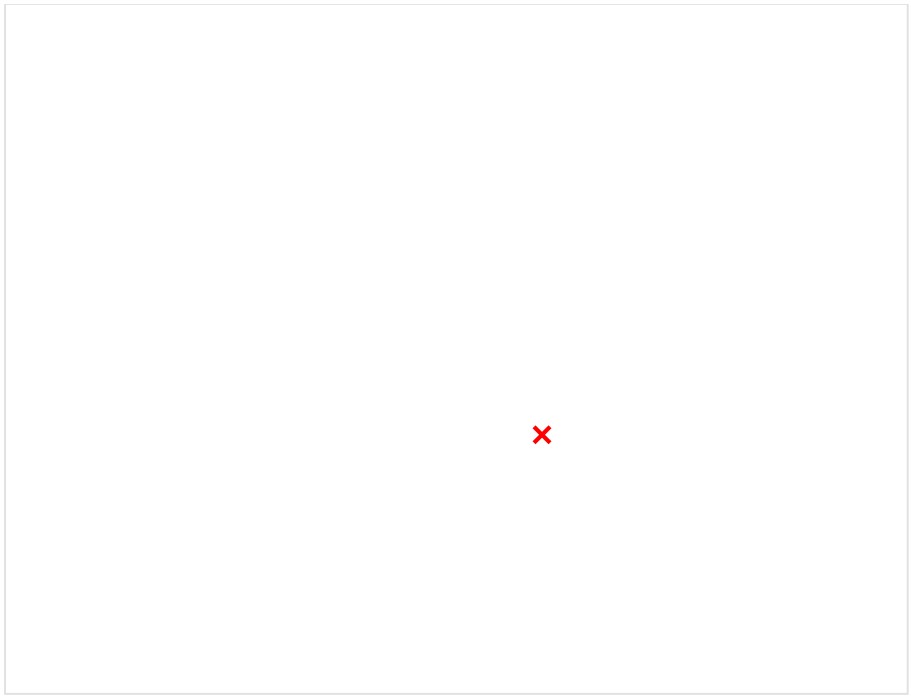


4. Configuramos la autenticación con una clave compartida, que tendrá como nombre, el asignado con anterioridad a Madrid**.** En el apartado de algoritmo a utilizar, dejamos el por defecto:

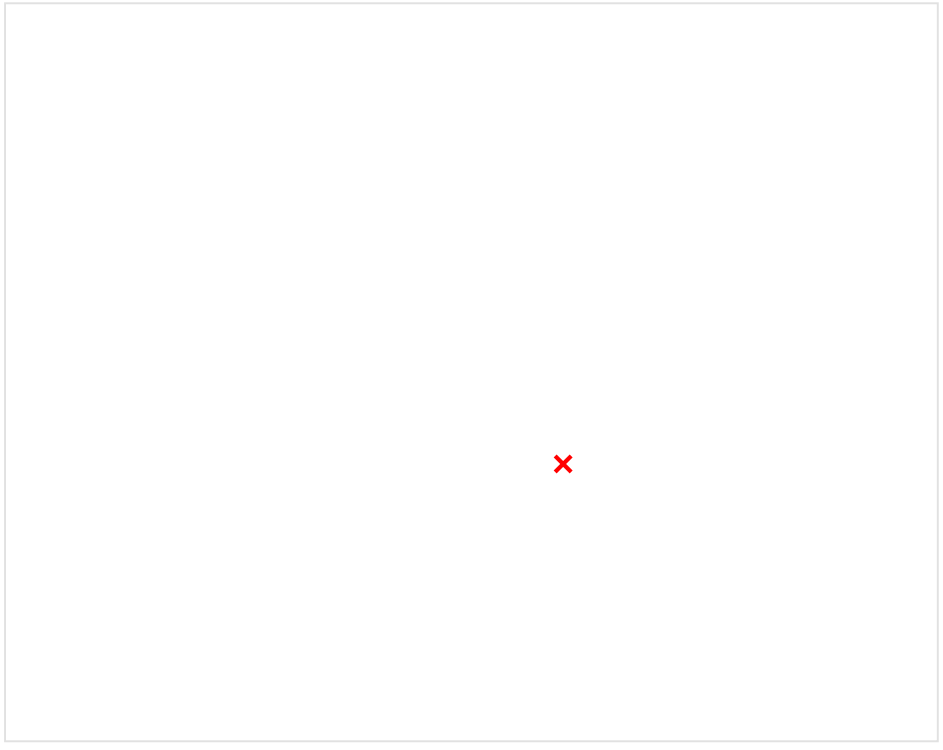


5. Terminada la primera parte, configuramos la segunda entrando en Show Phase 2 Entries – Add p2:

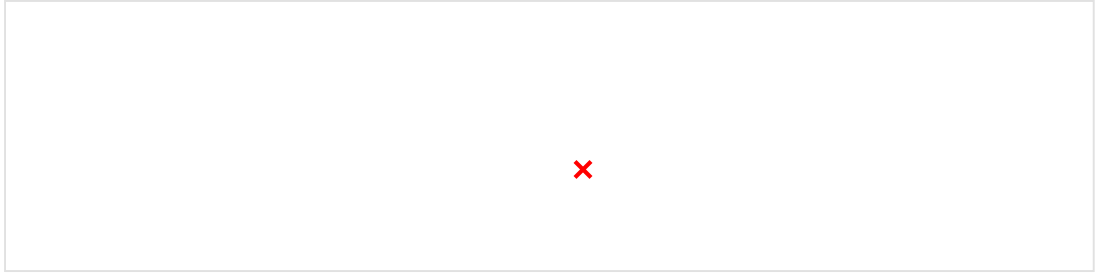
6. Configuramos esta parte 2, indicando que utilizará como Remote Network, la red local del pfsense de **Madrid**:



7. El algoritmo de encriptación que vamos a utilizar será solo el AES256-GCM de 2048bit:

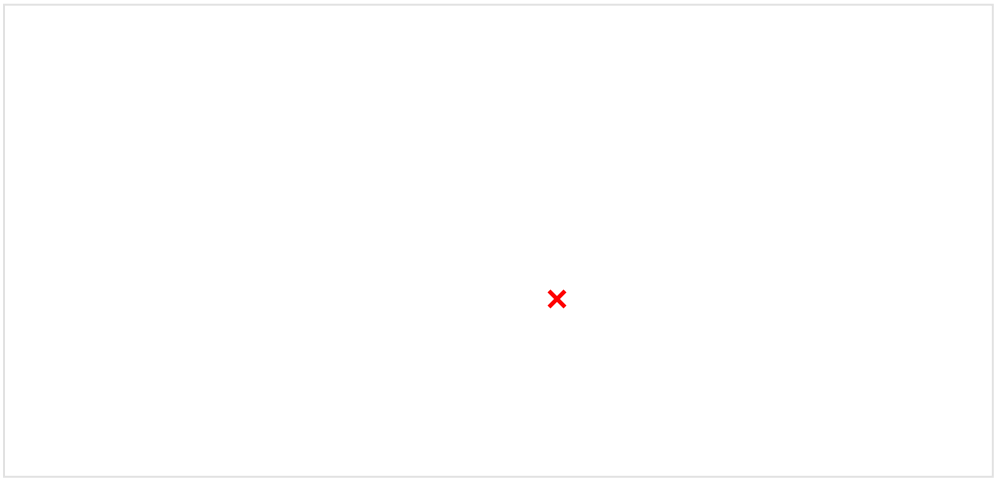


8. Por último, creamos una regla para permitir el tráfico entre Barcelona y Madrid, añadiendo como origen la red de Madrid y como destino la de Barcelona:

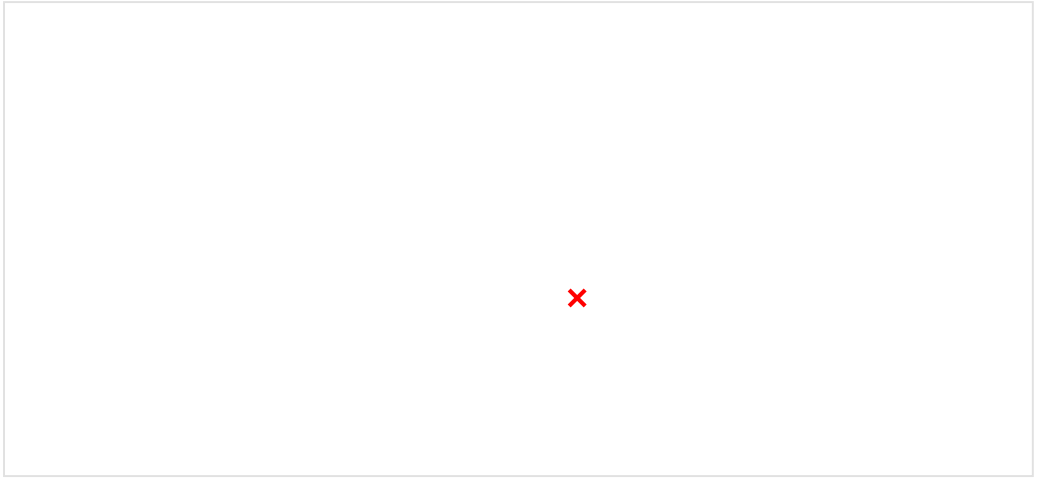


Comprobaciones

-Realizamos un ping desde un cliente de la oficina de Madrid hacia un cliente de la oficina de Barcelona:



-Realizamos un ping desde un cliente de la oficina de Barcelona hacia un cliente de la oficina de Madrid:



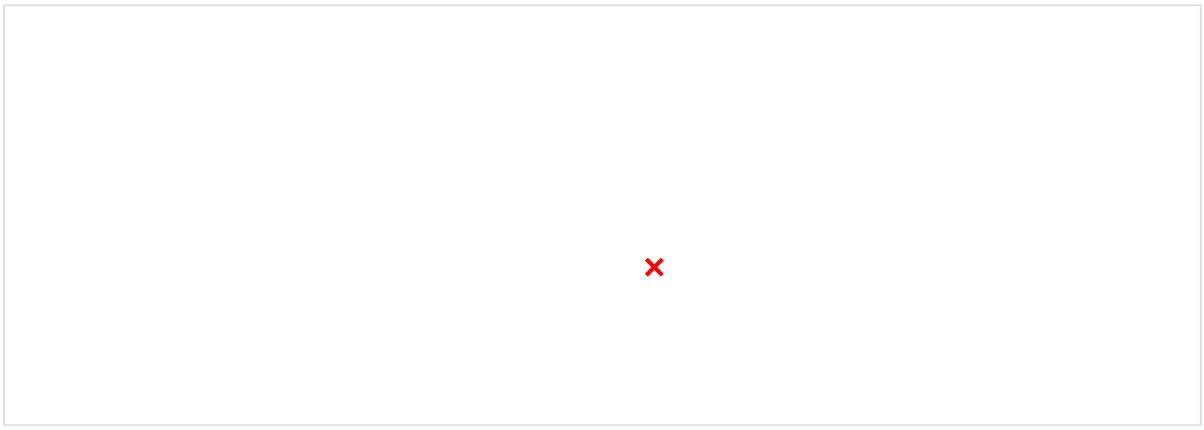
Configuración de VPN (IPSEC con Entidad Certificadora) mediante Firewalls Pfsense

El objetivo de esta práctica es implementar a la VPN entre la oficina de Madrid y Barcelona el uso de entidad certificadora mediante el protocolo IPSEC, este método es mucho más eficaz y seguro que el uso de una clave precompartida, aunque es más complejo de configurar. Dependiendo de la configuración elegida, podemos usar una CA (autoridad de certificación) compartida entre las oficinas que conforman la VPN o, utilizar una CA única

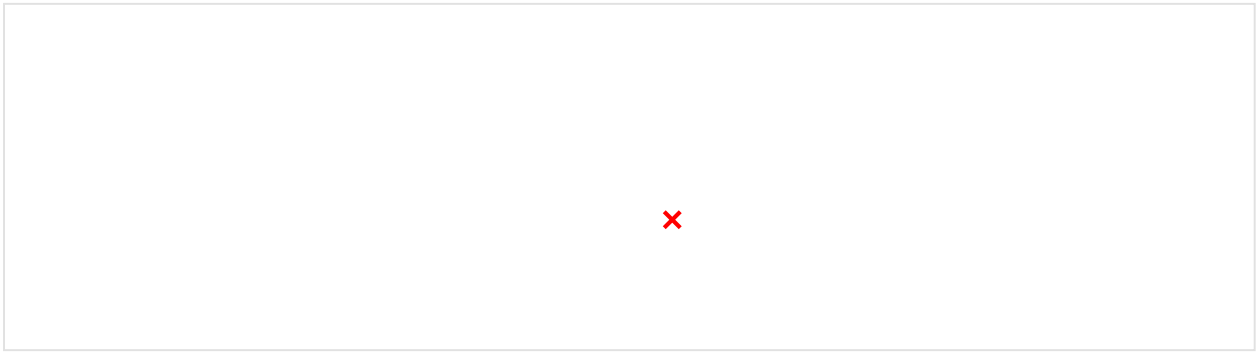
para cada oficina, nosotros utilizaremos la segunda opción.

Creación CA en Madrid y Barcelona:

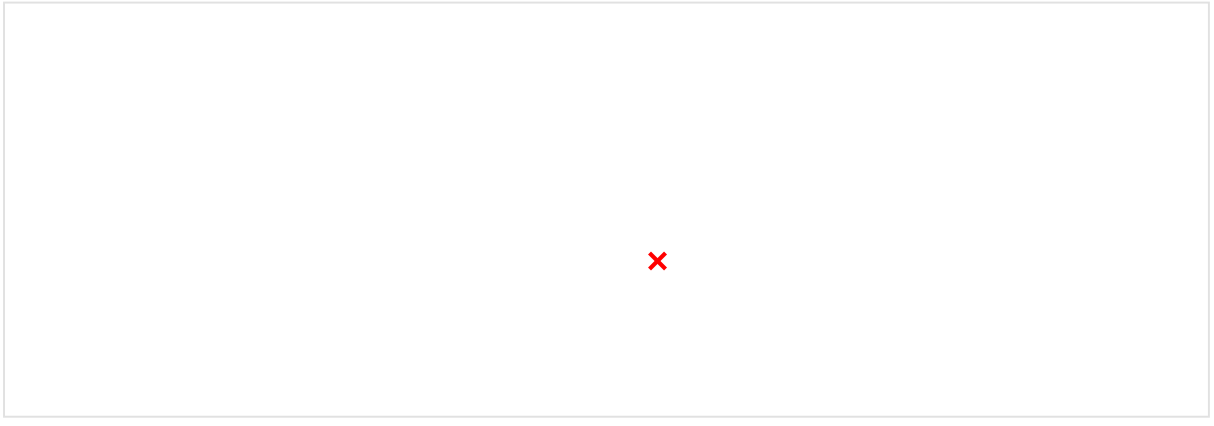
1. El primer paso es, crear la autoridad certificada de **Madrid** dentro de **System** > **Certificates** > **Authorities** > **Add (añadimos un nombre y los demás valores por defecto):**

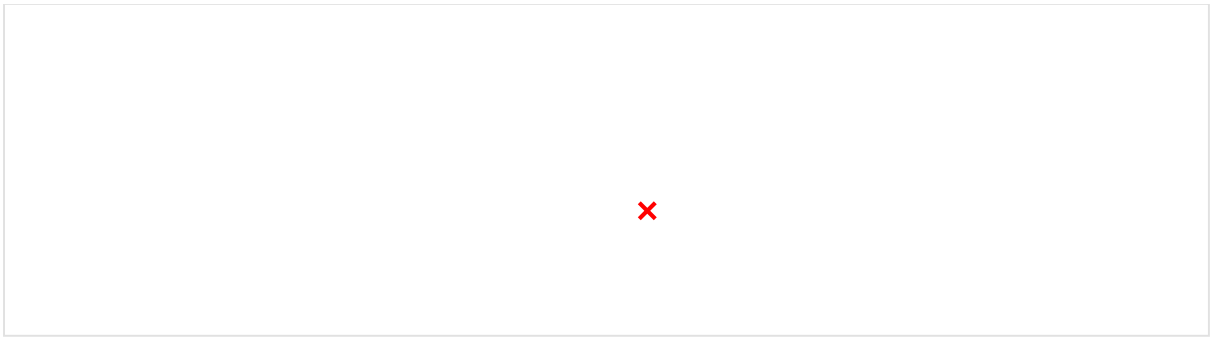


2. Una vez creada la CA de Madrid, procedemos a exportar la clave pulsando en este icono, la cual utilizaremos más tarde:



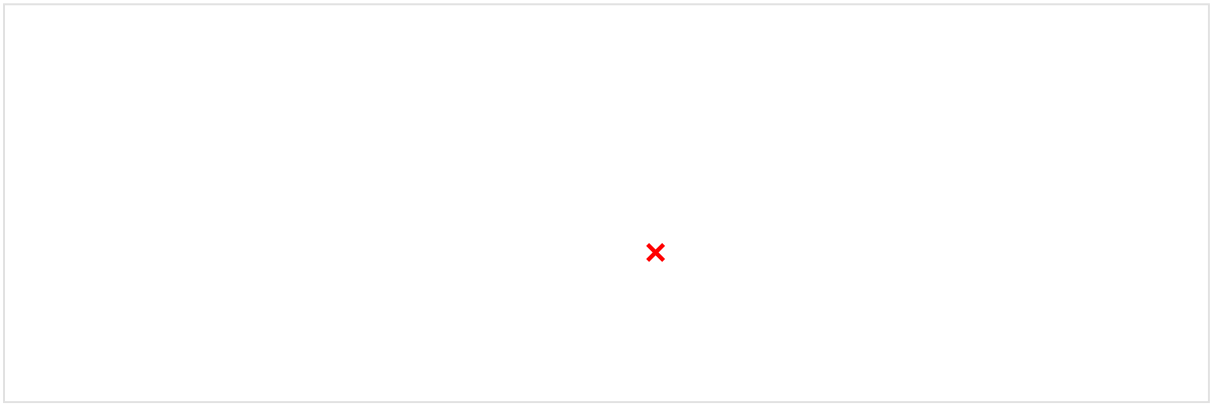
3. A continuación, creamos la entidad certificada de **Barcelona** y exportamos la clave, siguiendo los pasos utilizados en Madrid:



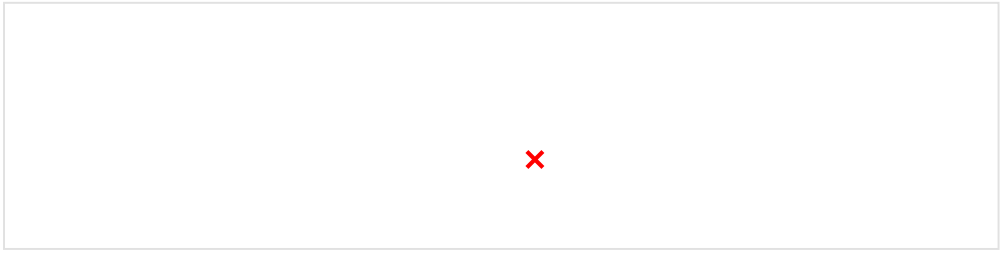


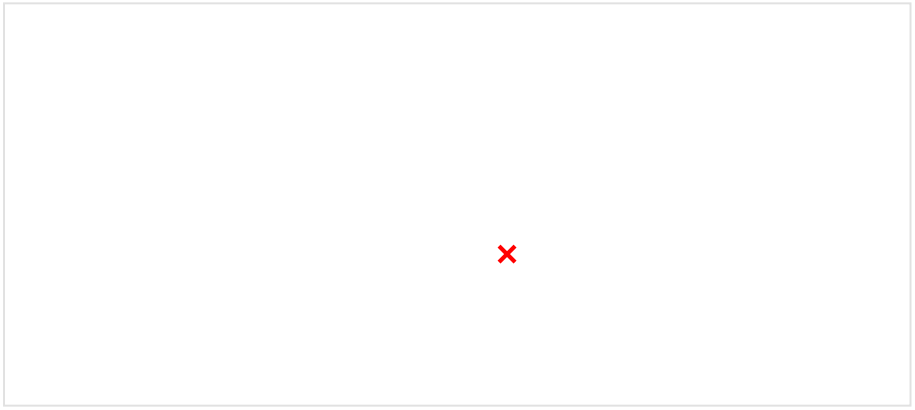
Importación de CA en Madrid y Barcelona:

1. Importamos la CA de **Barcelona** en la oficina de **Madrid** dentro de **System** > **Certificates** > **Authorities** > **Add**…asignamos el nombre dado al **CA** de Barcelona y en este caso tenemos que indicarle que queremos importar un certificado ya existente:

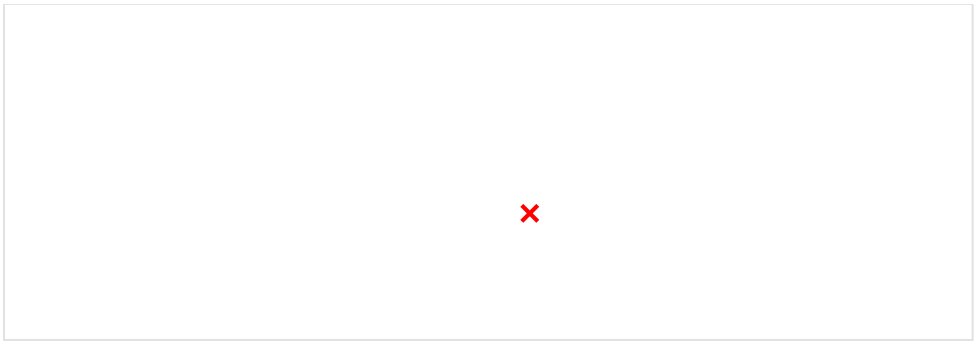


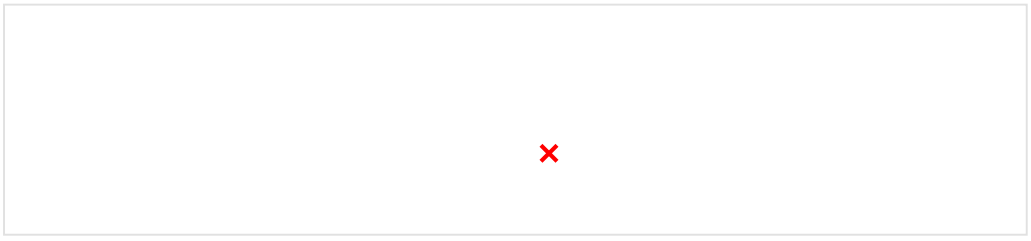
2. Dentro de Certificate data, pegamos el contenido del CA de Barcelona exportado anteriormente:

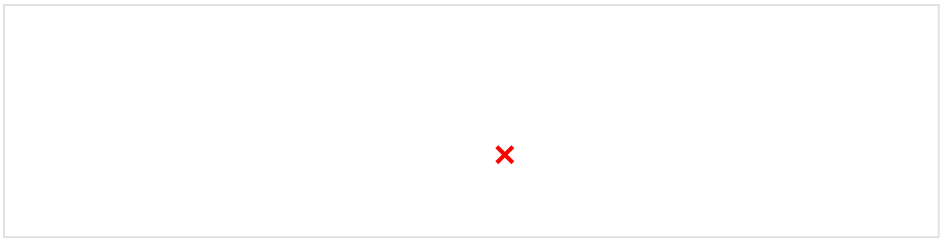




3. Terminado el paso en Madrid, realizamos lo mismo, pero en **Barcelona**, importamos la CA de Madrid dentro de Barcelona:

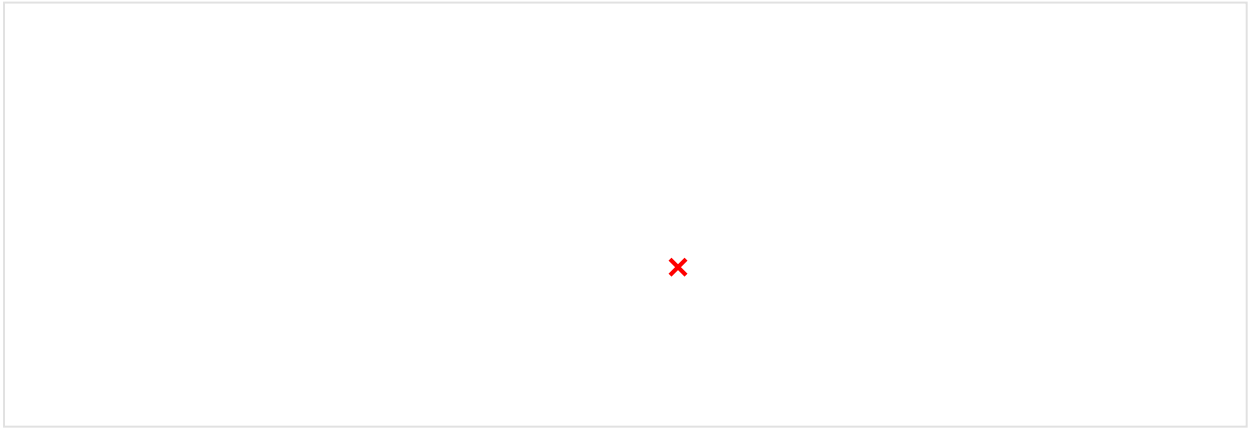




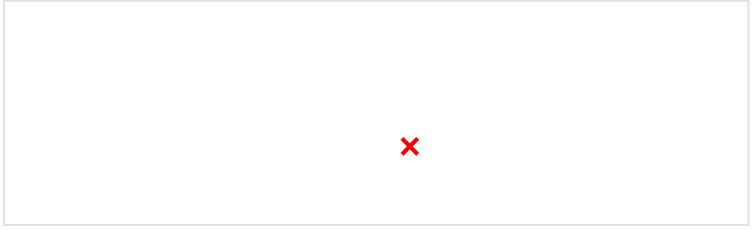


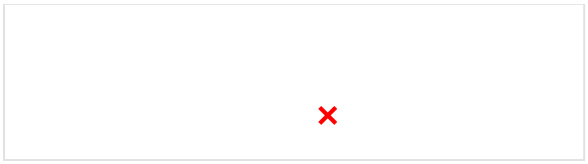
Creación de certificados de punto final en Madrid y Barcelona:

1. Creamos el certificado de punto final en Madrid dentro de **System** > **Certificates** > **Certificates** > **Add:**

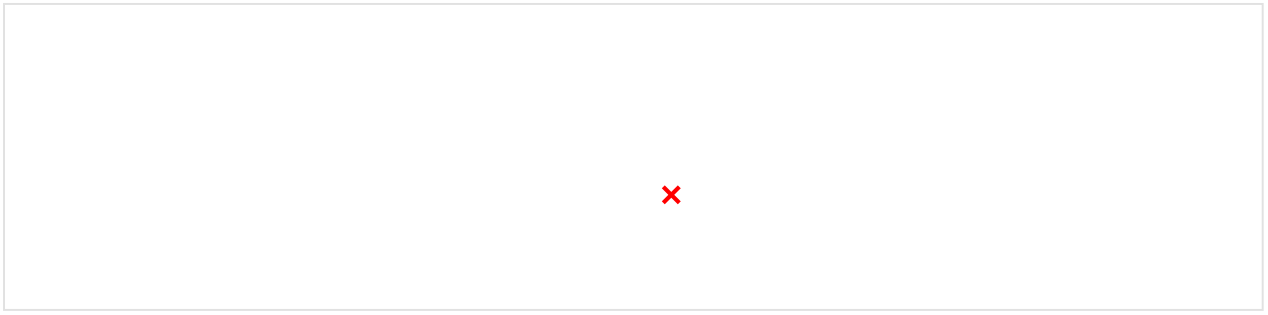


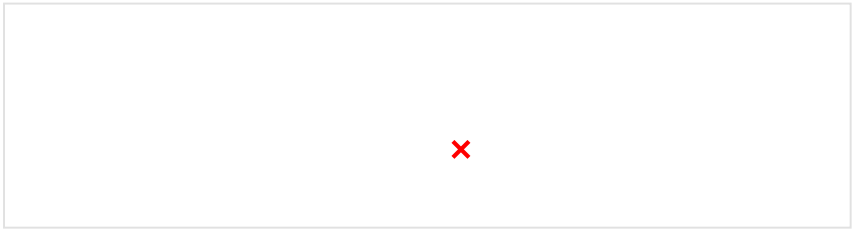
2. Indicamos que use la **CA** creada anteriormente en Madrid:



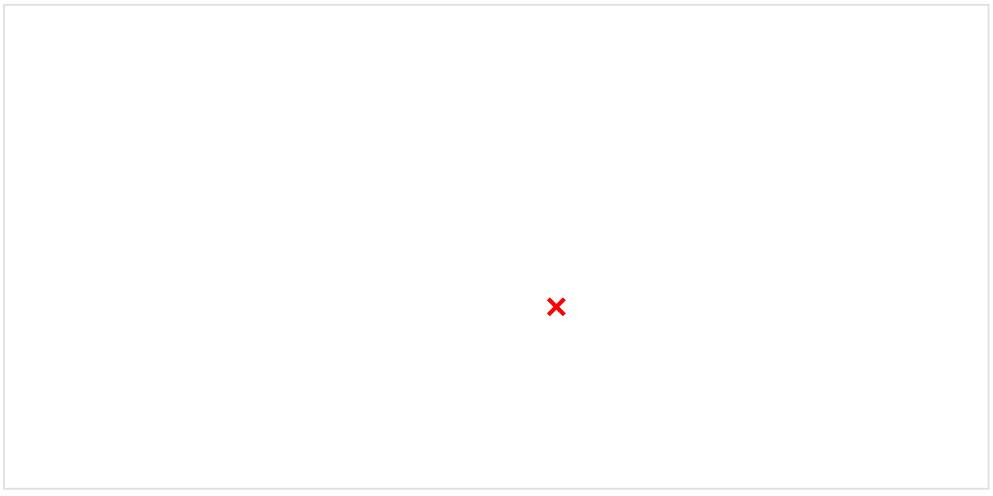


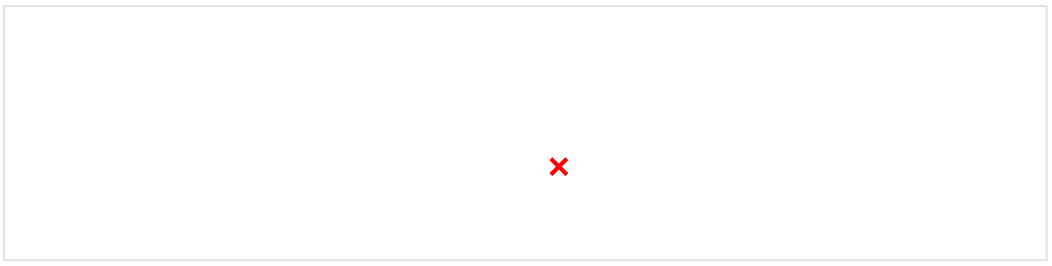
3. Asignamos la IP pública de Madrid:

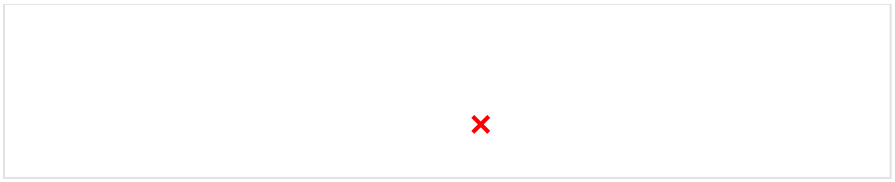




4. Realizamos la misma operación con **Barcelona**:

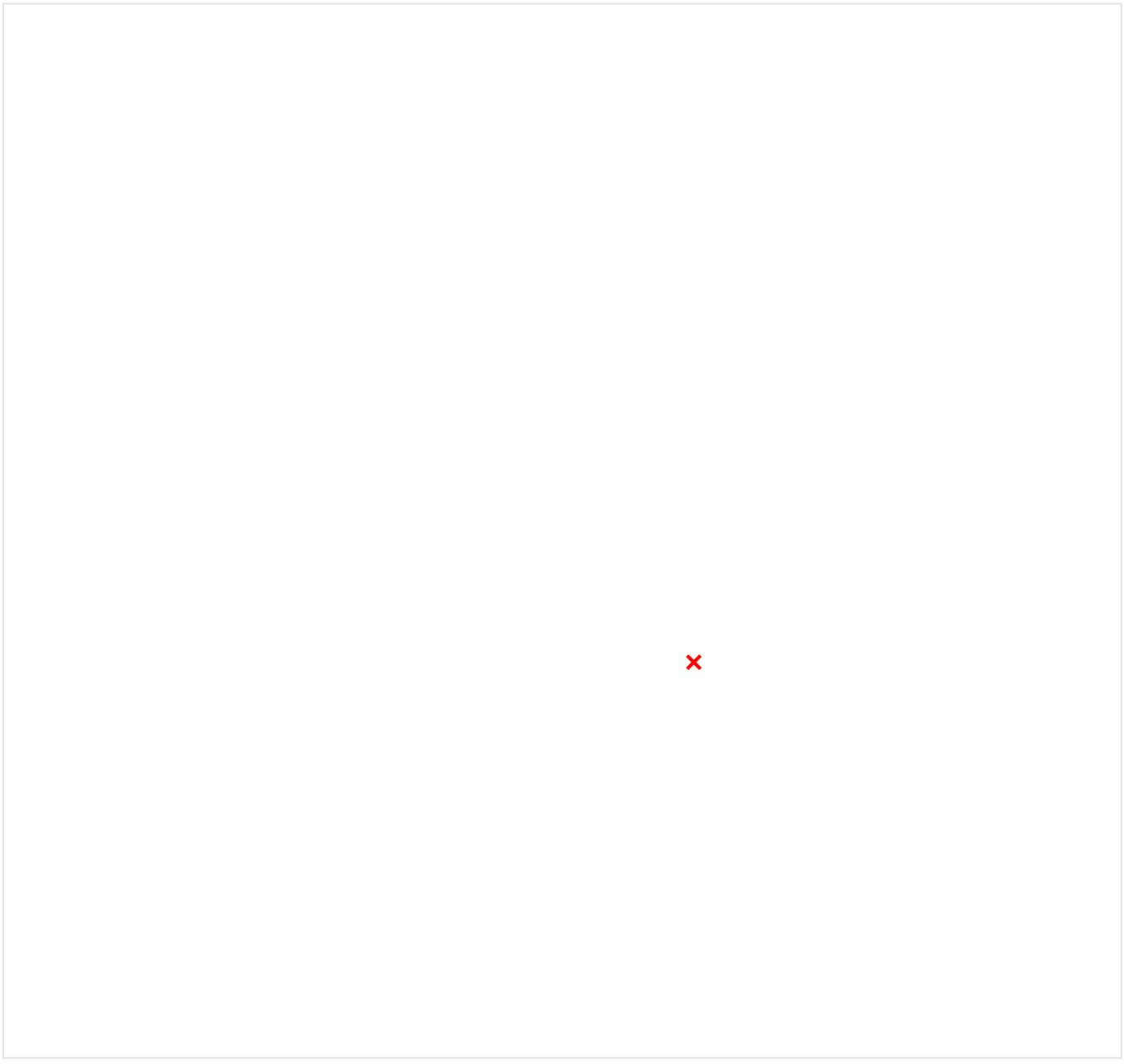




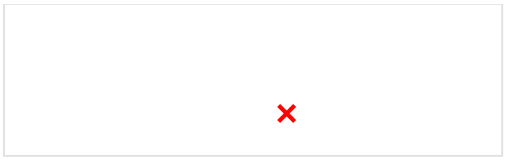


Creación de túnel entre Madrid y Barcelona:

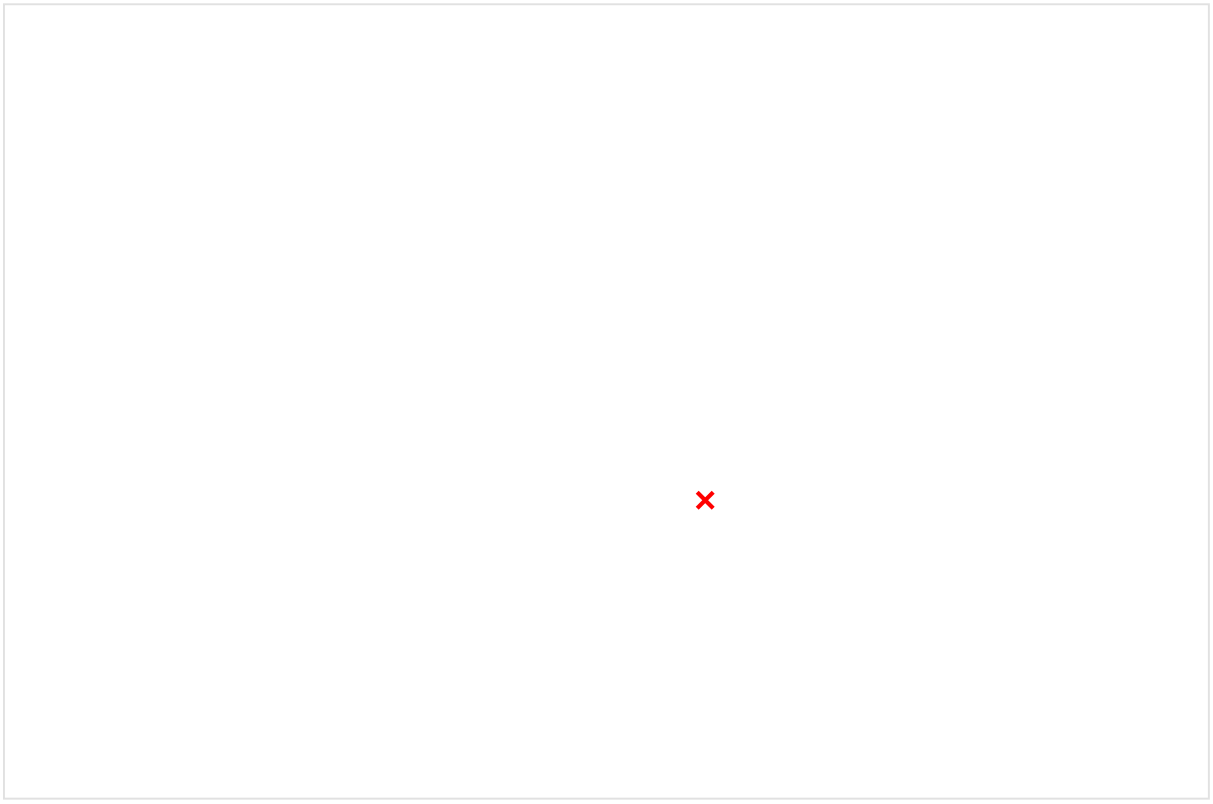
-Asignamos la dirección Pública de Barcelona y le indicamos que utilice el certificado de Madrid junto a la autoridad certificada de Barcelona.



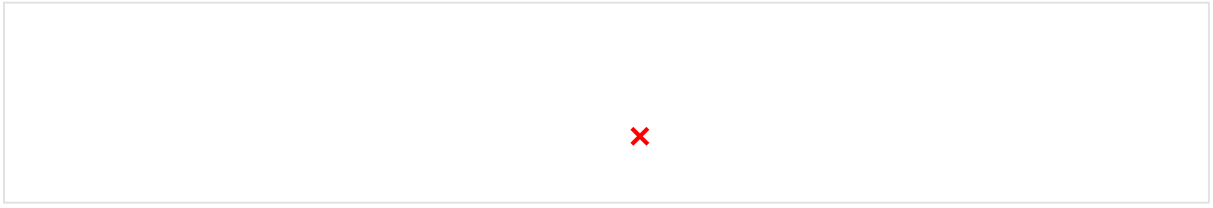
-Entramos en la fase 2 de configuración del túnel:



-Añadimos la red local de Barcelona utilizando el algoritmo AES256-GCM

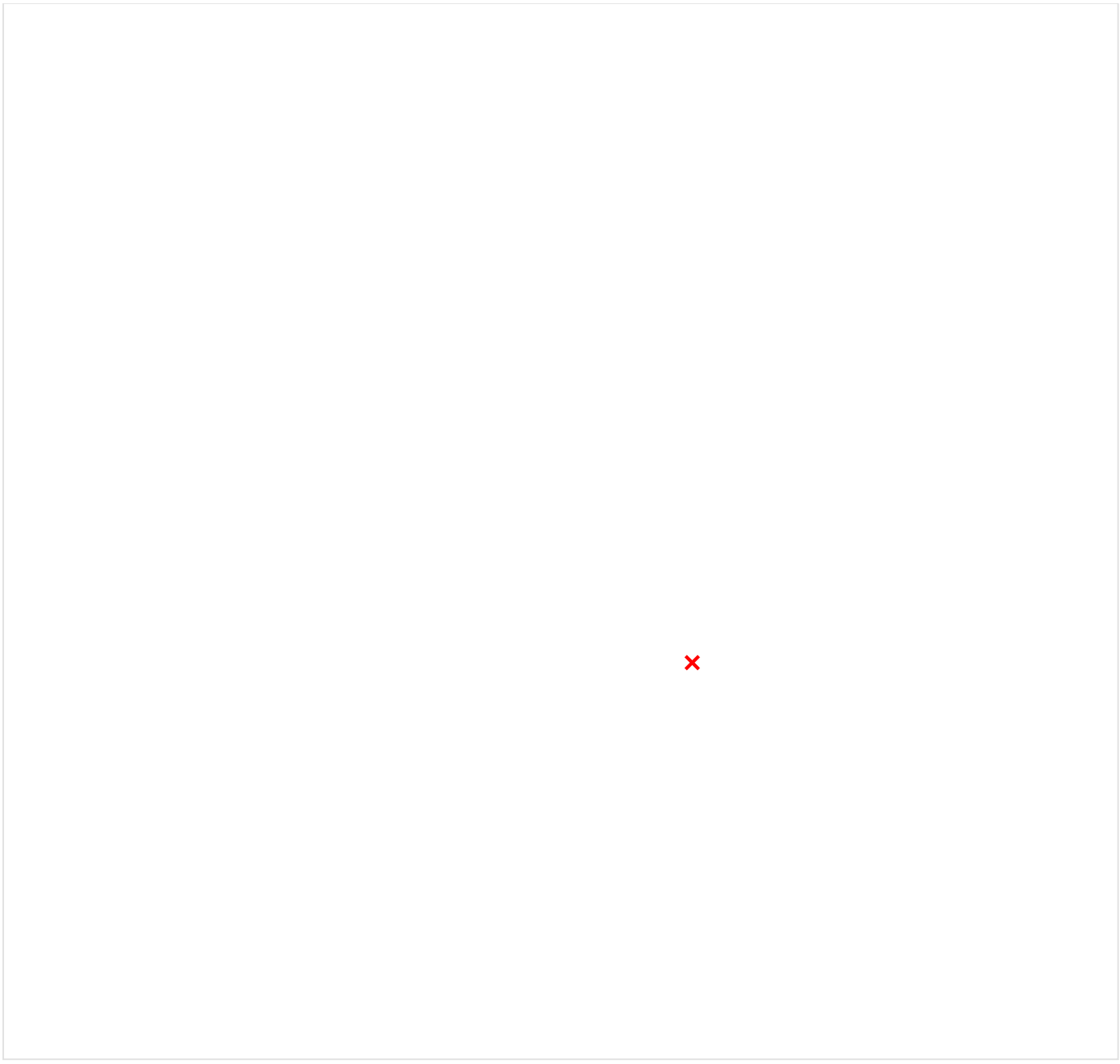


-Configuramos una regla para permitir las conexiones desde la oficina de Madrid, indicando que el origen es la red local de Madrid y el destino la LAN net:

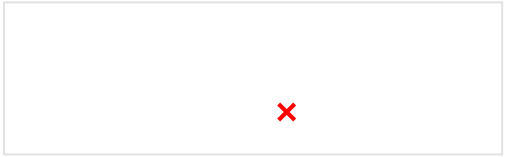


Creación de túnel entre Barcelona y Madrid:

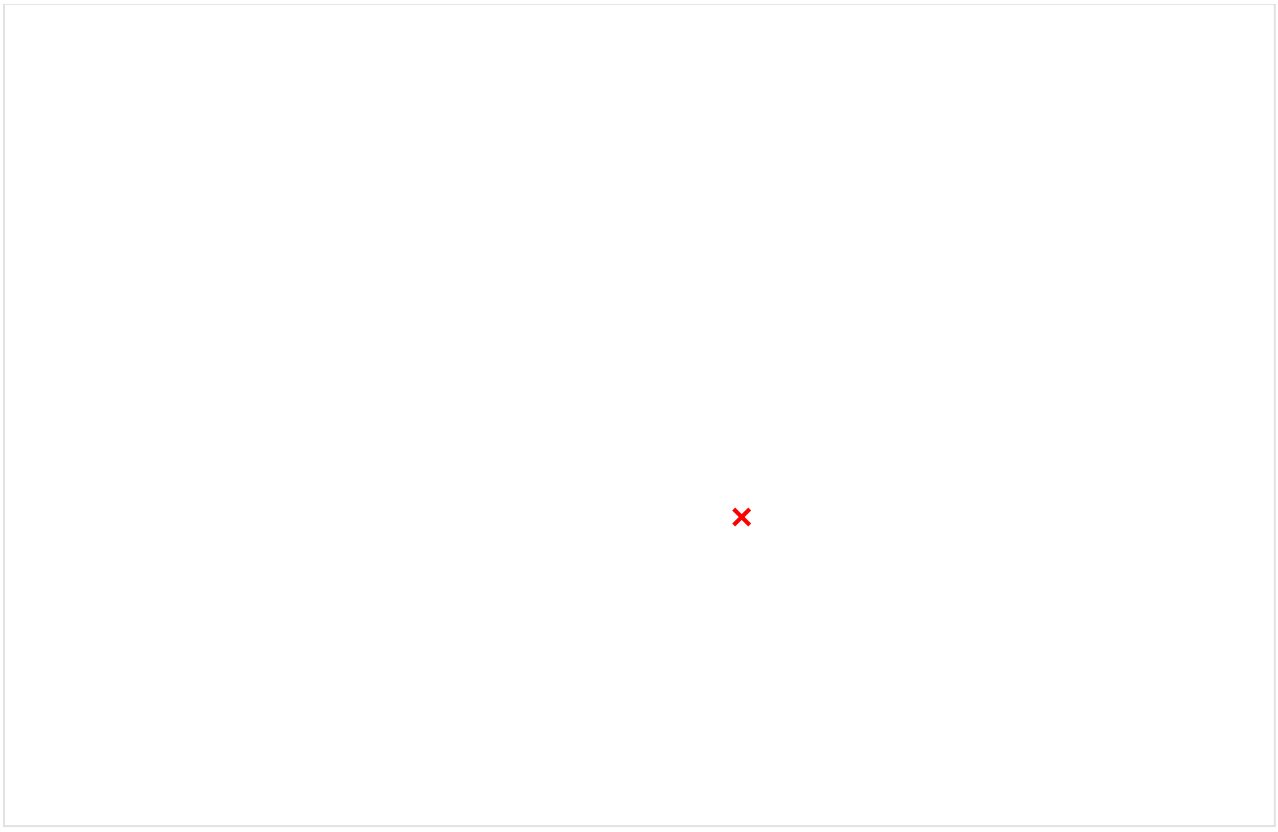
-Asignamos la dirección Pública de Madrid y le indicamos que utilice el certificado de Barcelona junto a la autoridad certificada de Madrid.



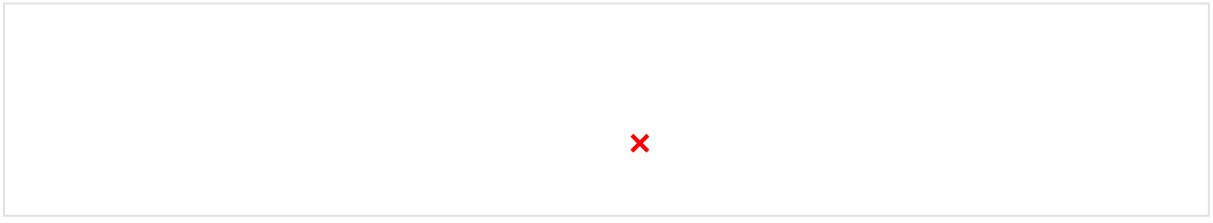
-Entramos en la fase 2 de configuración del túnel:



-Añadimos la red local de Madrid utilizando el algoritmo AES256-GCM



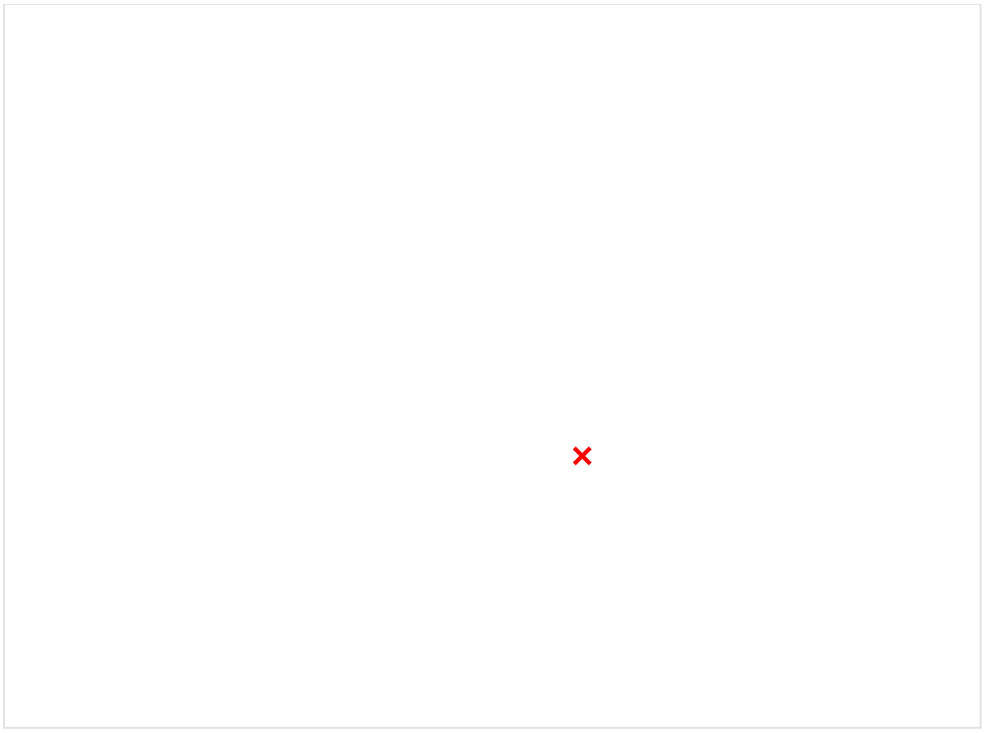
-Configuramos una regla para permitir las conexiones desde la oficina de Barcelona, indicando que el origen es la red local de Barcelona y el destino la LAN net:



Las direcciones IP públicas no corresponden con las adecuadas, debido a que he tenido que realizar el documento en casa, por la falta de asistencia a clase del día 30/10.

Comprobaciones:

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



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