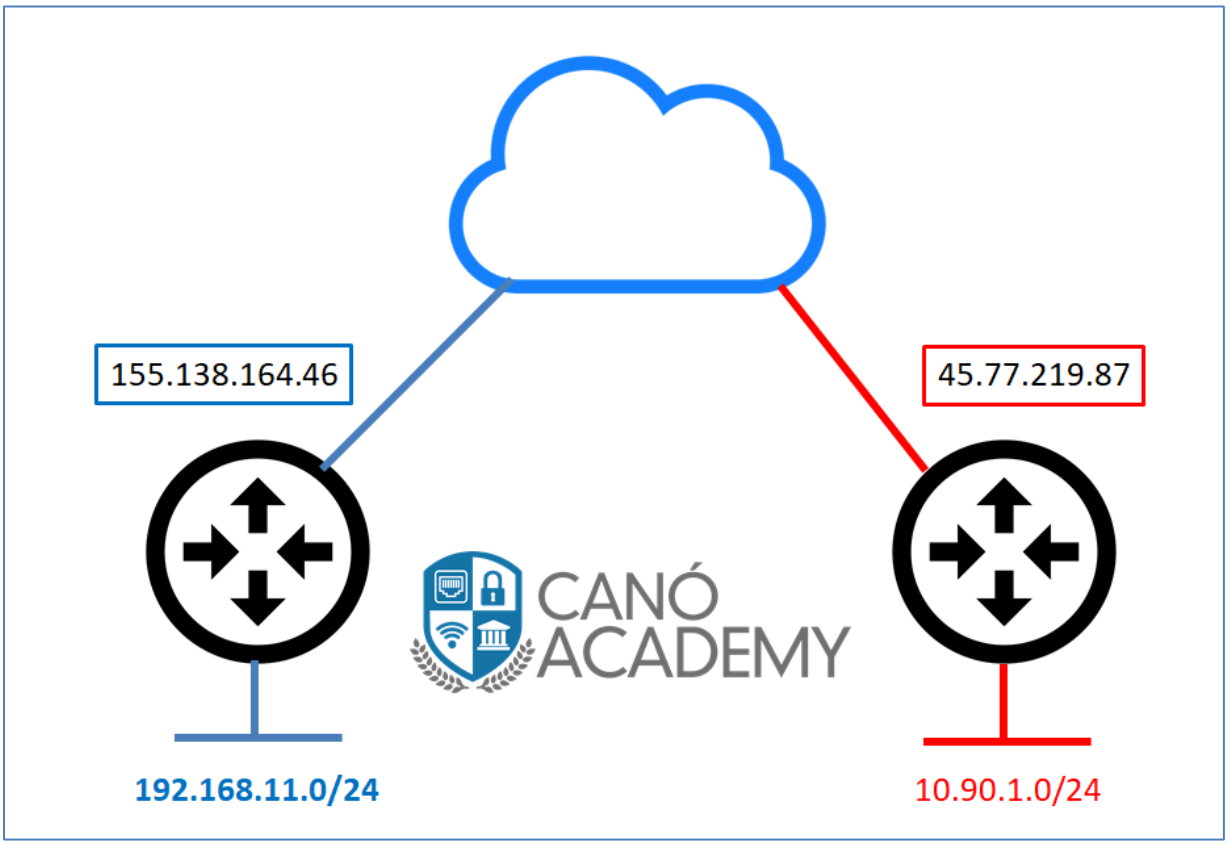
Laboratorio IPSEC: Configuración site to site MikroTik-MikroTik.

Objetivo: configurar un VPN IPsec site to site entre routers Mikrotik.

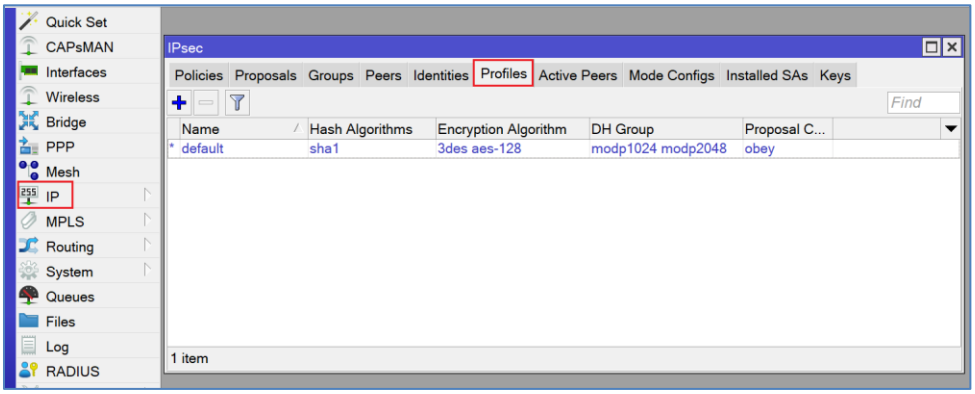


Router-A:

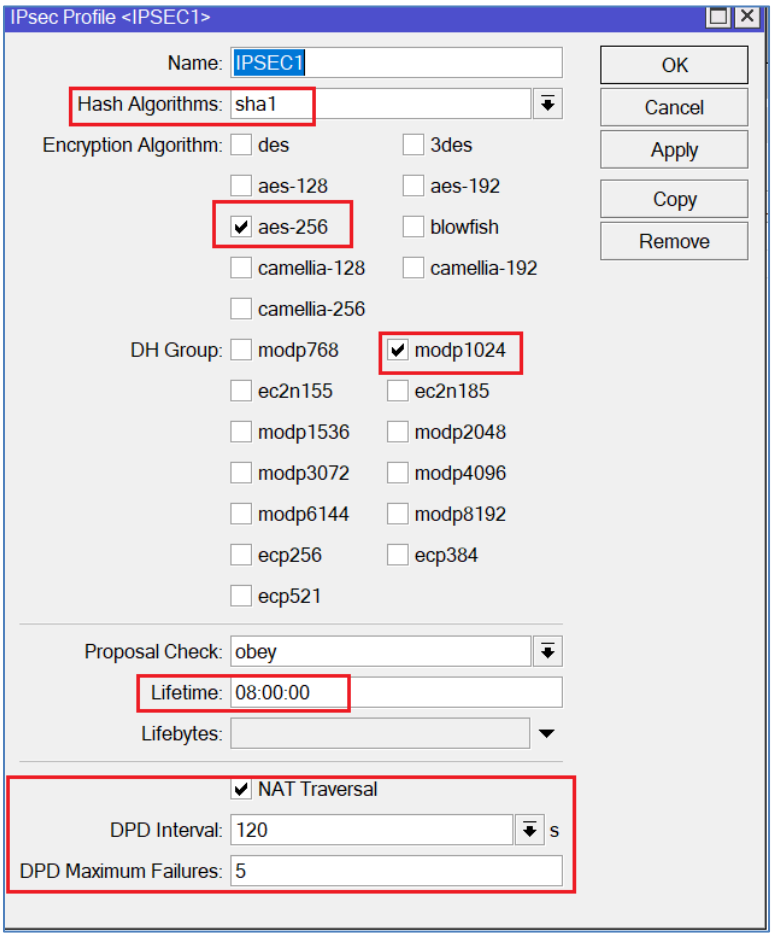
FASE 1

Paso 1: Nos dirijimos al menú **IP** y luego vamos a **IPSEC**.

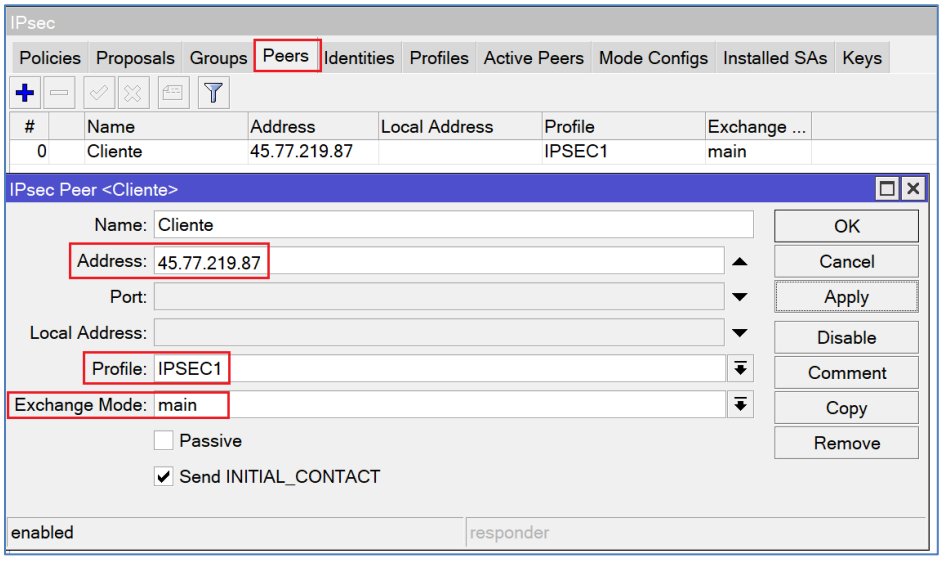
Dentro del menú IPSEC vamos a Profiles:



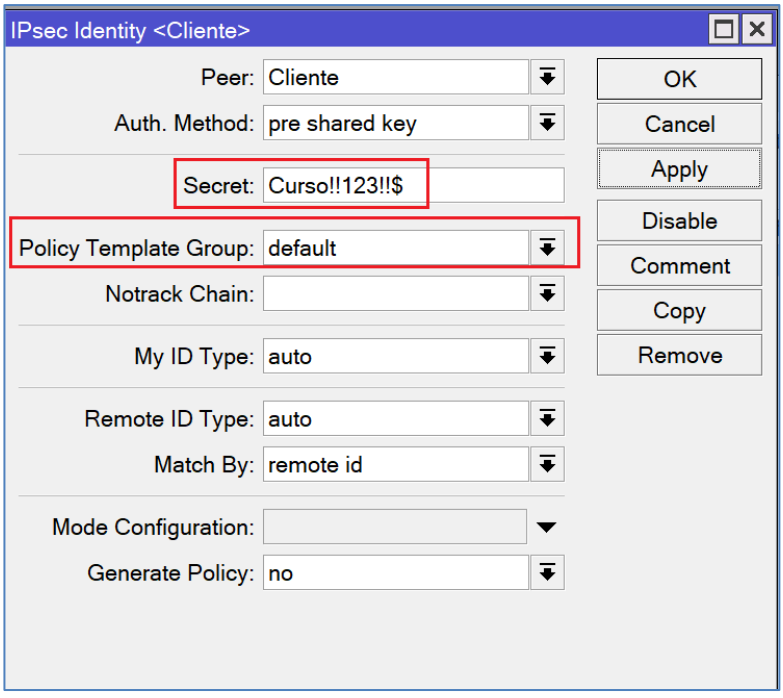
Agregamos un nuevo perfil llamado **IPSEC1** y configuramos de la siguiente forma:



Paso 2: Nos dirigimos a Peer y **colocamos la IP** de nuestro cliente junto al **profile** que hemos creado recientemente llamado **IPSEC1.**

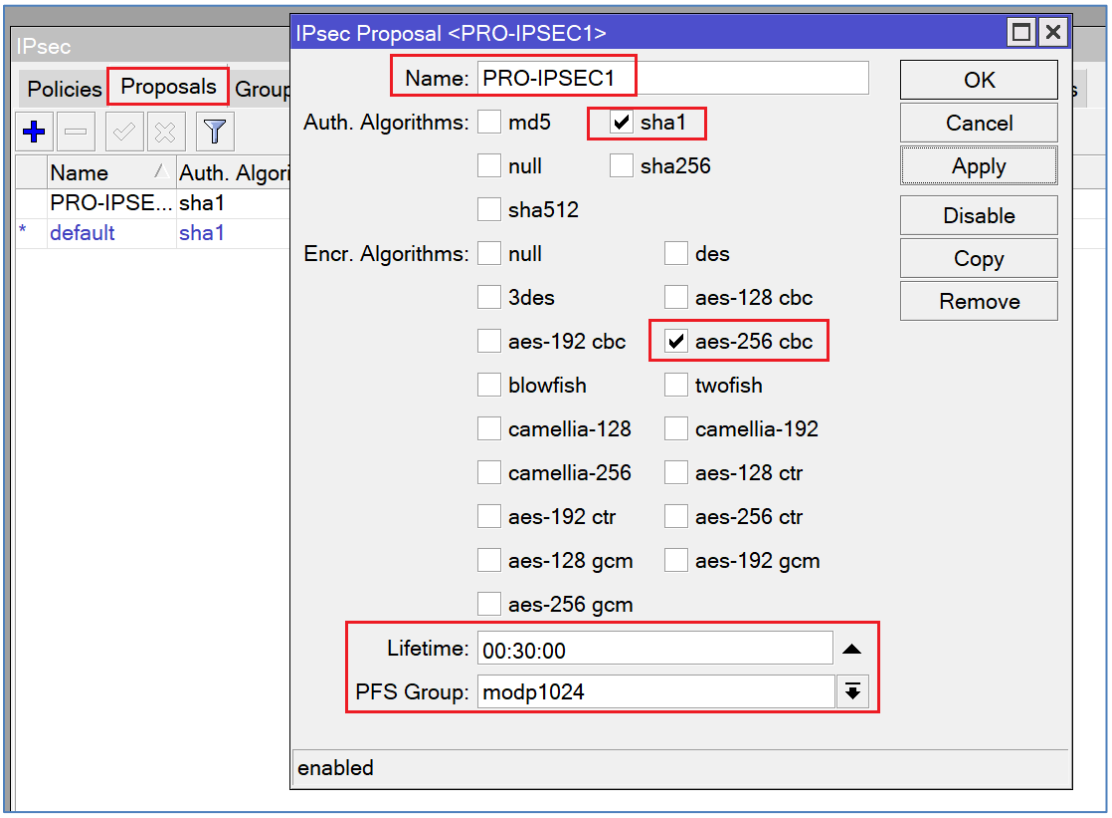


Paso 3: Ahora vamos a configurar el método de autenticación. Para eso vamos a **Identities.** Elegimos el Peer y el Policy Template IPSEC. Luego elegimos el método de **pre share Key** y colocamos la clave **Curso!!123!!$** en secret**.**

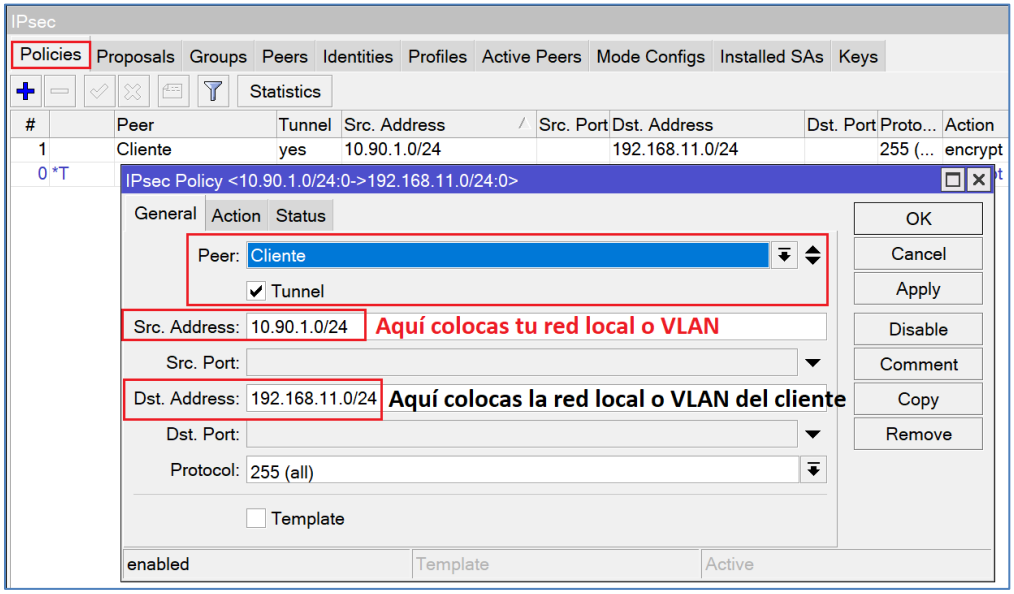


FASE 2

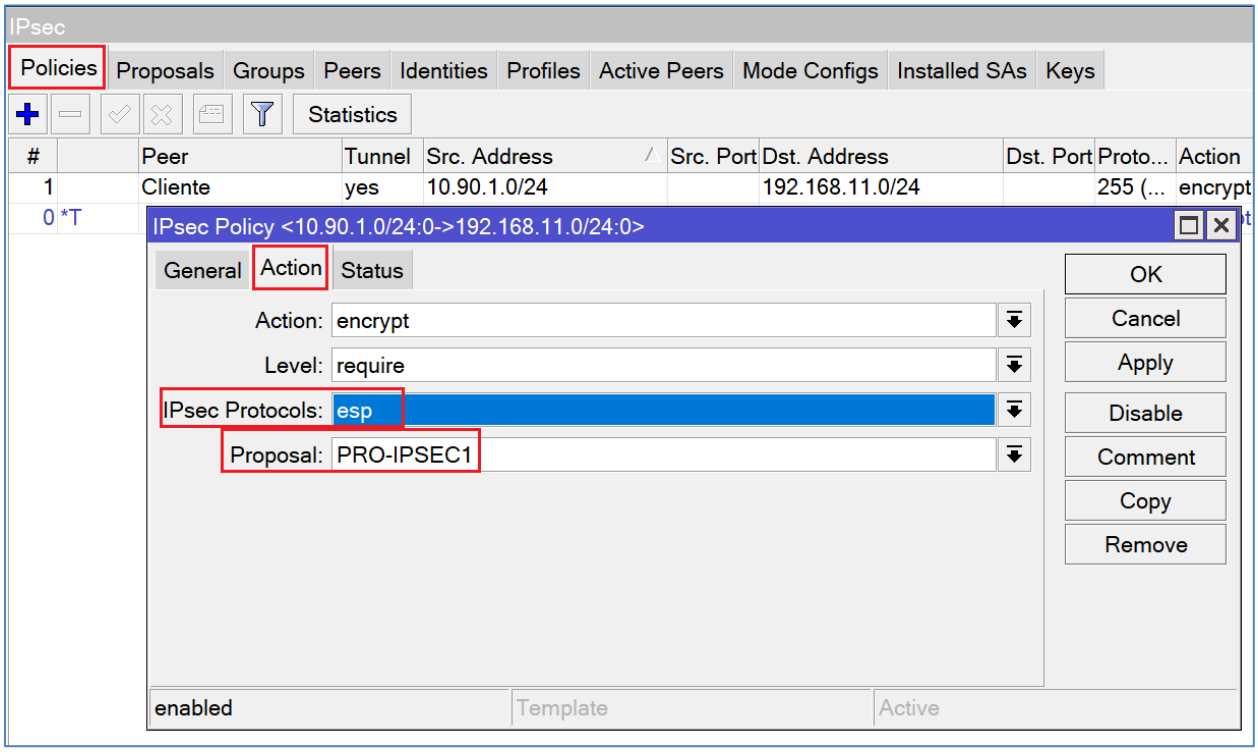
Paso 4: Nos dirigimos al menú **Proposal** y configuramos de la siguiente forma. Algoritmo de autenticación **sha1**, algoritmo de encriptación **aes-256cbc**, **lifetime 30** minutos y **PFS Group modp1024**.



Paso 5: Configuración del **Policies** o política de IPSEC. Aquí es donde definimos que nuestro IPSEC va a trabajar en modo túnel con el peer indicado. El **source address** es la red local y el dst address es la red remota del cliente.



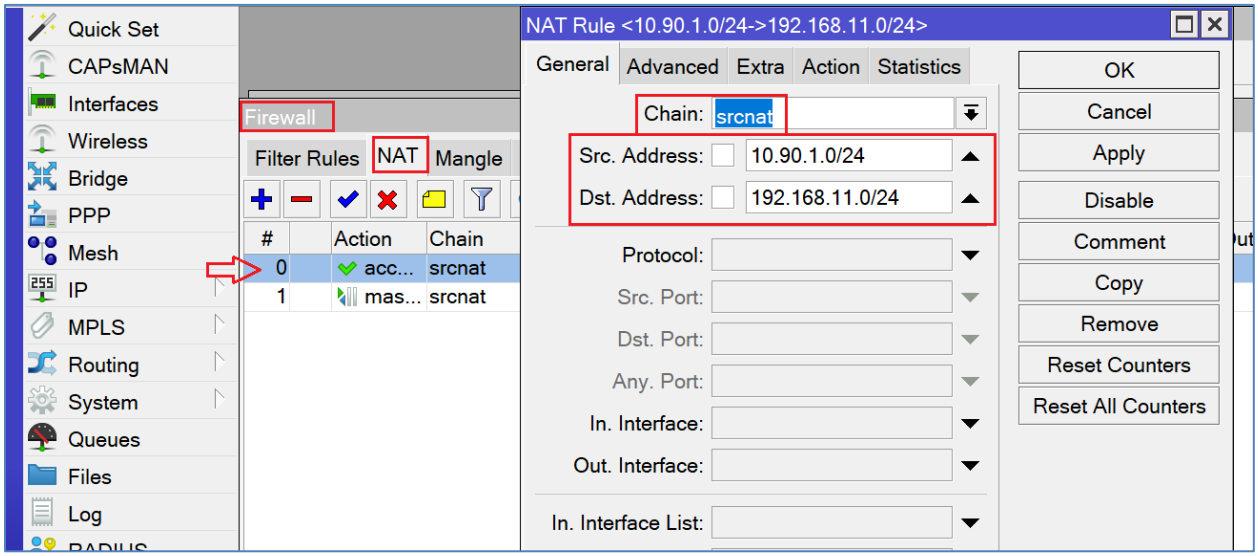
Para completar la configuración vamos al menú **Action** de nuestra política IPSEC. Aquí elegimos el protocolo **esp** y el **proposal** para nuestra fase 2. La encriptación será requerida ya que trabajaremos un túnel seguro esp.



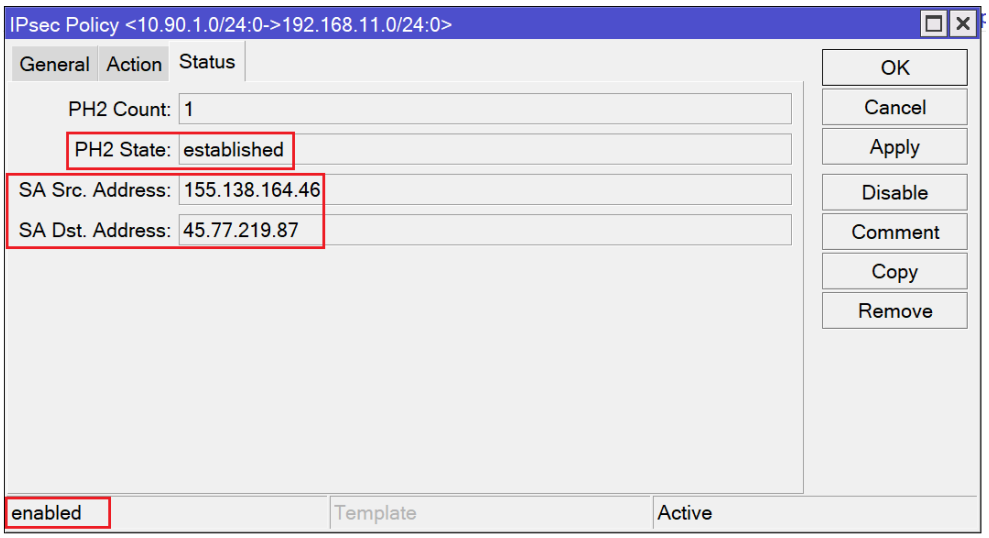
Paso 6: configuración de regla de NAT

Ahora vamos a aceptar el tráfico de la red local y la red remota. Esta regla debe colocarse en la primera posición para aceptar el tráfico entre las dos redes que vamos a compartir por IPSEC. Sin esta regla no hay tráfico y por eso es muy importante colocarla en el orden correcto.

Primero colocamos la red local(src-address) y luego la red remota(dst-address).

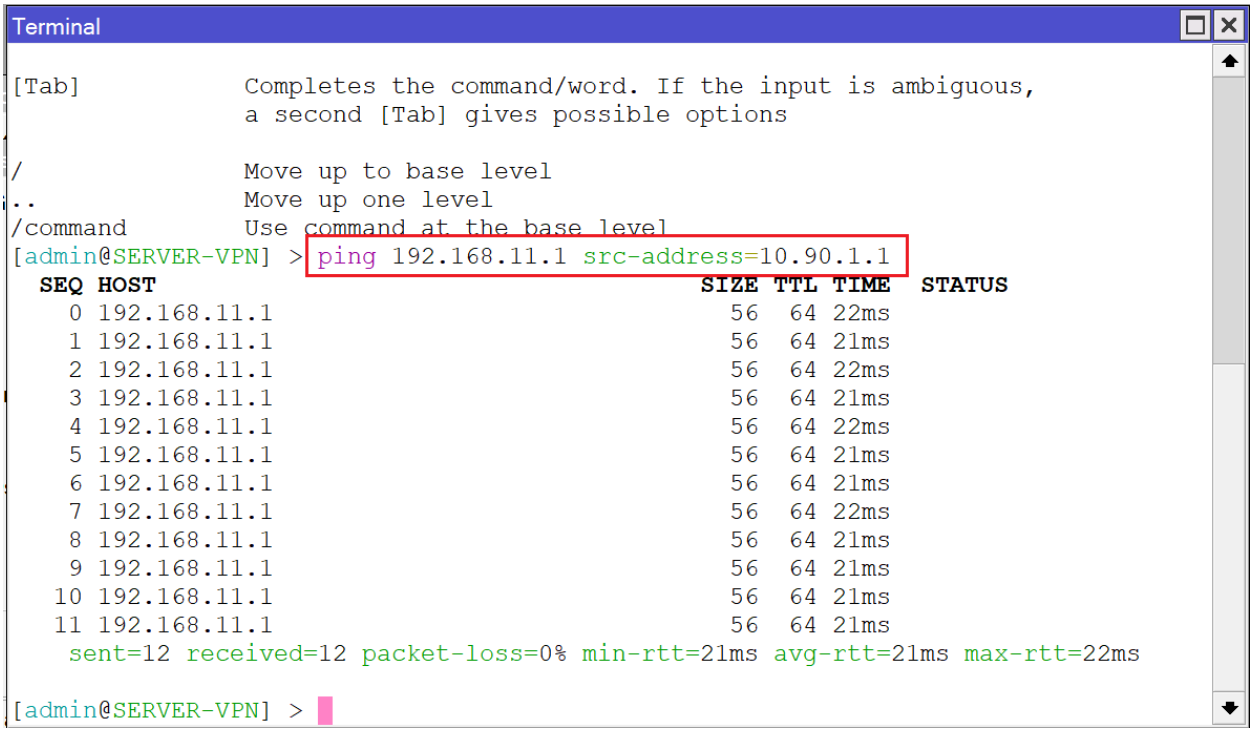


Debemos repetir estos pasos en el cliente teniendo en cuenta que intercambiaremos las redes locales y remotas. Lo demás es igual. Tras completar los pasos vamos a tener un túnel establecido completamente.



Paso 7: Probar la conexión entre las redes via IPSEC.

Como realizaremos la prueba desde nuestro propio router, debemos especificar nuestro src-address, simulando un ping desde la IP 10.90.1.1. Si no lo hacemos así, el router intentará realizar un ping por la ruta por defecto.



Cabe destacar que en IPSEC no utilizamos enrutamiento. Las rutas se comparten en el IPSEC Policy.