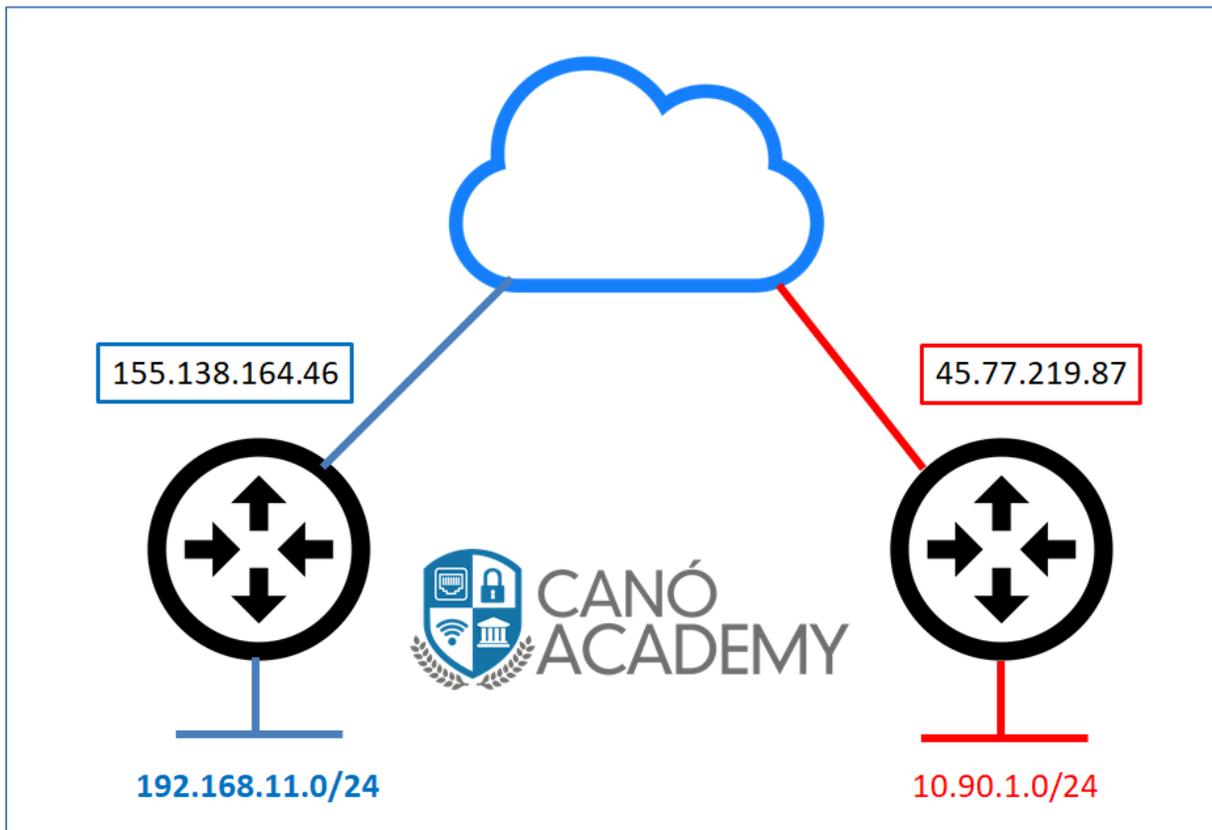


## Laboratorio IPSEC: Configuración site to site MikroTik- MikroTik.

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

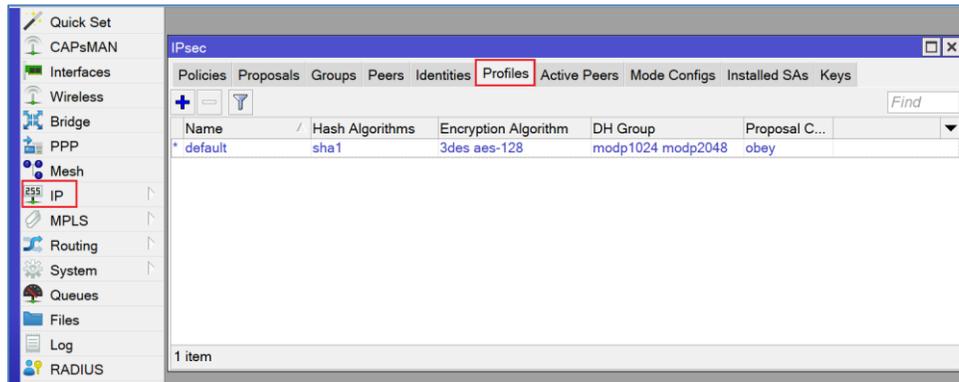


## Router-A:

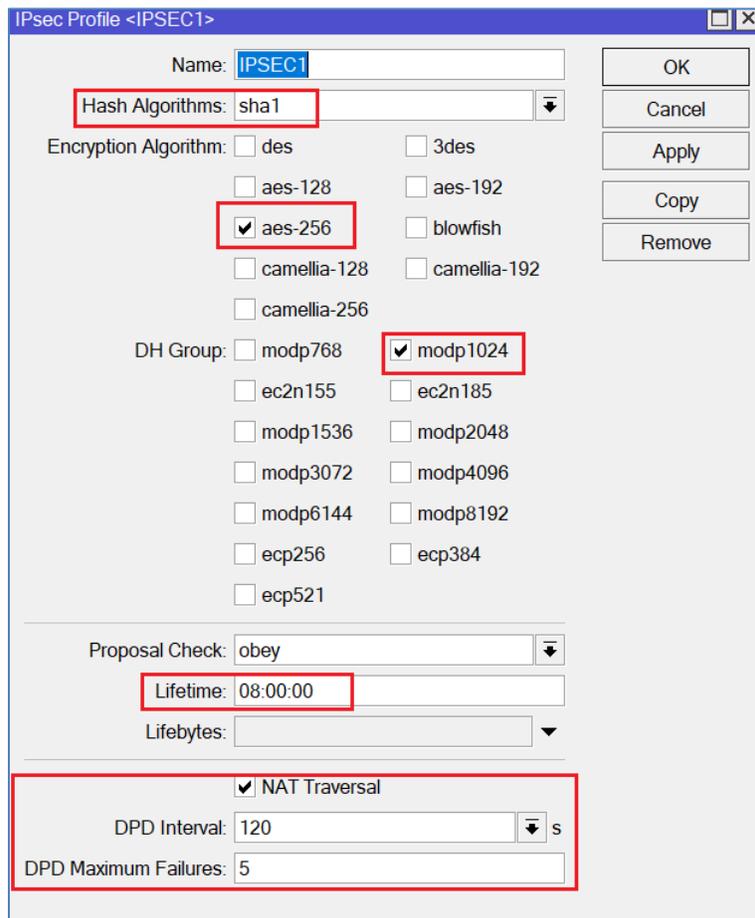
### FASE 1

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

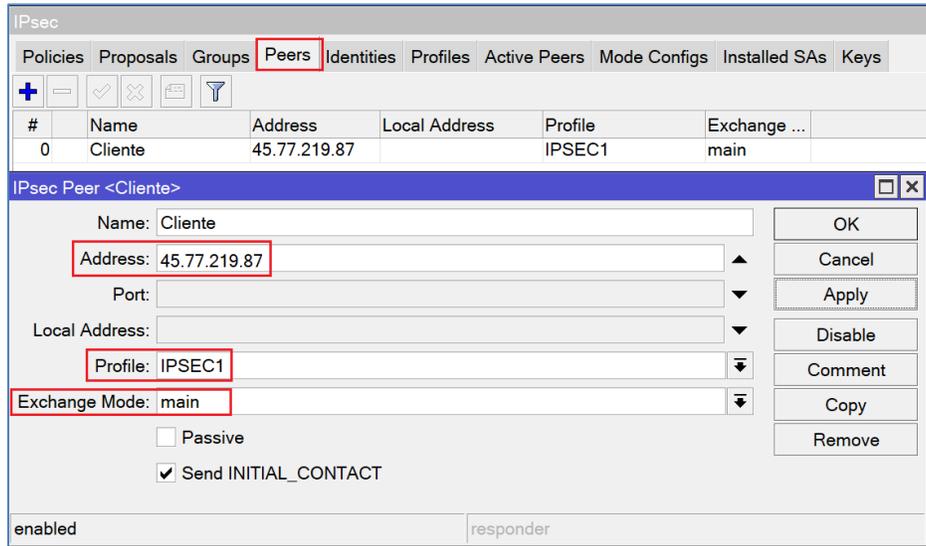
Dentro del menú IPSEC vamos a Profiles:



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**.



The screenshot shows the IPsec configuration interface. The 'Peers' tab is selected, and a table lists the peers. Below the table, the 'IPsec Peer <Cliente>' dialog is open, showing the configuration for the 'Cliente' peer. The 'Address' field is set to '45.77.219.87', the 'Profile' is 'IPSEC1', and the 'Exchange Mode' is 'main'. The 'Send INITIAL\_CONTACT' checkbox is checked.

#	Name	Address	Local Address	Profile	Exchange ...
0	Cliente	45.77.219.87		IPSEC1	main

IPsec Peer <Cliente>

Name: Cliente

Address: 45.77.219.87

Port:

Local Address:

Profile: IPSEC1

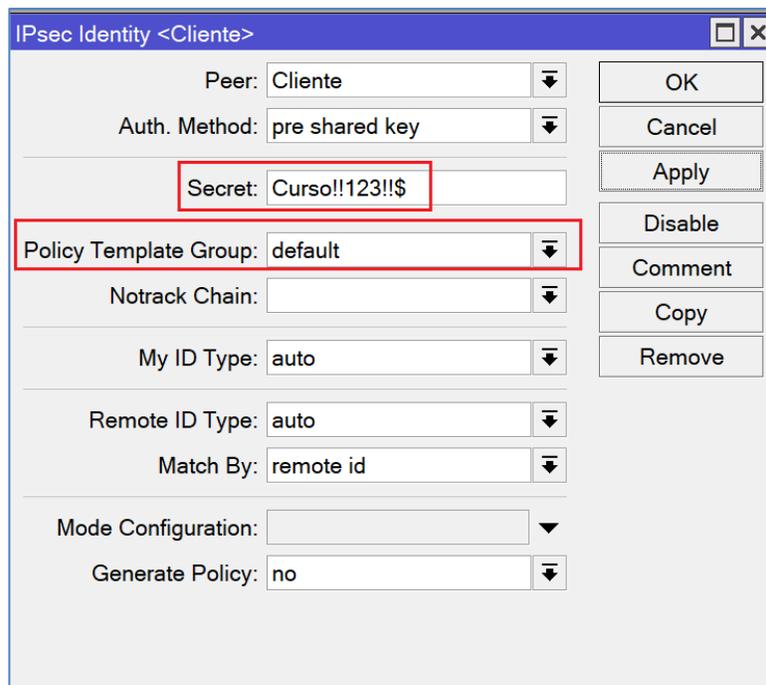
Exchange Mode: main

Passive

Send INITIAL\_CONTACT

enabled responder

**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.



The screenshot shows the 'IPsec Identity <Cliente>' dialog. The 'Peer' is set to 'Cliente', the 'Auth. Method' is 'pre shared key', and the 'Secret' is 'Curso!!123!!\$'. The 'Policy Template Group' is set to 'default'. Other fields include 'Notrack Chain', 'My ID Type', 'Remote ID Type', 'Match By', 'Mode Configuration', and 'Generate Policy'.

IPsec Identity <Cliente>

Peer: Cliente

Auth. Method: pre shared key

Secret: Curso!!123!!\$

Policy Template Group: default

Notrack Chain:

My ID Type: auto

Remote ID Type: auto

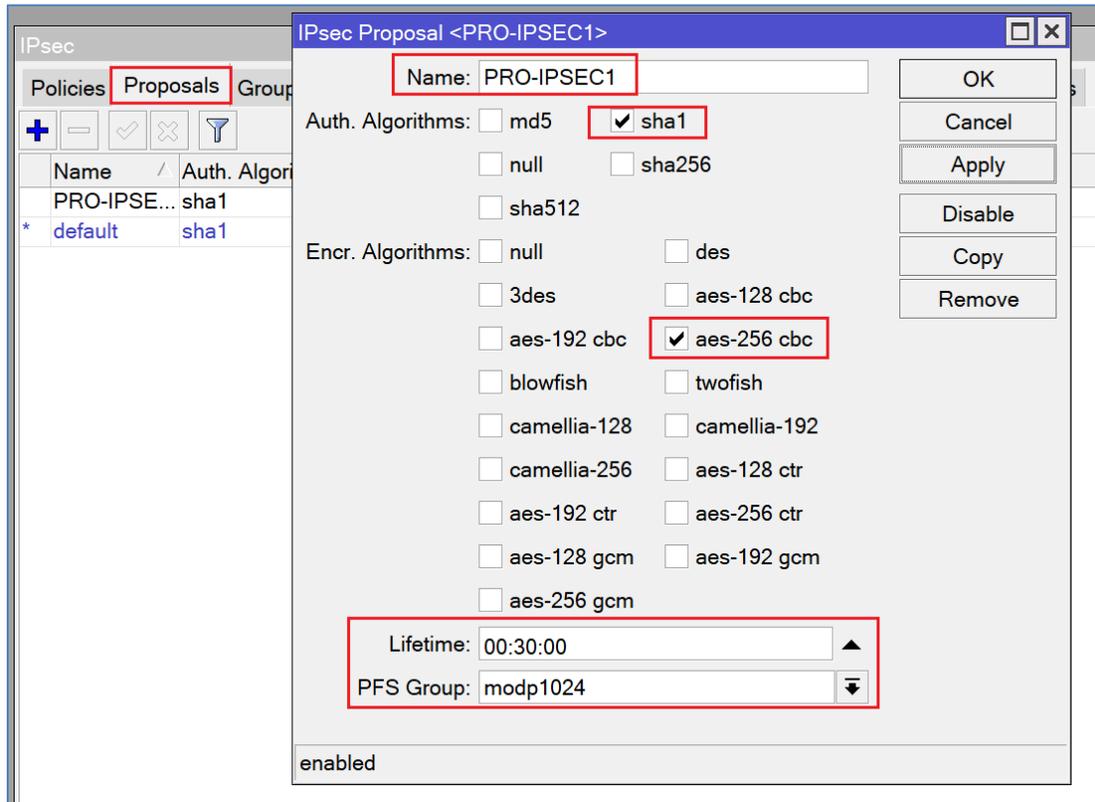
Match By: remote id

Mode Configuration:

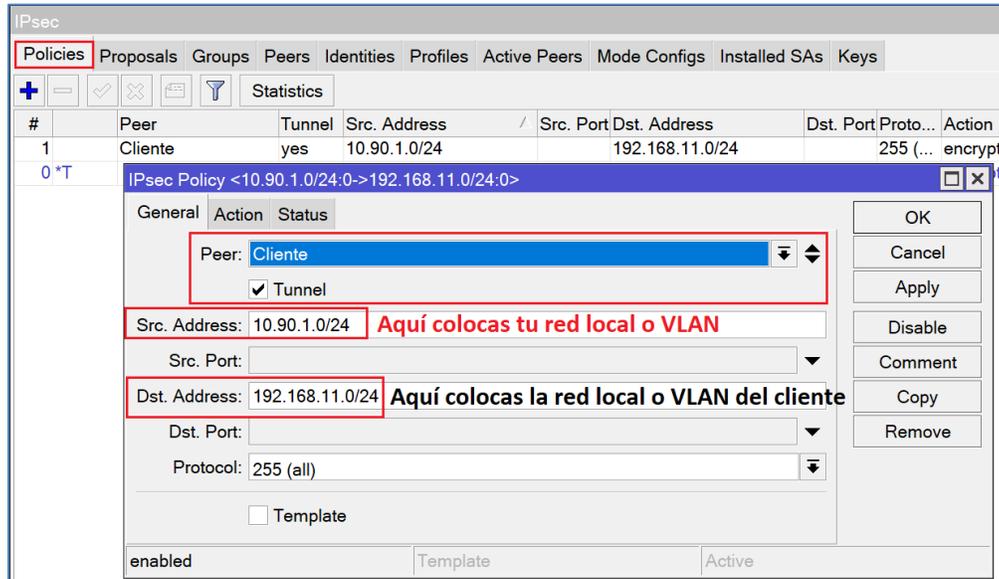
Generate Policy: no

## FASE 2

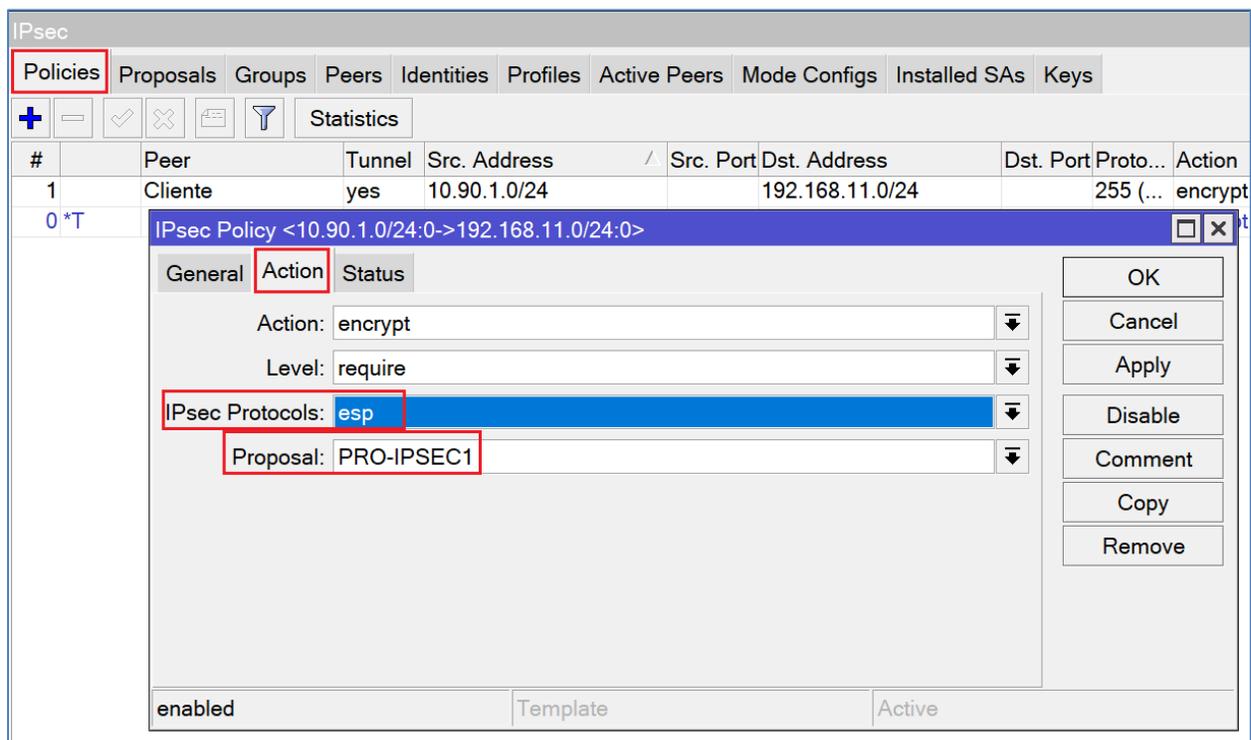
**Paso 4:** Nos dirigimos al menú **Proposal** y configuramos de la siguiente forma. Algoritmo de autenticación **sha1**, algoritmo de encriptación **aes-256cbc**, **lifetime 30** minutos y **PFS Group modp1024**.



**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.



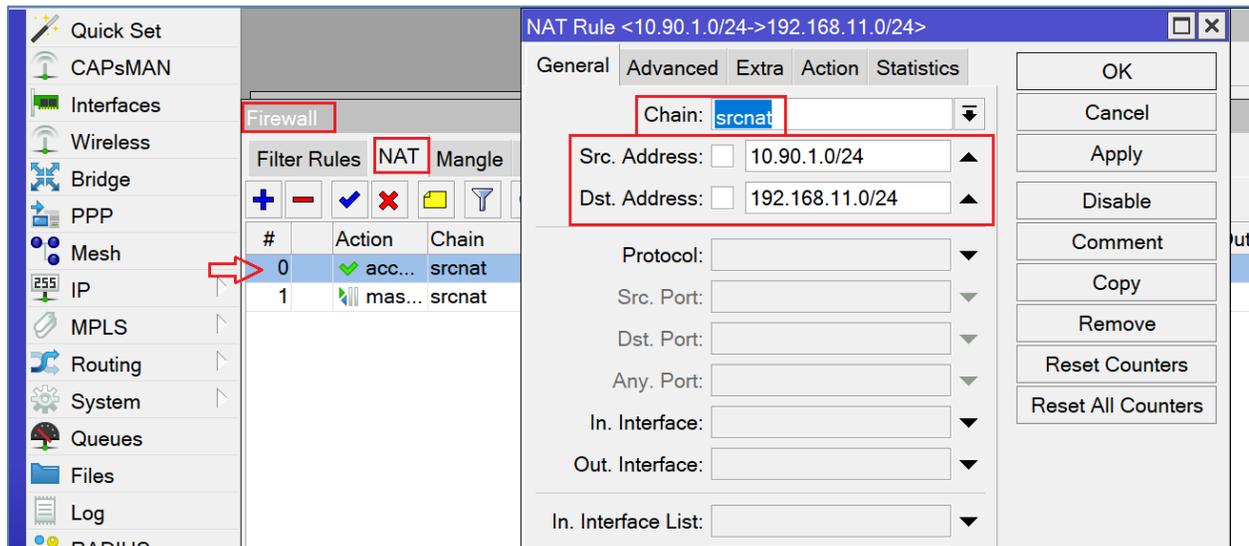
Para completar la configuración vamos al menú **Action** de nuestra política IPSEC. Aquí elegimos el protocolo **esp** y el **proposal** para nuestra fase 2. La encriptación será requerida ya que trabajaremos un túnel seguro esp.



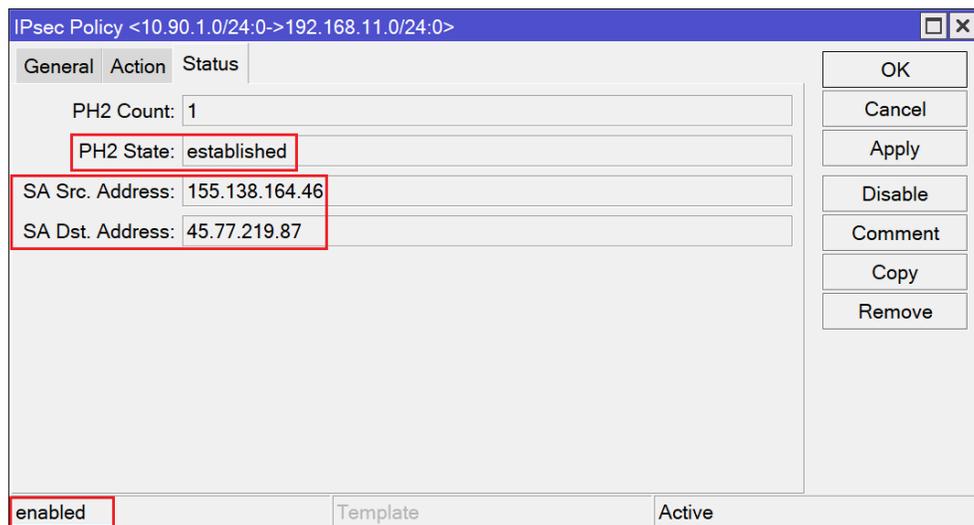
## Paso 6: configuración de regla de NAT

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.

```
Terminal
[Tab]          Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options
/              Move up to base level
..            Move up one level
/command      Use command at the base level
[admin@SERVER-VPN] > ping 192.168.11.1 src-address=10.90.1.1
  SEQ HOST                SIZE TTL TIME  STATUS
    0 192.168.11.1         56  64 22ms
    1 192.168.11.1         56  64 21ms
    2 192.168.11.1         56  64 22ms
    3 192.168.11.1         56  64 21ms
    4 192.168.11.1         56  64 22ms
    5 192.168.11.1         56  64 21ms
    6 192.168.11.1         56  64 21ms
    7 192.168.11.1         56  64 22ms
    8 192.168.11.1         56  64 21ms
    9 192.168.11.1         56  64 21ms
   10 192.168.11.1         56  64 21ms
   11 192.168.11.1         56  64 21ms
    sent=12 received=12 packet-loss=0% min-rtt=21ms avg-rtt=21ms max-rtt=22ms
[admin@SERVER-VPN] > █
```

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