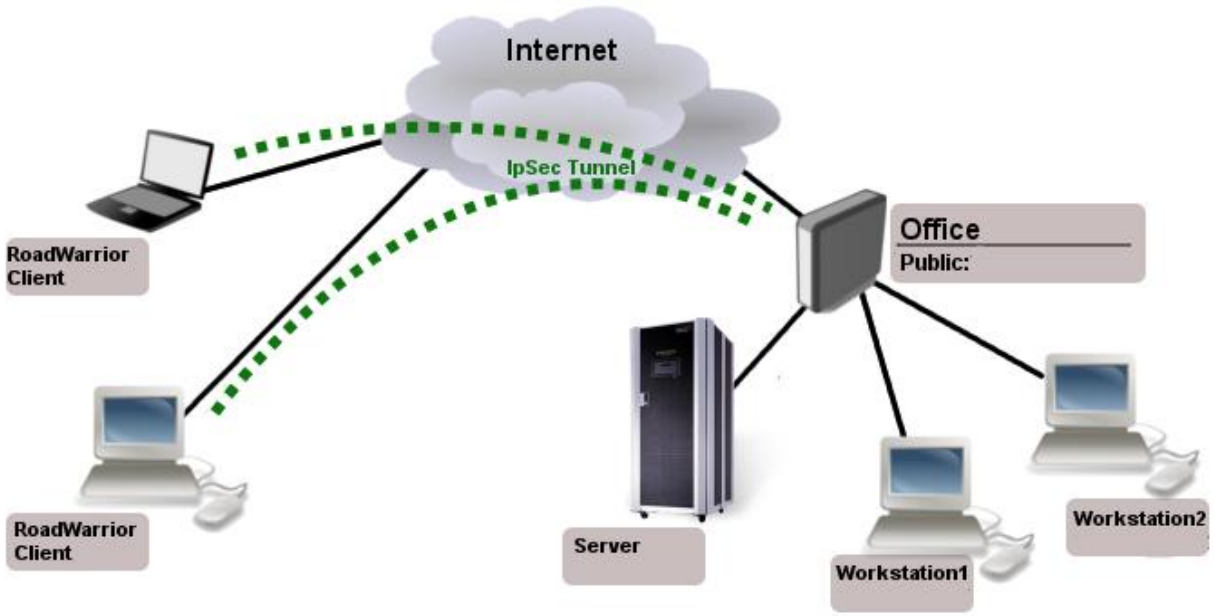
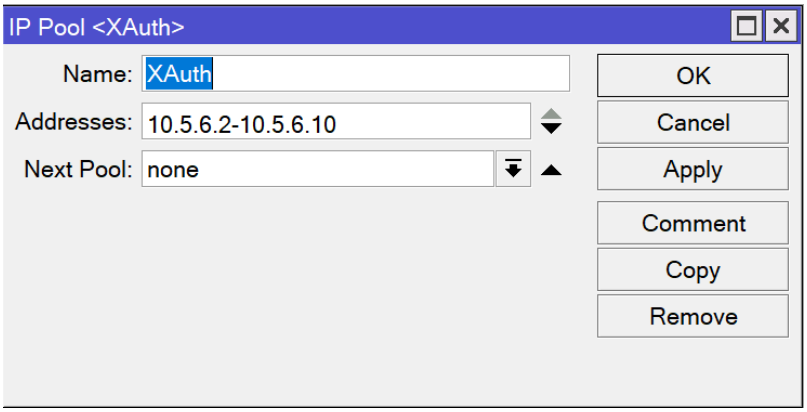
Laboratorio: Configuración de IPsec Server Xauth PSK

Objetivo: Configurar un VPN IPsec server Xauth PSK para Roadwarriors



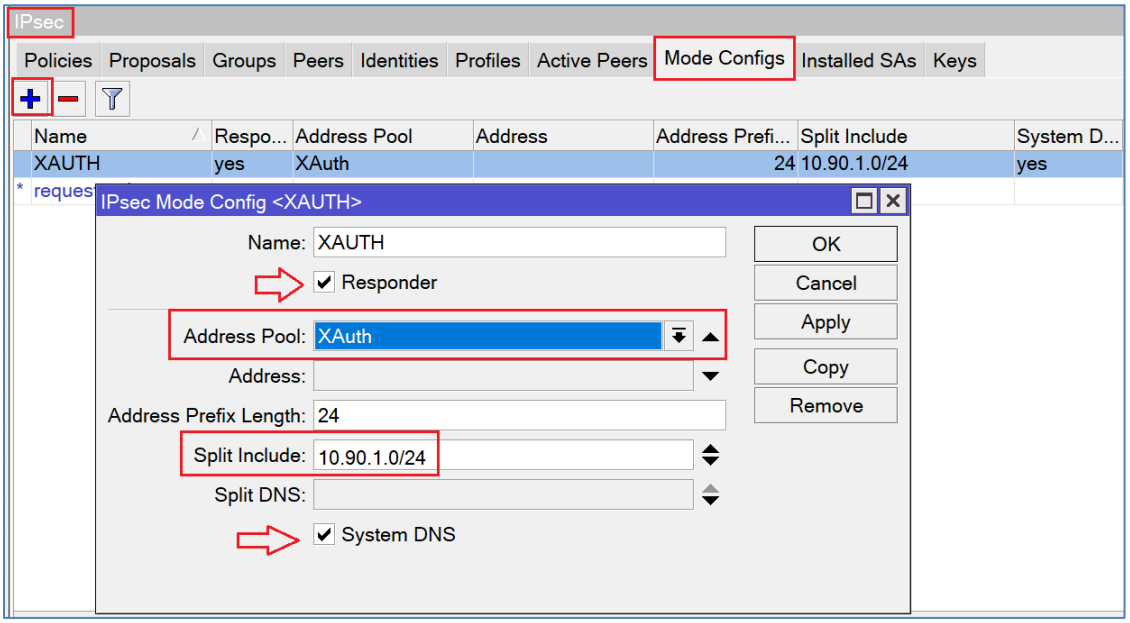
CONFIGURACIÓN DE LA FASE 1

- **Paso 1:** Vamos a crear un pool de IPs con el rango que ustedes prefieran. Este pool será utilizado para asignarle a cada cliente conectado.En mi caso, utilizaré **10.5.6.2-10.5.6.10**.

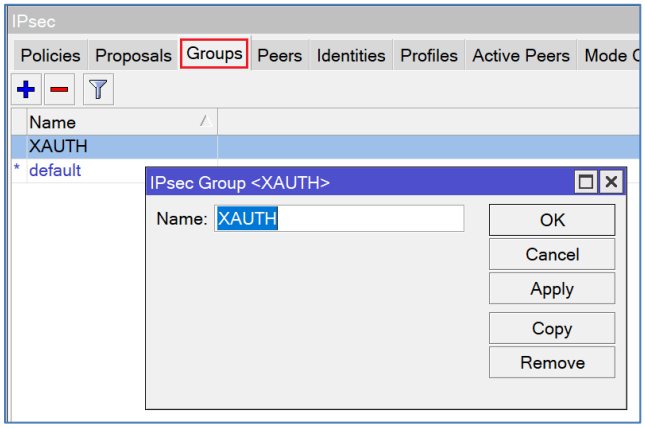


- **Paso 2:** Vamos a la menú **IP-IPsec**, una vez allí vamos a la pestaña **Mode Configs** y le damos al boton de + . Una vez pulsado nos saldrá un una ventana en la cual configuraremos los siguientes parámetros.

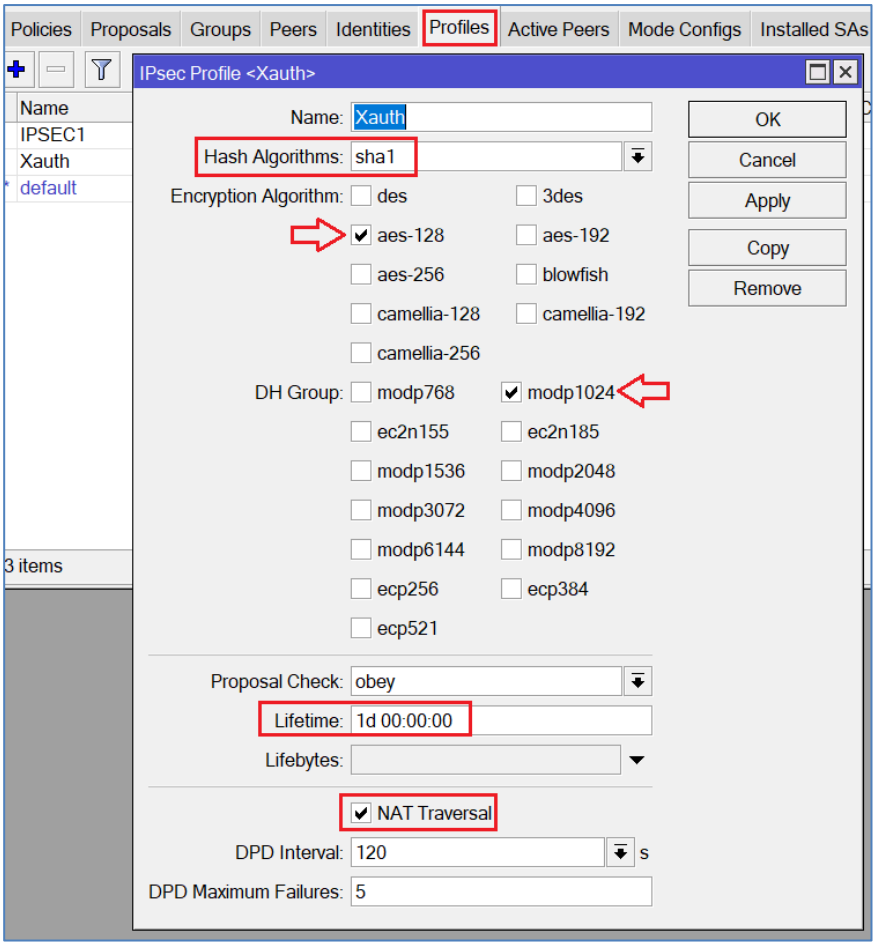
Name: Nombre el modo de configuración.
Address Pool: Pool de direcciones creado anteriormente.
Split Include: **Redes a las cuales nuestros clientes tendrán acceso.**
System DNS: Añade los DNS existente a nuestros clientes una vez se conecten.



- **Paso 3:** Luego vamos a **Groups** para crear una plantilla de configuración especial e independiente de cualquier otra configuración. Hacemos click en el signo de + y le ponemos el nombre **XAUTH.**

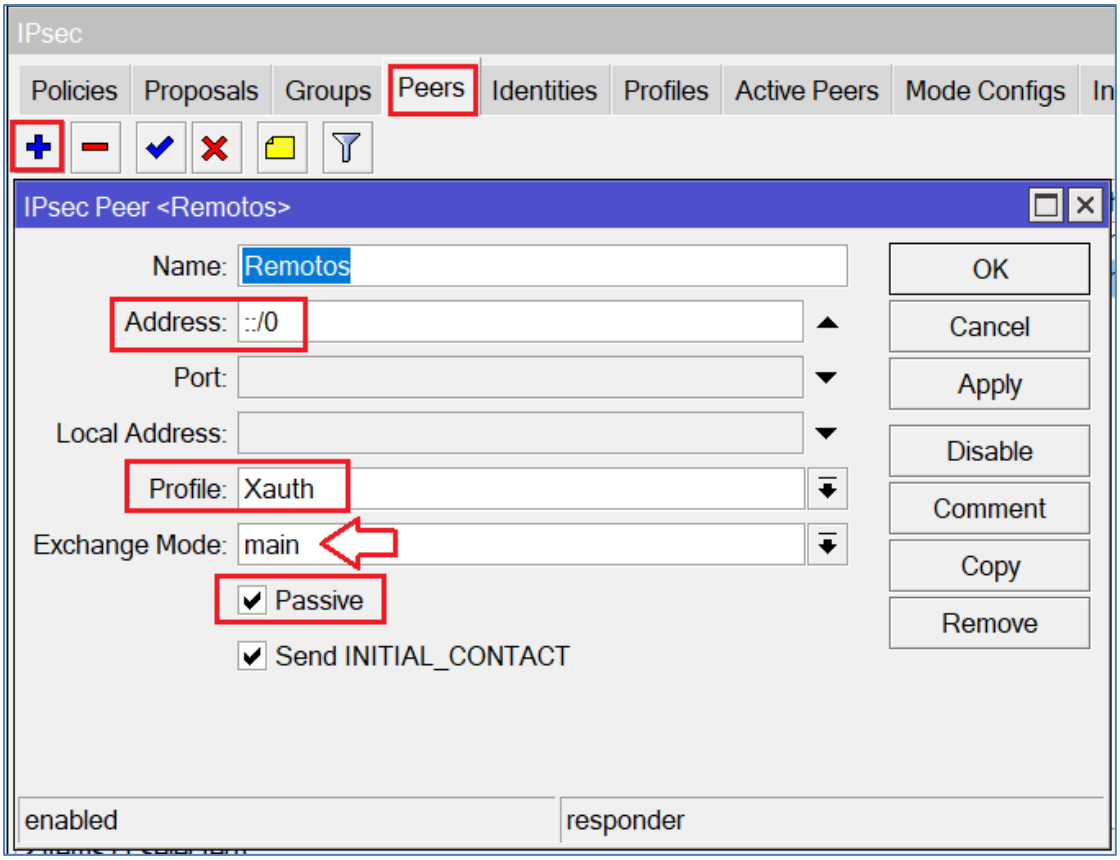


- **Paso 4:** Ahora vamos a la pestaña **Profile** para empezar con lo que sera la **fase 1** de nuestro server y configuraremos los siguiente parámetros:



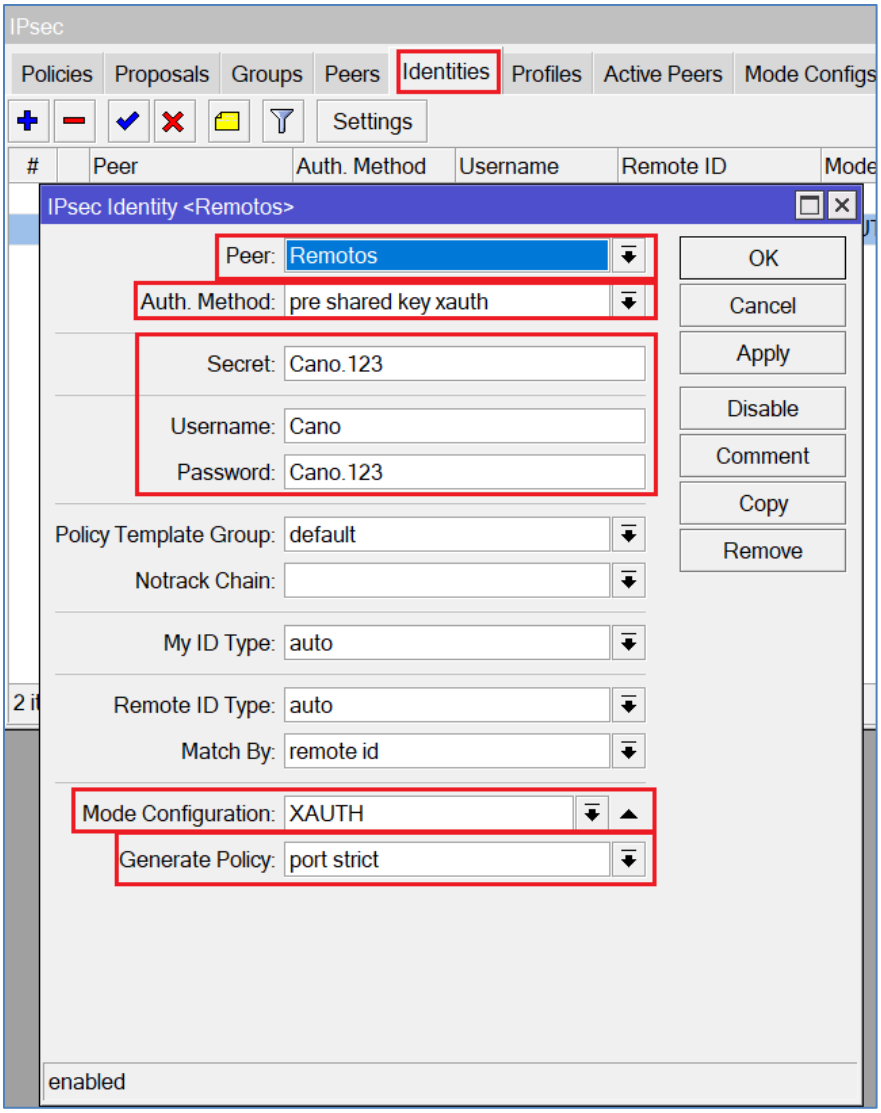
- **Paso 5:** Ahora vamos a la pestaña **Peer** para asignar el perfil y colocar las direcciones que permitimos conectar a nuestro VPN:

Nombre = Remotos: Es un identificador de los clientes a conectar.
Address = 0.0.0.0/0: Para establecer la negociación con cualquier dirección que solicite. Al completar este paso se visualizará **::/0** como en la imagen.
Passive= yes: Esto nos sirve para que nuestro túnel se mantenga a la espera de un tráfico inicial.
Exchange Mode = Main: Es nuestro intercambio inicial de llaves **IKEv1** en modo Main. **Luego de completar el laboratorio vamos a cambiar a IKEv2**



- **Paso 6:** Vamos a **Identities** configuraremos los siguientes parámetros:

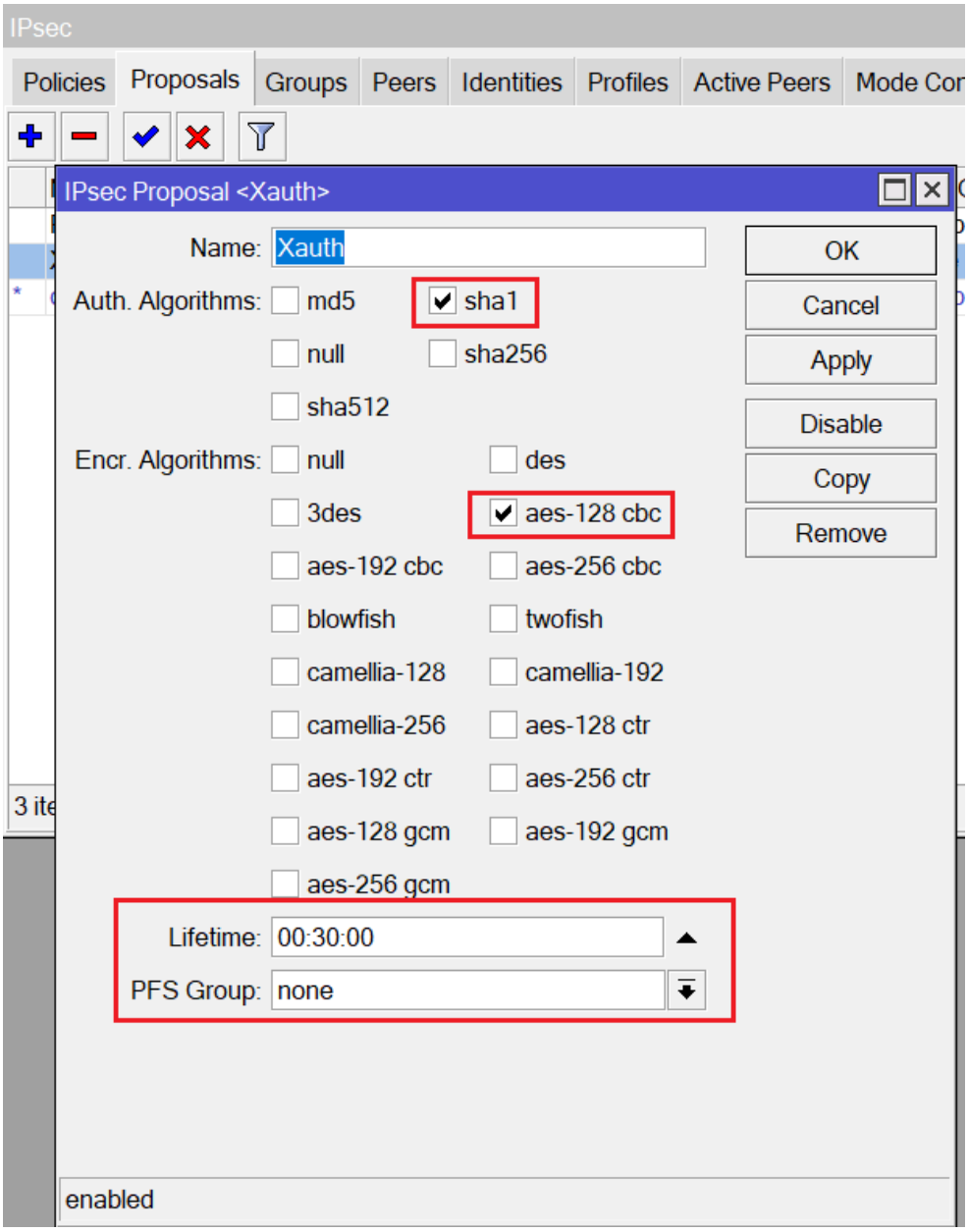
Peer: Seleccionamos creado en el paso anterior llamado Remotos
Auth Method: Seleccionamos el modo de autorización pre shared key xauth
Secret: Es el secret IPSEC general
Username: Es el usuario que configuraremos en el cliente para conectarnos
Password: Contraseña para el usuario anterior.
Mode Configuration: Seleccionamos el modo de configuración XAUTH
Generate Policy: Port strict



FASE 1 completada

CONFIGURACIÓN DE LA FASE 2

- **Paso 7:** Vamos a configurar el **Proposals** con los siguientes algoritmos de autenticación, encriptación, lifetime y PFS group.



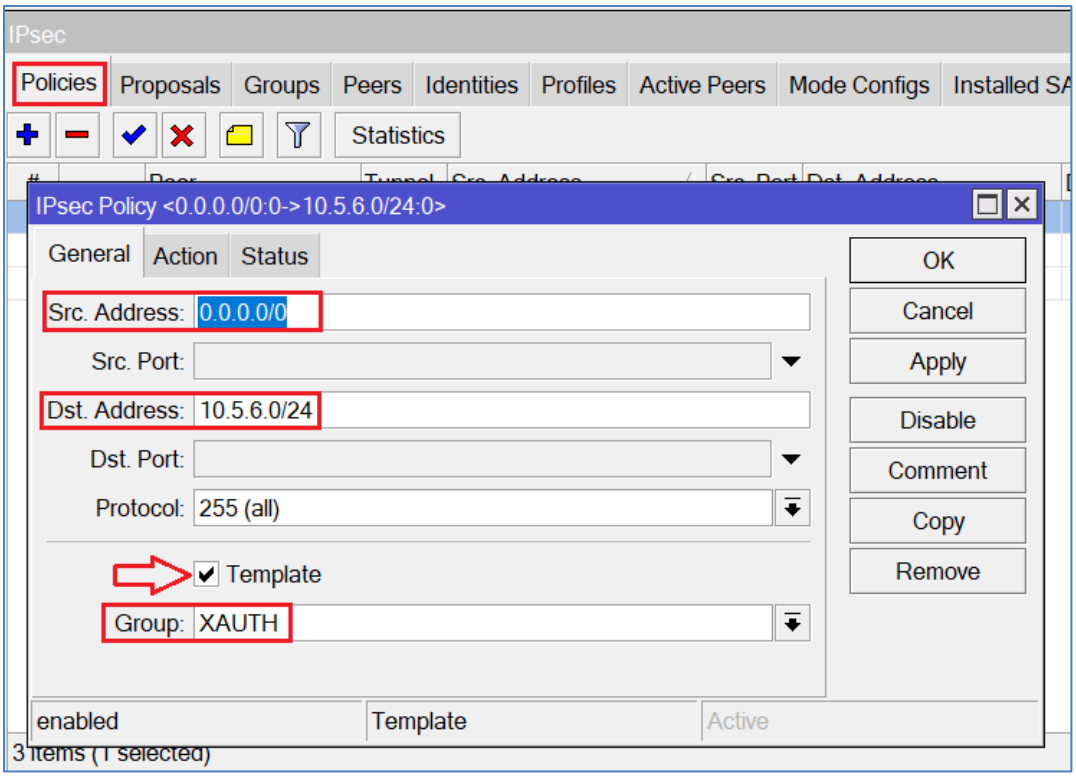
- **Paso 8:** Nos dirigimos a la pestaña **Policies**. **Lo primero que debemos hacer es dar click en Template, luego veremos la configuración como la imagen.**

El **Src. Address:** 0.0.0.0/0 representa cualquier dirección entrante, ya que nuestros clientes se conectarán desde cualquier IP pública.

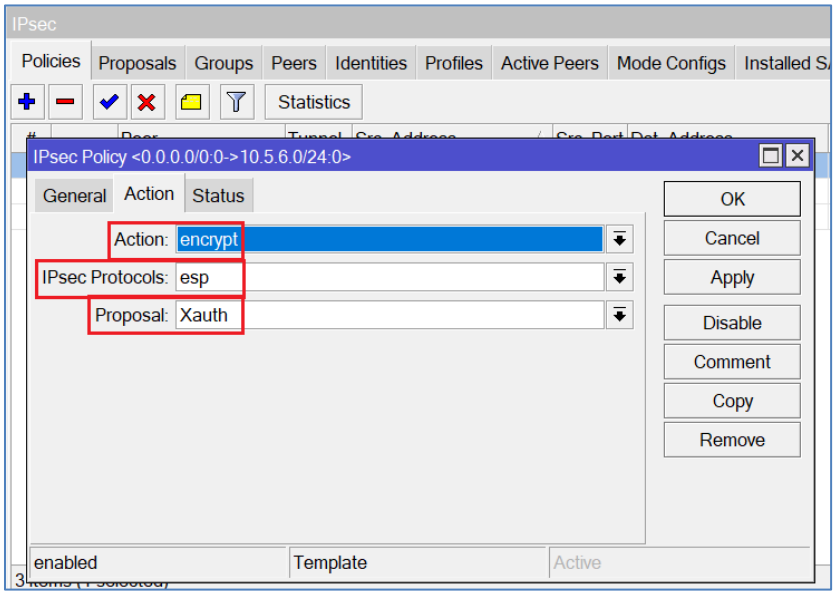
El **Dst. Address**: será el rango del pool designado para nuestra VPN. Al conectarse el cliente, vamos a recibir una de estas IPs del pool.

Por último, agregamos el **Group XAUTH** creados por nosotros anteriormente.

Hacemos click en Action para configurar el resto



- **Paso 9:** Aquí vamos a seleccionar la acción de encriptar con el proposal creado y como protocolo IPSEC elegimos ESP para mejor seguridad.



- **Paso 10:** Configurar un cliente para este VPN en su celular.
  Para crear el cliente debe ir al menú de VPNs y elegir IPSEC XAUTH.
  Aquí debe configurar con los siguientes parámetros:

  - IP Pública de su servidor IPSEC
  - Secret del IPSEC
  - Usuario
  - Contraseña

Al completar, vamos a active peers y probamos tráfico a la red que ha permitido en el túnel VPN. La mía ha sido 10.90.1.0/24. Prueba haciendo Ping a la VLAN tuya.