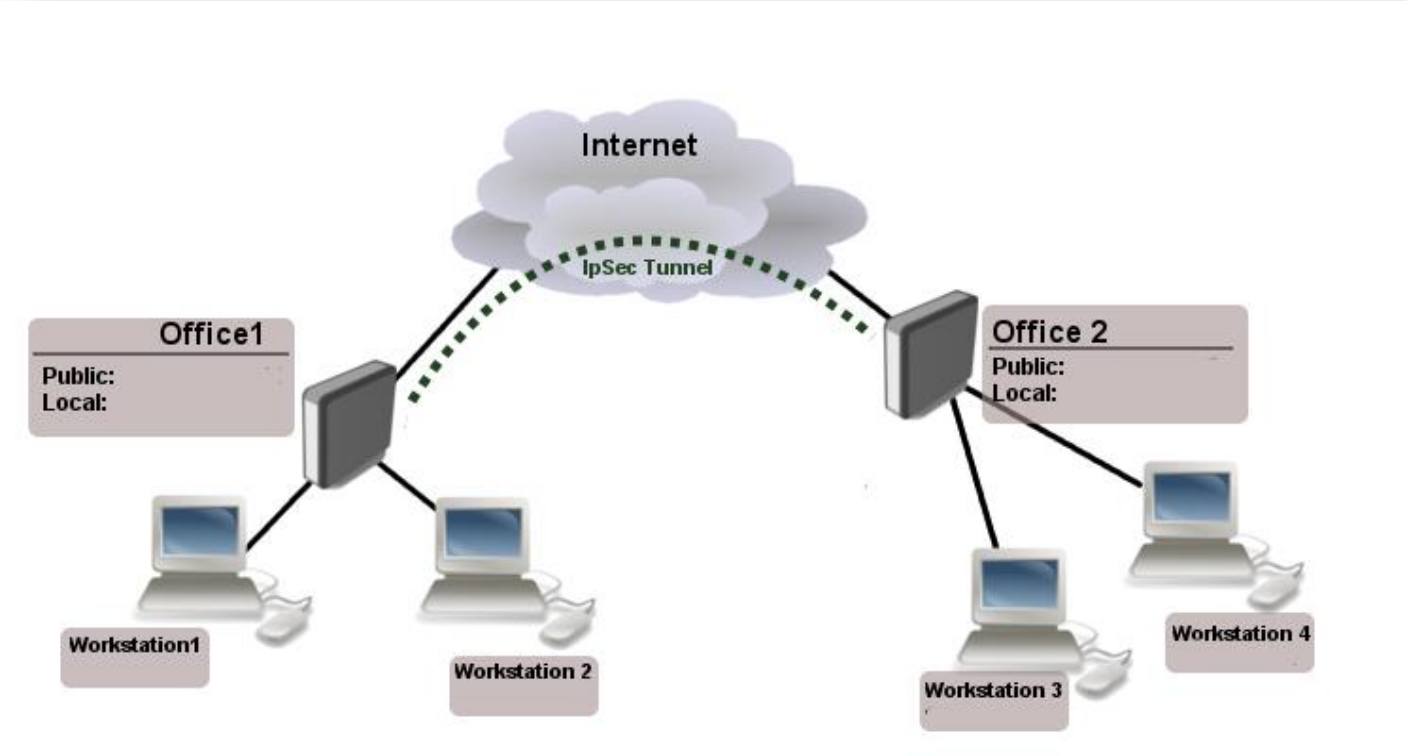
Laboratorio 2.3: Configuración IPsec site to site MikroTik-MikroTik.

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

Site to Site IPsec tunnel MikoTik-Mikoritk

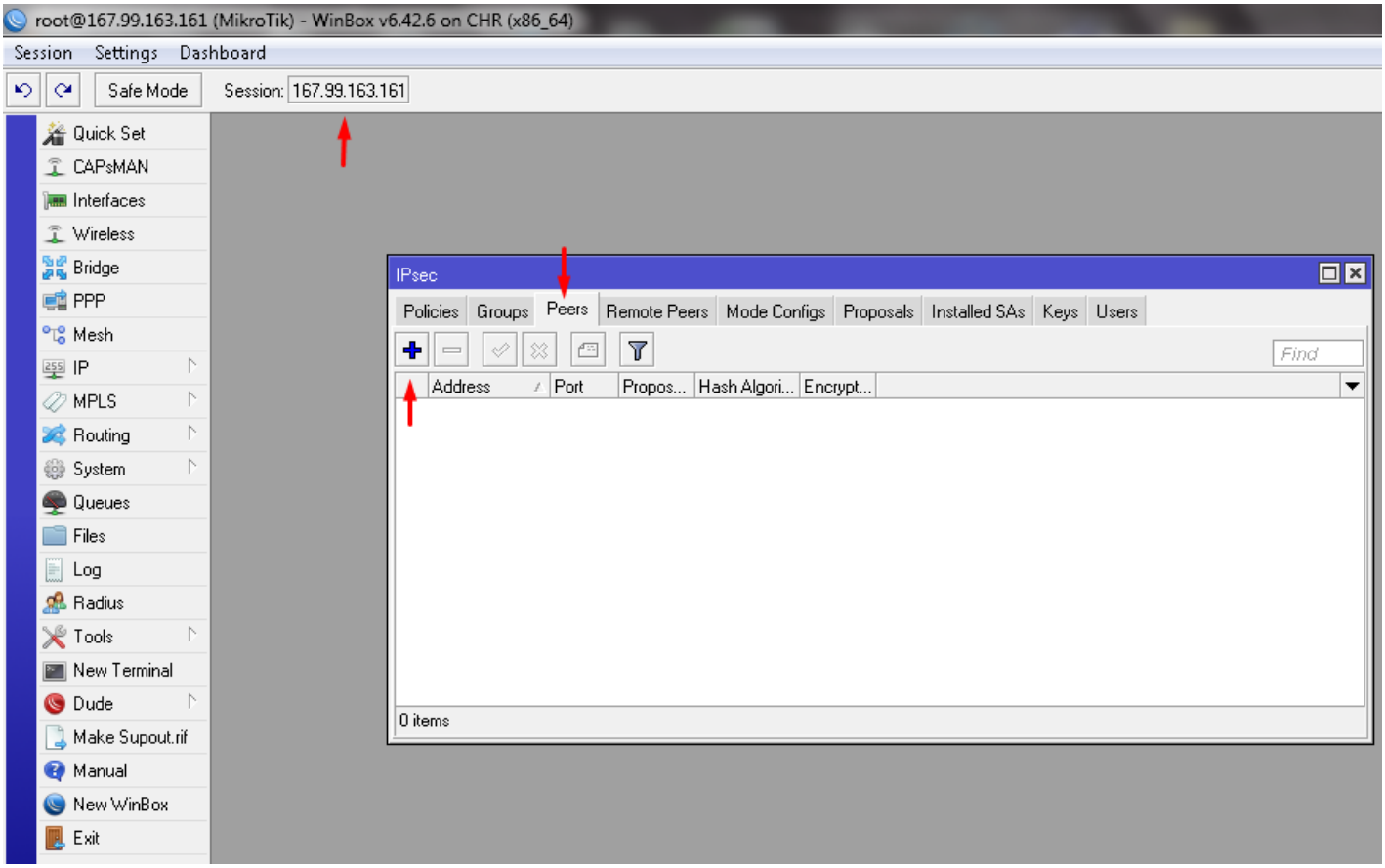
Router A----------IPsec---------RouterB



Router-A:

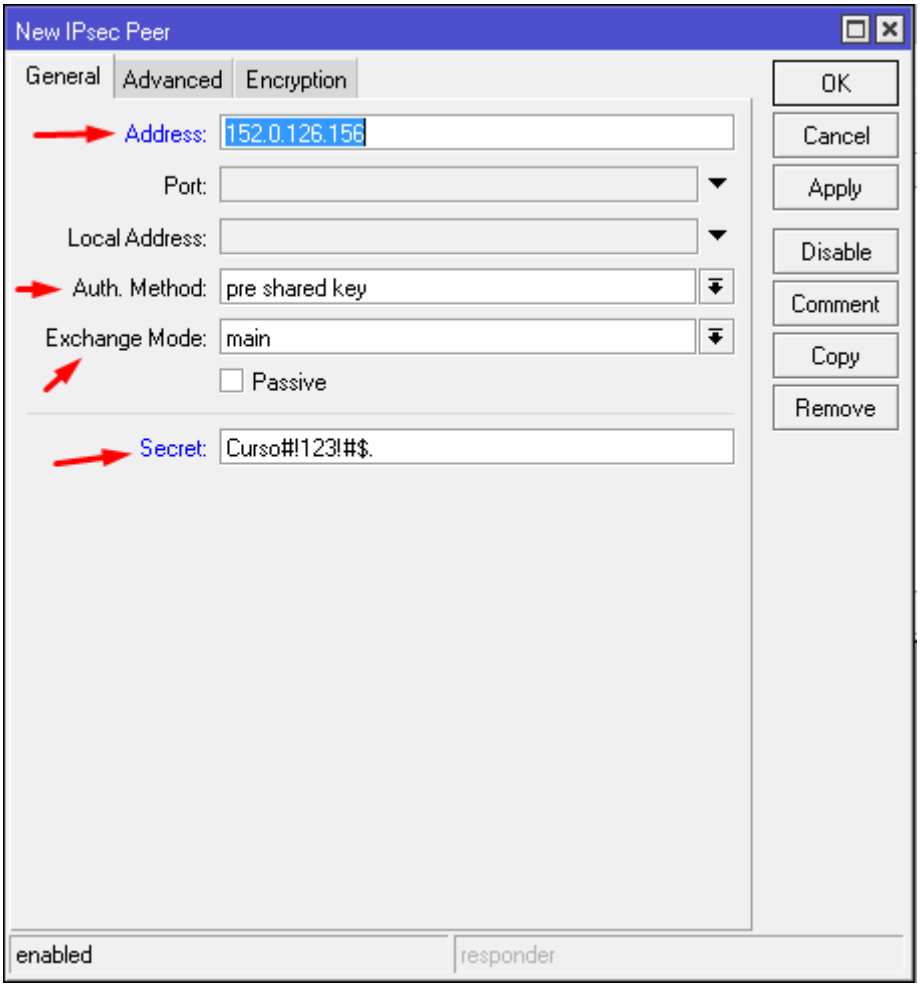
Fase 1:

Paso 1: Empezamos nuestro túnel dirigiendo a la opción IP damos click en IPsec y se nos abrirá una ventana donde podremos ver todas las pestañas de configuración, lo primero que haremos será dirigirnos a la pestaña Peers le daremos click al botón + para empezar con la Fase 1 De nuestra VPN. 2.3.1.



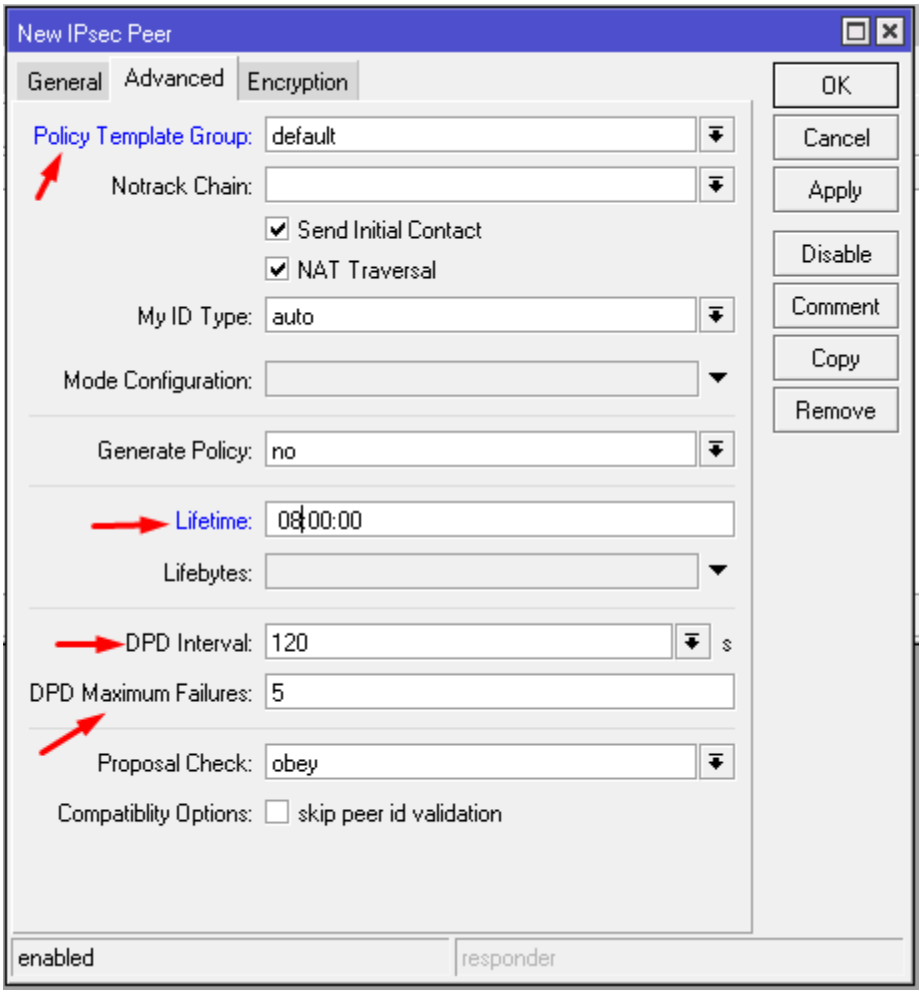
2.3.1

Paso 2: Ahora procederemos a empezar nuestra configuración de la Fase 1 llenando los siguientes: Address: IP Publica del otro router, Auth Method: pre share key, Exchange Mode: Main, y por ultimo Nuestro secret: Curso#!123!#$. Ver imagen 2.3.2.



2.3.2

Paso 3: Ahora vamos a la pestaña advanced a configurar los siguientes parámetros, Send Inicitial Contact=yes, Nat Traversal=yes en esta ocasión abra ocasiones donde no será necesario, Lifetime igual a 8 horas ojo este parámetro debe ser igual en ambos routers, DPD Interval=120 y DPD Maximun Failures=5, los últimos dos parámetros se pueden modificar teniendo muy en cuenta que en ambas partes deben tener los mismo valores para evitar contratiempos. Ver imagen 2.3.2.



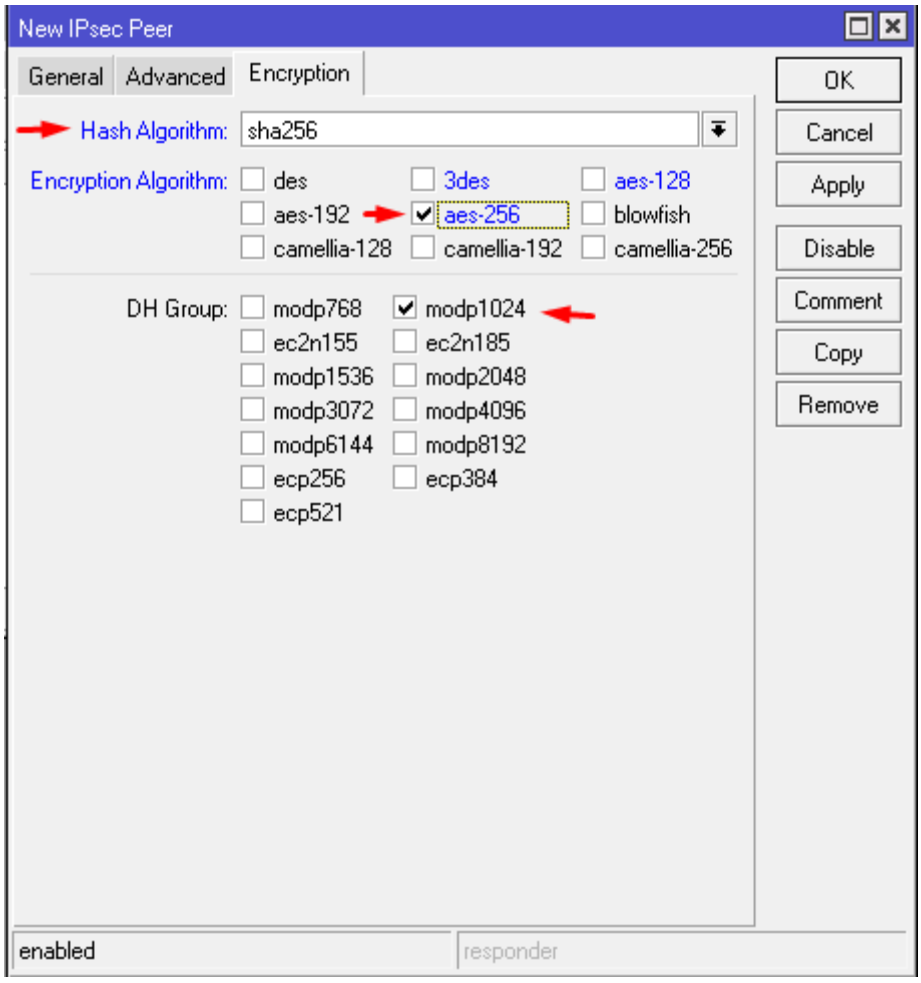
2.3.2

Paso 4: Esta parte es muy importante aquí definiremos los protocolos de autenticación, encriptación y DH (**Diffie-Hellman**) de la Fase 1 de nuestro tunnel ipsec. Recuerden esta configuración es modificable a su gusto siempre y cuando en ambos routers tengan la misma configuración. Ver imagen 2.3.4

Autenticación: Hash Algorithm: Sha256, *aun muy seguro.*

Encriptación: encryption Algorithm: aes-256, *Muy complejo, seguro y rápido.*

DH Group: modp1024.



2.3.4

Fase 2:

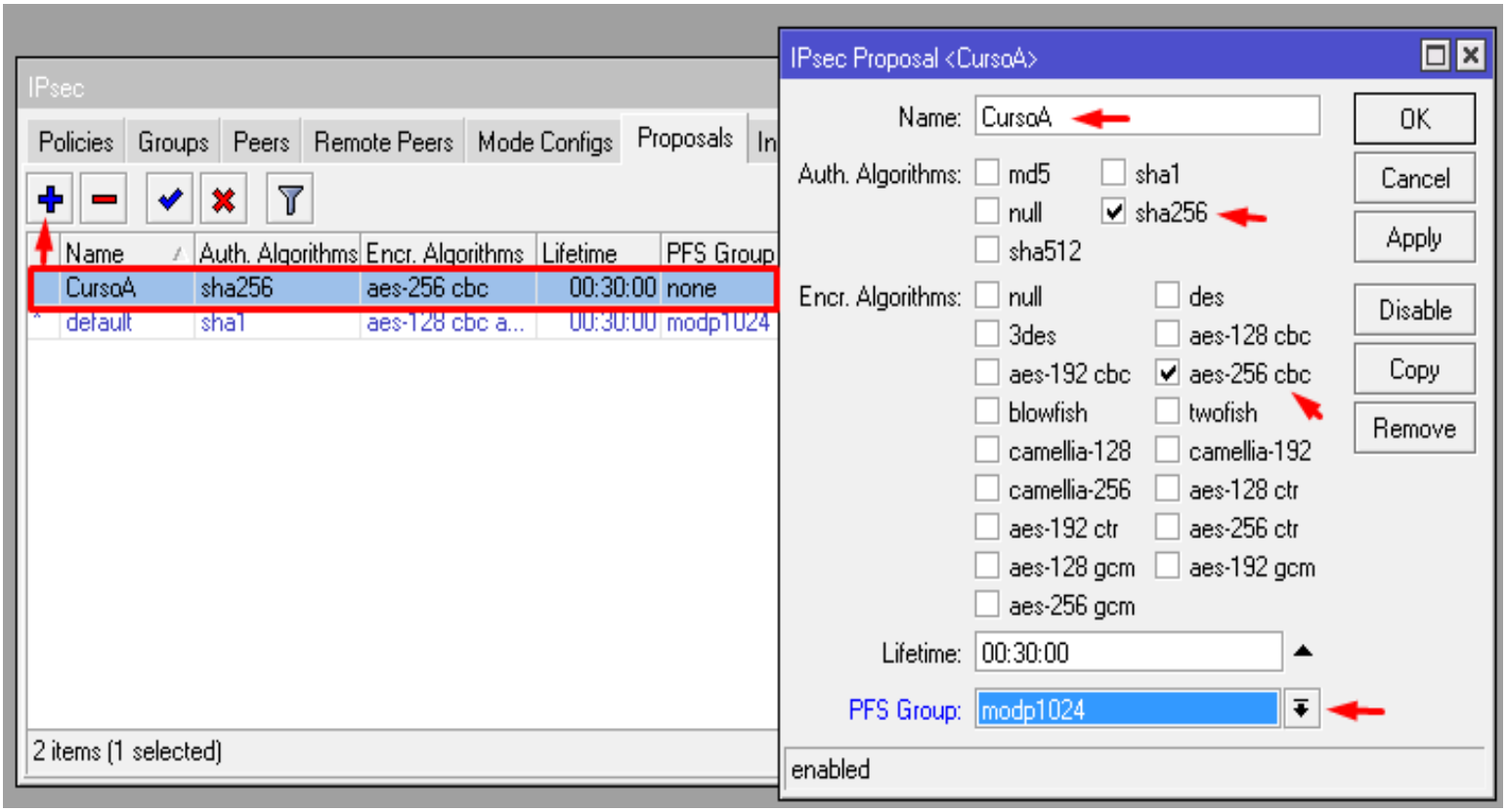
Paso 5: Ya llegamos a la configuración de la fase 2 de nuestro ipsec, para ello nos dijimos a la pestaña Proposals una vez allí crearemos un nuevo Proposal el cual se llamara CursosA, en el mismo configuraremos los siguientes parámetros:

Hash Algorithm: Sha256.

encryption Algorithm: aes-256 cbc.

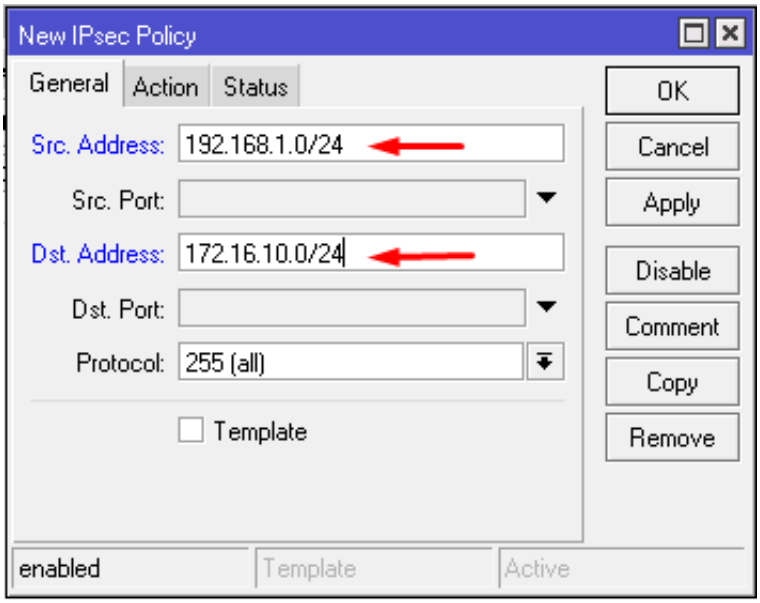
PFS Group: modb1024

Una vez configurados los pasos anteriores le damos Apply y luego OK**.**



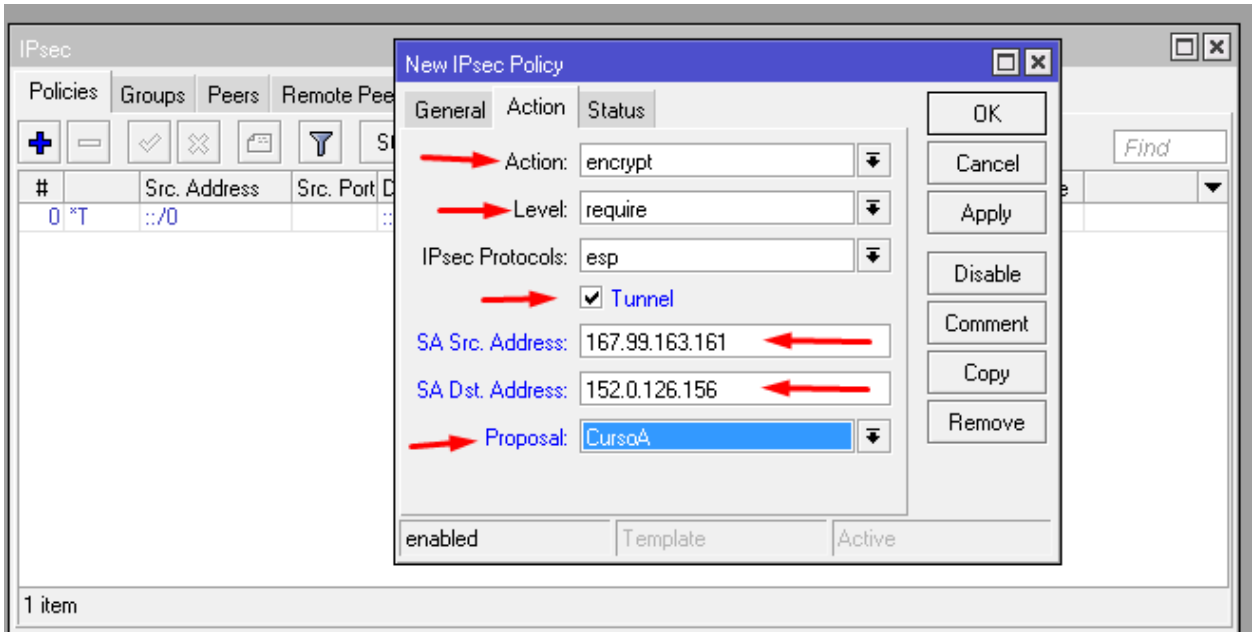
2.3.5

Paso 6: Ahora nos dirigimos a la pestaña Policy allí crearemos una nueva política para nuestro IPsec, primero vamos a General una vez allí configuraremos los siguientes parámetros Src. Address: pondremos el rango de IP de nuestra LAN , en Dst. Address: La red LAN de nuestro destino, significa la red interna que maneja el otro router. Ver imagen 2.3.6.



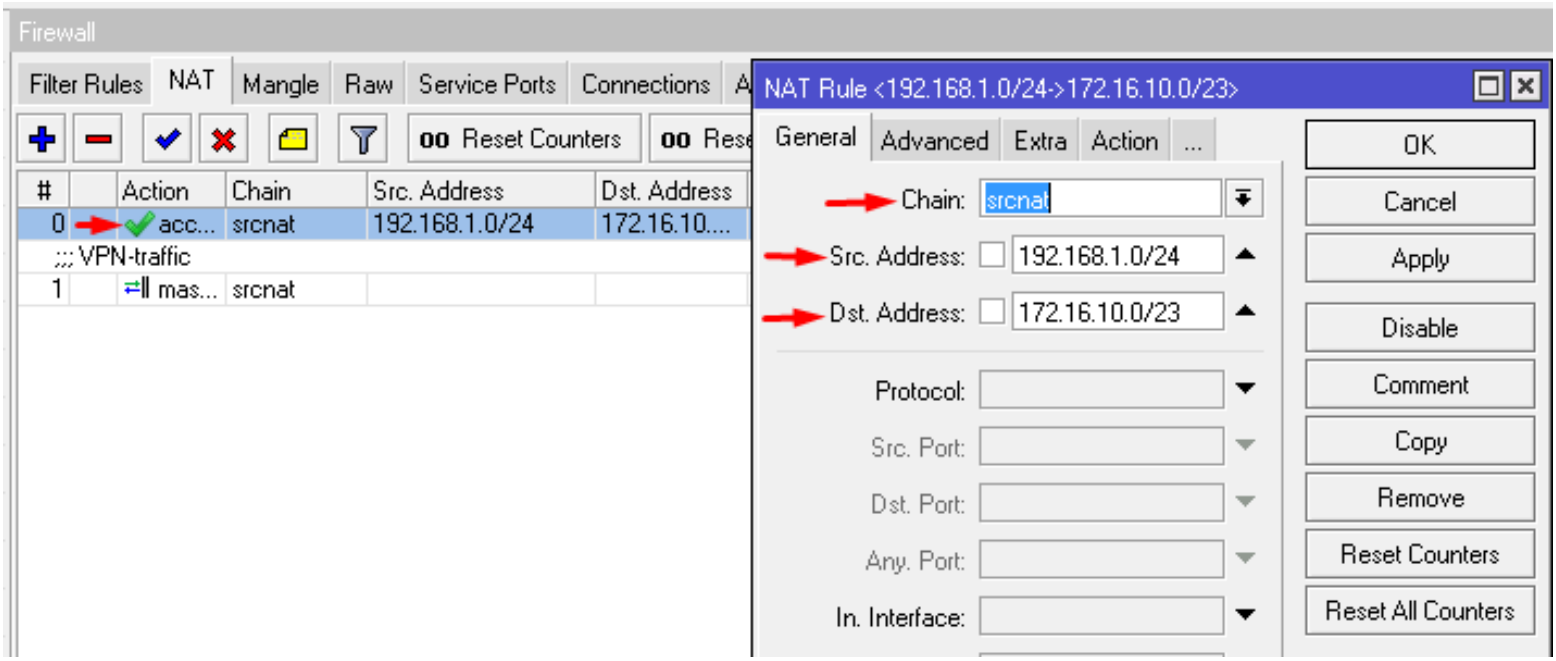
2.3.6

Paso 7: Luego nos dirigimos a la parte de Action una vez allí configuraremos los siguientes parámetros Action: encrypt, Level:require, IPsec Protocols:esp, Habilitar la casilla de Tunnel, SA Src. Address: Aquí va la dirección IP de su interfaces WAN en este caso la mía es:167.99.163.161 luego va la SA Dst Address: en este campo pondremos la IP publica del otro router la cual será:152.0.126.156 por ultimo seleccionamos el proposal creado anteriormente **CursoA.** Ver imagen 2.3.7**.**



2.3.7

Paso 8: En **Firewall – NAT** agregamos un bypas aceptando el tráfico de las dos redes LAN que se verán transparentes Src. Address: LAN de RouterA, Dst.Address: LAN de RouterB. Ver imagen 2.3.8

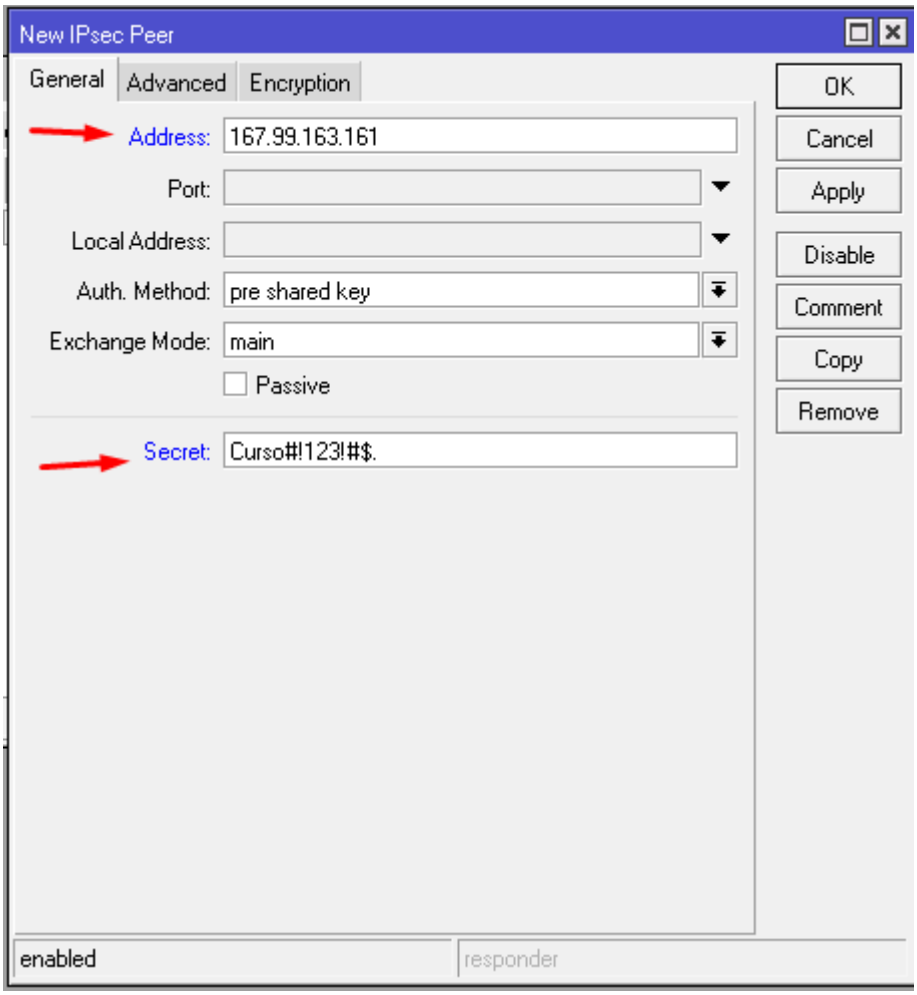


2.3.8

Router-B

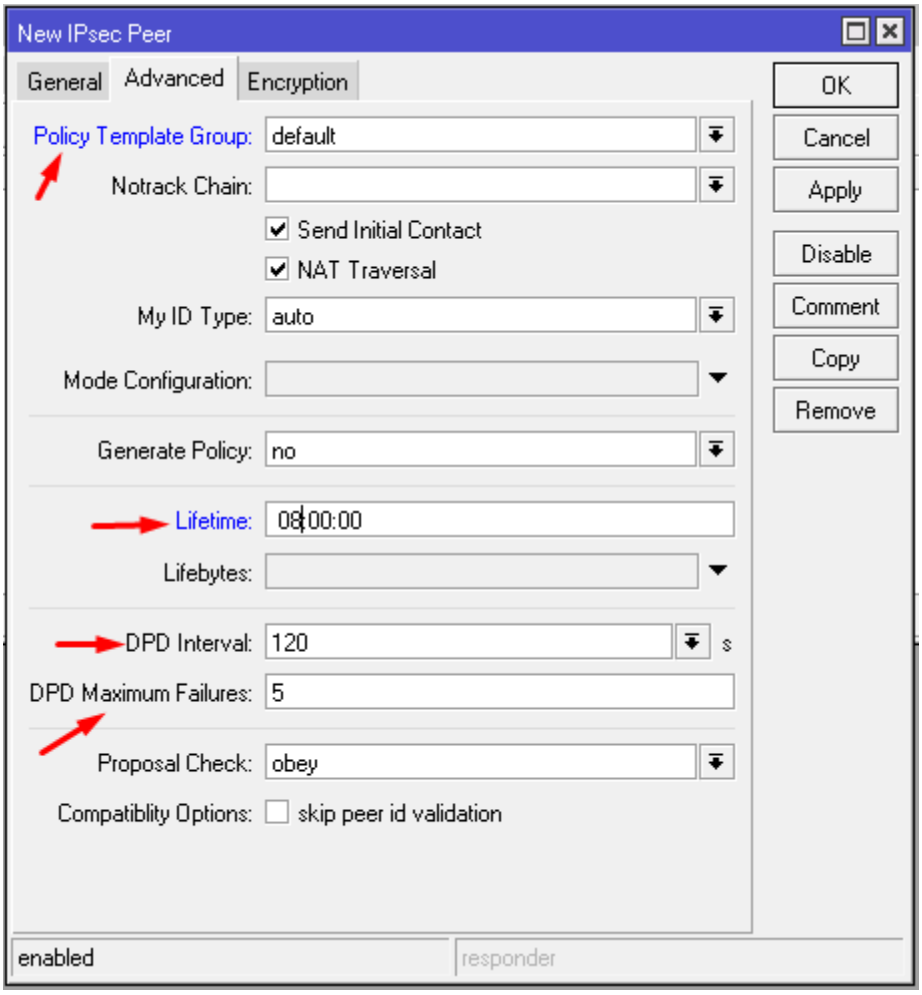
Fase 1:

Paso 1: **Ahora** procederemos a empezar nuestra configuración de la Fase 1 llenando los siguientes: Address: IP Publica del otro routerA, Auth Method: pre share key, Exchange Mode: Main, y por ultimo Nuestro secret: Curso#!123!#$. Ver imagen 2.3.9.



2.3.10

Paso 2: Ahora vamos a la pestaña advanced a configurar los siguientes parámetros, Send Inicitial Contact=yes, Nat Traversal=yes en esta ocasión abra ocasiones donde no será necesario, Lifetime igual a 8 horas ojo este parámetro debe ser igual en ambos routers, DPD Interval=120 y DPD Maximun Failures=5, los últimos dos parámetros se pueden modificar teniendo muy en cuenta que en ambas partes deben tener los mismo valores para evitar contratiempos. Ver imagen 2.3.2.



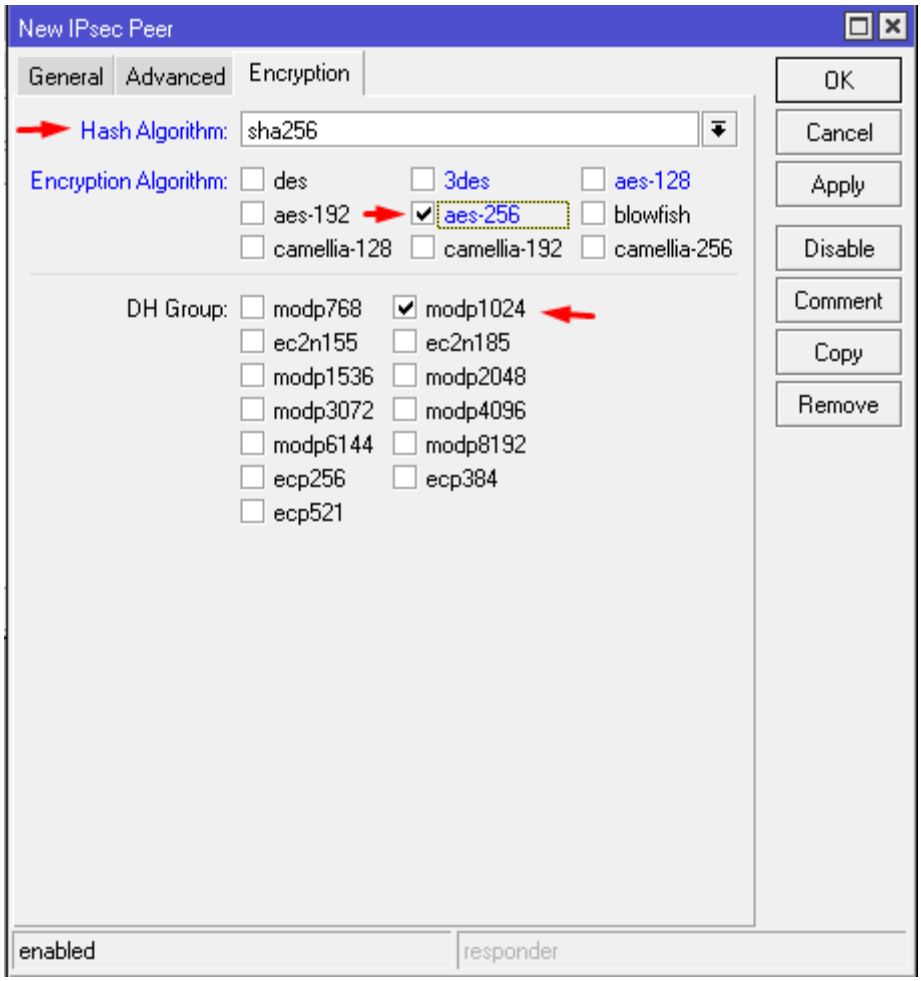
2.3.11

Paso 3: Nuevamente definiremos los protocolos de autenticación, encriptación y DH (Diffie-Hellman) de la Fase 1 de nuestro tunnel ipsec. Recuerden esta configuración es modificable a su gusto siempre y cuando en ambos routers tengan la misma configuración. Ver imagen 2.3.12

Autenticación: Hash Algorithm: Sha256, aun muy seguro.

Encriptación: encryption Algorithm: aes-256, Muy complejo, seguro y rápido**.**

DH Group: modp1024.



2.3.12

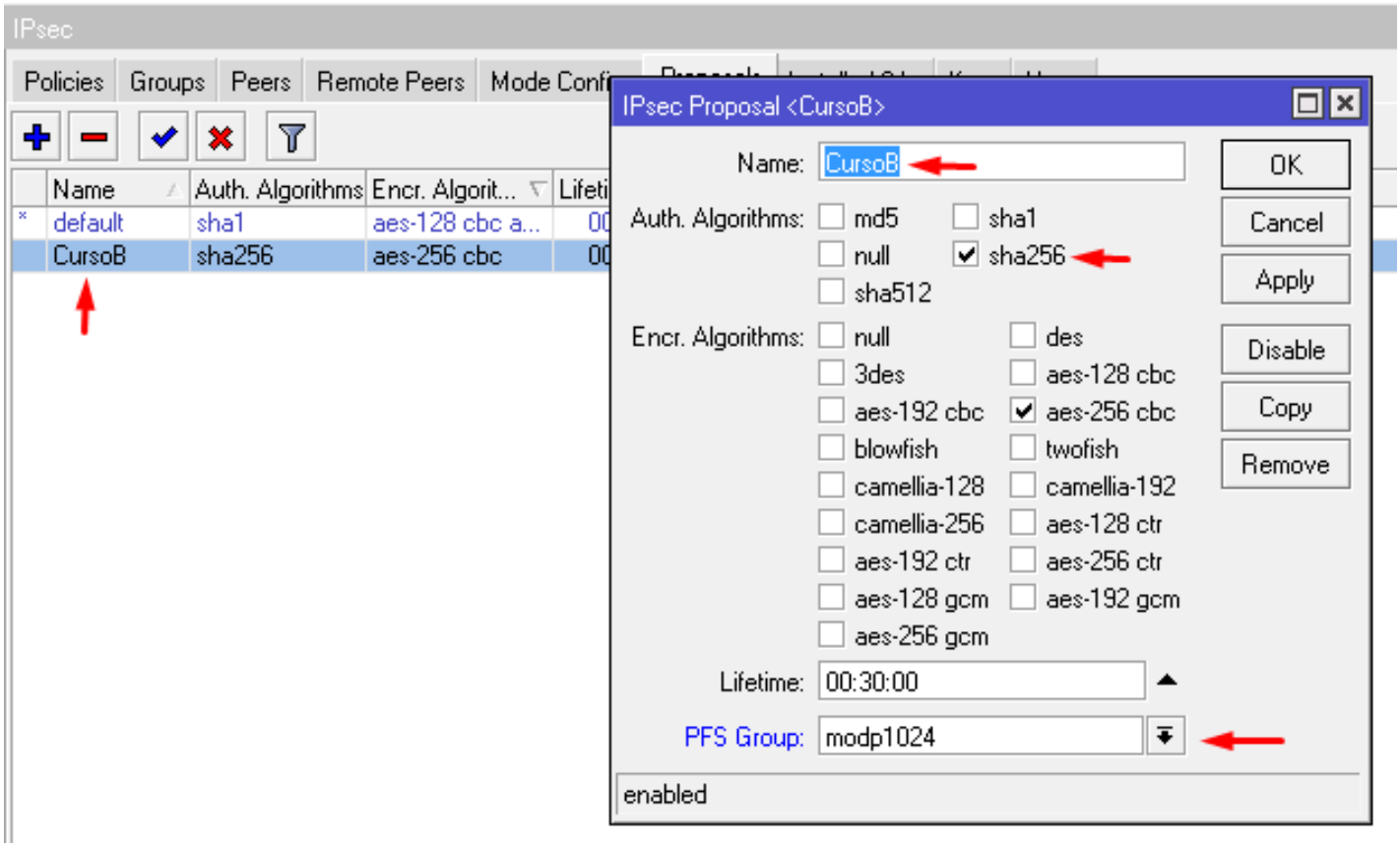
Paso 4: Llegamos a la configuración de la fase 2 de nuestro RouterB, para ello nos dijimos a la pestaña Proposals una vez allí crearemos un nuevo Proposal el cual se llamara CursosB, en el mismo configuraremos los siguientes parámetros:

Hash Algorithm: Sha256.

encryption Algorithm: aes-256 cbc.

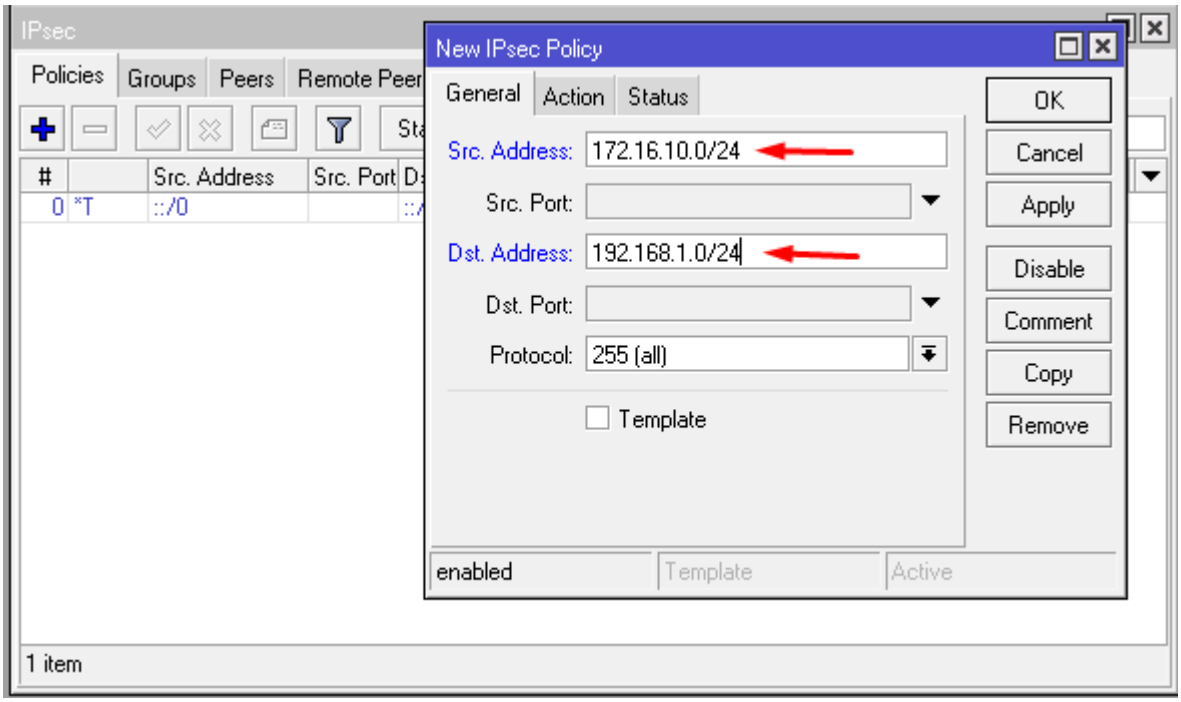
PFS Group: modb1024

Una vez configurados los pasos anteriores le damos Apply y luego OK**.**



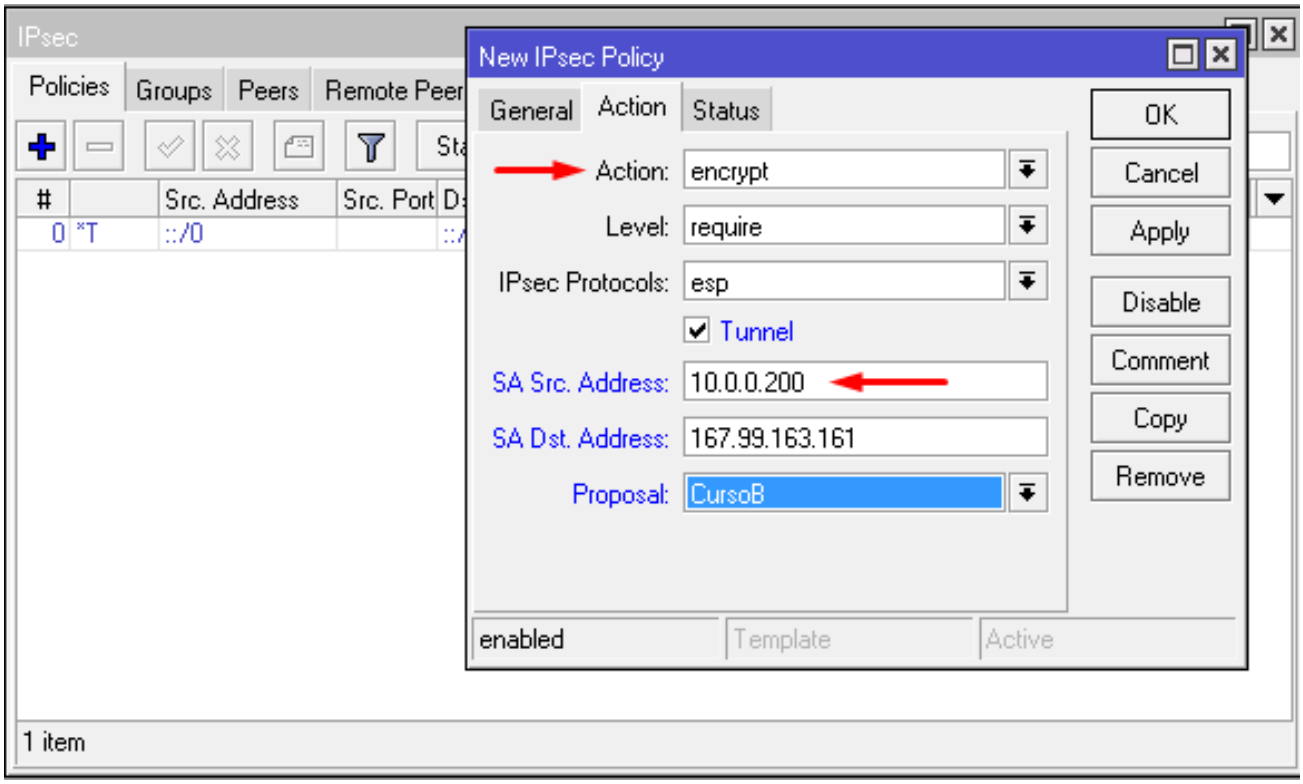
2.3.13

Paso 5: nos dirigimos a la pestaña Policy allí crearemos una nueva política para nuestro IPsec, primero vamos a General una vez allí configuraremos los siguientes parámetros Src. Address: pondremos el rango de IP de nuestra LAN, en Dst. Address: La red LAN de nuestro destino, significa la red interna que maneja el otro router. Ver imagen 2.3.14.



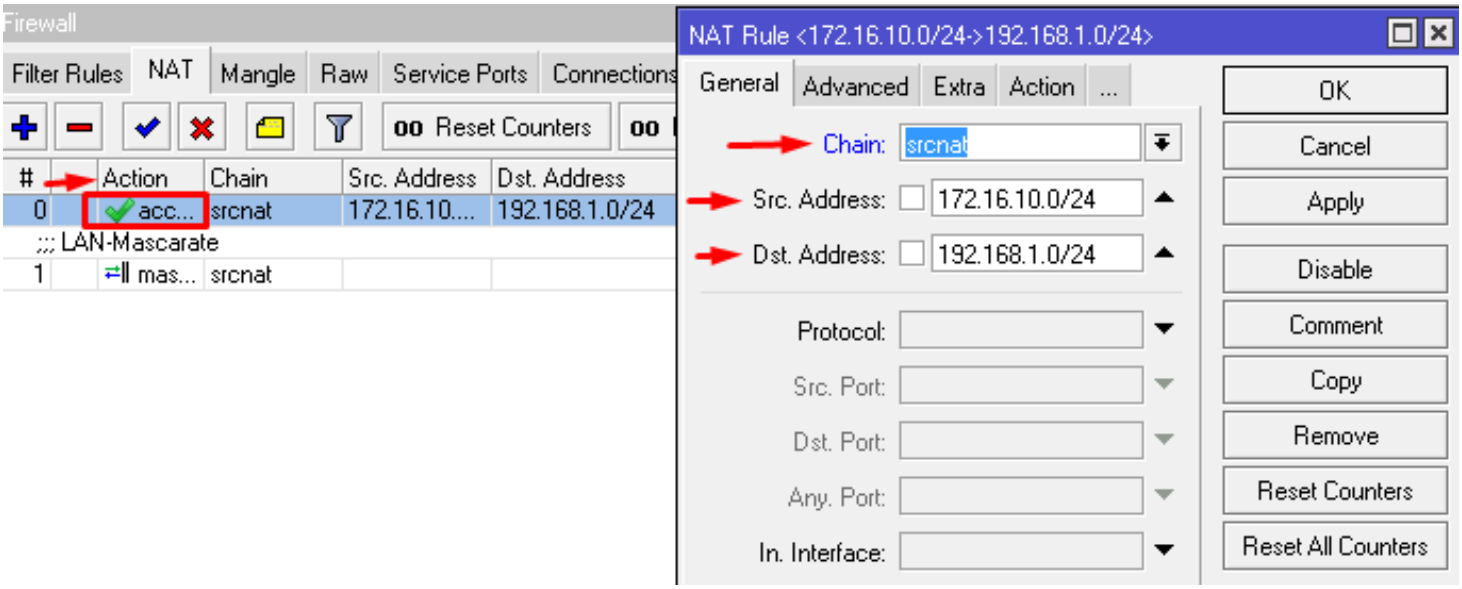
2.3.14

Paso 6: Luego nos dirigimos a la parte de Action una vez allí configuraremos los siguientes parámetros Action: encrypt, Level:require, IPsec Protocols:esp, Habilitar la casilla de Tunnel, SA Src. Address: Aquí va la dirección IP de su interfaces WAN en este caso la mía es:10.0.0.200 como el Router B no maneja una ip public si no que esta nateado por un dispositivo llamado Moden huawei que me asigna la dirrecion ip, luego va la SA Dst Address: en este campo pondremos la IP publica del otro routerA la cual será:167.99.163.161 por ultimo seleccionamos el proposal creado anterior mente **CursoB.** Ver imagen 2.3.15**.**



2.3.15

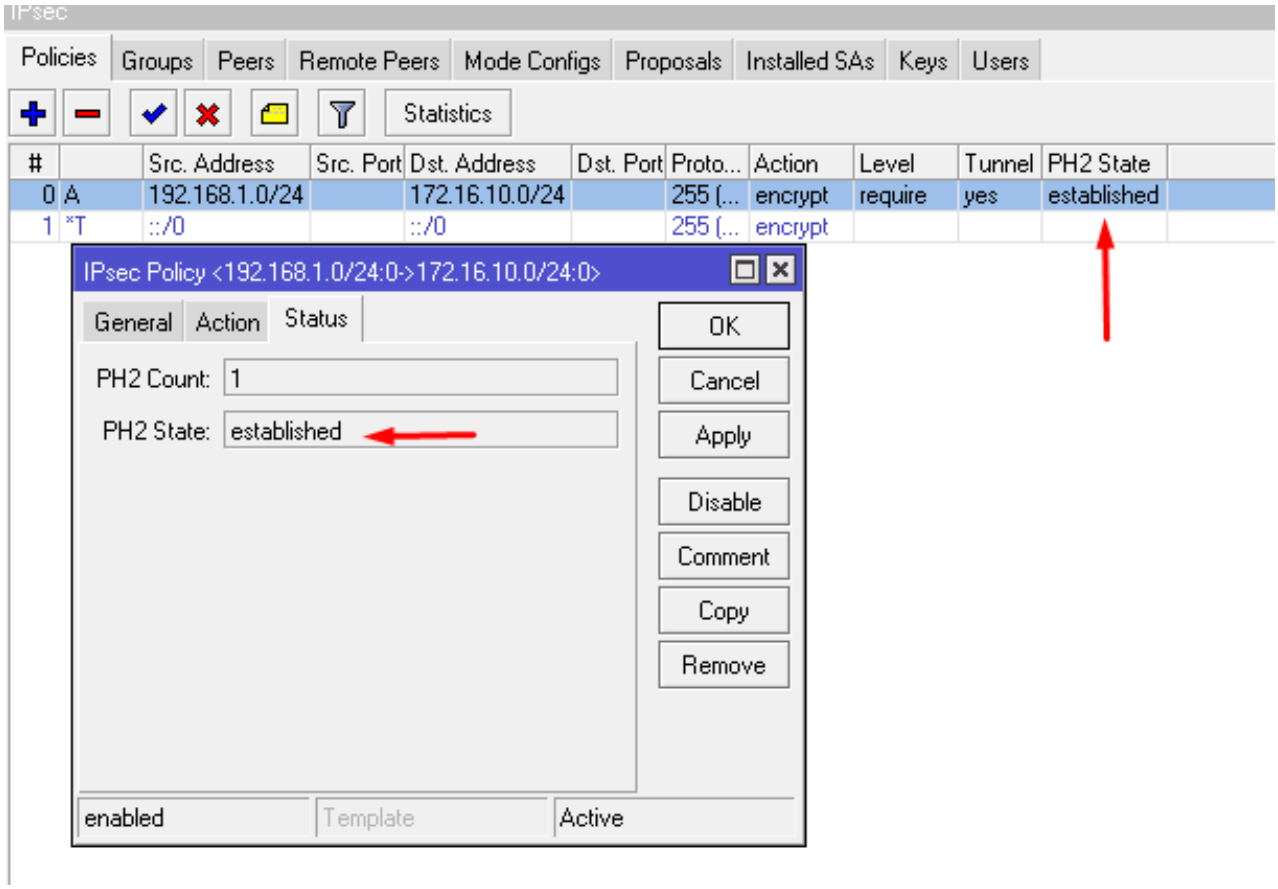
Paso 7: Agregamos un bypas aceptando el trafico de las dos redes LAN que se verán transparentes Src. Address: LAN de RouterB, Dst.Address: LAN de RouterA. Ver imagen 2.3.16



.2.3.16

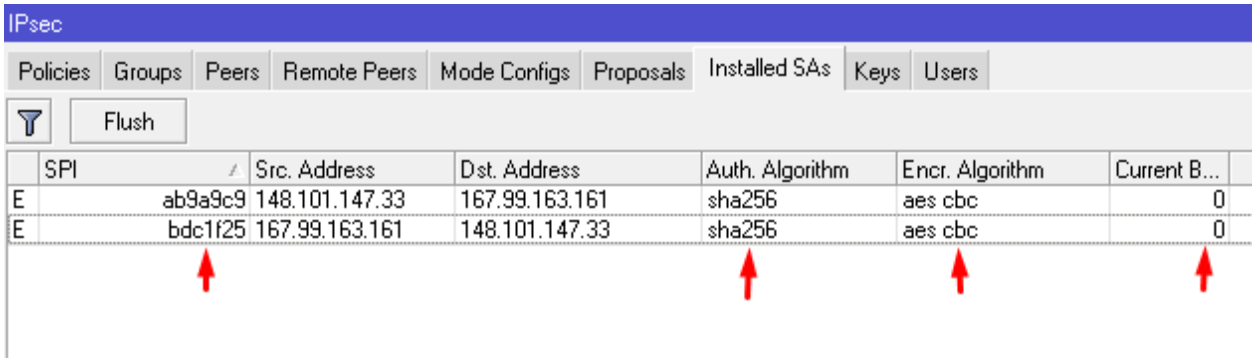
Paso 8: Una vez completado todo los pasos anteriores, Verificaremos el status de nuestro Túnel para ello vamos para Policies y veremos como en la pestaña PH2 State nos mostrara established. Ver imagen 2.3.17

Router A



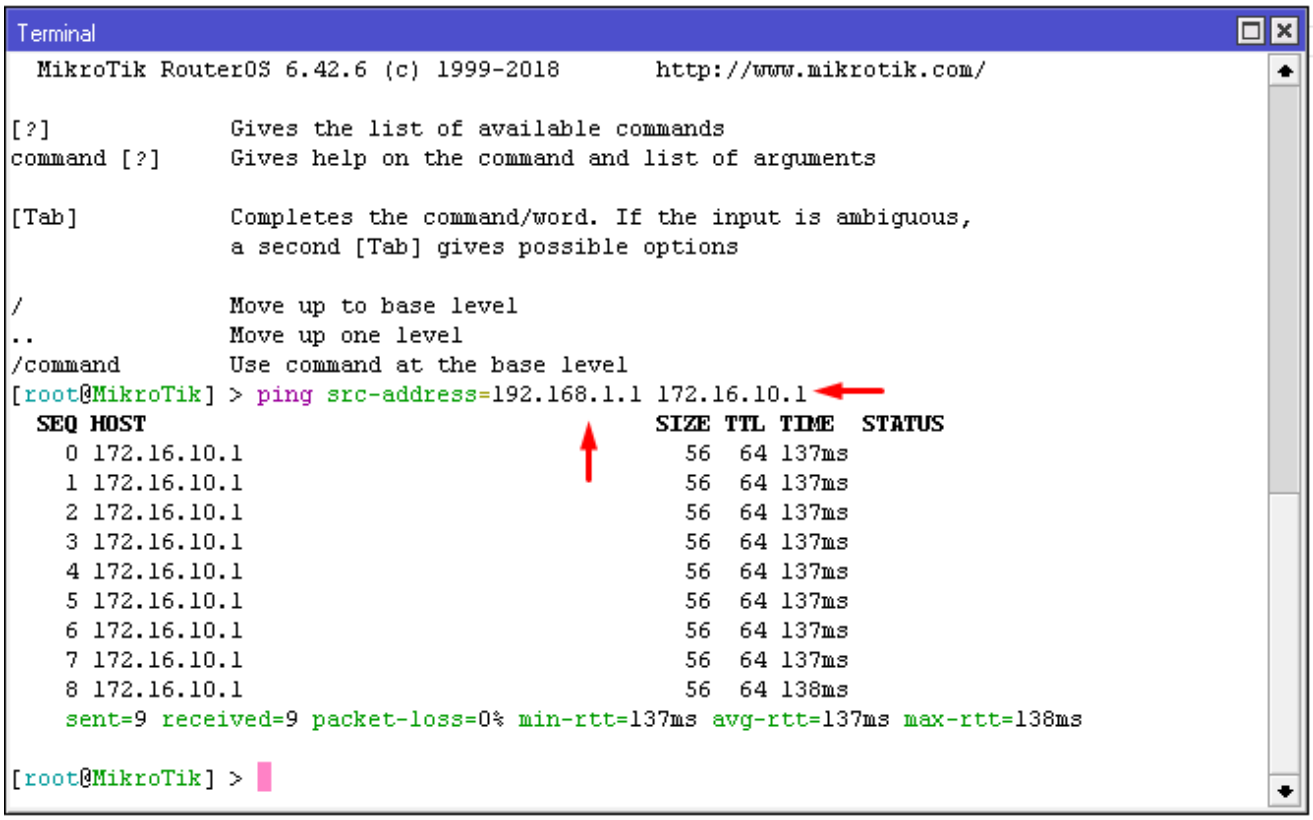
2.3.17

Paso 9: Ahora nos dirigiremos a la pestaña Installed SAs, allí veremos la encriptación de 32bit SPI, Src. Address , Dst Address, vesmo también la encriptación de autenticación sha256 y aes cbc para la encriptación , si vemos estas información en esta pestaña es porque nuestra conexión entre los dos routers está establecida **.**



2.3.18

Ahora Hacemos un ping Desde Router A al rango LAN de router B. Porque src-address?



Router B.

En Router B nos aparcera una configuración similar a la de Router A, por eso omitiré volver a repetir todo pero podemos ver en la siguiente imagen como el túnel está establecido, y luego como le damos ping a la red LAN de Router A