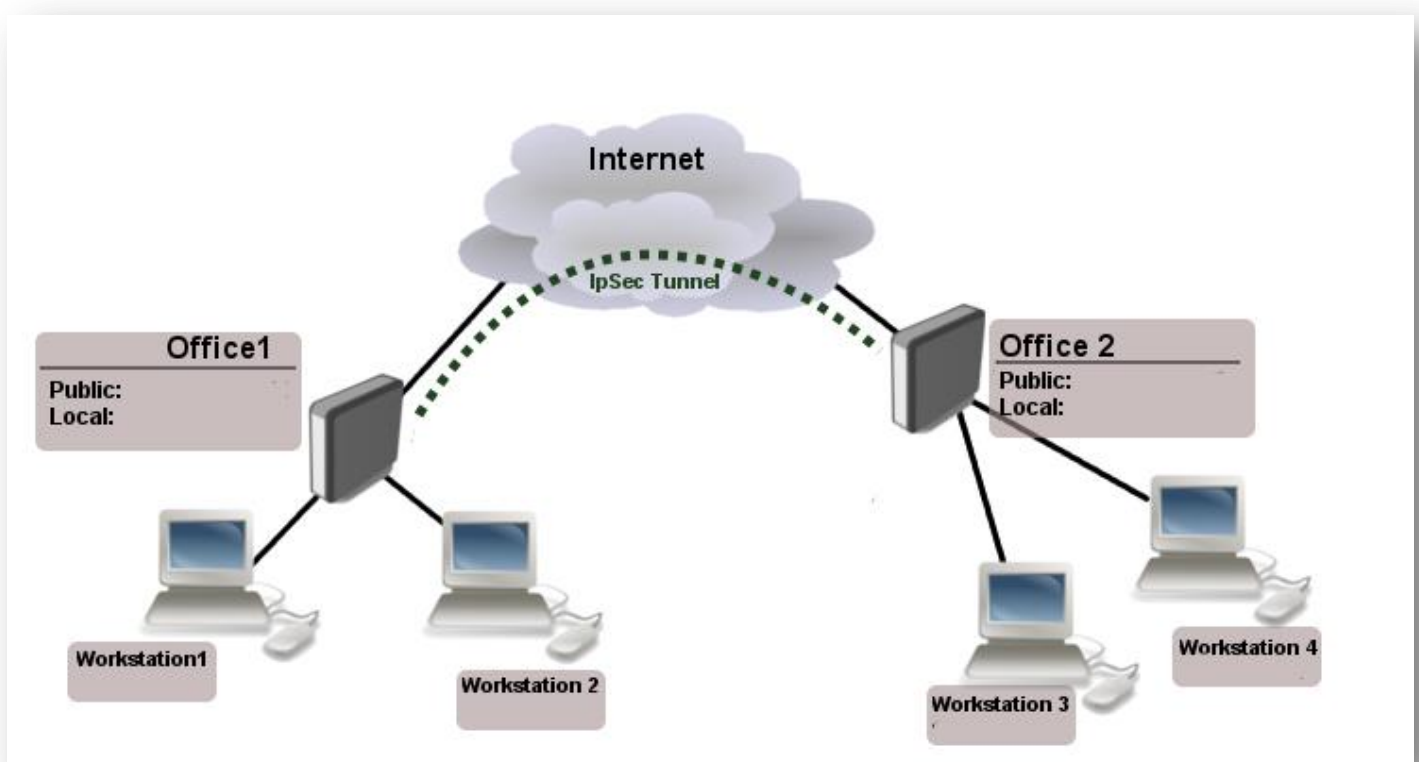


Laboratorio 2.3: Configuración IPsec site to site MikroTik- MikroTik.

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

Site to Site IPsec tunnel MikoTik-Mikoritk

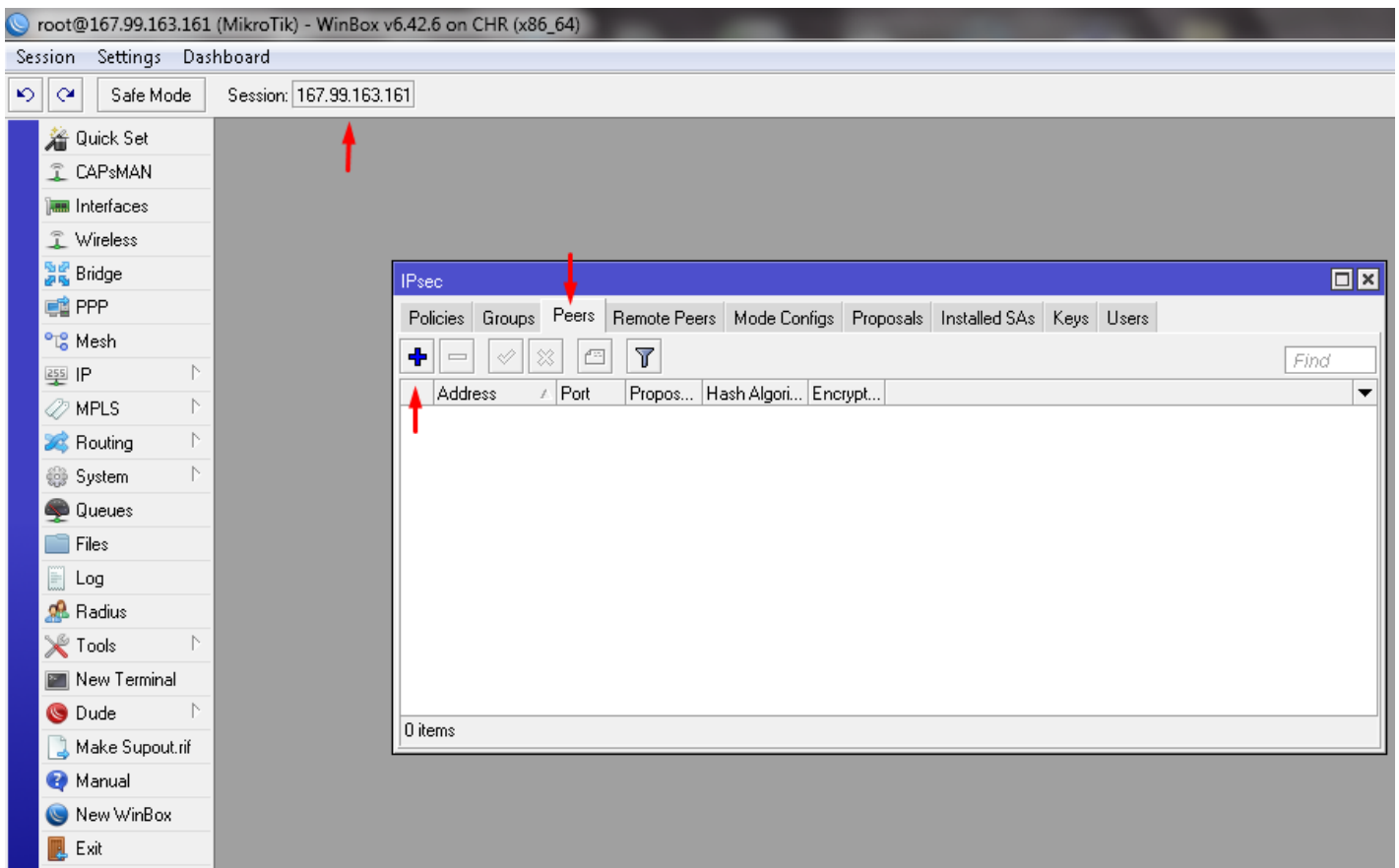
Router A-----IPsec-----RouterB



Router-A:

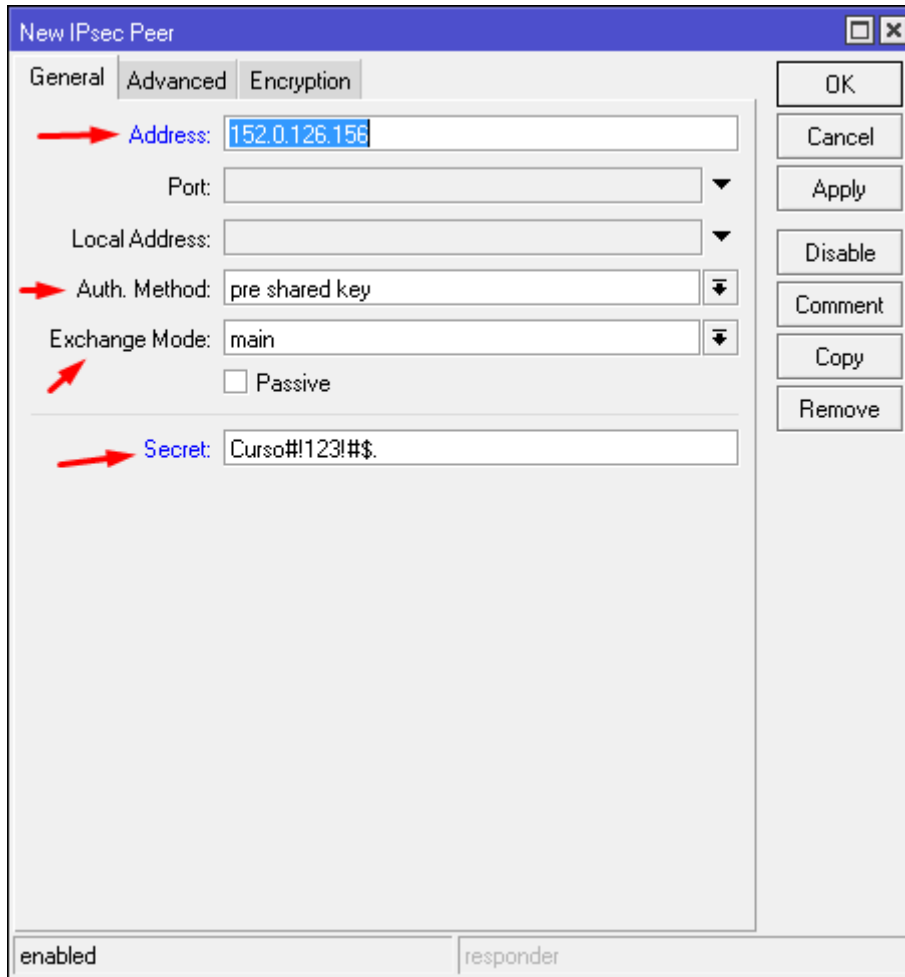
Fase 1:

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.



New IPsec Peer

General Advanced Encryption

Address: 152.0.126.156

Port: ▼

Local Address: ▼

Auth. Method: pre shared key ▼

Exchange Mode: main ▼

Passive

Secret: Curso#!123!#\$

OK

Cancel

Apply

Disable

Comment

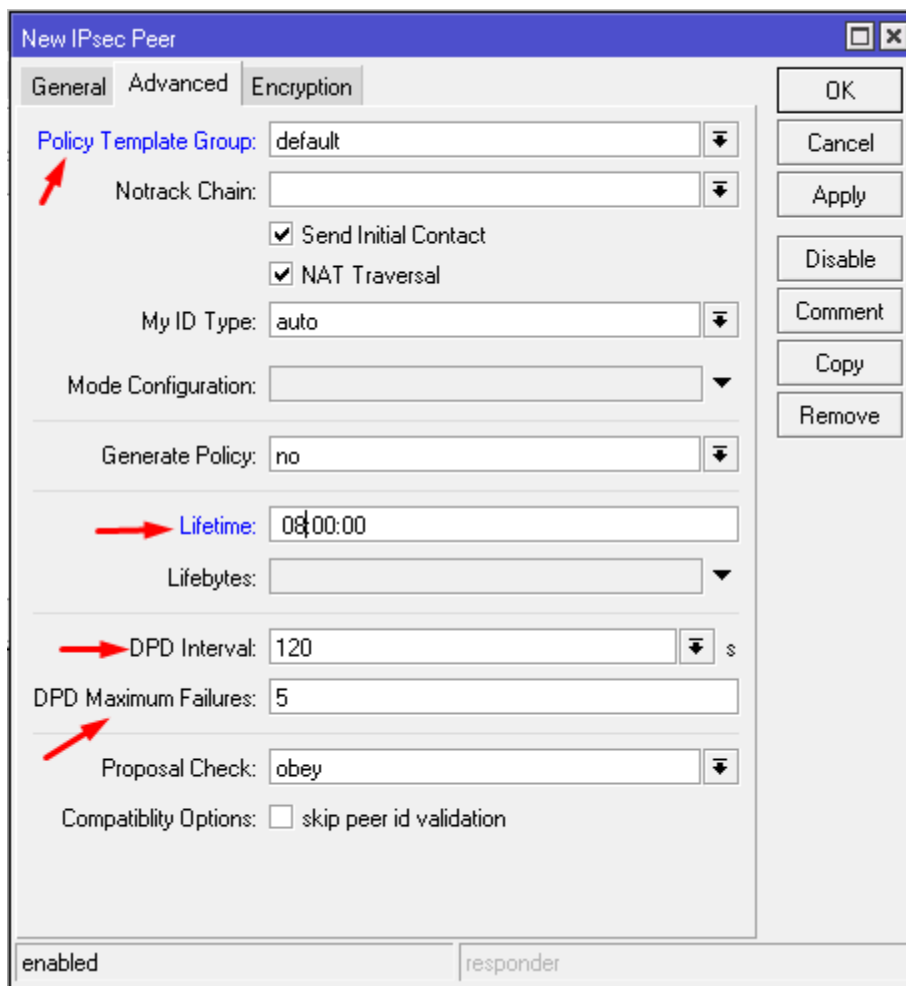
Copy

Remove

enabled responder

2.3.2

Paso 3: Ahora vamos a la pestaña advanced a configurar los siguientes parámetros, Send Inicial 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.



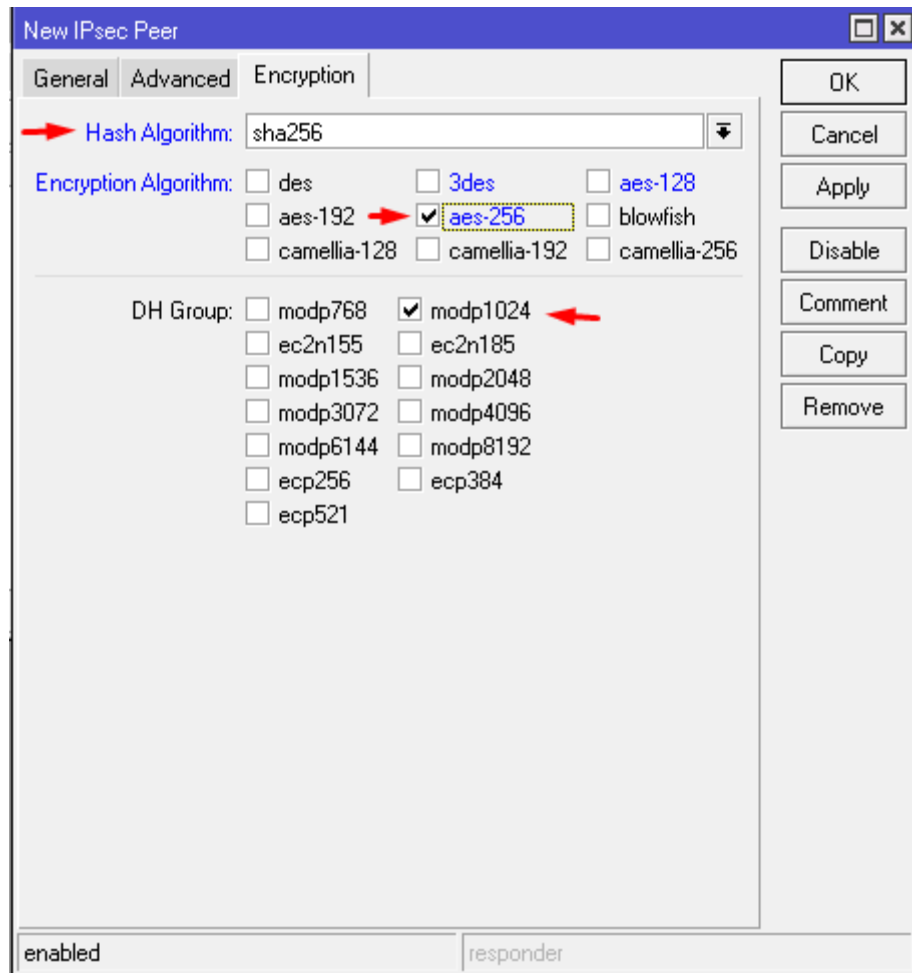
2.3.2

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:

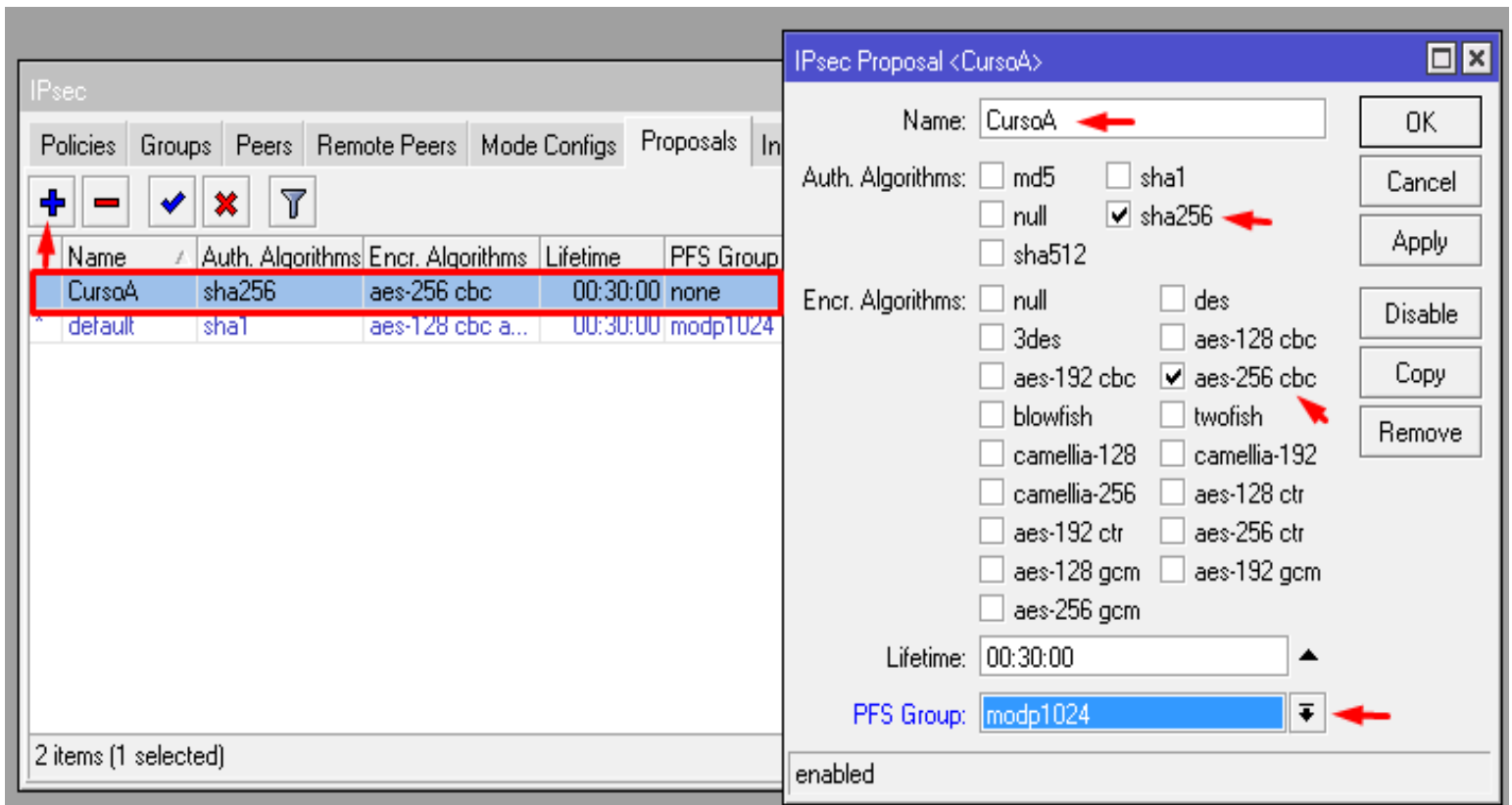
Paso 5: Ya llegamos a la configuración de la fase 2 de nuestro ipsec, para ello nos dirigimos a la pestaña Proposals una vez allí crearemos un nuevo Proposal el cual se llamará CursoA, en el mismo configuraremos los siguientes parámetros:

Hash Algorithm: Sha256.

encryption Algorithm: aes-256 cbc.

PFS Group: modp1024

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



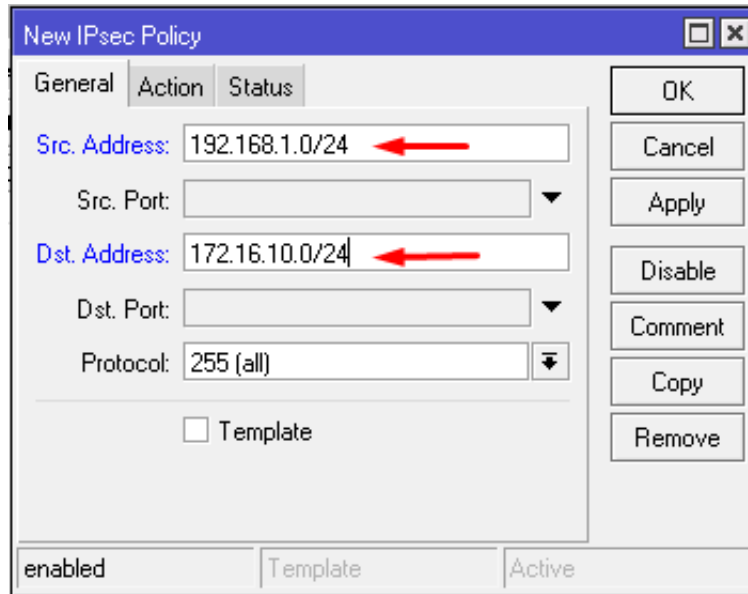
The screenshot displays the Mikrotik WinBox IPsec configuration interface. On the left, the 'Proposals' tab is active, showing a table with the following data:

Name	Auth. Algorithms	Encr. Algorithms	Lifetime	PFS Group
CursoA	sha256	aes-256 cbc	00:30:00	none
default	sha1	aes-128 cbc a...	00:30:00	modp1024

The 'CursoA' row is highlighted in red. On the right, the 'IPsec Proposal <CursoA>' configuration window is open. The 'Name' field is set to 'CursoA'. Under 'Auth. Algorithms', the 'sha256' checkbox is checked. Under 'Encr. Algorithms', the 'aes-256 cbc' checkbox is checked. The 'Lifetime' is set to '00:30:00'. Under 'PFS Group', the 'modp1024' dropdown is selected. Red arrows point to these specific settings.

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.



New IPsec Policy

General Action Status

Src. Address: 192.168.1.0/24

Src. Port: [dropdown]

Dst. Address: 172.16.10.0/24

Dst. Port: [dropdown]

Protocol: 255 (all)

Template

OK

Cancel

Apply

Disable

Comment

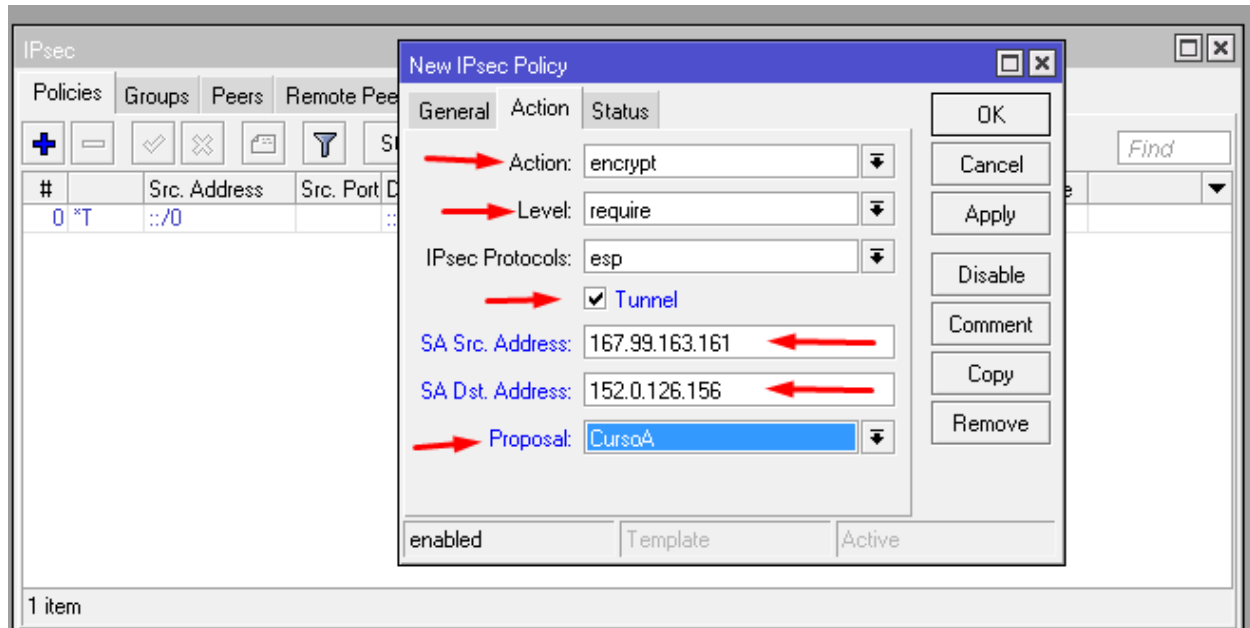
Copy

Remove

enabled Template Active

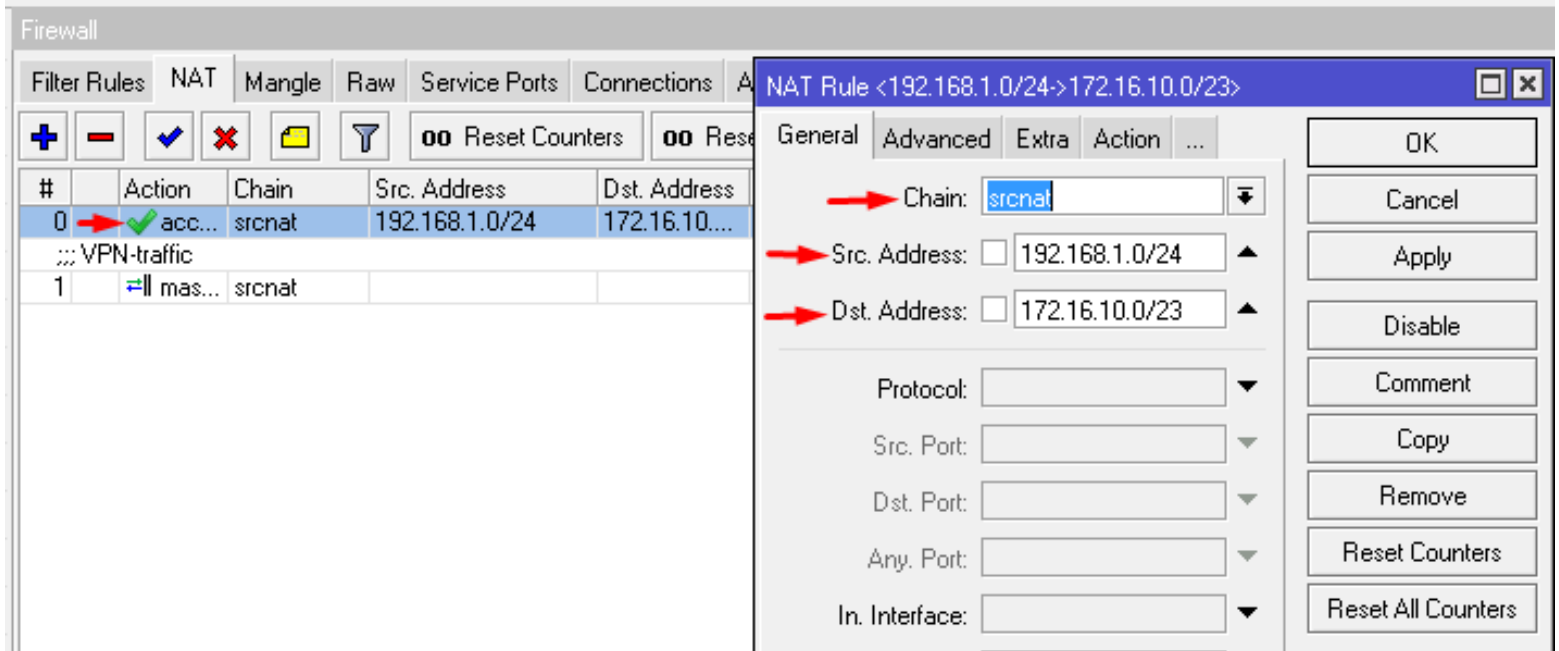
2.3.6

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



The screenshot shows the Mikrotik WinBox Firewall configuration interface. The main window displays a table of NAT rules. Rule 0 is selected, showing Action: acc..., Chain: srcnat, Src. Address: 192.168.1.0/24, and Dst. Address: 172.16.10.0/23. A dialog box titled 'NAT Rule <192.168.1.0/24>172.16.10.0/23>' is open, showing the configuration for rule 0. The Chain is set to 'srcnat', Src. Address is '192.168.1.0/24', and Dst. Address is '172.16.10.0/23'.

#	Action	Chain	Src. Address	Dst. Address
0	acc...	srcnat	192.168.1.0/24	172.16.10.0/23
1	mas...	srcnat		

The dialog box 'NAT Rule <192.168.1.0/24>172.16.10.0/23>' shows the following configuration:

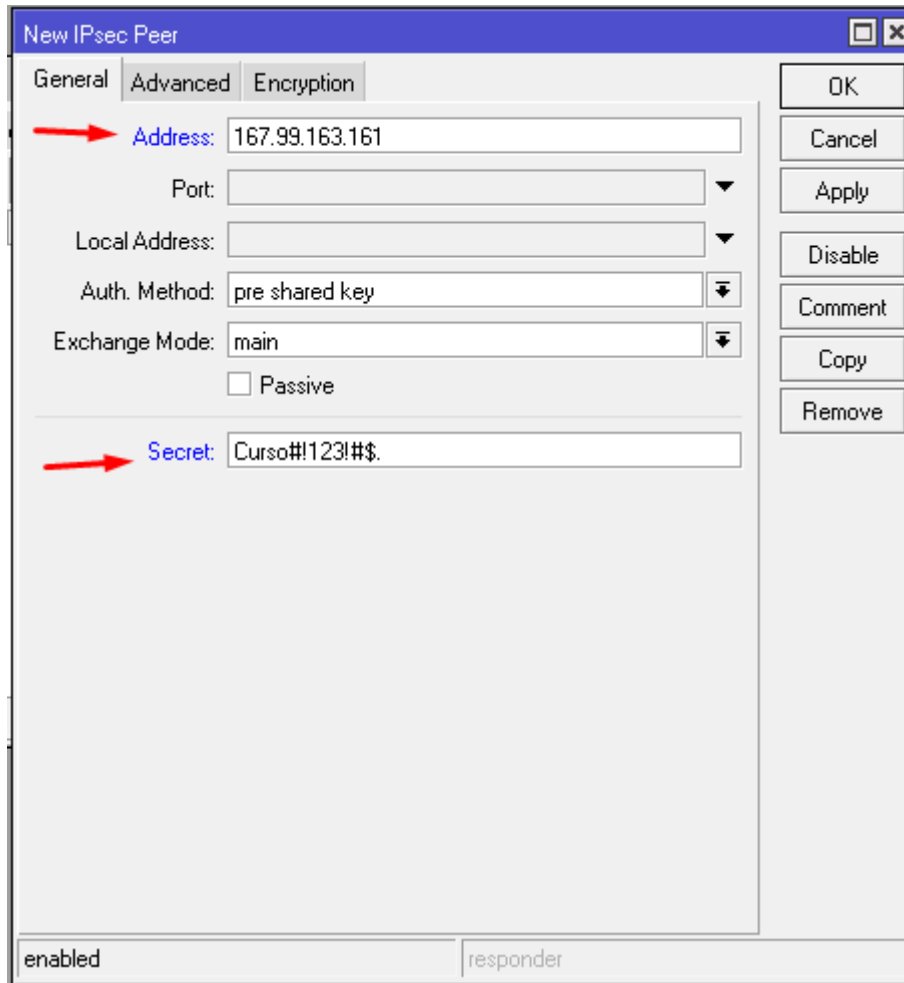
- Chain: srcnat
- Src. Address: 192.168.1.0/24
- Dst. Address: 172.16.10.0/23
- Protocol: (empty)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)

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.



New IPsec Peer

General Advanced Encryption

Address: 167.99.163.161

Port: [dropdown]

Local Address: [dropdown]

Auth. Method: pre shared key [dropdown]

Exchange Mode: main [dropdown]

Passive

Secret: Curso#!123!#\$

OK

Cancel

Apply

Disable

Comment

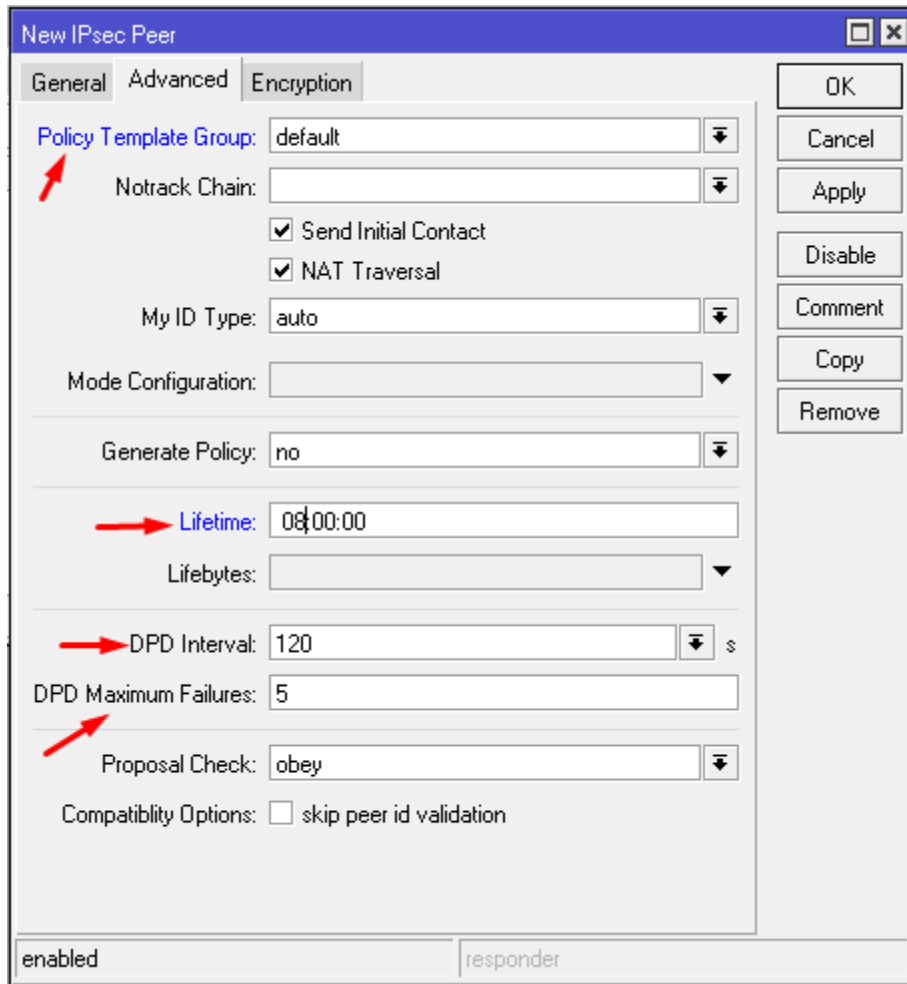
Copy

Remove

enabled responder

2.3.10

Paso 2: Ahora vamos a la pestaña advanced a configurar los siguientes parámetros, Send Inicial 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.



Policy Template Group: default

Notrack Chain:

Send Initial Contact

NAT Traversal

My ID Type: auto

Mode Configuration:

Generate Policy: no

Lifetime: 08:00:00

Lifebytes:

DPD Interval: 120 s

DPD Maximum Failures: 5

Proposal Check: obey

Compatibility Options: skip peer id validation

enabled responder

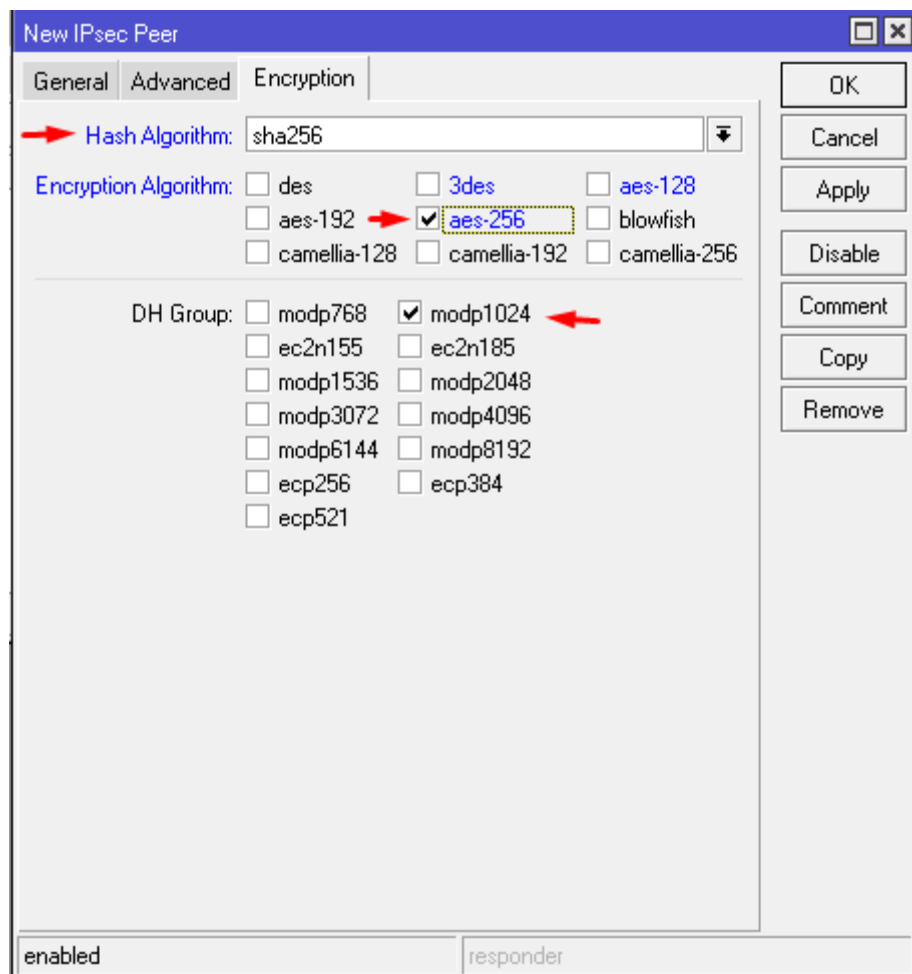
2.3.11

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

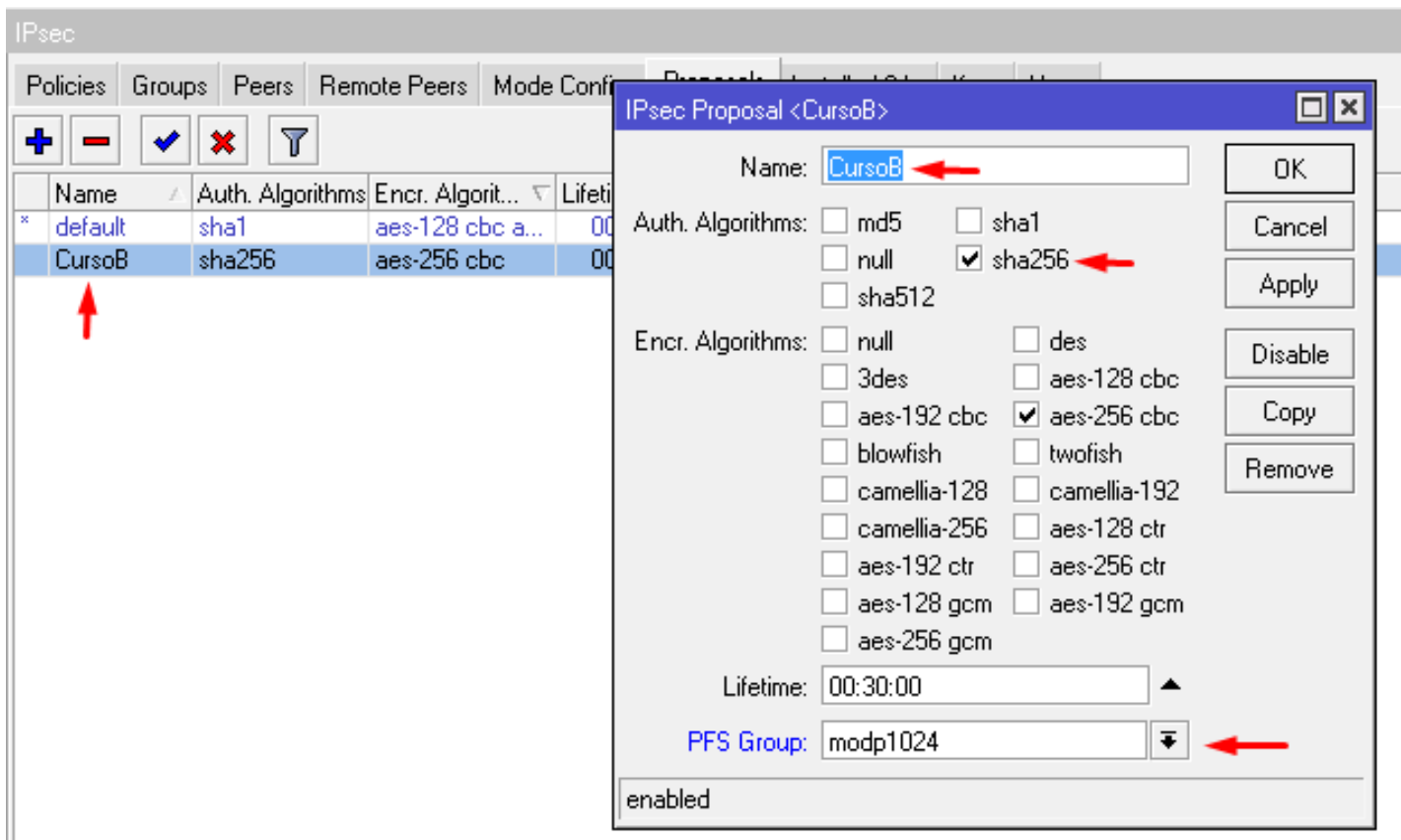
Paso 4: Llegamos a la configuración de la fase 2 de nuestro RouterB, para ello nos dirigimos a la pestaña Proposals una vez allí crearemos un nuevo Proposal el cual se llamará CursosB, en el mismo configuraremos los siguientes parámetros:

Hash Algorithm: Sha256.

encryption Algorithm: aes-256 cbc.

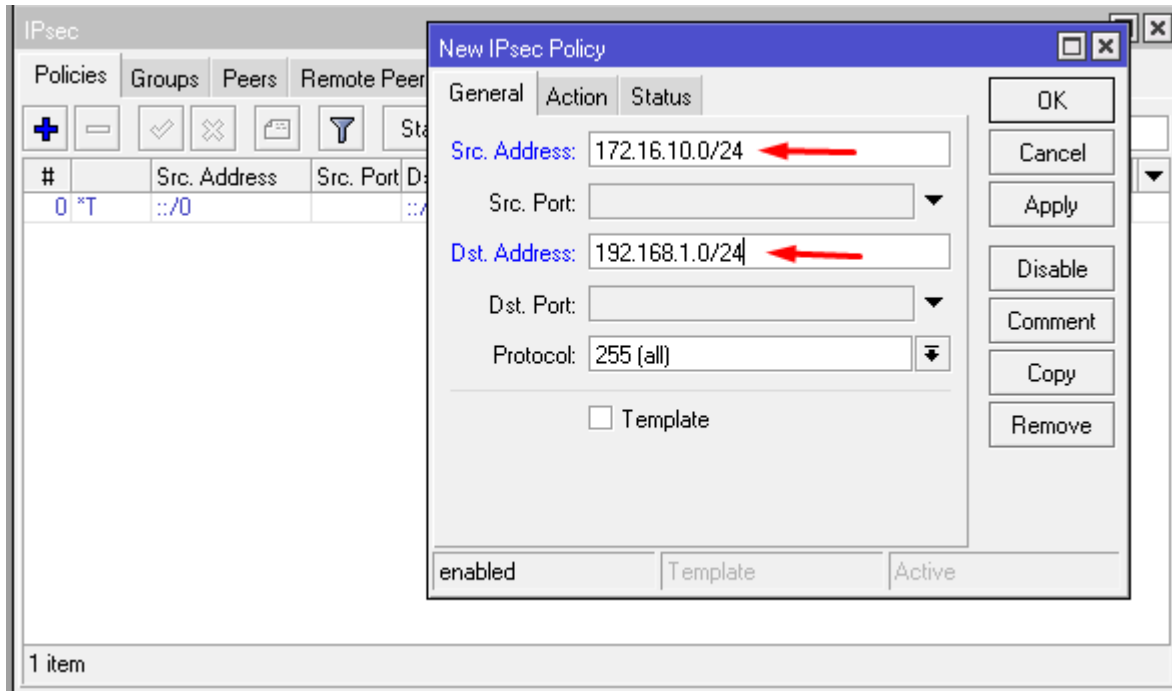
PFS Group: modp1024

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



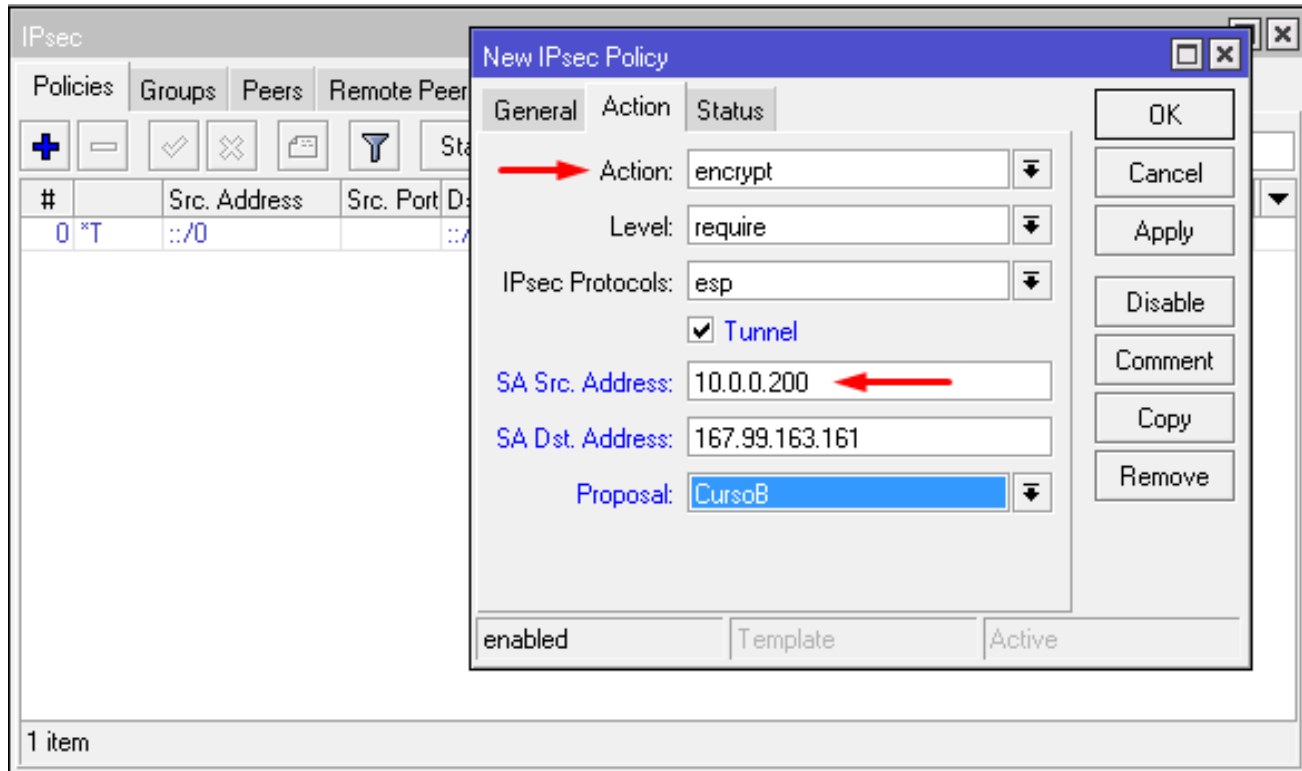
2.3.13

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.



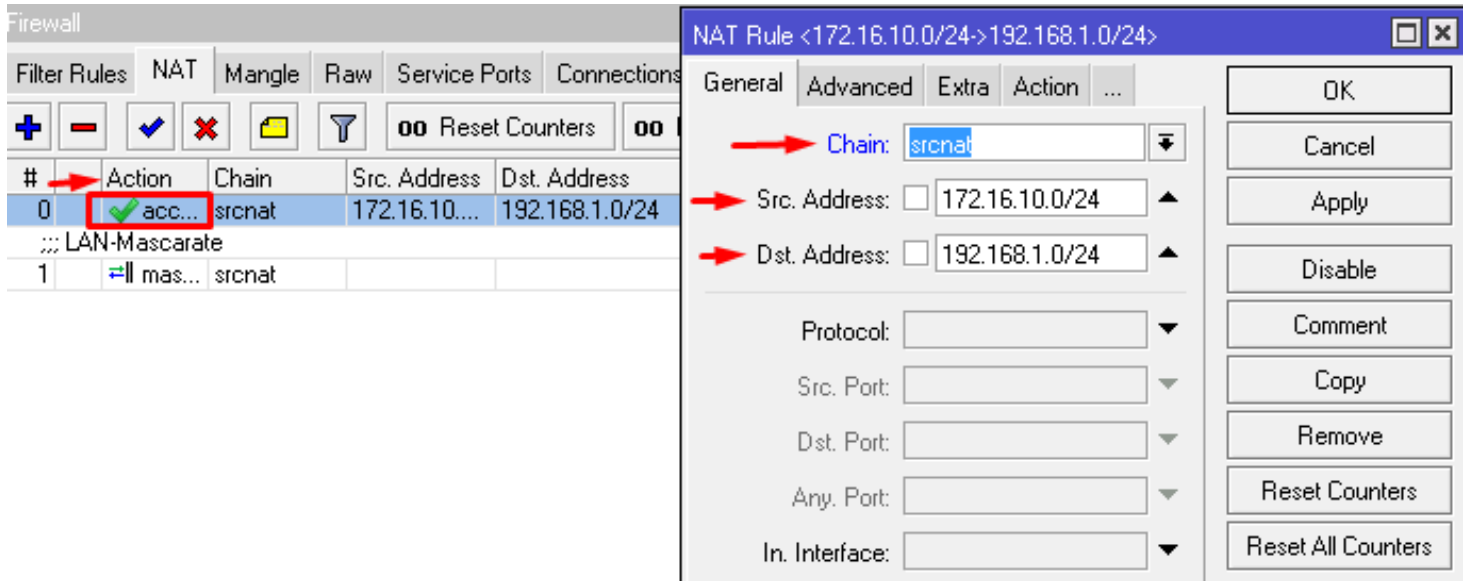
2.3.14

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 Modem huawei que me asigna la dirreccion 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 bypass aceptando el tráfico de las dos redes LAN que se verán transparentes Src. Address: LAN de RouterB, Dst.Address: LAN de RouterA. Ver imagen 2.3.16



The screenshot shows the Mikrotik WinBox Firewall configuration interface. On the left, the Firewall rule list is visible, with rule 0 selected. The rule details are as follows:

#	Action	Chain	Src. Address	Dst. Address
0	acc...	srcnat	172.16.10.0/24	192.168.1.0/24
::: LAN-Mascarate				
1	mas...	srcnat		

On the right, the NAT Rule configuration dialog is open for rule 0. The configuration is as follows:

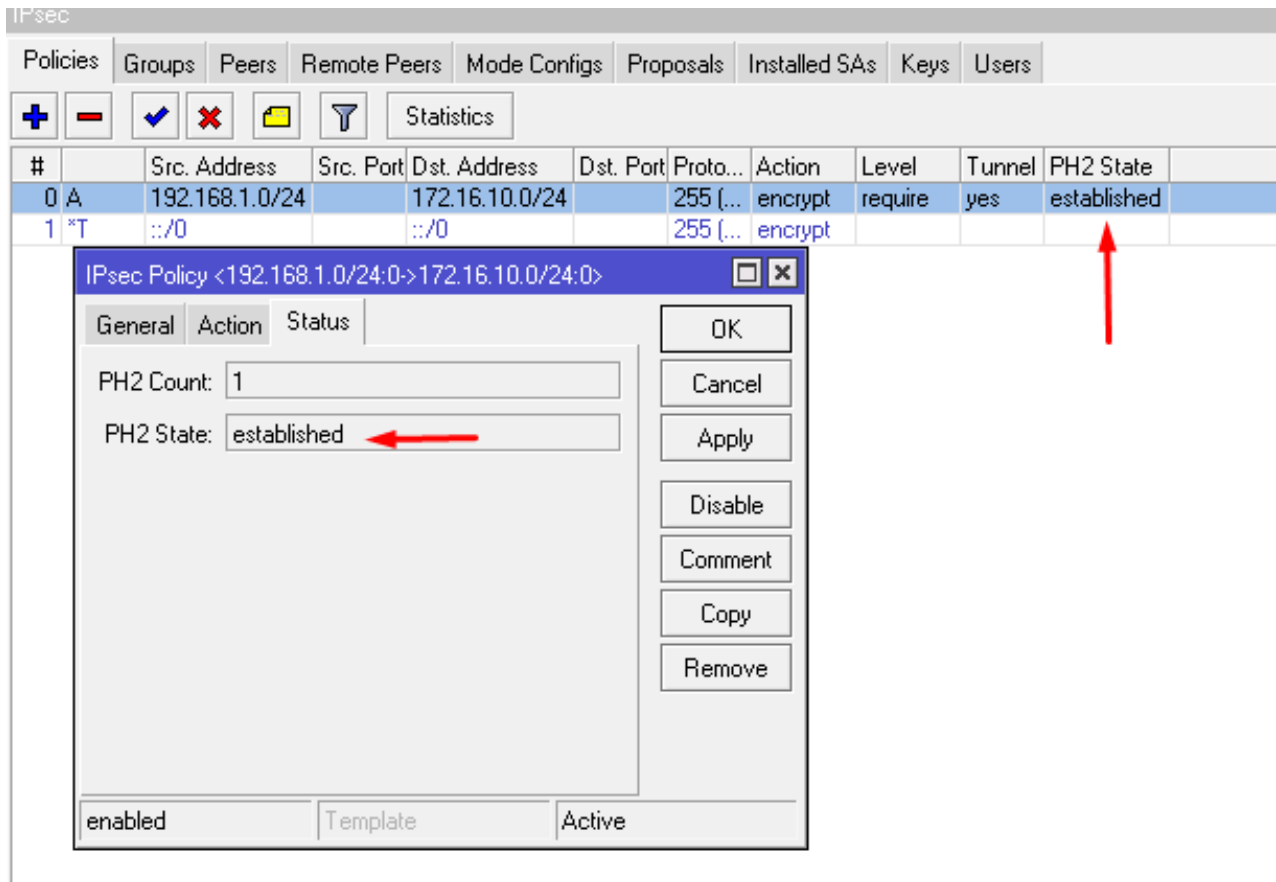
- Chain: srcnat
- Src. Address: 172.16.10.0/24
- Dst. Address: 192.168.1.0/24
- Protocol: (empty)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)

Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

.2.3.16

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

Router A



The screenshot displays the Mikrotik WinBox interface for IPsec Policies. The main table lists the following policies:

#		Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel	PH2 State
0	A	192.168.1.0/24		172.16.10.0/24		255 (...)	encrypt	require	yes	established
1	*T	::/0		::/0		255 (...)	encrypt			

A dialog box titled "IPsec Policy <192.168.1.0/24:0->172.16.10.0/24:0>" is open, showing the configuration for Policy A. The "PH2 State" field is set to "established".

2.3.17

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

IPsec							
Policys Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users							
Flush							
	SPI	Src. Address	Dst. Address	Auth. Algorithm	Encr. Algorithm	Current B...	
E	ab9a9c9	148.101.147.33	167.99.163.161	sha256	aes cbc	0	
E	bdc1f25	167.99.163.161	148.101.147.33	sha256	aes cbc	0	

2.3.18

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

```

Terminal
MikroTik RouterOS 6.42.6 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

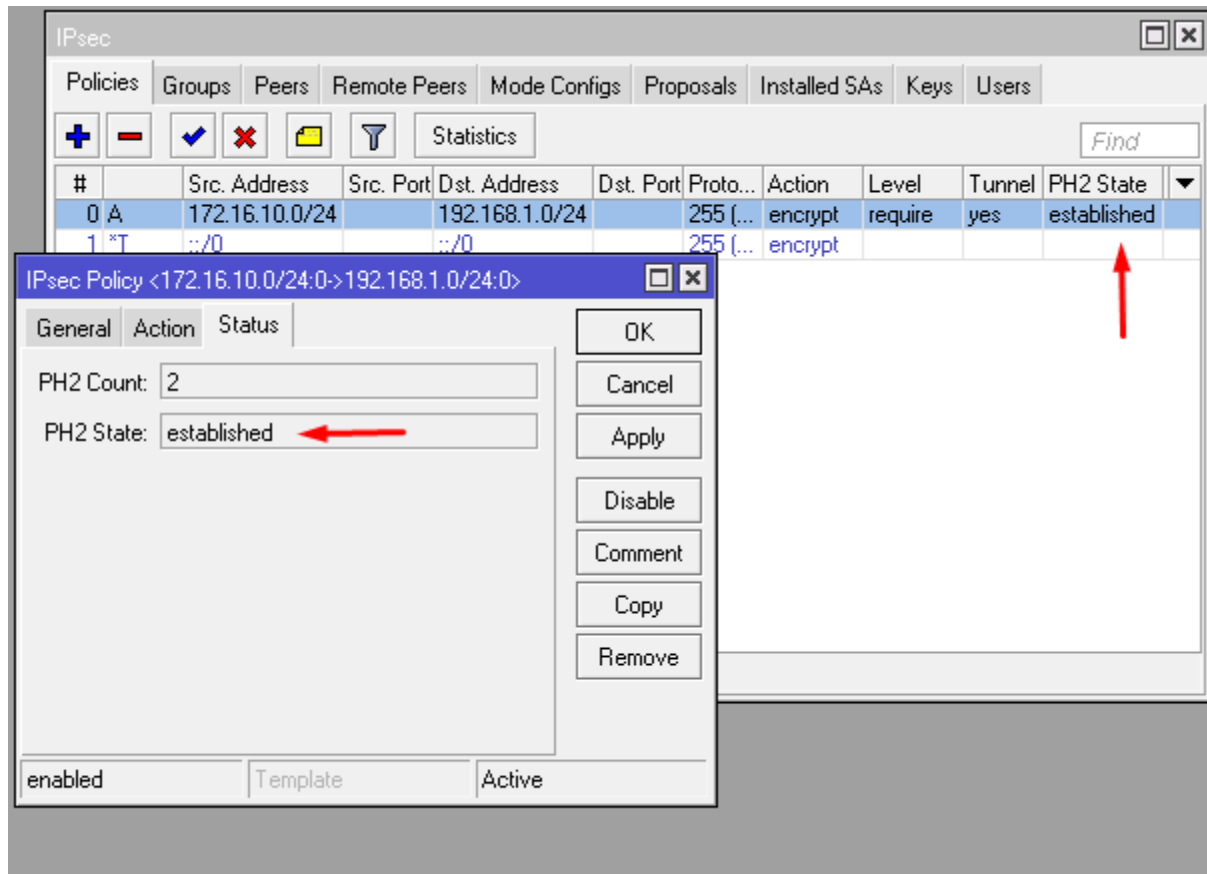
[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..          Move up one level
/command    Use command at the base level
[root@MikroTik] > ping src-address=192.168.1.1 172.16.10.1
  SEQ HOST                SIZE TTL TIME  STATUS
  0 172.16.10.1            56  64 137ms
  1 172.16.10.1            56  64 137ms
  2 172.16.10.1            56  64 137ms
  3 172.16.10.1            56  64 137ms
  4 172.16.10.1            56  64 137ms
  5 172.16.10.1            56  64 137ms
  6 172.16.10.1            56  64 137ms
  7 172.16.10.1            56  64 137ms
  8 172.16.10.1            56  64 138ms
sent=9 received=9 packet-loss=0% min-rtt=137ms avg-rtt=137ms max-rtt=138ms

[root@MikroTik] >
  
```

Router B.

En Router B nos aparecerá 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



```
Terminal
command [?]    Gives help on the command and list of arguments

[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@MikroTik] > ping src-address=172.16.10.1 192.168.1.1
SEQ HOST                                SIZE TTL TIME STATUS
  0 192.168.1.1                            56 64 137ms
  1 192.168.1.1                            56 64 137ms
  2 192.168.1.1                            56 64 137ms
  3 192.168.1.1                            56 64 137ms
  4 192.168.1.1                            56 64 137ms
  5 192.168.1.1                            56 64 137ms
  6 192.168.1.1                            56 64 137ms
  7 192.168.1.1                            56 64 137ms
  8 192.168.1.1                            56 64 137ms
  9 192.168.1.1                            56 64 137ms
  sent=10 received=10 packet-loss=0% min-rtt=137ms avg-rtt=137ms
  max-rtt=137ms

[admin@MikroTik] >
```