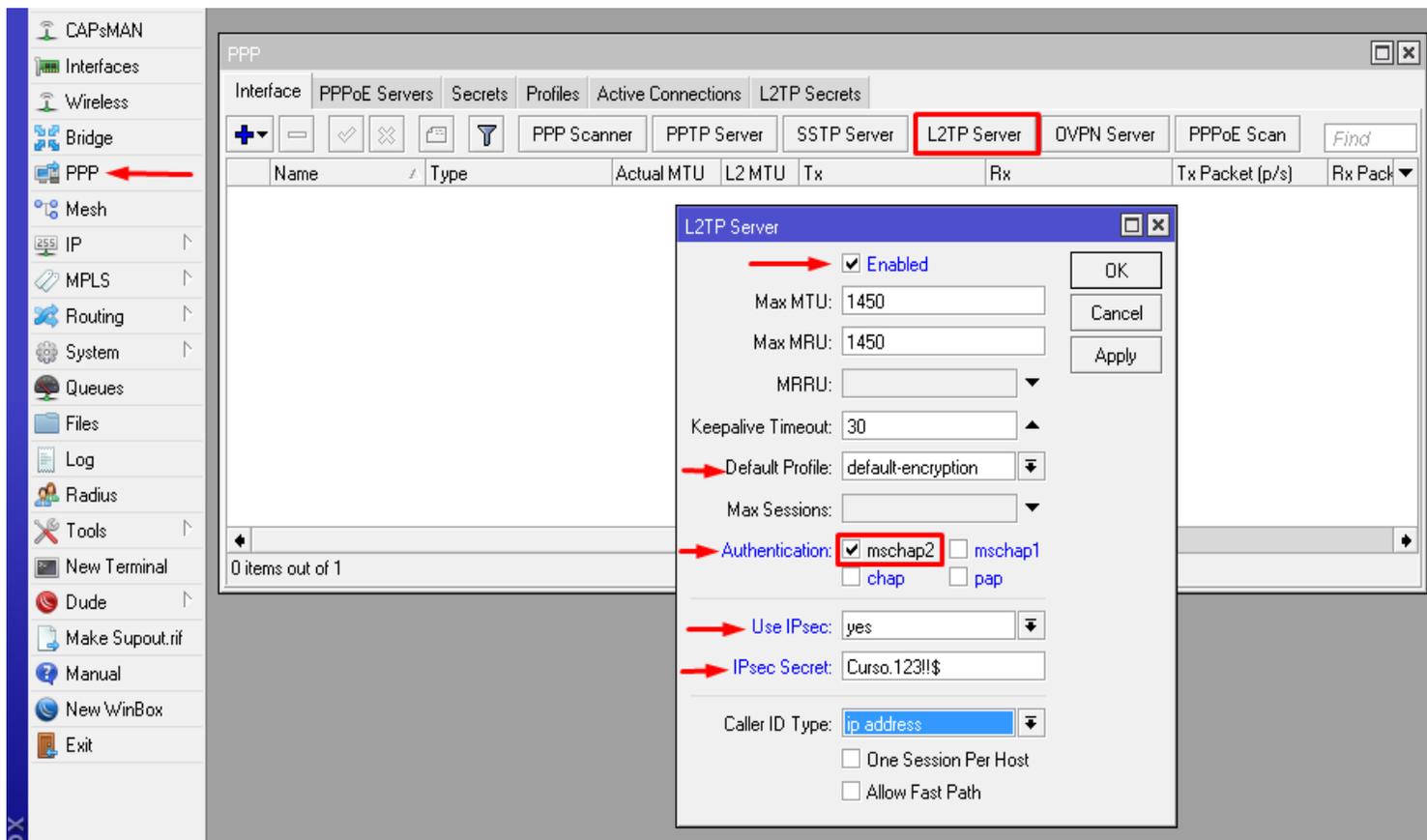


Laboratorio 2.1: Laboratorio L2TP/IPsec Server Mikrotik

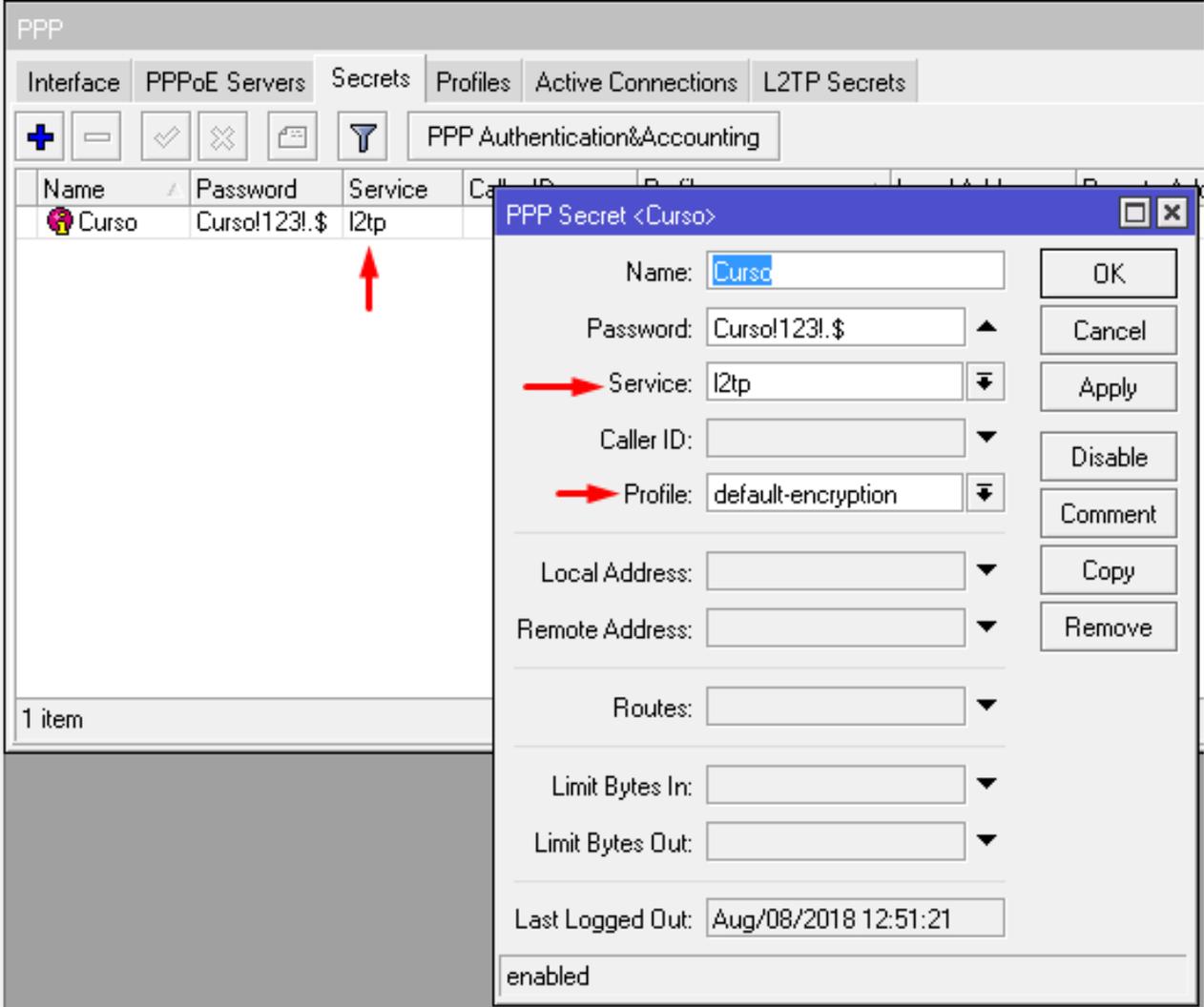
Objetivo: Configurar un Túnel L2TP/IPsec server en su Router MikroTik.

Paso 1: En esta ocasión vamos a configurar un L2TP/IPsec server en nuestro MikroTik, para ello volvemos a la parte PPP, una vez allí nos dirigimos a la pestaña Interface y luego le damos al botón L2TP Server, se nos abrirá una nueva ventana donde vamos a configurar los siguientes campos: enabled: se activa esta casilla para habilitar el túnel, Default Profile: aquí procedemos a elegir nuestro profile si ya hemos creado uno si no dejarlo en default-encryption, Authentication: en esta opción solo seleccionamos Mschap2, Use IPsec: esta valr será igual a yes para habilitar IPsec en nuestro túnel, IPsec Secret: aquí escribimos nuestra contraseña que servirá como llave de encriptación y des encriptación para nuestros clientes Nota el password colocado en todos sus credenciales de seguridad deben ser Fuertes Por ejemplo: PliniO..!123!\$!!! etc, ver imagen 2.1



2.1

Paso 2: una vez hecho el paso anterior, nos dirigimos a la pestaña Secrets una vez allí brimos nuestro anterior usuario creado para la pasada practica de PPTP o pueden crearce una nuevo a eleccion de ustedes, una vez dentro de la pestaña de configuracion vamos a configurar los valores como los vemos en al imagen 2.2, alli tendremos muy en cuenta la opcion Service que debe ser L2TP y el profile ver que sea el que usted configuro previamente para las conexiones VPN.



PPP

Interface | PPPoE Servers | **Secrets** | Profiles | Active Connections | L2TP Secrets

PPP Authentication&Accounting

Name	Password	Service	Caller ID	Local Address	Remote Address	Routes	Limit Bytes In	Limit Bytes Out	Last Logged Out
Curso	Curso!123!.\$	I2tp							

1 item

PPP Secret <Curso>

Name: Curso

Password: Curso!123!.\$

Service: I2tp

Caller ID:

Profile: default-encryption

Local Address:

Remote Address:

Routes:

Limit Bytes In:

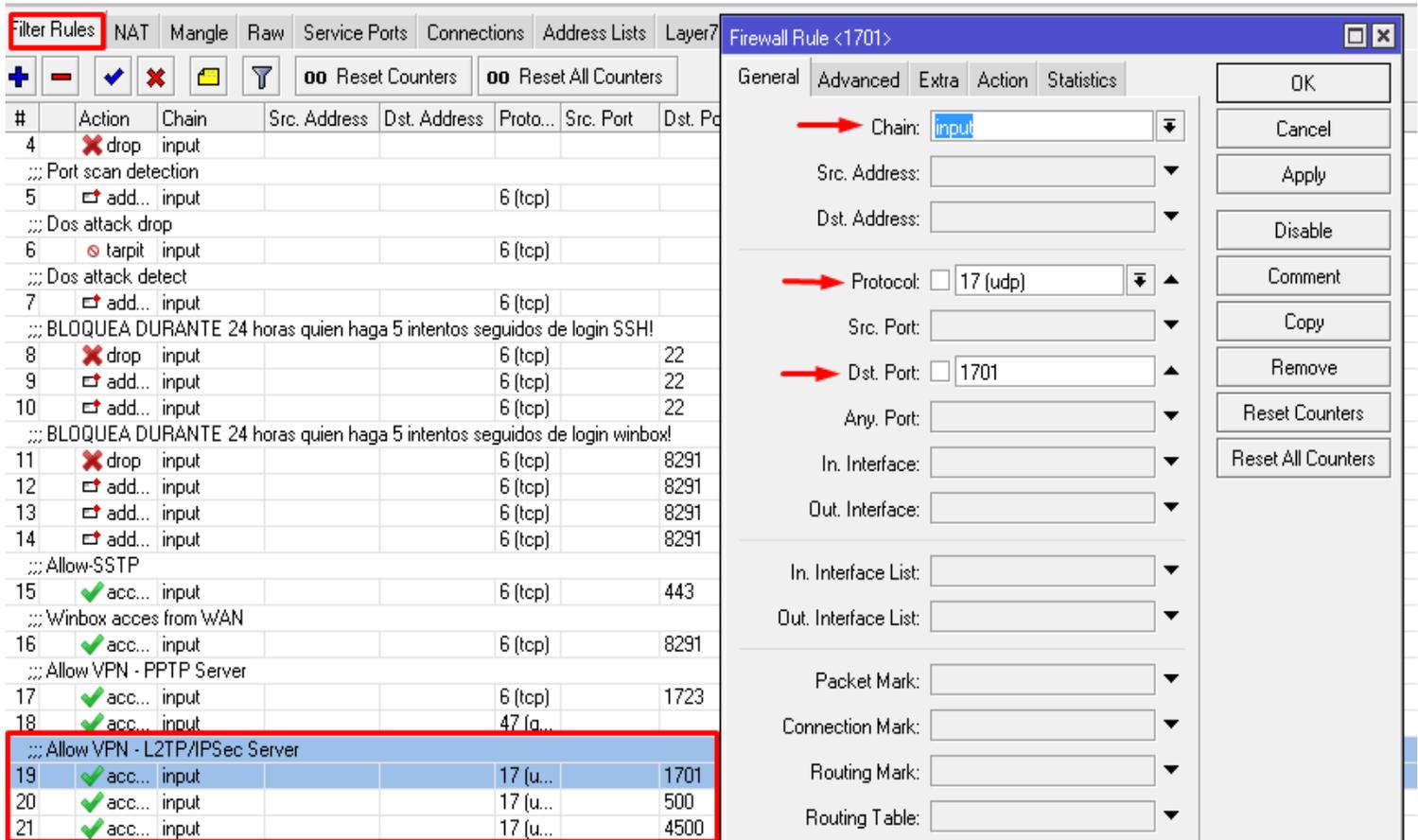
Limit Bytes Out:

Last Logged Out: Aug/08/2018 12:51:21

enabled

2.2

Paso 3: Ahora nos dirigimos a la parte de firewall y agregamos nuestra regla de input para aceptar el trafico entrante de los siguientes puertos **UPD 1701: L2TP**, **UDP: 500:** Usado por el protocolo **IPsec** y el **UDP: 4500:** usado por IPsec para manejar la encryptacion y el nateo de nuestro túnel L2TP/IPsec. Ver imagen 2.3,



The image shows the Mikrotik WinBox interface. On the left, the 'Filter Rules' window displays a list of rules. Rules 19, 20, and 21 are highlighted with a red box. Rule 19 is 'Allow VPN - L2TP/IPSec Server' with action 'accept' and ports 1701, 500, and 4500. Rules 20 and 21 also have action 'accept' and ports 1701, 500, and 4500.

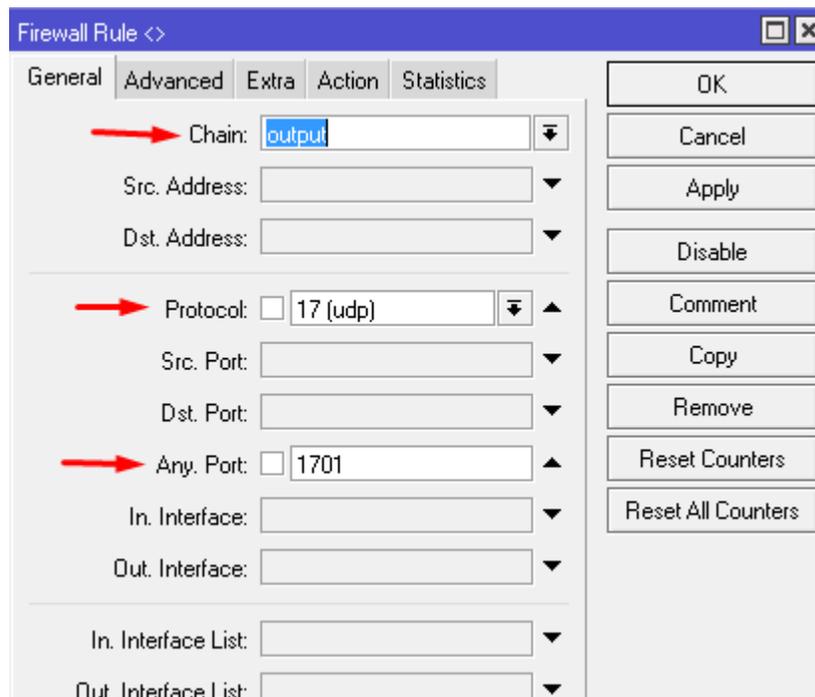
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Po
4	drop	input					
5	add...	input			6 (tcp)		
6	tarpit	input			6 (tcp)		
7	add...	input			6 (tcp)		
8	drop	input			6 (tcp)		22
9	add...	input			6 (tcp)		22
10	add...	input			6 (tcp)		22
11	drop	input			6 (tcp)		8291
12	add...	input			6 (tcp)		8291
13	add...	input			6 (tcp)		8291
14	add...	input			6 (tcp)		8291
15	acc...	input			6 (tcp)		443
16	acc...	input			6 (tcp)		8291
17	acc...	input			6 (tcp)		1723
18	acc...	input			47 (g...		
19	acc...	input			17 (u...		1701
20	acc...	input			17 (u...		500
21	acc...	input			17 (u...		4500

On the right, the 'Firewall Rule <1701>' dialog is open, showing the configuration for rule 1701. The 'Chain' is set to 'input', the 'Protocol' is '17 (udp)', and the 'Dst. Port' is '1701'. The 'Src. Address' and 'Dst. Address' fields are empty. The 'In. Interface' and 'Out. Interface' fields are also empty. The 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Routing Table' fields are empty. The 'Action' tab is selected, and the 'Action' field is empty.

2.3

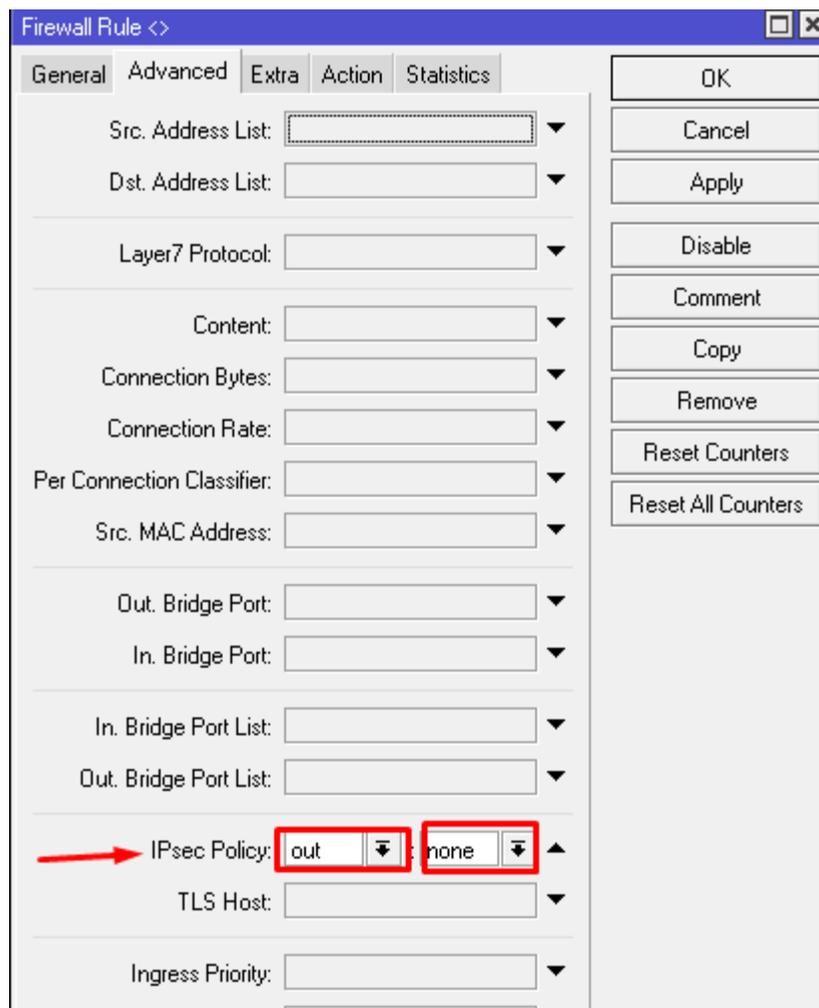
Seguridad a la Conexión L2TP/IPsec:

Paso 4: Ahora creamos una regla la cual nos permite hacer que los clientes **L2TP/IPsec** obligatoriamente se conecten al túnel utilizando encriptación **IPsec**, para ello crearemos una regla output especificando el protocolo y por cualquier puerto sea desde mi red o fuera de la misma. Ver imagen 2.4



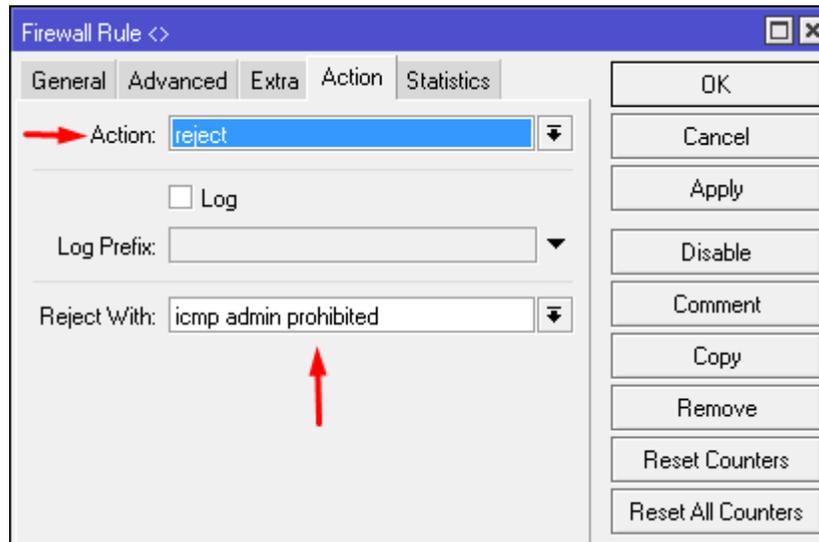
2.4

Paso 5: En la siguiente ventana alojada en **Advanced** vamos a configurar la parte de **IPsec policy** donde le especificamos que el tráfico saliente no encriptado por IPsec me lo envíe a la siguiente acción que veremos en el siguiente paso. Ver imagen 2.5.

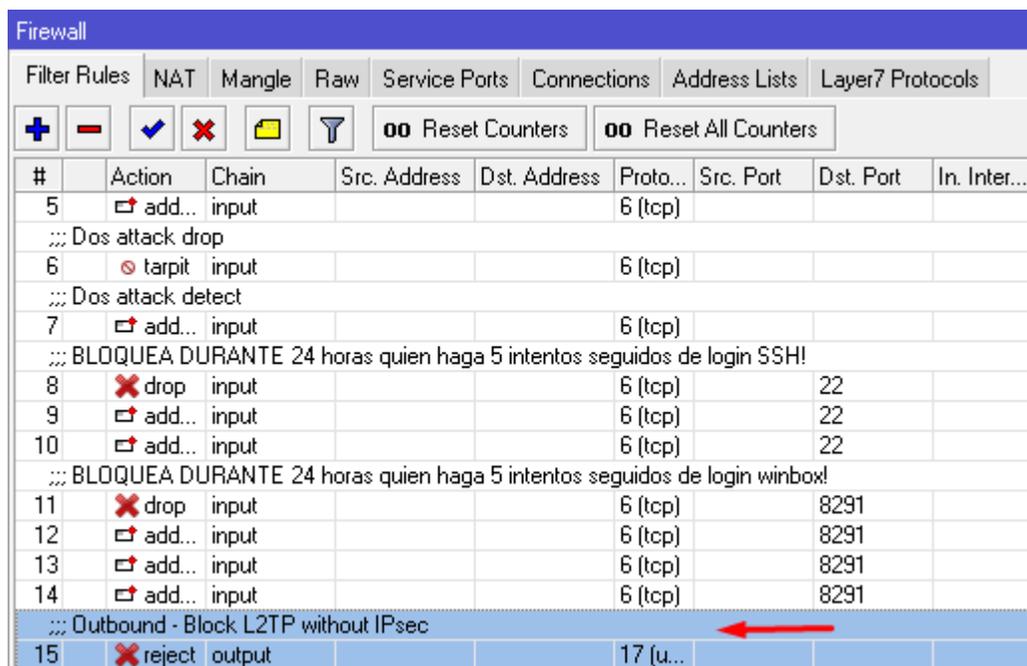


2.5

Paso 6: y por ultimo le configuramos un **Action=reject**, esto me redirije el trafico que no use **IPsec** a una política por defecto de mikrotik llamada **icmp admin prohibited**, esto me indica que si una persona quiere loguearse solo por L2TP no podrá por lo que necesitara el secret, debido a que nuestro router solo acepta el trafico encriptado por IPsec. Ver imagen 2.6 y 2.7.



2.6



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...
5	add...	input			6 (tcp)			
::: Dos attack drop								
6	tarpit	input			6 (tcp)			
::: Dos attack detect								
7	add...	input			6 (tcp)			
::: BLOQUEA DURANTE 24 horas quien haga 5 intentos seguidos de login SSH!								
8	drop	input			6 (tcp)		22	
9	add...	input			6 (tcp)		22	
10	add...	input			6 (tcp)		22	
::: BLOQUEA DURANTE 24 horas quien haga 5 intentos seguidos de login winbox!								
11	drop	input			6 (tcp)		8291	
12	add...	input			6 (tcp)		8291	
13	add...	input			6 (tcp)		8291	
14	add...	input			6 (tcp)		8291	
::: Outbound - Block L2TP without IPsec								
15	reject	output			17 (u...			

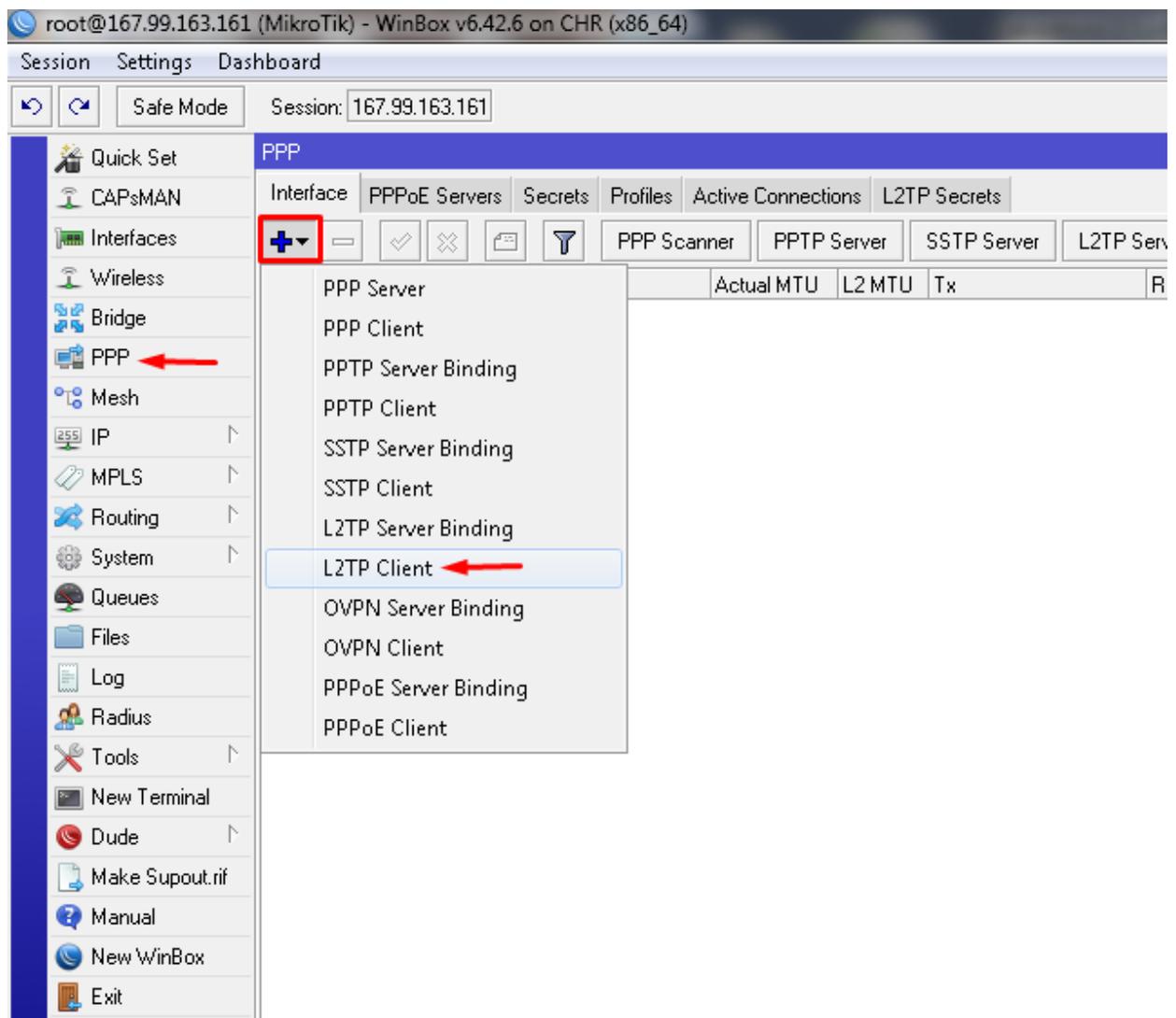
2.7

Laboratorio 2.2: Configuración de L2TP/IPsec Cliente en Mikrotik y Windows.

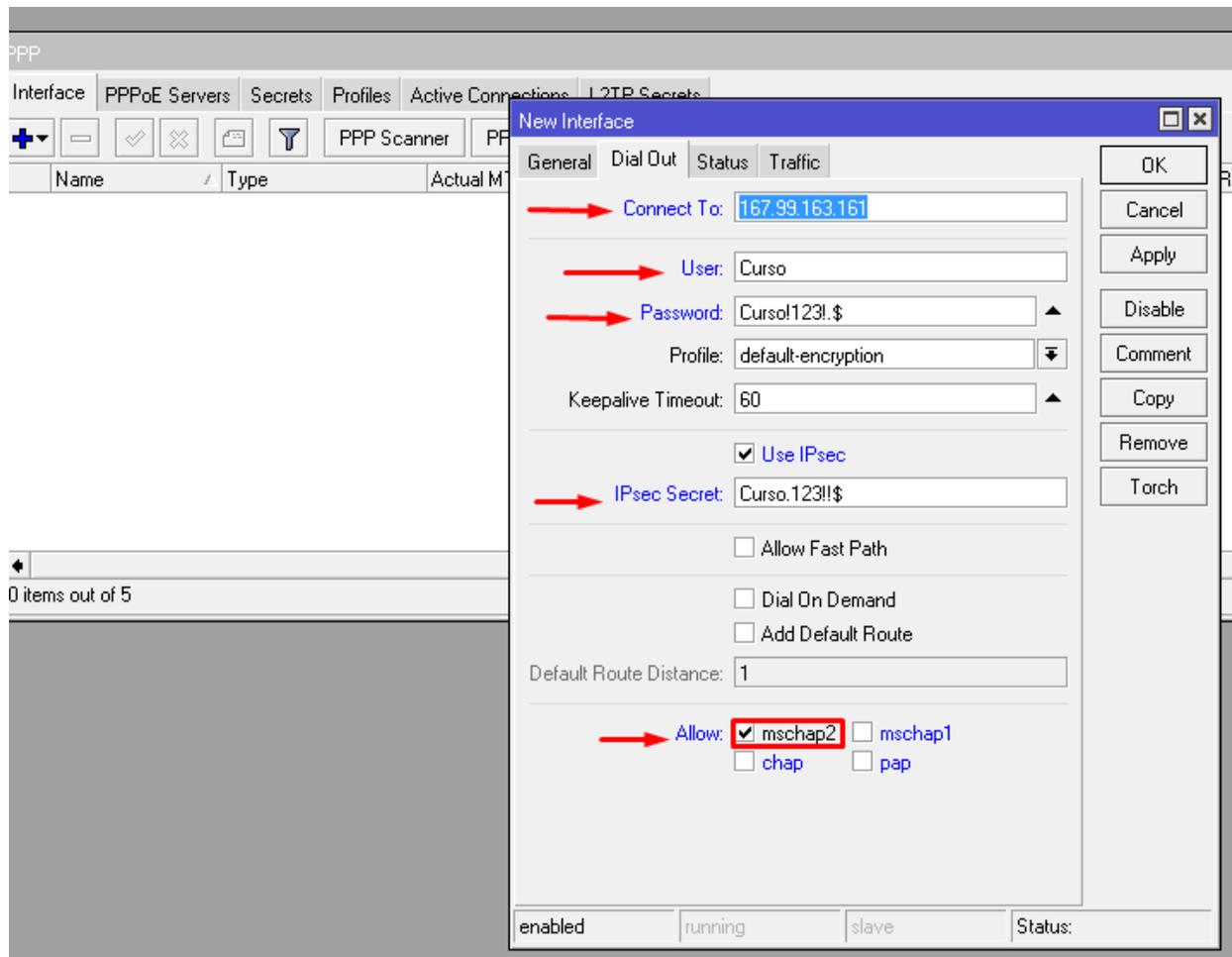
Objetivos: Configurar un L2TP/IPsec Client en Mikrotik y Windows.

Mikrotik:

Paso 1: A continuación procedemos a configurar nuestro cliente en el MikroTik como. Podemos ver en la imagen 2.8 nos dirigimos a la parte de configuración PPP-Interfaces damos click al signo de + y seleccionamos la opción L2TP client.

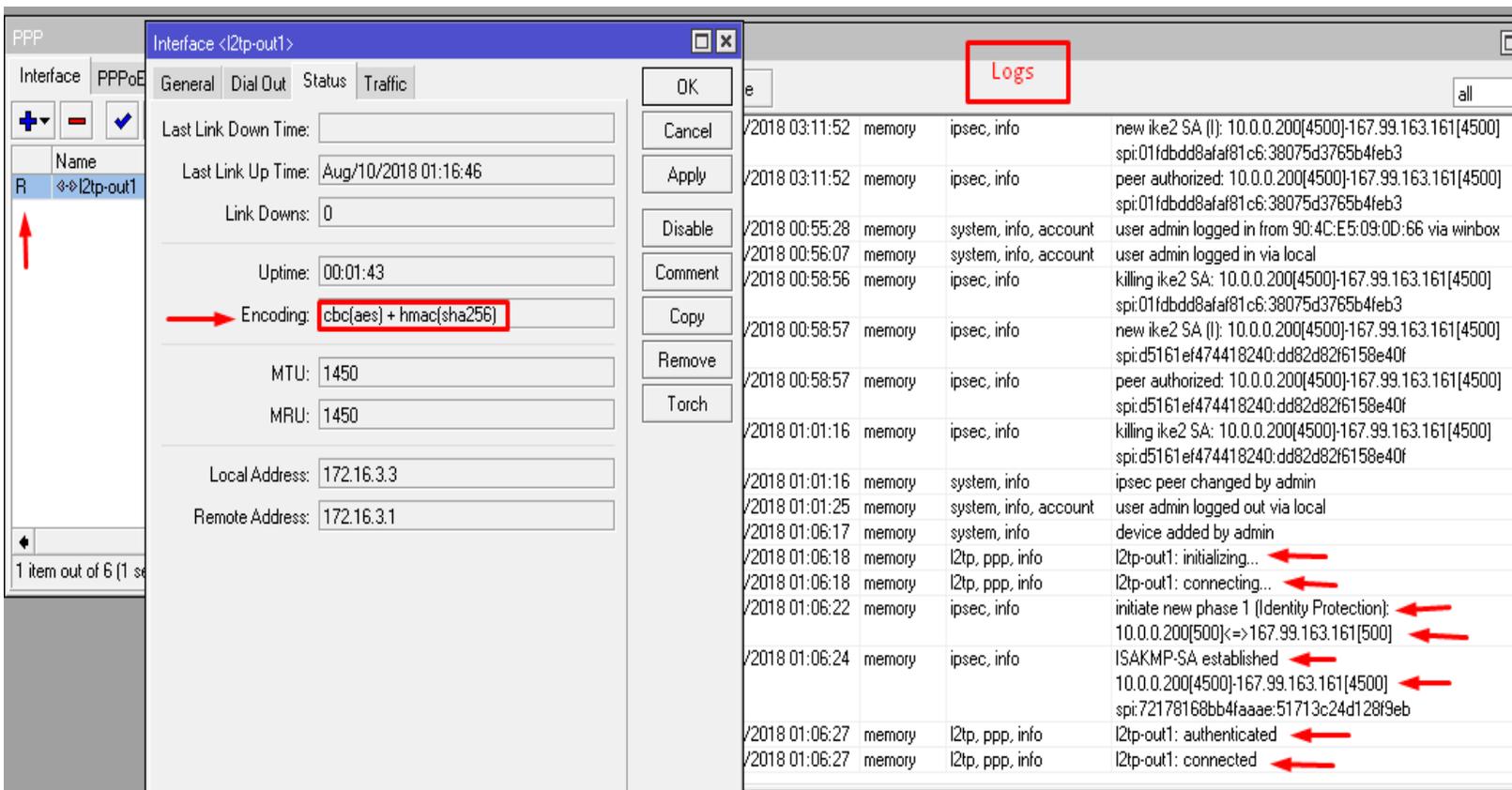


Paso 2: Ahora nos aparece la ventana de configuración en donde llenaremos los campos Connect To: dirección Publica de mi server, User, Password, y más adelante seleccionamos la casilla **Use IPsec** habilitando el uso del antes mencionado protocolo en nuestro túnel L2TP. Mas debajo en IPsec secret configuramos nuestra clave compartida o Pre-Share-Key, y permitimos el protocolo de autenticación **Mschap2**. Ver imagen 2.9.



2.9

Paso 3: Como lo muestra la imagen 2.10, ya nuestro túnel L2TP/ipsec está establecido. En la ventana de la izquierda en la pestaña de Status podemos ver las informaciones que se agregaron tan pronto nos conectamos al túnel como el Encondig: esto nos muestra los protocolos de encriptación y autenticación que está usando nuestro túnel. Como podemos ver, este utiliza como protocolo de encriptación de información **cbc(aes)** + el protocolo de autenticación **hmac(sha256)**. Más abajo nos muestra la IP entregada por nuestro server y la IP remota del mismo. Del otro lado en la ventana de logs podemos ver el proceso de inicialización autenticación, encriptación y conexión del antes mencionado túnel.



The screenshot displays the Mikrotik WinBox interface for configuring a PPP interface. The 'Interface' list on the left shows 'l2tp-out1' selected. The 'Status' tab of the configuration window shows the following details:

- Last Link Down Time: (empty)
- Last Link Up Time: Aug/10/2018 01:16:46
- Link Downs: 0
- Uptime: 00:01:43
- Encoding: **cbc(aes) + hmac(sha256)** (highlighted with a red box and arrow)
- MTU: 1450
- MRU: 1450
- Local Address: 172.16.3.3
- Remote Address: 172.16.3.1

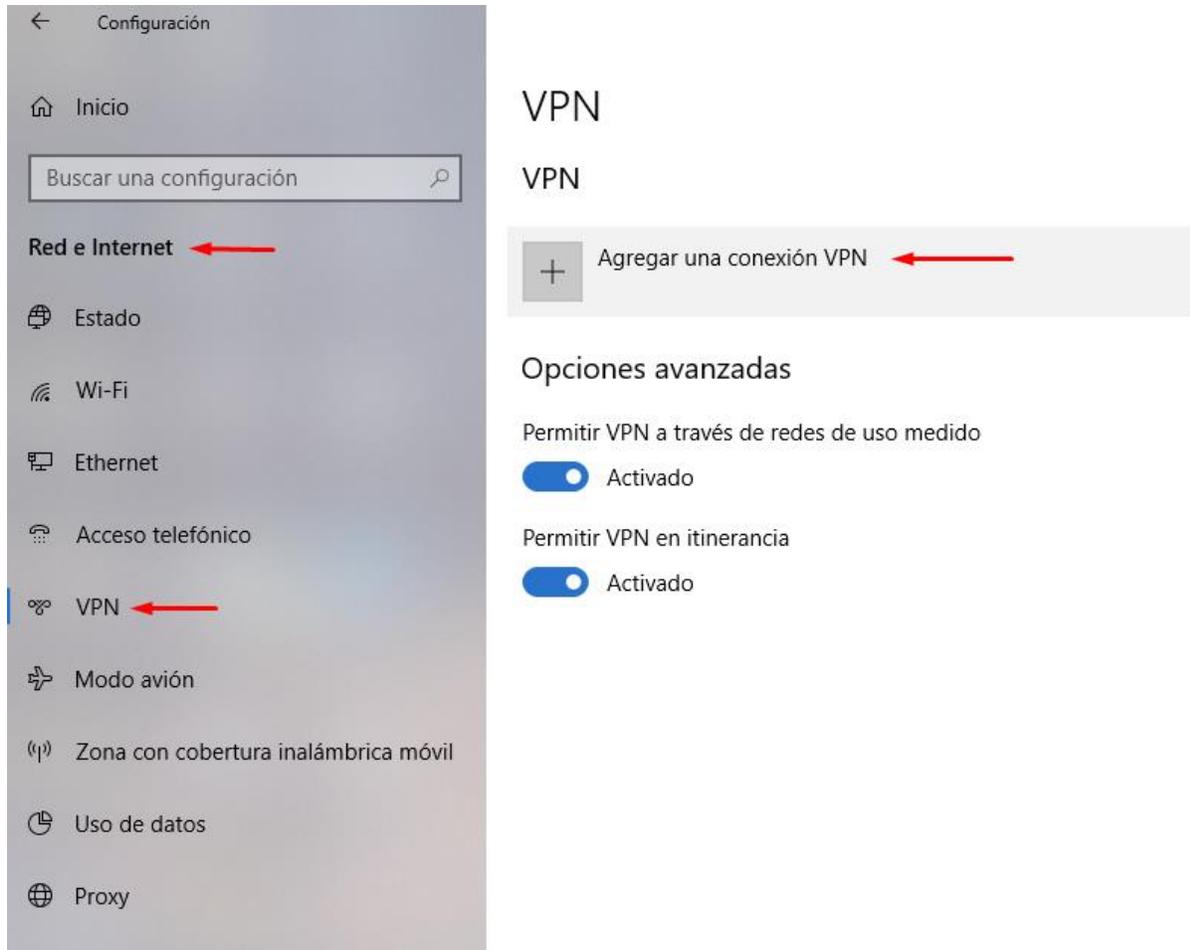
The 'Logs' window on the right shows the following log entries:

Time	Level	Category	Message
2018 03:11:52	memory	ipsec, info	new ike2 SA (I): 10.0.0.200[4500]-167.99.163.161[4500]
2018 03:11:52	memory	ipsec, info	spi:01fdbdd8afaf81c6:38075d3765b4feb3
2018 00:55:28	memory	system, info, account	peer authorized: 10.0.0.200[4500]-167.99.163.161[4500]
2018 00:56:07	memory	system, info, account	user admin logged in from 90:4C:E5:09:0D:66 via winbox
2018 00:58:56	memory	ipsec, info	user admin logged in via local
2018 00:58:56	memory	ipsec, info	killing ike2 SA: 10.0.0.200[4500]-167.99.163.161[4500]
2018 00:58:57	memory	ipsec, info	spi:01fdbdd8afaf81c6:38075d3765b4feb3
2018 00:58:57	memory	ipsec, info	new ike2 SA (I): 10.0.0.200[4500]-167.99.163.161[4500]
2018 00:58:57	memory	ipsec, info	spi:d5161ef474418240:dd82d82f6158e40f
2018 00:58:57	memory	ipsec, info	peer authorized: 10.0.0.200[4500]-167.99.163.161[4500]
2018 01:01:16	memory	ipsec, info	spi:d5161ef474418240:dd82d82f6158e40f
2018 01:01:16	memory	ipsec, info	killing ike2 SA: 10.0.0.200[4500]-167.99.163.161[4500]
2018 01:01:16	memory	ipsec, info	spi:d5161ef474418240:dd82d82f6158e40f
2018 01:01:16	memory	system, info	ipsec peer changed by admin
2018 01:01:25	memory	system, info, account	user admin logged out via local
2018 01:06:17	memory	system, info	device added by admin
2018 01:06:18	memory	l2tp, ppp, info	l2tp-out1: initializing...
2018 01:06:18	memory	l2tp, ppp, info	l2tp-out1: connecting...
2018 01:06:22	memory	ipsec, info	initiate new phase 1 (Identity Protection):
2018 01:06:22	memory	ipsec, info	10.0.0.200[500]<=>167.99.163.161[500]
2018 01:06:24	memory	ipsec, info	ISAKMP-SA established
2018 01:06:24	memory	ipsec, info	10.0.0.200[4500]-167.99.163.161[4500]
2018 01:06:24	memory	ipsec, info	spi:72178168bb4faaae:51713c24d128f9eb
2018 01:06:27	memory	l2tp, ppp, info	l2tp-out1: authenticated
2018 01:06:27	memory	l2tp, ppp, info	l2tp-out1: connected

2.10

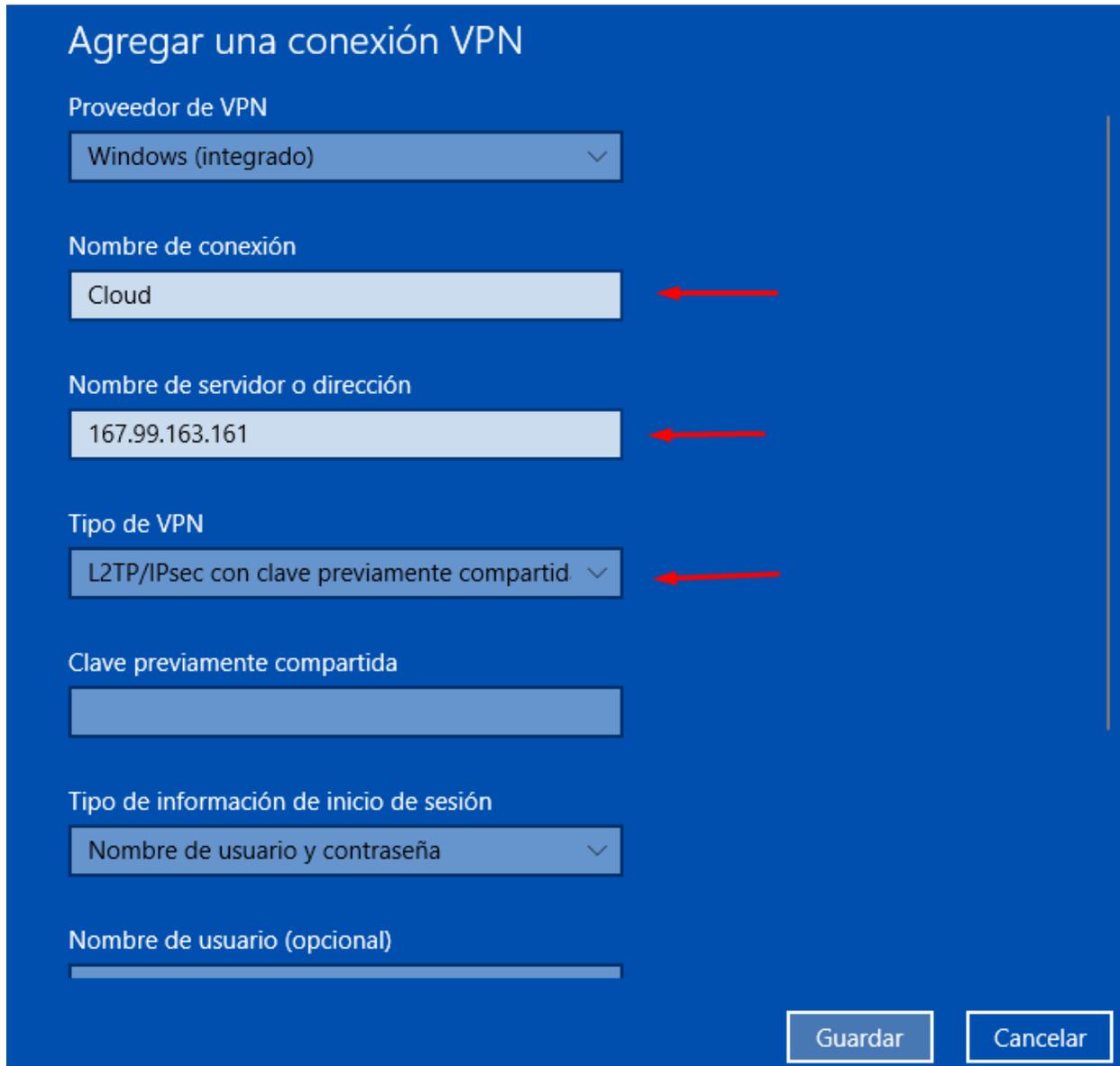
Windows:

Paso 1: Ahora vamos a configurar nuestro cliente Windows 10, para ello nos dirigimos Configuraciones y luego a Red Internet, una vez allí seleccionamos VPN y damos click a Agregar conexión VPN. Ver imagen 2.11.



2.11

Paso 2: Una vez hecho el paso anterior nos saldrá una ventana para la configuración de nuestro cliente L2TP/IPsec, Nombre de Conexión: será un nombre de su gusta para identificar su vpn. Nombre de servidor o dirección: aquí pondremos nuestro DDNS o IP publica de nuestro server luego seleccionamos el tipo de VPN, y por ultimo en Clave Previamente compartida: colocamos nuestro **Secret IPsec**, una vez hecho todo esto damos click al botón Guardar. Ver imagen 2.12.



Agregar una conexión VPN

Proveedor de VPN
Windows (integrado) ▾

Nombre de conexión
Cloud ←

Nombre de servidor o dirección
167.99.163.161 ←

Tipo de VPN
L2TP/IPsec con clave previamente compartid ▾ ←

Clave previamente compartida
[Empty text box]

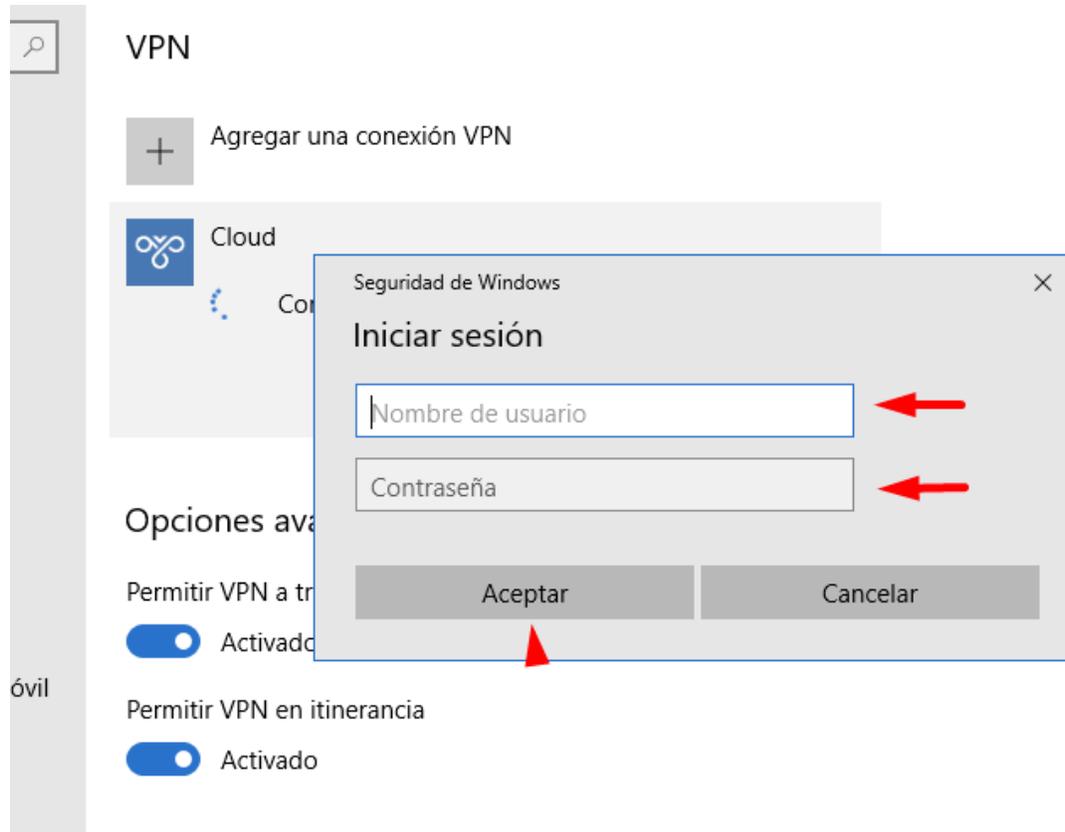
Tipo de información de inicio de sesión
Nombre de usuario y contraseña ▾

Nombre de usuario (opcional)
[Empty text box]

Guardar Cancelar

2.12

Paso 3: Ahora ingresamos nuestro usuario y password para conectarnos a nuestra VPN. Ver imagen 2.13.



2.13

Paso 4: Una vez completado todos los pasos correctamente, se nos conectara nuestro Cliente L2TP/IPsec tal y como se en la imagen 2.14.



2.14

Laboratorio especial:

Cliente Windows L2TP/IPsec cuando El server Mikrotik está detrás de un NAT.

Paso 1: en esta ocasión les dejare una imagen y un link expedido por Microsoft para solucionar este inconveniente con los clientes L2TP/IPsec Windows.

- Haga clic en **Start** , señale **Todos los programas**, haga clic en **Accesorios**, haga clic en **Ejecutar**, escriba regedit y luego haga clic en **Aceptar**. Si aparece el cuadro de diálogo **Control de cuentas de usuario** en la pantalla y le pide que eleve su token de administrador, haga clic en **Continuar**.
- Ubique y luego haga clic en la siguiente subclave del registro:

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ PolicyAgent

Nota: También puede aplicar el valor **AssumeUDPEncapsulationContextOnSendRule** DWORD a una computadora cliente VPN basada en Microsoft Windows XP Service Pack 2 (SP2). Para hacer esto, busque y luego haga clic en la siguiente subclave del registro:

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ IPsec

- En el menú **Edición**, seleccione **Nuevo** y luego haga clic en **Valor DWORD (32 bits)**.
- Tipo **AssumeUDPEncapsulationContextOnSendRule**, y presiona ENTRAR.
- Haga clic con el botón derecho en **AssumeUDPEncapsulationContextOnSendRule**, y luego haga clic en **Modificar**.
- En el cuadro **Información del valor**, escriba uno de los siguientes valores:
 - 0
Un valor de 0 (cero) configura Windows para que no pueda establecer asociaciones de seguridad con los servidores que se encuentran detrás de los dispositivos NAT. Este es el valor predeterminado.
 - 1
Un valor de 1 configura Windows para que pueda establecer asociaciones de seguridad con los servidores que se encuentran detrás de los dispositivos NAT.
 - 2
Un valor de 2 configura Windows para que pueda establecer asociaciones de seguridad cuando tanto el servidor como la computadora cliente VPN basada en Windows Vista o Windows Server 2008 están detrás de los dispositivos NAT.

Para más información consultar el siguiente link

<https://support.microsoft.com/en-us/help/926179/how-to-configure-an-l2tp-ipsec-server-behind-a-nat-t-device-in-windows>