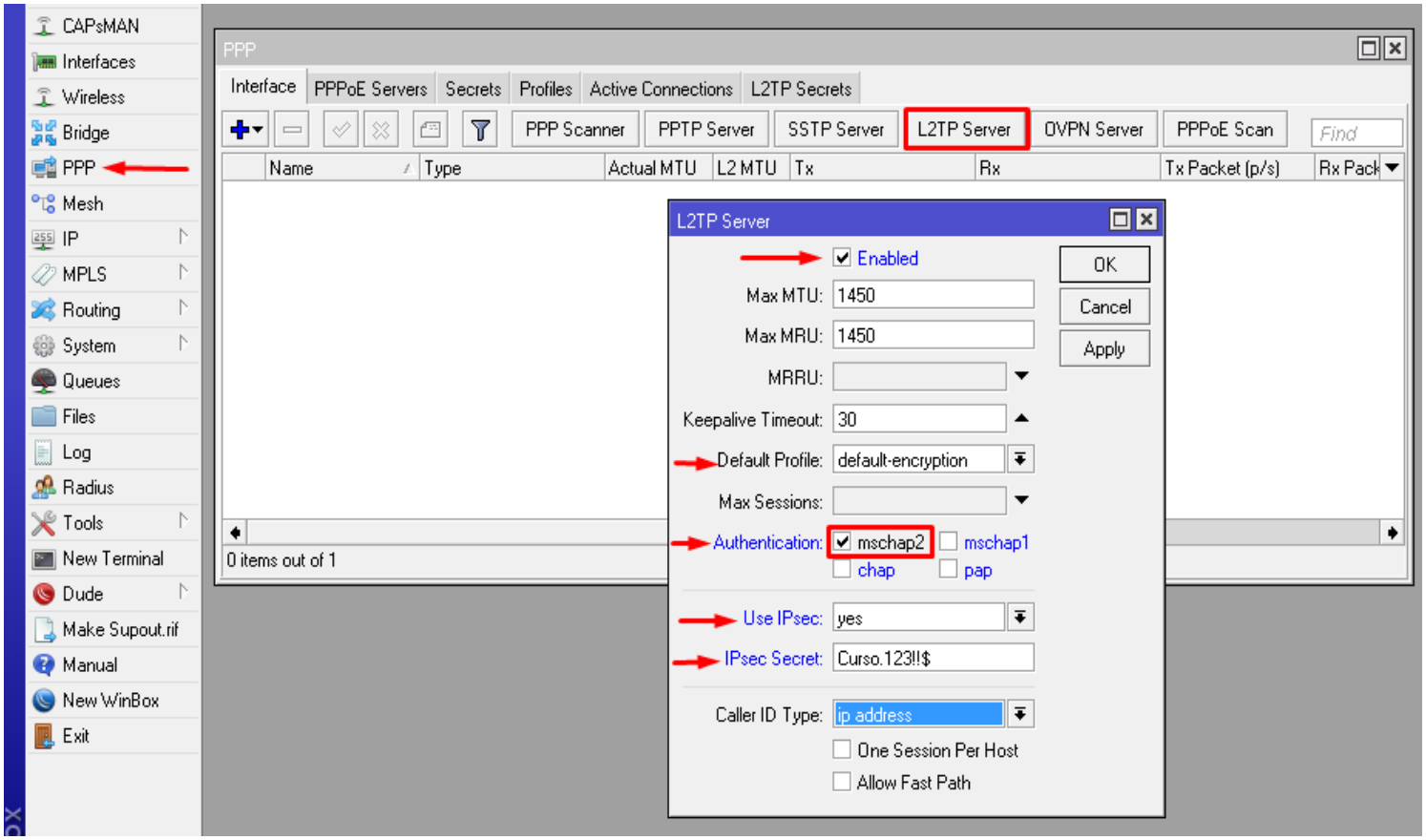
Laboratorio 2.1: Laboratorio L2TP/IPsec Server Mikrotik

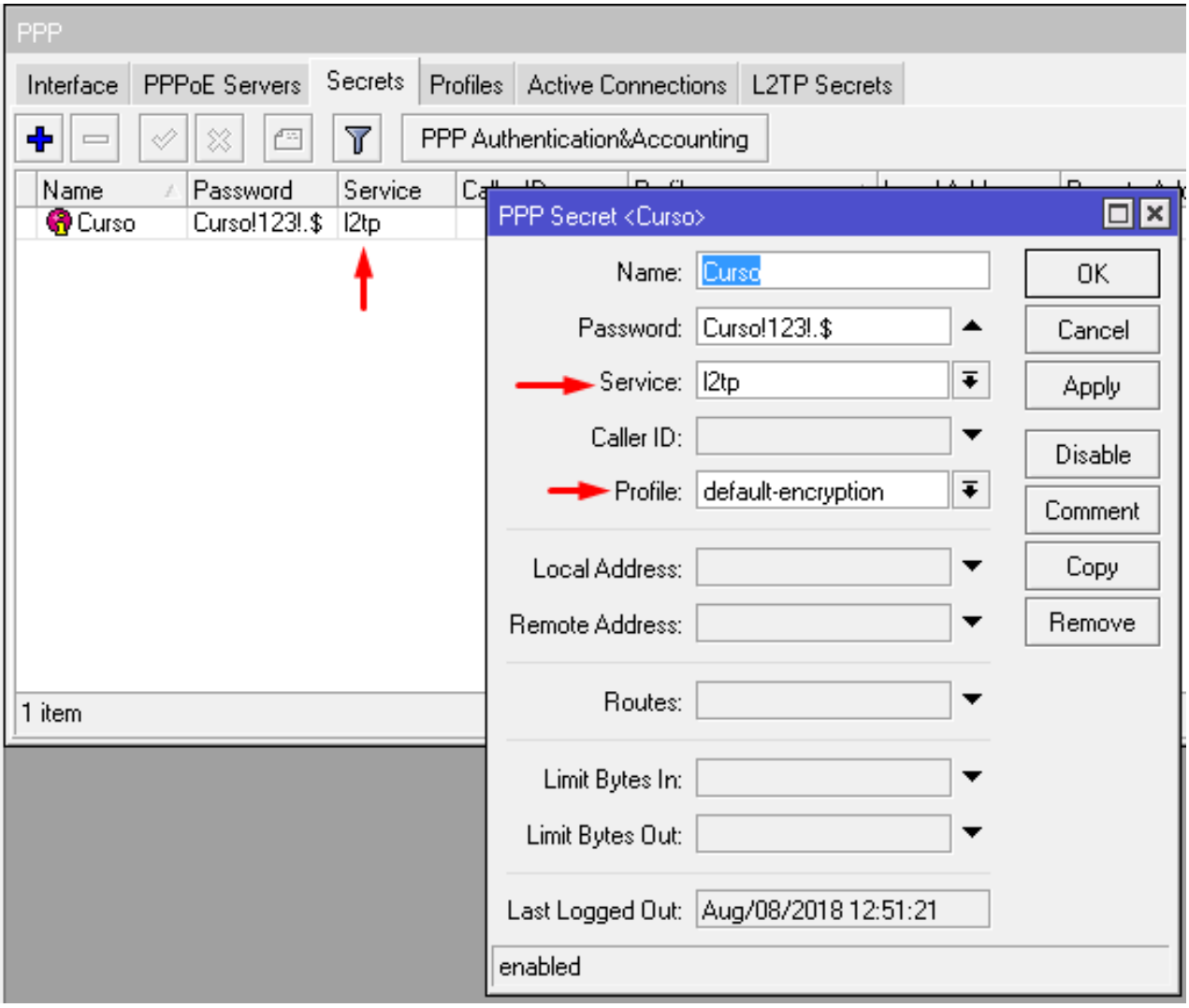
Objetivo: **Configurar un Túnel L2TP/IPsec server en su Router MikroTik.**

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



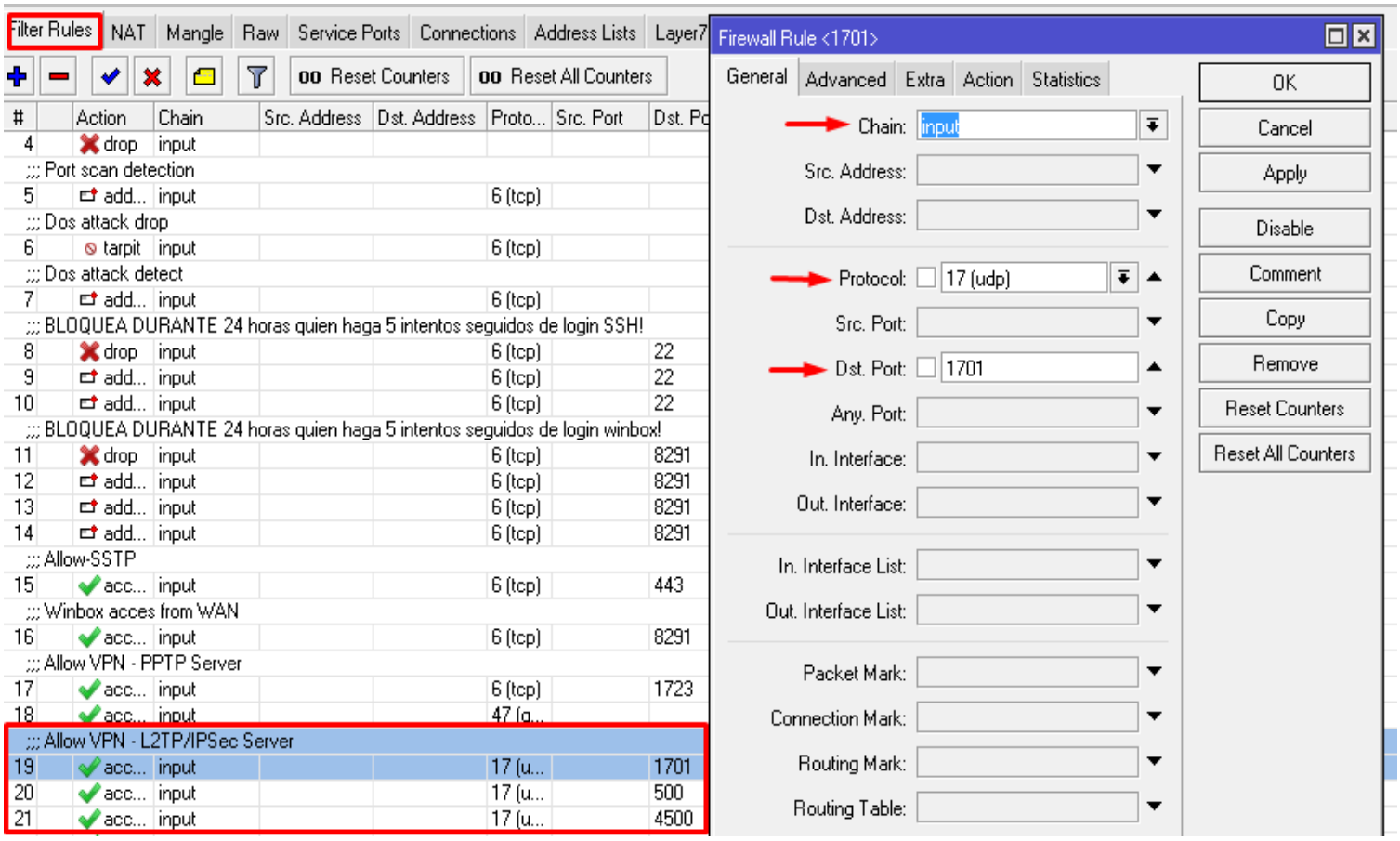
2.1

Paso 2: una vez hecho el paso anterior, nos dirijimos a la pestaña Secrets una vez alli 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**.**



2.2

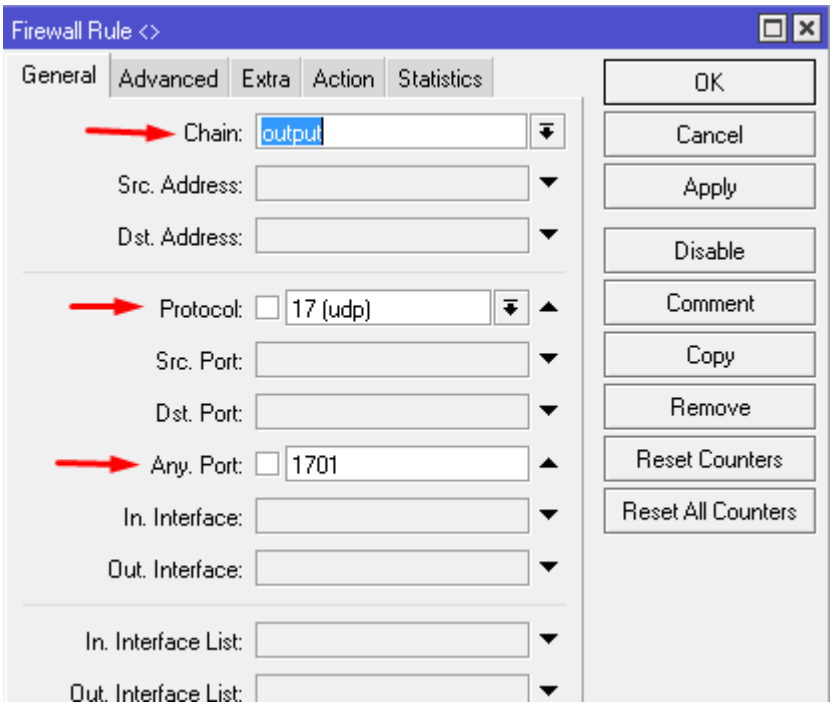
Paso 3: Ahora nos dirigimos a la parte de firewall y agregamos nuestra regla de input para aceptar el trafico entrante de los siguientes puertos **UPD 1701: L2TP, UDP: 500:** Usado por el protocolo **IPsec** y el **UDP: 4500**: usado por IPsec para manejar la encryptacion y el nateo de nuestro túnel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



2.3

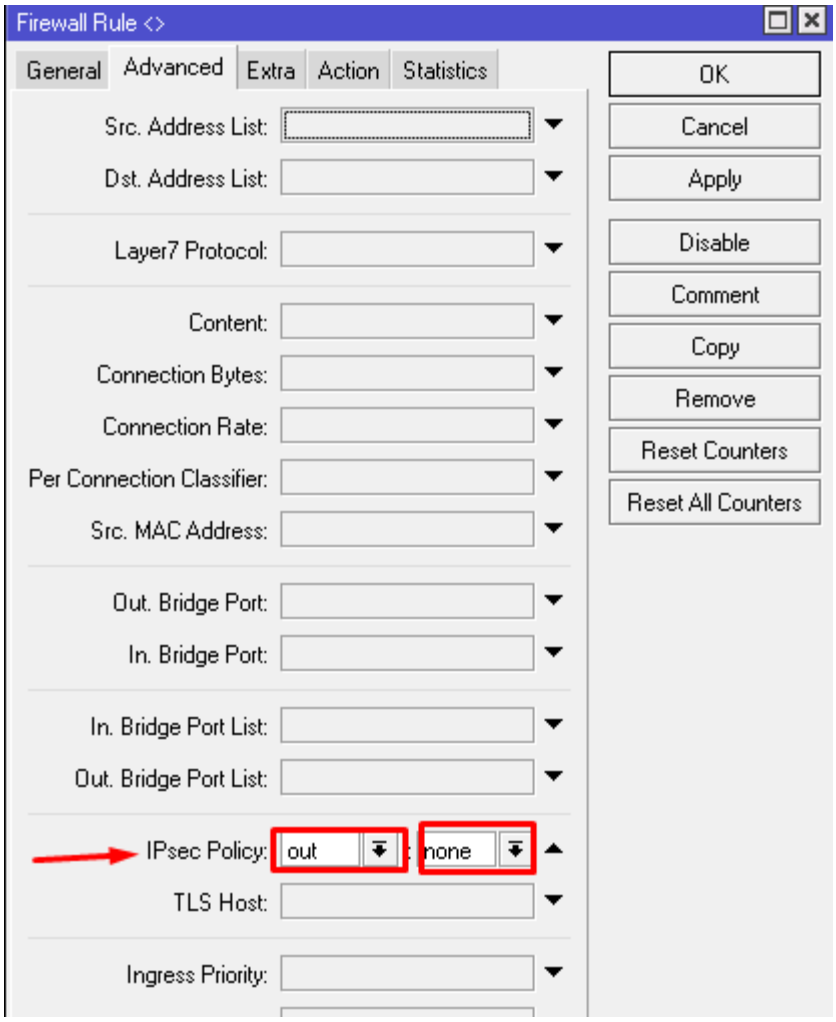
Seguridad a la Conexión L2TP/IPsec:

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



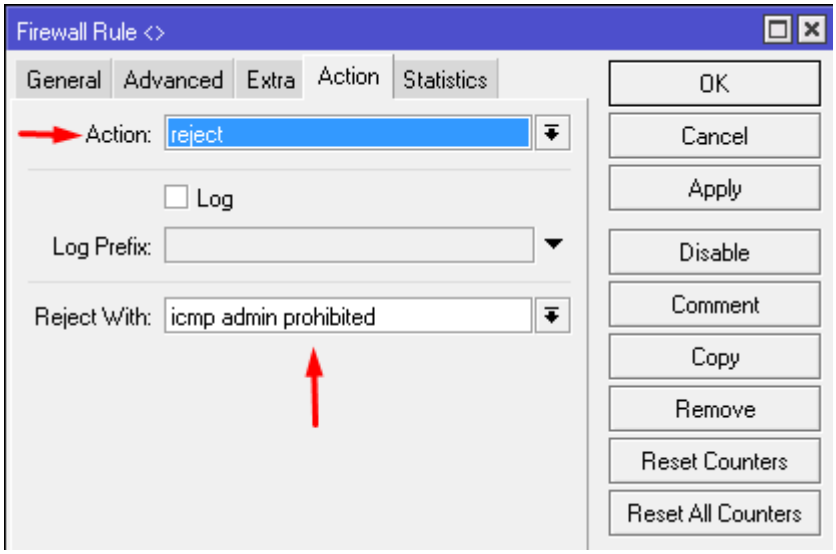
2.4

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

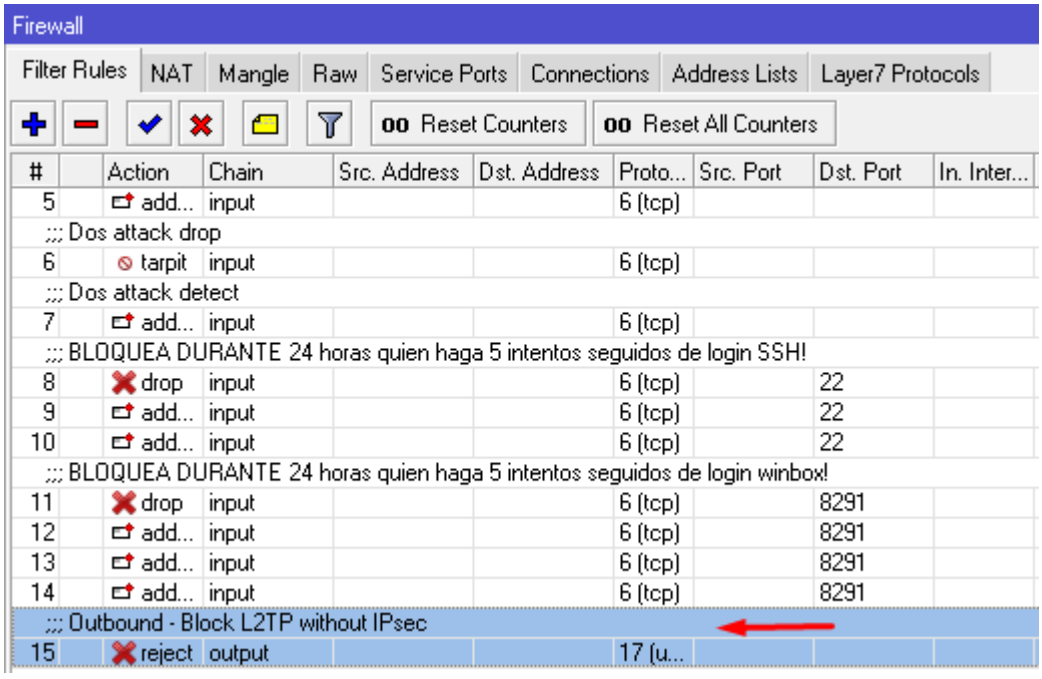


2.5

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



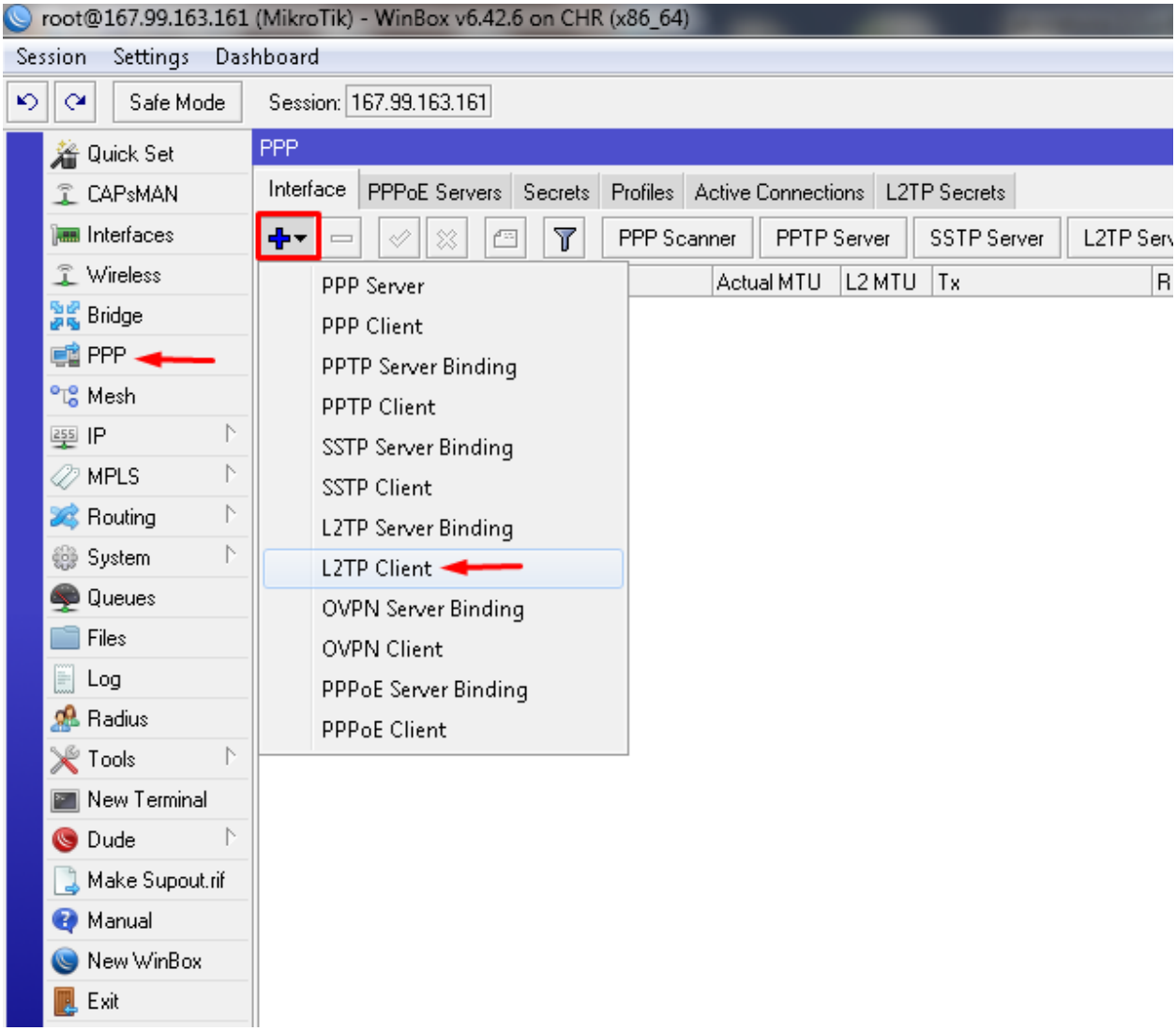
2.7

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

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

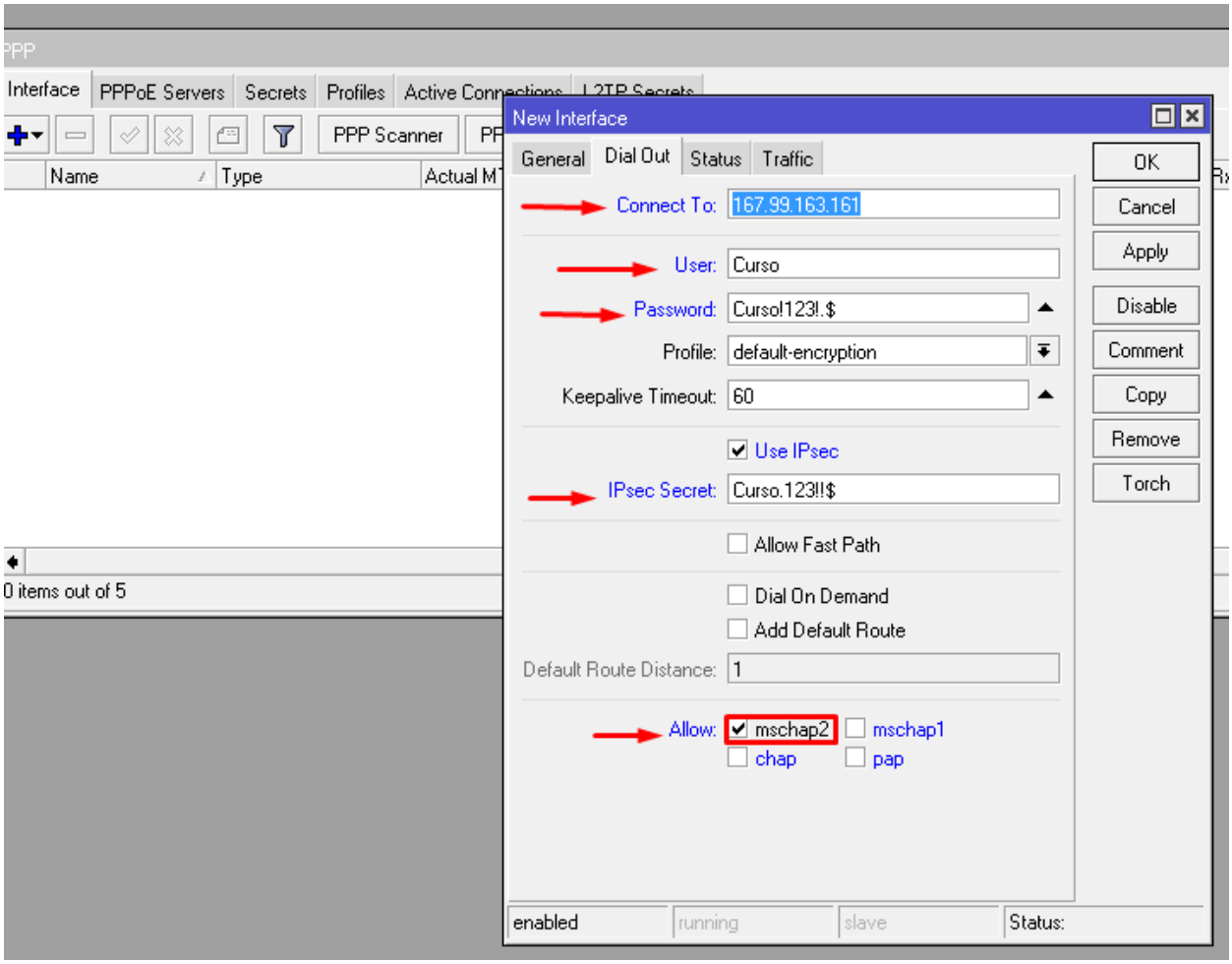
Mikrotik:

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.



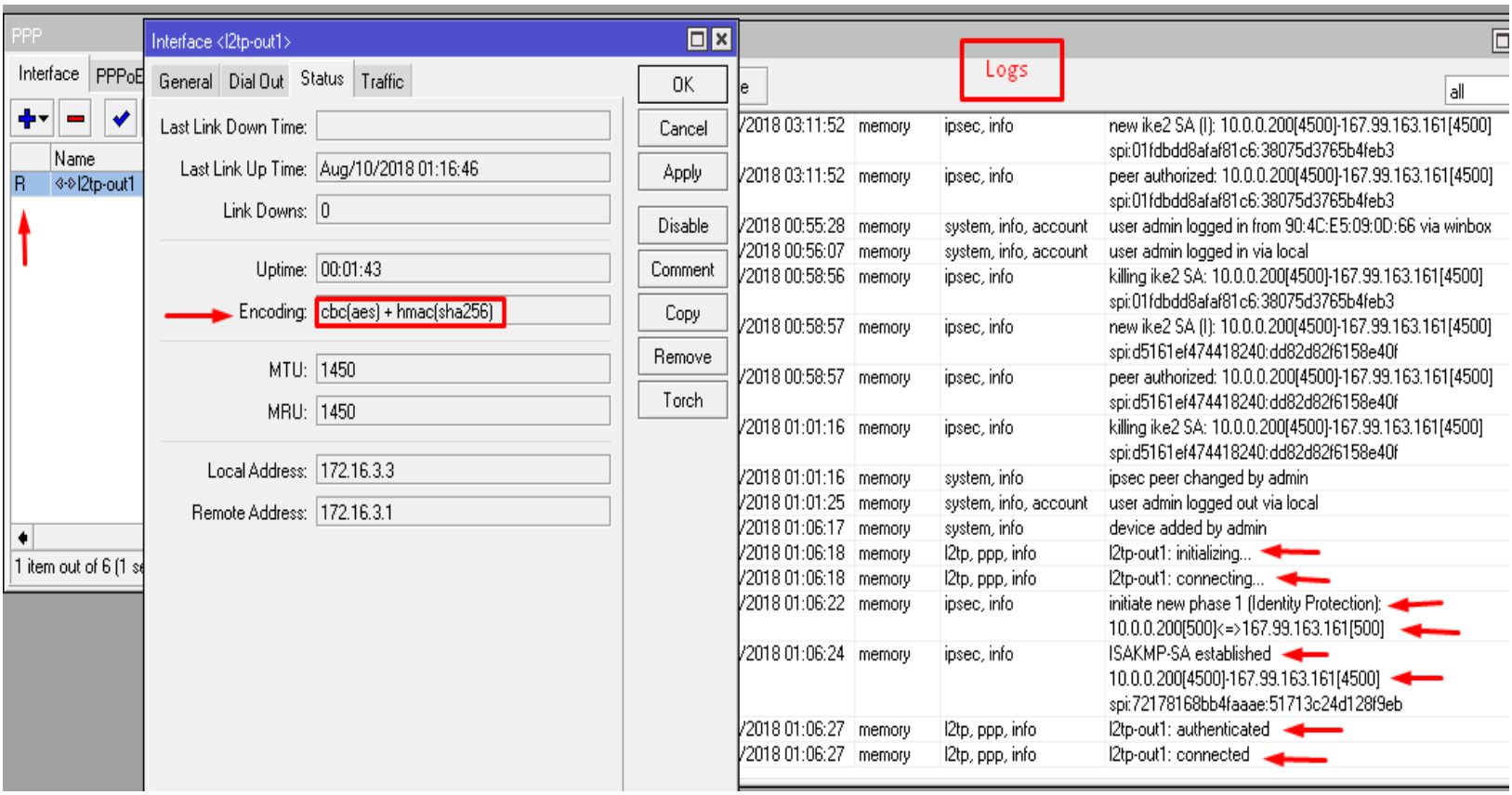
2.8

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

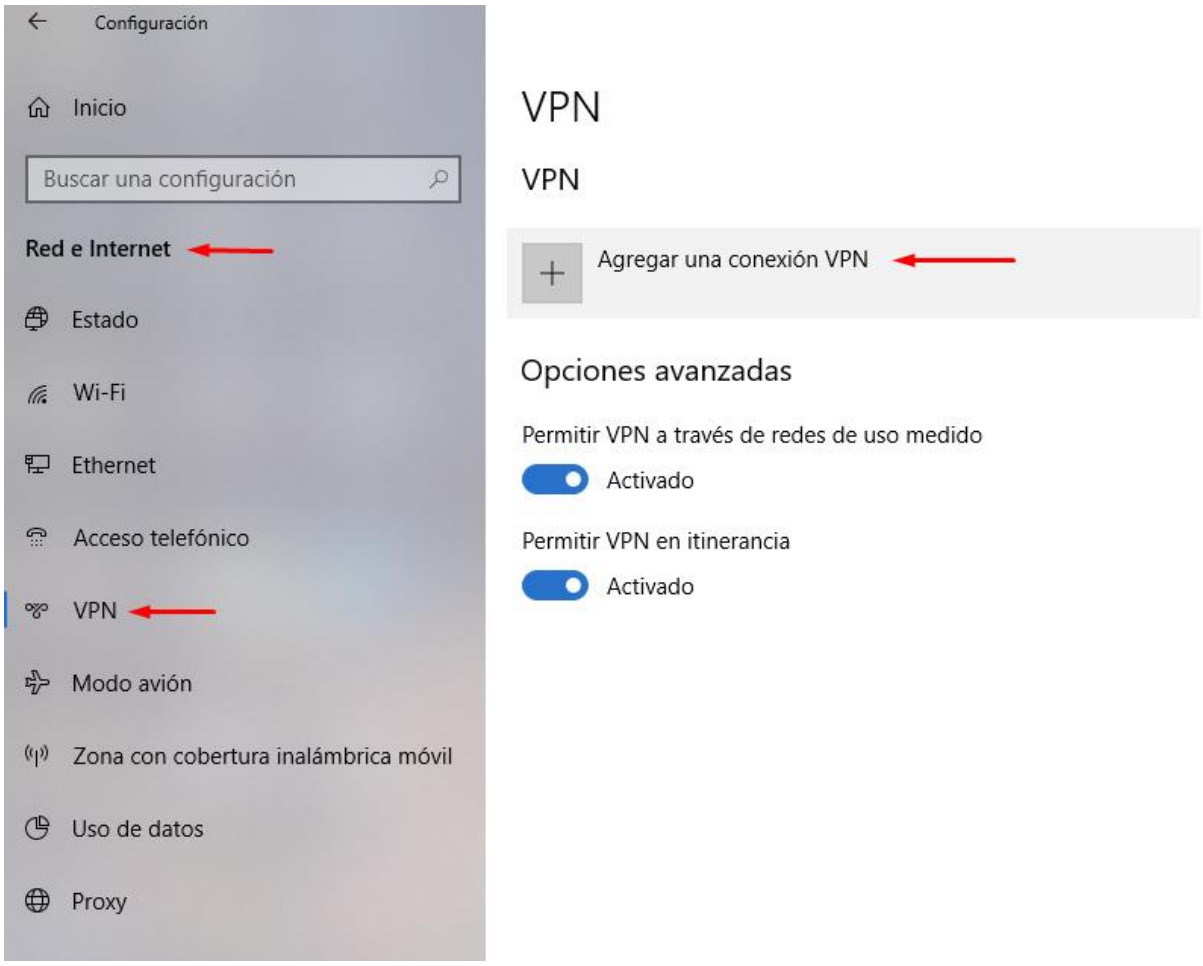
Paso 3: Como lo muestra la imagen 2.10, ya nuestro túnel L2TP/ipsec está establecido. En la ventana de la izquierda en la pestaña de Status podemos ver las informaciones que se agregaron tan pronto nos conectamos al túnel como el Encondig: esto nos muestra los protocolos de encriptación y autenticación 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.



2.10

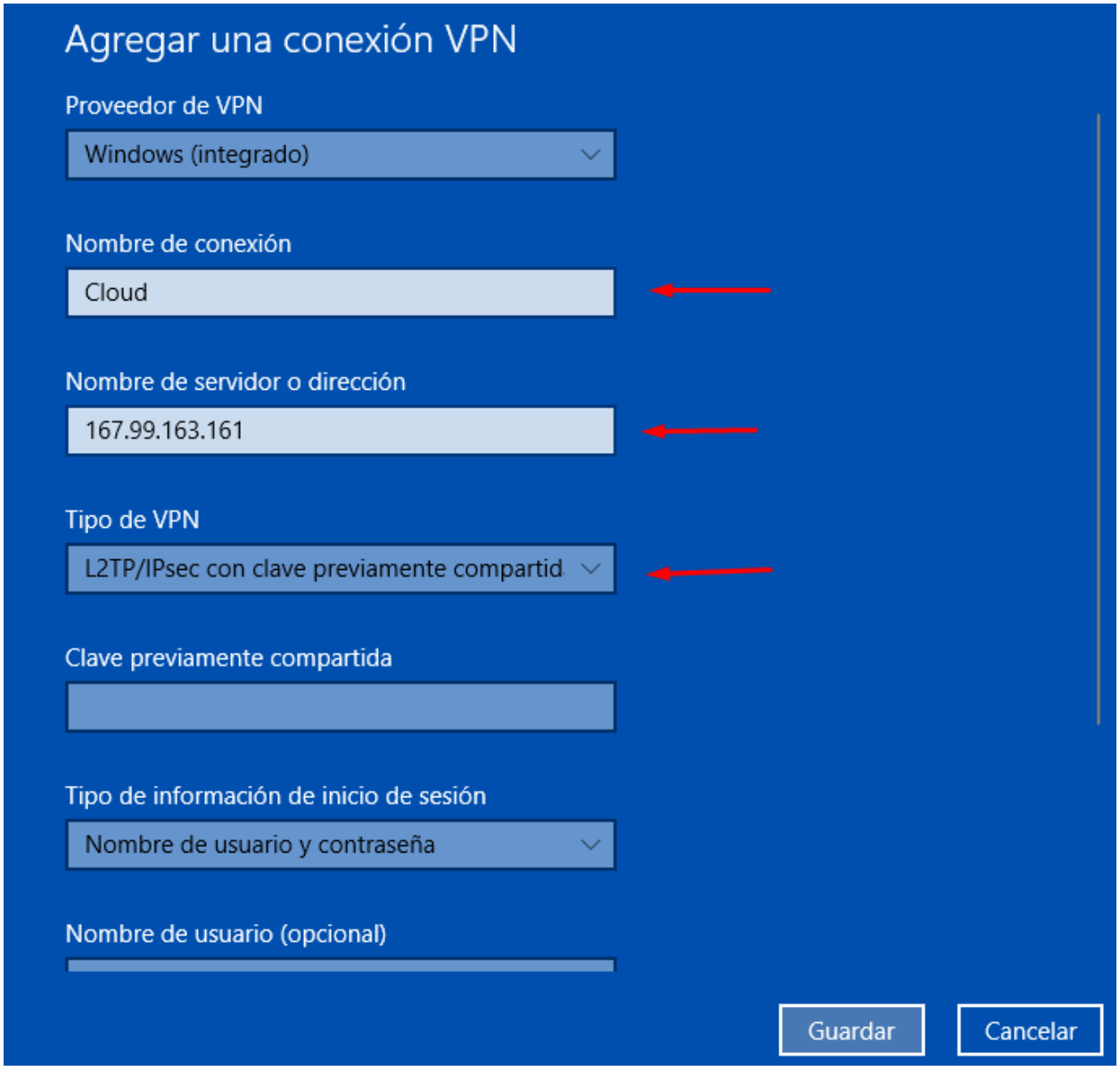
Windows:

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.



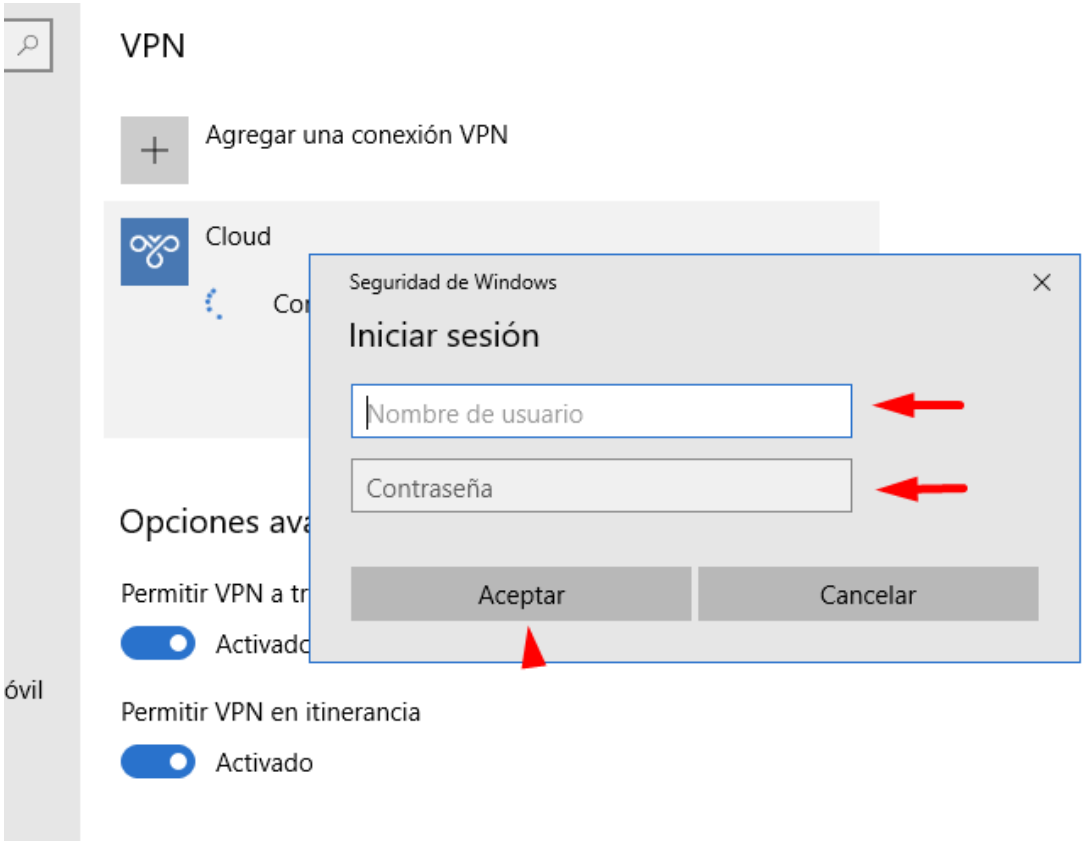
2.11

Paso 2: Una vez hecho el paso anterior nos saldrá una venta 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.



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.

2. 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** .
3. 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

4. En el menú **Edición** , seleccione **Nuevo** y luego haga clic en **Valor DWORD (32 bits)** .
5. Tipo AssumeUDPEncapsulationContextOnSendRule , y presiona ENTRAR.
6. Haga clic con el botón derecho en **AssumeUDPEncapsulationContextOnSendRule** , y luego haga clic en **Modificar** .
7. 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