

MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE UNA VPN LOCAL



En este manual se enseñará a instalar y configurar su propia VPN local desde cero.

C.F.G.S: Administración de sistemas informáticos en red.
Autores: Daniel Polo Gómez y Álvaro Vizuite Martín.
Tutor: Ramón González.
IES La Arboleda.



Esta obra está bajo una [Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/).

Índice

1. Introducción	2
1.1 ¿Qué es una VPN?	2
1.2 Para qué sirven las conexiones VPN	3
1.3 Ventajas de VPN.....	4
1.4 Inconvenientes de VPN.....	4
2. Creación de la VPN	5
2.1 Previo a la instalación	5
3. Configuración del servidor	9
4. Prueba de funcionamiento	15
4.1 Ubuntu	15
4.2 Windows	17
4.3 Android	19
5. Bibliografía	20

1. Introducción

1.1 ¿Qué es una VPN?

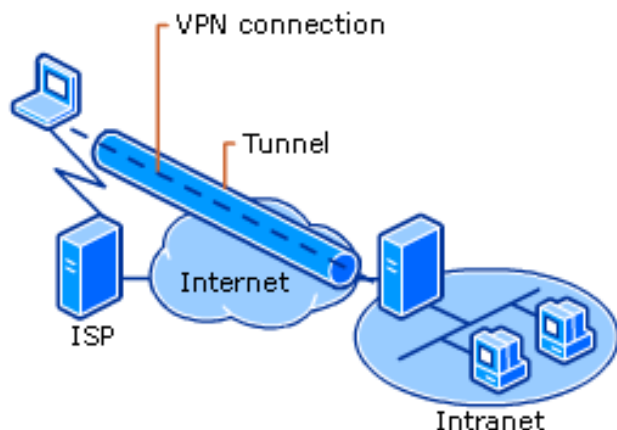
Las conexiones VPN se están empezando a tener más en cuenta. Inicialmente tenían un uso común en las empresas y organizaciones, la gran versatilidad de este tipo de conexiones y sus múltiples usos las hacen cada vez más populares.

VPN son las siglas de Virtual Private Network, o red privada virtual. La palabra clave aquí es virtual, es esta propiedad la que genera la necesidad de la VPN en sí, así como la que permite a las conexiones VPN ofrecerte los múltiples usos que veremos más adelante.

Una conexión VPN lo que te permite es crear una red local sin necesidad que los usuarios estén físicamente conectados entre sí, sino a través de Internet. Obtienen las ventajas de la red local, con una mayor flexibilidad, pues la conexión es a través de Internet y puede por ejemplo ser de una punta del mundo a la otra.

Normalmente, mientras usas Internet tu dispositivo se pone en contacto con tu proveedor de Internet, que es el que conecta con los distintos servicios web para ofrecerte, por ejemplo, los vídeos de YouTube.

Cuando te conectas a una conexión VPN, esto cambia. Todo tu tráfico de red sigue yendo desde tu dispositivo a tu proveedor de Internet, pero de ahí se dirige directo al servidor VPN, desde donde partirá al destino. Idealmente la conexión está cifrada, de modo que tu proveedor de Internet realmente no sabe a qué estás accediendo. A efectos prácticos, tu dirección IP es la del servidor VPN, en muchos aspectos es como si estuvieras físicamente ahí, conectándose a Internet.



1.2 Para qué sirven las conexiones VPN

Actualmente uno de los usos más importantes de las VPN es el teletrabajo, permite la interconectividad en redes que no están físicamente conectadas, como es el caso de trabajadores que trabajan fuera de la oficina o empresas con sucursales en varias ciudades que necesitan acceder a una única red privada. Además, el acceso está protegido, la conexión está previsiblemente cifrada y el trabajador tiene el mismo acceso que si estuviera presencialmente ahí.

Otra función de las VPN es la de evitar censura y bloqueos geográficos de contenido, al conectarte con VPN, tu dispositivo se comunica con el servidor VPN, y es éste el que habla a Internet. Si estás en China y el servidor VPN está en Estados Unidos, generalmente los servidores web creerán que estás navegando desde este país, dejándote acceder a los contenidos disponibles únicos de allí.

Además de todos los usos mencionados anteriormente también da una capa extra de seguridad, es común que las conexiones VPN vengán acompañadas de un cifrado de los paquetes que se transmiten con ellas, por lo que es normal oír la recomendación de que, si necesitas conectarte a un punto de acceso Wi-Fi público, al menos uses te conectes con una VPN.

Otro uso común de las conexiones VPN se encuentra en las descargas P2P. Las conexiones VPN también tienen usos en la descarga P2P aunque bajes torrents completamente legales. Desgraciadamente cada vez es más común que los proveedores de Internet decidan inmiscuirse en lo que enviamos y recibimos en la Red.

Algunos proveedores bloquean por completo las descargas P2P, mientras que otros simplemente la boicotean para que funcione mal seas tú mismo el que lo deje. Igual que puedes usar una conexión VPN para evitar la censura de tu país, también puedes en ocasiones evitar que tu proveedor de Internet boicotee tus descargas P2P.

1.3 Ventajas de VPN

- Funciona en todas las aplicaciones, ya que enruta todo el tráfico de Internet, a diferencia de los servidores proxy, que sólo puedes usar en el navegador web y un par de aplicaciones más que dejan configurar las opciones de conexión avanzadas.
- Se conecta y desconecta fácilmente, además, una vez configurado, puedes activar y desactivar la conexión cuando quieras.
- Seguridad adicional en puntos de acceso Wifi, siempre y cuando la conexión este cifrada.
- Falseo de tu ubicación, como ya hemos visto en el apartado anterior, una conexión VPN es un modo eficaz de evitar la censura o acceder a contenido limitado a cierta región.
- Tu proveedor de Internet no puede saber a qué te dedicas en Internet. Con una VPN no sabrán a qué te dedicas, pero sí lo sabrá la compañía que gestiona el VPN.

1.4 Inconvenientes de VPN

Usar conexiones VPN parece estar lleno de ventajas: más seguridad, privacidad mejorada, salto de los bloqueos geográficos... Antes de usar un servicio de VPN, hay algunos apartados que debes tener en cuenta:

- El precio. Aunque hay servicios VPN gratuitos, obviamente no puedes esperar mucho de ellos, pues con frecuencia estarán muy limitados, serán muy lentos o no serán muy fiables.
- La velocidad. La diferencia entre conectarte a Internet directamente o que tus datos tracen una ruta que atraviesa medio mundo puede ser abrumadora. Si tu servidor VPN está muy lejos, experimentarás mucha latencia a la hora de navegar por la red. Además de latencia, es normal que la velocidad de descarga y subida máxima estén limitadas.
- Su seguridad no es infalible. Solo porque el icono de la conexión tenga un candado no quiere decir que la conexión sea segura.
- No siempre pueden falsear tu ubicación. Especialmente en el móvil, cada vez hay más tecnologías por las cuales se puede triangular y aproximar tu ubicación más allá de tu dirección IP.
- No te proporcionan anonimato. Usar una VPN no supone que la navegación sea anónima.

2. Creación de la VPN

2.1 Previo a la instalación

Lo primero será disponer de una máquina virtual o anfitrión con Ubuntu. En nuestro caso estamos utilizando la versión 18.04.

Para facilitarnos el trabajo escribe en el terminal de Ubuntu “sudo su”, de esta forma trabajaremos con el superusuario o usuario root y no será necesario tener que estar escribiendo sudo antes de utilizar un comando que necesite permisos de superusuario.

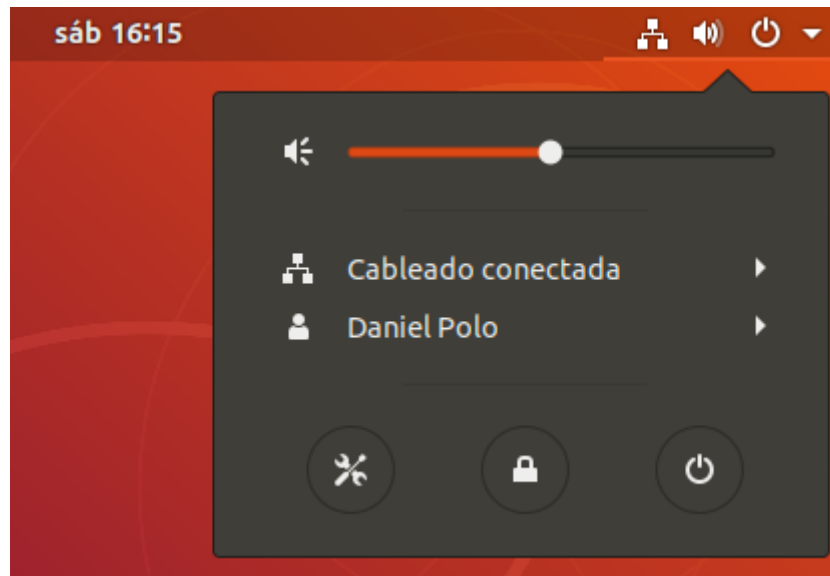
```
danielpolo@danielpolo:~$ sudo su  
root@danielpolo:/home/danielpolo#
```

1. Activación del usuario root.

Antes de comenzar con la instalación es necesario tener la IP estática ya que los clientes no encontrarán al servidor si se asigna de forma dinámica y de esta forma se permite la localización en la red.

Para cambiar la IP en Ubuntu 18.04 nos serviremos del entorno gráfico el cual nos facilitará el proceso.

Vamos a configuración de Ubuntu:



2. Configuración de cableado.

También podemos ir al icono de la barra inferior donde dice «mostrar aplicaciones» y teclear «red» nos aparecerá Configuración de red. Una vez dentro hacemos clic sobre el icono en forma de tuerca.



3. Configuración de cableado.

Nos aparecerá una pantalla con diferentes pestañas. Seleccionamos IPv4 y cambiamos de Automático (DHCP) a Manual y modificamos los parámetros de direcciones poniendo una IP libre de la red de nuestra casa seguido de la máscara de red y la puerta de enlace.



4. Configuración de cableado.

Cuando hayamos realizado las modificaciones clicamos en aplicar para guardar los cambios. Comprobamos escribiendo "ip a" o "ifconfig" en el terminal como ha cambiado la IP.

```
root@danielpolo:/home/danielpolo# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6d:5a:a2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.79/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::7f:47f4:7ca3:b34/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@danielpolo:/home/danielpolo#
```

5. Comprobación cambio de IP.

2.2 Instalación

Antes de empezar con la instalación, actualizaremos los repositorios de Ubuntu “apt-get update”.

Actualizados los repositorios instalaremos el protocolo PPTPD (Point to Point Tunneling Protocol), el cual usaremos para crear nuestro servidor VPN “apt-get install pptpd”.

Espera un poco hasta que se instalen todos los paquetes.

```
root@danielpolo:/home/danielpolo# apt-get update
Des:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88,7 kB]
Obj:2 http://es.archive.ubuntu.com/ubuntu bionic InRelease
Des:3 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease [88,7 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease [74,6 kB]
Descargados 252 kB en 1s (220 kB/s)
Leyendo lista de paquetes... Hecho
root@danielpolo:/home/danielpolo#
```

6. Actualización de repositorios.

```
root@danielpolo:/home/danielpolo# apt-get install pptpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  linux-headers-4.15.0-136 linux-headers-4.15.0-136-generic
  linux-image-4.15.0-136-generic linux-modules-4.15.0-136-generic
  linux-modules-extra-4.15.0-136-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  bcrelay
Se instalarán los siguientes paquetes NUEVOS:
  bcrelay pptpd
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 344 no actualizados.
Se necesita descargar 87,3 kB de archivos.
Se utilizarán 299 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

7. Instalación del protocolo PPTPD.

3. Configuración del servidor

Una vez instalados todos los paquetes necesarios, editaremos el archivo de configuración de pptpd. Para ello escribe “nano /etc/pptpd.conf”. Para guardar las modificación del archivo presiona Ctrl+X para salir y después presiona Y cuando te pregunte si deseas guardar las modificaciones, por último presiona la tecla enter.

```
GNU nano 2.9.3 /etc/pptpd.conf

#####
# $Id$
#
# Sample Poptop configuration file /etc/pptpd.conf
#
# Changes are effective when pptpd is restarted.
#####

# TAG: ppp
#     Path to the pppd program, default '/usr/sbin/pppd' on Linux
#
#ppp /usr/sbin/pppd

# TAG: option
#     Specifies the location of the PPP options file.
#     By default PPP looks in '/etc/ppp/options'
#
option /etc/ppp/pptpd-options

# TAG: debug
#     Turns on (more) debugging to syslog
#
#debug
Buscar: localip
^G Ver ayuda      M-C Mayús/minú  M-B Ir atrás    M-J JustifTodo  ^W Ini de pár.
^C Cancelar      M-R Exp. reg.  ^R Reemplazar   ^T Ir a línea   ^O Fin de pár.
```

8. Edición del archivo de configuración de PPTPD.

Cuando estés dentro del archivo edita la línea localip. Puedes encontrarla al final del fichero. Es necesario quitar la almohadilla (#) ya que esta función sirve para comentar la línea y no se tiene en cuenta a la hora de leer el fichero. Además, sustituye la dirección IP por la IP de tu servidor (la IP que cambiaste antes durante la configuración del cableado).

El siguiente paso es editar la línea que se encuentra justo debajo donde pone remoteip, descoméntala también.

Esta línea define la IP que va a recibir cada ordenador que se conecte a nuestro servidor, esta IP se asigna por medio de un rango el cual establecemos nosotros.

Por defecto se pueden dar un máximo de 4 direcciones.

```
GNU nano 2.9.3 /etc/pptpd.conf Modificado
#       you must type 234-238 if you mean this.
#
#       4. If you give a single localIP, that's ok - all local IPs will
#          be set to the given one. You MUST still give at least one remote
#          IP for each simultaneous client.
#
# (Recommended)
localip 192.168.1.79
remoteip 192.168.1.234-238,192.168.1.245
# or
#localip 192.168.0.234-238,192.168.0.245
#remoteip 192.168.1.234-238,192.168.1.245

^G Ver ayuda  ^O Guardar    ^W Buscar     ^K Cortar Texto^J Justificar
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar txt   ^T Ortografía
```

9. Modificación de localip y remoteip.

Ahora vamos a cambiar el nombre a nuestro servidor, edita el archivo pptpd-options con “nano /etc/ppp/pptpd-options”.

Donde aparece la línea name modifica el nombre por defecto y escribe el de tu servidor VPN, en mi caso se llamará LockVPN.

```
GNU nano 2.9.3 /etc/ppp/pptpd-options Modificado
#####
# $Id$
#
# Sample Poptop PPP options file /etc/ppp/pptpd-options
# Options used by PPP when a connection arrives from a client.
# This file is pointed to by /etc/pptpd.conf option keyword.
# Changes are effective on the next connection. See "man pppd".
#
# You are expected to change this file to suit your system. As
# packaged, it requires PPP 2.4.2 and the kernel MPPE module.
#####

# Authentication

# Name of the local system for authentication purposes
# (must match the second field in /etc/ppp/chap-secrets entries)
name LockVPN

# Optional: domain name to use for authentication
# domain mydomain.net

# Strip the domain prefix from the username before authentication.

^G Ver ayuda  ^O Guardar    ^W Buscar     ^K Cortar Texto^J Justificar
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar txt   ^T Ortografía
```

10. Configuración de cableado.

Busca las líneas en las que aparece `require-mschap-v2` y `require-mppe-128`, asegúrate de que están descomentadas.

- `Require-mschap-v2` sirve para que la conexión entre cliente y servidor sea obligada a pasar por ese protocolo.
- `Require-mppe-128` es el cifrado que va a tener nuestra conexión, tendremos un cifrado de 128 bits de mppe.

```
GNU nano 2.9.3 /etc/ppp/pptpd-options Modificado
#chapms-strip-domain

# Encryption
# (There have been multiple versions of PPP with encryption support,
# choose with of the following sections you will use.)

# BSD licensed ppp-2.4.2 upstream with MPPE only, kernel module ppp_mppe.o
# {{{
refuse-pap
refuse-chap
refuse-mschap
# Require the peer to authenticate itself using MS-CHAPv2 [Microsoft
# Challenge Handshake Authentication Protocol, Version 2] authentication.
require-mschap-v2
# Require MPPE 128-bit encryption
# (note that MPPE requires the use of MSCHAP-V2 during authentication)
require-mppe-128
# }}}

^G Ver ayuda  ^O Guardar    ^W Buscar     ^K Cortar Texto ^J Justificar
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar txt    ^T Ortografía
```

11. Configuración de cableado.

Ahora deberemos buscar `ms-dns`, que es el DNS que utilizarán los ordenadores que se conecten, esto no es necesario, pero si recomendable para que los usuarios puedan conectarse a internet.

Vamos a poner los servidores de Google 8.8.8.8 y 8.8.4.4.

```
GNU nano 2.9.3 /etc/ppp/pptpd-options Modificado

# Network and Routing

# If pppd is acting as a server for Microsoft Windows clients, this
# option allows pppd to supply one or two DNS (Domain Name Server)
# addresses to the clients. The first instance of this option
# specifies the primary DNS address; the second instance (if given)
# specifies the secondary DNS address.
# Attention! This information may not be taken into account by a Windows
# client. See KB311218 in Microsoft's knowledge base for more information.
ms-dns 8.8.8.8
ms-dns 8.8.4.4

# If pppd is acting as a server for Microsoft Windows or "Samba"
# clients, this option allows pppd to supply one or two WINS (Windows
# Internet Name Services) server addresses to the clients. The first
# instance of this option specifies the primary WINS address; the
# second instance (if given) specifies the secondary WINS address.
#ms-wins 10.0.0.3
#ms-wins 10.0.0.4

# Add an entry to this system's ARP [Address Resolution Protocol]
# table with the IP address of the peer and the Ethernet address of this
# system. This will have the effect of making the peer appear to other

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía
```

12. Asignación de servidores DNS de Google.

Hecho esto edita el archivo chap-secrets con “nano /etc/ppp/chap-secrets”. Aquí deberemos escribir el nombre del cliente seguido del nombre del servidor, la contraseña que utilizará el cliente para conectarse y la dirección IP a la que se aplicará estas modificaciones (el asterisco significa que se aplica para todas las IP's), deja una tabulación entre cada uno de estos cambios.

```
GNU nano 2.9.3 /etc/ppp/chap-secrets

# Secrets for authentication using CHAP
# client      server  secret          IP addresses
cliente LockVPN 1234 *
```

13. Modificación del archivo chap-secrets.

Edita el fichero sysctl.conf “nano /etc/sysctl.conf” y descomenta la línea en la que aparece net.ipv4.ip_forward=1.

```
GNU nano 2.9.3 /etc/sysctl.conf Modificado

# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

Búsqueda recomendada

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía
```

14. Modificación del archivo sysctl.conf.

Ahora escribe “nano /etc/rc.local”. Aquí crearemos la excepción de las iptables.

Iptables es la forma de introducir reglas en el firewall y sirven para que cliente y servidor puedan conectarse entre ellos y salir a internet.

Deja el fichero tal que así con tu IP de origen e interfaz de red.

```
GNU nano 2.9.3 /etc/rc.local Modificado

#!/bin/bash
iptables -t nat -A POSTROUTING -s 192.168.1.1/24 -o eth0 -j MASQUERADE
exit 0
```

15. Creación de iptables en rc.local.

Por último otorga permisos de ejecución con “chmod +x /etc/rc.local” y actívalo con “systemctl enable rc-local”.

```
root@danielpolo:/home/danielpolo# chmod +x /etc/rc.local
root@danielpolo:/home/danielpolo# systemctl enable rc-local
Created symlink /etc/systemd/system/multi-user.target.wants/rc-local.service →
/etc/systemd/system/rc-local.service.
root@danielpolo:/home/danielpolo# █
```

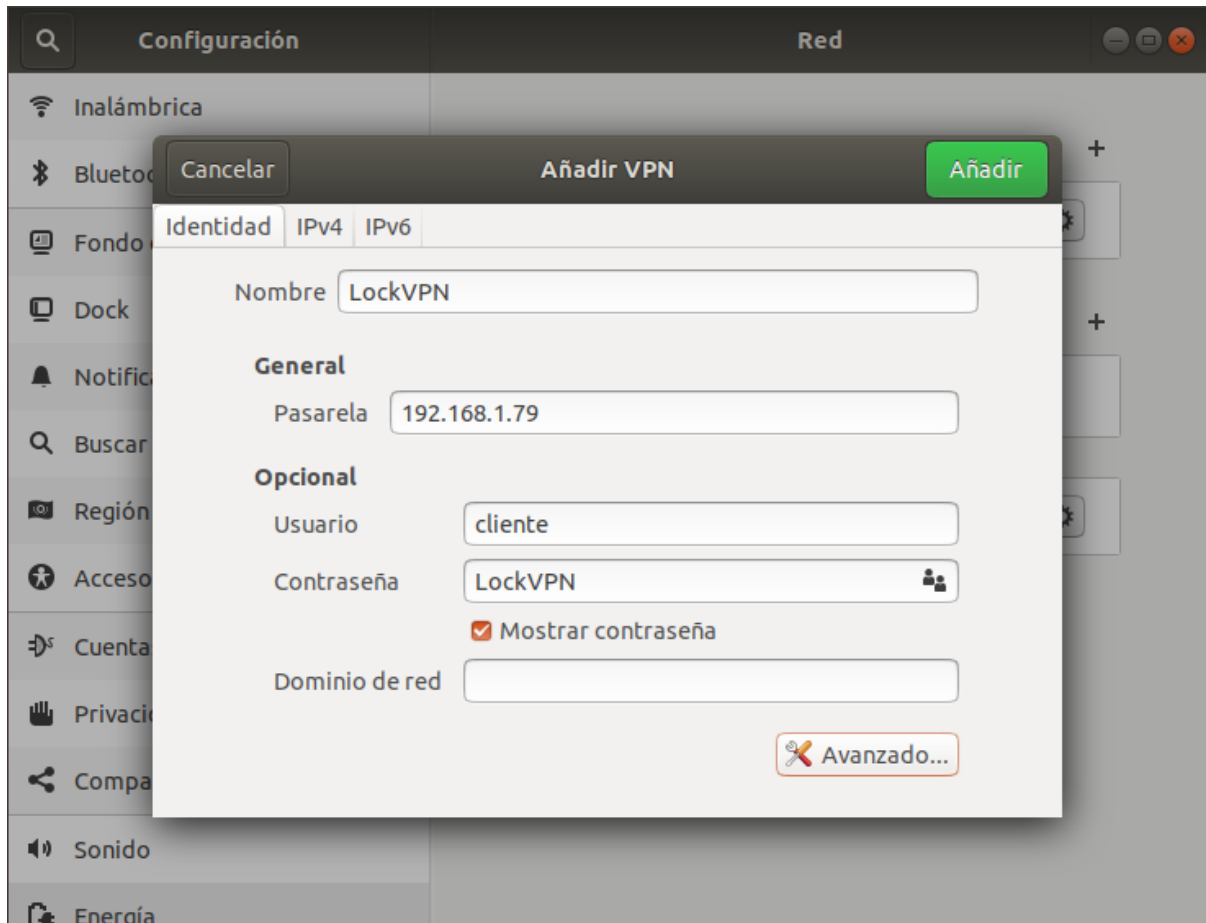
16. Activación y permisos de ejecución.

La configuración del servidor ha finalizado.

4. Prueba de funcionamiento

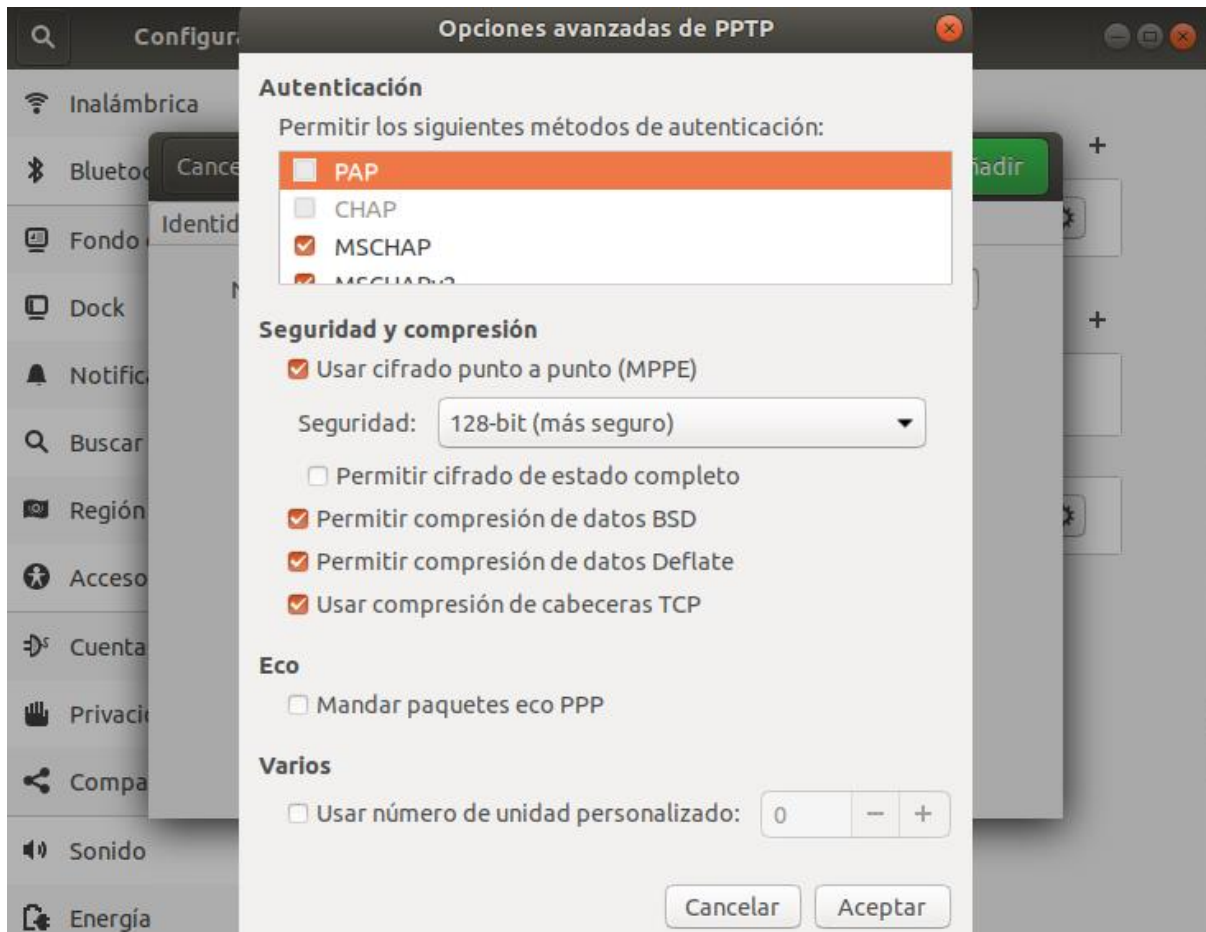
4.1 Ubuntu

Ahora prueba a añadir la VPN en otra máquina virtual con los parámetros que añadiste en los pasos anteriores.



17. Modificación del archivo `sysctl.conf`.

Después ve a los ajustes avanzados y deja los parámetros como en la siguiente captura:

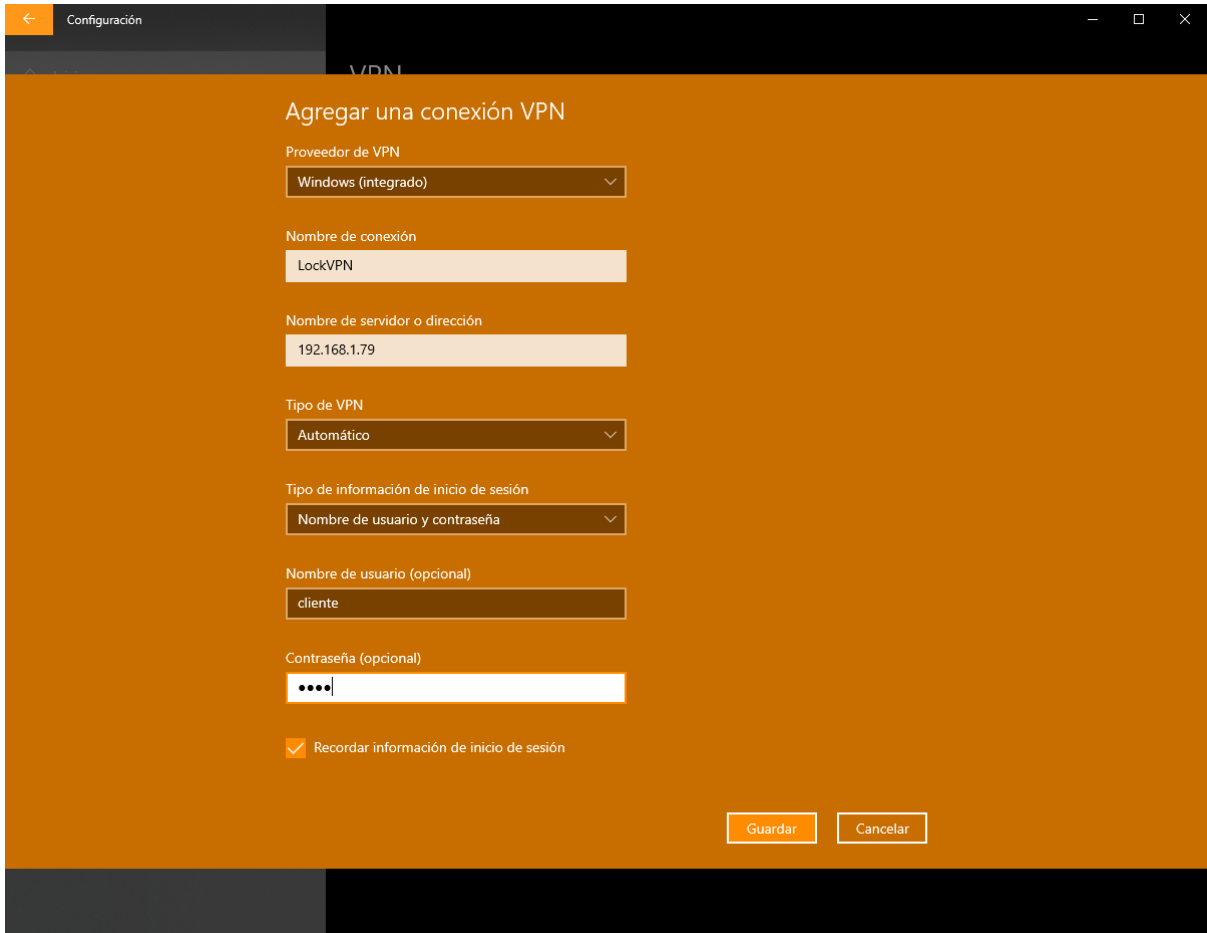


18. Opciones avanzadas de PPTP.

Si has realizado todos los pasos correctamente podrás conectarte a tu servidor VPN, ten en cuenta que el servidor debe estar encendido con el servicio PPTPD activo en todo momento, de lo contrario los clientes no podrán conectarse al servidor ya que no lo encontrarán.

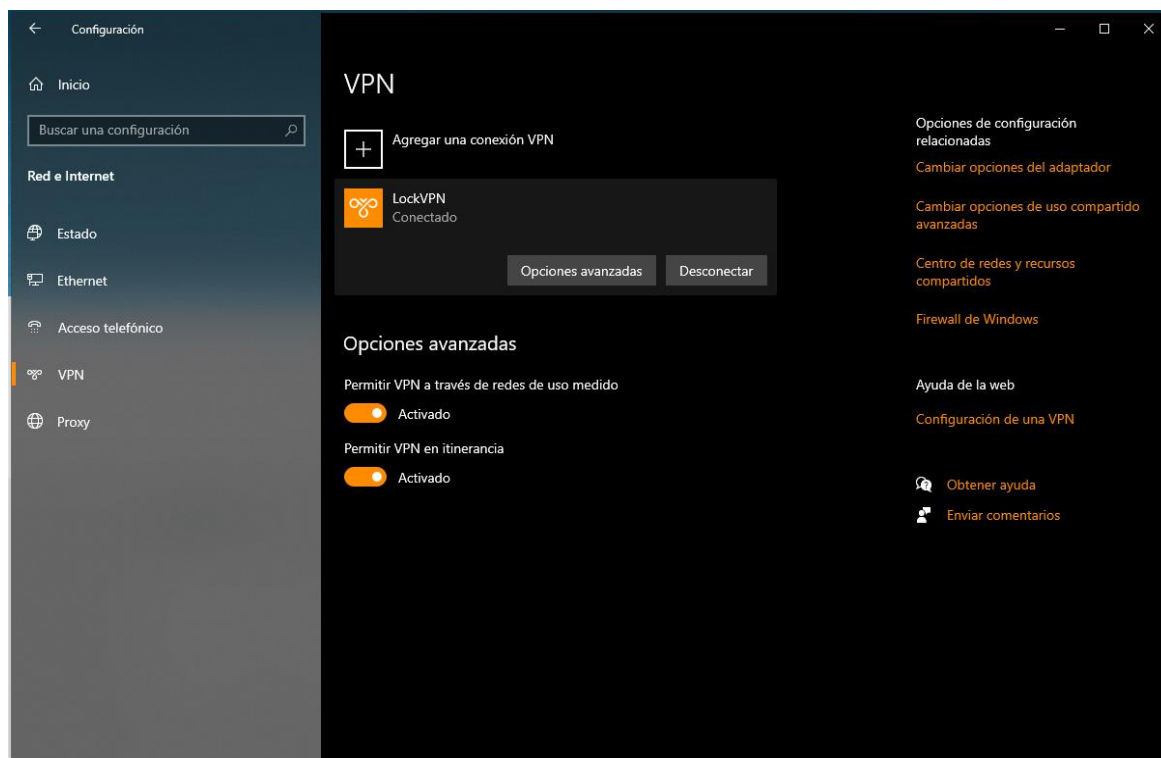
4.2 Windows

Ve a la configuración de tu Windows y en red e internet entra en VPN, a continuación, agrega una nueva conexión VPN con los parámetros añadidos anteriormente.



19. Agregar conexión VPN en Windows.

Como se puede ver la VPN ha sido agregada correctamente y se ha establecido la conexión con el servidor.



20. Agregar conexión VPN en Windows.

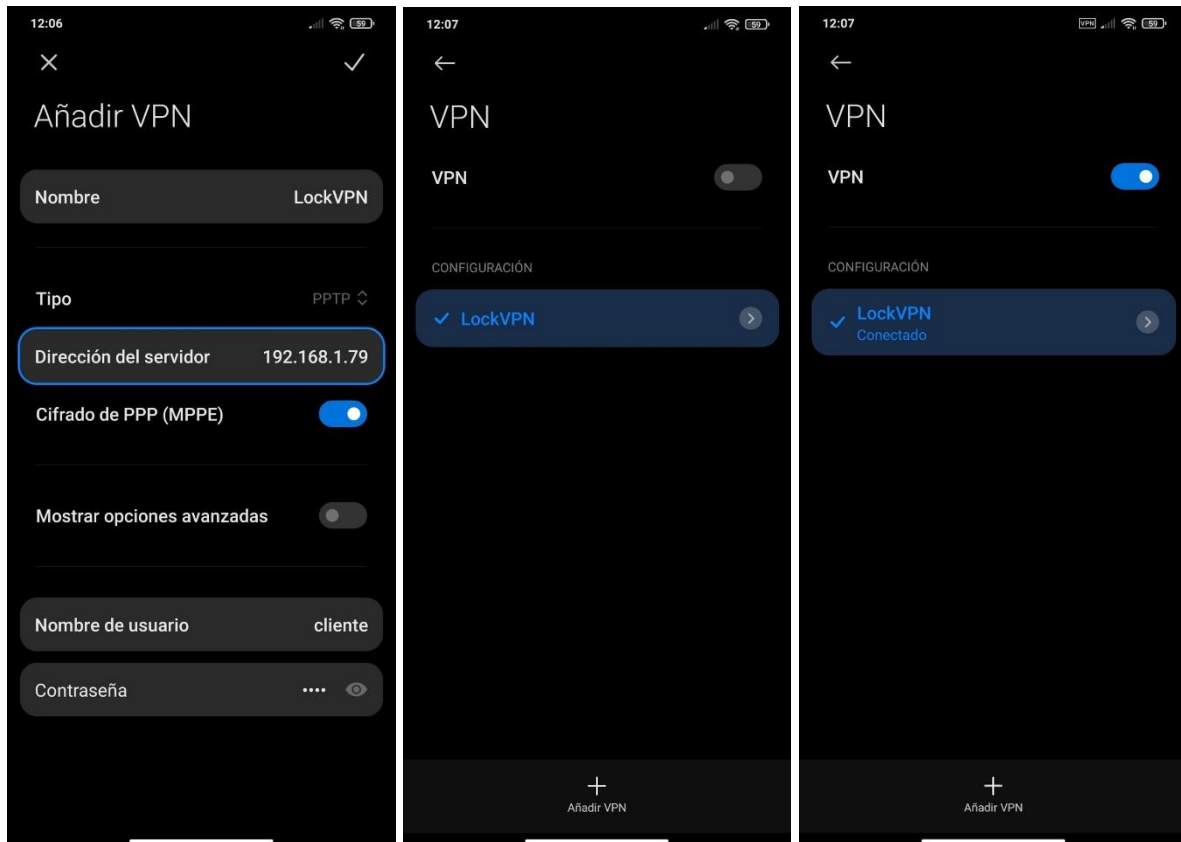
También podemos ver como la dirección IP se ha modificado. Al haberse conectado a la VPN, el servidor le ha otorgado una nueva IP entre el rango que tenía disponible.



21. Comprobación cambio de IP en Windows.

4.3 Android

Selecciona la opción de añadir una VPN y rellena los parámetros como en los pasos anteriores, después activa la utilización de la VPN y estarás conectado con el servidor.



5. Bibliografía

<https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene>

<https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion>

<https://geekland.eu/crear-un-servidor-vpn-pptp/>

https://www.youtube.com/watch?v=JBS9o6LliM0&ab_channel=JavierdePrado