



FACULTAD CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACION

Cátedra: *Redes II*

Tema: *“VPN con GNU / Linux”*

Catedrático: *Ing. Manuel Flores Villatoro*

Presentado por:

<i>Nombres</i>	<i>Apellidos</i>	<i>N° Carnet</i>	<i>Participación</i>
<i>Isabel Guadalupe</i>	<i>Hernández Peña</i>	<i>HP02110790</i>	<i>100%</i>
<i>Mauricio Edgardo</i>	<i>Vasquez Cerón</i>	<i>VC02110805</i>	<i>100%</i>

San Salvador, 30 de noviembre de 2013

Contenido

1. Introducción.....	2
2. Objetivos.....	3
3. PPTPD.....	3
La Especificación PPTP.....	3
4. Configuración del servidor.....	9
5. Configuración de los clientes.....	17
6. Diagrama de GANT.....	24
7. Conclusiones.....	24
8. Recomendaciones.....	24
9. Bibliografía.....	25

1. Introducción

En el presente documento se describe las configuraciones de el proyecto de instalación y configuración de VPN con GNU / LINUX.

Para el proyecto antes mencionado se utilizará solo software libre se inicio configurando Open VPN debido a que no alcanzamos el objetivo propuesto, optamos por utilizar el protocolo PPTPD point-to-point tunneling protocol, el cual permite intercambio de datos de un cliente a un servidor formando un VPN o mejor conocida “red privada virtual”.

Basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada.

Esta tecnología que hace posible el PPTP es una extensión del acceso remoto del PPP (point-to-point-protocol.....RFC 1171). La tecnología PPTP encapsula los paquetes ppp en datagramas IP para su transmisión bajo redes basadas en TCP/IP. El PPTP es ahora mismo un boceto de protocolo esperando por su estandarización.

2. Objetivos

- **Objetivo General**

- *Detallar los avances obtenidos hasta la fecha en la instalación y configuración de VPN con GNU / LINUX.*

- **Objetivos Específicos**

- *Describir el proyecto que se está desarrollando.*
- *Detallar las herramientas a ser utilizadas.*
- *Documentación y análisis de los resultados.*

3. PPTPD

La Especificación PPTP

La especificación para PPTP fue publicada por el RFC 2637, aunque no ha sido ratificada como estándar por el IETF.

Point-To-Point Tunneling Protocol (PPTP) permite el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual (VPN, por el anglicismo Virtual Private Network), basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada.

Esta tecnología que hace posible el PPTP es una extensión del acceso remoto del PPP (point-to-point-protocol.....RFC 1171). La tecnología PPTP encapsula los paquetes ppp en datagramas IP para su transmisión bajo redes basadas en TCP/IP. El PPTP es ahora mismo un boceto de protocolo esperando por su estandarización. Las compañías "involucradas" en el desarrollo del PPTP son Microsoft, Ascend Communications, 3com / Primary Access, ECI Telematics y US Robotics.

PPTP y VPN: El protocolo Point-To-Point Tunneling Protocol viene incluido con WindowsNT 4.0 Server y Workstation. Los Pc`s que tienen corriendo dentro de ellos este protocolo pueden usarlo para conectar con toda seguridad a una red privada como un cliente de acceso remoto usando una red pública como Internet.

Una característica importante en el uso del PPTP es su soporte para VPN. La mejor parte de esta característica es que soporta VPN's sobre public-switched telephone networks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

Usando PPTP una compañía puede reducir en un gran porcentaje el coste de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones cifradas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

Vulnerabilidades de PPTP

La seguridad de PPTP ha sido completamente rota y las instalaciones con PPTP deberían ser retiradas o actualizadas a otra tecnología de VPN. La utilidad ASLEAP puede obtener claves de sesiones PPTP y descifrar el tráfico de la VPN. Los ataques a PPTP no pueden ser detectados por el cliente o el servidor porque el exploit es pasivo.

El fallo de PPTP es causado por errores de diseño en la criptografía en los protocolos handshake LEAP de Cisco y MSCHAP-v2 de Microsoft y por las limitaciones de la longitud de la clave en MPPE.

Distribución Standard del PPTP

En la práctica general hay normalmente tres ordenadores involucrados en una distribución:

- Un cliente PPTP
- Un servidor de acceso a la red
- Un server PPTP

NOTA: El servidor de acceso a la red es opcional, y no es necesario para la distribución PPTP. En la distribución normal quizás, están presentes.

En una distribución típica de PPTP comienza por un PC remoto o portátil que será el cliente PPTP. Este cliente PPTP necesita acceso a la red privada (private network) utilizando un ISP (internet service provider). Los clientes que usan WindowsNT Server o Workstation como S.O. usaran el Dial-up networking y el protocolo PPP para conectar a su ISP. Son también conocidos como Front-End Processors (FEP`s) o Point-Of-Presence servers (POP`s). Una vez conectados, el cliente tiene la capacidad de extraer datos de Internet. Los "network access servers" usan el protocolo TCP/IP para el mantenimiento de todo el tráfico.

Después que el cliente ha hecho la conexión PPP inicial al ISP, la segunda llamada Dial-up es hecha a través de la conexión PPP ya establecida. Los datos enviados usando la segunda conexión son en forma de datagramas IP que contienen paquetes PPP. Es la segunda llamada la que crea la conexión VPN a un servidor PPTP en la red privada de la compañía. Esto es llamado un TUNEL.

El Tunneling es el proceso de intercambio de datos de un ordenador en una red privada de trabajo enrutándolos sobre otra red. Los otros enrutamientos de la otra red no pueden acceder porque esta en la red privada. Sin embargo, el tunneling activa el enrutamiento de la red para transmitir el paquete a un ordenador intermediario, como un server PPTP .Este server PPTP esta conectado a ambas, a la red privada de la compañía y a la red de enrutamiento, que en este caso es Internet. Ambos ,el cliente PPTP y el server PPTP usan el tunneling para transmitir paquetes de forma segura a un ordenador en la red privada.

Cuando el server PPTP recibe un paquete de la red de enrutamiento (Internet) lo envía a través de la red privada hasta el ordenador de destino. El server PPTP hace esto procesando el paquete PPTP para obtener el nombre del ordenador de la red privada o la información de la dirección que esta encapsulada en el paquete PPP.

NOTA: El paquete PPP encapsulado puede contener datos multi-protocolo como TCP/IP,IPX/SPX o NetBEUI.Debido a que el servidor PPTP esta configurado para comunicar a través de la red privada usando protocolos de esta red privada ,es capaz de entender Multi-Protocolos.

PPTP encapsula el encriptado y comprimido paquete PPP en datagramas IP para su transmisión a través de Internet. Estos datagramas IP son enrutados a través de Internet como un paquete PPP y después son desenscriptados usando el protocolo de red de la red privada. Como mencionamos antes, los protocolos soportados por el PPTP. son...TCP/IP, IPX/SPX y NetBEUI.

PPTP Clients

Un ordenador que es capaz de usar el protocolo PPTP puede conectarse a un servidor PPTP de dos maneras diferentes:

- Usando un ISP que soporte las conexiones PPP
- Usando una red con soporte para TCP/IP para conectar a un server PPTP

Los clientes PPTP que quieran usar un ISP deben estar perfectamente configurados con un módem y un dispositivo VPN para hacer las pertinentes conexiones al ISP y al server PPTP. La primera conexión es dial-up usando el protocolo PPP a través del módem a un ISP. La segunda conexión requiere la primera conexión porque el túnel entre el dispositivo VPN es establecido usando el módem y las conexiones PPP a Internet.

La excepción a estos dos procesos de conexión es usar PPTP para crear una VPN entre ordenadores físicamente conectados a una LAN. En este escenario, el cliente está de hecho conectado a una red y solo usa dial-up networking con un dispositivo VPN para crear la conexión a un server PPTP en la LAN.

Los paquetes PPTP remotos de un cliente PPTP y una LAN local PPTP son procesados de diferente manera. Un paquete PPTP de un cliente remoto es puesto en el dispositivo de telecomunicación de medio físico, mientras que el paquete PPTP de la LAN PPTP es puesto en el adaptador de red de medio físico.

Arquitectura PPTP

La siguiente área expone la arquitectura del PPTP sobre WindowsNT server 4.0 y NT Workstation 4.0. La siguiente sección abarca:

- Protocolo PPTP
- Control de conexión PPTP
- Tunneling de datos PPTP

Vista por encima de la arquitectura:

La comunicación segura que es establecida usando PPTP involucra tres procesos, cada uno de los cuales requiere la completa realización del proceso anterior. Ahora explicaremos estos procesos y como funcionan:

1. **Conexión y Comunicación PPTP:** Un cliente PPTP utiliza PPP para conectarse a un ISP usando una línea telefónica normal o una línea RDSI. Esta conexión usa el protocolo PPP para establecer la conexión y encriptar los paquetes de datos.
2. **Control de Conexión PPTP:** Usando la conexión a Internet establecida por el protocolo PPP, el PPTP crea una conexión controlada del cliente PPTP al server PPTP en Internet. Esta conexión usa TCP para establecer la comunicación y está llamada PPTP Tunnel.
3. **Tunneling de datos PPTP:** El protocolo PPTP crea datagramas IP conteniendo paquetes PPP encriptados que son enviados a través del Tunnel PPTP al PPTP server. El server PPTP desensambla los datagramas IP y

desencripta los paquetes PPP, y los enrutamientos los paquetes desencriptados a la red privada.

PPP Protocol:

No trataremos información profunda sobre el PPP. sino sobre el papel que juega el PPP en el medio PPTP. El PPP es un protocolo de acceso remoto usado por el PPTP para enviar datos a través de redes basadas en TCP/IP. El PPP encapsula paquetes IP, IPX y NetBEUI entre marcos PPP y envía los paquetes encapsulados creando un link point-to-point entre los ordenadores de origen y destino.

Muchas de las sesiones PPTP comienzan con la llamada de un cliente y un ISP. El protocolo PPP es usado para crear la conexión entre el cliente y el servidor de acceso a la red y presenta las siguientes funciones:

- 1. **Establece y termina la conexión física.** El protocolo PPP usa una secuencia definida en el RFC 1661 para establecer y mantener la conexión entre dos ordenadores remotos*
- 2. **Autentifica usuarios.** Los clientes PPTP son autenticados usando PPP. Limpieza de texto, encriptado o MS-CHAP pueden ser usados por el protocolo PPP.*
- 3. **Crea datagramas PPP.** Que contienen paquetes IPX,NetBEUI o TCP/IP*

Control de conexión PPTP

El protocolo PPTP especifica una serie de mensajes que son usados para la sesión de control. Estos mensajes son enviados entre el cliente PPTP y el servidor PPTP. Los mensajes de control establecidos, mantienen y terminan el Tunnel PPTP. La siguiente lista presenta el control primario de mensajes usados para establecer y mantener la sesión PPTP:

Message Type Purpose

PPTP_START_SESSION_REQUEST Starts Session

PPTP_START_SESSION_REPLY Replies to Start Session Request

PPTP_ECHO_REQUEST Maintains Session

PPTP_ECHO_REPLY Replies to Maintain Session Request

PPTP_WAN_ERROR_NOTIFY Reports an error in the PPP connection

PPTP_SET_LINK_INFO Configures PPTP Client / Server Connection

PPTP_STOP_SESSION_REQUEST Ends Session

PPTP_STOP_SESSION_REPLY Replies to End Session Request

Los mensajes de control son enviados dentro de los paquetes de control en un datagrama TCP. Una conexión TCP es activada entre el cliente PPTP y el server. Este path es usado para enviar y recibir mensajes de control. El datagrama contiene una cabecera PPP, una TCP, un mensaje de control PPTP y sus apropiadas reglas. La construcción es como sigue:

<i>PPP Delivery Header</i>
<i>IP Header</i>
<i>PPTP Control Message</i>
<i>Trailers</i>

Transmisión de datos PPTP

Después de que el Tunnel PPTP ha sido creado, los datos del usuario son transmitidos entre el cliente y el server PPTP. Los datos son enviados en datagramas IP conteniendo paquetes PPP. El datagrama IP es creado usando una versión modificada de la versión de Generic Routing Encapsulation (GRE) protocol (RFC1701-2). La estructura de datagrama IP es:

<i>PPP Delivery Header</i>
<i>IP Header</i>
<i>GRE Header</i>
<i>PPP Header</i>
<i>IP Header</i>
<i>TCP Header</i>
<i>Data</i>

Prestando atención a la construcción del paquete, podrás ver como es capaz de ser transmitido a través de Internet desmenuzando las cabeceras. La cabecera de envío del PPP proporciona información necesaria para el datagrama para atravesar Internet. La cabecera GRE es usada para encapsular el paquete PPP sin el datagrama IP. El paquete PPP es creado por RAS. El paquete PPP es encriptado y si es interceptado, será ilegible.

Entendiendo la seguridad PPTP

El PPTP usa la estricta autenticación y encriptacion de seguridad disponible por los ordenadores que corren RAS bajo WindowsNT Server v4.0.El PPTP puede también proteger el server PPTP y la red privada ignorando todo excepto el trafico PPTP. A pesar de esta seguridad es fácil configurar un firewall para permitir al PPTP acceder a la red interna.

Autenticación:

La autenticación inicial en la llamada puede ser requerida por un ISP de servidor de acceso a la red. Un servidor PPTP es un gateway a tu red, y necesita la base estándar de "login" de WindowsNT. Todos los clientes PPTP deben proporcionar un login y password. De todas formas, el login de acceso remoto usando un PC bajo NT server o Workstation es tan seguro como hacer un login en un PC conectado a una LAN (teóricamente). La autenticación de los clientes remotos PPTP es hecha usando los mismos métodos de autenticación PPP usados para cualquier cliente RAS llamando directamente en un NT Server. Porque esto, soporta completamente MS-CHAP.

Control de acceso:

Después del "auth", todo el acceso a la LAN privada continúa usando las estructuras de seguridad basadas en NT. El acceso a recursos en dispositivos NTFS o otros recursos de la red requieren los permisos correctos, tal como si estuvieses conectado dentro de la LAN.

Encriptación de los datos:

Para la encriptación de datos, el PPTP usa el proceso de encriptación RAS "shared secret". Es referido a un "shared-secret" porque ambos terminan la conexión "sharing" the encryption key. Bajo la implementación del RAS de MS, el secreto "shared" es el pass del usuario (Otros métodos incluyen llave pública de encriptación. El PPTP usa la encriptación PPP y los métodos de compresión PPP. El CCP (Compression Control Protocol es usado para negociar la encriptación usada. El nombre de usuario y el passwd esta disponible al server y sustituida por el cliente. Una llave de encriptación es generada usando una mínima parte del passwd situados en cliente y server. El RSA RC4 standard es usado para crear estos 40 bits (128 dentro de EEUU y Canada) de llave de sesión basada en el passwd de un cliente. Esta llave es después usada para encriptar y desencriptar todos los datos intercambiados entre el server PPTP y el cliente. Los datos en los paquetes PPP son encriptados. El paquete PPP que contiene un bloque de datos encriptados es después metido en un largo datagrama IP para su ruteo.

Filtrado de paquetes PPTP:

La seguridad de la red contra intrusos puede ser mejorada activando el filtro PPTP en el server PPTP. Cuando el filtro PPTP esta activado, el server PPTP en la red privada acepta y rutea solo paquetes PPTP. Esto previene de todos los tipos de paquetes de la red entera. El tráfico PPTP usa el puerto 1723.

4. Configuración del servidor

- Tener una dirección estática
- Router debe tener puerto PPTP(1723 TCP) abierto
- Iniciamos una terminal



Instalar los paquetes

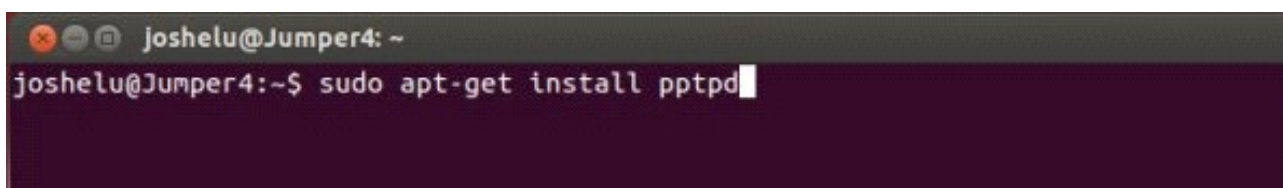
En el terminal tecleamos la siguiente orden:

```
sudo apt-get install pptpd
```

Una vez tecleada pulsamos **ENTER** para que se ejecute. Ahora vamos a ver **qué significa** cada una de las palabras:

- **sudo**: Dice al sistema que ejecute lo que le sigue como administrador.
- **apt-get**: Programa encargado de gestionar los paquetes del sistema.
- **install**: Parámetro que dice a apt-get que deseamos instalar paquetes.
- **pptpd**: Paquete a instalar, en este caso el servidor de PPTP.

Dado que el comando se ejecutará como administrador, el sistema **pedirá nuestra contraseña** de usuario. Para mayor seguridad **no se mostrará ningún tipo de símbolo** en la pantalla mientras escribimos dicha contraseña.



En este caso, apt-get ha detectado que para que se pueda instalar el paquete **pptpd** necesita, además, el paquete **bcrelay**. Antes de realizar acción alguna pide **nuestra aprobación**. Dado que estamos de acuerdo presionamos la tecla “S” y luego **ENTER** para que comience la **descarga y posterior instalación** de los paquetes.

```
joshelu@Jumper4: ~
joshelu@Jumper4:~$ sudo apt-get install pptpd
[sudo] password for joshelu:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  bcrelay
Se instalarán los siguientes paquetes NUEVOS:
  bcrelay pptpd
0 actualizados, 2 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 95,2 kB de archivos.
Se utilizarán 330 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s
```

Configuración

Una vez finalizado el proceso se iniciará el servidor PPTP automáticamente, pero aún no está configurado, para lo cual ejecutaremos:

```
sudo nano /etc/pptpd.conf
```

Al igual que hicimos con la orden anterior, procedemos a su **explicación**:

- **sudo**: Dice al sistema que ejecute lo que le sigue como administrador.
- **nano**: editor de texto para terminal. Hay cientos de editores pero creo que este es de los más sencillos de utilizar.
- **/etc/pptpd.conf**: Ruta absoluta del archivo que queremos modificar.

```
Joshelu@Jumper4: ~
untu2 [11,2 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu/ precise/main pptpd amd64 1.3.4-5ubun
tu2 [84,0 kB]
Descargados 95,2 kB en 1seg. (56,7 kB/s)
Seleccionando paquete bcrelay previamente no seleccionado
(Leyendo la base de datos ... 170093 ficheros o directorios instalados actualme
nte.)
Desempaquetando bcrelay (de ../bcrelay_1.3.4-5ubuntu2_amd64.deb) ...
Seleccionando paquete pptpd previamente no seleccionado
Desempaquetando pptpd (de ../pptpd_1.3.4-5ubuntu2_amd64.deb) ...
Procesando disparadores para ureadahead ...
ureadahead will be reprofiled on next reboot
Procesando disparadores para man-db ...
Configurando bcrelay (1.3.4-5ubuntu2) ...
Configurando pptpd (1.3.4-5ubuntu2) ...
Starting PPTP Daemon: pptpd.
joshelu@Jumper4:~$ sudo nano /etc/pptpd.conf
```

Tras ejecutarlo aparecerá **en la misma ventana** del terminal el editor nano. Usando los cursores bajamos hasta **el final del todo e insertamos**, como si se tratara del bloc de notas, las líneas (en la captura la hemos seleccionado para distinguirlas del resto del texto):

```
localip 10.10.10.1
```

```
remoteip 10.10.10.100-200,10.10.10.245
```

Explicación:

- **Primera línea:** Especificamos cuál será **la dirección IP de nuestro servidor** dentro de la VPN. Para que no haya conflicto con las direcciones IP “domésticas”, hemos **seleccionado un rango de direcciones distinto**.
- **Segunda línea:** Especifica el **rango de direcciones** que usaremos para asignar **a los clientes**. En la parte anterior a la “,” (coma) hemos especificado un rango y detrás una dirección simple. Con esto hemos querido mostraros las **dos posibles formas** de especificar las direcciones de los clientes, es decir, que podéis especificar simplemente un rango.

Para guardar los cambios presionamos “**Control + O**” y para salir “**Control + X**”.

```
joshelu@Jumper4: ~
GNU nano 2.2.6 Archivo: /etc/pptpd.conf
#           be set to the given one. You MUST still give at least one$
#           IP for each simultaneous client.
#
# (Recommended)
#localip 192.168.0.1
#remoteip 192.168.0.234-238,192.168.0.245
# or
#localip 192.168.0.234-238,192.168.0.245
#remoteip 192.168.1.234-238,192.168.1.245
localip 10.10.10.1
remoteip 10.10.10.100-200,10.10.10.245

^G Ver ayud^O Guardar ^R Leer Fic^Y RePág. ^K Cortar T^C Pos actual
^X Salir ^J Justific^W Buscar ^V Pág. Sig^U PegarTxt^T Ortografía
```

Añadiendo usuarios

Ahora vamos a añadir usuarios a nuestra VPN. Para hacerlo **modificaremos el archivo chap-secrets:**

```
sudo nano /etc/ppp/chap-secrets
```

Añadiendo usuarios

Ahora vamos a añadir usuarios a nuestra VPN. Para hacerlo **modificaremos el archivo chap-secrets:**

```
sudo nano /etc/ppp/chap-secrets
```

```
joshelu@Jumper4: ~
joshelu@Jumper4:~$ sudo nano /etc/ppp/chap-secrets
```

Formato (cada espacio es en realidad una tabulación):

*nombre_de_usuario pppd contraseña **

En nuestro **ejemplo** hemos usado los siguientes pares **usuario/contraseña**:

- **usuariovpn / password**
- **usuario2 / 12345**

Ahora guardamos y salimos, ya sabéis “**Control + O**” y “**Control + X**”

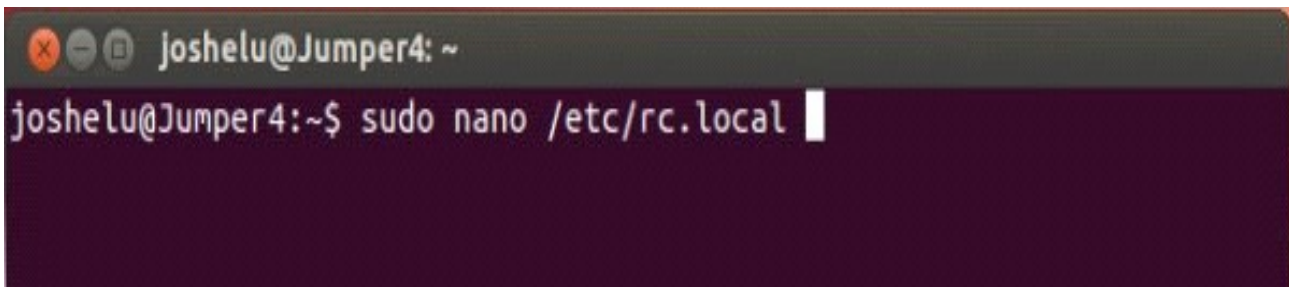
```
joshelu@Jumper4: ~
GNU nano 2.2.6 Archivo: /etc/ppp/chap-secrets
# Secrets for authentication using CHAP
# client      server  secret          IP addresses
usuariovpn    pptpd   password        *
usuario2      pptpd   12345           *
```

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar T ^C Pos actual
^X Salir ^J Justific ^W Buscar ^V Pág. Sig ^U PegarTxt ^T Ortografía

Configurando iptables

Hasta este punto ya tenemos todo lo referente a **nuestra VPN configurado**, tan sólo queda **configurar el cortafuegos** de Ubuntu para que permita el acceso a las conexiones entrantes y **redirija el tráfico**. Para que la configuración **se mantenga** con cada reinicio modificaremos el script **rc.local**:

```
sudo nano rc.local
```



```
joshelu@Jumper4: ~  
joshelu@Jumper4:~$ sudo nano /etc/rc.local
```

Vamos hasta el final del fichero e **insertamos ANTES** de la última línea lo siguiente:

```
iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -o eth0 -j MASQUERADE
```

A tener en cuenta:

- **10.10.10.0/24** : Rango de direcciones que elegimos cuando estábamos configurando PPTPD.
- **eth0** : Nombre de la interfaz de red. En nuestro caso se trata de **cable**, si fuera **WiFi** recibiría el nombre de **wlan0** .

Una vez realizados los cambios, **cerramos y guardamos** como hasta ahora.

```
joshelu@Jumper4: ~
GNU nano 2.2.6 Archivo: /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -o eth0 -j MASQUERADE
exit 0
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar T ^C Pos actual
^X Salir ^J Justific ^W Buscar ^V Pág. Sig ^U PegarT xt ^T Ortografía
```

Ahora vamos a proceder a activar el IP forwarding, para ello vamos a modificar el archivo `/etc/sysctl.conf`:

```
sudo nano /etc/sysctl.conf
```

```
joshelu@Jumper4: ~
joshelu@Jumper4:~$ sudo nano /etc/sysctl.conf
```

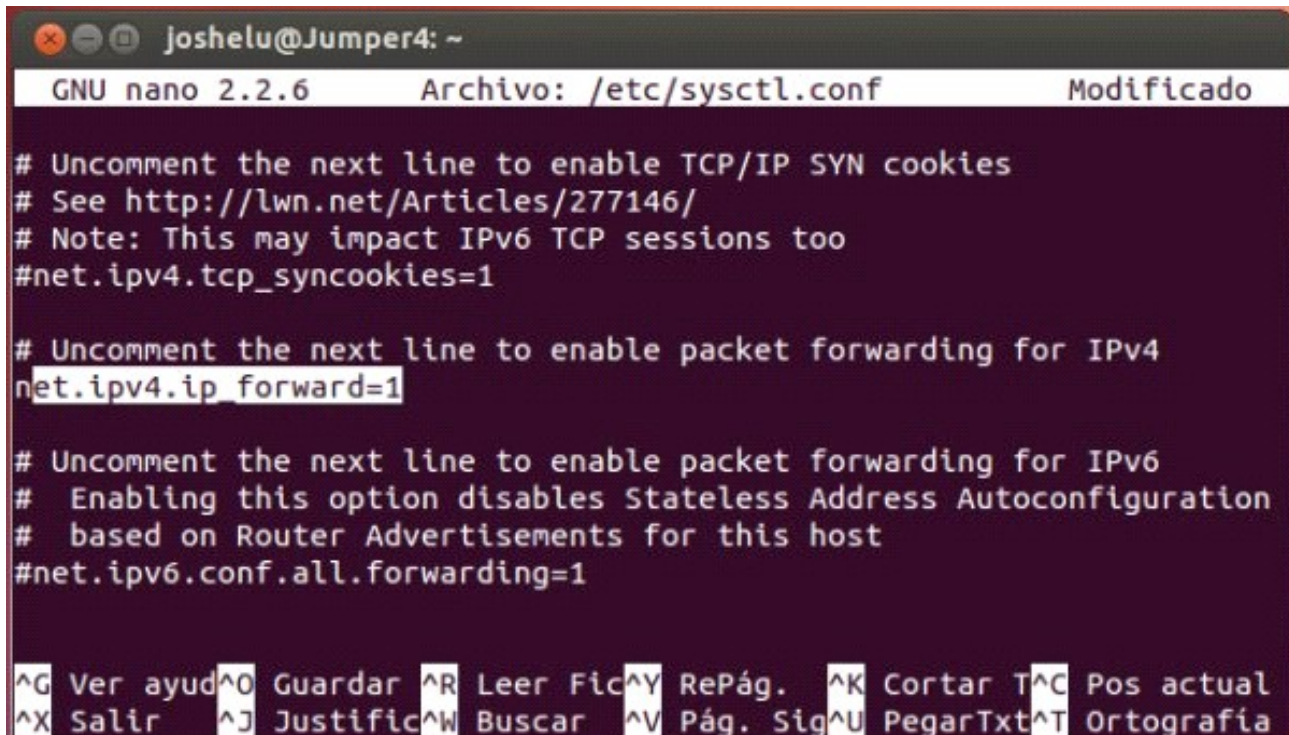
Buscamos la línea:

```
#net.ipv4.ip_forward=1
```

Y le **quitamos la #**:

```
net.ipv4.ip_forward=1
```


Guardamos los cambios y **cerramos** el archivo.



```
Joshelu@Jumper4: ~
GNU nano 2.2.6 Archivo: /etc/sysctl.conf Modificado

# 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

^G Ver ayud^O Guardar ^R Leer Fic^Y RePág. ^K Cortar T^C Pos actual
^X Salir ^J Justific^W Buscar ^V Pág. Sig^U PegarTxt^T Ortografía
```

Aunque en un principio podríamos aplicar los cambios **sin necesidad de reiniciar** el ordenador, creo que es interesante **verificar que después de reiniciar** todo continúa funcionando perfectamente. Así que vamos a reiniciar el ordenador desde el propio terminal:

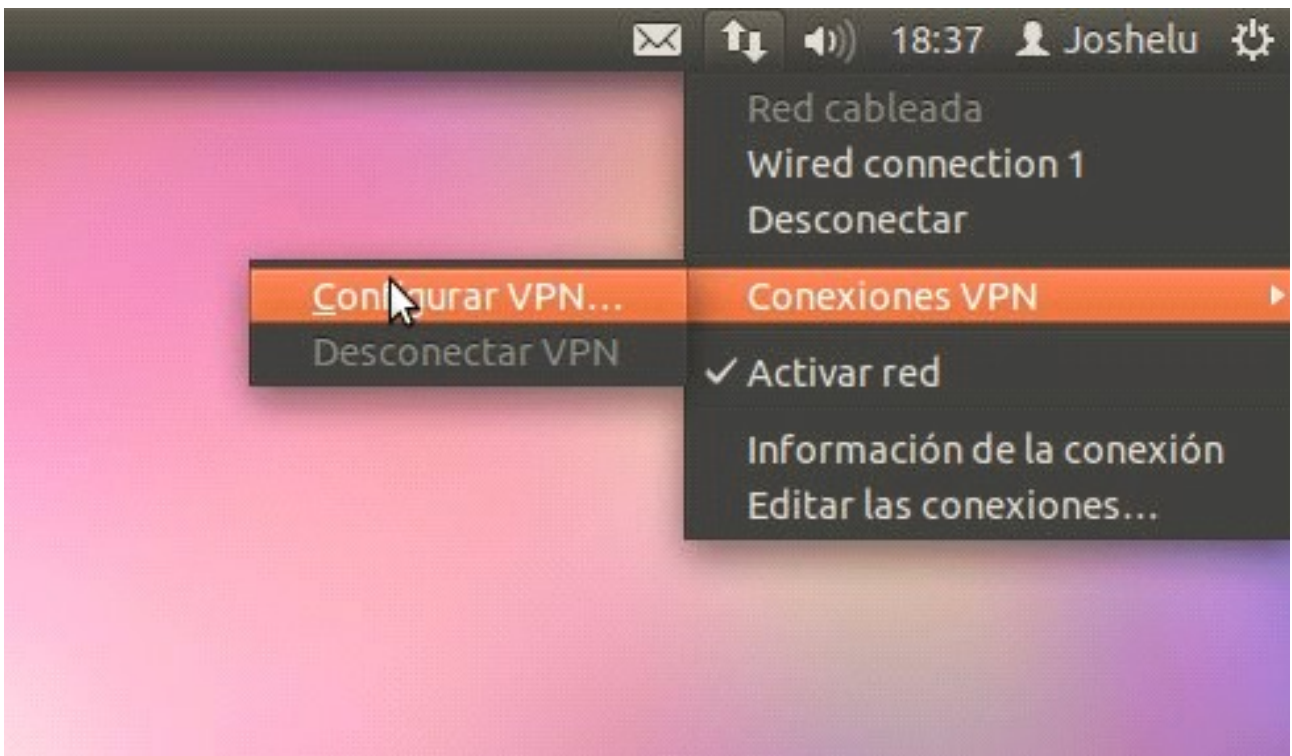
```
sudo telinit 6
```

Listo, ya sólo queda **configurar los clientes** y disfrutar de nuestra VPN.

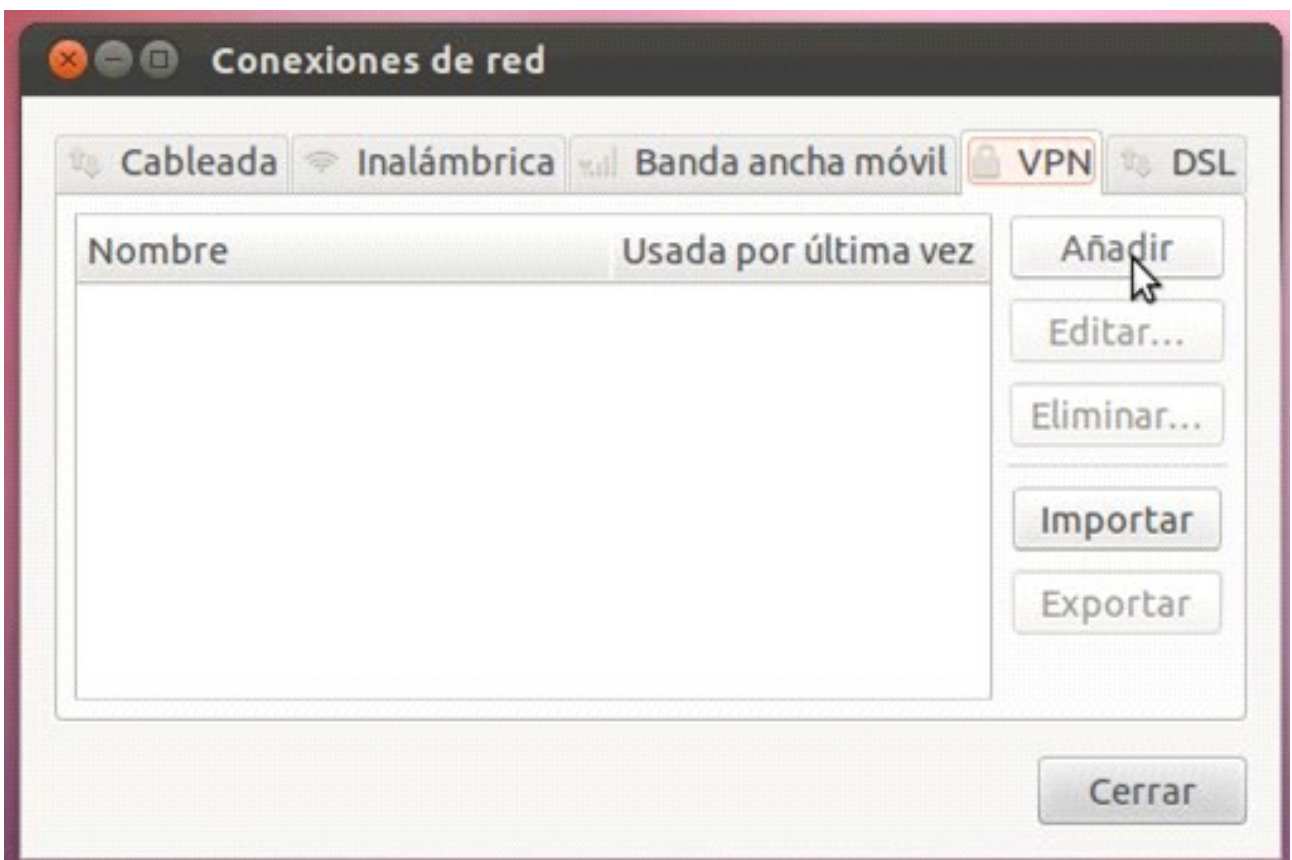
5. Configuración de los clientes

VPN: Conexiones de red

Empezaremos por pulsar sobre el icono de la red (en mi caso salen dos flechas por ser una conexión de cable, si fuera WiFi saldrían las típicas barras de cobertura), posteriormente iremos a: Conexiones VPN -> Configurar VPN...

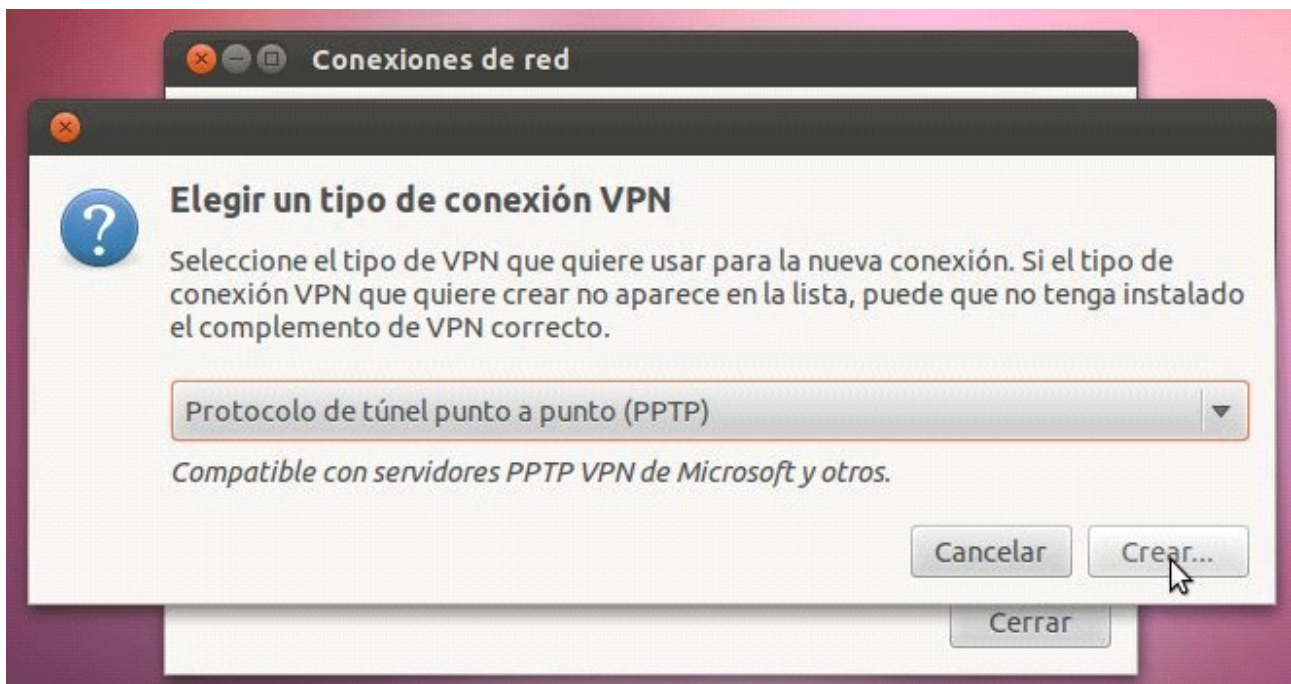


Vamos a la pestaña VPN y presionamos sobre el botón Añadir.



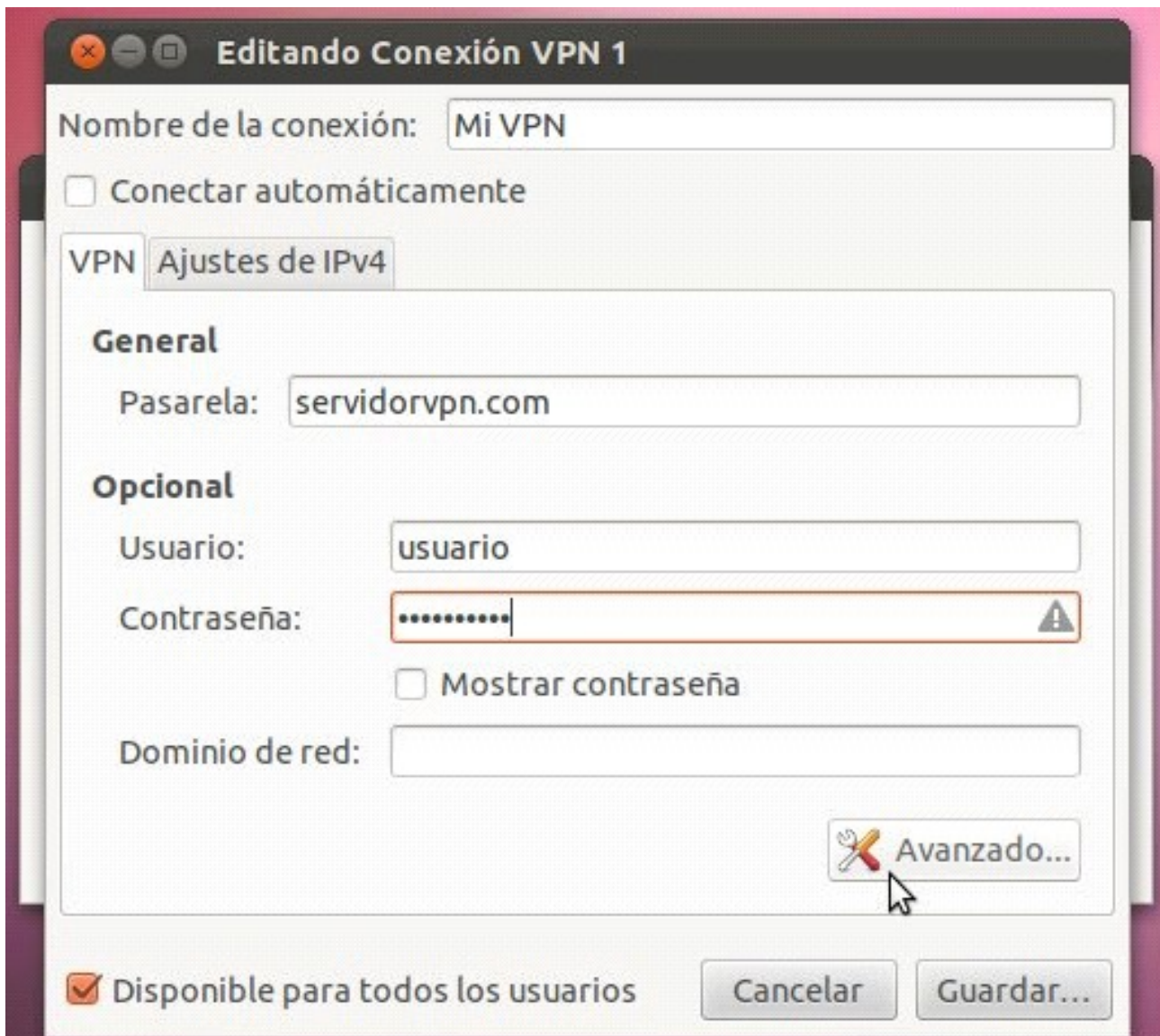
VPN: El asistente

Seleccionamos el tipo de conexión VPN que utilizaremos, en nuestro caso PPTP.



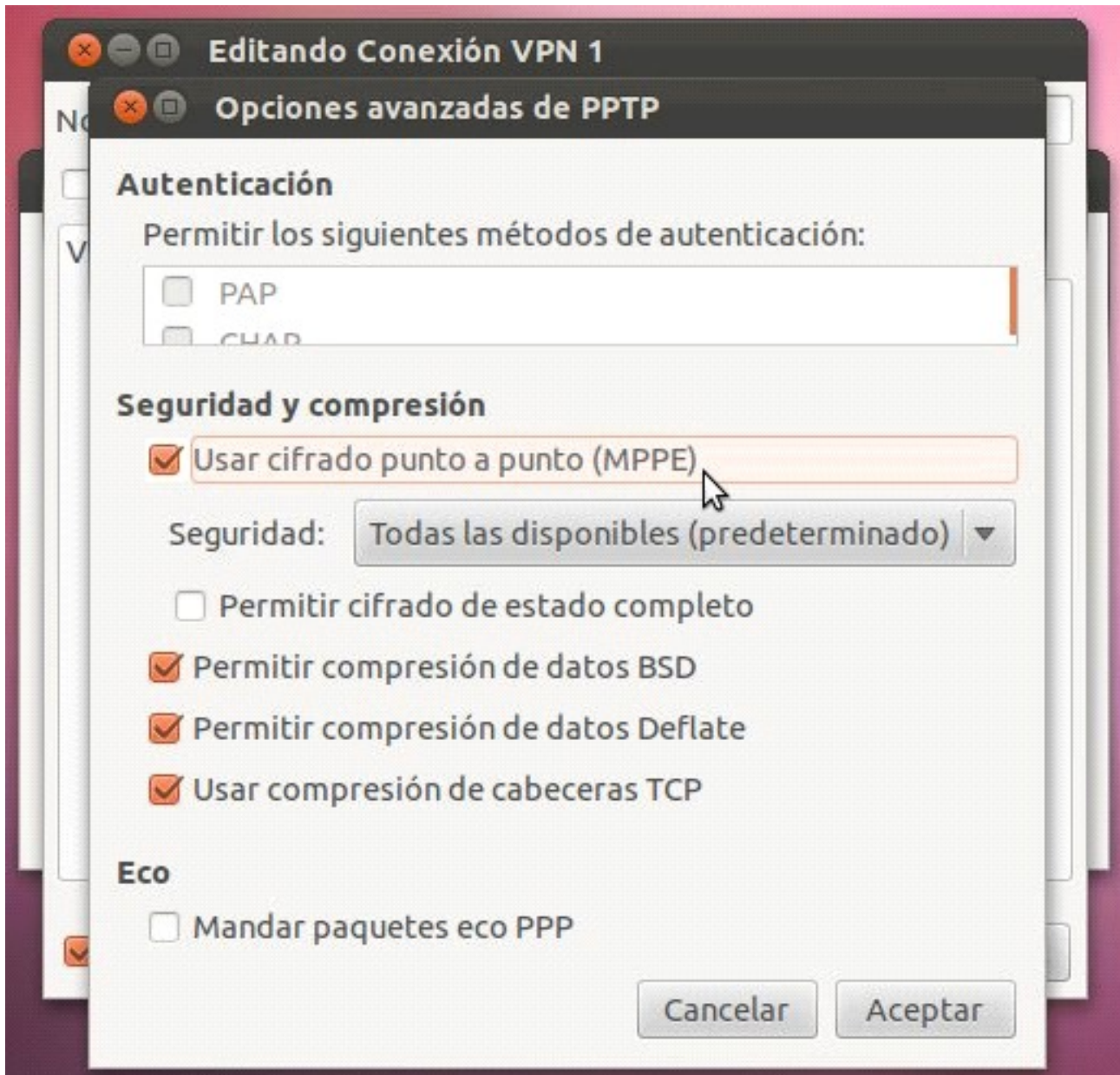
Ahora nos encontramos en la parte de la configuración:

- Nombre de la conexión: Nombre que asignaremos a esta conexión, se utilizará para diferenciarla del resto de conexiones VPN que tengamos.
- Pasarela: Dirección del servidor de la VPN. Puedes ser una DNS o una dirección IP.
- Usuario: Nuestro usuario para la VPN.
- Contraseña: No necesita descripción.

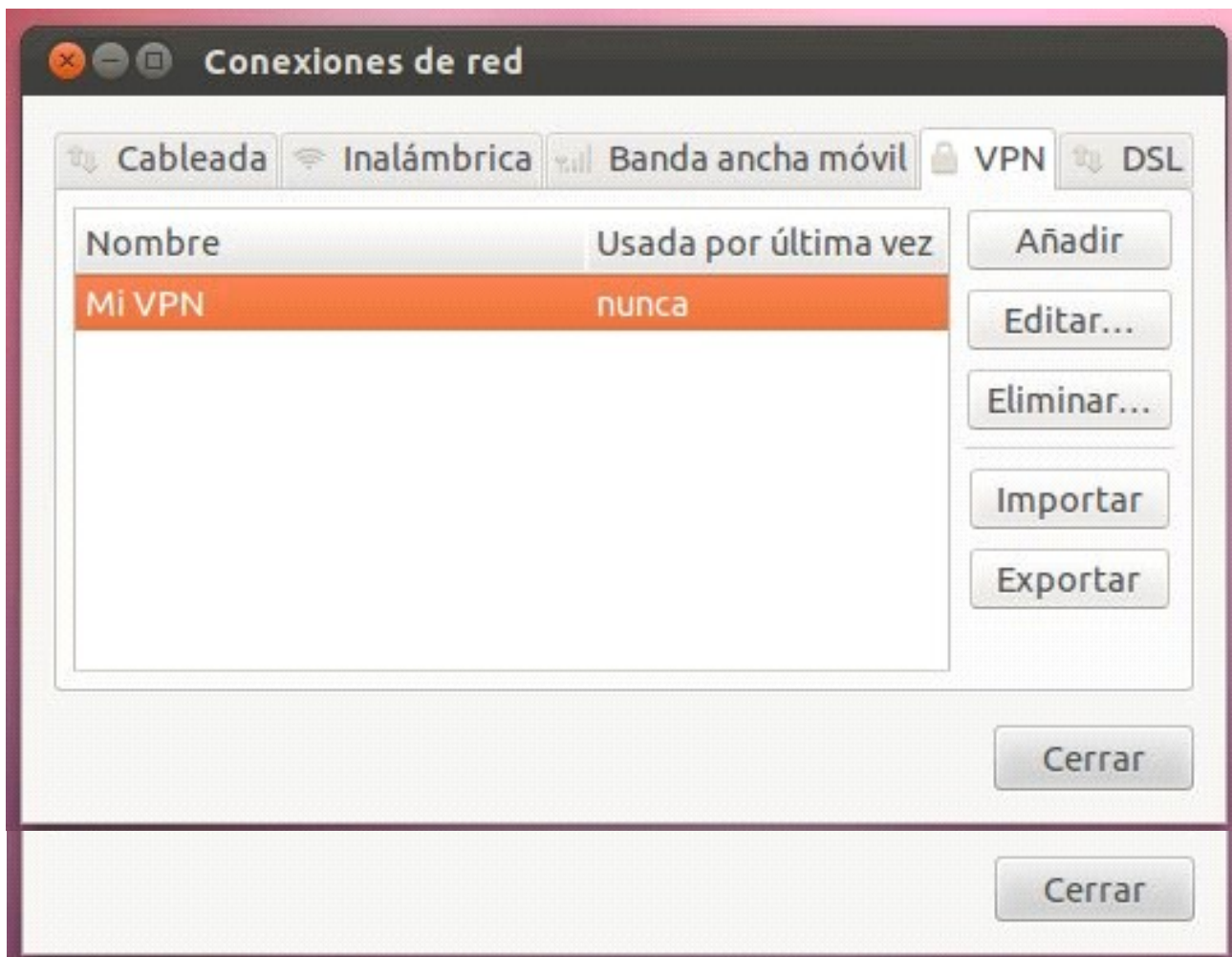


VPN PPTP

Presionamos sobre el botón "Avanzado...". En esta ventana marcamos la casilla "Usar cifrado punto a punto (MPPE)", el resto lo dejamos como está por defecto.

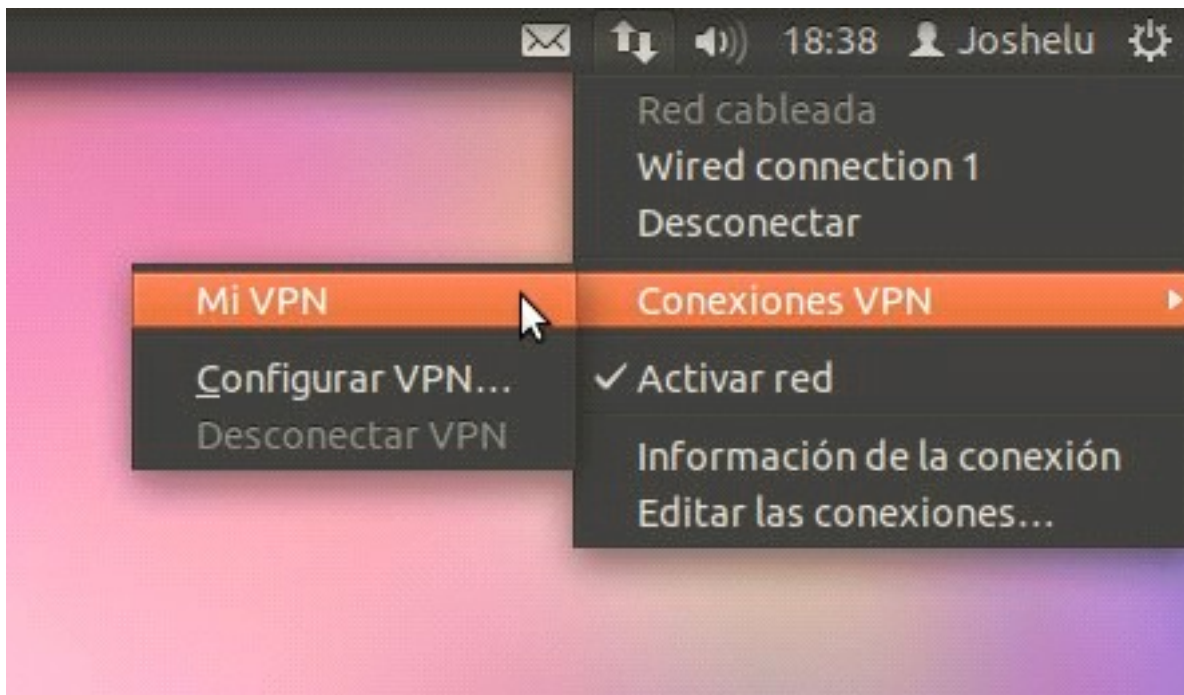


Aceptamos todo hasta llegar de nuevo a la ventana “Conexiones de Red”, en la cual veremos la nueva conexión ya creada.

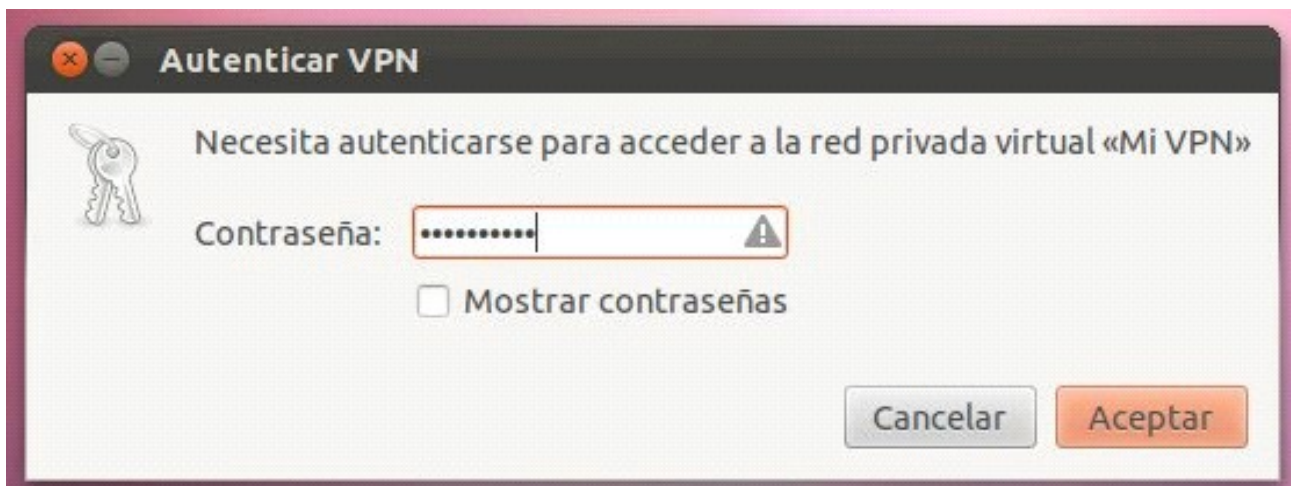


VPN: Conectar y desconectar

Por último sólo nos queda activar la conexión, para ello sólo tendremos que pulsar sobre el icono de la red, a continuación en Conexiones VPN y por último pulsar en la conexión VPN que querámos activar.



Introducimos la contraseña del usuario del ordenador.



6. Diagrama de GANT

No.	Actividad	Semanas														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Recopilación y análisis de la información necesaria.	■														
2	Recopilación de Hardware y Software necesario.		■	■	■											
3	Pruebas en configuracion VPN					■	■	■	■	■	■					
4	Documentación y análisis de los resultados.											■	■	■		
5	Generación de reporte final.															■

Realizado	■
Retrasado	■
En curso	■
Programado	■

7. Conclusiones

Hoy en día una conexión vpn es de mucha importancia para las empresas que tienen diferentes edificios o sucursales en diferentes partes geográficas ya que para mantener todos sus equipos conectados a una misma red es necesario tener configurado un vpn.

8. Recomendaciones

Usando PPTP una compañía puede reducir en un gran porcentaje el costo de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones encriptadas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

9. Bibliografía

<http://es.wikipedia.org/wiki/PPT> 10 – Septiembre – 2013

<http://www.pablin.com.ar/computer/info/varios/pptnvpn.htm> 09 – Noviembre – 2013

<http://usuariodebian.blogspot.com/2013/01/servidor-vpn-pptp-para-windows.html> 09 – Nov - 2013