Contenido

1. Introducción.

La Escuela Técnica Superior de Ingenieros Informáticos de la Universidad Politécnica de Madrid, ofrece a sus usuarios, a través de su Centro de Cálculo, un servicio de *Virtual Private Network (VPN)* para acceder desde Internet a la red de la Universidad a través de un canal cifrado.

1.1. Protocolos.

Este servicio se ofrece a través de un servidor SoftEther VPN albergado en el equipo **vpn.fi.upm.es**, que es multiprotocolo, permitiendo conectarse a través de los siguientes protocolos y puertos:

- *SSTP (Secure Socket Tunneling Protocol)*: puerto TCP 443
- *L2TP (Layer 2 Tunneling Protocol)* sobre *IPSec* (*Internet Protocol Security)*:
  - puerto UDP 500: IKE *(Internet Key Exchange)*
  - puerto UDP 4500: IPSec NAT-T *(IPsec NAT Traversal)*
- *OpenVPN:* puerto UDP y TCP 1194
- *SSL-VPN*: puerto TCP 443

Esto permite soporte nativo de VPN en cualquier sistema operativo actual (Windows, Linux, MacOS, Android), sin tener que instalar el cliente del propio servicio SoftEther.

1.2. Ámbito de los usuarios.

Cada usuario, a la hora de la autenticación con el servidor VPN de la Escuela, habrá de indicar el ámbito al que pertenece especificando uno de los siguientes dominios:

- usuario***@fi.upm.es****:* para personal PDI o PAS
- usuario***@alumnos.upm.es****:* para el alumnado

Asimismo, la clave será la utilizada para acceder a los servicios propios de la Escuela.

2. Configuración de la conexión VPN en Linux Ubuntu 16.04.

Para conectarse a la VPN de la Escuela podemos utilizar alguno de los protocolos soportados a través de *Network Manager.*

La opción preferida en este caso es OpenVPN. Simplemente hay que descargarse el perfil de la página web de descripción del servicio e importarla en Network Manager.

Otra opción es *L2TP sobre IPSec.* La pega en este caso es que la implementación del *plugin* de strongSwan para *Network Manager* tiene varios *bugs*, por lo que hay que recurrir al repositorio de un tercero. Además se necesita tener funcionando un par de demonios para realizar las conexiones L2TP e IPSec. Asimismo, el dispositivo que ofrece conexión a Internet al usuario tendrá que tener abiertos los puertos UDP 500 y 4500 comentados anteriormente, para realizar la conexión con los puertos equivalentes del servidor VPN. Esta forma de conexión también se efectúa por UDP, por lo que es menos sensible a cortes y permite recuperarse mejor de ellos frente a otros protocolos que utilizan sesiones TCP.

La **autenticación IPSec** entre equipos se efectuará **mediante *PSK*** *(Pre-Shared Keys)*. Esta clave está disponible, previa autenticación del usuario, en la página web de descripción del servicio. Conviene consultarla periódicamente porque **se cambiará regularmente**.

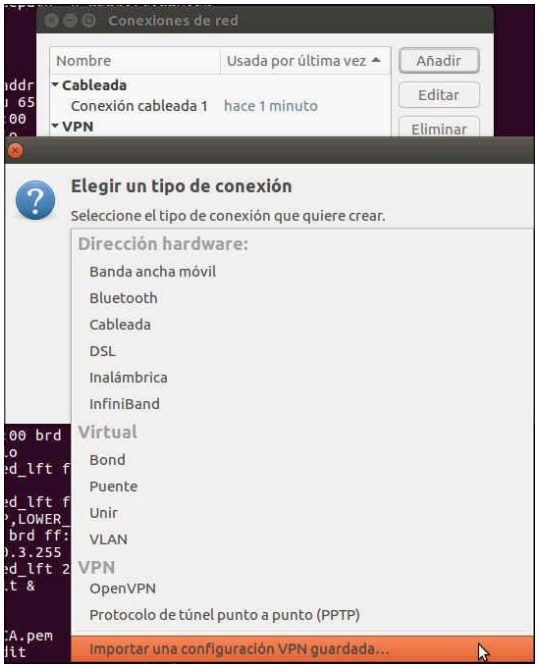
También podemos emplear el cliente VPN propio de SoftEther, disponible en www.softether.com, para conectarnos vía SSL-VPN. Pero en este caso la configuración habrá de realizarse por línea de comandos.

2.1. Conexión mediante OpenVPN.

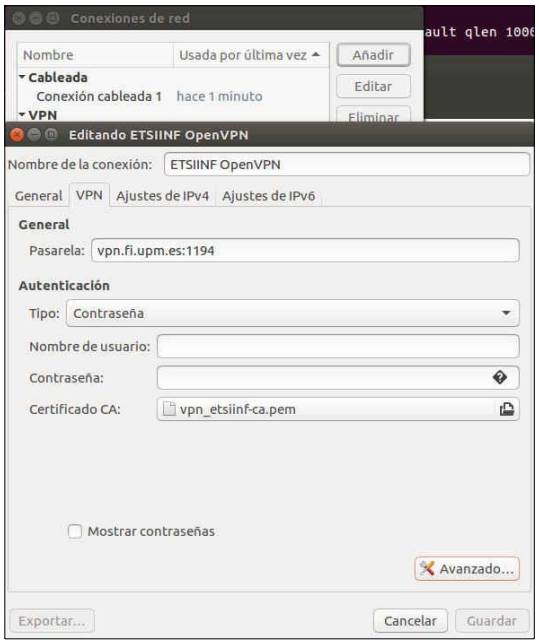
Para utilizar OpenVPN desde Network Manager, instalamos el plugin correspondiente y los paquetes necesarios para poder utilizarlo:

```
$ sudo apt install network-manager-openvpn-gnome
Se instalarán los siguientes paquetes NUEVOS:
libpkcs11-helper1 network-manager-openvpn network-manager-openvpn-gnome openvpn
```

Ahora podemos descargar el perfil de conexión de OpenVPN e importarlo en Network Manager:



De esta manera rápidamente estará definida la conexión para conectarse al servidor *vpn.fi.upm.es*:

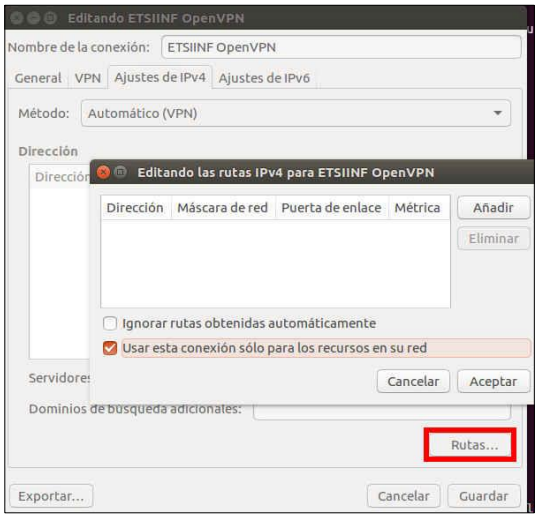


El perfil está configurado para realizar la conexión por UDP, pero el servidor también admite conexiones por el puerto TCP 1194.

2.1.1. Configuración adicional.

Una vez se haya establecido la conexión VPN, si no se indica otra cosa, Linux la utilizará como ruta por defecto para todo el tráfico que haya en el equipo cliente. Esto no es conveniente ya que puede limitar la velocidad de descargas de sitios "no UPM", además de las implicaciones de privacidad que quiera tener el usuario.

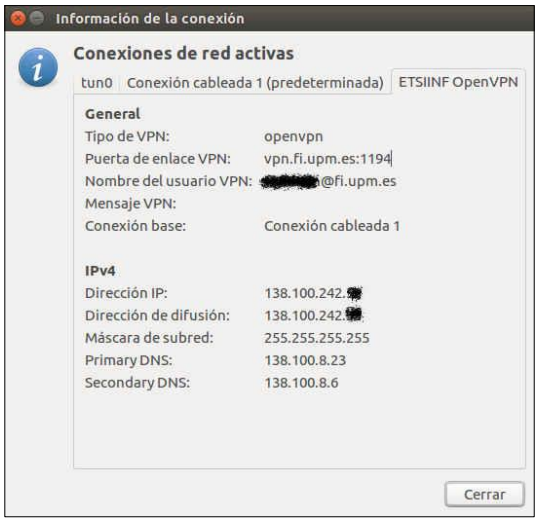
Para evitarlo **es necesario configurar** que la conexión VPN sólo se utilice para tráfico cuyo destino final sean equipos de la Universidad (el servidor VPN también proporciona qué rutas son específicas de la red de la UPM), desde la opción *Rutas* en la pestaña *Ajustes de IPv4* marcamos *Usar esta conexión sólo para los recursos en su red.*



2.1.2. Establecimiento de la conexión.

Para realizar la conexión se habrá de añadir al usuario, dependiendo del colectivo al que se pertenezca, el dominio *@fi.upm.es* o bien *@alumnos.upm.es*.

Una vez establecida la conexión VPN con el servidor *vpn.fi.upm.es*, desde *Información de la conexión* podemos ver los detalles de la conexión.



2.2. Conexión mediante L2TP/IPSec.

Para utilizar L2TP sobre IPSec desde Network Manager, en Ubuntu 16.04 hemos de instalar el plugin de un repositorio de terceros.

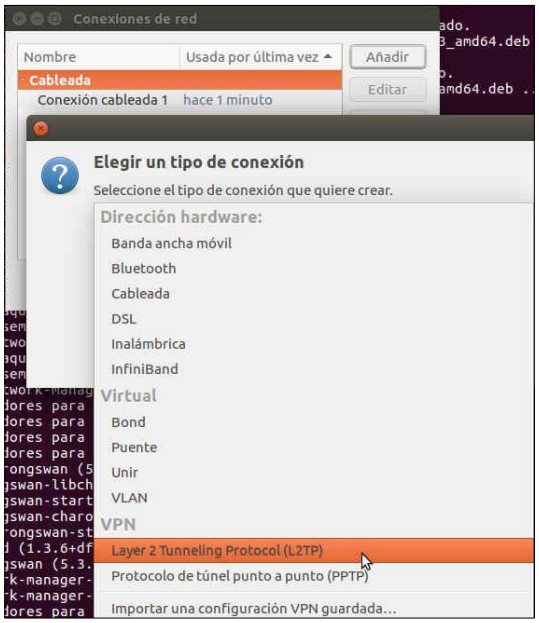
```
$ sudo add-apt-repository ppa:nm-l2tp/network-manager-l2tp
$ sudo apt update
```

```
$ sudo apt-get install network-manager-l2tp-gnome
Se instalarán los siguientes paquetes NUEVOS:
libstrongswan libstrongswan-standard-plugins network-manager-l2tp network-manager-l2tp-gnome
strongswan strongswan-charon strongswan-libcharon strongswan-starter xl2tpd
```

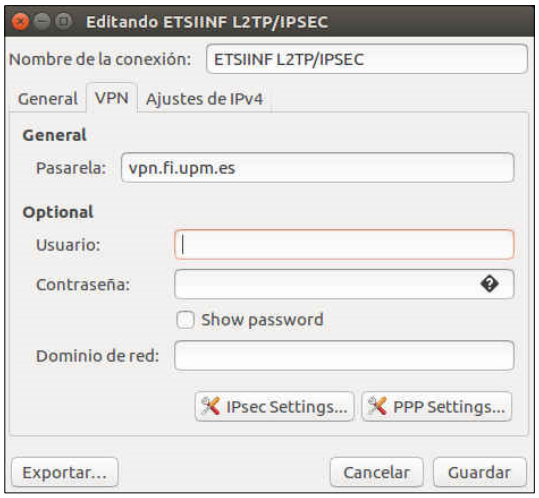
Como se ve, entre los paquetes que se instalarían se encuentran *xl2tpd* y *strongswan-charon*, que arrancarán sendos demonios para establecer las conexiones L2TP (puerto UDP 1701) e IPSec (puertos UDP 500 para IKE y UDP 4500 para NAT-T) con el servidor VPN.

```
$ sudo netstat -tulpn | egrep "xl2tpd|charon"
Proto  Recib Enviad Dirección local  Dirección remota  Estado  PID/Program name
udp        0      0 0.0.0.0:4500     0.0.0.0:*                3143/charon
udp        0      0 0.0.0.0:500      0.0.0.0:*                3143/charon
udp        0      0 0.0.0.0:1701     0.0.0.0:*                3305/xl2tpd
udp6       0      0 :::4500          :::*                     3143/charon
udp6       0      0 :::500           :::*                     3143/charon
```

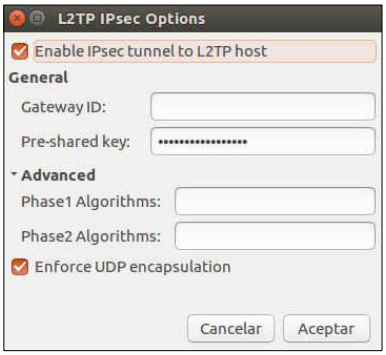
Ahora estará disponible en Network Manager la opción *Layer 2 Tunnel Protocol (L2TP)* para definir la conexión VPN.



Indicamos que el servidor VPN es *vpn.fi.upm.es*,



y en la opción *IPSec Settings* se proporciona la clave compartida IPSec y se indica que la conexión L2TP irá encapsulada dentro del túnel que se establecerá con el servidor VPN.

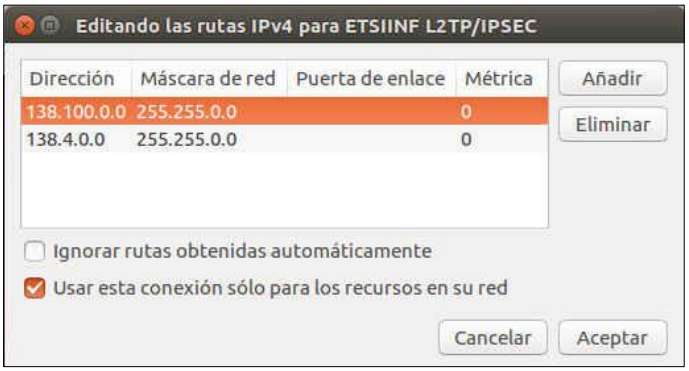


2.2.1. Configuración adicional.

Como ya se ha comentado antes, si no se indica otra cosa, Linux la utilizará como ruta por defecto para todo el tráfico que haya en el equipo cliente. Esto no es conveniente ya que puede limitar la velocidad de descargas de sitios “no UPM”, además de las implicaciones de privacidad que quiera tener el usuario.

Para evitarlo **es necesario configurar** que la conexión VPN sólo se utilice para tráfico cuyo destino final sean equipos de la Universidad desde la opción *Rutas* en la pestaña *Ajustes de IPv4* marcamos *Usar esta conexión sólo para los recursos en su red.*

Este plugin no es capaz de recoger las rutas de las redes de la UPM que le proporciona el servidor, por lo que habremos de introducir manualmente las rutas.



2.2.2. Configuración opcional.

En la opción *PPP Settings* se puede dejar únicamente *MSCHAPv2* como método de autenticación pues es algo más seguro ya que lo que se intercambia con el servidor es un *hash*, no la clave en claro como en *PAP* (aunque se hace dentro del túnel cifrado).

2.2.3. Establecimiento de la conexión.

Para realizar la conexión se habrá de añadir al usuario, dependiendo del colectivo al que se pertenezca, el dominio *@fi.upm.es* o bien *@alumnos.upm.es*.

Una vez establecida la conexión VPN con el servidor *vpn.fi.upm.es*, desde *Información de la conexión* podemos ver los detalles de la conexión.