# 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 Windows 7.

Windows, desde su propia instalación, nos aporta dos formas de conexión al servidor SoftEther.

Por una parte se puede utilizar el protocolo L2TP encapsulado en un túnel IPSec. En este caso, el dispositivo que ofrece conexión a Internet al usuario tendrá que tener abiertos los puertos UDP 500 y 4500 comentados anteriormente, para así realizar la conexión con los puertos equivalentes del servidor VPN. Esta forma de conexión, además, al ser por UDP es menos sensible a cortes y permite recuperarse mejor de ellos frente a otros protocolos que utilizan sesiones TCP.

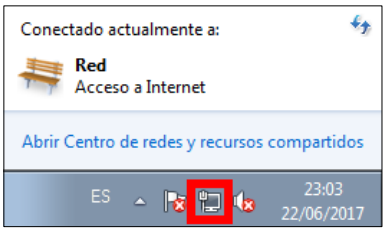
La **autenticación IPSec** entre equipos se efectuará **mediante *PSK*** *(Pre-Shared Keys)*. Esta clave está disponible, previa autenticación del usuario, en la página web de descripción del servicio. Conviene consultarla periódicamente porque **se cambiará regularmente**.

Además, Windows desde su versión Vista ofrece el protocolo SSTP, que no es más que una sesión PPP sobre el protocolo HTTPS. La ventaja en este caso es que los firewalls no suelen prohibir las conexiones al puerto TCP 443.

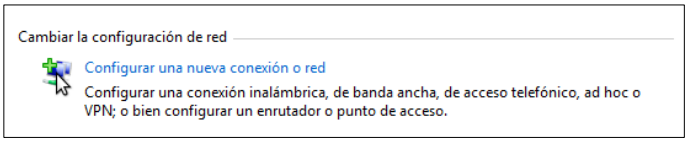
Aparte de los protocolos nativos de Windows también podemos conectarnos vía la implementación SSL-VPN propia del servidor VPN. Para ello necesitaremos instalar el software *Software VPN Client* disponible en www.softether.com.

## 2.1. Conexión mediante SSTP.

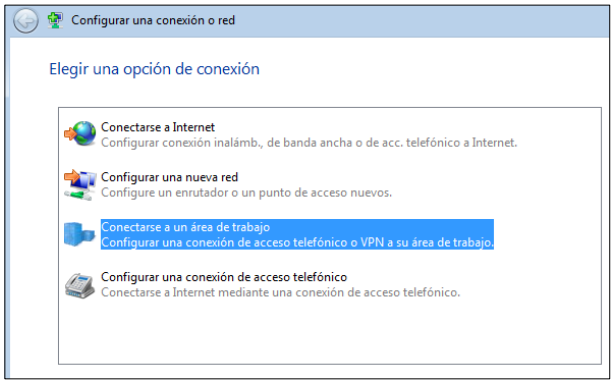
Para definir una nueva conexión de red de tipo VPN, accedemos al *Centro de redes y recursos compartidos* desde el icono de la barra de tareas.



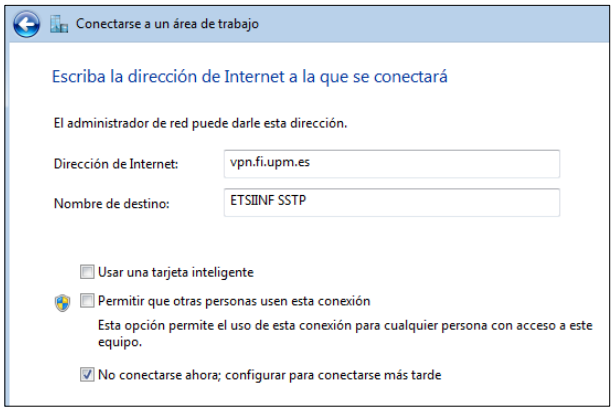

Desde aquí, procedemos a *Configurar una nueva conexión o red*:




Indicamos que la conexión será una *VPN a su área de trabajo,*

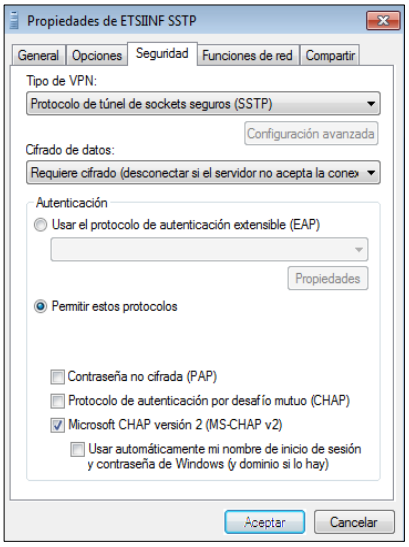



y el servidor VPN de la Escuela.

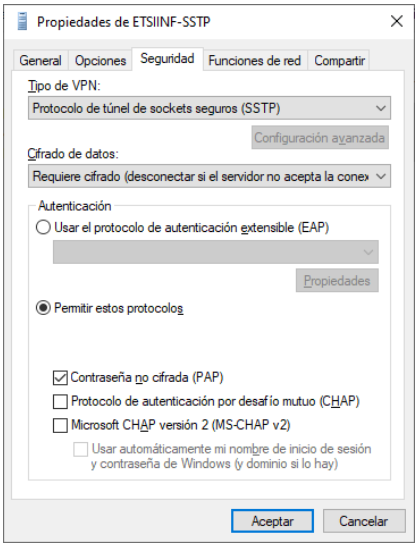



Para forzar que el protocolo utilizado en la conexión sea SSTP hay que volver al *Centro de redes y recursos compartidos* para *Cambiar la configuración del adaptador,*

estableciendo en la pestaña de Seguridad de las *Propiedades* de la conexión el *Tipo de VPN* a *Protocolo de túnel de sockets seguros (SSTP)*.




Para personal

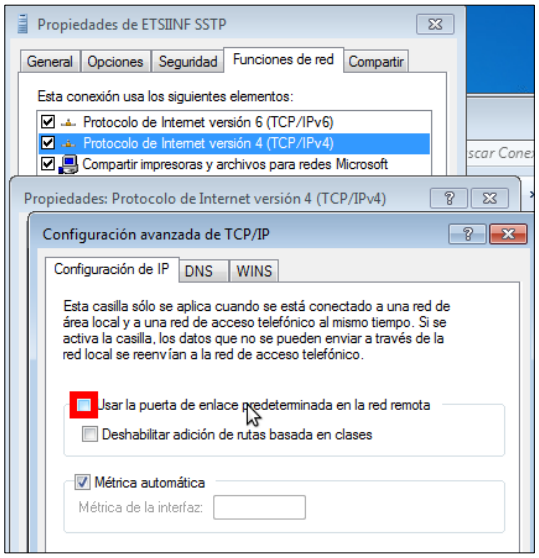



Para alumnos

## 2.1.1. Configuración adicional

Una vez se haya establecido la conexión VPN, si no se indica lo contrario, Windows 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 pestaña *Funciones de red* desmarcamos *Usar la puerta de enlace predeterminada en la red remota*.




## 2.1.2. Protocolo de intermcabio de claves.

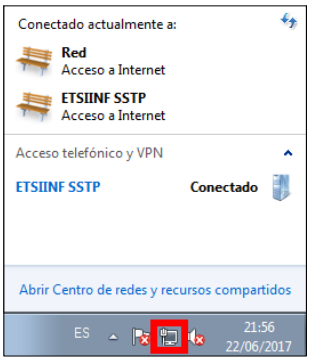
En la pestaña de Seguridad, en la que se ha elegido el protocolo SSTP, en el caso del personal, también podemos dejar *MS-CHAPv2* como único protocolo de transmisión de la contraseña. En el caso de los **alumnos debe**

**utilizarse sólo protocolo *PAP***, en este caso la clave se enviaría en claro, pero eso sí, siempre dentro de un canal cifrado.

### 2.1.3. Establecimiento de la conexión.

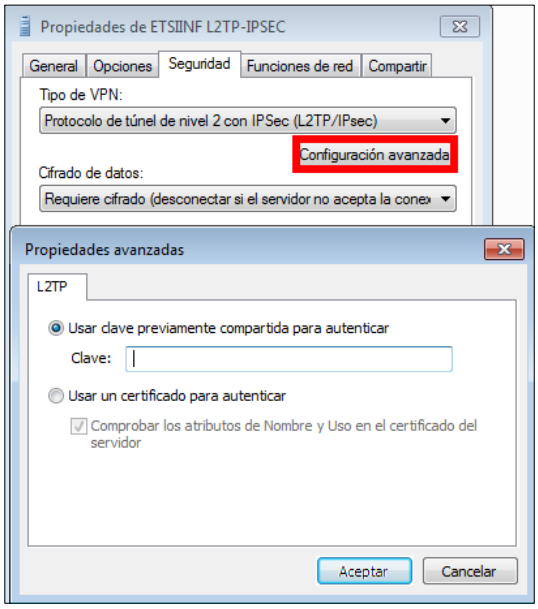
Para realizar la conexión se habrá de añadir al usuario, dependiendo del colectivo al que se pertenezca, el dominio *@fi.upm.es* o bien *@alumnos.upm.es*.

Una vez establecida la conexión VPN con el servidor *vpn.fi.upm.es*, nos aparecerá como conectada en la sección de *Red* accesible desde la barra de tareas.

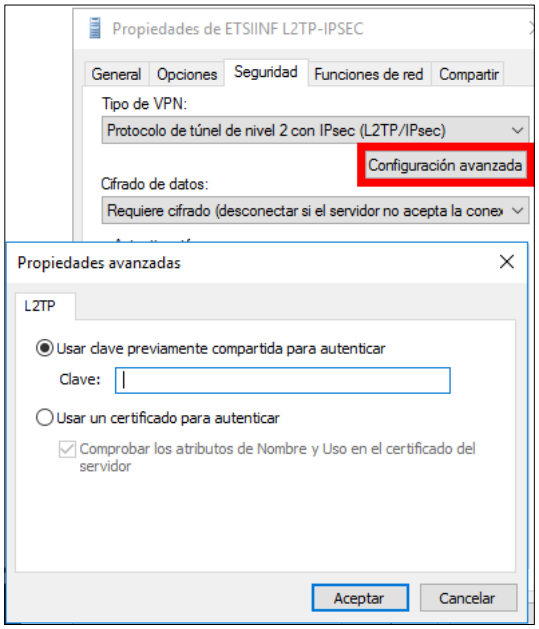



## 2.2. Conexión mediante L2TP/IPSec.

Como antes, agregamos una nueva conexión VPN. Esta vez en *Tipo de VPN* forzamos el modo a *Protocolo de túnel de nivel 2 con IPSec (L2TP/IPsec)*.




La autenticación IPSec entre equipos se efectuará mediante *Clave previamente compartida (PSK)*, la cual se podrá consultar en la página web de descripción del servicio, previa autenticación del usuario. Se habrá de indicar en el apartado de *Configuración avanzada* de la pestaña de *Seguridad* en las *Propiedades* de la conexión (ver 2.1.1.Configuración opcional)




### 2.2.1. El resto de pasos para la configuración son los mismos que los indicados para la conexión SSTP (ver puntos 2.1.1.Configuración adicional, 2.1.2.Configuración opcional y 2.1.3.Establecimiento de la conexión)