Contenido

1. Introducción.	1
1.1. Protocolos	1
1.2. Ámbito de los usuarios	1
2. Configuración de la conexión VPN en Windows 10.	2
2.1. Conexión mediante SSTP	2
2.1.1. Configuración opcional	3
2.1.2. Establecimiento de la conexión	4
2.2. Conexión mediante L2TP/IPSec.	5

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 10.

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 a la *Configuración de la red* desde el icono de la barra de tareas.



Ahora, desde la sección VPN, seleccionamos *Agregar una conexión VPN*. Cambiamos el *Tipo de VPN* para forzar el modo a *Protocolo de túnel de sockets seguros (SSTP)*.

Agregar una conexión VPN	
Proveedor de VPN	
Windows (integrado) \sim	
Nombre de conexión	
ETSIINF SSTP	
Nombre de servidor o dirección	
vpn.fi.upm.es	
Tipo de VPN	
Protocolo de túnel de sockets seguros (SSTP) $ \sim $	

2.1.1. Configuración adicional.

Para acceder a mayores detalles de configuración, hay que irse ahora a la opción *Cambiar opciones del adaptador* de la sección *Ethernet*.

Configuración	
② Inicio	Ethernet
Buscar una configuración $ ho$ Red e Internet	Red Conectado
Æ Estado	Configuración relacionada
토 Ethernet	Cambiar opciones del adapta or

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*.

Propiedades de ETSIINF SSTP ×	xión »
General Opciones Seguridad Funciones de red Compartir Esta conexión usa los siguientes elementos:	ETSIINF SS Desconect WAN Mini
Protocolo de internet versión 4 (TCP/IPv4) Protocolo de Internet versión 4 (TCP/IPv4) So compartido de archivos e impresoras para redes Micr. Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)	×
Configuración avanzada de TCP/IP	×
Esta casilla solo se aplica cuando se está conectado a una red d área local y a una red de acceso telefónico al mismo tiempo. Si s activa la casilla, los datos que no se pueden enviar a través de la red local se reenvían a la red de acceso telefónico.	le e a
Jaar la puerta de enlace predeterminada en la red remota	
Métrica automática Métrica de la interfaz:	

2.1.2. Protocolo de intercambio de claves

Opcionalmente para el personal y **obligatorio para los alumnos**, también podemos cambiar detalles en la pestaña *Seguridad* dentro de las *Propiedades* de la conexión que hayamos definido, tales como:

- utilizar cifrado en cualquier caso.
- transmisión de la contraseña únicamente vía *PAP*, se enviará en claro, aunque dentro, eso sí, de un canal cifrado.

Propiedades de	ETSIINF SST	P		×	Prop	iedades de	ETSIINF-SS	TP		
eneral Opciones	Seguridad	Funciones de red	Compartir		General	Opciones	Seguridad	Funciones d	e red	Comp
Tipo de VPN:					Tipo de	VPN:				
Protocolo de túne	l de sockets s	eguros (SSTP)		~	Protoc	olo de túnel	de sockets	seguros (SSTF	')	
Cifrado de datos:		Configura	ción avanzad	а	<u>C</u> ifrado	de datos:		Cor	nfigurad	ción a <u>v</u>
Requiere cifrado (desconectar s	i el servidor no ace	pta la conex 🕚	~	Requie	ere cifrado (d	desconectar	si el servidor n	ю асер	ota la c
Usar el protoc	olo de autenti protocolos	cación extensible (E	EAP)		O Us	ar el protoco	olo de auten protocolo <u>s</u>	licación <u>e</u> xten:	sible (E	AP) Propieda
Contraseña	a no cifrada (P	AP)			\checkmark	Contraseña	no cifrada (PAP)		
Protocolo (de autenticaci	ón por desafío mutu	uo (CHAP)			Protocolo d	e autenticad	ión por desafí	o mutu	ю (С <u>Н</u> А
Microsoft (CHAP versión	2 (MS-CHAP v2)				Microsoft C	H <u>A</u> P versiór	2 (MS-CHAP	v2)	
Usar a y contr	utomáticamen aseña de Win	te mi nombre de inic dows (y dominio si l	cio de sesión o hay)			Usar au y contra	itomáticame aseña de Wi	nte mi nom <u>b</u> re ndows (y domi	de inici nio si lo	io de s o hay)
Usar a y contr	utomáticamen aseña de Win	te mi nombre de inic dows (y dominio si l Aceptar	tio de sesión o hay) Cancela	ar		Usar au y contra	itomáticame aseña de Wi	nte mi nom <u>b</u> re ndows (y domi Ace	de ir nio s ptar	nic si lo

Para personal

Para alumnos

2.1.3. Establecimiento de la conexión.

Procedemos seguidamente a lanzar la conexión VPN que hemos definido, la cual nos aparecerá si pulsamos en el icono de red de la barra de tareas.

Windows 10

臣	Red 3 Conec	tado				
యా	ETSIIN	F SSTP				
				Conectar		
(i.	Segura	a				
(h.	Segura	3				
(h.	Segura	a				
Configuración de red e Internet Cambia los ajustes de configuración, como hacer que una conexión sea de uso medido.						
<i>II</i> . Wi-Fi		ър Modo avión	(ျာ) Zona con cobertura			
		^	1 - 1	18:14 💭		

Windows nos pedirá las credenciales del usuario. Dependiendo del colectivo al que se pertenezca, el usuario ha de completarse con el dominio *@fi.upm.es* o bien *@alumnos.upm.es*.

Seguridad de Windows	×
Iniciar sesión	
@fi.upm.es	
•••••	୕
Aceptar	Cancelar

Una vez establecida la conexión VPN con el servidor *vpn.fi.upm.es*, nos aparecerá como conectada en el apartado de *Red*.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	ETSIINF SSTP Conectado		
		Opciones avanzadas	Desconectar

# 2.2. Conexión mediante L2TP/IPSec.

Como antes, agregamos una nueva conexión VPN. Esta vez en *Tipo de VPN* forzamos el modo a *L2TP/IPsec con clave previamente compartida*.



La clave compartida, que permite la autenticación IPSec entre equipo cliente y servidor, 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 adicional)

	Propiedades de ETSIINF L2TP-IPSEC	)
	General Opciones Seguridad Funciones de red Compartir	
	Tipo de VPN:	_
	Protocolo de túnel de nivel 2 con IPsec (L2TP/IPsec)	~
	Configuración avanzad Cifrado de datos:	а
	Requiere cifrado (desconectar si el servidor no acepta la conex	~
Propied	lades avanzadas X	
L2TP		
● Us	ar dave previamente compartida para autenticar	
Cl	lave:	
OUs	ar un certificado para autenticar	
	Comprobar los atributos de Nombre y Uso en el certificado del servidor	
	Aceptar Cancelar	]

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. Protocolo de intercambio de claves y 2.1.3.Establecimiento de la conexión)