Como crear una red privada virtual (VPN) en Windows XP

Introducción
Cada vez es más habitual moverse en escenarios en donde se requiere el acceso a recursos remotos desde cualquier lugar, incluso recursos que no están disponibles directamente en Internet, pero sí en nuestra intranet. Mediante una VPN podemos acceder de forma segura a todos los recursos de nuestra intranet usando una conexión pública como Internet y trabajabo como si estuviésemos en la red local.

¿Qué aborda este artículo?
En este artículo abordaremos el tema de las VPN's domésticas, es decir, veremos como con Windows 2000 y XP es posible crear rápidamente redes privadas que nos permiten compartir nuestros recursos con otros usuarios de forma segura.

¿Qué no encontrarás en este artículo?
No analizaremos las VPN's a fondo, simplemente abordamos una solución sencilla para usuarios domésticos. No trabajaremos con ningún servidor VPN ni de acceso remoto. Ese es tema para otro artículo.

¿Qué es una VPN?
En pocas palabras una VPN es una red virtual que se crea "dentro" de otra red, como por ejemplo Internet. Generalmente las redes privadas se crean en redes *públicas*, en las que se quiere crear un entorno confidencial y privado. La VPN nos permitirá trabajar como si estuviésemos en la red local, es totalmente transparente para el usuario.

Una vez establecida la conexión de la red privada virtual los datos viajan encriptados de forma que sólo el emisor y el receptor son capaces de leerlos.

Para poder realizar una VPN se necesita un servidor (o host) que espera conexiones entrantes, y uno o varios clientes, que se conectan al servidor para formar la red privada.

¿Qué podemos hacer con una VPN?
Al permitirnos establecer conexiones seguras entre otros equipos podremos acceder a los recursos del otro equipo de forma segura y confidencial, por ejemplo a impresoras, documentos, servidores de base de datos, aplicaciones específicas, etc.

¿Cómo funciona una VPN?
Como ya se ha dicho anteriormente se trata de un proceso totalmente transparente para el usuario y para la mayoría de las aplicaciones. Funciona exactamente igual que cualquier otra conexión de red, es decir, dentro de la VPN cada equipo tendrá una IP, todas las conexiones usando esa IP estarán funcionando dentro de la VPN y serán encriptadas, el usuario simplemente tendrá que usar las IPs de la VPN, y no preocuparse de nada más, el resto ya lo hace el cliente VPN y el servidor VPN.

Cultura general sobre VPN's
Antes de comenzar a trabajar con VPN's es bueno poseer unas nociones básicas del mundo en el que nos estamos metiendo.
Son dos las tecnologías más utilizadas para crear VPN's, en realidad son diferentes protocolos o conjuntos de protocolos, **PPTP** y **L2TP**.

PPTP: Point to Point Tunneling Protocol
PPTP es un protocolo desarrollado por Microsoft y disponible en todas las plataformas Windows. Es sencillo y fácil de implementar pero ofrece menor seguridad que L2TP. En este artículo implementaremos una conexión VPN mediante PPTP usando MS-CHAP v2. También es posible usar PPTP con EAP-TLS para soportar certificados de seguridad.

L2TP: Layer Two Tunneling Protocol
Se trata de un estándar abierto y disponible en la mayoría de plataformas Windows, Linux, Mac, etc. Se implementa sobre IPSec y proporciona altos niveles de seguridad. Se pueden usar certificados de seguridad de clave pública para cifrar los datos y garantizar la identidad de los usuarios de la VPN.

Comparativa entre PPTP y L2TP

- Con PPTP, el cifrado de datos comienza después de que la conexión se procese (y, por supuesto, después de la autentificación PPP). Con L2TP/IPSec, el cifrado de datos empieza antes de la conexión PPP negociando una asociación de seguridad IPSec.
- Las conexiones PPTP usan MPPE, un método de cifrado basado en el algoritmo de encriptación Rivest-Shamir-Aldeman (RSA) RC-4, y usa llaves de 40, 56 o 128 bits. Las conexiones L2TP/IPSec usan Data Encryption Standard (DES), con llaves de 56 bits para DES o tres llaves de 56 bits para 3-DES. Los datos se cifran en bloques (bloques de 64 bits para el caso de DES).
- Las conexiones PPTP requieren sólo autentificación a nivel de usuario a través de un protocolo de autentificación basado en PPP. Las conexiones L2TP/IPSec requieren el mismo nivel de autentificación a nivel de usuario y, además nivel de autentificación de máquina usando certificados digitales.

Existen más diferencias, pero hacer un estudio más pormenorizado se saldría de la idea inicial de este artículo por lo que lo dejaremos en estas tres diferencias fundamentales.

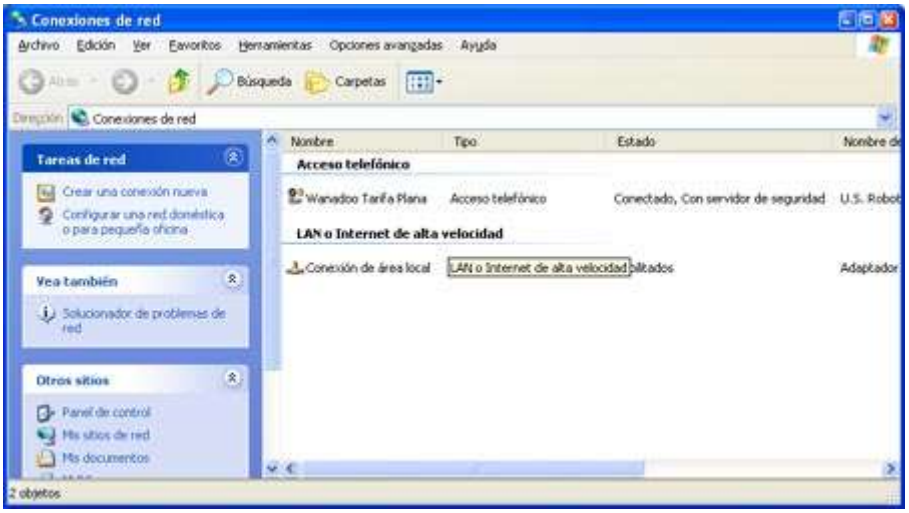
Caso práctico
La mejor forma de entender y ver como funciona es implementándolo, y eso es lo que haremos a continuación.

- **Escenario:** Dos (o más) equipos distantes y conectados a Internet quieren compartir sus recursos (ficheros, impresoras, etc.) entre ellos de forma privada y sencilla.
- **Software:** Windows XP o 2000, también es posible realizar la conexión con equipos con Windows 98 y 95 descargando los ficheros de actualización de la web de Microsoft.
- **Solución:** Montar una VPN a través de Internet entre estos equipos.

Necesitamos establecer un equipo como servidor, éste será el encargado de la autenticación, el resto de equipos establecerán la conexión con él.

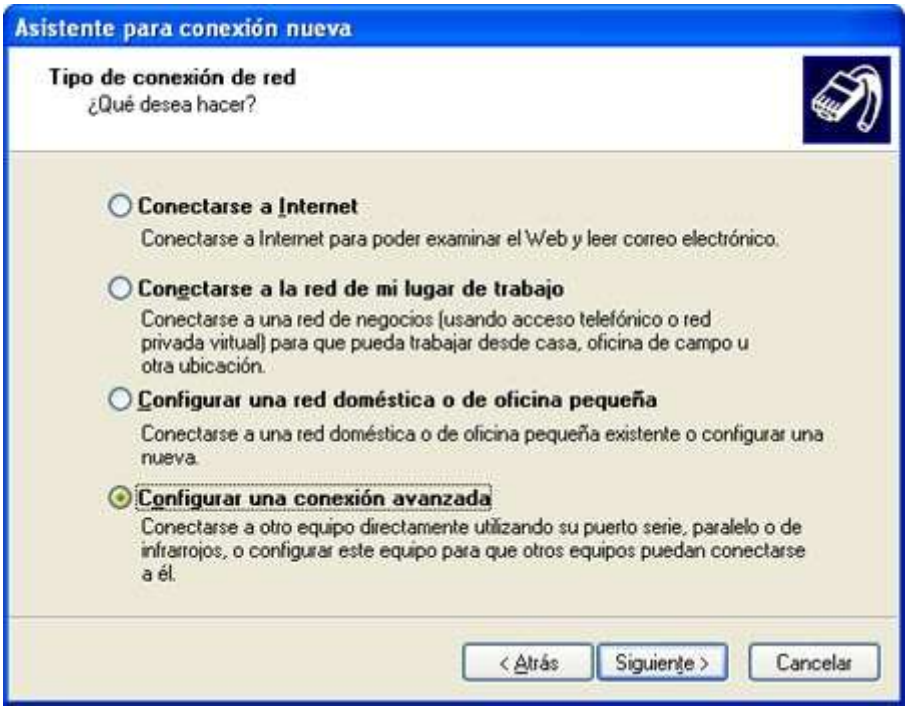
Servidor VPN

- Vamos al Panel de control, y abrimos la carpeta de "Conexiones de red" y en el menú Archivo seleccionamos "Nueva conexión".

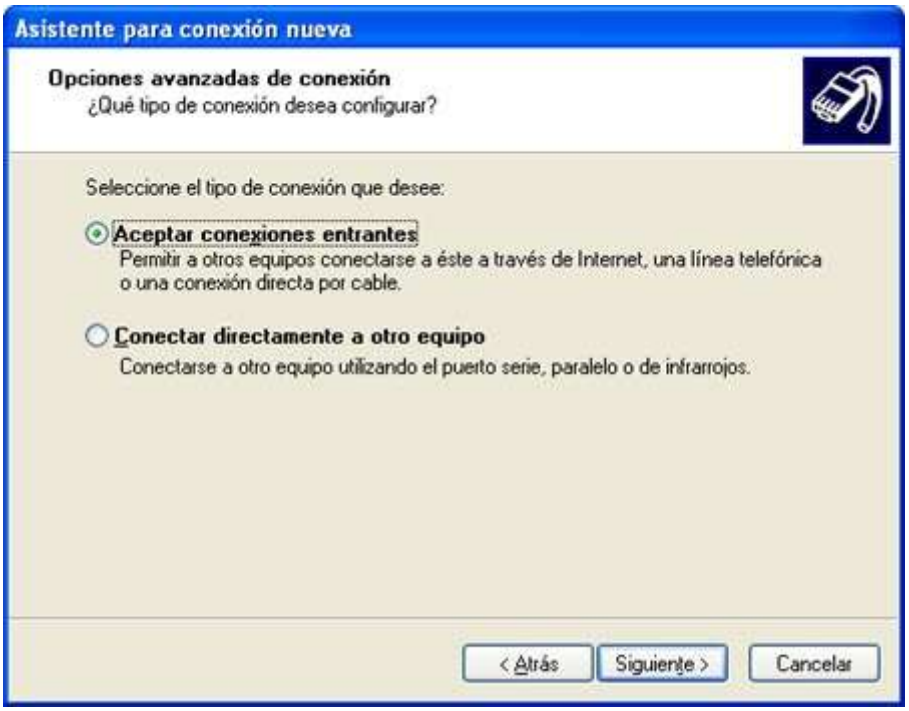


- Ahora estamos en el "Asistente para conexión nueva". Pulsamos en el botón "Siguiente" para continuar.

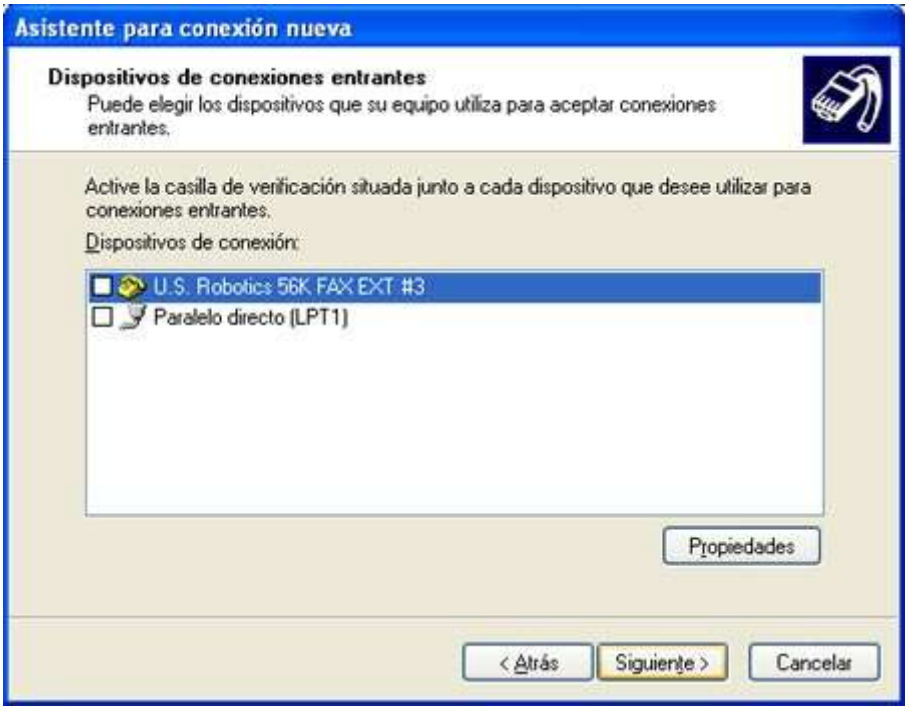
- Entre las opciones disponibles seleccionamos "Configurar una conexión avanzada", y pulsamos en "Siguiente".



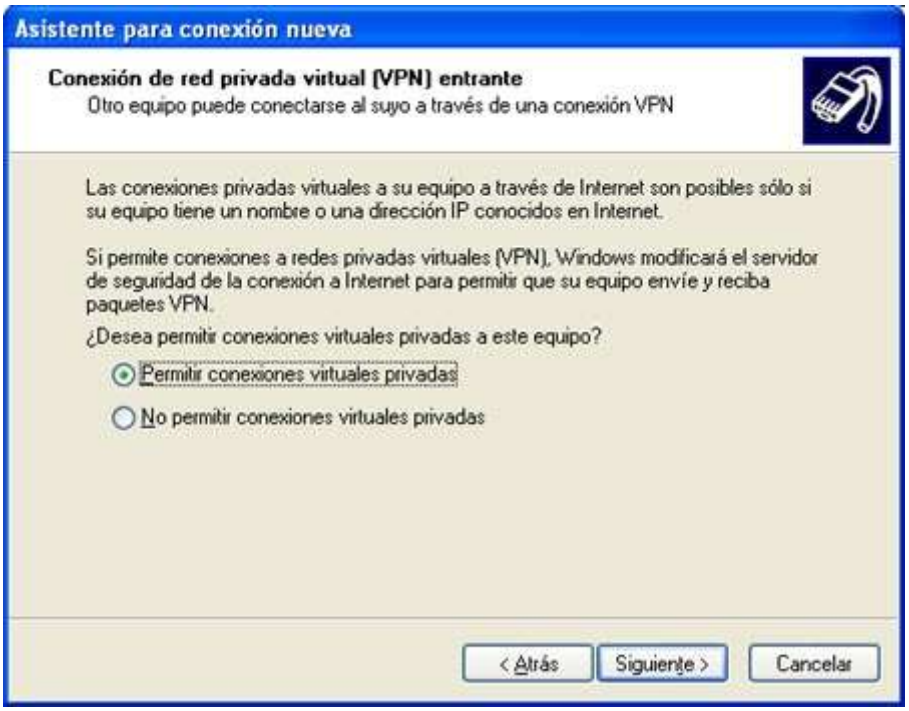
- Ahora seleccionamos "Aceptar conexiones entrantes" y pulsamos "Siguiente" para continuar.



- En la pantalla "Dispositivos de conexiones entrantes" no seleccionamos ninguno, pues no queremos que se conecten a este equipo haciendo una llamada o usando el puerto paralelo. Pulsamos en "Siguiente".



- En la pantalla "Conexión de red privada virtual (VPN) entrante" debemos seleccionar "Permitir conexiones virtuales privadas". Pulsamos en "Siguiente".



- En la pantalla "Permisos de usuarios" seleccionamos los usuarios que podrán conectarse a nuestro equipo usando la VPN. Desde esta misma pantalla podremos crear nuevos usuarios. Pulsamos en "Siguiente".

- Ahora debemos seleccionar los protocolos que habilitaremos en la VPN. Como queremos compartir ficheros e impresoras marcaremos "Protocolo Internet (TCP/IP)", "Compartir impresoras y archivos para redes Microsoft". Podremos agregar los protocolos que queramos usando el botón Instalar. Seleccionamos el protocolo "Protocolo Internet (TCP/IP)" y pulsamos en el botón Propiedades para proceder a configurarlo.

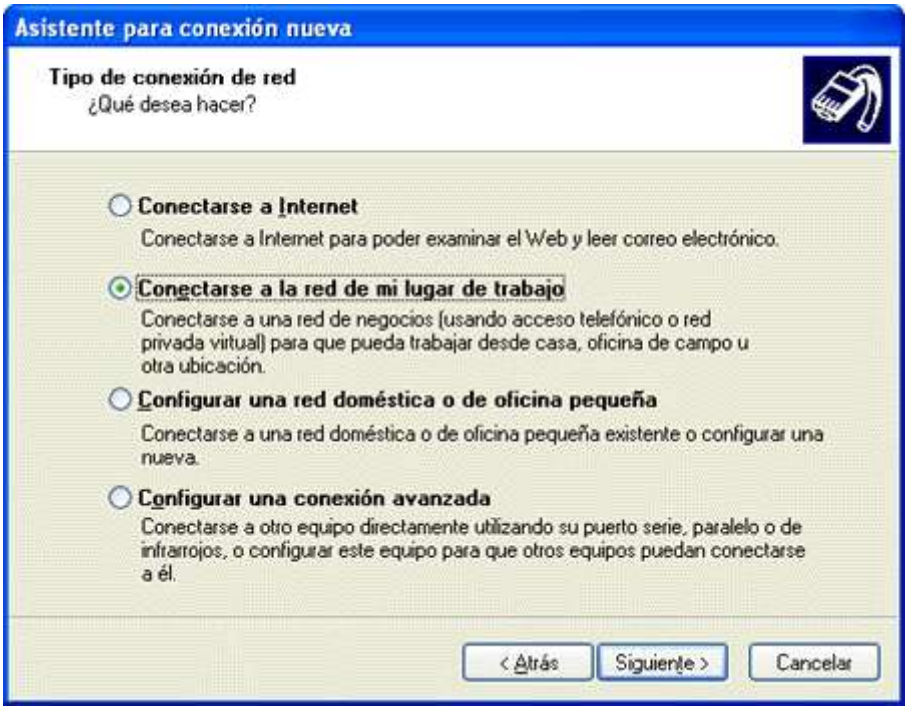
- Ahora podemos configurar las propiedades del protocolo TCP/IP. Si queremos que los clientes que se conectan a nosotros puedan acceder a la red local en la que tenemos nuestro servidor deberemos activar la primera casilla. Además podemos dejar que el servidor asigne las IPs de los clientes o establecer un intervalo de IPs, o incluso permitir que los clientes especifiquen su IP.

- Guardamos la configuración de TCP/IP y pulsamos en el botón siguiente del asistente y ya habremos terminado. En este momento tendremos una nueva conexión en la carpeta de Conexiones de red. Seleccionando la nueva conexión podremos ver el estado de ésta, los clientes conectados, cambiar las opciones de configuración, etc.

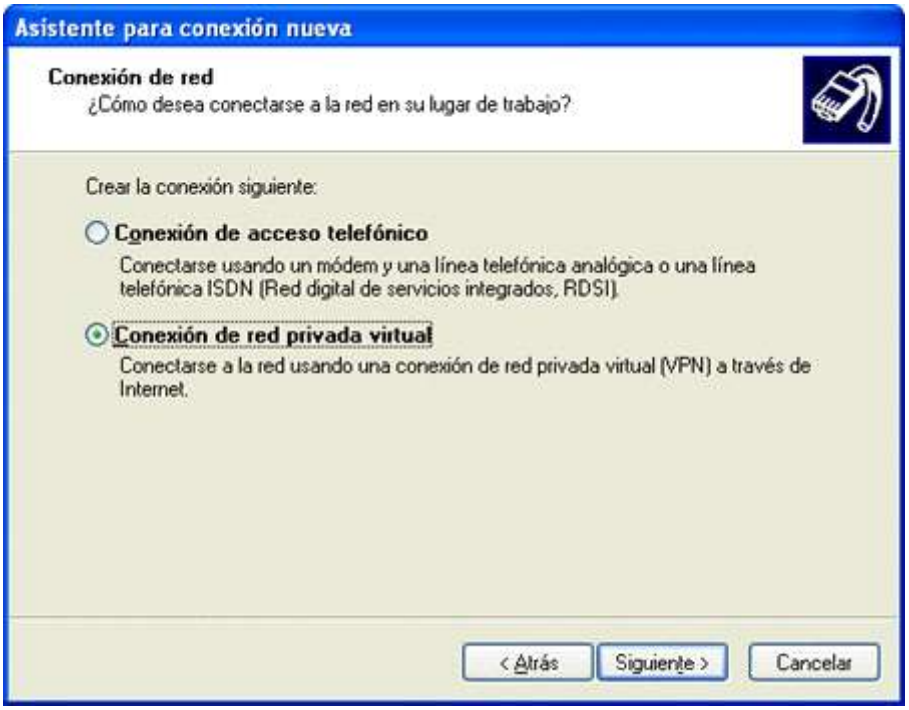
Ahora ya tenemos configurado el servidor VPN y ya está listo para aceptar clientes VPN.
A continuación configuraremos una conexión VPN para que se conecte al servidor.

Cliente VPN

- Abrimos la carpeta de "Conexiones de red" y en el menú Archivo seleccionamos "Nueva conexión". En el asistente para conexión nueva seleccionamos "Conectarse a la red de mi lugar de trabajo", y pulsamos siguiente.

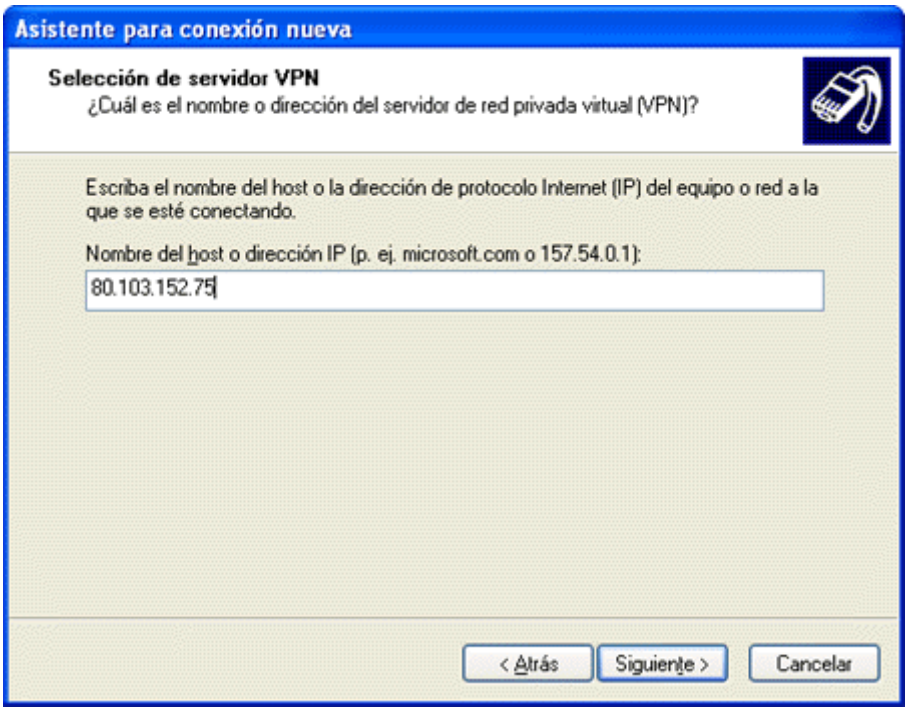


- Seleccionamos "Conexión de red privada virtual", y pulsamos siguiente.



En la siguiente ventana, marcaremos la opción "no usar conexion inicial" a menos que queramos que con la vpn se utilice otra de nuestras conexiones a internet, si indicamos que al activar esta conexión se active antes otra conexión, por ejemplo una conexión telefónica, se conectará primero a Internet y luego se

establecerá la VPN. Si disponemos de cable o ADSL no es necesario activar ninguna de estas conexiones. Tampoco lo es si estamos conectados a Internet cuando activamos la conexión VPN o no queremos que ésta marque ninguna conexión. Por último indicamos la dirección IP del servidor VPN, esta es la dirección IP pública, es decir, la que tiene en Internet en el momento de establecer la conexión entre los clientes y el servidor.



- Al finalizar el asistente ya tendremos la conexión lista para activarse. Ahora debemos indicar el usuario y las password que hemos activado en el servidor y ya podremos conectarnos con el servidor.
  Si el servidor VPN se conecta a Internet usando un modem o Cable la IP puede cambiar (IPs dinámicas) por lo que será necesario indicarle la IP que tiene en cada momento.

Ya tenemos la conexión VPN lista para funcionar.
Si trabajamos con conexiones lentas (móden o similar) la VPN también irá lenta. Es recomendable disponer de conexiones de banda ancha para sacarle todo el rendimiento a este tipo de conexiones.

Para realizar las comunicaciones usando la VPN deberemos usar las IPs de la VPN. Es decir, además de la IP de Internet que tiene el servidor y los clientes se han generado otras IPs internas de la VPN, pues esas deberemos usar para comunicarnos con los equipos de la VPN, estas se obtendrán como las habituales, pero en el icono de la nueva conexión que aparece en la barra de notificación (junto al reloj).

En conexiones lentas, el Explorador de Windows no será capaz de mostrar los otros equipos de la red, o le llevará mucho tiempo, en ese caso, podremos acceder a ellos escribiendo en la barra de direcciones del Explorardor de Windows "\\ip_en_la_VPN" o "\\nombre_maquina" de la máquina a la que queremos acceder, por ejemplo, si la IP (en la VPN) de la otra máquina es 169.254.3.117 pondremos \\169.254.3.117 en la barra de direcciones del Explorador de Windows y de esta forma ya tendremos acceso a los ficheros e impresoras de la máquina indicada.
Para usar otros recursos, como servidores de base de datos, etc. simplemente usamos la IP en la VPN de la máquina destino.

Además, si los equipos no tienen realizada la configuración de red adecuadamente, o tienen mal asignados los permisos puede ocurrir que no se pueda acceder a recursos. Esto no es un problema de la VPN sino de cómo se tienen establecidos los permisos en cada ordenador, al igual que pasa en una red local.

Por último, y como recomendación final, es aconsejable mantener el equipo actualizado e instalar los parches y services packs que va publicando Microsoft. Al tratarse de un

servicio de red es muy vulnerable a ser atacado y si no está convenientemente actualizado podemos ser víctimas de ataques, o nuestros datos quizás no viajen lo suficientemente seguros como esperábamos.