Empecemos por lo básico. VPN son las siglas de Virtual Private Network, o red privada virtual que, a diferencia de otras palabras informáticas más crípticas como DNS o HTTP, sí nos dan pistas bastante precisas sobre en qué consisten.

La palabra clave aquí es virtual, pues es esta propiedad la que genera la necesidad de la VPN en sí, así como la que permite a las conexiones VPN ofrecerte los múltiples usos que veremos más adelante.

Para conectarse a Internet, tu móvil, PC, televisión y demás dispositivos generalmente se comunican con el router o módem que conecta tu casa con tu proveedor de Internet, ya sea mediante cable o inalámbricamente. Los componentes son distintos si estás usando la conexión de datos de tu móvil (que incluye su propio módem y habla con la antena de telefonía) pero la esencia es la misma: tu dispositivo se conecta a otro, que le conecta a Internet.

Lo más normal es que no tengas uno, sino varios dispositivos conectados al mismo router: móviles, ordenadores, consolas... En este caso cada uno tendrá asignada una dirección IP local, que no es visible desde Internet. Esto es una red local, un conjunto de dispositivos conectados de tal modo que puedan compartir archivos e impresoras sin necesidad de pasar por Internet.

Una conexión VPN lo que te permite es crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet. Es el componente "virtual" del que hablábamos antes. Obtienes las ventajas de la red local (y alguna extra), con una mayor flexibilidad, pues la conexión es a través de Internet y puede por ejemplo ser de una punta del mundo a la otra.

Cuando te conectas a una conexión VPN, esto cambia. Todo tu tráfico de red sigue yendo desde tu dispositivo a tu proveedor de Internet, pero de ahí se dirige directo al servidor VPN, desde donde partirá al destino. Idealmente la conexión está cifrada, de modo que tu proveedor de Internet realmente no sabe a qué estás accediendo. A efectos prácticos, tu dirección IP es la del servidor VPN: en muchos aspectos es como si estuvieras físicamente ahí, conectándote a Internet.

Las VPN se pueden usar de tres maneras en tu PC. Puedes añadirlas automáticamente desde los ajustes, instalar aplicaciones con ellas o simplemente recurrir a las extensiones VPN.

Para qué sirven las conexiones VPN

Seguro que con las explicaciones anteriores ya te has imaginado unas cuantas situaciones en las que las conexiones VPN podrían ser útiles. Es un secreto a voces que son especialmente importantes en el entorno corporativo, pero sus usos no acaban ni mucho menos ahí. Estos son los principales usos de las conexiones VPN.

1. Teletrabajo

El uso más obvio de una conexión VPN es la interconectividad en redes que no están físicamente conectadas, como es el caso de trabajadores que están en ese momento fuera de la oficina o empresas con sucursales en varias ciudades que necesitan acceder a una única red privada.

Desde el punto de vista de la seguridad, permitir el acceso indiscriminado a la red propia de una empresa desde Internet es poco menos que una locura. Aunque el acceso esté protegido con una contraseña, podría ser capturada en un punto de acceso WiFi público o avistada por un observador malintencionado.

Por el contrario, el riesgo disminuye si el trabajador y la empresa se conectan mediante una conexión VPN. El acceso está protegido, la conexión está previsiblemente cifrada y el trabajador tiene el mismo acceso que si estuviera presencialmente ahí.

2. Evitar censura y bloqueos geográficos de contenido

Con el apogeo de Internet y la picaresca tanto de los proveedores de contenidos como de los usuarios, se han ido popularizando otros usos más lúdicos de las conexiones VPN, muchos de ellos relacionados con un concepto muy sencillo: falsear dónde estás.

Al conectarte con VPN, tu dispositivo se comunica con el servidor VPN, y es éste el que habla con Internet. Si tú estás en China y el servidor VPN está en Estados Unidos, generalmente los servidores web creerán que estás navegando desde este país, dejándote acceder a los contenidos disponibles solo allí, como podría ser Netflix.

De igual modo, esta misma lógica se puede usar para acceder a aquellos contenidos que estuvieran censurados o bloqueados en tu país, pero no allí donde se encuentra el servidor VPN. Así es como millones de ciudadanos chinos logran conectarse a Facebook y otras 3.000 webs bloqueadas en el país.

3. Capa extra de seguridad

Aunque no es estrictamente necesario, sí es común que las conexiones VPN vengan acompañadas de un cifrado de los paquetes que se transmiten con ellas, por lo que es normal oir la recomendación de que, si necesitas conectarte a un punto de acceso Wi-Fi público, al menos uses te conectes con una VPN.

Iniciar sesión en tus cuentas bancarias mientras estás conectado a una red WiFi pública en la que no confías probablemente no sea la mejor idea del mundo, pues es relativamente sencillo para un ladrón capturar los paquetes sin cifrar y hacerse con tus cuentas de usuario. Aquí es donde entra la capa extra de seguridad que puedes conseguir mediante una conexión VPN, pues los paquetes se enviarían cifrados, de modo que aquel que está escuchando probablemente no podría hacer nada con ellos.

No obstante, hay letra pequeña en esto, pues mientras estás desconfiando de la red pública Wi-Fi, estás poniendo toda tu fé en el servidor de VPN, que puede de igual modo capturar todo tu tráfico, guardar registros de lo que haces o incluso vender tu ancho de banda al mejor postor. Una VPN es tan segura y útil como su proveedor. Si no confías en tu VPN, no la uses, pues en vez de tener una capa de seguridad adicional, tendrás al enemigo en casa y mirando absolutamente todo lo que haces en Internet.

4. Descargas P2P

Otro uso común de las conexiones VPN se encuentra en las descargas P2P, lo cual en estos tiempos generalmente es sinónimo de descargar desde BitTorrent. Antes de que me pongas un parche en el ojo, una pata de palo y me obligues a pasar por la quilla, las conexiones VPN también tienen usos en la descarga P2P aunque bajes torrents completamente legales.

Desgraciadamente es cada vez común que los proveedores de Internet decidan meter las narices en cómo enviamos y recibimos los ceros y unos en la Red, y aunque les encanta que visitemos páginas web normales, que descarguemos no les hace tanta gracia: demasiado tráfico, y además probablemente te estás descargando algo ilegal.

Algunos proveedores bloquean por completo las descargas P2P, mientras que otros simplemente la boicotean para que funcione mal y te rindas por ti mismo. Igual que puedes usar una conexión VPN para evitar la censura de tu país, también puedes en ocasiones evitar que tu proveedor de Internet boicotee tus descargas P2P.

Ventajas de las conexiones VPN

Ahora que ya sabemos qué es una conexión VPN y para qué sirve, es hora de resumir una lista de las ventajas e inconvenientes que te supone el uso de esta tecnología. Primero, la parte positiva:

- Funciona en todas las aplicaciones, pues enruta todo el tráfico de Internet, a diferencia de los servidores proxy, que solo puedes usar en el navegador web y un puñado de aplicaciones más que te dejan configurar las opciones de conexión avanzadas.

- Se conecta y desconecta fácilmente. Una vez configurado, puedes activar y desactivar la conexión a tu antojo.

- Seguridad adicional en puntos de acceso WiFi, siempre y cuando la conexión esté cifrada, claro

- Falseo de tu ubicación, como ya hemos visto en el apartado anterior, una conexión VPN es un modo eficaz de evitar la censura o acceder a contenido limitado a cierta región.

- Tu proveedor de Internet no puede saber a qué te dedicas en Internet. ¿No te apetece que tu proveedor de Internet sepa que te pasas horas viendo vídeos de gatitos en YouTube? Con una VPN no sabrán a que te dedicas, pero ojo, que sí lo sabrá la compañía que gestiona el VPN.

Cosas que debes tener en cuenta

Hasta ahora todo muy bonito, usar conexiones VPN parece estar lleno de ventajas: más seguridad, privacidad mejorada, salto de los bloqueos geográficos... Antes de que te lances a comprar un servicio de VPN o registrarte en uno gratuito, hay unos cuantos apartados que debes tener en cuenta:

- El precio. Aunque hay servicios VPN gratis, obviamente no puedes esperar mucho de ellos, pues con frecuencia estarán muy limitados, serán muy lentos o no sean muy de fiar. Hay algunas excepciones, no obstante.

- La velocidad se resiente. La diferencia entre conectarte a Internet directamente o que tus datos tracen una ruta que atraviesa medio mundo puede ser abrumadora. Si tu servidor VPN está muy lejos, experimentarás mucha latencia a la hora de navegar por la red. Además de latencia, es normal que la velocidad de descarga y subida máxima estén limitadas.

- Su seguridad no es infalible. Esto ya lo hemos dicho varias veces, pero nunca está de más repetirlo. Solo porque el icono de la conexión tenga un candado no quiere decir que la conexión sea segura, especiamente si estamos hablando de conexiones VPN basadas en el protocolo PPTP.

- No siempre pueden falsear tu ubicación. Especialmente en el móvil, cada vez hay más tecnologías por las cuales se puede triangular y aproximar tu ubicación más allá de tu dirección IP.

- No te proporcionan anonimato. Usar una VPN no supone que la navegación sea anónima. La combinación ganadora para un mayor anonimato, si hacemos caso a Edward Snowden, es usar a la vez una conexión VPN y Tor.

Usa VPN de terceros... o crea tu propio servidor

Lo más normal y rápido para empezar a saborear las ventajas de las conexiones VPN es registrarse en una de las múltiples empresas que ofrecen servicios de VPN. Pagas una cuota mensual que puede ir desde un par de euros hasta más de 10 euros y obtienes las credenciales para iniciar sesión en su servicio y con frecuencia un cliente VPN oficial propio que te facilita mucho las cosas.

Sin embargo, si quieres un control total y absoluto de tu conexión o no te fías de nadie, puedes seguir la filosofía de "si quieres algo bien hecho, debes hacerlo tú mismo". El problema con esto es que es raro que tengas acceso a un PC en otro país con el cual puedas disfrutar de algunas de las ventajas que comentábamos antes (evitar censura, bloqueos geográficos).

Hay algunas excepciones, como los trota-mundos que viajan con frecuencia e instalando un VPN en su PC en casa encuentran pueden seguir accediendo a sus archivos allá donde estén, disfrutando también de los servicios que solo estuvieran disponibles en su país, como pueden ser Netflix o Spotify.