PROXY
Un proxy es un dispositivo intermedio que se usa en la comunicación de otros dos. Mediante un proxy, la información va, primero, al ordenador intermedio (proxy), y éste se lo envía al ordenador de destino, de manera que no existe conexión directa entre el primero y el último. Lo único que hace un servidor proxy es esconder tu IP, no suelen eliminar ningún otro tipo de identificador que pueda revelar tu identidad, alguien con acceso a tu red y los datos que transmites podría espiar tu tráfico.
Si necesitas más seguridad, es recomendable usar vpn.

QUE ES VPN
Una VPN (red privada virtual) es un software sencillo que fue creado para proteger la privacidad en línea al anonimizar tu tráfico y ubicación. Esto es fundamental si quieres utilizar torrents o evitar los geobloqueos y la censura. Significa que puedes acceder a cualquier contenido del mundo y navegar con total libertad desde cualquier ubicación.

COMO FUNCIONA
Cuando usted se conecta a internet con una VPN, el cliente de su dispositivo establece una conexión con un servidor VPN seguro. Su tráfico de internet fluye por un túnel encriptado a cuyo interior no se puede acceder. Su tráfico todavía pasa por su ISP, pero debido a que está cifrado, este ya no puede ver los sitios web a los que accedes, dónde estás ubicado ni rastrearte. Las páginas web que usted visita ya no pueden ver su dirección IP original, solo la dirección IP del servidor VPN, la cual es compartida por muchos otros usuarios y cambia regularmente. Las mejores VPN utilizan miles de servidores y actualizan sus direcciones IP de forma periódica, así que los sitios no tienen suficiente tiempo para ponerlos en la lista negra y bloquearlos.

AUTENTICACIÓN
Una vez autenticados, el cliente VPN y el servidor VPN pueden estar seguros de que solo están hablando entre sí y nadie más.

TUNELIZACIÓN
La tunelización es un proceso mediante el cual cada paquete de datos es encapsulado dentro de otro paquete de datos. Esto dificulta que terceros puedan leerlos durante su tránsito.

ENCRIPTACIÓN
Los datos dentro del túnel también son encriptados de tal manera que solo el destinatario previsto puede desencriptarlos. El cifrado impide que cualquier persona o entidad, vean información confidencial que introduces en los sitios web, como tus contraseñas. Una VPN se asegura de que incluso si alguien roba tus datos, no podrían descifrarlos ni entenderlos.

POLITICA CERO REGISTROS
Una VPN de buena reputación, debería tener una estricta política de no registros y servidores basados en RAM. Los servidores basados en la RAM borran permanentemente tus registros cada vez que se reinician, por lo que tu VPN no tendrá ninguna información que compartir sobre ti, incluso si se lo exigen legalmente.

VENTAJAS

Fáciles de instalar y utilizar.

Compatibilidad con la mayoría de los dispositivos

Velocidad.

No se ve afectada por el software de cifrado y los servidores.

DESVENTAJAS

Encriptación débil.

Fallos del software.

Esto puede ocasionar que los mensajes viajen sin cifrar y fuera de la red VPN

Políticas de registro variadas

Las VPN manejan mucha información sensible, por lo que necesitan tener políticas de privacidad robustas y fuertes medidas de seguridad, las que no son fiables podrían tener acceso a tu actividad de navegación.

Si utilizas un proveedor de peor reputación, no hay forma de que te asegures de que no le echarán un vistazo a tu actividad de navegación o la compartan con terceros.

Si tu proveedor se encuentra bajo sospecha incluso te podrían obligar a compartir esta información con el gobierno.