Proxy o VPN, ¿Cuál elegir? ¿Qué nos conviene?

¿Qué elegir entre un proxy y una VPN para ser anónimo en la web? Además del servidor proxy (concepto que ya desarrollamos anteriormente), también hay otra forma de protegerse al conectarse a Internet. De hecho, con una red privada virtual o VPN también es posible proteger su conexión a Internet.

Un proxy lo conecta a una computadora remota y una VPN también lo conecta a una computadora o servidor remoto, por lo que estas dos tecnologías no deberían ser tan diferentes, ¿verdad? En realidad no … Echemos un vistazo a ambos para averiguar qué es lo que realmente necesita.

Algunas diferencias

Aunque son fundamentalmente diferentes, las VPN y los Proxies todavía tienen una cosa en común: ambos le permiten aparecer con una dirección IP diferente en Internet (para fingir que está conectado desde una ubicación diferente).

Sin embargo, su método para realizar esta tarea y el grado de protección de datos privados, cifrado de datos, etc., varían mucho entre las dos soluciones.

Los proxies ocultan su dirección IP

Un servidor proxy es un servidor que actúa como intermediario en el flujo de su tráfico de Internet, por lo que sus actividades en Internet parecen provenir de otro lugar. Por ejemplo, si vive fuera de Colombia pero desea acceder a un sitio inaccesible en el extranjero, puede conectarse a un

servidor proxy en Colombia y luego conectarse al sitio web. El tráfico de su navegador parece provenir de la computadora remota, no de su propia computadora.

Los proxies son excelentes para tareas que requieren poco ancho de banda, como ver un video de YouTube, omitir un filtro de sitio web o restricciones de IP. Desde otro punto de vista, los proxies no son tan buenos para tareas que consumen más ancho de banda. Un servidor proxy simplemente enmascarará su IP. No cifran el tráfico entre su computadora y el servidor proxy, generalmente no eliminan las credenciales después de que otra persona accede a la misma IP y, a menudo, no prestan atención a proteger su información personal.

Cualquiera que tenga acceso a su fuente de datos (su ISP, el gobierno, algún tipo que olfatee sus datos en el aeropuerto, etc.) puede encontrar toda la información de tráfico sobre usted. Además, ciertos exploits (fallas), como Flash malicioso o código JavaScript en su navegador, pueden revelar su verdadera identidad. Esto hace que los servidores proxy no se puedan utilizar para tareas más serias, como evitar que un hacker robe sus datos a través de una red WiFi pública.

Una VPN también tiene muchas ventajas

Protección de su identidad

Al conectarse a Internet con una VPN, toda la información sobre su identidad estará segura. Casi no hay posibilidad de que se filtre un poquito de información. Su dirección IP estará enmascarada, nadie podrá comunicarse con usted de esta manera.

También es una forma de protegerse de los ladrones de información personal que utilizan los datos que han recopilado para crear perfiles falsos en Internet.

Acceda a todo el contenido en Internet con total seguridad

A menudo sucede que no puede acceder a ciertos contenidos en Internet debido a una restricción vinculada a su área geográfica. Con una VPN, ya no tendrá este tipo de problemas. De hecho, una VPN le permite evitar todos estos bloqueos relacionados con el área de residencia. Solo tiene que elegir

un servidor en el país que quiera y podrá acceder a contenido de todo el mundo.

Protección de sus datos de navegación

Con una VPN, ningún software espía o incluso un espía podrá acceder a sus datos de navegación. Al tratarse de un servidor virtual, no recuerda ninguno de sus datos de navegación.

Las diferencias con un proxy

Por lo tanto, la VPN es una herramienta muy poderosa para protegerse cuando se conecta a Internet. El único inconveniente de una VPN es que se puede cobrar a diferencia de muchos proxies que puede encontrar de forma gratuita. Por otro lado, es más eficaz en todos los ámbitos a la hora de garantizar tu seguridad y anonimato en Internet.

También puede encontrar multitud de ofertas en Internet. Un proxy web puede ser suficiente si solo desea eludir el firewall de su escuela, sin usar información confidencial. Sin embargo, si está utilizando datos que no desea que se divulguen al departamento de TI de su Universidad o empresa,el VPN es mejor que un proxy.

Aunque los buenos servicios de VPN son de pago, es una herramienta imprescindible para poder conectarse a Internet de forma anónima mediante un proceso de cifrado. Un proxy es tan bueno para enmascarar su IP; sin embargo, los datos no están encriptados y, por lo tanto, están expuestos a piratas informáticos, gobiernos, etc. Dependiendo de su uso deseado, es importante elegir entre un proxy o una VPN.

Para evitar riesgos y la máxima seguridad, recomendamos encarecidamente el uso de una VPN.

Un proxy

Le permite modificar su IP en una sola aplicación o software a la vez, como su navegador o µtorrent. ✓

Sus datos no están encriptados y, por lo tanto, pueden ser interceptados por cualquier persona. ✓

Muchos proxies web son gratuitos. ✓

No permite pasar por alto todos los firewalls y el sistema de censura. ✓

La mayoría de los proxies le proporcionarán una conexión más lenta de lo normal. ✓

Un VPN

Una VPN cambia la IP en todas sus aplicaciones y software en su dispositivo. ✓

Cifrar sus datos hasta 256 bits, lo que hace que sus datos sean casi imposibles de piratear. ✓

Las buenas VPN son de pago. ✓

Acceso a cualquier sitio, gracias a IPs de casi cualquier país del mundo. ✓

Gracias al proxy SOCKS o al DNS inteligente, la velocidad de conexión apenas se verá afectada.✓

Leer también: Cómo proteger a su organización de las amenazas de seguridad en medio del aumento de los teletrabajadores ; ¿Qué es un Firewall como servicio, FWaaS? Ventajas ; Nginx como un proxy inverso, equilibrador de carga, cómo funciona