Proxy vs. VPN: 4 differences you should know

Written by Dan Rafter for NortonLifeLock

Worried about your privacy when searching the Internet? Wondering if hackers, government agencies, or companies can track what sites you visit, files you download, or links you click?

You might be wondering if it's time to sign up with a virtual private network (VPN) or proxy server to hide your location and internet-service-provider address from any snoops.

But be aware: There are significant differences between a proxy and a VPN. While both tools can protect your identity, only a VPN will encrypt your data as you browse the web.

This means that only a VPN can help hide your online activity from hackers, government agencies, and companies that might be looking to learn more about how you spend your time on the internet.

What VPNs and proxy servers are

Both VPNs and proxy servers are tools you can use to help keep your activity private when browsing the internet, sending emails, reading online message boards, streaming video, and downloading files. But both of these tools work in different ways.

A proxy server is a computer that sits between you and a server, acting as a gateway when you access the internet. When you connect to a specific website, video-streaming app, or file-sharing program from your laptop, tablet, smart phone, or any other device, you can first connect to a proxy. Once you do this, you'll be connecting to the site or app through an outside host server.

There's a clear benefit to this if you want to hide your identity. The website you are visiting — or the streaming service you are accessing or file-sharing site you are using — will only see the IP address belonging to the proxy server. It won't see your address. This will keep your identity and true location hidden from these sites and apps.

There are different types of proxies. Here are three of the most common ones.

HTTP proxies

You'd use these proxies to access websites. You can also use this type of proxy to access geo-restricted content. For instance, maybe an online video is restricted in your region. You can use a proxy server to log onto the site hosting the video, hiding the fact that your original IP address is restricted from watching it. Keep in mind, this may violate the user agreement with your content provider.

SOCKS5 proxies

These proxies don't work only on websites. You can use a SOCKS5 proxy to access video streaming services, file-sharing sites, or online games. Be aware, though, that connecting to an app through a SOCKS5 proxy might be slower because free proxies can have less configuration options, support, and slower infrastructure.

Transparent proxies

You might have used a transparent proxy without realizing that. That's the whole point. Employers — or parents, schools or libraries — might set up a transparent proxy as a way to filter user's content when they connect to the internet or block users from accessing certain websites.

A VPN is similar to a proxy, but instead of working with single apps or websites, it works with every site you visit or app you access.

Like a proxy, when you visit a website after first logging into a VPN, your IP address is hidden and replaced with the IP address of your VPN provider. This keeps your identity shielded. But unlike a proxy, this protection will remain in place as you surf to new websites, visit online streaming sites, or send emails or download files.

You can access the internet through free VPN providers. But providers that charge for VPN access are less likely to share data with third parties.

How VPNs and proxies differ

Here are four ways VPNs and proxies are different.

1. VPNs encrypt your information

The biggest benefit of a VPN over a proxy server? With VPN enabled, your browsing and any data you send or receive, will be encrypted. This is important: It means that hackers, government agencies, businesses, or anyone else won't be able to see what you're doing when online.

Say you access your online bank account while using a VPN. Because your information is encrypted, hackers won't be able to access your bank account numbers. The same is true if you log onto your credit card provider's online portal: Because your data is encrypted, criminals won't be able to snag your credit card number or the password you use to log onto the portal.

2. VPN providers promote online privacy

If you want total privacy, work with a VPN provider that has a no-log policy. "No log" means the providers pledge not to track and store your activity while you are using the service to connect to the internet. This means that these providers won't have any data to give to anyone else who wants information about what sites you browse or files you share. On the other hand, a free proxy may monitor traffic and sell data to third-parties.

3. Free proxy connections can be slower

Both proxy servers and VPNs can slow down your browsing, depending on how many users are accessing these services. Free proxy connections however can be slower and less secure because of less support, less configuration options, and slower infrastructure.

4. You may spend more with a VPN

You can connect through free VPNs. However, many tech experts recommend going with a VPN provider that charges a fee because paid services often offer more data privacy, more secure connections, and more reliable performance. Security of free VPN can be unreliable, as many providers use only one VPN connection, called point-to-point tunneling protocol (PTTP). A paid VPN service, on the other hand, can offer users data encryption which is more secure.

Do you need a proxy if you have a VPN?

No. A VPN and proxy server both mask your IP address. But a VPN will also encrypt the data you send and receive, something that a proxy server doesn't do. If you are already using a VPN, then, connecting to a website or app through a proxy server would be an unnecessary step.

What should you use, a VPN or proxy server?

When it comes to proxy vs. VPN and which one to use, the differences between the two might help you decide what's the best choice for you.

If you want to hide your IP address, using either a proxy server or VPN will work. And if you're worried about browsing speed, and you're only worried about hiding your IP address from a single site or app, then a free proxy server will do the job.

If cost is an issue, then connecting to single sites, apps, or file-sharing services through a proxy server might be the smart move. It's easy to find free proxy servers that will hide your IP address.

But if you want to keep your browsing activity hidden from snoops, logging onto the internet through a VPN is the better choice. Again, it comes down to encryption: VPNs encrypt your data while online. Proxy servers don't.

If you plan to access several sites while online, especially if you're connecting to sites such as your bank account or credit card portal, a VPN provides more security.

And while many of the preferred VPN providers will charge for their services, this price might be a small one to pay if it means that your most sensitive personal and financial information is shielded from the eyes of online snoops.

Retrieved from https://us.norton.com/blog/privacy/proxy-vs-vpn on 29 Sep 2022.