[COVID-19] 10 Tips to Speed Up Your Home Virtual Private Network

Devolutions

CORONAVIRUS PANDEMIC HAS TRIGGERED A MASSIVE DEMAND FOR VIRTUAL PRIVATE NETWORK (VPN)

The surge in employees working from home during the coronavirus pandemic has triggered a massive demand for Virtual Private Network (VPN) technology. For example, reports show that global use of some VPNs has jumped a whopping 165 percent since March 11.

The good news is that VPNs significantly improve security by routing internet traffic between an endpoint and a server through an encrypted virtual tunnel. The bad news is that VPNs aren't designed to handle this much activity — and as such, many users are experiencing S-L-O-W data connections. Not only is this tedious, but it can make it impossible to participate in video conferences or watch streams.

Granted, VPN usage is not the only reason for the slowdown. There are many more people continuously accessing the internet today than there was just a couple months ago. But VPN usage is a significant factor that is causing a lot of frustration.

Obviously, shutting down VPNs is not an option. While they are not bulletproof, they are massively more secure than ordinary public Wi-Fi access (including home networks, which by default are not as secure as many non-IT business users believe!). As such, the only way forward is to find ways to accelerate VPNs as much as possible.

To that end, here are 10 VPN speed-boosting tips. If you are already using these, then we invite you to share this information with your end users who, in an effort to increase speed, may be tempted to shut down their VPN or remove critical security protections (e.g. firewall, antivirus, etc.).

1. If your home network Wi-Fi router supports both 2.5 GHz and 5 GHz, switch to 5 GHz for a faster connection. However, keep in mind that the shorter waves used by the 5 GHz band for 5G means that it is less capable of penetrating walls and solid objects (e.g. furniture). If this occurs, you may be able to overcome it by using a good range extender. Or better yet, use a hardwired ethernet connection.
2. Use a tier 1 VPN service, which, unlike a tier 2 VPN service, can reach any address on the internet without needing to make stops or take detours along the way. This is because tier 1 VPN service providers own their network, while tier 2 VPN service providers don't.
3. Set up the VPN on each device instead of on your router. If you prefer a router-based VPN to cut down on administration (i.e. each device doesn't need its own login), then get a dedicated VPN router. They are more expensive than standard routers, but they have next-gen CPUs and RAM to support faster connectivity.
4. Pick a server that's nearby. If you're located in Chicago, then you'll probably get faster data connection by choosing a server located in St. Louis vs. a server located in Los Angeles. Why "probably" instead of "definitely"? Because sometimes nearby servers are so popular that they get overloaded. In such cases, it can actually be beneficial to choose a server that is located further away. You'll probably need to do some experimenting and speed testing to find the optimal connection.
5. Shut down background apps you don't currently need that are taking up bandwidth and resources.
6. Update your VPN client. Sometimes, issues and bugs can lead to slowdowns.

7. Switch the protocol from TCP to UDP. However, keep in mind that in some cases this may lead to a more unstable connection.
8. Use split tunneling to route sensitive device or app traffic through the encrypted VPN tunnel, while non-sensitive device or app traffic is sent directly to the ISP.
9. Speaking of your ISP: it could be the source of your frustration, rather than your VPN. If so, then look into upgrading to a faster tier. If this isn't possible, switching ISPs may be necessary.
10. And speaking of switching: when it comes to speed, your VPN may be over-promising and under-delivering. If so, look into upgrading to a faster tier or finding another service. Keep in mind that free VPN services are always going to be slower than paid services, and there are some serious security concerns as well.

The Bottom Line

Before the coronavirus pandemic, using a VPN was important. But now that hackers are specifically targeting remote workers, using a VPN is essential. We hope the above tips help you and your users stay safe and productive — since you need both, and not one or the other.

Do you have any other tips or advice to speed up VPNs? Please comment below so that the community can benefit from your knowledge and experience.