

- Computer networks / Internet service providers / Intranets

## Make a VPN faster: 10 tips & tricks

If you use a VPN, it can slow down the speed of your internet connection. Here are tips on how to avoid this.

PCWorld (USA) · 1 Mar 2024 · 98 · BY FLORIAN KASTNER & BIRGIT GÖTZ

A virtual private network (VPN) is an ideal solution for protecting your privacy and hiding your location from the view of others on the web. But using a VPN can sometimes lead to reduced internet speed. In this article, we will present various methods for and tips on how you can optimize the speed of your VPN.



### 1. TEST THE SPEED OF YOUR INTERNET CONNECTION

Firstly, disconnect from your VPN such as NORDVPN ([fave.co/3odm11r](https://fave.co/3odm11r)) or Cyberghost ([fave.co/3umving](https://fave.co/3umving)) and then test the speed of your internet connection with Speedtest ([fave.co/3i27uhv](https://fave.co/3i27uhv)). Run the test again when you are connected to the VPN to see if the problem is really with the VPN or with your broadband provider.

### 2. CHANGE THE LOCATION OF YOUR VPN SERVER

One of the most effective ways to speed up your VPN is to change the location of your server. The location of the VPN server has a direct impact on your internet speed.

For example, if you are in the United States and the geographical location of the server is not critical for your activities, you should choose a server in your region of the country. This keeps the distance short and improves the speed.

The latency time—that is, the time it takes for data to reach the server and back—is significantly higher with a distant server. Even a high-quality VPN cannot change this physical fact, although the latency can vary depending on the quality of the VPN provider.

Another important aspect is server utilization. An overloaded server responds more slowly than a less frequented one. It is therefore worth choosing a server with a smaller number of users.

In most VPN applications, you will find a list of available servers, often with information on the current utilization or ping—meaning the response time. For activities such as online gaming, where every millisecond counts, you should choose a server with the lowest possible ping in your geographical area to minimize latency. These small adjustments can make a big difference to the speed and performance of your VPN.

### 3. RESTART YOUR DEVICE

It is possible that your device's operating system is overwhelmed by the complex encryption of the VPN service. A restart can provide a quick and easy solution here.

Another tip: Test the VPN connection on another device. This will help you determine whether the problem is specific to your original device.

### 4. RESTART YOUR ROUTER

Restarting your router can also be helpful if your VPN is slow. Disconnect the router either by unplugging it from the power supply or by pressing the power button. Then wait 10 to 15 seconds before switching the device back on. Please note that it may take a short moment for the router to re-establish the internet connection.

## 5. CONNECT ROUTER AND PC VIA CABLE

An effective way to improve your VPN connection is to connect your laptop or PC directly to the router via a LAN cable. This avoids potential performance issues that could arise from a Wi-fi connection. While Wi-fi is practical and convenient, it can lead to increased latency, especially if objects in the room or walls affect the signal strength.

## 6. CHOOSE A DIFFERENT PROTOCOL

Each VPN protocol uses different encryption standards to secure your data. While some protocols are more performance orientated, others offer higher security, but often at the expense of performance. Wireguard, for example, is a modern and fast protocol that is also supported by providers such as IVPN ([fave.co/3sq9zu7](https://fave.co/3sq9zu7)). IKEV2 and OPENVPN, on the other hand, are two established, reliable standard protocols, but they can lag behind Wireguard in terms of speed.

With OPENVPN ([fave.co/3szrldy](https://fave.co/3szrldy)), you also have the option of choosing between the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols. UDP is faster, which is why it is normally used for streaming.

You should therefore switch from TCP to UDP as a trial. In addition to OPENVPN and IKEV2/ Ipsec, there are also protocols such as L2TP/ Ipsec that you can try out. Please note, however, that L2TP is less secure. If you use a VPN primarily for security reasons and less to access regionally restricted content, this step is not recommended.

## 7. CHANGE THE PORT

In addition to adjusting the protocol and security settings, you should also pay attention to the port selection. When a VPN connects to the web, it does so via a previously defined port. In general, this is fine. However, some networks can also throttle or restrict the use of this port, which in turn can lead to problems. Check the settings of your VPN to see if there is a way to change the port used. If so, try opting for port 443. This is the most common solution for VPN speed issues related to port selection.

## 8. SWITCH OFF YOUR FIREWALL AND ANTIVIRUS SOFTWARE

Just as encryption can overload your PC'S data processing workload, so can antivirus and firewall settings. If you notice a drop in performance, switch off the firewall and antivirus program temporarily and see if this improves the situation.

If this solves the problem, you should look for alternative software that does not affect PC performance. However, do not leave your PC running without security software.

## 9. USE SPLIT TUNNELLING

Premium providers such as Expressvpn ([fave.co/42djtqo](https://fave.co/42djtqo)) or NORDVPN ([fave.co/3ODM11R](https://fave.co/3ODM11R)) are among the best split-tunneling VPNs. Split tunneling is a function that allows you to split your device's data traffic: Part of the data is routed through the VPN, while the other part goes directly through your normal internet connection. This method can significantly improve the internet speed and efficiency of your VPN, as not all data needs to be rerouted through the VPN server.

This is particularly useful if you want to access local network resources and access the internet via the VPN at the same time.

For example, you can use local services such as printers or file shares while simultaneously accessing geographically restricted content via the VPN. By reducing the amount of data routed through the VPN, you can increase the speed and reduce the load on the VPN server.

## 10. CHANGE YOUR VPN PROVIDER

Some VPNs are faster than others. If the one you are currently using is not fast enough for you, go to another provider. However, keep in mind that VPN speeds change depending on the time of day, day of the week, and other factors, such as server selection. Here you will find a comparison of the best VPN services currently available: [fave.co/3fttms](https://fave.co/3fttms). As many VPN providers offer refunds or free trials, you can at least download their app, sign up, and try the service.