A short guide to find a good VPN service provider

Clemens Prill

01.05.2017

Preamble

The market is full of VPN service providers – from cheap to expensive providers, from very bad ones to very good ones. This makes it hard to do a good choice! With this short aricle I want to give you some advices to make a good choice! Keep in mind that this article is written from what I have learned by good and bad experiences.

A short note: This guide is not designed for persons who really need extreme bulletproof-alike VPN service providers. Rather this guide is made for newbies and advanced users of VPN service providers.

I'm sorry for any linguistical mistakes I did in this document. Please, feel free to correct me and to let me know so I can fix them! Furthermore I'm open for all kind of feedback, suggestions and corrections. You will find the latest version of this guide at this Github repository.

General

First of all: Keep in mind that offering a VPN is not different to offering you any other service like serving you your ordered meal in a diner. At the end of the day you can expect the same quality and quantity – because you paid for it!

What does this mean, regarding expectations we can have towards our VPN service provider? This means that we can expect:

a) a company and person who is legally and personally responsible,

b) someone who helps us with issues we might face,

c) a working and secure provider website,

d) a working and secure VPN service.

Let's talk about what this means in detail:

Legal and personal responsibility

We pay for a service and thus we can expect it to work. If it doesn't work, we want someone to take the responsibility for it! Thus it is necessary that we know who runs the service. Our VPN service provider should be registered as a juristic person and a natural person should be stated on their website. This makes sure we could sue them if necessary but more important: the person who runs the service can't simply get away if his or her reputation gets damaged and just found a new anonymous company under a new name. A serious business doesn't have to hide who runs it nor does it want to. Always look up reviews about the VPN service provider. A short list of websites with VPN service provider reviews:

- BestVPN.com
- TorrentFreak.com

I'm not related to any of these websites. Use them as a first impression and evaluate yourself how much you can trust these reviews and the reviewed providers, optionally with assistance of this guide. Also it could be useful to search for the provider to find threads about downtimes, issues other people faced, etc.

Support

At first you might think that you will never need any support from your VPN service provider. This is the case when everything works out like you expect it. Sadly, there are situations which we can't predict or prevent. So let us predict that you have bad luck and you have issues.

Of course I could use a search engine for days and solve my issue myself. But let's be honest: Who wants to invest a lot of time and effort to get a service working you have paid? Nobody! Rather we should take support quality in account when we choose our future VPN service provider. We can expect the support to reply within 24 hours and to be technically skilled. Thus they should be able to help us fix our issue. A bonus they have: They deal all the time with VPN issues and they are up to date regarding technology and important changes in the market. A customer will never have more experience than a professional provider. This counts for any kind of business or industry!

If you want to know how good their support could be, before becoming a customer of them: Just ask their presale team or if none exists the support directly some questions. Then you will get a first impression of their response time and answer's quality.

Another quite important thing related to support inquiries: If you can't write a ticket over the VPN service provider's website, you have to write an email. Emails are insecure by default and thus not designed for sensitive data. If you

can't write encrypted emails to your provider: Do not transfer any sensitive data. Better: Look for a provider who can be contacted safely.

Website

This point may sound weird to you but it is essential: Did you ever realize how much a provider's website says about its business? A lot! If your provider is not able to provide a modern website with bearing industry-standards in mind: **Run away!**

If one of these things is given, please don't choose that VPN service provider:

a) no TLS or only TLS < version 1.2 (version 1.2 is from 2008!),

b) tracking-scripts included like Google Adwords, Google Analytics or similar services,

c) no Terms of Service (ToS) or Privacy Policy,

d) external support scripts like providesupport.com or similar services,

e) non-working features on the site.

If one of these applies, it is very likely that you won't have fun with that provider. If more than one these applies, it is nearly guaranteed that you are going to choose a bad provider!

VPN service itself

A VPN service should protect us from surveillance and monitoring by curious governments and ISPs. Furthermore it should protect us while we are in insecure networks like WIFIs, owned by third parties or networks where we can't trust every device. This is done by encrypting the whole traffic from our system and forward it over the servers of our VPN service provider. Sadly there are sometimes badly configured VPN services. The security of a VPN service depends highly on how they are configured and set up.

DNS leak

A common problem is that the VPN service could leak your IP address. To see if this happens, connect to your VPN service and visit this site:

DNSleaktest.com

Enable JavaScript for this page and click on 'extended test'. Wait till the test is finished. If you see a DNS server in the list which is **not** owned by your

VPN service provider, you got a DNS leak here. This is a serious issue. It will affect your privacy and anonymity online! You should contact your VPN service provider to get help to fix this. Multiple situations could lead to this.

Another test I suggest is this one:

IPleak.net

Again, enable JavaScript and wait for the results. While you are connected to your VPN service, you shouldn't see your real IP address or ISP's DNS servers in the results. Additionally you can try the torrent test on this site.

Protocols and encryption strength

There are different protocols for VPN services. Each of these protocols have pros and cons. There are more safety protocols, there are less safe protocols. I suggest to read a comparison of the different protocols to know which one you should use and when you can't use a specific one. See this link:

- Guide: PPTP vs L2TP vs OpenVPN vs SSTP vs IKEv2, BestVPN.com.

You should only send as little as possible and necessary information over a VPN service. A VPN service could be hacked too, like any other service. This makes it a risk to send sensitive data over a VPN service, even though it is a tiny risk maybe. Do not expect a VPN provider to disclose ever that its VPN service has been hacked. Such an admission is the dead for any VPN service provider because it lost its trust forever towards customers.

Please keep in mind that an encryption is only strong if it is not vulnerable to known attacks and if the used key length is big enough. I suggest a read on this article:

- English Wikipedia: Key size.

Your VPN service provider should know this and configure its servers appropriate.

Server locations

Your VPN service provider should provide servers near to you and in different countries. You need servers near to you so that you can still surf safely without a high latency. Servers in different countries is necessary because not everything is allowed in every country. You have to respect the local laws of the server's location because if it is legal in your country, it doesn't mean it is legal in the other country. Otherwise in worst case the server could be taken offline by the local police.

Port forwarding

Sometimes you need open ports to use certain software behind a VPN service, for example P2P-applications. Make sure your VPN service provider does provide you with open ports by default or that you can do port forwarding yourself in customer panel or by opening a support inquiry.

Good luck!

As my last words, I want to wish you good luck with finding a good VPN service provider. If you made a bad choice, just change your provider. It is always quite hassle free and easily done!