Everything you need to know about Virtual Private Networks (VPNs)

Route your traffic through another network
Virtual Private Networks (VPNs) What Is a VPN, Why Would I need one and what is VPN service providers

©DFR, 2017

All rights reserved. No part of the publication may be reproduced or transmitted in any form or by any means without the prior permission of the publisher.

First published in sep 2016

…
Virtual Private Networks (VPNs) are veritable Swiss Army Knives when it comes to privacy enhancement, censorship avoidance, anonymous file sharing, and more. But not all VPNs are created equal, and there’s no sense paying for features you don’t need. We’re about to walk you through what VPNs are, why people use them, how to assess your VPN needs, and the important questions to ask when shopping for a VPN. If you’re impatient and you just want a really good VPN right this second, you can always jump right to the end and check out our recommendations. A thorough read from start to finish, however, will show you why we’re recommending the services we are.
1. What Is Virtual Private Networking, and Why Do People Use It?

Through the use of software (and sometimes, at the corporate and governmental level, hardware) a VPN creates a virtualized network between two physically separate networks.

VPN use, for example, allows an IBM employee to work from home in a Chicago suburb while accessing the company intranet located in a building in New York City, as if he was right there on the New York office’s network. The same technology can be used by consumers to bridge their phones and laptops to their home network so, while on the road, they can securely access files from their home computers.
VPNs have other uses cases, though. Because they encrypt your connection, VPNs allow users to prevent others from seeing the data they’re transferring. This keeps data secure, particularly on public Wi-Fi networks in places like coffee shops and airports, ensuring no one can snoop your traffic and steal your passwords or credit card numbers.

Since VPNs route your traffic through another network, you can also make it appear as if it’s coming from another location. That means if you’re in Sydney, Australia, you can make your traffic appear to come from New York City. This is useful for certain sites that block content based on your location (like Netflix).
It also allows some people (we’re looking at you, Australians) have to deal with insanely high import taxes on software that see them paying twice (or more) what US consumers pay for the same products.

Since VPNs route your traffic through another network, you can also make it appear as if it’s coming from another location. That means if you’re in Sydney, Australia, you can make your traffic appear to come from New York City. This sites block content based on your location (like Netflix). It also allows some people have to deal with insanely high import taxes on software that see them paying twice (or more) what US consumers pay for the same products.
2. Assessing Your VPN Needs

Every user is going to have slightly different VPN needs, and the best way to pick the ideal VPN service is to take careful stock of what your needs are before you go shopping. You may even find you don’t need to go shopping because home-grown or router-based solutions you already have are a perfect fit. Let’s run through a series of questions you should ask yourself and highlight how different VPN features meet the needs highlighted by those questions.

To be clear, many of the following questions can be satisfied on multiple levels by a single provider, but the questions are framed to get you thinking about what is most important for your personal use.
3. Do You Need Secure Access to Your Home Network?

If the only use case you care about is securely accessing your home network to, then you absolutely do not need to invest in a VPN service provider. This isn’t even a case of the tool being overkill for the job; it’s a case of the tool being *wrong* for the job. A remote VPN service provider gives you secure access to a remote network (like an exit node in Amsterdam), not access to your own network.

To access your own home network, you want a VPN server running on either your home router or an attached device (like a Raspberry Pi or even an always-on desktop computer).
Ideally, you’ll run the VPN server at the router level for best security and minimal power consumption. To that end, we recommend either flashing your router to DD-WRT (which supports both VPN server and client mode) or purchasing a router that has a built-in VPN.

4. Do You Need Secure Casual Browsing?

Even if you aren’t particularly security or privacy conscious, everyone should have a VPN if they regularly use public Wi-Fi networks. When you use Wi-Fi at the coffee shop, the airport, or the hotel you’re staying at while traveling cross-country, you have zero idea whether or not the connection you’re using is secure.
The router could be running outdated and compromised firmware. The router could actually be malicious and actively sniffing packets and logging your data. The router could be improperly configured and other users on the network could be sniffing your data or probing your laptop or mobile device. You never have any guarantee whatsoever that an unknown Wi-Fi hotspot isn’t, either through malice or poor configuration, exposing your data. (A password doesn’t indicate a network is secure, either—even if you have to enter a password, you could be subject to any of these problems.)

In such scenarios, you don’t need a beastly VPN provider with massive bandwidth to secure your email, Facebook, and web browsing activities.
In fact, the same home VPN server model we highlighted in the previous section will serve you just as well as a paid solutions. The only time you might consider a paid solution is if you have high-bandwidth needs that your home connection can’t keep up with (like watching large volumes of streaming video through your VPN connection).

5. Do You Need to Geo-Shift Your Location?

If your goal is to appear as if you’re in another country so you can access content only available in that are (e.g. BBC Olympic coverage when you’re not in the UK) then you’ll need a VPN service with servers located in the geographic region you wish to exit the virtualized network in.
Need UK access for that Olympic coverage your crave? Make sure your provider has UK servers. Need a US IP address so you can watch YouTube videos in peace? Pick a provider with a long list of US exit nodes. Even the greatest VPN provider around is useless if you can’t access an IP address in the geographic region you need.

Do You Need Anonymity and Plausible Deniability?

If your needs are more serious than watching Netflix, a VPN may not be for you. Many VPNs promise anonymity, but few can actually provide it—and you’re still trusting the VPN provider with access to your traffic, which isn’t ideal. For that, you likely want something more like Tor,
which—while not perfect—is a better anonymity solution than VPNs.

Many users do, however, rely on VPNs to create some plausible deniability when doing things like file sharing on BitTorrent. By making their traffic appear as if it’s coming from a different IP address, they can put one more brick on the wall obscuring them from others in the swarm. Again, it isn’t perfect, but it is helpful.

If that sounds like you, you want a VPN provider that doesn’t keep logs and has a very large user base. The bigger the service, the more people poring through every exit node and the more difficult it is to isolate a single user from the crowd.
A lot of people avoid using VPN providers based out of the United States on the premise that US law would compel those providers to log all VPN activity. Counterintuitively, there are no such data logging requirements for US-based VPN providers. They might be compelled under another set of laws to turn over data if they have any to turn over, but there is no requirement they even keep the data in the first place.

In addition to logging concerns, an even bigger concern is the type of VPN protocol and encryption they use (as it’s much more probable a malicious third party will try and siphon up your traffic and analyze it later than they will reverse engineer your traffic in an attempt to locate you).
Considering logging, protocol, and encryption standards is a great point to transition into the next section of our guide where we shift from questions focused on our needs to questions focused on capabilities of the VPN providers.
6. Selecting Your VPN Provider

What makes for a VPN provider? Aside from the most obvious matter, a good price point that sits well with your budget, other elements of VPN selection can be a bit opaque. Let’s look at some of the elements you’ll want to consider.

It’s up to you to answer these questions by reading over the documentation provided by the VPN service provider before signing up for the service. Better yet, read over their documentation and then search for complaints about the service to ensure that even though they claim they don’t do X, Y, or Z, that users aren’t reporting that they are in fact doing just that.
6.1. What Protocols Do They Support?

Not all VPN protocols are equal (not by a long shot). Hands down, the protocol you want to run in order to achieve high levels of security with low processing overhead is OpenVPN.

You want to skip PPTP if at all possible. It’s a very dated protocol that uses weak encryption and due to security issues should be considered compromised. It might be good enough to secure your non-essential web browsing at a coffee shop (e.g. to keep the shopkeeper’s son from sniffing your passwords), but it’s not up to snuff for serious security. Although L2TP/IPsec is a significant improvements over PPTP, it lacks the speed and the open security audits found with OpenVPN.
Long story short, OpenVPN is what you want (and you should accept no substitutions until something even better comes along).

There’s currently only one scenario where you would entertain using L2TP/IPsec instead of OpenVPN and that’s for mobile devices like iOS and Android phones. Currently neither Android nor iOS supports native OpenVPN (although there is third-party support for it). Both mobile operating systems do, however, support L2TP/IPsec natively and, as such, it’s a useful alternative.

A good VPN provider will offer all of the above options. An excellent VPN provider will even provide good documentation and steer you away from using PPTP for the same reasons we just did.
You should also check the pre-shared keys they use for those protocols, since many VPN providers use insecure and easy-to-guess keys.

6.2. How Many Servers Do They Have and Where?

If you’re looking to access US media sources like Netflix and YouTube without geo-blocking, then a VPN service with the majority of its nodes in Africa and Asia is of very little use to you.

Accept nothing less than a diverse stable of servers in multiple countries. Given how robust and widely used VPN services have become it isn’t unreasonable to expect hundreds, if not thousands, of servers across the world.
In addition to checking how many servers they have and where those servers are located, it’s also wise to check into where the company is based and if that location aligns with your needs (if you’re using a VPN to avoid persecution by your government, then it would be wise to avoid a VPN provider in a country with close ties to your country).

6.3. How Many Concurrent Connections Are Allowed?

You might be thinking: “I only need one connection, don’t I?” What if you want to set up VPN access on more than one device, for more than one family member, on your home router, or the like? You’ll need multiple concurrent connections to the service.
Or, perhaps, if you’re particularly security oriented, you’d like to configure multiple devices to use multiple different exit nodes so your collective personal or household traffic isn’t all bundled together.

At minimum, you want a service that allows for at least two concurrent connections; practically speaking at the more the better (to account for all your mobile devices and computers) and with the ability to link your router to the VPN network is preferable.
6.4. Do They Throttle Connections, Limit Bandwidth, or Restrict Services?

ISP throttling is one of the reasons many people turn to VPN networks in the first place, so paying extra for a VPN service on top of your broadband bill just to get throttled all over again is a terrible proposition.

Bandwidth restrictions might not have been a big deal in the pre-streaming era, but now that everyone is streaming videos, music, and more, the bandwidth burns up really fast. Avoid VPNs that impose bandwidth restrictions unless the bandwidth restrictions are clearly very high and intended only to allow the provider to police people abusing the service.
In that vein, a paid VPN service restricting you to GBs worth of data is unreasonable unless you’re only using it for occasional, basic browsing. A service with fine print that restricts you to X number of TBs of data is acceptable, but really unlimited bandwidth should be expected.

Finally, read the fine print to see if they restrict any protocols or services you wish to use the service for. If you want to use the service for file sharing, read the fine print to ensure your file sharing service isn’t blocked. Again, while it was typical to see VPN providers restrict services back in the day (in an effort to cut down on bandwidth and computing overhead) it’s more common today to find VPNs with an anything-goes policy.
6.5. What Kind of Logs, If Any, Do They Keep?

Most VPNs won’t keep any logs of user activity. Not only is this of benefit to their customers (and a great selling point) it’s also of huge benefit to them (as detailed logging can quickly consume disk after disk worth of resources). Many of the largest VPN providers will tell you as much: not only do they have no interest in keeping logs, but given the sheer size of their operation they can’t even begin to set aside the disk space to do so. Although some VPNs will note that they keep logs for a very minimum window (such a only a few hours) in order to facilitate maintenance and ensure their network is running smoothly, there is very little reason to settle for anything less than zero logging.
6.6. What Payment Methods Do They Offer?

If you’re purchasing a VPN for securing your traffic against snooping Wi-Fi nodes while traveling, or to route your traffic safely back to the US, anonymous payment methods aren’t likely a very high priority for you. If you’re purchasing a VPN to avoid political persecution or wish to remain as anonymous as possible, then you’ll be significantly more interested in services that allow for payment through anonymous sources like cryptocurrency or gift cards.

A number of VPN providers have systems in place where they will accept gift cards from major retailers (that are totally unrelated to their business) like Wal-Mart or Target in exchange for VPN credit.
You could buy a gift card to any number of big box stores using cash, redeem it for VPN credit, and avoid using your personal credit card or checking information.

6.7. Do They Have a Kill Switch System?

If you are depending on your VPN to keep your activities even mildly anonymous, you need some sense of security that the VPN isn’t just going to go down and dump all your traffic out into the regular internet. What you want is tool known as a “kill switch system”. Good VPN providers have a kill switch system in place such that if the VPN connection fails for any reason it automatically locks down the connection.
7. Our Recommendations

At this point, your head might be understandably spinning at the thought of all the homework you’ve got ahead of you. We understand that selecting a VPN service can be a daunting task and that even armed with the questions we outlined above you’re just not sure where to turn.

We’re more than happy to help cut through all the jargon and ad copy to help get to the bottom of things and, to that end, we’ve selected three VPN service providers that we have direct personal experience with and that meet our VPN selection criteria.
7.1. StrongVPN

Our current top recommendation, as it meets the needs of both power users and casual users alike, is StrongVPN. Prices start at $10 a month and drop quickly, when you purchase a year of service at a time, to $5.83 a month. The ease of setup is fantastic—if you’re new to VPNs and/or don’t have extra time to fuss with manual settings, you can just download their setup app for Windows, OS X, iOS,
and Android to automate the setup process. If you want a more granular control or need to manually configure devices like your router, you can follow one of their many guides for different operating systems and hardware to do it manually.

StrongVPN has exit nodes in 43 cities, 20 countries, and supports PPTP, L2TP, SSTP, IPSec, and OpenVPN protocols—you’ll be hard pressed to find a device you can’t configure to use their service. There are no bandwidth caps, speed limits, or restrictions on protocols or services (torrenting, Netflix, you name it, they don’t care). Additionally, StrongVPN maintains no server logs.
Although StrongVPN does limit you to two concurrent connections per account (not installation on two devices, mind you, two different connections at one time), you can configure your home router to connect to their service, so it’s really more like you have a connect for at home and a connection for your device while you’re out and about.
If you’re looking for a VPN service with a big name behind them, SurfEasy might be just the service you’re looking for. You may recall much chatter in the spring of 2015 when Opera announced there web browser would now come with a free unlimited VPN service. That integrated service is driven by SurfEasy, the company they acquired for the task.
Despite the acquisition, however, the company still runs full service VPN access for non-Opera users and for $11.99 a month (or $6.49 a month when paid for yearly), you can use it on up to five of your devices. (They also have a free trial for the first 500MB.)

It doesn’t log, doesn’t block protocols like BitTorrent, and has no bandwidth restrictions. There are servers in 13 countries with thousands of servers available to support high speed use by a large customer base.

There’s less variety for power users in terms of which protocol they can use, compared to StrongVPN, but practically speaking the restriction of Windows, Mac, and Android devices to OpenVPN and iOS devices to IPsec isn’t cause for concern.
And what you lose in power, you make up for with an incredibly easy-to-use app.

Of interest to the particularly privacy conscious, you can pay cash for a SurfEasy gift card at U.S. locations like Best Buy and OfficeMax to redeem anonymously.
7.3. TunnelBear

If you’re looking for something free, look no further. If StrongVPN and SurfEasy are like like a solid mid-class sedan, **TunnelBear** is more like the econo-car (if you buy a TunnelBear subscription) or the city bus (if you use their generous free program). That’s not a knock on TunnelBear, either—they’ve been around for years and their free service tier has been of great utility to people in need all over the world.
The free TunnelBear service offers up to 500MB per month. That’s not a whole lot of data, but it’s enough for occasional light browsing on public networks. If you need more data than that, you can upgrade to their professional accounts for $7.99 per month.

The free account is limited to a single user, while the premium account enabled unlimited bandwidth for up to five computers or mobile devices. TunnelBear doesn’t list the total number of servers on their site, but they do offer servers in 20 countries. Their Windows and Mac OS X client is based on OpenVPN and their mobile VPN system uses L2TP/IPsec. Unlike the previous two sites, however, TunnelBear has a firmer stance against file sharing activities and BitTorrent is blocked.
Their speeds also aren’t quite as fast as the others, so you might experience a slower connection with TunnelBear.

From a feature-to-dollar standpoint, TunnelBear’s premium offering doesn’t beat out our two previous recommendations. StrongVPN and SurfEasy are better bets if you’re willing to pay. But, TunnelBear does offer a free tier, doesn’t maintain logs, and it is extremely easy to get up and running with their dead-simple apps for desktop and mobile users alike.