A guide to use the internet anonymous and secure.

Version 0.0.1 May, 2015

A big thanks to all Open Source Software Creators, The TOR Project and Anonymous.

You may discuss this guide on http://www.anonboards.com/
and download the offline version here: http://anonguide.za.ru/

Notice: You won't see how to setup or configure this concepts exactly step by step. But you will learn how it works. For detailed information about how to setup you may visit the homepage of the particular service. For example how to setup a VM on VMware Player you may visit the Knowledge Base. Or to know how to install i.e. Ubuntu you may visit their official website. But in most cases you just need to run any installer and it will tell you what to do.

Index

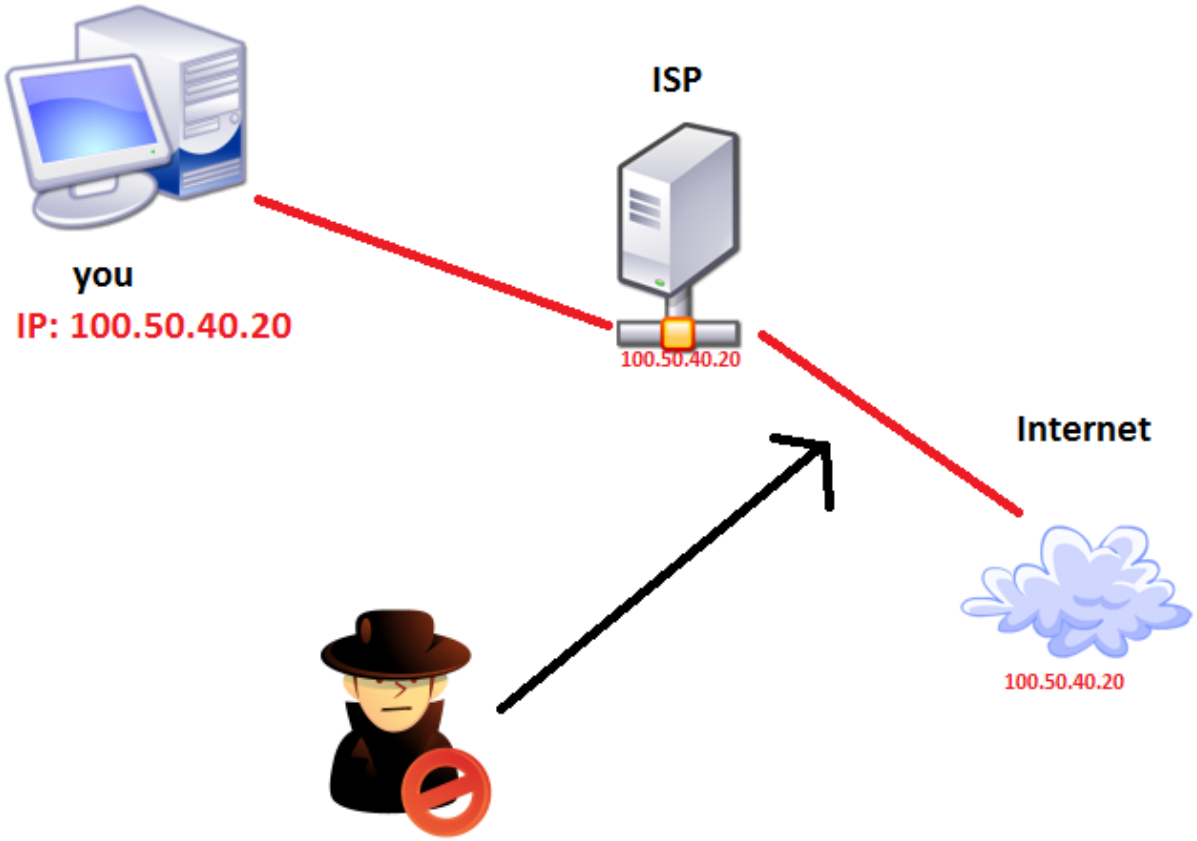
1. Anonymity and privacy

Websites to test your anonymity:
http://ipleak.net/
https://www.dnsleaktest.com/
http://www.cloakfish.com/
http://whoer.net/extended

Open the websites above before continue reading.

Caution! Anonymity does not make you safe from hackers (not directly), viruses, malicious software or spyware. When I write <secure> in terms of anonymity, it means your internet connection between you and the internet itself and your anonymity is secure.

Not secured internet connection



How it works: your router/modem connects to your ISP and you get an IP. With this IP you surf the web and every website you visit knows your IP. Therefore your ISP also knows what websites you are visiting. He knows everything about you and what you are doing. The connection is NOT encrypted so he sees all the data being transferred between you and others (chats, files, mails, streams, videos etc.). Also you may visit a malicious website made by hackers. Now they know your IP, they may connect to you and harm your system, steal your data (pics, credit card numbers etc.) or even take over your identity.

Another point is the government or police. If you do something illegally by mistake or else, they'll go to your ISP and will ask for your name and address so they can charge you for breaking the laws. **Your IP is your identity**. Normally an ISP is not allowed to give anyone your real address and name, but only police or gov. This request is going through a court. For example if you've downloaded illegally music/movie/anything, the court will allow your ISP to give your personal info. You're fucked.

Solutions:

Preparations:

First of all, configure your browser!

I'm using **Firefox**, but I know you need to disable the same things on Google Chrome. For all other browsers, just google for more information how to disable this things, if needed.

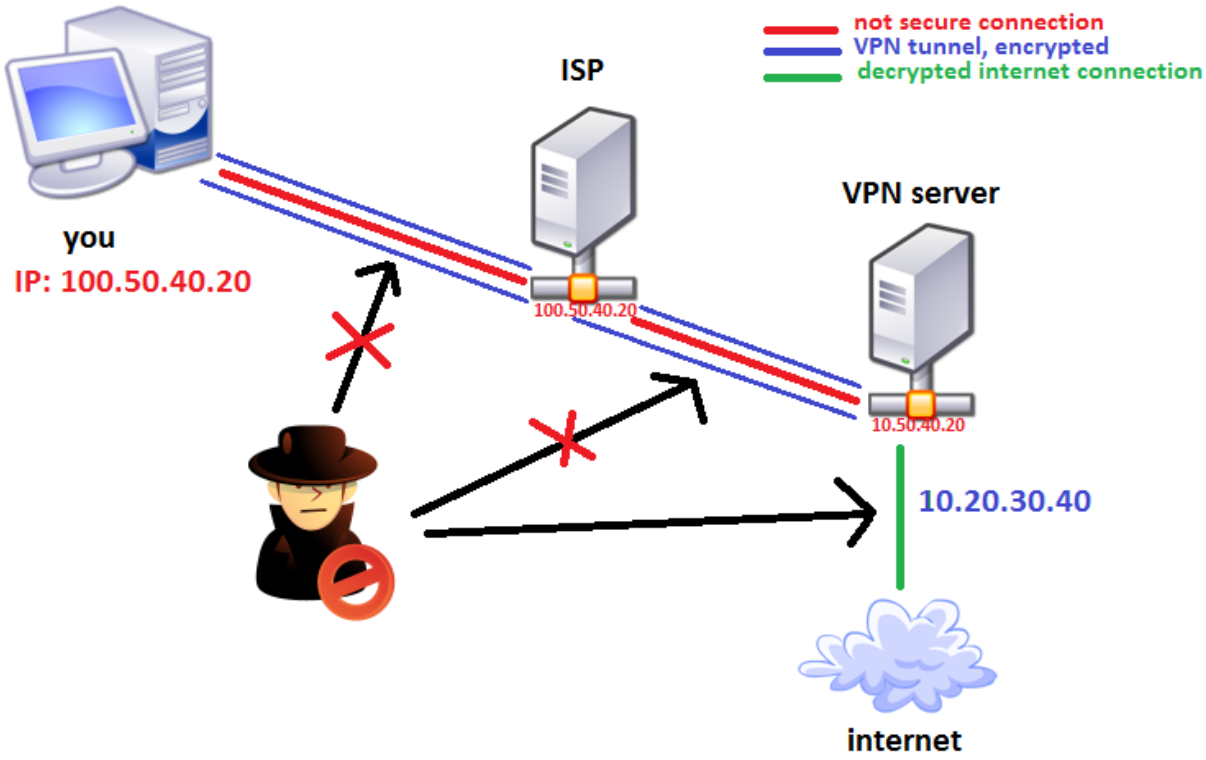
1. Go to Options -> Privacy -> History -> Accept third-party cookies -> choose [**never**]
2. The same path -> Keep until -> choose [**I close Firefox**]
3. navigate to **about:config** -> media.peerconnection.enabled -> change to **false** (this is needed due to WebRTC detection which leaks IPs) *(WebRTC = Real-Time Communications, it allows the browser to video/voice chat with other browser user)*
4. navigate to **about:config** -> network.websocket.enabled -> change to **false** (old Firefox or -> TOR - Browser <-) *(This will disable the forced connection to <standard/nearest DNS server".)*
5. navigate to **about:config** -> geo.enabled -> set the value to **false** *(This will disable geo-locations for your browser.)*

I recommend you this Firefox addons:

- BetterPrivacy 1.68 - *deletes all cookies from the HDD after each Firefox restart.*
- (Very **important**) CanvasBlocker - *(inform yourself what canvas are, they are being used for identifying you, even if you change your IP, mostly used by advertising companies) blocks canvas fingerprinting*
- Flagfox - *to see in which country the server of the particular website is located.*
- Flash Control - *it stops or allows flash content on websites*
- (Very **important**) Ghostery - *kills every tracking activities. So the website you are visiting doesn't know where you came from.*
- GoogleSharing - *makes searching google anonymous without knowing what did you search earlier and who you are.*
- (Very **important**) NoScript - *The name says it all. It allows you to block a single script on a website or all of them.*
- User-Agent Switcher - *experimenting with this one atm, but it should tell the website what browser you are using, you may choose a fake browser instead.*
- WorldIP - *it's additional information for Flagfox, shows the locationsand IPs of websites you are visiting.*
- WOT - *this addon is based on a community, it tells you if a website is safe or not*
- (Very **important** for anyone without a VPN or proxy) ZenMate - *VPN for your browser, only for browser. All other activities in other browser are not secured by this VPN*.

Now again, open the websites given in the beginning of this article in new tabs and you will see the difference. You already hid some information, but there is more to go.

Version a: VPN

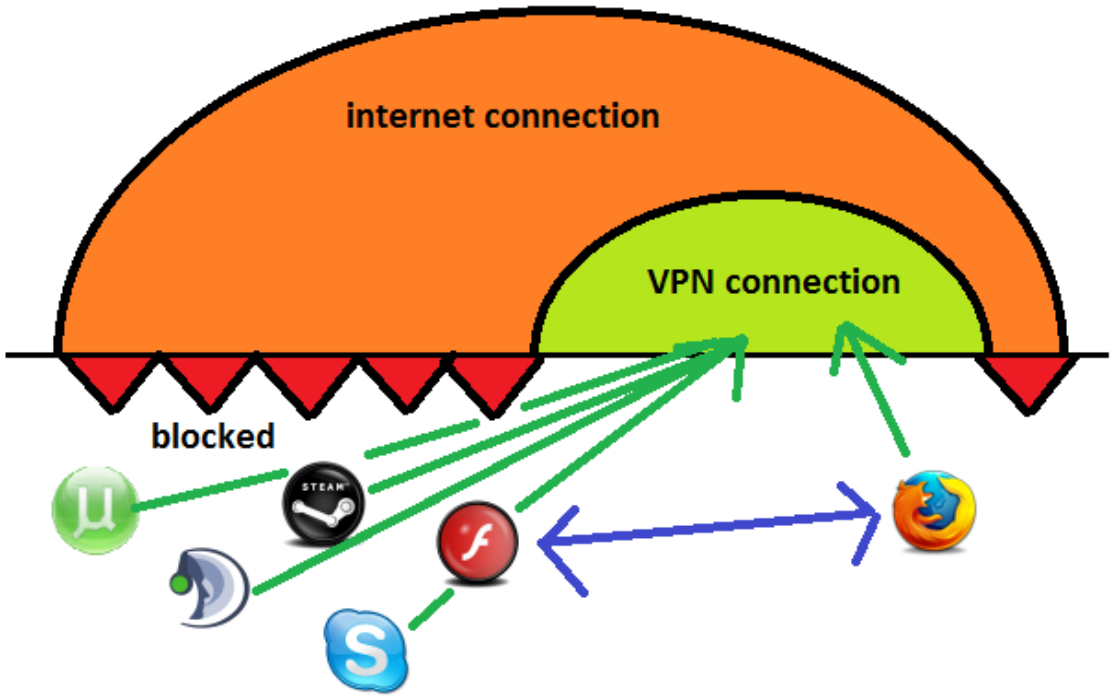


With a VPN you are not only anonymous on the internet, but you also don't leak any information to your ISP.
How to use: you download the client. Install it, run it then in most cases you just press a button like "Connect" or "Go" or something like this. Then you wait a couple of seconds and voila, you are connected to a VPN. You may also choose a specific IP and/or a specific country.
How it works: you are connected to your ISP, so you have your IP: 100.50.40.20. Then you start the VPN client and it creates an encrypted tunnel between you and your VPN provider. Now your encrypted connection goes only to the VPN server. That means the ISP sees only a connection to a VPN sever, but because it's encrypted and he can't decrypt it, he can't see what packages/data is being transferred between you and your VPN. In other words he can't see what website you are visiting, what files you are sending and receiving. That allows you to visit by your ISP blocked websites and use blocked services. Only the VPN itself can decrypt the transferred data and see what you are "doing" on the internet. On the other side of your VPN provider, you get a new IP provided by the virtual network service. With this IP: 10.20.30.40 you are surfing the web.

Another aspect is the security. No hacker can attack you by using your IP (which is 10.20.30.40, not your real IP) because every good VPN is using NAS firewalls. They check the data between you and the internet. Of course there are several ways to get viruses and stuff on the internet, but being hacked directly is nearly impossible. So be careful what you are downloading.

Now you may ask what happens if I download the song "Bitch Better Have My Money - by Rihanna" and some tracking service will inform the song owner/producer so he goes to court and asks for my real identity? Well, he probably will get the VPN provider's name and stuff, but because this IP belongs to the particular VPN provider and is being used by several users at once, only the log files can show who exactly downloaded this song.
In other words, police can't get your personal data (address and name) because a good VPN provider first of all does not log any user. **This is the golden rule**. If you are looking for a VPN service, be sure the provider does not log any activities. Secondly, there are several users for each IP. There is a law which says that the case is closed if it is not clear who exactly broke the law. So with no logs the VPN provider can't tell what his customers do on the internet.

The main benefit of using VPN is that your whole computer is using the internet through the VPN tunnel. Here the tunnel from another point of view:



Pros:
- anonymous on the internet
- no leaking data to your ISP
- better security through NAS and encrypted tunnel
- no internet speed throttling
- all services, programs, games, just everything that is using internet goes through VPN

Cons:
- for better privacy and comfort you better take a payable VPN service

http://netforbeginners.about.com/od/readerpicks/tp/Reasons-to-Use-a-VPN-Service.htm - *nice article about why you should use a VPN.*

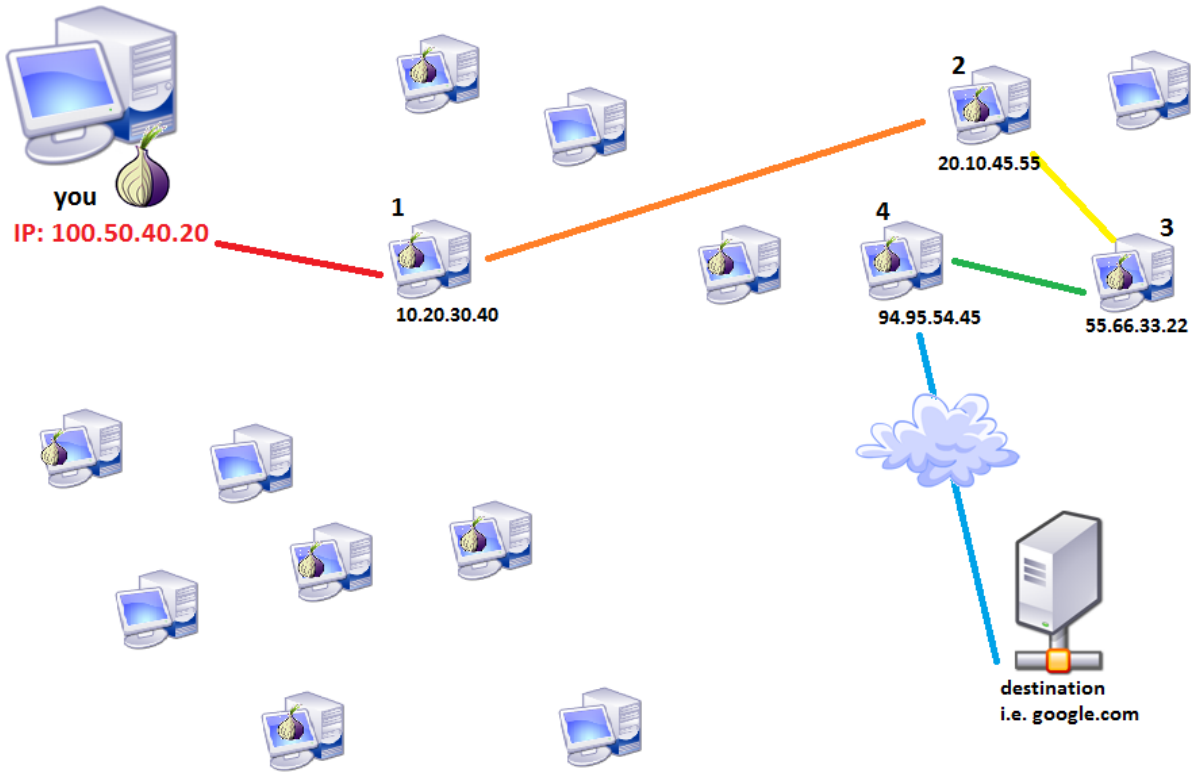
Choose VPNs by reading comments/ratings/other experiences. A good VPN is one you pay for. Although there are some good payable providers that offer a decent free version but never ever use a free-only VPN service or any unpopular ones. Trusted service means this service is being used by several users and all or at least some of them are more than satisfied.

Some good links to start with:
1. https://www.bestvpn.com/blog/15400/5-best-vpn-providers-for-2015/ - *VPN ratings, tells you what to look at when choosing a VPN.*
2. http://www.pcmag.com/article2/0,2817,2403388,00.asp - *a table of different services, showing their offerings.*
3. http://www.bestvpnsites.com/- *reviews of many different VPNs*
4. https://torrentfreak.com/vpn-services-that-take-your-anonymity-seriously-2013-edition/ - *all in all good reviews of different VPNs.*

There is also an option to use a VPN as an addon in any browser (like ZenMate in Firefox/Google Chrome). But first of all, it's free. So don't trust it your whole identity. Secondly, only your browser is secured. This means all other programs are using the internet normally with your real IP. This means that certain cervices like the flash player, which is being used by Firefox while watching videos, will leak your real IP. In other words ZenMate is or at least it behaves like a web proxy. Therefore you need to go through the "preparations" section before choosing what anonymity version you want to use. How the leaking is working will be explained in section "version b".

Version b: TOR

Another option is using a TOR Browser. Because we know that every connection is going through your ISP, I will not show every ISP in this picture. Just remember every computer exits through an ISP.



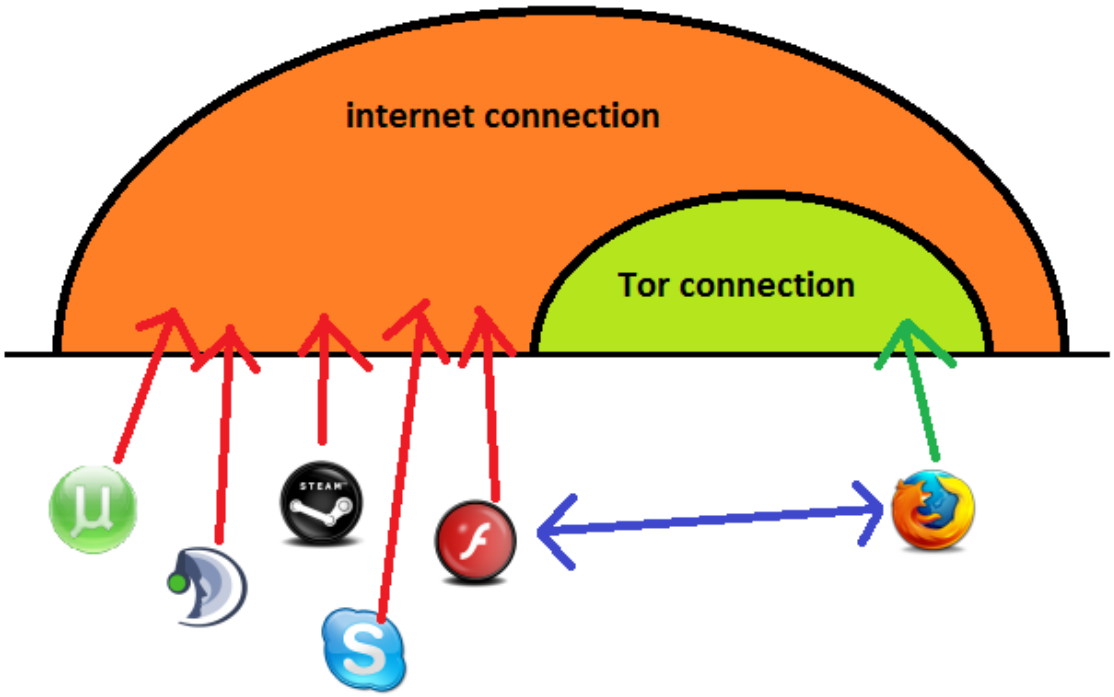
How to use: You download i.e. the tor browser here: https://www.torproject.org/projects/torbrowser.html.en and you may run it, or put on an USB flash drive and use it there. It takes a while after you started it, because it creates all connections. Then you need to do the same steps of "preparation" on this browser as told in the beginning of the article.

How it works: The benefits of TOR are the multiple encryptions between the nodes (user computer). Every computer to whom you are connected is a node. The last computer is the exit node. So in the picture you see how it generally works. Your TOR client connects to another random client and encrypts the data. The other node connects to the second random node and again encrypts the data. this procedure repeats till the software finds the "perfect" route between you and the exit node. Every connection is encrypted. So no middle man attack is possible. The Exit nodes then decrypts the data and connects to your desired address, in this example google.com. Now Google may know everything about the last node. He's IP is 94.95.54.45. The destination also knows that Tor is being used but he **doesn't** know from whom the request came from. So the same here. Your ISP does not know what you are doing on the web because you are using a tunnel created by TOR. The only thing he knows is that you are using TOR and you are connected to someone.

This is actually the power of TOR. Every node sees only that it is connected to someone. It sees that there is a connection from someone and a connection to someone. Although the node does not know what data is being transferred, it lays another layer of encryption and sends the data further. In our example you want to visit google.com. You send the data to node 1. This node don't know your request, but it knows where it comes from and where it should go, so it sends your request to the node 2. This node again does know it comes from node 1 and needs to go to node 3. Node 3 knows that it comes from node 2 and it should send the data to node 4. The last node decrypts the data and it knows it's a request. It does not know where it came from except that the node 3 just pushed it further. So the request is decrypted and the exit node just sends it to the next DNS server and you see Google's website on your screen. And when this is not secure enough every 2 minutes TOR generates a new random route. This means you will get every 2 minutes a new IP.

The same schema works for uploading, downloading chatting, whatever you do **within your browser.**

Careful! All other applications like games, messengers, players whatever except your Tor-browser are using the internet normally. This bring us the IP leak through services. Imagine we look at our TOR-tunnel from another point of view:



As you see, our TOR-browser is using the flash player to watch videos, if you would want to. In this case you are connected to YouTube through TOR-tunnel and your browser tells flash player what video you want to watch. Now the player itself is connecting to YouTube servers through your normal internet connection and YouTube knows your real IP. Now imagine you visit a website that uses flash to get your IP. Therefore it's highly important not to turn off the **NoScript** addon.

Also the WebRTC option in your browser is leaking your real IP. It works quite the same as flash player but to disable this one you need to go through the "preparation" section. In this section you also disable the network websocket option which instead of using the proxy DNS let your Firefox use your local DNS server. Which also leaks your real IP.

But after configuring your Tor-browser you are ready to go.

Pros:
- multiple encryption through multiple nodes
- multiple proxies (nodes)
- no leaking data to your ISP
- every 2 min a new random IP
- access to The Darknet (onions)

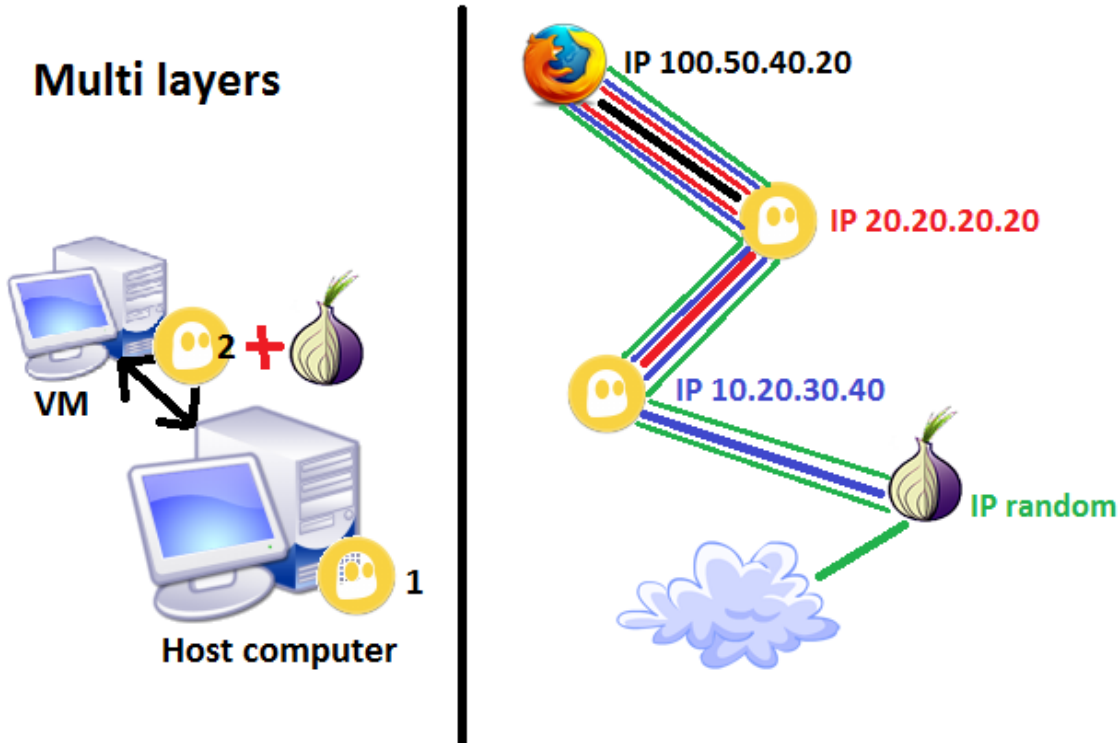
Cons:
- your internet is as fast as the slowest node
- proxy provided only inside the browse

Darknet
A quick *offtopic* here. There are websites which are not accessible via the normal internet which you may use right now. There are .i2p or .onion websites running on computers using TOR or I2P exit nodes. So normal DNS servers can't listen them and you can't see them. By using TOR you of course can access any .onion website if it exists and is online. Because The Draknet is running through TOR network, everyone is anonymous there. You have access to black market and websites that Google would never show in its search results. Here you may also hire hacker groups to find people if you need so. All further information you will find in the hidden wiki, just follow the first steps after starting your TOR-browser.

Like in mostly every Anon-guides there is a saying: **"It's not about <how paranoid are you?>, it's about <are you paranoid enough?>"** . In general the more secure layers of encryption you use, the more secure is your connection. That means more security for you and more reliable anonymity.

Version c: VPN + TOR

I like this version the most, because it gives you all the pros of each version. You may install a VPN client so the whole computer is being secured by an encrypted tunnel between you and your VPN provider. From now on you are anonymous on the internet. Then besides the normal browser you just install TOR-Brower and you may use it for "not so personal purposes". There your connection is going through VPN into a TOR Network and exit's somewhere 10 Nodes further. So if TOR on your side is compromised (with chances as big as being struck by a lightning) you still are anonymous through VPN. Now as written above. More layers = better security and anonymity. You may create a virtual machine by using VMware Player or VirtualBox. Then install Windows or Linux and use another VPN on top of your host's VPN. Like shown in the picture:



On the left side you see your environment. Your host PC is the one you are probably using right now. You start your VM on this PC and start VPN then TOR.
On the right side you see how your connections are being encrypted by multiple layers.

1. The black connection to the first VPN is encrypted with red lines shown in the picture.
2. It's also encrypted by the second VPN and the outgoing connection from first VPN is being encrypted.

3. The outgoing connection from second VPN and all others are encrypted by TOR and the outgoing connection from TOR's network is going to wherever on the internet.

This means only the first VPN knows your real IP. The second one, on your VM knows only the VPN nr. 2 IP. Not yours! And of course TOR only knows the VPN nr. 2 IP. You may see where this is going. Don't forget that TOR is also encrypting your connection several times from node to node.

Version d: VPN router

There are also routers which are configured for using VPNs. This means every device that is connected to your router via LAN or WLAN is using VPN automatically. So you don't need to configure anything on this devices. Even your guests at home are using your VPN. This may be considered for someone who is using several devices at home that need internet connection and/or someone who lives with several ppl together. I suggest you inform yourself on http://www.flashrouters.com/. You may just choose a VPN provider on their website and choose a router you want. Because they are preconfigured it cost's something more than a normal router. But you have to decide if it is worth or not.

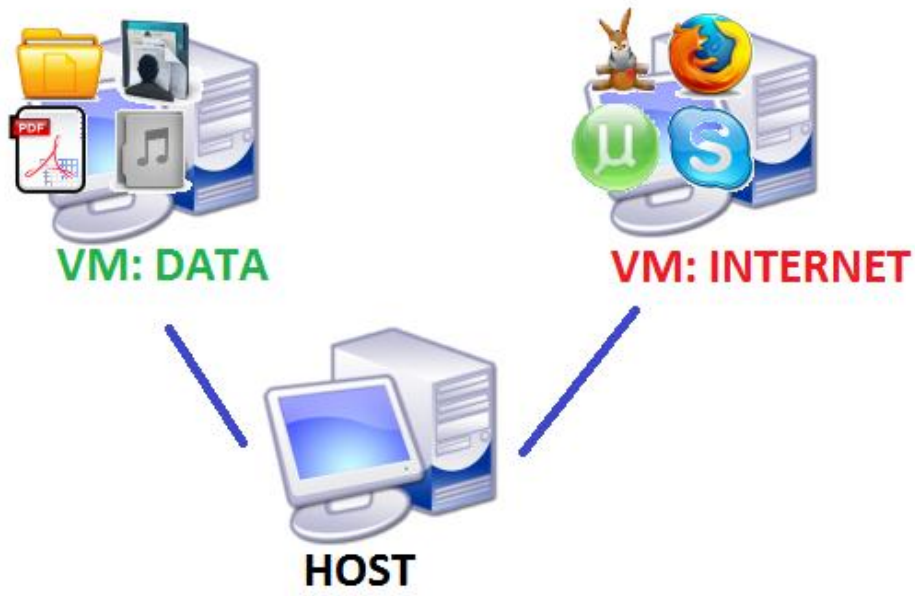
If you want to safe some bucks, you may buy an DD-WRT or Tomato router which allows OpenVPN, by yourself. You will probably not safe more than 10$ but who knows? In router configs you just need to write your VPN subscription or provide a configure file which can be obtained by the VPN provider you are using or want to use.

Version e: I2P

i2p is similar to TOR but was differently funded and works a little bit different. But the idea is the same. You install the software: https://geti2p.net/en/ , configure it like you want or let all configs on default. But some default settings may not work with VPN. In my case the needed UDP ports which were used by i2p were blocked by my VPN provider, so the internet speed was awful... Try this out, experiment. There are rumors that TOR users merge to i2p. It has also a connection to The Darknet but not via onions like when using TOR. Instead you will see websites with ending .i2p. Obviously.

2. Secure computer

The idea of any "secure computers" is that your personal data is safe from viruses, hackers etc. look at this environment:



Your computer has 2 VMs installed. This virtual machines are separated. So your data is "safe" from viruses and spyware from internet if you don't use the internet on VM: DATA at all or only for updating your system. Let's look closer why.
First of all it is the best if the host computer is using Linux. Just go ahead and try Ubuntu if you are new to Linux. VMs' operating systems are not important. Here you may use Windows or whatever.
You download stuff and chat with people you don't know. You get viruses, spyware, adware or other malicious software on your VM. You may use an Anti Virus or not. If you know your VM is infected. Just reverse the last snapshot.
Snapshot is a feature that allows you to safe the whole VM status (system, files, software) and reverse to his status anytime you want. So the best case is when you create a snapshot after installing all stuff you need on the VM. If anything goes wrong, roll back to last snapshot and all bad is gone. This is the great benefit of VMs.
But what happens if you don't know that your VM system is infected. Well then you still don't have to be afraid of losing or infecting your personal data. All viruses and stuff will stay only on your virtual machine, where you are using the internet. Most viruses are designed for Windows, because this system is the weakest and the most used one. So they won't know if they are on a virtual machine or not. Now let's imagine you got a virus which knows you are using a VM. This case is really rare. But nevertheless it will then go through your VM to your host system and that's it. It can't do anything there because your host machine is using Linux. A Windows virus can't be run or do anything on Linux. The other way around is

the same thing.
Now let's imagine you are being struck by lightning every time it rains and you get a hybrid virus. So it can harm both systems Windows and Linux. As mentioned above you are using a VM and it just do its stuff on that particular VM.
Nevertheless your bad luck with lightning you are being struck 10 times a day. So the hybrid virus can also detect any VM and break through it on to your host computer. Here to mention every vitalizing software has its own bugs/weak spots and ways out of VM. So the virus has also to know how to break out of the particular VM (for example VMware and Virtual Box have different ways out). Now the virus can harm your VM: INTERNET and your host system. But your private data is still safe in the other VM.

So you can say a VM is isolating viruses and other software from your host machine and your other VMs. Now you may also encrypt the virtual drive on your VM: DATA so it's more secure. But this is a topic for "Anonymous computer".

You need to know that by using a VM your computing power is dropped about 10% and you can't play any games on any VM. It will lag the shit out of your patience. If you want to play games on your computer, you have to use Windows on your host machine. *(Because most games are designed for Windows)*

Now if you don't like to switch between the VM windows, too. You may just enable the **unity** feature. All opened windows in your VMs will be shown on your host machine like a normal window. It allows you to use your host's and your VM's programs like on a single machine. You don't need to switch between the VMs anymore.

3. Anonymous computer

In this chapter I just will introduce you to another aspect of Anonymity. How to create such a system, visit the links below.
Till now we had anonymity only on one side, the internet. But you may stay anonymous on both sides. That means only you can access this particular system. Either you or no one. In addition to all previous schemas you may not only encrypt your data, but the whole partition. This will need you to format everything and reinstall the whole system.
How it works: you either install a Linux system on your USB drive and encrypt your whole partition. Or you install a Linux OS on your computer and use a USB device as a boot key to your system. In both ways your USB flash drive will be the key to your privacy. You may lose it, then all data is gone. Today's flash drives are so tiny, so easy to lose. No one will ever find this in your hands. So here only you have access to your operating system and the data. If anyone else is using your computer without the key, he will boot something different, not your encrypted system.

You see where this is going. I won't recreate a wheel on this part. There is already a perfect guide from Anons: https://anonguide.cyberguerrilla.org/anonguide.pdf

Read it for more information. There you will also learn more about Whonix, the anonymous Linux. How to encrypt emails, documents, chats.

Conclusion

If you have read every section till now, then you know the possibilities of different setups shown above. You may use all of them together in one system. You may combine all of them or just some of them together. You may also create an anonymous computer and implement VMs and VPNs into it. It's all up to you.

No matter how good your system is set up, your biggest enemy and threat will be yourself. Your best security and anonymity will be your brain. Use it. Do not post personal data anywhere. Only you are responsible for your own security on the internet.

Thank you for reading this guide. You may discuss this guide on http://www.anonboards.com/viewtopic.php?f=10&t=190.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.