Network Security

Dr. Farhana Jabeen
Associate Professor

Network Security

VPN

Dr. Farhana Jabeen
Associate Professor

3/25/23

Links

https://thebestvpn.com/what-is-vpn-beginners-guide/
https://www.geeksforgeeks.org/virtual-private-network-vpn-introduction/
https://ocw.mit.edu/courses/civil-and-environmental-engineering/1-264j-database-internet-and-systems-integration-technologies-fall-2013/lecture-notes-exercises/MIT1_264JF13_lect_37.pdf
https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/introduction-to-vpns
https://www.cse.wustl.edu/~jain/cse571-07/ftp/l_17vpn.pdf

How To Install And Configure Free VPN On Kali Linux

♦ https://www.youtube.com/watch?v=T8sGTy5jl-I

♦ https://www.youtube.com/watch?v=PaV5H8xpASY

♦ https://support.ipvanish.com/hc/en-us/articles/360002787473-How-to-Configure-OpenVPN-in-Kali-Linux-

♦ https://medium.com/@kalilinux.in/how-to-set-up-own-vpn-server-in-10-minutes-on-kali-linux-using-openvpn-9824320ff176

♦ https://www.hackingtutorials.org/general-tutorials/installing-vpn-on-kali-linux/

Introduction

- VPN stands for virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.
- Virtual Private network is a way to extend a private network using a public network such as internet.
- The name only suggests that it is Virtual “private network” i.e. user can be the part of local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

Lets understand VPN by an example:

Think of a situation where corporate office of a bank is situated in Washington,USA.This office has a local network consisting of say 100 computers.

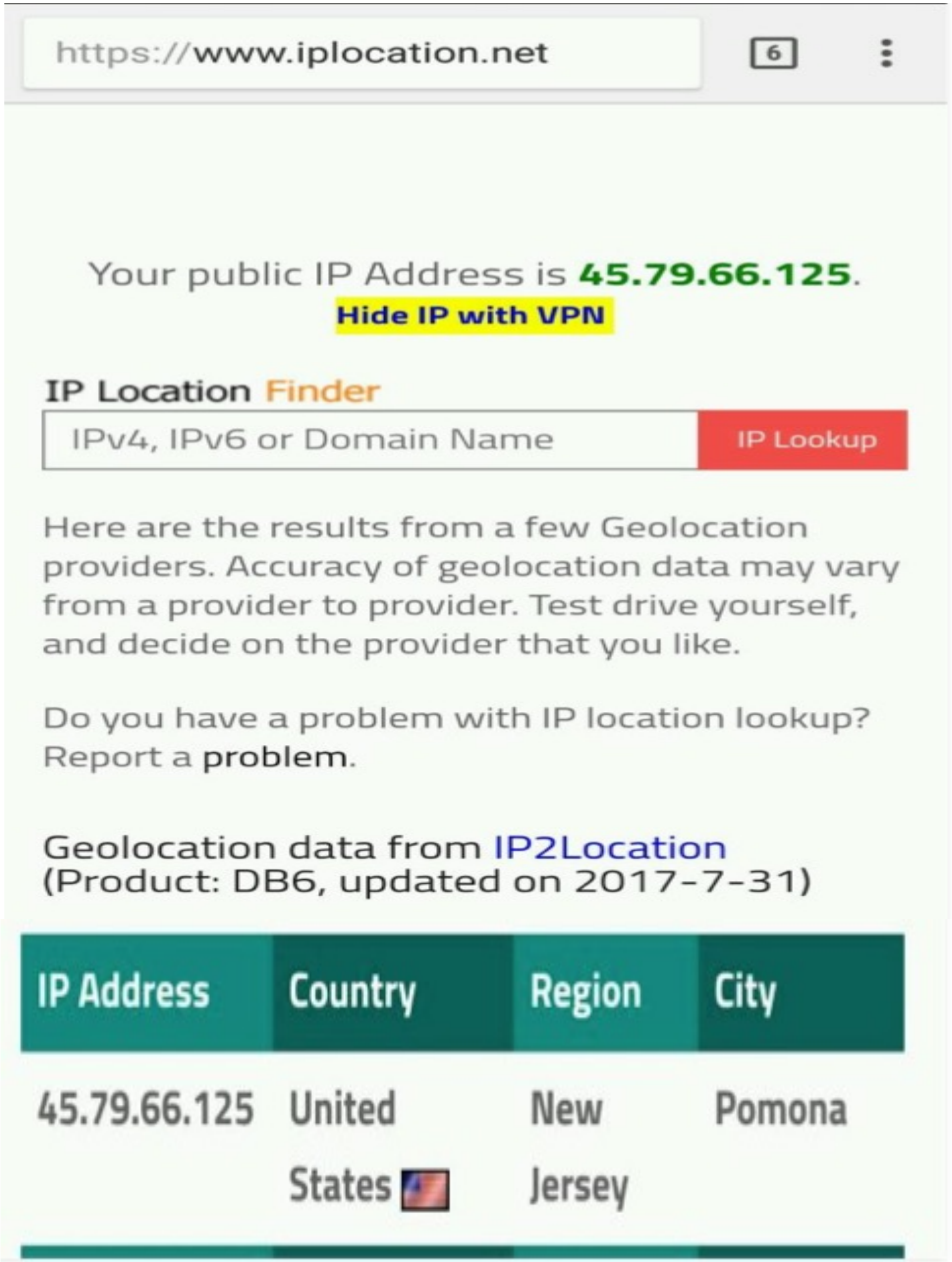
Suppose another branches of bank are in Mumbai, India and Tokyo, Japan. The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was very costly as well as troublesome job. VPN let us overcome this issue in an effective manner.

Lets understand VPN by an example:

The situation is described below:
All 100 hundred computers of corporate office at Washington are connected to the VPN server(which is a well configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in US head office).
The person sitting in the Mumbai office connects to The VPN server using dial up window and VPN server return an IP address which belongs to the series of IP addresses belonging to local network of corporate office.
Thus person from Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
So this is the intuitive way of extending local network even across the geographical borders of the country.

VPN is well exploited all across the globe

- Ali use regularly in his smartphone Spotify-a swedish music app which is not active in India. But he is using full use of it sitting in India . so how ?? VPN can be used to camouflage our geo location. Let me explain you step by step.
- Ali IP address is 101.22.23.3 which belongs to india. That’s why Ali device is not able to access spotify music app.
- But the magic begins when Ali used Psiphon app which is an android app and is used to change the device IP address to the IP address of the location Ali want(say US where spotify works in a seamless manner).
- The IP address is changed using VPN technology. Basically what happens is that your device will connect to a VPN server of respective country that you have entered in your location textbox of psiphon app and now you will inherit a new IP from this server.



Your public IP Address is **45.79.66.125**.

Hide IP with VPN

IP Location Finder

Here are the results from a few Geolocation providers. Accuracy of geolocation data may vary from a provider to provider. Test drive yourself, and decide on the provider that you like.

Do you have a problem with IP location lookup? Report a problem.

Geolocation data from IP2Location (Product: DB6, updated on 2017-7-31)

IP Address	Country	Region	City
45.79.66.125	United States	New Jersey	Pomona

Benefits

- VPN also ensures security by providing an encrypted tunnel between client and vpn server.
- VPN is used to bypass many blocked sites.
- VPN facilitates Anonymous browsing by hiding your ip address.
- Also most appropriate Search engine optimization(SEO) is done by analyzing the data from VPN providers which provide country wise stats of browsing a particular product . This method of SEO is used widely my many internet marketing managers to form new strategies.

Security

- When you use a VPN service, your data is encrypted (because you're using their app), goes in encrypted form to your ISP then to the VPN server. The VPN server is the third party that connects to the web on your behalf.
- This solves the privacy and security problem for us in a couple of ways:
- The destination site sees the VPN server as the traffic origin, not you.
- No one can (easily) identify you or your computer as the source of the data, nor what you're doing (what websites you're visiting, what data you're transferring, etc.).
- Your data is encrypted, so even if someone does look at what you're sending, they only see encrypted information and not raw data

How Secure is a VPN?

- VPN security causes debate among IT pros and others in the industry, and no two services are identical in their offerings or security. There are two main factors:
- The limitations of the type of VPN technology used by a provider.
- Legal and policy limitations affecting what can be done with that technology. The laws of the country where the server and the company providing the VPN are located and the company’s own policies affect how the company implements this technology in their service.

VPN Protocols

VPN protocols define how the service handles data transmission over a VPN. The most common protocols are PPTP, L2TP, SSTP, IKEV2, and OpenVPN. Here's a brief overview:

PPTP (Point-To-Point Tunneling Protocol). This is one of the oldest protocols in use, originally designed by Microsoft. Pros: works on old computers, is a part of the Windows operating system, and it's easy to set up. Cons: by today's standards, it's barely secure. **Avoid a provider if this is the only protocol offered.**

L2TP/IPsec (Layer 2 Tunneling Protocol). This is a combination of PPTP and Cisco's L2F protocol. The concept of this protocol is sound — it uses keys to establish a secure connection on each end of your data tunnel — but the execution isn't very safe. The addition of the IPsec protocol improves security a bit, but there are reports of NSA's alleged ability to break this protocol and see what's being transmitted. No matter if those are actually true, the fact that there's a debate at all is perhaps enough to **avoid this as well.**

VPN Protocols

SSTP (Secure Socket Tunneling Protocol). This is another Microsoft-built protocol. The connection is established with some SSL/TLS encryption (the *de facto* standard for web encryption these days). SSL's and TLS's strength is built on symmetric-key cryptography; a setup in which only the two parties involved in the transfer can decode the data within. **Overall, SSTP is a very secure solution.**

IKEv2 (Internet Key Exchange, Version 2). This is yet another Microsoft-built protocol. It's an iteration of Microsoft's previous protocols and a much more secure one at that. **It provides you with some of the best security.**

OpenVPN. This takes what's best in the above protocols and does away with most of the flaws. It's based on SSL/TLS and it's an open source project, which means that it's constantly being improved by hundreds of developers. It secures the connection by using keys that are known only by the two participating parties on either end of the transmission. Overall, **it's the most versatile and secure protocol out there.**

VPN Protocols

Generally speaking, most VPNs allow you to select the protocol you use. **The more secure protocol you connect through (OpenVPN, IKEv2), the more secure your whole session will be.**

Unfortunately, not all devices will allow you to use all these protocols. Since most of them were built by Microsoft, you'll be able to use them on all Windows PCs. For Apple devices, you will come across some limitations. For example, L2TP/IPsec is the default protocol for iPhone. And Android … well, Android has some problems of its own, which we'll get to later on.

Is it legal to use VPN

First off, VPN as a concept is somewhat new in “legal years,” so not all jurisdictions have managed to keep up. This means that the rules are murky and can be interpreted in many ways.

In overall, VPNs seem to be okay to use in most countries, especially in the US, Canada, the UK, the rest of Western Europe. (Important! What matters here is **your** physical location when using the VPN.)

Generally, VPNs are often **not okay in** China, Turkey, Iraq, United Arab Emirates, Belarus, Oman, Russia, Iran, North Korea, and Turkmenistan.

Does a VPN Make Me Fully Anonymous Online?

- In a word, **no**. But the extent to which it does is still impressive.
- Without a VPN, your connection is fully open, and your ISP, the cafe WiFi router, any server along the way, or a person with the right tools can look at your data. Using a VPN solves many of those problems by encrypting your transmission and making it appear as if it’s the server itself that’s making the connection and not you.
- Investigate the following to help determine the extent of your anonymity.
- Does the service keep logs?
- The jurisdiction under which the VPN is established. In some cases, they might be legally forced to keep records. What happens when a government comes asking questions?
- Does the service keep payment records? Do those records include identifying information?
- Is there sufficient encryption and a secure connection protocol?
- Not every VPN will protect you the same. If you make your choice wisely, you can address the concerns described above. Here’s our comparison of the top VPNs in the market to help you out.

VPN logging policies

The logs a VPN keeps significantly affects the level of anonymity and privacy you have with their service. The logs a provider may keep include:

- user activity
- IP addresses
- connection/disconnection timestamps
- devices used
- payment logs

Any such logs make you a tiny bit less anonymous since your IP can be connected to a given browsing session that you had. Of course, tying this to you personally is very difficult but still kind of doable if some agency is deliberate enough.

Overall, the fewer logs your provider keeps the better, with “no logs” the ideal.

Be careful. Many services state you have privacy on their sales material, but you need to look at their privacy policy to see their fine print and what data they actually keep, or they will state that their country does not require data retention yet they do not state their own data retention policy.

Free VPN versus Paid VPN

Running a good VPN service costs serious money — robust servers, data transfer, infrastructure, employees, and so on. If the service is offered for free, consider what compromises may have been made. Are they logging activity for their own reasons? Are they displaying their own ads? Is your data being sold to a third party?

Paying for a VPN isn’t a huge investment. We’ve tested some great solutions for as little as $3-5 per month, which doesn’t seem a lot in exchange for peace of mind and improved online privacy.

Can I Use a VPN to Watch Netflix and Hulu?

Yes. But like with most things on this list, it all comes down to the specific VPN that you use.

The way Netflix and Hulu block some of their content in parts of the globe is based on **location filters**. Meaning that if you're in a country that's banned, you're banned.

VPNs make this easy to fix. Since you can select the server that you want to connect with, all you need to do to unlock certain Netflix shows is connect to a server in a country where that show is available.

VPN & Tor — How to Use Them Together

Even though Tor and VPN are fundamentally different, they can still be used together for maximum security and online privacy.

♦Tor gives you the ability to access the web by routing your connection through a number of random nodes, while also encrypting that connection at every stage.

♦VPN gives you access to one server at a time.

♦One of the good things about Tor is that you can use it 100% free and there are no built-in limitations to that free version. All you need to do is grab the official Tor web browser.

♦How to combine your VPN and Tor:

♦Enable your VPN connection normally.

♦Open your Tor browser and connect with Tor.

♦At this stage, you have the VPN connection and the Tor web browser running at the same time. The main downside with such a setup is that it's going to be much slower than your standard, VPN-only connection. Tor on its own slows down your experience noticeably, and when combined with a VPN, the results can be even more dramatic. On the plus side, it gives you *super privacy*, which is a huge plus.

When to Use a VPN

- There are a number of good reasons to use a VPN:

  It encrypts your activity on the web.

  It hides your activity from anyone who might be interested in it.

  It hides your location, enabling you to access geo-blocked content (e.g. on Netflix and other sites).

  Makes you more anonymous on the web.

  Helps you keep the connection protected when using a public WiFi hotspot.

IP Leaks and Kill Switches

IP leaks

IP leaks are a known vulnerability with some setups people use to access the web. It’s not entirely a VPN problem at its core.

IP leaks can happen when your VPN fails to hide your actual IP as you’re browsing the web. For example, you want to access a geo-restricted show on Netflix, so you change the server to an approved country and reload the page. Then you realize that the content is still blocked. This means that your real IP might have just been leaked.

The best VPNs all have some clever scripts programmed into their apps to minimize this risk. As I mentioned, your IP leaking is not always the VPN’s fault. Sometimes the configuration of your computer and the many apps within are to blame. Even the browser you use and the add-ons installed in it can cause IP leaks.

kill switch

A kill switch is a feature that automatically kills your internet access if the encrypted, safe connection should ever drop. If there's any connectivity issue at all, the kill switch will trigger and block all activity until the secure connection returns.

If your VPN *doesn't* have a kill switch and a connectivity issue arises, it's probable your device might attempt to restore the standard, unprotected connection, thus exposing what you've been doing up until that point.

According to our research, the following VPNs have a kill switch: NordVPN, Surfshark, ExpressVPN, PIA.