**Lab Objective:** Write article on how to change the IP address by using proxies and mention the differences between proxies and VPN

What is IP Address?

An Internet Protocol address is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication.

An IP address serves two main functions: host or network interface identification and location addressing.

What is a Proxy Server?

In computer networking, a proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource.

Instead of connecting directly to a server that can fulfill a requested resource, such as a file or [web page](https://en.wikipedia.org/wiki/Web_page), the client directs the request to the proxy server, which evaluates the request and performs the required network transactions.

How To Change IP Address Using Proxy

Most devices on the internet use IPv4 addresses to communicate, and the world is slowly adopting IPv4’s replacement, IPv6. Every device connected to the internet needs a unique IP address in order to connect and communicate with other devices online.

An IPv4 address looks like this:

123.45.67.89

And an IPv6 address looks like this:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

If you’re connected to wifi right now, you probably share a **public IP address** with everyone else connected to the same wifi network, but each device has its own **local IP address**. However, if you’re on a smartphone and using a mobile data connection, you might well have your very own public IP address.

When most people talk about changing their IP address, they’re referring to their **public IPv4 address**. This is the address seen and used by most websites, servers, online games, and other devices on the internet.

This article, however, will cover changing your IP address whether it be IPv4 or IPv6, public or private.

**Proxy to change your IP address**

Proxies work similarly to VPNs but with far less versatility and security. Your internet connection goes through a middleman server so that websites and other online resources see the proxy server’s IP address and not your own. Unlike VPNs, proxies often lack encryption, only affect certain apps, and can leak your IP address through other means.

A few different types of proxies can be used to change your IP address:

* HTTP/S proxies – Usually either browser extensions or special websites that work like a browser within your browser. They only change the IP address on data sent to and from your browser, but do not affect other apps or even DNS traffic. If encryption is included, these are sometimes called SSL proxies.
* SOCKS proxies – General purpose proxy servers that can be configured for specific apps including most web browsers. [SOCKS5](https://www.comparitech.com/blog/vpn-privacy/how-to-set-up-a-socks5-proxy-on-a-virtual-private-server-vps/), the latest version, includes support for encryption.
* SSH proxies – SSH proxies forward internet traffic from apps like your web browser through a Secure Shell ([SSH](https://www.comparitech.com/blog/information-security/ssh-encryption/)) connection to a server, so your IP address is changed to that of the server. Although encryption is included, SSH is not a particularly fast protocol, and many websites and apps might not function properly when connected.

Types Of Proxy/VPN IP Address

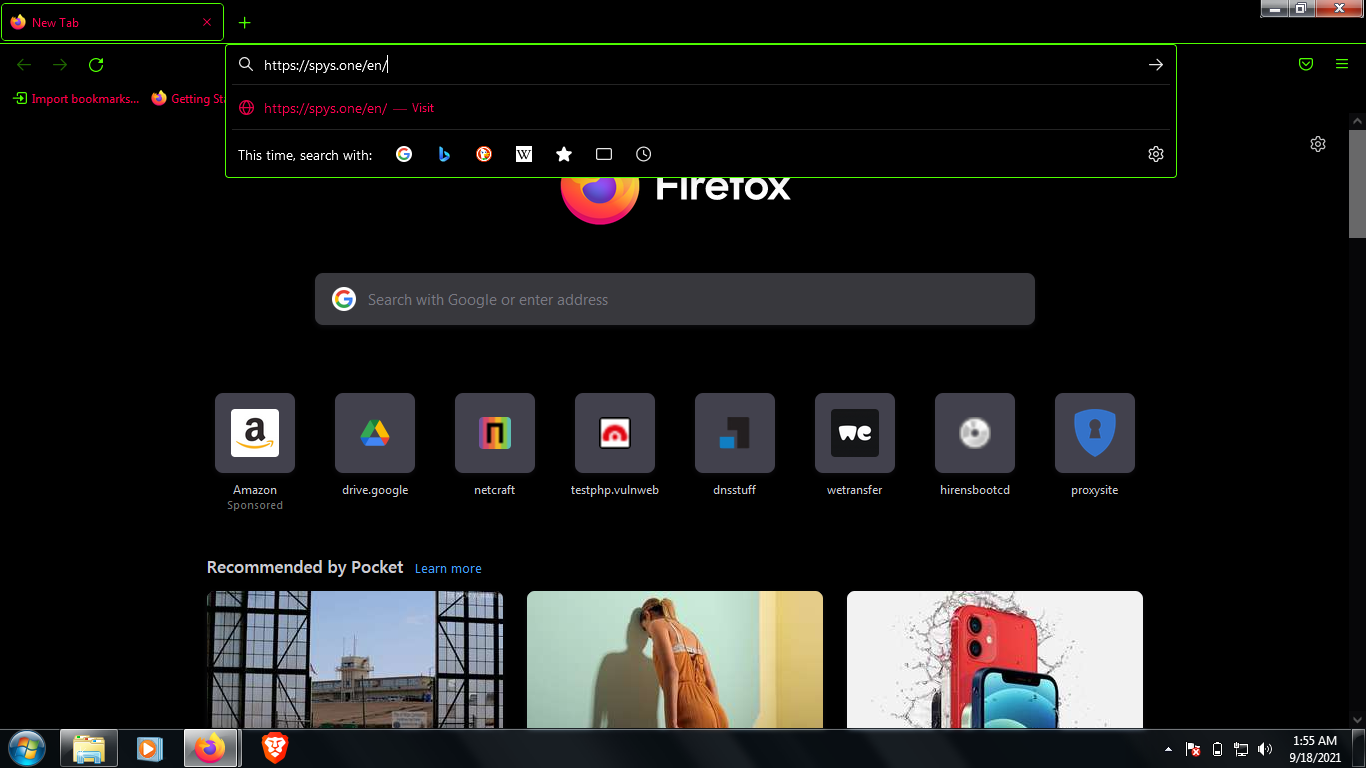
* Transparent proxy: It tells websites that it is a proxy server and it will pass along your IP address anyway.
* Anonymous proxy: It will identify itself as a proxy, but it wont pass your IP address to the website.
* Elite Proxy: It passes along an incorrect IP address for you, while identifying itself as a proxy.
* High Anonymity proxy: The proxy and your IP address stay in a secret. The website just sees a random IP address connecting to it…that isn’t yours.

Things we need:

* IP Address & Port Number
* Web Browser- Google Chrome/Firefox/Brave etc.

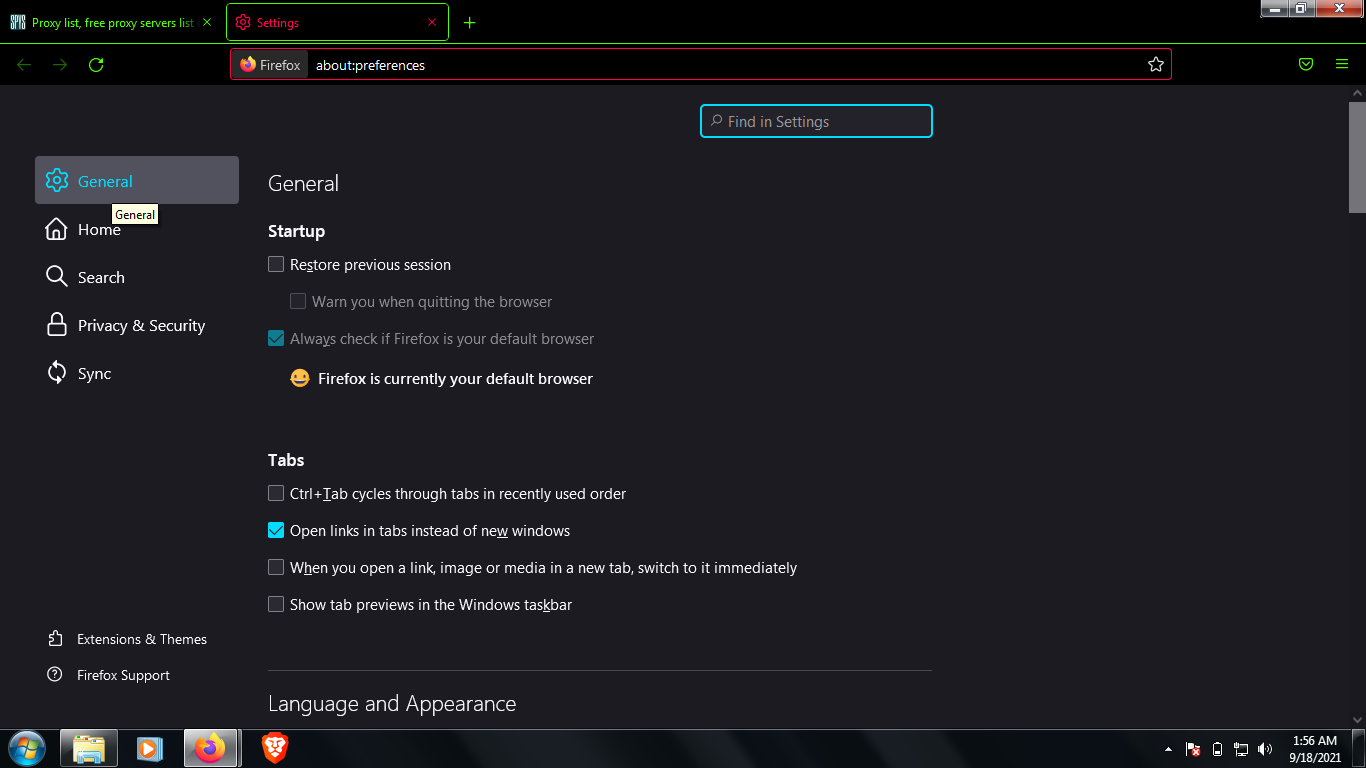
Steps to change the IP address Using Proxy Server

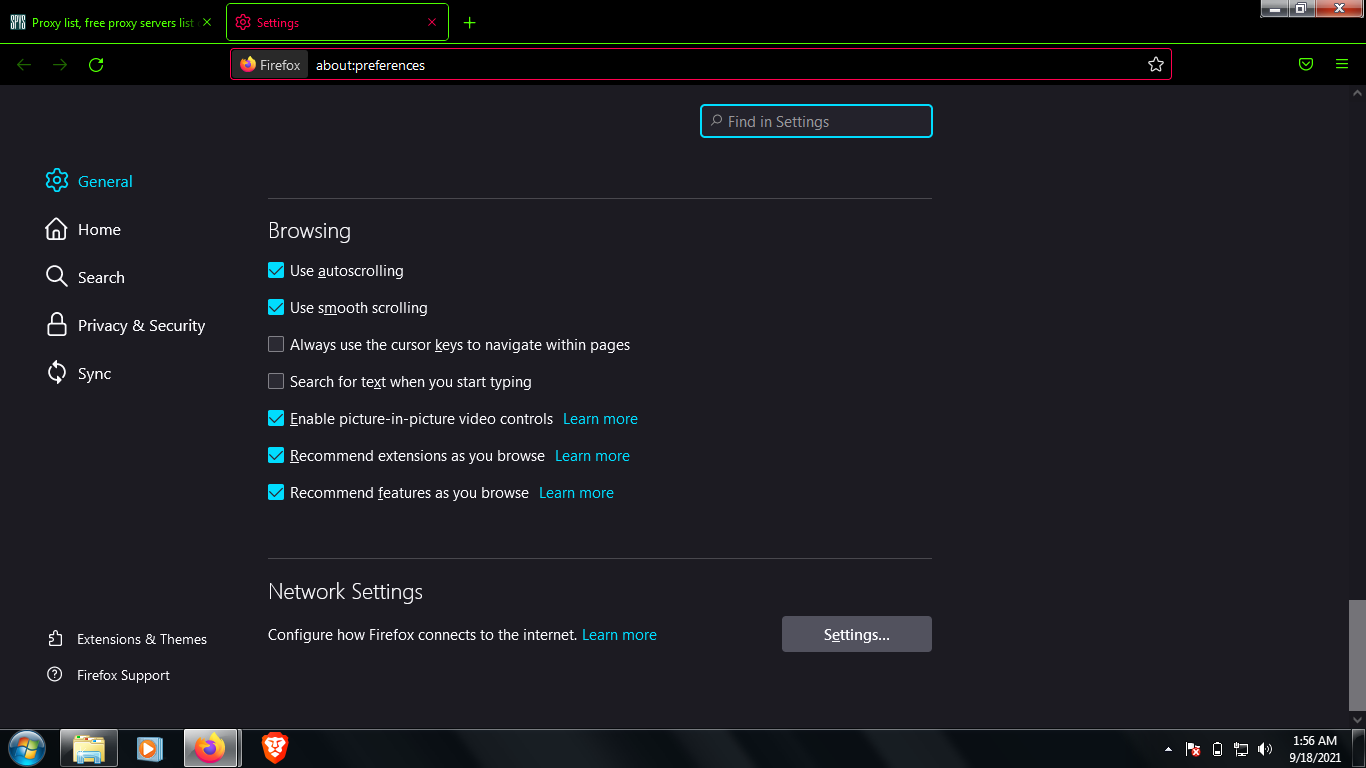
1. Open Your Web Browser (I am using Firefox) and go to https://spys.one/en/.
2. Copy the IP Address and port number you want to use.
3. Go to Main menu of your browser and select ‘Settings’.
4. Go to General Menu and drop down to bottom and select ‘Network Settings’.
5. Select the ‘Manual Proxy Configuration’ option.
6. Paste the IP Address and port number in their respective dialog box and click ‘OK’.
7. To check if your IP Address is changed, go to <https://whatismyipaddress.com/>

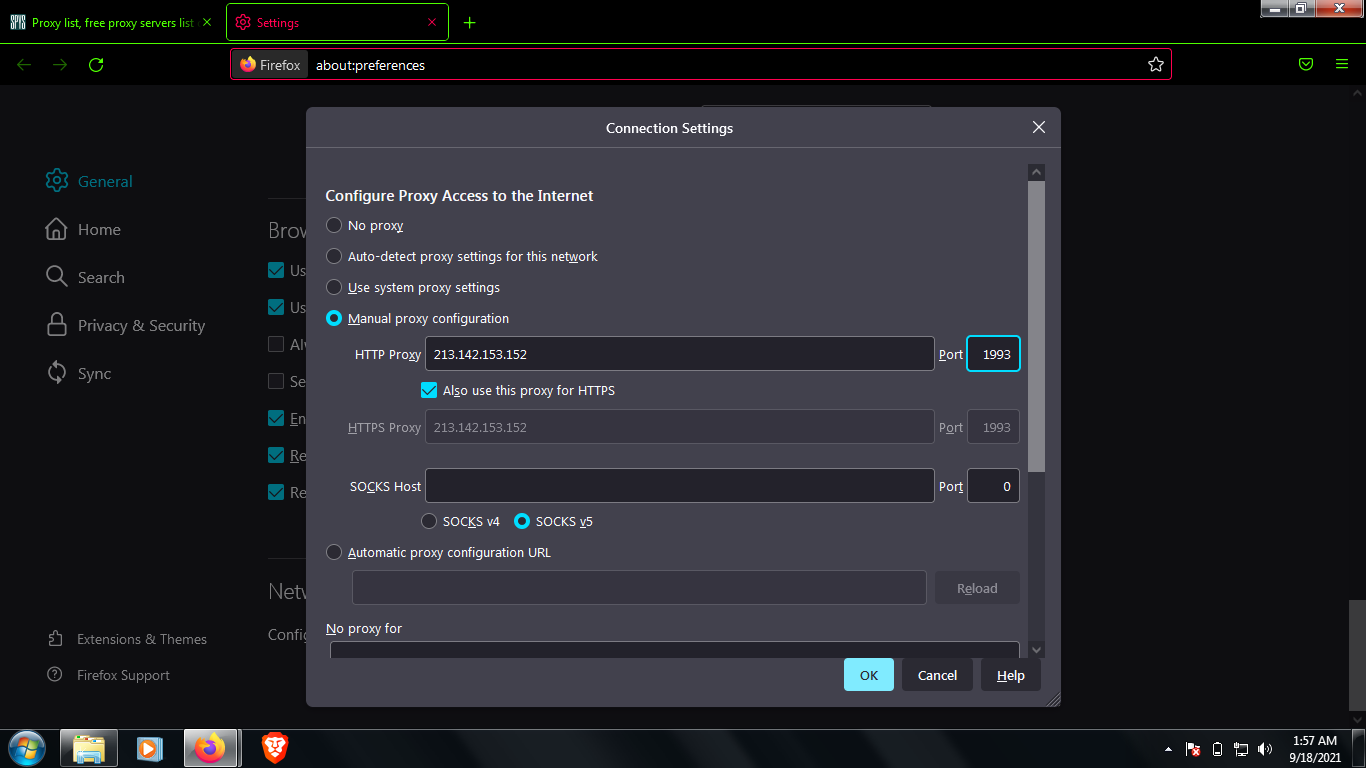




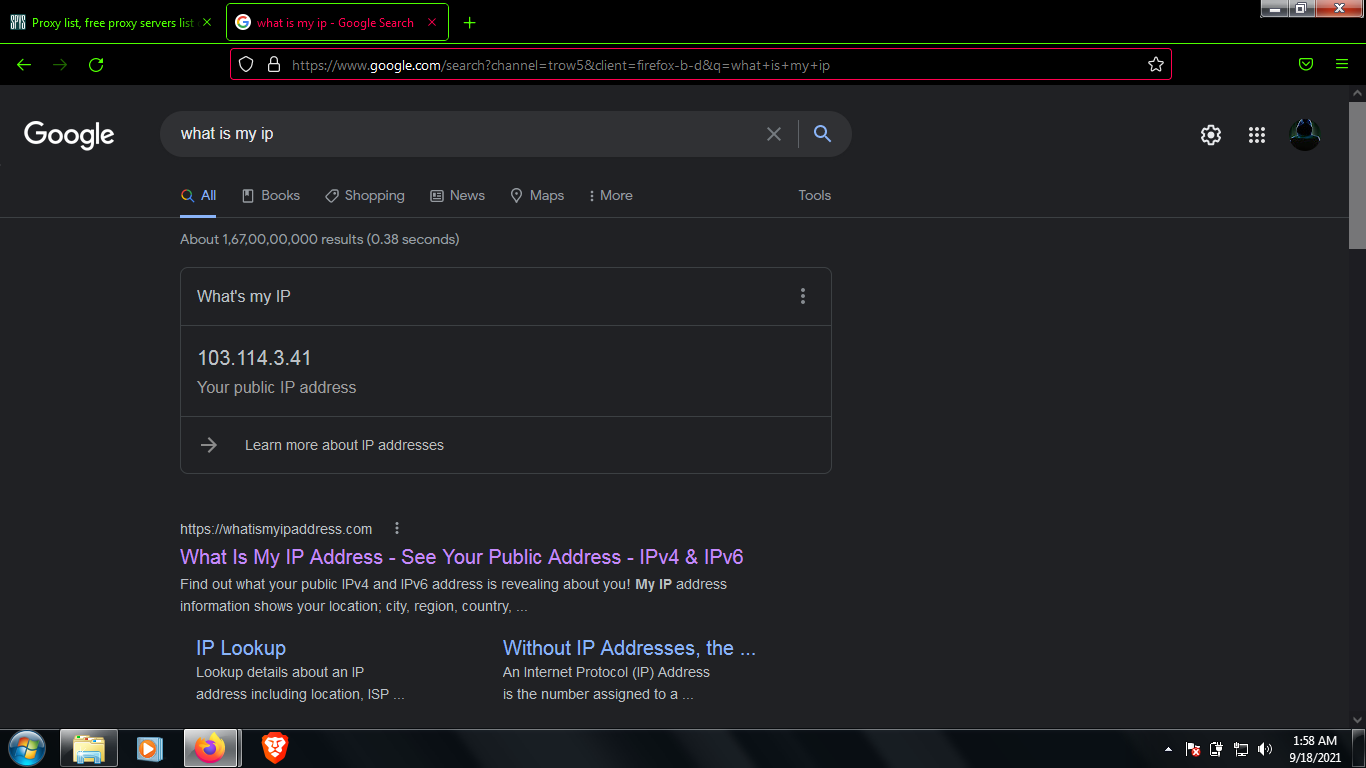






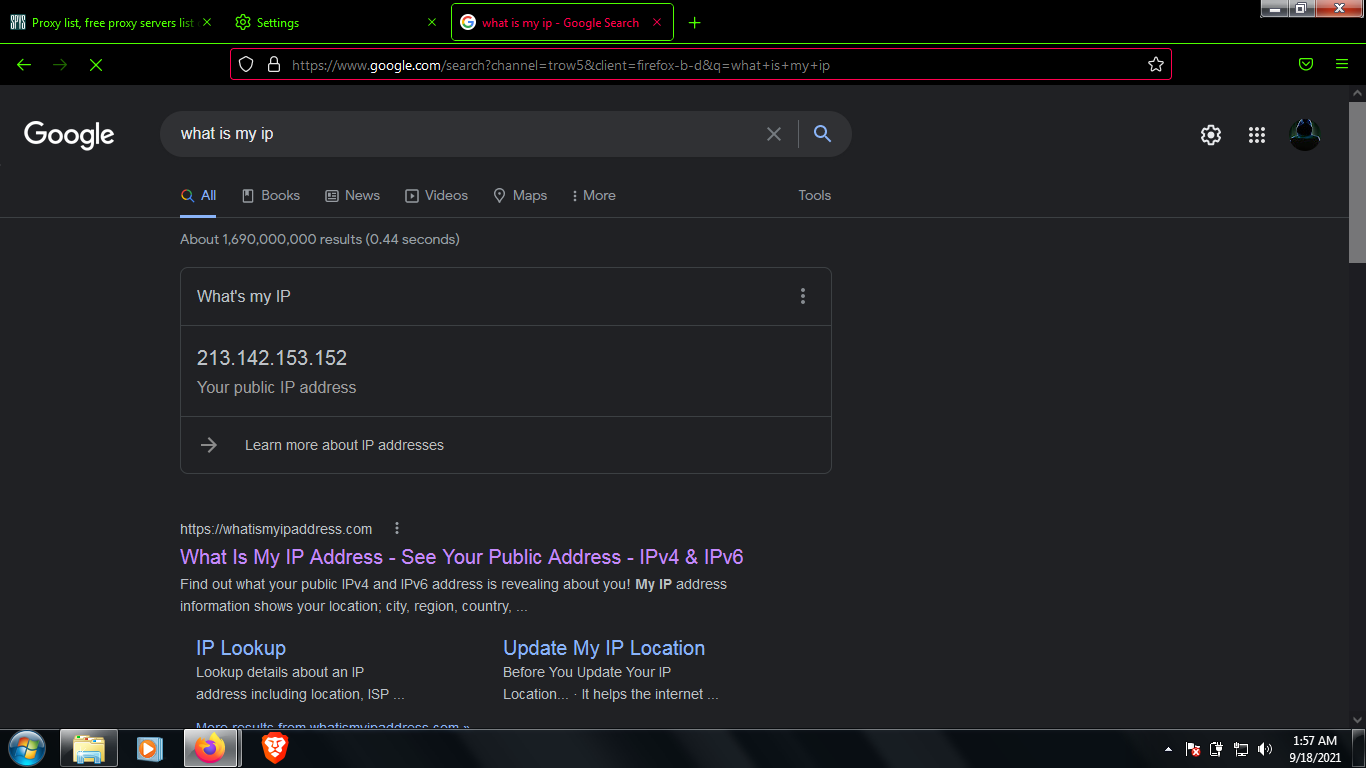


MY IP Address before using proxy



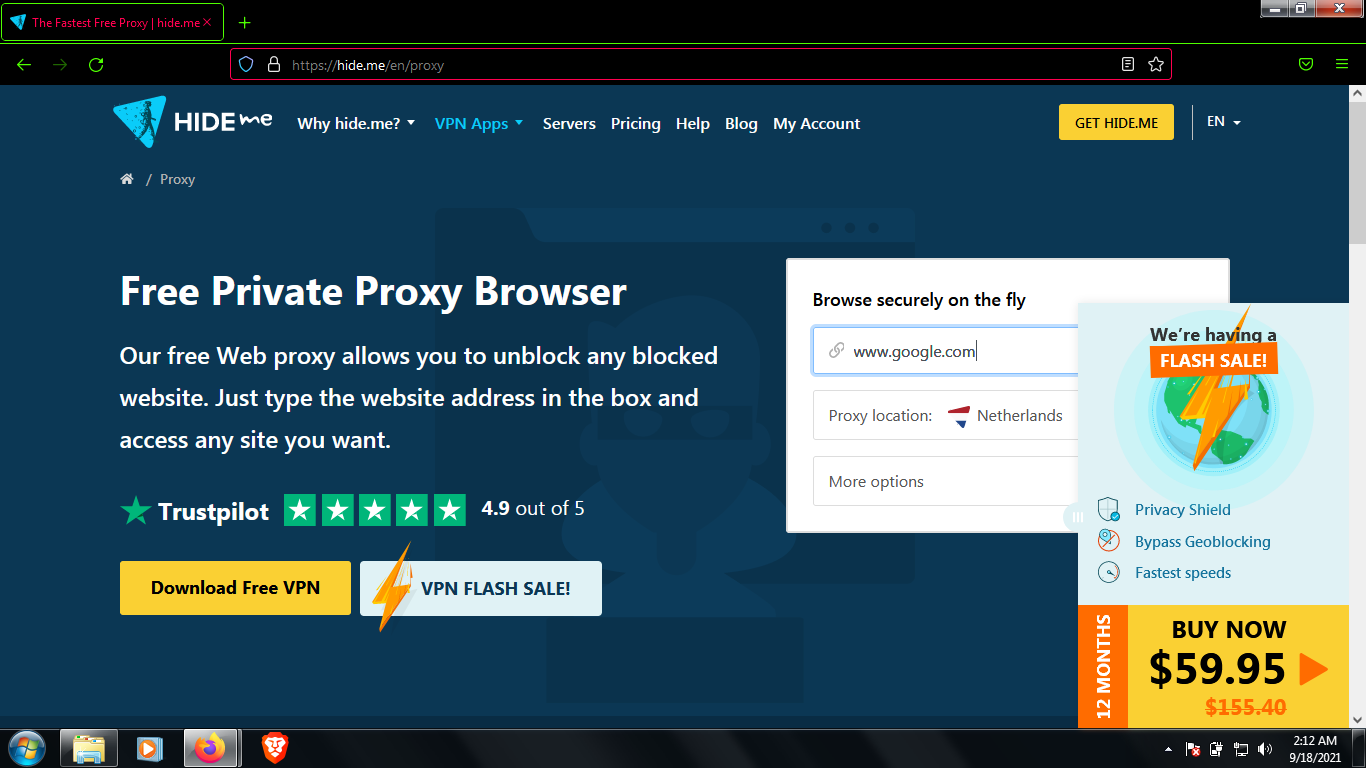


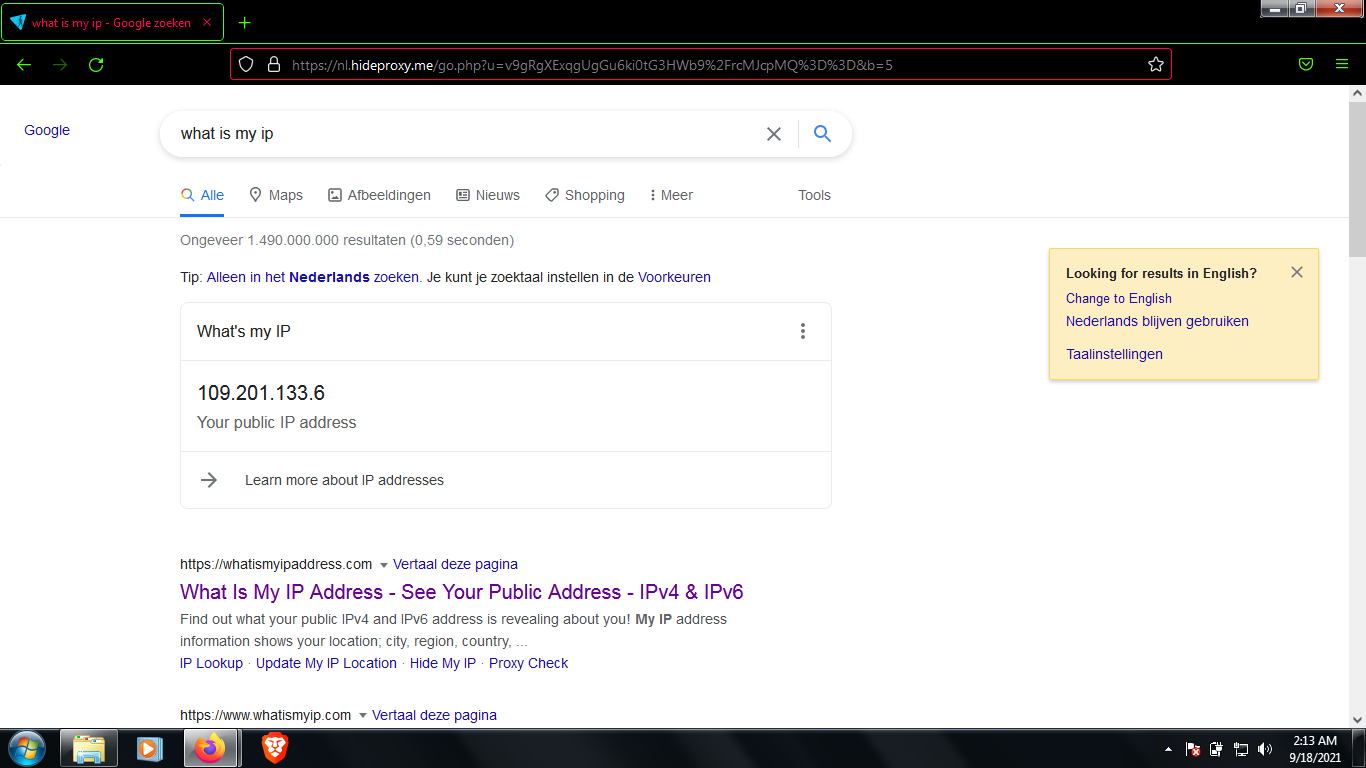
My IP Address after using proxy



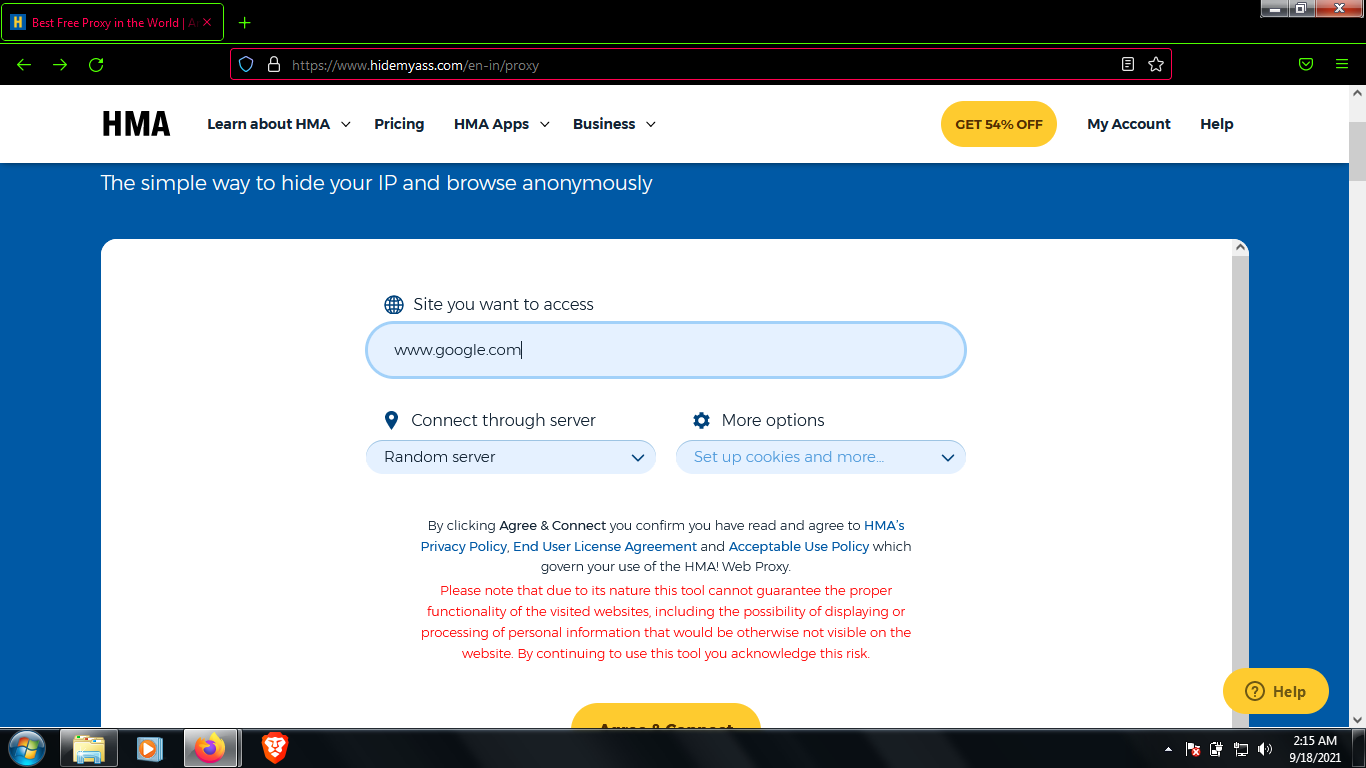
By using this method we can change the proxy configuration manually, we can also use free proxy websites to change our IP address like <https://hide.me/en/proxy> , <https://www.proxysite.com/> , <https://www.hidemyass.com/en-in/proxy> , and many more

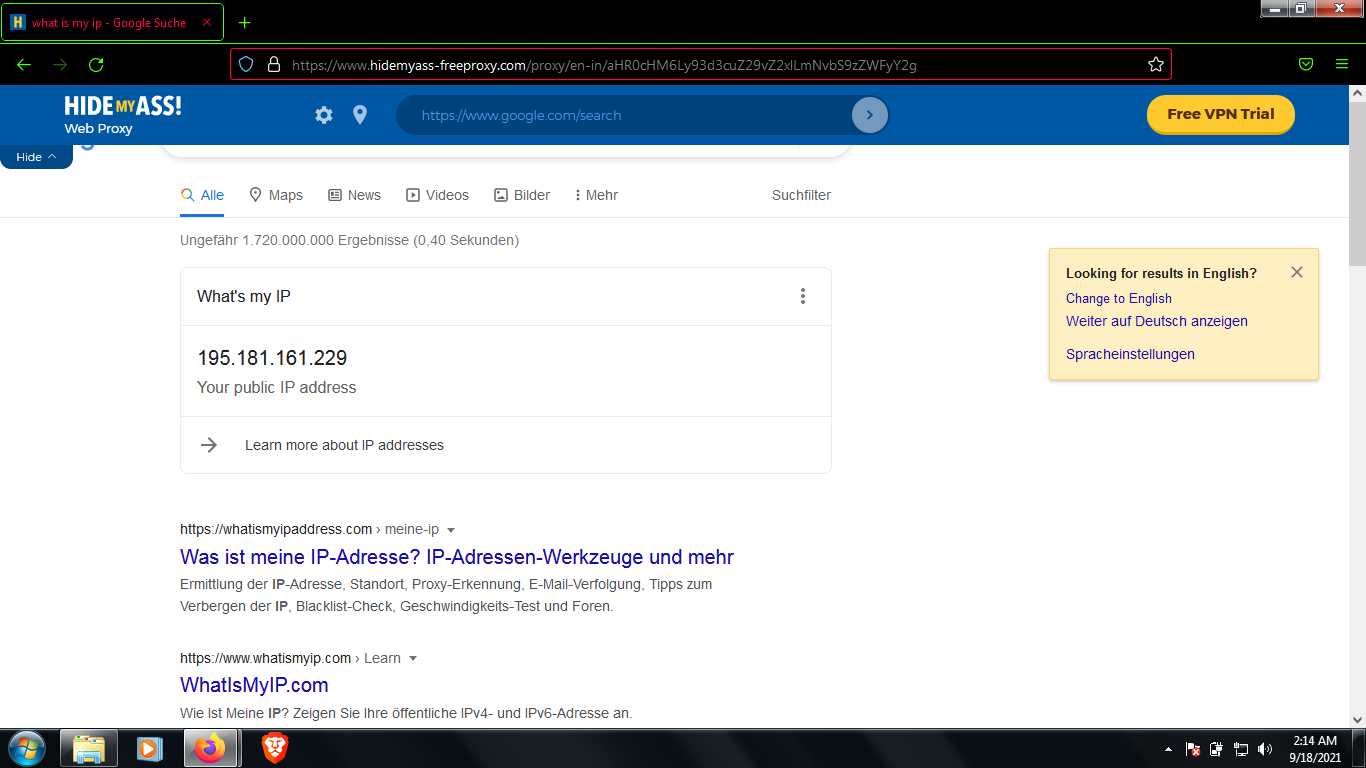
**Example of** [**https://hide.me/en/proxy**](https://hide.me/en/proxy)





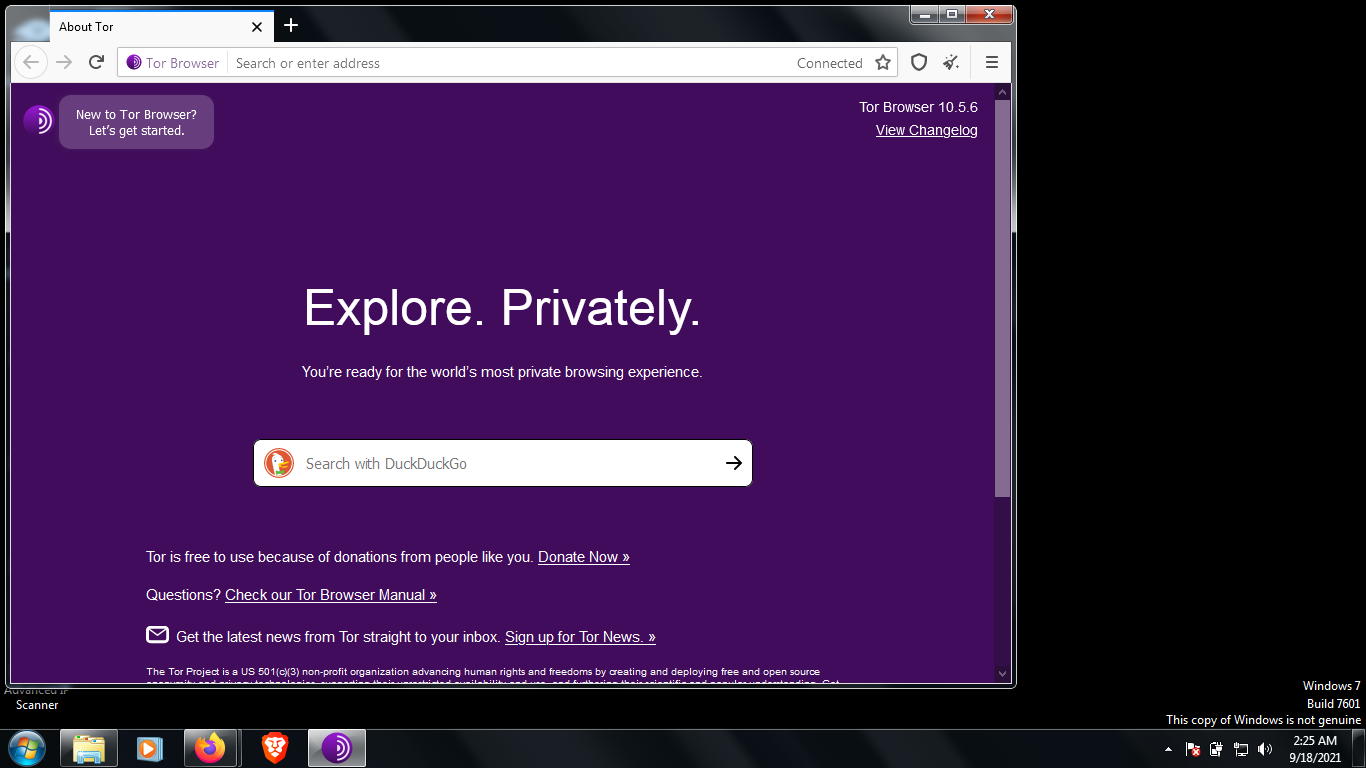
**Example of** [**https://www.hidemyass.com/en-in/proxy**](https://www.hidemyass.com/en-in/proxy)

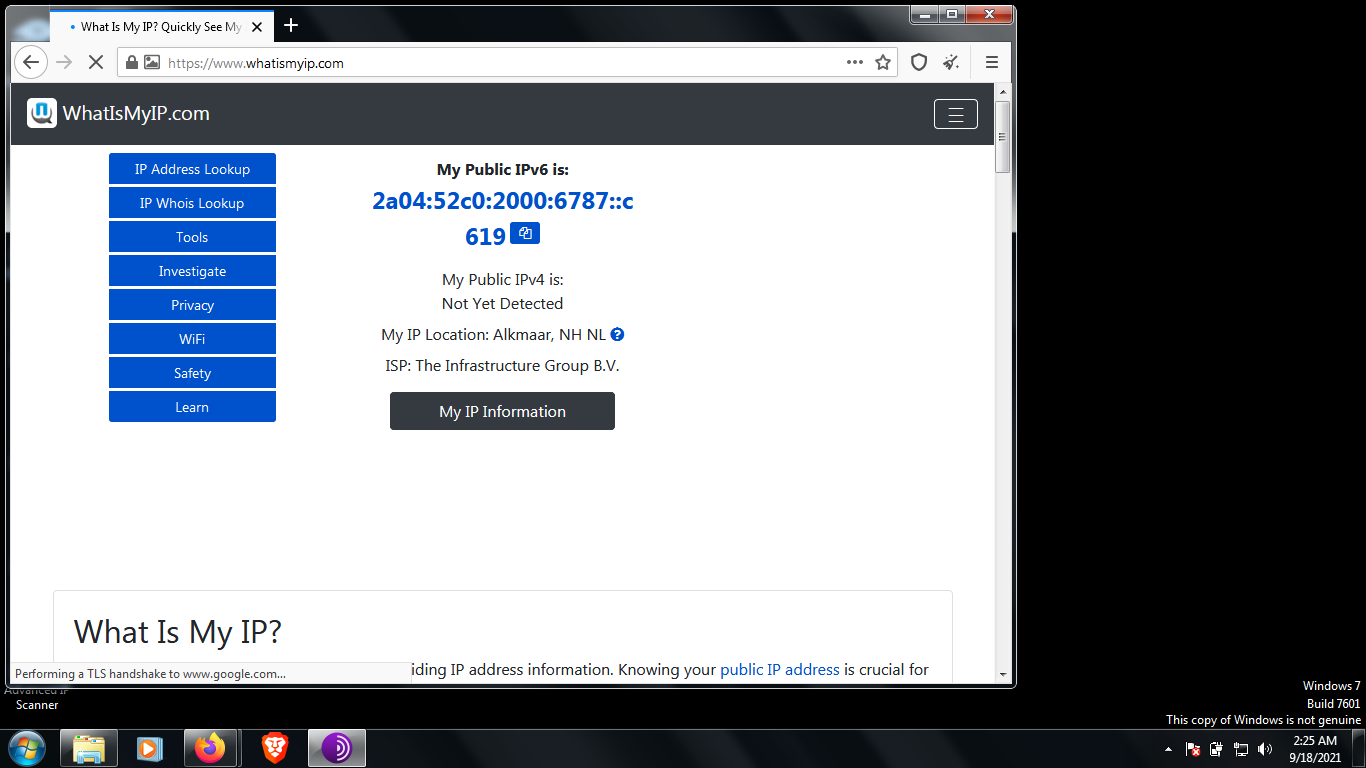
****

****

**There are also tools for proxy servers one of the tool is known a TOR browser.**

**Tor, short for The Onion Router, is** [**free and open-source software**](https://en.wikipedia.org/wiki/Free_and_open-source_software) **for enabling** [**anonymous communication**](https://en.wikipedia.org/wiki/Anonymity)**. It directs Internet traffic through a free, worldwide, volunteer** [**overlay network**](https://en.wikipedia.org/wiki/Overlay_network)**, consisting of more than six thousand relays, for concealing a user's location and usage from anyone conducting** [**network surveillance**](https://en.wikipedia.org/wiki/Computer_and_network_surveillance#Network_surveillance) **or** [**traffic analysis**](https://en.wikipedia.org/wiki/Traffic_analysis#In_computer_security)**. Using Tor makes it more difficult to trace the Internet activity to the user. Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities unmonitored.**

****

****

**Now this were some methods of changing proxies in Windows, Now I will show you how to change proxy chains in Kali Linux.**

**Changing Your Network Information with kali:**

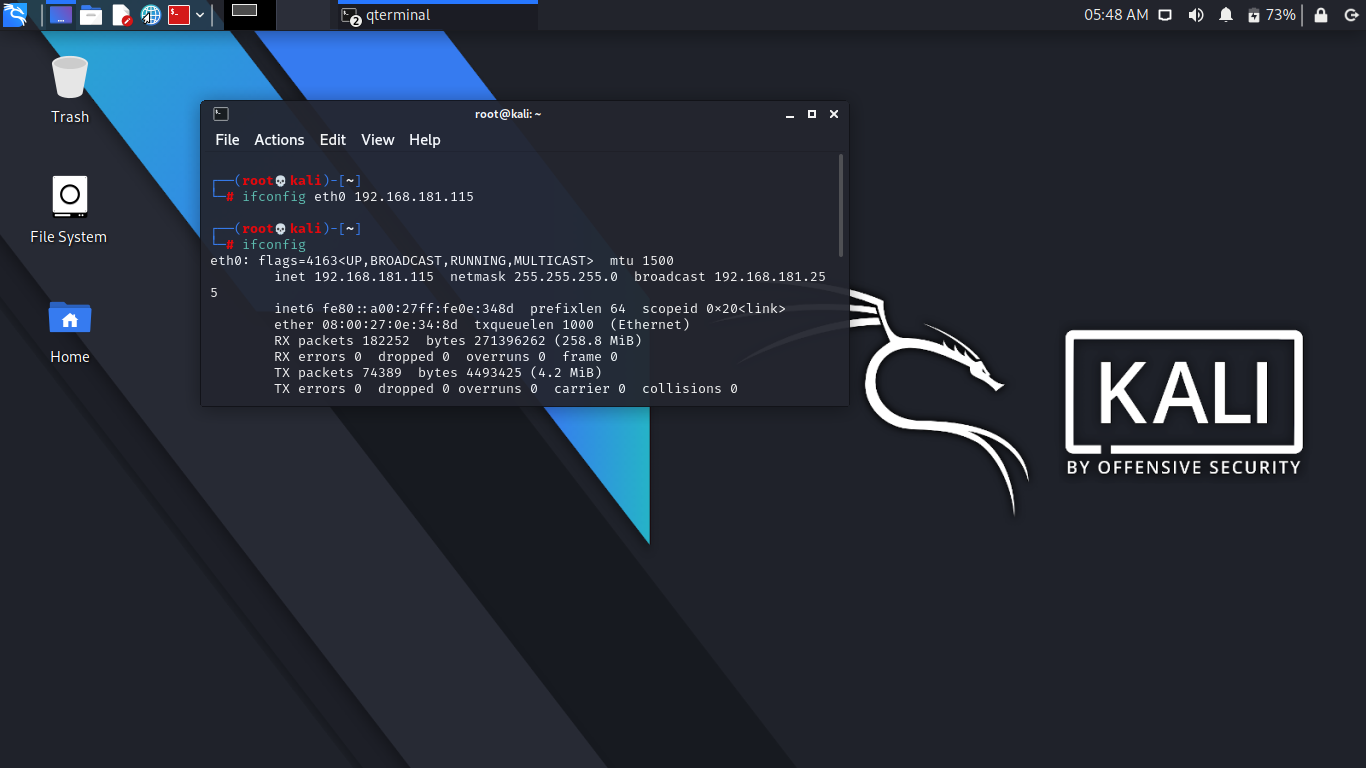
Being able to change your IP address and other network information is a useful skill because it will help you access other networks while appearing as a trusted device on those networks. For example, in a denial-of-service (DoS) attack, you can spoof your IP so that that the attack appears to come from another source, thus helping you evade IP capture during forensic analysis. This is a relatively simple task in Linux, and it’s done with the ifconfig command**.**

Changing Your IP Address

To change your IP address, enter ifconfig followed by the interface you want to reassign and the new IP address you want assigned to that interface. For example, to assign the IP address 192.168.181.115 to interface eth0, you would enter the following:

kali >ifconfig eth0 192.168.181.115

kali >



When you do this correctly, Linux will simply return the command prompt and say nothing. This is a good thing! Then, when you again check your network connections with ifconfig, you should see that your IP address has changed to the new IP address you just assigned.

Changing Your Proxy Chain:

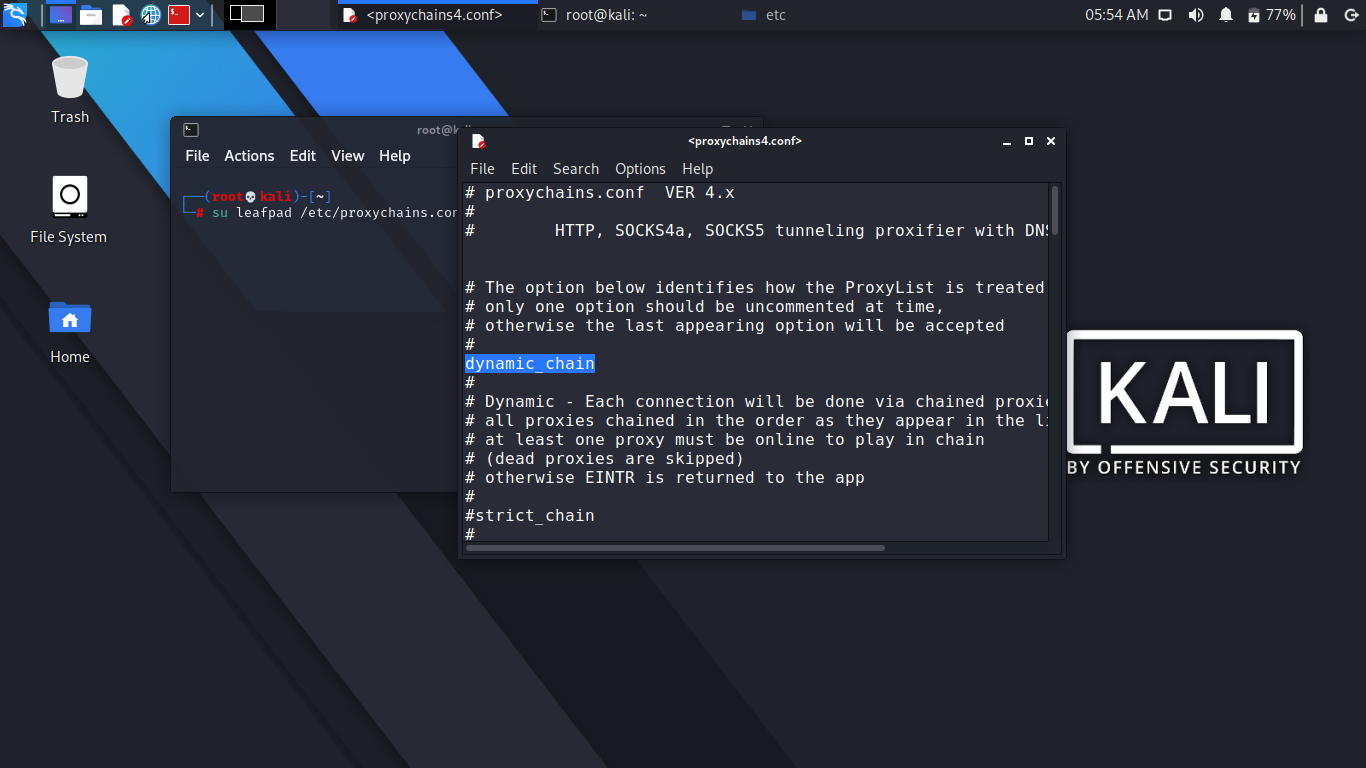
In this case, you need to configure your proxychains.conf file. You will find this file in your etc folder.

Open the configuration file using the Leafpad text editor.

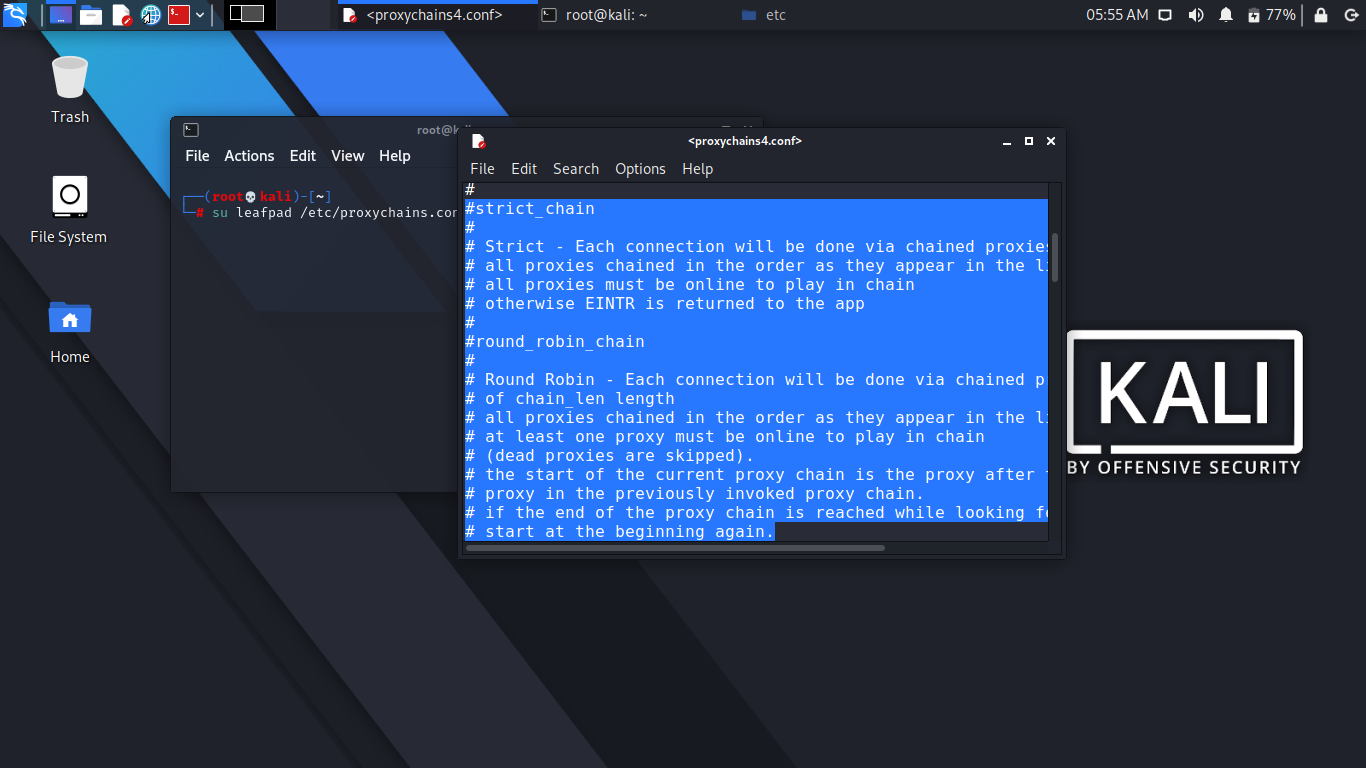
Open your Kali Linux terminal as a root user and enter this command:

su leafpad /etc/proxychains.conf

This will open the proxychains.conf file . There are three types of proxies that you can use. But you can’t use all the proxies at a time. Let’s first see how this file looks. The documentation is clear and to the point.



Uncomment the line where dynamic\_chain is located. After that, comment out strict\_chain and random\_chain one after the other, before testing the proxy.



The advantage of choosing dynamic\_chain over others is clearly stated. If your connection does not get one working proxy, then it automatically jumps to the other. The other two don’t give you that opportunity to route your traffic.

Let me explain it more. Suppose you have two proxies in place: A and B. What happens in the case of strict\_chain is that when you browse web pages, your connection is routed through A and B strictly. This means A and B should be in order and live. Otherwise, your connection simply fails. In the case of dynamic\_chain, this does not happen. If A is down, then it jumps to take B. For that reason, you are going to use dynamic\_chain so that if one proxy is down, the other may replace it.

In between you get a line like this:

# Proxy DNS requests - no leak for DNS data proxy\_dns

This is an important line to be considered seriously. You see I have uncommented proxy\_dns. This will protect against leaking DNS data. You can’t allow DNS data to be leaked. In other words, your real IP address should not be leaked by chance. That is why I have uncommented this line so that your proxies are in the proper place working without any hitches.

At the end of the list you’ll find this line:

[ProxyList]

# add proxy here ...

# meanwile

# defaults set to "tor"

socks4 127.0.0.1 9050

socks5 127.0.0.1 9050

socks5 185.43.7.146 1080

socks5 75.98.148.183 45021

Inspect the last two lines that I have added. I’ll explain them, but first I’ll explain the example lines just given before. They read like this:

# ProxyList format

# type host port [user pass]

# (values separated by 'tab' or 'blank')

# Examples:

# socks5 192.168.67.78 1080 lamer secret

# http 192.168.89.3 8080 justu hidden

# socks4 192.168.1.49 1080

# http 192.168.39.93 8080

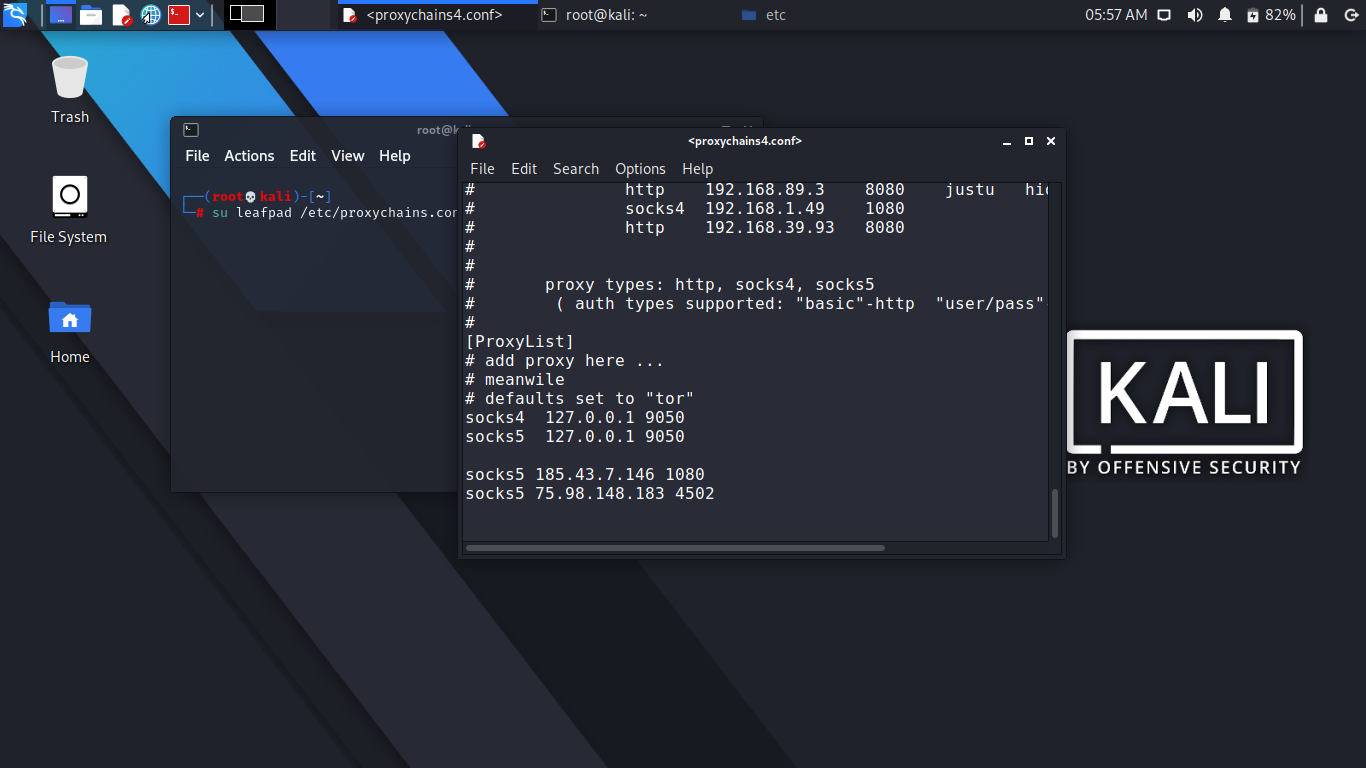
This clearly states how your proxy list should be formatted. Consider the first line:

# socks5 192.168.67.78 1080 lamer secret

This means the first word is the type of the proxy. It should be socks5. The second one is the host. The third one is the port, and the last two words stand for username and password in case you pay for it. Sometimes people buy VPN services; in such cases, the service provides the login credentials. Another important thing is that you must separate the words using either a Tab or space.

There are several free proxies, so don’t worry about the username and password just now. Now you can again go back to the last lines that I added. In the last lines, the defaults are set to Tor. Before adding the last two lines, you need to add this line:

socks5 127.0.0.1 9050



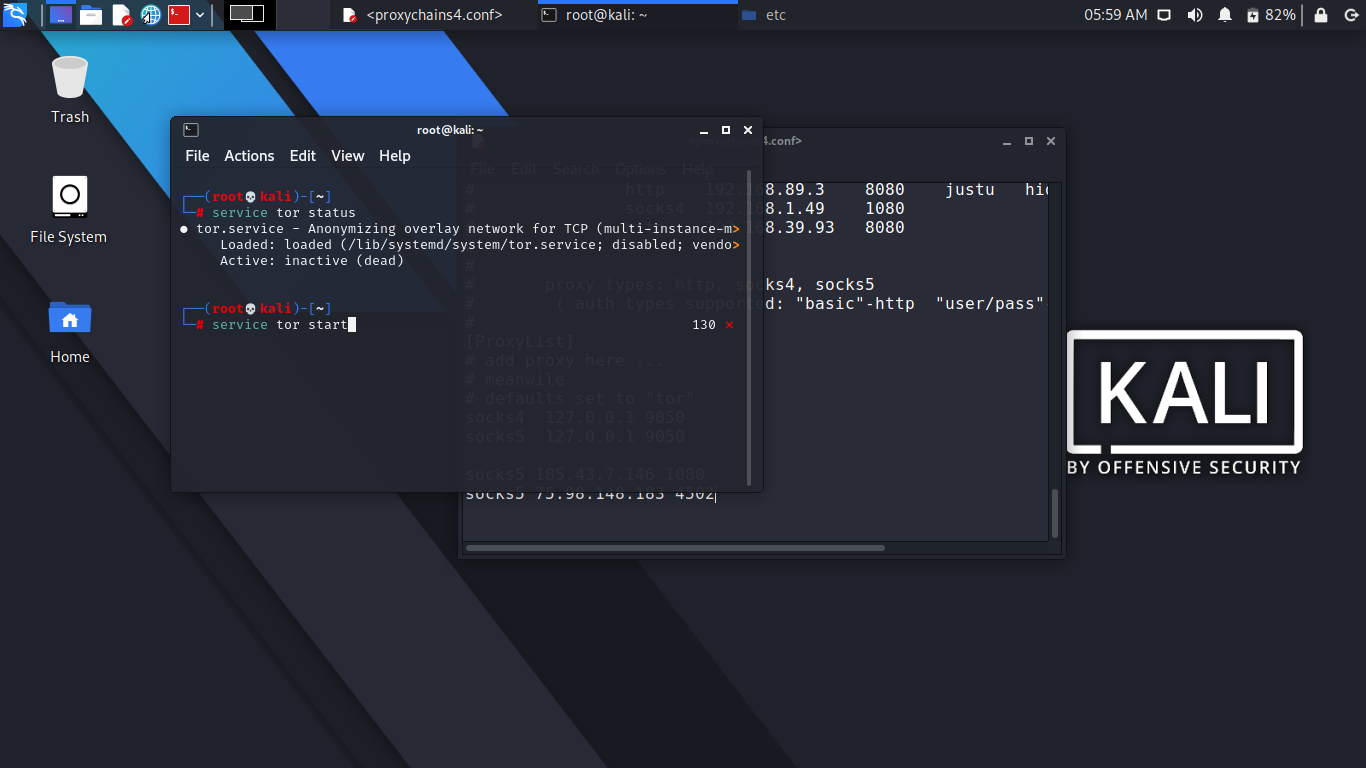
You should do this because usually your proxychains.conf file comes up with only socks4, so you need to add socks5 that supports modern technology. Now you can test your Tor status.

1. Open your terminal and type the following:

root@kali:~service tor status

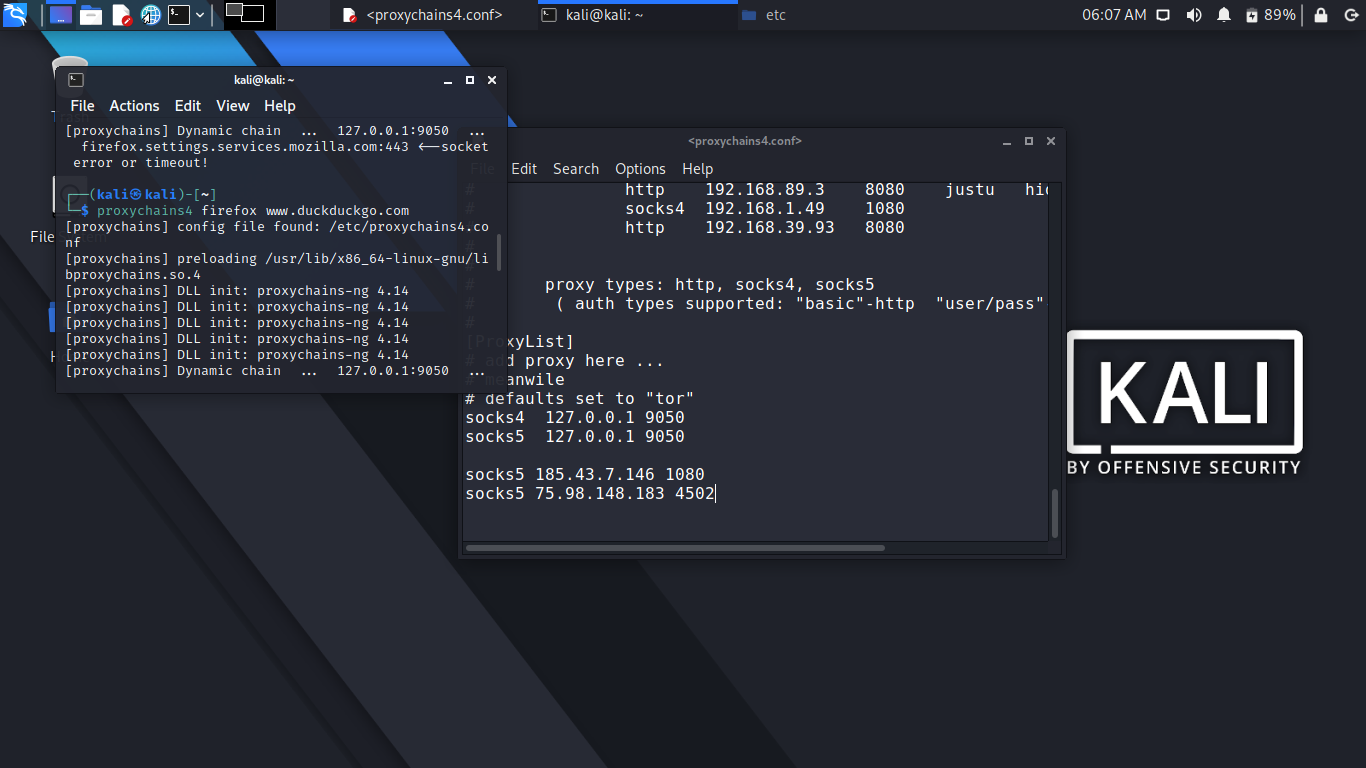
2. It will fail if you don’t start it. Type the following to start the service:

root@kali:~ service tor start



Now you can open your browser through the terminal. Just type the following:

root@kali:~#proxychains firefox [www.duckduckgo.com](http://www.duckduckgo.com)



This search engine does not usually track IP addresses. Your browser will open, and you can check your IP address. You can also see the DNS leak test result. Let’s do that by typing dns leak test in the search engine. There are several services; you can click any one of them to see what it says.

I found that www.dnsleaktest.com is working to find out my original IP address and fails to find out. It shows an IP like 8.0.116.0, and it is from Germany. This is wrong as I am currently staying near Mumbai.

You can simultaneously test this in your normal browser, and you’ll find your actual IP address.

**So these were some methods to change your IP Address in Windows and Kali Linux.**

## Advantages of Proxy

**1. Anonymity**  
Proxy has been used primarily for masking the IP addresses. From this way any hacker trying to access your computer will not be able to do it so. While trying to access your computer, they will be logged into the proxy instead of the real IP address. Besides that the websites will not be able to track you since the original IP address is hidden. This way a proxy can provide anonymity to the user.   
  
**2. Protection**  
While you are browsing the web, there are high chances you may end up visiting malicious websites. In case if you visit such as site, the malware will sneak onto your system causing irreversible damages. Likewise there are numerous untrustworthy websites setup by hackers. Accessing one of them will end up placing all of your personal informations at risk. When you are using a proxy server, your system will not make the request directly to those sites. Always the proxy end will be facing the threats imposed by such sites. This allows your system to maintain maximum protection.  
  
**3. Unblock Websites**  
Many website owners restrict contents to certain geographical areas, basically due to its copyright law. Any person living outside those regions will not be able to access those contents. Since the IP address is hidden using proxy you can access those geo-restricted sites regardless of your location. Additionally some ISPs and organizations too impose restrictions to certain websites. Proxy can be used to bypass these restrictions too.  
  
  
**4. Performance**  
Some of the proxies use cache data. Once a user visits a website, these proxies will store all the necessary informations through the cache data. Due to this, when a user visits a same page, the page will be displayed faster. However this can happen only if the proxy has the necessary cache data from the website. Otherwise, it needs to request it from the remote server. In this case you may fail to notice any page loading speeds.  
  
**5. Control Contents**  
Same as how a proxy can be used to unblock websites, it can be used to restrict access to specific sites. Organizations can use proxy to prevent its employees from logging onto certain websites, so that they can improve their overall productivity.

## Disadvantages of Proxy

**1. Tracking**  
The cache data the proxies use can remember all of the personal informations including that of passwords. This will not be a problem unless someone from outside gathers them. However the problem may comes from the side of proxy itself. There are chances where employees working under proxy misuses these informations. Therefore, it is always recommended to invest in a proxy from a legitimate service provider.  
  
**2. Security**  
Although proxies provide the benefits of anonymity, it lacks on the side of encryption. Most proxies use SSL certificates for encrypting the data. This isn't strong enough to prevent today's attacks. Especially from the attacks known as SSL stripping. Hence, when the SSL type encryptions are used, the data traveling through the server will be less secure.  
  
**3. Incompatibility**  
Proxy may not always be compatible with your local network. Both the proxy and the network has its own configurations. In this case if you need to use the proxy in your location network, you have to either configure them or go with a proxy that completely matches with the network you are using.  
  
**4. Cost**  
Setup and maintenance of a proxy server can be costly. Even though large organizations can easily cover up this expense it will be not for small businesses. Besides installation there are various other expenses involved here.  
  
**5. Configurations**  
The configurations of the proxies are pre programmed for one specific goal. Therefore, there must be some coding that must be done to fulfill one's requirement. But the configurations of a proxy can be quite difficult. It must be made perfectly in a way that no any ports are left open, so that no hackers can spy on your personal informations.

**Difference Between Proxy and VPN**

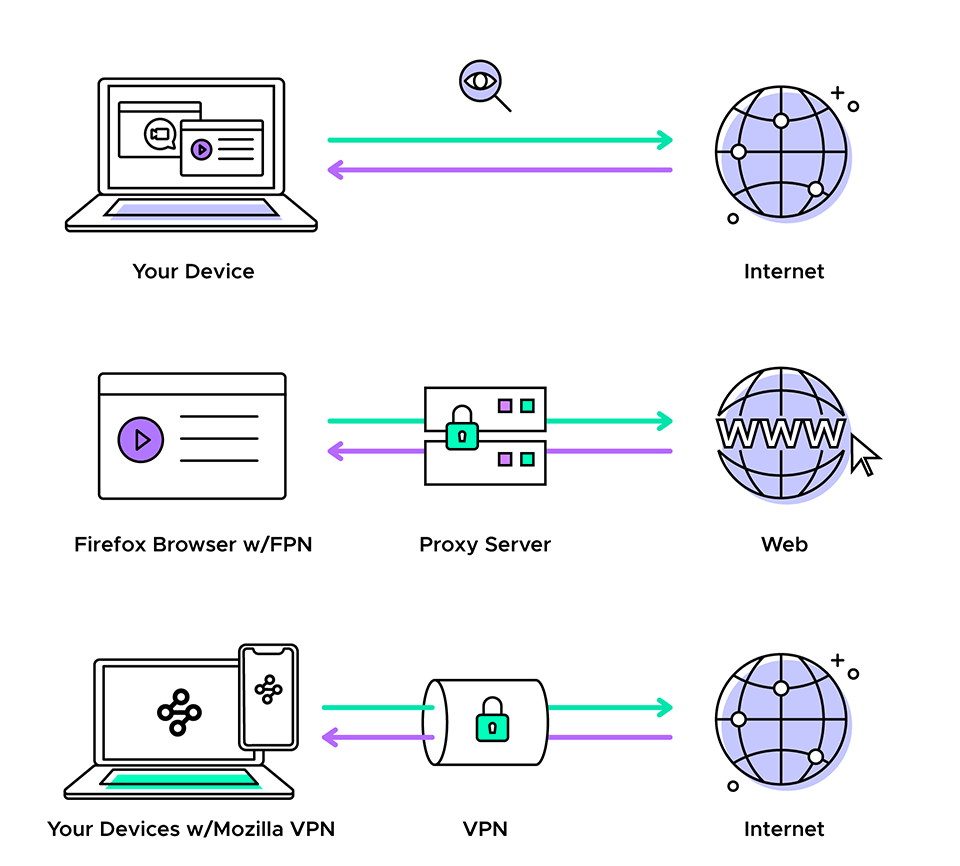
## Proxy and VPN Defined

Both VPNs and proxies enable a higher degree of privacy than you might otherwise have, allowing you to access the internet anonymously by hiding your IP in various ways. But how they do that is quite different.

A proxy acts as a gateway – it’s ideal for basic functions like anonymous web browsing and managing (or circumventing) content restrictions. Proxy servers excel at [IP masking and misdirection](https://www.techradar.com/vpn/what-is-a-proxy-server-and-why-a-vpn-is-a-better-alternative), making them good for viewing geographically limited content. They allow users to bypass content restrictions and monitoring, or enforce website content restrictions – so that you can’t log into certain web pages on company time.

A VPN client on your computer establishes a secure tunnel with the VPN server, replacing your local ISP routing. VPN connections encrypt and secure all of your network traffic, not just the HTTP or SOCKS calls from your browser like a proxy server.

VPNs are great when you need to use the [WIFI at a local coffee shop](https://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/): using a VPN instead of the potentially completely unencrypted local WIFI adds another layer of privacy – who knows who is lurking on that network, just sitting in the corner sipping coffee and waiting to steal your credit card digits?



## Proxy and VPN Drawbacks

If you’re using proxy servers to mask your internet activity, you might see performance issues that prevent you from streaming or downloading the thing you are trying to get. High ping times and other traffic on the proxy server can cause web pages to load slowly. For this reason, some users pay for a private proxy server which limits the number of users that access it, speeding up your connections.

Proxies are also vulnerable to security exploits: they can be open to attack, allowing the bad guys to infiltrate networks or steal private data. Some proxies can still track (and store) your browsing habits, as well as recording usernames and passwords – rendering that promise of anonymity null.

VPNs can also suffer from performance issues, depending on proximity to the VPN server you’re connecting with. VPNs use a local client to create the connection to the VPN server, so any local CPU or memory issues will slow down the connections. VPNs are typically more expensive to use (and maintain) than a proxy server, and they are often more complex to manage.

Just like proxy servers, VPNs can’t guarantee anonymity while browsing. Neither of these services will always encrypt your traffic all the way to the web server. A VPN only guarantees an end-to-end encrypted connection if you use the [HTTPS protocol](https://www.eff.org/https-everywhere) when you go to a new web address. Your data will be encrypted to the VPN, but from that point on, it could be unencrypted to the web server. For some sites, this may be irrelevant: an information-only webpage with no login or payment options for example, but for any sites that require a login or online payments – or any sensitive data – make sure the website is enabled to use HTTPS. Remember, the S stands for moderately more secure.

## Proxy and VPN Benefits

The biggest argument to use a VPN instead of a proxy is the total encryption for all traffic you get with the VPN. Dollar for dollar, a VPN is more secure than a similarly priced proxy. VPN providers maintain their own networks and you use their IP addresses for your connections. The top VPN providers advertise a logless policy, which means they don’t have data to provide to anyone about your browsing habits.

If you’re an IT business owner charged with the security of data and users, there are advantages to both, and you likely have both configured for your company. For users in the network, you might route traffic through a proxy server to log web traffic, protect the organization from malware or other attacks, and enforce a web content policy.

When users are operating out of the office, you will want to use a VPN to create a secure connection to access the company resources (email, internal shares, etc.).

## Proxy vs VPN: Which is Right for me?

Privacy and security matter these days, regardless of if it’s your company data or your own personal data you need to protect. Make sure you’re investing time and money into the correct tools for your security goals: both proxies and VPNs add an additional layer of security and privacy to your data.

If you want to enable your team to work remotely with secure access to the company resources, set up and maintain a VPN users to access the network with the VPN.

If your concerns are more around “what websites are my users hitting,” a proxy server is a better tool.



To get the most bang for the buck (and to protect your data as a security-aware citizen), [sign up for a well-regarded VPN service](https://www.wired.com/2017/03/want-use-vpn-protect-privacy-start/). For the most part, VPN services allow you to use servers in different locations to work around content restrictions. If you need to use a free proxy server occasionally for that purpose as well, just be aware of the risks.

If you’re just starting to implement your data security strategy on an enterprise level, there are more complex attack vectors to account for. [Insider threats](https://www.varonis.com/blog/insider-threats/), [APTs](https://www.varonis.com/blog/advanced-persistent-threat/), privileged account escalations – along with plain old social engineering – are just as dangerous to your data as an unencrypted data stream.

**Neither a proxy nor a VPN will protect you from 100% of the cybersecurity threats your company will encounter: they won’t stop an insider from stealing personal data, a ransomware attack, or a coordinated infiltration effort.**