

MAY 1, 2020 / #CYBERSECURITY

What is a Proxy Server? In English, Please.



Milecia McGregor



Have you ever been traveling and couldn't get the same shows you normally watch back home on Hulu? Or have you noticed that some websites are blocked or you can't access certain services while you're connected to

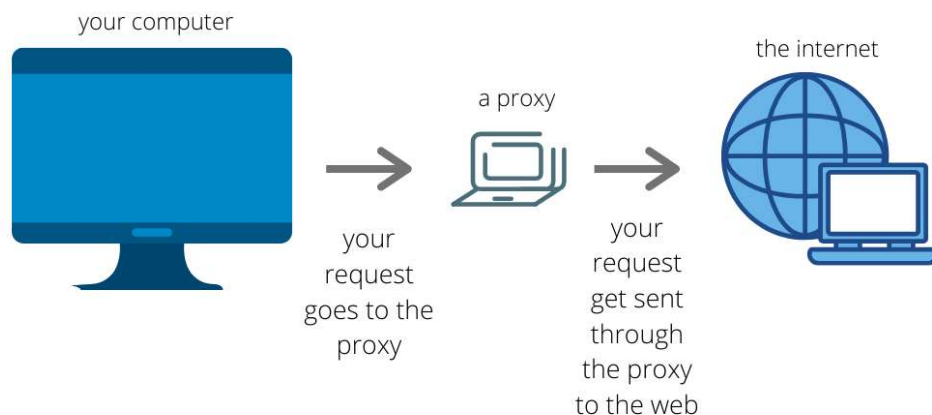
different Wi-Fi networks? That's likely due to a proxy being in place.

What is a proxy server?

A proxy server, or just proxy for short, is like having another computer that your internet requests get sent to before going to the real website. It's a server that takes all of the information you've sent out, like a request to buy new shirts on H&M, and routes it through a different IP address.

That's what makes a proxy so powerful. They can make all of your internet activity appear as if it's coming from a completely different location.

Companies use them for security and network performance purposes, individuals use them for privacy concerns, and there's also some cool functionality you can tap into when using proxy servers for your internet browsing that we'll talk about later.



A proxy can be physically located anywhere. You can set up a proxy on your home computer or you can deploy one to the cloud. The main thing that matters is that the proxy has the configurations you need for the functionality you want.

Just remember that a proxy acts like a fancy IP address filter. Similar to filters, there are different kinds of proxies and they all have their specific uses.

To get started, let's talk about the most common kind of proxy and how it works, the forward proxy.

How a proxy works

When you hear or see people talking about proxies, they're most likely referring to forward proxies. These are the most common types of proxy because they easily handle what most people need. Forward proxies act as the middleman between your requests and the server you're trying to connect to.

The way a proxy works is first you make a request, for example you try to go GitHub. So you type in the URL and hit enter. With a proxy, instead of connecting you directly to GitHub with your computer's IP address, your request gets intercepted by the proxy.

Then the proxy takes your request, updates it, and sends it from its own IP address. This can completely remove your IP address and identifying information from the request to the GitHub server.

One of the ways that proxies handle changing your request is directly in the request headers it sends to the server. A proxy request can set

headers like *Forwarded* and *Via* in the original request before it sends the message to the server you're trying to get information from.

Once the proxy has updated the information from your request, it will send your reformatted request to the GitHub server. That server now thinks your request has come from a different location and it will send the data you wanted back through that location.

Next the proxy takes the data from the GitHub server and does any checks it has been configured to do with that data. It could check for any malicious scripts or other security issues. Then it finally sends the data back to your computer and your page loads.

A proxy server isn't necessarily limited to one user at a time. There can be multiple people sending requests through the same proxy and they can all share the same benefits. There are plenty of reasons you might use a proxy, even if it's a shared one.

Why you would use a proxy

Now that you know what a proxy is, it's good to know some of the common use cases for them.

- You can increase network security by encrypting requests
 - Prevent hackers from intercepting sensitive information
 - Block malware sites from your real network
- You can lower the amount of network traffic by caching sites
 - Cache websites so that only one request to the site is made no matter how many users are on the proxy
- You can control how people use the internet
 - Block specific domains

- Monitor and log all web requests
- You can get around blocks set up by companies and countries
 - Access content from a different country
 - Get around corporate firewalls

This isn't a comprehensive list of everything you can do with proxies, but I also wanted to include some of the other benefits that don't quite fall under the typical categories.

- You always have cookies blocked
- You always have ads blocked
- You can access the deep web
- It removes any search tailoring or tracking your previous searches
- You can scrape data
- You can do research on your competition

Different types of Proxies

There are many different types of proxies that will cover just about any configuration that you can think of. Here, I'll give you a quick overview of 14 different proxy types.

Transparent proxy

Transparent proxies are the simplest kind of proxy. They pass all of your information along, but with the proxy's IP address. These proxies don't offer any kind of privacy protection.

They tell the server you're sending your request to that the request is coming through a proxy. This is enough to get you around simple IP bans. A common use for transparent proxies is setting up website filtering, like schools and companies do.

Anonymous proxy

Anonymous proxies are a commonly used type of proxy. They never pass your IP address to the website you are browsing although they will identify themselves as a proxy in the request. This helps keep your browsing activity private.

When you don't want targeted ads following you around the internet or you don't want your location attached to your request, these are some standard proxies to use. This is usually enough to get around most targeting activities, but there is still a chance that your information might be revealed.

High anonymity proxy

These proxies are the most secure type because they don't pass along your IP address and personal data and they don't identify themselves as a proxy when making requests. They also sporadically change the IP address they use for requests. That's what allows high anonymity proxies to give you the most privacy online.

The TOR browser uses this type of proxy. Since the IP address changes occasionally, that makes it extremely hard for servers to keep track of what traffic belongs to what client. If you don't want to be tracked, this is the best option.

Distorting proxy

A distorting proxy works similarly to an anonymous proxy except it passes an IP that is purposely false. It identifies itself as a proxy and uses that false IP address in requests. This is great when you want to appear as if you were in a specific location.

This is useful when you want to get around specific content restrictions. It's like you get to choose the IP address you want the proxy to use.

Residential proxy

Residential proxies are proxies that use real IP addresses. That means they are the addresses of real computers. These are the best types of proxies to use because they look like regular clients to servers.

Any of the proxy types discussed so far can be a residential proxy. As long as the proxy's IP address is associated with a physical device, these types of proxies tend to be undetectable and they get around some of the geographic problems other proxy types have.

Data center proxy

These are kind of the opposite of residential proxies. Data center proxies have computer generated IP addresses that aren't attached to a real device. It's like having a proxy in the cloud.

An advantage to this kind of proxy is their speed. Usually cloud service providers have incredible internet connections that give you speeds you couldn't get otherwise. Although they would all share similar IP addresses, one server could host hundreds of data center proxies.

Public proxy

Of all the proxy types, these are the most insecure, unreliable proxies available. They can go down at any moment and many are set up by hackers to steal data. The only reason people still use them is because they are free.

While it isn't difficult to find lists of free public proxies, it is a challenge to find good ones. You never know who these proxies are hosted by and it's a huge gamble to send any of your sensitive information through one. Any number of users can be on a public proxy at any time and there's no one regulating who uses it.

Private proxy

Private proxies have some ambiguity around what they are because they're defined by the provider offering the service. This could mean your proxy can only be used by one client at a time or that your proxy needs authentication before you can use it. These are like more reliable versions of public proxies.

A private proxy can be transparent or have high anonymity, similar to some of the others above like the residential or data center proxy. This proxy type has more to do with who can connect to it than how it handles your requests.

Dedicated proxy

A dedicated proxy is like a specific type of private proxy. It just means that the proxy can't be shared by multiple clients at the same time. So only one client can connect and send requests.

This helps prevent the IP address of the proxy from getting banned by different websites and services. It's one of the ways that a proxy

provider can control who has access to the proxy to make sure that it isn't being abused.

Shared proxy

These are some of the cheapest proxies available and they work similar to shared servers. Clients pool together and split the cost of the proxy and they can all access it at the same time. Shared proxies have a more complex architecture because they handle a lot of requests at the same time.

Depending on how resources are allocated on the shared proxy, requests might be slower than over your own IP address. Because it's handling multiple requests from multiple users, the configurations of these types of proxies is more critical than the others.

Rotating proxy

Rotating proxies work a little differently from the others. Every time a client connects to the proxy, a new IP address is created for it. So they never use the same IP address more than once.

Every time a client sends a request a new IP address is generated. This is how proxies like the TOR browser work to keep your anonymity. A rotating proxy provides a high level of security and privacy when combined with some of the other types.

SSL proxy

These proxies follow the same protocol as HTTPS requests. The 'S' in HTTPS means SSL which means your web requests are secure between your client and the server you're trying to get to.

That means you get even more security because all of your requests through the proxy are encrypted. Most proxies should be using this by default, but there is still a chance you'll run into some that use HTTP.

Reverse proxy

Reverse proxies are completely different from everything we've covered so far. A reverse proxy hides the IP address of a server you're trying to send a request to. When a server needs security and privacy from clients, that's when these types of proxies come in.

These proxies are great if you need to monitor access to a server for reasons like keeping clients from having unmonitored access to a database. It can also help lower traffic on the network by passing on cached information instead of making a query each time.

Proxy Services

If you've done a quick search for proxy services, you'll know that there are a lot to choose from. Not all of them are created equally, so it's important that you know what features you want from your proxy service.

Most of these services offer combinations of the proxy types. For example, you'll be able to find residential, high anonymity, SSL proxies rolled into one service. There are a few that stand out from the others so here's a list of them, but make sure you research them to see if they meet your needs.

- <https://smartproxy.com/>
- <https://www.megaproxy.com/>
- <https://whoer.net/webproxy>

- <https://www.proxysite.com/>
- <https://hide.me/en/proxy>
- <https://www.kproxy.com/>
- <https://www.vpnbook.com/webproxy>

Proxy server vs VPN

If you're familiar with VPNs (virtual private networks), then you might be wondering how a proxy is different. The main difference is that a VPN secures all of your network traffic where proxies only secure your internet traffic.

Some things that VPNs secure that proxies don't include FTP uploads or downloads and background operating system processes, like updates.

The only thing proxies and VPNs have in common is that they make your internet traffic look like it's coming from a different IP address. That is all they have in common. The way they handle this is wildly different because of what they're used for.

A proxy just passes along your internet requests, acting like a middleman. A VPN on the other hand tunnels all of your network activity down to the operating system level. Proxies are typically used by a single application like a browser or torrenting client.

Companies tend to use VPNs to let employees access corporate resources without worrying about the traffic being intercepted or recorded by an ISP (internet service provider). These are usually hosted on a physical computer somewhere on premises.

The great thing about VPNs is that they conceal everything you do. If your ISP were to get a history of your usage, it would only see that you were connected to a VPN. Nothing about your traffic would be seen. When you connect to public Wi-Fi, a VPN is the most secure choice.

With all of the benefits that come with using a VPN, there are still good reasons people choose proxies. To start with, VPNs are typically more expensive than a proxy. You also need decent computer hardware to run a VPN. The connection is usually slower than a proxy would be.

There are plenty of times when you don't necessarily need the kind of security that a VPN offers. When you just want to mask your activities on a single application at a low cost, a proxy might be worth considering.

Benefits and risks

Now that you know everything about proxies, here's a list of some of the benefits and risks associated with using them.

Benefits

- Secure and private internet browsing
- Ability to get around geo-location restrictions
- Better network performance
- Ability to control what websites clients have access to
- Many types to choose from to suit specific needs

Risks

- Your requests might return really slow
- Not all proxies encrypt your requests so your information could still leak out
- Free or cheap proxies could be set up by hackers or government agencies
- Proxies can disappear at any time
- All of your requests and information always go through a third party that could be run by anyone

There are plenty more benefits and risks to using any of the proxy server types. That's why it is important to only connect to proxy servers you trust. When you are connected to a trusted proxy, the risks should have been taken into account in the configurations so you have less to worry about.

How to set up a simple proxy server

Creating your own private proxy sounds a lot harder than it is. You can make a proxy with a computer in your house that's just as secure as most proxies you can buy. It just takes some patience and a little curiosity.

On a Linux server, you can install Squid and set the configurations for the proxy you want to create. You'll be able to do things like block specific websites or require authentication before a client can connect to the proxy.

Here's a great walk through on setting up a Squid proxy on Linux:
<https://devopscube.com/setup-and-configure-proxy-server/>

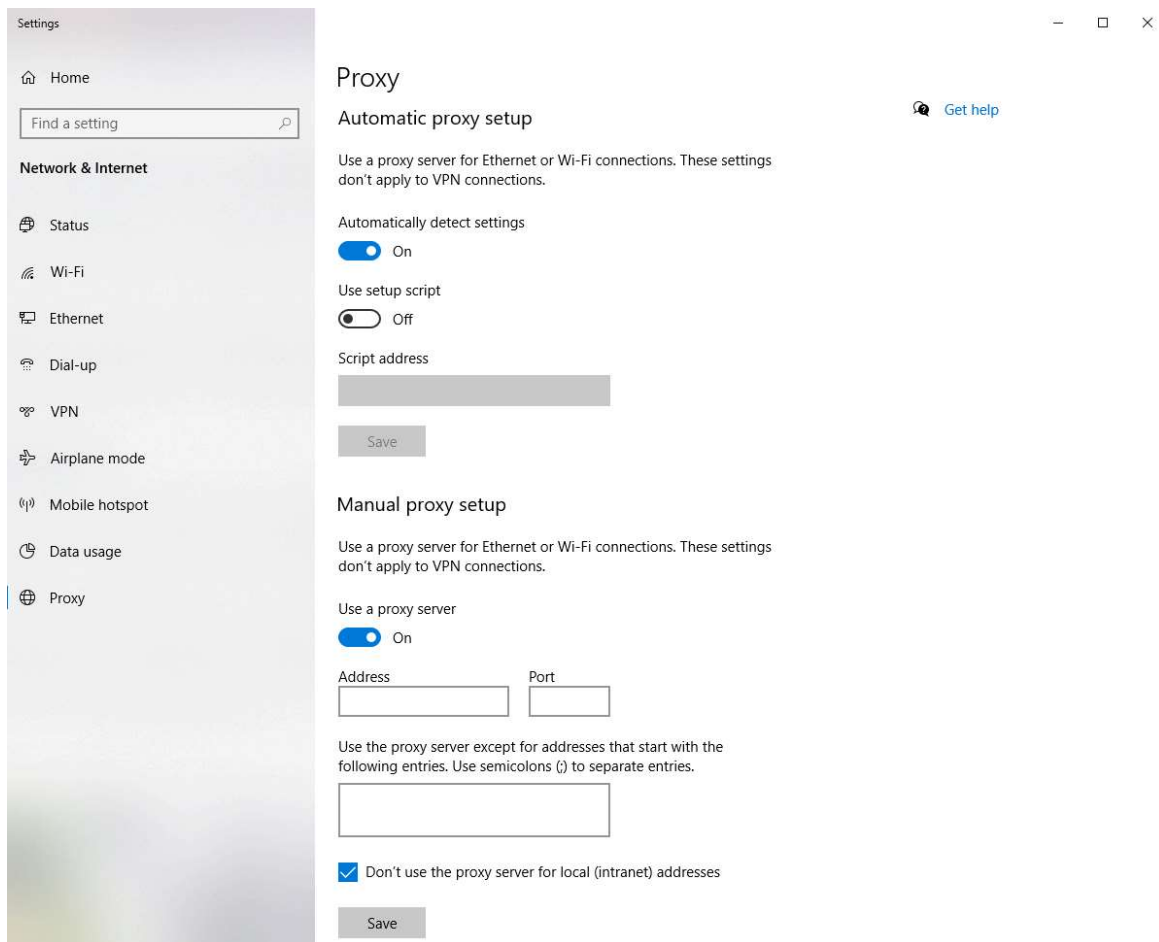
On Windows and Mac, you have the option of making a proxy server using Python and the [Google App Engine](#). You will have to pay for the Google App Engine service, but they make it fairly affordable.

Setting up a proxy like this is a little more involved than on Linux, but here's a great walk through: <https://www.hongkiat.com/blog/proxy-with-google-app-engine/>

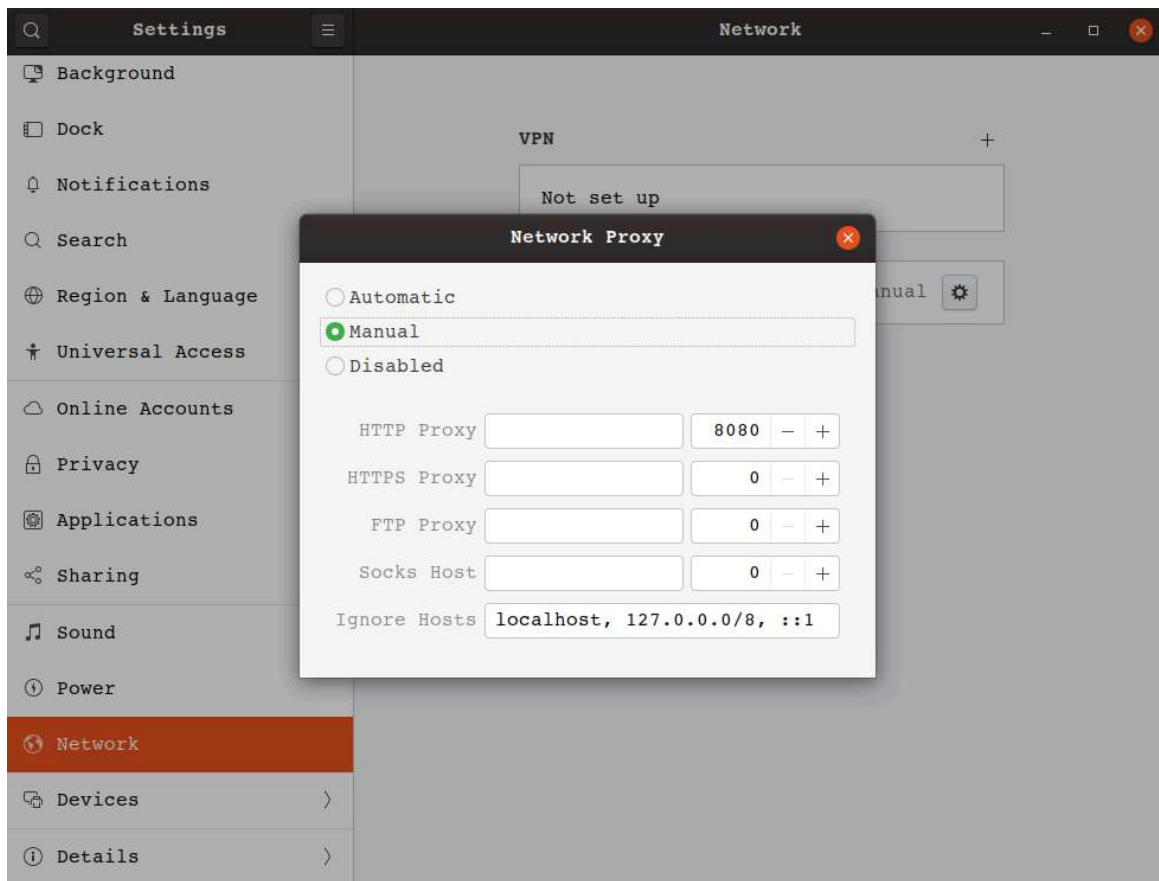
How to connect to an existing proxy

Connecting to proxies is usually a straightforward process once you know your proxy's information, like its IP address and port number. No matter what operating system you use, proxies are usually quick to set up.

Typically you'll go into your network settings and find where you can enter your proxy information. Then you should be able to connect and a web page might appear if there's an authentication step included by the proxy. Here's what it looks like on Windows and Ubuntu.



setting up a proxy server though the Windows Settings



setting up a proxy server through the Ubuntu Network Settings

Conclusion

Now you know everything about proxy servers from what they are to how to create one for yourself! I have a little proxy set up on my home network and it does make some things a lot easier to access when I'm away from home.

I write about other random stuff in tech too, like machine learning and VR. You should follow me on [Twitter](#) to learn stuff that is just cool sometimes. Plus [I've got a website](#) where you can check out my other articles and watch my slow transition from the current site to my shiny new one.



Milecia McGregor

International tech conference speaker | <New courses & books coming soon!> |
Super Software Engineering Nerd | Still a mechanical engineer at heart | Lover
of difficult tech problems

If you read this far, tweet to the author to show them you care.

[Tweet a thanks](#)

Learn to code for free. freeCodeCamp's open source curriculum has helped more than 40,000 people get jobs as developers.

[Get started](#)

freeCodeCamp is a donor-supported tax-exempt 501(c)(3) nonprofit organization (United States Federal Tax Identification Number: 82-0779546)

Our mission: to help people learn to code for free. We accomplish this by creating thousands of videos, articles, and interactive coding lessons - all freely available to the public. We also have thousands of freeCodeCamp study groups around the world.

Donations to freeCodeCamp go toward our education initiatives, and help pay for servers, services, and staff.

You can [make a tax-deductible donation here](#).

Trending Guides

Our Nonprofit

[About](#) [Alumni Network](#) [Open Source](#) [Shop](#) [Support](#) [Sponsors](#) [Academic Honesty](#)
[Code of Conduct](#) [Privacy Policy](#) [Terms of Service](#) [Copyright Policy](#)