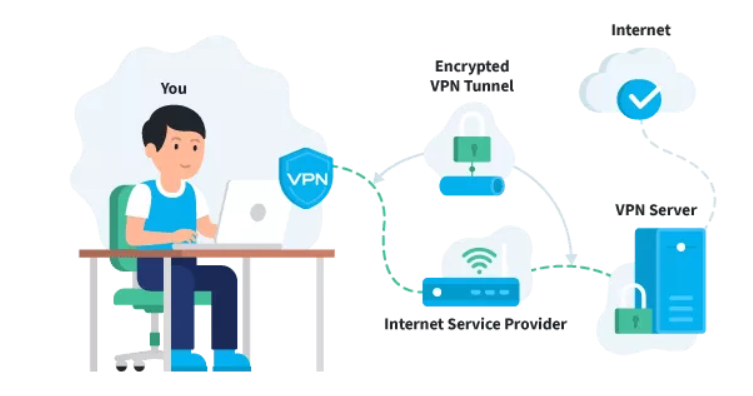
**What is a VPN?**

fter subscribing to a VPN provider, you can usually download and install an easy application on your smartphone, tablet, computer or smart-TV.  With a couple of clicks, you select your preferred security settings and set up a safe connection with your desired VPN server. Connecting to a VPN is generally simple. When the connection has been established, the following will happen to your data:

1. The VPN software on your computer encrypts your data traffic and sends it (via your Internet Service Provider) to the VPN server through a secure connection.
2. The encrypted data from your computer is decrypted by the VPN server.
3. The VPN server will send your data on to the internet and receive a reply, which is meant for you, the user.
4. The traffic is then encrypted again by the VPN-server and is sent back to you.
5. The VPN-software on your device will decrypt the data so you can actually understand and use it.
6. The VPN connection will encrypt your data traffic, making it much more difficult for hackers and other parties to intercept and view your personal information. The secure connection also provides the user with increased anonymity, because the internet traffic is rerouted through an external VPN server. Since you’re surfing the web via the IP address of the VPN server, your real IP address will remain hidden.
7. Normally, your location and even your identity could be revealed through your IP address, because it’s unique to your internet connection. By [using a different IP](https://vpnoverview.com/privacy/anonymous-browsing/hide-or-change-ip-address/) (the one assigned to the VPN server) none of your actions online are traceable to you, allowing you to surf the web more anonymously.
8. The VPN application runs in the background of your computer, tablet, or smartphone. You can access the internet as you normally would and won’t notice anything different – save for the fact that you’ll be able to get around online restrictions.

****

A VPN (Virtual Private Network) is a piece of software that **masks your IP** address by routing your network connection through a remote server. VPN providers usually have servers located in multiple locations over the world so you can choose to which one you want to connect to based on your needs.

Because you'll be connected through a different server, it means that your ISP, the government, or the websites you visit won't be able to see pinpoint your real location as they'll see the IP address of the VPN server.

Besides making you anonymous online, **the VPN client also encrypts all the network data by creating a secure tunnel**. So even if someone manages to get access to the data transmitted between your device and the internet, they won't be able to read it.

With a VPN service, your ISP, the government, or other snooping eyes cannot see what you're doing online. Even though a VPN doesn't protect your computer against malware or viruses, it does improve your online security by hiding your presence and activity from hackers, making it more challenging for them to steal your private information and use it for identity theft or other fraudulent activities.

VPN services are the most efficient way to keep your online privacy.

A VPN server gives you a **secure private network**, lets you connect to your business network even if you're remote, and gives you the opportunity to private internet browsing.

A VPN (Virtual Private Network) represents a service that makes your connections secure and private. Simply put, a VPN server hides you online and protects your data across the internet.

A VPN extends a private network inside a local network. What does this mean?

Let's say you need to exchange a big amount of data with one of the coworkers who work remotely and you both must be connected to your business's local network. **The easiest way to handle this situation is to set up a VPN connection to your local network**. This will let your coworker connect to the network as you are both connected to the same local network.

To understand how a VPN works, you must first understand how the traffic on the internet works.

When you send a *request* online (navigating, downloading), the request is made through your *local network* (LAN). Meaning your data (like the IP) is visible and trackable.

When you connect to the internet through a VPN server, things change. The request won't be made through your LAN, but it'll be made *through* the VPN connection you set up. Your IP won't be visible anymore and the data you send is *encrypted*.

**The VPN client** **encrypts your data**, meaning that your internet provider (ISP) *won't* be able to read it. **When the data reaches the VPN server**, it **gets decrypted and sent forward to the website you want to access**. The website won't see your IP and location but the IP and location of the VPN server you're connected to.

Hence, the internet provider (ISP) won't be able to track your moves online. This makes for private internet browsing.

**Between the client and VPN server, it is a tunneled and encrypted connection**, but the connection from here to the internet **IS NOT encrypted by VPN**.

Example of what I found on PIA's site: [](https://i.stack.imgur.com/3Bu2j.jpg)

Its has an encrypted connection to the VPN server but an 'anonymous connection from there to the internet.

No the data from the PIA-servers to the website hosts is **no more secure** than it would be if you were to connect to them directly.

If you connect to a website via http (unencrypted) your data would be visible. If you connect via https your data would be encrypted and not readable by other parties.

Whether your data comes from your computer, or PIA-servers does not make a difference.

**The benefit of a VPN service is that your ip-address/location information is unlikely to be detected by the last member of a connection (e.g. website).**

**Non-VPN traffic** could be simplified to show as:

**Browser > OS > internet > web server**

Above, the browser asks your computer's operating system (OS) for a connection to the internet, which most likely first goes through some modem/router in your own network, and your ISP's servers.

When using a **public VPN** (like to securely use untrusted public WiFi networks, or to fool a web server you're in a different country), the flow is like:

**Browser > OS > encrypt > internet > VPN provider > decrypt > internet > web server**

So, the browser does not even know it's using a VPN (the operating system takes care of that) and the VPN provider decrypts the VPN traffic and then forwards it to the target server.

When visiting **a HTTPS** website, the traffic is encrypted by the browser and web server as well. **Without VPN**:

Browser > **encrypt** > OS > internet > web server > **decrypt**

When using both HTTPS and VPN the traffic is encrypted twice. In that case the VPN provider can only decrypt the VPN traffic but cannot see what the browser is actually transmitting:

**Browser > encrypt > OS > *encrypt* > internet > VPN provider > *decrypt* > internet > web server > decrypt**

Note that if it's a **private VPN** (like to connect to a company's network) then the VPN server might also allow traffic to the internet:

**Browser > OS > encrypt > internet > company VPN > decrypt > company network > internet > web server**

However, private VPNs are often configured to not route traffic to any external website:

Browser > OS > encrypt > internet > company VPN > decrypt > **company network only**

To get around that, the VPN client on your computer's OS might allow for using VPN only for *some* of the traffic. Like on a Windows computer, by disabling options [such as](https://superuser.com/questions/29922/2-internet-connections-with-vpn/29928#29928) "Use default gateway on remote network" the OS will only use the VPN for traffic to your company's network, but for other traffic just connect to the internet as usual. That might be a security risk though (like malware on your computer can connect to both the company network and any other server on the internet at the same time!) and should not be changed unless you truly understand the risks.

**To access a website**:

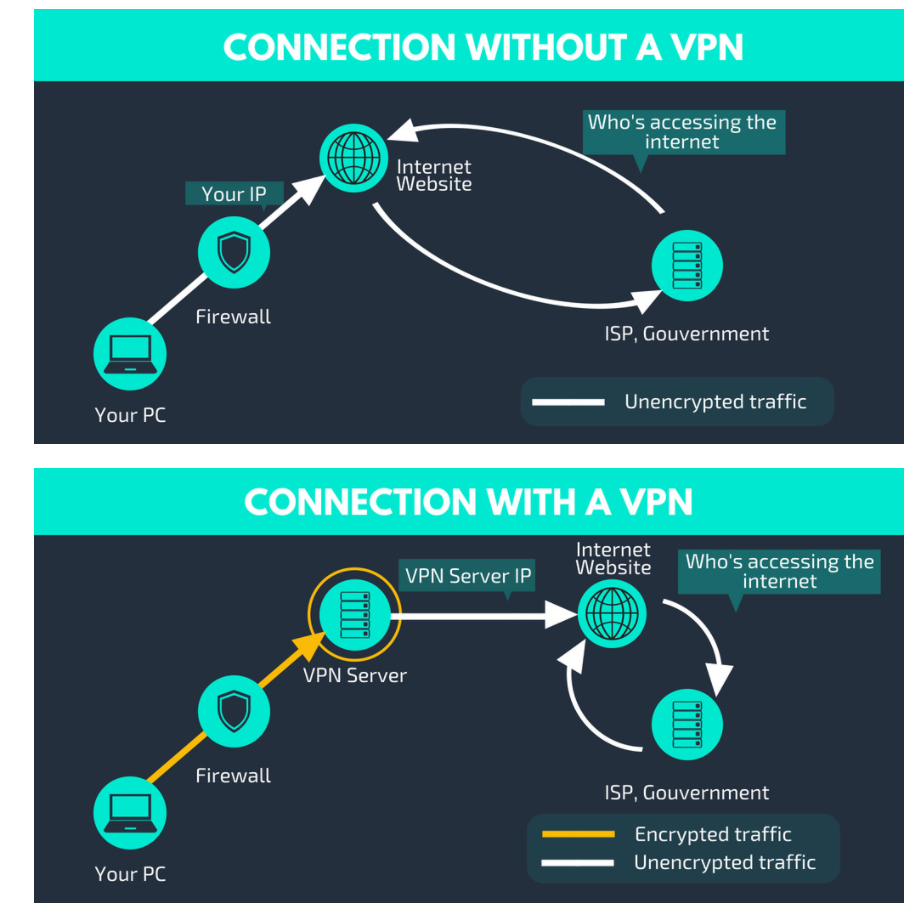
**Without VPN:**

**User -> ISP1 -> Internet -> ISP3 -> Website**

**With VPN:**

**User (Through VPN client) -> ISP1 -> Internet -> ISP2 -> (VPN Server) -> ISP2 -> Internet -> ISP3 -> Website**

The **VPN Encryption is only between the User and the VPN server**. Data travelling after the VPN server is as secure as the website you are contacting.



This is when connecting using a VPN server successfully and efficiently solves the problem. When you connect to a VPN server, the firewall will be able to see the connection between your device and the VPN server. But because the connection is **encrypted**, it won't be able to see the data that's being transferred. Hence, you'll be able to access any website without the firewall blocking your connections.

## **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.

[](https://www.varonis.com/blog/wp-content/uploads/2018/05/proxy-vs-vpn.png)

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.

**VPN vs. Proxy: how do they work?**

When you try to open a web page, your device sends a request to your [Internet Service Provider (ISP)](https://clario.co/blog/internet-service-provider-tracking/). The ISP sees the request and shares your IP address with the website you are trying to access. The website then receives your IP and grants you access. Boom, you’re in.

Your IP address is associated with who you are, where you live, and what you do online. A proxy will mask this information from other parties online.

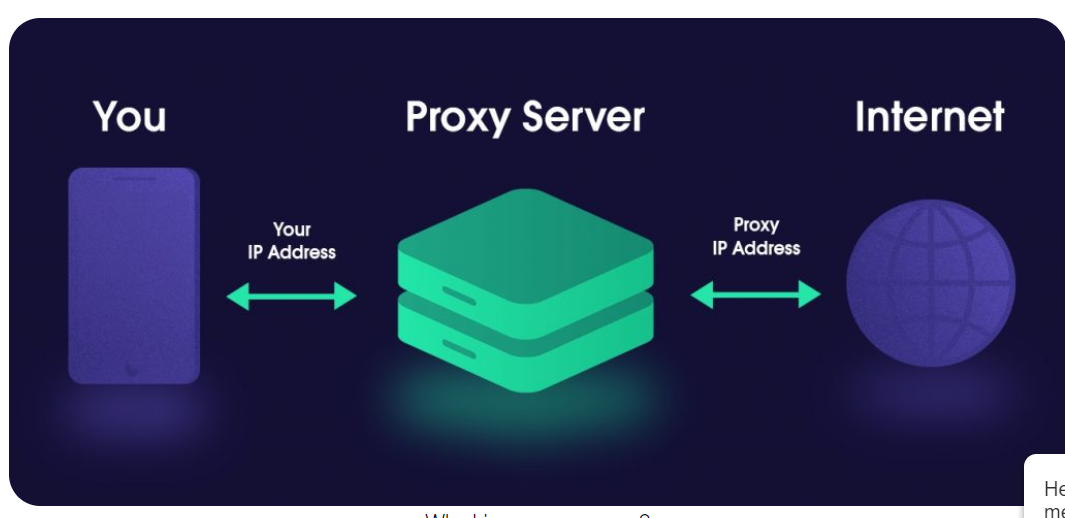
**A proxy server acts as a middleman between you and the internet.** When using a proxy, the exchange between your ISP and the website you are trying to access is remodeled. Your ISP sends the IP of your proxy server to the website instead of your device’s IP. Hence, it looks like your proxy, not you, has visited the website.

**Similarly to a proxy server, a VPN (Virtual Private Network) hides your IP address.** But alongside this, a [VPN](https://clario.co/blog/do-i-need-vpn/)**encrypts all the data** flowing between you and the web.

This is the main difference between a proxy server and a VPN. But there is more to help you differentiate a proxy from a VPN. Let’s look at the key factors.

### What is a proxy?

A [proxy](https://oxylabs.io/blog/what-is-proxy) acts as an intermediary between you and the internet. Think of a proxy as a web filter that performs the internet’s request transactions on your behalf. The website that you are visiting will only be able to determine the proxy IP address, meaning your real IP address will be hidden.



## **Why use a proxy server?**

There are several types of proxy servers and use cases as they can be configured for a wide variety of roles. For you, a proxy server may allow you to access content not available in your country. For your boss, the proxy server they set up may also be the reason why you can’t watch Crunchyroll at work.

A proxy server might be closer geographically to you than your destination – or it might be a “reverse proxy,” closer to the website and service, fulfilling a task it needs, like managing visitor flows.

But if you’re purposefully connecting to a proxy server, why? Here are several reasons why you’d want to do that.

[**Bypass restrictions**](https://surfshark.com/use-cases/unblock-websites)**:** oh no, your school or workplace doesn’t allow you to access some great websites or services via the internet; what can you do? Well, you can connect to a proxy server. That way, the firewall at your work/school will see you connecting to the proxy server, not *kittens247.com*. And if the system isn’t told to block the proxy connection, it will allow any traffic between you without any issues. It works in a similar way when it comes to country-wide censorship as well.

[**Fool geo-blocking**](https://surfshark.com/blog/geo-blocking)**:** if the content is marked as unavailable in your country, stop trying to access it from your country. What you can do instead is connect to a proxy server in a country that has access to the entertainment/news/cat pictures you need.

**Improve online security:** from individual users to corporations, a proxy can act as a firewall defending against malicious attacks online. And on the most basic level, it can keep you more secure by **obscuring your IP** – your device’s address online. If you don’t personally identify yourself, nobody will know it was you who visited the website!

**Control internet usage:** this mostly matters to companies or others who set up their own proxies rather than streaming fans. If you control the proxy, you can ban some web addresses to keep your kids, employees, or whoever uses the network running through the proxy from going where you don’t want them to go.

**Improve speed, save bandwidth**: another use more interesting for companies than people is having **proxy servers cache** (save) copies of frequently accessed websites. Additionally, if five users visit the same web page, the server can ping it once and then dole out the information to the five users, lessening the network load.

Normally when you browse the web, your computer connects to a website directly and begins downloading the pages for you to read. This process is simple and direct.

When you use a proxy server, your computer sends all web traffic to the proxy first. The proxy forwards your request to the target website, downloads the relevant information, and then passes it back to you.  
Why would you do this? There’s a couple of reasons:

* You want to browse a website anonymously – all traffic appears to come from the proxy server, not your computer.
* You need to bypass a content restriction. Famously, your UK Netflix subscription won’t work in the USA. But if you connect to a UK proxy server it looks like you are watching TV from the UK and everything works as expected.

Although they work very well, there’s also a few problems with proxies:

* All of the web traffic that passes through a proxy can be seen by the server owner. Do you know the proxy owner? Can they be trusted?
* Web traffic between your computer and proxy, and proxy and website is unencrypted, so a skilled hacked can intercept sensitive data in transit and steal it.

**What is a firewall?**

A firewall, simply explained, is a **shield** between the **internal network** (your computer) and **the external network** (the internet).

The firewall can be either software or hardware and, in both cases, **it keeps an eye on the ongoing and outgoing traffic and decides what data packets to let in or out based on a set of rules**. The firewall is the first line of defense for your computer as it will block the traffic coming from suspicious sources to communicate with your computer.

With a firewall, you can set up your **own security rules**. You can choose to **block the traffic from certain websites or services** or whitelist programs and websites as firewall exceptions. You have probably noticed that in places like offices and schools, you're not able to access specific platforms (such as social media platforms). This is because the **firewall was set up to restrict users' access to those specific pages**.

While the firewall creates a pretty strong layer of security for your computer, it cannot do it all. For example, it might decide some data packets are theoretically safe to pass through because they come from a source that's not blocked by the rules, but it's not able to tell if those packets are malicious.

Starting with Windows XP, all Windows operating systems come with a pre-installed firewall. It was upgraded to Windows Firewall with Advanced Security as of Windows Vista and, even though the revised version offers more protection, there are still other firewalls out there with a better interface, configuration, and which provide a higher level of security.

**What is antivirus?**

Antivirus software is a program designed to detect and remove malicious software such as viruses, worms, Trojan horses, adware, ransomware, and other types of malware. You might also come across the term "antimalware programs", which is basically the same thing as an antivirus.

Hackers and cybercriminals use different types of malware so they can infect their victims' computers with the purpose of damaging the devices, stealing private information, and even for identity theft or other fraudulent activities. The antivirus prevents you from becoming a victim of such attacks.

Antivirus software scans the data your computer comes in contact with - the **web pages**, **the files you download**, **the applications**, the pieces of software. It searches for known malware and monitors to see if there's any suspicious behavior going on. If it spots something unusual, the antivirus blocks and removes the malicious files as quickly as possible.

Because new types of malware are created every day by prolific cybercriminals, antivirus software relies on updates. They are continuously updating their database so they can detect as many types of malware possible for the best protection for their users.

Windows 10 comes with a built-in antivirus software called Windows Defender which has seen great improvements compared to the older versions of Windows' antivirus. There are still other antivirus software out there that perform better in terms of detecting malware and that also come with extra features. It's best to invest in a paid program to get the highest level of security, but there are also free alternatives which provide you a basic layer of online security.

**VPN vs Firewall**

The differences between VPN vs firewall are pretty obvious.

* A **VPN secures your internet connection**, making sure no one is able to monitor your online activities and steal your private data such as account credentials or credit card information. However, **it does not secure your computer**.
* **A firewall lets you configure the way your computer communicates with the internet by setting your own set of security rules**, which prevents malicious traffic from entering your device.
* A VPN is not able to set up security rules and restrict data packets from entering your computer. On some VPN clients, you might find the Killswitch feature which kills the internet access if there's a problem connecting to the VPN server. But this only prevents you from having your real IP address exposed by mistake.
* While a VPN will help you bypass geographical restrictions so you'll be able to access any content online even if it is not available in your country, a firewall cannot do this. The firewall can only create restrictions on websites that can be accessed from your computer.

**VPN vs antivirus**

While both VPN and antivirus have the same purpose of protecting your data, they do it in completely different ways.

* A **VPN keeps you private when browsing online** so hackers are not able to monitor your online activities.
* An **antivirus protects your computer from getting infected with malware** by scanning every file you download from the internet and removing the malicious files if it detects something suspicious.
* A VPN is not able to protect your computer from malware. It does encrypt your online traffic and data, but if you download or click on something malicious, the VPN is not able to detect it.