What's a VPN?

Don't worry it's not just for porn (not that there's anything wrong with that)

Justin
Dec 7, 2020

The TL;DR

A Virtual Private Network (VPN) lets you route your internet access through a specialized server that keeps your sensitive information private.

- Accessing the internet (sending requests to servers) directly reveals your IP address, and public WiFi networks can **expose sensitive information** like your passwords
- VPNs help you keep your information safe by **routing your requests through a proxy server** that masks your location and information
- You can set up a VPN server yourself, or use a **third party service** like ExpressVPN
- Some companies have **internal VPNs** for accessing company services like admin tools

Almost a quarter of all internet users have used a VPN before, and it's a $20B+ market.

IPs, location, and public networks

Every time you access the internet directly from your laptop or phone – think opening your Facebook app, refreshing your email, or using Slack – you're making requests to servers from your IP address. Now, I'm no privacy freak, but it is pretty jarring how much you can learn about someone from just their IP; the biggest piece of information is your physical location. This is pretty easy to demonstrate: follow this link, find your IP address (it should populate automatically), and see the results. It will pinpoint where you are to a pretty remarkable degree of accuracy.

> 🔍 **Deeper Look** 🔍

> If you're wondering *why* it's so easy to find out the location of an IP address, it's because of the Regional Internet Registry, or RIR – they take care allocating and managing IP addresses across the world, and they're committed to information transparency about each IP. The U.S. is covered by a sub-organization called ARIN.
>
> 🔍 **Deeper Look** 🔍

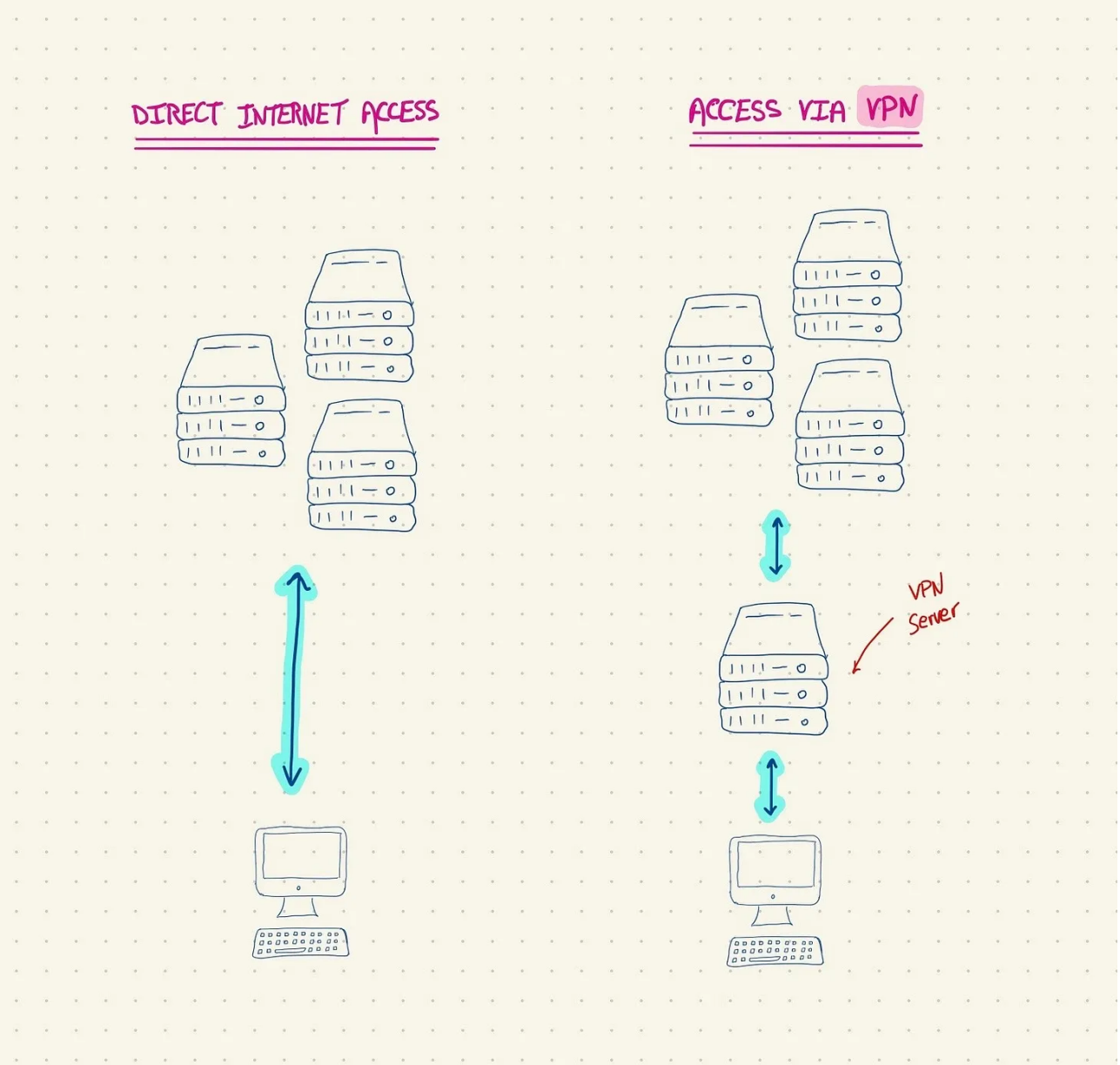
If you've ever tried (and failed) to access Netflix from a foreign country, this is how they know where you are (*they know, they know, they know*).

Location isn't the only thing you're exposing when you access the web directly - if you're on a public WiFi network (read: no username and password), the information you send over the web is *very vulnerable*. If you log into your Bank of America account on a coffee shop's WiFi network, that information is traveling over an unsecured network, and can get stolen via Man in the Middle attacks, malware, snooping, etc. It has definitely taken a while, but it's universally accepted these days that public WiFi is really insecure and you need to be careful (I'm not, of course).

This information isn't supposed to make you paranoid, but it's illustrative of a broader point: accessing the web directly from your devices comes with baggage.

How VPNs work

VPNs are actually pretty simple in theory. Instead of you making requests to origin servers (the Twitter servers, Gmail servers, etc.) directly from your laptop or phone, you route your request to a server in the cloud, and *that server* makes the request *for you*. From Twitter or Gmail's perspective, they see the VPN server's IP address making requests, and your personal IP (your device's IP) remains masked and Very Very Safe. That's it.



This model of a “server in the middle of things” isn’t unique to VPNs. The pattern is generally called a **proxy server**, and it’s a popular choice for web apps that don’t want to expose their infrastructure to clients directly (and also for caching). It’s sort of like using a middle man, which has benefits for *both sides* of the transaction.

VPNs have been around for ages, and there are a bunch of **open source protocols** that simplify the process of actually setting one up (we’ll talk more about this down below).

> 🧠 **Jog your memory** 🧠

> A protocol is a communication standard: it defines a rigid way that two devices talk to each other so that they're not speaking nonsense.
>
> 🧠 **Jog your memory** 🧠

The most in-vogue VPN protocol right now is OpenVPN, which was originally released in 2001. It takes care of encryption standards, managing ports, firewalls, and a lot of the ugly network and security stuff that's above my pay grade. The repo on Github has 5K+ stars, but there's also a managed version you can pay for on the site. There are a bunch of other protocols available, like L2TP and SSTP, but you're not really going to need to worry about that - typically, you'll be accessing a VPN that someone else has already set up.

Third party clients and intranets

It's good to know what OpenVPN is, but chances are you're not going to need to use it directly; there are **two typical use cases** for interfacing with VPNs that you'll come across in your day to day.

1. **Personal VPNs**

If the first section of this post scared you and you're ready to upgrade your personal security, you can get started by purchasing a third-party VPN service. There are literally hundreds (it's cheap and easy to build one of these companies), and a lot of them are really sketchy. You can *theoretically* find a free one but it's kind of difficult, and at around $10/mo it's usually worth just paying up. There are 34281 articles on the web that break down your best options – personally, I use ExpressVPN and it's great. It works on my phone and computer, and is generally aesthetically pleasing (gasp!) and easy to use.

2. **Company VPNs**

Another context where you might need to deal with a VPN: at work. If you're working at a *really really* big company, you probably have an intranet that doesn't actually interface with public networks. But plenty of mid-late stage startups restrict access to internal tools (think: email, admin panels, data, etc.) to a VPN that you need to connect to. For example, my current employer has

important tools (managing subscriptions, our staging server, etc.) that need to stay secure, and I need to use the company VPN to get access to them.

For connecting to company VPNs (this also applies if you set up your own server), there are a bunch of free desktop apps that make it easier to connect and manage your traffic. I use Wireguard, which is pretty solid. You basically input the IP address of your VPN and some authentication credentials (username / password, SSH key, etc.) and you're good to go.

Terms and concepts covered

`VPN`

`Proxy server`

`RIR`

`ARIN`

---

2 Comments

Write a comment...

Lydia Cohen Feb 18, 2022

I am using PandaVPN on my computer and Android phone. Not bad.

♡ Reply Gift a subscription Collapse •••

Lindy Writes Lindy's Newsletter Jan 12, 2022

Hi Justin, I hire tech writers and am wondering if you would like to talk. Please find me through Linked In. Lindy Earl

♡ Reply Gift a subscription Collapse •••