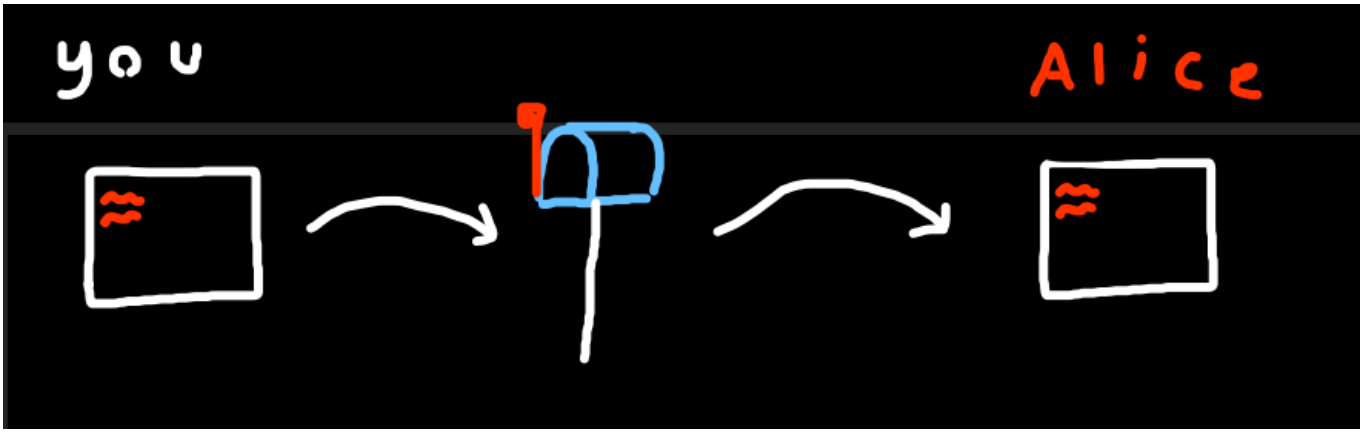
Why does my VPN not work on the school network?

TLDR: VPN traffic is filtered out by our network firewall.

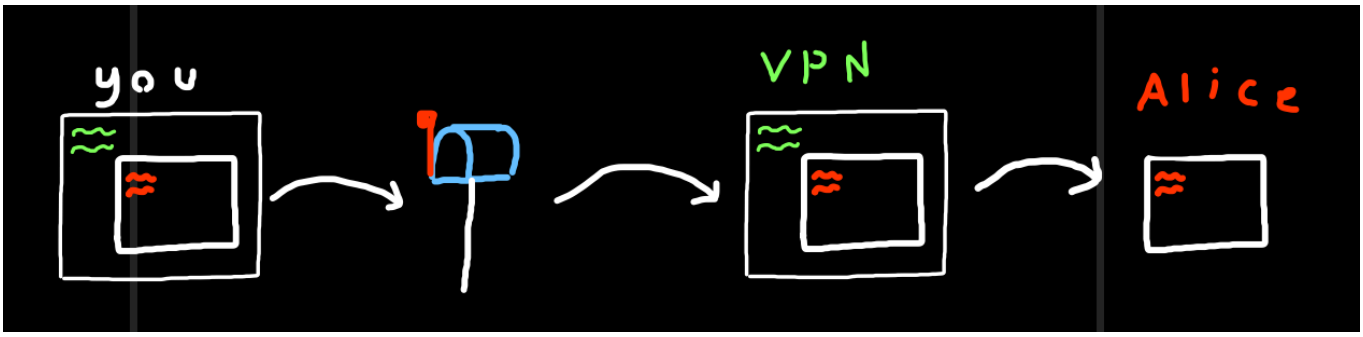
You are probably familiar with the word **proxy**. In the context of IP Networks, a proxy server is a server that forwards traffic from a client to another server, or in other words it is a computer that is a liaison between two other computers.

VPNs serve as a special type of proxy. One that encrypts and encapsulates traffic.

Imagine you are sending a letter to your friend Alice. First you would write your letter, then you would encapsulate that letter in an envelope and write your friends address on it, then you would send that letter to a post office which would look at that address and forward it to Alice.



In the case where you are using a VPN it works more like this: You write your letter, you encapsulated it in an envelope, write Alice's address, but then rather that send it straight to the post office, you put that envelope in a bigger envelope and write the VPN's address on it. When that letter arrives at the post office, they forward it to your VPN who opens that letter, reads Alice's address, and forwards the letter to her.



The key difference in this arrangement is that the post office only sees communication between you and your VPN. They don't even know that Alice was involved in this transaction.

Of course this process also works in reverse. If Alice wants to reply to you she can send a letter with the same method. The post office will know that Alice is communicating with someone AND that you are communicating with someone, but they don't know that you are communicating with each other or that what you are sending is a letter. The only thing they see is envelopes marked with your VPNs address.

There are other uses and considerations for VPNs other than this anonymity, but anonymity is the main use for consumers AND the main problem for us. This process poses many problems for a public school network, I will outline three.

1. Certain types of network traffic can pose security risks, for example, computers like the servers that run in the background of a network can be controlled remotely by network admins, as useful as this is, it also means we have to consider the risk that someone unauthorized could hijack this access. One of the things we do to mitigate this risk is only allow the kind of network traffic meant for remote access on certain ports. With VPN traffic however it is infeasible to know the true nature of the traffic involved, thus there is no way to filter out traffic coming or going to places it shouldn't be.
2. VPNs are often used by malicious actors to disguise their identity and avoid consequences. Although this isn't the only or even the best way of doing so, it is still best practice to mitigate network attacks.
3. As a public school we bear a heightened responsibility to ensure that our facilities are not used in ways that go against public values. Blocking traffic to illicit sites becomes not just a matter of preference, but one of liability. VPNs by their nature, make blocking that traffic nearly impossible.

TLDR: VPN traffic is filtered out by our network firewall.