02. Accessing Methods

- 01. VPN
- 02. Cloudflare Tunnels
- 03. Publicly Accessible

01. VPN

02. Cloudflare Tunnels

03. Publicly Accessible

Now, yes a VPN or using Cloudflare tunnels is the most secure option of protecting your applications. Especially, since your websites are not publicly accessible only if you are invited with a Wireguard configuration file. This is extremely secure and almost impossible to get hacked from. However, it also forces you and all your users to always have your VPN on when you use your phone or laptop or any device to connect to your apps. Maybe this might not be a big problem for you but if you have other users like your family and friends that are not tech savy it is another step they need to think about each time they want to access your application.

Now, even if they did it then you still have the latency problem. If my home server is in Amsterdam and I go on holidays in the USA and assume I convince some other friends there to use my server then each time they make a local call they will be routed through the Netherlands. This is of course not convenient if they just want to call rob next door.

Longer routes also introduce more potential points of congestion and packet loss. If packets don't arrive reliably or in the correct order, video quality degrades—you might see pixelation, freezing, or audio drops. VPN encryption can also consume slightly more bandwidth overhead.

Sure it is still possible and maybe you don't even measure a difference but it is something to think about. However, the main reason is forcing users to install another application on their phone, laptop or any device to connect to your apps. Also some public wifi's in public transport, airports or other places might not accept a standard Wireguard connection over a different port then 443.

My recommendation is to have the front ends available to the public but all the backends not. This means, any application or configuration dashboard does not need to be publicly available. Put HA dashboard, proxmox dashboard, docker vm dashboard, grafana dashboard, your router dashboard etcetera behind your VPN. Then have other apps such as Jellyfin and Ente publicly accessible for others to use.