3. VPN Server (WireGuard)

> We will use **LXC container** to save resources, however configure Wireguard through proxmox directly (some people use protainer or rancher), we can install an ubuntu server image and use it to save resources. We will use 1 core and 2GB Ram

Steps

1. Download Ubuntu Image Link (or just copy the download link)
2. Go to Datacenter > Node > (if you cannot see `local` only and/or just see `local-lvm` then
   a. Go to Datacenter > Storage > Select first and click edit > Select Container and Images in drop down, Check Enable button > Ok
   b. Now go to `local` that just appeared > CT Templates > Templates > Ubuntu-20.04-standard
3. Datacenter > Right Click on Node > Create CT > Add a Hostname (e.g Wireguard) > Template: the image > finish

> Proxmox allows LXC to be stored on local and VMs on local-lvm

WireGuard steps

We will use PiVPN, a vpn installer that supports wireguard and openvpn. Why we will use it? it saves time and hassle, and configures things rapidly.

The steps will be as follows

1. Go to Proxmox > Node > Wireguard (LXC) > Network > Edit > Create a static ip by Entering 192.168.1.100/24 and gateway as your router's gateway (We are using ..1.100 instead of 2.10 because we didnt configure the firewall yet. Hence the device should be in same subnet as gateway which in this case would be router)
2. Type this in Wireguard LXC Terminal `curl -L https://install.pivpn.io | bash`
3. Keep clicking next, and for port, I entered `4312` and then reboot the machine.
4. Now go to your router's "port forwarding" or "port mapping" option and enter the IP of the Wireguard LXC (which would be PiVPN's IP), and enter the port you chose.
5. Return to WireGuard terminal, and type `pivpn add` > it will then ask to choose an IP, just click enter (this ip is assigned to vpn client entering the network). > then choose a name for your client. Like for me, it will be Ameen-Laptop.
6. Type `cd /etc/wireguard/Ameen-Laptop.conf`
7. To copy the conf file to your client's laptop, type this in their terminal `scp` `root@192.168.1.100` `:/etc/wireguard/configs/Ameen-Laptop.conf`
8. Now download "Wireguard" from your AppStore / MS Store and upload the file.
9. Now upload the file

> The Public IP of the WireGuard LXC will change. So you need to setup a DNS that would prevent the public IP from changing.
>
> You can get one from DDNS.com or no-ip. To learn more how to do it, open "Creating DDNS" PDF File in "Additional Documentation" directory

> NOTE: Uncheck "Block untunneled traffic (kill-switch)". You can find this option when you upload the .conf file to WireGuard Windows app, and click Edit in button right.

Debugging

Notes

How does this work?

When a VPN Session is Initiated:

- **Client Connection:** The client uses the VPN configuration file, which contains an `Endpoint` that is either your public IP or your DDNS hostname with the port number (e.g., `myhome.ddns.net:4312`).
- **Routing:**The connection request goes to your router’s public interface. Because of your port forwarding rule, that traffic is forwarded to the WireGuard LXC container’s internal IP (192.168.1.100) on the specified port.
- **Result:**The VPN tunnel is established with the WireGuard server inside your home network. After the connection is up, your client traffic flows through the VPN tunnel.

```
graph TD
    A[VPN Client - Ameens PC] -->|Connects via DDNS/Public IP| B[Router]
    B -->|Port Forwarding UDP 4312| C[Proxmox Host]
    C -->|Traffic forwarded| D[WireGuard LXC - 192.168.1.100]
    D -->|VPN tunnel established| A
```

How can attacker hack?

- **If They Obtain a Config File:** If someone gets hold of a valid client configuration (for example, by compromising your device or intercepting an insecure transfer), they could potentially connect to your VPN.
- **Exploiting Vulnerabilities:**Like any network service, if there were a vulnerability in the VPN server software or in your overall network configuration, an attacker might attempt to exploit that. However, WireGuard’s design is intentionally simple and secure, making this a less likely scenario if you keep your software updated.
- **Brute Force or Other Attacks:**Because of the strong cryptography, brute forcing the keys is computationally unfeasible.