Create a pritunl vpn server

1. Create pair of ssh-keys
2. Add keys as a metadata
3. Create an instance for VPN
4. Reserve static IP for it in a network interface settings.
5. Login onto an instance
6. Enable HTTP and HTTPS traffic in firewall
7. Use script for installing vpn client on an instance
8. Go to https://vm-public-ip/setup skip SSL error and continue
9. Create user and password for an admin user in a control panel of vpn interface
10. Create an organization, and add user to it (use this pin (pass) for a user: 6214157507237678334670591556762)
11. Create server add it to organization and enable it.
12. Create a firewall rule to open a port in a vpn (check in a server settings which port needs to be opened), add it as a network tag to your instance
13. Download vpn configuration of your user and add to your openvpn client

Add a valid SSL certificate to your VPN server

1. Turn off your VPN server using the following command:

sudo systemctl stop pritunl

1. Install certbot

sudo apt update

sudo apt install certbot

1. Obtain certificate using the following command:

sudo certbot certonly --standalone -d vm-public-ip.sslip.io

1. Start the VPN server using the following command:  
   sudo systemctl start pritunl
2. Log in to the **Pritunl web interface**
3. Navigate to **settings and add to Let’s Encrypt Domain following address:**vm-public-ip.sslip.io
4. Automate Certificate Renewal

First test it using the following command: sudo certbot renew --dry-run

Add a cron job to renew the certificate and restart Pritunl using the following commands:  
crontab -e

0 3 \* \* \* certbot renew --quiet && systemctl restart pritunl

This crontab job renews the certificate every day at 3 AM and restarts pritunl vpn server.