OpenVPN Server Setup

This document provides a step-by-step tutorial for setting up an OpenVPN server and creating user profiles to connect Arduino devices.

Overview

OpenVPN is an open-source VPN protocol that allows for secure remote access to a network. By setting up an OpenVPN server, you can create a secure connection for your Arduino devices to communicate with your network.

Requirements

VPS running Ubuntu/CentOS/Red Hat

Putty (SSH client)

Filezilla or WinSCP (FTP client)

OpenVPN client (desktop/mobile)

Step 1: Getting Ready

Create a directory to store OpenVPN configurations:

mkdir OpenVPN

Download the OpenVPN installer script:

wget https://raw.githubusercontent.com/angristan/openvpn-install/master/openvpn-install.sh

Make the script executable:

chmod +x openvpn-install.sh

Run the script with sudo permissions:

sudo ./openvpn-install.sh

Step 2: Setup Server

Keep the default IP and hit "Enter".

Disable IPv6 support (NAT) by entering "n".

Choose a port for OpenVPN to listen to.

Select the protocol for OpenVPN (UDP or TCP).

Choose DNS resolvers for the VPN.

Disable compression by entering "n".

Customize encryption settings if needed.

Choose cipher for the data channel.

Choose certificate type.

Choose curve for the certificate's key.

Choose cipher for the control channel.

Choose Diffie-Hellman key.

Choose curve for the ECDH key.

Choose digest algorithm for HMAC.

Add an additional layer of security for the control channel.

Press any key to continue and wait for the process to finish.

Step 3: Create User

Enter a client name (e.g., vpn-user-1).

Protect the configuration file with a password.

Step 4: Download .ovpn

Connect to the server using an FTP client and download the username.ovpn file.

or use SCP command to copy .Ovpn file form remote server and download it on local system on given path

like this:

scp root@35.208.45.157:/home/muhammadhassanb122/Hassan.ovpn /home/hassan/Projects/OPENVPN/

for this you need to:
- install ssh server in remote server. then enable it.
- set root password
- permit root under **ssh_config file** also allow authentication by setting **yes** in this file. then **reload/restart** the ssh service

Step 5: Setup More Clients

Install the OpenVPN client on your device and import the .ovpn profile. Connect to the server using the client app.

Adding More Users

Run the script again with sudo permissions.

Select "Add a new user".

Enter a new username and set no password.

Download the .ovpn file for the new user.

you need to also allow the default 1194 port for OPENVPN in remote OPENVPN server(like vm-instance)

Client Session

To install the OpenVPN client on your local system, follow these steps:

sudo apt update

sudo apt install openvpn

Remove old OpenVPN entry:

sudo rm /etc/apt/sources.list.d/openvpn3.list

sudo apt update

To connect to the remote VPN server:

sudo cp Hassan.ovpn /etc/openvpn/   # Move client Hassan.ovpn file to etc if not available in etc.

sudo openvpn Hassan.ovpn

Verify VPN client connectivity on the remote VPN server:

sudo cat /var/log/openvpn-status.log

sudo netstat -tunap | grep openvpn

By following these steps, you can set up an OpenVPN server and connect Arduino devices securely to your network.

More Clarification

For additional clarification on specific steps, you can refer to the following link: [OpenVPN Server Setup - Step 3: Create User](#)

This link provides detailed instructions and explanations for creating user profiles on the OpenVPN server. It covers the process of adding new users, setting up passwords for configuration files, and completing the installation process.

By following the instructions provided in the linked resource, you can gain a better understanding of the user creation process and ensure that user profiles are set up correctly to connect to the OpenVPN server.

Feel free to refer to the [OpenVPN Server Setup](#) repository on GitHub for more information and clarification on various steps of the OpenVPN server setup process.