Rogelio Perez-Montero
Axel Sandoval-Pineda

Raspberry Pi Router: Wi-Fi & VPN

Project Overview

The objective is to connect the Raspberry Pi to any public Wi-Fi network and enable it to broadcast its own Wi-Fi signal, effectively functioning as a router. Additionally, the project incorporates an added layer of security by implementing a VPN (Virtual Private Network) on the Raspberry Pi. This setup not only extends the Wi-Fi coverage but also ensures secure internet connectivity for devices connected to the Raspberry Pi's network.

Requirements

- Raspberry Pi (4B)
- Power Supply
- Micro SD card
- USB Micro SD card reader: built into our pi
- Ethernet Cable: internet provider
- Monitor
- USB wifi adaptors built into our raspberry
- wifi broadcaster

Software Requirements

- RaspAP
- WireGuard
- Raspberry Pi Lite operating system

Key Steps

1. Configure Raspberry Pi 4B with Raspberry Lite Operating System
    a. Using the official Raspberry Pi imager, Raspberry Lite OS was downloaded and installed on a micro SD card. The micro SD card needs to be inserted into the Raspberry Pi 4 B.
2. Installing and configuring RaspAP software
    a. After starting up the Raspberry Pi, an internet connection must be made to download the RaspAP software
    b. Invoke the installer with option flags for installation using,
        i. curl -sL https://install.raspap.com | bash -s -- --help
    c. Install the software by answering the options for additional services
        i. Only type “Yes” to WireGuard, HostSpot, and Ad Blocking
    d. Reboot to save and start services
3. Setting up GUI
    a. Rebooting will create an accessible user interface running on the local network.
    b. Access the interface by typing the IP address of the Raspberry Pi into the web address or by going to “raspap.local”
    c. By default, the username should be admin, the password should be “magic”
    d. The interface should have a variety of options that will be used to provide the services needed

Rogelio Perez-Montero
Axel Sandoval-Pineda

4. Configuring the Hotspot service
    a. The “interface” option should be changed to the interface that will be used to output the internet to other devices.
    b. If there is an external Wifi adapter, this option can be picked to output the wifi signal
    c. However, we used the built-in interface (Wlan0) to project the wifi signal to other devices
    d. Under “Security” the “PSK” option should be changed to the password needed to access the the hotspot/wifi for other devices
    e. The country code should be modified to the country the Raspberry Pi is being configured in, to give accurate information
    f. The device must be rebooted to save the settings
5. Configuring WiFi Client
    a. The WiFi Client is the internet that will be used to create the Hotspot/Access Point for other devices
    b. We redistribute the internet provided to other devices with an encrypted layer and VPN.
    c. Press “Rescan” to scan the networks around the Raspberry Pi, and connect to the desired connection
    d. Once the connection is made, reboot the Raspberry Pi. It should reboot with the Hotspot service on. Other devices should be able to connect to it by entering the password set by the administrator
6. Configuring WireGuard
    a. Under the WireGuard option, there should be an option to manually configure the VPN
    b. After pressing, the manual configuration, there should be a way to generate a random key
    c. This random key will be imputed in the VPN configuration file in the WireGuard directory
    d. The Raspberry Pi must be rebooted to save the configuration
    e. From the boot, there the service should be enabled along with the hotspot and WiFi Client connection

Conclusion

The objective of the project is to provide a safe way of using public WiFi, especially while traveling. By taking the internet of the space, we can redirect it to other devices with double encryption. The Hostpot provides encryption through the password set by the administrator. The services allow the administrator to monitor devices connected to the hotspot and provide protective services. The VPN provides the second protective layer by filtering the internet packets more. The packets are less vulnerable to people on the regular public network. This setup not only extends the Wi-Fi coverage but also ensures secure internet connectivity for devices connected to the Raspberry Pi's network.