

CIT 490

RASPBERRY PI

VPN PROJECT

By: Michael Short

Mentored By: Blaine Robertson

Brigham Young University Idaho

September – December 2021

TABLE OF CONTENTS

Table of Contents	1
Introduction	2
Preparation	2
Connecting	3
Main Menu	4
Network Setup	5
VPN Server Setup	6
VPN Clients Setup	8
Connecting Clients to VPN	10
Project Contact Information	11

Introduction

This project was created to solve a problem of needing to find a simple, modern, and secure way to connect client computers to a private internal network over the public internet. A device was to be created using a Raspberry Pi computer and ARM based Linux distribution. The device to be created needed to have two network interfaces, one for an inside facing and one outside facing connection. Users establish a connection to the VPN device and then are able to access network resources on the internal network as if the client computer was physically on that network, even though it could be anywhere in the world.

Preparation

Download the Raspberry Pi VPN Project Disk Image from:

<https://alcatraz.fawkesengineering.com/mike/privado/WGVPN.img.xz>

Uncompress the image archive using 7-Zip on windows, xz on OSX or Linux, or other decompression software that can uncompress the xz format.

The result will be a .img file containing a clean and bootable fully installed Raspberry Pi VPN Project image ready for use. The img file needs to be written to a 64GB Raspberry Pi compatible MicroSD card.

The process of writing the image to the MicroSD can be done under Windows using software such as Rufus and under OSX or Linux using the dd command.

Rufus has a GUI that will allow selection of the destination and the image to be written. Usage of Rufus will not be full explained here.

A Simple use of dd under Linux may look like this when the microSD card is detected at /dev/sdf:

```
dd if=WGVPN.img of=/dev/sdf bs=4M
```

This will write the file WGVPN.img to the disk at /dev/sdf in blocks of 4 MB at a time.

WARNING: Please use caution or request assistance from another individual with more experience if uncertain about performing this task. The results of entering an incorrect destination or selecting the incorrect drive to write the image to can cause permanent data loss. By attempting to create a disk image, you acknowledges and accept all responsibilities associated with using disk imaging utilities.

The USB Adapter used in this project is available on Amazon and was ordered using the following link:

<https://smile.amazon.com/gp/product/B0874TYG5X>

The item description reads: USB 3.0 to Ethernet Adapter, Driver Free 10/100/1000 Mbps Network RJ45 LAN Wired Gigabit Ethernet Adapter for Windows 10, 8.1, 7, XP, Linux, Mac OS, Chrome OS

Insert the imaged MicroSD into the Raspberry Pi, connect USB Ethernet Adapter, connect network cables, and connect power. If your power adapter has an on/off switch or button, toggle it to apply power to the Raspberry Pi. The Raspberry Pi will boot and have the network configured to the preset values listening on port 80 for web requests on the external USB connected Ethernet adapter. The following section will go over the initial connection process.

Connecting

Upon initial powering up of a freshly imaged install of this VPN project, the system will be configured to use DHCP on the onboard network interface and be set manually to use 192.168.200.1 on the external USB 3.0 Ethernet adapter.

Configuration can be done easily with a laptop that has an Ethernet port by connecting an Ethernet cable between the laptop Ethernet adapter and the external USB Ethernet adapter on the Raspberry Pi. In some cases it may be necessary to use a crossover Ethernet cable or place a network switch between the two Ethernet adapters connected via regular Ethernet patch cables to the switch. This is due to the nature of some devices not having auto switching Ethernet ports. Most modern systems will be able to simply place a cable between a laptop/computer and the Raspberry Pi external USB network adapter and be able to communicate.

The Laptop/Computer should be configured manually using the below IPv4 settings:

IP: 192.168.200.2

Subnet: 255.255.255.0

Gateway: 192.168.200.1

DNS can be left empty, or if required, set to 192.168.200.1.

If there is an option to verify before applying uncheck and apply the settings.

The computer should now be able to connect to the VPN Web based configuration tool by using a web browser and visiting: <http://192.168.200.1>

The first time a connection is made the user will be prompted to authenticate.

The default credentials are:

- Login: **admin**
- Password: **password**

Once successfully authenticated the user will be at the main menu.

Main Menu

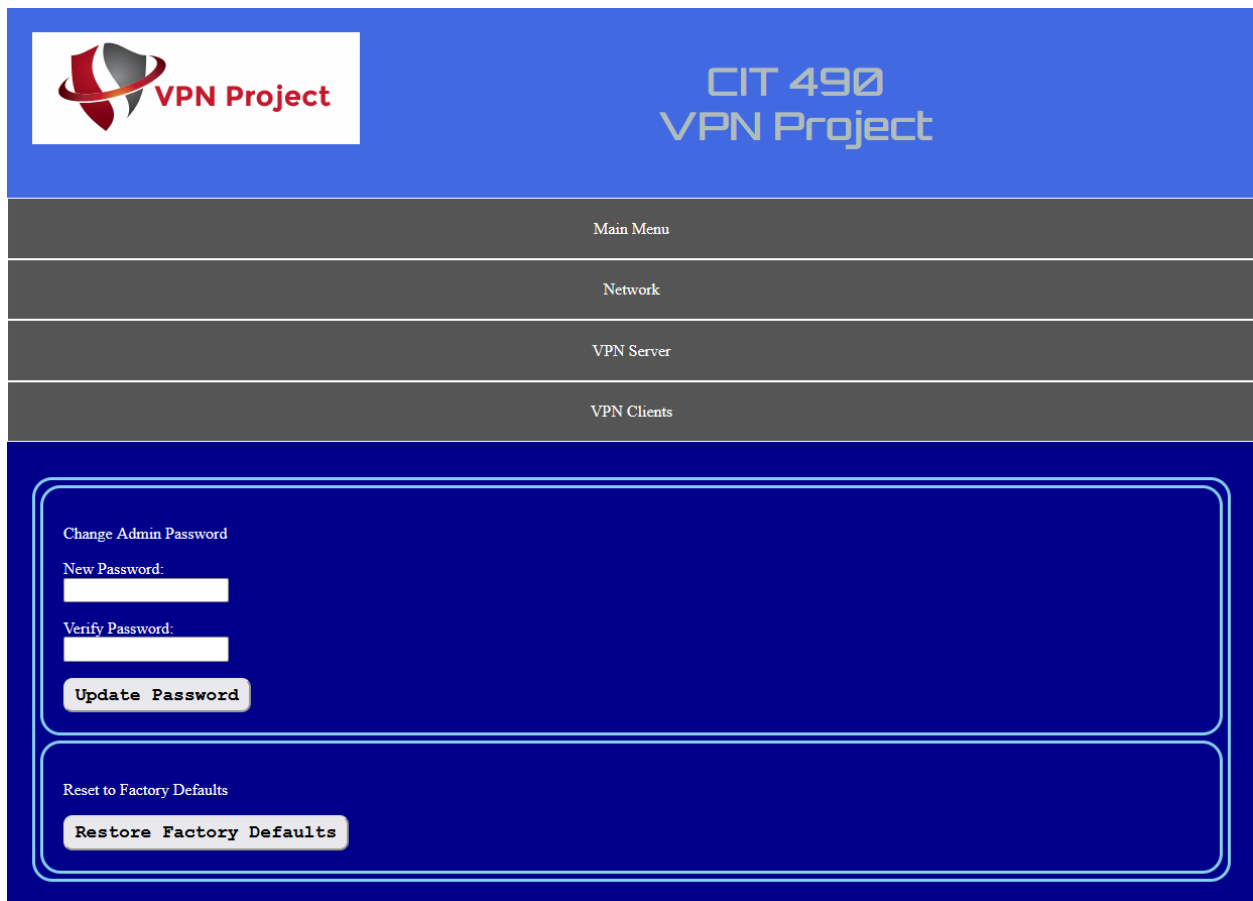
The Main Menu offers two options.

Change Admin Password:

By entering a new admin password, verifying it, and pressing the Update Password button, the admin password for the web configuration will be immediately updated. Upon any new attempt to open a page on the VPN device web configuration, the user will be prompted to enter the new password.

Restore to Factory Defaults:

This will cause the device to reset all settings and reboot into a factory state. This will cause new Private/Public Keys to be generated for the device, all network settings will revert to defaults, and all VPN Server/Client configurations will be removed.



The screenshot displays the 'Main Menu' of the VPN Project web configuration interface. The header is blue with the 'VPN Project' logo on the left and 'CIT 490 VPN Project' on the right. Below the header is a dark grey navigation bar with four menu items: 'Main Menu', 'Network', 'VPN Server', and 'VPN Clients'. The main content area has a dark blue background and contains two sections. The first section, titled 'Change Admin Password', includes input fields for 'New Password:' and 'Verify Password:', and an 'Update Password' button. The second section, titled 'Reset to Factory Defaults', includes a 'Restore Factory Defaults' button.

Network Setup

IMPORTANT NOTICE: In order for the VPN Device to be able to receive incoming data, it may be necessary to create a port forwarding rule on your router to allow data coming to the VPN data port to be forwarded from the outside facing internet connection to the VPN device on the inside.

It is recommended not to have the outside facing Ethernet Adapter on the VPN device connected directly to the internet as this may pose a security risk. Although it may pose a security risk, it is still a valid configuration. No penetration testing was done with the VPN device connected directly to the internet on the outward facing Ethernet adapter other than ensuring that the web server did not server pages on that interface. Masking its presence using an NAT enabled router and creating a port forwarding of the UDP data over the configured VPN port appears to be a much safer practice. Users deciding to expose the device directly to the internet acknowledge that this configuration was not thoroughly tested during development and doing so may or may not pose a higher security risk.

The Network Setup Page allows the configuration of the Network settings on the VPN Device. Below is an explanation of the available configuration options.

Outbound Traffic Routing Priority: **(Experimental)**

This option allows the selection of the network device that should have priority for routing outbound data packets.

NOTE: This option is currently experimental and has not been widely tested. It is known to function properly and without issue when set to External Network. It has not been extensively tested with the Internal Network option. Some routing propriety bugs were fixed nearing the end of the project and this feature was not thoroughly tested after the bug fixes. Leaving this on External may be the safest for now as this has been verified as working properly.

Internal / External Facing Network Configuration:

The Network configuration options consist of the same fields for the Internal and External facing adapters.

Configuration Type:

- **DHCP:**
 - Obtain network configuration using DHCP and allow the local DHCP server to assign our network settings.
- **Manual:**
 - For manual IP configuration the following data must be provided:
 - IP Address
 - Subnet Mask
 - Gateway
 - Name Servers (comma separates list)

APPLY SETTINGS: submits the specified settings to be validated and applied as the active network configuration if the settings pass all validity checks.

NOTE: the VPN Device will restart after new network settings are configured, it may take 15 to 20 seconds before the device is available using the new network settings.

The screenshot displays a configuration interface with a dark blue background and white text. It is divided into three main sections, each with a title and a configuration type selector.

Outbound Traffic Routing Priority
Use Gateway from:
☒ Internal Network
☐ External Network

Internal Facing Network Configuration
Configuration Type:
☒ DHCP
☐ Manual
IP Address: 207.110.16.77
Subnet Mask: 255.255.255.0
Gateway:
Name Server(s): 8.8.8.8,1.1.1.1

External Facing Network Configuration
Configuration Type:
☒ DHCP
☐ Manual
IP Address: 207.110.16.78
Subnet Mask: 255.255.255.0
Gateway: 207.110.16.1
Name Server(s): 8.8.8.8

At the bottom of the interface is a button labeled "Apply Settings".

VPN Server Setup

The VPN Server Page allows the configuration of the WireGuard VPN. Below is an explanation of the different configuration fields.

External Facing Name or IP Address:

This is the Outside DNS name or IP Address that will be used to establish a connection to the VPN.

VPN Port Number:

This is the VPN port that will be listening for incoming connections.

NOTE: Please not that it is important to create a port forwarding rule if the VPN device is behind a router or firewall appliance that is using NAT or filtering/blocking traffic.

Internal Network DNS Server:

This is the DNS server that should be used by clients that are sending all IPV4 traffic through the VPN. This will ensure DNS queries are answered by the internal network where all traffic is being directed.

WireGuard Network IP:

This CIDR value describes two pieces of information, the IP address for the VPN Device inside of the WireGuard Network, and the scope of the network.

Server Private Key:

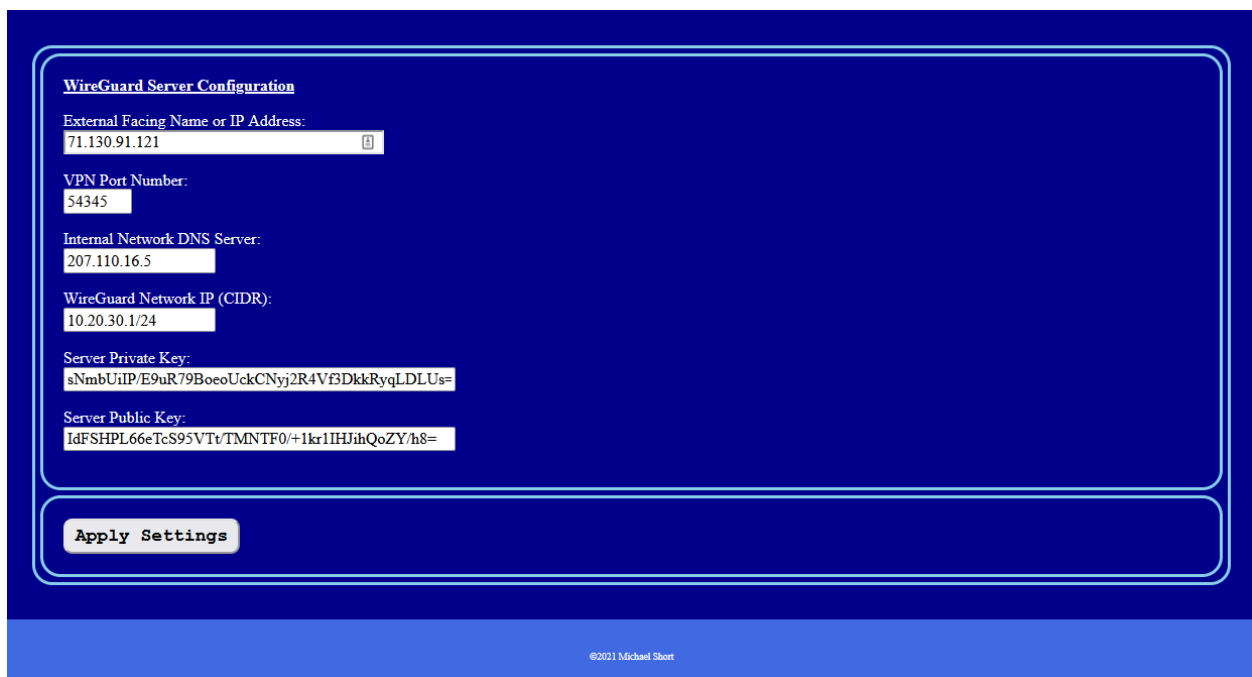
This is the Private Key used by the VPN Device, it is auto generated at first boot, or when no private/public keys are present on the system at boot time.

Server Public Key:

This is the Public Key used by all VPN Clients to encrypt data being sent to the VPN Device. The values is generated automatically from the Private Key.

APPLY SETTINGS:

Button used to apply the specified settings and cause the device to bring down and up the VPN interface allowing the new settings to become the active configuration.

A screenshot of a terminal window with a dark blue background and light blue text. The title is "WireGuard Server Configuration". It contains several input fields for configuration: "External Facing Name or IP Address:" with the value "71.130.91.121"; "VPN Port Number:" with the value "54345"; "Internal Network DNS Server:" with the value "207.110.16.5"; "WireGuard Network IP (CIDR):" with the value "10.20.30.1/24"; "Server Private Key:" with a long alphanumeric string; and "Server Public Key:" with another long alphanumeric string. At the bottom of the configuration area is a button labeled "Apply Settings". The footer of the terminal shows "©2021 Michael Short".

WireGuard Server Configuration

External Facing Name or IP Address:
71.130.91.121

VPN Port Number:
54345

Internal Network DNS Server:
207.110.16.5

WireGuard Network IP (CIDR):
10.20.30.1/24

Server Private Key:
sNmBUiIP/E9uR79BoeoUckCNyj2R4Vf3DkkRyqLDLU=

Server Public Key:
IdFSHPL66eTcS95VTt/TMNTF0/+1kr1IHJihQoZY/h8=

Apply Settings

©2021 Michael Short

VPN Clients Setup

The VPN Clients Page allows the addition of new VPN client configurations. Below is an explanation of the different configuration fields.

WireGuard Client Network IP (CIDR):

This is the IP address that will be used on the WireGuard VPN Network. If my Wireguard VPN Network is 10.10.30.0/24 and I wish to give my client the address of 10.20.30.25, then the correct value for this field would be: 10.20.30.25/32. This is denoting the exact client IP in CIDR format.

Network(s) Client will Access through VPN:

These are the Networks that will be accessed on the other end of the VPN by the client, or in other words, this is the list of networks that the client will channel traffic for through the VPN. This should consist of the WireGuard VPN Network as well as any other network address space on the inside that the client will be accessing through the VPN. If my VPN network is 10.20.30.0/24 and my internal private network on the inside facing Ethernet adapter is configured as 192.168.1.0/24, then I would specify in this field the following: 10.20.30.0/24, 192.168.1.0/24. When multiple networks are listed, they should be separated by a comma between entries.

Client Private Key:

Client private key used in the client configuration, auto generated each time the VPN Client configuration page is loaded

Client Public Key:

Client Public Key used by server configuration to encrypt packets destined for client, auto generated from private key each time page loads.

Persistent Keep Alive:

This value represents the number of seconds the client should perform a handshake to keep the VPN connection open. This option is helpful when a client is behind a device using NAT. The keep alive will ensure that the NAT enabled router at the client location does not close the VPN connection.

Add Client:

Button to add the client described in the WireGuard Client Configuration section to the system. If the values are valid, then the client configuration and corresponding client configuration download will be created, otherwise an error message will explain what values were invalid.

Client Info Section


Public Key and VPN Network IP are listed to help identify the client that we desire to delete or download the configuration to configure a client system to connect to the VPN.

DOWNLOAD CLIENT CONFIGURATION link:

This link is for downloading the .zip file containing the client configuration. By downloading the configuration file, the client configuration will be as easy as clicking a button to add tunnels and choosing the file offered by the download link. Tunnels will be imported into the client and need no further configuration on the client side.

Delete Client:

Button that will remove the corresponding client configuration from the device.

WireGuard Client Configuration
WireGuard Client Network IP (CIDR):
 
Network(s) Client will Access through VPN:

Client Private Key:

Client Public Key:

Persistent Keep Alive (Seconds):

Add Client

Client Info
Public Key: SkS1u0SblEBSIR0o+knO/WsSHDgWiS3mSD1NJSYAOC0=
VPN Network IP: 10.20.30.5/32
[DOWNLOAD CLIENT CONFIGURATION](#)
Delete Client

Client Info
Public Key: gMiqdsfI9NPL11sj8PGjKaEMAyH61shDv8iKZfvWIS4=
VPN Network IP: 10.20.30.10/32
[DOWNLOAD CLIENT CONFIGURATION](#)
Delete Client

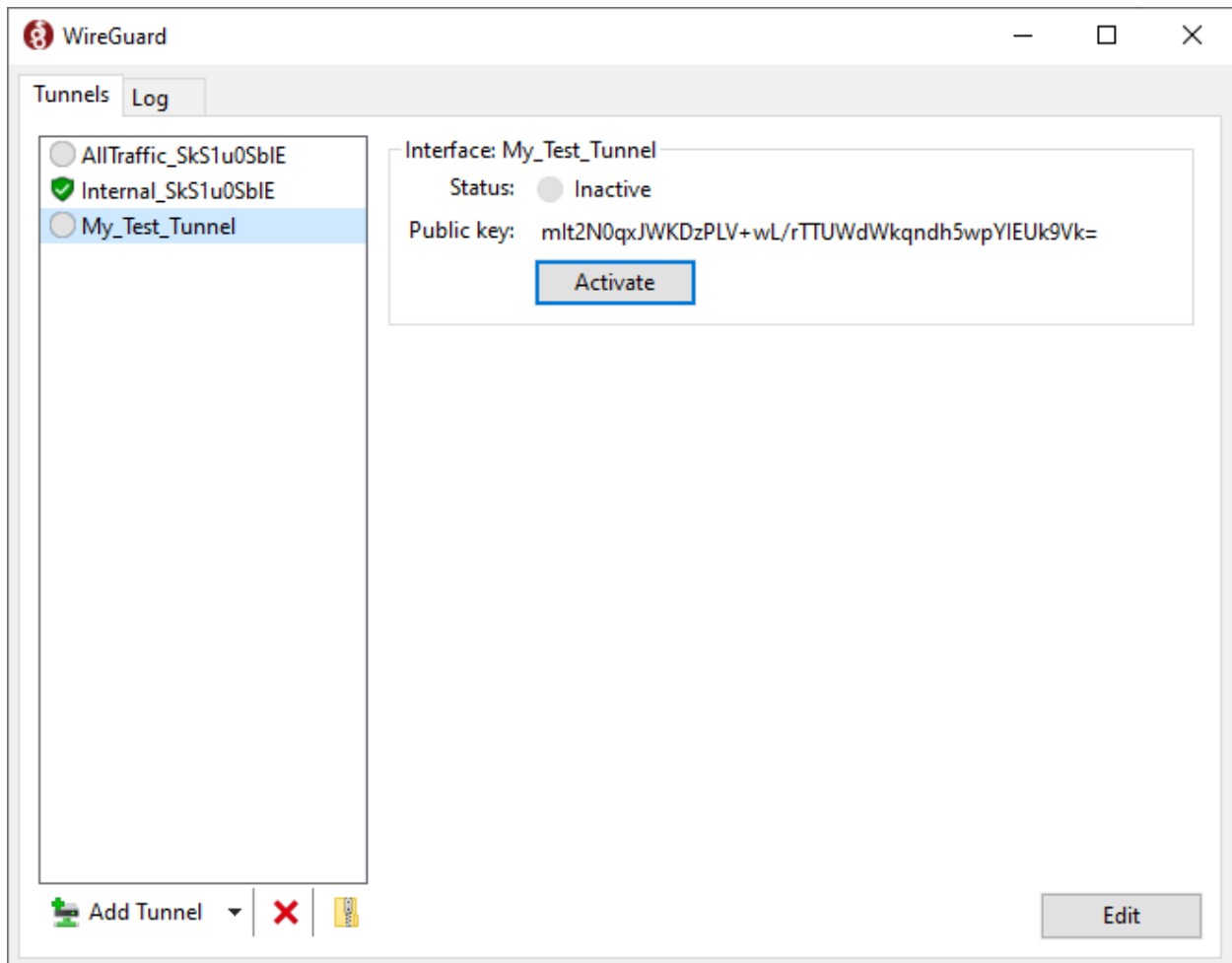
Connecting Clients to VPN

Install the WireGuard Client for Your Operating System. Available here:

<https://www.wireguard.com/install/>

Open VPN Clients web page in browser and download the corresponding configuration file for the client.

Open the WireGuard VPN Client UI.



Select the Add Tunnel Option, then Import Tunnels from file, then select the .zip file that was downloaded containing the client configurations through the web browser. The configurations should now appear in the list of Tunnels. There should be 2 new tunnel configurations, one that allows normal internet access, but sends traffic destined for the networks in the VPN client configuration through the VPN. The other Tunnel configuration is to send all internet traffic through the VPN. The connection names will be prefixed with AllTraffic_ or Internal_ to distinguish which configuration it represents.

Select the desired tunnel and activate the connection. This should establish the VPN tunnel and allow communication. The data sent and received is displayed in the VPN client.

Project Contact Information

For questions, comments, or inquiries regarding this project, please contact:

Michael Short

mike.short@fawkesengineering.com