

Assignment – ICT171

35577001

Kyle Mckenzie

DNS name: <http://www.kylemurdochproject.com/>

IP address(13.210.1.190): <http://13.210.1.190/>

This entire process was created on the AWS EC2 free tier. Once signed in and on the main page of instances, complete the following steps.

Server set up:

Create and launch a new instance, this is what the entire assignment will run on:

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents Quick Start

▼ Summary

Number of instances [Info](#)

Software Image (AMI)
Amazon Linux 2023 AMI 2023.7.2...[read more](#)
ami-07b7cae50f732535f

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

[Cancel](#) [Launch Instance](#)

[Preview code](#)

Now, set the OS to Ubuntu, as it will be more beneficial when setting up the VPN later

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents Quick Start

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-06c19207c1ab181f0 (64-bit (x86)) / ami-017b8eca16b194f27 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Set instance type to t3.micro, this is still within the free tier

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

t3.micro

Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand Ubuntu Pro base pricing: 0.0167 USD per Hour
On-Demand RHEL base pricing: 0.042 USD per Hour
On-Demand Windows base pricing: 0.0224 USD per Hour
On-Demand SUSE base pricing: 0.0132 USD per Hour
On-Demand Linux base pricing: 0.0132 USD per Hour

☐ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

Create a new key pair, this is how we will access the back end later

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Select



[Create new key pair](#)

Create key pair



Key pair name

Key pairs allow you to connect to your instance securely.

Enter key pair name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type



RSA

RSA encrypted private and public key pair



ED25519

ED25519 encrypted private and public key pair

Private key file format



.pem

For use with OpenSSH



.ppk

For use with PuTTY

[Cancel](#)

[Create key pair](#)

Create a security group and change the settings to allow http/https

Firewall (security groups) [Info](#)


A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called **'launch-wizard-3'** with the following rules:

- ☒ Allow SSH traffic from Anywhere
0.0.0.0/0
Helps you connect to your instance
- ☒ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server
- ☒ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.



Launch the instance

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64...[read more](#)
ami-06c19207c1ab181f0

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

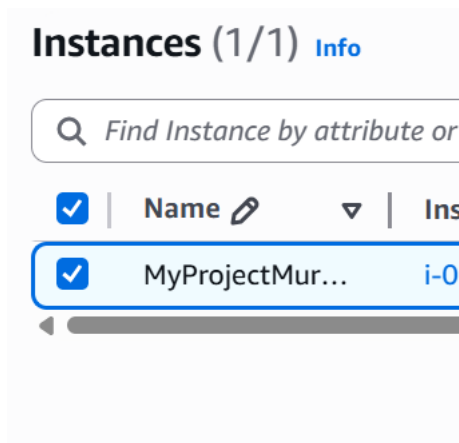
Storage (volumes)

[Cancel](#)

[Launch instance](#)

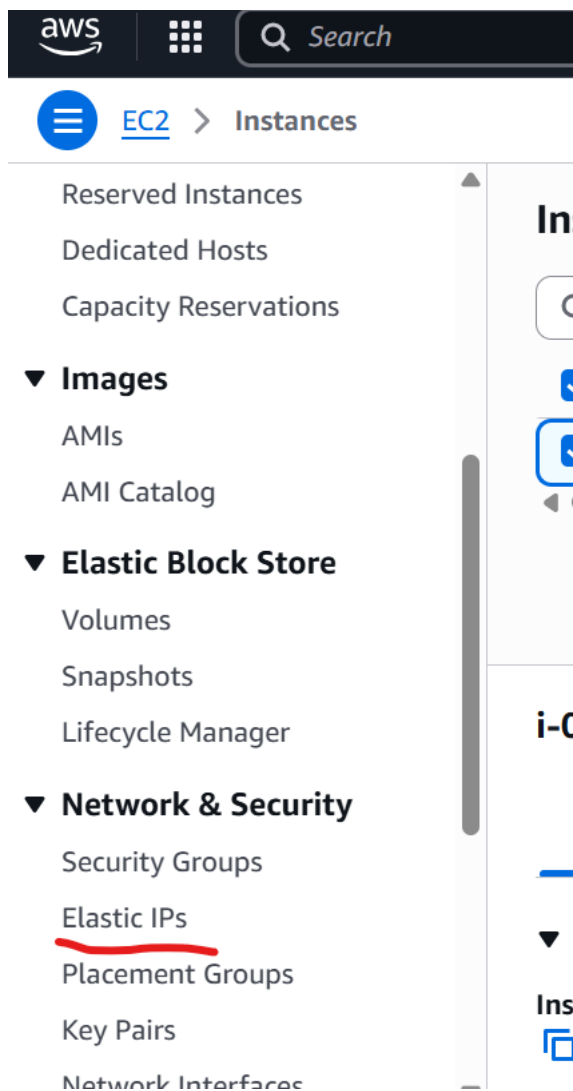
 [Preview code](#)

Name the instance (optional)



Assign it an Elastic IP:

Scroll down the menu bar and open “Elastic IP”; this is where we can allocate an Elastic IP to the instance we just launched.



Click on “Allocate Elastic IP address”, the orange button

Elastic IP addresses (1) [Info](#)

Find elastic IP addresses by attribute or tag

☐

Name

▼

Allocated IPv4 addr...

▼

Type

▼

Allocation ID

▼

Re...

☐

my project ip

[13.210.1.190](#)

Public IP

eipalloc-0bc3aa0abc0f36698

–

◀

▶

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Public IPv4 address pool

☒ Amazon's pool of IPv4 addresses

☐ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#) [↗](#)

☐ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#) [↗](#)

☐ Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group [Info](#)

Q ap-southeast-2

✕

Scroll down and click “Allocate”

Cancel

Allocate

If there is more than 1 instance, click on the “associate IP” to associate it with the wanted instance, and then click the desired instance to associate it to the correct one.

Actions ▲

Allocate Elastic IP add

View details

>

Release Elastic IP addresses

▼

Associate Elastic IP address

8

Disassociate Elastic IP address

Update reverse DNS

Enable transfers

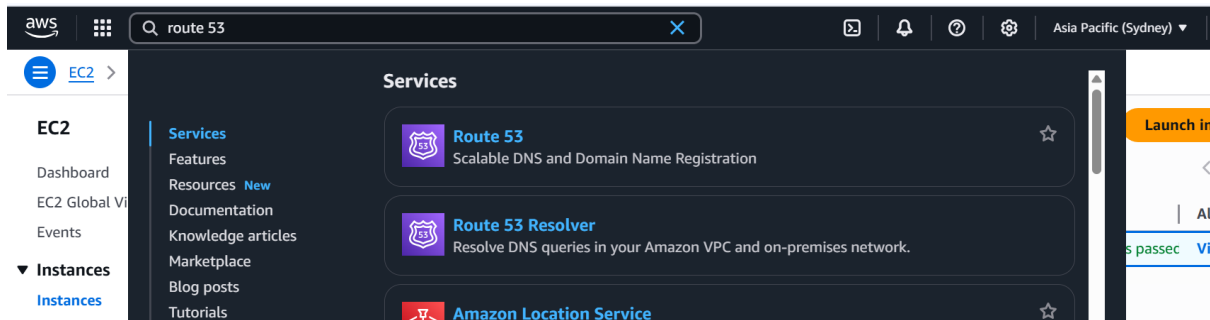
Disable transfers

Accept transfers

⚙

Open Route 53:

Type in the top search bar “Route 53”, then right-click it to open the link in another tab, this is where the DNS Name can be sorted.



Route 53 Dashboard [Info](#)

DNS management

1
Hosted zone

Traffic management

A visual tool that lets you easily create policies for multiple endpoints in complex configurations.

[Create policy](#)

Availability monitoring

Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.

[Create health check](#)

Domain registration

1
Domain

Register and purchase a DNS name (kylemurdochproject.com)

Registered domains Info				Download billing report	Transfer in	Register domains
<input type="text" value="Search domains by name"/>				1		
Domain name	Expiration date	Auto-renew	Transfer lock			
kylemurdochproject.com	June 03, 2026	Off	Off			

Then go to DNS management – hosted zones

Hosted zones (1) View details Edit Delete Create hosted zone						
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.						
<input type="text" value="Filter records by property or value"/>						
	Hosted zone name	Type	Created by	Record co...	Description	Hosted z...
<input type="radio"/>	kylemurdochproject.com	Public	Route 53	3	HostedZone...	Z0356750...

Create a hosted zone, then configure by entering the purchased and registered DNS name in the domain name prompt, leave all the other setting as is and confirm it

Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name [Info](#)
This is the name of the domain that you want to route traffic for.

Valid characters: a-z, 0-9, ! " # \$ % & ' () * + , - / : ; < = > ? @ [\] ^ _ ` { | } . ~

Description - optional [Info](#)
This value lets you distinguish hosted zones that have the same name.

The description can have up to 256 characters. 0/256

Type [Info](#)
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

☒ **Public hosted zone**
A public hosted zone determines how traffic is routed on the internet.

☐ **Private hosted zone**
A private hosted zone determines how traffic is routed within an Amazon VPC.

Create it

[Cancel](#) [Create hosted zone](#)

Add a record, which tells the internet where to go when someone enters your domain name, linking it to the IP address. To do this, press on the name of our instance in the hosted zones, it will then show the prompt to add records

► Hosted zone details [Edit hosted zone](#)

[Records \(3\)](#) | DNSSEC signing | Hosted zone tags (0)

Records (3) [Info](#) [Refresh](#) [Delete record](#) [Import zone file](#) [Create record](#)

Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)

[Type](#) ▼ [Routing p...](#) ▼ [Alias](#) ▼ < 1 > [Settings](#)

<input type="checkbox"/>	Record ... ▼	Type ▼	Routin... ▼	Differ... ▼	Alias ▼	Value/Route traffic to ▼	TTL (s...
<input type="checkbox"/>	kylemurd...	NS	Simple	-	No	ns-1825.awsdns-36.co.uk. ns-1079.awsdns-06.org. ns-492.awsdns-61.com. ns-807.awsdns-36.net.	172800
<input type="checkbox"/>	kylemurd...	SOA	Simple	-	No	ns-1825.awsdns-36.co.uk. a...	900
<input type="checkbox"/>	www.kyle...	A	Simple	-	No	13.210.1.190	300

Add the elastic IP into the value section of the record description

Quick create recordSwitch to wizard

▼ Record 1

Record name [Info](#)

kylemurdochproject.com

Keep blank to create a record for the root domain.

Record type [Info](#)

A – Routes traffic to an IPv4 address and some AWS resources

☐ Alias

Value [Info](#)

Enter multiple values on separate lines.

TTL (seconds) [Info](#)

1m 1h 1d

Recommended values: 60 to 172800 (two days)

Routing policy [Info](#)

Simple routing

Security, firewall settings and open ports:

Go back to ec2 instances dashboard

Instances (1) Info		Last updated 1 minute ago	Refresh	Connect	Instance state ▼	Actions ▼	Launch instances ▼
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>		All states ▼		< 1 > Settings			
<input type="checkbox"/>	Name 🔗 ▼	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	
<input type="checkbox"/>	MyProjectMur...	i-017c13913ad79205d	Running 🔍 🔍	t3.micro	3/3 checks passed	View alarms +	

Click on the instance ID, which will take you to the instance summary, - scroll down

Instance summary for i-017c13913ad79205d (MyProjectMurdoch) Info		
<div>Refresh Connect Instance state ▼ Actions ▼</div> <div>Updated less than a minute ago</div>		
Instance ID i-017c13913ad79205d	Public IPv4 address 13.210.1.190 open address	Private IPv4 addresses 172.31.47.27
IPv6 address –	Instance state Running	Public DNS ec2-13-210-1-190.ap-southeast-2.compute.amazonaws.com open address
Hostname type IP name: ip-172-31-47-27.ap-southeast-2.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-47-27.ap-southeast-2.compute.internal	Elastic IP addresses 13.210.1.190 (my project ip) [Public IP]
Answer private resource DNS name IPv4 (A)	Instance type t3.micro	AWS Compute Optimizer findings
Auto-assigned IP address	VPC ID	

Once at this point in the instance summary...

Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags

▼ Instance details Info

AMI ID

ami-0f5d1713c9af4fe30

AMI name

ubuntu/images/hvm-ssd-amzn-2017.04/ubuntu-18.04-lts-amzn-hvm-ssd-g2

Monitoring disabled

Allowed image

Platform details

Linux/UNIX

Termination protection


Disabled

Click on “security”


Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags

▼ Security details

IAM Role
—

Owner ID
 134763639657

Launch time
Tue Jun 03 2025 17:05:11 GMT+0800
(Australian Western Standard Time)

Security groups


sg-0b2a90e4a8be5900d (launch-wizard-2)

Scroll down to “inbound rules” and then select the security group link

Details

Status and alarms

Monitoring

Security

Networking

Storage


Iags

▼ Security details

IAM Role

–


Owner ID

 134763639657


Launch time

Tue Jun 03 2025 17:05:11 GMT+0800
(Australian Western Standard Time)

Security groups


sg-0b2a90e4a8be5900d (launch-wizard-2)

▼ Inbound rules

 Filter rules

<

This is where you need to create a new rule for port 51820 as UDP

Security group name

launch-wizard-2

Owner

134763639657

Security group ID

sg-0b2a90e4a8be5900d

Inbound rules count

4 Permission entries

Description

launch-wizard-2 created 2025-06-03T09:01:20.734Z

Outbound rules count

1 Permission entry

VPC ID

vpc-0d8158bc3b3cf4687

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (4)

Manage tags

Edit inbound rules

Search

	Name	Security group rule ID	IP version	Type	Protocol
<input type="checkbox"/>	-	sgr-081e89900ccfcde32	IPv4	Custom UDP	UDP
<input type="checkbox"/>	-	sgr-0a7db970a43b29188	IPv4	HTTPS	TCP
<input type="checkbox"/>	-	sgr-0d1eb4baeafae01af	IPv4	HTTP	TCP
<input type="checkbox"/>	-	sgr-07dbcfc5e84077722	IPv4	SSH	TCP

As a result, the rule should be added to inbound rules like this

Inbound rules

Filter rules

< 1 >

Name	Security group rule ID	Port range	Protocol	Source
-	sgr-081e89900ccfcde32	51820	UDP	0.0.0.0/0
-	sgr-0a7db970a43b29188	443	TCP	0.0.0.0/0
-	sgr-0d1eb4baeafae01af	80	TCP	0.0.0.0/0
-	sgr-07dbcfc5e84077722	22	TCP	0.0.0.0/0

Connect to Instance:

Instance summary for i-017c13913ad79205d (MyProjectMurdoch) Info

Connect

Instance state

Actions

Updated less than a minute ago

Instance ID

i-017c13913ad79205d

IPv6 address

-

Hostname type

IP name: ip-172-31-47-27.ap-southeast-2.compute.internal

Answer private resource DNS name

IPv4 (A)

Public IPv4 address

13.210.1.190 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-172-31-47-27.ap-southeast-2.compute.internal

Instance type

t3.micro

Private IPv4 a

172.31.47

Public DNS

ec2-13-210-1-2.compute.am | open address

Elastic IP add

13.210.1.

When in the terminal, it should look like this, then enter the following codes

```
System load: 0.08      Temperature: -273.1 C
Usage of /: 44.3% of 6.71GB Processes: 116
Memory usage: 35%     Users logged in: 0
Swap usage: 0%        IPv4 address for ens5: 172.31.47.27

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Sun Jun  8 01:12:35 2025 from 13.239.158.5
ubuntu@ip-172-31-47-27:~$
```

i-017c13913ad79205d (MyProjectMurdoch)

PublicIPs: 13.210.1.190 PrivateIPs: 172.31.47.27

What to enter:

Sudo apt update

Sudo apt install wireguard

sudo mkdir /etc/wireguard/

This is to make a directory for all the files

wg genkey | sudo tee /etc/wireguard/privatekey | wg pubkey | sudo tee /etc/wireguard/publickey

This is to generate the public and private keys for the VPN

sudo nano /etc/wireguard/wg0.conf

This is to create an edit the file

Enter this into the file:

[Interface]

Address = 10.0.0.1/24

SaveConfig = true

ListenPort = 51820

PrivateKey = private_key

PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

Swap the private key with the actual private key created

sudo systemctl enable wg-quick@wg0

sudo systemctl start wg-quick@wg0

This starts the WireGuard service

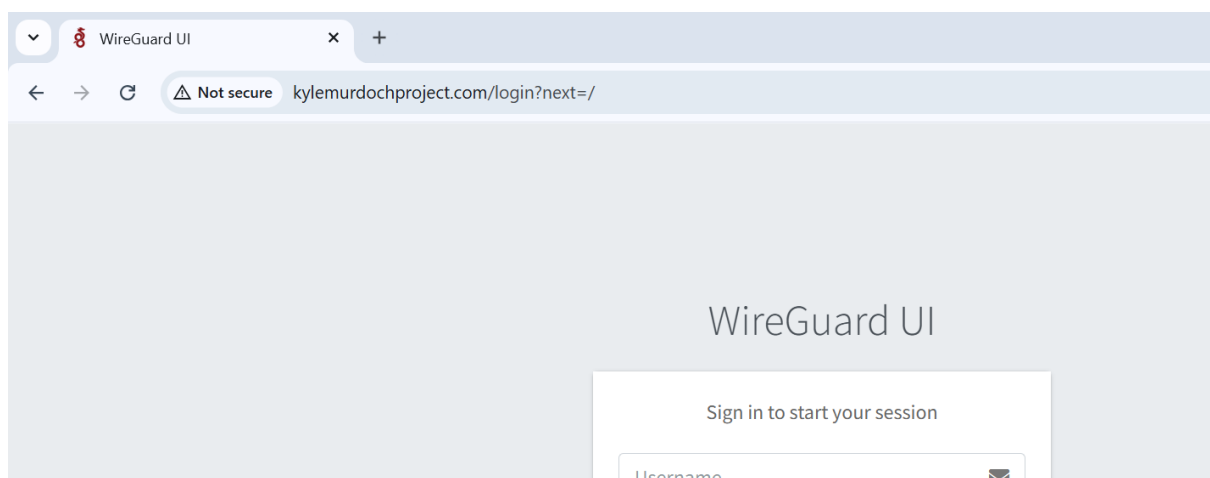
sudo wg-quick up wg0

This opens up the interface

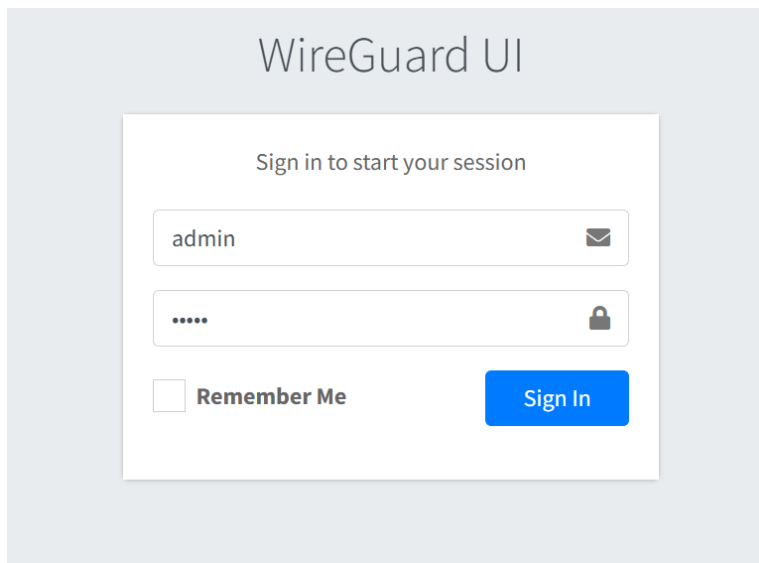
this is all you need to input

Accessing the Wireguard VPN:

In a new tab search up the instance's address, either the IP address or the DNS

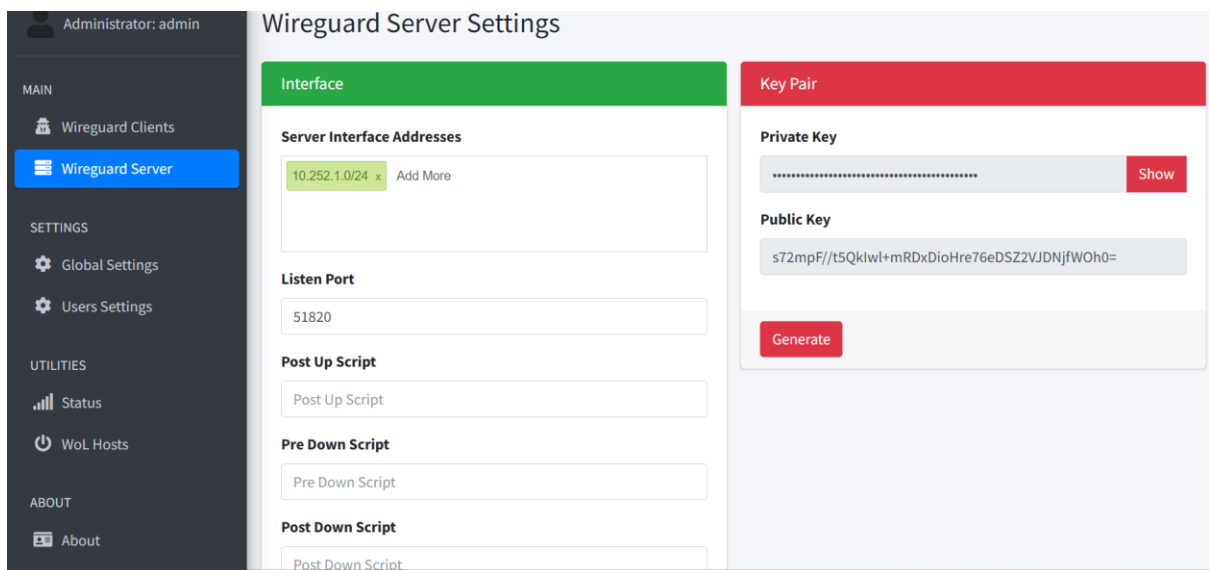


Enter username - “admin”, password- “admin” to access the host privilege



The image shows the WireGuard UI login screen. It has a light gray background with the title "WireGuard UI" at the top. Below the title is a white box containing the login form. The form has the text "Sign in to start your session" at the top. There are two input fields: the first is for the username, containing "admin", and the second is for the password, containing six dots. To the right of the password field is a lock icon. Below the input fields is a checkbox labeled "Remember Me" and a blue button labeled "Sign In".

(WireGuard interface)



The image shows the WireGuard Server Settings interface. It has a dark gray sidebar on the left with the following menu items: "MAIN" (with a sub-item "Wireguard Clients"), "Wireguard Server" (highlighted in blue), "SETTINGS" (with sub-items "Global Settings" and "Users Settings"), "UTILITIES" (with sub-items "Status" and "WoL Hosts"), and "ABOUT" (with a sub-item "About"). The main content area is titled "Wireguard Server Settings" and is divided into two columns. The left column is titled "Interface" and contains the following sections: "Server Interface Addresses" (with a list containing "10.252.1.0/24" and an "Add More" button), "Listen Port" (with a text input field containing "51820"), "Post Up Script" (with a text input field containing "Post Up Script"), "Pre Down Script" (with a text input field containing "Pre Down Script"), and "Post Down Script" (with a text input field containing "Post Down Script"). The right column is titled "Key Pair" and contains the following sections: "Private Key" (with a text input field containing a long string of dots and a "Show" button), "Public Key" (with a text input field containing "s72mpF//t5Qklwl+mRDxDioHre76eDSZ2VJDNjfWOH0="), and a "Generate" button.

Administrator: admin

MAIN

Wireguard Clients

Wireguard Server

SETTINGS

Global Settings

Users Settings

UTILITIES

Status

WoL Hosts

ABOUT

About

Global Settings

Wireguard Global Settings

Endpoint Address

13.210.1.190

Suggest

DNS Servers

1.1.1.1

Add More

MTU

1450

Persistent Keepalive

15

Firewall Mark

0xca6c

Table

Help

1. Endpoint Address

The public IP address of your Wireguard server that the client will connect to. Click on **Suggest** button to auto detect the public IP address of your server.

2. DNS Servers

The DNS servers will be set to client config.

3. MTU

The MTU will be set to server and client config. By default it is **1450**. You might want to adjust the MTU size if your connection (e.g PPPoE, 3G, satellite network, etc) has a low MTU.

4. Persistent Keepalive

By default, WireGuard peers remain silent while they do not need to communicate, so peers located behind a NAT and/or firewall may be unreachable from other peers until they reach out to other peers themselves. Adding **PersistentKeepalive** can ensure that the connection remains open.

WIREGUARD UI

Administrator: admin

MAIN

Wireguard Clients

Wireguard Server

SETTINGS

Global Settings

Users Settings

UTILITIES

Status

WoL Hosts

Users Settings

+ New Client

✓ Apply Config

Logout

+ New User

Edit

Delete

admin

Administrator

Add users and confirm changes

WIREGUARD UI

Administrator: admin

MAIN

Wireguard Clients

Wireguard Server

SETTINGS

Global Settings

Users Settings

UTILITIES

Status

WoL Hosts

Wireguard Clients

Search

All

+ New Client

✓ Apply Config

Logout

New Wireguard Client



Name

User1

Email

Subnet range

Any

IP Allocation

10.252.1.1/32 

Add More

Allowed IPs

0.0.0.0/0 


Add More


Extra Allowed IPs

WIREGUARD UI


Administrator: admin


MAIN

 Wireguard Clients

 Wireguard Server


SETTINGS



 Global Settings

 Users Settings

UTILITIES

 Status

 WoL Hosts

Search  All 

Wireguard Clients

[Download](#) [QR code](#) [Email](#) [More](#) 

 User1



2025/06/04 09:03:23



2025/06/04 09:03:23



DNS enabled



IP Allocation

10.252.1.1/32

Allowed IPs


0.0.0.0/0

Wireguard Clients


[Download](#) [QR code](#) [Email](#) [More](#) 

 User_1

 kyle.mckenzie4808@gmail.com

 2025/06/04 09:13:08

 2025/06/04 09:13:08

 DNS enabled



IP Allocation

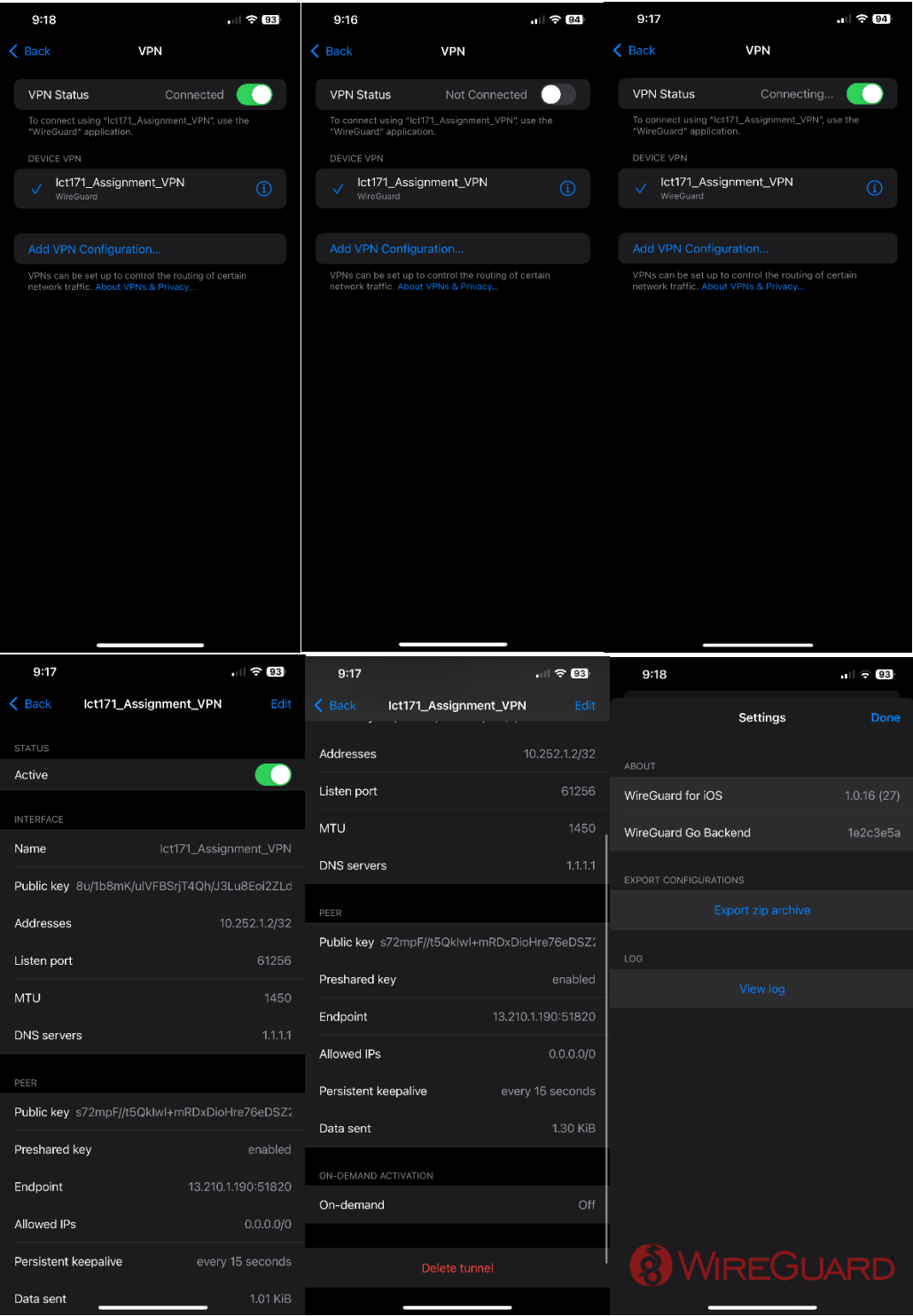
10.252.1.2/32

Allowed IPs

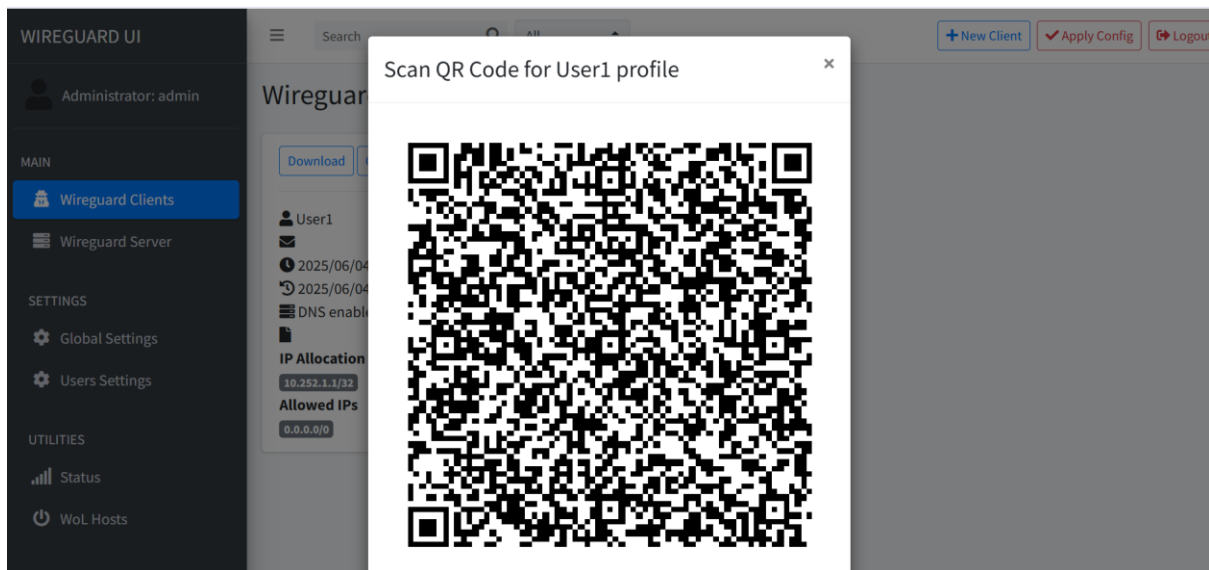
0.0.0.0/0

Get the user who is using it to download the application “WireGuard”

(Wireguard app/ iphone settings)



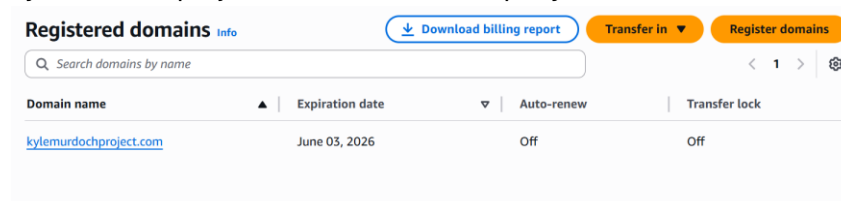
Scan the QR code and the VPN will be set up



DNS linking process:

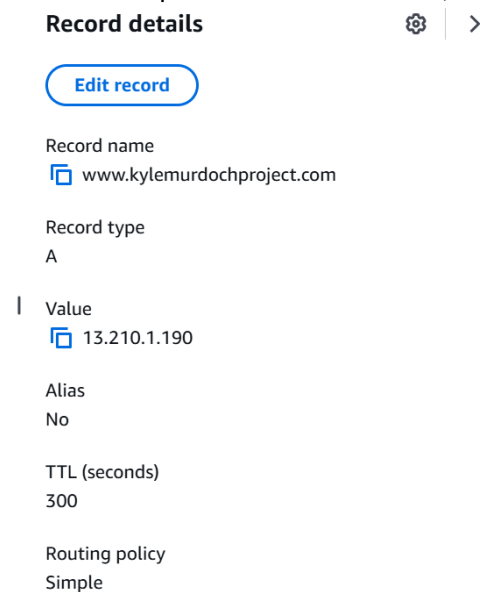
1. Purchase a domain name

This domain was purchased from Amazon AWS Route 53. The domain name is kylemurdochproject.com, \$14.50 USD/per year



2. Created an A record

The type of the record – “A”,
the name of the record is www.kylemurdochproject.com,
The record points to 13.210.1.190,



3. Waited roughly 10 minutes for DNS to propagate

Configuration files and setting changes:

Input of these configurations;

/etc/wireguard/wg0.conf

Enter : [Interface]

Address = 10.0.0.1/24

SaveConfig = true

ListenPort = 51820

PrivateKey = private_key

PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

/etc/sysctl.conf

net.ipv4.ip_forward=1

sudo sysctl -p

sudo systemctl enable wg-quick@wg0

sudo systemctl start wg-quick@wg0

Script:

Final script below:

```
#!/bin/bash
```

```
# My WireGuard Status Report Script
```

```
# This script checks the status of all the active users on my WireGuard service
```

```
# It also prints the system info like the hostname, public IP and the uptime
```

```
# Check if wg command is available
```

```
if ! command -v wg &> /dev/null; then
```

```
    echo "Error: WireGuard is not installed or 'wg' command is not in PATH."

    exit 1

fi

# Get system information

HOSTNAME=$(hostname)

UPTIME=$(uptime -p)

PUBLIC_IP=$(curl -s ifconfig.me || echo "N/A")

# Print system info

echo "WireGuard VPN Status Report"

echo "Hostname    : $HOSTNAME"

echo "Public IP    : $PUBLIC_IP"

echo "System Uptime : $UPTIME"

# Get all active WireGuard interfaces

WG_INTERFACES=$(wg show interfaces)

if [ -z "$WG_INTERFACES" ]; then

    echo "No active WireGuard interfaces found."

    exit 0

fi

# Loop through each interface

for iface in $WG_INTERFACES; do

    echo "Interface    : $iface"

    # Interface info

    LISTEN_PORT=$(wg show "$iface" | grep "listen port" | awk '{print $3}')
```

```
echo "Listen Port : $LISTEN_PORT"
```

```
# Show peers
```

```
PEERS=$(wg show "$iface" peers)
```

```
if [ -z "$PEERS" ]; then
```

```
    echo "No peers connected."
```

```
else
```

```
    echo "Connected Peers:"
```

```
for peer in $PEERS; do
```

```
    ENDPOINT=$(wg show "$iface" endpoint | grep "$peer" | awk '{print $2}')
```

```
    HANDSHAKE=$(wg show "$iface" latest-handshakes | grep "$peer" | awk '{print $2}')
```

```
# Convert UNIX timestamp to readable format
```

```
if [ "$HANDSHAKE" -eq 0 ]; then
```

```
    LAST_HANDSHAKE="Never"
```

```
else
```

```
    LAST_HANDSHAKE=$(date -d @"$HANDSHAKE")
```

```
fi
```

```
RX=$(wg show "$iface" transfer | grep "$peer" | awk '{print $2}')
```

```
TX=$(wg show "$iface" transfer | grep "$peer" | awk '{print $4}')
```

```
echo "Peer: $peer"
```

```
echo " Endpoint      : $ENDPOINT"
```

```
echo " Last Handshake : $LAST_HANDSHAKE"
```

```
echo " Transfer (RX/TX) : $RX / $TX"
```

```
echo ""
```

```
done
```

```
fi
```

```
done
```

Use of script

This Bash script creates a live status report for my Wireguard VPN server. It shows the system hostname, public IP, and uptime, and checks all active WireGuard interfaces. For each interface, it lists peers, their connection endpoint, the timestamp of the last successful handshake, and data transferred in both directions. This gives a good summary of everything going on so that if anything isn't working it can be shown through a simple script.

Output

```
ubuntu@ip-172-31-47-27:~$ ./wg-status.sh
WireGuard VPN Status Report
Hostname      : ip-172-31-47-27
Public IP     : 13.210.1.190
System Uptime : up 5 days, 18 hours, 13 minutes
Interface     : wg0
Unable to access interface: Operation not permitted
Listen Port   :
Unable to access interface: Operation not permitted
No peers connected.
ubuntu@ip-172-31-47-27:~$
```

```
ubuntu@ip-172-31-47-27:~$ sudo ./wg-status.sh
WireGuard VPN Status Report
Hostname      : ip-172-31-47-27
Public IP     : 13.210.1.190
System Uptime : up 5 days, 18 hours, 16 minutes
Interface     : wg0
Listen Port   :
No peers connected.
ubuntu@ip-172-31-47-27:~$
```

References:

Wireguard:

Donenfeld, J. A. (n.d.). *WireGuard: Fast, modern, secure VPN tunnel*. WireGuard.
<https://www.wireguard.com/>

Wireguard set up:

Tetzner, G. (2021, September 5). *Setting up a VPN with WireGuard server on AWS EC2*. DEV Community. <https://dev.to/gabrielnetzner/setting-up-a-vpn-with-wireguard-server-on-aws-ec2-4a49>

Set up assistance and understanding:

Numberphile. (2015, May 14). Why basic research is important [Video]. YouTube.
<https://www.youtube.com/watch?v=6gnsQjPCC>