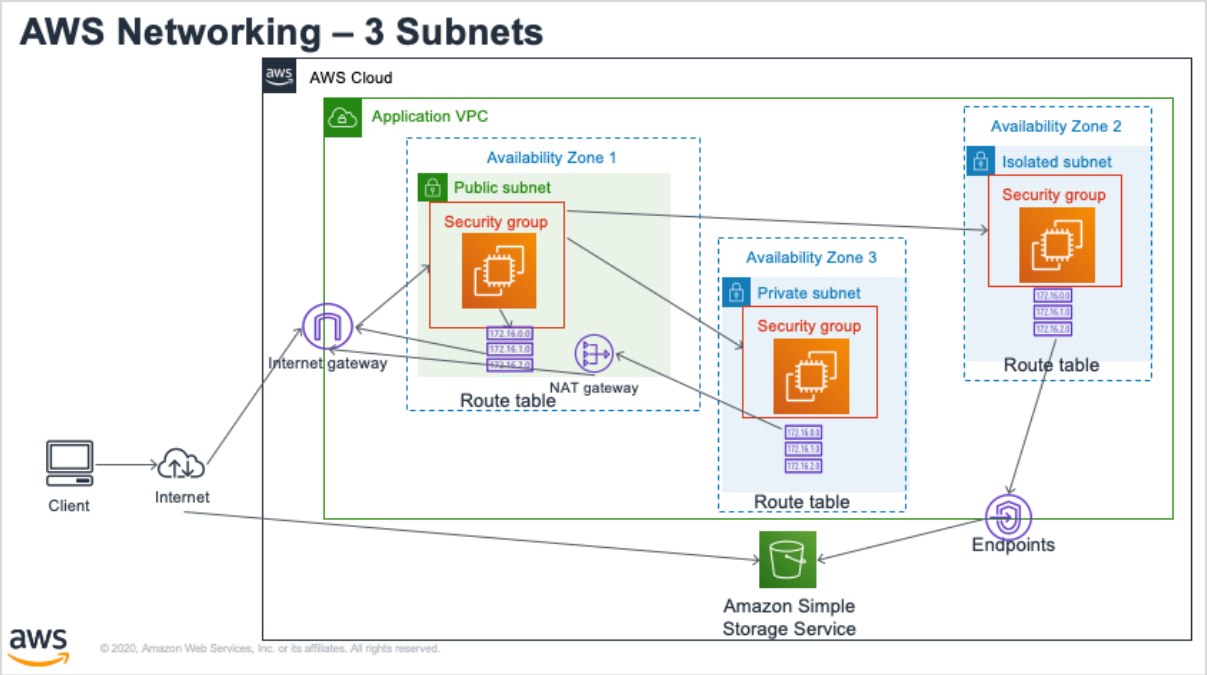
AWS Networking 101

- Material gathered from course: Udemy 'Clear and Simple AWS Advanced Networking 2020'
- Goal is to cover the basics
- Audience
  - Not familiar with AWS Network basics like VPC/Subnets/Routers
  - Some familiarity with AWS Console
  - Basic level of comfort with Linux



Intro

We are going to create a VPC with 3 different subnets in 3 different availability zone, each with different network configurations.

We are going to cover the following AWS Networking concepts

- VPC
- Availability Zones
- Subnets (Public, Private, Isolated)
- Security Groups
- Network ACL
- Router / Route Table

- NAT Gateway
- Internet Gateway
- VPC Endpoints

Public Subnet - Bastion EC2

This subnet will host an EC2 instance that can access the internet, and is accessible from the internet. It will also be configured as a jump box to get to EC2 instances in the private and Isolated Subnets

Private Subnet

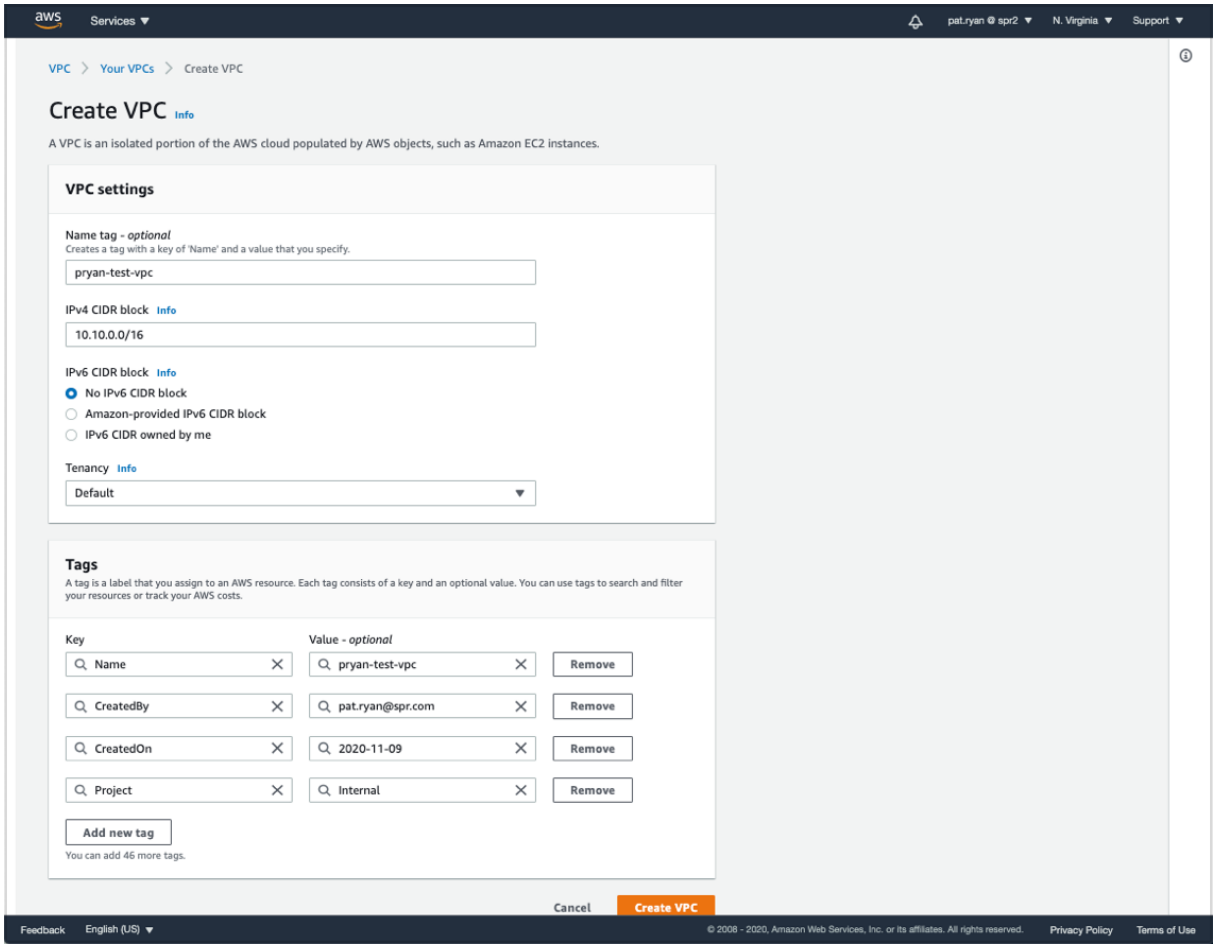
This subnet will host an EC2 instance that can get out to the internet, but there is no access from the internet to this EC2 instance. This subnet will have a router configured to allow traffic to flow to a NAT Gateway. It will also setup a security group to only allow SSH traffic from the Public EC2 instance.

Isolated Subnet

This subnet will host an EC2 instance that cannot get to the internet, nor is it accessible from the internet. This subnet will be configured to use an VPC Endpoint to access S3. It will also setup a security group to only allow SSH traffic from the Public EC2 instance.

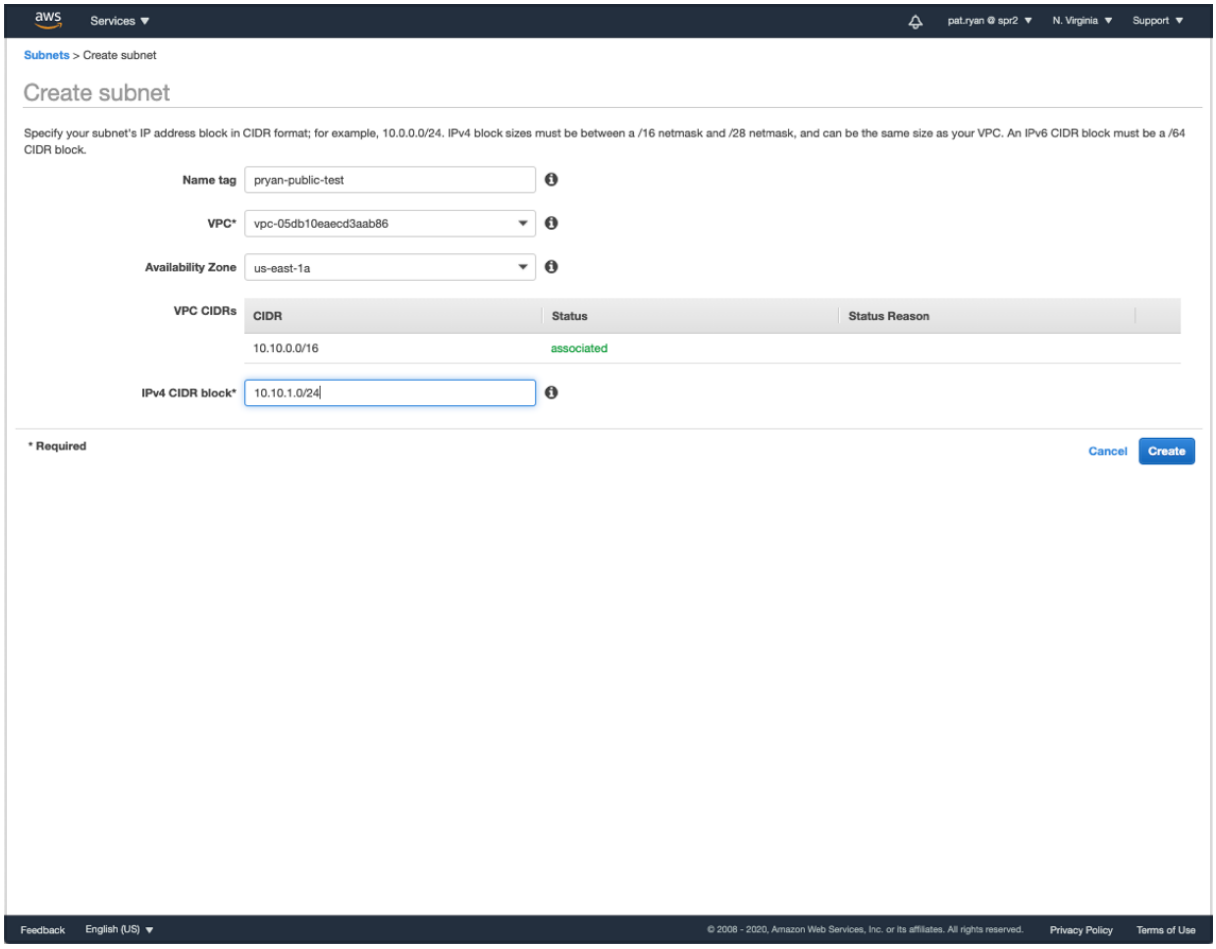
Create VPC

- Open AWS Console and search for VPC



- name
- CIDR Block
  - 10.100.0.0/16
    - Note that students will have to pick a different cider range.
    - I suggest 10.<studentid>.0.0/16
  - Add tags

Create Subnets



- Create Public Subnet
  - Note in the 'Description' tab, that the '**Auto-assign public IPv4 address** is set to no
  - Select 'Actions' ➔ 'Modify auto assign IP settings'
  - 'Auto-assign IPv4' make sure that is checked.
- Create Private Subnet
- Create Isolated Subnet
- Note - that at the moment they are public, private, isolated in name only

Subnet Creation

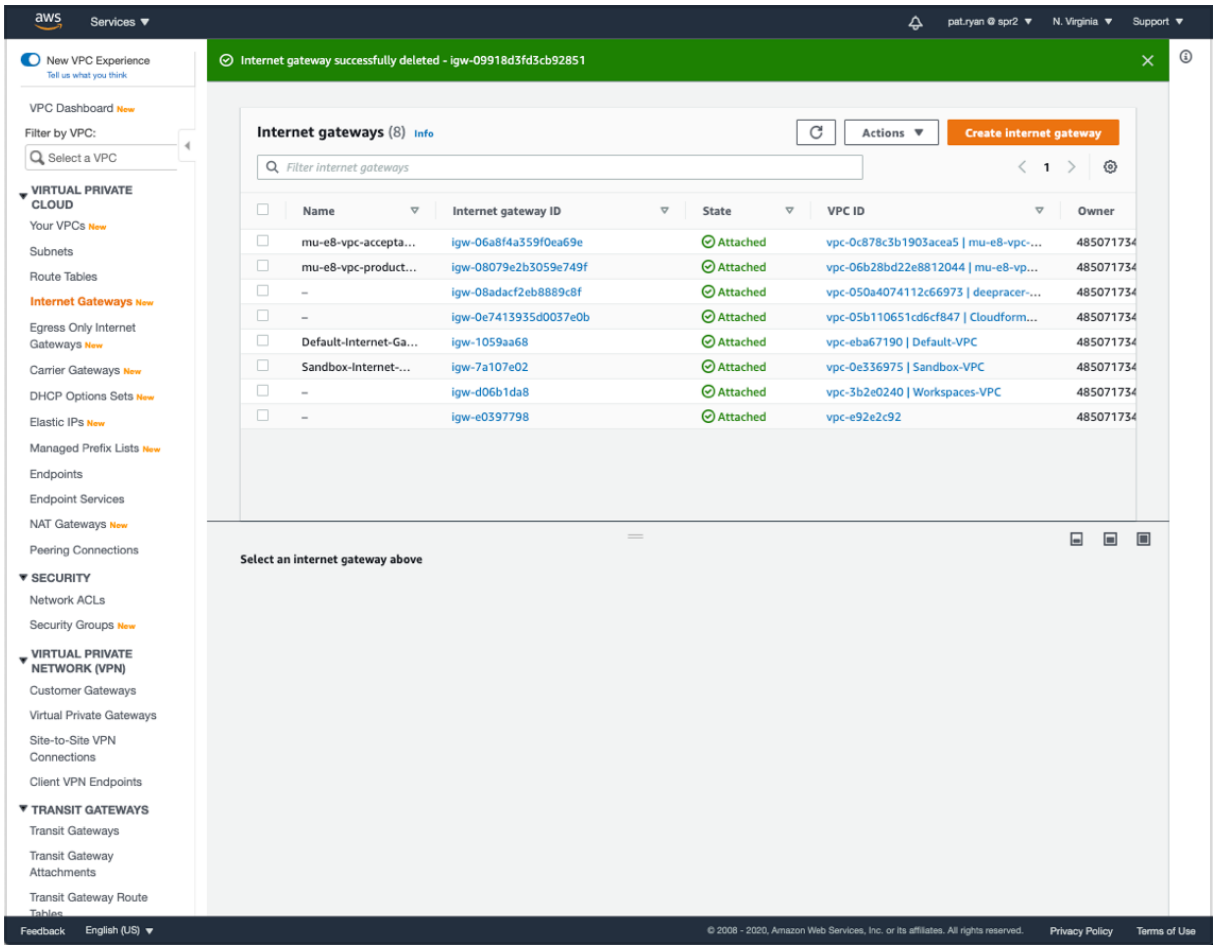
- name: pryan-public-subnet
- VPC: choose the vpc you just created
- Availability Zone: select us-east-1a
- IPv4 CIDR Block: XX.XX.1.0/24 For public use .1, for private .2, for isolated .3

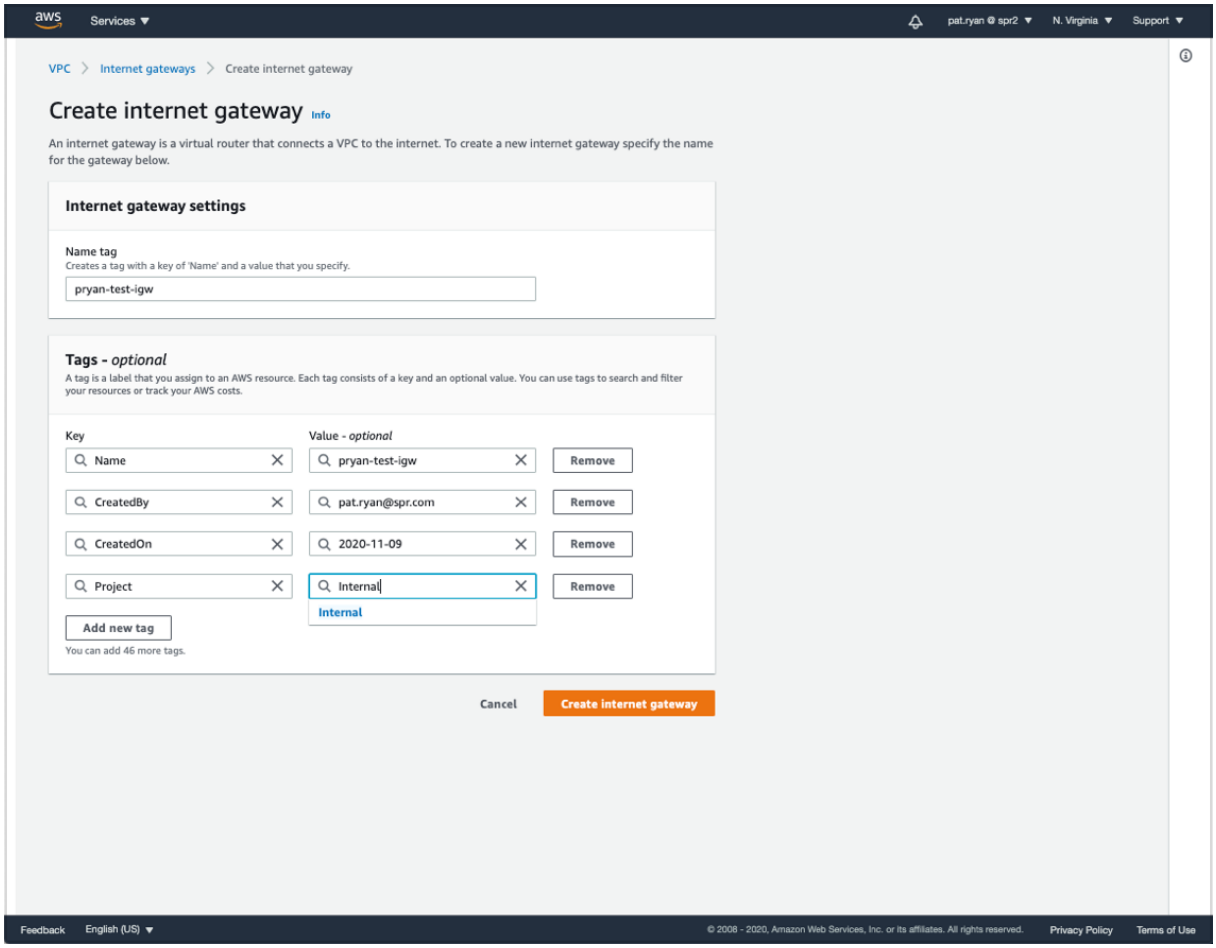
- Build out the public subnet. It is going to need access to an Internet Gateway to route subnet traffic to/from the internet. This is what makes the subnet public.
- NOTE: Every new subnet gets the VPC Default Route Table. We will see how we change that later on.

UPDATE THE PUBLIC SUBNET TO ALL PUBLIC IPV4 ADDRESSES

Create Internet Gateway

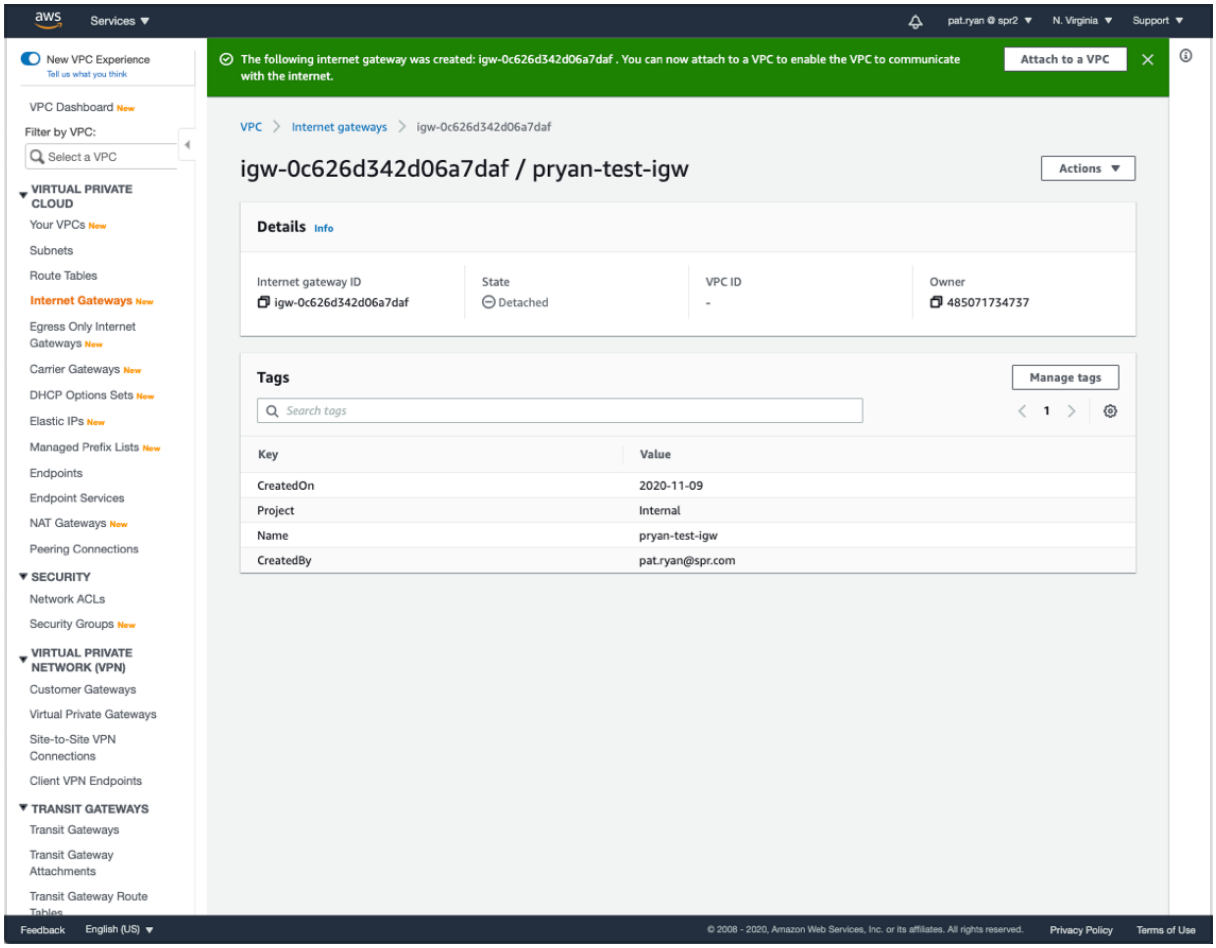
- select ‘Internet Gateways’ in left nav



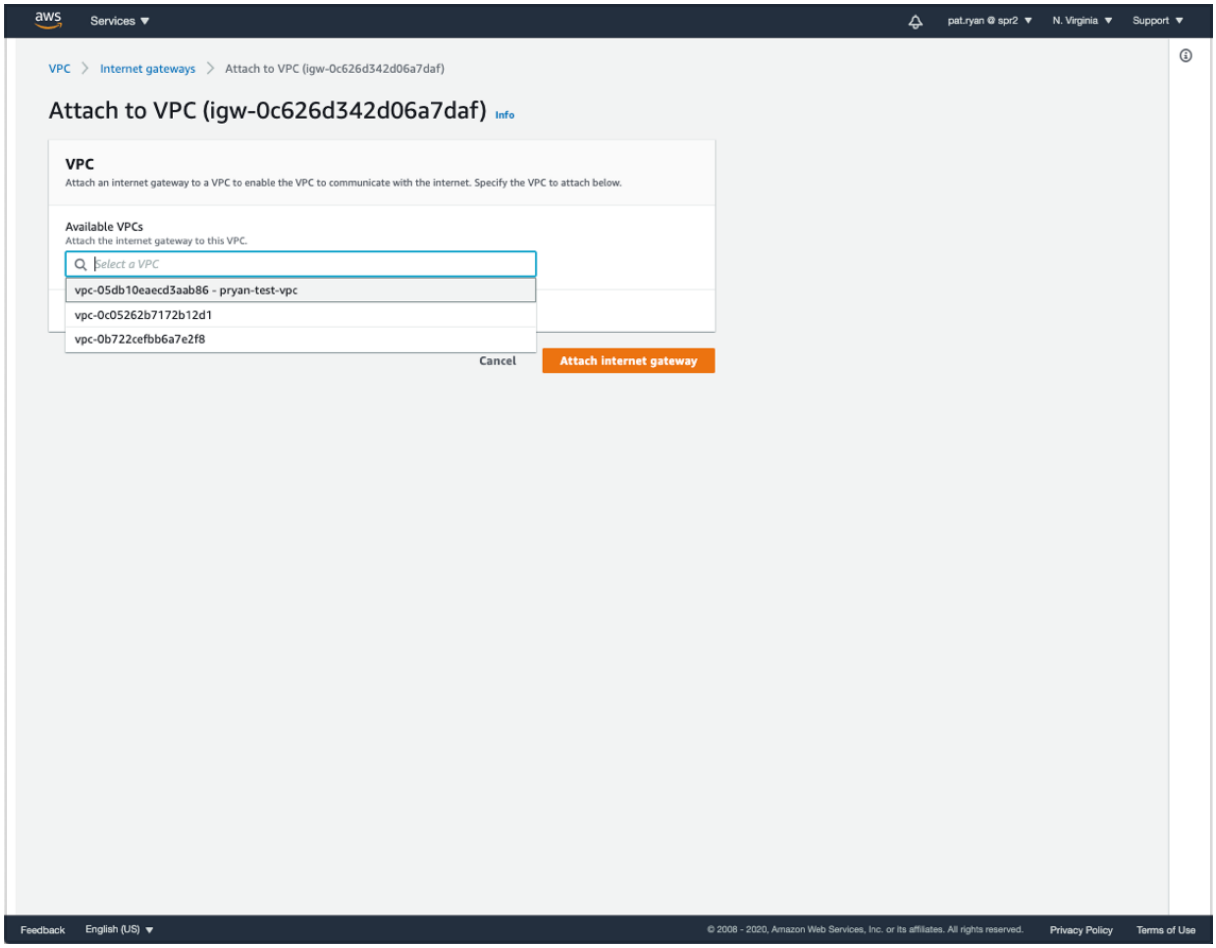


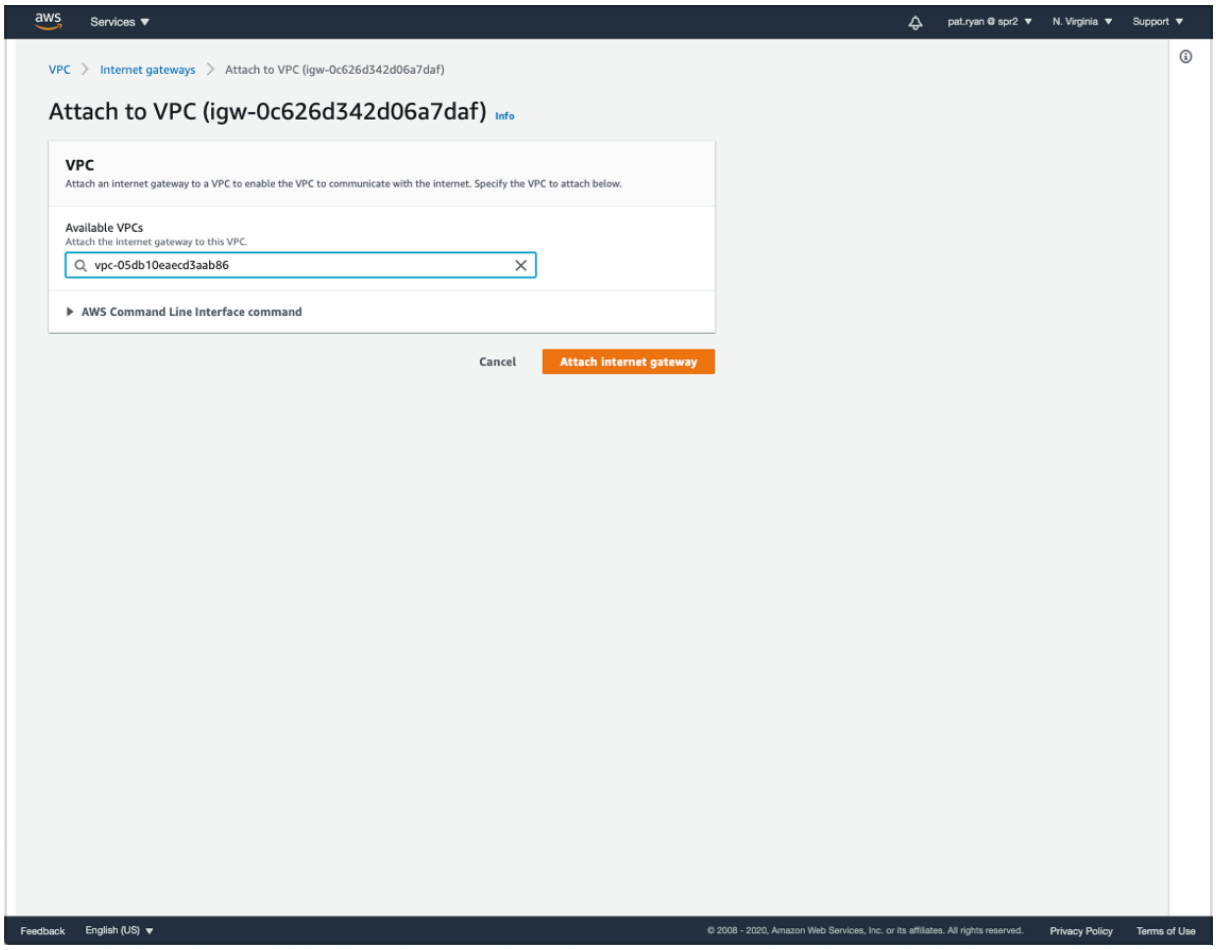
- Select 'Create Internet gateway' button
- Notice that the Internet gateway is **Detached**
- Select 'Actions' or Green banner 'Attach to a VPC'.
  - Notice we are attaching the Internet gateway to a VPC

- Attach to VPC, this will take a few minutes to complete

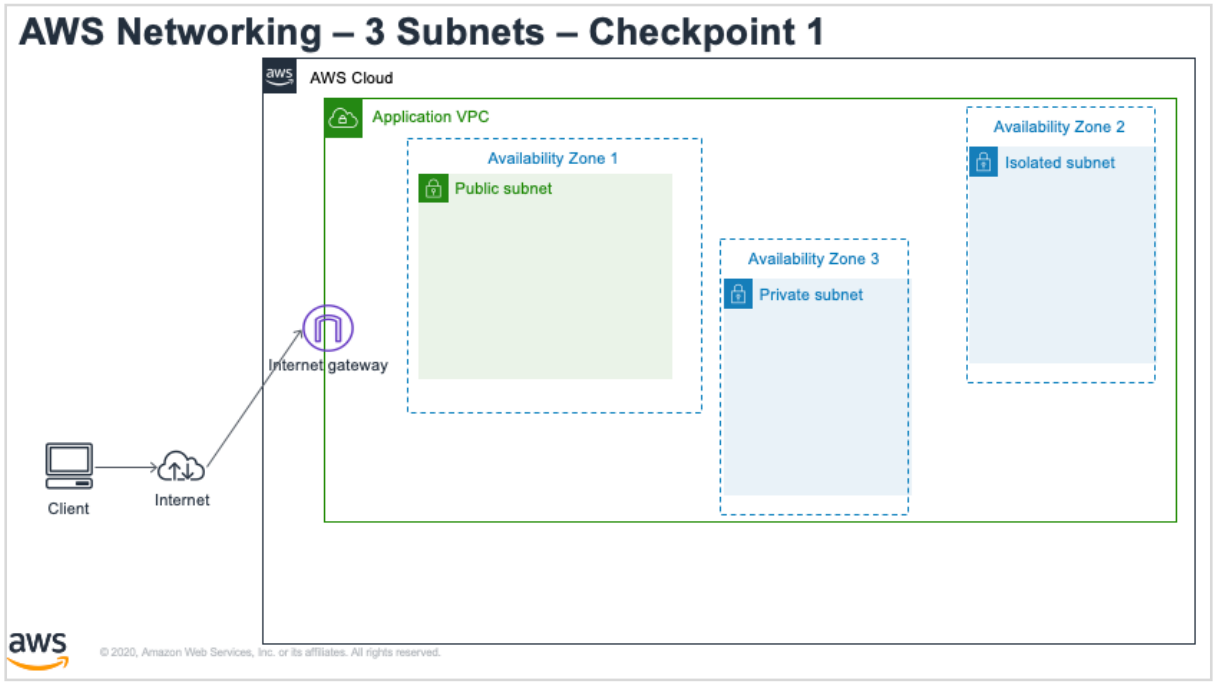


- Select your VPC and press, ‘Attach internet gateway’


aws
Services
pat.ryan @ spr2
N. Virginia
Support
VPC
Internet gateways
Attach to VPC (igw-0c626d342d06a7daf)
Attach to VPC (igw-0c626d342d06a7daf) Info
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.
Available VPCs
Attach the internet gateway to this VPC.
Select a VPC
vpc-05db10eaecd3aab86 - pryan-test-vpc
vpc-0c05262b7172b12d1
vpc-0b722cefbb6a7e2f8
Cancel
Attach internet gateway
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use



- This may take a minute
- STOP here. Show picture below and talk through where we are at.



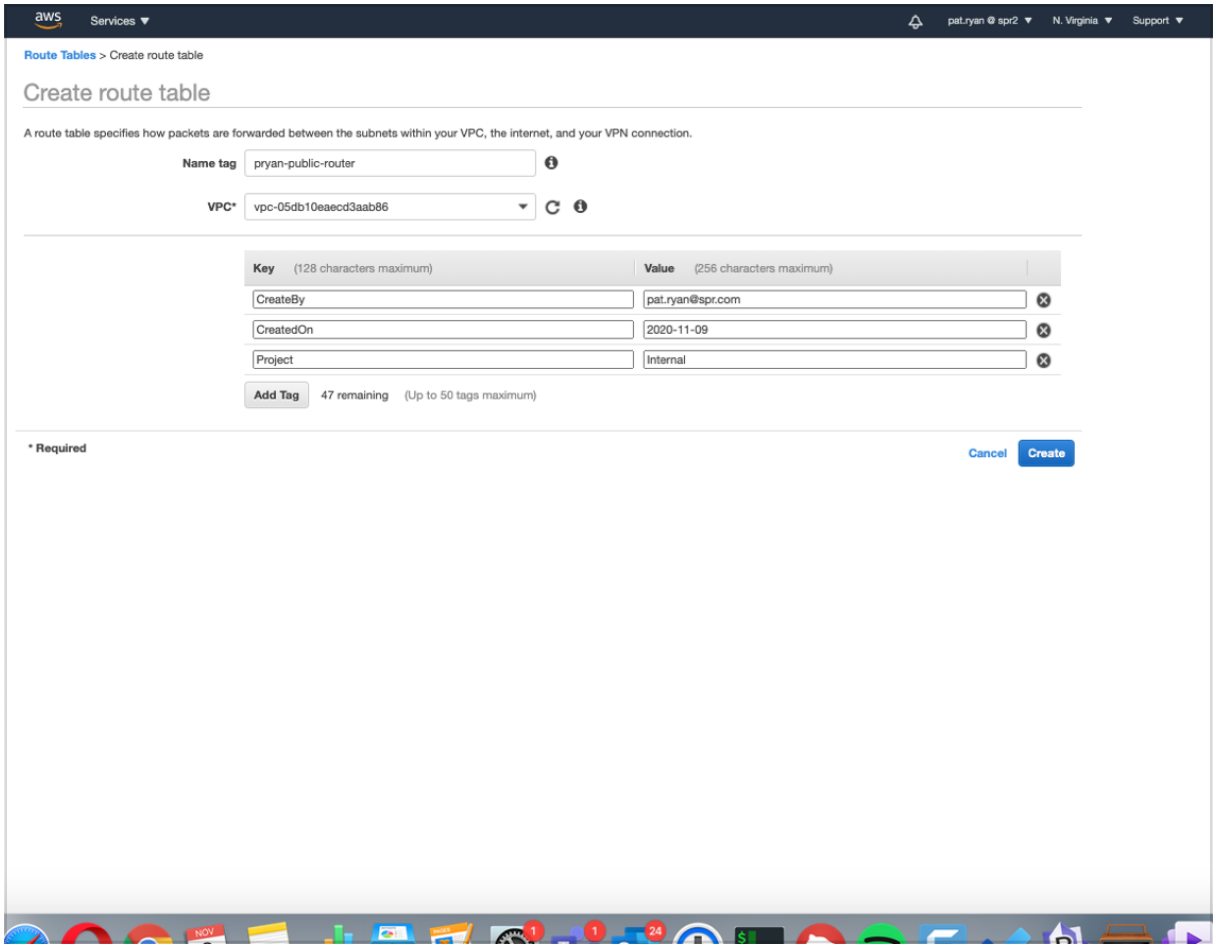

```
Lets build out the Public Subnet to add an Bastion or Jump EC2 instance.  This
```

```
will require us to give access to the internet to EC2 instances in the Public Subnet.

To do that, we will create a route table that will allow us to route traffic either internally to the VPC OR externally to the Internet Gateway
```

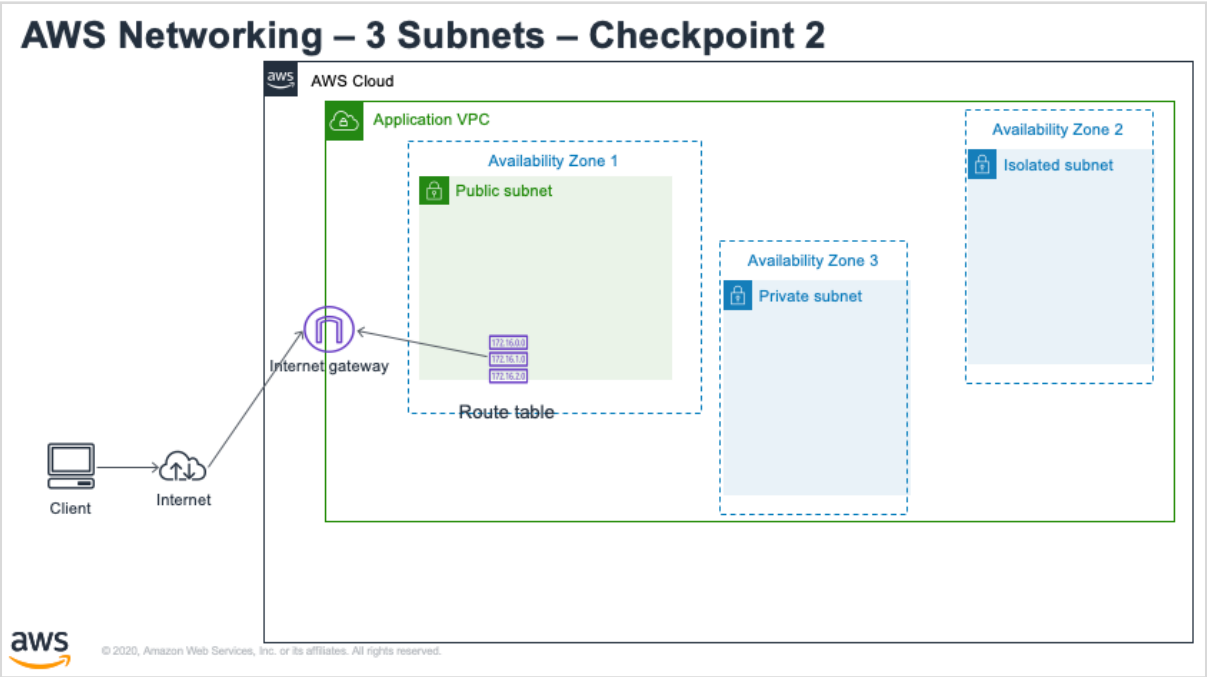
Create Public Route Table

- Each subnet gets the VPC default router and routing table
- Select Subnets ➜ Public Subnet ➜ Route Table
  - Note it only allows the routing of traffic within the VPC.
- We DO NOT want to change the default VPC route table
- Create a new route table, just for the public Subnet.
- Select Route Tables ➜ Create route table
- Select 'Create Route Table' button
- Add tag name (name of route table)
- Select your vac
- Add tags
- 'Create' button
- 'Close' button
- Select newly created route table
- Select "Routes" tab in bottom
- Select 'Edit Routes'
  - We want to add a route for any default traffic to go to internet gateway
- 'Add route' button
- Destination: 0.0.0.0/0
- Target: Internet Gateway ➜ Select your internet gateway
- Select 'Save routes'
- Select 'Close'
-

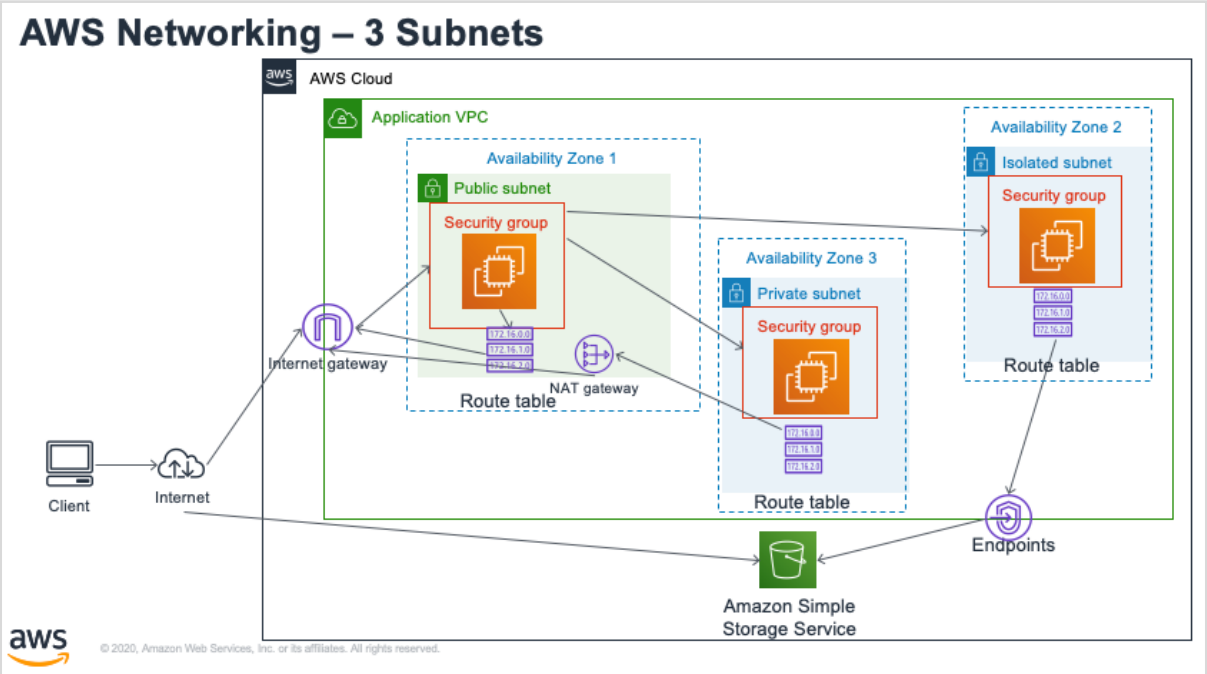


- At this point we have a new route table, but we have NOT associated it with a subnet yet
- Select 'Subnets' left nav
- Select your public subnet
- Select 'Route Table' below
- Select 'Edit route table association'
- In DropDown select new route table
  - It should show the routes, one being to IGW
- Select 'Save' and then 'Close'

- STOP and recap
- Replaced the default route table in the public subnet, with a new route table that includes a default route of anything that does not match internal traffic, to go to the internet gateway.



- Remember the ultimate network architecture



- Now - lets create an EC2 and associate it with the Public Subnet and create a security group for the EC2

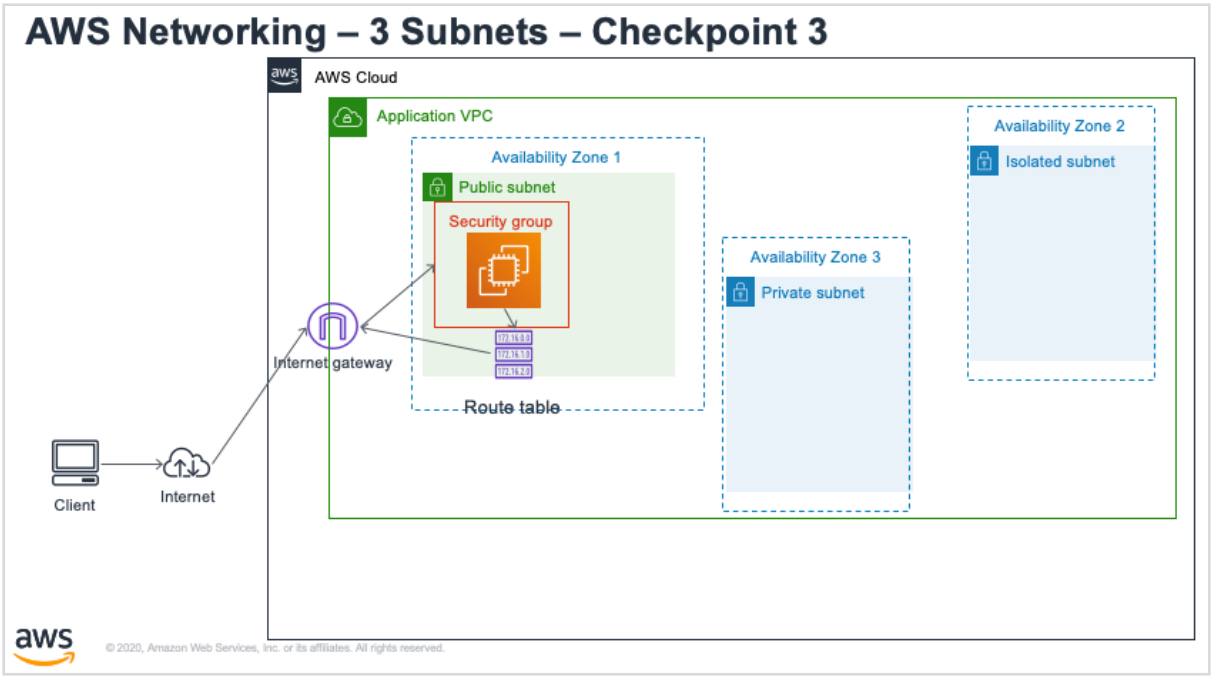
  Security Group / Router / Network ACL

- What is the difference between a Router and a Security Group
  - Router routes traffic in a subnet. Not specific to an EC2
    - applies to all EC2 instances in the subnet
  - Security Group is associated with a ENI (elastic network interface) like an EC2.
    - Only applied to the EC2 instances it is associated with

        - Inbound / Outbound Security Rules
        - update to 5 security groups per ENI
    - Security Groups are stateful
        - Allows a response (return traffic) to an outgoing request.
        - understands status of connections
    - Network ACL
        - Stateless
        - Ordered rules on what is or is not allowed.
        - Associated with a Subnet
        - Show Subnet in console and then 'Network ACL'
        - The VPC default Network ACL allows all IN/OUT rules
        - Rules are interrogated top down. Once rule is matched it is enforced and lower rules are ignored
        - New Network ACLs block all IN/OUT traffic
        - Typically you would have deny all, then start to open up as needed

Create an EC2 Instance in the Public Subnet

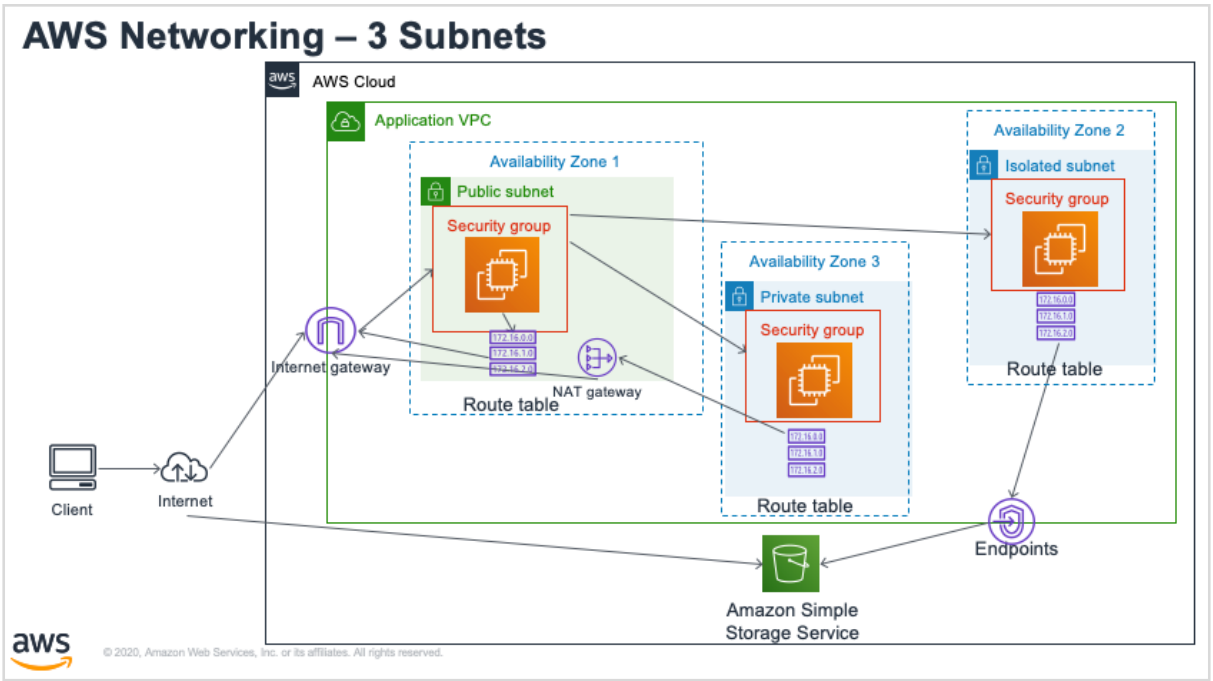
- new tab ➜ AWS Console
- EC2
- Launch Instance
- **Amazon Linux 2 AMI (HVM), SSD Volume Type**
- t2.micro
- Select: 'Next: Configure Instance Details'
    - because we want to specify VPC and Subnet
    - **NOTE I have seen it ignore the Subnet Setting for auto assign. In this case select 'Assign' to be sure you get a public IP**
- Configure Security Group
    - Create a new security group
    - Change name: pryan-public-sg
    - This allows SSH traffic from anywhere (source = 0.0.0.0/0)
        - recommend for now change to 'My IP'
- Either select a key pair or create a new one
- When running show the networking values
- STOP: Checkpoint



- ssh into the public EC2

```
ssh –i “pryan-spr3.pem” ec2-user@174.129.82.221
```

RECAP



- Add the private subnet elements.
- **Private Subnet**
  - Private subnet allows for traffic out to the internet, but there are no direct routes from the internet to the private subnet
  - To do this, we need to add a ‘NAT Gateway’ to the Public subnet, and route outbound

traffic from the private subnet to the 'NAT Gateway'.
    - We are also going to setup a security group on the EC2 instance in the private subnet to allow ssh traffic from the EC2 in the public subnet.

Add a NAT Gateway

- VPC service
- NAT Gateways left nav
- Create NAT Gateway Button
- Name:
- Subnet: Put into PUBLIC subnet
- Allocate Elastic IP button
- Tags

Create EC2 in Private Subnet

- EC2 Service
- Make sure to select new VPC and Private Subnet
- Configure Security Group:
    - Setup SSH to use the security group of public ec2
- Launch

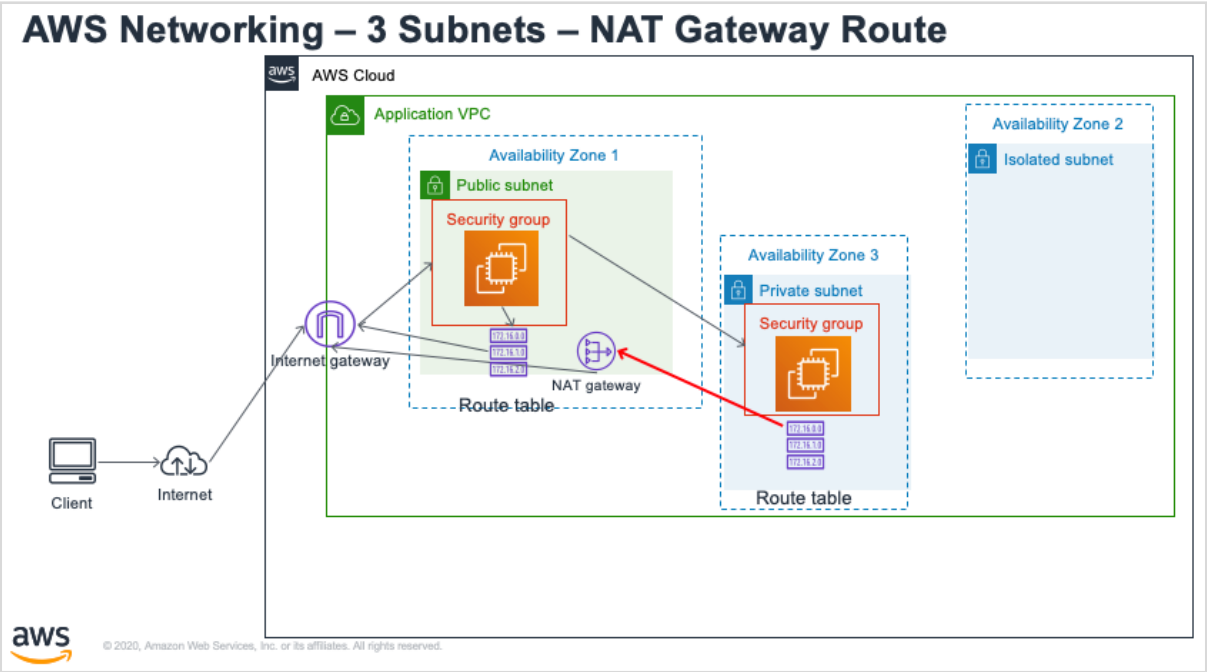
```
Show that the Private EC2 cannot reach the internet.

Log into the Public EC, setup the pryan-spr3.pem file, then SSH to the Private EC2.

On the Private EC2 try to perform a sudo yum update

It will just hang.
```

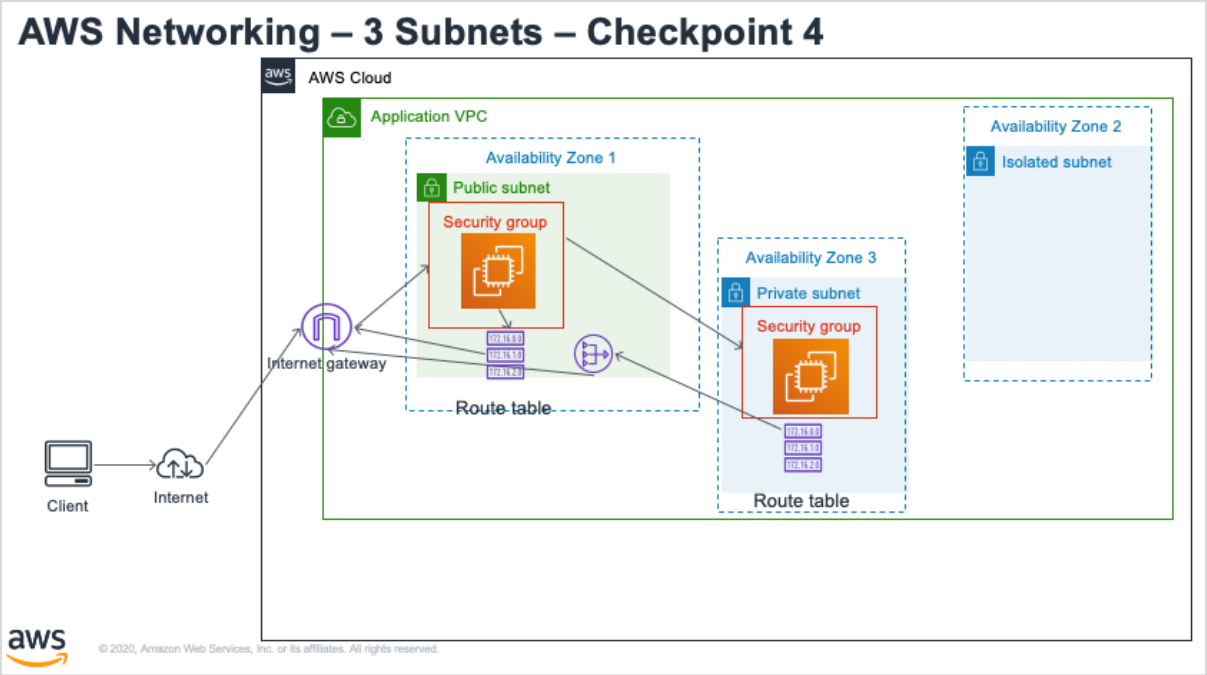
- Picture below shows missing piece. The Private Subnet route table has no route to the NAT Gateway.



Create a new Route Table for the Private Subnet

- VPC Service
- Route Tables
- Create
- Select link to edit route table
- Routes tab
- Edit Routes
- Add Route
  - 0.0.0.0/0 to NAT Gateway
- Save Route
- Close
- Subnet Associations Tab
- Edit subnet associations
  - Select private subnet

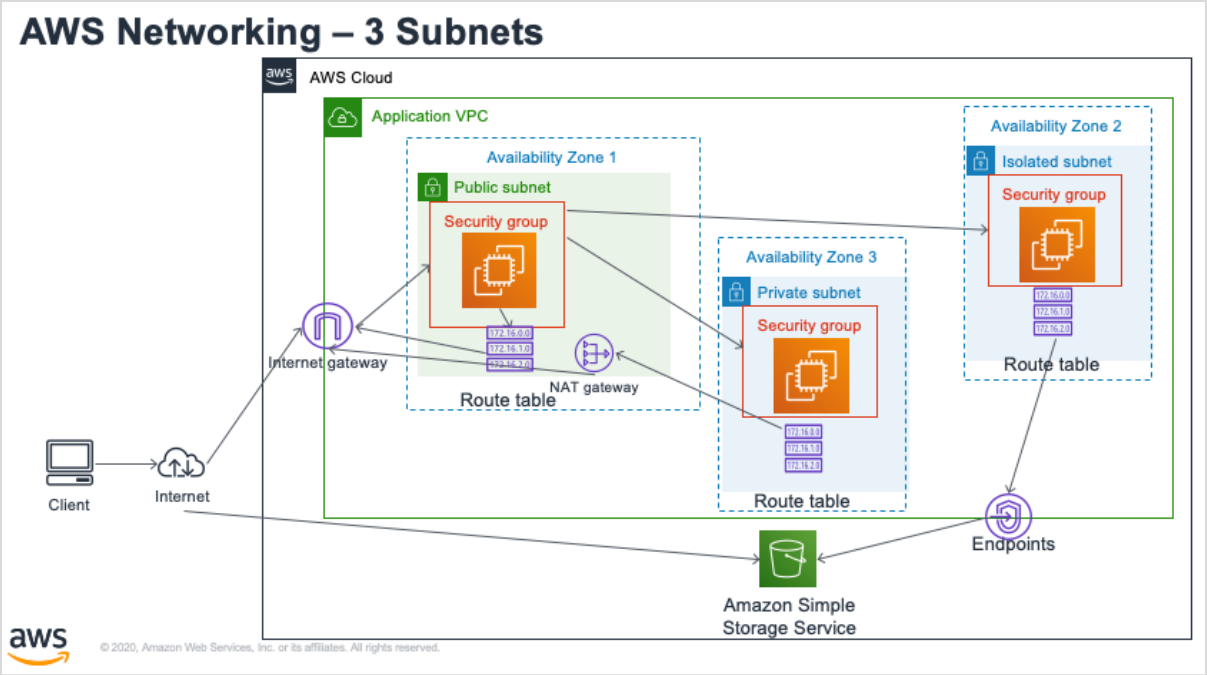
- Review Private EC2 Settings
- STOP: CHECKPOINT
-



- We should be able to ssh to the public EC2, then ssh to the private EC2
- The private EC2 should be able to reach the internet
- NOTE: We have to copy our PEM to the public EC2
-

Build out Isolated Subnet

- Isolated subnet has no access to the internet, and is not accessible from the internet.
- Why would you do this?
  - You likely would not for an ec2 - but maybe
  - You might for a DB server. The only access to the DB server, is internal to the VPC
  - You want servers in an isolated network to only be accessible inside the VPC, with no access to the internet, and only those services that are allowed.
- We are going to create a VPC Endpoint to allow EC2 to get to S3 (you can also have it get to other services like DynamoDB.
- **RECAP**



Create EC2 in Isolated Subnet

- Service EC2
- Create EC2
  - Security group ssh for public sg
- On Public EC2, SSH into Isolated EC2
  - execute: `sudo yum update`
-

```
Log into the Public EC2, SSH to Isolated EC2.

Perform a sudo yum update

and it will hang.

Instead of a NAT Gateway – we are going to create a VPC Endpoint to allow
certain service access.  in this case S3.
```

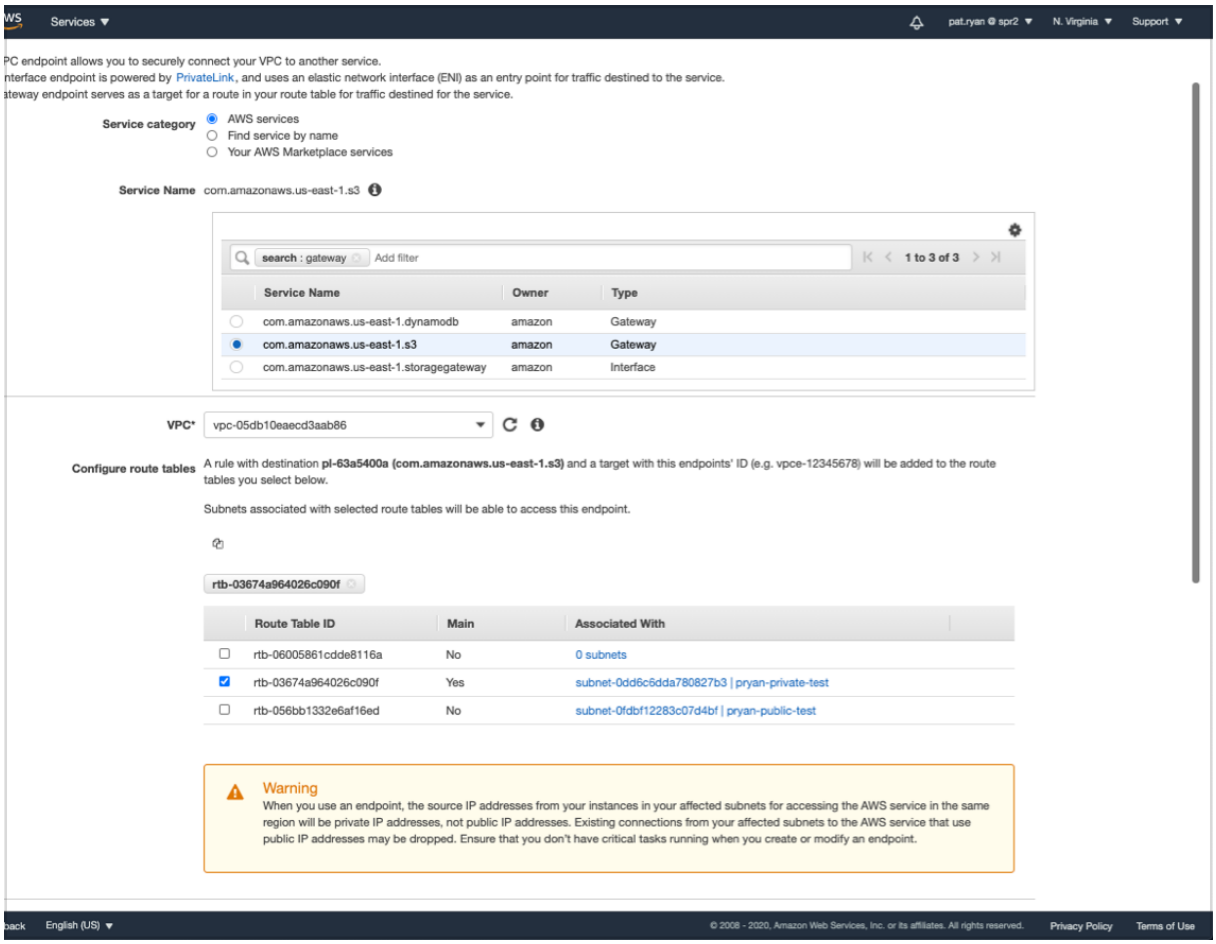
Create Route table for isolated subnet

- Service: VPC
- Route Table left nave
- **Associate** with Isolated Subnet

    - Subnet
    - select Subnet
    - Route Table tab
    - ‘Edit route table association’ button
    -
- VPC Endpoints
    - Allow for communication with services like S3 without going over the internet
    - Communication stays in AWS Network
    -

Create VPC Endpoint to S3

- Service: VPC
- Endpoints left nav
- find s3, search for ‘gateway’



- select you vpc
- add it to the route table associated with the subnet
- this might take a moment.

Review the Isolated Subnet Route table

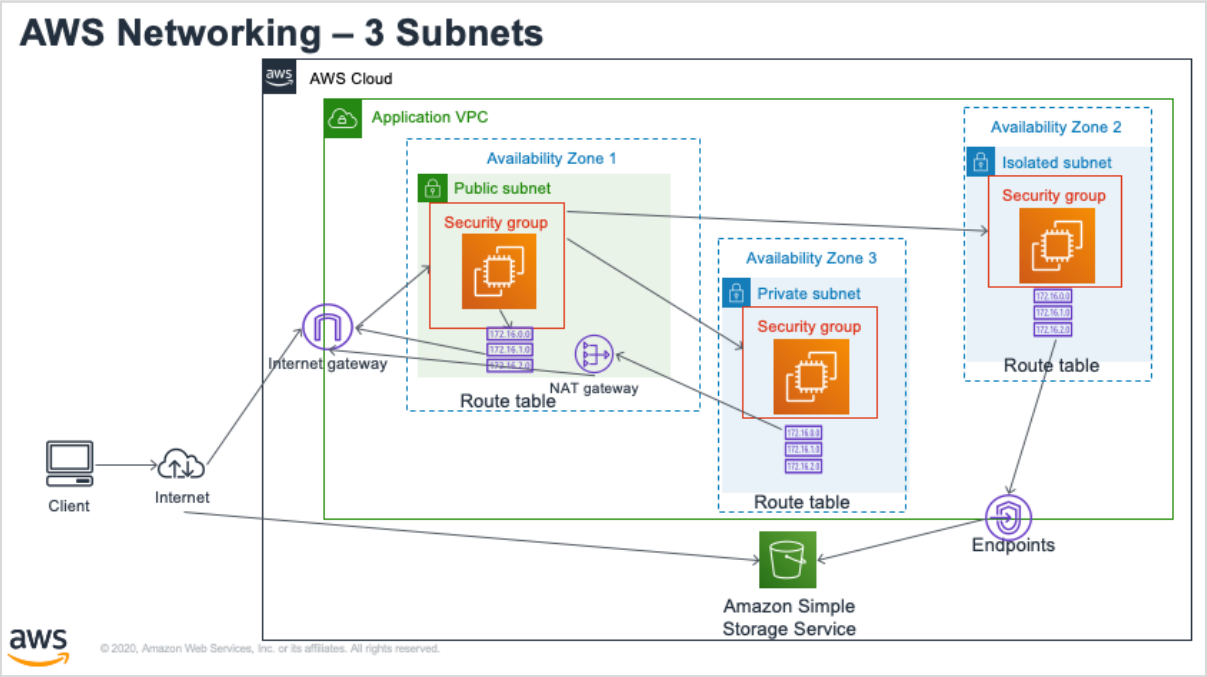
```
NOTE:  I have noticed that the Route Table is not always updated with the VPC Endpoint.  However, if you go to EC2 – it will allow for a yum update through S3.

Eventually the Route table is updated.
```

Go to Isolated EC2

- Go back to ssh window on isolated network
  - execute: `sudo yum update`
  - this works because yum packages are stored on s3

RECAP



REMOVE VPC

- Service: VPC
- Select VPC ➜ Actions ➜ Delete VPC
- You should see Warning for:
  - VPC Contains Instances
  - Network Interfaces (Associated with EC2 Instance)
  - Nat Gateways
- Remove NAT Gateway
- NAT Gateways ➜ Actions ➜ Delete NAT Gateway
- Terminate EC2 Instances
-