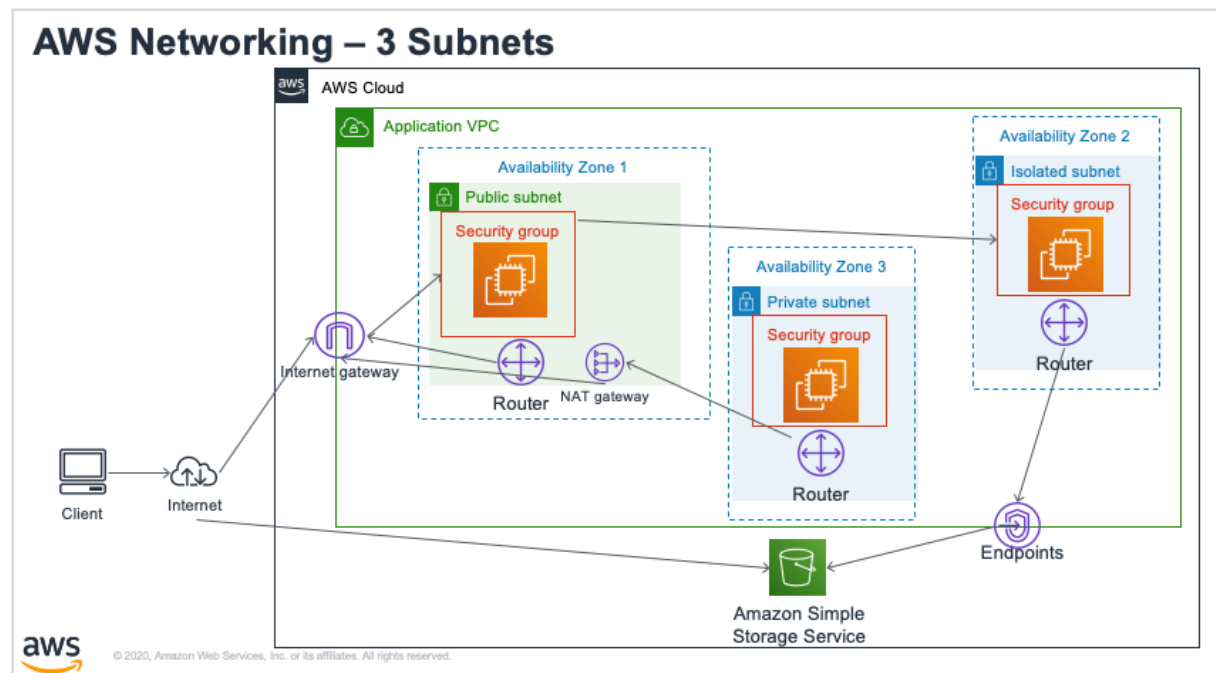


# AWS Networking - Lecture 44



## 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
- Router
- NAT Gateway
- Internet Gateway
- VPC Endpoints

## Public Subnet

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 a 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

The screenshot shows the 'Create VPC' page in the AWS Management Console. The breadcrumb navigation at the top reads 'VPC > Your VPCs > Create VPC'. The page title is 'Create VPC' with an 'Info' link. Below the title is a descriptive sentence: 'A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.'

The 'VPC settings' section contains the following fields and options:

- Name tag - optional:** A text input field with the value 'pryan-test-vpc'. Below it is a small text: 'Creates a tag with a key of 'Name' and a value that you specify.'
- IPv4 CIDR block:** A text input field with the value '10.10.0.0/16'. Below it is a small text: 'Info'.
- IPv6 CIDR block:** Three radio button options: 'No IPv6 CIDR block' (selected), 'Amazon-provided IPv6 CIDR block', and 'IPv6 CIDR owned by me'. Below them is a small text: 'Info'.
- Tenancy:** A dropdown menu with 'Default' selected. Below it is a small text: 'Info'.

The 'Tags' section contains a table of tags:

Key	Value - optional	
Name	pryan-test-vpc	Remove
CreatedBy	pat.ryan@spr.com	Remove
CreatedOn	2020-11-09	Remove
Project	Internal	Remove

Below the table is a button 'Add new tag' and a note: 'You can add 46 more tags.'

At the bottom of the form are two buttons: 'Cancel' and 'Create VPC'.

- name
- CIDR Block
  - 10.100.0.0/16
    - Note that students will have to pick a different cidr range.

- I suggest 10.<studentid>.0.0/16
- Add tags

## Create Subnets

Subnets > Create subnet

### Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC\*

Availability Zone

VPC CIDRs	CIDR	Status	Status Reason
	10.10.0.0/16	associated	

IPv4 CIDR block\*

\* Required

Cancel Create

- 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.

## Create Internet Gateway

- select 'Internet Gateways' in left nav

Internet gateway successfully deleted - igw-09918d3fd3cb92851

### Internet gateways (8) [Info](#)

Filter internet gateways

	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	mu-e8-vpc-accepta...	igw-06a8f4a359f0ea69e	Attached	vpc-0c878c3b1903acea5   mu-e8-vpc...	485071734
<input type="checkbox"/>	mu-e8-vpc-product...	igw-08079e2b3059e749f	Attached	vpc-06b28bd22e8812044   mu-e8-vp...	485071734
<input type="checkbox"/>	-	igw-08adacf2eb8889c8f	Attached	vpc-050a4074112c66973   deepracer...	485071734
<input type="checkbox"/>	-	igw-0e7413935d0037e0b	Attached	vpc-05b110651cd5cf847   Cloudform...	485071734
<input type="checkbox"/>	Default-Internet-Ga...	igw-1059aa68	Attached	vpc-eba67190   Default-VPC	485071734
<input type="checkbox"/>	Sandbox-Internet-...	igw-7a107e02	Attached	vpc-0e336975   Sandbox-VPC	485071734
<input type="checkbox"/>	-	igw-d06b1da8	Attached	vpc-3b2e0240   Workspaces-VPC	485071734
<input type="checkbox"/>	-	igw-e0397798	Attached	vpc-e92e2c92	485071734

Select an internet gateway above

**Create internet gateway** [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

**Internet gateway settings**

**Name tag**  
Creates a tag with a key of 'Name' and a value that you specify.

pryan-test-igw

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
Name	pryan-test-igw	Remove
CreatedBy	pat.ryan@spr.com	Remove
CreatedOn	2020-11-09	Remove
Project	Internal	Remove

[Add new tag](#)  
You can add 46 more tags.

[Cancel](#) [Create internet gateway](#)

- 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

AWS Services

pat.ryan @ spr2 N. Virginia Support

New VPC Experience  
Tell us what you think

VPC Dashboard **New**

Filter by VPC:  
Select a VPC

**VIRTUAL PRIVATE CLOUD**

- Your VPCs **New**
- Subnets
- Route Tables
- Internet Gateways **New****
- Egress Only Internet Gateways **New**
- Carrier Gateways **New**
- DHCP Options Sets **New**
- Elastic IPs **New**
- Managed Prefix Lists **New**
- Endpoints
- Endpoint Services
- NAT Gateways **New**
- Peering Connections

**SECURITY**

- Network ACLs
- Security Groups **New**

**VIRTUAL PRIVATE NETWORK (VPN)**

- Customer Gateways
- Virtual Private Gateways
- Site-to-Site VPN Connections
- Client VPN Endpoints

**TRANSIT GATEWAYS**

- Transit Gateways
- Transit Gateway Attachments
- Transit Gateway Route Tables

The following internet gateway was created: igw-0c626d342d06a7daf. You can now attach to a VPC to enable the VPC to communicate with the internet. **Attach to a VPC**

VPC > Internet gateways > igw-0c626d342d06a7daf

**igw-0c626d342d06a7daf / pryan-test-igw** **Actions**

**Details** **Info**

Internet gateway ID igw-0c626d342d06a7daf	State Detached	VPC ID -	Owner 485071734737
--	-------------------	-------------	-----------------------

**Tags** **Manage tags**

Search tags

Key	Value
CreatedOn	2020-11-09
Project	Internal
Name	pryan-test-igw
CreatedBy	pat.ryan@spr.com

Feedback English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- Select your VPC and press, 'Attach internet gateway'

[VPC](#) > [Internet gateways](#) > Attach to VPC (igw-0c626d342d06a7daf)

## Attach to VPC (igw-0c626d342d06a7daf) [info](#)

### VPC

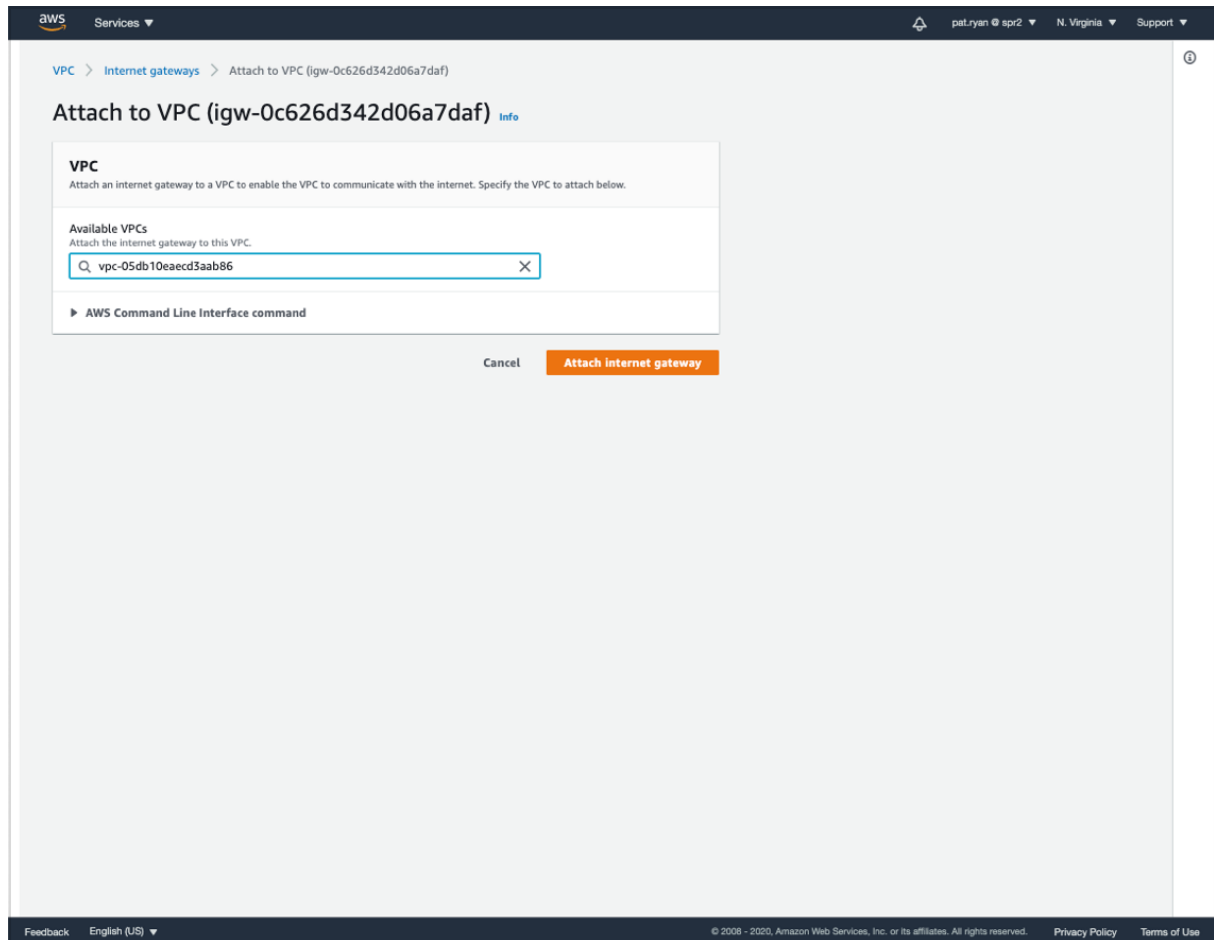
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

#### Available VPCs

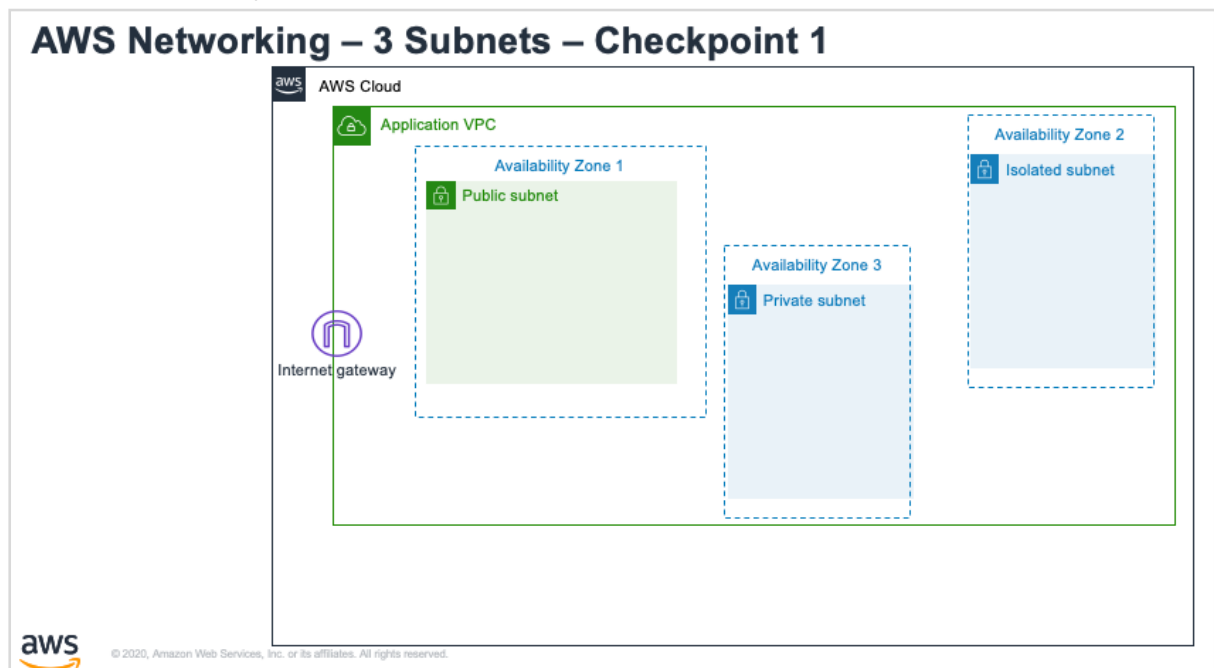
Attach the internet gateway to this VPC.

vpc-05db10eaecd3aab86 - pryan-test-vpc
vpc-0c05262b7172b12d1
vpc-0b722cefb6a7e2f8

[Cancel](#)[Attach internet gateway](#)



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





## Create Public Router

- 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 vpc
- 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'
-

Route Tables > Create route table

## Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

**Name tag**

**VPC\***

Key (128 characters maximum)	Value (256 characters maximum)
CreateBy	pat.ryan@spr.com
CreatedOn	2020-11-09
Project	Internal

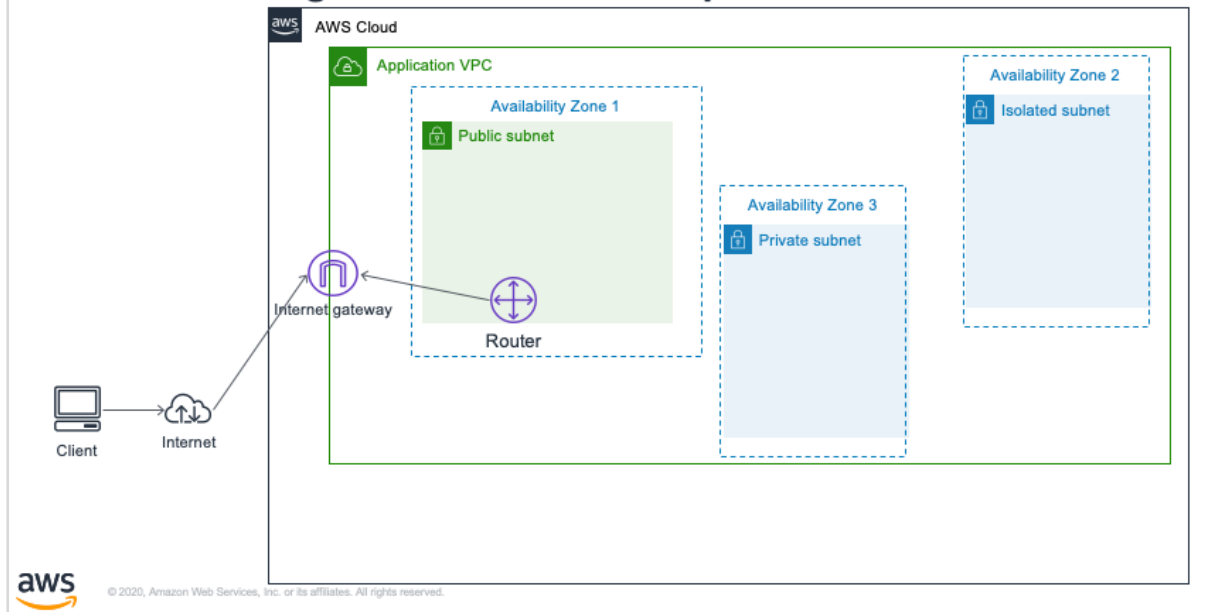
**Add Tag** 47 remaining (Up to 50 tags maximum)

\* Required

[Cancel](#) [Create](#)

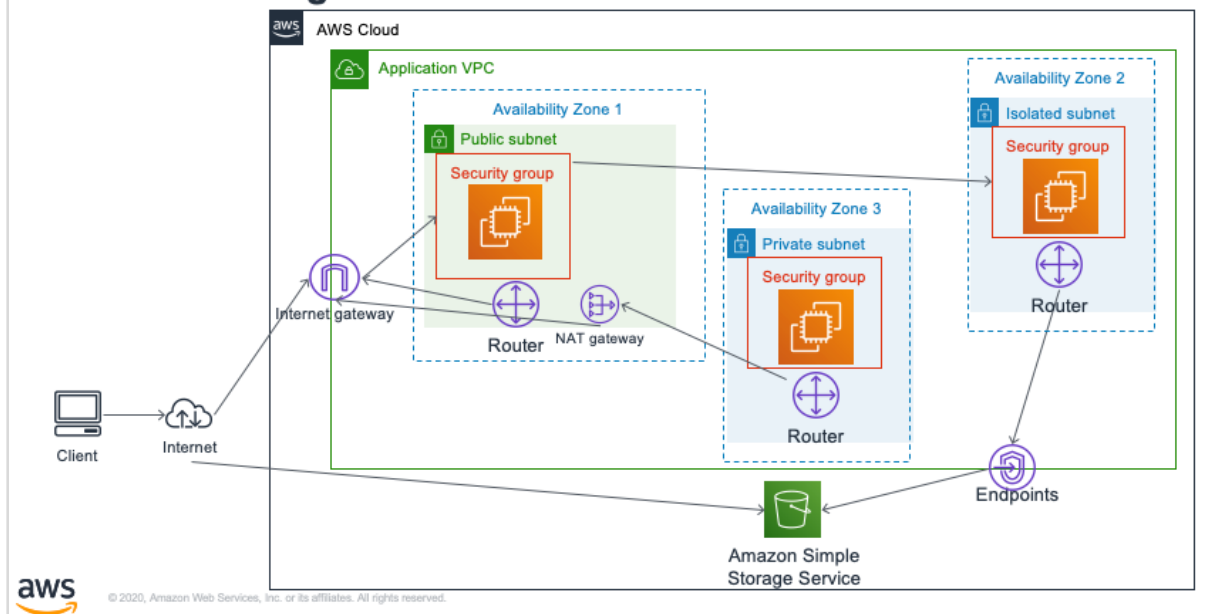
- At this point we have a new route table, but we have NOT associated it with a subnet yet
- Select 'Subnets' left nav
- Select your public subnet
- Select 'Route Table' below
- Select 'Edit route table association'
- In DropDown select new route table
  - It should show the routes, one being to IGW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

## AWS Networking – 3 Subnets – Checkpoint 2



- Remember the ultimate network architecture

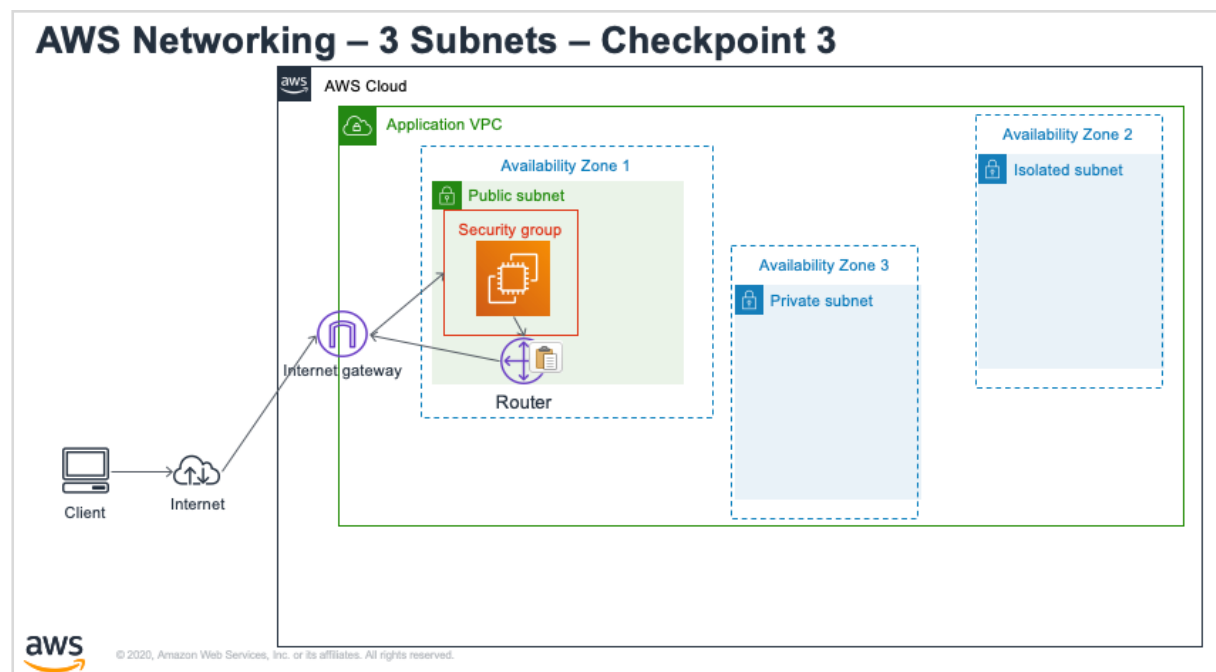
## AWS Networking – 3 Subnets



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

## 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

The diagram illustrates a multi-availability zone AWS Cloud architecture designed for high availability and disaster recovery. The architecture is organized as follows:

- AWS Cloud:** The overall environment, represented by the top-level box.
- Application VPC:** A Virtual Private Cloud containing all the resources.
- Availability Zones:** Three distinct Availability Zones are shown, each represented by a dashed blue box.
  - Availability Zone 1:** Contains a **Public subnet** (green box) with a **Security group** (orange box with a server icon). It also contains a **Router** (purple circle with a cross) and a **NAT gateway** (purple circle with a cross).
  - Availability Zone 2:** Contains an **Isolated subnet** (blue box) with a **Security group** (orange box with a server icon). It also contains a **Router** (purple circle with a cross).
  - Availability Zone 3:** Contains a **Private subnet** (blue box) with a **Security group** (orange box with a server icon). It also contains a **Router** (purple circle with a cross).
- Internet Gateway:** A purple circle with a cross, located in Availability Zone 1. It connects the public subnet to the Internet.
- Endpoints:** A purple circle with a cross, located in Availability Zone 2. It connects the isolated subnet to the Amazon Simple Storage Service.
- Amazon Simple Storage Service:** A green box with a server icon, located in Availability Zone 3. It is the target for data storage.
- Client:** A computer icon on the left, representing the user or application.
- Internet:** A cloud icon in the center, representing the public Internet.

**Connections and Flow:**

- The **Client** connects to the **Internet**.
- The **Internet** connects to the **Internet Gateway** in Availability Zone 1.
- The **Internet Gateway** connects to the **Public subnet** in Availability Zone 1.
- The **Public subnet** connects to the **Router** in Availability Zone 1.
- The **Router** in Availability Zone 1 connects to the **NAT gateway** in Availability Zone 1.
- The **NAT gateway** connects to the **Private subnet** in Availability Zone 3.
- The **Private subnet** connects to the **Router** in Availability Zone 3.
- The **Router** in Availability Zone 3 connects to the **Endpoints** in Availability Zone 2.
- The **Endpoints** connect to the **Amazon Simple Storage Service**.
- The **Isolated subnet** in Availability Zone 2 also connects to the **Amazon Simple Storage Service**.

- ## Add a NAT Gateway

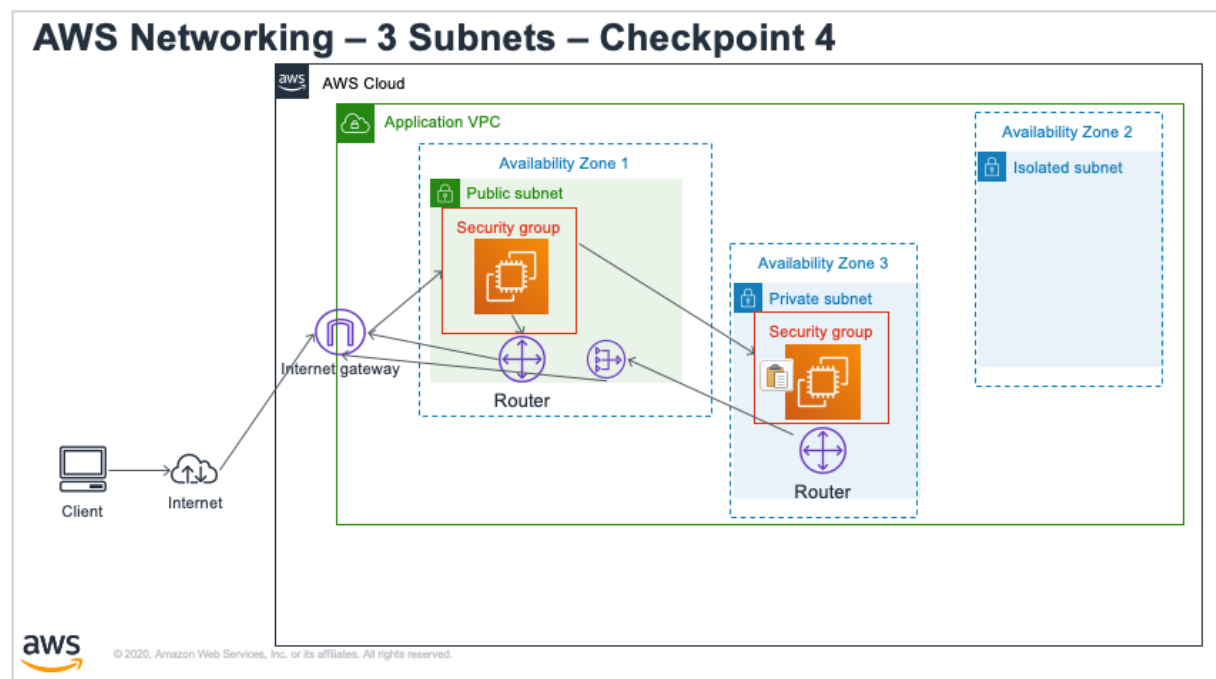
- ## Create EC2 in Private Subnet

- 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

## 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

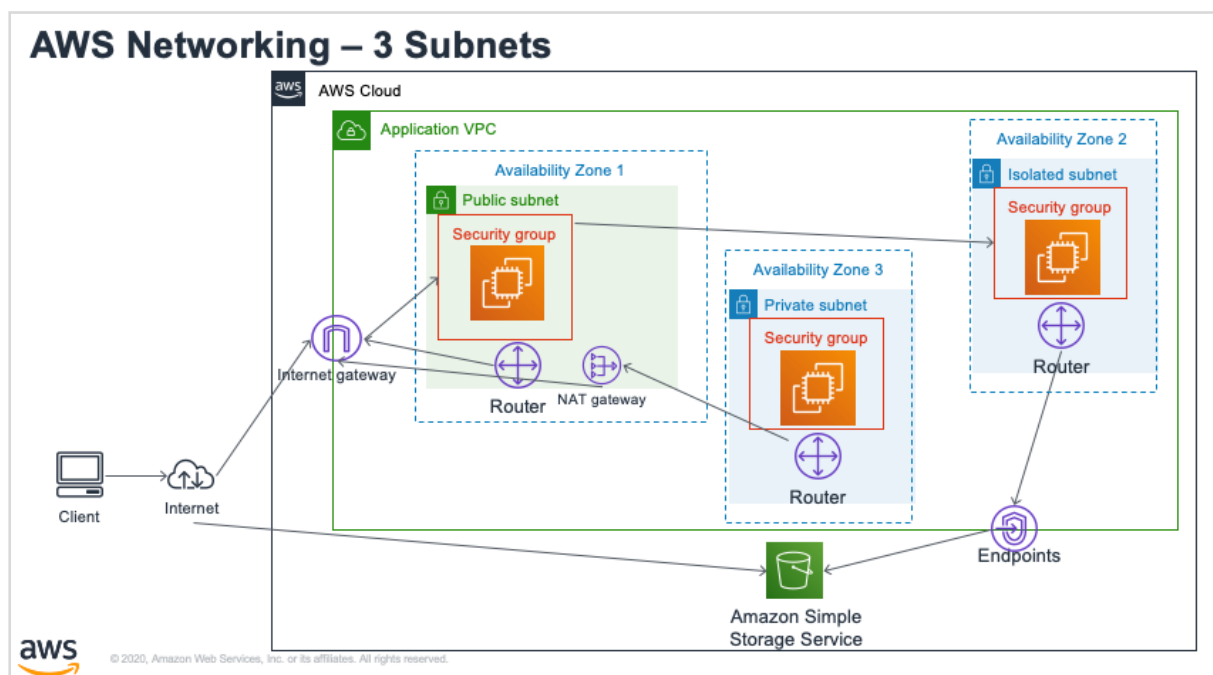
- Review Private EC2 Settings
- STOP: CHECKPOINT



- 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
  - You might for a DB server. The only access to the DB server, is internal to the VPC
- 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`
- 

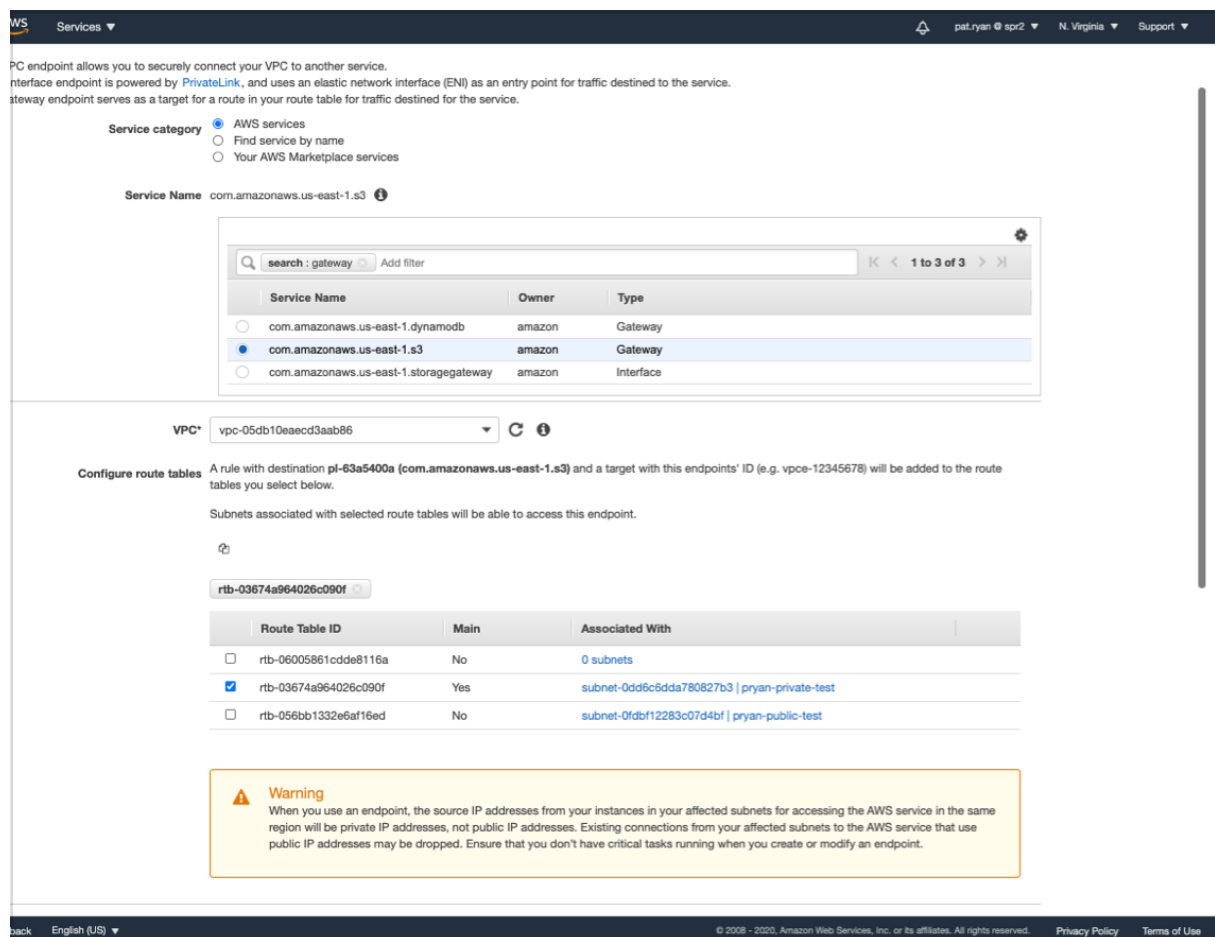
## Create Route table for isolated subnet

- 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'



VPC endpoint allows you to securely connect your VPC to another service. The interface endpoint is powered by [PrivateLink](#), and uses an elastic network interface (ENI) as an entry point for traffic destined to the service. A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

**Service category**

- ☒ AWS services
- ☐ Find service by name
- ☐ Your AWS Marketplace services

**Service Name** `com.amazonaws.us-east-1.s3`

search: gateway Add filter 1 to 3 of 3

Service Name	Owner	Type
<input type="radio"/> com.amazonaws.us-east-1.dynamodb	amazon	Gateway
<input checked="" type="radio"/> com.amazonaws.us-east-1.s3	amazon	Gateway
<input type="radio"/> com.amazonaws.us-east-1.storagegateway	amazon	Interface

**VPC** `vpc-05db10eaecd3aab86`

**Configure route tables** A rule with destination `pl-63a5400a` (`com.amazonaws.us-east-1.s3`) and a target with this endpoints' ID (e.g. `vpce-12345678`) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

`rtb-03674a964026c090f`

Route Table ID	Main	Associated With
<input type="checkbox"/> rtb-06005861cdde8116a	No	0 subnets
<input checked="" type="checkbox"/> rtb-03674a964026c090f	Yes	subnet-0dd6cdda780827b3   pryan-private-test
<input type="checkbox"/> rtb-056bb1332e6af16ed	No	subnet-0fdbf12283c07d4bf   pryan-public-test

**Warning**

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

- select you vpc
- add it to the route table associated with the subnet
- this might take a moment.
- Go back to ssh window on isolated network
  - execute: `sudo yum update`



- this works because yum packages are stored on s3

## RECAP

