Amazon AWS (http://www.studytrails.com/category/amazon-aws/)

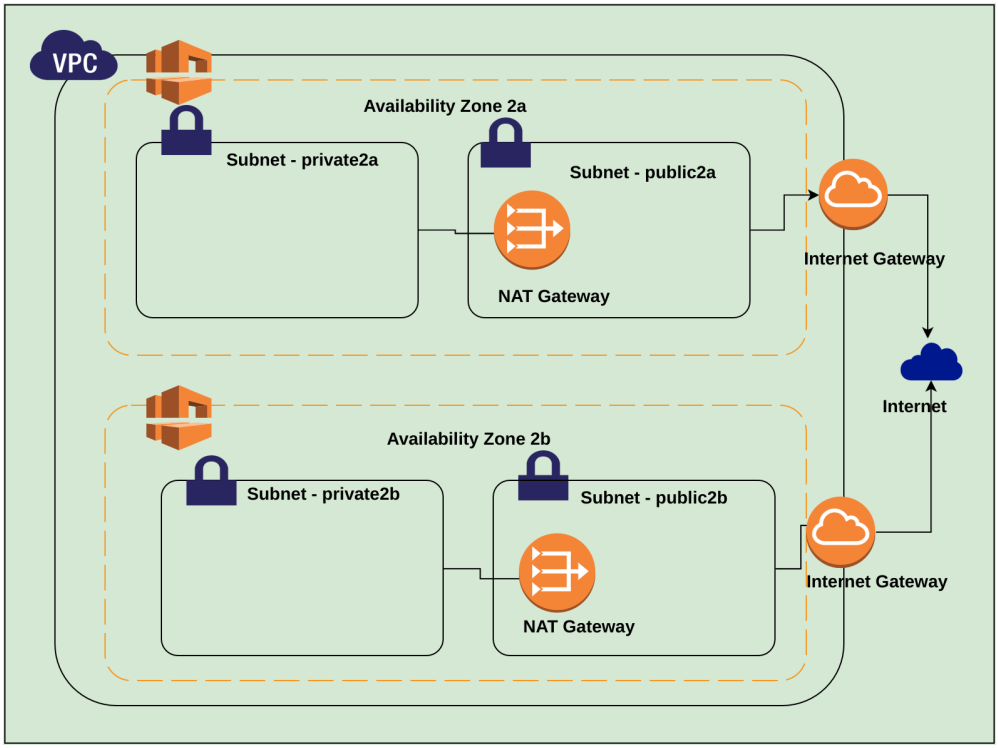
AWS VPC Tutorial – Part II subnets

November 25, 2016 (http://www.studytrails.com/amazon-aws/aws-vpc-tutorial-part-ii-subnets/) Mithil Shah (http://www.studytrails.com/author/user/) 0 Comment (http://www.studytrails.com/amazon-aws/aws-vpc-tutorial-part-ii-subnets/#respond)

In this AWS VPC tutorial, we will look at how to create the VPC, public and private subnets, route table, and an internet gateway.

AWS VPC Tutorial – Recap

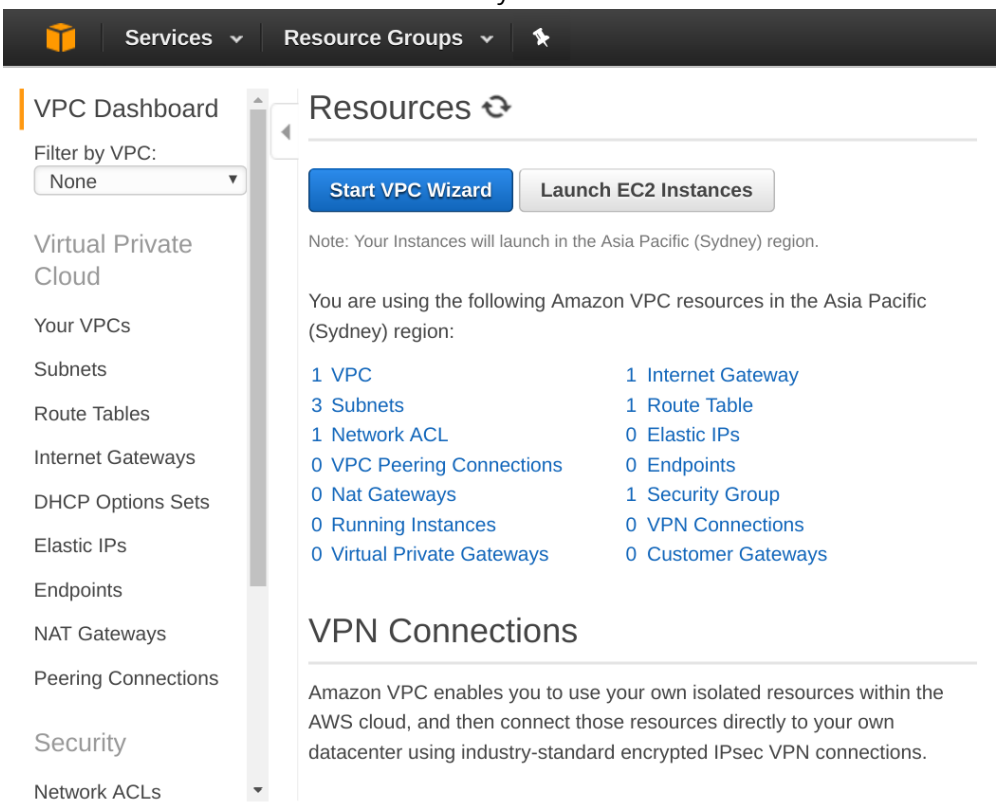
In the previous (http://www.studytrails.com/amazon-aws/aws-vpc-tutorial/) tutorial we saw an introduction to Amazon VPC and also looked at the key concepts in VPC. Here's the diagram of what we are trying to accomplish



(http://www.studytrails.com/wp-content/uploads/2016/11/VPCTutorial.png)
We begin by creating the VPC.

AWS VPC tutorial – creating VPC

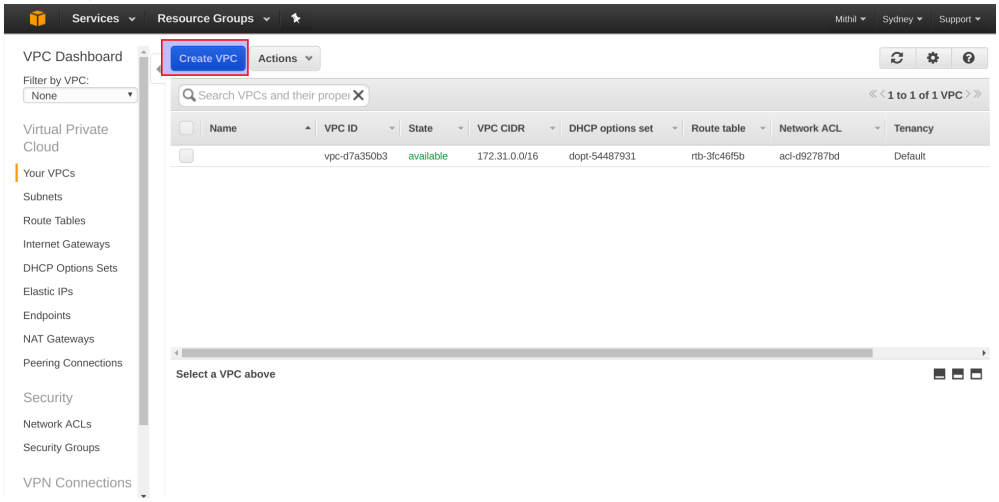
We will look at how to create the VPC using the AWS management console. Login to the console and click on VPC. This is what you should see:



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_239.png)
We will not be using the Wizard since we want to learn the inner workings of the VPC. Click on the link that says '1 VPC'. If you havent created a VPC before, you should still see 1 VPC which is the default that AWS creates for you. In the next

5. Amazon AWS VPC Introduction and Features (http://www.studytrails.com/amazon-aws/amazon-aws-vpc-tutorial/)
6. Amazon S3 Bucket – Creation, Lifecycle, Version, Access (http://www.studytrails.com/amazon-aws/amazon-s3-bucket-creation-lifecycle-version-access/)
7. Create AWS EC2 instance using CLI (http://www.studytrails.com/amazon-aws/create-aws-ec2-instance-using-cli/)
8. Amazon Elastic Cloud Compute (EC2) – Creating an Instance (http://www.studytrails.com/amazon-aws/amazon-elastic-cloud-compute-ec2-creating-an-instance/)
9. Amazon Elastic Cloud Compute (EC2) – Introduction (http://www.studytrails.com/amazon-aws/amazon-elatics-cloud-compute-ec2-creating-instance/)
10. Mount Amazon Elastic File System (EFS) to EC2 (http://www.studytrails.com/amazon-aws/mounting-amazon-elastic-file-system-efs-ec2/)

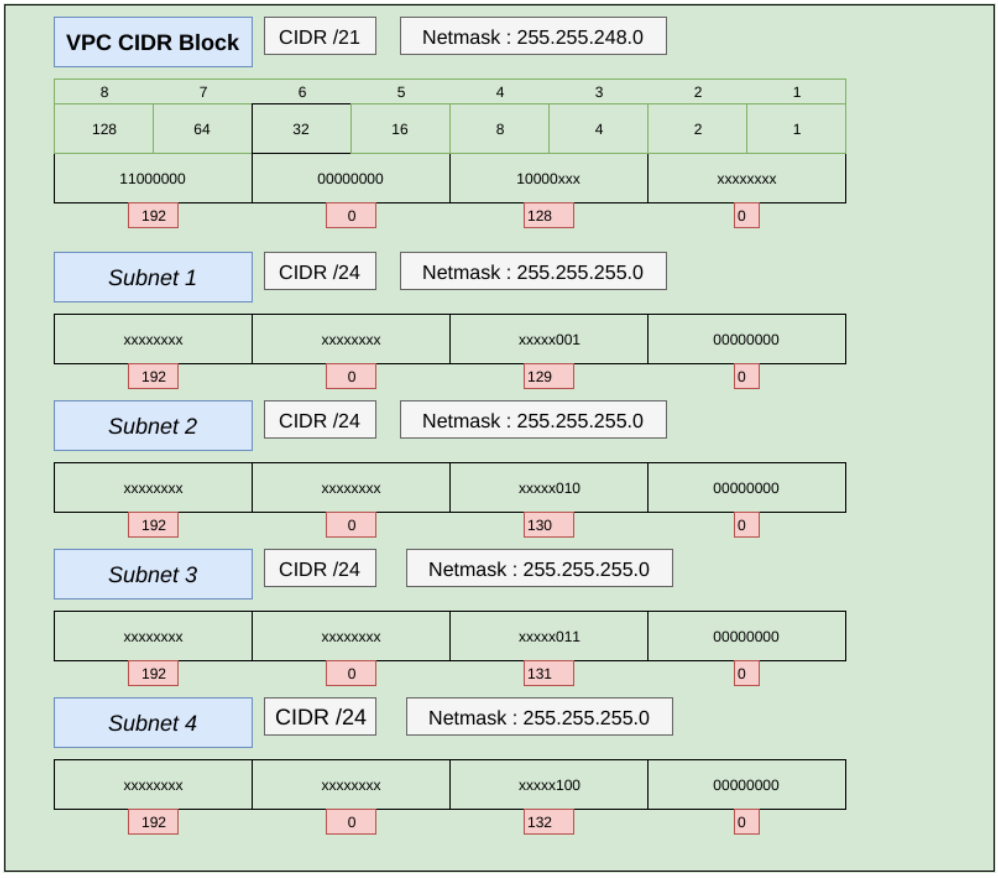
screen you should see that one VPC and a button to 'Create VPC'



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_240.png)

Creating CIDR block for VPC and Subnets

When you click 'Create VPC', you should see a popup where you can enter the VPC name and a CIDR block. This CIDR block determines the range of IP addresses that your VPC can have. It also specifies the network part of the IP addresses and the subnet mask. Here's how our VPC and the subnets in the VPC will look like.

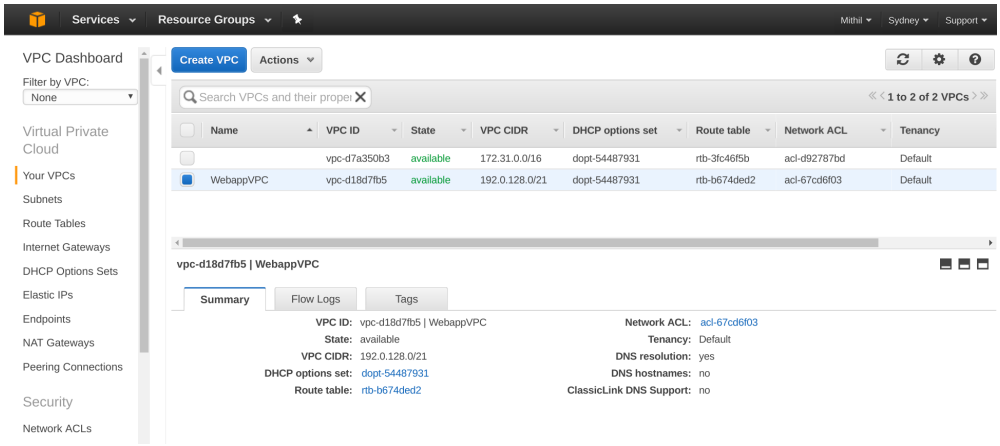


(http://www.studytrails.com/wp-content/uploads/2016/11/Subnets.png)

CIDR block for the AWS VPC

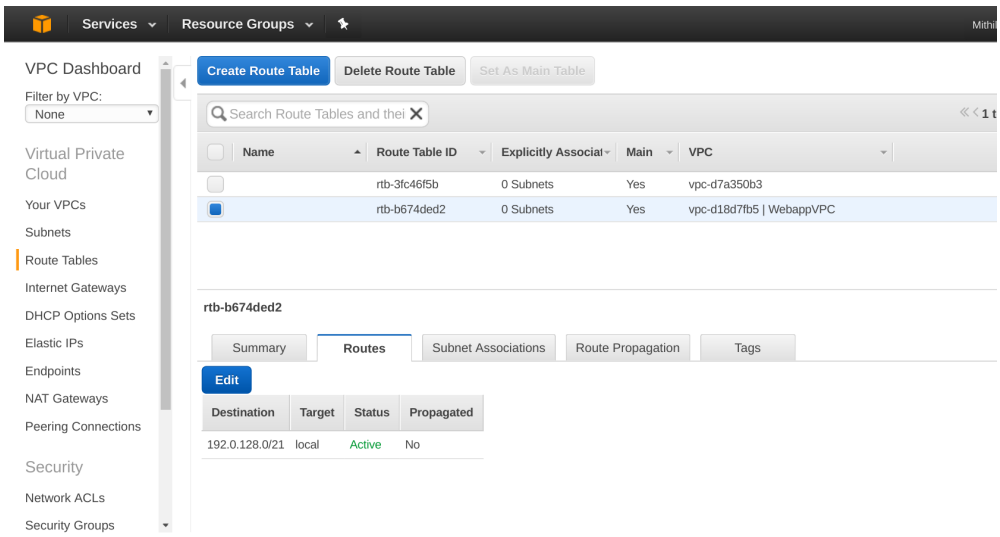
We create a CIDR block keeping in mind the number of IP addresses that we want in our VPC. In this example, we have chosen a CIDR block of 192.0.128.0/21 . What this means is that the first 21 bits of the 32 bits that form the IP address are part of

the network. The remaining bits (11) are for the IP addresses in the VPC. Hit 'yes, Create' and it should create the VPC for you. When it creates the VPC it also creates a default route table and a default network ACL.



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_242.png)

The default Route table allows access to instances within the VPC. It does not allow access to instances outside the VPC.



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_243.png)

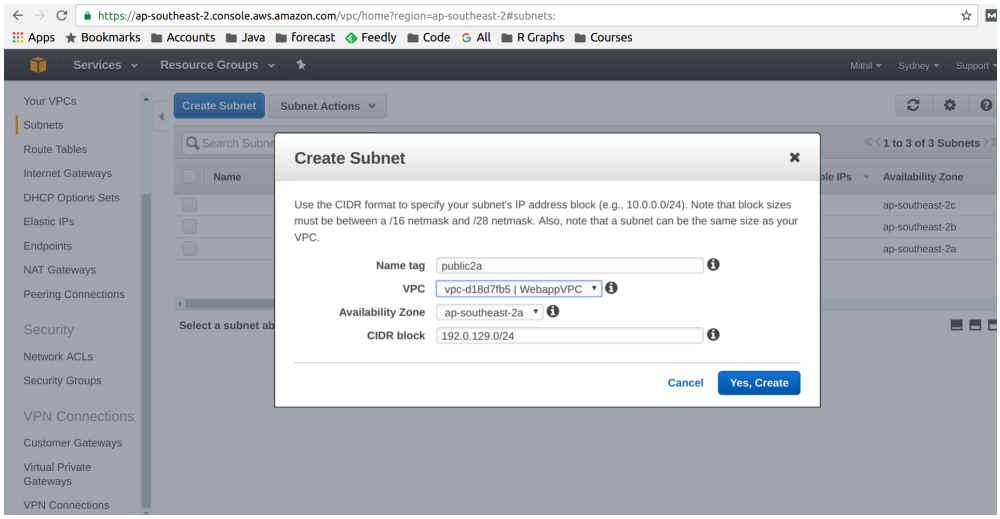
What is network ACL

VPC has two layers of security: security groups and network ACLs. Security Group can be allowed to modify permission any instance that it is attached to. ACLs, on the other hand, are applicable for the whole subnet that they are attached to. Also, ACL's are stateless so the rules for inbound and outbound traffic are separate. Amazon recommends using security groups as the first choice. The screenshot below shows the default ACL that allows all inbound traffic within the subnet.

Creating an AWS VPC Subnet Group

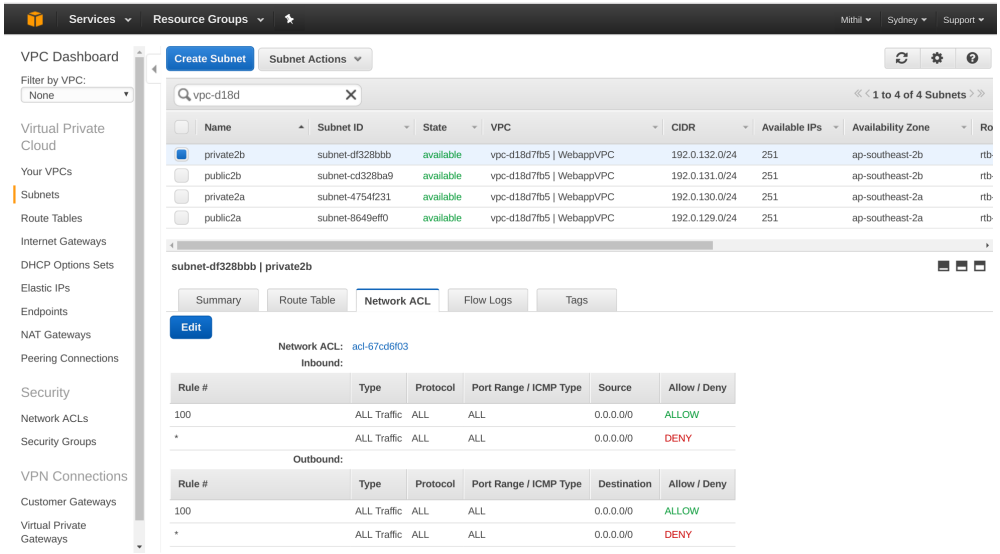
As shown in our network diagram, we will create four subnets spanning two Availability Zones(AZ). Each AZ will have one private and one public subnet. The idea is that if one AZ goes down, our system still works. Let's say, you are creating a web server, an application server and an RDS instance. We will have the RDS instance and the application server in the private subnet and the web server in the public subnet. This setup will be replicated in both AZ. We use a CIDR block of

129.0.12.0/24 for the first subnet. This would give us 251 usable IPs. Amazon reserves 5 addresses.



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_245.png)

We similarly create the other three subnets.



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_246.png)

Creating an AWS Internet Gateway

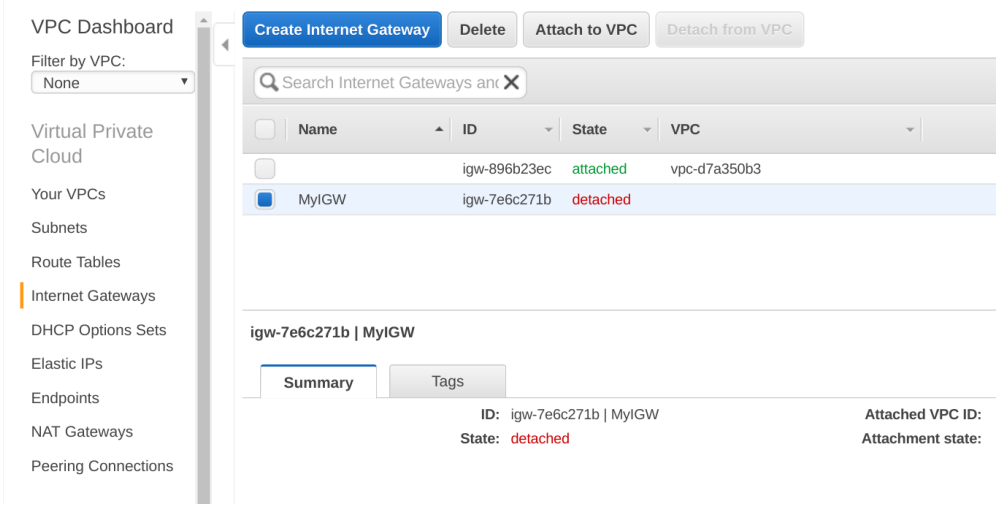
Two out of four of our Subnets are public. We need a gateway that allows the instances and services from the public subnet to access the internet. Here's how we create the gateway: click on the link on the left that says 'Internet Gateways'

(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_247.png)

We call it 'MyIGW'.

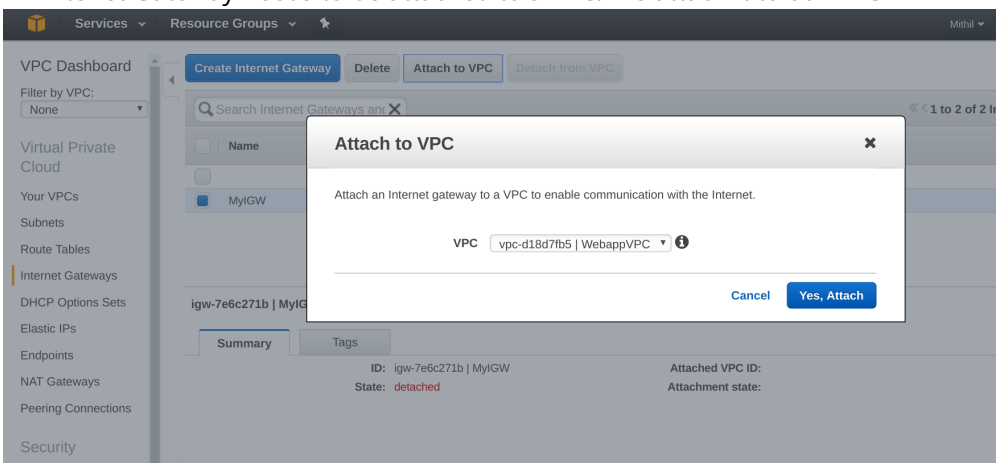
Attaching an internet gateway to a VPC

When you create a new gateway it is in a detached state.



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_251.png)

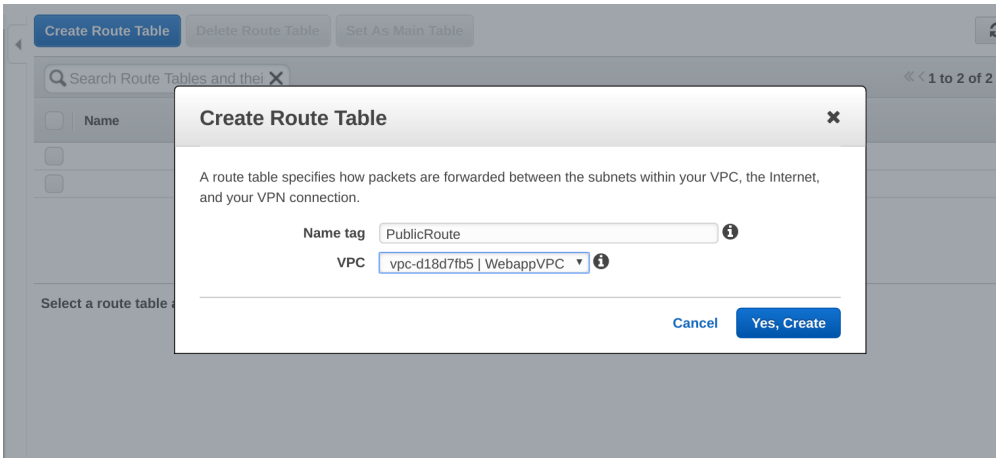
An Intenet Gateway needs to be attached to a VPC. We attach it to our VPC



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_252.png)

Adding route to a VPC

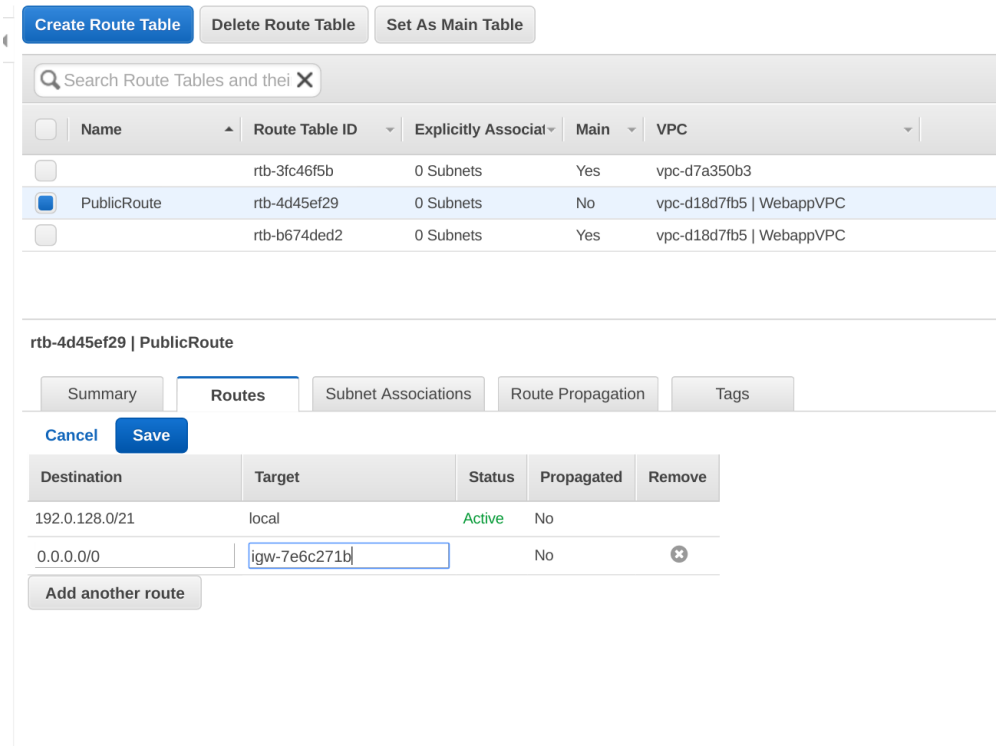
We will now create a new route table that allows instances inside a subnet to direct all traffic to the Internet gateway so that the gateway can direct it out to the internet. Click on 'Route Table' link on the left and then click on 'Create Route Table'



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_254.png)

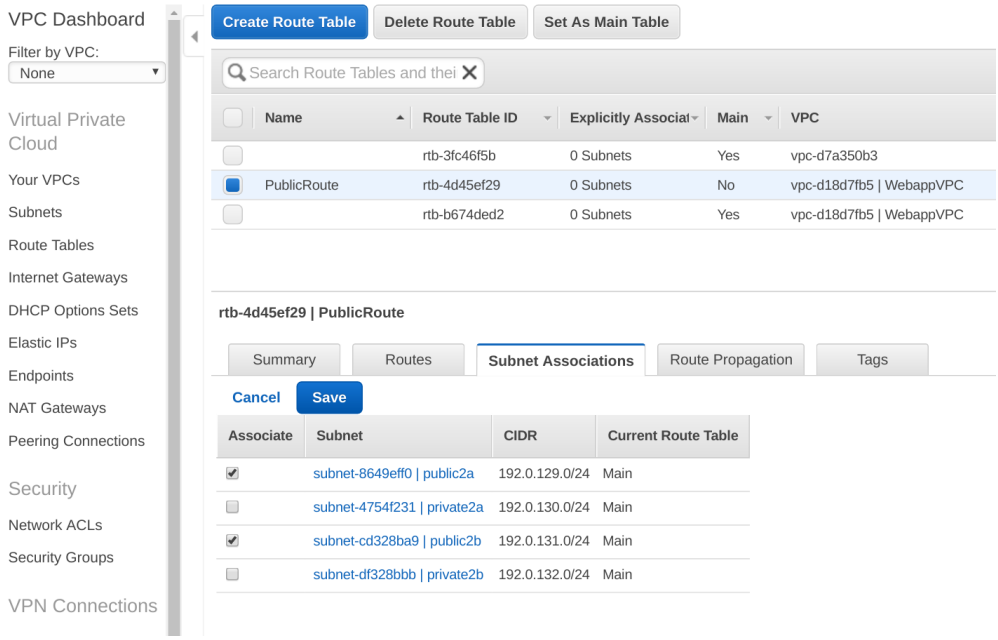
Add a new route that redirects all traffic (0.0.0.0/0) to the internet gateway that we

created



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_255.png)

As the last step we assign this route table to the subnets that we want to be public



(http://www.studytrails.com/wp-content/uploads/2016/11/Selection_256.png)

This finishes the second part of the tutorial. In the third and the last part we will look at how to create an Elastic IP address and assign that address to a NAT gateway so that instances in the private subnet can talk to the internet.

← AWS VPC Tutorial – Part I Introduction
(http://www.studytrails.com/amazon-aws/aws-vpc-tutorial/)