AWS Networking

Let’s work through the big architectural diagram below as it relates to what we’ve learnt so far about launching VPC.

Graphical user interface

Description automatically generated

**Region the geographical location of your network**

So the first thing you'll want to do when you want to launch AWS resources, is to choose a region to launch them in and so a region is a geographical location of your network. So that could be US East one, which is North Virginia, or maybe you would choose Canada Central which is based on Montreal. In class we were advised to use N. Virginia. Once you've decided what region you want to launch resources in, you're going to need a VPC.

**VPC**

VPC stands for virtual private cloud, it is a logic isolated section of the AWS Cloud, it’s a slice of the AWS network just for you. And then once you have your VPC you're going to want to subdivide it up into subnets.

**Subnets a logical partition of an IP network into multiple, smaller network segments**

So, you could have public and private subnets the difference between a public and a private subnet is that the public one is generally accessible to the internet, whereas a private subnet as Dr Lucky would say, it’s like your private room in your apartment while the public is you living room(parlor). So when you have things that need to be super secure you're going to put Those in your private subnet. Yes o! And so, subnets are defined within an availability zone.

**Availability Zones (AZs)**

AZ is just a data center, from where you're going to launch your AWS resources. Those AZs are contained or are specific to specific regions. Now we have a region, we have a VPC, we have our subnets and so we can go ahead and start launching resources into our subnets.

We could launch an EC2 instance or an RDS instance. So how is that instance going to reach the internet? In order to do so we're going to need a gateway to the internet and that's where internet gateway comes into play.

**Internet Gateway**

Internet Gateway enables access to the internet. You can think of it as a door to the internet from your VPC outward. You remember Dr Lucky referred to it as front facing, but just having internet gateway is not enough because the subnet has to know how to reach that internet gateway to route the internet. and that's where a route tables come in.

**Route Tables**

Route tables determine where network traffic from your subnets is directed. You'd create a a route and your route table direct traffic, like a traffic Warden it says go here and go out to the Internet. Now that we have a way to the internet and we can launch our resources into our subnets. What about security and that's where security groups and NACLs are going to come in.

**Security groups**

Security groups are access to firewall at the instance level. In the above diagram you can see that we have an EC2 instance and RDS and they span subnets. We have a border drawn around it to say that the security group is protecting those two instances.

NACLs

NACLs is another form of security but it's at the subnet level, so it sits in front of subnets and controls access in and out of those.