AWS LAB

Create my Virtual Private Cloud (VPC) to produce customized network.

VPC will contain a Public Subnet and a Private Subnet, each subnet with 1 EC2 instance

Purpose: pink to google.com from the EC2 located in the Private Subnet

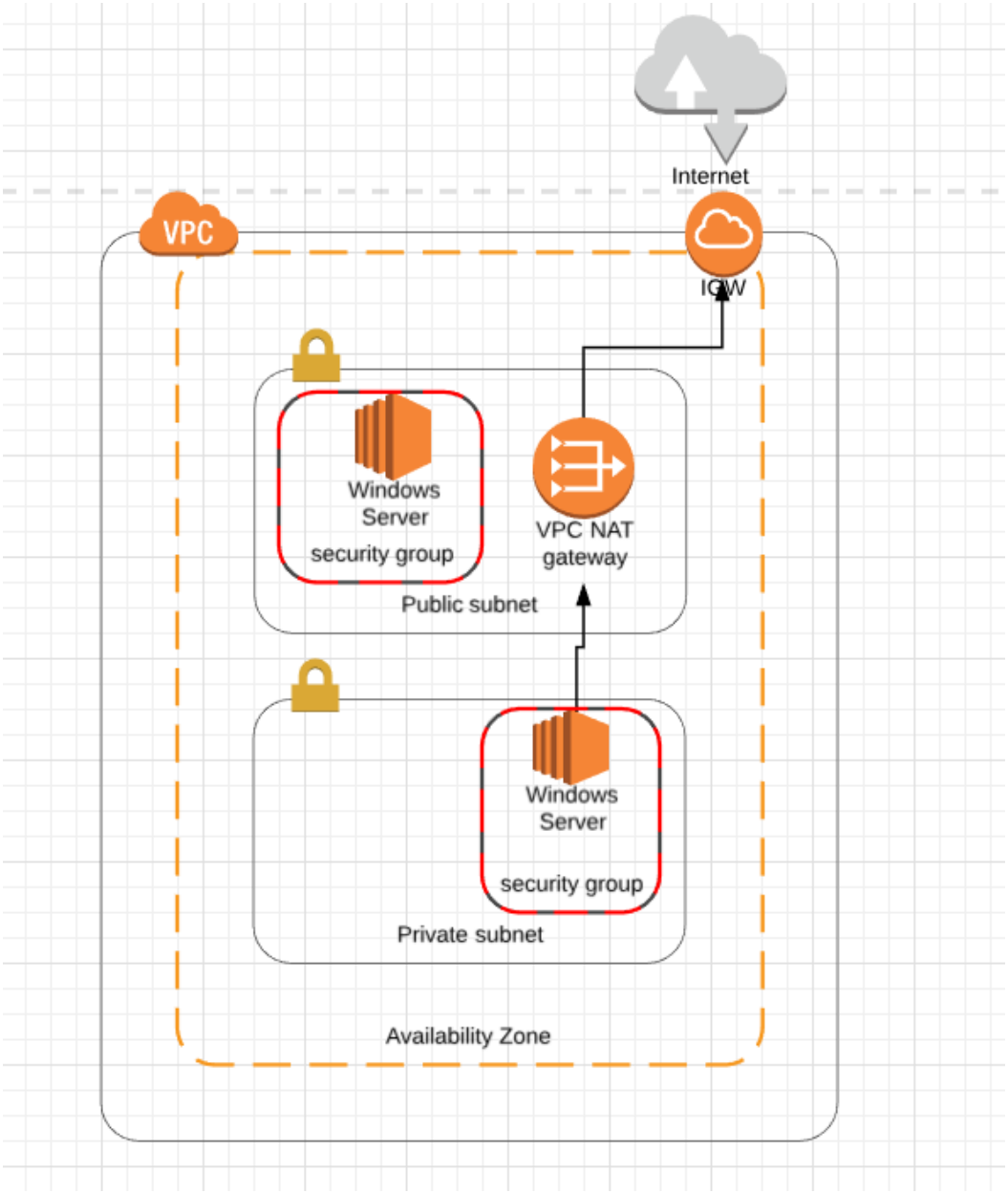
For this, a NAT Gateway will be configured in the public subnet.

Private subnet traffic should be routed through the NAT instance or Gateway for Internet access.

The IGW allows communication between instances in my VPC and Internet

Even if it is recommended to start with at least 2 Availability Zones, for this Lab I will use only 1, to simplify

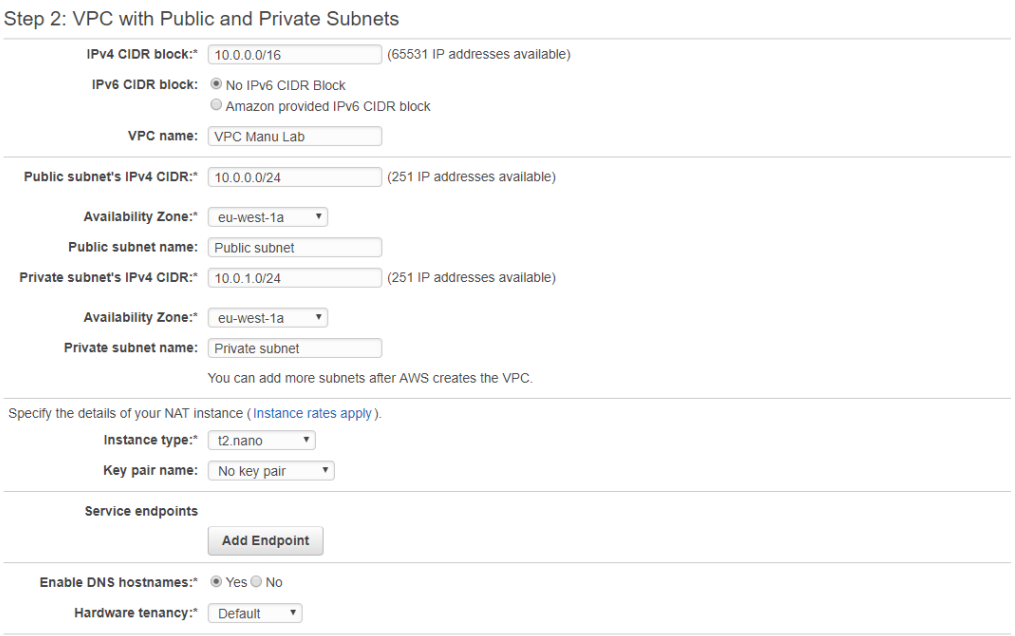
Here is what looks like my Infrastructure:



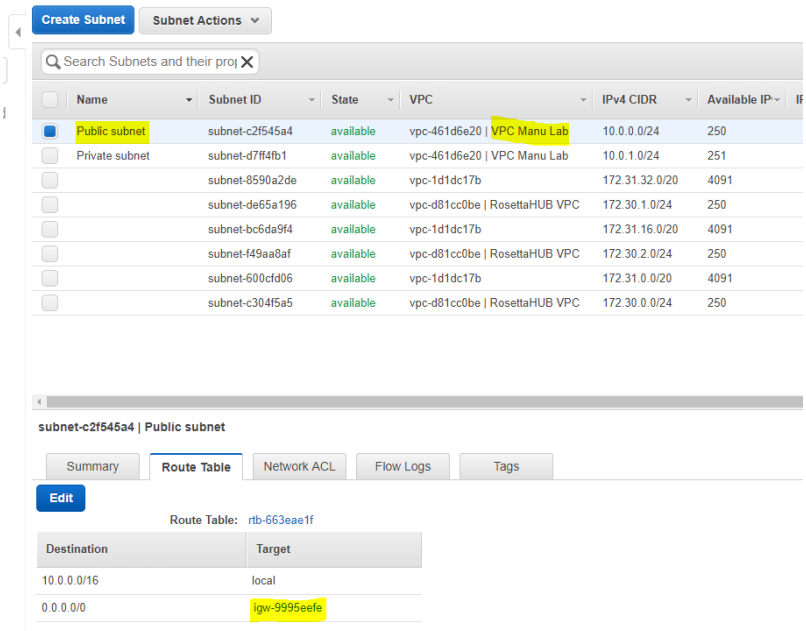
AWS Console

- **VPC -> Start VPC Wizard**

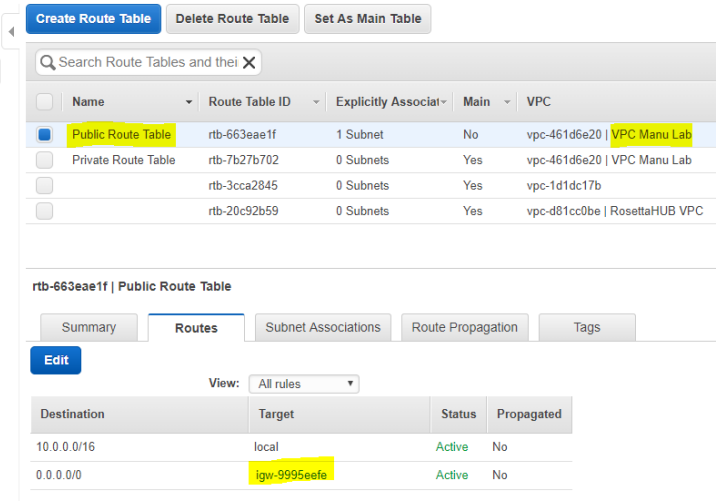
Select VPC Configuration: VPC with Public and Private Subnets, in the same ZA



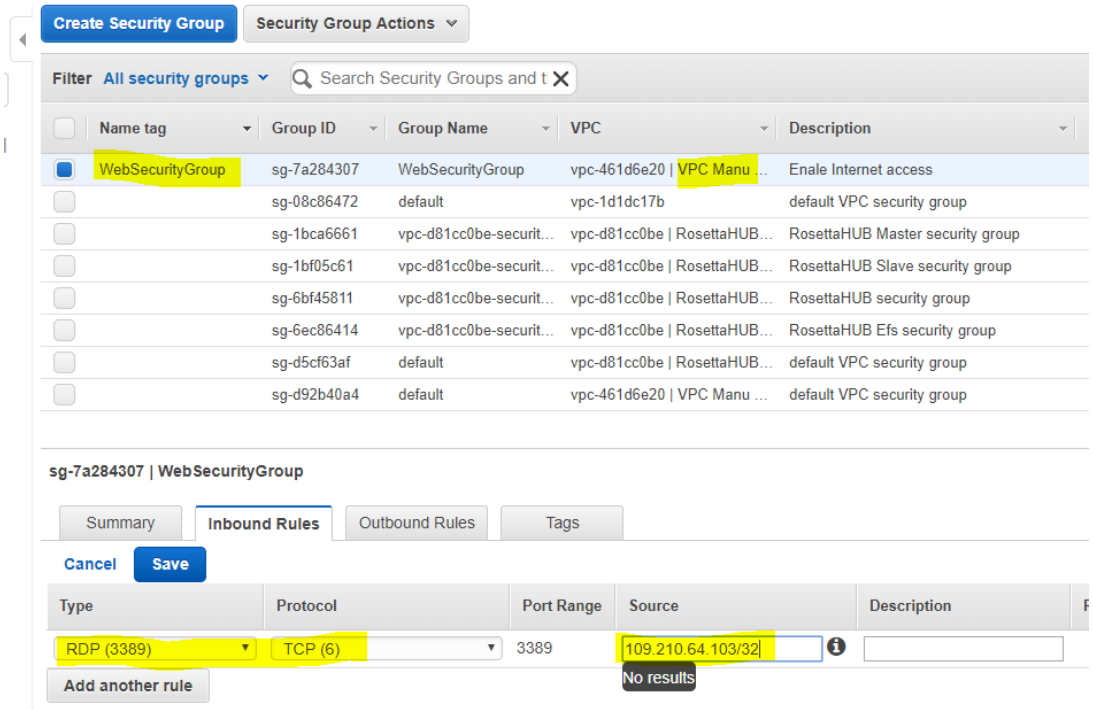
At this step, we have “VPC Manu Lab” created with the 2 Subnets: one Public, one Private



- **Route Table configuration**



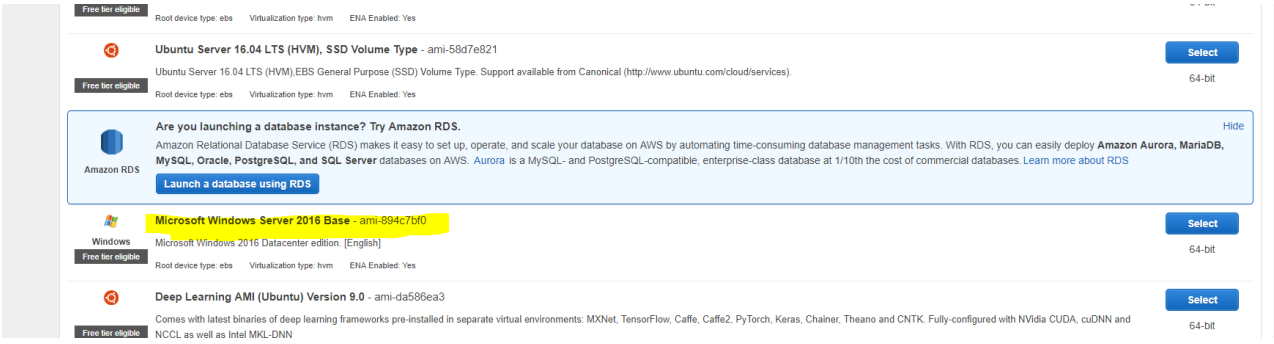
- **Create my VPC secutity group**, with Inbound Rule set to RDP, in order to be able to connect to instances (Windows Servers) of my VPC from my laptop (set IP address where I am connecting from):



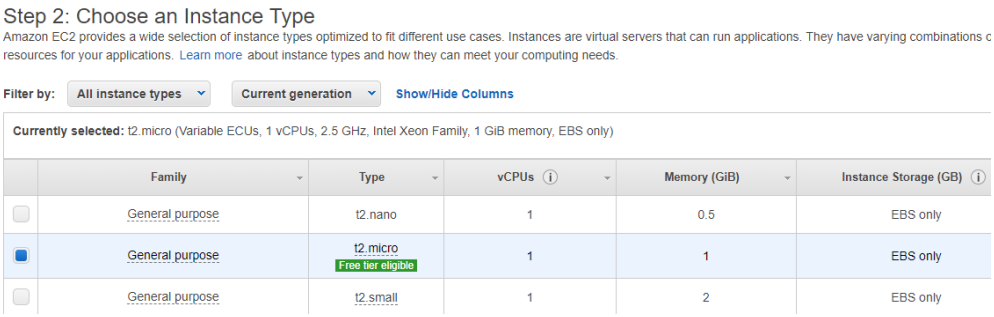
- **Launch Instances**

Service menu -> EC2 -> Launch Instance

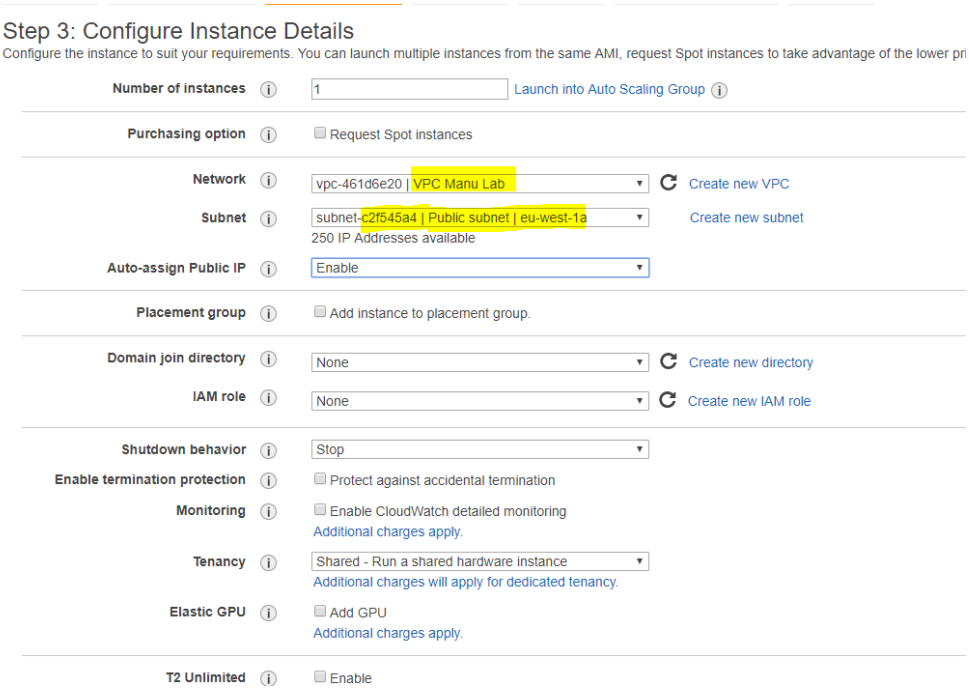
Microsoft Windows Server 2016 Base



Choose T2.micro type

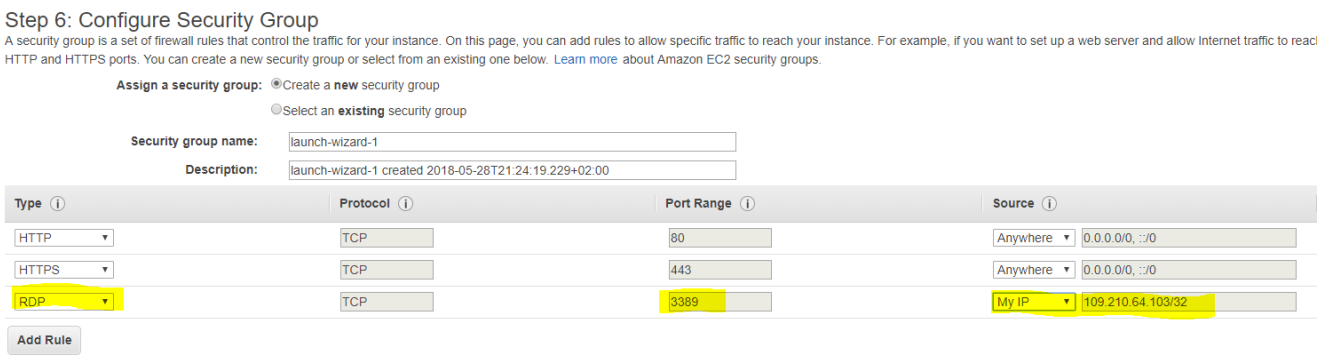


1st Instance in the Public Subnet

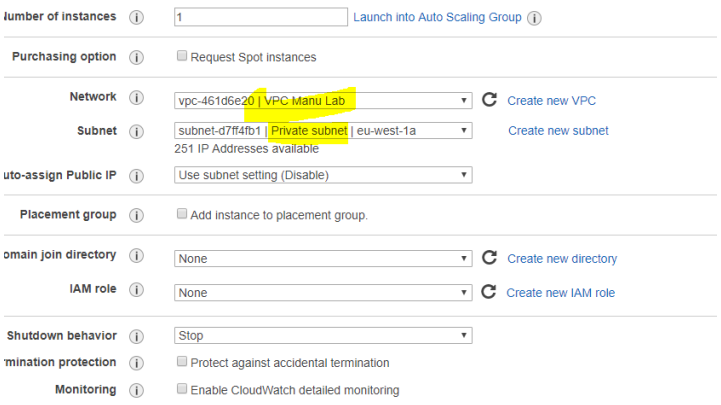


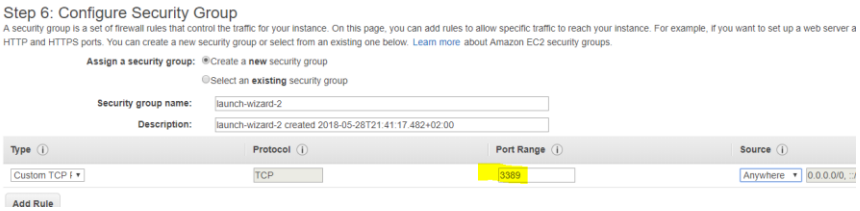
Create a new security group

- RDP Port 3389 to connect to this instznce as the AMI requires port 3389 to be open in order to have access
- HTTP and HTPPS ports to allow Internet traffic (unrestricted access)



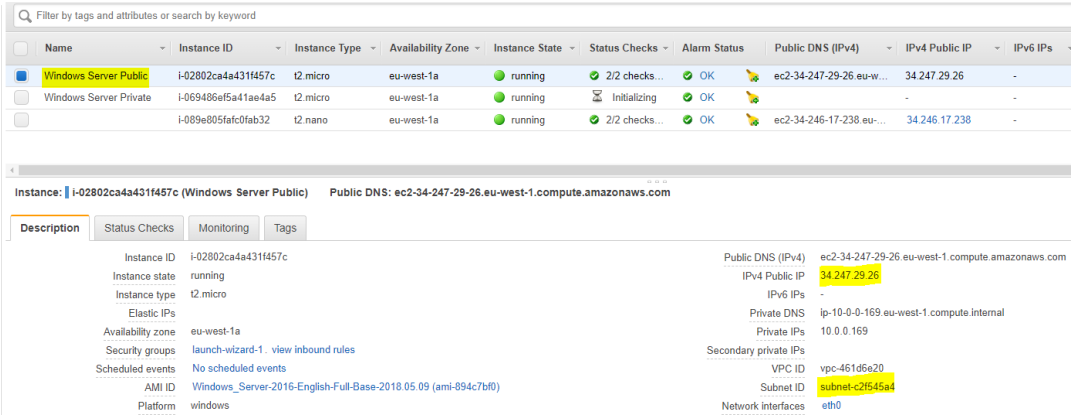
Create the 2nd instance in the private subnet



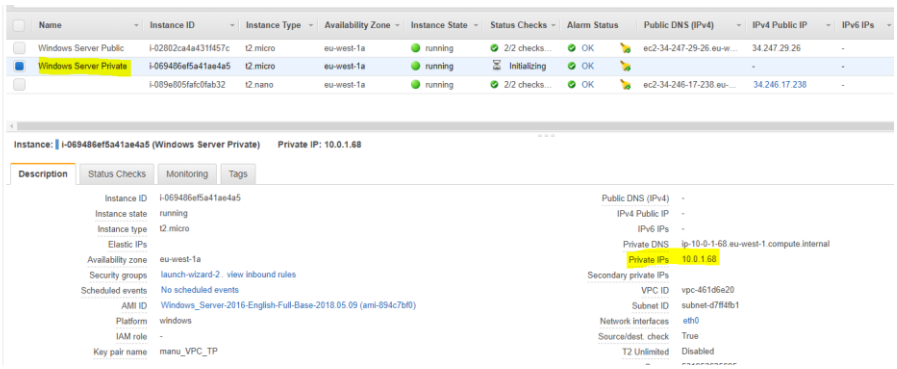


I have now 3 instances:

- 2 inside my public Subnet:
  - Windows Server Public, created by myself
  - Nat Instance, created automatically by Wizard VPC



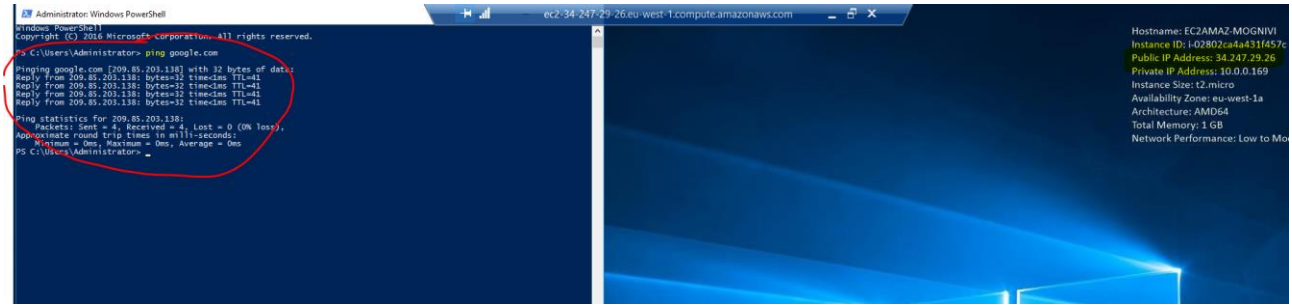
- 1 inside my Private Sunet
  - Windows Server Private, created by myself



Before to configure the NAT Gateway (Bastion), let's connect to the instance and check if ping is working

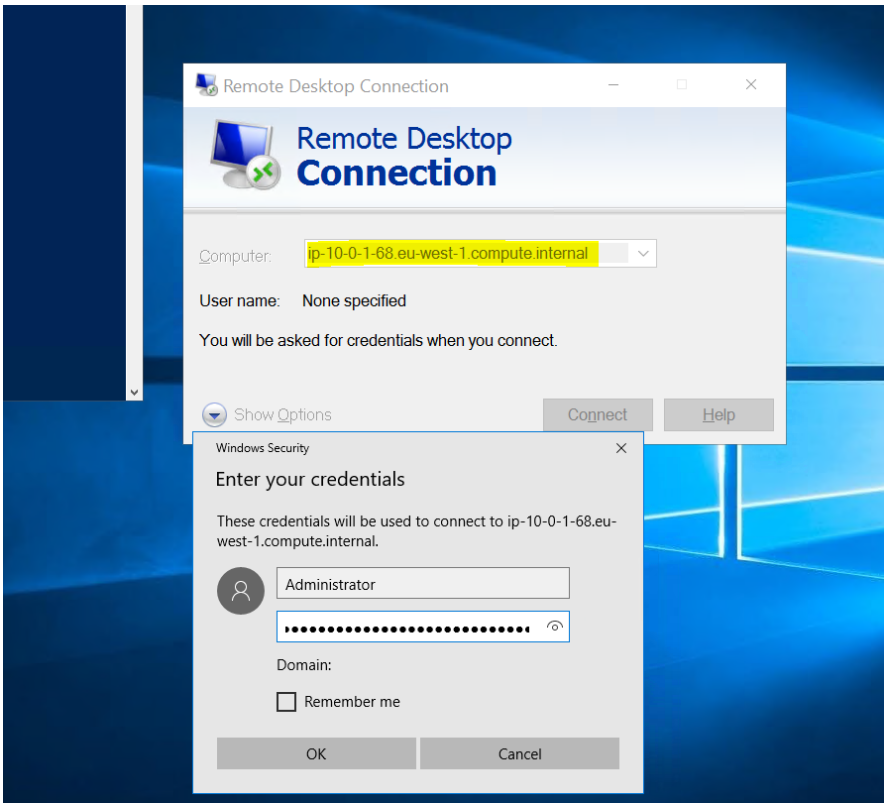
- **Connect to the Instance Windows Server Public**

  Let's do the ping …



… it is working

- **Launch instance in Private Subnet, from instance in public subnet**

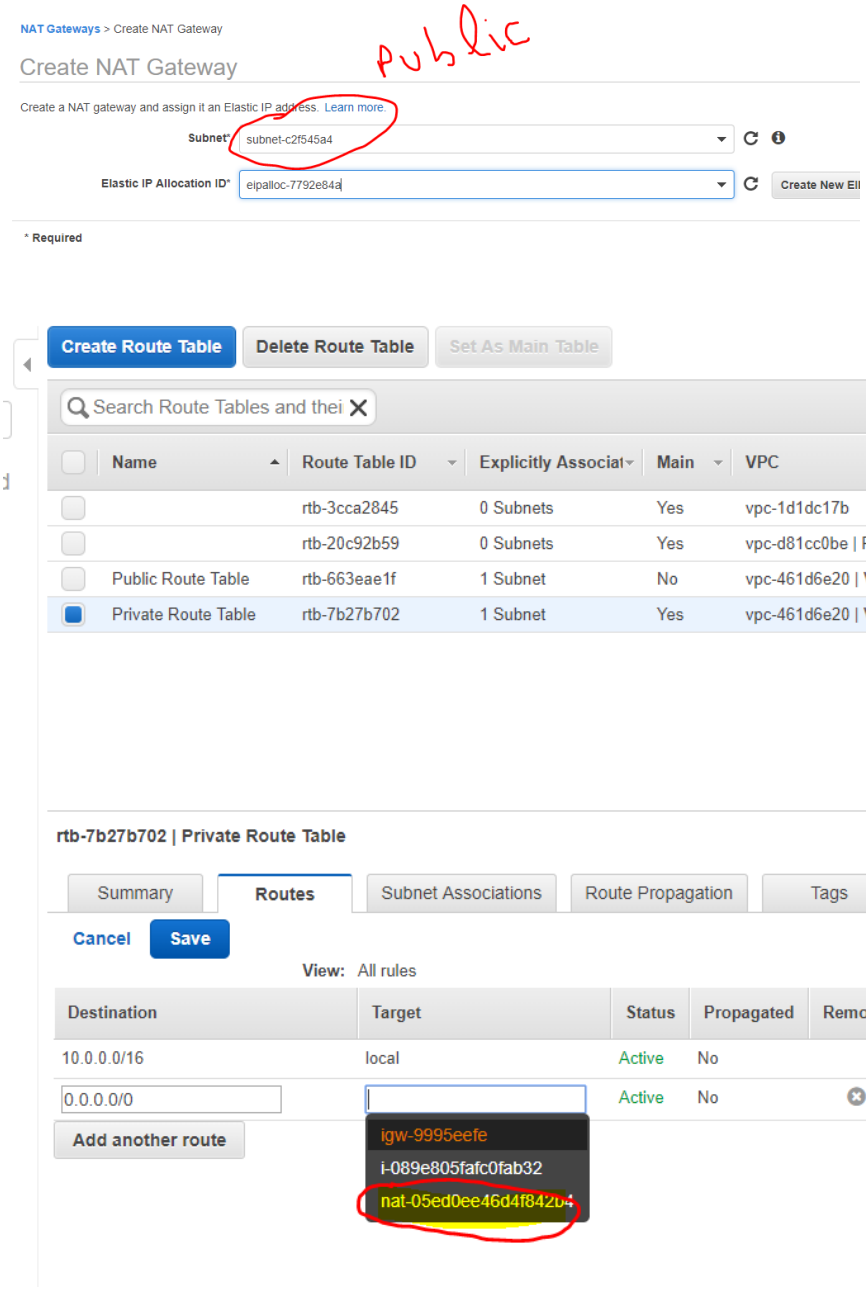


Let's do the ping …

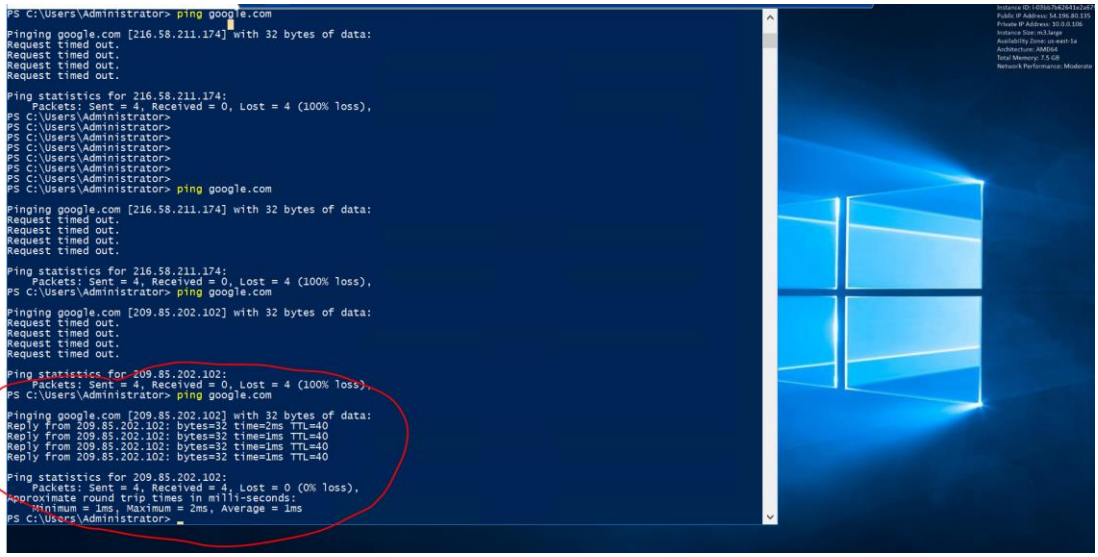
It' s not working.

This is expected.

Let 's now create the NAT Gateway, in the Public Subnet, And edit the private Route Table to associate it to the NAT Gateway.



And now test again the ping …



… Magic, it is replying now 😊