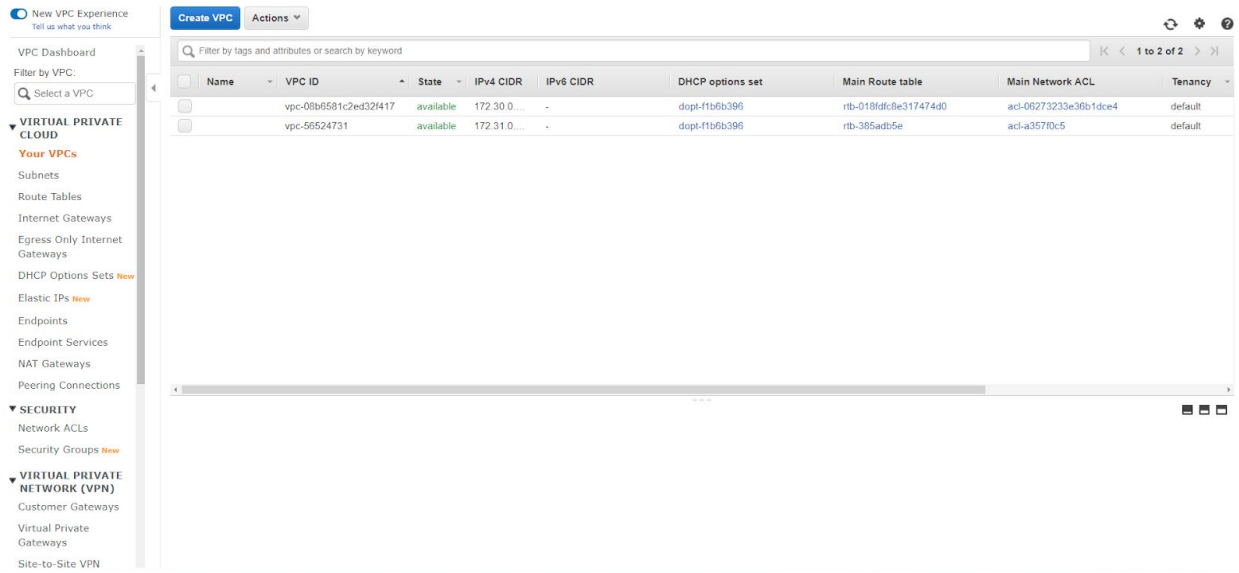
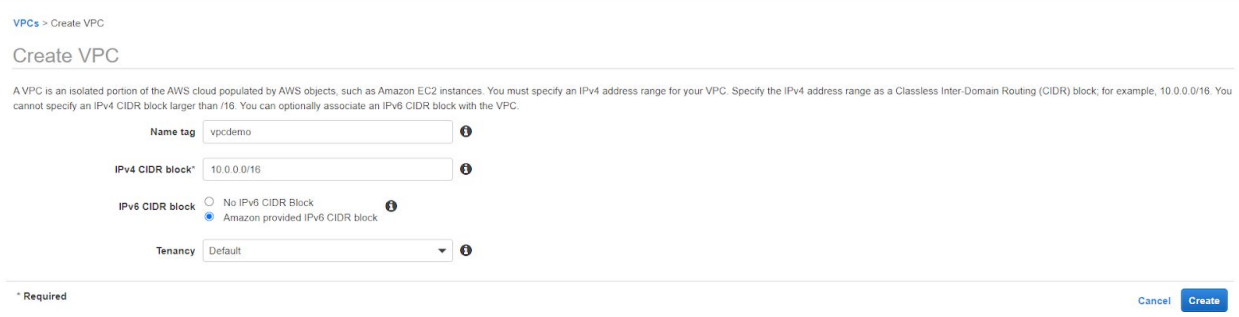
Module 7 Lab 1: Virtual Private Cloud Subnets

VPC Dashboard



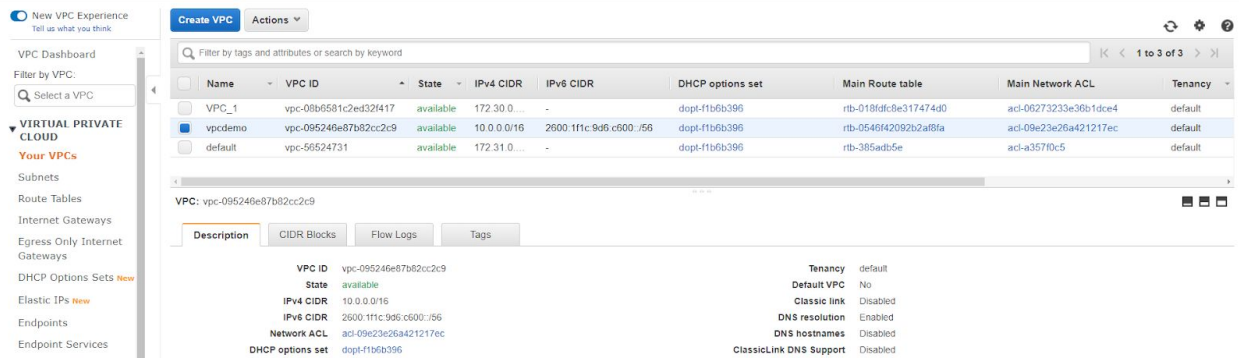
Starting at the VPC Dashboard, select Create VPC.

VPC - Create VPC



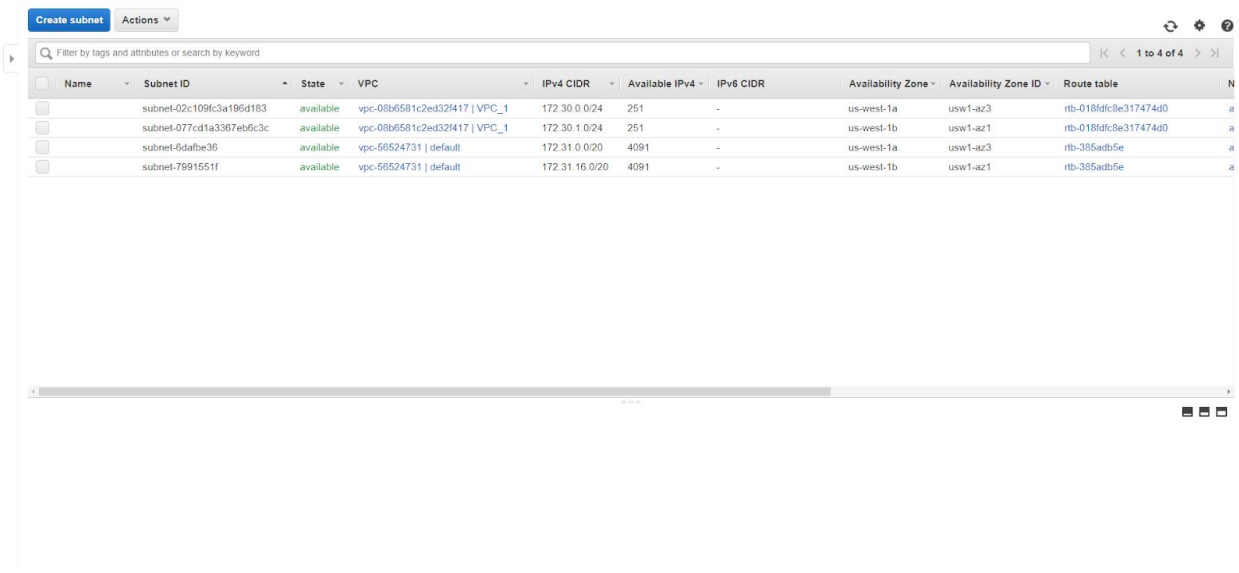
The IPv4 CIDR block is inputted manually to reflect the internal VPC network.

VPC Dashboard



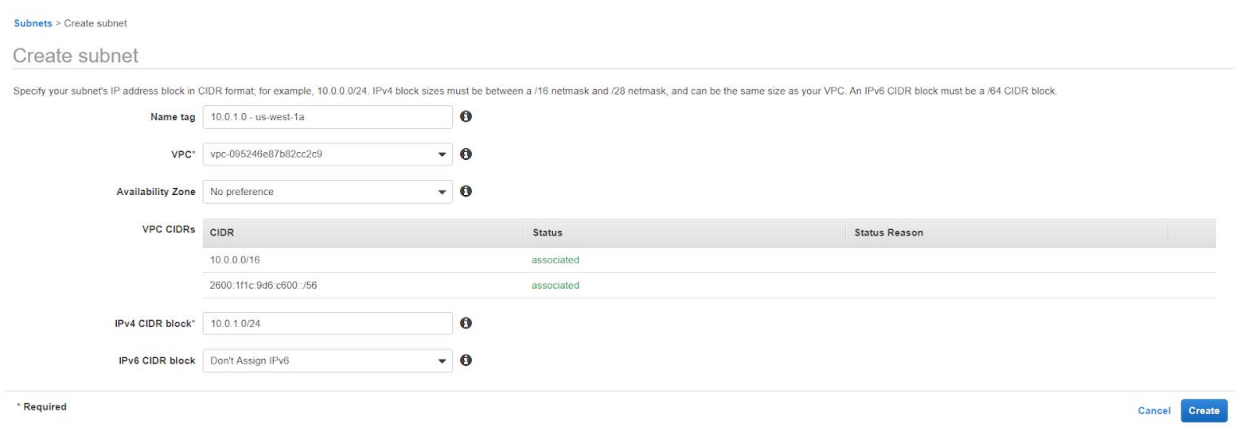
The new VPC has been created (vpc-095246e87b82cc2c9).

VPC Dashboard - Subnets



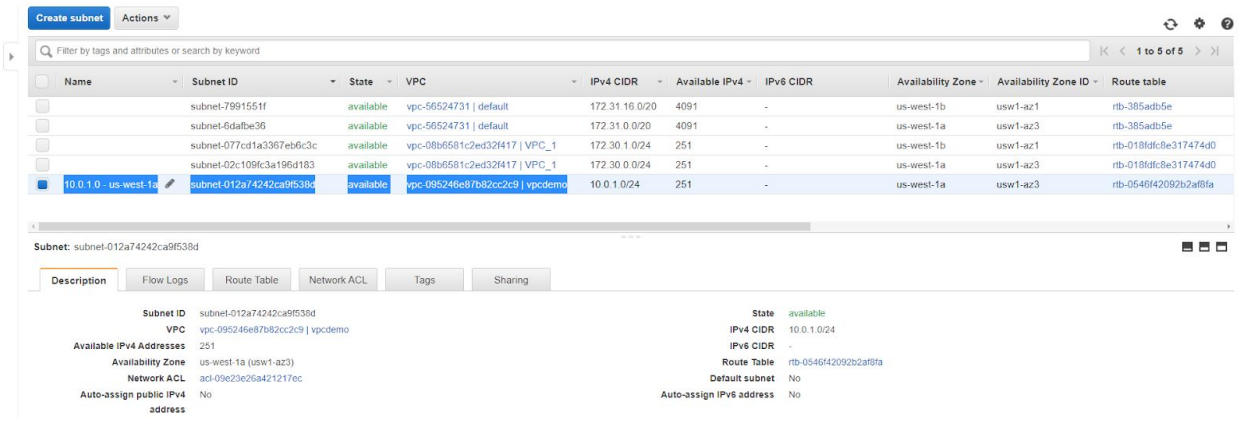
The current subnets refer to other AWS projects. New subnets are required for this vpcdemo just created.

Subnets - Create subnet



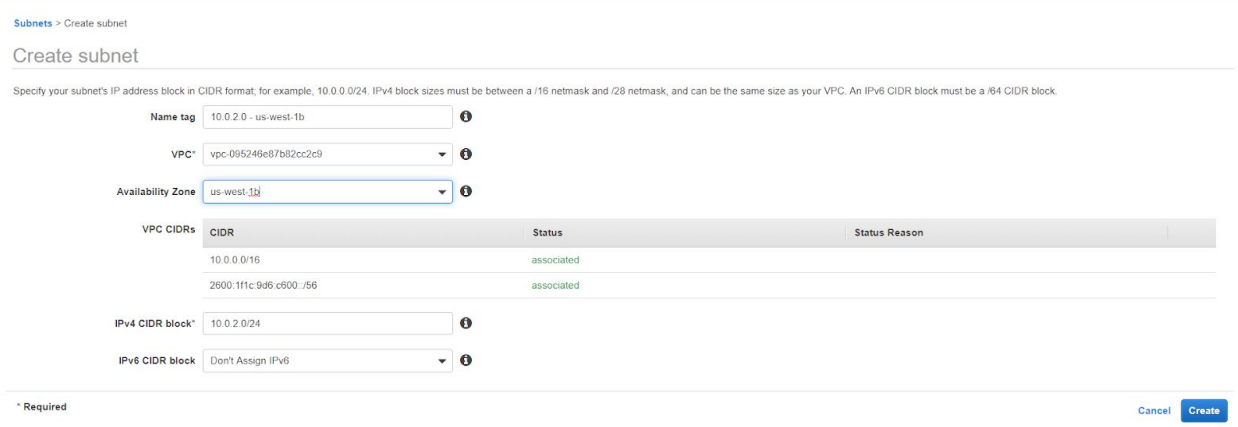
IPv4 CIDR block manually set to 10.0.1.0/24, to AZ us-west-1a

VPC Dashboard



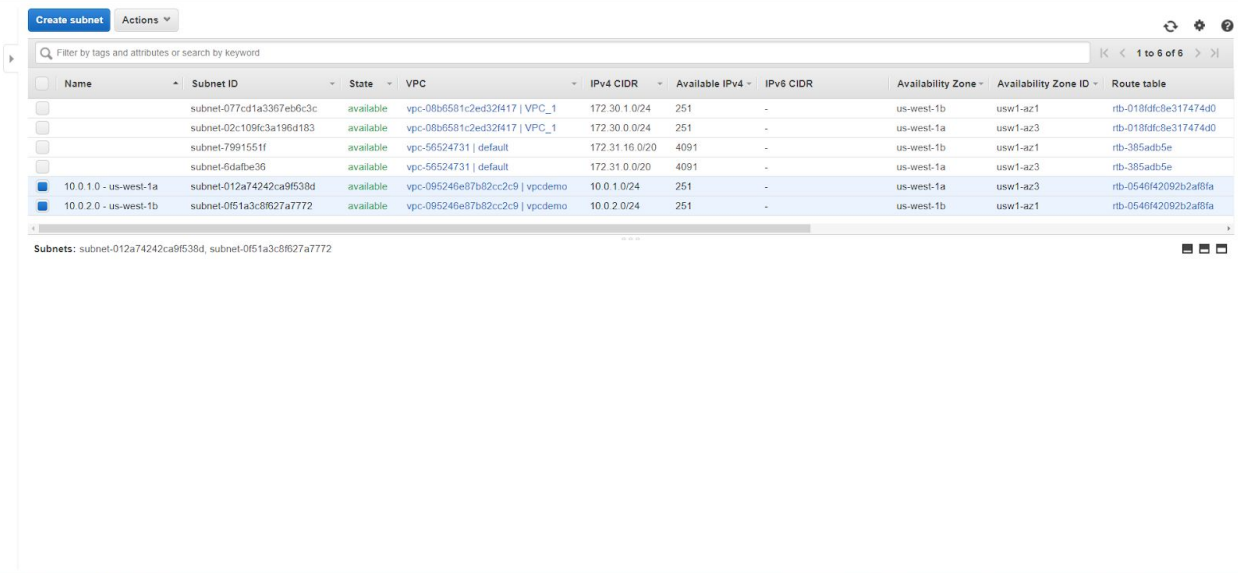
The internal subnet (or internal datacenter) was created inside the vpcdemo VPC.

Subnets - Create subnet



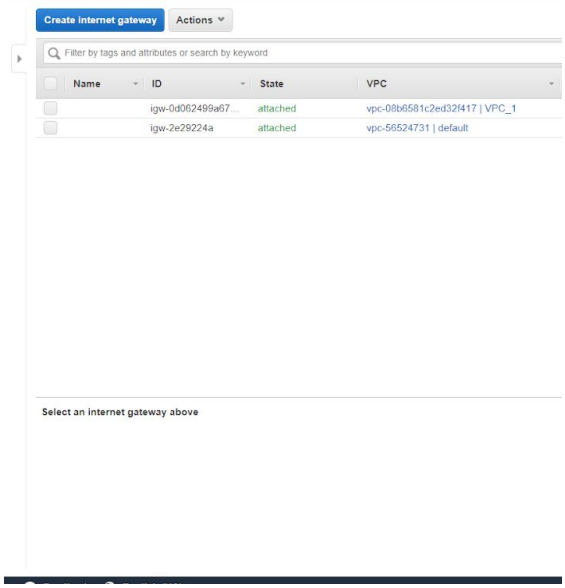
A second private subnet is created for internal use only. Note for high availability, us-west-1b was selected.

VPC Dashboard - Subnets



By default, at this moment both subnets are private because there is no Internet Gateway (IGW) attached.

VPC Dashboard - Create internet gateway

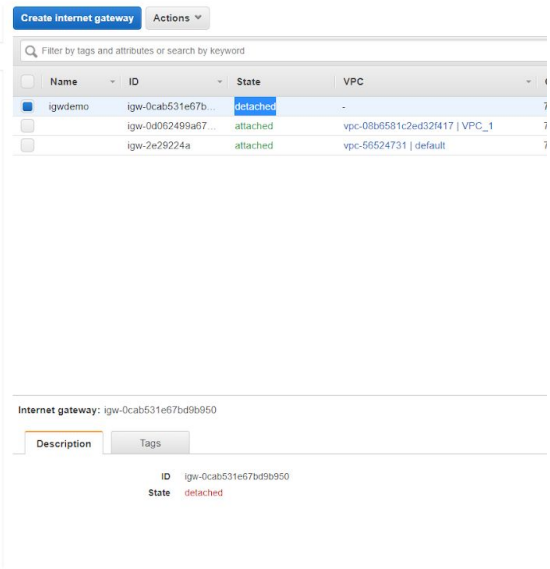


For VPC_1 and default, an internet gateway is already set up.

Internet gateways - Create internet gateway

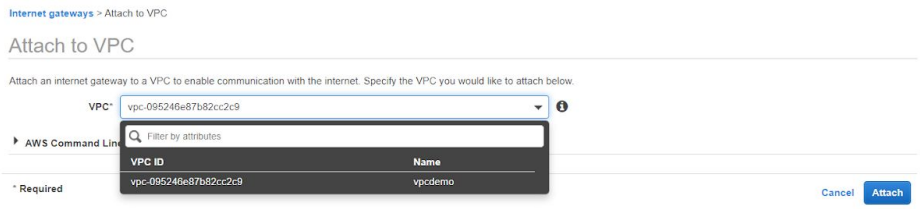
A new igw is created to support the vpcdemo VPC

VPC Dashboard - Internet Gateways



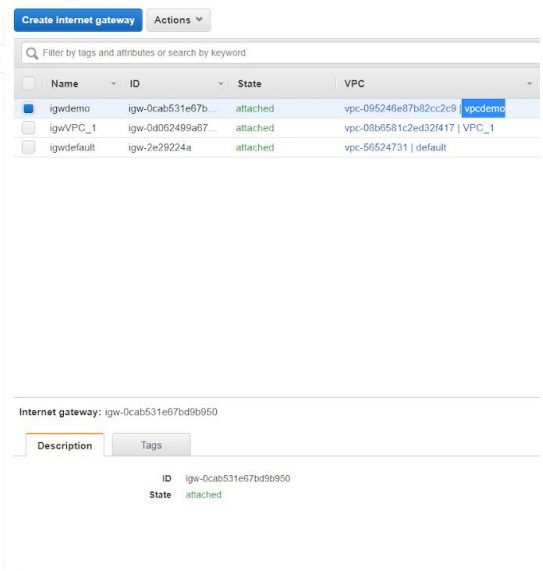
Note that igwdemo is detached.

Internet Gateways - Attach to VPC



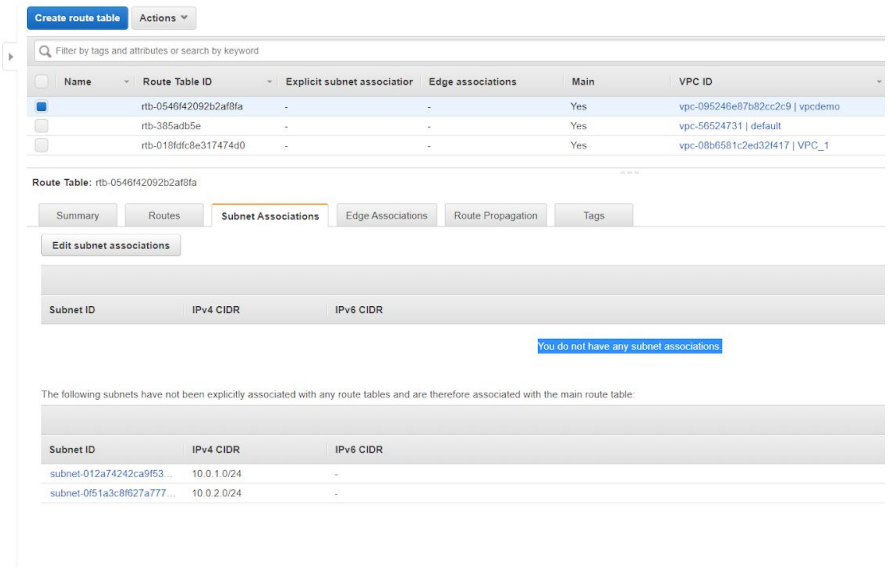
igwdemo will be attached to vpcdemo. Note that only one internet gateway can be attached to any VPC's.

VPC Dashboard - Create internet gateway



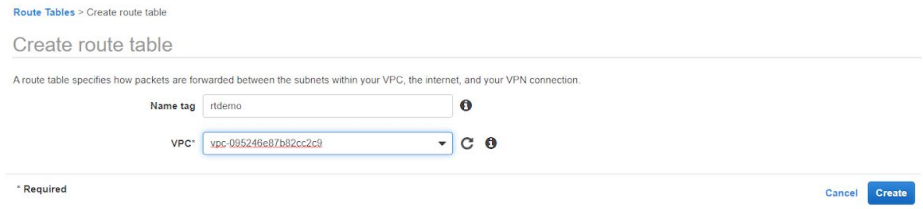
igwdemo is now attached to vpcdemo.

VPC Dashboard - Create route table



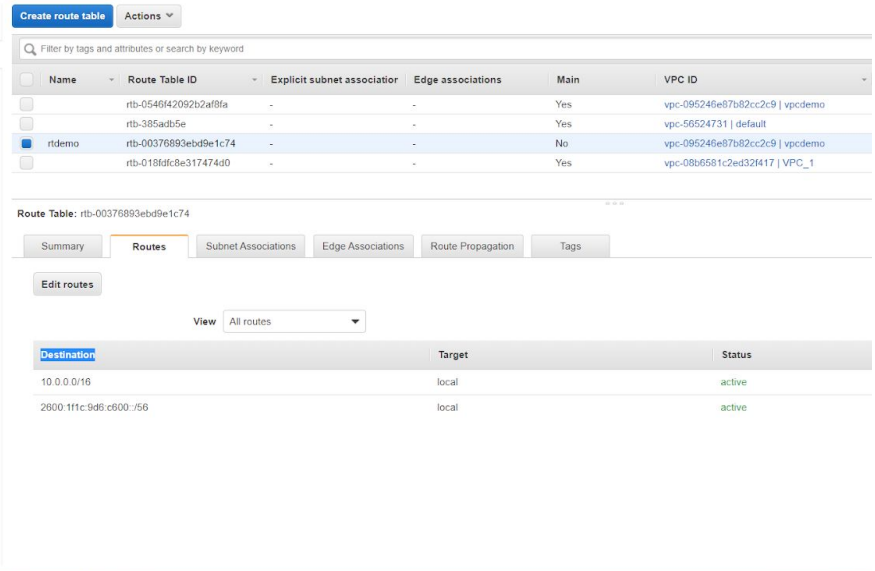
No associated subnets are established to the vpcdemo VPC.

Route Tables - Create route table



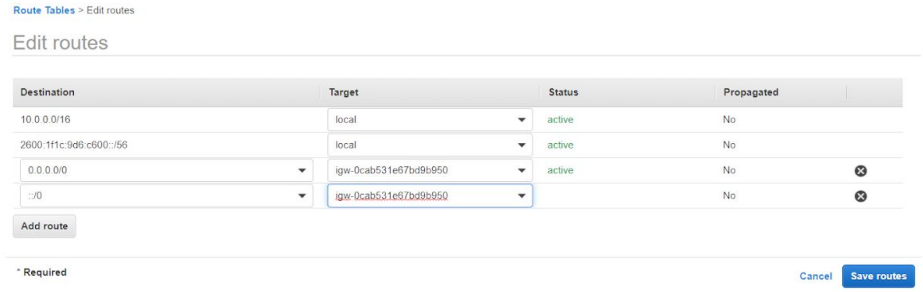
A new route table (rtdemo) is created in the vpcdemo VPC.

VPC Dashboard - Create route table



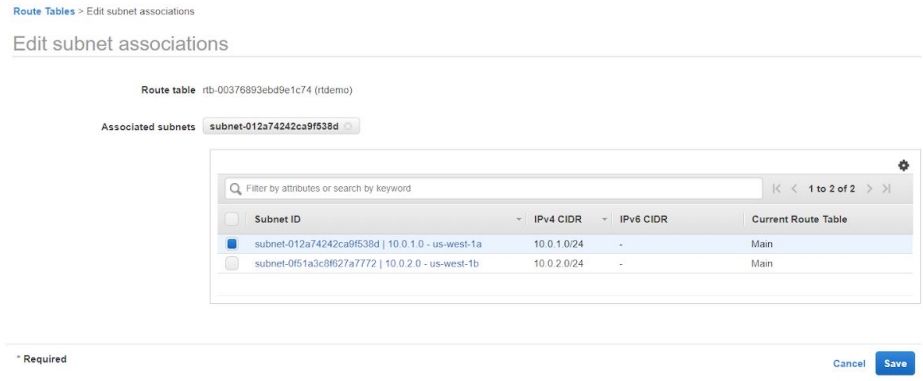
There are no routes established for internet traffic at 0.0.0.0/0

Route Tables - Edit routes



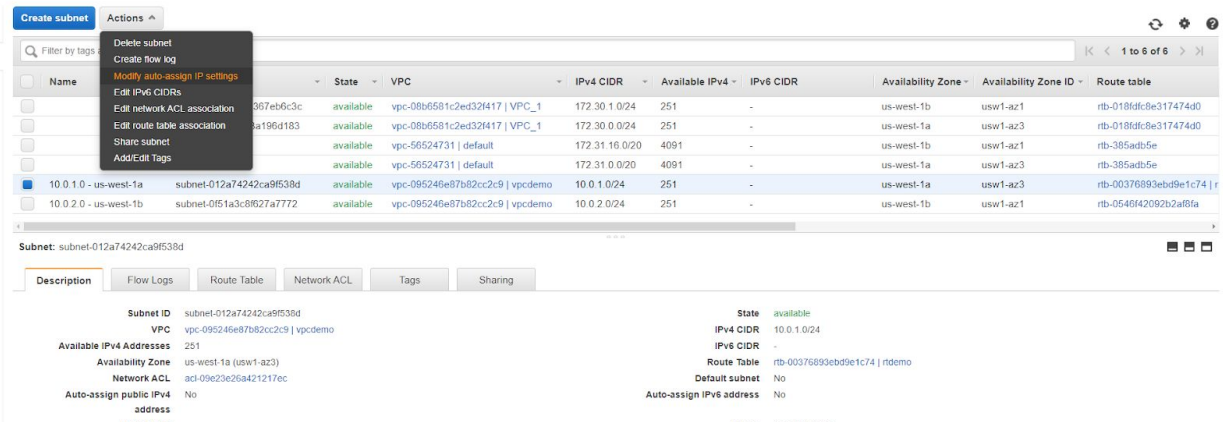
All internet traffic (IPv4 and IPv6) will route through the igwdemo internet gateway.

Route Tables - Edit subnet associations



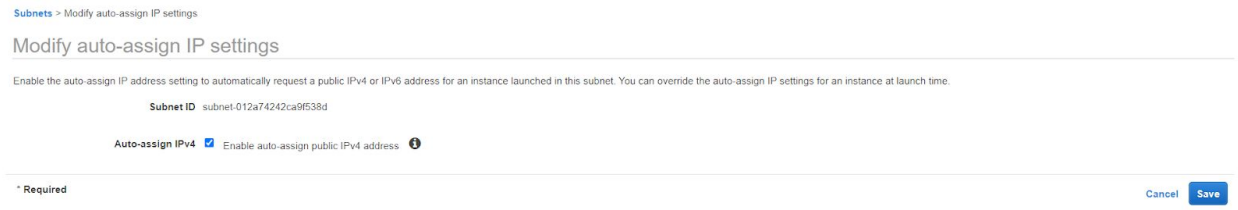
Now the public subnet can be associated with the private subnet.

VPC Dashboard - Create subnet



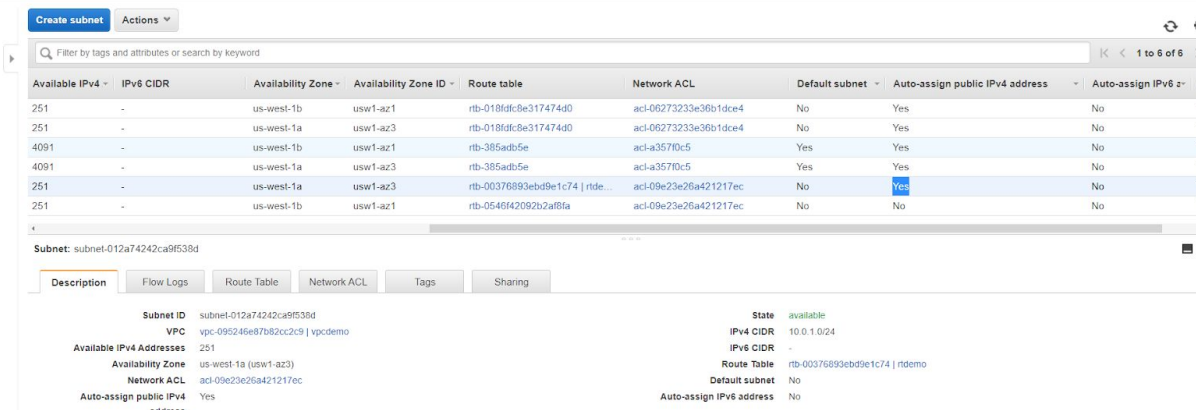
The public facing subnet needs to be allowed a public IP address.

Subnets - Modify auto-assign IP settings



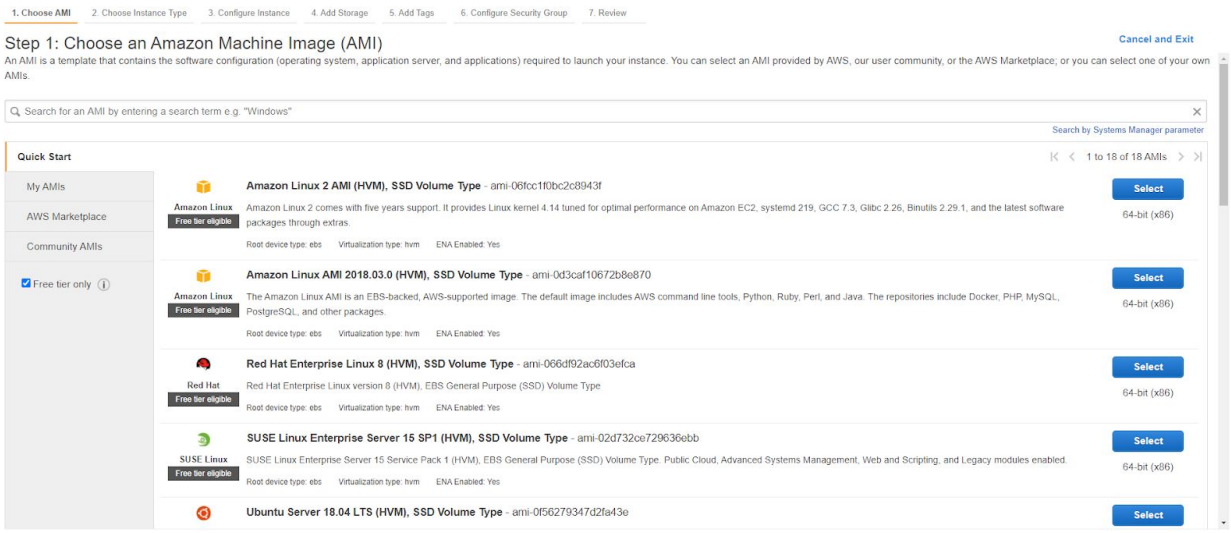
Now when EC2 instances are launched, auto assigned public IPv4 addresses can be established.

VPC Dashboard - Create subnet



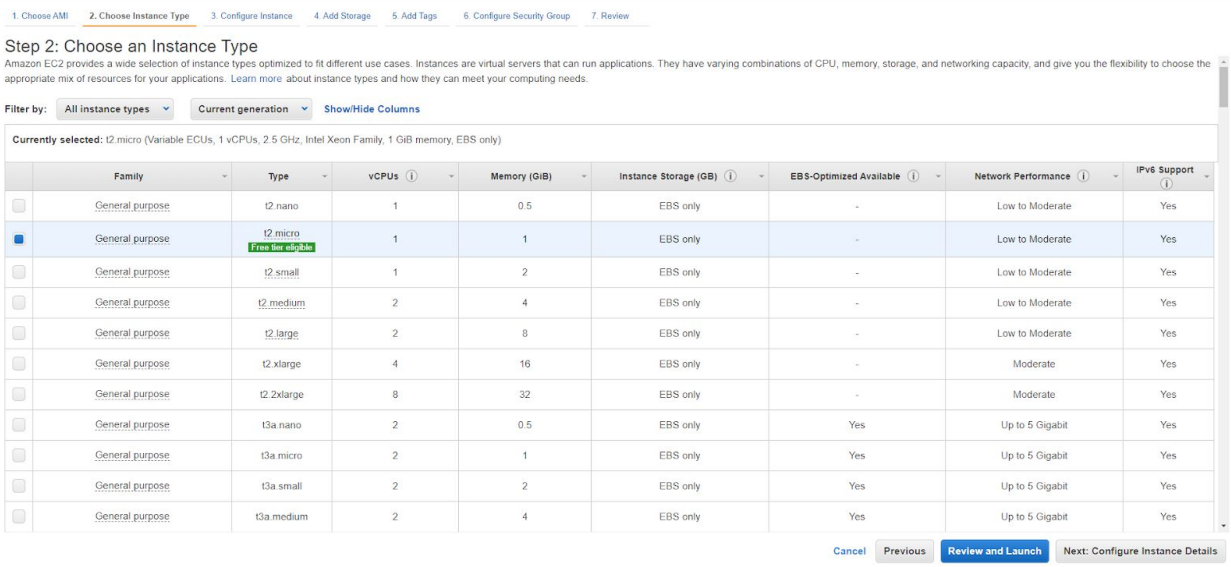
IPv4 addresses will now be assigned automatically for EC2 instances.

EC2 - AMI



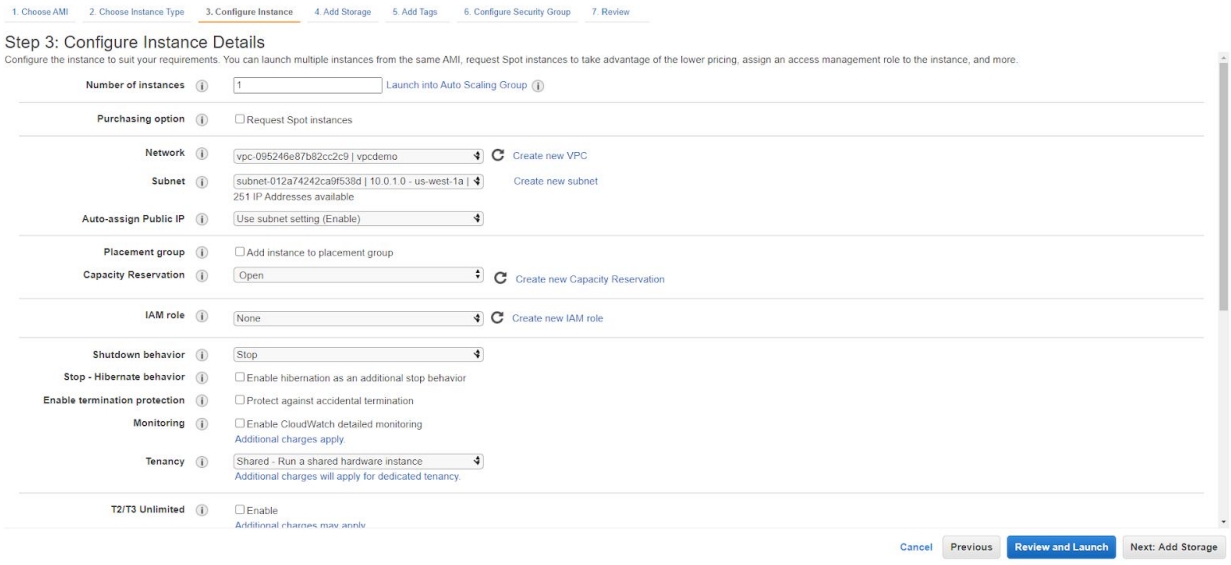
To utilize the subnets and VPC, two instances will be started. Linux AMI 2018.03.0 is selected.

EC2 - Instance type



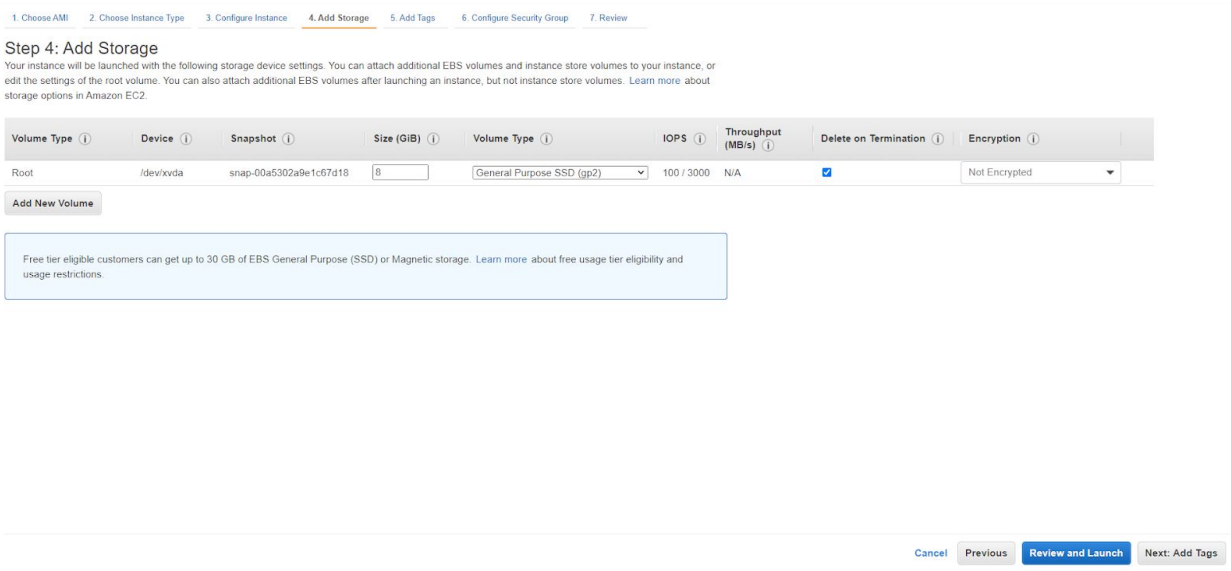
t2.micro is selected.

EC2 - Configure Instance Details



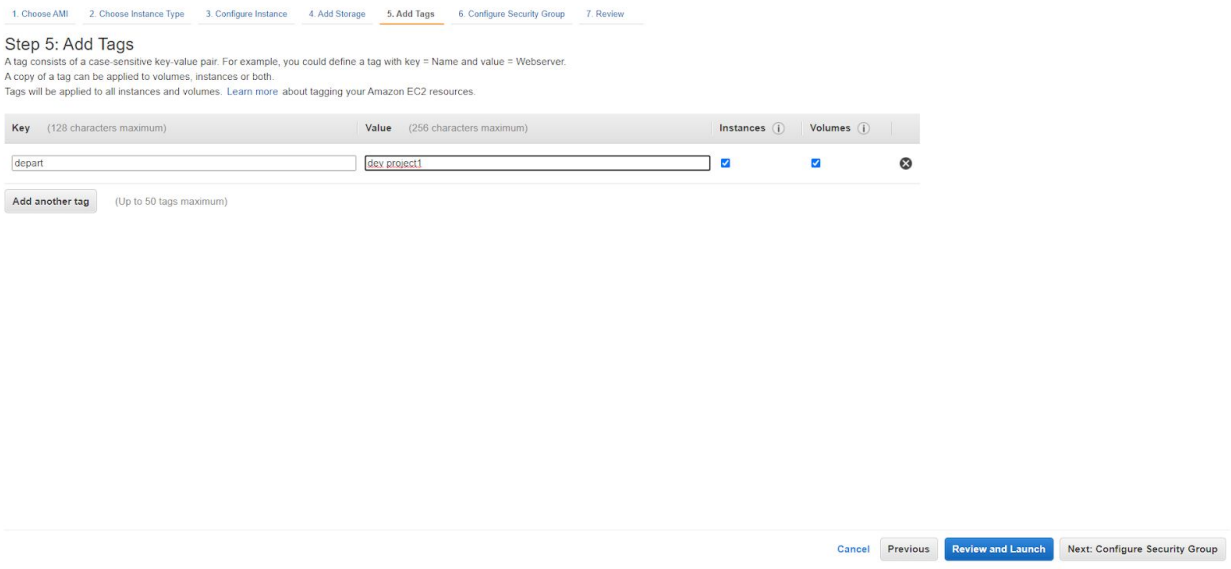
Note that vpcdemo and the public facing subnet 10.0.1.0 is selected.

EC2 - Add Storage



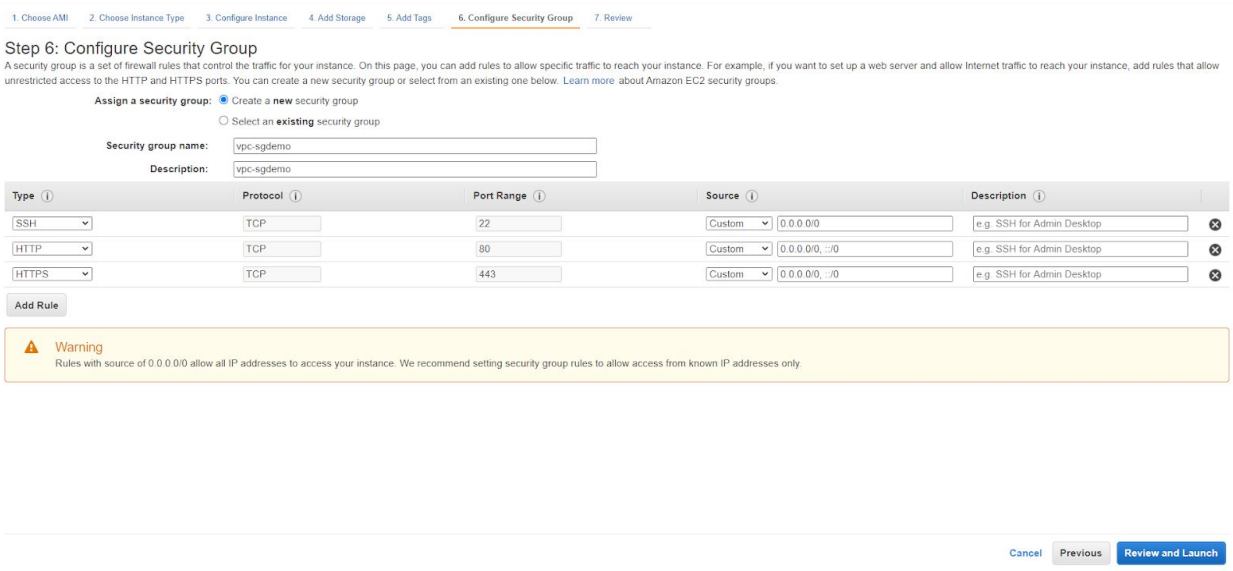
Default storage is selected.

EC2 - Add Tags



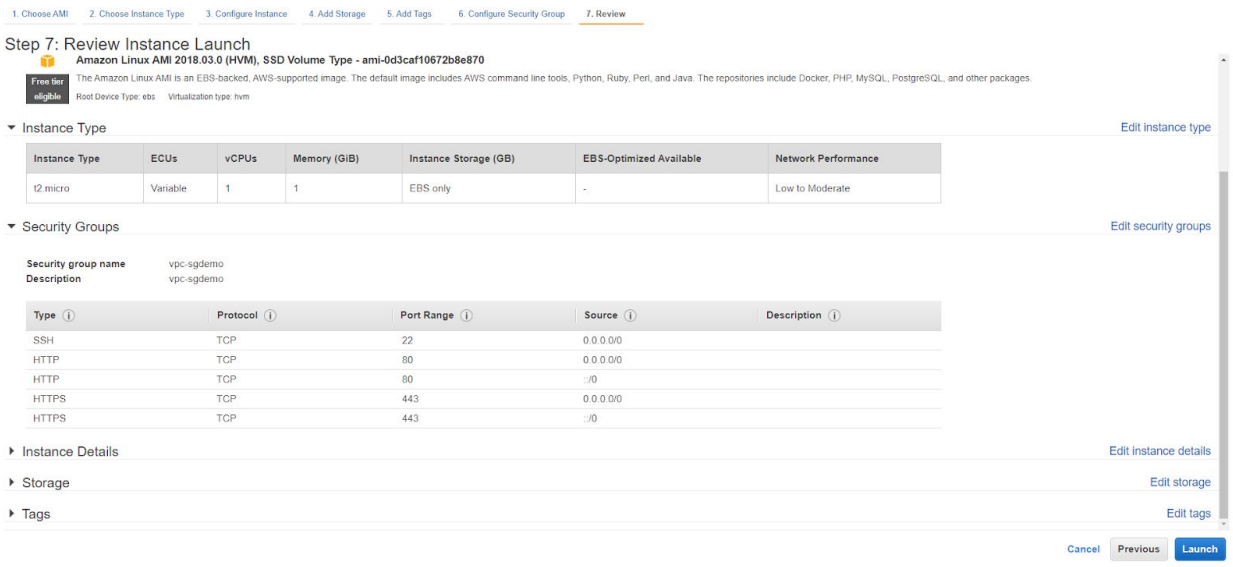
Tags defined.

EC2 - Configure Security Group



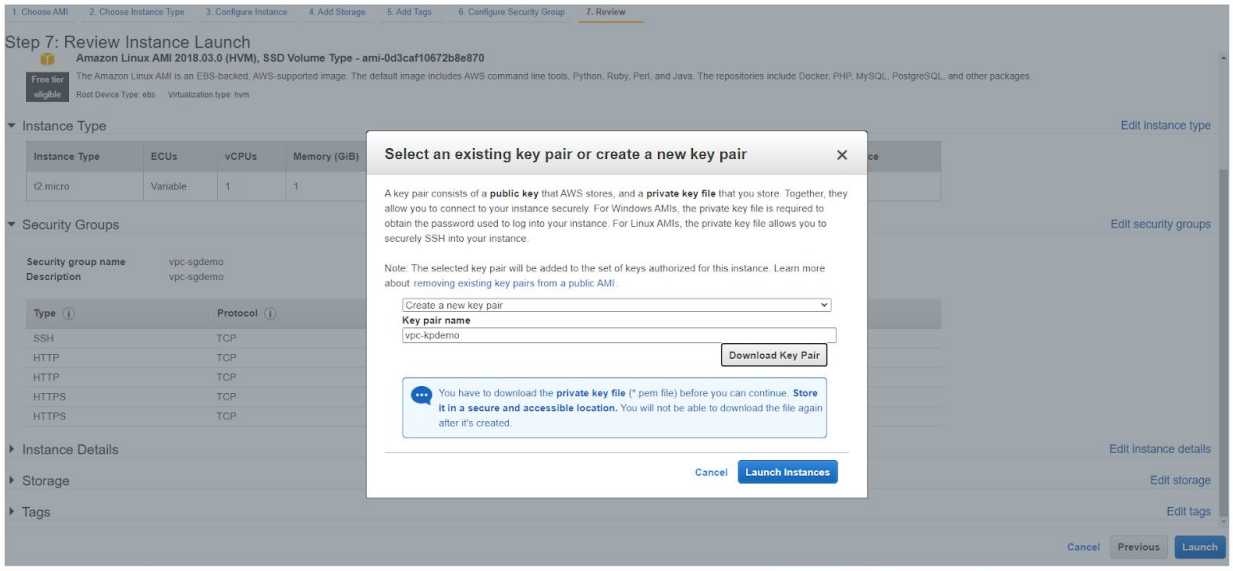
Security group created with SSH for administration and HTTP/HTTPS for public accessible web services. However, for this lab only SSH is required.

EC2 - Review Instance Launch



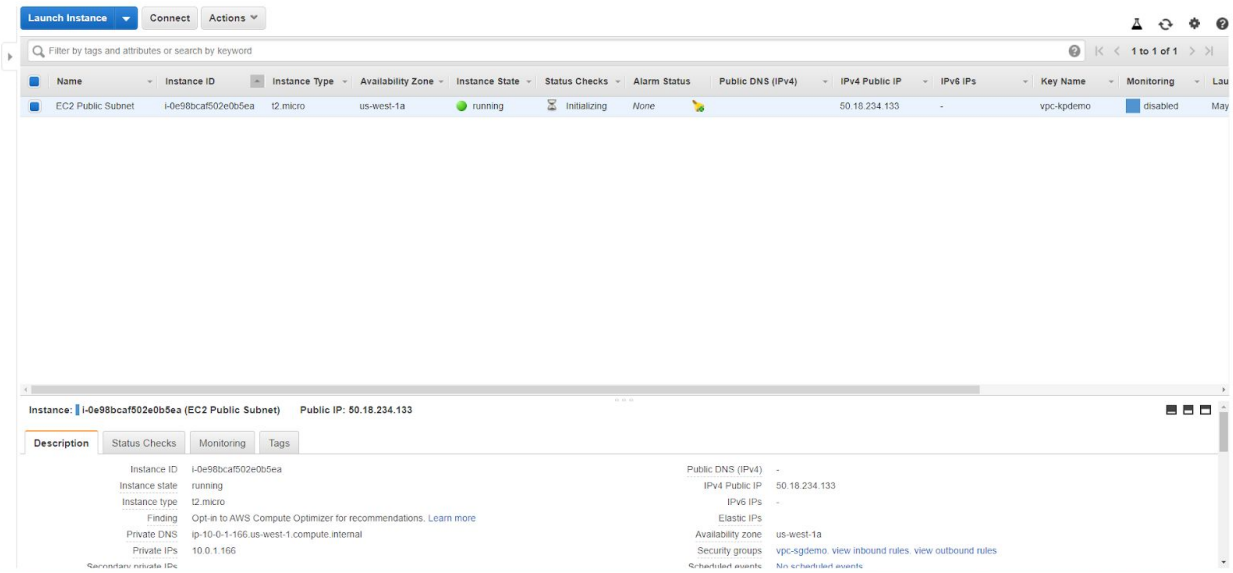
Note HTTP/HTTPS show up twice for IPv4 and IPv6 addressing.

EC2 - Keypair



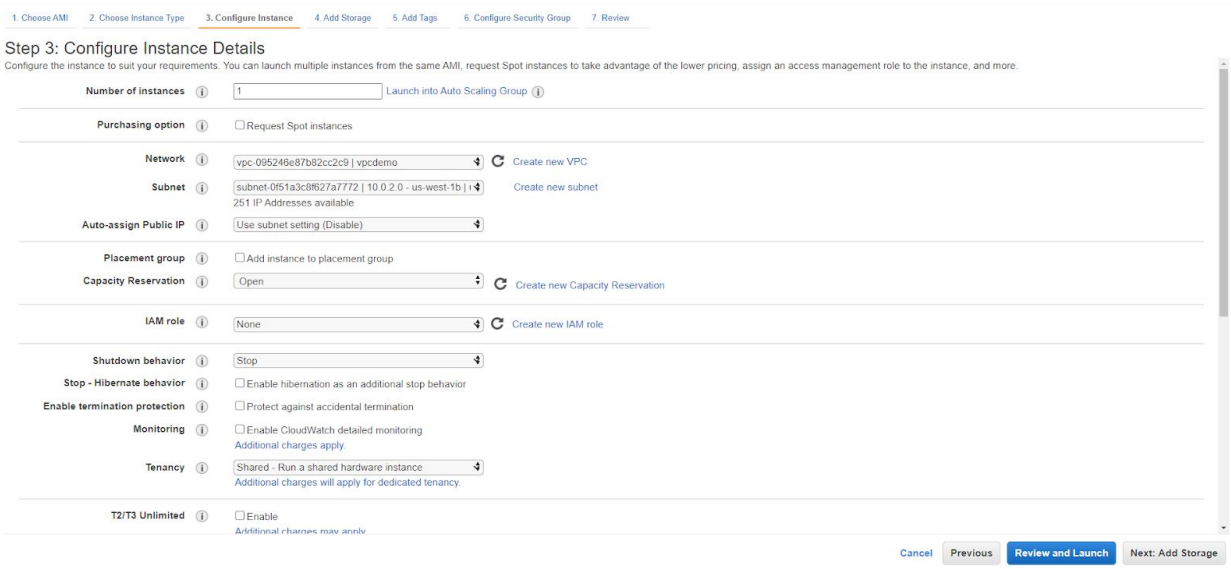
A new keypair has been created and downloaded locally.

EC2 Dashboard



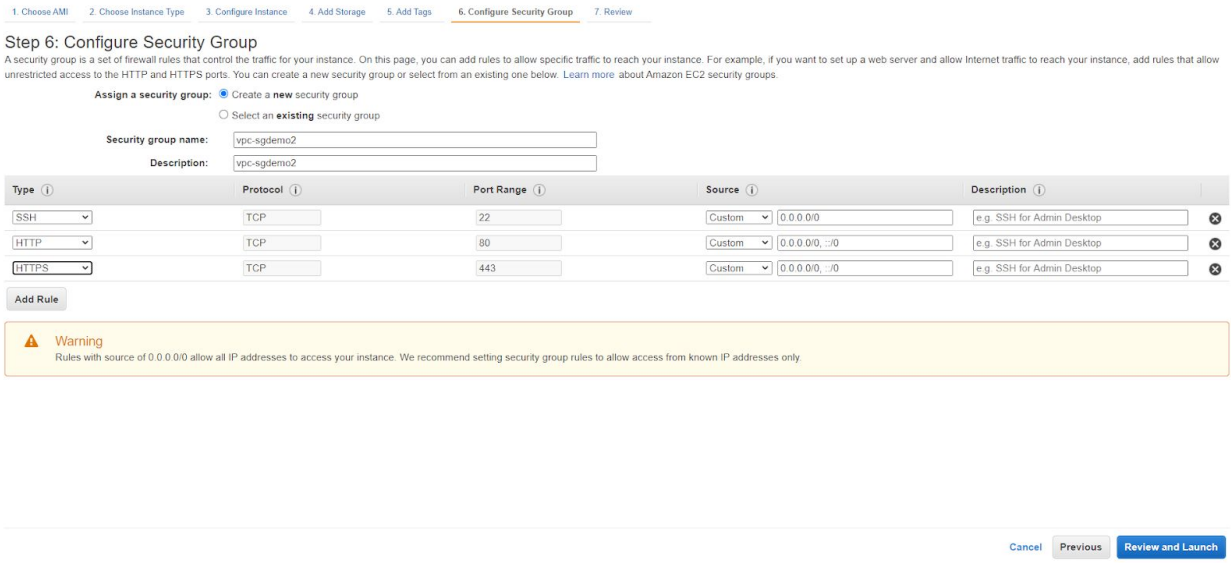
Instance has been successfully created. Another private instance is now required.

EC2 - Configure Instance



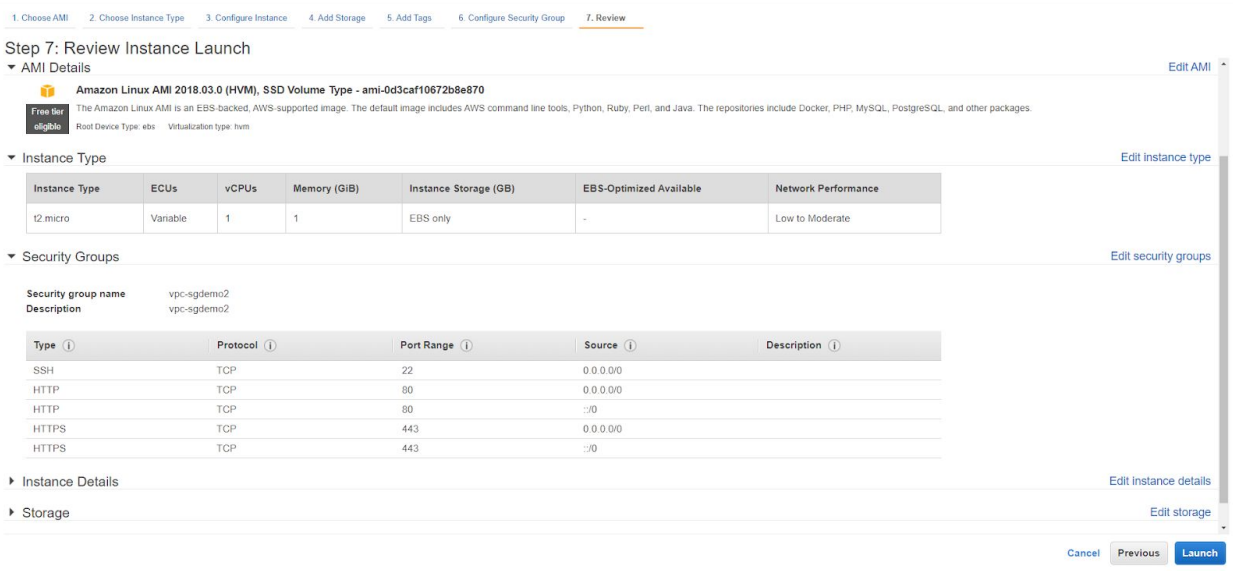
However, this instance will be set to 10.0.2.0, the private subnet in the vpcdemo VPC.

EC2 - Configure Security Group



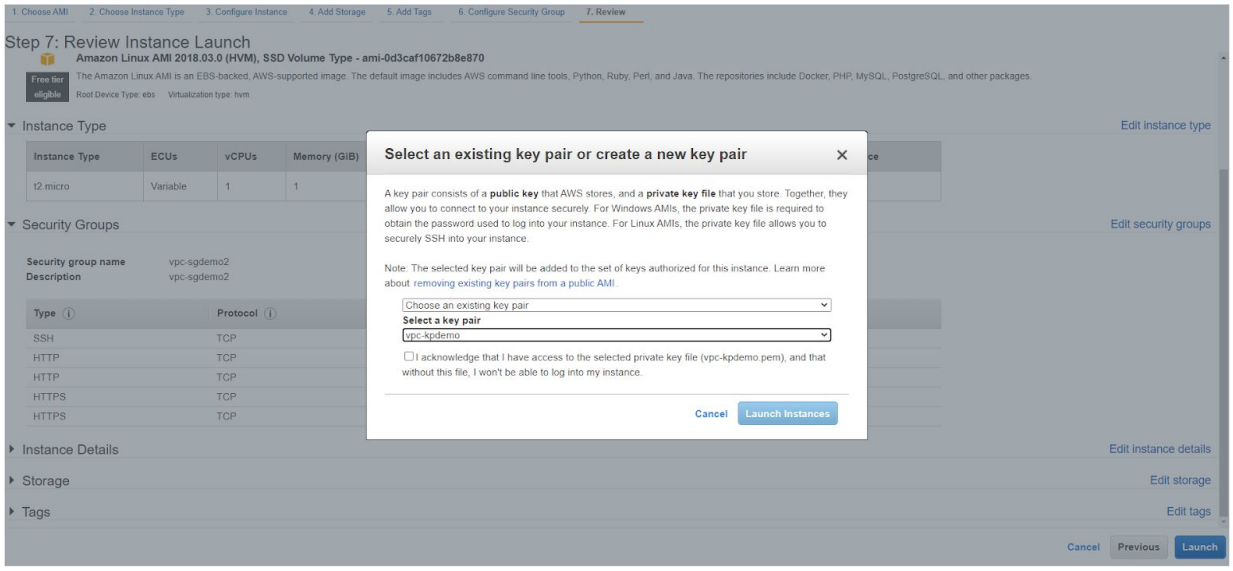
The instance is given HTTP/HTTPS and SSH port access.

EC2 - Review



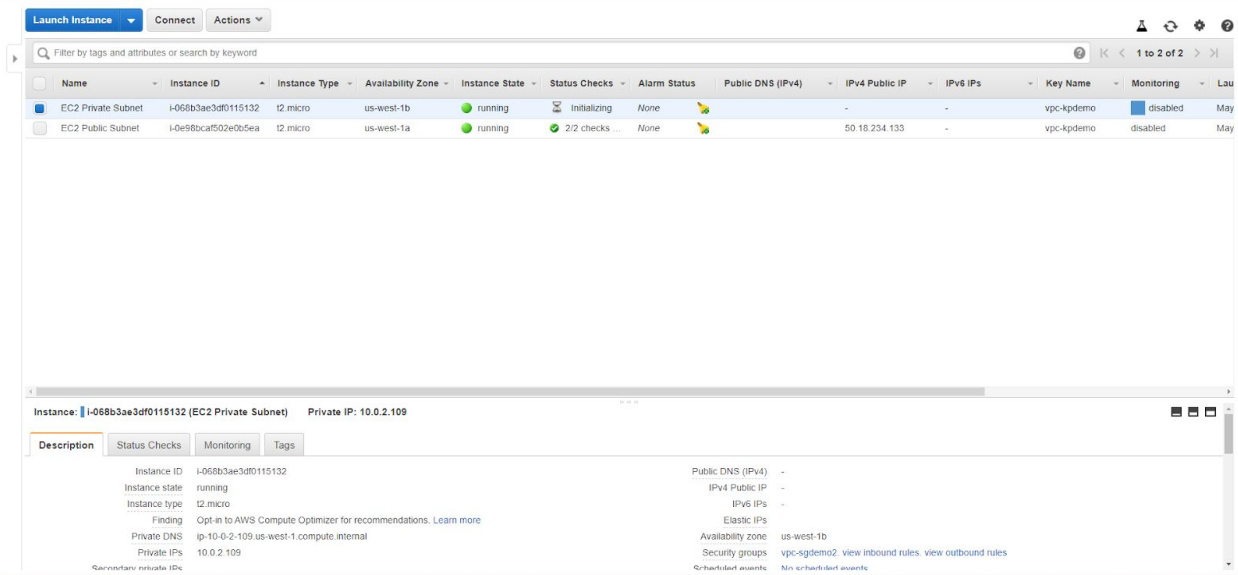
All settings match the public subnet except for the subnet itself.

EC2 - Keypair



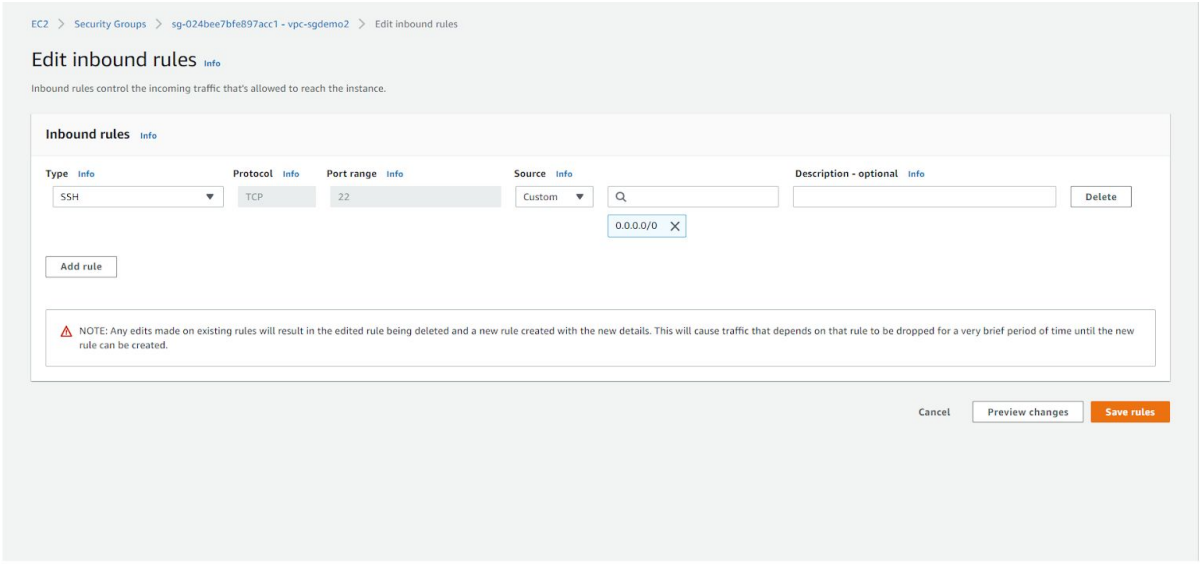
For brevity, the same keypair used for the public subnet is selected.

EC2 Dashboard



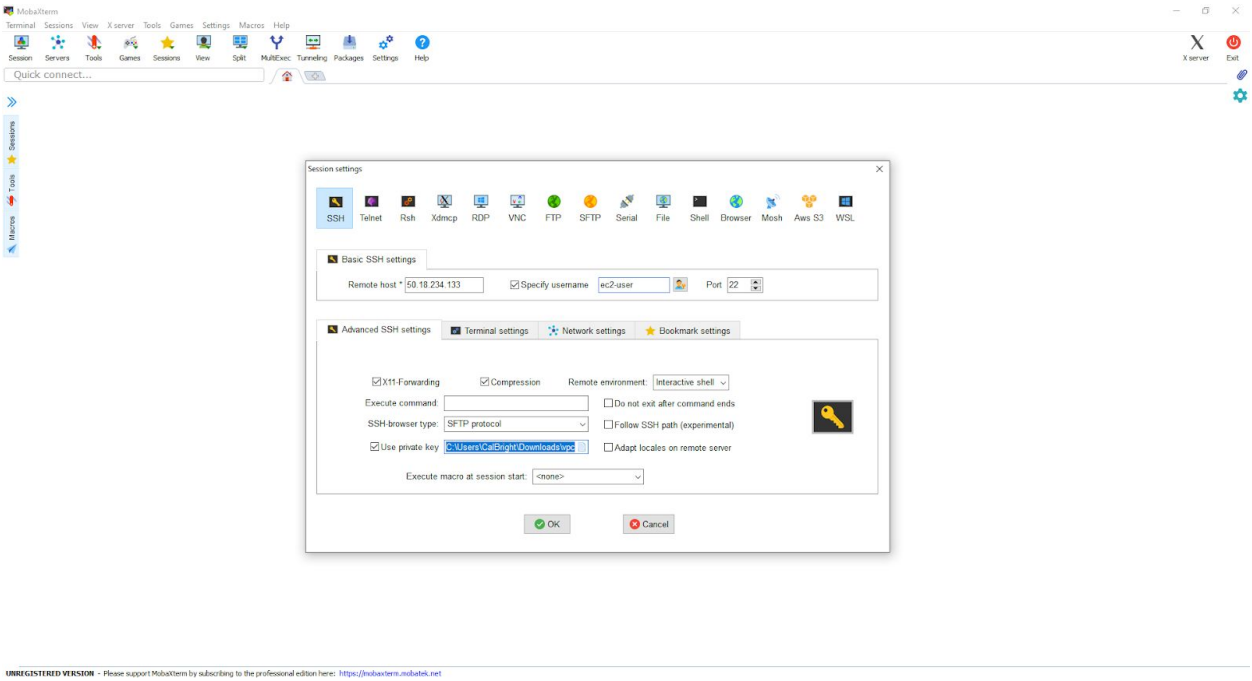
A private subnet is now active. Note that a public IPv4 IP address has not been assigned.

Security Groups - Edit inbound rules - sgdemo2



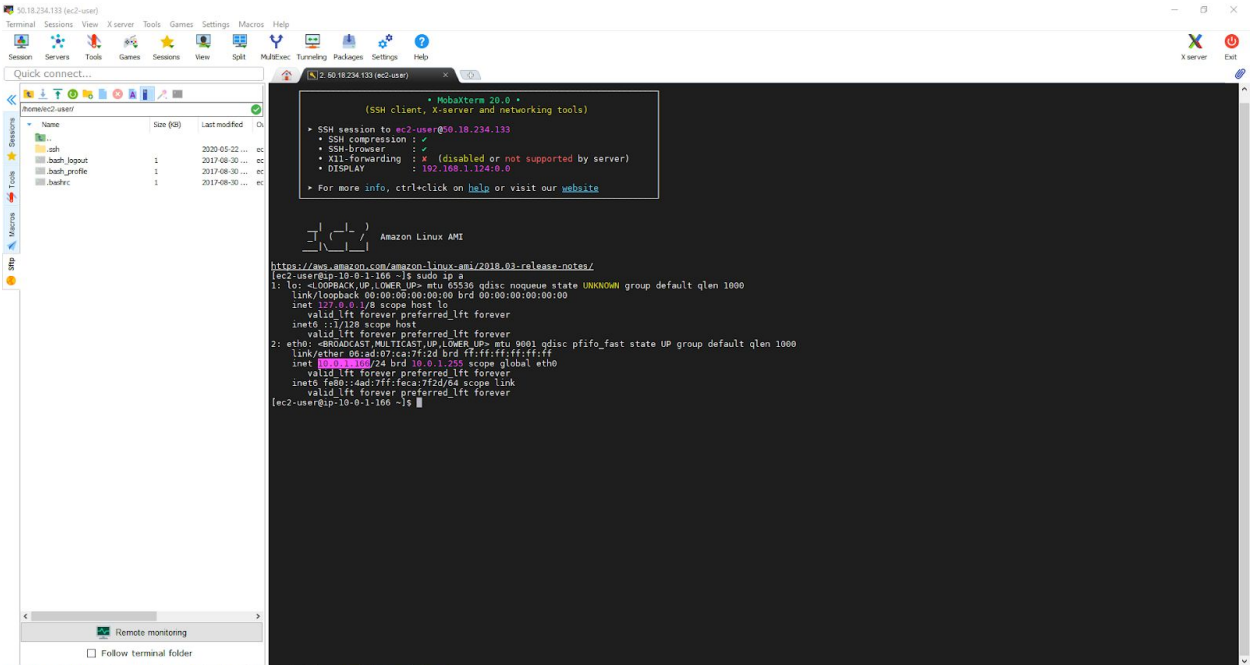
For best practices, unused ports are closed.

MobaXterm



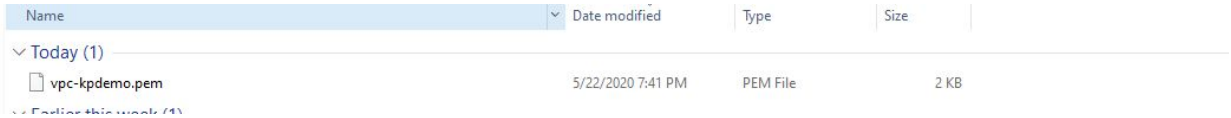
MobaXterm is used to SSH into the public facing subnet attached to the vpcdemo VPC.

MobaXterm



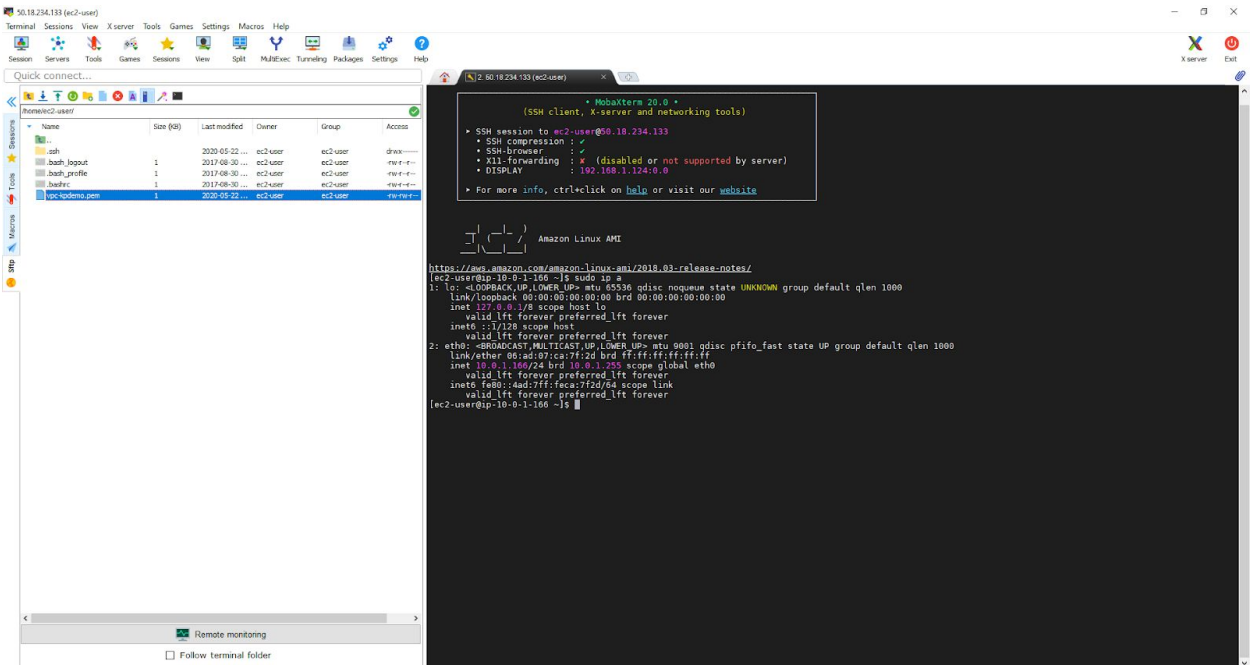
Note the correct public subnet IPv4 address has been assigned, 10.0.1

Windows 10 - Local Folder



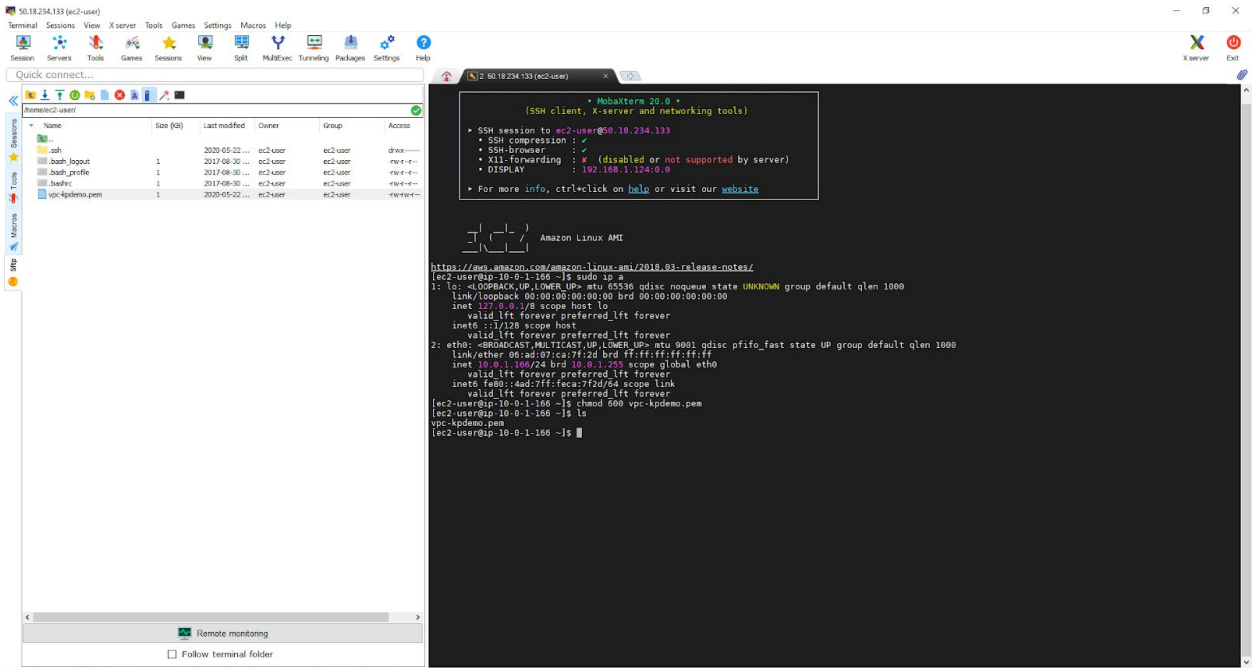
The pem keypair must be copied over to the EC2 instance home directory. This is accomplished by dragging and dropping the pem keypair into the /home/ec2-user/ sidebar in MobaXterm.

MobaXterm



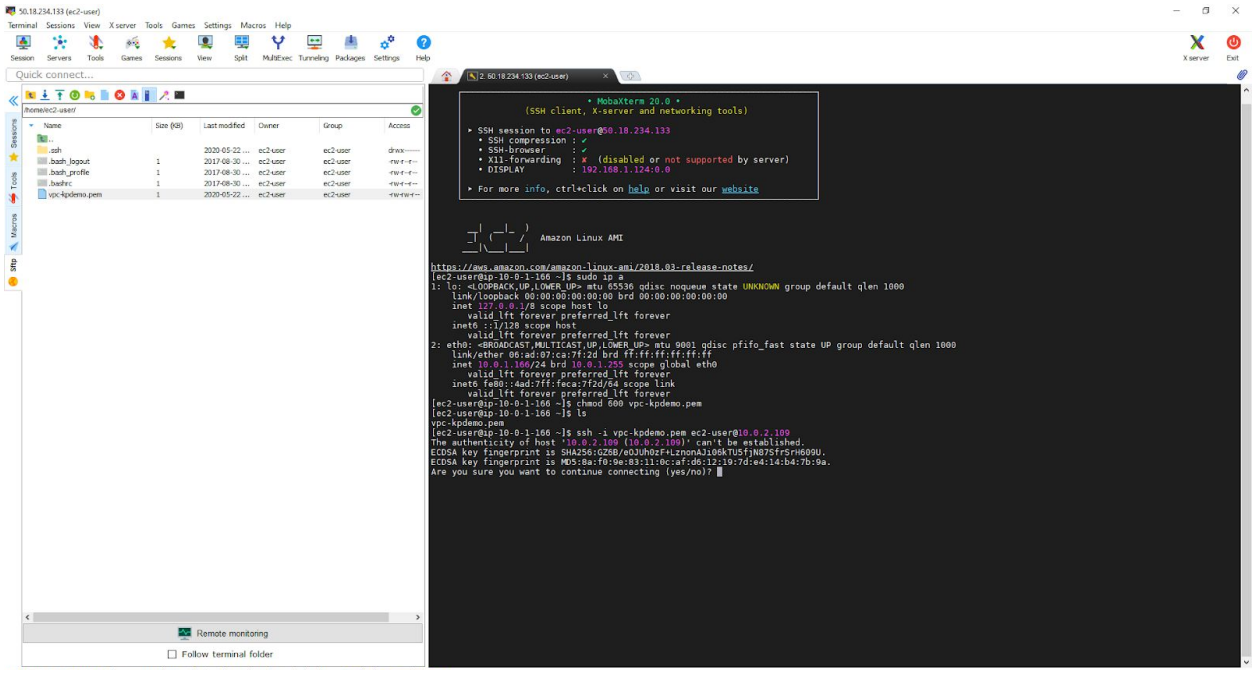
Note the vpc-kpdemo.pem file is now in the home directory.

MobaXterm



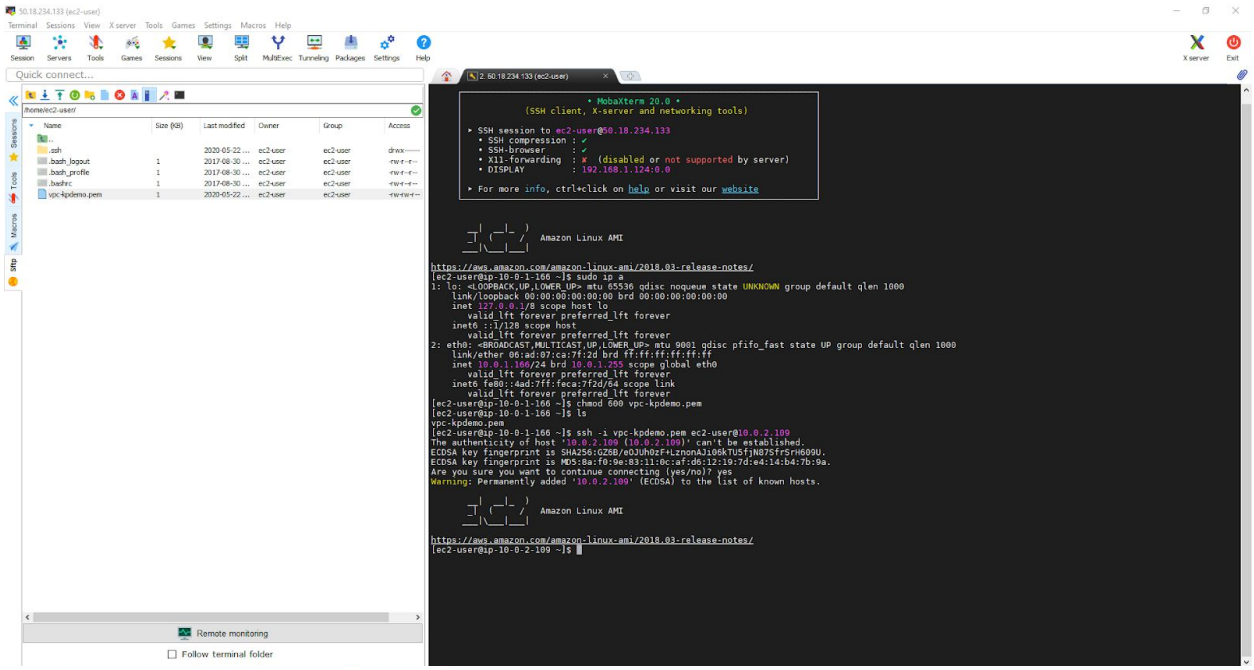
Permissions of the pem file must be changed to 600 before an SSH connection can be established to the private subnet.

MobaXterm



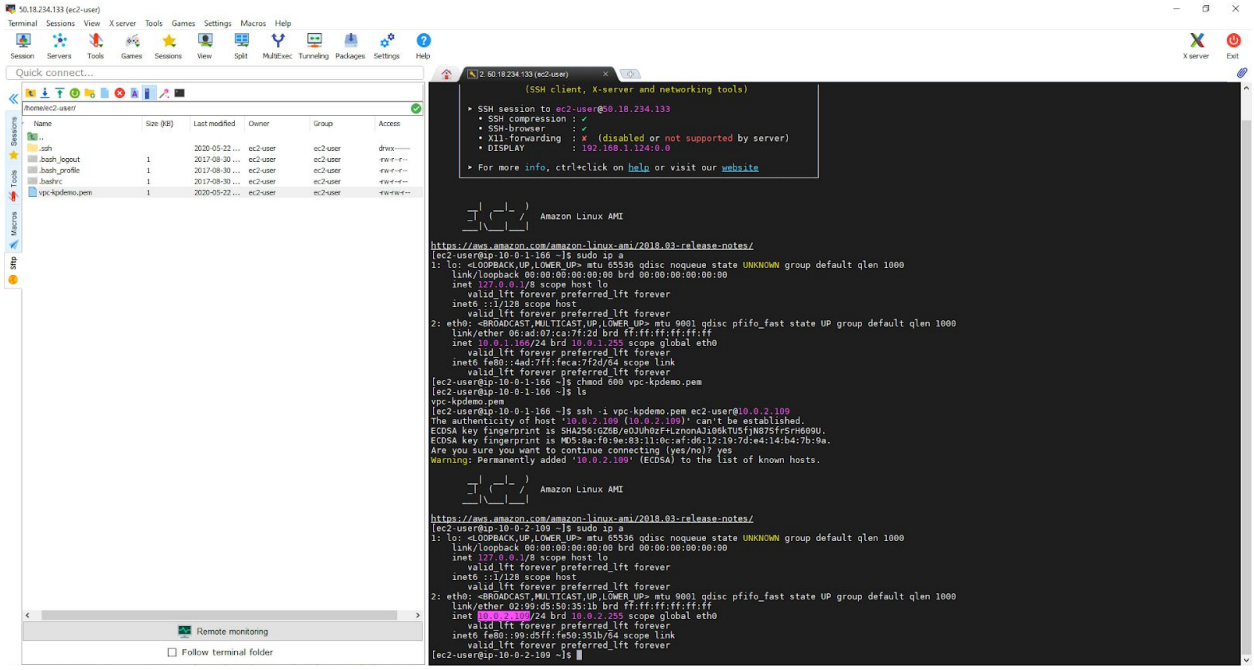
A warning that the private IPv4 address cannot be authenticated.

MobaXterm



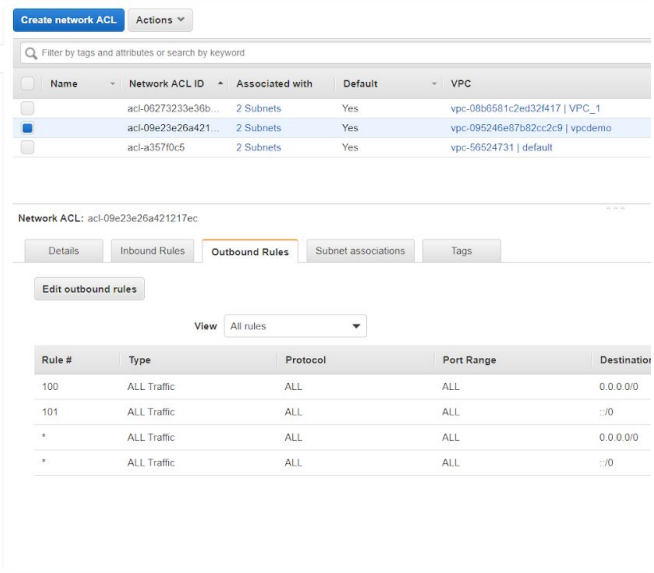
Successful connection to the private subnet through the public subnet.

MobaXterm



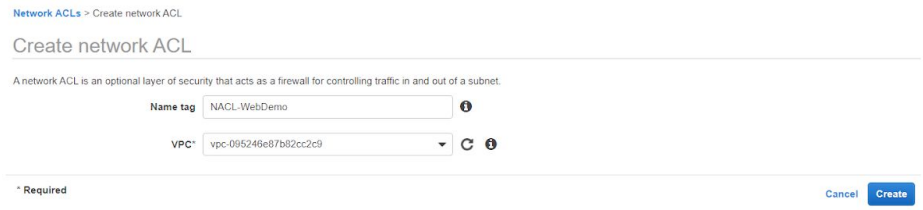
The IP is now consistent with the private IPv4 created in the vpcdemo VPC.

VPC Dashboard - Network ACLs



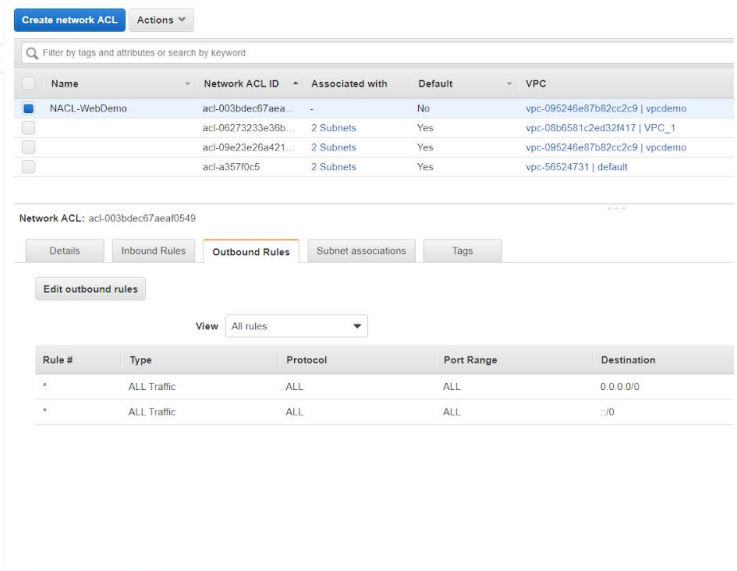
A new Access Control List (NACL-WebDemo) will close the default open ports.

Network ACLs - Create network ACL



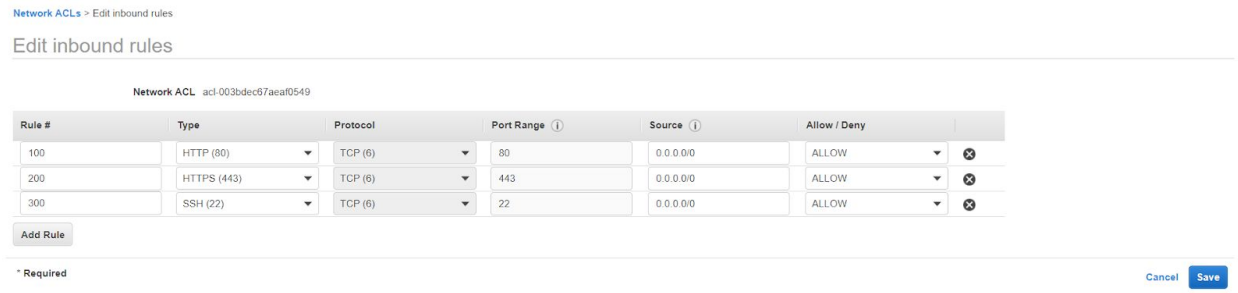
As default all ports will be in the DENY state.

VPC Dashboard - Network ACLs



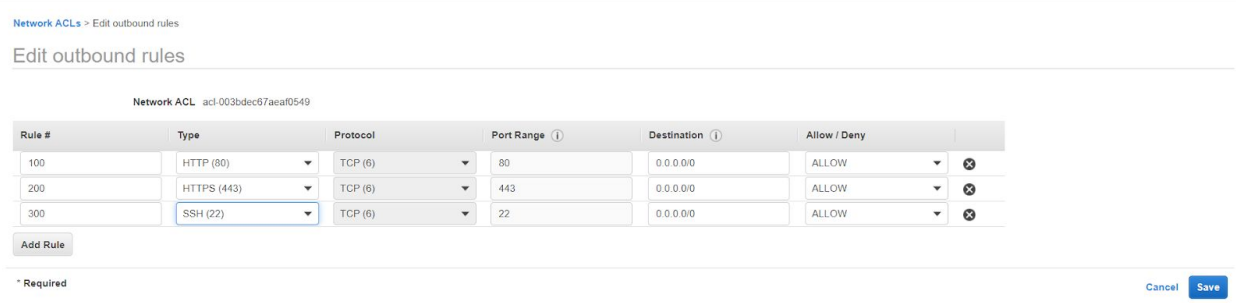
All Traffic is now in the DENY state for Outbound Rules.

Network ACLs - Edit inbound rules



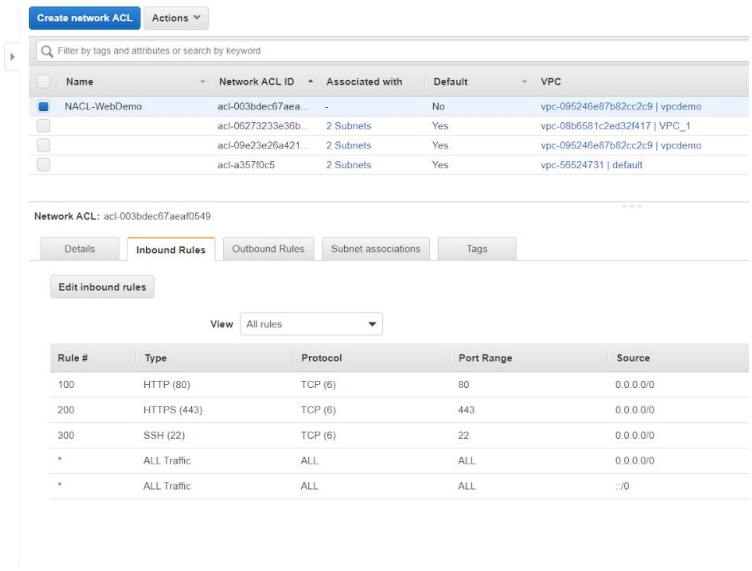
Inbound rules are edited to reflect the required ports.

Network ACLs - Edit outbound rules



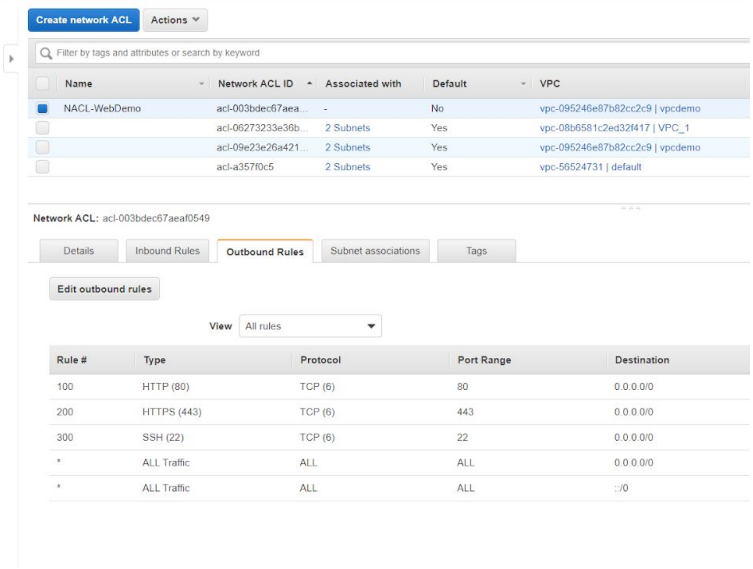
Outbound rules are now set.

VPC Dashboard - Network ACL



Inbound rules set for NACL-WebDemo

VPC Dashboard - Network ACL



Outbound rules set for NACL-WebDemo