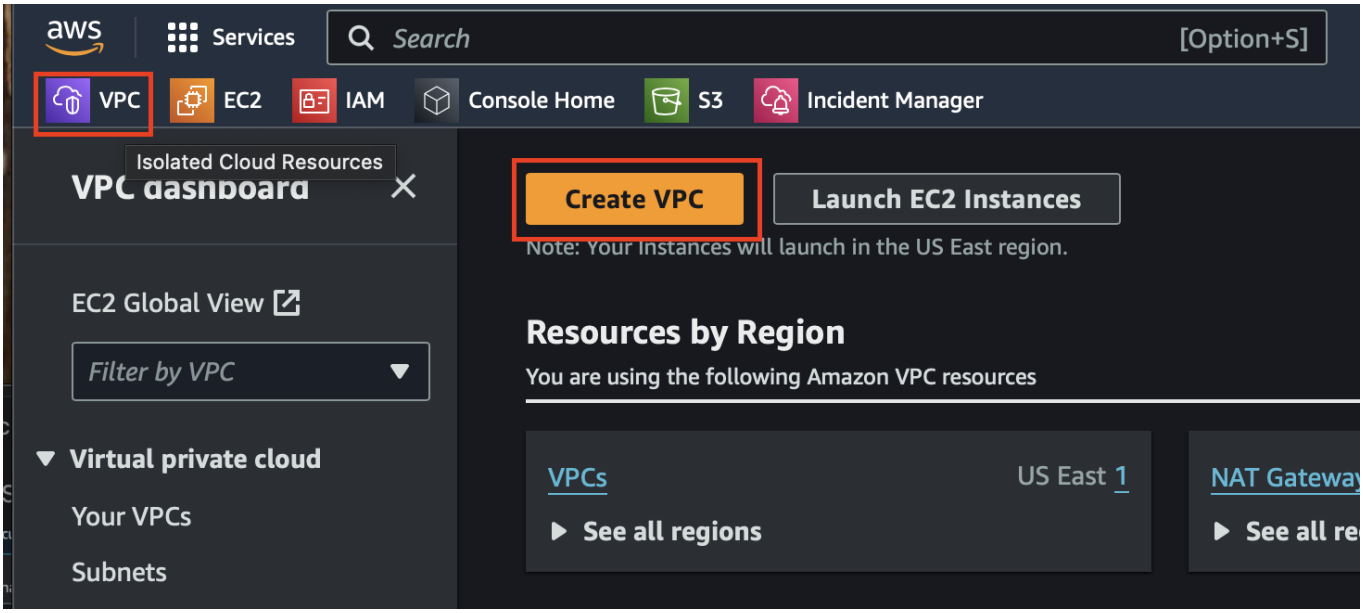
01. AWS SecOnion Lab Setup - Initial Configuration

AWS Security Operations Lab Setup

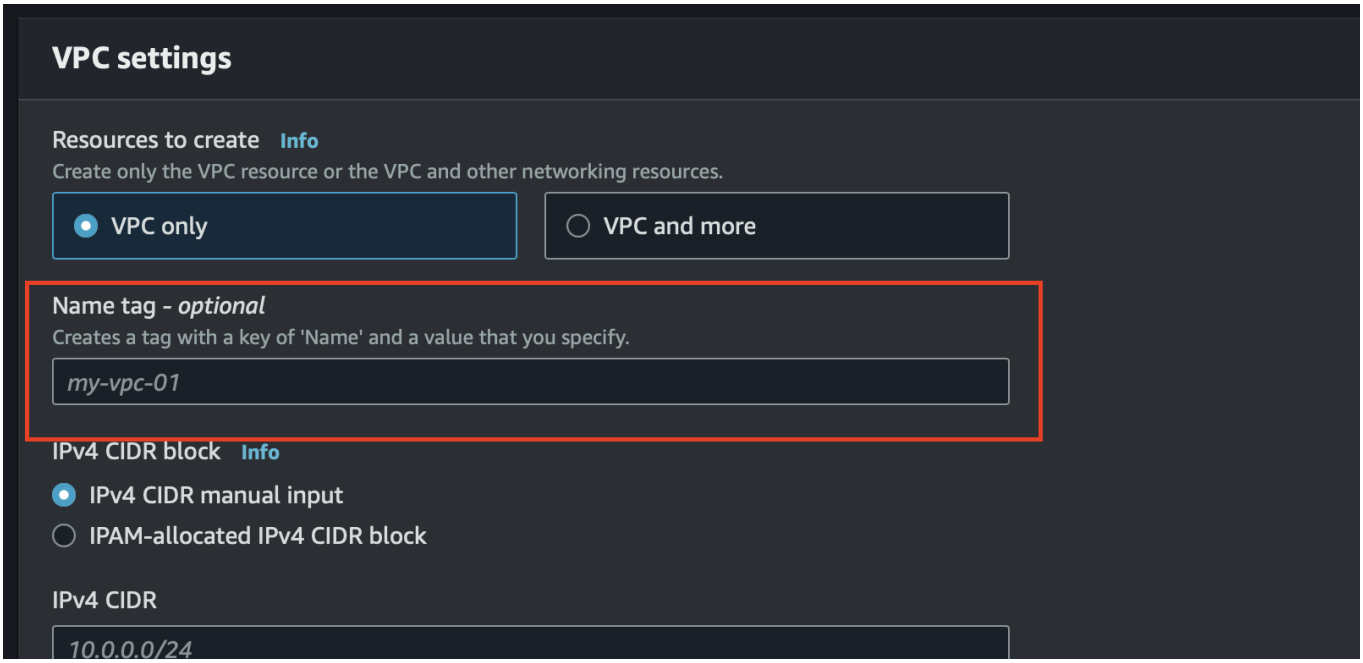
Creating the VPC

Navigate to VPC:

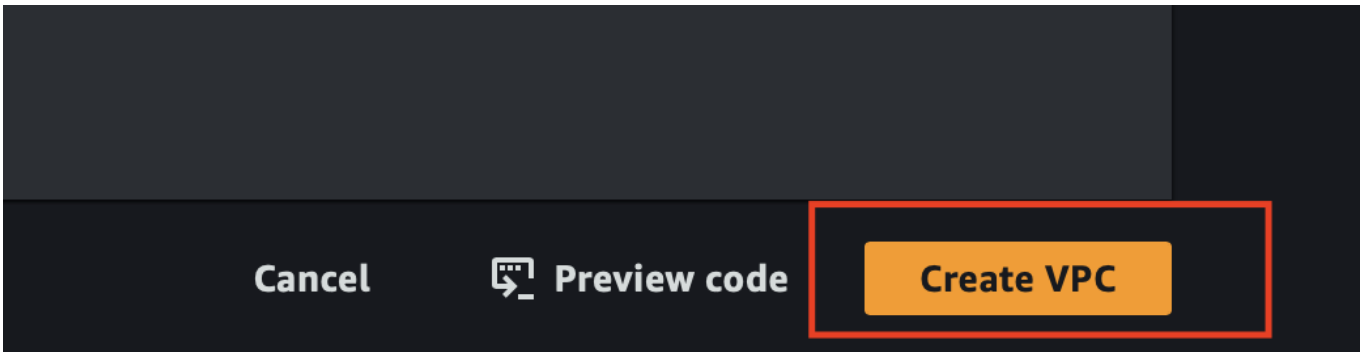


Click the Create VPC button and change the following setting:
Name tag - optional

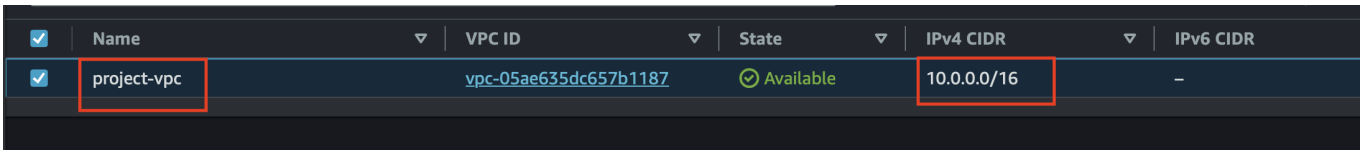
Leave all other options as default



After changing the Name tag, click Create VPC



Take note of the Name and the IPv4 CIDR
The IPv4 CIDR will be used throughout the setup to allow traffic flow through the VPC

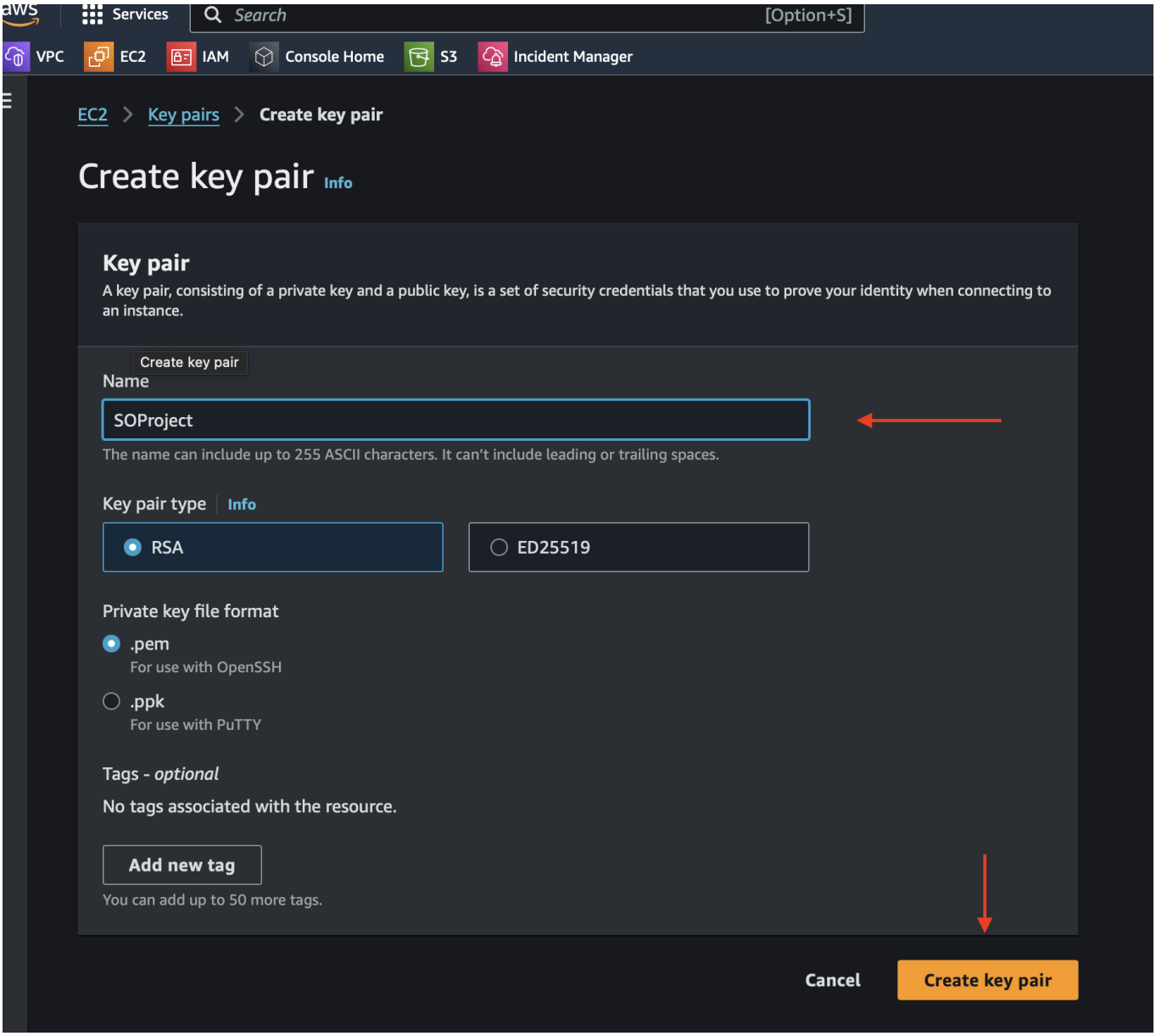


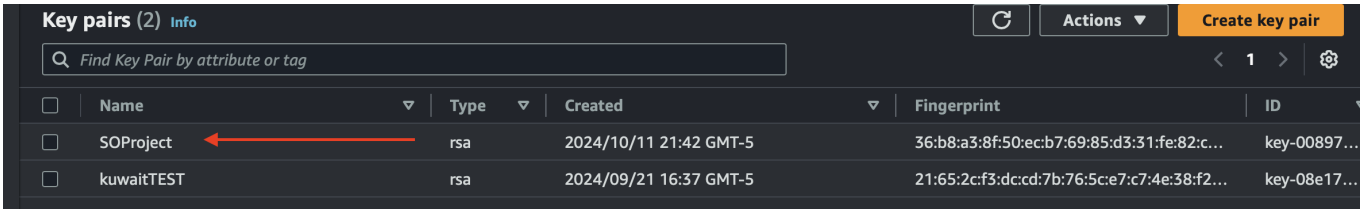
Creating a AWS Key pair

NOTE: The following OS may be beneficial to use different key type:
Windows - suggested to use .ppk with PuTty
Unix/Linux - suggested to use .pem keys

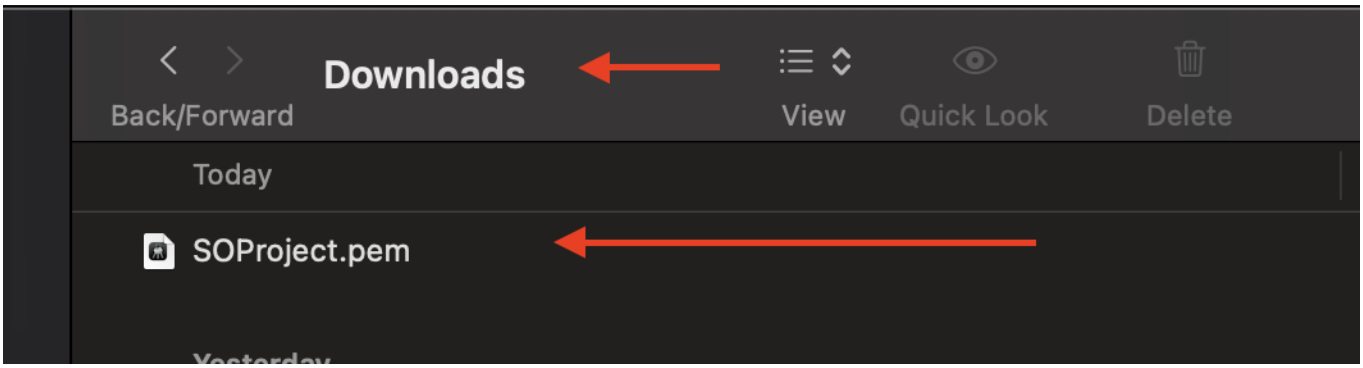
For this instruction we are using a Unix/Linux OS

Next head to EC2 > Key pairs > Create key pair





Once created the key will automatically download to your system:

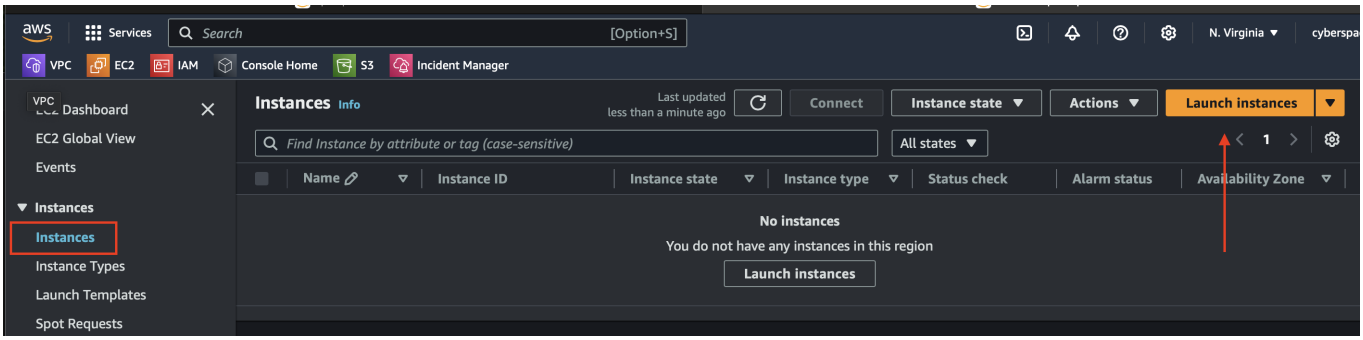


Configuring the Security Onion AMI Instance (Prelaunch)

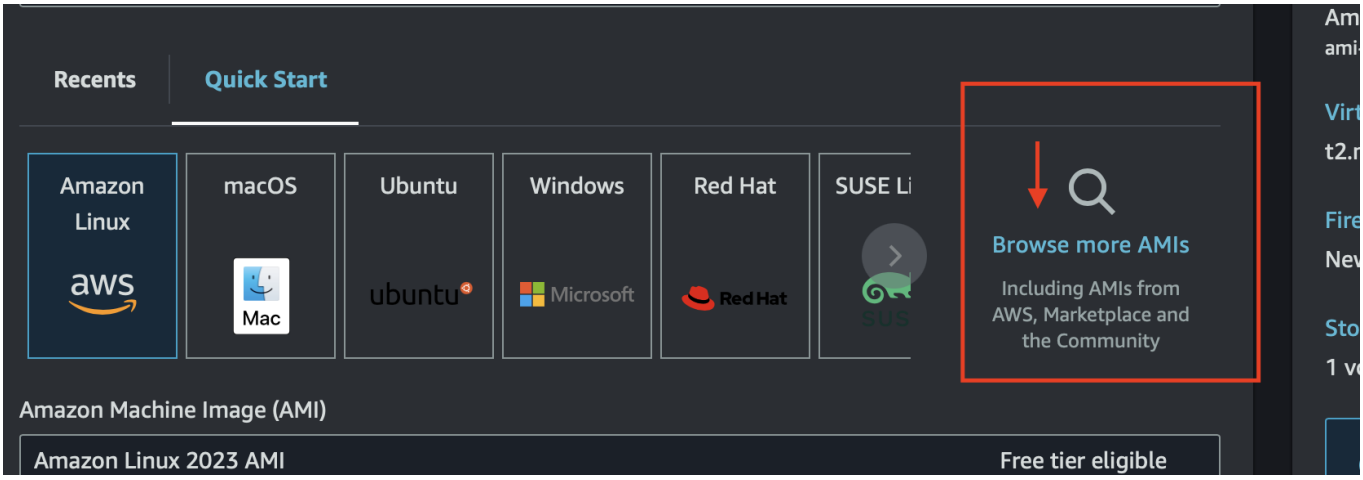
Click the EC2 tab and select "Launch instances"

NOTE: Charges are included as long as the instance is on so ensure to shutdown after use

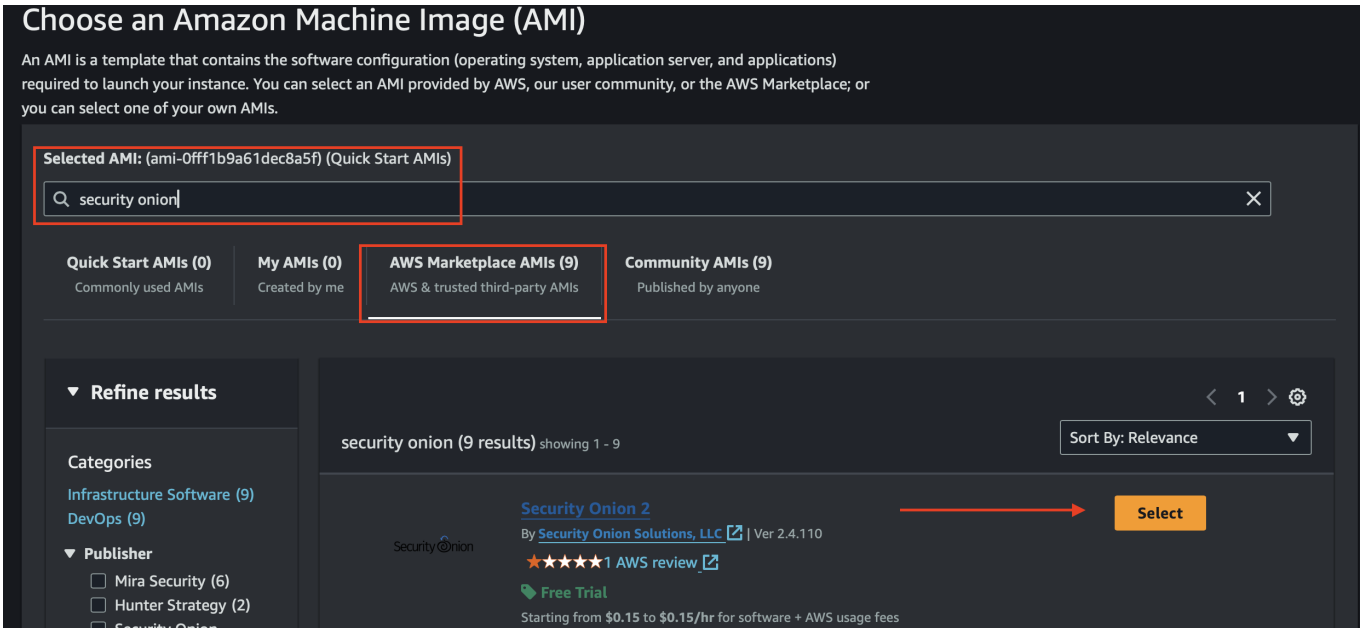
On the left hand pane click Instances > Launch Instances



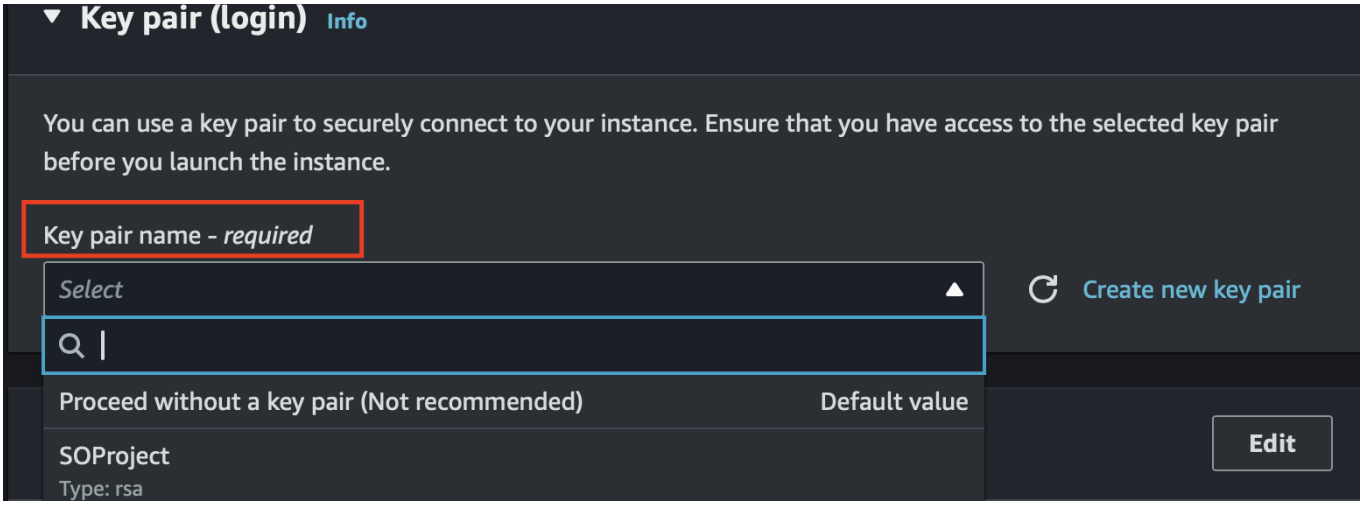
Browse more AMIs



Enter "Security Onion" and click enter and select the Security Onion AMI



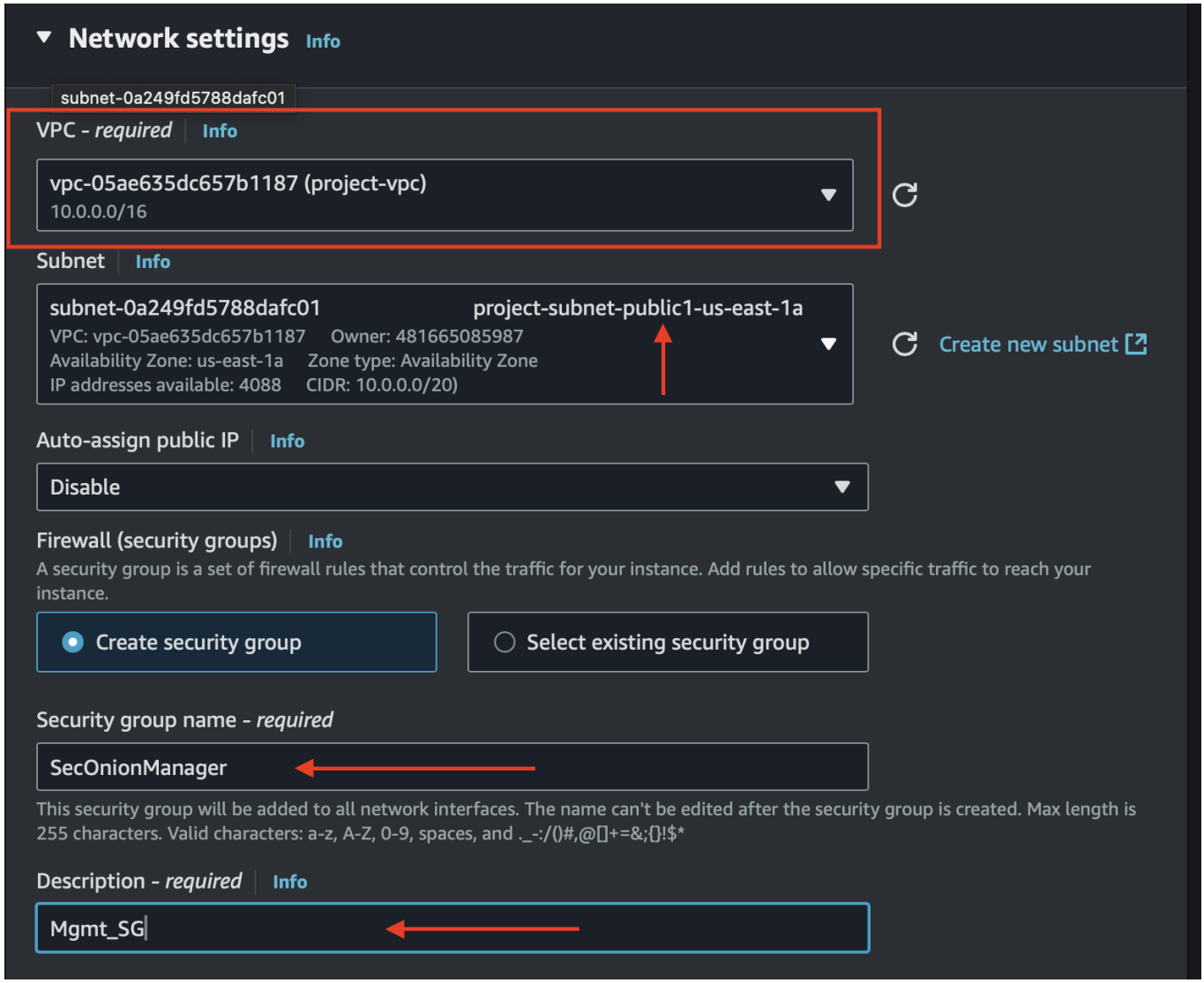
Select the Key pair you create or create a new one



Configuring Security Onion AMI Network Settings

Ensure the following settings are applied: -- Click Edit
VPC - Use the one you create initially
Subnet - Public1
Security Group Name - SecOnionManager (Or the name of your choosing)

Description - Mgmt_SG (Or the name of your choosing)



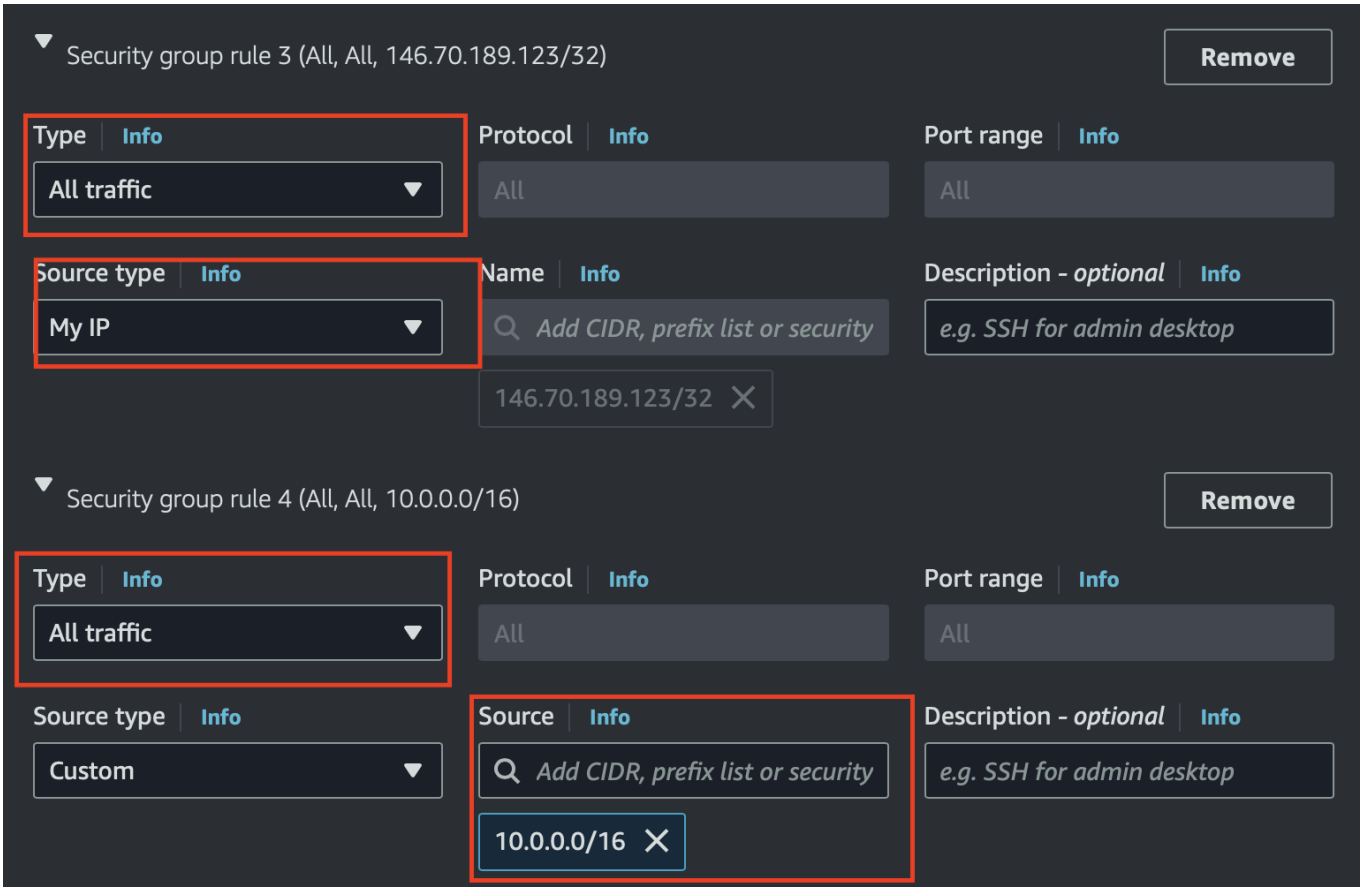
Inbound Security Group Rules

Things to do:
Add two security group rules
Add an additional network interface (monitoring/sniffing)

Add two security group rules

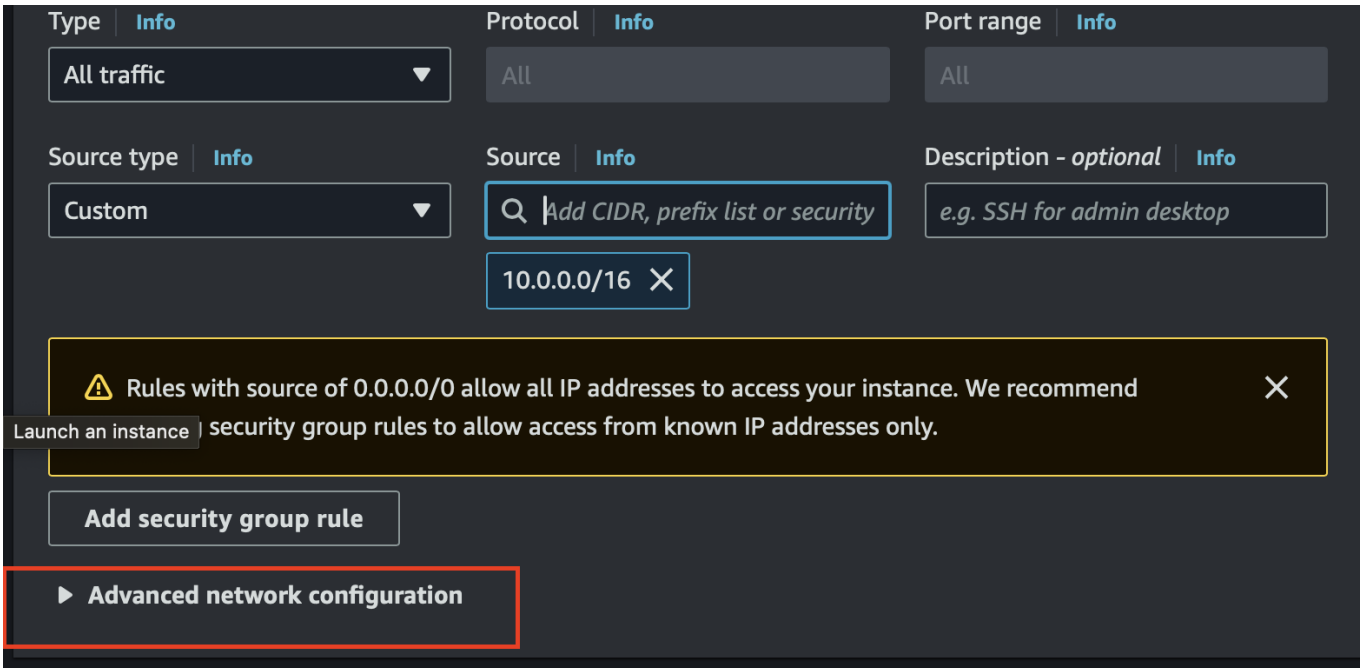
Adjust the sections in each new rule to match the screenshot
Rule3 allows all traffic to the IP

Rule 4 allows traffic flow through the VPC

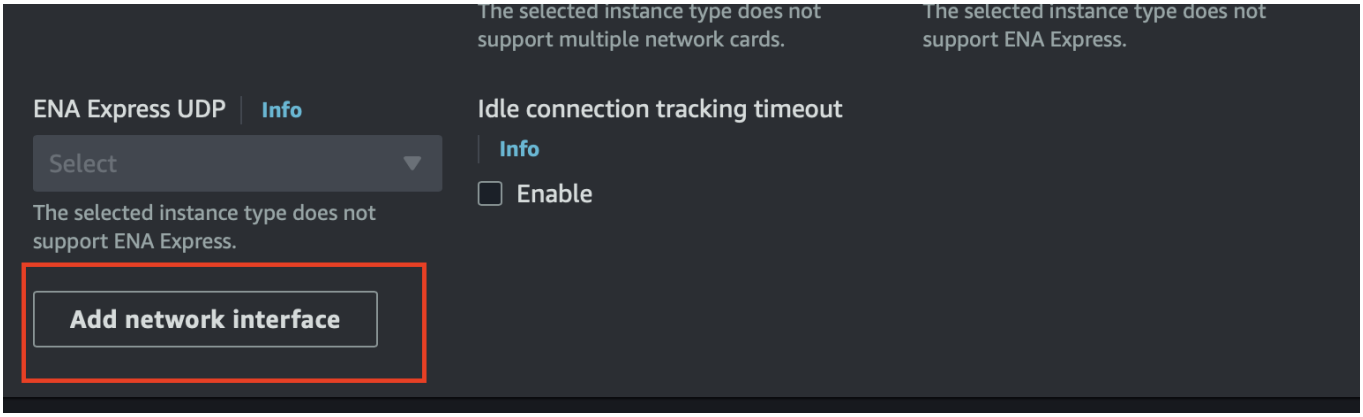


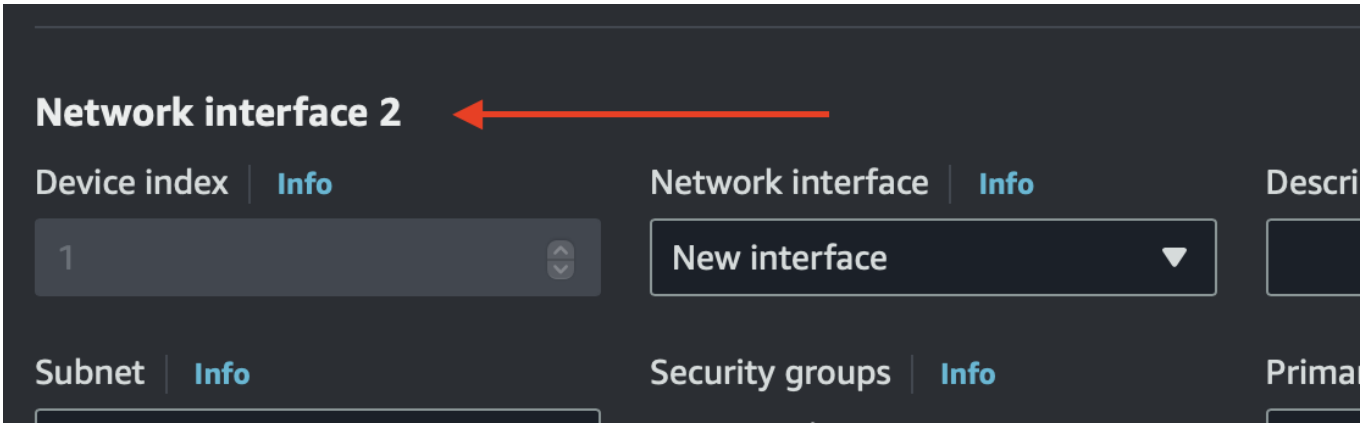
Add an additional network interface (monitoring/sniffing)

Click Advanced network configuration



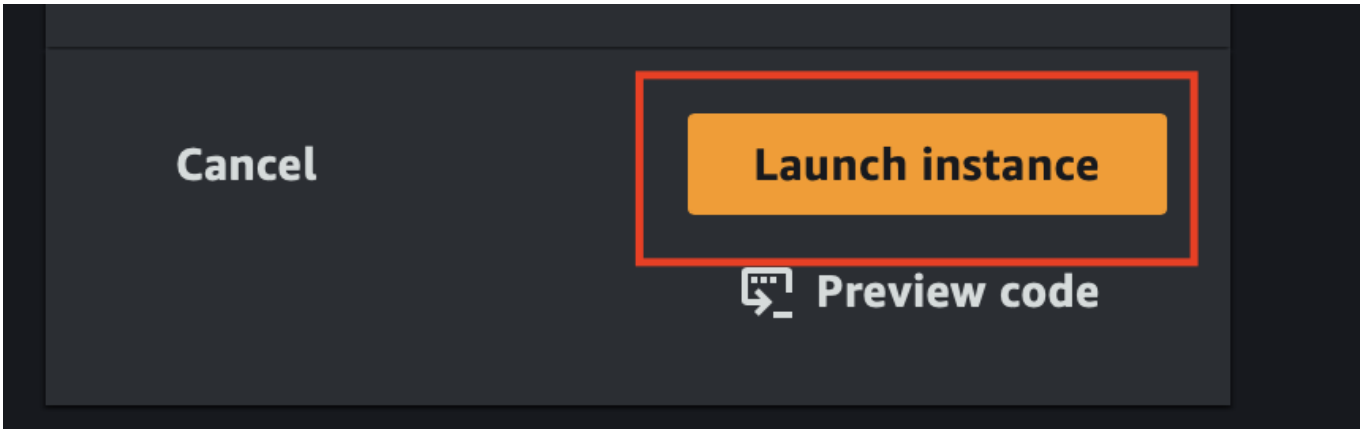
Leave the Defaults and click "Add network interface"





You are ready to launch the instance

Launch the instance



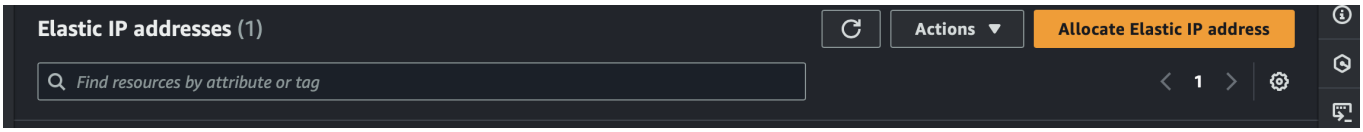
AWS Network Configuration Post Security Onion Launch

Things to do:
Associate an Elastic Public IP
Ensure the Public IP is connect

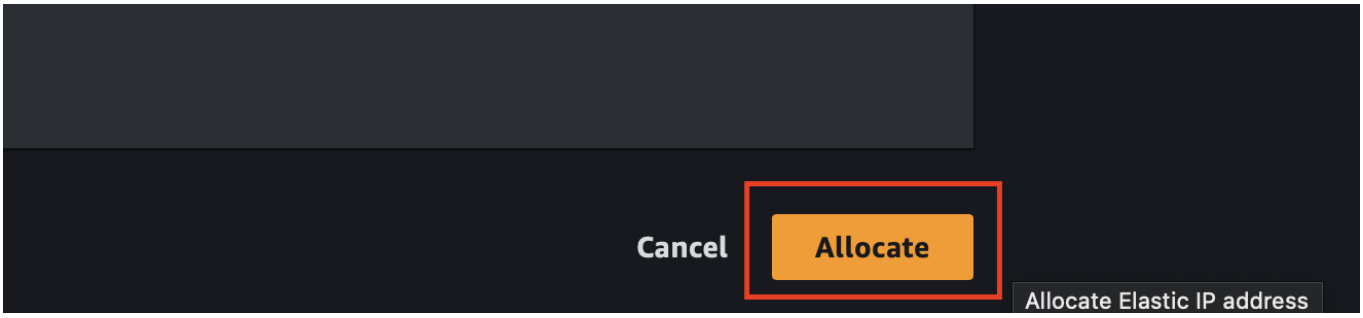
Create a Security Group for the Sniffing Interface (and remove the interface from the Manager Security Group)
Add traffic rules

Associate an Elastic Public Ip

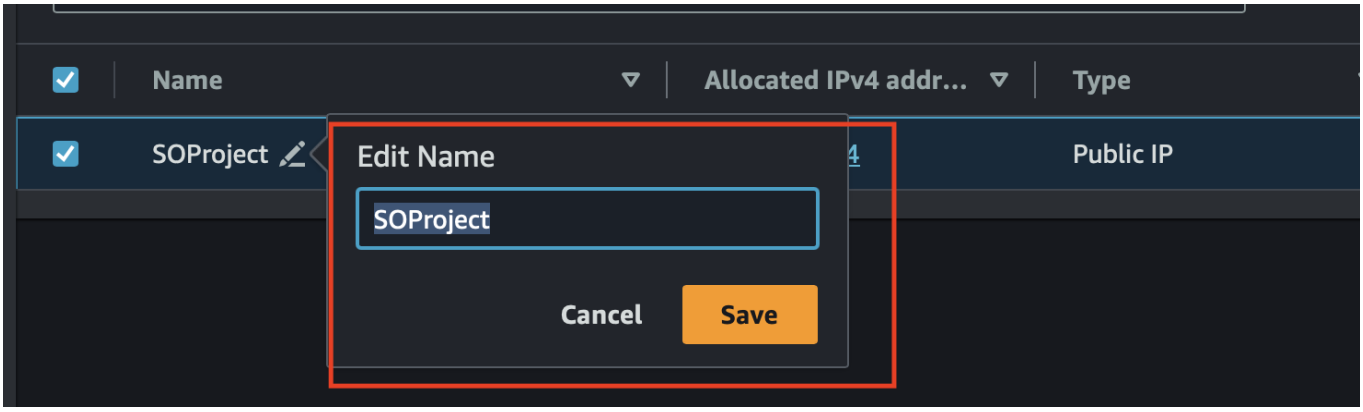
In the left pane under Network & Security, Click Elastic IPs
Click "Allocate Elastic IP address"

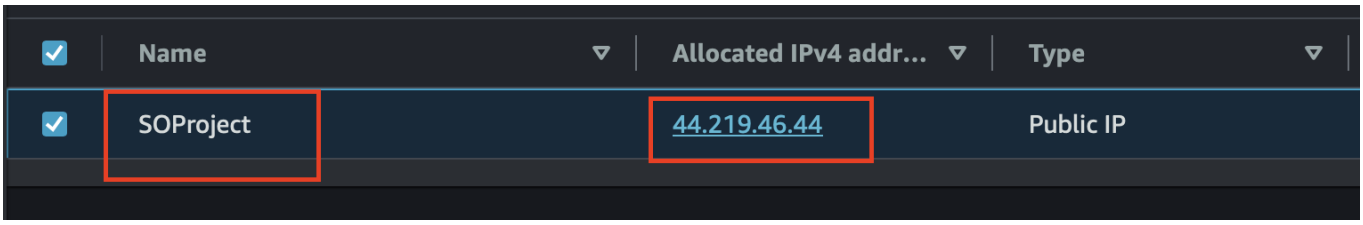


Leave the defaults and click Allocate



Edit the IP name and take note of the Allocated IP

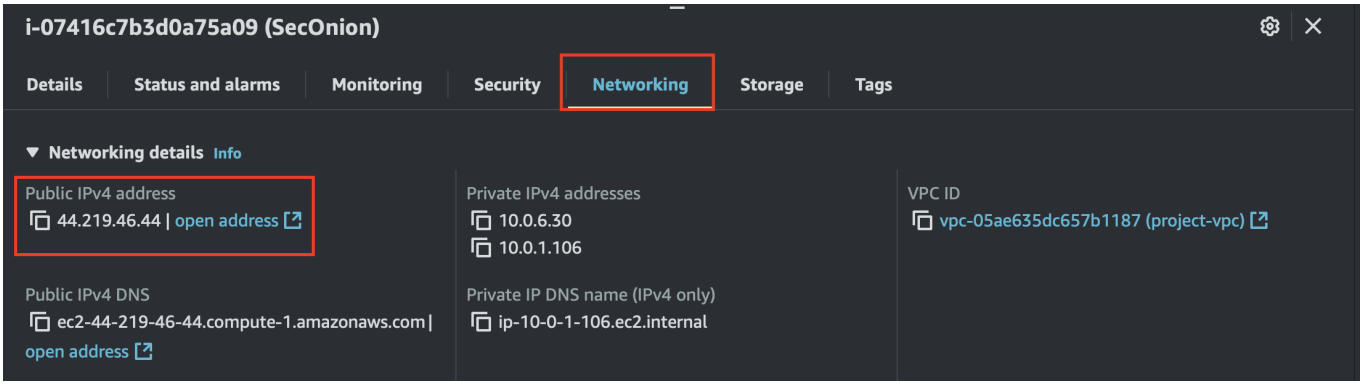




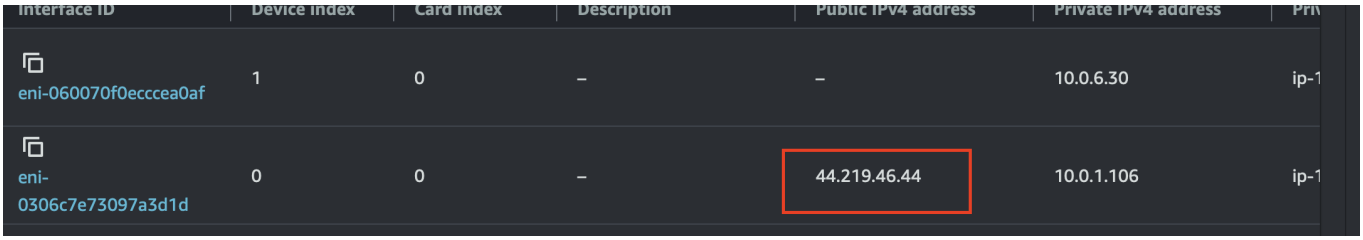
Ensure the Elastic Public IP is Properly Allocated

Navigate and click Instance > your instance > and scroll down:
Ensure there is a Public IPv4 address

If not, create and allocate a new Elastic IP



In the Network tab scroll to the bottom and take note of which interface the public IP is allocated to:

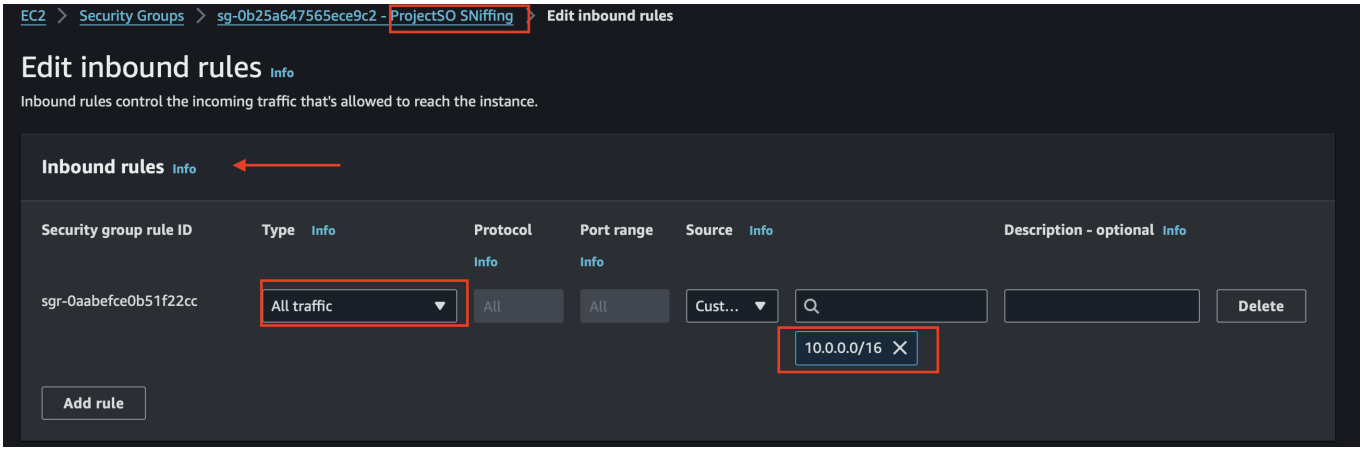


These interfaces will enable us to set the appropriate security group and traffic monitoring rules later.

Create a Security Group for the Sniffing Interface

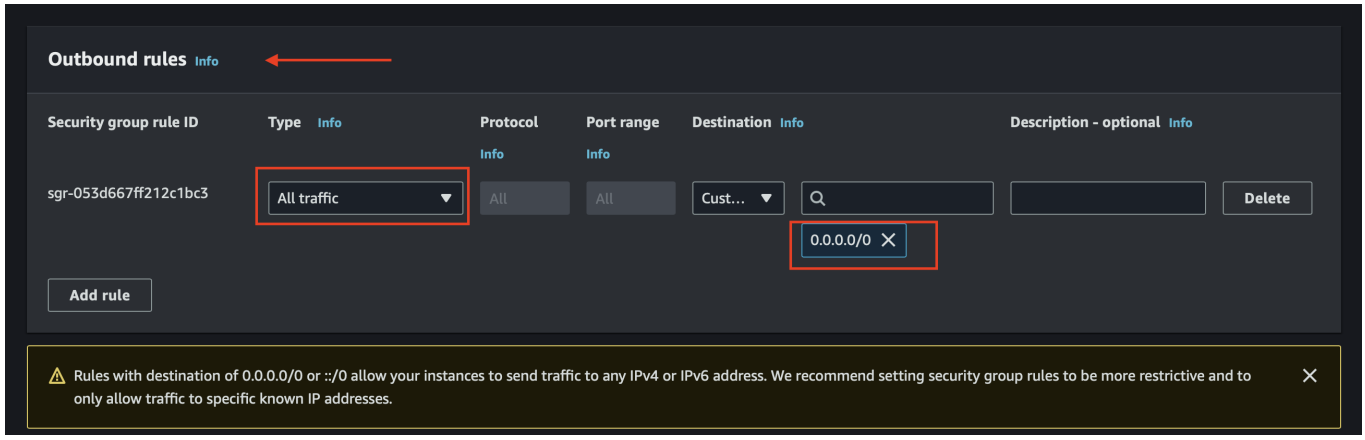
In the left pane under Network & Security, click on Security Groups (SG)
Click on "Create security group"
Select your desired name keeping in mind that this is the sniffing interface SG
Ensure the "Sniffing SG" has the follwing inbound and outbound rules

Inbound Rules:

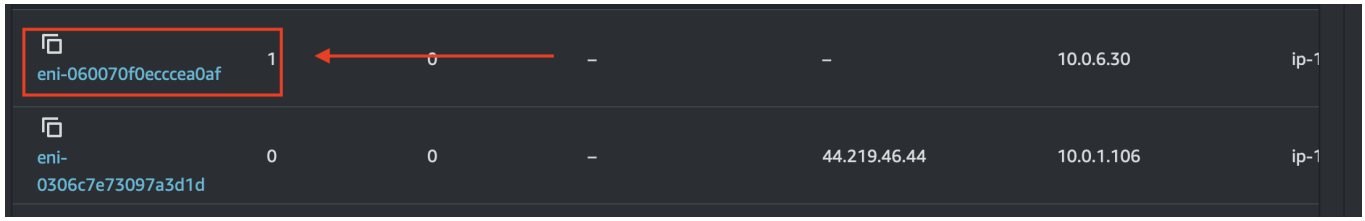


This allows all traffic inbound on the sniffing from the VPC

Outbound Rules:

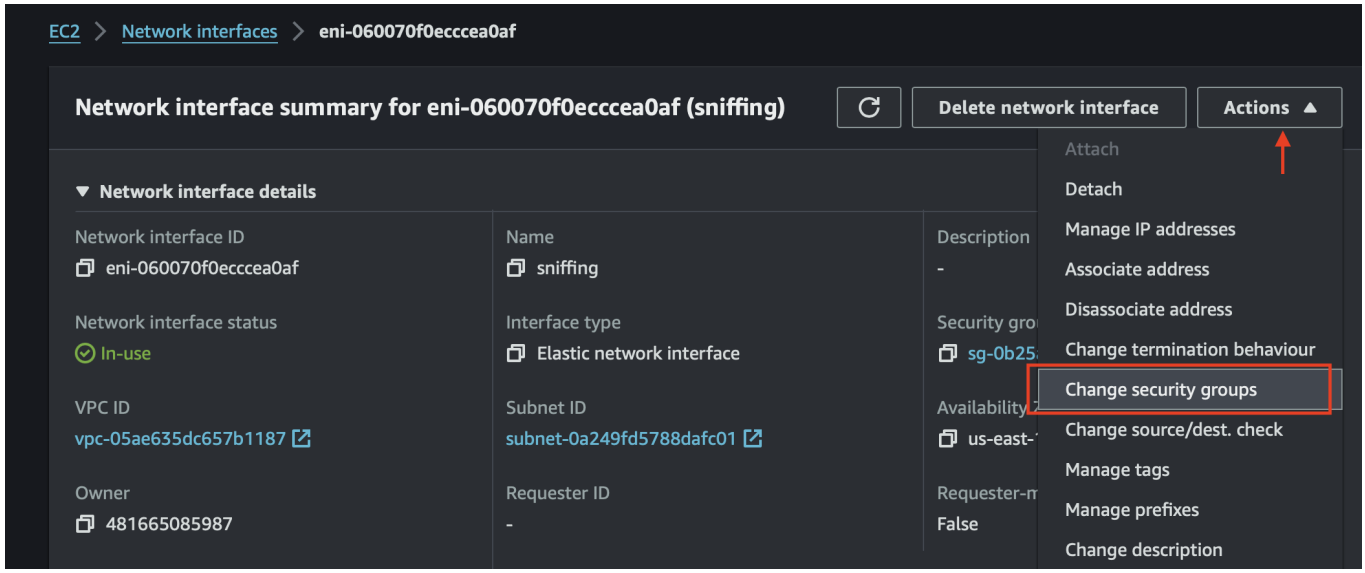


Next, head back to the Interface > Network tab an click on the interface that "IS NOT" allocated to the Elastic IP:

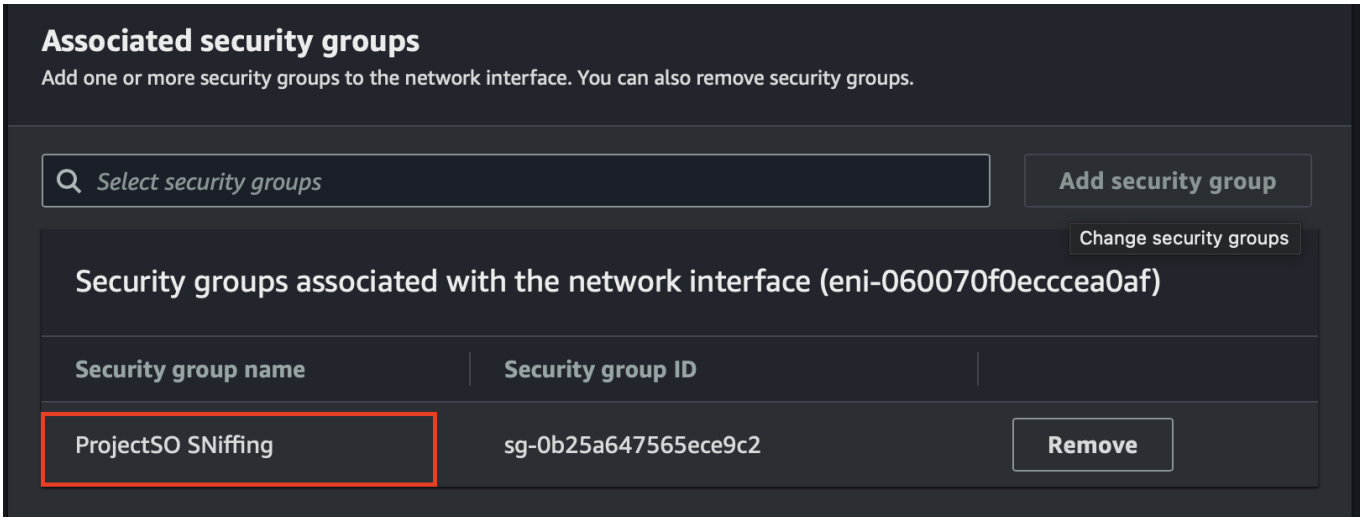


NOTE: By default, The Security Onion instance is launched with both interfaces belonging to the initial security group (management). The following steps must be taken to ensure the monitoring interface has its own Security Group:

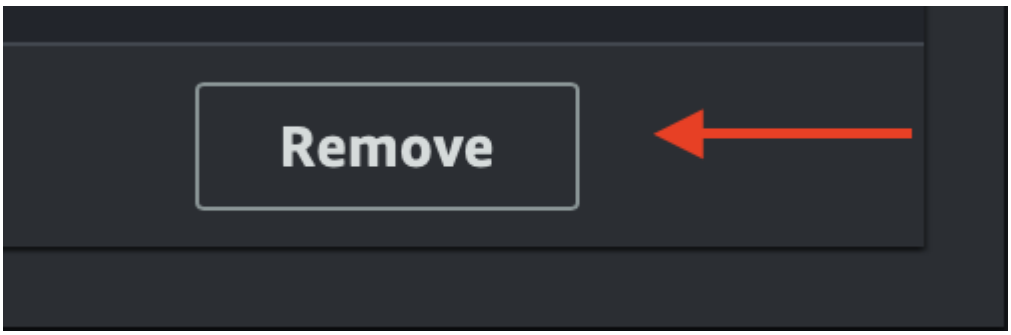
In the left pane go to Network & Security > Interfaces > and select the sniffing interface. Click on Actions > Change security groups



In the dropdown menu add the sniffing security group you created:

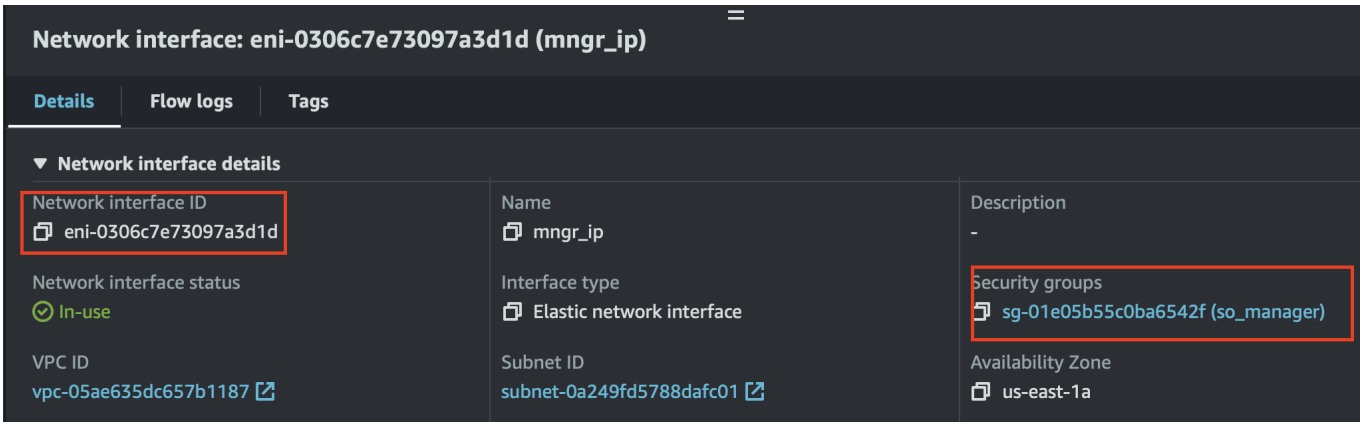


Next click Remove to disassociate the sniffing network from the "Management SG" (or the main SG associated to the Security Onion instance)



Click Save

Check to ensure both interfaces are in their respective security groups:
Manager Interface:



Sniffing Interface: