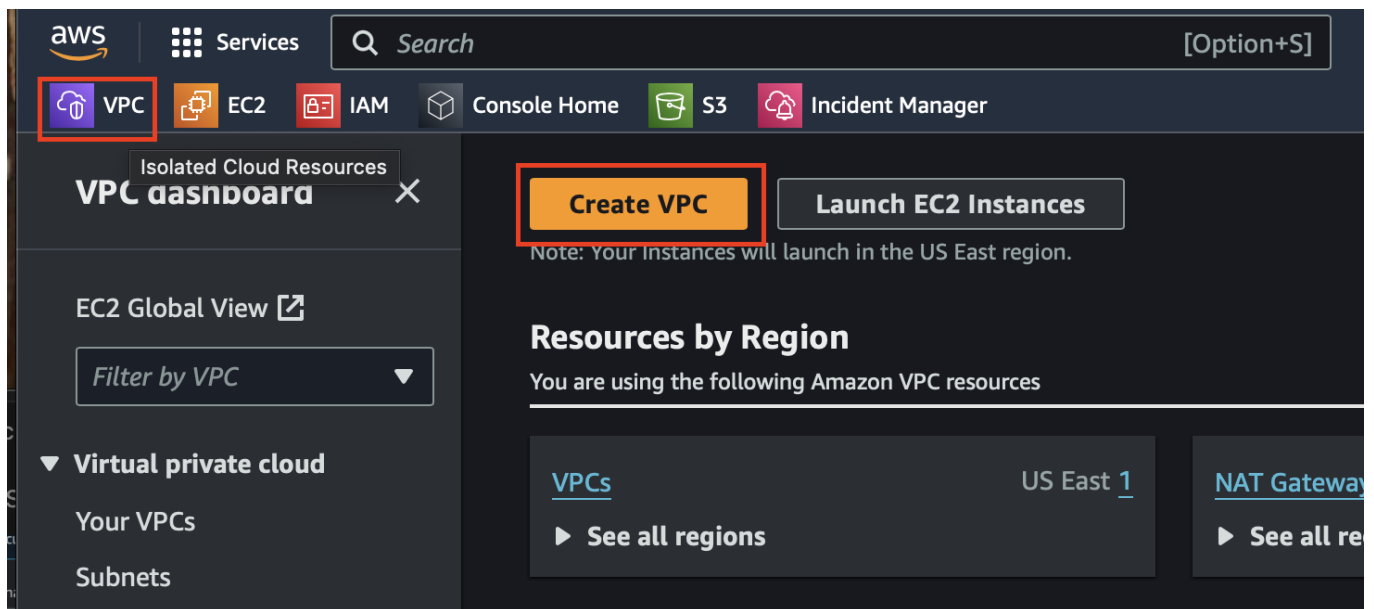


01. AWS SecOnion Lab Setup - Initial Configuration

AWS Security Operations Lab Setup

Creating the VPC

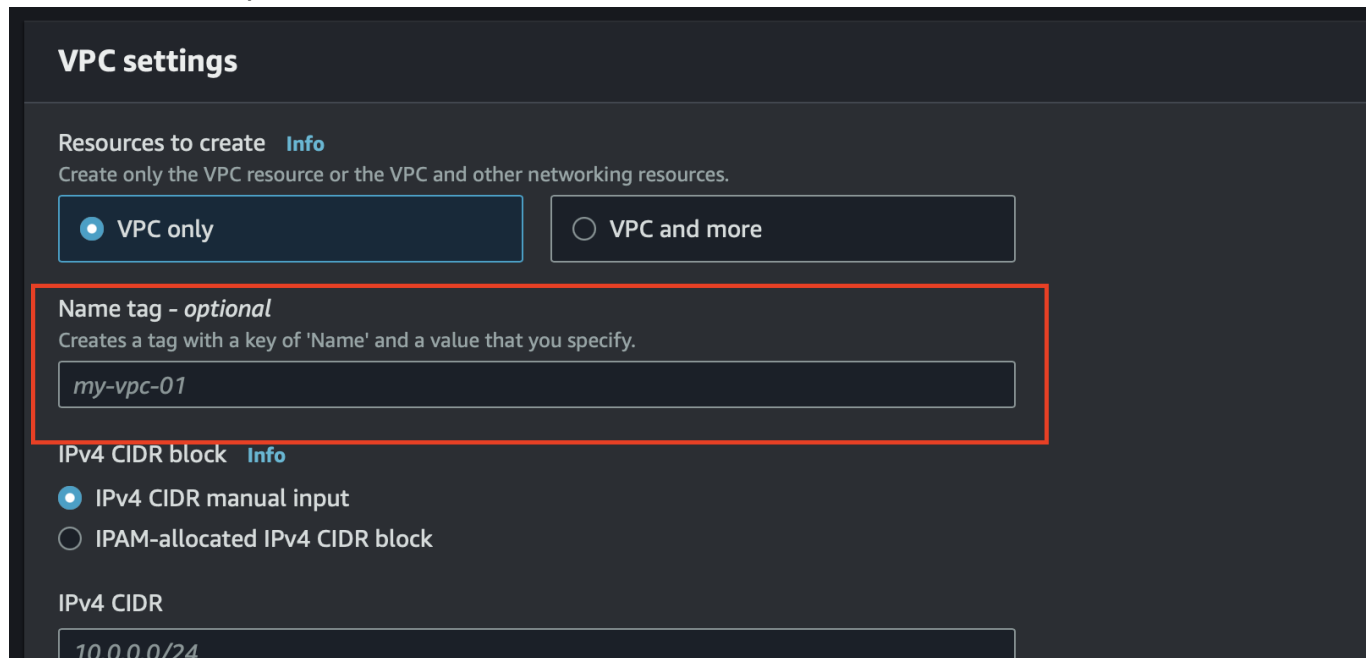
Navigate to VPC:



Click the **Create VPC** button and change the following setting:

Name tag - optional

Leave all other options as default



VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

my-vpc-01

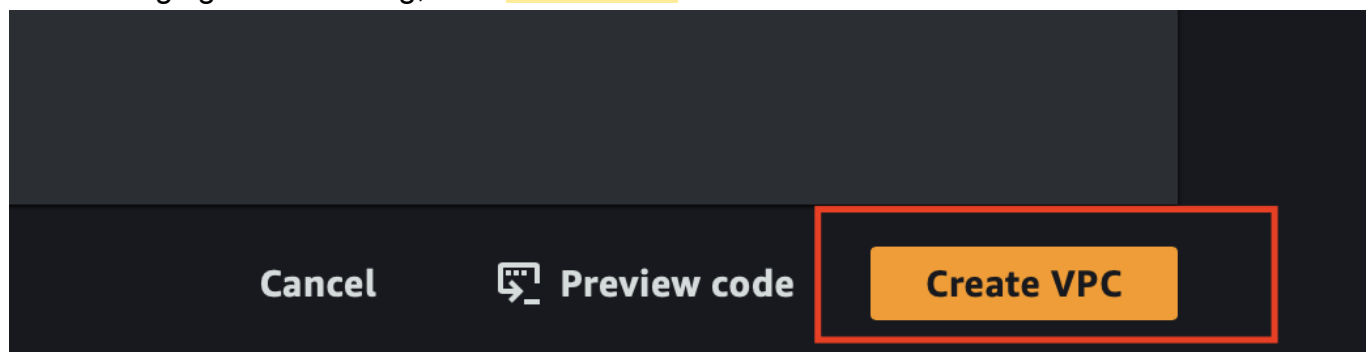
IPv4 CIDR block [Info](#)


☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/24

After changing the Name tag, click **Create VPC**



Cancel  Preview code **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

<input checked="" type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	project-vpc	vpc-05ae635dc657b1187	Available	10.0.0.0/16	-

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

aws Services Search [Option+S]

VPC EC2 IAM Console Home S3 Incident Manager

EC2 > Key pairs > Create key pair

Create key pair Info

Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Create key pair

Name
SOProject
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type Info
☒ RSA ☐ ED25519

Private key file format
☒ .pem For use with OpenSSH
☐ .ppk For use with PuTTY

Tags - optional
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.

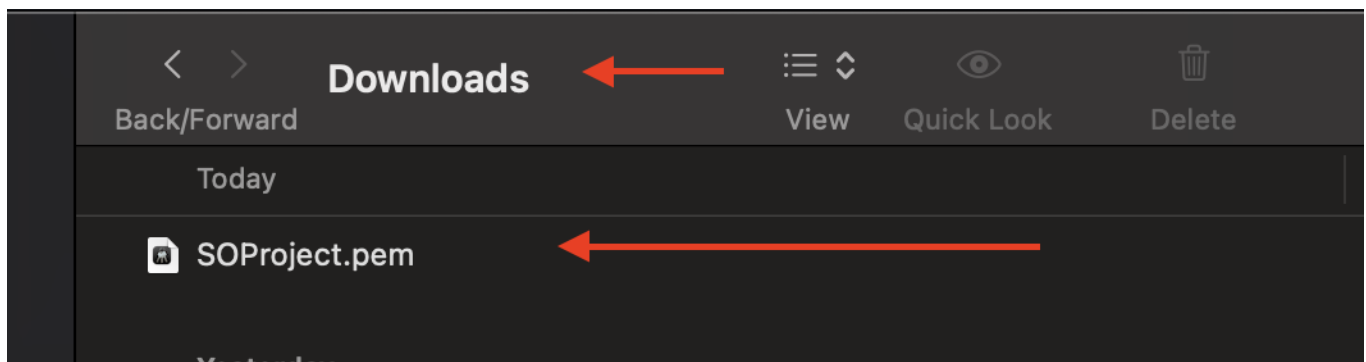
Cancel **Create key pair**

Key pairs (2) Info

Find Key Pair by attribute or tag

	Name	Type	Created	Fingerprint	ID
<input type="checkbox"/>	SOProject	rsa	2024/10/11 21:42 GMT-5	36:b8:a3:8f:50:ec:b7:69:85:d3:31:fe:82:c...	key-00897...
<input type="checkbox"/>	kuwaitTEST	rsa	2024/09/21 16:37 GMT-5	21:65:2c:f3:dc:cd:7b:76:5c:e7:c7:4e:38:f2...	key-08e17...

Once created the key will automatically download to your system:

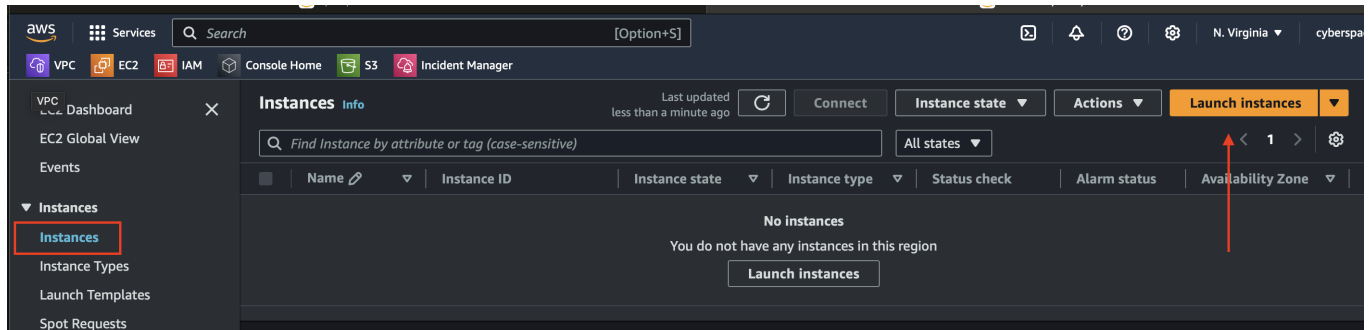


Configuring the Security Onion AMI Instance (Prelaunch)

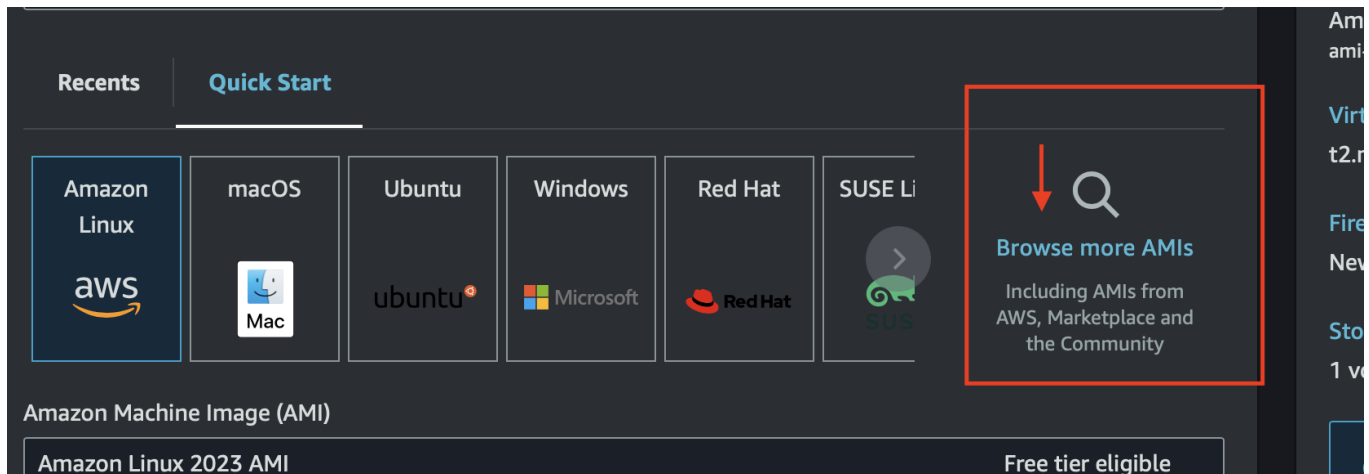
Click the EC2 tab and select "Launch instances"

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

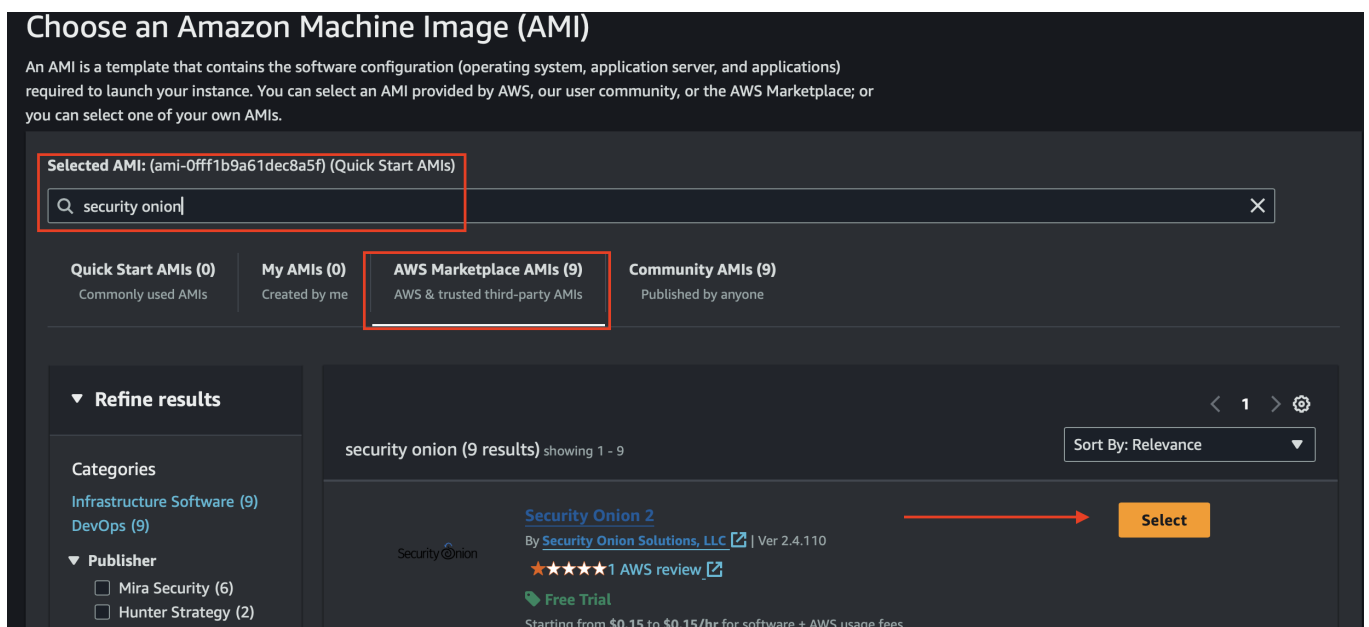
On the left hand pane click Instances > Launch Instances



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

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▲

Q |

Proceed without a key pair (Not recommended) Default value

SOProject
Type: rsa

Create new key pair

Edit

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)

▼ **Network settings** [Info](#)

subnet-0a249fd5788dafc01

VPC - required [Info](#)

vpc-05ae635dc657b1187 (project-vpc)
10.0.0.0/16

Subnet [Info](#)

subnet-0a249fd5788dafc01 project-subnet-public1-us-east-1a
VPC: vpc-05ae635dc657b1187 Owner: 481665085987
Availability Zone: us-east-1a Zone type: Availability Zone
IP addresses available: 4088 CIDR: 10.0.0.0/20

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required

SecOnionManager

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and . _ - / () # , @ [] + = & ; ! \$ *

Description - required [Info](#)

Mgmt_SG

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

▼ Security group rule 3 (All, All, 146.70.189.123/32) Remove

Type Info
All traffic ▼

Protocol Info
All

Port range Info
All

Source type Info
My IP ▼

Name Info

146.70.189.123/32 ✕

Description - optional Info

▼ Security group rule 4 (All, All, 10.0.0.0/16) Remove

Type Info
All traffic ▼

Protocol Info
All

Port range Info
All

Source type Info
Custom ▼

Source Info

10.0.0.0/16 ✕

Description - optional Info

Add an additional network interface (monitoring/sniffing)

Click Advanced network configuration

Type Info
All traffic ▼

Protocol Info
All

Port range Info
All

Source type Info
Custom ▼

Source Info

10.0.0.0/16 ✕

Description - optional Info

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend ✕

Launch an instance security group rules to allow access from known IP addresses only.

Add security group rule

► Advanced network configuration

Leave the Defaults and click "Add network interface"

The screenshot shows the AWS console configuration for a network interface. At the top, there are two error messages: "The selected instance type does not support multiple network cards." and "The selected instance type does not support ENA Express." Below these, there are sections for "ENA Express UDP" (with a dropdown menu set to "Select" and a message "The selected instance type does not support ENA Express.") and "Idle connection tracking timeout" (with an "Info" link and an "Enable" checkbox). A red rectangle highlights the "Add network interface" button.

The screenshot shows the AWS console configuration for a network interface. At the top, there is a section for "Network interface 2" with a red arrow pointing to it. Below this, there are sections for "Device index" (with a dropdown menu set to "1"), "Network interface" (with a dropdown menu set to "New interface"), "Subnet" (with an "Info" link), "Security groups" (with an "Info" link), and "Primary" (with a dropdown menu). A red arrow points to the "Network interface 2" section.

You are ready to launch the instance

Launch the instance

The screenshot shows the AWS console configuration for a network interface. At the top, there is a section for "Network interface 2" with a red arrow pointing to it. Below this, there are sections for "Device index" (with a dropdown menu set to "1"), "Network interface" (with a dropdown menu set to "New interface"), "Subnet" (with an "Info" link), "Security groups" (with an "Info" link), and "Primary" (with a dropdown menu). A red arrow points to the "Network interface 2" section.

AWS Network Configuration Post Security Onion Launch

Things to do:

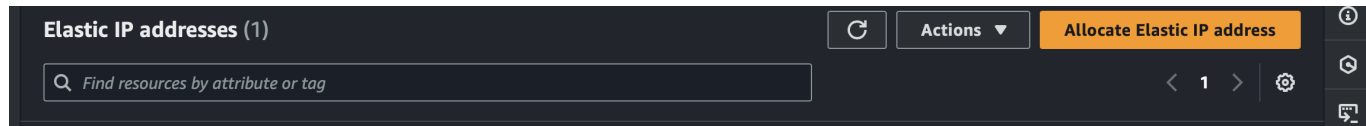
Associate an Elastic Public IP

Ensure the Public IP is connect

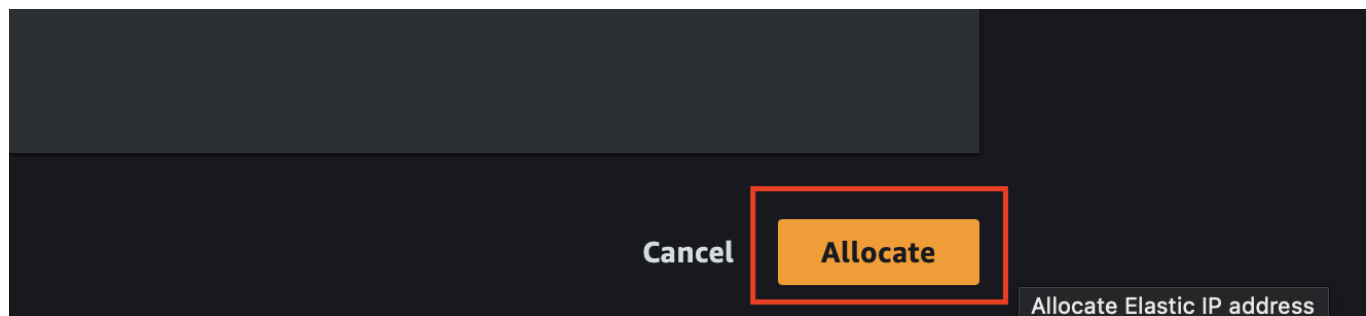
Create a Security Group for the Sniffing Interface (and remove the interface from the Manager Security Group)
Add traffic rules

Associate an Elastic Public Ip

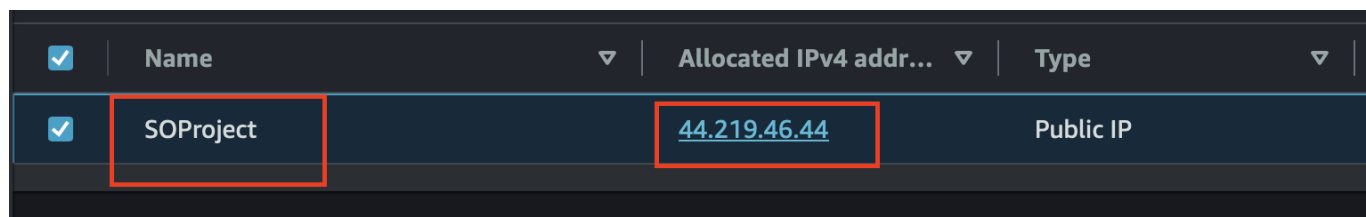
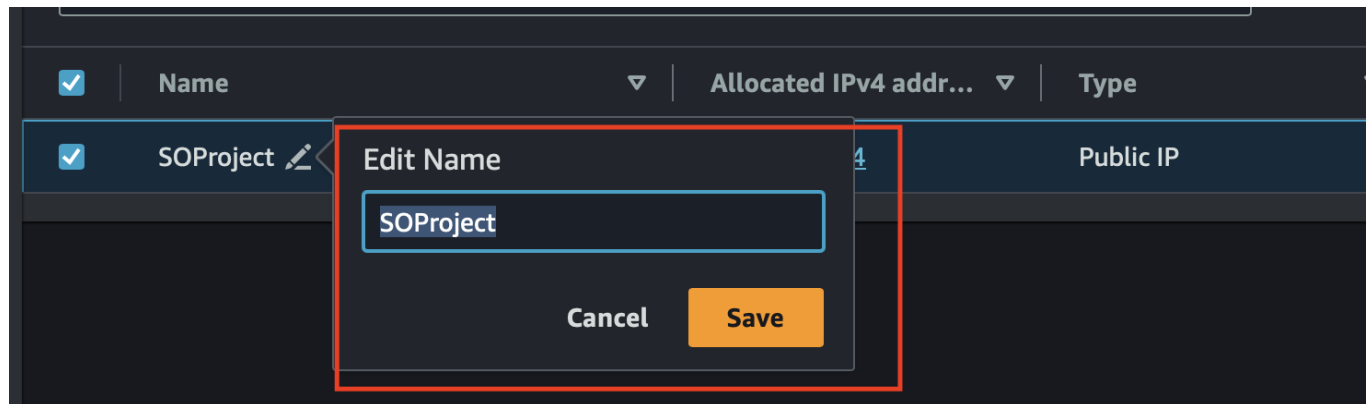
In the left pane under Network & Security, Click Elastic IPs
Click "Allocate Elastic IP address"



Leave the defaults and click Allocate



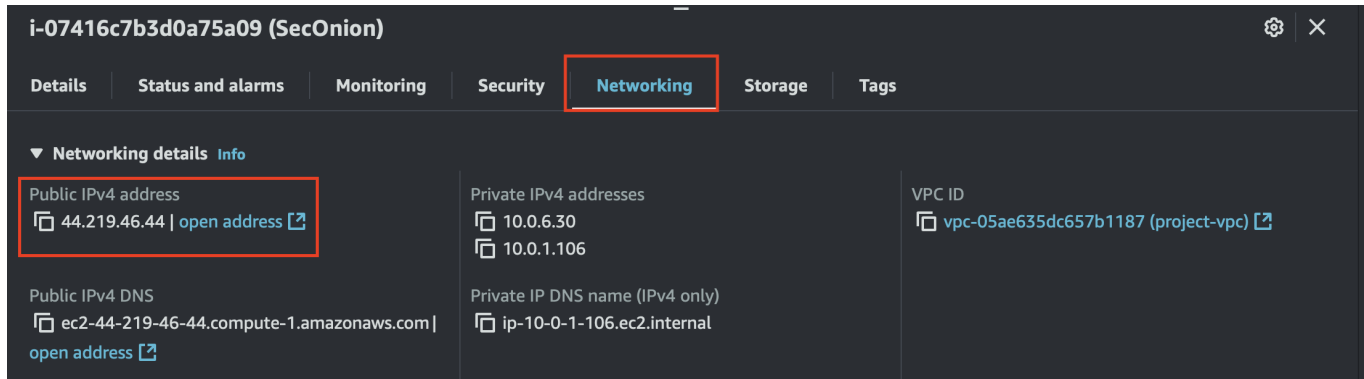
Edit the IP name and take note of the Allocated IP



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



i-07416c7b3d0a75a09 (SecOnion)

Details | Status and alarms | Monitoring | Security | **Networking** | Storage | Tags

▼ Networking details Info

Public IPv4 address
44.219.46.44 | [open address](#)

Private IPv4 addresses
10.0.6.30
10.0.1.106

VPC ID
vpc-05ae635dc657b1187 (project-vpc)

Public IPv4 DNS
ec2-44-219-46-44.compute-1.amazonaws.com | [open address](#)

Private IP DNS name (IPv4 only)
ip-10-0-1-106.ec2.internal

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

Interface ID	Device index	Card index	Description	Public IPv4 address	Private IPv4 address	Private IP DNS name
eni-060070f0ecccea0af	1	0	—	—	10.0.6.30	ip-10-0-1-106.ec2.internal
eni-0306c7e73097a3d1d	0	0	—	44.219.46.44	10.0.1.106	ip-10-0-1-106.ec2.internal

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

Create a Security Group for the Sniffing Interface

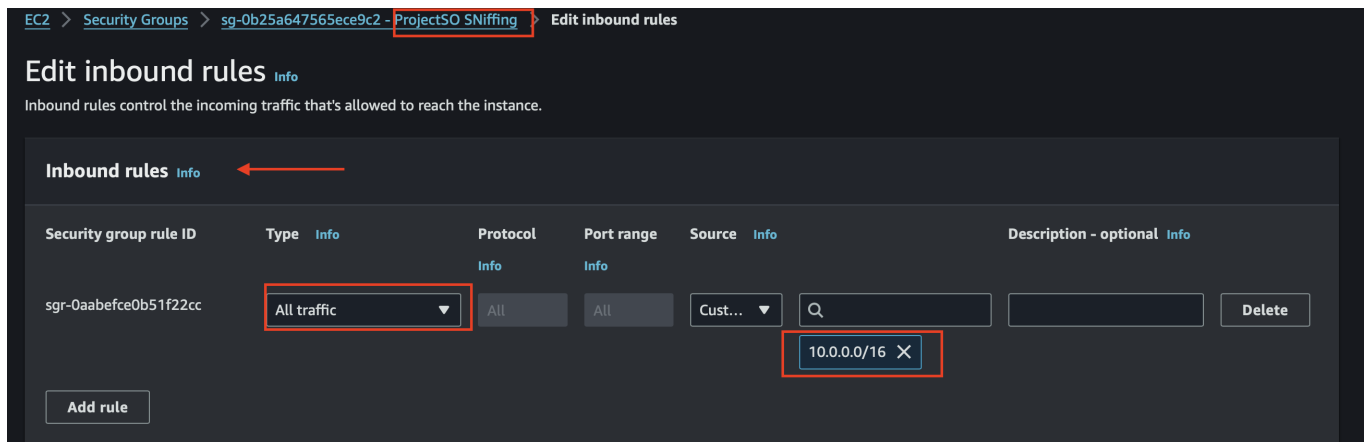
In the left pane under Network & Security, click on Security Groups (SG)

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 following inbound and outbound rules

Inbound Rules:



EC2 > Security Groups > sg-0b25a647565ece9c2 - **ProjectSO Sniffing** > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sg-0aabe9ce0b51f22cc	All traffic	All	All	Cust... 10.0.0/16	

Add rule

This allows all traffic inbound on the sniffing from the VPC

Outbound Rules:

The screenshot shows the 'Outbound rules' configuration for a security group. A red arrow points to the 'Outbound rules' tab. The table below shows the existing rule:

Security group rule ID	Type	Protocol	Port range	Destination	Description - optional
sgr-053d667ff212c1bc3	All traffic	All	All	0.0.0.0/0	

A red box highlights the 'All traffic' dropdown, and another red box highlights the '0.0.0.0/0' destination field. A warning message at the bottom states: 'Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.'

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

Network interface ID	Private IP address	Public IP address	Subnet	Availability Zone	Private DNS name
eni-060070f0ecccea0af	10.0.6.30				ip-1
eni-0306c7e73097a3d1d	10.0.1.106	44.219.46.44			ip-1

A red box highlights the first interface (eni-060070f0ecccea0af) and a red arrow points to its ID.

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

The screenshot shows the 'Network interface summary for eni-060070f0ecccea0af (sniffing)'. The 'Actions' menu is open, and 'Change security groups' is highlighted with a red box. A red arrow points to the 'Actions' button.

Network interface details	Network interface ID	Name	Description
eni-060070f0ecccea0af	sniffing	-	-

Other details shown include: Network interface status (In-use), VPC ID (vpc-05ae635dc657b1187), Subnet ID (subnet-0a249fd5788dafc01), and Requester ID (481665085987).

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

Associated security groups

Add one or more security groups to the network interface. You can also remove security groups.

Select security groups

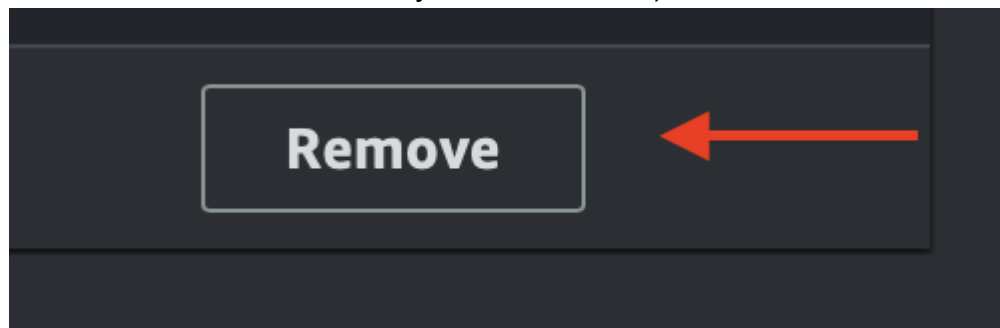
Add security group

Change security groups

Security groups associated with the network interface (eni-060070f0ecccea0af)

Security group name	Security group ID	
ProjectSO SNIffing	sg-0b25a647565ece9c2	Remove

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:









Network interface: eni-0306c7e73097a3d1d (mngr_ip)

Details

Flow logs

Tags

▼ Network interface details

Network interface ID  eni-0306c7e73097a3d1d	Name  mngr_ip	Description -
Network interface status  In-use	Interface type  Elastic network interface	Security groups  sg-01e05b55c0ba6542f (so_manager)
VPC ID vpc-05ae635dc657b1187 	Subnet ID subnet-0a249fd5788dafc01 	Availability Zone  us-east-1a

Sniffing Interface:

Network interface: eni-060070f0ecccea0af (sniffing)

Network interfaces

Details

Flow logs

Tags

▼ Network interface details

Network interface ID eni-060070f0ecccea0af	Name sniffing	Description -
Network interface status In-use	Interface type Elastic network interface	Security groups sg-0b25a647565ece9c2 (ProjectSO SNiffing)
VPC ID vpc-05ae635dc657b1187	Subnet ID subnet-0a249fd5788dafc01	Availability Zone us-east-1a