Technical Documentation:

Setting Up EC2 Instance for Metasploitable2 on Docker

Steps:

1. Launch EC2 Instance:

- Access the AWS Management Console and navigate to the EC2 service.
- Launch a new EC2 instance using Ubuntu as the operating system.
- Choose an appropriate instance type and configure instance details, including network settings and storage.

2.Create a new key pair named "metaAWS" and download the private key file to a secure location.

3. Connect to the Instance:

- Open a terminal or command prompt and navigate to the directory where the private key file is located.
- Use SSH to connect to the EC2 instance using Git Bash for Windows or a compatible terminal emulator:
- Add the private key to the SSH agent for authentication:

4. Installing Docker:

- Once connected to the EC2 instance, install Docker using Git Bash or a terminal emulator
- After installation, verify the Docker version to ensure successful installation

5. Recreate Instances (Optional):

- If needed, recreate additional instances with private subnets for specific purposes.
- Terminate instances when they are no longer needed to avoid unnecessary charges.

Setting Up Kali Linux Instance and Bastion Host on EC2

1. Connecting to EC2 Instance and Adding Kali Image:

- Use Git Bash or a compatible terminal emulator to connect to the EC2 instance via SSH:
- Add the Kali Linux image from Docker Hub:
- As Docker Hub does not store persistent Kali Linux images, switch to the official Kali Linux image from the AWS Marketplace:
- Launch the Kali Linux instance from the AWS Marketplace, ensuring to install Kali tools as they are not preinstalled.

2. Troubleshooting Kali AMI Image:

- If facing issues such as inability to ping, perform Nmap scans, or install tools, consider troubleshooting:
    - Identify root causes using diagnostic commands (e.g., ping, traceroute).
    - Use AWS documentation and forums to identify common issues and solutions.
    - Switch to the official Kali Linux image from the AWS Marketplace if Docker Hub image lacks persistence.

3. Launching Bastion Host Instance:

- Access the AWS Management Console and navigate to EC2.
- Launch a new EC2 instance, selecting Ubuntu as the operating system.
- Configure instance details, including network settings and storage.
- Launch the instance in the public subnet 1A to serve as the bastion host.

4. Verification and Monitoring:

- Verify the status of the Kali Linux and bastion host instances in the EC2 dashboard.
- Monitor the instances for proper functionality and resource utilization.

Using Bastion Host for SSH Access and Configuring Security

1. SSH into Bastion Host:

- Open a terminal or command prompt and SSH into the bastion host instance
- Enter the bastion host's private key passphrase if prompted.

2. Obtain Private IP Addresses:

- Once connected to the bastion host, retrieve the private IPv4 addresses of the Kali and Metasploitable2 instances:
- Note down the private IPv4 addresses of both instances on a notepad or similar tool for future reference.

3. Create Security Group:

- Access the AWS Management Console and navigate to the EC2 service.
- Click on "Security Groups" in the left sidebar and select "Create Security Group."
- Name the security group appropriately (e.g., "Kali-to-Metasploitable2-SG") and provide a description.
- Configure inbound rules to allow communication from Kali to Metasploitable2:
    - Add a rule for SSH (port 22) to allow inbound traffic from the Kali instance's private IP address.
    - Optionally, add additional rules for other required services or protocols.
- Review and create the security group.

4. Apply Security Group to Instances:

- Once the security group is created, associate it with both the Kali and Metasploitable2 instances:
    - Navigate to the instances section in the EC2 dashboard.
    - Select the Kali instance, click "Actions," then "Networking," and "Change Security Groups."
    - Choose the newly created security group and save the changes.
    - Repeat the process for the Metasploitable2 instance.

Using Bastion Host for SSH Connection and Ping Troubleshooting

1. Connect to Instances Using Bastion Host and Git Bash:

- Open Git Bash or a compatible terminal emulator on your local machine.
- SSH into the bastion host instance using the private key:
- Once connected to the bastion host, establish SSH connections to the Kali and Metasploitable2 instances using their private IP addresses
- Enter the respective private key passphrase if prompted.

2. Troubleshoot Ping Connectivity:

- Attempt to ping from Kali to Metasploitable2:
- If the ping fails, verify that the necessary network tools are installed on the Kali instance:
- Retry the ping command after installing the required network tools.

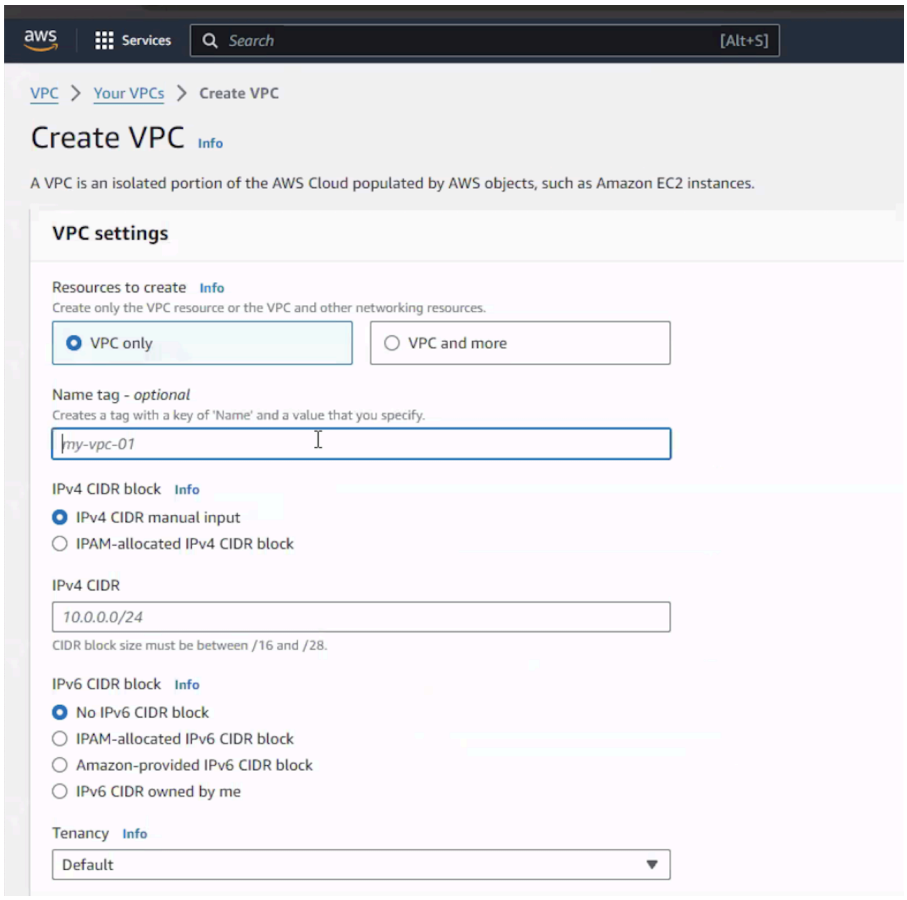
3. Verify Ping Connectivity:

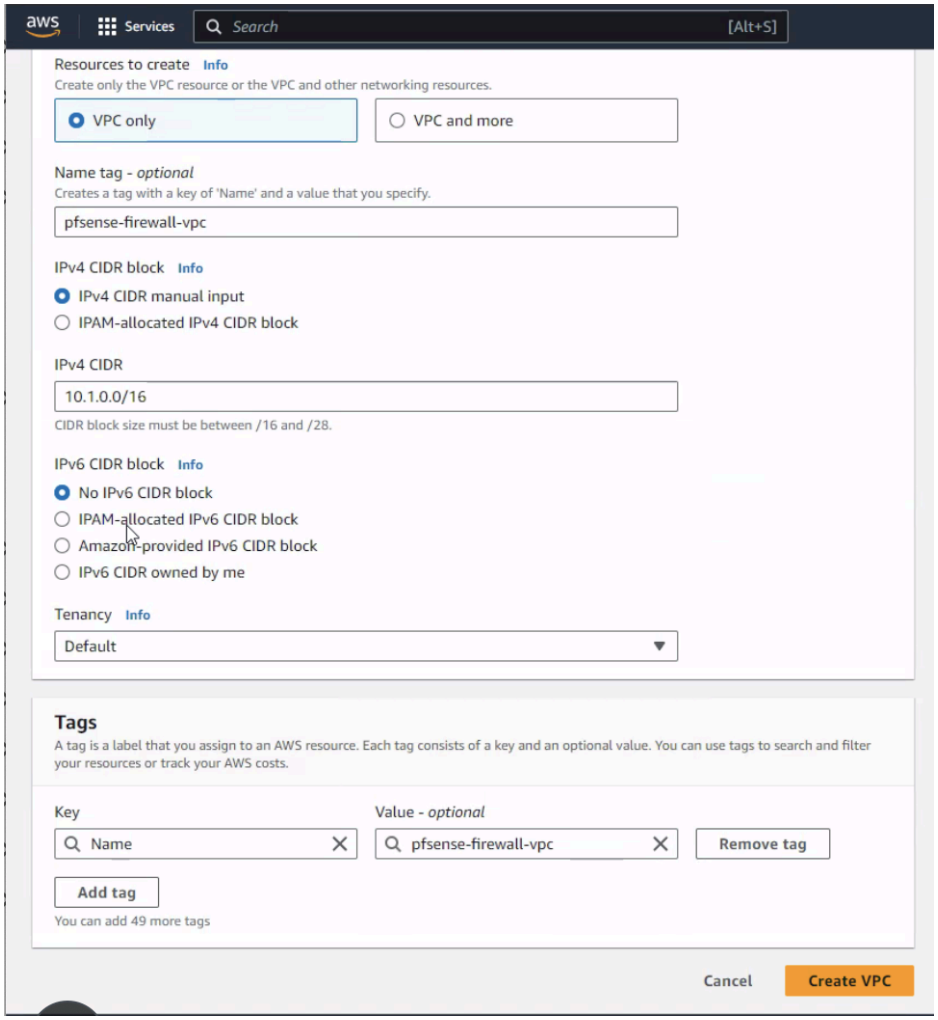
- After installing net-tools on Kali, retry the ping command to verify connectivity to Metasploitable2:
- Ensure that the ping is successful and that there is bidirectional connectivity between the Kali and Metasploitable2 instances.
- Additionally, verify that Metasploitable2 can ping Kali to confirm full connectivity.

Pfsense Installation Process:

1. Create VPC (Virtual Private Cloud):

- Navigate to the VPC dashboard.
- Click on "Create VPC" and enter the required details, such as VPC name and CIDR block (e.g., 10.0.0.0/16).
- VPC name is pfsense-firewall-vpc and CIDR block is 10.1.0.0/16

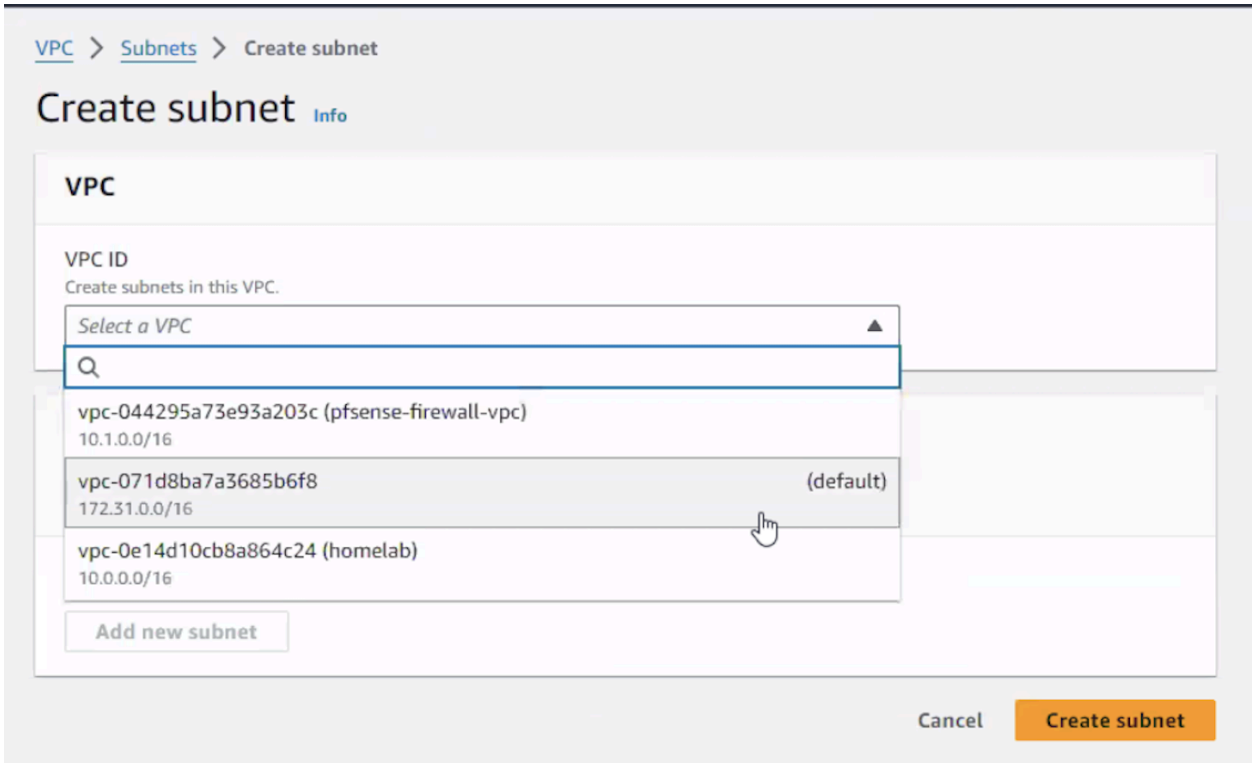




- Click on "Create" to create the VPC.

2. Create Subnets:

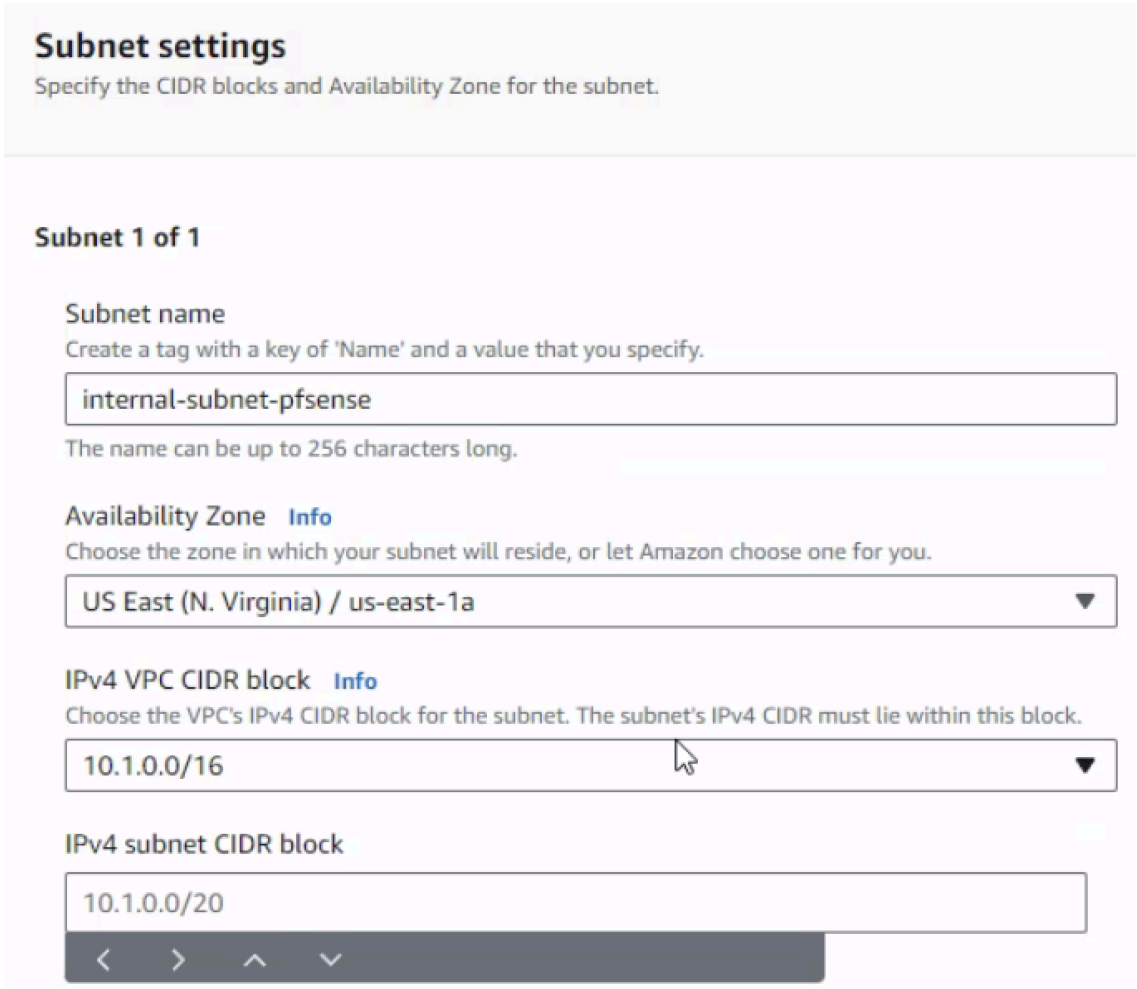
- Within the created VPC, navigate to the "Subnets" section.
- Click on "Create subnet" and enter the subnet details, including subnet name, VPC, availability zone, and CIDR block (e.g., 10.0.1.0/24).
    - **`VPC Configuration:`**
    - **`VPC ID: pfsense-firewall-vpc`**



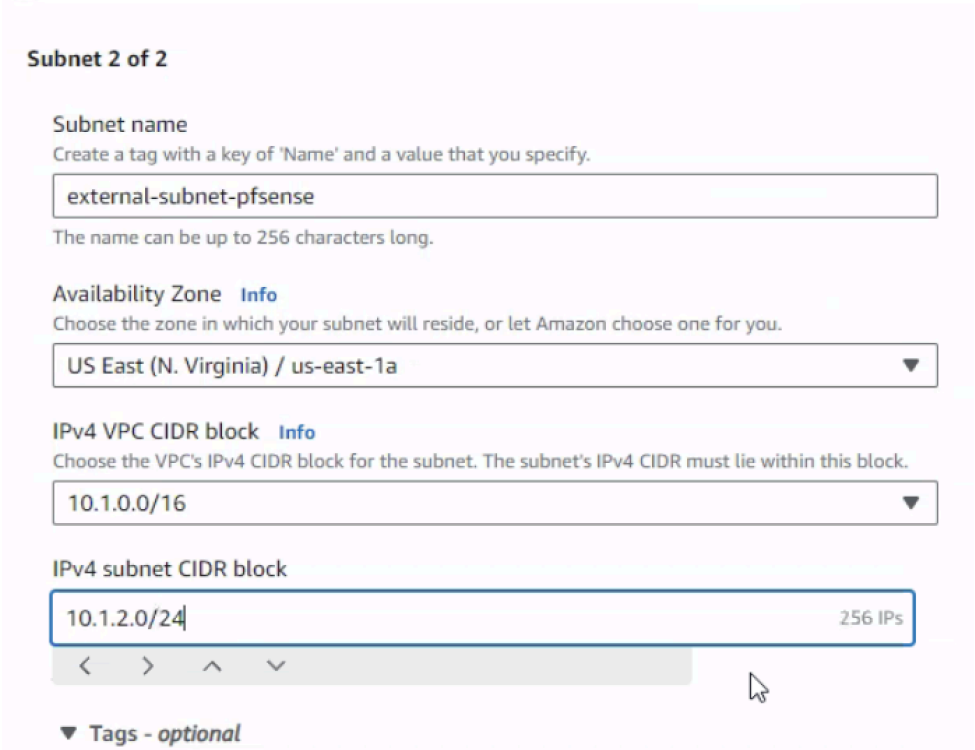
Subnet Settings:

Subnets:

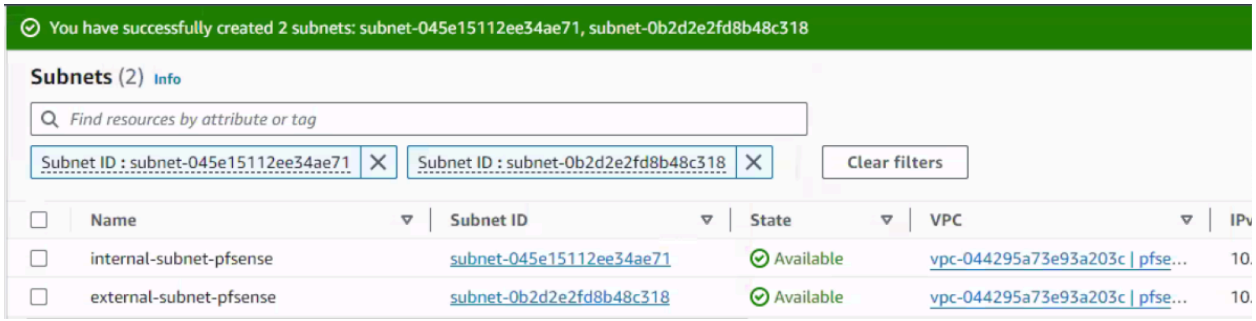
- **Internal (Private) Subnet:**
  - **Subnet Name:** internal-subnet-pfsense
  - **Availability Zone:** US East (N. Virginia) / us-east-1a
  - **CIDR Block:** 10.1.0.0/16



- **External (Public) Subnet:**
  - **Subnet Name:** external-subnet-pfsense
  - **Availability Zone:** US East (N. Virginia) / us-east-1a
  - **CIDR Block:** 10.1.0.0/24

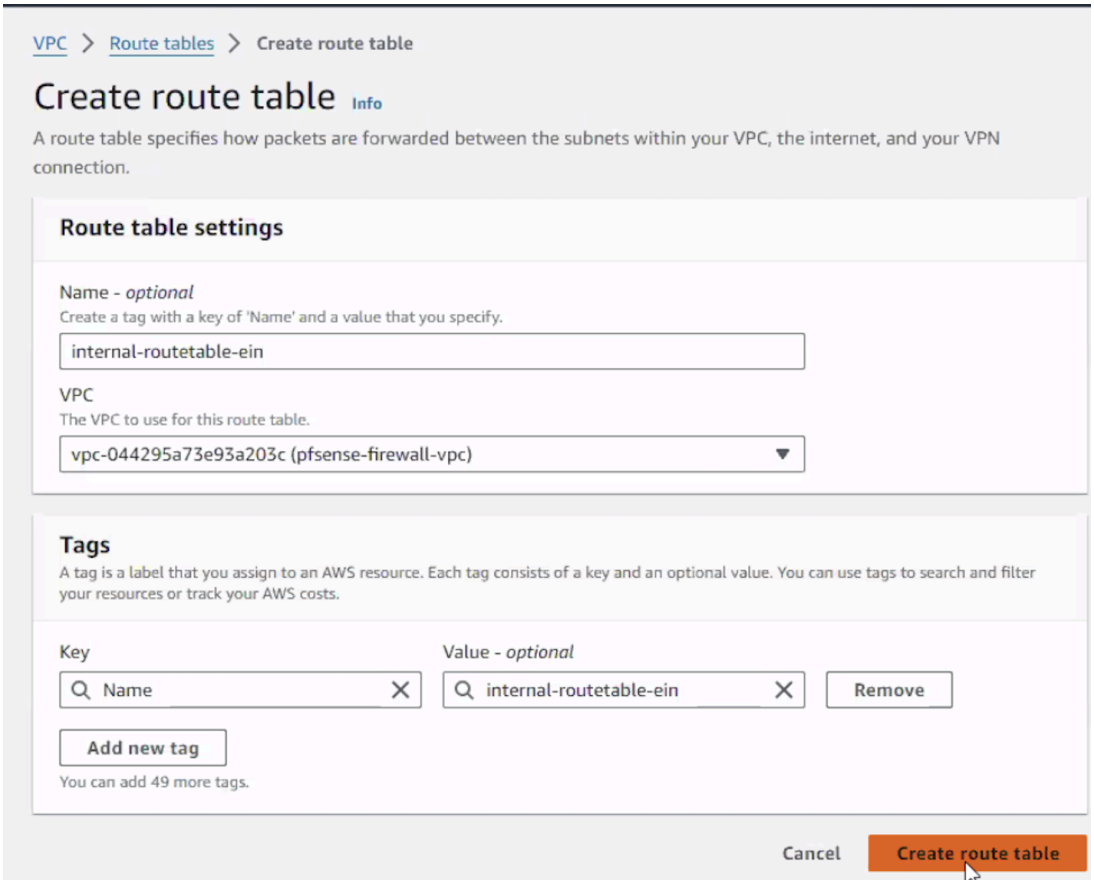


- We successfully created two subnets

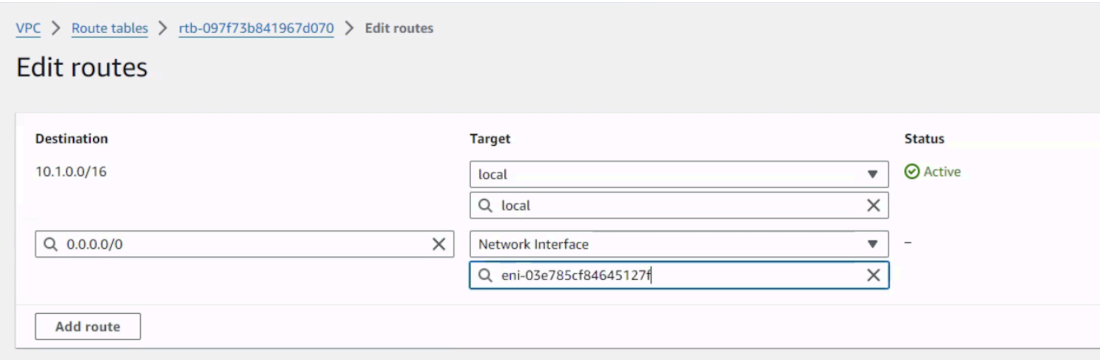


3. Create Route Tables:

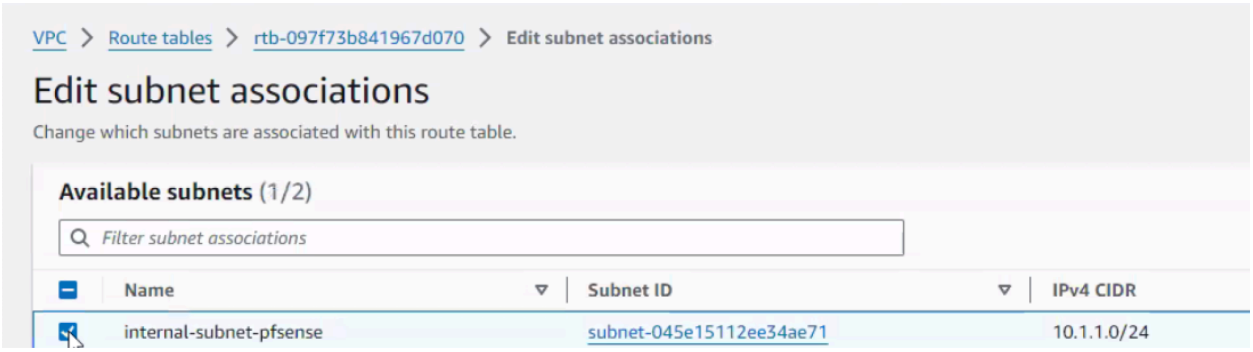
- In the VPC dashboard, go to the "Route Tables" section.
- Click on "Create route table" and specify the VPC association

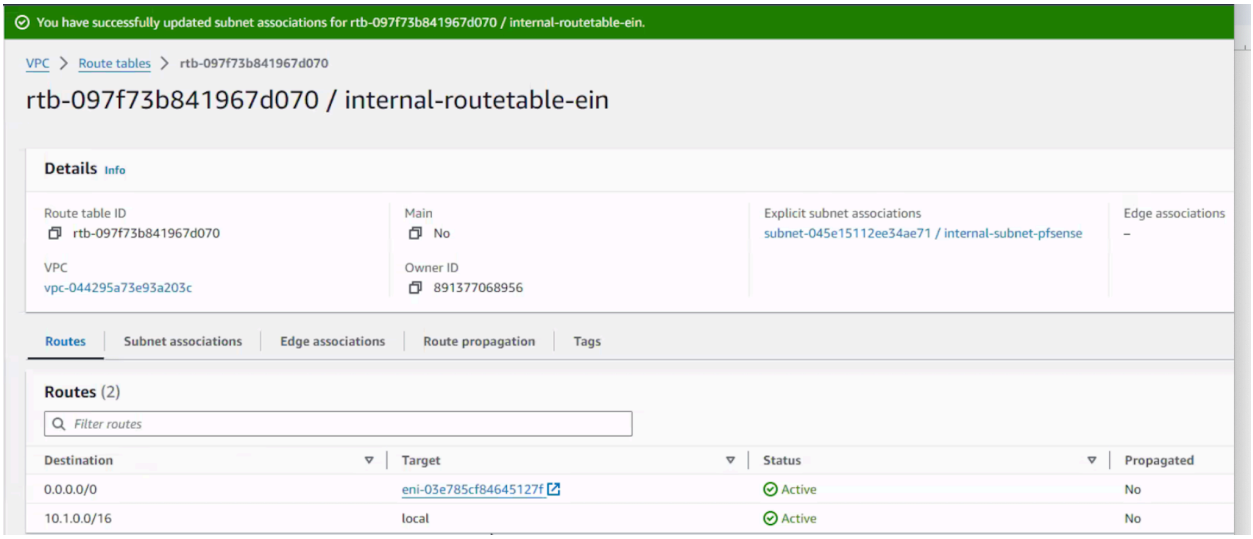


- Add routes to the route table for internet access and inter-subnet communication as needed.



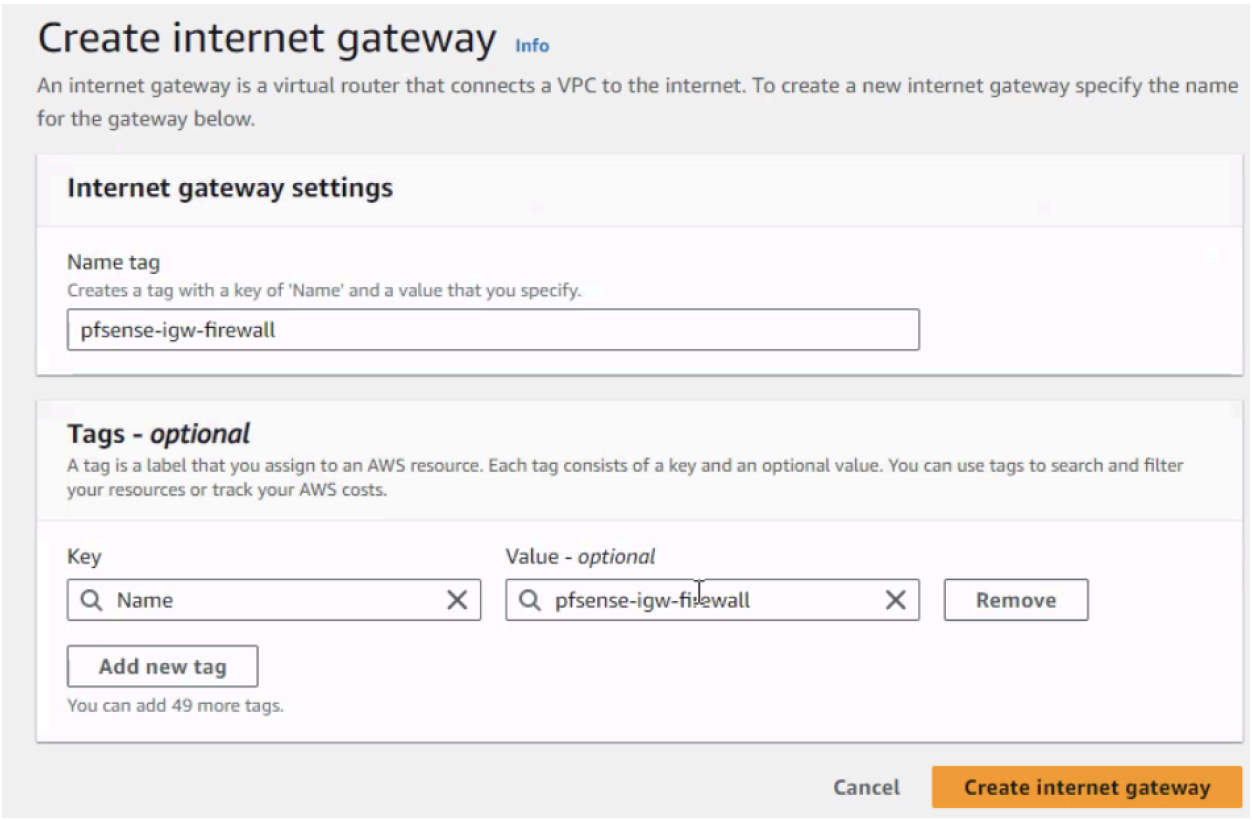
- Associate the route table with the appropriate subnets.



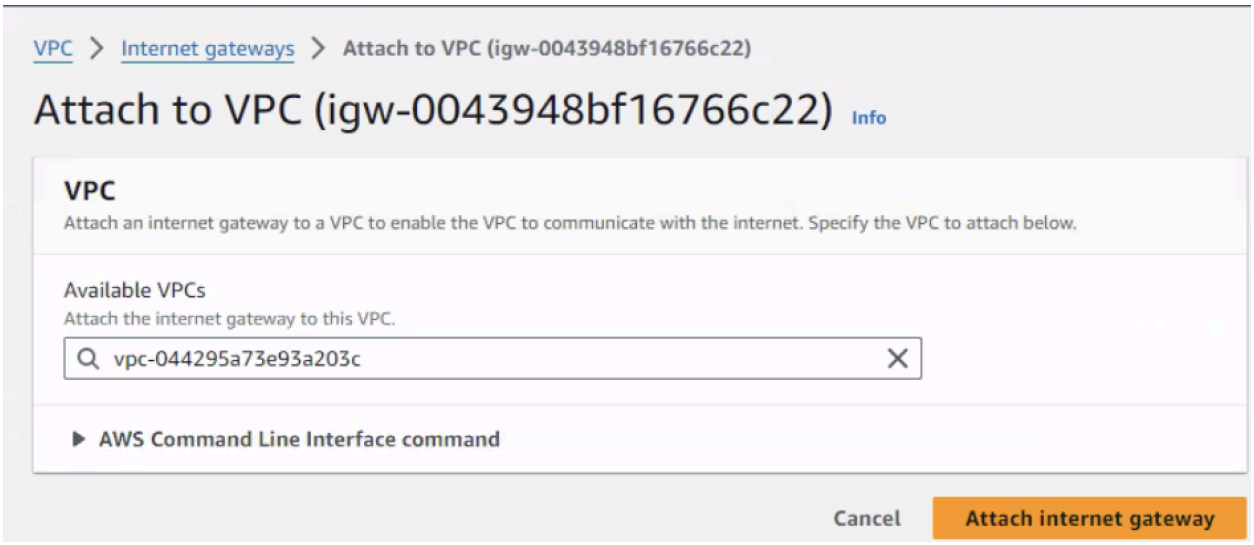


4. Create Internet Gateway:

- Navigate to the "Internet Gateways" section within the VPC dashboard.
- Click on "Create internet gateway" and give it a name.

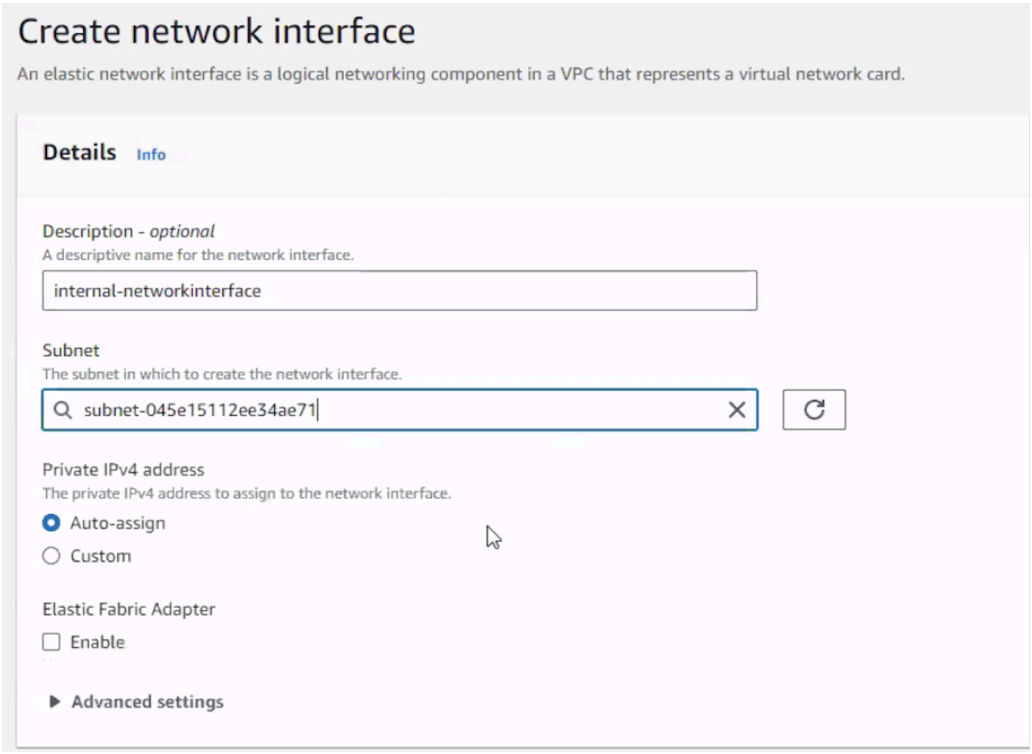


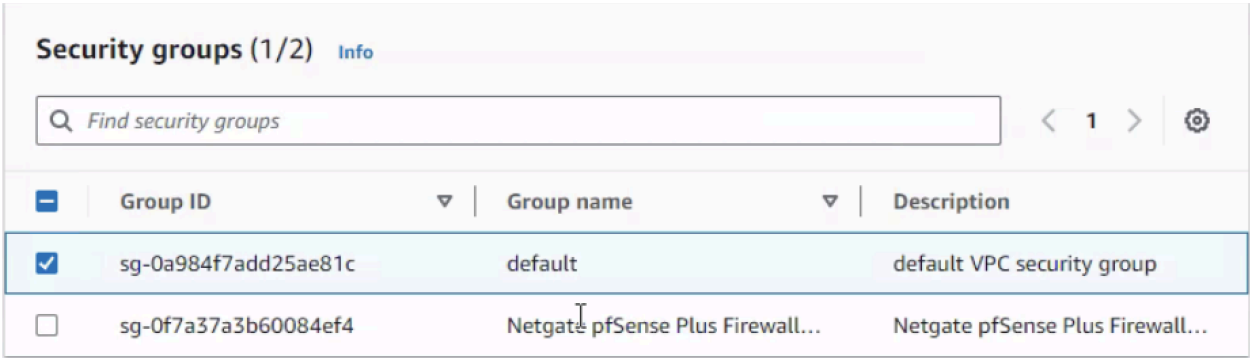
- Attach the internet gateway to the VPC created earlier.



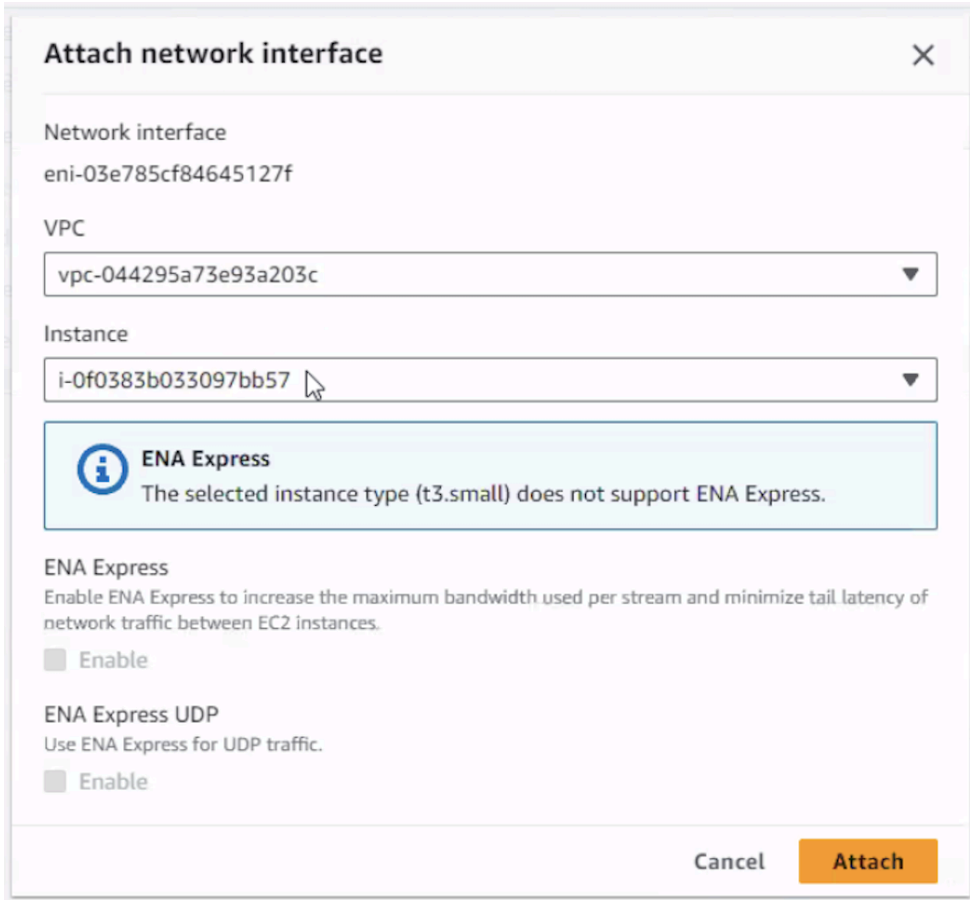
5. Attach Network Interface:

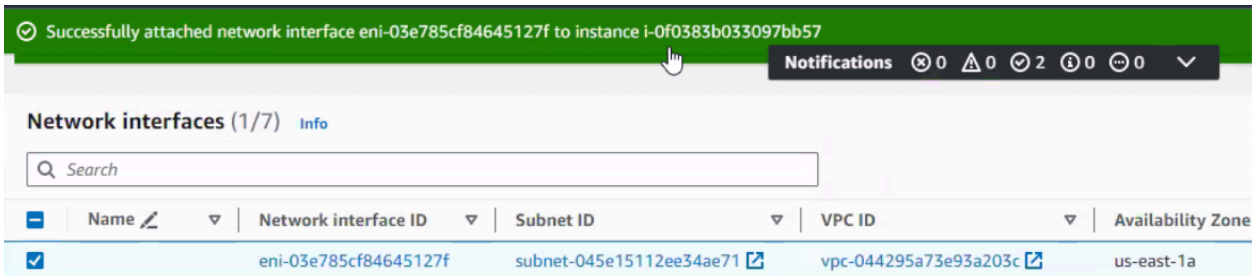
- Go to the EC2 dashboard and navigate to the "Network Interfaces" section.
- Click on "Create network interface" and select the subnet and security group.





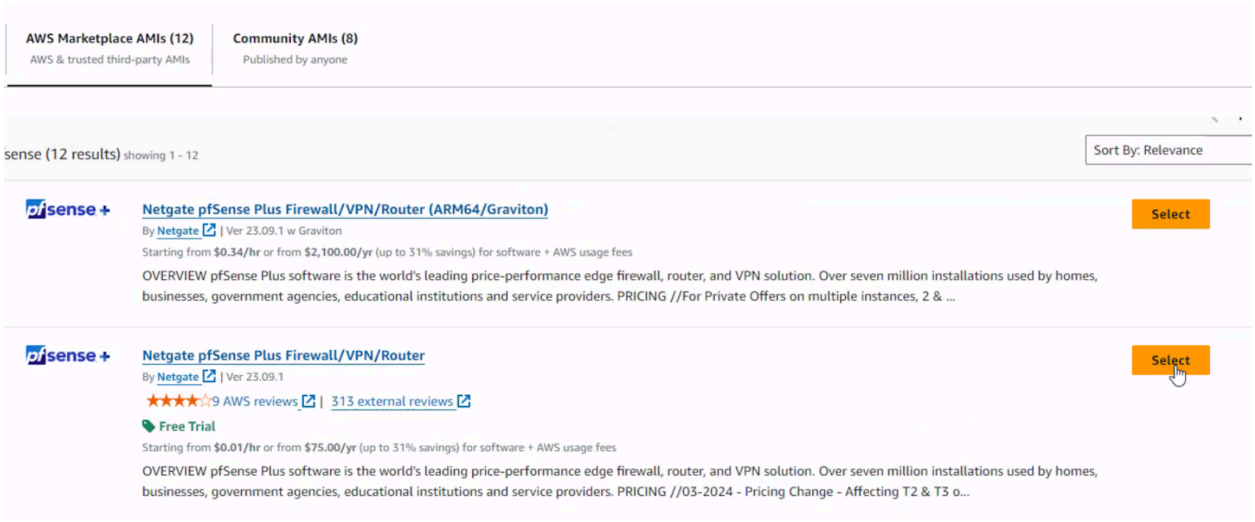
- Choose the appropriate options for IP addresses, network performance, and tags.
- Once created, attach the network interface to an EC2 instance or pfSense instance.

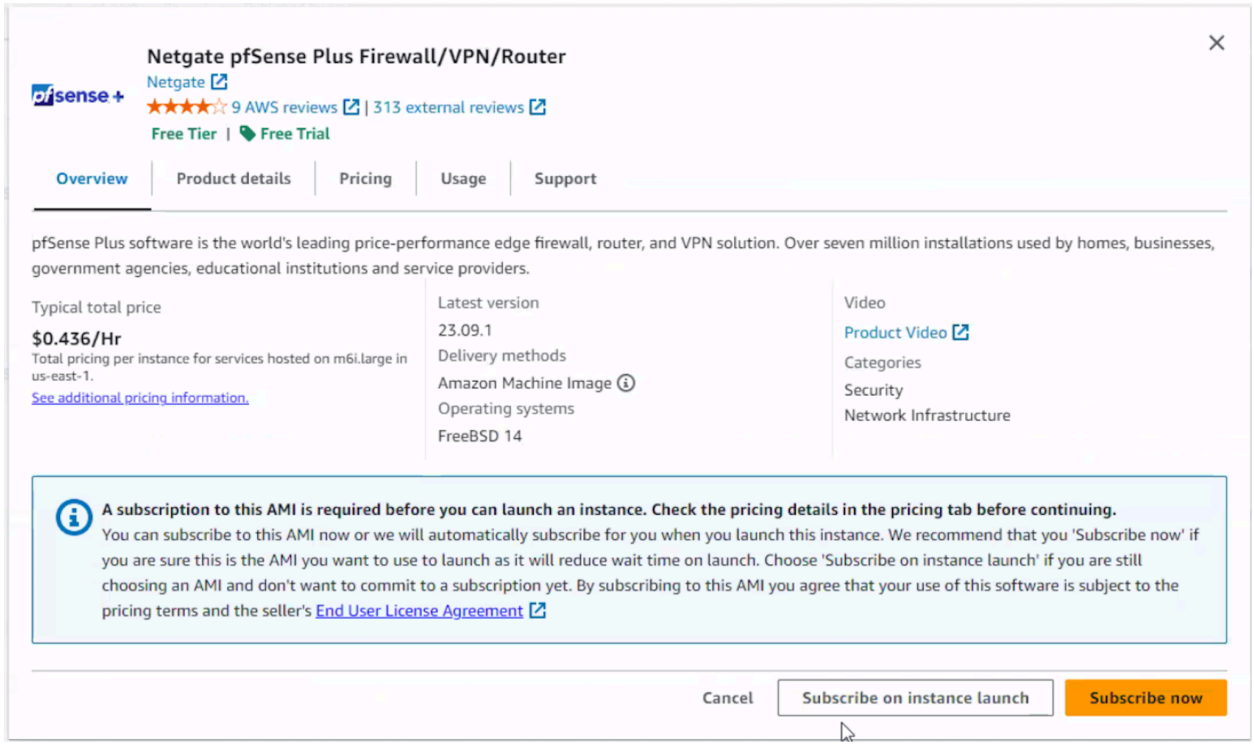




6. Launch pfSense Instance:

- In the EC2 dashboard, click on "Launch Instance" to launch a new instance.
- Search for the pfSense AMI in the AWS Marketplace and select the desired AMI.





- Choose an instance type, configure instance details, add storage, configure security groups, and review before launching.

Instance Type:

- **Type:** t3.small

Key Pair Configuration:

Key Pair Name:

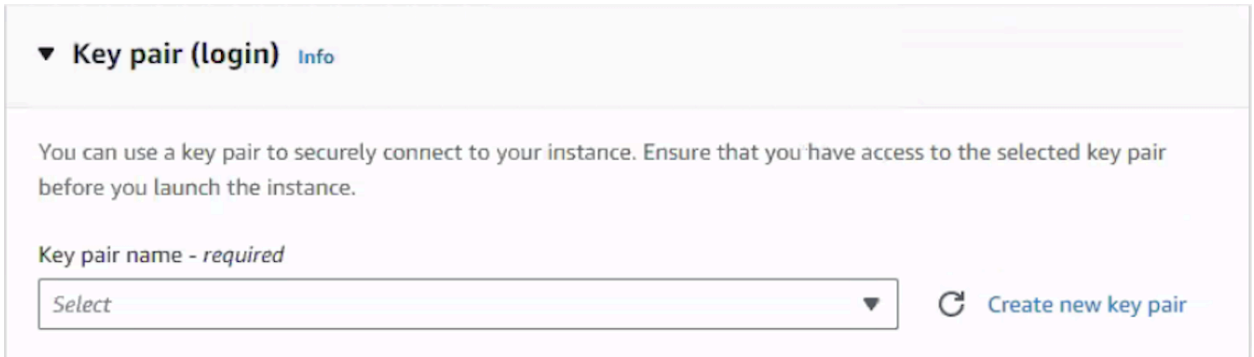
- **Name:** pfsenseawsvpc

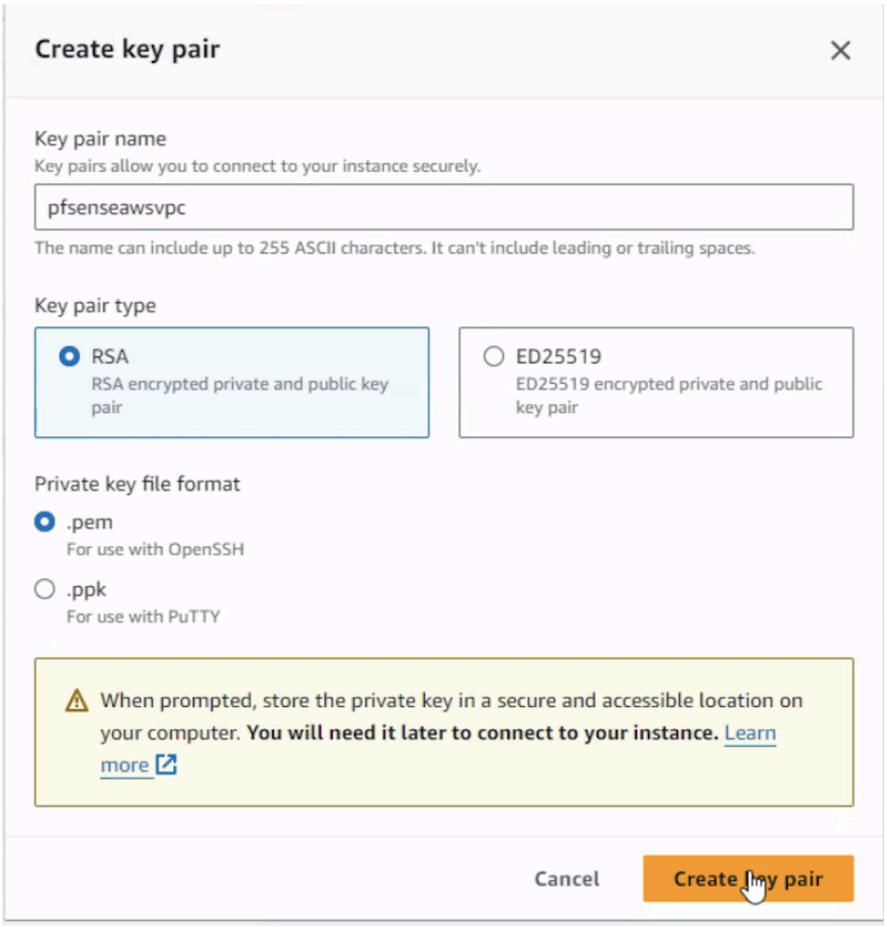
Key Pair Details:

- **Type:** RSA
- **Private Key File Format:** .pem

Action:

- **Selection:** Create New Key Pair
- **Create Key Pair**





Network Settings:

VPC:

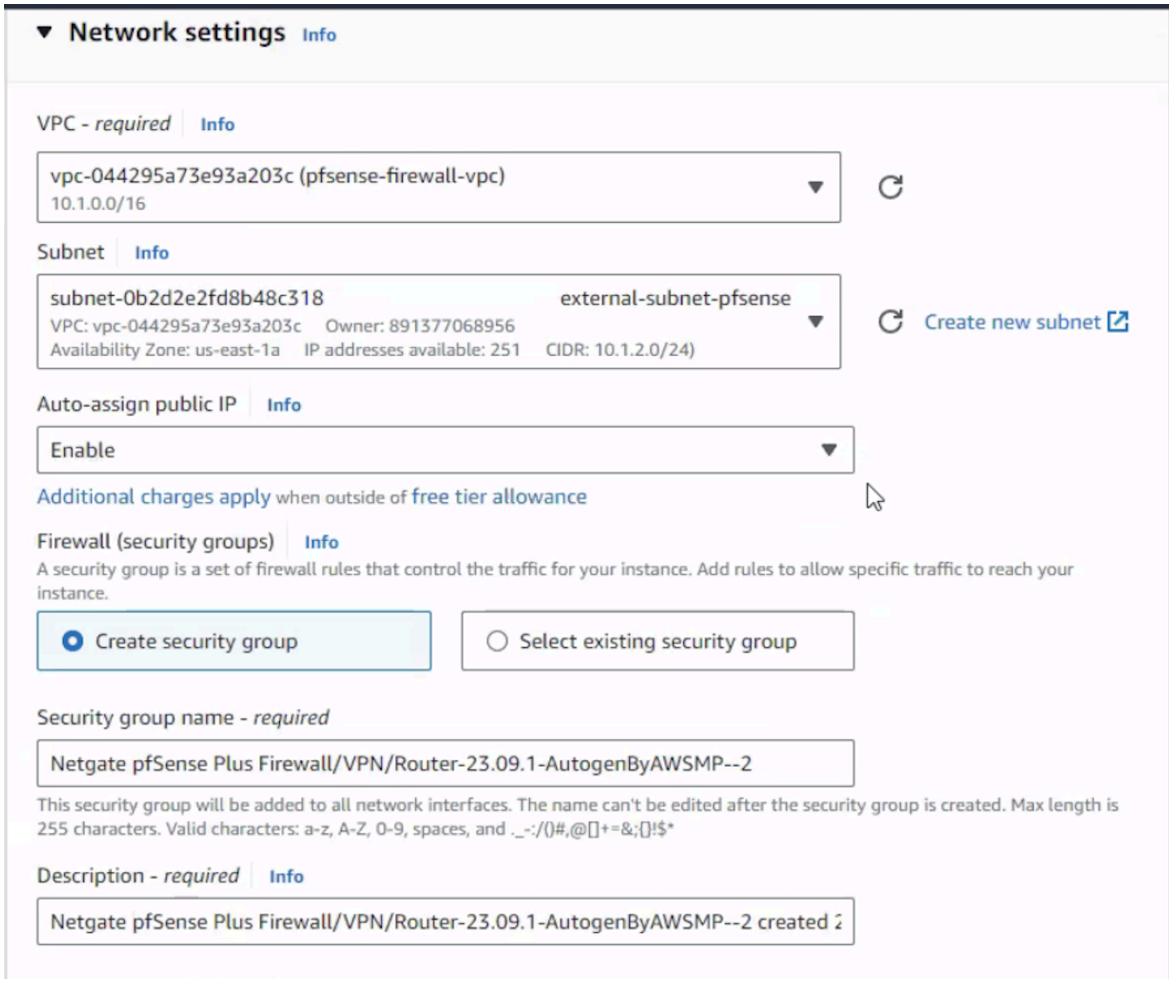
- **VPC:** pfsense-firewall-vpc

Subnet:

- **Subnet:** external-subnet-pfsense
- **Auto-assign Public IP:** Enabled

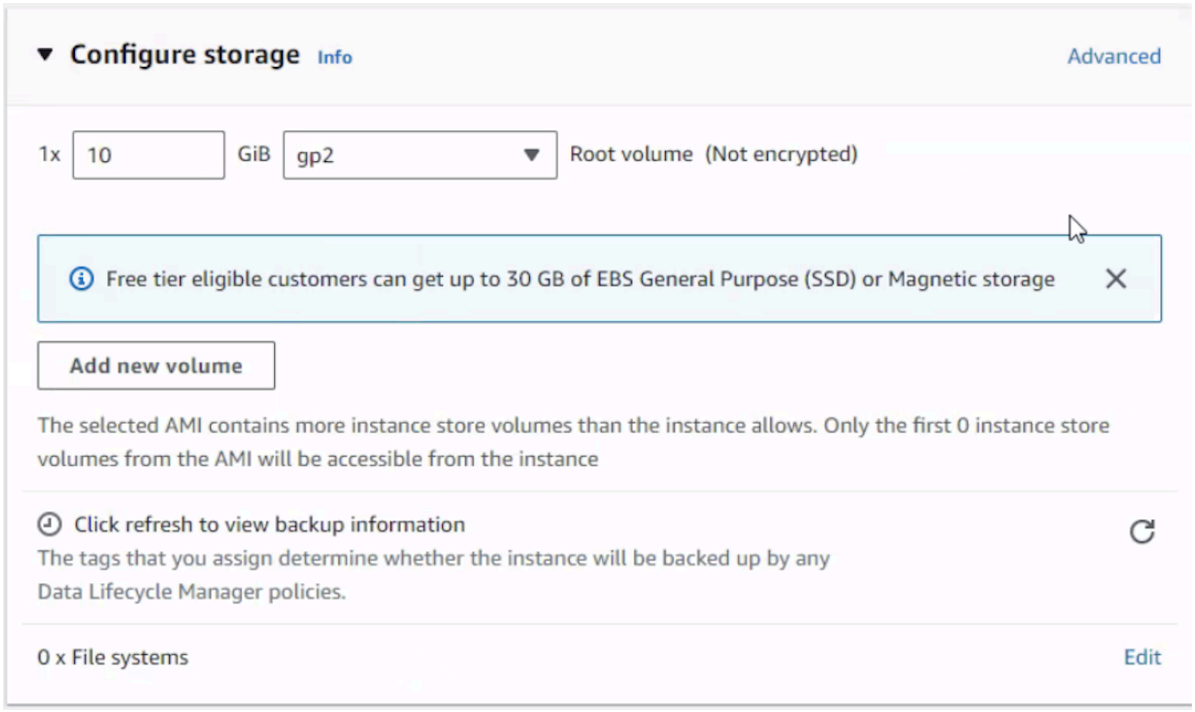
Firewall (Security Groups):

- **Action:** Selected Create Security Group
- **Security Group Name:** Netgate pfsense Plus Firewall/VPN/Router-23.09.1-AutogenByAWSMP-2

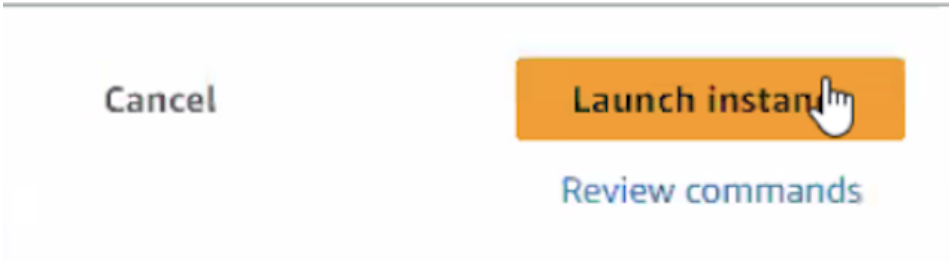

Network settings Info
VPC - required Info
vpc-044295a73e93a203c (pfsense-firewall-vpc)
10.1.0.0/16
Subnet Info
subnet-0b2d2e2fd8b48c318 external-subnet-pfsense
VPC: vpc-044295a73e93a203c Owner: 891377068956
Availability Zone: us-east-1a IP addresses available: 251 CIDR: 10.1.2.0/24)
Create new subnet
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
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
Netgate pfSense Plus Firewall/VPN/Router-23.09.1-AutogenByAWSMP--2
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
Netgate pfSense Plus Firewall/VPN/Router-23.09.1-AutogenByAWSMP--2 created 2

Storage Configuration:

- **1x 10 GiB gp2**

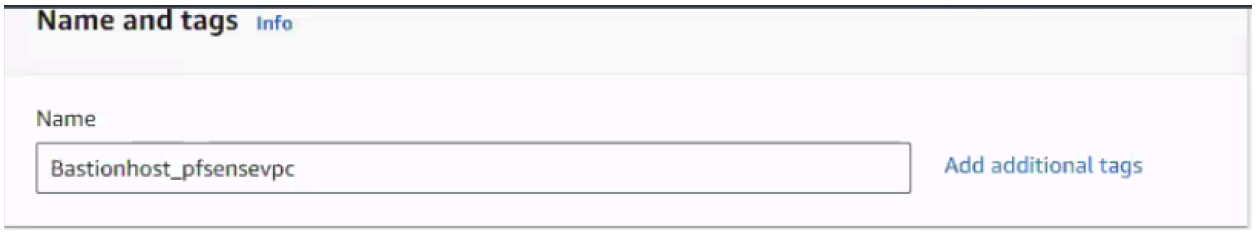


- Launch the instance



7.Launch Bastion Host Instance

- In the EC2 dashboard, click on "Launch Instance" to launch a new instance.



- Search for the **Ubuntu Server 22.04 LTS** AMI in the AWS Marketplace and select the desired AMI.
- Choose an instance type, configure instance details, add storage, configure security groups, and review before launching.

Instance Type:

- **Type:** t2.micro

Key Pair Configuration:

Key Pair Name:

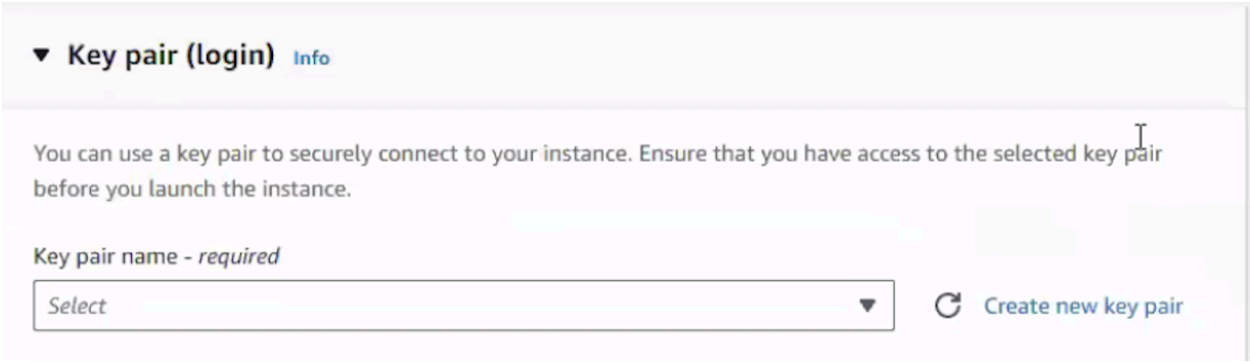
- **Name:** ubuntubastion

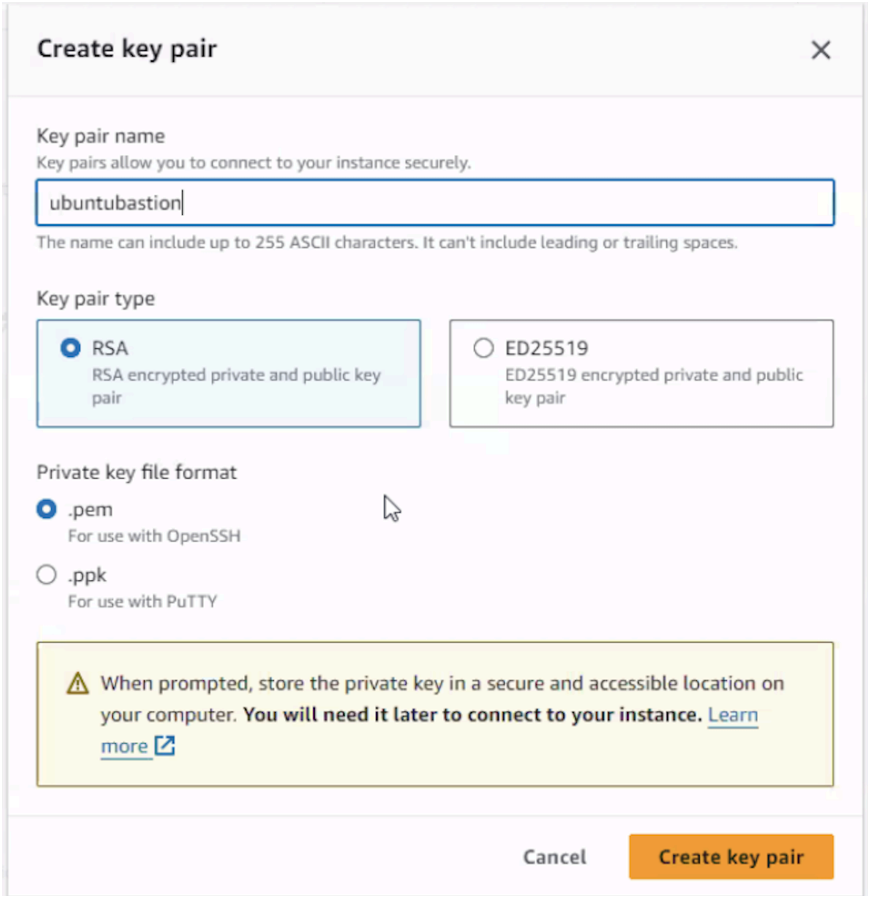
Key Pair Details:

- **Type:** RSA
- **Private Key File Format:** .pem

Action:

- **Selection:** Create New Key Pair
- **Create Key Pair**





Network Settings:

VPC:

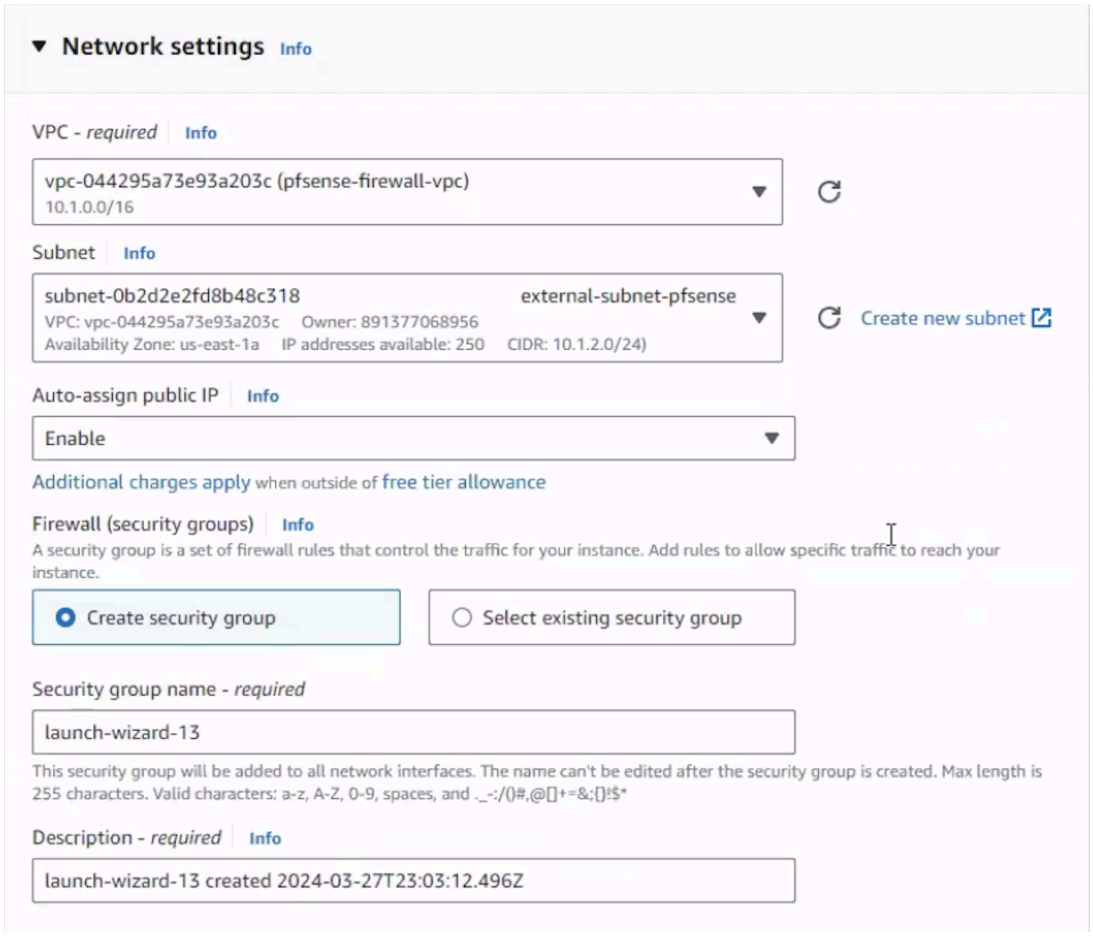
- **VPC:** pfsense-firewall-vpc

Subnet:

- **Subnet:** external-subnet-pfsense
- **Auto-assign Public IP:** Enabled

Firewall (Security Groups):

- **Action:** Selected Create Security Group
- **Security Group Name:** launch-wizard-13



8.Launch Internal Kali Host Instance

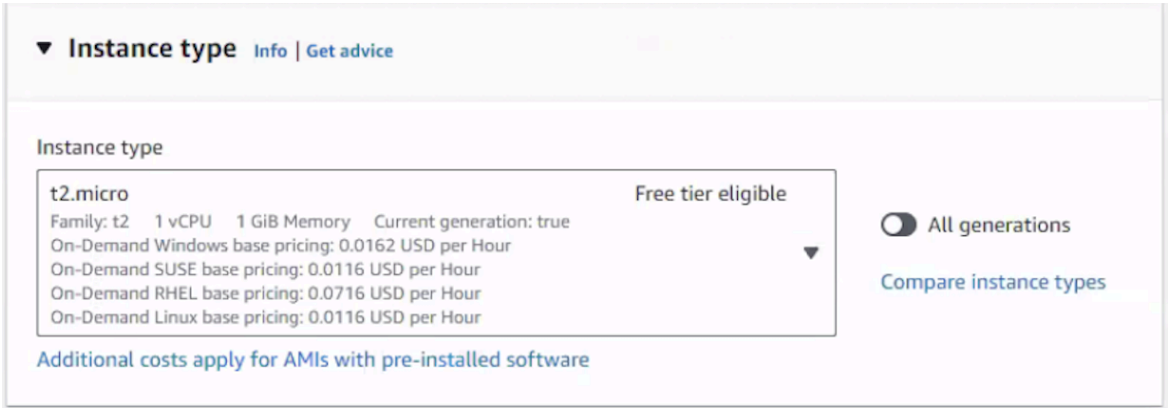
- In the EC2 dashboard, click on "Launch Instance" to launch a new instance.

- Search for the AMI in the AWS Marketplace and select the desired AMI.
    - Selected **kali_v2**

- Choose an instance type, configure instance details, add storage, configure security groups, and review before launching.

Instance Type:

- **Type:** t2.micro



Key Pair Configuration:

Key Pair Name:

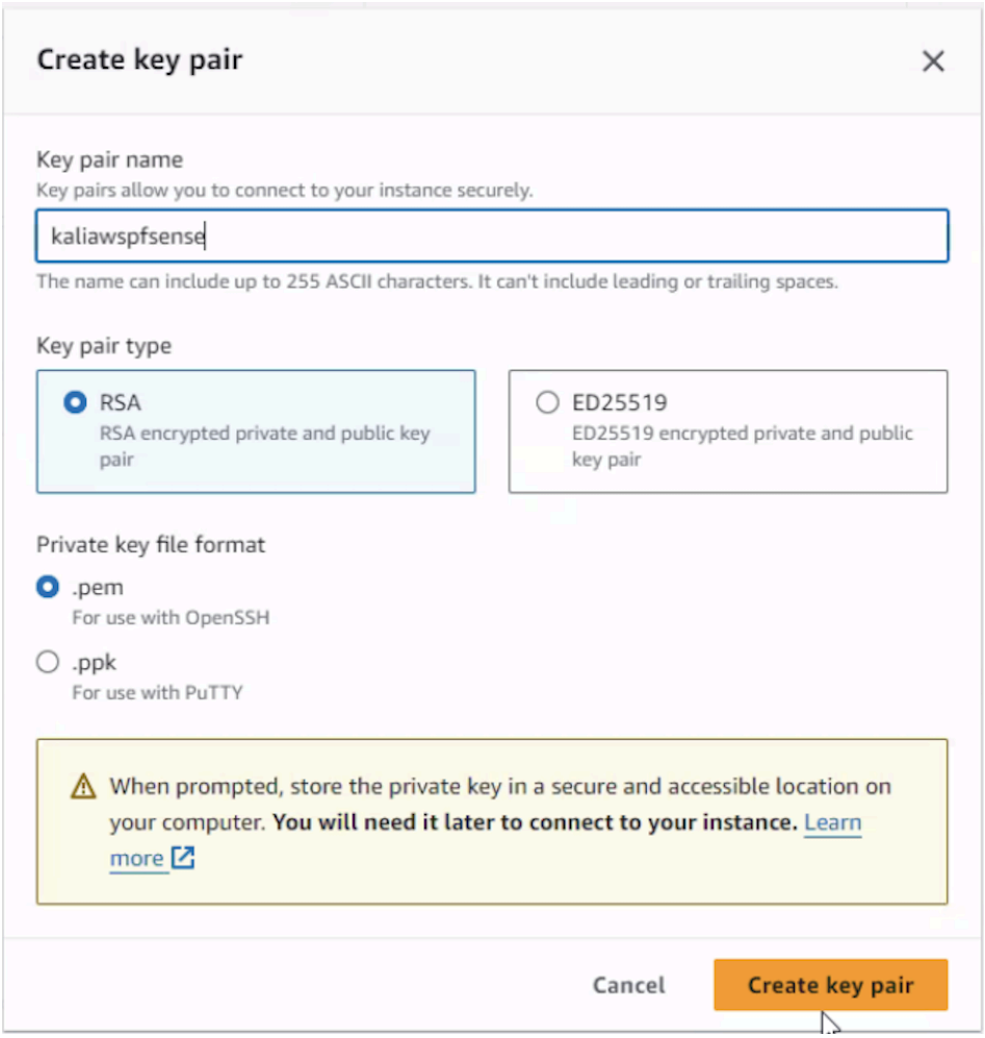
- **Name:** kaliawspfsense

Key Pair Details:

- **Type:** RSA
- **Private Key File Format:** .pem

Action:

- **Selection:** Create New Key Pair
- **Create Key Pair**



Network Settings:

VPC:

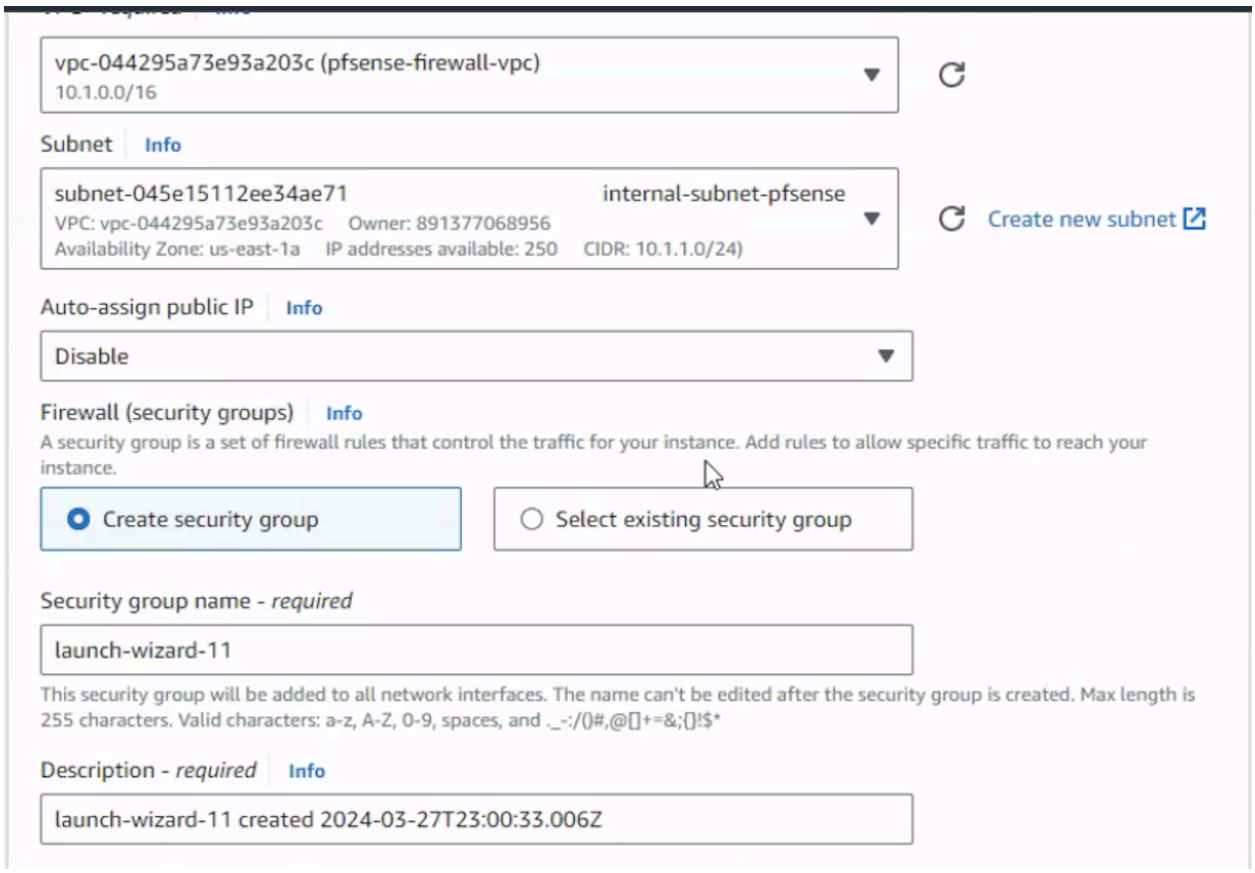
- **VPC:** pfsense-firewall-vpc

Subnet:

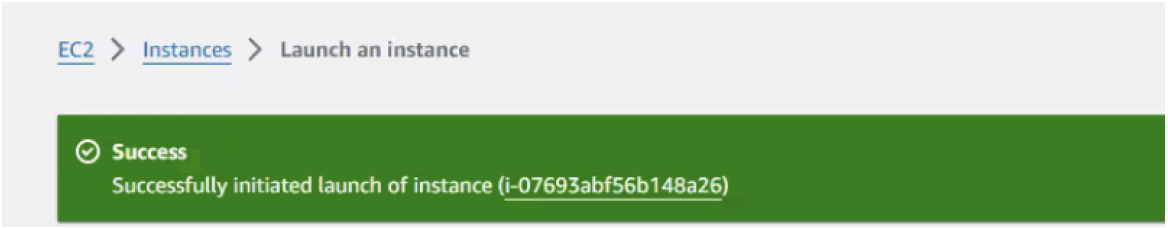
- **Subnet:** internal-subnet-pfsense
- **Auto-assign Public IP:** Disabled

Firewall (Security Groups):

- **Action:** Selected Create Security Group
- **Security Group Name:** launch-wizard-11

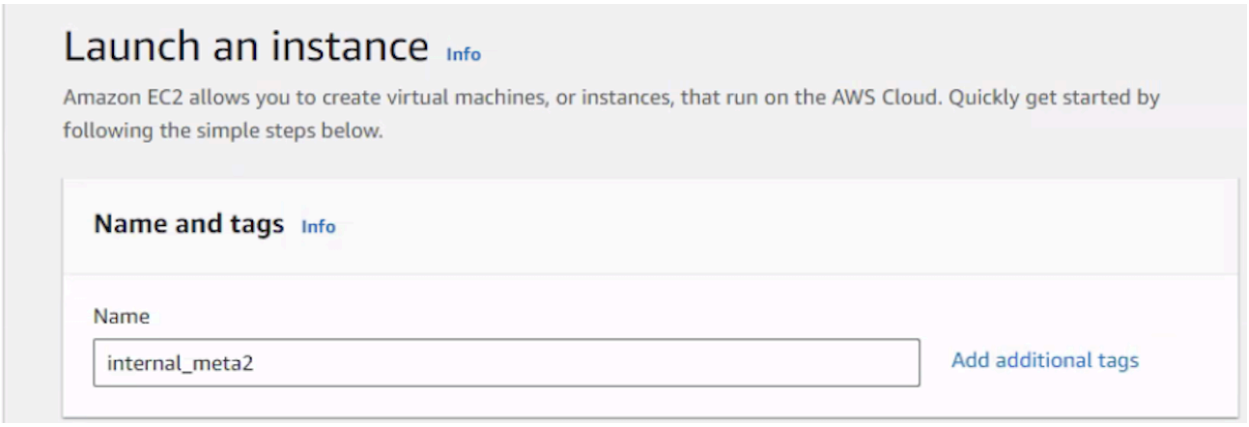


- Launch Instance



9.Launch Internal Kali Host Instance

- In the EC2 dashboard, click on "Launch Instance" to launch a new instance.



- Search for the AMI in the AWS Marketplace and select the desired AMI.
    - Selected **Metasploitable2_docker**

- Choose an instance type, configure instance details, add storage, configure security groups, and review before launching.

Instance Type:

- **Type:** t2.micro

Key Pair Configuration:

Key Pair Name:

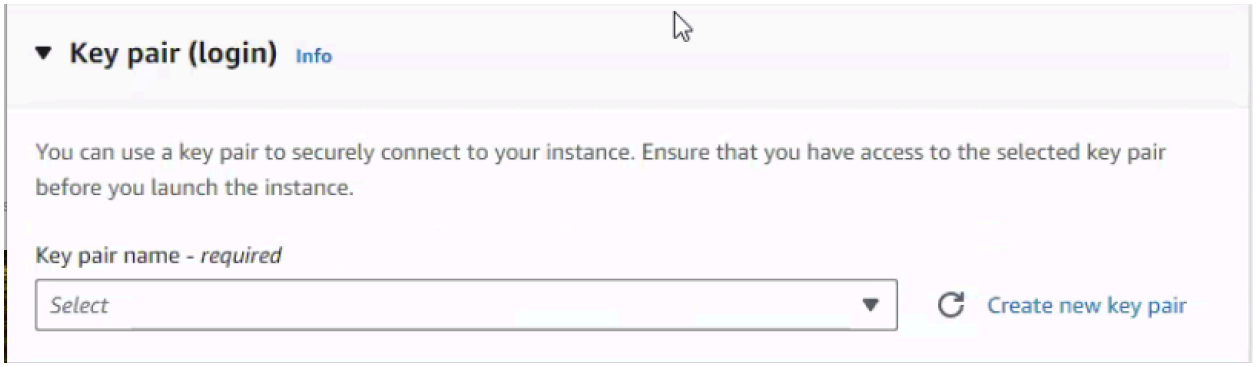
- **Name:** meta2pfsense

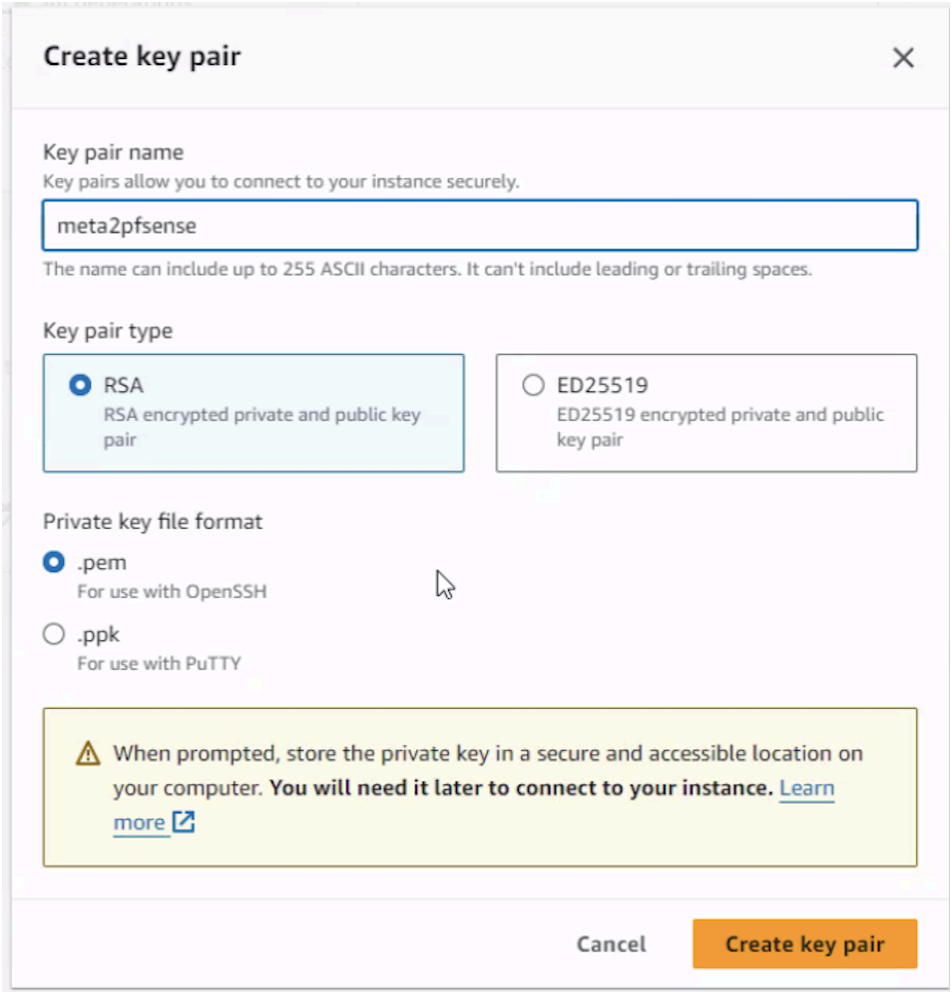
Key Pair Details:

- **Type:** RSA
- **Private Key File Format:** .pem

Action:

- **Selection:** Create New Key Pair
- **Create Key Pair**





Network Settings:

VPC:

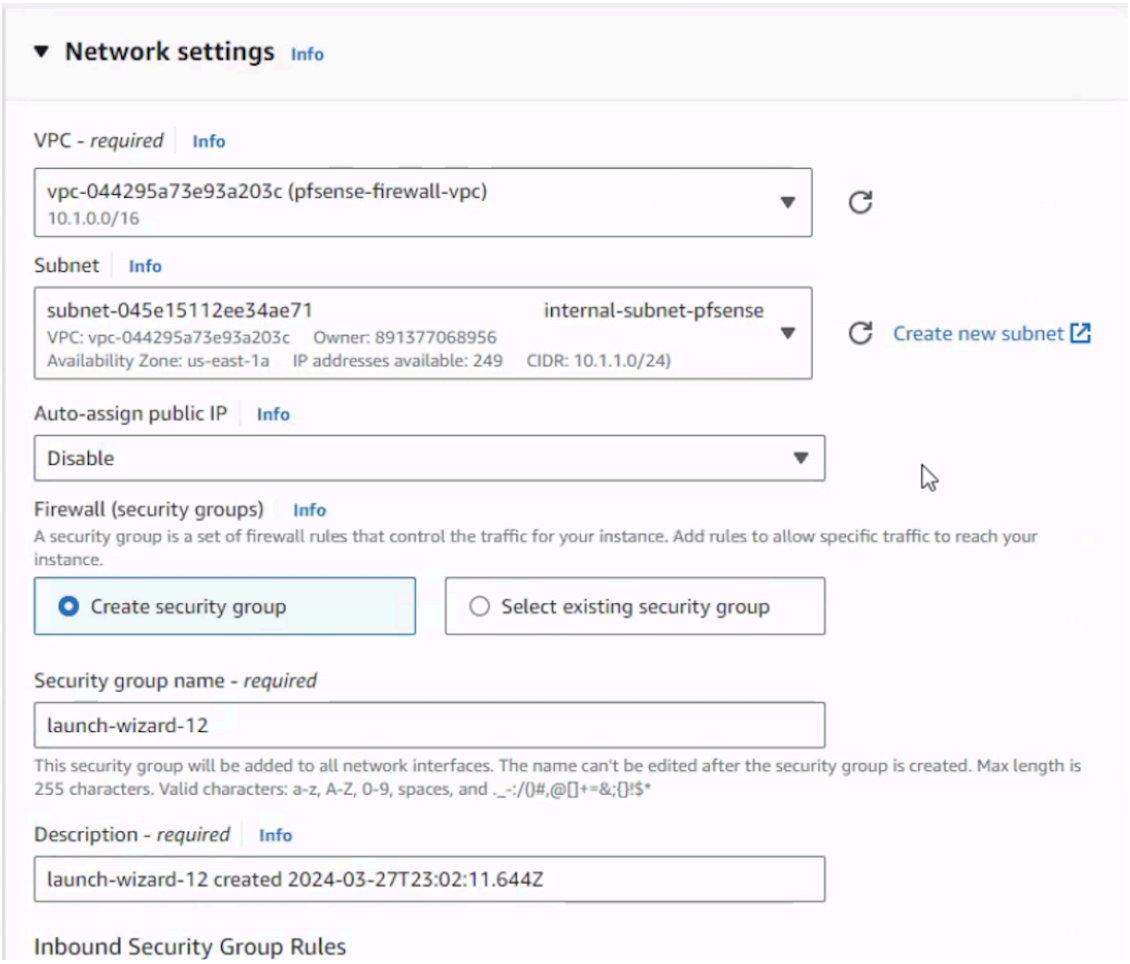
- **VPC:** pfsense-firewall-vpc

Subnet:

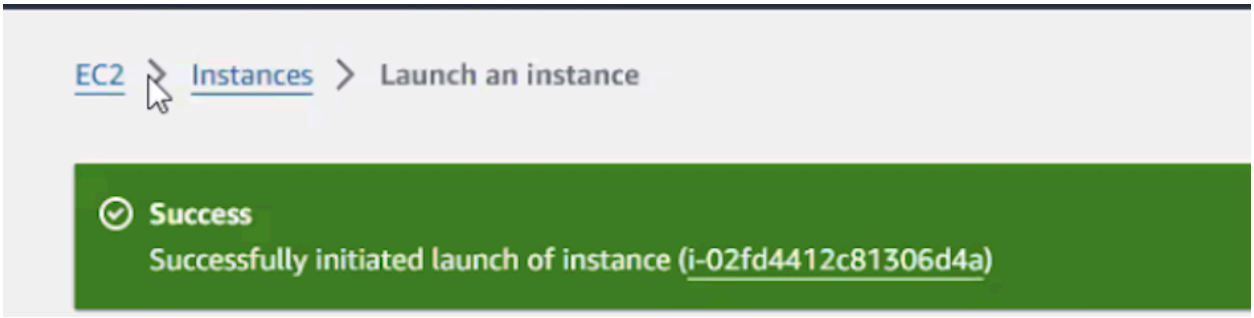
- **Subnet:** internal-subnet-pfsense
- **Auto-assign Public IP:** Disabled

Firewall (Security Groups):

- **Action:** Selected Create Security Group
- **Security Group Name:** launch-wizard-12

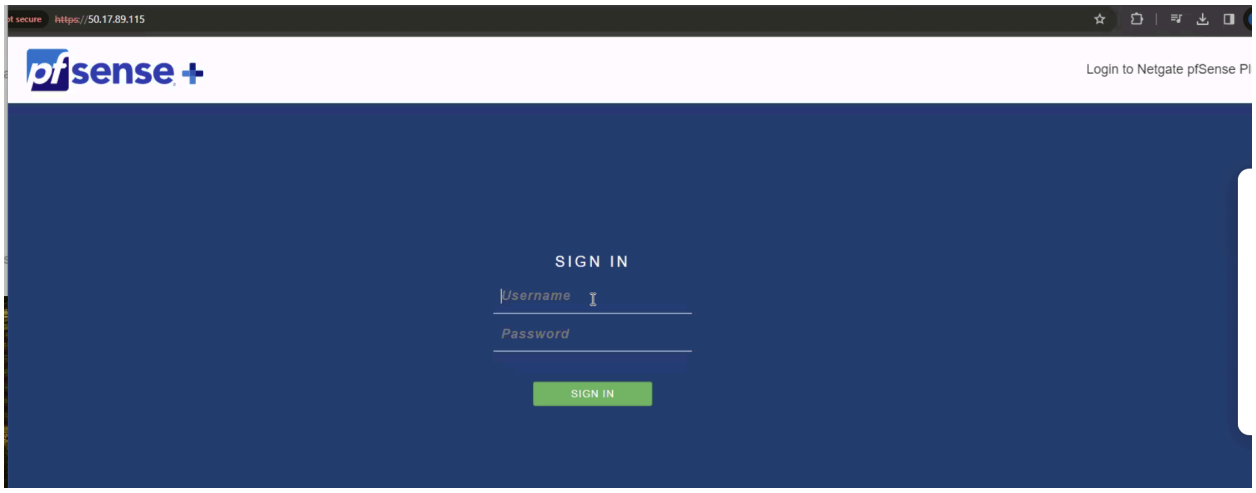


- Launch Instance



9.Configure pfsense

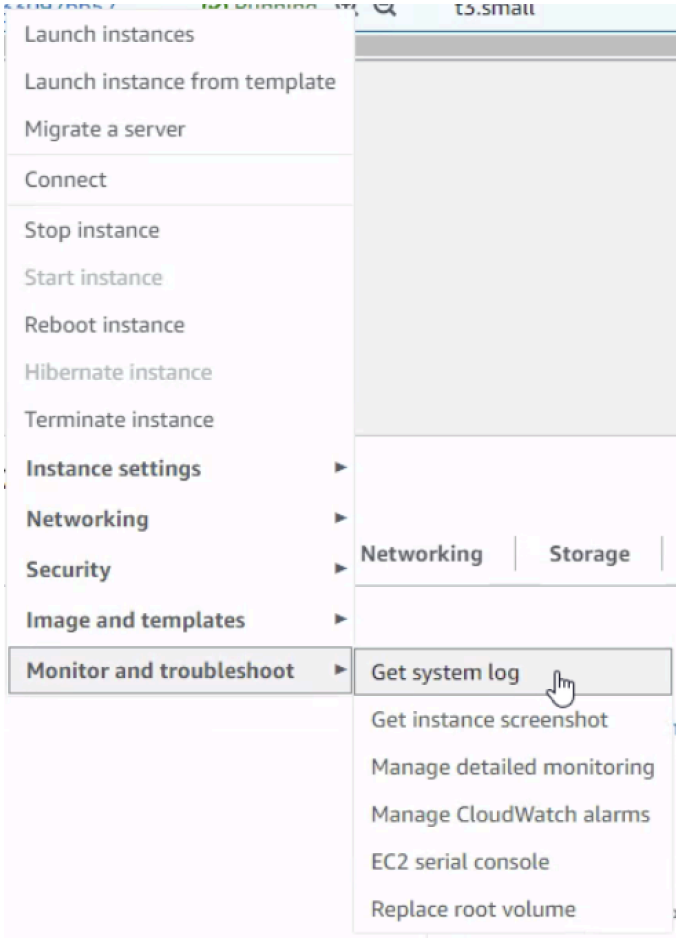
- Once the pfSense instance is running, access its web interface using the public IP address or DNS name.

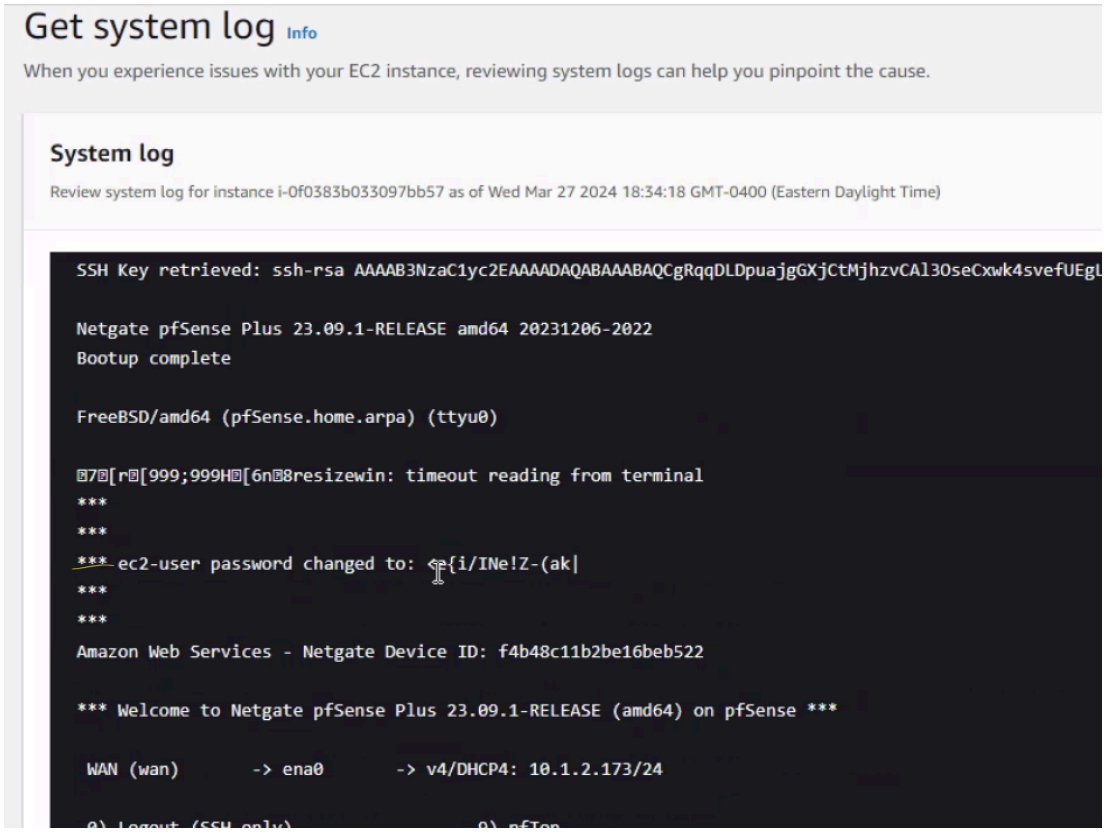


Username: admin
Password: Copied and pasted password from system log

Steps to retrieve Password:

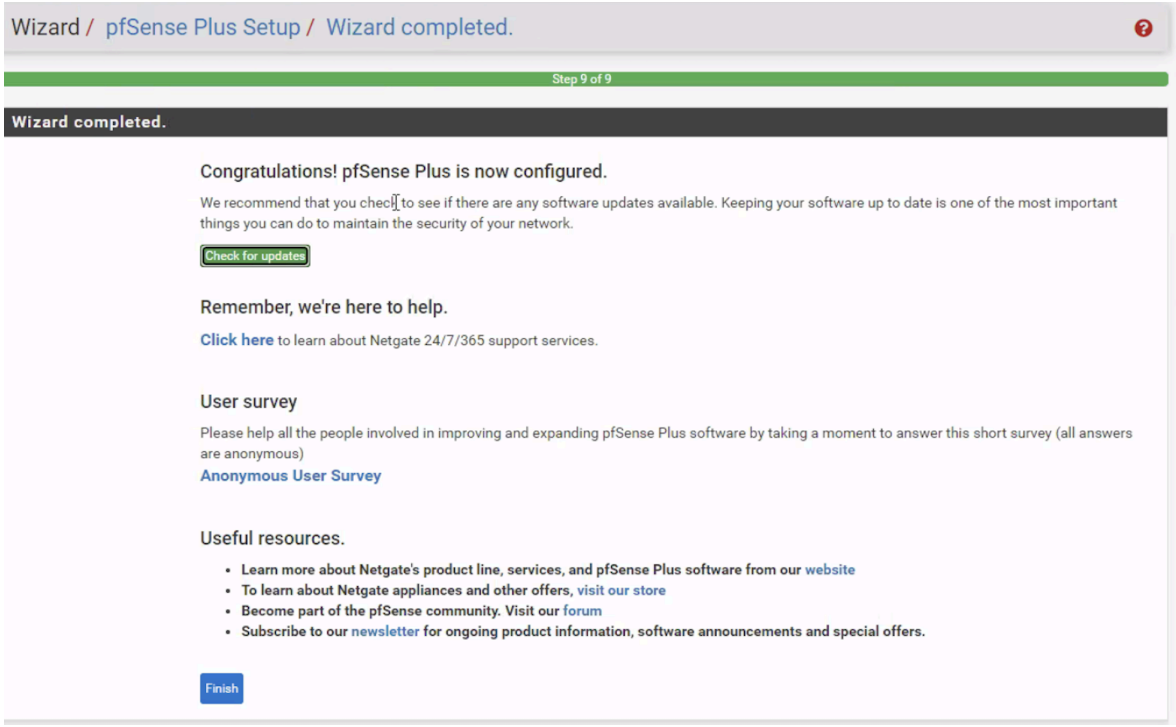
1. Navigate to instances on the side dashboard.
2. Select "Monitor and Troubleshoot".
3. Choose "Get system Log".


t3.small
Launch instances
Launch instance from template
Migrate a server
Connect
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate instance
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Networking
Storage
Get system log
Get instance screenshot
Manage detailed monitoring
Manage CloudWatch alarms
EC2 serial console
Replace root volume



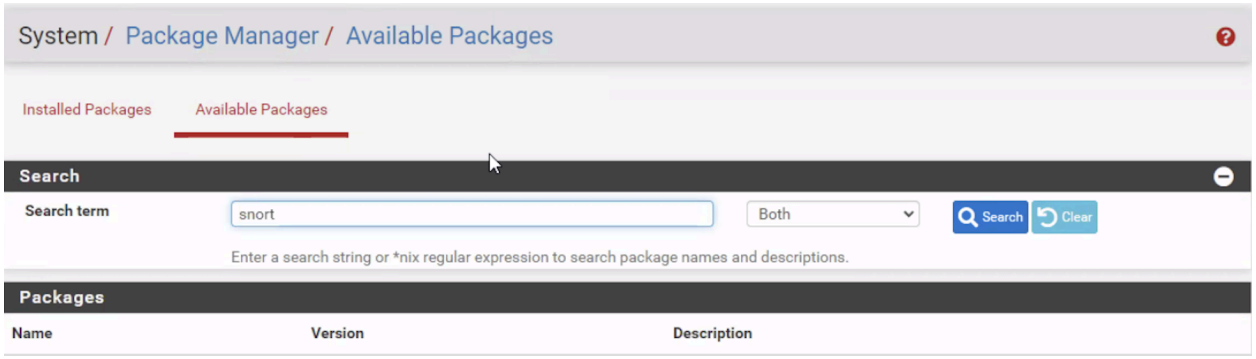
- The password can be found under "ec2-user password changed to."
- Return to the pfSense web page and enter the new password.

- Follow the initial setup wizard



Install Snort Package:

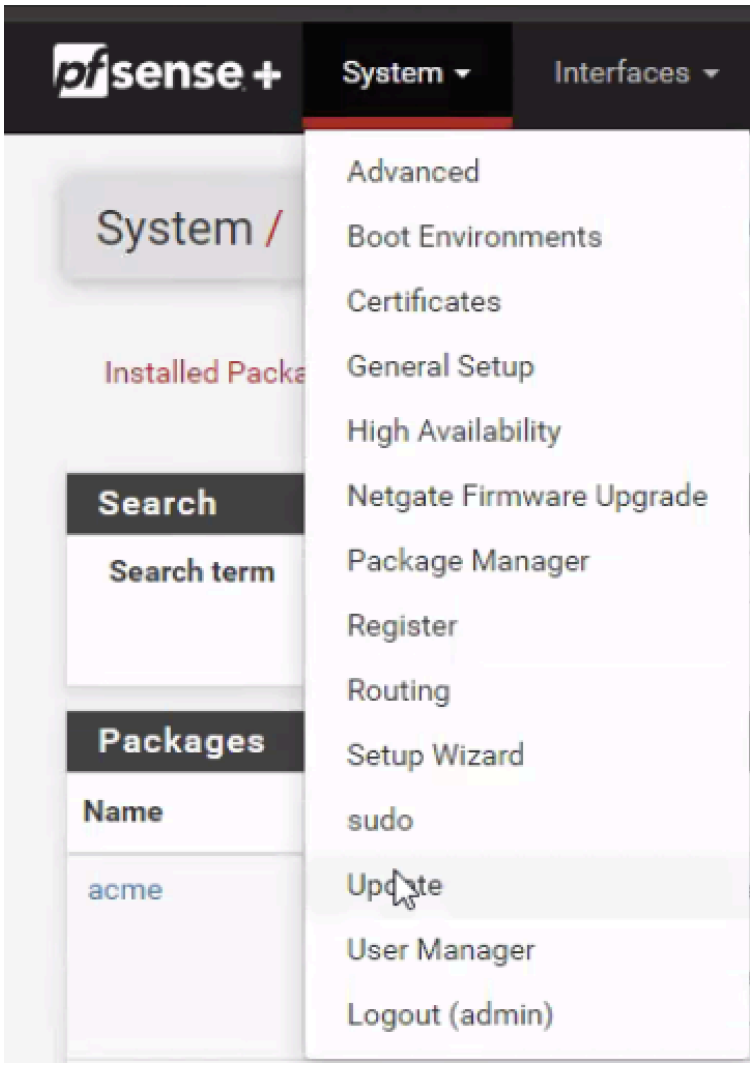
- In the pfSense web interface, go to "System" > "Package Manager".
- Click on the "Available Packages" tab.
- Search for "Snort" in the available packages list.

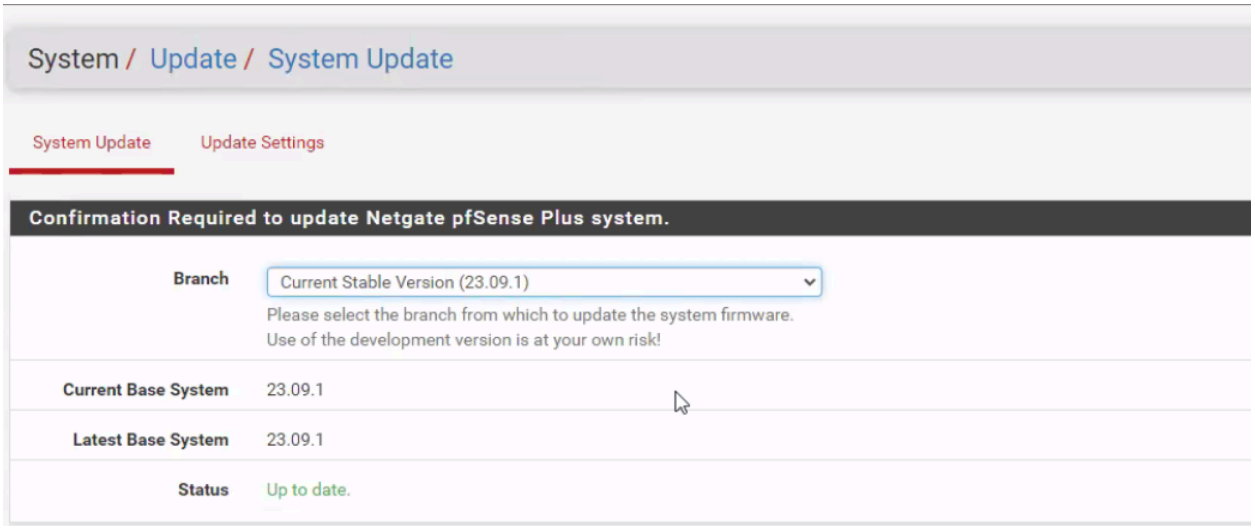


**** Issue encountered: The retrieval of available packages failed, necessitating troubleshooting measures.****

Steps taken to troubleshoot:

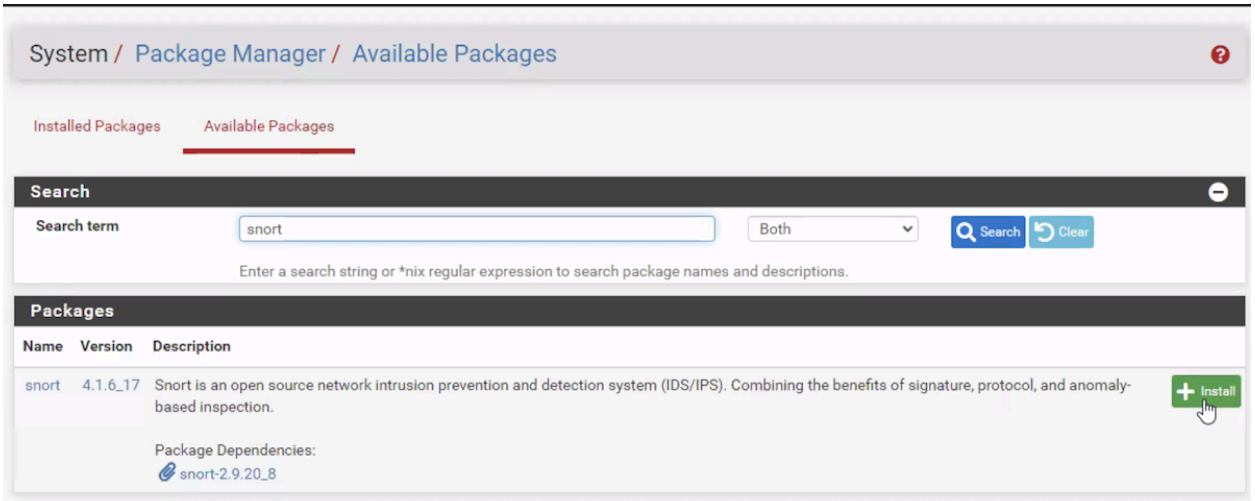
1. Navigate to "System" in the menu.
2. Select "Update" from the dropdown.
3. Choose "System Update."



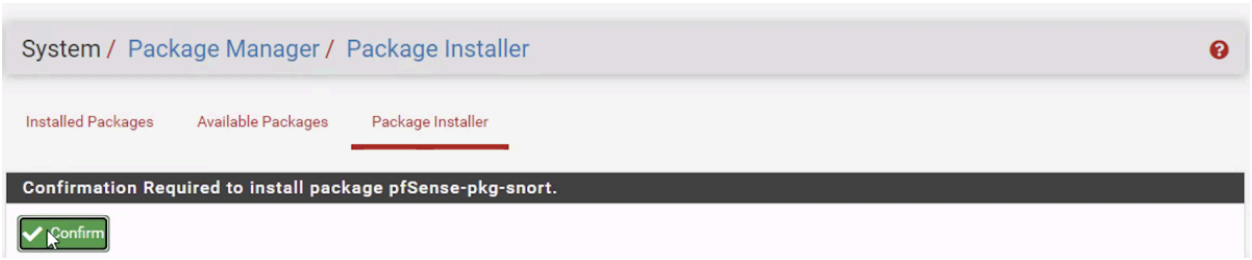


Repeat the following steps:

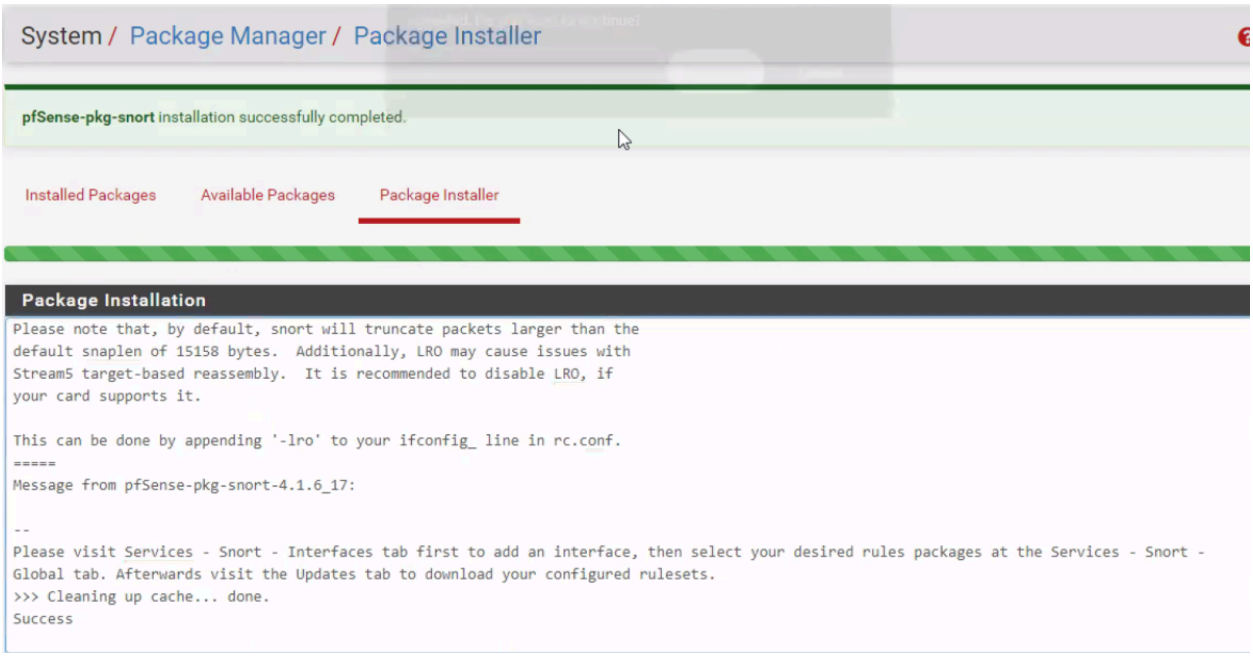
- Navigate to the "Available Packages" tab.
- Search for "Snort" within the list of available packages.



- Click on the "Install" button next to the Snort package to initiate the installation process.
- Follow the on-screen instructions to install the Snort package. It may take a few minutes to complete the installation.

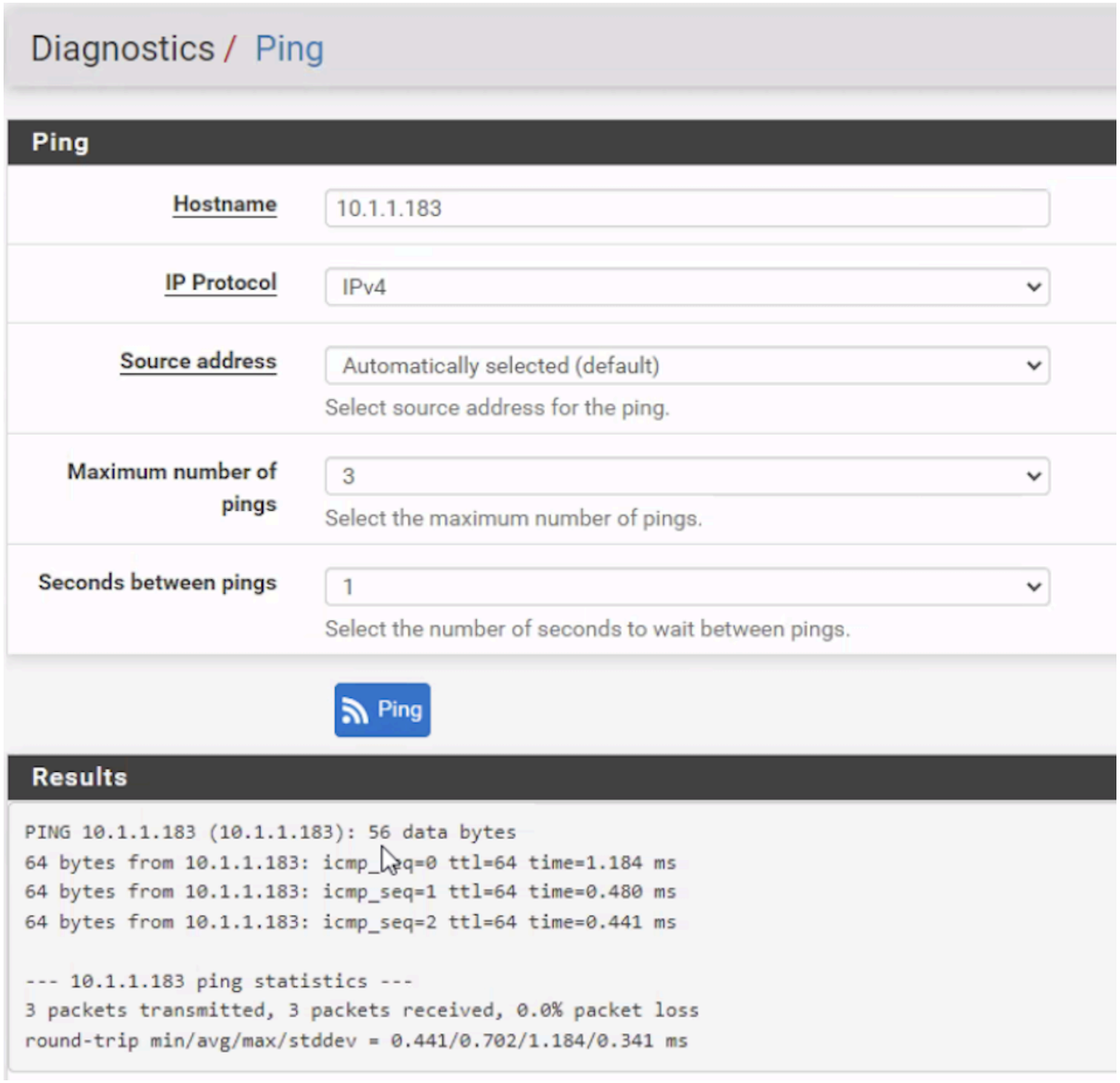


- Installation complete

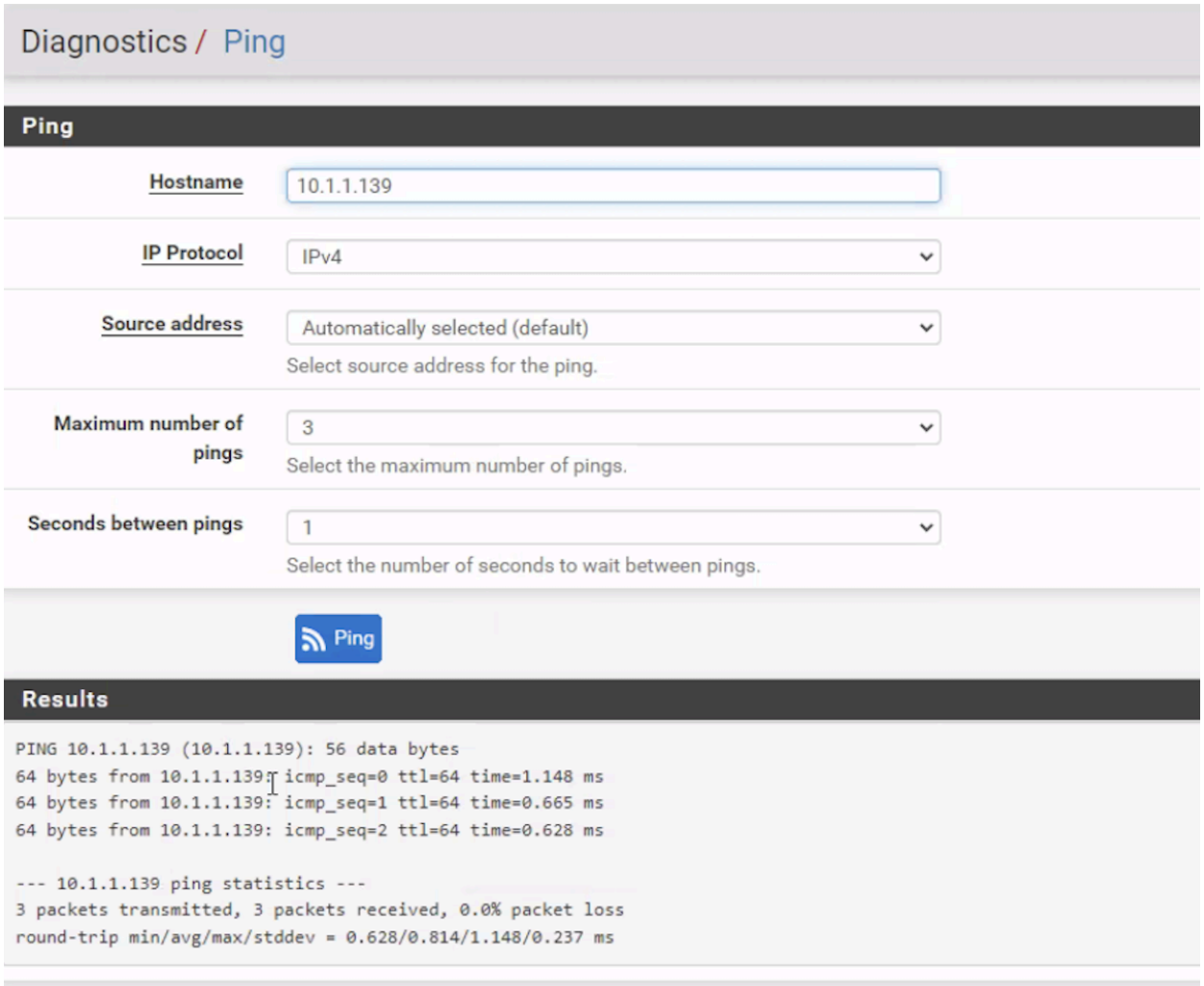


10. Test Connectivity and Security

- Successfully tested connection to hostname 10.1.1.83 from pfsense (ping)



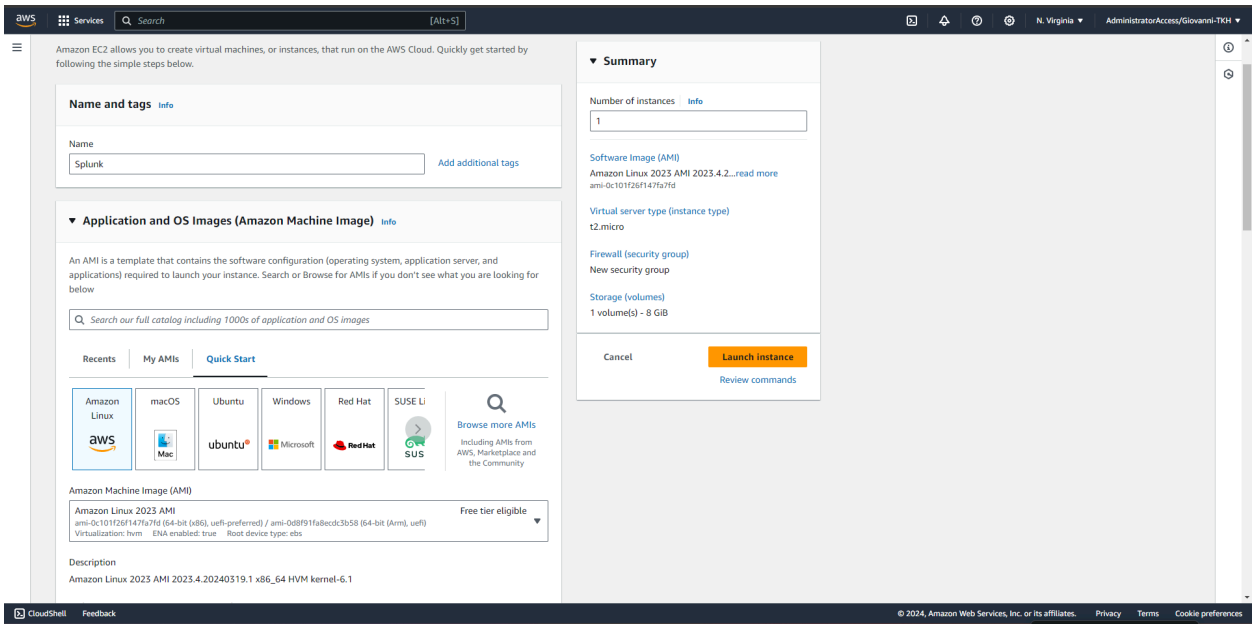
- Successfully tested connection to hostname 10.1.1.139 from pfsense (ping)



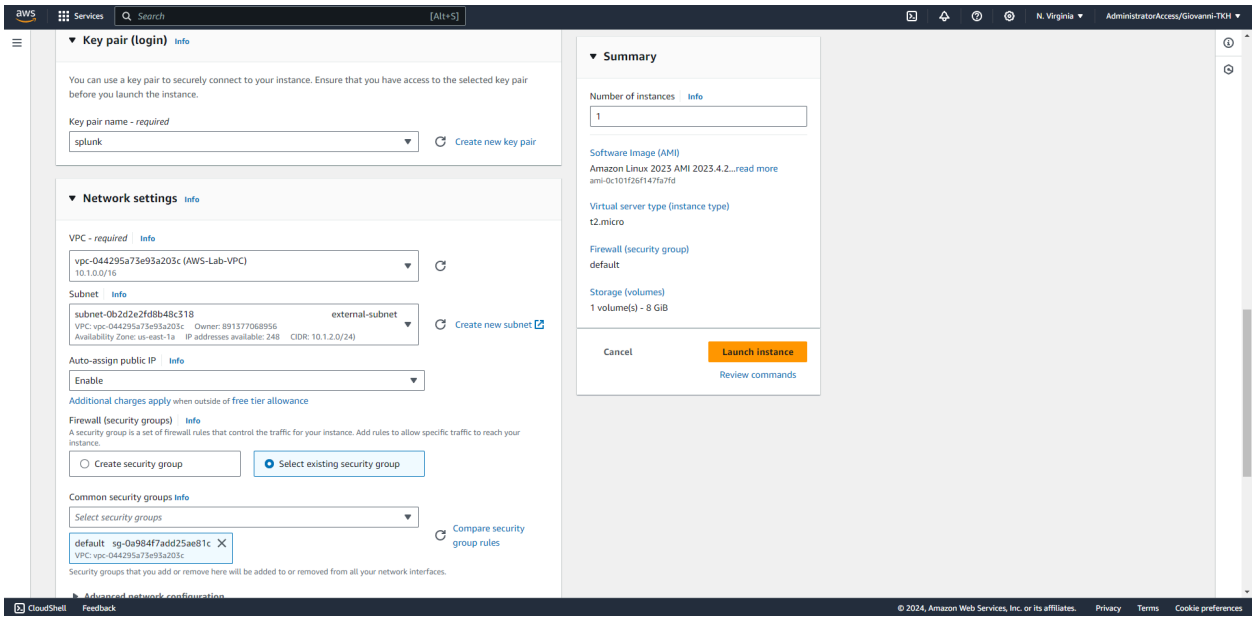
- Verify connectivity within the VPC, between subnets, and to the internet.
- Test pfSense firewall rules, VPN connections, and network segmentation to ensure proper security configurations.
- Monitor network traffic and security logs for any anomalies or security incidents.

Splunk Installation Process:

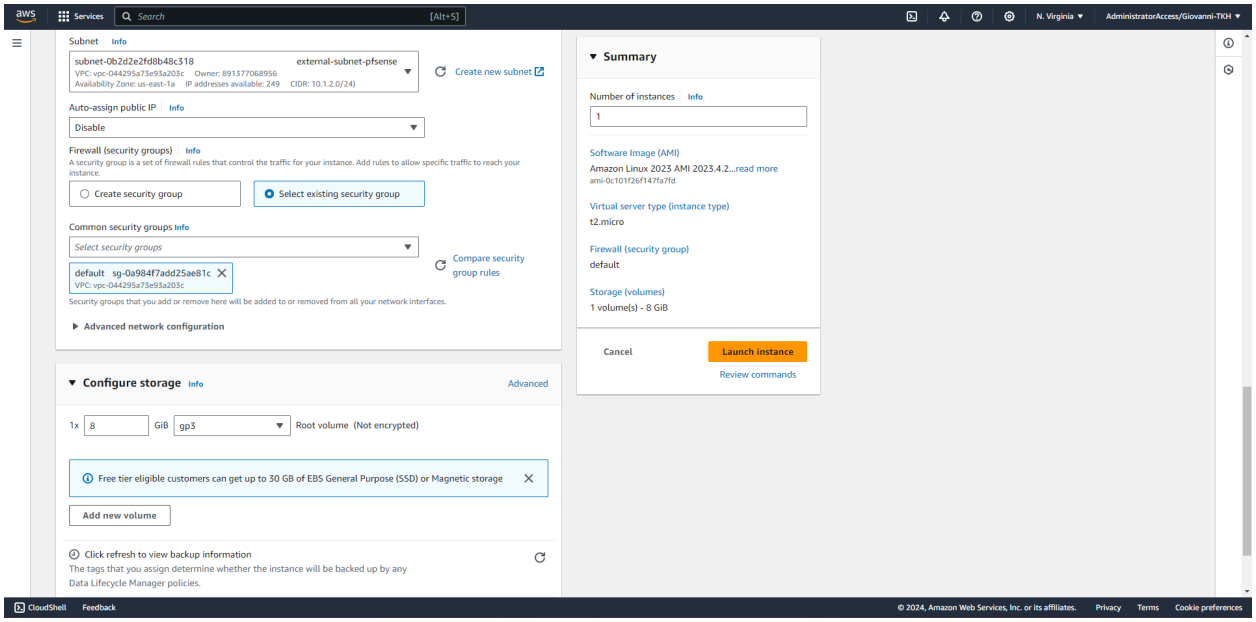
Go to launch and EC2 instance.



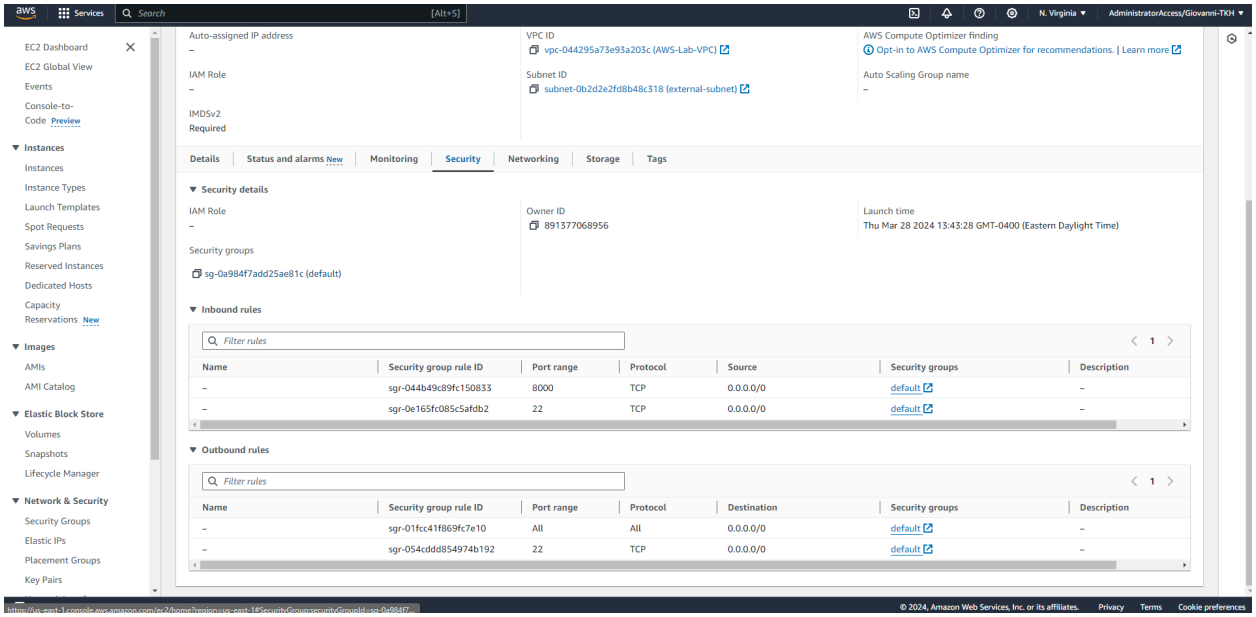
Choose the Amazon Linux Image with free tier



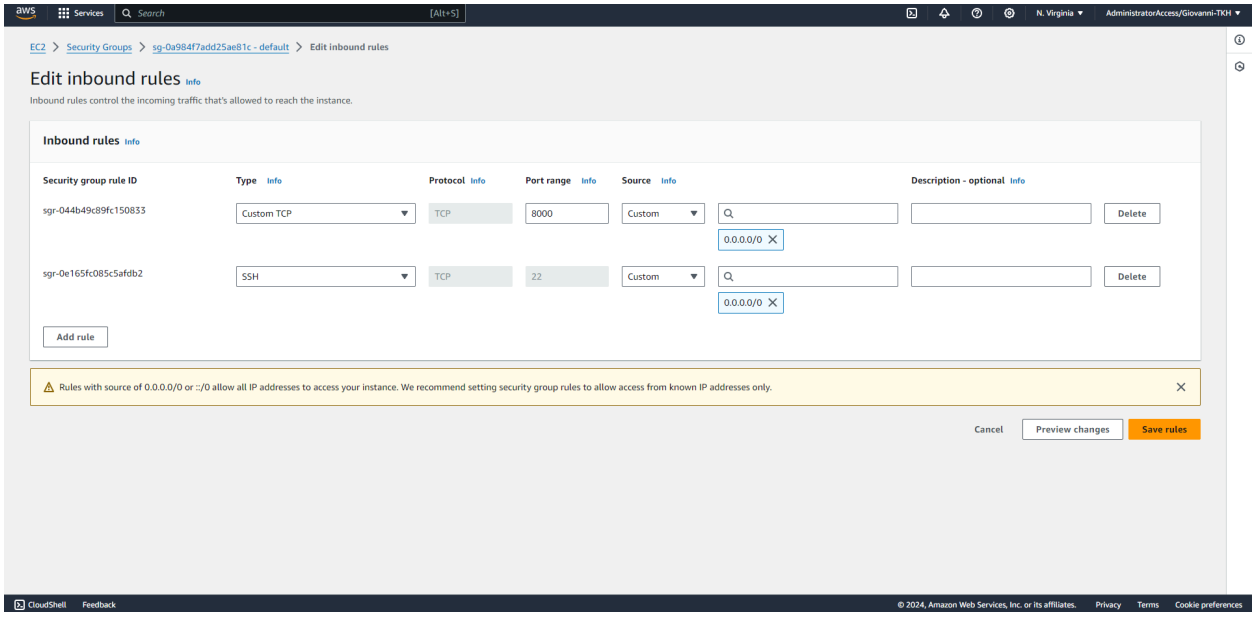
Grab your key pair and make sure to edit the network settings to match our lab's purposes.



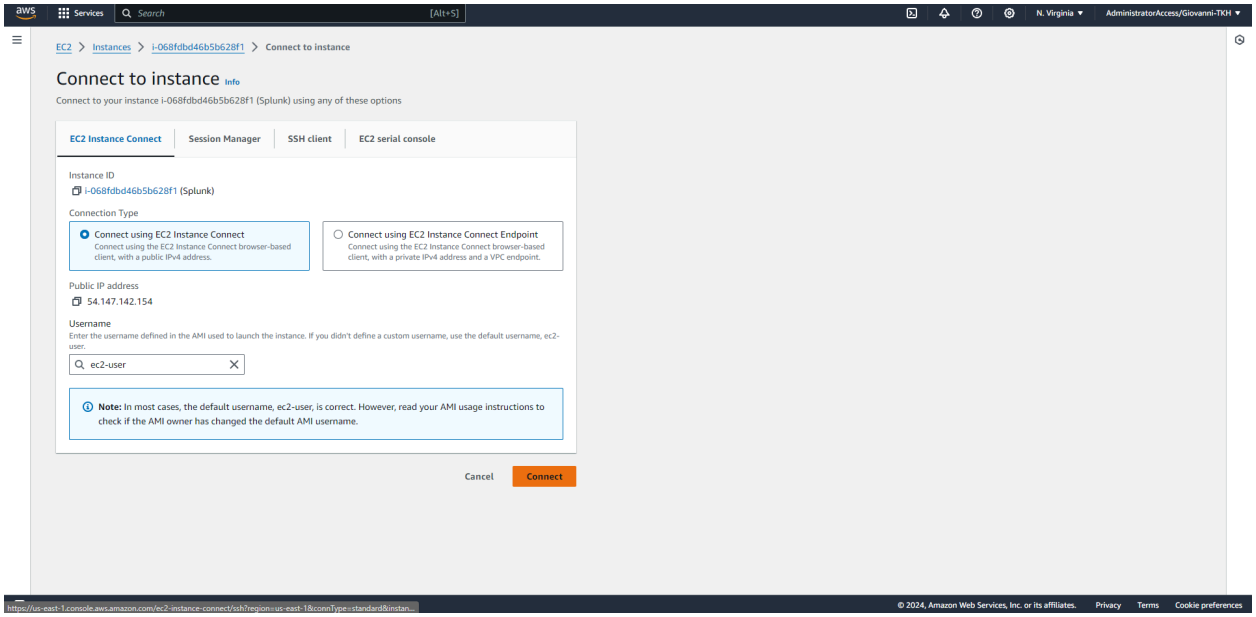
We'll select the default security group from the existing security groups. Then we can launch the instance.



Before we continue, we will change the inbound rule to accept port 8000 as this will be the port the splunk web ui exists.

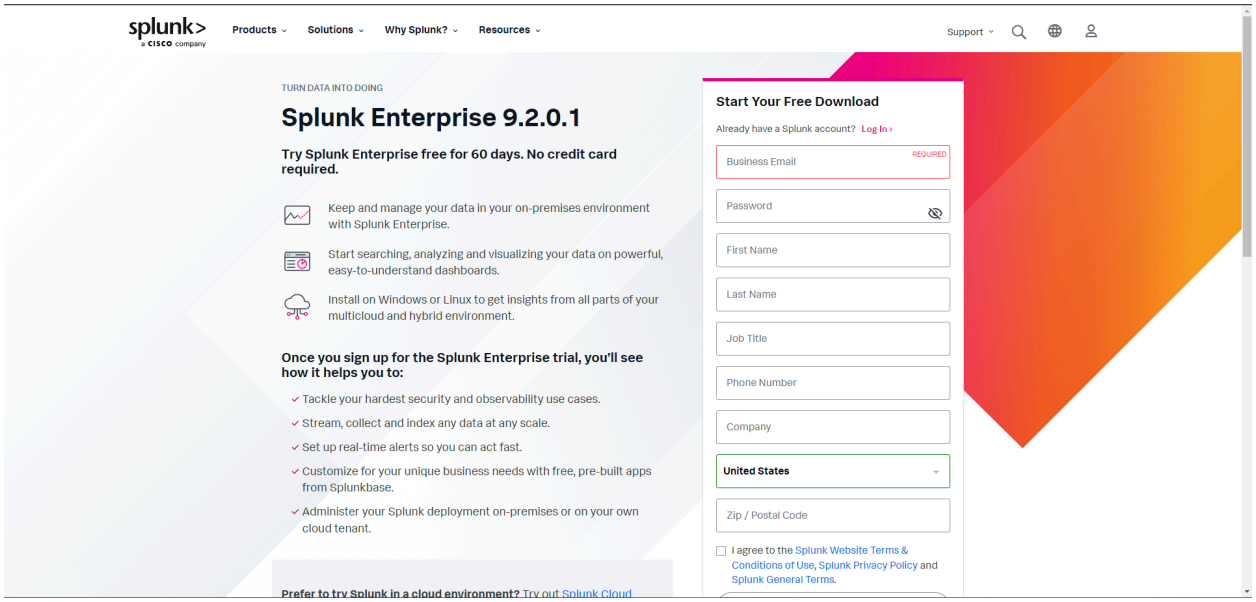


It should look like this. Now we can go and connect to our machine through instant connect.

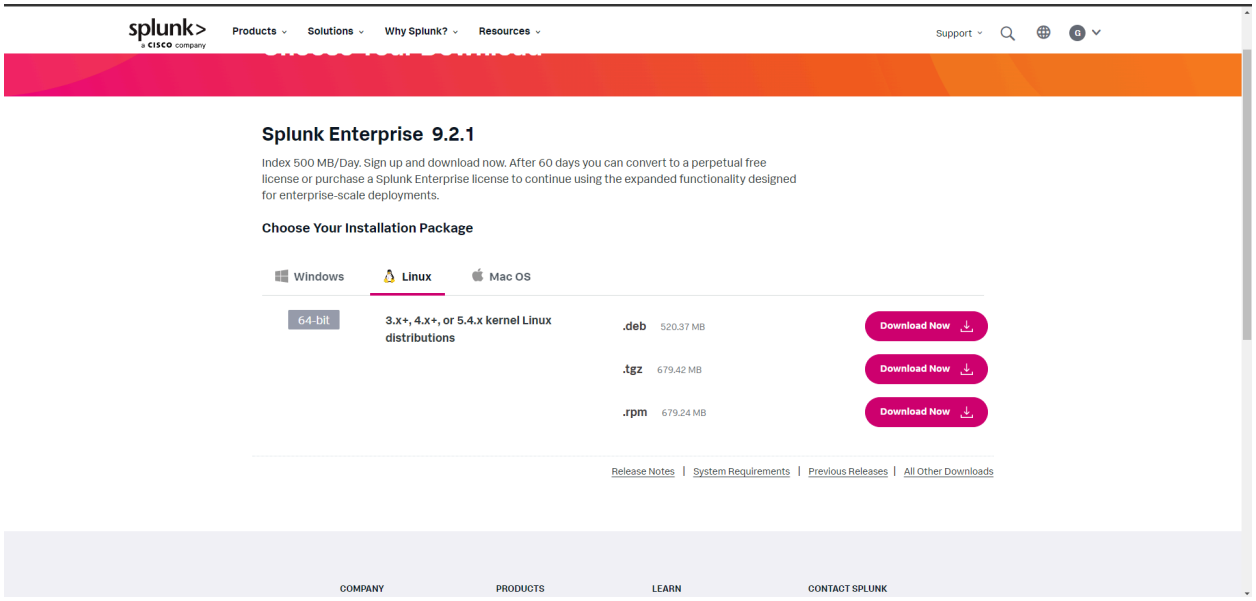


Click connect

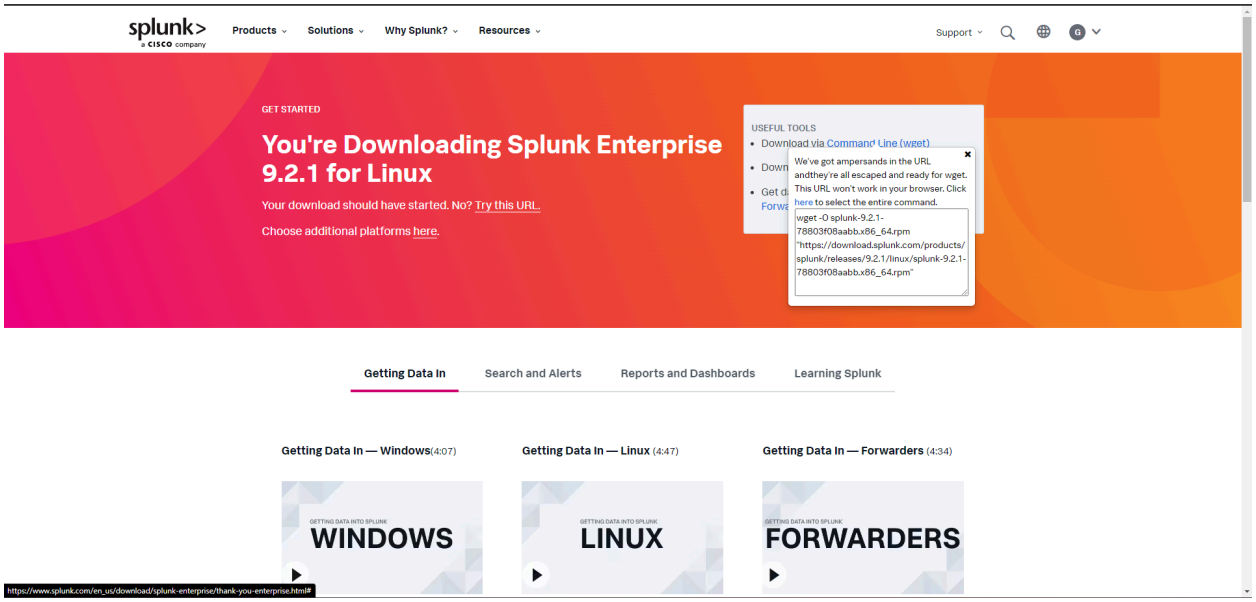
It should be getting you connected to the terminal. So before doing anything on it we need a Splunk Enterprise Free Trial Subscription.



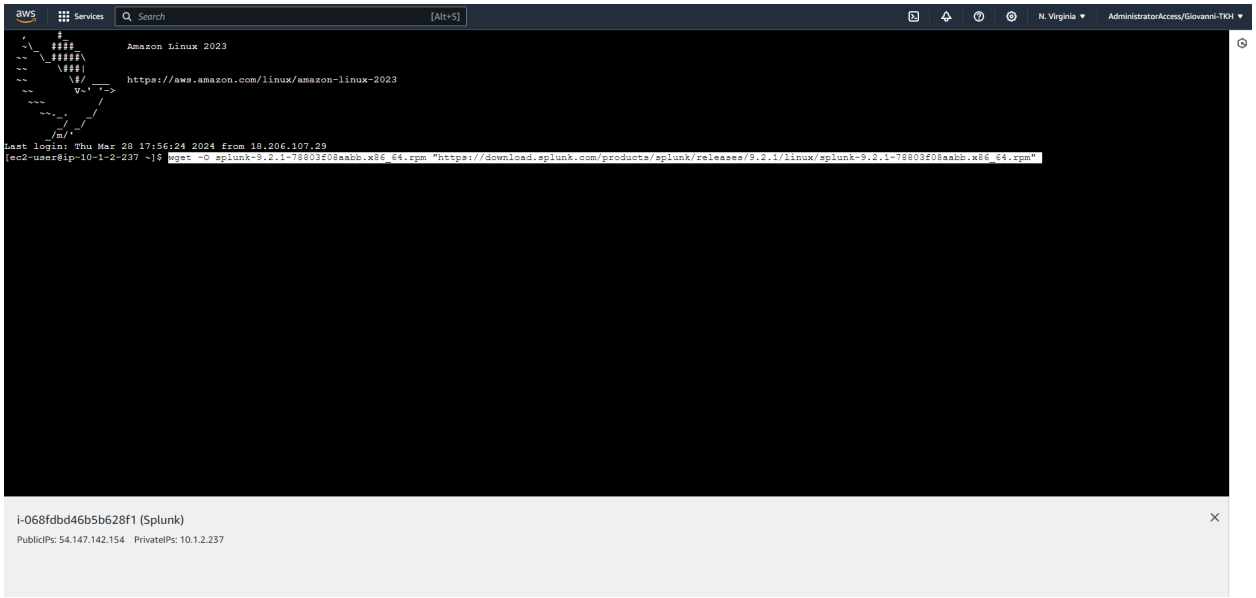
Just sign up and you'll get to the downloads section.



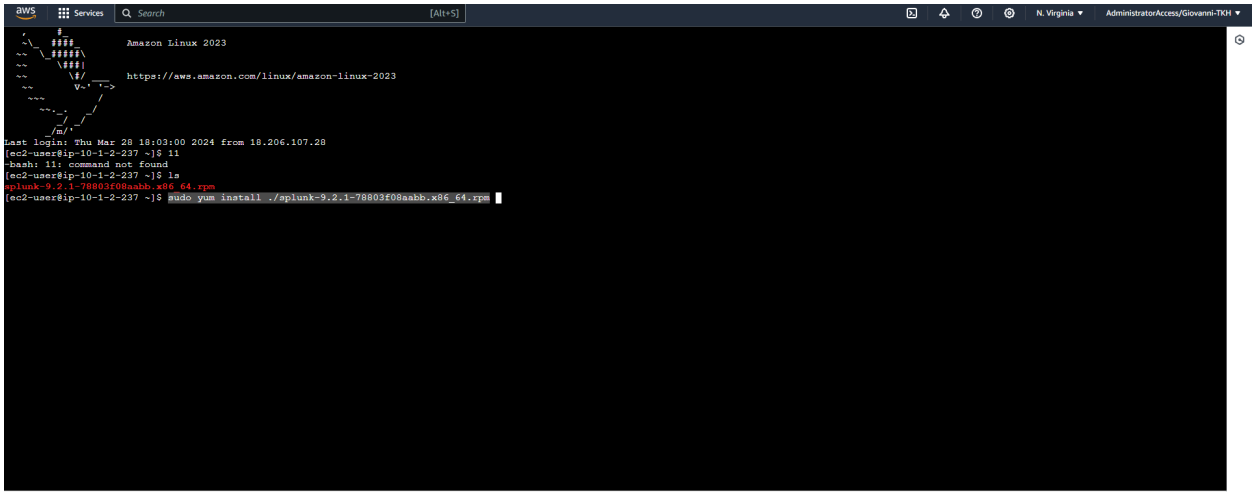
We'll be using the rpm version for linux. Click on the download for that



Copy this command line for installation and keep on a notepad for future reference.



Paste that installation command and let it run.



Then we will install it using *sudo yum install ./splunk-9.2.1-78803f08aabb.x86_64.rpm* and let it run and press y when prompted

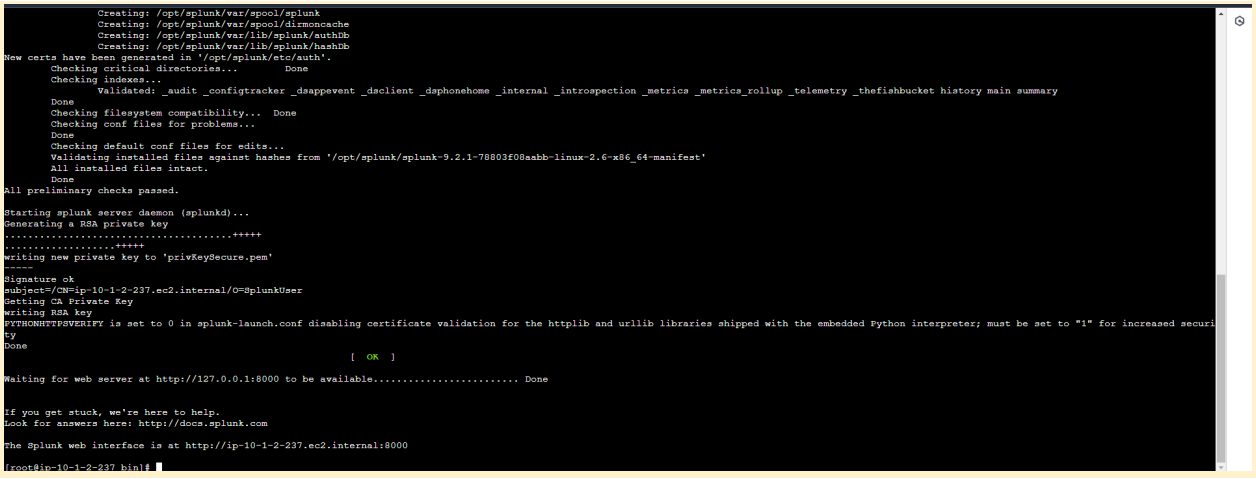
Once that's done go to root using *sudo bash*

Then we will change directories to re

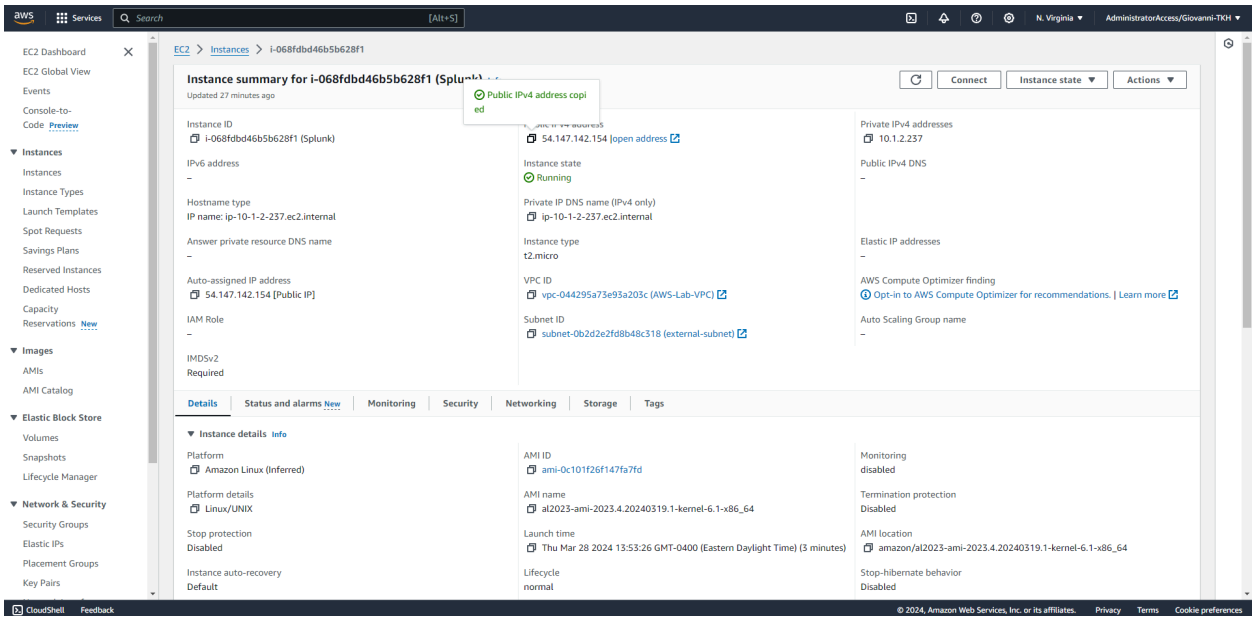
And lastly we will start our application using ./splunk start --accept-license --answer-yes

It will tell you to create a username, just press enter as we'll be using the default. Then it will ask you for a password, you can customize that yourself.

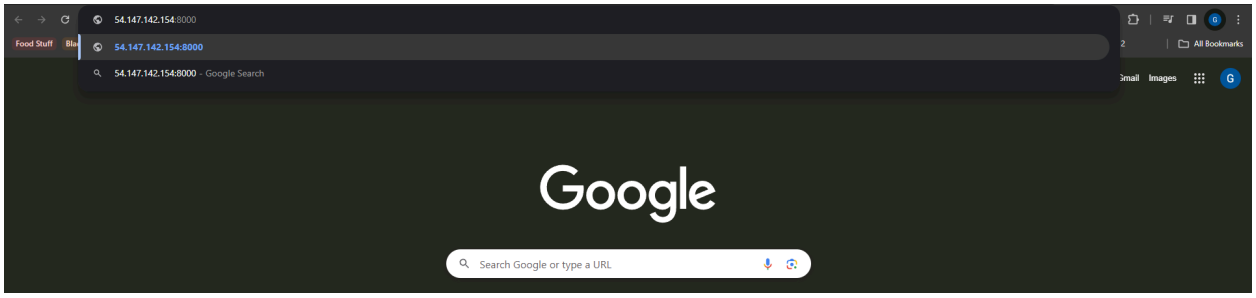
Once that's done it'll start initializing the setup for the webui interface.



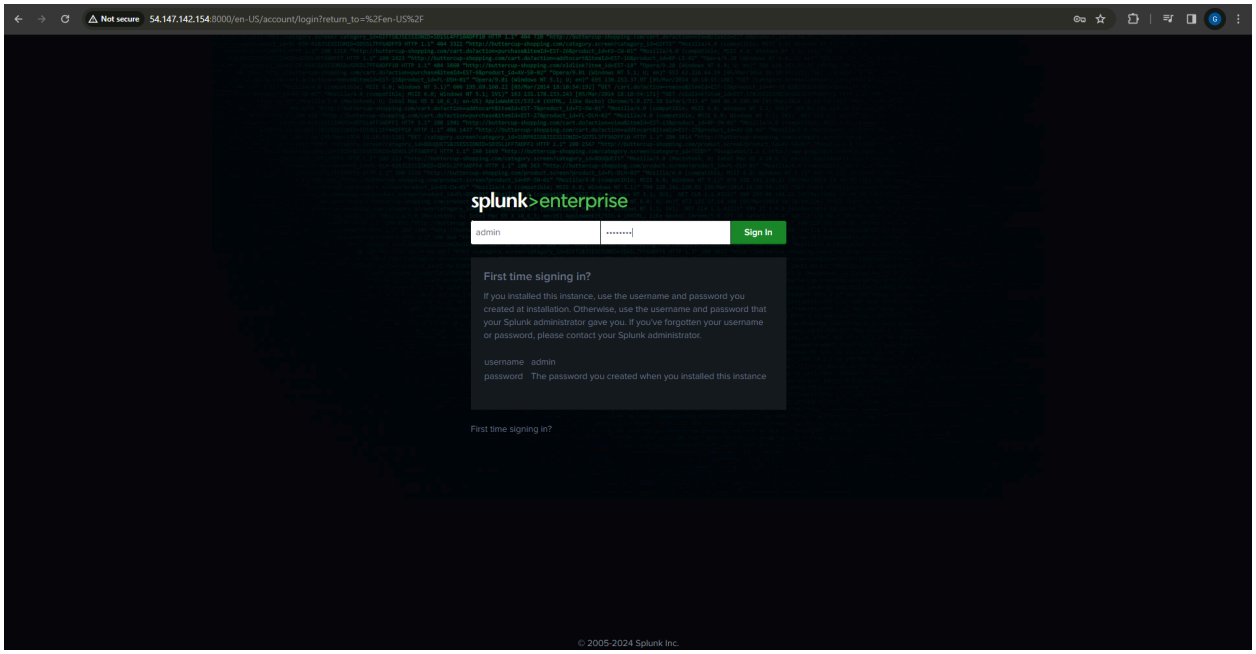
This is the end message and result



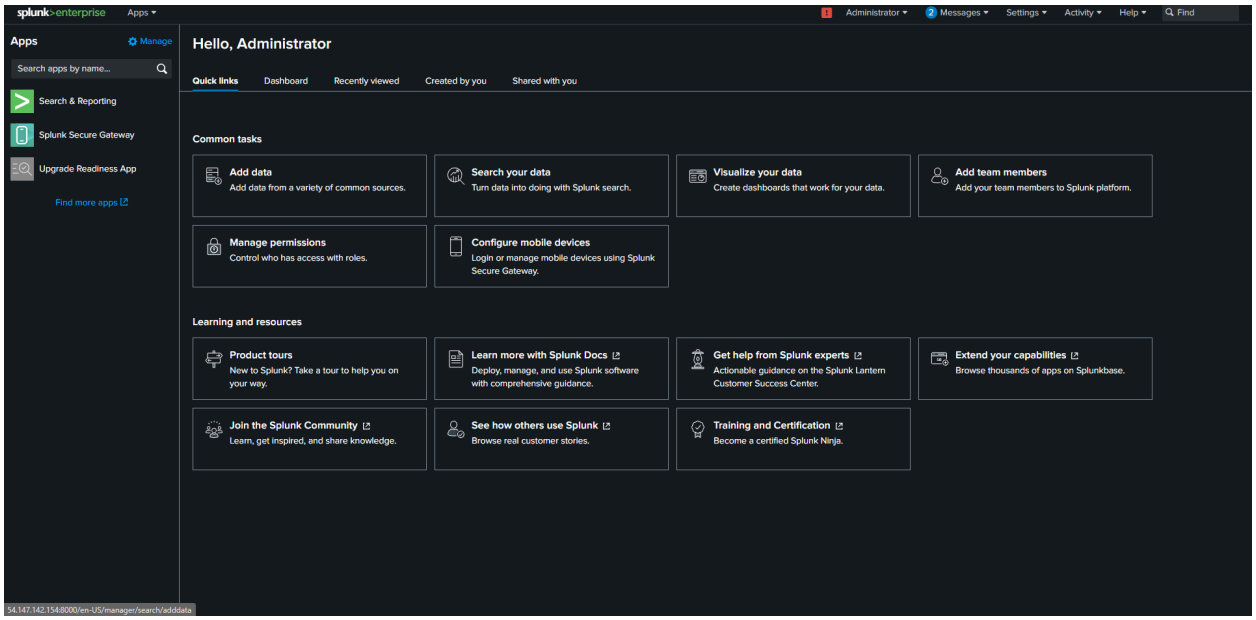
We will go back to our instance details page and copy the public ip address.



Open a new tab and paste the address but remember to put :8000 at the end of that address. Then press enter.



Enter the username (admin) and password you created before.



Now we have access to Splunk!