

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.

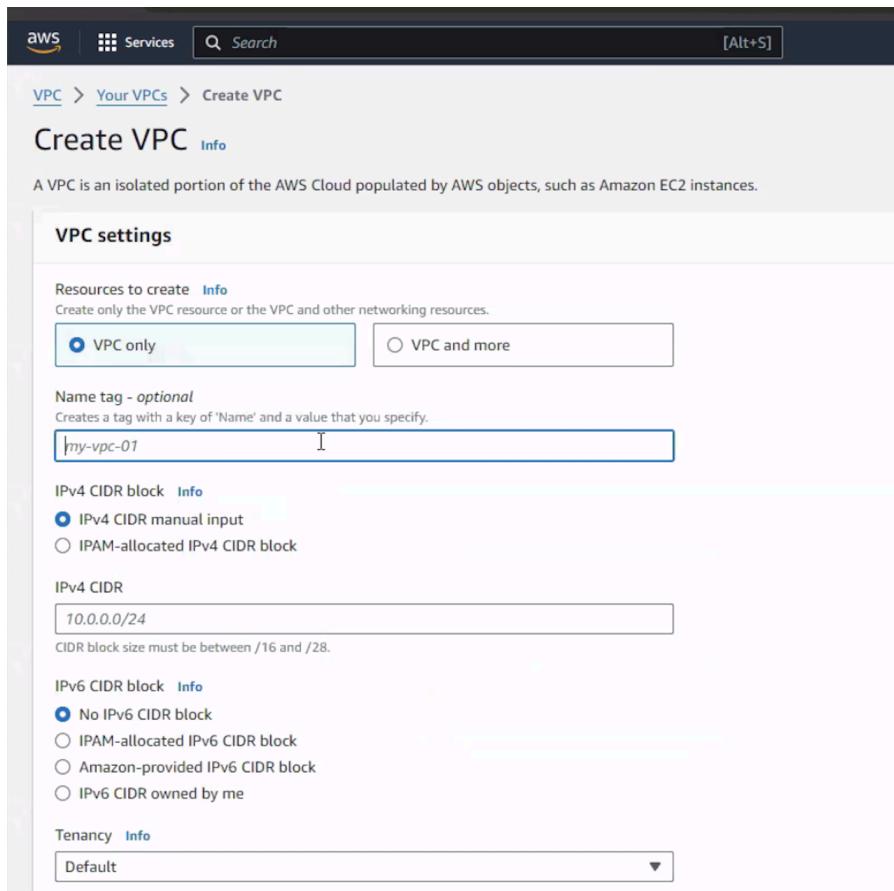
3. Verify Ping Connectivity:

- 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



The screenshot shows the 'Create VPC' wizard in the AWS Management Console. The first step is 'Resources to create'. The 'VPC only' option is selected. A 'Name tag - optional' field contains 'pfSense-firewall-vpc'. Under 'IPv4 CIDR block', 'IPv4 CIDR manual input' is selected, with '10.1.0.0/16' entered. Under 'IPv6 CIDR block', 'No IPv6 CIDR block' is selected. In the 'Tenancy' section, 'Default' is chosen. The 'Tags' section shows a single tag 'Name: pfSense-firewall-vpc'. At the bottom are 'Cancel' and 'Create VPC' buttons.

- 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

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

Select a VPC

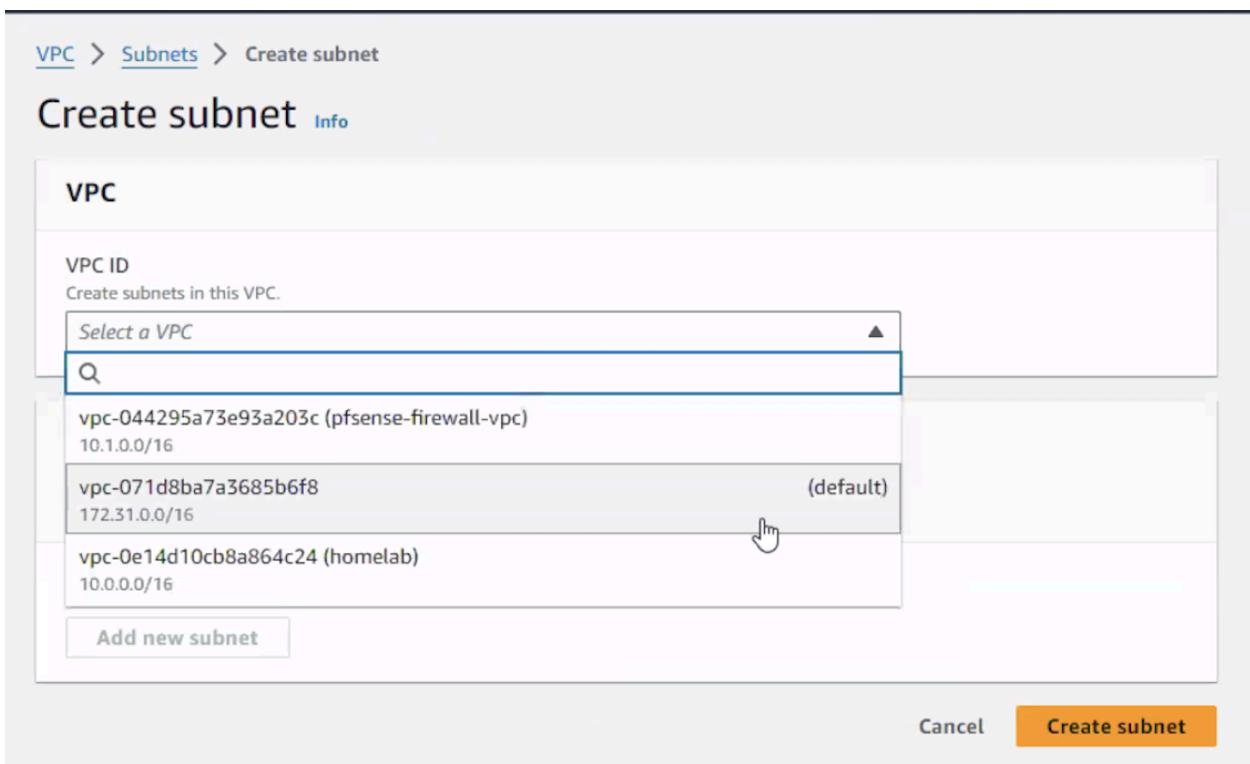
vpc-044295a73e93a203c (pfSense-firewall-vpc)
10.1.0.0/16

vpc-071d8ba7a3685b6f8 (default)
172.31.0.0/16

vpc-0e14d10cb8a864c24 (homelab)
10.0.0.0/16

Add new subnet

Cancel **Create subnet**



VPC

VPC ID
Create subnets in this VPC.

vpc-044295a73e93a203c (pfSense-firewall-vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.1.0.0/16



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

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.



IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.



IPv4 subnet CIDR block



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

Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.



IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.



IPv4 subnet CIDR block

256 IPs



▼ Tags - optional

- We successfully created two subnets

⌚ You have successfully created 2 subnets: subnet-045e15112ee34ae71, subnet-0b2d2e2fd8b48c318					
Subnets (2) Info					
<input type="text"/> Find resources by attribute or tag					
Subnet ID : subnet-045e15112ee34ae71	X	Subnet ID : subnet-0b2d2e2fd8b48c318	X	Clear filters	
Name	Subnet ID	State	VPC	IPv4 CIDR	
internal-subnet-pfsense	subnet-045e15112ee34ae71	Available	vpc-044295a73e93a203c pfs...	10.	
external-subnet-pfsense	subnet-0b2d2e2fd8b48c318	Available	vpc-044295a73e93a203c pfs...	10.	

3. Create Route Tables:

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

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

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

VPC
The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="internal-routetable-ein"/> X
Add new tag	

You can add 49 more tags.

[Cancel](#) [Create route table](#)

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

VPC > Route tables > rtb-097f73b841967d070 > Edit routes

Edit routes

Destination	Target	Status
10.1.0.0/16	<input type="text" value="local"/> X	<input checked="" type="checkbox"/> Active
<input type="text" value="0.0.0.0"/> X	<input type="text" value="Network Interface"/> X	-
	<input type="text" value="eni-03e785cf84645127"/> X	
Add route		

- Associate the route table with the appropriate subnets.

VPC > Route tables > rtb-097f73b841967d070 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)		
<input type="text"/> Filter subnet associations		
	Name	Subnet ID
	internal-subnet-pfsense	subnet-045e15112ee34ae71
		10.1.0.0/24

You have successfully updated subnet associations for rtb-097f73b841967d070 / internal-routetable-ein.

VPC > Route tables > rtb-097f73b841967d070 / internal-routetable-ein

Details <small>Info</small>	
Route table ID rtb-097f73b841967d070	Main No
VPC vpc-044295a73e93a203c	Owner ID 891377068956
Explicit subnet associations subnet-045e15112ee34ae71 / internal-subnet-pfsense	
Edge associations -	

Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (2)				
<input type="text"/> Filter routes				
Destination	Target	Status	Propagated	
0.0.0.0/0	eni-03e785cf84645127f	Active	No	
10.1.0.0/16	local	Active	No	

4. Create Internet Gateway:

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

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

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

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

 X

Value - optional

 XRemoveAdd new tag

You can add 49 more tags.

CancelCreate internet gateway

- Attach the internet gateway to the VPC created earlier.

[VPC](#) > [Internet gateways](#) > Attach to VPC (igw-0043948bf16766c22)

Attach to VPC (igw-0043948bf16766c22) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

 X

▶ AWS Command Line Interface command

CancelAttach internet gateway

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.

Create network interface

An elastic network interface is a logical networking component in a VPC that represents a virtual network card.

Details [Info](#)

Description - *optional*
A descriptive name for the network interface.

Subnet
The subnet in which to create the network interface.
 [X](#) [C](#)

Private IPv4 address
The private IPv4 address to assign to the network interface.
 Auto-assign [Custom](#)

Elastic Fabric Adapter
 Enable

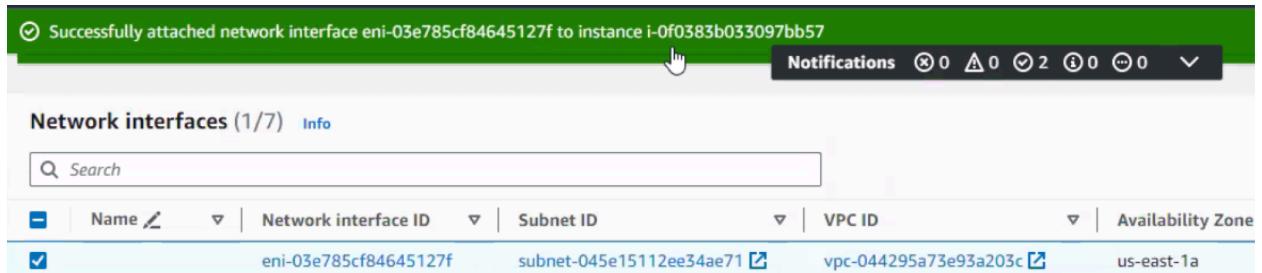
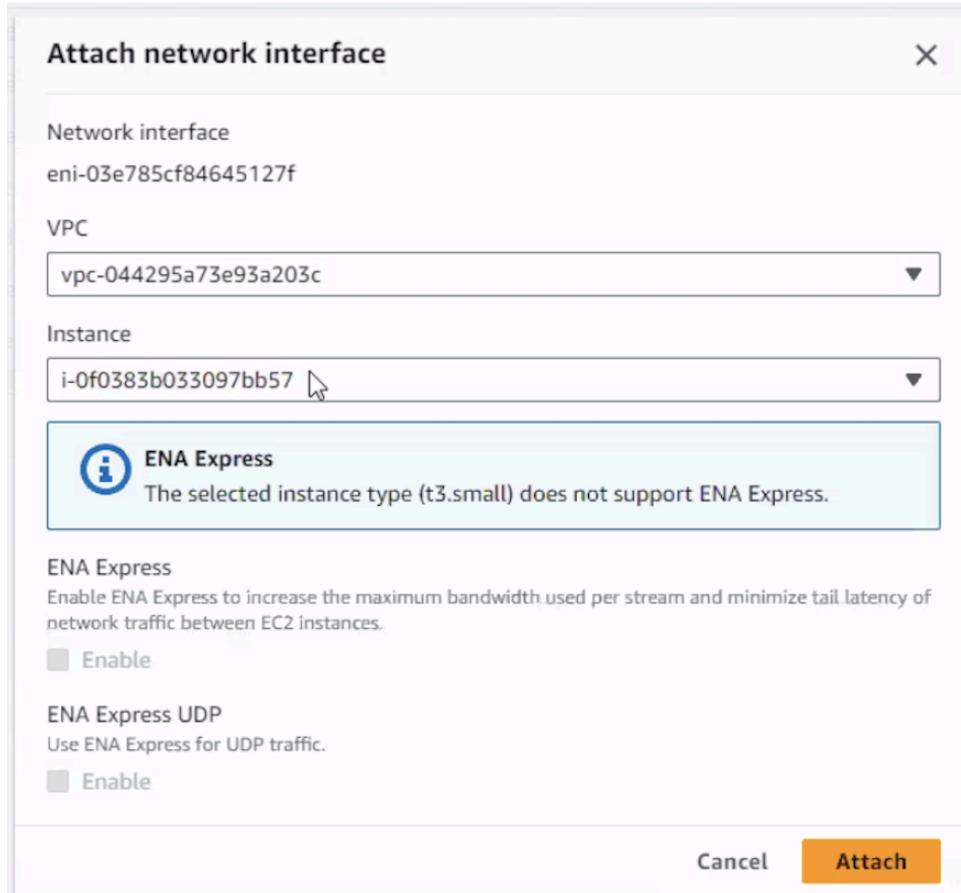
[Advanced settings](#)

Security groups (1/2) [Info](#)

[X](#) [1](#) [2](#) [3](#)

<input type="checkbox"/>	Group ID	Group name	Description
<input checked="" type="checkbox"/>	sg-0a984f7add25ae81c	default	default VPC security group
<input type="checkbox"/>	sg-0f7a37a3b60084ef4	Netgate pfSense Plus Firewall...	Netgate pfSense Plus Firewall...

- 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.

AWS Marketplace AMIs (12) AWS & trusted third-party AMIs

Community AMIs (8) Published by anyone

sense (12 results) showing 1 - 12 Sort By: Relevance

pfSense + Netgate pfSense Plus Firewall/VPN/Router (ARM64/Graviton)

By Netgate | Ver 23.09.1 w Graviton
Starting from \$0.34/hr or from \$2,100.00/yr (up to 31% savings) for software + AWS usage fees
OVERVIEW pfSense Plus software is the world's leading price-performance edge firewall, router, and VPN solution. Over seven million installations used by homes, businesses, government agencies, educational institutions and service providers. PRICING //For Private Offers on multiple instances, 2 & ...

pfSense + Netgate pfSense Plus Firewall/VPN/Router

By Netgate | Ver 23.09.1
★ ★ ★ ★ 9 AWS reviews | 313 external reviews
Free Trial
Starting from \$0.01/hr or from \$75.00/yr (up to 31% savings) for software + AWS usage fees
OVERVIEW pfSense Plus software is the world's leading price-performance edge firewall, router, and VPN solution. Over seven million installations used by homes, businesses, government agencies, educational institutions and service providers. PRICING //03-2024 - Pricing Change - Affecting T2 & T3 o...

Netgate pfSense Plus Firewall/VPN/Router

Netgate | ★ ★ ★ ★ 9 AWS reviews | 313 external reviews
Free Tier | Free Trial

[Overview](#) | [Product details](#) | [Pricing](#) | [Usage](#) | [Support](#)

pfSense Plus software is the world's leading price-performance edge firewall, router, and VPN solution. Over seven million installations used by homes, businesses, government agencies, educational institutions and service providers.

Typical total price \$0.436/Hr Total pricing per instance for services hosted on m6i.large in us-east-1. See additional pricing information.	Latest version 23.09.1	Video Product Video
Delivery methods Amazon Machine Image ⓘ	Categories Security	
Operating systems FreeBSD 14	Network Infrastructure	

i A subscription to this AMI is required before you can launch an instance. Check the pricing details in the pricing tab before continuing.
You can subscribe to this AMI now or we will automatically subscribe for you when you launch this instance. We recommend that you 'Subscribe now' if you are sure this is the AMI you want to use to launch as it will reduce wait time on launch. Choose 'Subscribe on instance launch' if you are still choosing an AMI and don't want to commit to a subscription yet. By subscribing to this AMI you agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#).

Cancel [Subscribe on instance launch](#) [Subscribe now](#)

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

Instance Type:

- Type: t3.small

The screenshot shows the 'Instance type' section of the AWS instance creation wizard. The 't3.small' option is selected from a dropdown menu. Below the dropdown, it says 'Family: t3' and '2 vCPU 2 GiB Memory Current generation: true'. To the right, there's a toggle switch labeled 'All generations' and a link 'Compare instance types'. A note at the bottom states: 'The AMI vendor recommends using a m6i.large instance (or larger) for the best experience with this product.'

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**

The screenshot shows the 'Key pair (login)' configuration screen. It includes a note: '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.' Below this is a 'Key pair name - required' field containing the placeholder 'Select'. To the right is a 'Create new key pair' button.

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

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

Key pair type

RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠️ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

[Cancel](#) [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 

Storage Configuration:

- 1x 10 GiB gp2

▼ Configure storage [Info](#) [Advanced](#)

1x GiB ▾ Root volume (Not encrypted)

 Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage [X](#)

[Add new volume](#)

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

 Click refresh to view backup information [C](#)
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

- Launch the instance

[Cancel](#)

[Launch instance](#) 

[Review commands](#)

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**

▼ 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*

▼

 [Create new key pair](#)

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

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

Key pair type
 RSA RSA encrypted private and public key pair
 ED25519 ED25519 encrypted private and public key pair

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

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

[Cancel](#) [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

▼ 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: 250 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

launch-wizard-13

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](#)

launch-wizard-13 created 2024-03-27T23:03:12.496Z



Successfully initiated launch of instance ([i-035c2883a7bac4d76](#))

8.Launch Internal Kali Host Instance

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



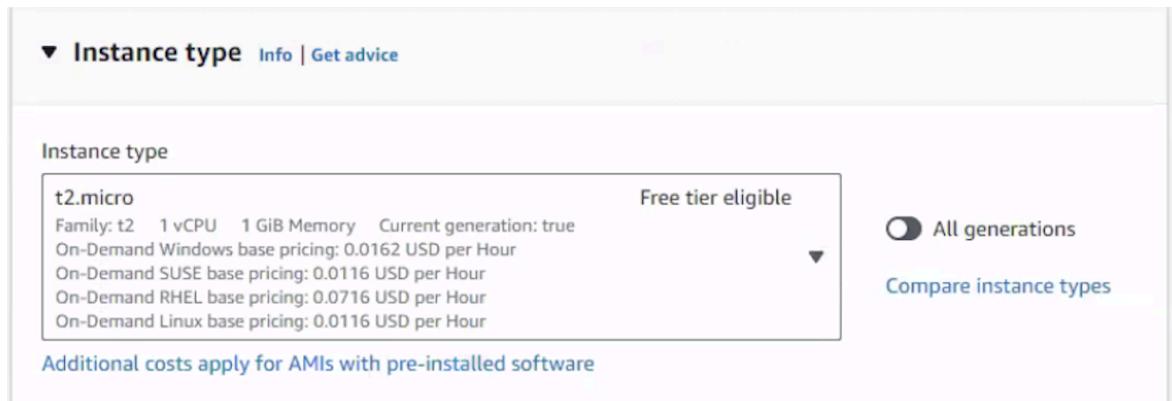
- Search for the AMI in the AWS Marketplace and select the desired AMI.
 - Selected **kali_v2**



- 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**

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

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

Key pair type

RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠️ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel **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

The screenshot shows the AWS Lambda function configuration page for the function 'lambda-function'. It includes sections for 'Environment' (with variable 'ENVIRONMENT' set to 'dev'), 'Triggers' (including CloudWatch Logs and CloudWatch Metrics), and 'Code' (selected as 'Lambda@Edge').

Environment Variables:

Name	Type	Value
ENVIRONMENT	String	dev

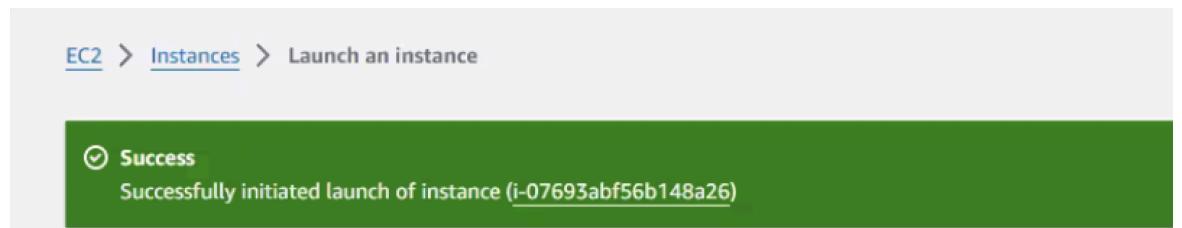
Triggers:

- CloudWatch Logs
- CloudWatch Metrics

Code:

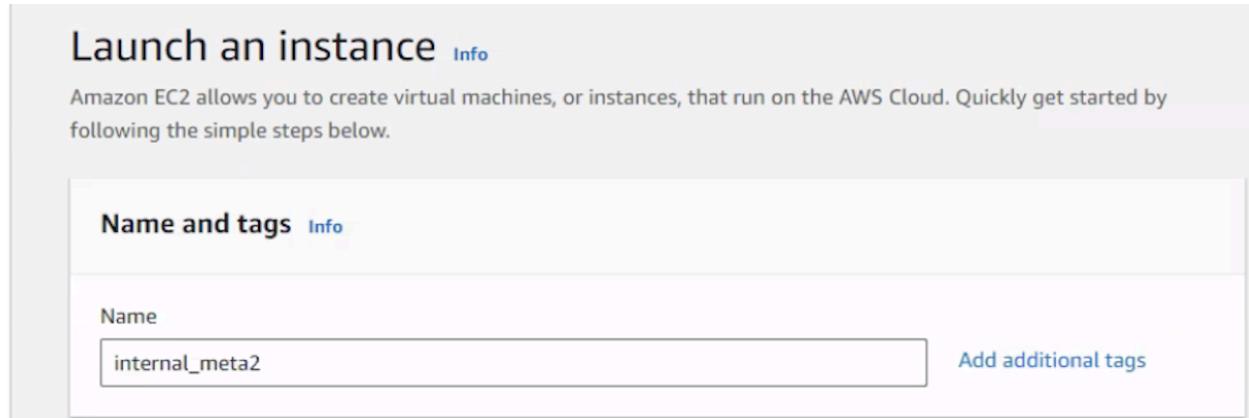
- Selected: Lambda@Edge
- Code Size: 18 KB
- Last Deployed: 2024-03-27T23:00:33.006Z

- 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

The screenshot shows the 'Instance type' section of the AWS CloudFormation template editor. A dropdown menu is open, showing the 't2.micro' instance type. The 'Free tier eligible' status is indicated. To the right, there are buttons for 'All generations' and 'Compare instance types'. A note at the bottom states: 'Additional costs apply for AMIs with pre-installed software'.

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**

The screenshot shows the 'Key pair (login)' section of the AWS CloudFormation template editor. It includes a note about using a key pair for secure connection. A dropdown menu for 'Key pair name - required' is shown with the value 'Select'. A 'Create new key pair' button is visible to the right.

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

meta2pfsense

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

Key pair type

RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠️ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel **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

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-044295a73e93a203c (pfsense-firewall-vpc)
10.1.0.0/16

Subnet [Info](#)

subnet-045e15112ee34ae71 internal-subnet-pfsense
VPC: vpc-044295a73e93a203c Owner: 891377068956
Availability Zone: us-east-1a IP addresses available: 249 CIDR: 10.1.1.0/24

Create new subnet

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

launch-wizard-12

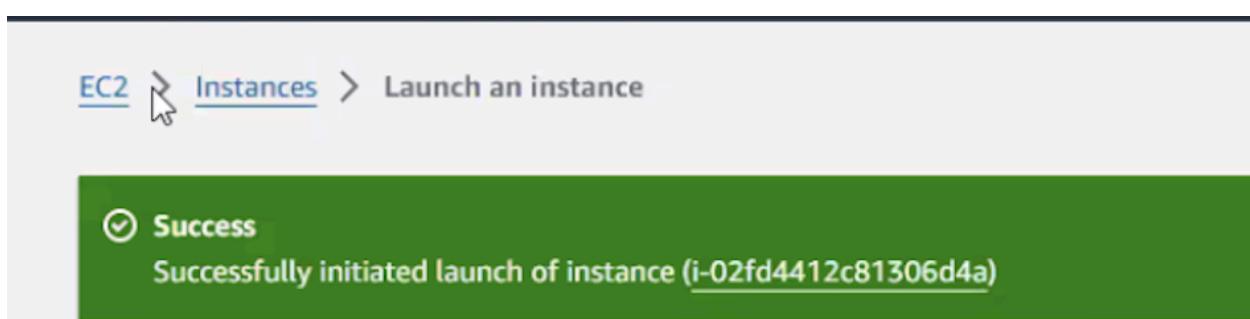
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#@[]+=&;!\$*

Description - required [Info](#)

launch-wizard-12 created 2024-03-27T23:02:11.644Z

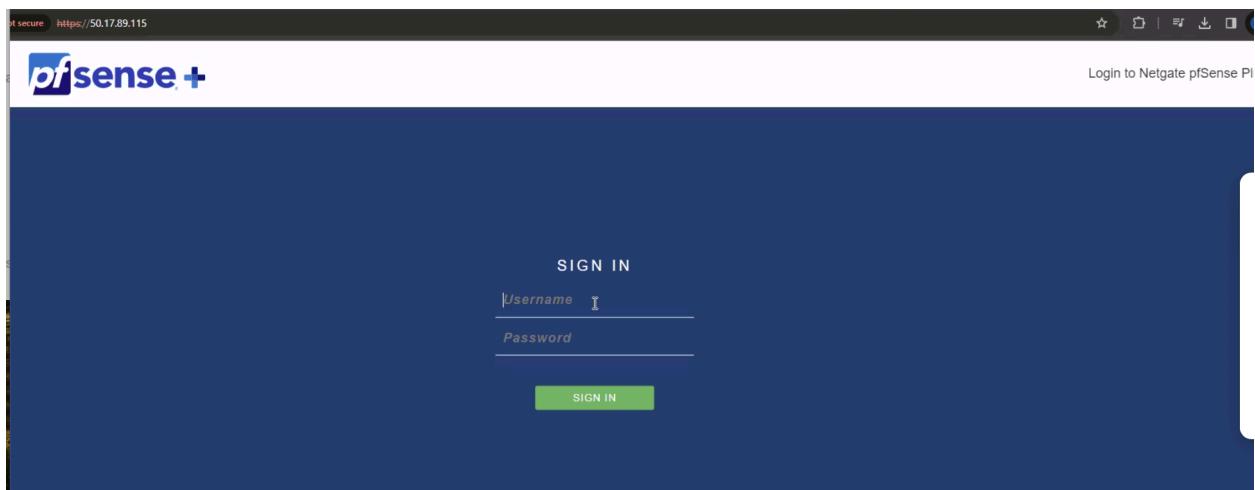
Inbound Security Group Rules

- Launch Instance



9. Configure pfSense

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

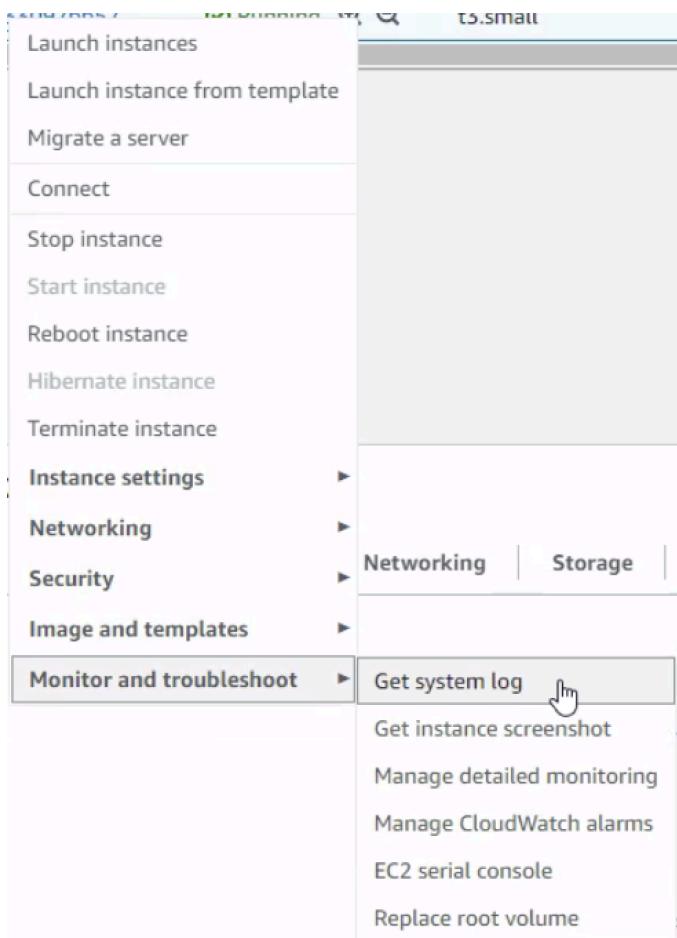


Username: admin

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".



Get system log Info

When you experience issues with your EC2 instance, reviewing system logs can help you pinpoint the cause.

System log

Review system log for instance i-0f0383b033097bb57 as of Wed Mar 27 2024 18:34:18 GMT-0400 (Eastern Daylight Time)

```
SSH Key retrieved: ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQGRRqqDLDpuajgGXjCtMjhzvCAL30seCxwk4svefUEgL

Netgate pfSense Plus 23.09.1-RELEASE amd64 20231206-2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyu0)

[07][r][999;999H[6n@resizewin: timeout reading from terminal
***  

***  

*** ec2-user password changed to: $1$INe!Z-(ak)  

***  

***  

Amazon Web Services - Netgate Device ID: f4b48c11b2be16beb522

*** Welcome to Netgate pfSense Plus 23.09.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> ena0      -> v4/DHCP4: 10.1.2.173/24

[0] Logout (SSH only) [1] Return
```

- 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

The screenshot shows the final step of the pfSense Plus Setup Wizard. The title bar reads "Wizard / pfSense Plus Setup / Wizard completed." A progress bar at the top indicates "Step 9 of 9". A black banner at the top says "Wizard completed.". Below it, a message says "Congratulations! pfSense Plus is now configured." It encourages users to check for updates and provides a "Check for updates" button. It also mentions support services with a link to "Click here to learn about Netgate 24/7/365 support services.". A section titled "User survey" asks for help in improving the software, with a link to "Anonymous User Survey". Another section titled "Useful resources" lists links to the product line, store, forum, and newsletter. A blue "Finish" button is at the bottom.

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.

The screenshot shows the "Available Packages" tab in the pfSense Package Manager. The title bar reads "System / Package Manager / Available Packages". Below it, there are tabs for "Installed Packages" and "Available Packages", with "Available Packages" being active. A search bar at the top has "snort" entered. Below the search bar is a placeholder text "Enter a search string or *nix regular expression to search package names and descriptions.". A table below is titled "Packages" and has columns for "Name", "Version", and "Description".

**** 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."

The screenshot shows the pfSense web-based configuration interface. At the top, there is a navigation bar with the pfSense logo, a "System" dropdown menu, and an "Interfaces" dropdown menu. Below the navigation bar, the main content area has a left sidebar with several sections: "System /", "Installed Packages", "Search" (with a "Search term" input field), and "Packages" (with a "Name" table). The "Name" table has one row for "acme". To the right of the sidebar, there is a list of system management options: Advanced, Boot Environments, Certificates, General Setup, High Availability, Netgate Firmware Upgrade, Package Manager, Register, Routing, Setup Wizard, sudo, Update, User Manager, and Logout (admin). The "Update" option is highlighted with a light green background and a cursor arrow pointing to it.

System / Update / System Update

System Update Update Settings

Confirmation Required to update Netgate pfSense Plus system.

Branch	Current Stable Version (23.09.1)
Please select the branch from which to update the system firmware. Use of the development version is at your own risk!	
Current Base System	23.09.1
Latest Base System	23.09.1
Status	Up to date.

Repeat the following steps:

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

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: snort Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
snort	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.

Package Dependencies:
 snort-2.9.20_8

- 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.



Installed Packages Available Packages Package Installer

Confirmation Required to install package pfSense-pkg-snort.

Confirm

- Installation complete



PfSense-pkg-snort installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

Please note that, by default, snort will truncate packets larger than the default snaplen of 15158 bytes. Additionally, LRO may cause issues with Stream5 target-based reassembly. It is recommended to disable LRO, if your card supports it.

This can be done by appending '-lro' to your ifconfig_ line in rc.conf.

=====

Message from pfSense-pkg-snort-4.1.6_17:

--
Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.

>>> Cleaning up cache... done.

Success

10. Test Connectivity and Security

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

Diagnostics / Ping

Ping

<u>Hostname</u>	10.1.1.183
<u>IP Protocol</u>	IPv4
<u>Source address</u>	Automatically selected (default) Select source address for the ping.
<u>Maximum number of pings</u>	3 Select the maximum number of pings.
<u>Seconds between pings</u>	1 Select the number of seconds to wait between pings.

 Ping

Results

```
PING 10.1.1.183 (10.1.1.183): 56 data bytes
64 bytes from 10.1.1.183: icmp_seq=0 ttl=64 time=1.184 ms
64 bytes from 10.1.1.183: icmp_seq=1 ttl=64 time=0.480 ms
64 bytes from 10.1.1.183: icmp_seq=2 ttl=64 time=0.441 ms

--- 10.1.1.183 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.441/0.702/1.184/0.341 ms
```

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

Diagnostics / Ping

Ping

Hostname

IP Protocol

Source address

Select source address for the ping.

Maximum number of pings

Select the maximum number of pings.

Seconds between pings

Select the number of seconds to wait between pings.



Results

```
PING 10.1.1.139 (10.1.1.139): 56 data bytes
64 bytes from 10.1.1.139: icmp_seq=0 ttl=64 time=1.148 ms
64 bytes from 10.1.1.139: icmp_seq=1 ttl=64 time=0.665 ms
64 bytes from 10.1.1.139: icmp_seq=2 ttl=64 time=0.628 ms

--- 10.1.1.139 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.628/0.814/1.148/0.237 ms
```

- 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.

The screenshot shows the AWS Launch Wizard interface. In the 'Name and tags' section, the name 'Splunk' is entered. Under 'Application and OS Images (Amazon Machine Image)', the 'Amazon Linux' AMI is selected. The 'Virtual server type' is set to 't2.micro'. The 'Storage (volumes)' option shows '1 volume(s) - 8 GiB'. In the 'Summary' section, the number of instances is set to 1. A large orange 'Launch instance' button is prominently displayed. The bottom of the screen shows standard AWS navigation links like CloudShell and Feedback.

Choose the Amazon Linux Image with free tier

This screenshot continues the AWS Launch Wizard process. In the 'Key pair (login)' section, 'splunk' is chosen as the key pair. The 'Network settings' section is expanded, showing a VPC configuration with 'vpc-044295a73e93a203c (AWS-Lab-VPC)' and '10.1.0.0/16'. A subnet is selected: 'subnet-0b2d2e2fd8b49c318' under 'external-subnet'. The 'Auto-assign public IP' setting is set to 'Enable'. In the 'Summary' section, the instance details are summarized: 1 instance, Amazon Linux 2023 AMI 2023.4.2, t2.micro instance type, and 8 GiB storage. The 'Launch instance' button is visible at the bottom.

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

Subnet - Info

subnet-0b2d2e2fd8b48c318 external-subnet-pfense
VPC: vpc-044295a73e93a203c Owner: 891377068956 Availability Zone: us-east-1a IP addresses available: 249 CIDR: 10.1.2.0/24

Create new subnet

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

Common security groups **Info**
Select security groups Compare security group rules

default sg-0a984f7add25ae81c X
VPC: vpc-044295a73e93a203c

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Advanced network configuration

Configure storage **Info** Advanced

1x 8 GB gp3 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.4.2... read more ami-0c101f26f147fa7fd

Virtual server type (instance type): t2.micro

Firewall (security group): default

Storage (volumes): 1 volume(s) - 8 GiB

Cancel Launch instance Review commands

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

EC2 Dashboard X Auto-assigned IP address

VPC ID: vpc-044295a73e93a203c (AWS-Lab-VPC)

Subnet ID: subnet-0b2d2e2fd8b48c318 (external-subnet)

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role: -

Owner ID: 891377068956

Auto Scaling Group name: -

Instances

Security groups: sg-0a984f7add25ae81c (default)

Launch time: Thu Mar 28 2024 13:43:28 GMT-0400 (Eastern Daylight Time)

Security details

Inbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-044b49c89fc150833	8000	TCP	0.0.0.0/0	default	-
-	sgr-0e165fc085c5afdb2	22	TCP	0.0.0.0/0	default	-

Outbound rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
-	sgr-01fcc41f069fc7e10	All	All	0.0.0.0/0	default	-
-	sgr-054cd854974b192	22	TCP	0.0.0.0/0	default	-

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

Inbound rules [Info](#)

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-044b49c89fc150833	Custom TCP	TCP	8000	Custom	<input type="text"/> 0.0.0.0/0 X
sgr-0e165fc085c5afdb2	SSH	TCP	22	Custom	<input type="text"/> 0.0.0.0/0 X

[Add rule](#)

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Preview changes](#) [Save rules](#)

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

EC2 > Instances > i-068fdbd46b5b628f1 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-068fdbd46b5b628f1 (Splunk) using any of these options

[EC2 Instance Connect](#) [Session Manager](#) [SSH client](#) [EC2 serial console](#)

Instance ID
i-068fdbd46b5b628f1 (Splunk)

Connection Type

Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
54.147.142.154

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

ec2-user [X](#)

ⓘ Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

[Cancel](#) [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.

TURN DATA INTO DOING

Splunk Enterprise 9.2.0.1

Try Splunk Enterprise free for 60 days. No credit card required.

- Keep and manage your data in your on-premises environment with Splunk Enterprise.
- Start searching, analyzing and visualizing your data on powerful, easy-to-understand dashboards.
- Install on Windows or Linux to get insights from all parts of your multicloud and hybrid environment.

Once you sign up for the Splunk Enterprise trial, you'll see how it helps you to:

- ✓ Tackle your hardest security and observability use cases.
- ✓ Stream, collect and index any data at any scale.
- ✓ Set up real-time alerts so you can act fast.
- ✓ Customize for your unique business needs with free, pre-built apps from Splunkbase.
- ✓ Administer your Splunk deployment on-premises or on your own cloud tenant.

Prefer to try Splunk in a cloud environment? Try our [Splunk Cloud](#).

Start Your Free Download

Already have a Splunk account? [Log In](#)

Business Email REQUIRED

Password

First Name

Last Name

Job Title

Phone Number

Company

United States

Zip / Postal Code

I agree to the [Splunk Website Terms & Conditions of Use](#), [Splunk Privacy Policy](#) and [Splunk General Terms](#).

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

Products Solutions Why Splunk? Resources Support

Splunk Enterprise 9.2.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Windows Linux Mac OS

64-bit

3.x+, 4.x+, or 5.4.x kernel Linux distributions

.deb 520.37 MB [Download Now](#)

.tgz 679.42 MB [Download Now](#)

.rpm 679.24 MB [Download Now](#)

[Release Notes](#) | [System Requirements](#) | [Previous Releases](#) | [All Other Downloads](#)

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

The screenshot shows the Splunk website's download page for Splunk Enterprise 9.2.1. A tooltip is displayed over a download link, providing instructions for using wget to download the file. The tooltip text is as follows:

```
USEFUL TOOLS
• Download via Command Line (wget)
  We've got ampersands in the URL, and they're all escaped and ready for wget. This URL won't work in your browser. Click here to select the entire command.
  wget -O splunk-9.2.1-78803f08abb.x86_64.rpm "https://download.splunk.com/products/splunk/releases/9.2.1/linux/splunk-9.2.1-78803f08abb.x86_64.rpm"
```

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

```
aws Services Search [Alt+S] N. Virginia AdministratorAccess/Giovanni-TKH
>Last login: Thu Mar 28 17:56:24 2024 from 19.206.107.29
[ec2-user@ip-10-1-2-237 ~]$ wget -O splunk-9.2.1-78803f08abb.x86_64.rpm "https://download.splunk.com/products/splunk/releases/9.2.1/linux/splunk-9.2.1-78803f08abb.x86_64.rpm"
[ec2-user@ip-10-1-2-237 ~]$
```

i-068fdbd46b5b628f1 (Splunk)
PublicIPs: 54.147.142.154 PrivateIPs: 10.1.2.237

Paste that installation command and let it run.

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

Last login: Thu Mar 28 18:03:00 2024 from 18.206.107.28
[ec2-user@ip-10-1-2-237 ~]$ ls
[ec2-user@ip-10-1-2-237 ~]$ ls
splunk-9.2.1-78803f08aabb.x86_64.rpm
[ec2-user@ip-10-1-2-237 ~]$ sudo yum install ./splunk-9.2.1-78803f08aabb.x86_64.rpm
```

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

```
Complete!
[ec2-user@ip-10-1-2-237 ~]$ sudo bash
```

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

```
Complete!
[ec2-user@ip-10-1-2-237 ~]$ sudo bash
```

Then we will change directories to re

```
Complete!
[ec2-user@ip-10-1-2-237 ~]$ sudo bash
[root@ip-10-1-2-237 ec2-user]# cd /opt/splunk/bin
```

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

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

Last login: Thu Mar 28 18:10:24 2024 from 18.206.107.29
[ec2-user@ip-10-1-2-237 ~]$ sudo bash
[root@ip-10-1-2-237 ec2-user]# cd /opt/splunk/bin
[root@ip-10-1-2-237 bin]# ./splunk start --accept-license --answer-yes

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Please enter the administrator username:
  WARNING: You are about to create using the default 'admin' username.
  Password must contain at least:
    - 8 total printable ASCII character(s).
Please enter a new password:
```

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.

```
Creating: /opt/splunk/var/spool/dimlock
Creating: /opt/splunk/var/spool/dimmoncache
Creating: /opt/splunk/var/lib/splunk/authdb
Creating: /opt/splunk/var/lib/splunk/hashdb
New certs have been generated at '/opt/splunk/etc/cauth'.
    Checking critical directories...          Done
    Checking indexes...
        Validated: audit _configuratir _daopevent _dcclient _dphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
    Done
    Checking filesystem compatibility...     Done
    Checking conf files for problems...
    Done
    Checking default conf files for edits...
    Validating installed files from '"/opt/splunk/splunk-9.2.1-78803f08abb-linux-2.6-x86_64.manifest'
    All installed files intact.
    Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
writing new private key to 'privKeySecure.pem'

Signature ok
subject=/CN=ip-10-1-2-237.ec2.internal/O=SplunkUser
Getting CA Private Key
writing RSA key
WTRONWHTFFSVERIFTF is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
E
Done
[ OK ]
Waiting for web server at http://127.0.0.1:8000 to be available..... Done

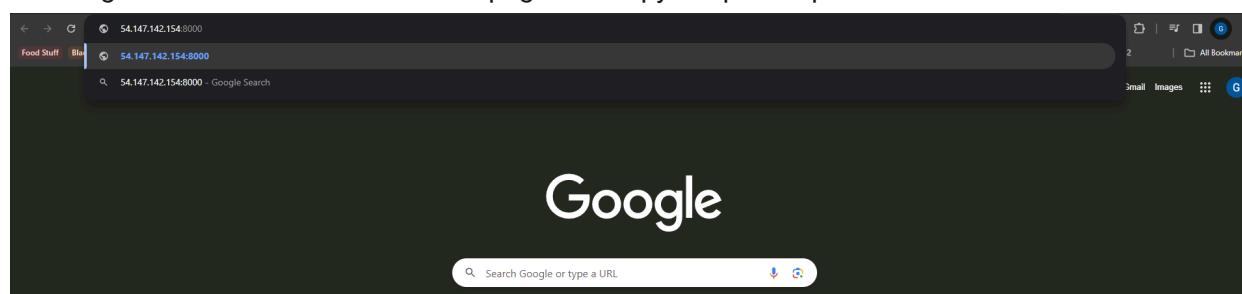
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://ip-10-1-2-237.ec2.internal:8000
root@ip-10-1-2-237 bin]$
```

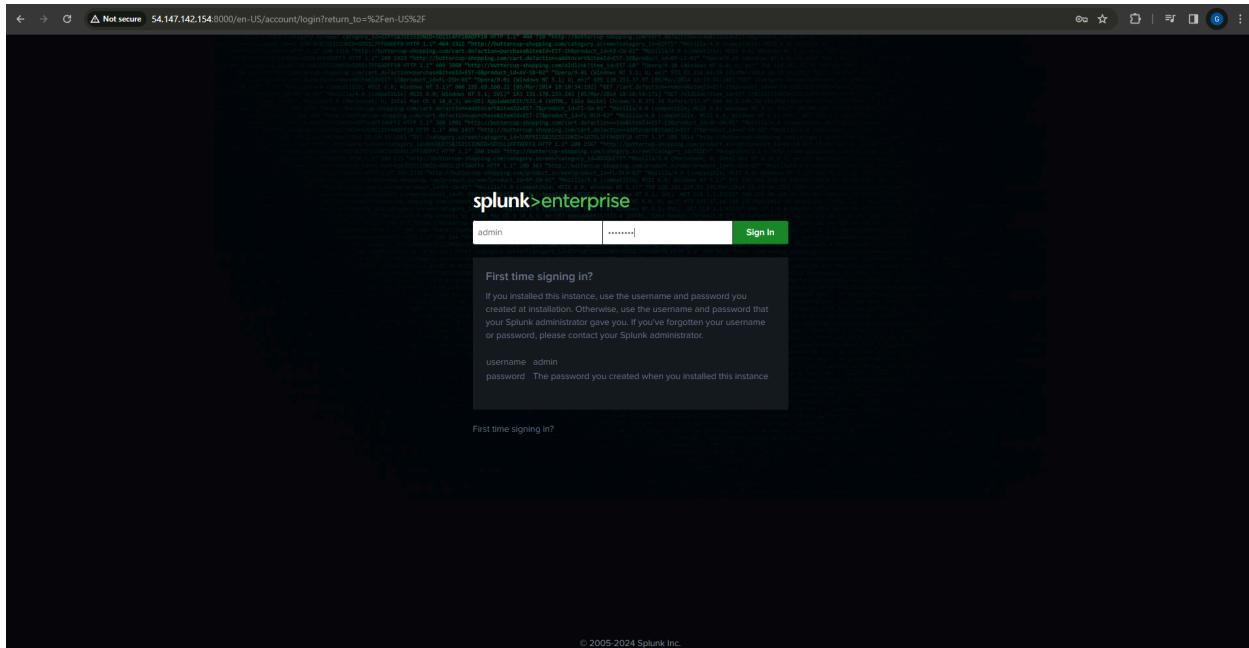
This is the end message and result

The screenshot shows the AWS EC2 Instances page. The instance summary for 'i-068fdbd46b5b628f1' is displayed, indicating it is running with a public IP of 54.147.142.154. The instance type is t2.micro, and it is associated with a VPC ID (vpc-044295a73e93a203c) and a subnet ID (subnet-0b2d2e2fd8b48c318). The instance has an Auto-assigned IP address (54.147.142.154 [Public IP]). The instance summary includes sections for Public IPv4 address copied, Private IPv4 addresses (10.1.2.237), and Private IPv4 DNS (10.1.2.237). The instance details tab is selected, showing the instance's AMI ID (ami-0c101f26f147fa7fd), AMI name (al2023-ami-2023.4.20240319.1-kernel-6.1-x86_64), and launch time (Thu Mar 28 2024 13:53:26 GMT-0400 (Eastern Daylight Time)). The instance also has a lifecycle status of normal.

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.

The dashboard includes a sidebar with 'Apps' management, a search bar, and links for 'Search & Reporting', 'Splunk Secure Gateway', 'Upgrade Readiness App', and 'Find more apps'.

Now we have access to Splunk!