

## **Create VPC Infrastructure (Task 1)**



**Zaeem Attique Ashar**

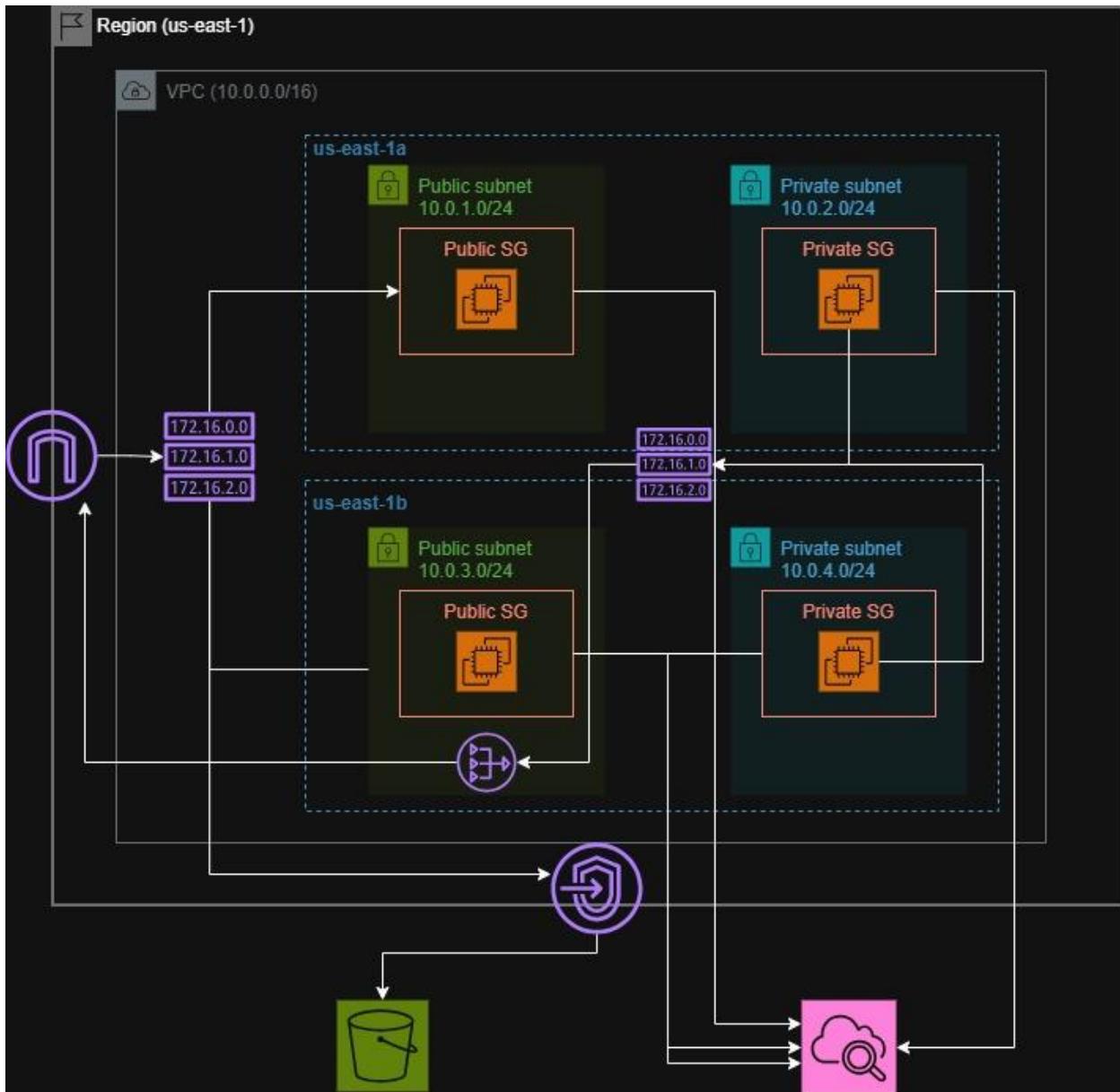
**Cloud Intern**

### **Task Description:**

Create a custom Virtual Private Cloud (VPC) setup to host secure and scalable AWS resources across public and private subnets with proper routing, NAT, and security configurations. Also enable VPC Flow Logs for network traffic monitoring and store them in S3 Bucket as well by creating VPC Endpoint.

Architecture Diagram: .....	3
Task 0.1: Create a custom VPC with a specified CIDR block .....	4
Task 0.2: Define public and private subnets across multiple Availability Zones.....	4
Task 0.3: Set up an Internet Gateway and attach it to the VPC. ....	5
Task 0.4: Create route tables and associate them with appropriate subnets. ....	5
Task 0.5: Configure NAT Gateway in a public subnet for private subnet internet access. ....	7
Task 0.6: Launch EC2 instances in private and public subnets as needed .....	8
Task 0.7: Implement security groups and network ACLs for traffic control.....	11
Task 0.8: Enable VPC Flow Logs for network traffic monitoring .....	12
Task 0.9: Create VPC Endpoints for secure private connectivity to AWS services .....	13
Task 0.10: Use Elastic IPs for NAT Gateway or public-facing resources.....	14
Task 0.11: Test connectivity between subnets and to the internet .....	15

## Architecture Diagram:



## Task 0.1: Create a custom VPC with a specified CIDR block

- Go to the VPC Dashboard and select the Create VPC button.
- Configuration:
  - Resources to create: VPC only
  - Name tag: Task0VPC
  - IPv4 CIDR block: IPv4 CIDR manual input
  - IPv4 CIDR: 10.0.0.0/16
  - IPv6 CIDR block: No IPv6 CIDR block
  - Tenancy: Default
- Click on create VPC.

The screenshot shows the AWS VPC Dashboard. At the top, there's a search bar with 'Find VPCs by attribute or tag' and a filter button 'Clear filters'. Below that is a table titled 'Your VPCs (1/1)'. The table has columns: Name, VPC ID, State, Block Public Access, IPv4 CIDR, and IPv6 CIDR. A single row is selected for 'Task0VPC' with VPC ID 'vpc-03aab790ff86195eb', State 'Available', Block Public Access 'Off', IPv4 CIDR '10.0.0.0/16', and IPv6 CIDR '-'. Above the table, it says 'Last updated 1 minute ago' and has 'Actions' and 'Create VPC' buttons. Below the table, there's a detailed view for 'vpc-03aab790ff86195eb / Task0VPC'. It has tabs for 'Details' and 'Subnets'. The 'Details' tab shows various configuration settings:

VPC ID	State	Block Public Access	DNS hostnames
vpc-03aab790ff86195eb	Available	Off	Disabled
DNS resolution	Tenancy	DHCP option set	Main route table
Enabled	default	dopt-014d84d6309c97046	rtb-03e6821e0603341b3
Main network ACL	Default VPC	IPv4 CIDR	IPv6 pool
acl-0d63c38fe8f52b675	No	10.0.0.0/16	-
IPv6 CIDR (Network border group)	Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID
-	Disabled	-	880958245574

## Task 0.2: Define public and private subnets across multiple Availability Zones

- Go to the subnets tab in the VPC dashboard.
- Click on create subnets button and select the VPC created in the last step.
- Create subnet with the following config:
  - Name: Task0-pub-1a, Zone: us-east-1a, CIDR Block: 10.0.1.0/24
  - Name: Task0-priv-1a, Zone: us-east-1a, CIDR Block: 10.0.2.0/24
  - Name: Task0-pub-1b, Zone: us-east-1b, CIDR Block: 10.0.3.0/24
  - Name: Task0-priv-1b, Zone: us-east-1b, CIDR Block: 10.0.4.0/24

Subnets (4) <small>Info</small>						
<span>Last updated 1 minute ago</span> <span>Actions ▾</span> <span>Create subnet</span>						
<input type="text"/> Find subnets by attribute or tag						
<input type="button"/> Subnet ID : subnet-0abb6619e9f22d8e7 <span>X</span> <input type="button"/> Subnet ID : subnet-0a9664e0e2e3d746c <span>X</span> <input type="button"/> Subnet ID : subnet-09c710bbff34ae0bc <span>X</span> <input type="button"/> Show more (+1)						
<span>Clear filters</span>						
<input type="checkbox"/> Name <span>▼</span> <span>Subnet ID</span> <span>▼</span> <span>State</span> <span>▼</span> <span>VPC</span> <span>▼</span> <span>Block Public...</span> <span>▼</span> <span>IPv4 CIDR</span>						
<input type="checkbox"/> Task0-private-sn-1a <span>subnet-0a9664e0e2e3d746c</span> <span>Available</span> <span>vpc-03aab790ff86195eb   Task...</span> <span>Off</span> <span>10.0.2.0/24</span>						
<input type="checkbox"/> Task0-private-sn-1b <span>subnet-09124e18a3f5c5a9b</span> <span>Available</span> <span>vpc-03aab790ff86195eb   Task...</span> <span>Off</span> <span>10.0.4.0/24</span>						
<input type="checkbox"/> Task0-public-sn-1a <span>subnet-0abb6619e9f22d8e7</span> <span>Available</span> <span>vpc-03aab790ff86195eb   Task...</span> <span>Off</span> <span>10.0.1.0/24</span>						
<input type="checkbox"/> Task0-public-sn-1b <span>subnet-09c710bbff34ae0bc</span> <span>Available</span> <span>vpc-03aab790ff86195eb   Task...</span> <span>Off</span> <span>10.0.3.0/24</span>						

## Task 0.3: Set up an Internet Gateway and attach it to the VPC.

- Go to the Internet Gateways tab in the VPC Dashboard.
- Use the Create VPC button.
- Name your VPC and click Create.
- Now click on the Actions button and choose to attach VPC.
- Select the VPC previously created for the task and click on the attach IGW button.

igw-05d011edb29557134 / Task0-igw										
<span>Actions ▾</span>										
<span>Details <small>Info</small></span>										
Internet gateway ID <span>igw-05d011edb29557134</span>	State <span>Attached</span>	VPC ID <span>vpc-03aab790ff86195eb   Task0VPC</span>	Owner <span>880958245574</span>							
<b>Tags (1)</b>										
<span>Search tags</span> <table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>Task0-igw</td> </tr> </tbody> </table>							Key	Value	Name	Task0-igw
Key	Value									
Name	Task0-igw									
<span>Manage tags</span>										

## Task 0.4: Create route tables and associate them with appropriate subnets.

- Go to route tables tab on the VPC Dashboard.
- Click on create route table and name the public route table.
- Select the VPC created for this task.
- Hit create route table.
- Repeat above steps to create a private route table.
- Now associate the public RT with the public subnet and private RT with private subnets.

**Route tables (1/3) Info**

Last updated 1 minute ago Actions Create route table

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
Task0-public-rt	rtb-01d2102b6c7e69894	2 subnets	-	No	vpc-03aab790ff86195eb   Task0
<b>Task0-private-rt</b>	<b>rtb-0025f22ff12bf885e</b>	<b>2 subnets</b>	-	No	vpc-03aab790ff86195eb   Task0

**rtb-0025f22ff12bf885e / Task0-private-rt**

Details Routes **Subnet associations** Edge associations Route propagation Tags

**Explicit subnet associations (2)**

Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Task0-private-sn-1a	subnet-0a9664e0e2e3d746c	10.0.2.0/24	-
Task0-private-sn-1b	subnet-09124e18a3f5c5a9b	10.0.4.0/24	-

**Route tables (1/3) Info**

Last updated 2 minutes ago Actions Create route table

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
<b>Task0-public-rt</b>	<b>rtb-01d2102b6c7e69894</b>	<b>2 subnets</b>	-	No	vpc-03aab790ff86195eb   Task0
Task0-private-rt	rtb-0025f22ff12bf885e	2 subnets	-	No	vpc-03aab790ff86195eb   Task0

**rtb-01d2102b6c7e69894 / Task0-public-rt**

Details Routes **Subnet associations** Edge associations Route propagation Tags

**Explicit subnet associations (2)**

Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Task0-public-sn-1a	subnet-0abb6619e9f22d8e7	10.0.1.0/24	-
Task0-public-sn-1b	subnet-09c710bbff34ae0bc	10.0.3.0/24	-

- Go to the public route table and create the following route(s)
  - Instance to IGW:
    - Destination: 0.0.0.0/0
    - Target: igw

**Routes (2)**

Both Edit routes

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-05d011edb29557134	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

- Go to the private route table and create the following route
  - Instance to NGW:
    - Destination: 0.0.0.0/0

- Target: NGW

rtb-0025f22ff12bf885e / Task0-private-rt

**Details**

Route table ID: rtb-0025f22ff12bf885e  
Main  
Owner ID: 880958245574  
VPC: vpc-03aab790ff86195eb | Task0VPC

**Explicit subnet associations:** 2 subnets

**Edge associations:** —

**Routes (2)**

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	nat-0355a10596289fa40	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Both < 1 > Edit routes

## Task 0.5: Configure NAT Gateway in a public subnet for private subnet internet access.

- Go to the NAT Gateway tab in the VPC Dashboard.
- Click on create NAT Gateway, set a name for the NAT Gateway.
- Select the public subnet Task0-public-sn-1a.
- Click on the allocate elastic IP button and then create the NAT Gateway.

nat-0c4e6a4a7858b9868 / Task0-ngw-1a

**Details**

NAT gateway ID: nat-0c4e6a4a7858b9868  
NAT gateway ARN: arn:aws:ec2:us-east-1:880958245574:natgateway/nat-0c4e6a4a7858b9868  
VPC: vpc-03aab790ff86195eb / Task0VPC

Connectivity type: Public  
Primary public IPv4 address: —  
Subnet: subnet-0abb6619e9f22d8e7 / Task0-public-sn-1a

**State:** Pending  
**Primary private IPv4 address:** 10.0.1.121  
**Created:** Wednesday, November 5, 2025 at 19:24:08 GMT+5

**State message:** Info  
**Primary network interface ID:** eni-05d6e2003a7eb66c9 ↗  
**Deleted:** —

**Secondary IPv4 addresses**

Private IPv4 address	Network interface ID	Status	Failure message
----------------------	----------------------	--------	-----------------

Secondary IPv4 addresses are not available for this nat gateway.

Edit secondary IPv4 address associations

- Follow the same steps to create another NAT Gateway in the Task0-private-sn-1b.

**nat-0335a10596289fa40 / Task0-ngw-1a**

**Details**

NAT gateway ID <a href="#">nat-0335a10596289fa40</a>	Connectivity type Public	State <a href="#">Pending</a>	State message -
NAT gateway ARN <a href="#">arn:aws:ec2:us-east-1:880958245574:natgateway/nat-0335a10596289fa40</a>	Primary public IPv4 address -	Primary private IPv4 address -	Info Primary network interface ID -
VPC <a href="#">vpc-03aab790ff86195eb / Task0VPC</a>	Subnet subnet-09c710bbff34ae0bc / Task0-public-sn-1b	Created <a href="#">Wednesday, November 5, 2025 at 19:27:38 GMT+5</a>	Deleted -

**Secondary IPv4 addresses** | Monitoring | Tags

**Secondary IPv4 addresses**

Search

Private IPv4 address	Network interface ID	Status
Secondary IPv4 addresses are not available for this nat gateway.		

Edit secondary IPv4 address associations

## Task 0.6: Launch EC2 instances in private and public subnets as needed

- Go to the EC2 Dashboard and click on the launch instance button.
- Configure the Public instance 1 as follows:
  - Name: Task0-public-1a
  - AMI: Amazon Linux 2023 (x86)
  - Instance type: t3.micro
  - Keypair: Proceed without key pair
  - VPC: Task0VPC
  - Subnet: Task0-private-sn-1a
  - Auto-assign public IP: Enabled
  - Create security group, rule: Type=HTTP, Source Type=Anywhere
  - Storage: 8GiB, gp3
  - Connect via SSH and run command `sudo dnf install nginx`

**Instance summary for i-0dbb28dee54c1b9ae (Task0-Public-1a)** [Info](#)

Updated 10 minutes ago

Instance ID <a href="#">i-0dbb28dee54c1b9ae</a>	Public IPv4 address <a href="#">3.95.165.154   open address ↗</a>	Private IPv4 addresses <a href="#">10.0.1.62</a>
IPv6 address -	Instance state <a href="#">Running</a>	Public DNS -
Hostname type IP name: ip-10-0-1-62.ec2.internal	Private IP DNS name (IPv4 only) <a href="#">ip-10-0-1-62.ec2.internal</a>	Elastic IP addresses -
Answer private resource DNS name -	Instance type t3.micro	AWS Compute Optimizer finding <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   Learn more ↗
Auto-assigned IP address <a href="#">3.95.165.154 [Public IP]</a>	VPC ID <a href="#">vpc-03aab790ff86195eb (Task0VPC) ↗</a>	Auto Scaling Group name -
IAM Role -	Subnet ID <a href="#">subnet-0abb6619e9f22d8e7 (Task0-public-sn-1a) ↗</a>	Managed false
IMDSv2 Required	Instance ARN <a href="#">arn:aws:ec2:us-east-1:880958245574:instance/i-0dbb28dee54c1b9ae</a>	
Operator -		

- Configure the Public instance 2 as follows:
  - Name: Task0-public-1b
  - AMI: Amazon Linux 2023 (x86)
  - Instance type: t3.micro
  - Keypair: Proceed without key pair
  - VPC: Task0VPC
  - Subnet: Task0-private-sn-1b
  - Auto-assign public IP: Enabled
  - Create security group, rule: Type=HTTP, Source Type=Anywhere
  - Storage: 8GiB, gp3
  - Connect via SSH and run command `sudo dnf install nginx`

Instance summary for i-01a81a23b5d1572ad (Task0-public-1b) <a href="#">Info</a>		Actions	
Updated less than a minute ago		<a href="#">C</a> <a href="#">Connect</a> <a href="#">Instance state ▾</a> <a href="#">Actions ▾</a>	
Instance ID	i-01a81a23b5d1572ad	Public IPv4 address	<a href="#">54.226.58.189</a>   <a href="#">open address ↗</a>
IPv6 address	-	Instance state	<a href="#">Running</a>
Hostname type	IP name: ip-10-0-3-181.ec2.internal	Private IP DNS name (IPv4 only)	<a href="#">ip-10-0-3-181.ec2.internal</a>
Answer private resource DNS name	-	Instance type	t3.micro
Auto-assigned IP address	<a href="#">54.226.58.189 [Public IP]</a>	VPC ID	<a href="#">vpc-03aab790ff86195eb (Task0VPC)</a> ↗
IAM Role	-	Subnet ID	<a href="#">subnet-09c710bbff34ae0bc (Task0-public-sn-1b)</a> ↗
IMDSv2	Required	Instance ARN	<a href="#">arn:aws:ec2:us-east-1:880958245574:instance/i-01a81a23b5d1572ad</a>
Operator	-	AWS Compute Optimizer finding	<a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   <a href="#">Learn more ↗</a>
		Auto Scaling Group name	-
		Managed	false

- Configure the Private instance 1 as follows:
  - Name: Task0-private-1a
  - AMI: Amazon Linux 2023 (x86)
  - Instance type: t3.micro
  - Keypair: Proceed without key pair
  - VPC: Task0VPC
  - Subnet: Task0-private-sn-1a
  - Auto-assign public IP: Enabled
  - Create security group, rule: Type=HTTP, Source Type=Anywhere
  - Attach Role: ssmManagedInstanceIdCore
  - Storage: 8GiB, gp3

Instance summary for i-0fff2951751421d35 (Task0-private-1a) <a href="#">Info</a>		
Updated 2 minutes ago		
<b>Instance ID</b> i-0fff2951751421d35	<b>Public IPv4 address</b> -	<b>Private IPv4 addresses</b> 10.0.2.109
<b>IPv6 address</b> -	<b>Instance state</b> Running	<b>Public DNS</b> -
<b>Hostname type</b> IP name: ip-10-0-2-109.ec2.internal	<b>Private IP DNS name (IPv4 only)</b> ip-10-0-2-109.ec2.internal	<b>Elastic IP addresses</b> -
<b>Answer private resource DNS name</b> -	<b>Instance type</b> t3.micro	<b>AWS Compute Optimizer finding</b> Opt-in to AWS Compute Optimizer for recommendations. <a href="#">  Learn more</a> ▾
<b>Auto-assigned IP address</b> -	<b>VPC ID</b> vpc-03aab790ff86195eb (Task0VPC) ▾	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> role-for-ssm-instance-core ▾	<b>Subnet ID</b> subnet-0a9664e0e2e3d746c (Task0-private-sn-1a) ▾	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> arn:aws:ec2:us-east-1:880958245574:instance/i-0fff2951751421d35	
<b>Operator</b> -		

- Configure the Private instance 2 as follows:
  - Name: Task0-private-1b
  - AMI: Amazon Linux 2023 (x86)
  - Instance type: t3.micro
  - Keypair: Proceed without key pair
  - VPC: Task0VPC
  - Subnet: Task0-private-sn-1b
  - Auto-assign public IP: Enabled
  - Attach Role: ssmManagedInstanceIdCore
  - Create security group, rule: Type=HTTP, Source Type=Anywhere
  - Storage: 8GiB, gp3

Instance summary for i-02734a617f23182e7 (Task0-private-1b) <a href="#">Info</a>		
Updated less than a minute ago		
<b>Instance ID</b> i-02734a617f23182e7	<b>Public IPv4 address</b> -	<b>Private IPv4 addresses</b> 10.0.4.77
<b>IPv6 address</b> -	<b>Instance state</b> Running	<b>Public DNS</b> -
<b>Hostname type</b> IP name: ip-10-0-4-77.ec2.internal	<b>Private IP DNS name (IPv4 only)</b> ip-10-0-4-77.ec2.internal	<b>Elastic IP addresses</b> -
<b>Answer private resource DNS name</b> -	<b>Instance type</b> t3.micro	<b>AWS Compute Optimizer finding</b> Opt-in to AWS Compute Optimizer for recommendations. <a href="#">  Learn more</a> ▾
<b>Auto-assigned IP address</b> -	<b>VPC ID</b> vpc-03aab790ff86195eb (Task0VPC) ▾	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> role-for-ssm-instance-core ▾	<b>Subnet ID</b> subnet-09124e18a3f5c5a9b (Task0-private-sn-1b) ▾	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> arn:aws:ec2:us-east-1:880958245574:instance/i-02734a617f23182e7	
<b>Operator</b> -		

## Task 0.7: Implement security groups and network ACLs for traffic control

Security Group for public instance in SN 1a:

- In the EC2 Dashboard, go to the security groups tab.
- Click on the create security group button.
- Give the new SG a name, Select the VPC: Task0VPC
- Now create the following inbound rules.
  - Type: HTTP, Source: 0.0.0.0/0 (Hosting Web Server)
  - Type: HTTPS, Source: 0.0.0.0/0 (Secure connection to the webserver)
  - Type: ICMP, Source: 0.0.0.0/0 (Test traffic like ping)
  - Type: SSH, Source: 0.0.0.0/0 (Connecting to the machine via SSH)

Create the same SG for the public instance in SN 1b.

The screenshot shows the AWS Security Groups console for a security group named "sg-0ef892bb8957b3146 - launch-wizard-4". The "Details" section includes fields for Security group name (sg-0ef892bb8957b3146), Security group ID (sg-0ef892bb8957b3146), Description (created 2025-11-05T15:28:52.561Z), VPC ID (vpc-03aab790ff86195eb), Owner (880958245574), Inbound rules count (4 Permission entries), and Outbound rules count (1 Permission entry). Below the details, there are tabs for Inbound rules, Outbound rules, Sharing - new, VPC associations - new, and Tags. The Inbound rules table shows four entries:

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-0161d9e8e0d0252be	IPv4	HTTP	TCP	80
-	sgr-01a9de096a057c946	IPv4	HTTPS	TCP	443
-	sgr-0659b9fb214ae49d	IPv4	All ICMP - IPv4	ICMP	All
-	sgr-00436f9f212befeb2	IPv4	SSH	TCP	22

Security Group for private instance in SN 1a:

- In the EC2 Dashboard, go to the security groups tab.
- Click on the create security group button.
- Give the new SG a name, Select the VPC: Task0VPC
- Now create the following inbound rules.
  - Type: HTTP, Source: 0.0.0.0/0 (for connecting via SSM)
  - Type: All Traffic, Destination: 0.0.0.0/0 (sending traffic to NGW)

Create the same SG for the private instance in SN 1b

**sg-01822ec0b0fbcbdb8 - launch-wizard-6**

**Details**

Security group name <a href="#">launch-wizard-6</a>	Security group ID <a href="#">sg-01822ec0b0fbcbdb8</a>	Description <a href="#">launch-wizard-6 created 2025-11-05T16:00:52.288Z</a>	VPC ID <a href="#">vpc-03aab790ff86195eb</a>
Owner <a href="#">880958245574</a>	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

**Inbound rules**   **Outbound rules**   **Sharing - new**   **VPC associations - new**   **Tags**

**Inbound rules (2)**

<input type="checkbox"/> Name	Security group rule ID	IP version	Type	Protocol	Port range
<input type="checkbox"/> -	sgr-0e281a5dad4cb731d	IPv4	HTTP	TCP	80
<input type="checkbox"/> -	sgr-0cbbcd11143d36e6	IPv4	SSH	TCP	22

## Task 0.8: Enable VPC Flow Logs for network traffic monitoring

- Go to CloudWatch Dashboard
- Go to logs -> log groups tab.
- Create a new log group, give it the name Task0-VPC-Flow.
- Now go to the VPC Dashboard and open your VPC tab.
- Select VPC Task0VPC from the list.
- Now use the action dropdown and select create flow log.
- Using the following configurations:
  - Name: Task0-FlowLogs
  - Filter: all
  - Maximum aggregation interval: 10 min
  - Destination: Save to CW Logs
  - Destination log group: Task0-VPC-Flow
  - Service access: Create and use a new service role
  - Log record format: AWS default format
- Click on the create Flow Log button.

**Details**

Flow Log ID fl-0df8854182cce9574	Destination Type cloud-watch-logs	Traffic Type All	File Format -
Name Task0-FlowLogs	Destination Name Task0-VPC-Flow	Max Aggregation Interval 10 minutes	Hive Compatible Partitions -
State Active	IAM Role arn:aws:iam::880958245574:role/service-role/VPCFlowLogs-Cloudwatch-1762362047093	Log Format Default	Partition Logs -
Creation Time Wednesday, November 5, 2025 at 22:06:21 GMT+5	Cross Account IAM Role -		

**Tags**

Key	Value
Name	Task0-FlowLogs

**Integrations**

## Task 0.9: Create VPC Endpoints for secure private connectivity to AWS services

- Create an S3 bucket for demonstration purposes.
- Go to the VPC Dashboard and open the Endpoints tab.
- Following is the configuration:
  - Name: task0-s3-endpoint
  - Type: AWS Services
  - Service Name: com.amazonaws.us-east-1.s3 (Gateway)
  - VPC: Task0VPC
  - Route Table: Task0-rt-public
  - Policy: Full Access

**Endpoints (1/1) Info**

Find endpoints by attribute or tag		Actions		Create endpoint	
VPC endpoint ID	vpce-0bfd77689a5867114	Clear filters			
<input checked="" type="checkbox"/> Name	task0-s3-endpoint	<input checked="" type="checkbox"/> VPC endpoint ID	vpce-0bfd77689a5867114	<input checked="" type="checkbox"/> Endpoint type	Gateway
<input checked="" type="checkbox"/> Status	Available	<input checked="" type="checkbox"/> Service name	com.amazonaws.us-east-1.s3		

**vpce-0bfd77689a5867114 / task0-s3-endpoint**

**Details**

Endpoint ID vpce-0bfd77689a5867114	Status Available	Creation time Thursday, November 6, 2025 at 00:15:02 GMT+5	Endpoint type Gateway
VPC ID vpc-03aab790ff86195eb (Task0VPC)	Status message -	Service name com.amazonaws.us-east-1.s3	Private DNS names enabled No
DNS record IP type service-defined	IP address type ipv4	Service region us-east-1	

## Task 0.10: Use Elastic IPs for NAT Gateway or public-facing resources

- While creating the NGW, use the allocate elastic IP button to auto-assign EIP.

The screenshot shows the AWS Elastic IP addresses dashboard. At the top, there is a search bar with the placeholder "Find elastic IP addresses by attribute or tag" and a button labeled "Allocate Elastic IP address". Below the search bar is a table with the following columns: Name, Allocated IPv4 addr..., Type, Allocation ID, Reverse DNS record, and Assoc. There is one row in the table with the values: Name - 34.204.216.110, Allocated IPv4 address - 34.204.216.110, Type - Public IP, Allocation ID - eipalloc-0ec8a00cce80f29c6, Reverse DNS record - -, and Assoc - -. Below the table, the IP address 34.204.216.110 is selected, and its detailed summary is displayed. The summary includes fields such as Allocated IPv4 address (34.204.216.110), Association ID (eipassoc-0bd4151767d363ebf), Network interface ID (eni-044fb2c0e450c3f04), Address pool (Amazon), Type (Public IP), Scope (VPC), Network interface owner account ID (880958245574), Network border group (us-east-1), Allocation ID (eipalloc-0ec8a00cce80f29c6), Associated instance ID (-), Public DNS (-), Service managed (-), Reverse DNS record (-), Private IP address (10.0.3.28), and NAT Gateway ID (nat-0335a10596289fa40 (Task0-ngw-1b)).

- Now go to the VPC Dashboard and go to the Elastic IP tab.
- Select the allocate elastic IP button. Continue with the following configuration.
  - Amazon's pool of IPv4 addresses
  - Network Border Group: us-east-1.
- Then create the EIP.
- From the EIP dashboard, go to actions and attach the EIP to a public facing EC2 Instance () .

The screenshot shows the AWS Elastic IP details page for the IP address 44.221.133.223. At the top, there is a "Actions" dropdown and a "Associate Elastic IP address" button. Below the header, the "Summary" section displays the following information:

- Allocated IPv4 address: 44.221.133.223
- Association ID: eipassoc-0a20fd2f973f2529a
- Network interface ID: eni-0a17fbcde5e31d0650
- Address pool: Amazon
- Type: Public IP
- Scope: VPC
- Network interface owner account ID: 880958245574
- Network border group: us-east-1
- Allocation ID: eipalloc-0c4311eb77d4696ff
- Associated instance ID: i-0dbb28dee54c1b9ae
- Public DNS: -
- Service managed: -
- Reverse DNS record: -
- Private IP address: 10.0.1.62
- NAT Gateway ID: -

The "Tags(0)" section indicates that no tags are associated with this resource. A "Manage tags" button is available to add tags.

- Follow the same steps to allocate and attach the EIP to the other public facing EC2 instance.

Summary		Actions	
Allocated IPv4 address	<input type="checkbox"/> 98.90.117.196	Type	<input type="checkbox"/> Public IP
Association ID	<input type="checkbox"/> eipassoc-09a664d89fb6da4d9	Scope	<input type="checkbox"/> VPC
Network interface ID	<a href="#">eni-026e62af3a9450e06</a>	Network interface owner account ID	<input type="checkbox"/> 880958245574
Address pool	<input type="checkbox"/> Amazon	Network border group	<input type="checkbox"/> us-east-1
		Allocation ID	<input type="checkbox"/> eipalloc-0a6f18d3f31dbe89f
		Associated instance ID	<input type="checkbox"/> i-01a81a23b5d1572ad
		Public DNS	-
		Service managed	-
		Reverse DNS record	-
		Private IP address	<input type="checkbox"/> 10.0.3.181
		NAT Gateway ID	-

We can now access the NGINX webserver on the EIP.

## Task 0.11: Test connectivity between subnets and to the internet

- Connect to public EC2 instance using SSH from UI.
  - Ping [www.google.com](http://www.google.com) to check internet connectivity via IGW.

- Enter the EIP of public machine to test if HTTP traffic flows via IGW and is allowed by the SG:



The same can be done with the other public EC2 instance to check connectivity.

- Connect to the private EC2 instance using the Session Manager via NGW
- Use the ping command to check if the traffic is flowing through the NGW.

Session ID: Zaeem-6i5azgyj4ltit8fbllp6lq85h8      Instance ID: i-02734a617f23182e7

```
sh-5.2$ ping www.google.com
PING www.google.com (142.250.31.104) 56(84) bytes of data.
64 bytes from bj-in-f104.1e100.net (142.250.31.104): icmp_seq=1 ttl=105 time=2.38 ms
64 bytes from bj-in-f104.1e100.net (142.250.31.104): icmp_seq=2 ttl=105 time=1.57 ms
64 bytes from bj-in-f104.1e100.net (142.250.31.104): icmp_seq=3 ttl=105 time=1.54 ms
64 bytes from bj-in-f104.1e100.net (142.250.31.104): icmp_seq=4 ttl=105 time=1.60 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.544/1.772/2.377/0.349 ms
sh-5.2$
```

- To check the flow logs, head over to the CloudWatch Dashboard.
- Click on logs and then open the logs group tab.
- Select an interface to check the logs, and they will be displayed.

Timestamp	Message
2025-11-05T19:29:41.000Z	2 880958245574 eni-020533cec14bf85e4 13.217.79.194 10.0.2.109 443 53246 6 19 7098 1762370981 1762370997 ACCEPT OK
2025-11-05T19:29:41.000Z	2 880958245574 eni-020533cec14bf85e4 10.0.2.109 13.217.79.194 53246 443 6 13 3722 1762370981 1762370997 ACCEPT OK
2025-11-05T19:30:46.000Z	2 880958245574 eni-020533cec14bf85e4 10.0.2.109 52.207.222.58 40806 123 17 1 76 1762371046 1762371063 ACCEPT OK
2025-11-05T19:30:46.000Z	2 880958245574 eni-020533cec14bf85e4 52.207.222.58 10.0.2.109 123 40806 17 1 76 1762371046 1762371063 ACCEPT OK
2025-11-05T19:30:46.000Z	2 880958245574 eni-020533cec14bf85e4 10.0.2.109 98.87.174.74 97 56138 443 6 349 1762371046 1762371063 ACCEPT OK
2025-11-05T19:30:46.000Z	2 880958245574 eni-020533cec14bf85e4 98.87.174.74 10.0.2.109 443 56138 6 5 293 1762371046 1762371063 ACCEPT OK
2025-11-05T19:30:46.000Z	2 880958245574 eni-020533cec14bf85e4 10.0.2.109 13.217.79.194 53246 443 6 3 180 1762371046 1762371063 ACCEPT OK
2025-11-05T19:30:46.000Z	2 880958245574 eni-020533cec14bf85e4 13.217.79.194 10.0.2.109 443 53246 6 5 284 1762371046 1762371063 ACCEPT OK
2025-11-05T19:31:02.000Z	2 880958245574 eni-020533cec14bf85e4 1762371063 - NO DATA
2025-11-05T19:31:42.000Z	2 880958245574 eni-020533cec14bf85e4 3.94.91.31 10.0.2.109 123 59812 17 1 76 1762371103 1762371103 ACCEPT OK
2025-11-05T19:31:42.000Z	2 880958245574 eni-020533cec14bf85e4 10.0.2.109 3.94.91.31 10.0.2.109 123 17 1 76 1762371102 1762371103 ACCEPT OK