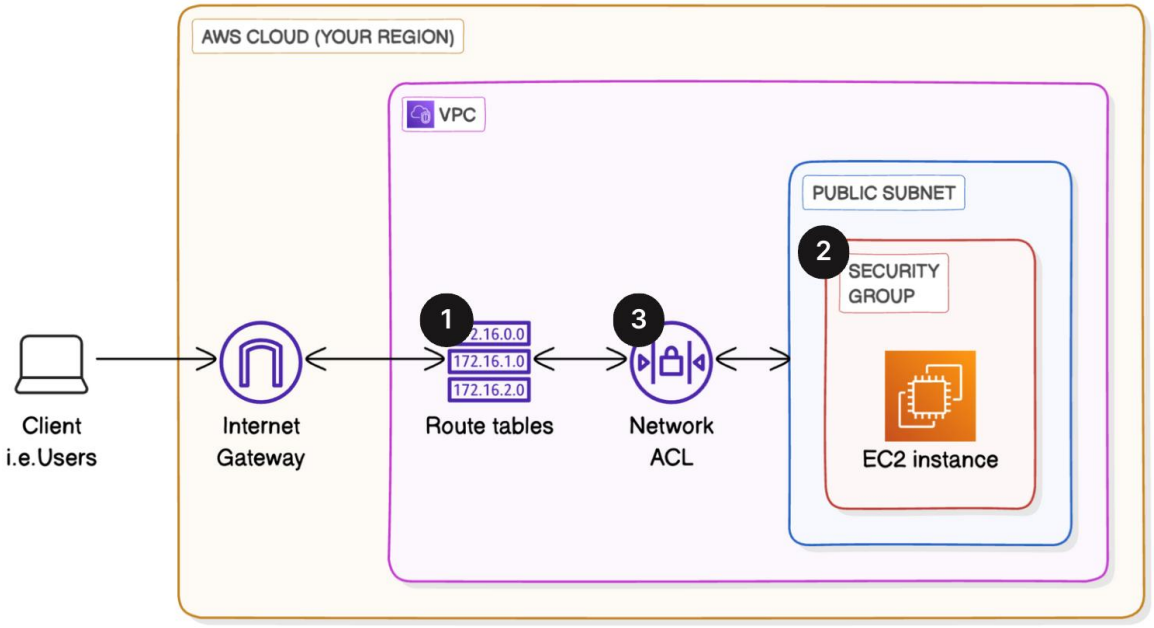
VPC Traffic Flow and Security - Step-by-Step Documentation



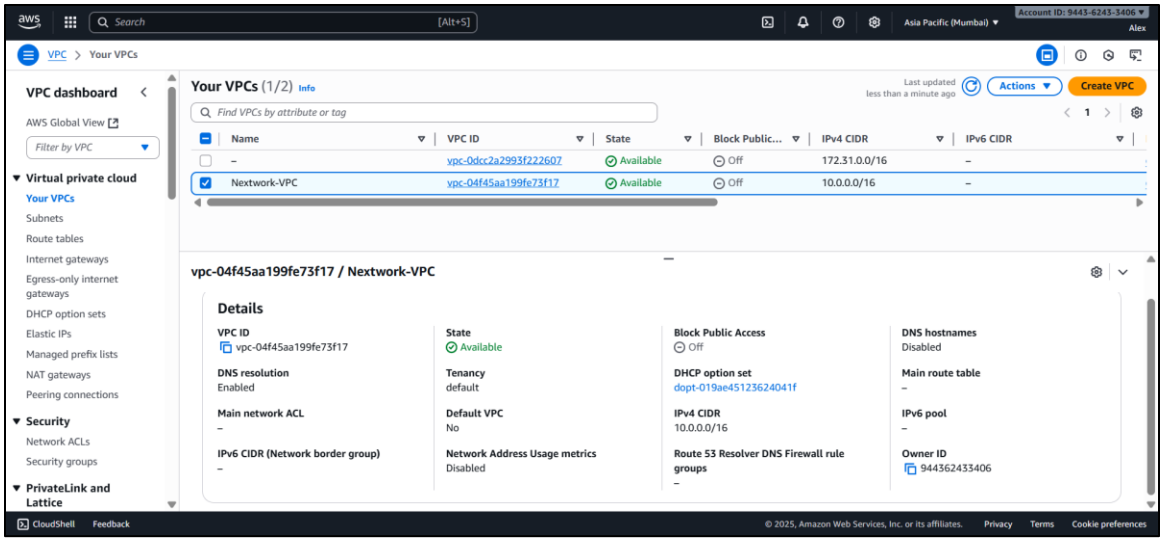
This documentation provides a comprehensive, step-by-step process for setting up and securing an Amazon VPC. It builds on the earlier project 'Build a Virtual Private Cloud' and includes both the foundational steps and the new steps for configuring traffic flow and security.

Step 1: Create a VPC

Set up a new Virtual Private Cloud in AWS.

Actions:

- - Log in to AWS Management Console.
- - Search for 'VPC' in the search bar and select it.
- - In the left-hand navigation pane, choose 'Your VPCs'.
- - Click 'Create VPC'.
- - Select 'VPC only' option.
- - Enter a Name tag (e.g., NextWork VPC).
- - Enter an IPv4 CIDR block (e.g., 10.0.0.0/16).
- - Click 'Create VPC' to finalize.

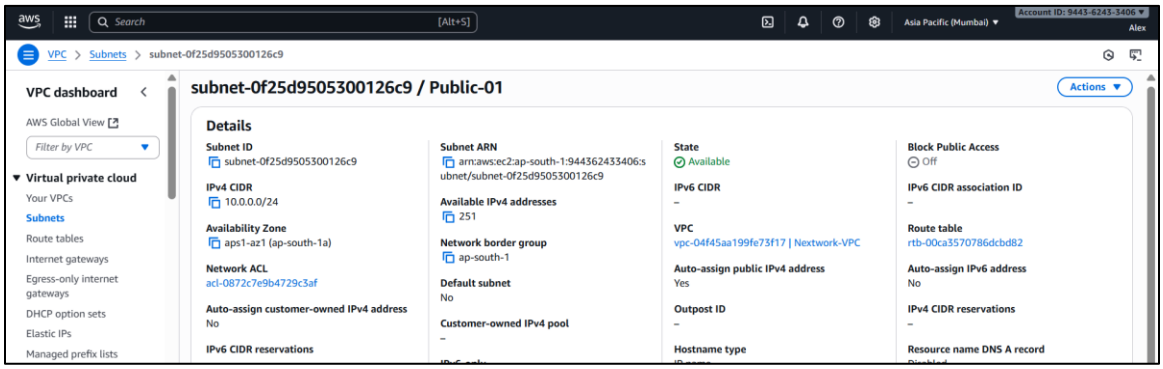


Step 2: Create Subnets

Divide your VPC into subnets for better resource organization.

Actions:

- - From the VPC Dashboard, select 'Subnets' in the navigation pane.
- - Click 'Create subnet'.
- - Choose the VPC you just created (NextWork VPC).
- - Enter a Subnet name (e.g., Public 1).
- - Select an Availability Zone.
- - Enter an IPv4 CIDR block for the subnet (e.g., 10.0.0.0/24).
- - Click 'Create subnet'.
- - Select your new subnet and go to 'Edit subnet settings'.
- - Enable 'Auto-assign public IPv4 address'.
- - Click 'Save' to apply changes.

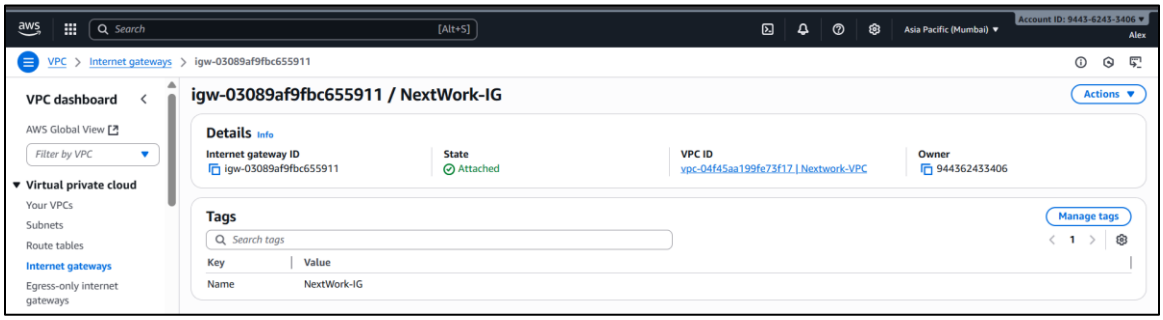


Step 3: Create an Internet Gateway

Attach an internet gateway to your VPC to enable internet access.

Actions:

- - In the VPC Dashboard, select 'Internet gateways' from the left-hand panel.
- - Click 'Create internet gateway'.
- - Enter a Name tag (e.g., NextWork IG).
- - Click 'Create internet gateway'.
- - Select your newly created gateway and choose 'Attach to VPC'.
- - Select your VPC (NextWork VPC) and confirm.
- - Your VPC is now connected to the internet.

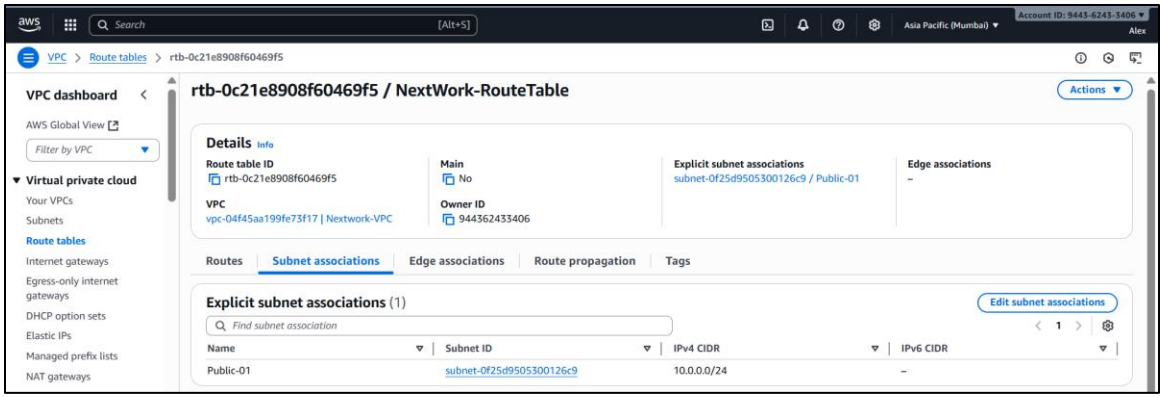


Step 4: Create a Route Table

Set up a route table to define how traffic flows in your VPC.

Actions:

- - In the VPC Dashboard, select 'Route tables' from the navigation pane.
- - Click 'Create route table'.
- - Enter a Name tag (e.g., NextWork-RouteTable).
- - Choose your VPC (NextWork VPC).
- - Click 'Create route table'.
- - Select your new route table and go to the 'Routes' tab.
- - Click 'Edit routes' and add a route with Destination = 0.0.0.0/0 and Target = your Internet Gateway.
- - Click 'Save changes'.
- - Associate the route table with your public subnet by going to the 'Subnet associations' tab and selecting 'Edit subnet associations'.
- - Choose your Public 1 subnet and save.

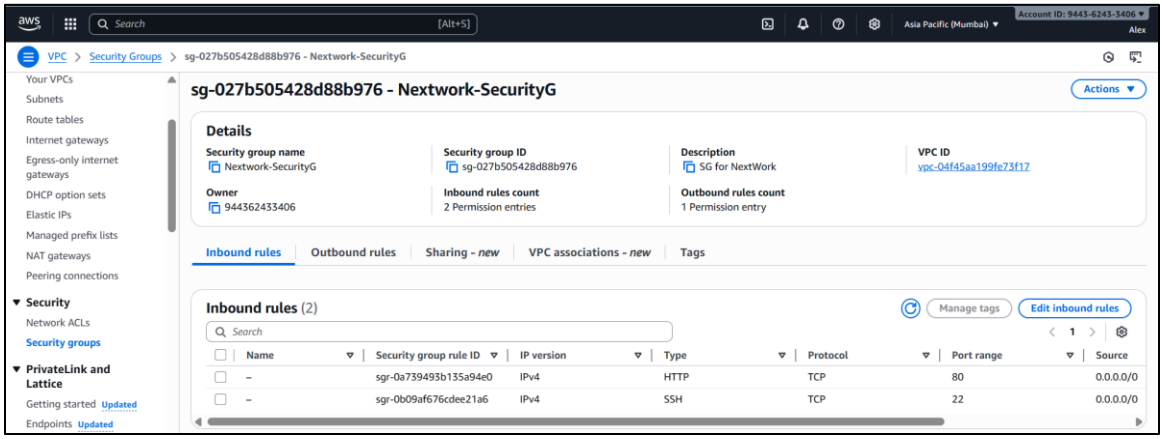


Step 5: Create a Security Group

Create a security group to control inbound and outbound traffic for your resources.

Actions:

- - In the VPC Dashboard, select 'Security groups'.
- - Click 'Create security group'.
- - Enter a Name tag (e.g., NextWork-SG).
- - Select your VPC (NextWork VPC).
- - Add inbound rules (e.g., allow HTTP on port 80, SSH on port 22).
- - Add outbound rules (default allows all traffic).
- - Click 'Create security group' to save.



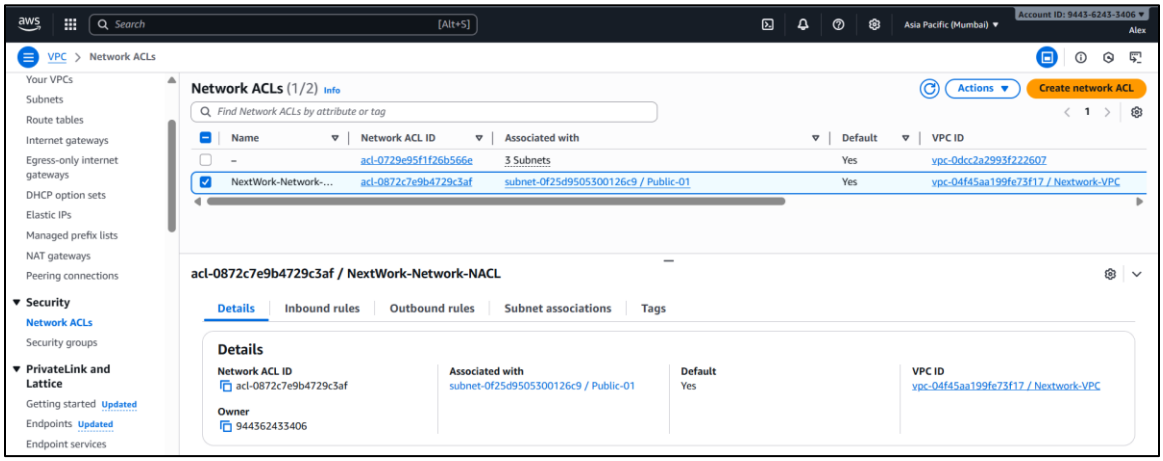
Step 6: Create a Network ACL (Access Control List)

Set up a network ACL to provide an additional layer of security at the subnet level.

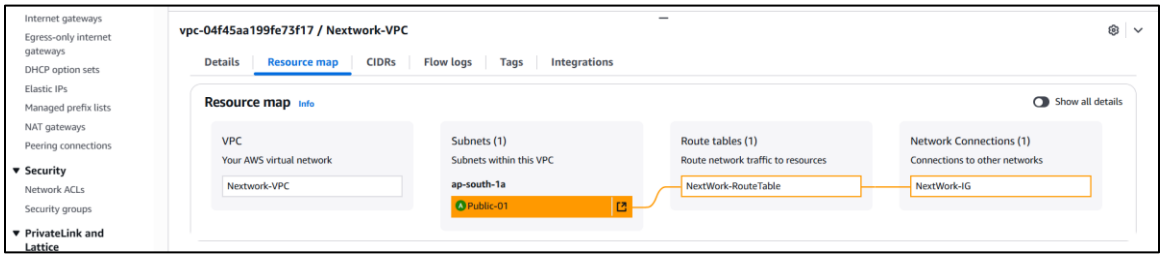
Actions:

- - In the VPC Dashboard, select 'Network ACLs' from the navigation pane.
- - Click 'Create network ACL'.
- - Enter a Name tag (e.g., NextWork-NACL).
- - Choose your VPC (NextWork VPC).
- - Click 'Create network ACL'.

- - Select your new NACL and go to the 'Inbound rules' tab. Add rules (e.g., allow HTTP, HTTPS, and SSH).
- - Go to the 'Outbound rules' tab and configure rules (e.g., allow all traffic).
- - Associate your NACL with the public subnet by selecting 'Subnet associations'.
- - Click 'Edit subnet associations', select your Public 1 subnet, and save.



VPC Resource Map -



1. **Client/User:** A user enters the URL of your website into their web browser and hits enter.
2. **Internet Gateway:** The request is sent from the user's browser through the internet and reaches your internet gateway, **NextWork IG**.
3. **VPC:** The internet gateway forwards the user's request to the VPC it's attached to, **NextWork VPC.**
4. **Route Table:** Your VPC has a route table for your public subnet (called **NextWork route table**), which directs traffic to your EC2 instance hosting the website. The user's request get put on the **local** route in the route table.
5. **Network ACL:** While en route to your EC2 instance, the request has to pass through the network ACL associated with your public subnet. The network ACL has an inbound rule (rule 100) that lets in traffic from anywhere (0.0.0.0/0), so your request is let through.
6. **Public Subnet:** The request enters your public subnet **Public 1** and travels to your EC2 instance within the subnet.

7. 👮 **Security Group:** The request reaches the security group **NextWork Security Group** attached to the EC2 instance. The security group has an inbound rule that allows HTTP traffic (Port 80) from anywhere (0.0.0.0/0), so the request can pass through.

8. 😤 **EC2 Instance:** The request reaches your EC2 instance hosting the website. The web server on the EC2 instance processes the request and prepares the response.

9. 💻 **Data gets sent back:** Website content is sent back to the user. The outbound traffic goes through the security group, public subnet, network ACL, route table, VPC, and internet gateway, and user gets to see website content load on their page.