SECURE VPC ARCHITECTURE WITH NAT GATEWAY & WEBHOSTING

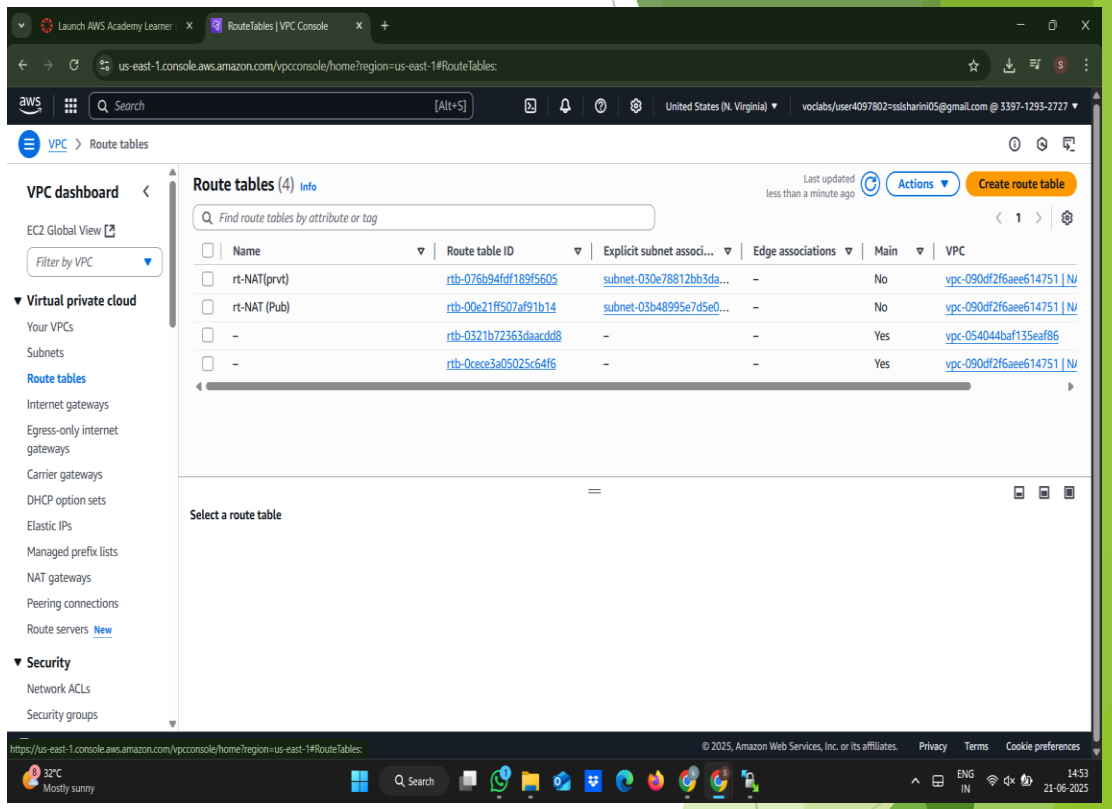
- 23P31A0437-M.SRI SATYA RAMA DEVI
- 23P31A04E6-G.SRI SAI DEEPTHY
- 23P31A0451-R.SAI PADMINI
- 23P31A0459-S.SRI LAKSHMI SATYA HARINI
- 23P31A0424-K.SATYA GOPIKA

ROAD MAP

- Create VPC : define CIDR block
- Add subnets : Public subnet
  : private subnet
- Attach internet gateway : enable internet access for public subnet.
- Configure route tables : Public route to IGW
  :Private route to NAT gateway
- Launch NAT gateway : In public subnet with elastic IP.
  :allows private subnet to access the internet securely.
- Deploy EC2 instances : web server(public subnet)
  :Db server (private subnet)
- Setup security
- Test & monitor : access web app
  :verify NAT,security and logs.

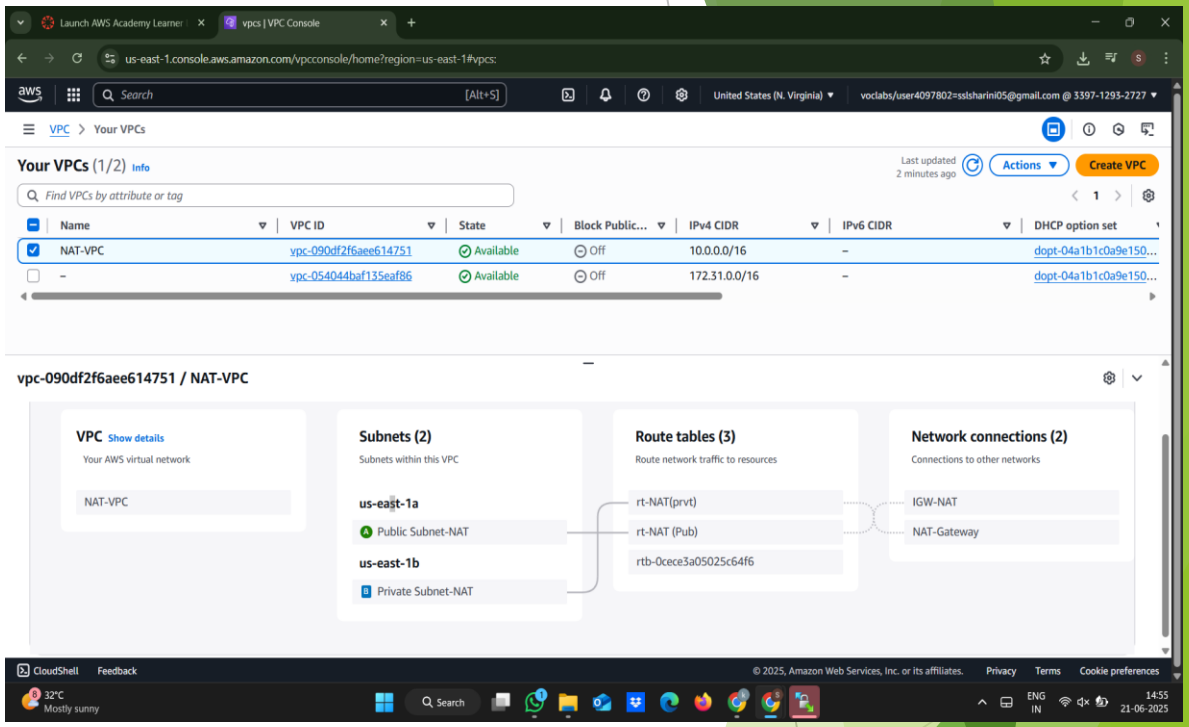
CREATE ROUTE TABLE

- **Create a VPC** with public and private subnets.
- **Attach an Internet Gateway** to the VPC for public internet access.
- **Launch a NAT Gateway** in the public subnet with an Elastic IP.
- **Public Route Table:** Add 0.0.0.0/0 → Internet Gateway; associate with public subnet.
- **Private Route Table:** Add 0.0.0.0/0 → NAT Gateway; associate with private subnet.



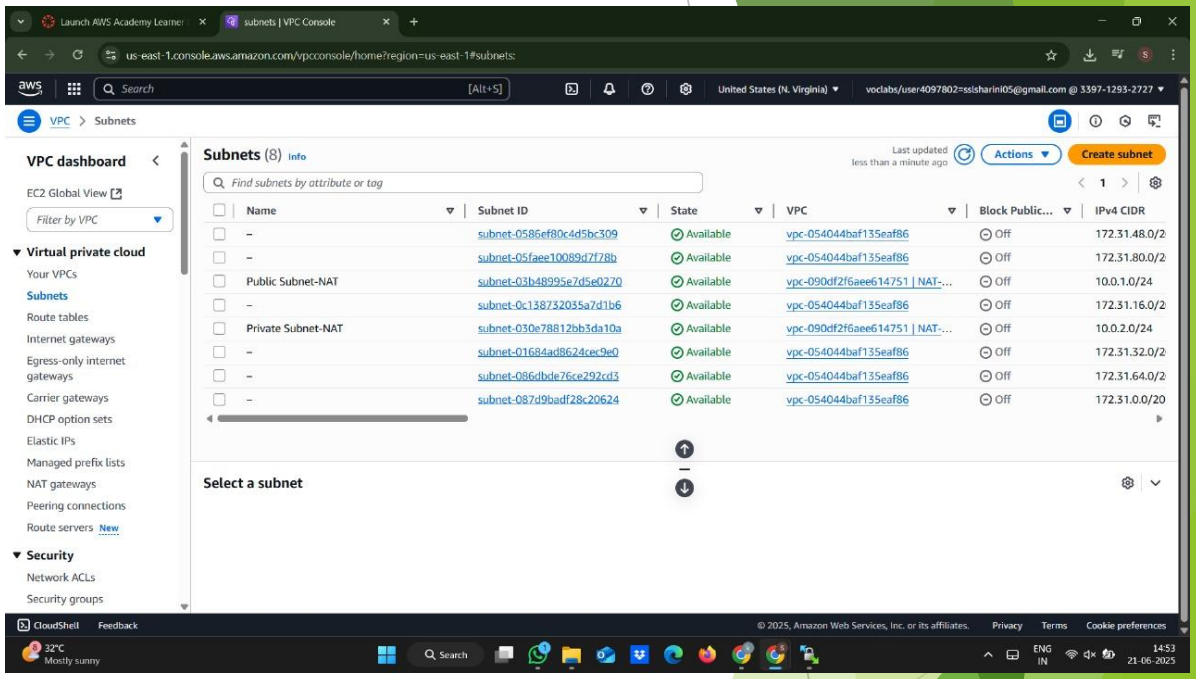
CREATE VPC

- Create a VPC with public subnet and a private subnet..
- Attach an internet gateway to the VPC and route from the public subnet to it…
- Create a NAT Gateway in the public subnet with an elastic IP and route from the private subnet to it…
- Launch a web server EC2 in the public subnet (with public IP) & an EC2 in the private subnet(no public IP)…
- Use security groups to allow HTTP to web server and restrict private ec2 access to internal traffic only…



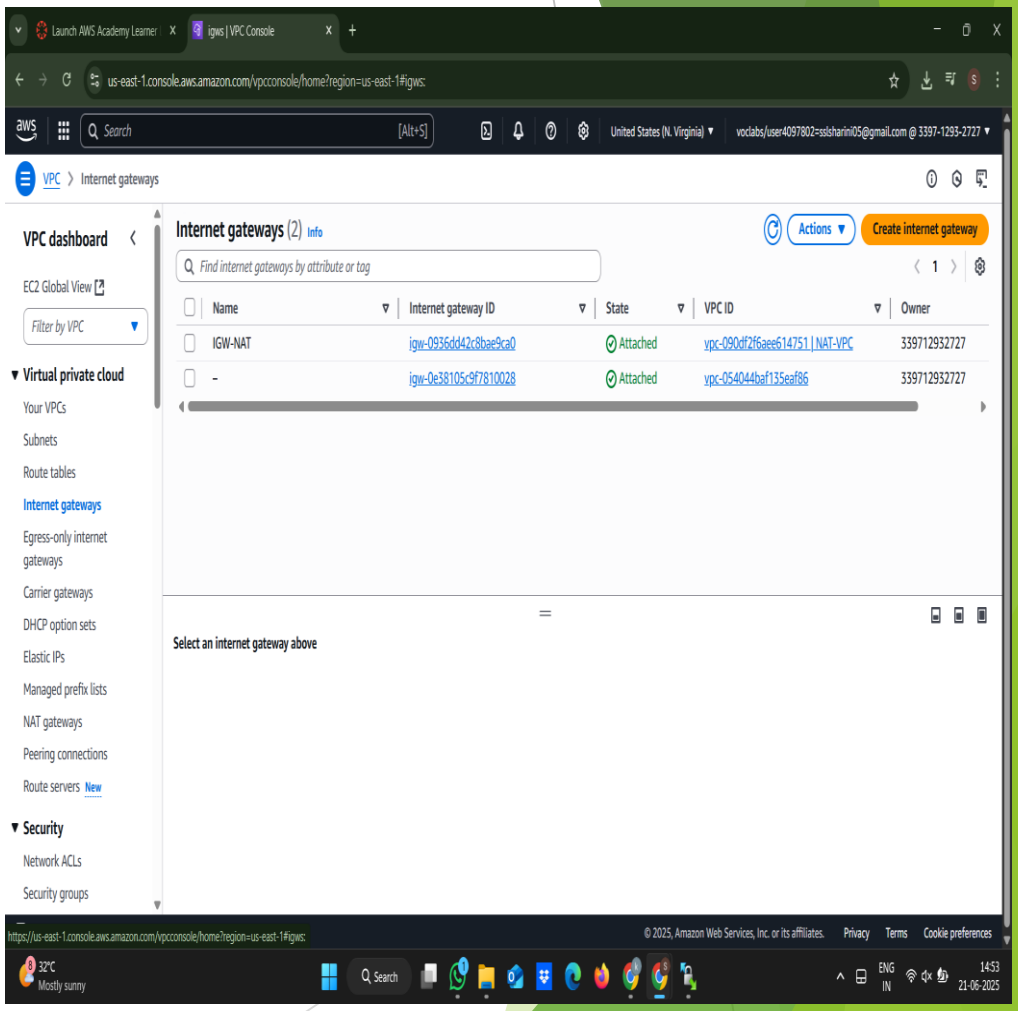
CREATE SUBNETS

- Create a **Public Subnet** for web server and NAT Gateway.
- Create a **Private Subnet** for app/database instances.
- Enable **auto-assign public IP** for the public subnet; disable it for the private one.
- Enable **auto-assign public IP** for the public subnet; disable it for the private one.
- Place **web server EC2** in the public subnet and **private EC2/RDS** in the private subnet.



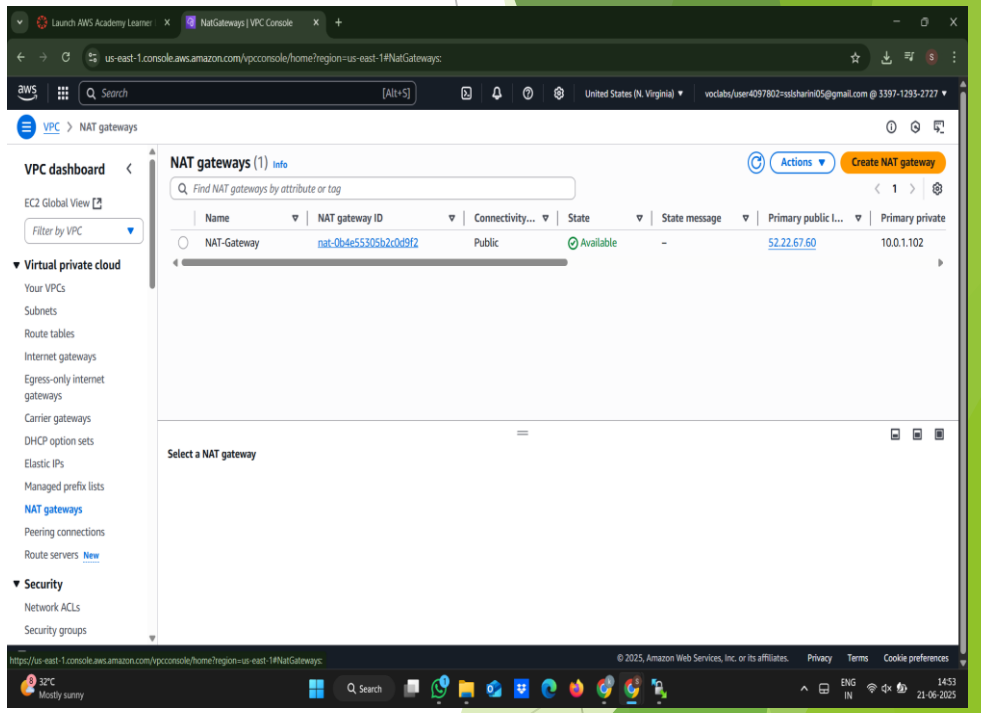
➢ ATTACH INTERNET GATEWAYS

- Go to VPC Dashboard > Internet Gateways > Create Internet Gateway.
- Name it and create it.
- Select the IGW and click Attach to VPC, then choose your VPC.
- Go to Route Tables, select the public route table, and click Edit routes.
- Add route: Destination → Target: your Internet Gateway.



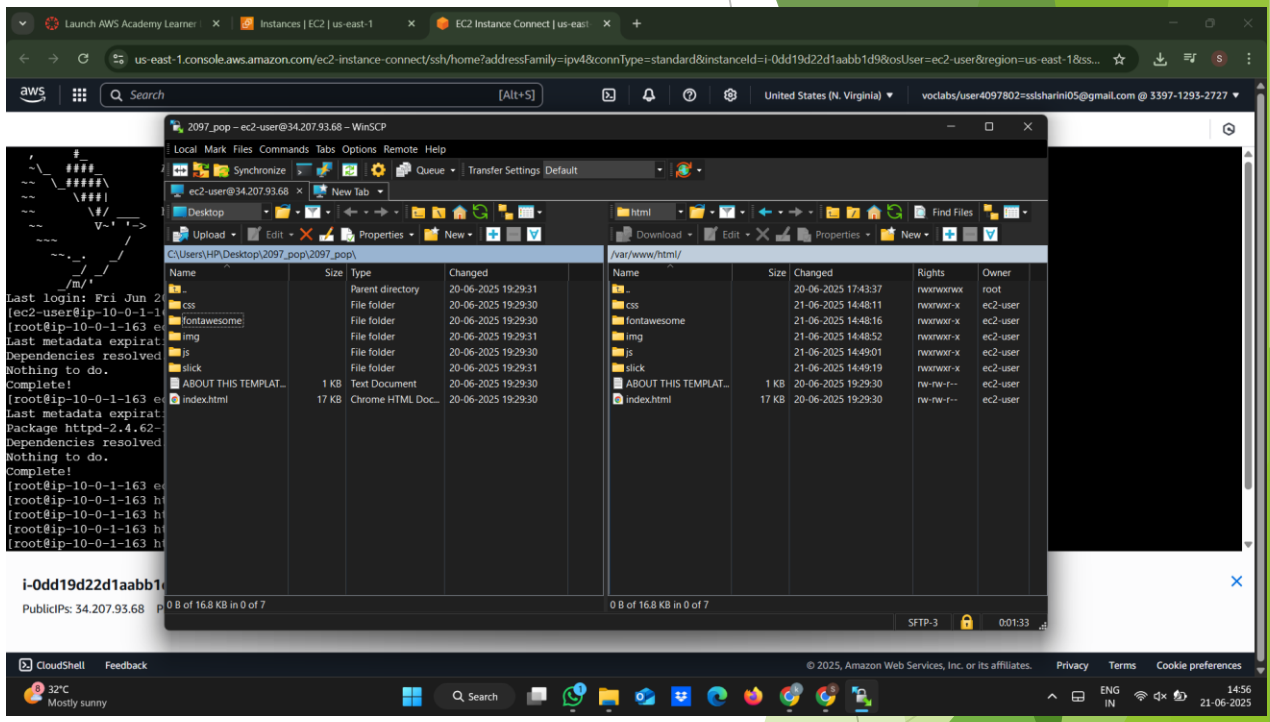
➢ CREATE A NAT GATEWAY

- Create a VPC with at least two subnets — one public and one private.
- Attach an IGW to the VPC and route public subnet traffic to the IGW.
- In the public subnet, create a NAT Gateway with an Elastic IP.
- Update the private subnet route table to route internet-bound traffic via the NAT Gateway.
- Deploy web servers (e.g., EC2) in public subnet and app/db servers in private subnet for secure hosting.



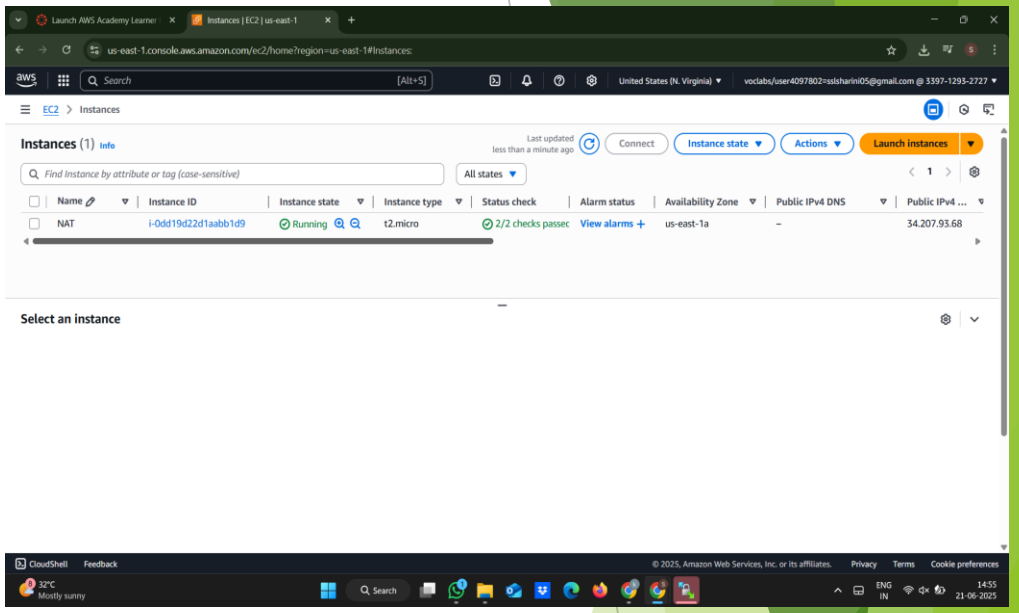
➢ LAUNCH WEB SERVER

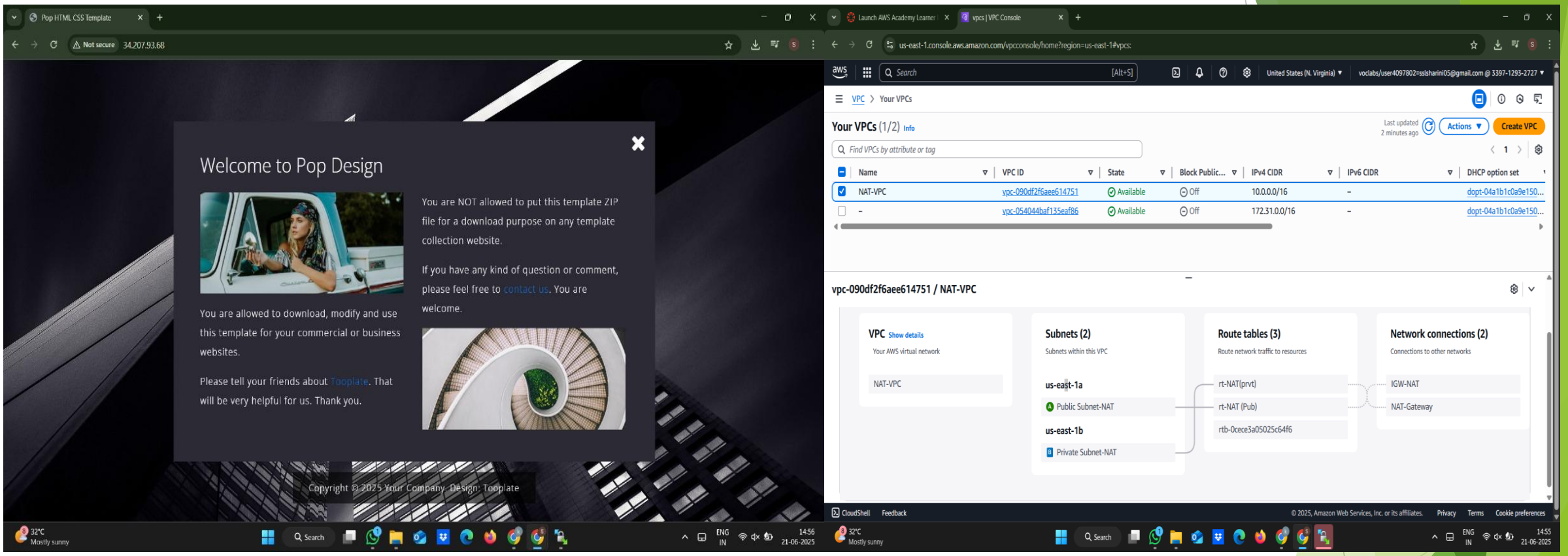
- Launch EC2 in Public Subnet: Deploy a web server (e.g., Amazon Linux) in the VPC's public subnet.
- Security Group: Allow inbound HTTP/HTTPS (ports 80/443) and SSH (port 22) from trusted IPs.
- User Data Script: Add a startup script to install and start a web server
- Elastic IP: Associate an Elastic IP to the EC2 instance for public access.
- Test Web Access: Open the browser with the EIP to verify the web server is serving content.



CONFIGURE SECURITY GROUPS

- Create a security group allowing inbound HTTP (80), HTTPS ,and SSH (22) from your IP.
- Allow inbound traffic only from the web server's SG on required ports.
- Allow all outbound traffic for updates and internet access (via NAT for private subnets).
- Assign the web SG to EC2 in the public subnet and app SG to EC2 in private subnet.
- Ensure the web server is publicly reachable and can securely connect to private-tier servers.





THANK YOU FOR YOUR ATTENTION....