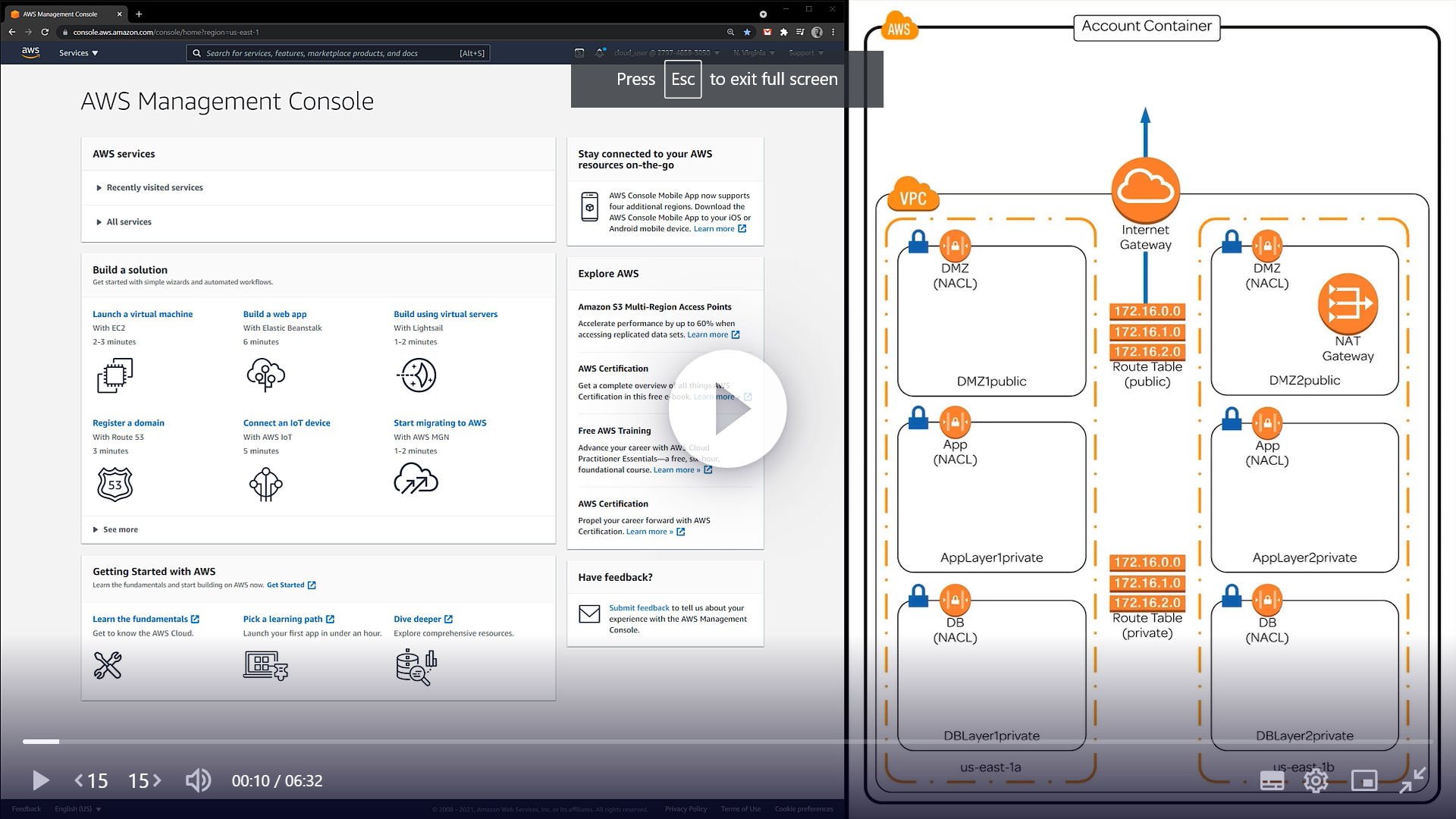
Basic Architecture:



1. **Create only VPC**
2. **Create 6 subnets –** **2 DMZpublic, 2 Applayer private, 2 DBlayer private**
3. **Create Internet Gateway to connect public subnets to open internet**
4. **Create NATGateway -**
5. **Create Public & private Route tables**
6. **Associate public RT to public subnets**
7. **Associate private RT to private subnets**
8. **To public RT add route to Internet gateway**
9. **To private RT add route to NAT gateway**
10. **Create NACL for 3 layers- DMZ, applayer,dblayer**
11. **Associate NACL to respective subnets**

CIDR’s used for subnets

10.99.1.0/24

10.99.2.0/24

10.99.11.0/24

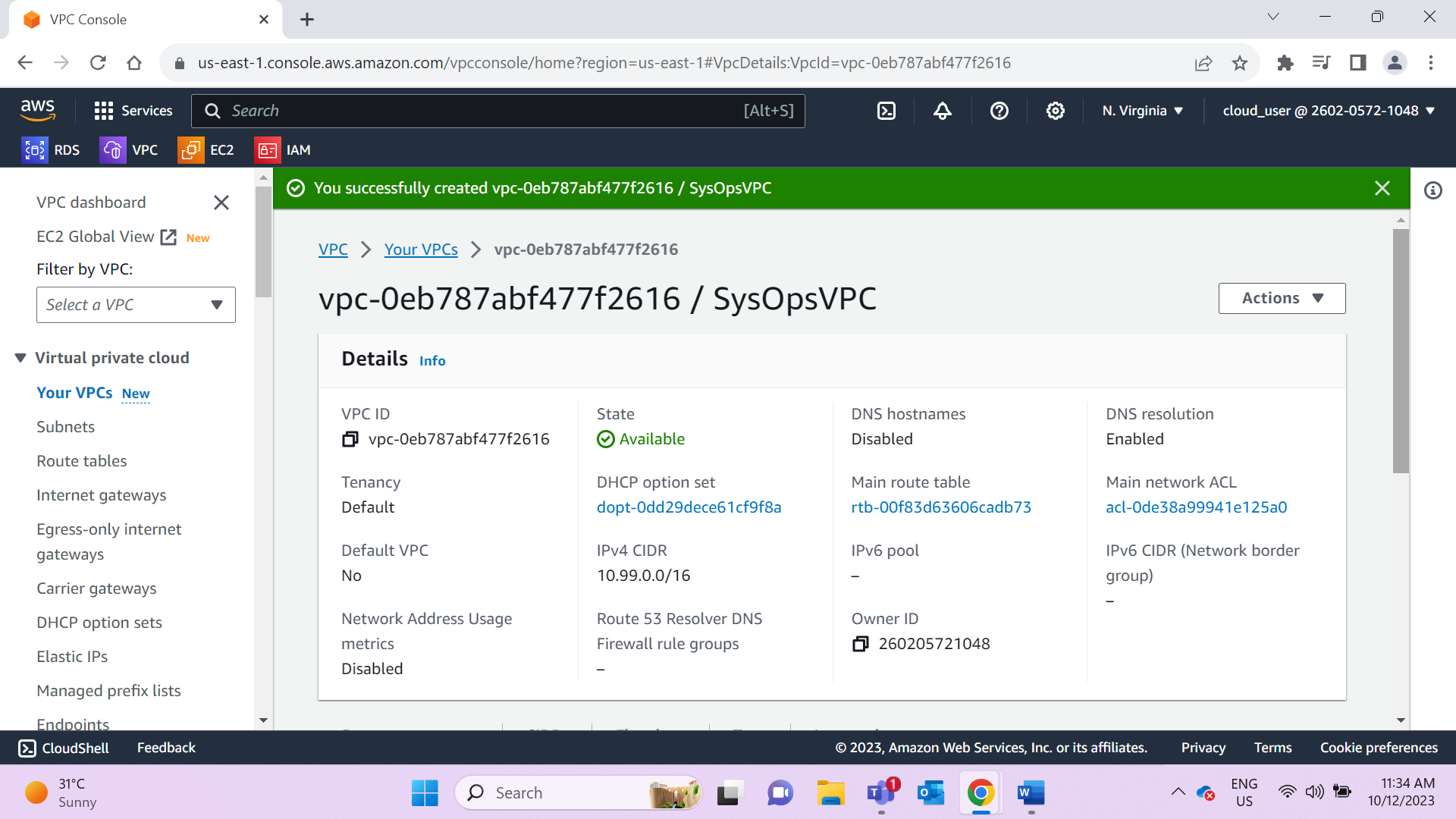
10.99.12.0/24

10.99.21.0/24

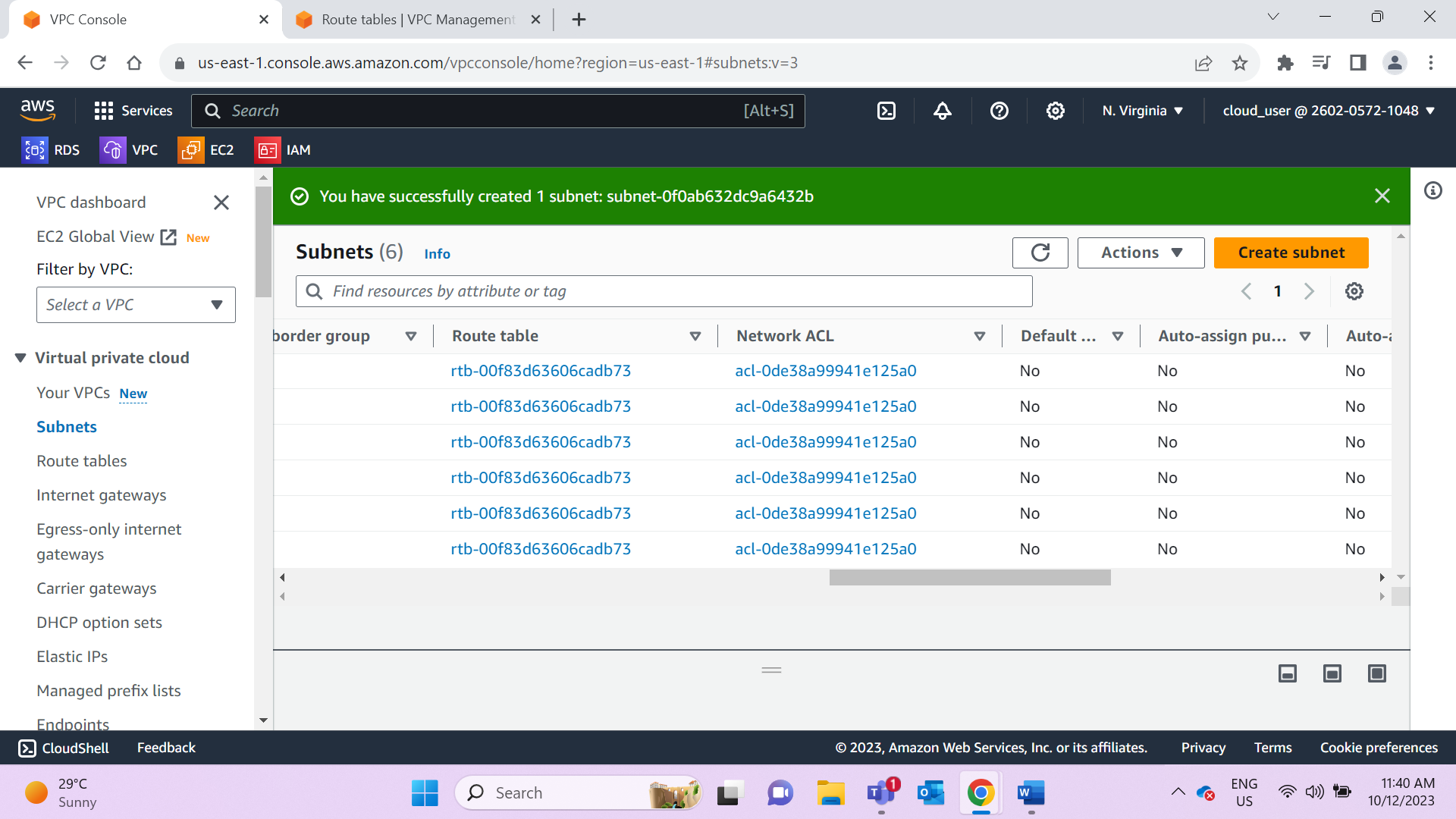
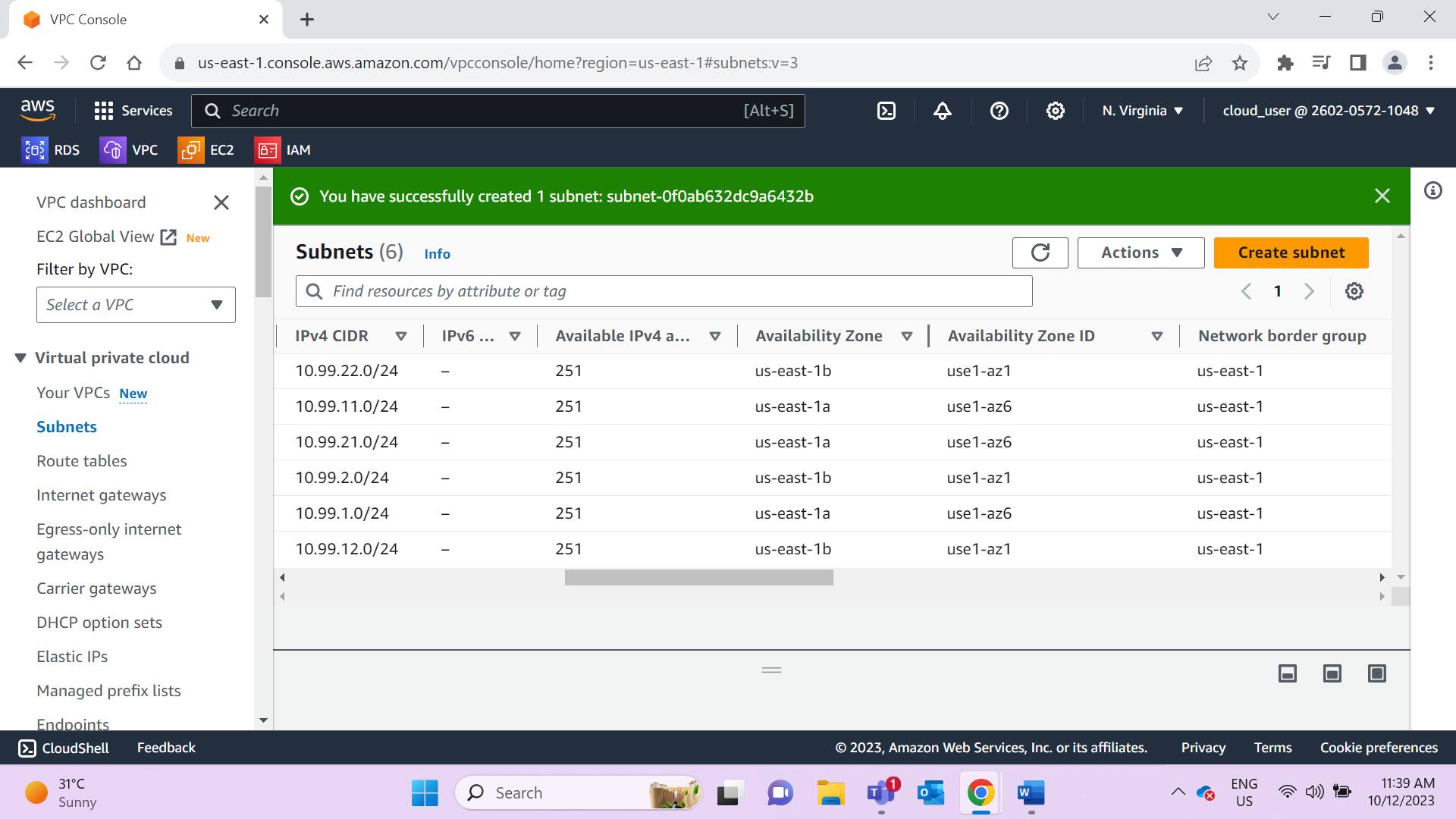
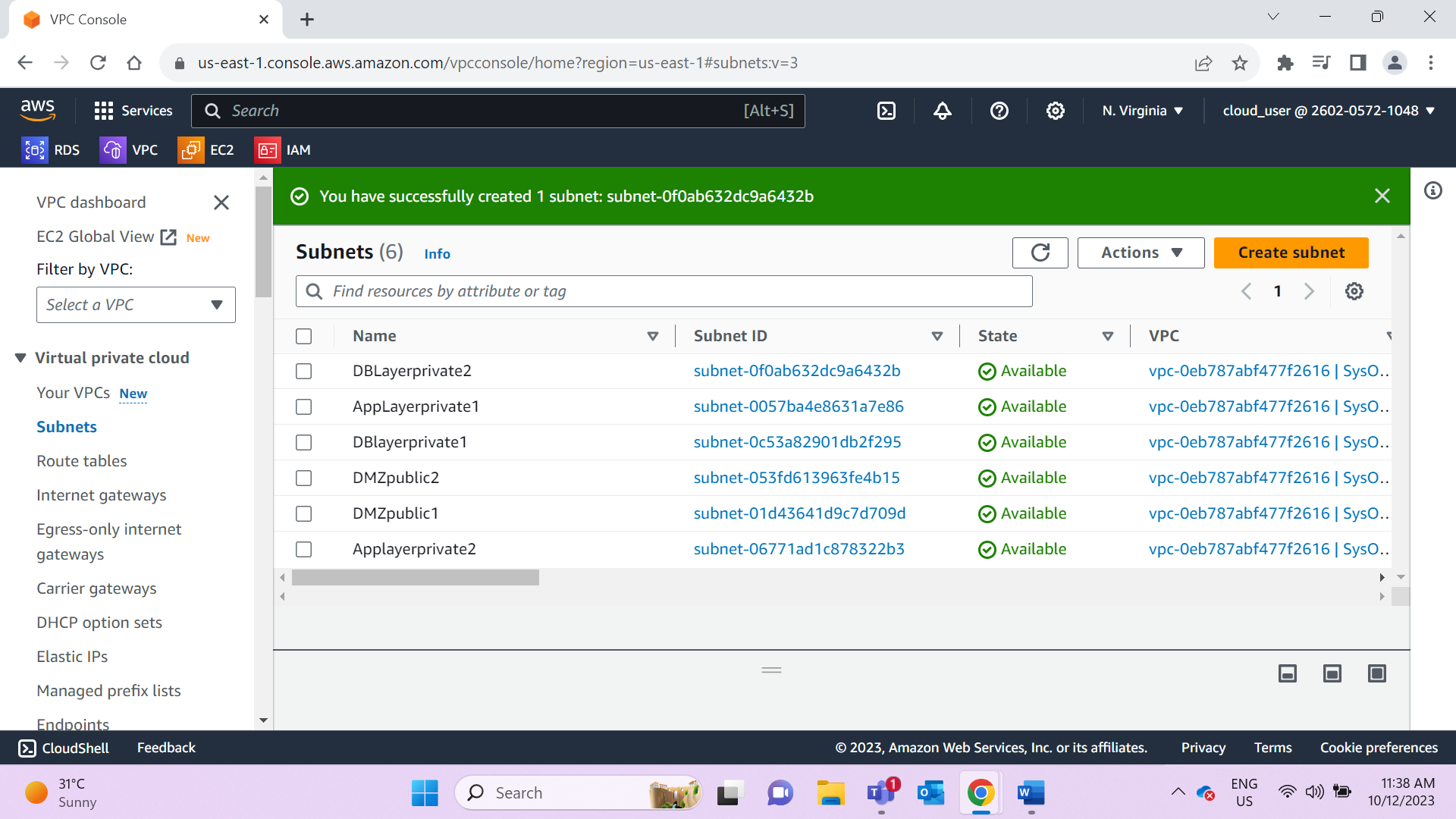
10.99.22.0/24

Create VPC:

* Create VPC by clicking on “Your VPC” rather than creating it from Wizard
* To create from Scratch select “VPC Only” under Resources to Create rather than “VPC and more”

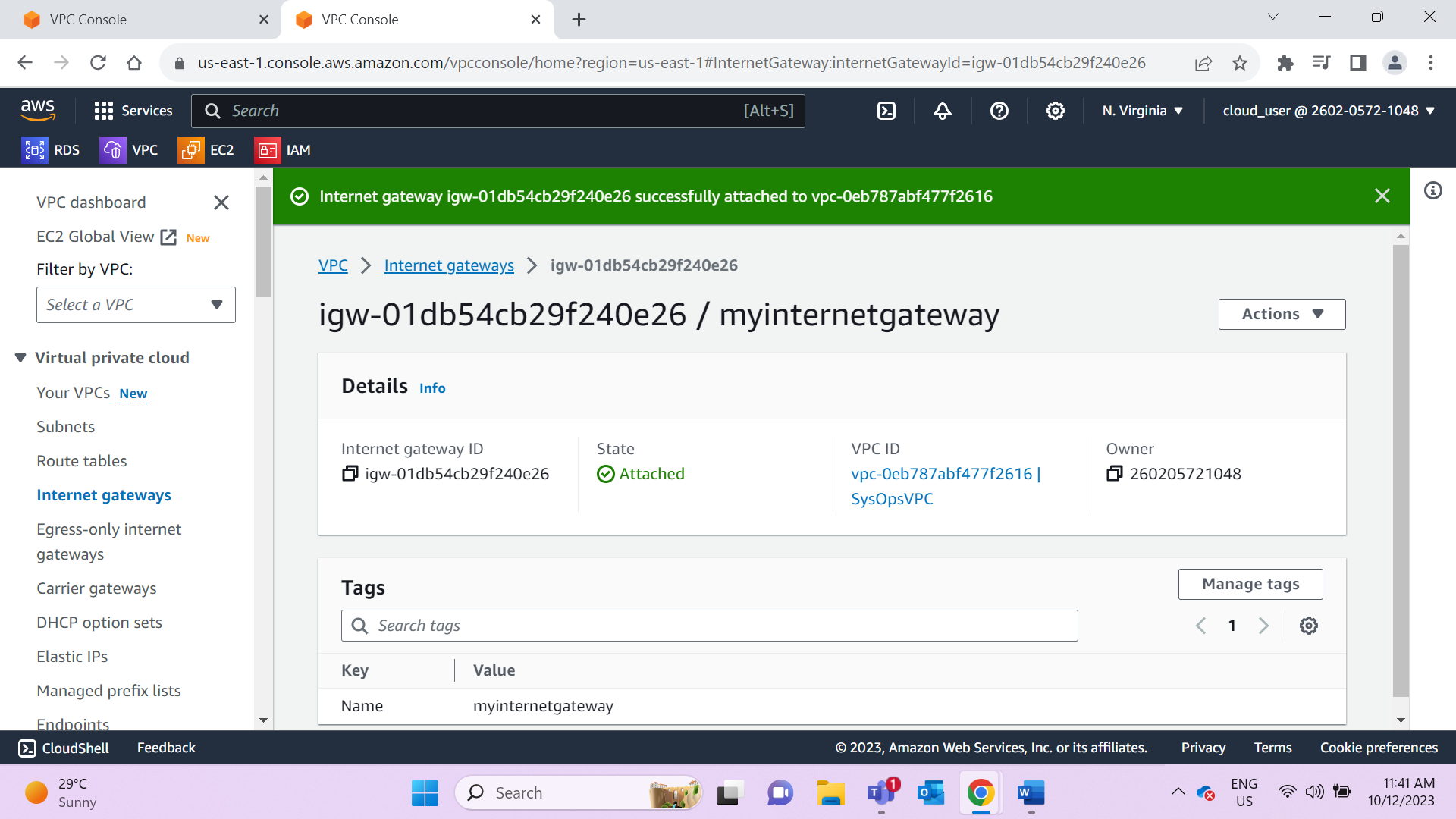


Create 6 subnets: **2 DMZpublic, 2 Applayer private, 2 DBlayer private each in 2 different AZs**



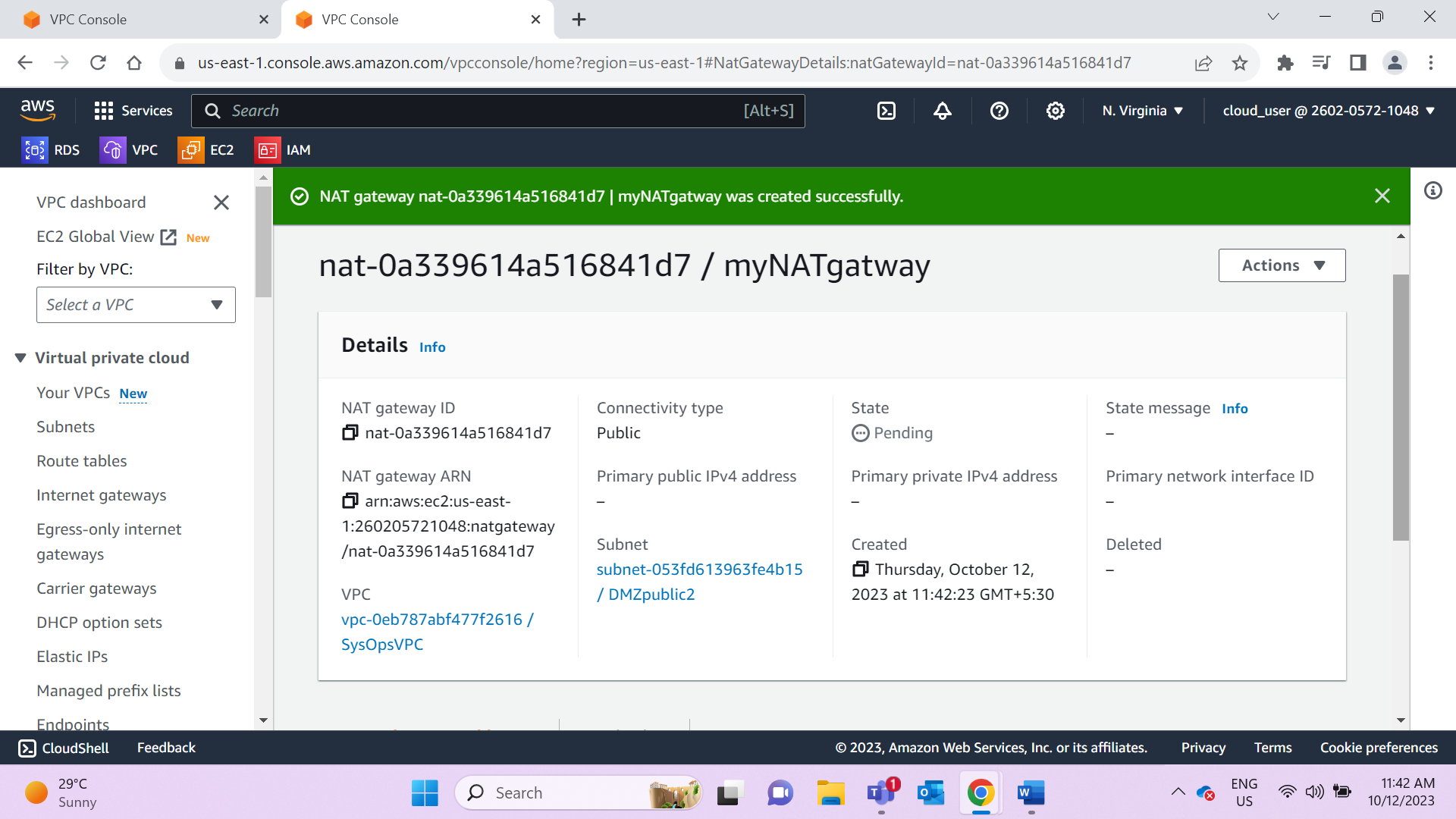
Create IG and attach VPC to it.

Internet Gateway is used to allow open/outside network to connect to VPC

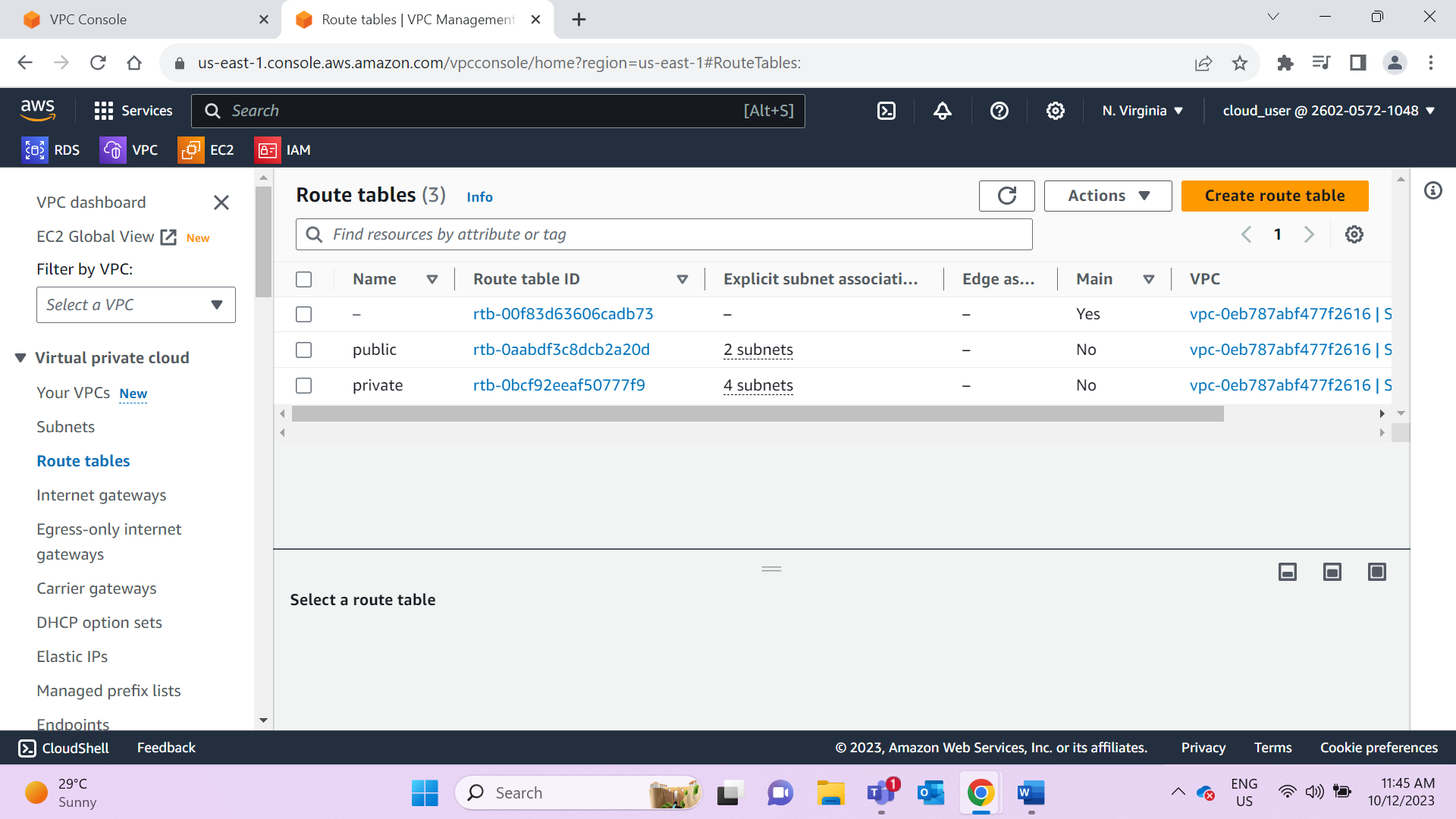


Create NATGATEWAY and add DMZpublic2 subnet to it

NATGateway is used to connect private subnets to outside NW with help of public subnet hence NATGateway is situated inside public subnet

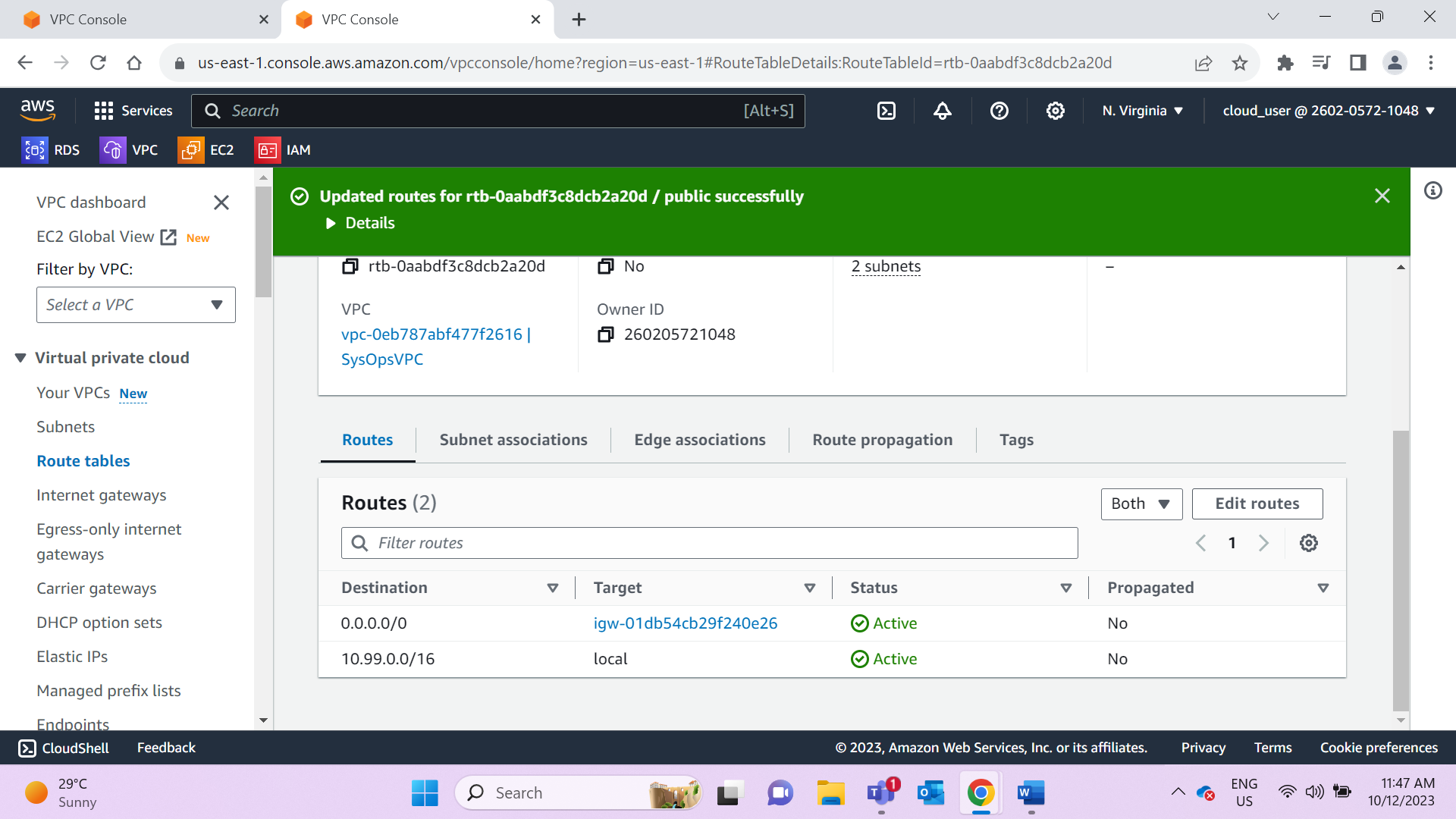


Create 2 Route tables- public & private and associate subnets to it accordingly



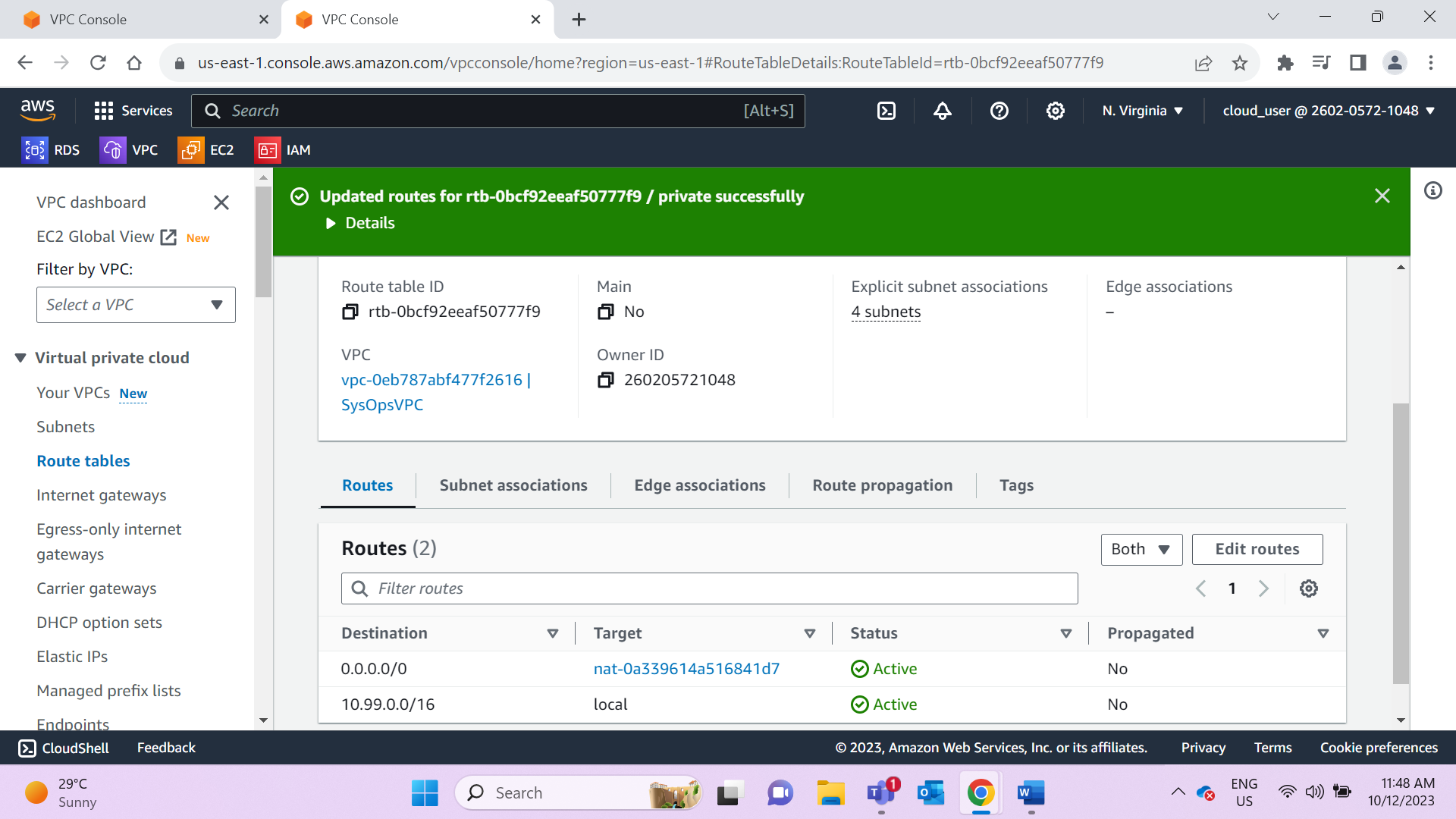
In public RT add another route to IG

By connecting Public Route to Internet Gateway this Route table becomes public



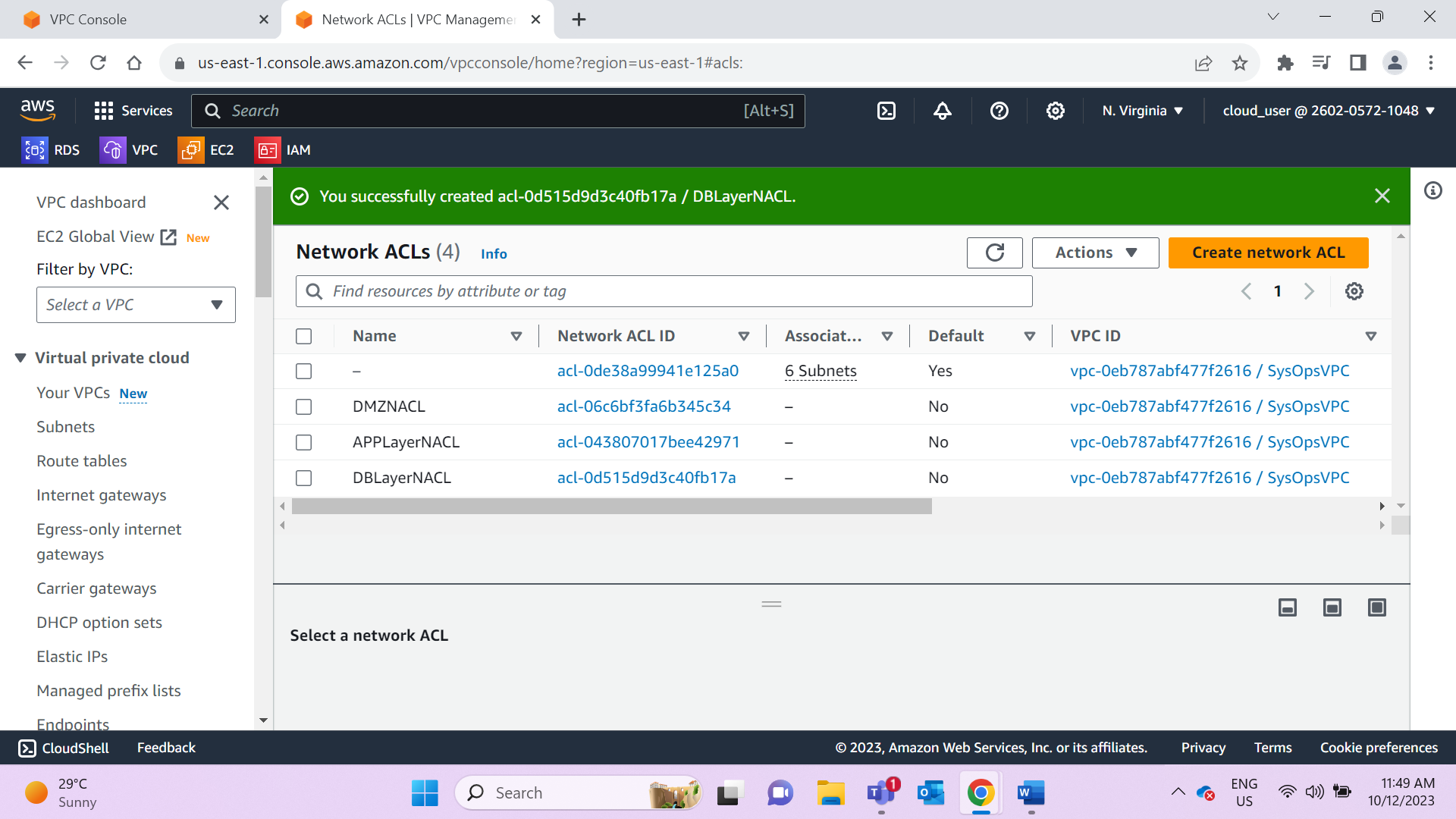
Private RT – add route to NATGW

By connecting NATGateway to private Route table this RT becomes private



Create 3 NACL

NACL provides additional security layer to subnets



Associate NACL to respective subnets

