**13.NetworkFirewall**

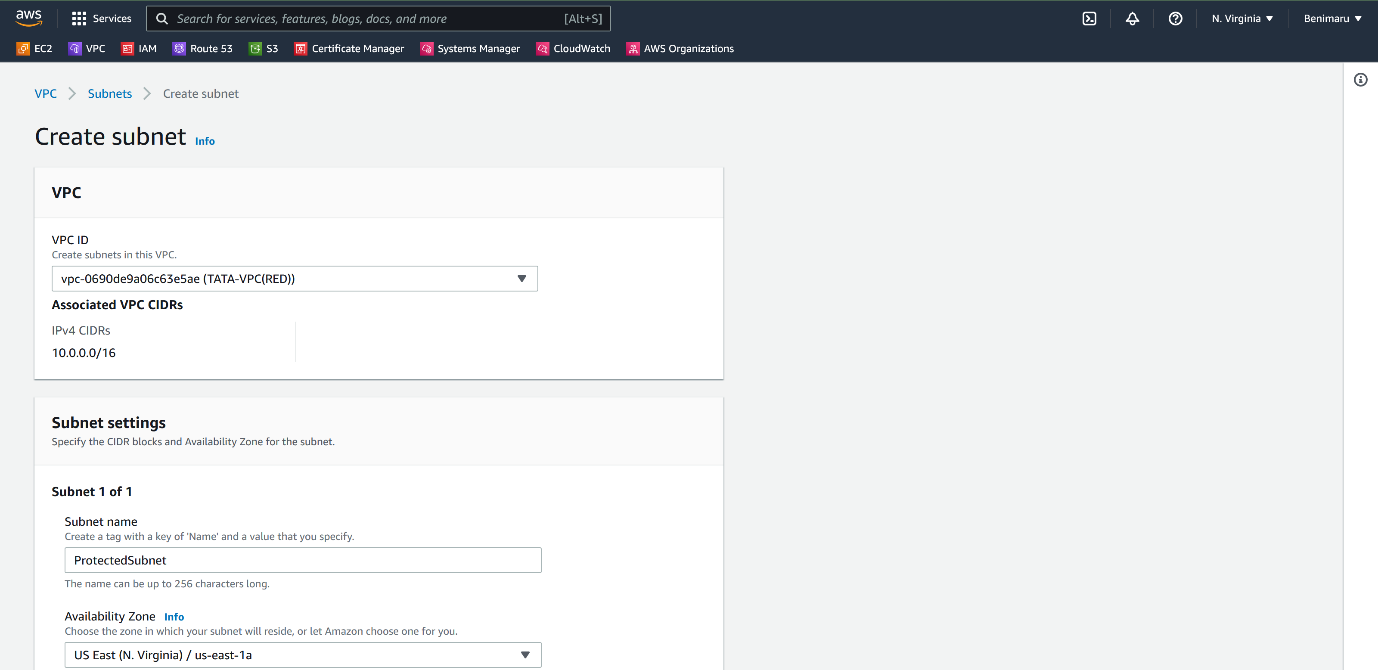
1. Create 2 subnets
2. Protected subnet
3. Firewall subnet
4. Deploy a windows server on protected subnet and login to it.
5. Create firewall rule group and select domain list and provide the domain names which needed to be blocked.
6. .facebook.com
7. .amazon.com
8. .flipkart.com
9. Create a firewall policy and add the firewall rule group which you have created in step 2.
10. Create firewall and select firewall subnet created in step1 and create az us-east-1 where both firewall & protected subnet are created.
11. Create 3 routing tables
12. Protected subnet RT
13. Firewall subnet RT
14. IGW ingress subnet RT
15. For protected subnet add 0.0.0.0/0 to firewall VPC eni interface like
16. For firewall subnet add 0.0.0.0/0 to IGW which is a public subnet
17. For IGW ingress subnet RT, select edge associations and select IGW. In the same routing table, select routes, in the destination provide CIDR range of protected subnet and give target as firewall vpc eni.

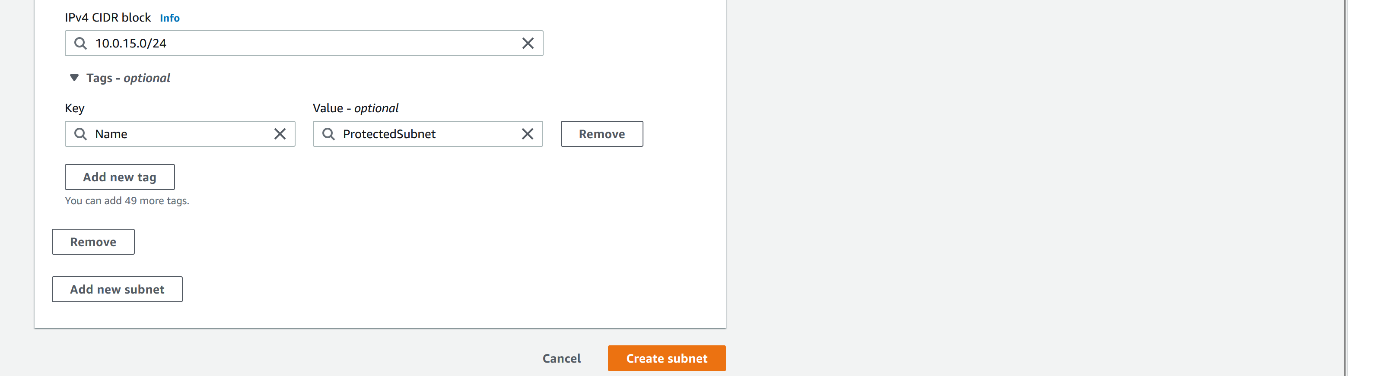
**1. Create 2 subnets**

--- here, we are going to create 2 subnets.

**a. ProtectedSubnet – 10.0.15.0/24**

--- go to vpc, my current vpc is TATA-VPC. I will create protectedsubnet under TATA-VPC.

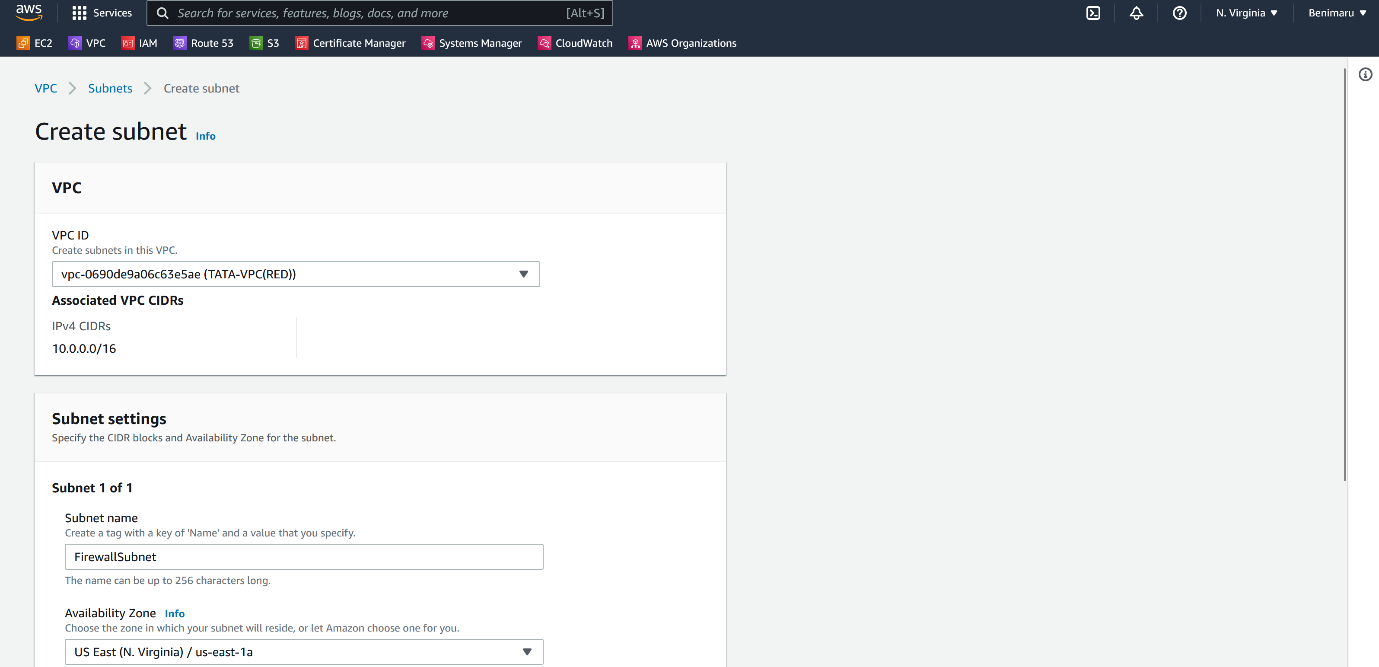


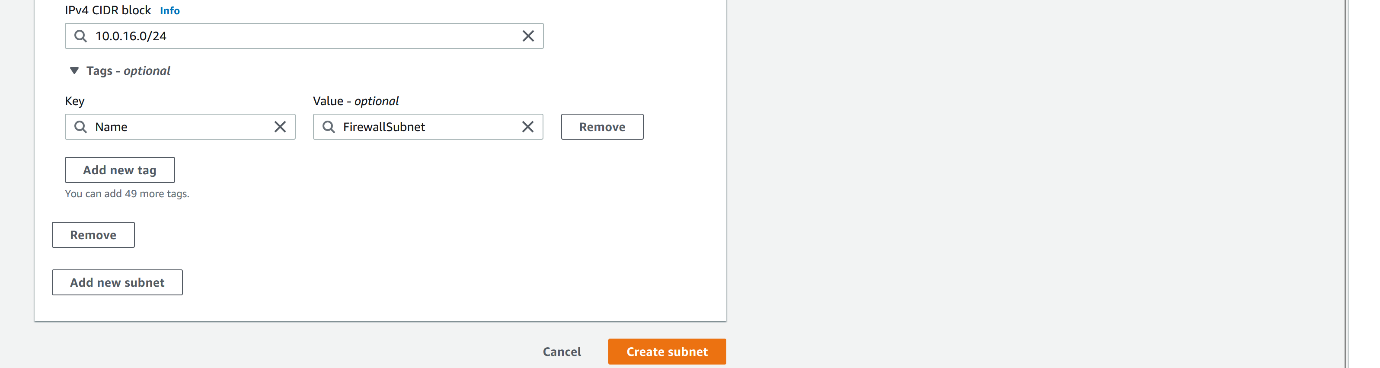


--- click on create subnet.

1. **FirewallSubnet – 10.0.16.0/24**

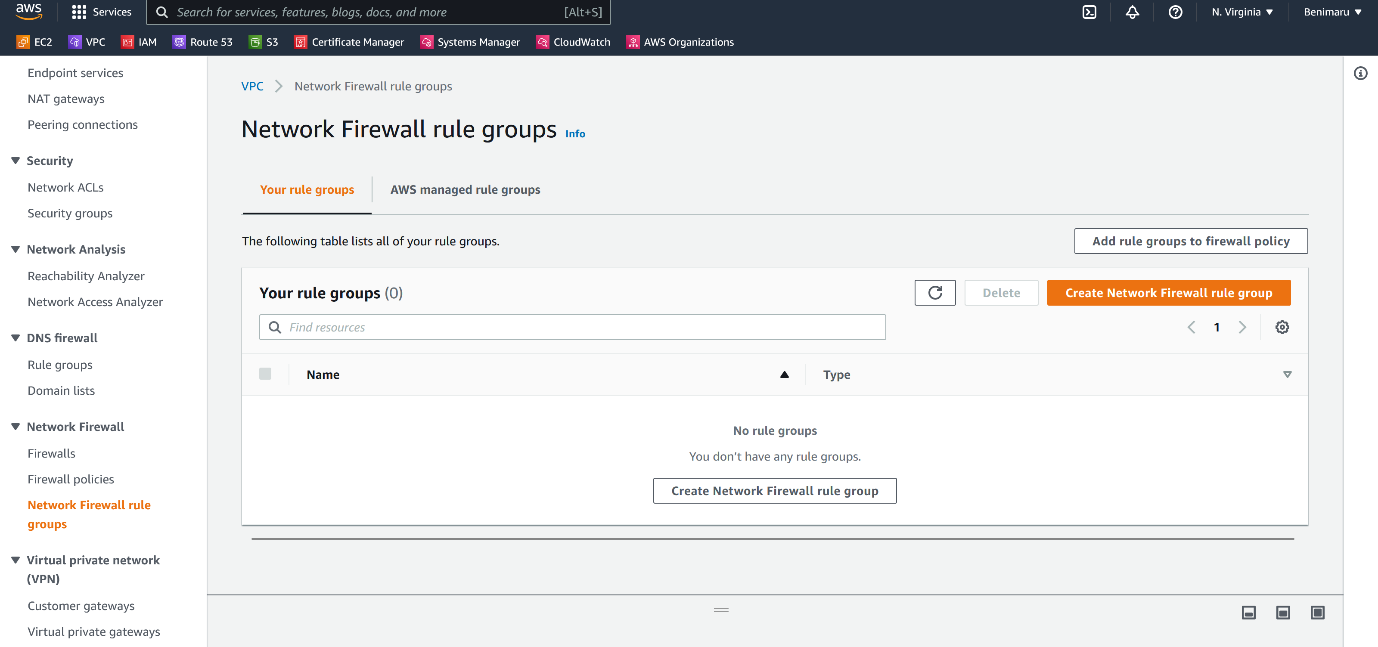
--- go to vpc



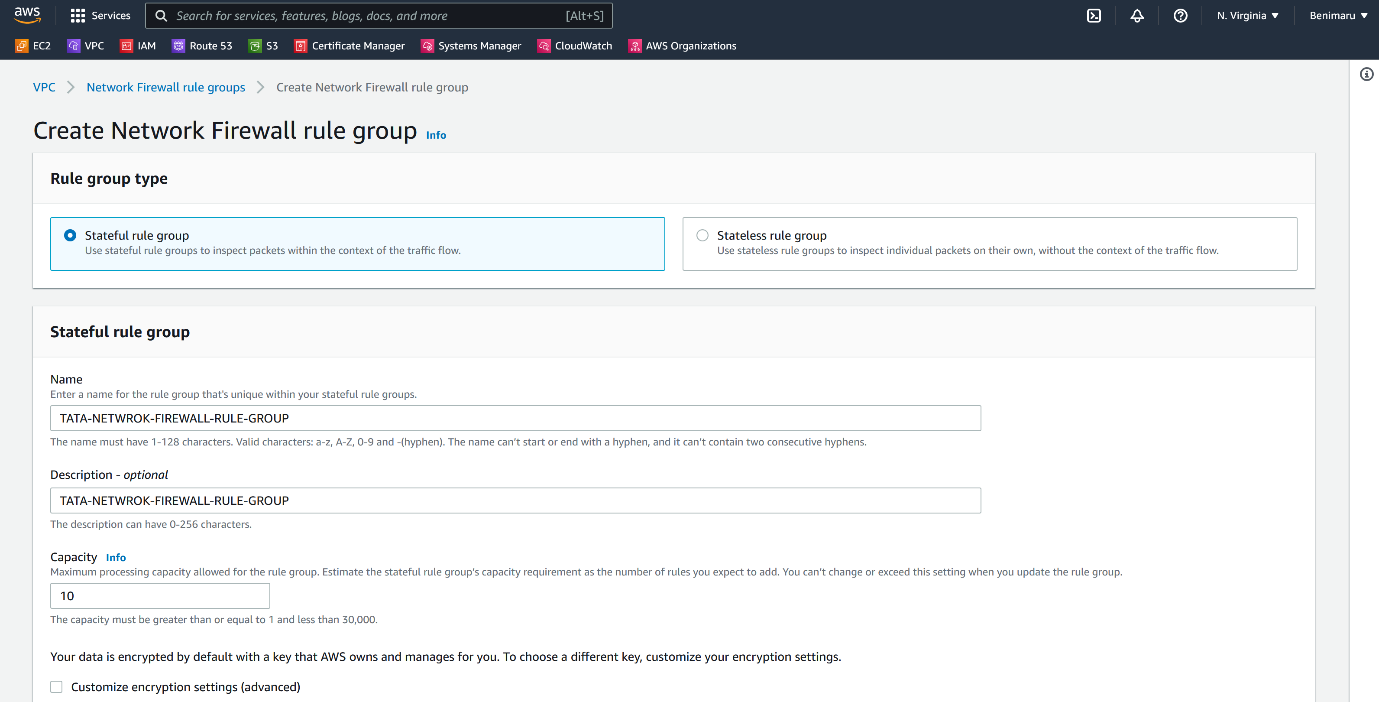


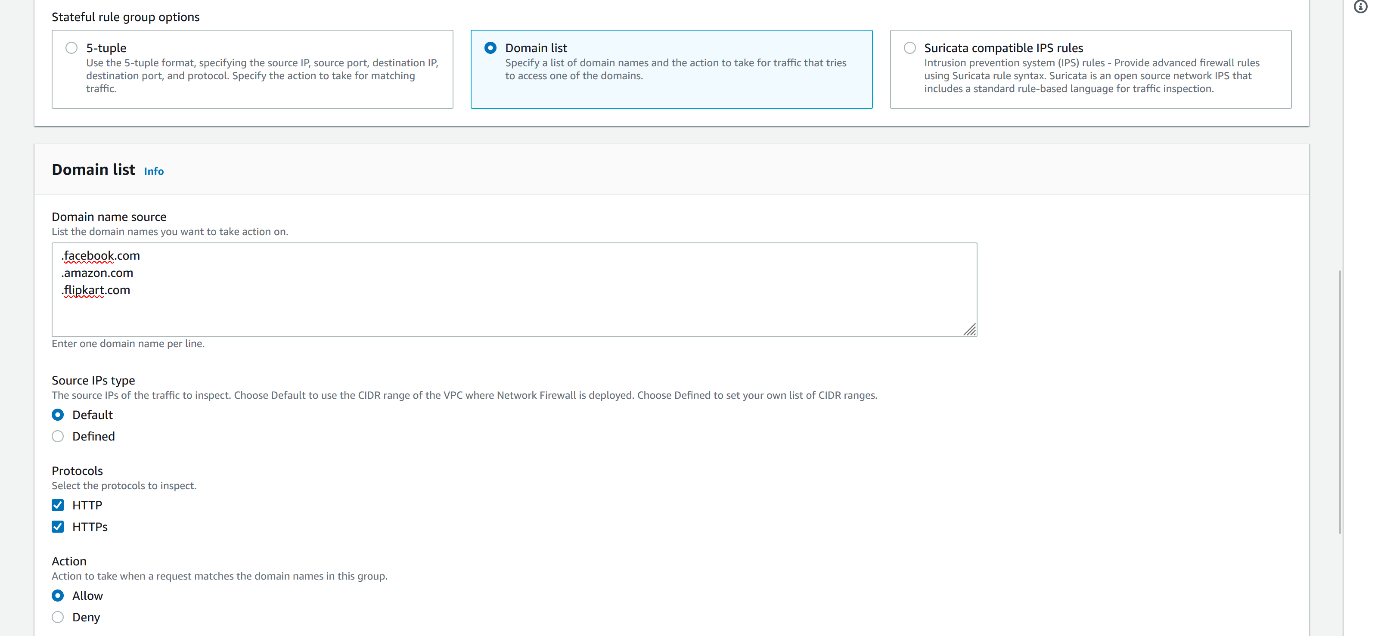
--- click on create subnet.

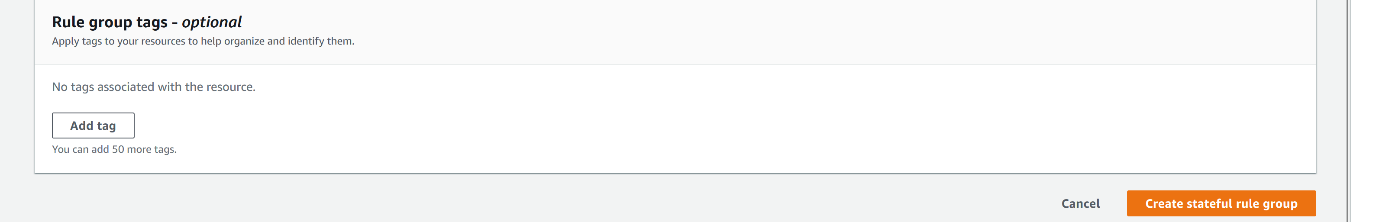
**Create network firewall rule group**



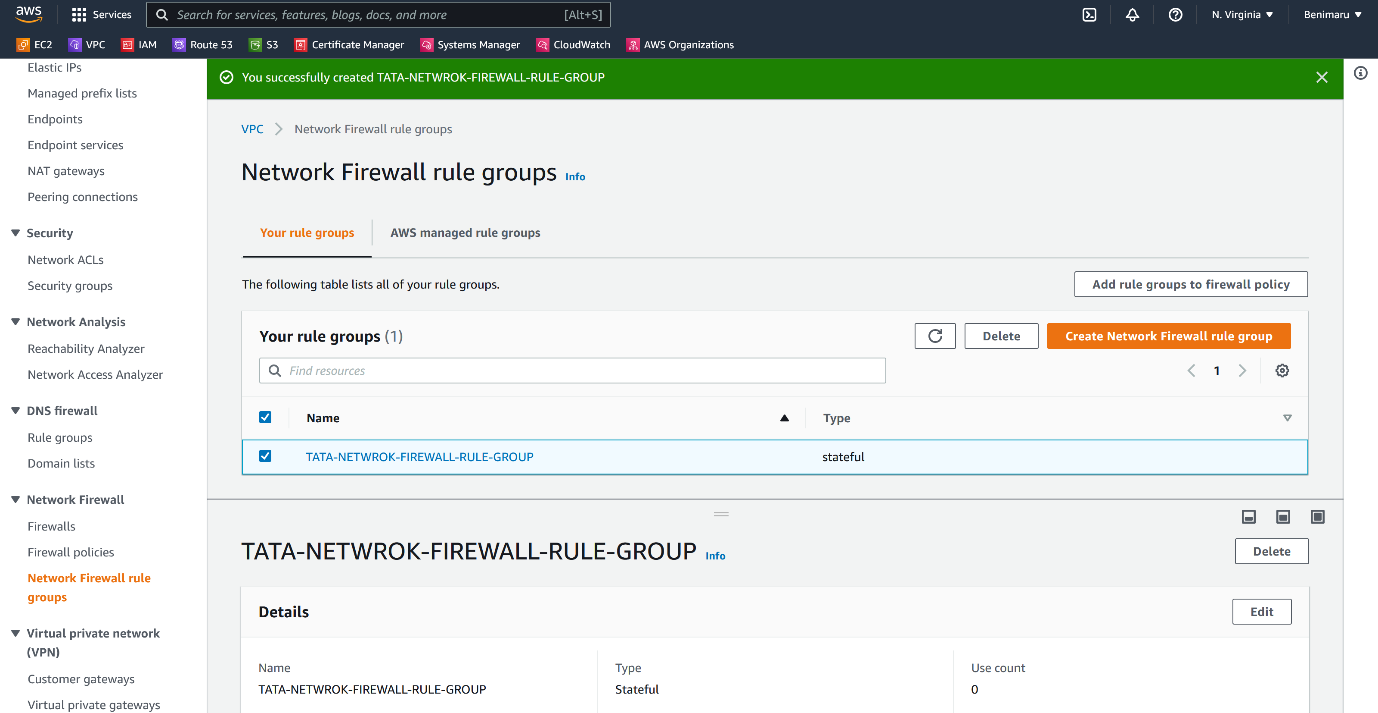
--- click on create network firewall rule group.





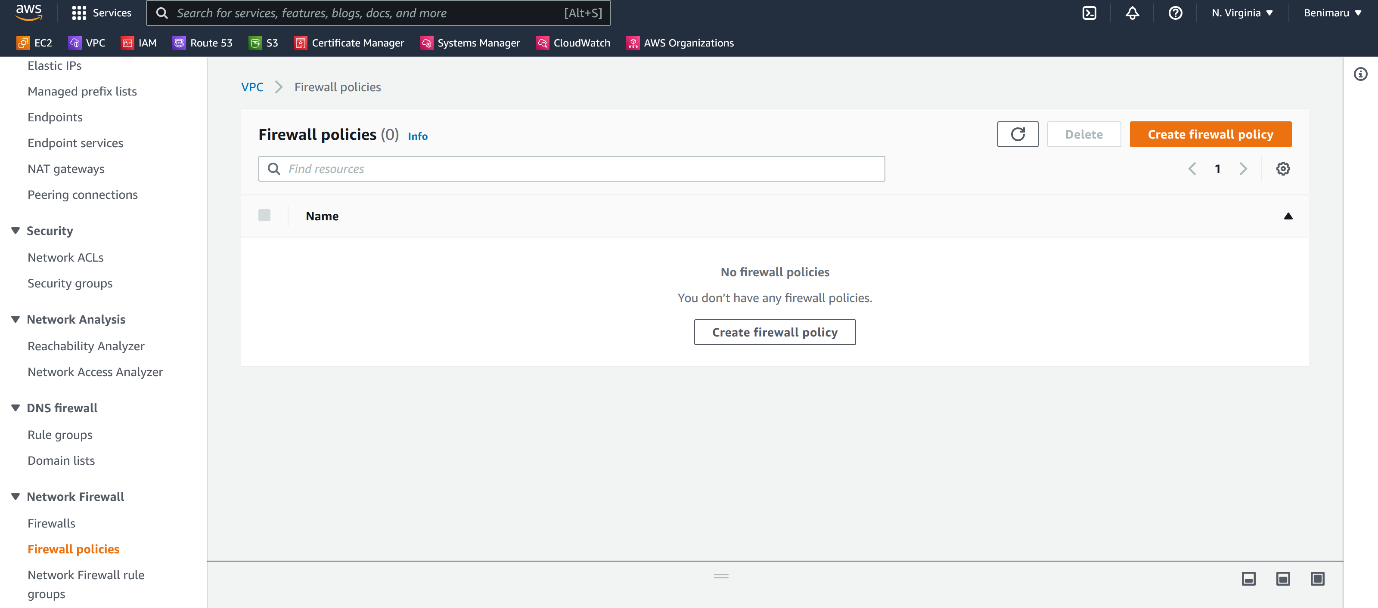


--- Click on create state full rule group.

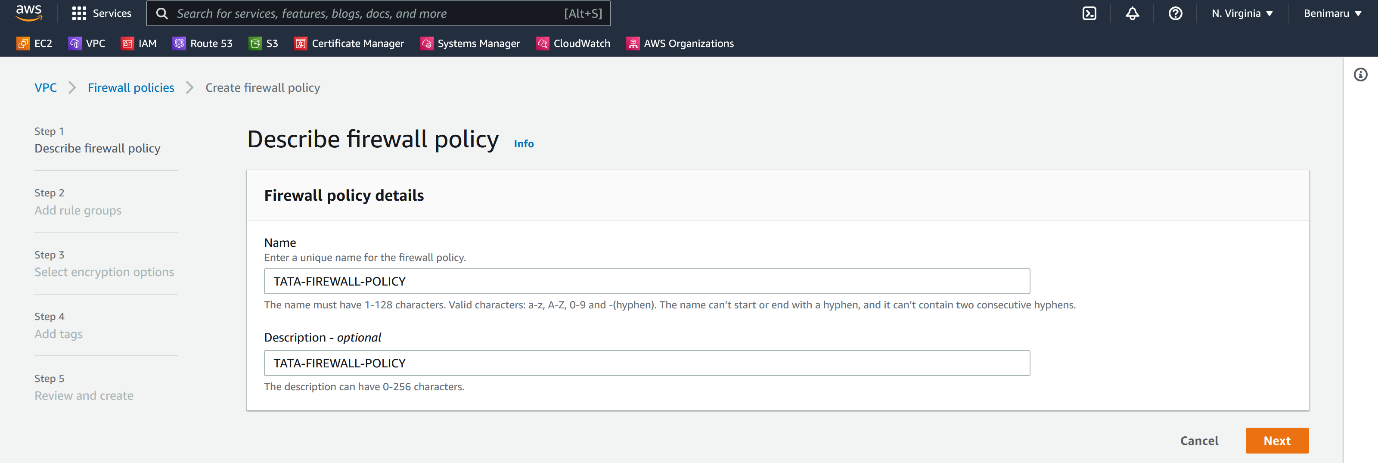


--- **note** – our network firewall rule groups got created.

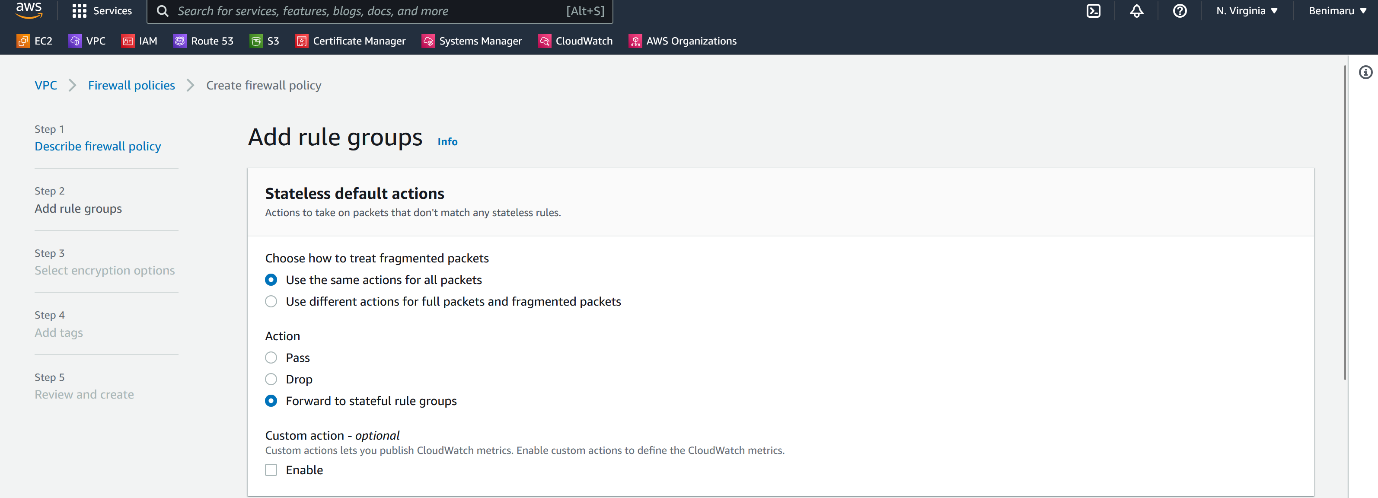
**Firewall policies**

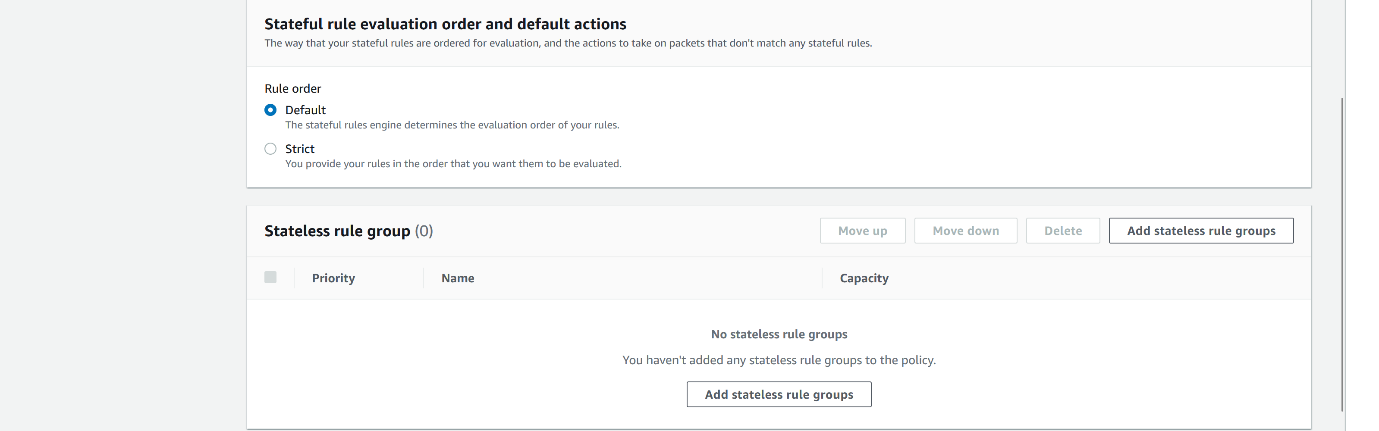


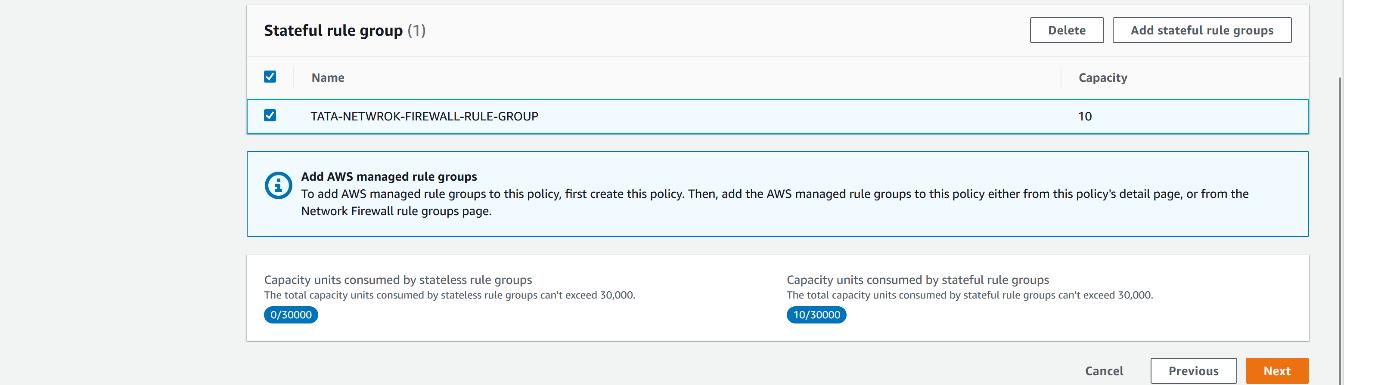
--- click on create firewall policy.



--- Click on next.

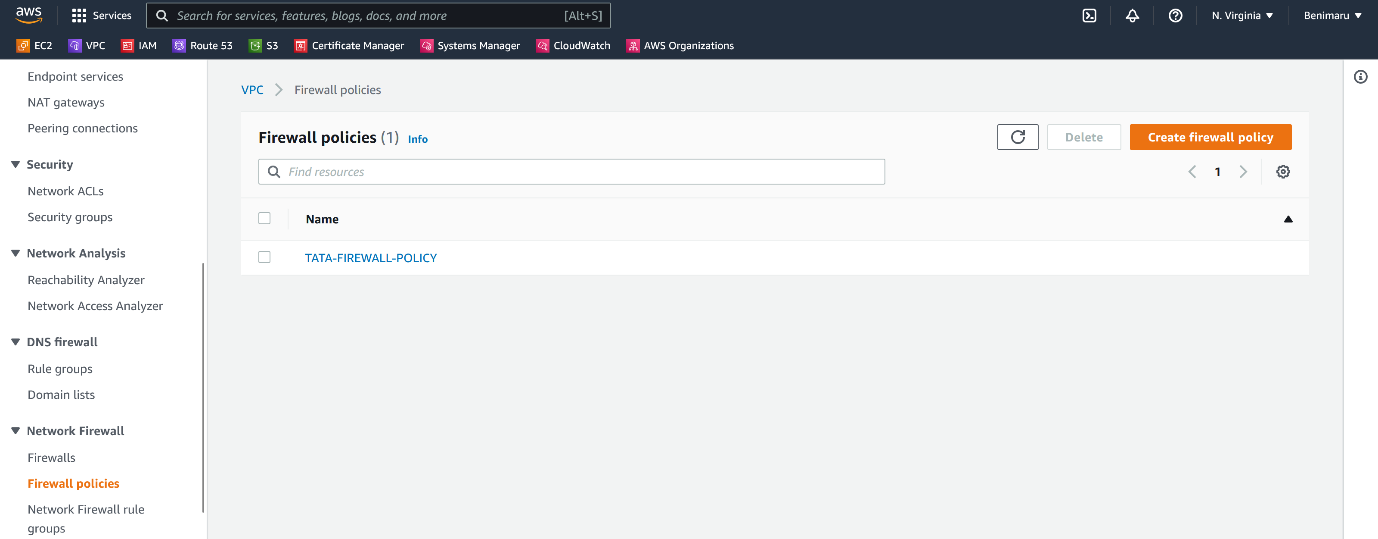






--- click on next.

--- click on create network firewall policy.



--- our firewall policies got created.