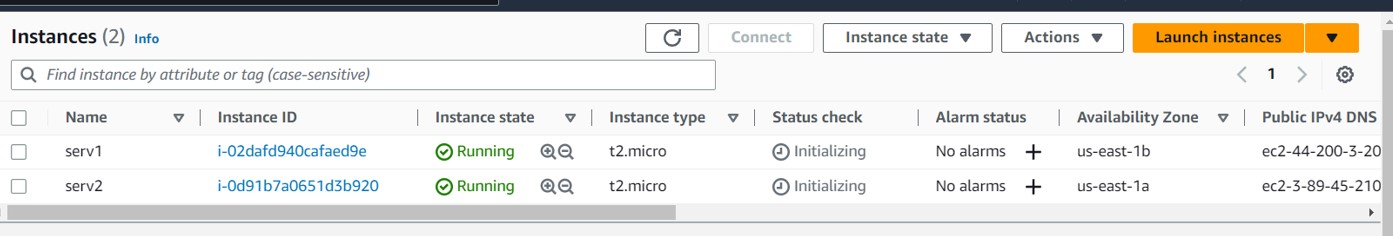
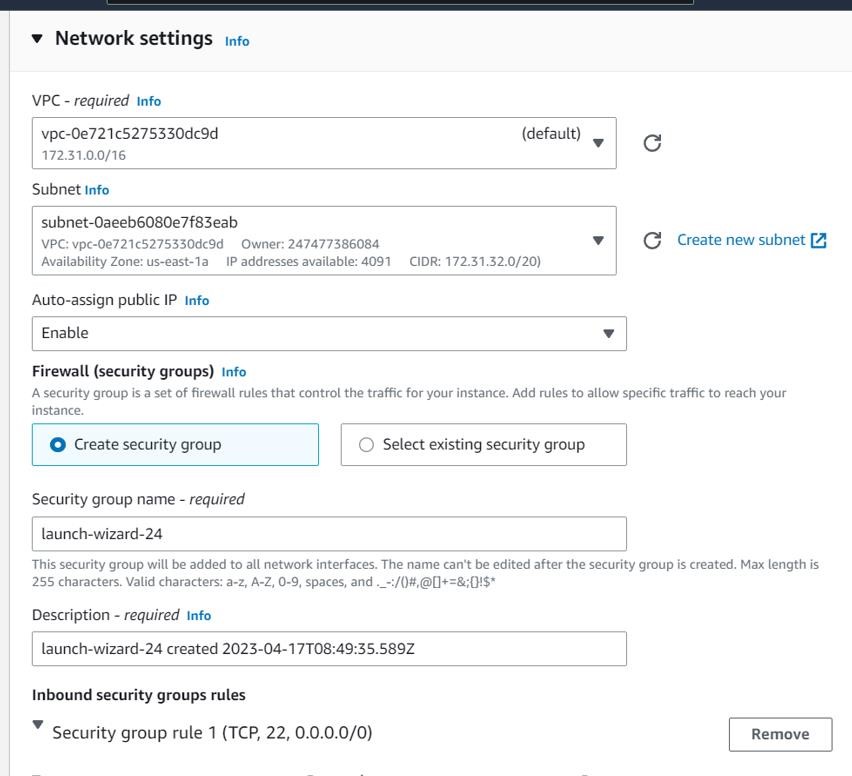
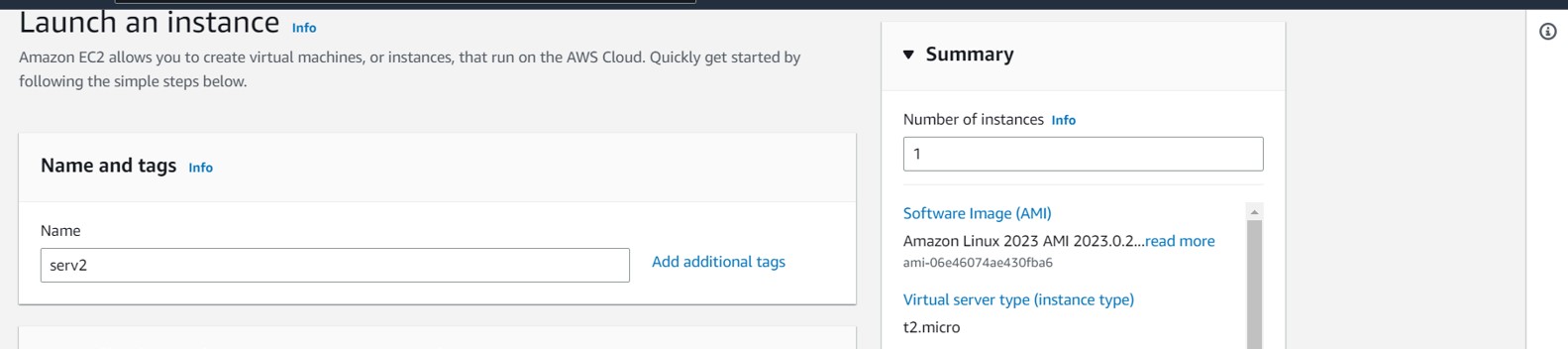
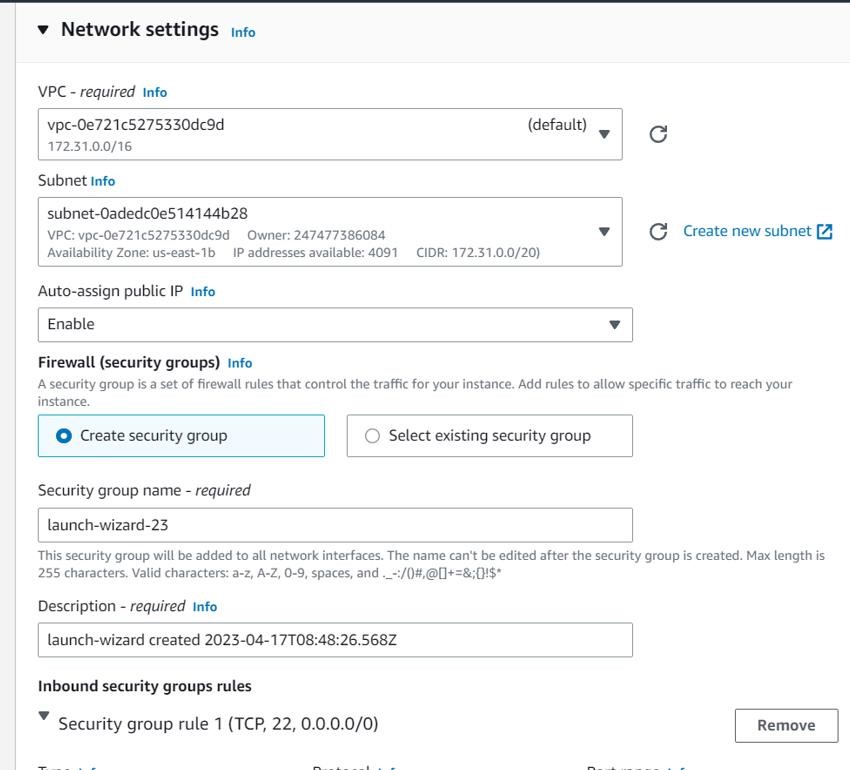
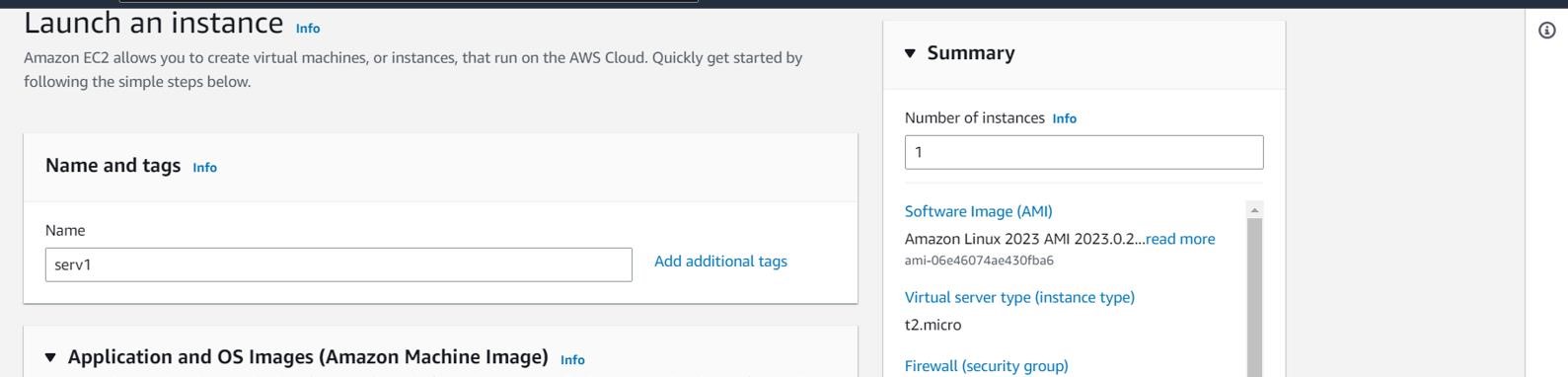
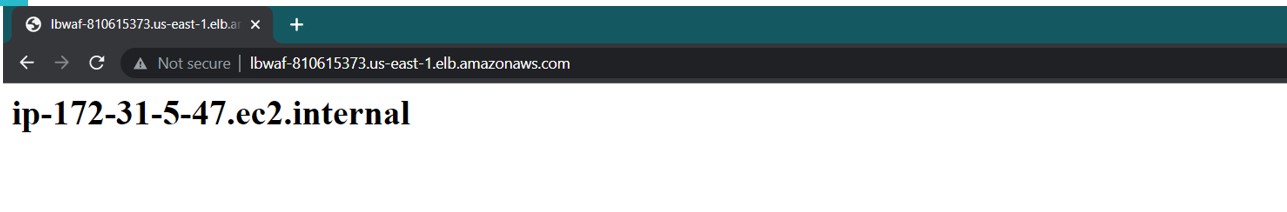
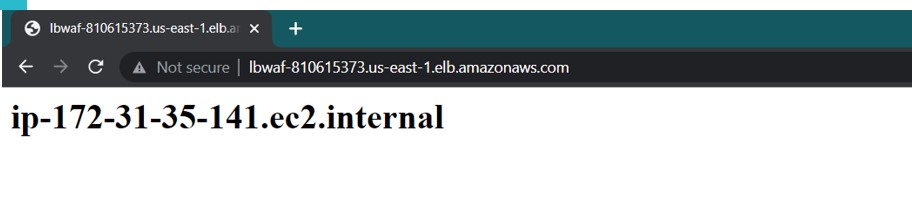
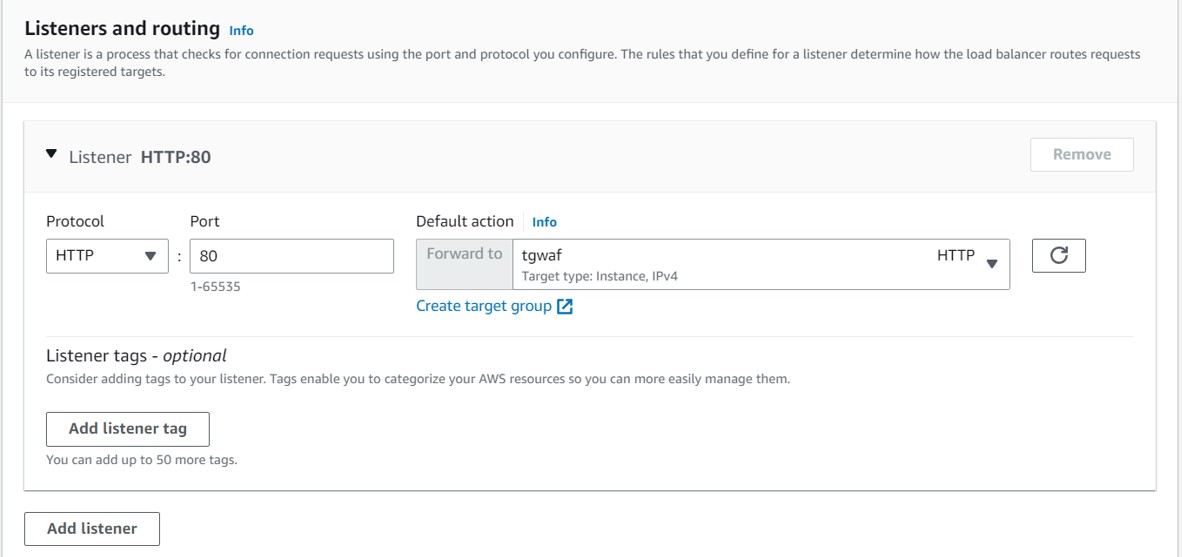
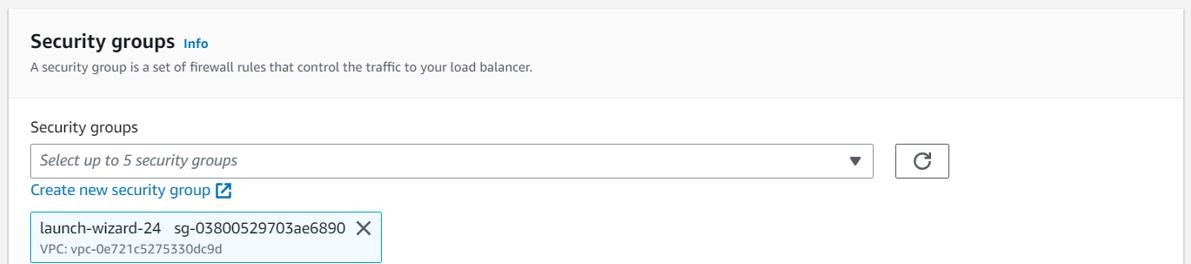
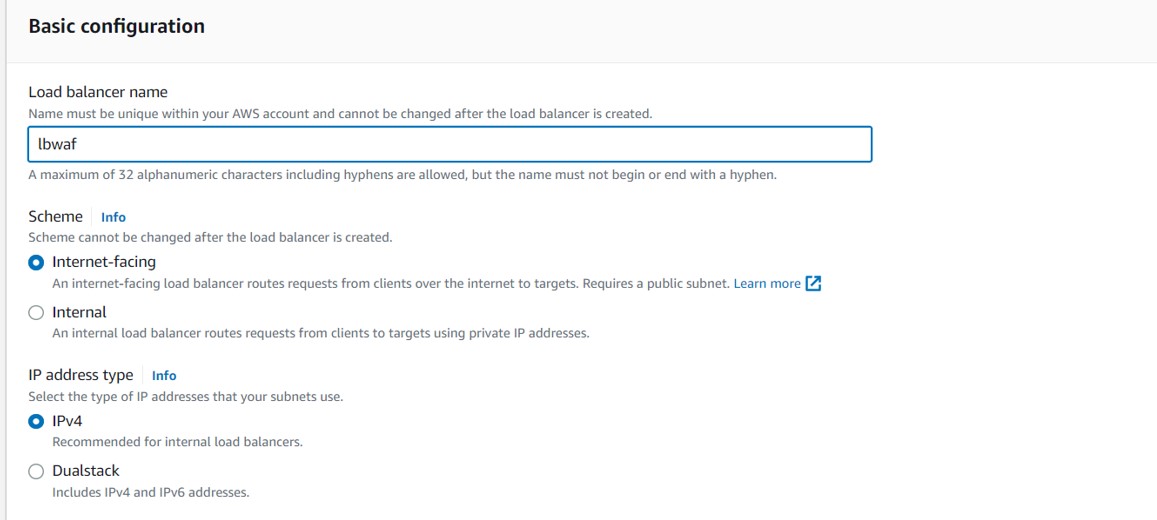
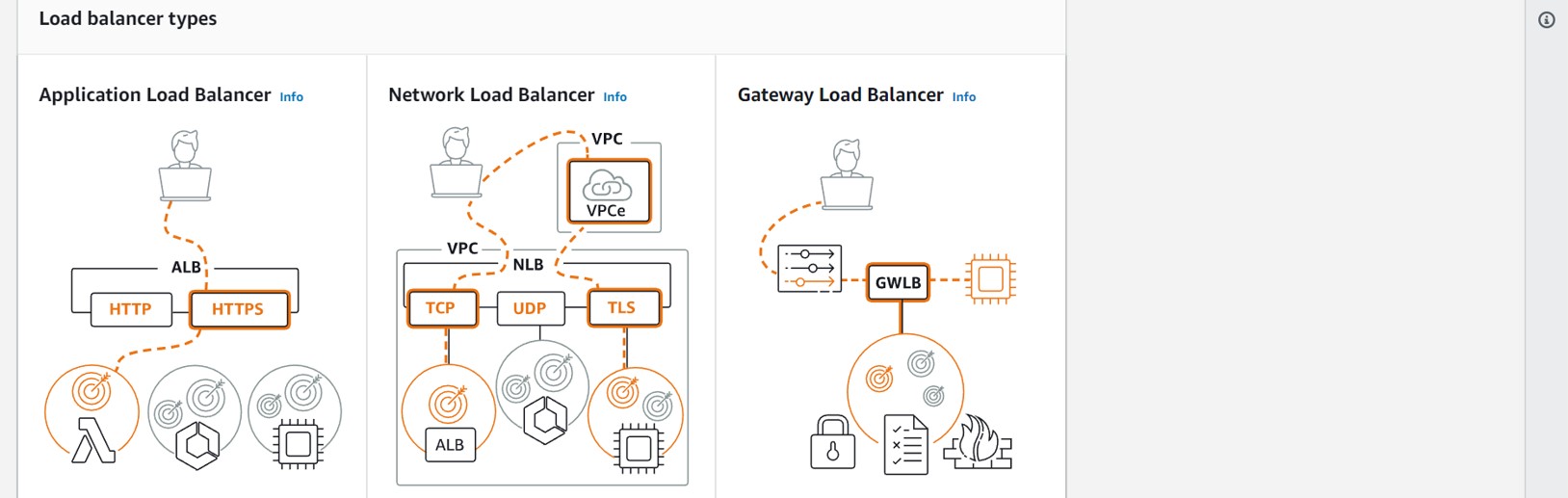
**Experiment-12: AWS Web Application Firewall**

**1.**  Adding a WAF to a Load balancer and blocking access

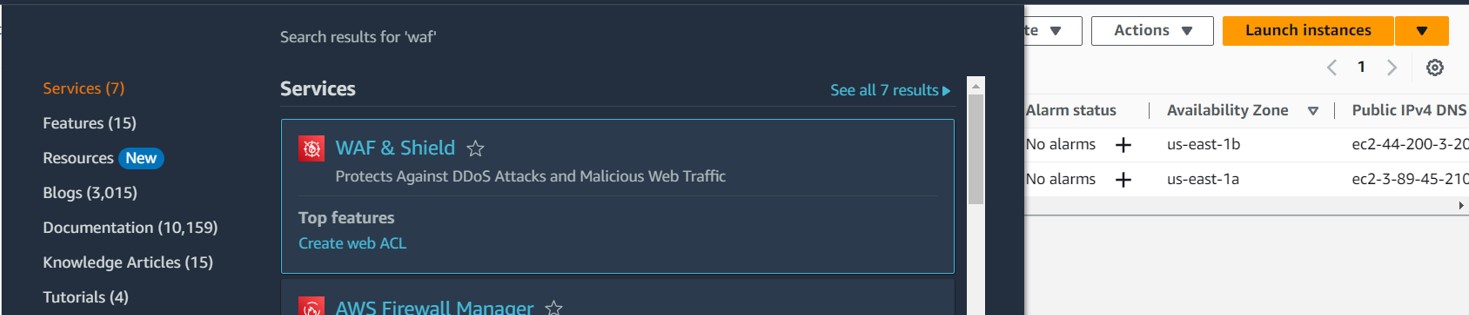
**Step 1:** Login to aws console & create 2 ec2 instances in different azs .

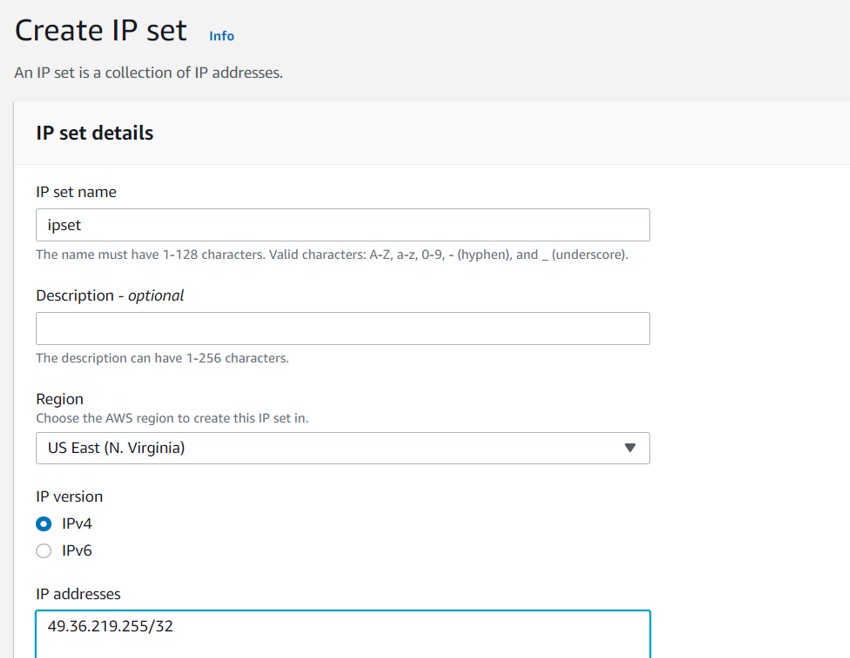
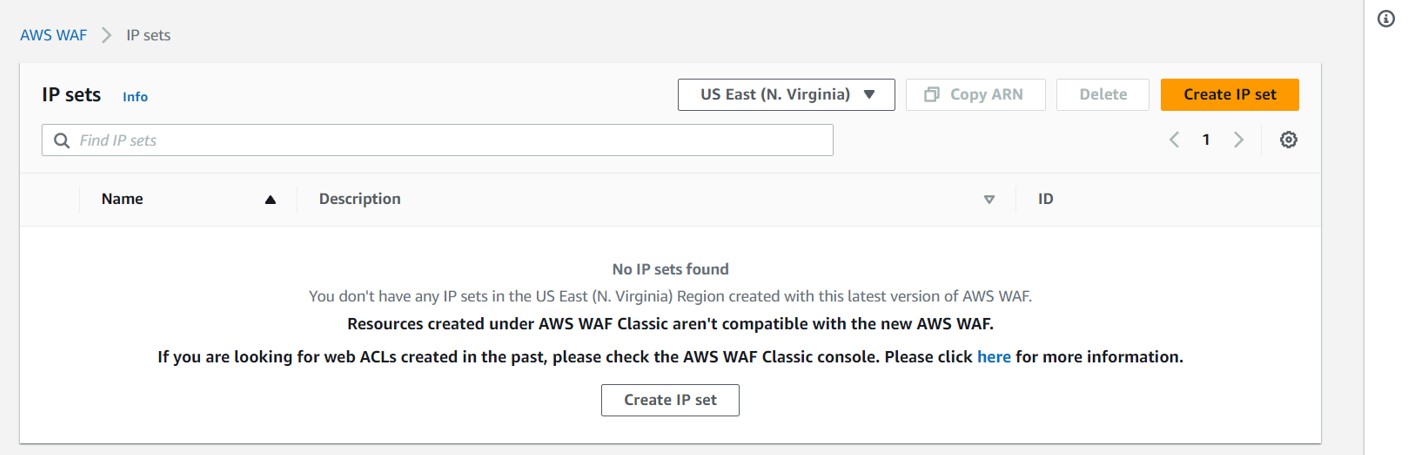


**Step 2:** Goto ec2-> LoadBalancer & add a application lb & check the lb

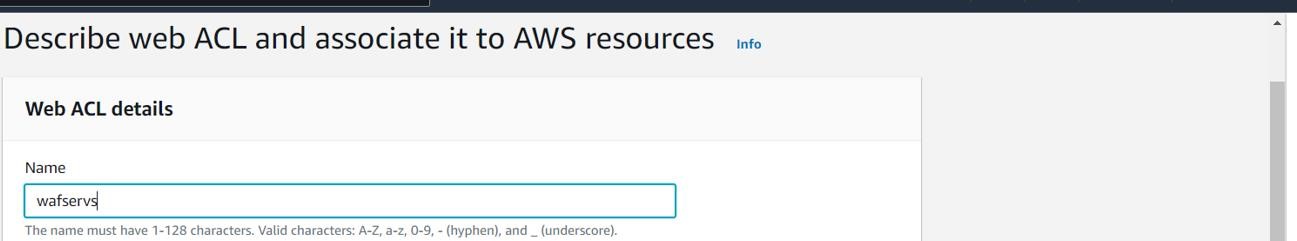


**Step 3 :**Goto WAF -> create ip set

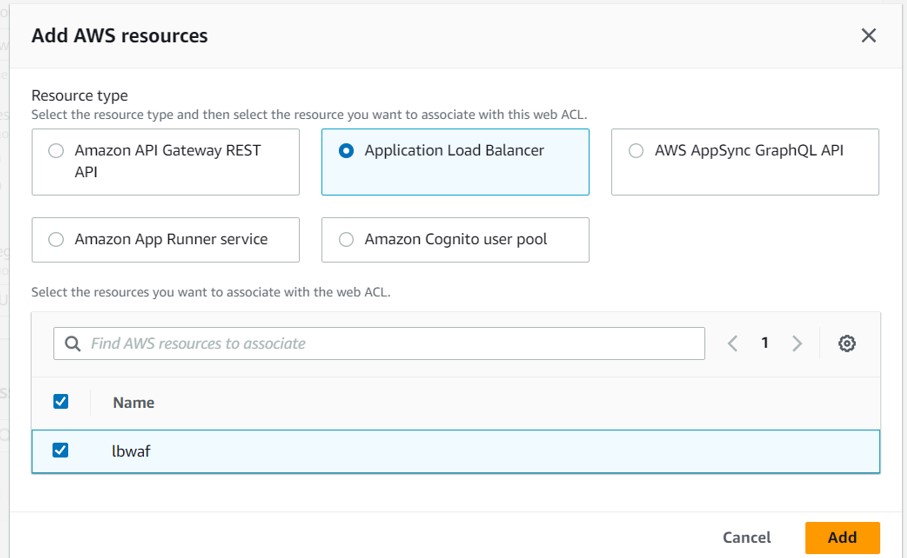




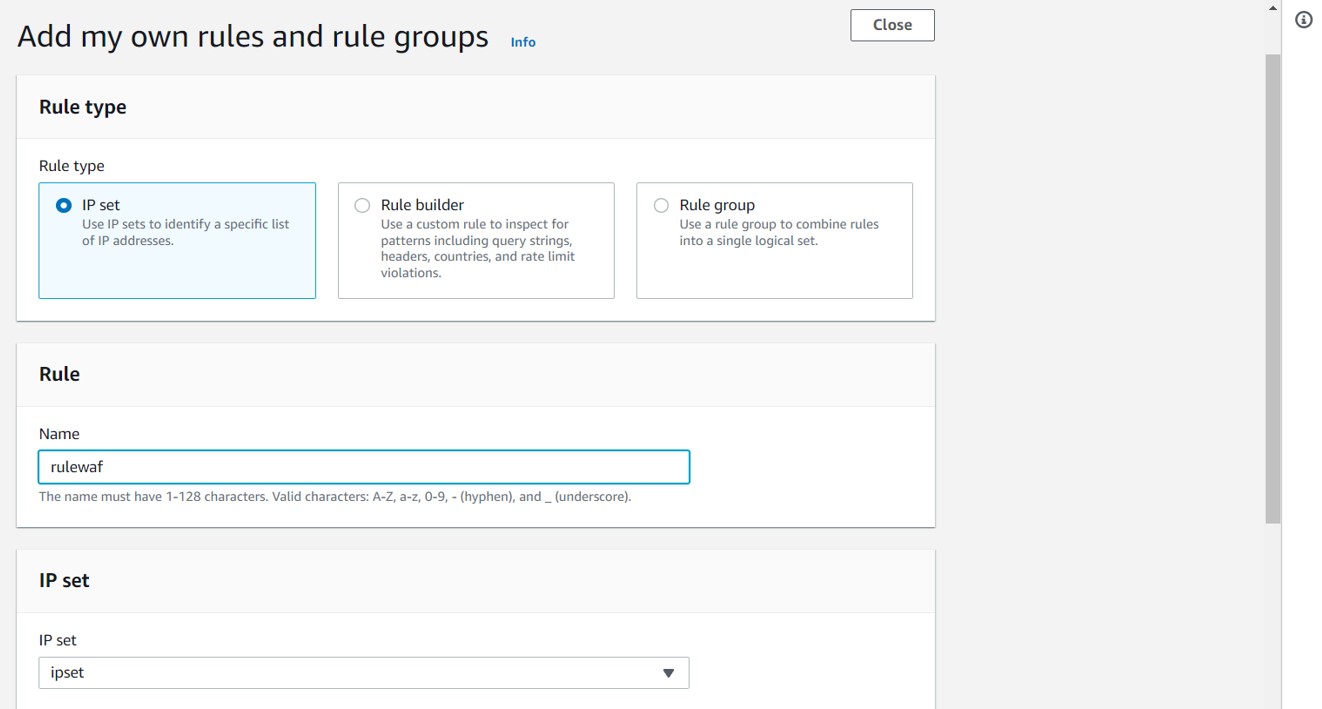
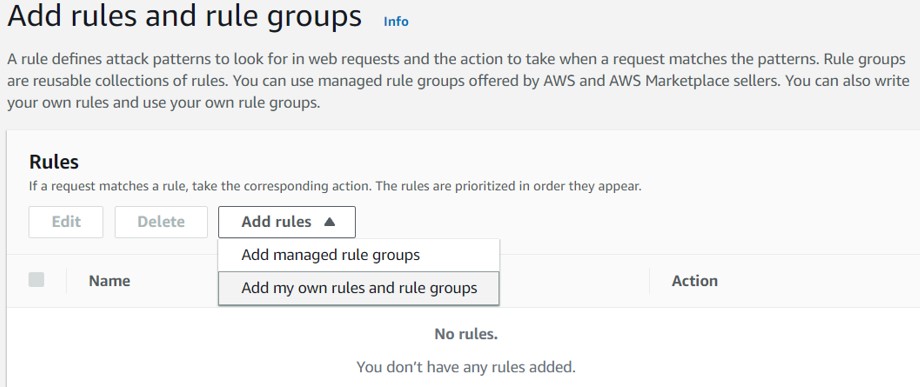
**Step 4 :** Create a web acl by giving name & appropriate configurations



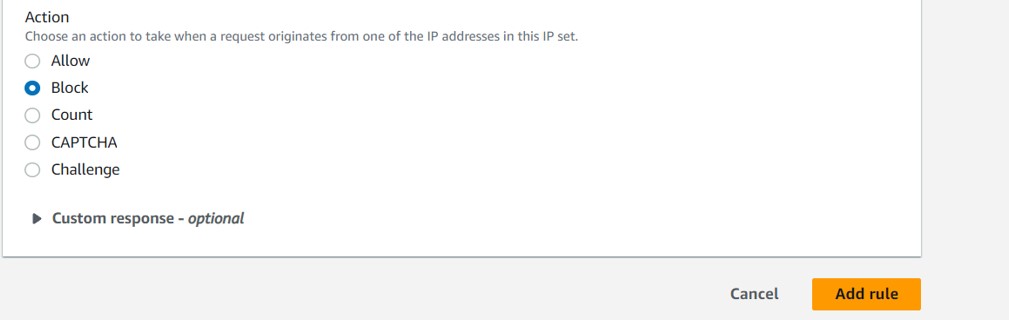
**Step 5 :** Add resources to the web acl (here lb created previously)



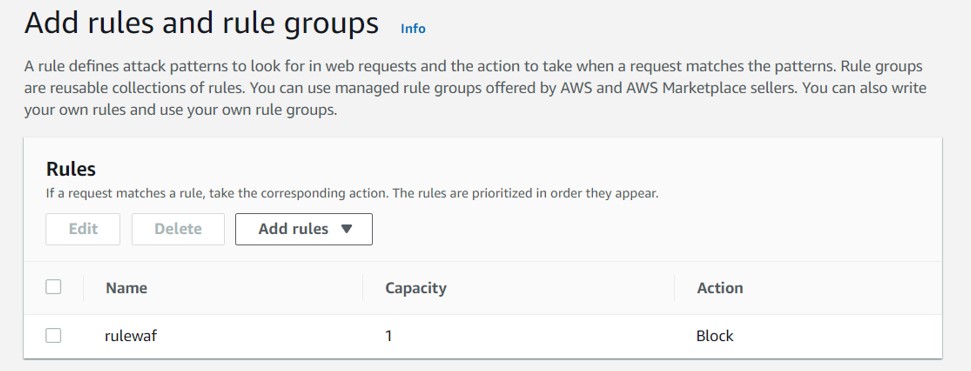
**Step 6:** In the rules & rule groups , add the ipset



**Step 7**: Under Action use the “block” action



**Step 8:** Click add rule



**Step 9:** Review and create the web acl



**Step 10:** Access the lb by its DNS



**Step 11:** If you change the action in step 7 to CAPTCHA , an authentication step is added

