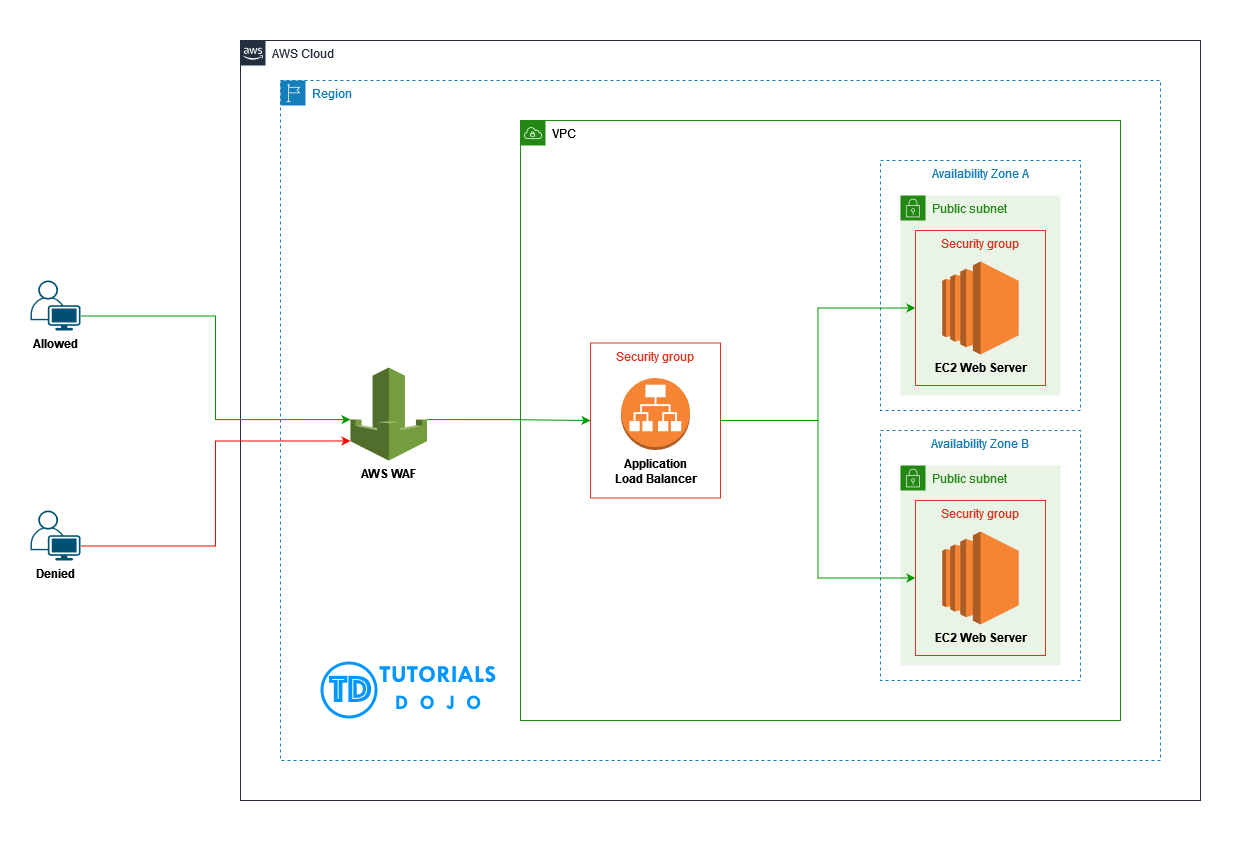
AWS WAF

**AWS WAF Implementation with ALB and EC2 in a Custom VPC**

## **Introduction**

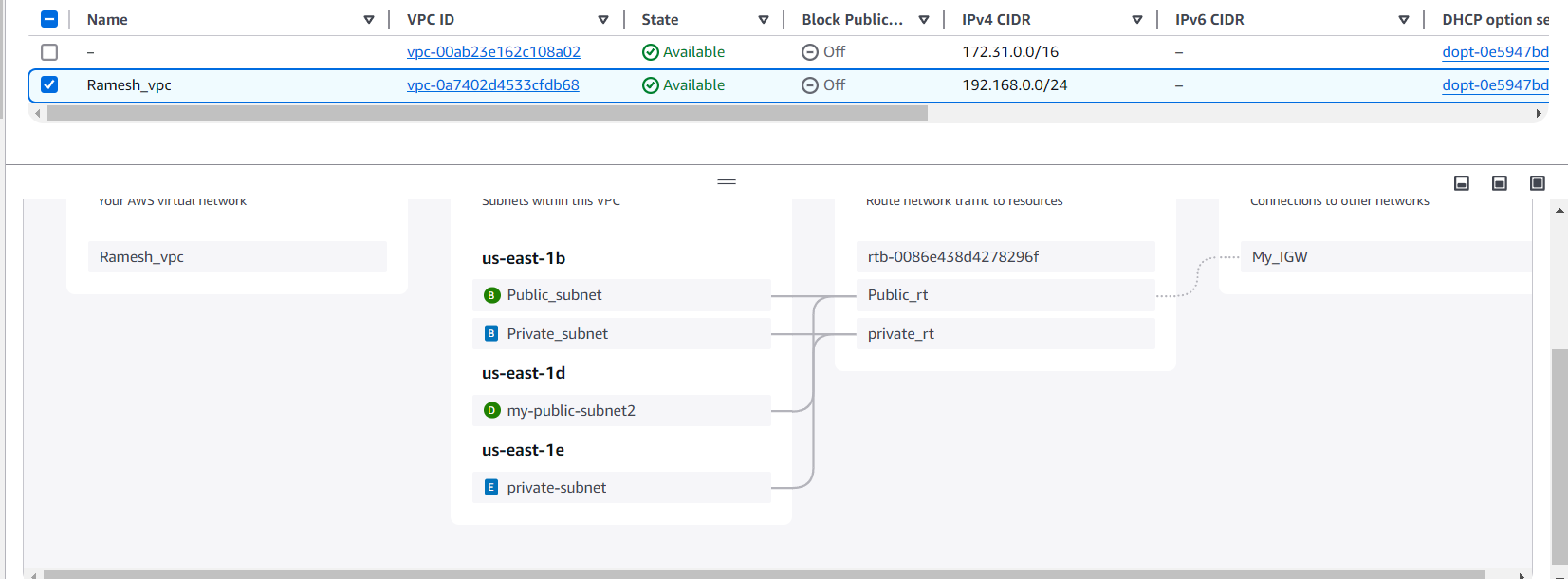
AWS Web Application Firewall (WAF) helps protect web applications from common threats such as SQL injection, cross-site scripting (XSS), and unauthorized access. This document explains the step-by-step implementation of AWS WAF with an Application Load Balancer (ALB) in a custom VPC, including rule configurations and testing.



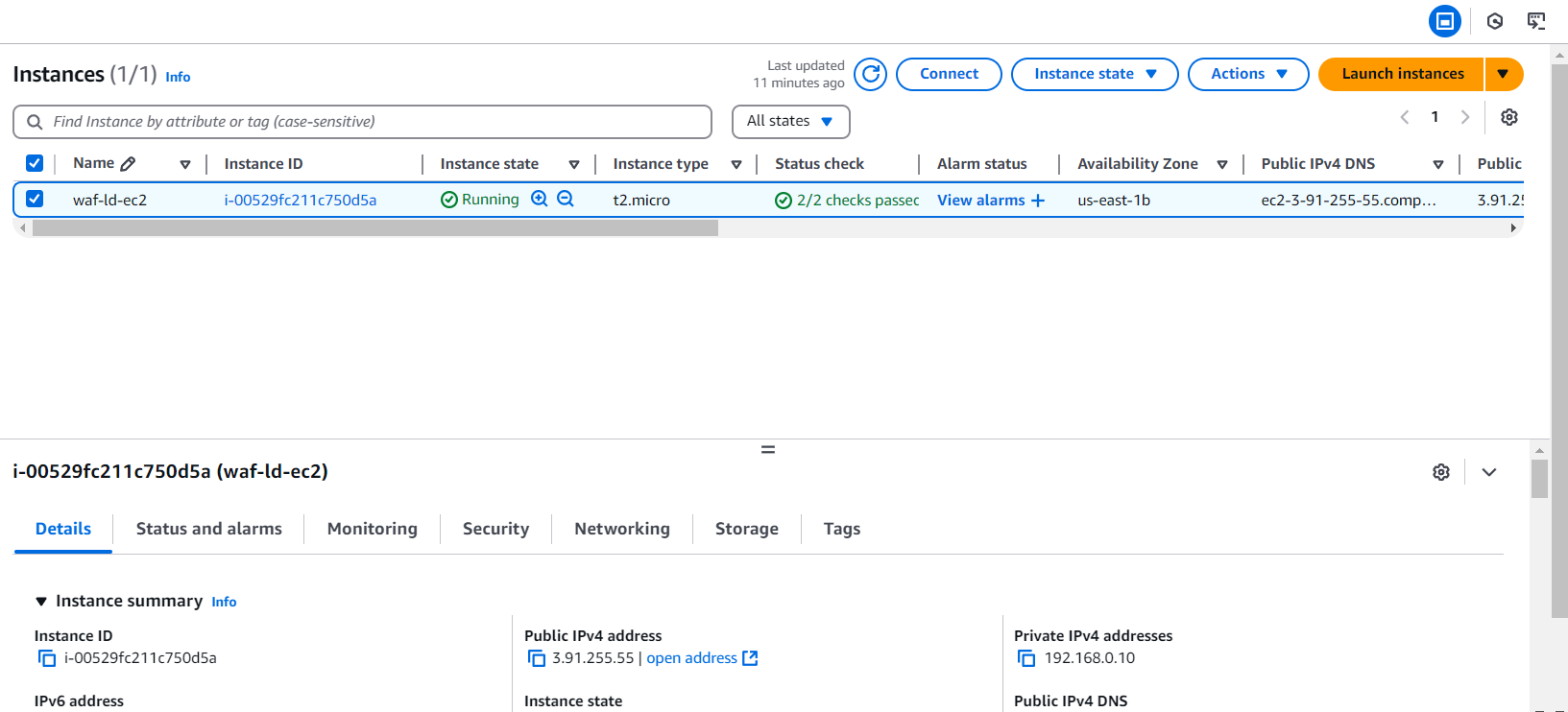
## **teps to Implement AWS WAF with ALB**

### **1. VPC and EC2 Setup**

1. **Create a Custom VPC**
   * Navigate to the AWS VPC console.
   * Create a new VPC with a custom CIDR range.
   * Configure subnets and route tables as needed.

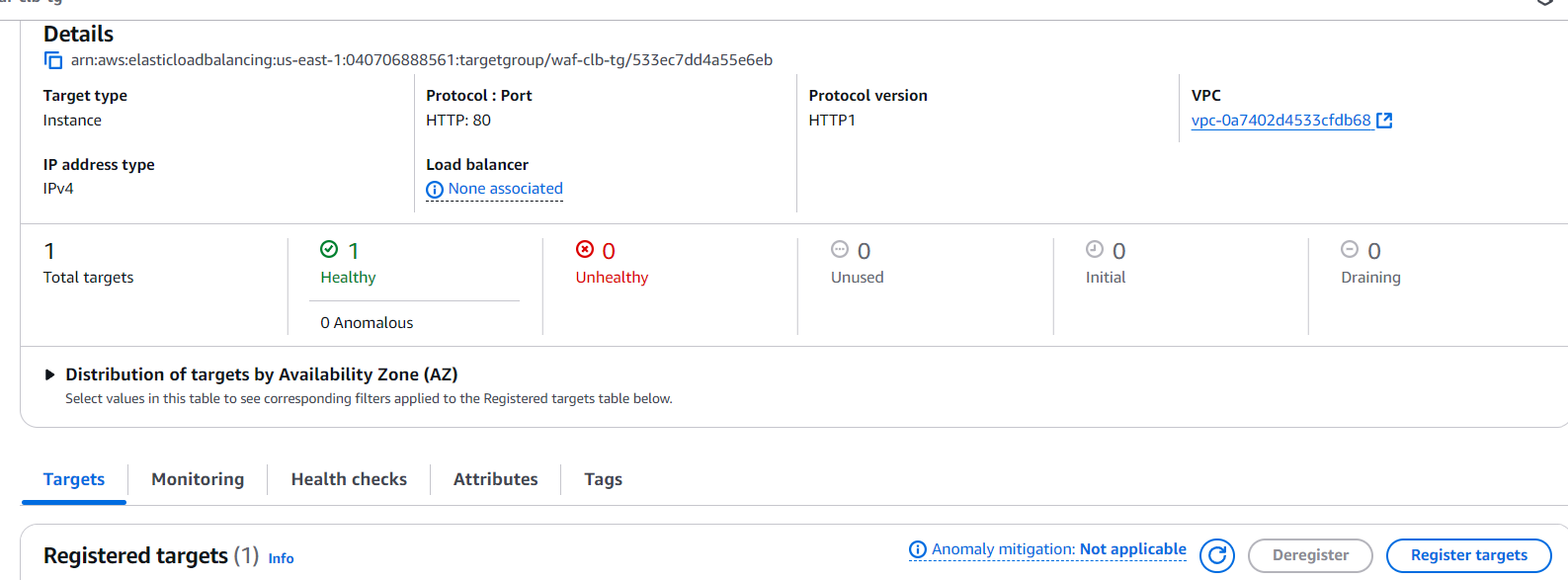


I have launched one ec2-instance with my own VPC and install apache and sample application

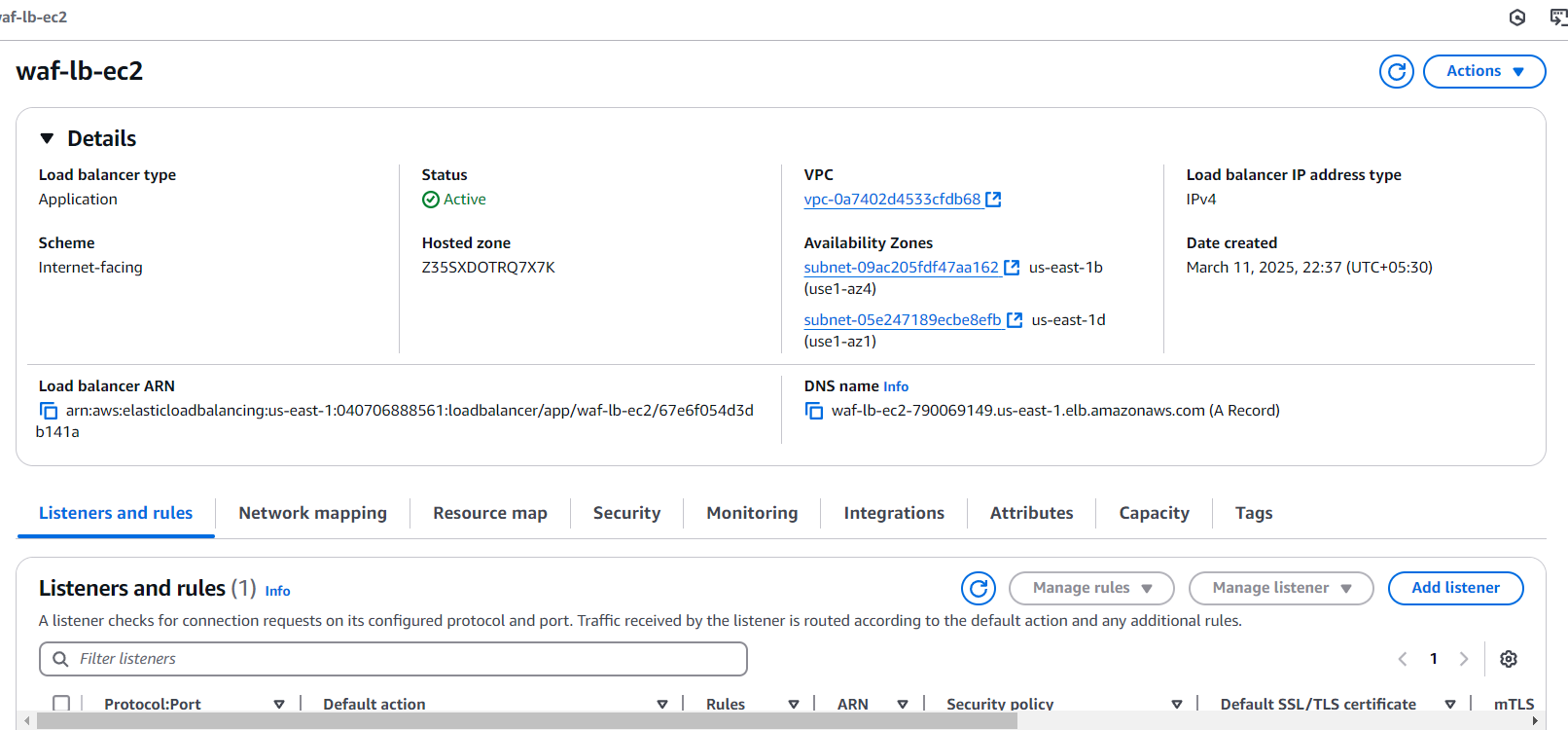


### **2. Create a Target Group and ALB**

1. **Create a Target Group**
   * Navigate to the EC2 Load Balancer Target Group section.
   * Create a new target group with the appropriate health check path (e.g., /index.html).
   * Register the EC2 instance to this target group.
2. **Create an Application Load Balancer (ALB)**
   * Navigate to the Load Balancer section in EC2.
   * Create an ALB and associate it with the VPC.
   * Attach the target group to the ALB.
   * Allow HTTP traffic in the ALB security group.

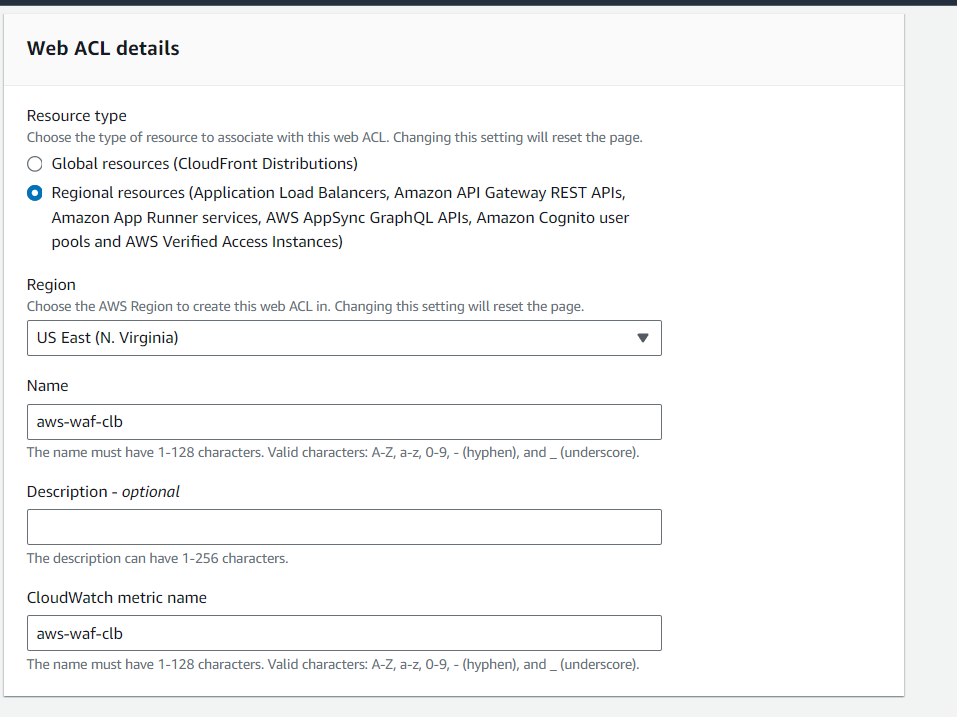


I have create a ALB with my own Vpc and attached my server also

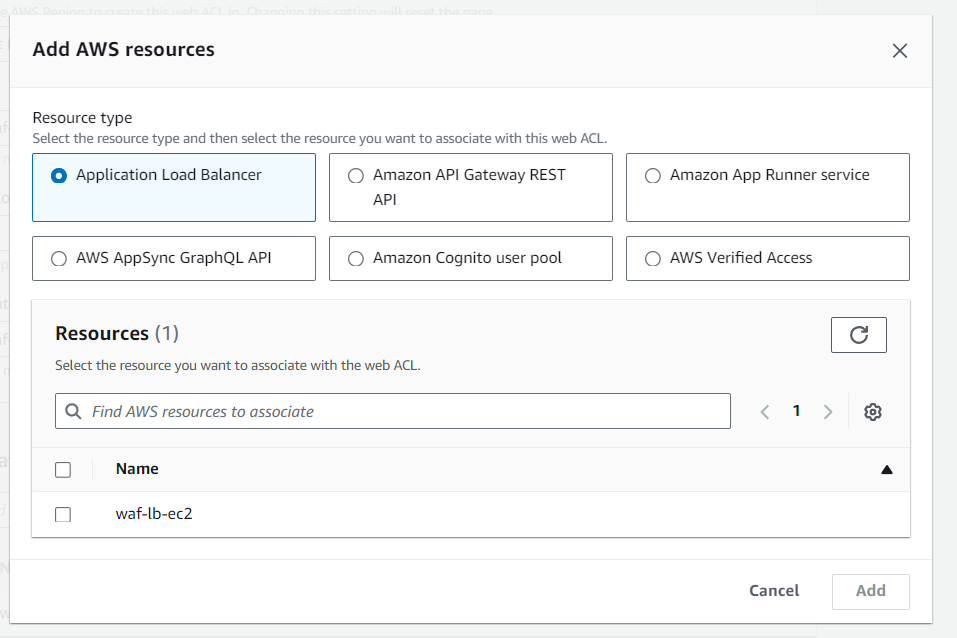


### **3. Configure AWS WAF**

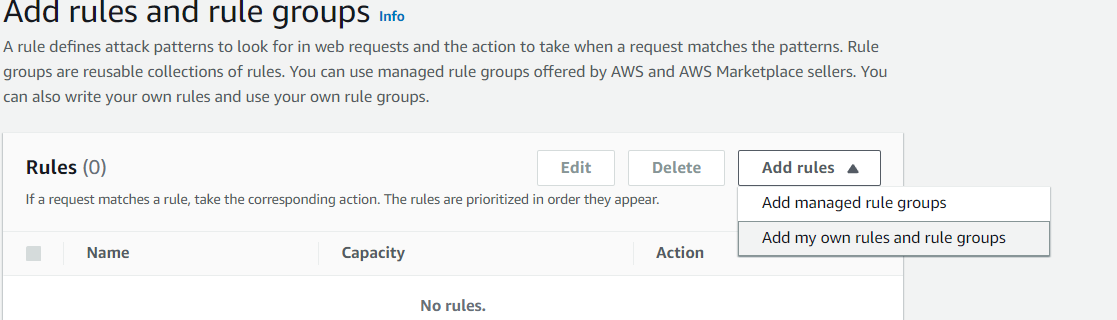
1. **Create a Web ACL**
   * Navigate to AWS WAF & Shield service.
   * Create a Web ACL and associate it with the ALB.
2. **Add Rules to the Web ACL**
   * Configure custom rules as per the security requirements.
   * Example rules:
     + **IP Blocking Rule**: Block or allow specific IP addresses.
     + **Rate-based Rule**: Limit excessive requests from a single IP.
     + **CAPTCHA Rule**: Require human verification for certain requests.
3. **Add a Rule to Block Specific IPs**
   * Choose the rule type as "IP Set".
   * Add your IP and configure the action to **Block**.
   * Save the rule and add it to the Web ACL.



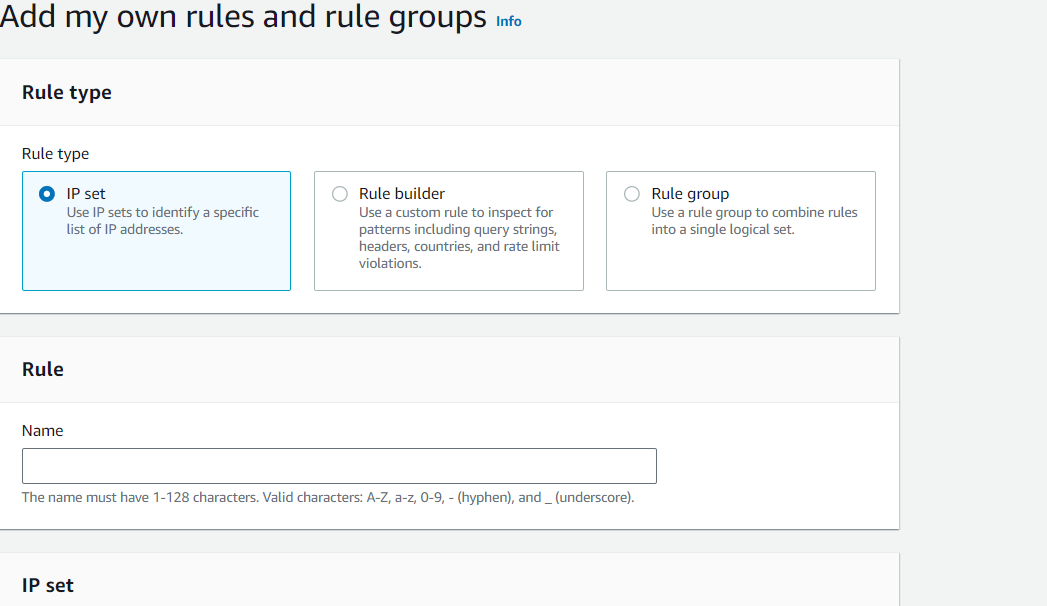
Add AWS Resources with different resources and I chose the ALB

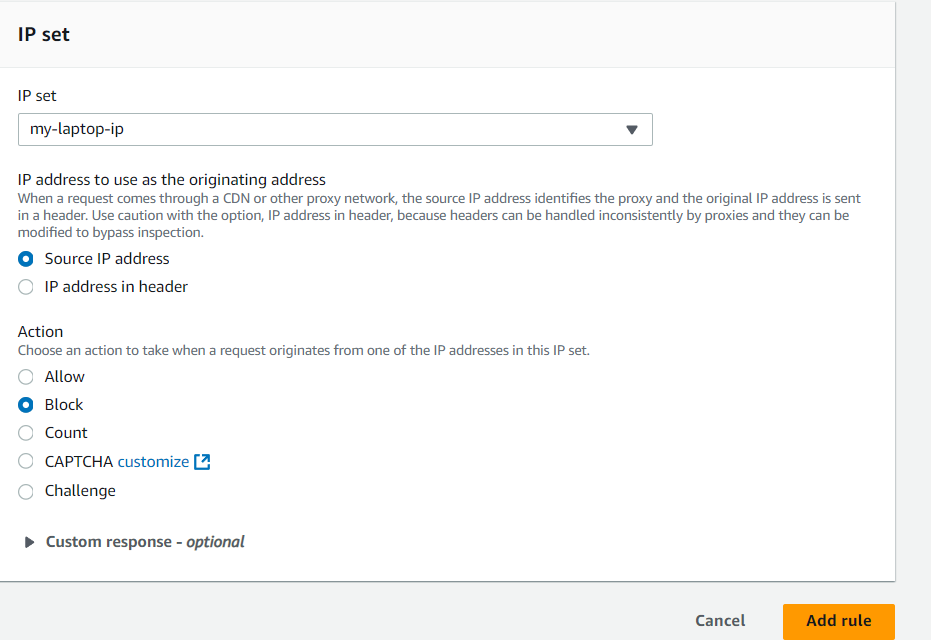


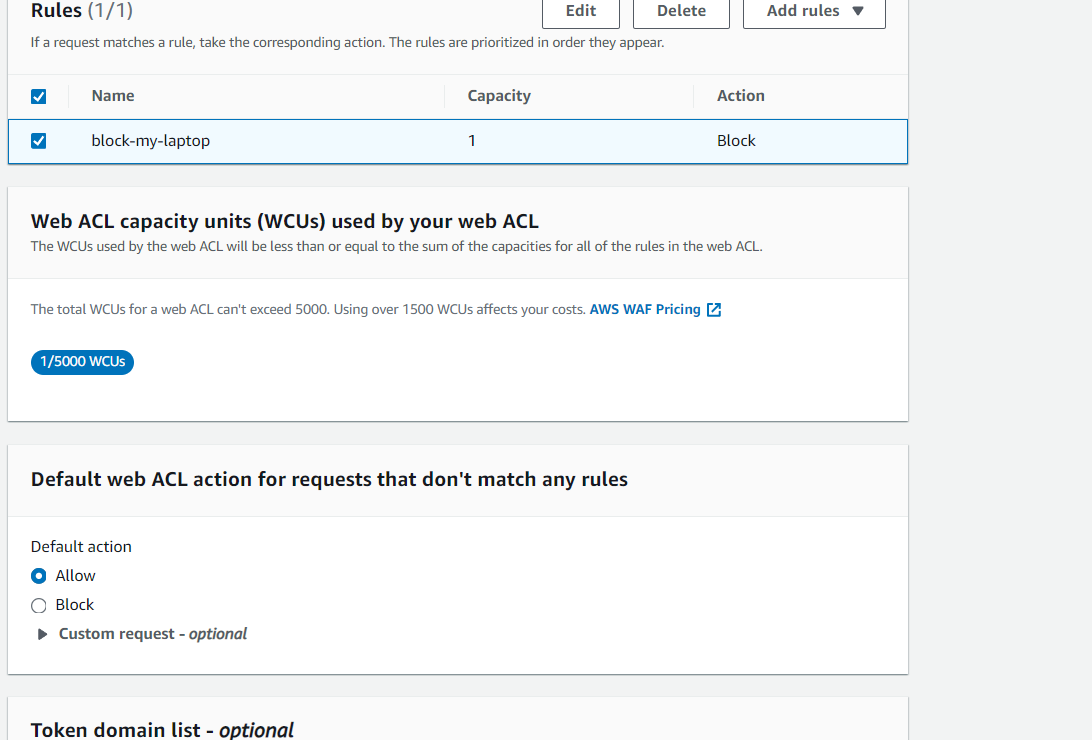
We have to add rules we can add our own rules and groups

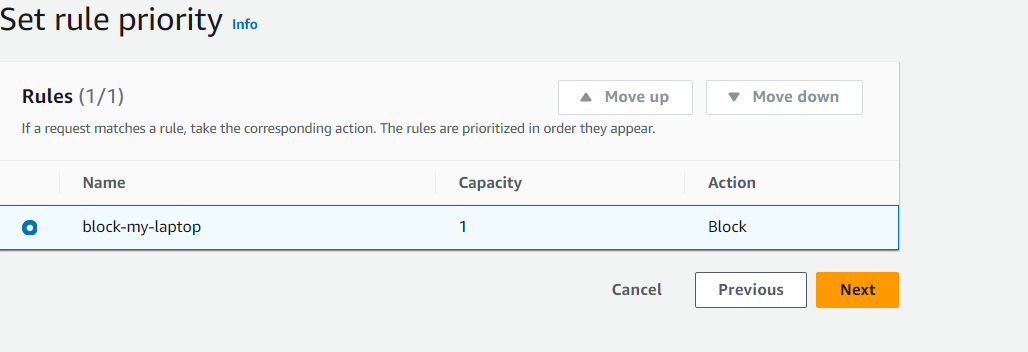


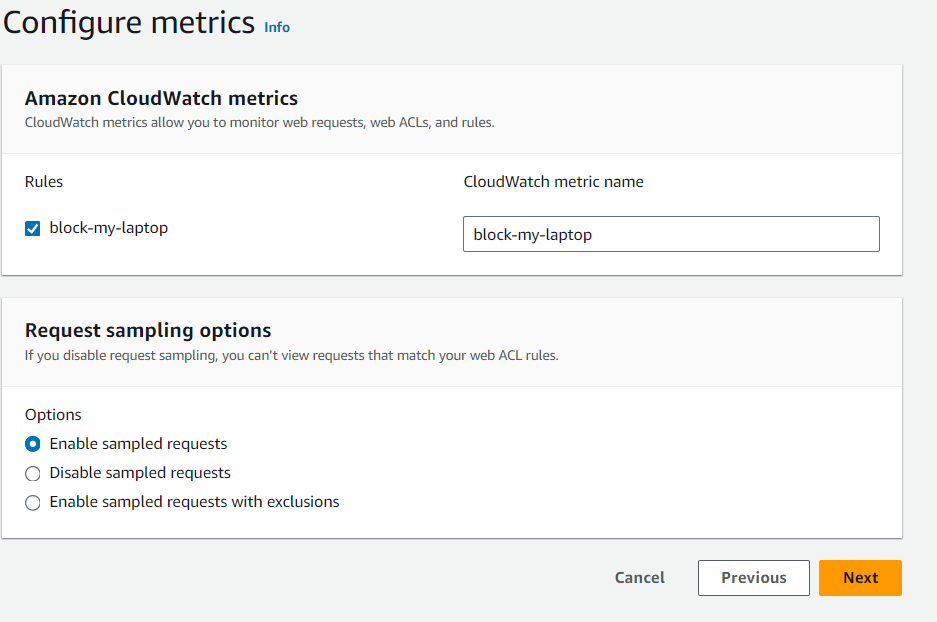
I have chosen My IP in Rule type





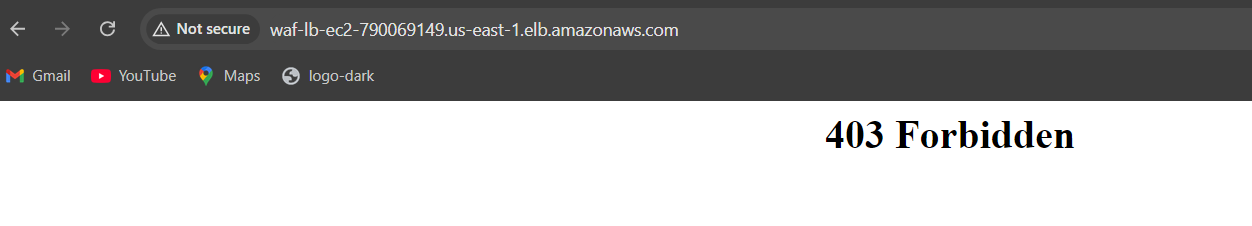




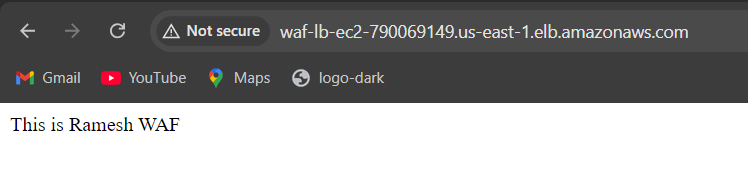


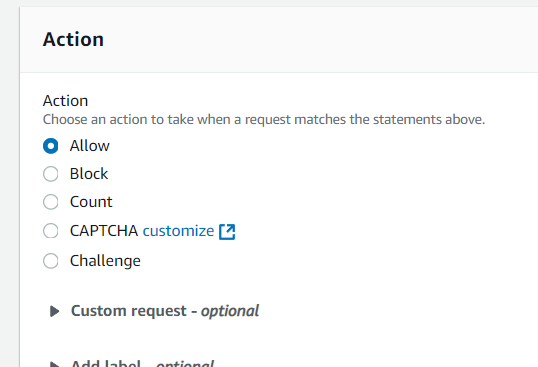
### **4. Testing AWS WAF Configuration**

1. **Validate Blocking Rule**
   * Attempt to access the ALB from the blocked IP.
   * Expect a 403 Forbidden error.

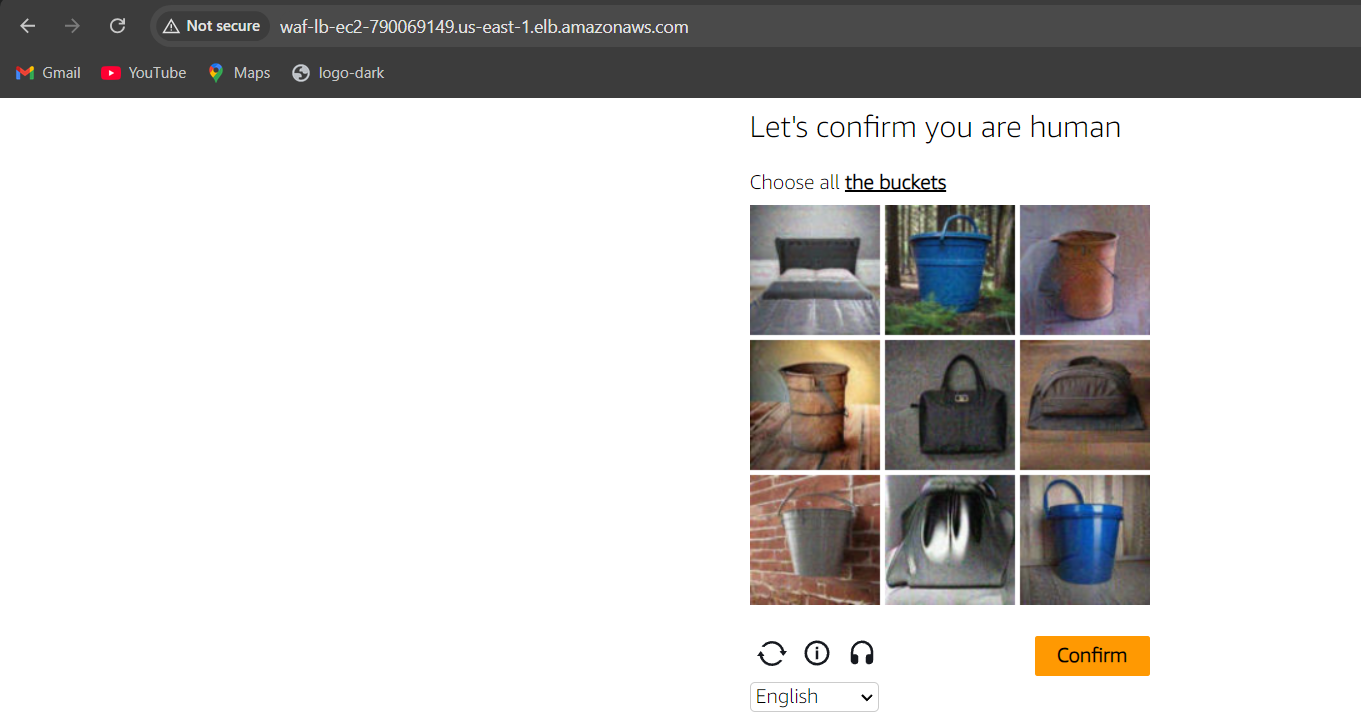


After changing Allow my rule i got the output of my ALB





You can see after adding the capacha it will ask the human verification



### **Conclusion**

AWS WAF provides a robust security mechanism to protect web applications hosted on AWS. By setting up Web ACLs, adding custom rules, and enabling CAPTCHA, we can ensure better security and control over incoming traffic. The testing steps confirm that the WAF rules work as expected, providing an effective security layer.