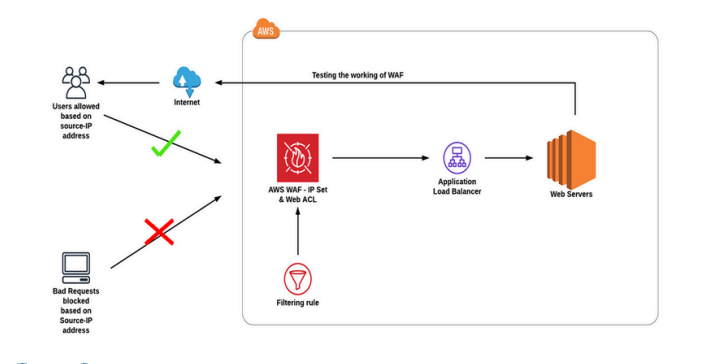
**Lab 9: Block Web Traffic with WAF in AWS**

**Objective:**

Learn to secure web applications by blocking traffic with AWS WAF.

**Architectural Diagram:**



**Steps:**

* Deploy servers in separate Availability Zones.
* Set up an Application Load Balancer.
* Set up WAF with IP sets and a web ACL, then test its effectiveness.

**Step-by-Step Instructions:**

**Step 1: Launch EC2 Instances**

1. **Create Two EC2 Instances**:
   * Go to the **EC2 Console** > **Launch Instances**.
   * Deploy two instances in different **Availability Zones** of the same region.

**Step 2: Create a Target Group**

1. Go to the **EC2 Console** > **Target Groups** > **Create target group**.
2. With Given Details.

**Step 3: Create the Load Balancer**

1. Go to **Load Balancers** > **Create Load Balancer** > **Application Load Balancer**.
2. Associate the previously created **target group**.
3. Confirm the ALB is functioning:
   * Retrieve the ALB's DNS name and test in your browser. It should alternate responses from the two servers.

**Step 4: Create an IP Set**

1. Go to the **WAF Console** > **IP Sets** > **Create IP Set**.
2. Configure:
   * Name: blocked-ip-set.
   * Region: Match your ALB's region.
   * Add IP addresses to block (e.g., 203.0.113.0/24).

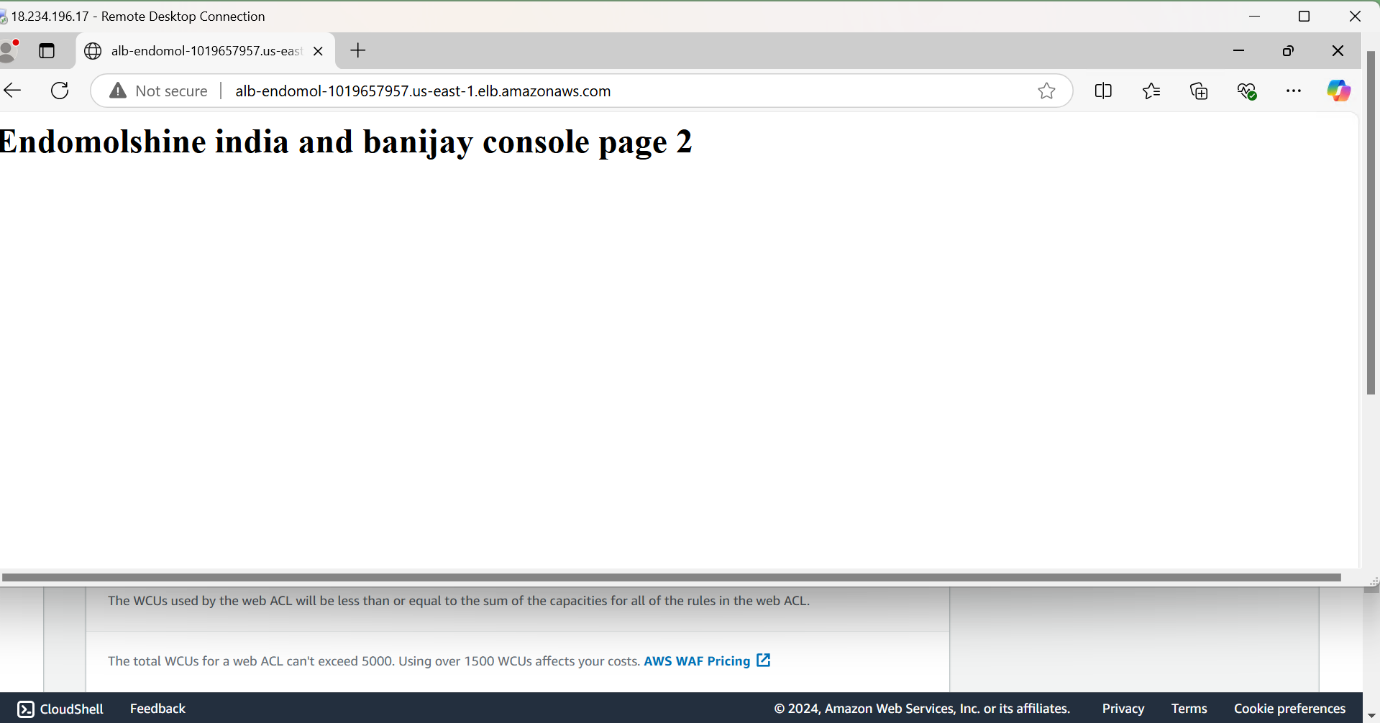
**Step 5: Create a Web ACL**

1. In the **WAF Console**, go to **Web ACLs** > **Create Web ACL**.
2. Configure:
   * Name: web-acl.
   * Region: Match your ALB's region.
   * Resource Type: **Application Load Balancer**.
   * Associate the ALB created earlier.
3. Add a Rule:
   * Rule Type: IP Set.
   * Name: block-specific-ips.
   * Action: Block.
   * Select the blocked-ip-set.
4. Save and activate the Web ACL.

**Test the WAF Effectiveness**

**Step 1: Verify Normal Access**

1. Use a device **not in the blocked IP set** to access the ALB’s DNS name.
   * Expected: You should see the web server responses.



**Step 2: Simulate Blocked Access**

1. Use a device with an IP address in the blocked-ip-set to access the ALB’s DNS name.
   * Expected: Access should be blocked with a 403 Forbidden error.

