# AWS WAF Setup Using ALB (Application Load Balancer) with S3 Logging

## ✨ Objective

Protect your EC2 instance using AWS WAF by placing an **Application Load Balancer (ALB)** in front of it. Configure WAF logging to an S3 bucket and test the protection using Linux commands.

## 🚀 Architecture Overview

User Request --> ALB --> EC2 Instance  
 | ^  
 v |  
 WAF Apache Web Server  
 |  
 v  
 Logs to S3

## ✅ Prerequisites

* A running EC2 instance (Amazon Linux 2)
* Elastic IP: 34.228.138.219
* Public DNS: ec2-34-228-138-219.compute-1.amazonaws.com

## 🔢 Step-by-Step Setup

### ✅ Step 1: Prepare the EC2 Web Server

SSH into your instance and set up a web server:

sudo yum update -y  
sudo yum install -y httpd  
sudo systemctl start httpd  
sudo systemctl enable httpd  
echo "WAF ALB Test Page" | sudo tee /var/www/html/index.html

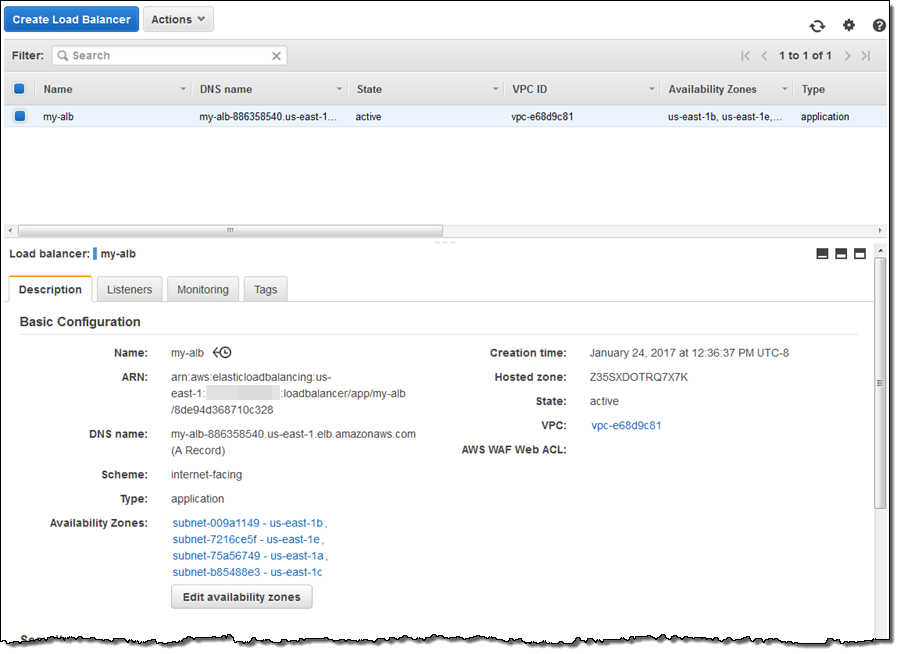
Test locally:

curl http://localhost

### ✅ Step 2: Create a Target Group

1. Go to **EC2 > Target Groups**
2. Click **Create target group**
   * Type: Instances
   * Protocol: HTTP
   * Port: 80
   * Target group name: waf-target-group
3. Register your EC2 instance
4. Click **Create target group**

### ✅ Step 3: Create an Application Load Balancer (ALB)

1. Go to **EC2 > Load Balancers**
2. Click **Create Load Balancer > Application Load Balancer**
3. Name: waf-alb
4. Scheme: Internet-facing
5. IP address type: IPv4
6. Listeners: Add HTTP:80
7. Availability Zones: Select one with your EC2
8. Target group: Select waf-target-group

After creation, note the **DNS name** of the ALB.

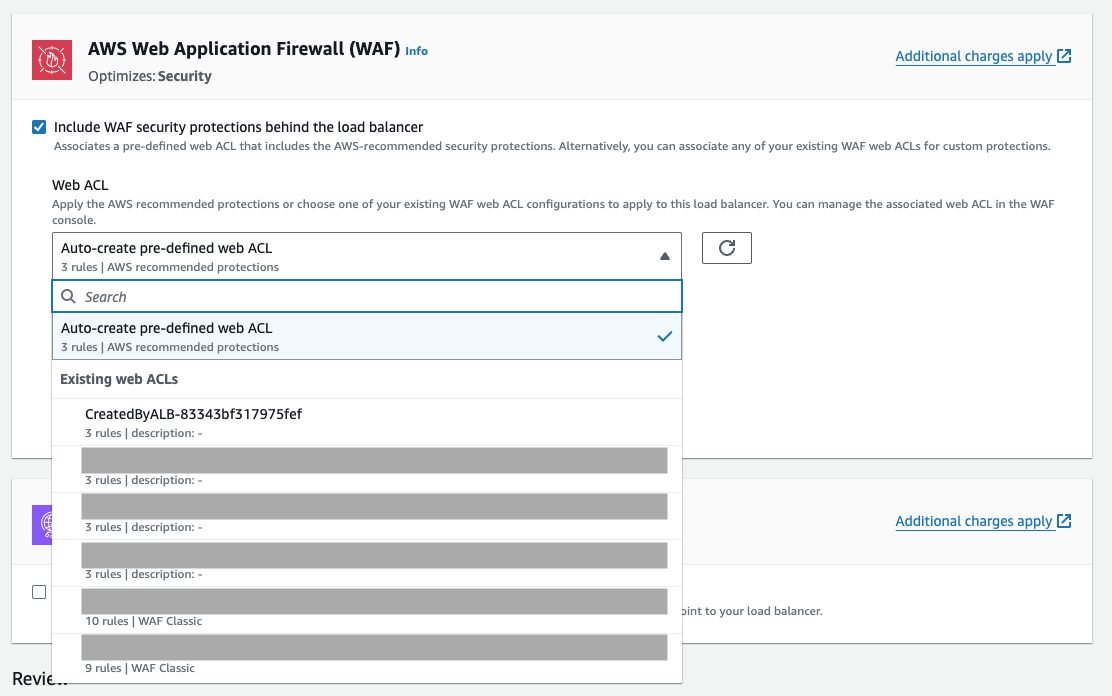
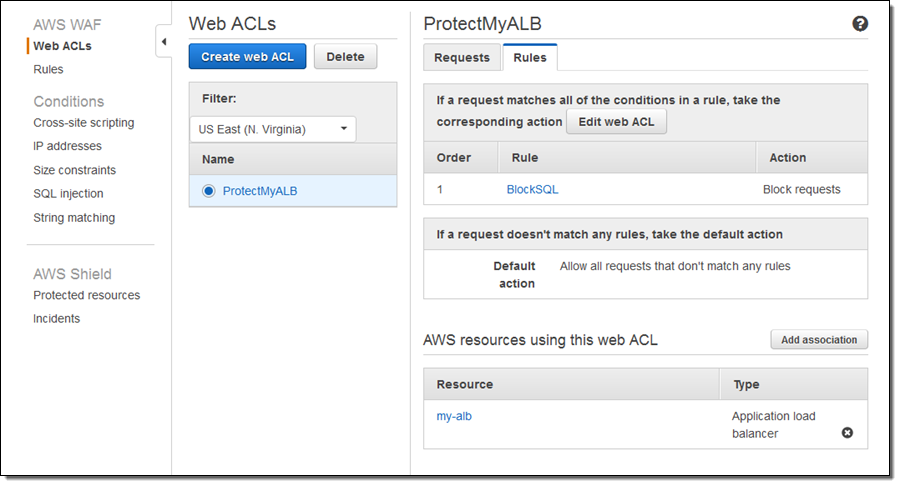
### ✅ Step 4: Create S3 Bucket for WAF Logs

1. Go to **S3 > Create Bucket**
   * Name: waf-alb-logs-bucket
   * Region: same as ALB
2. Disable “Block all public access”
3. Enable ACLs
4. Click **Create bucket**

**Bucket Policy:**

{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Principal": {  
 "Service": "waf.amazonaws.com"  
 },  
 "Action": "s3:PutObject",  
 "Resource": "arn:aws:s3:::waf-alb-logs-bucket/AWSLogs/\*"  
 }  
 ]  
}

### ✅ Step 5: Create Web ACL and Attach to ALB

1. Go to **AWS WAF > Web ACLs > Create web ACL**
   * Name: TestWebACL
   * Region: us-east-1 (same as ALB)
   * Resource Type: **ALB**
2. Associate with your **ALB**
3. Add managed rule groups:
   * AWSManagedRulesCommonRuleSet
   * AWSManagedRulesSQLiRuleSet  
       
     
4. Set default action: Allow
5. Enable Logging:
   * Select waf-alb-logs-bucket
   * Choose JSON format
6. Click **Create Web ACL**

### ✅ Step 6: Test the ALB

Get the DNS of your ALB (e.g., waf-alb-123456789.us-east-1.elb.amazonaws.com):

curl http://waf-alb-xxxxxxxx.us-east-1.elb.amazonaws.com

Should return:

WAF ALB Test Page

### ✅ Step 7: Test Attacks via Linux Commands

# SQL Injection  
curl "http://<alb-dns>/?id=1' OR '1'='1"  
  
# XSS  
curl "http://<alb-dns>/?q=<script>alert(1)</script>"  
  
# Path traversal  
curl "http://<alb-dns>/../../etc/passwd"

Expect 403 Forbidden if rules block them.

### ✅ Step 8: View WAF Logs in S3

1. Go to **S3 > waf-alb-logs-bucket > AWSLogs/**
2. Download the .json.gz file
3. Unzip and view logs:

gunzip log.json.gz  
cat log.json | jq .

Look for action, ruleGroupList, and terminatingRuleId

## 🎉 Done!

You now have:

* WAF protection on your EC2 via ALB
* Logging enabled to S3
* Confirmed that malicious requests are blocked