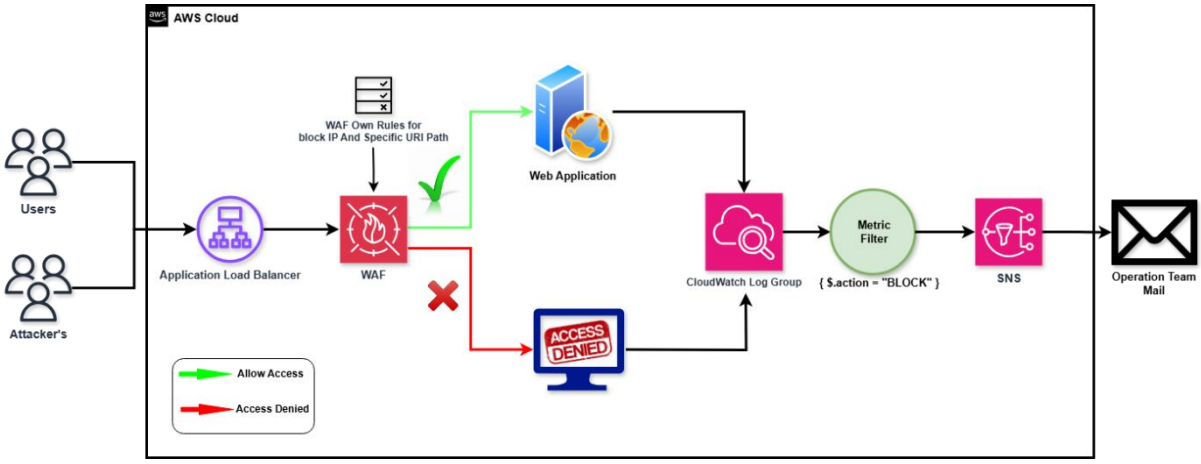
AWS WAF IP Block Monitoring with Notifications

Objective

The goal of this project is to set up a system to monitor blocked IPs in AWS WAF and send real-time notifications using Amazon SNS when an IP is blocked.

Architecture Overview



1. **Application Load Balancer (ALB): Distributes incoming traffic across multiple targets to ensure high availability.**
2. **AWS WAF: Protects your web applications by blocking malicious IPs or requests based on rules.**
3. **CloudWatch Logs: Captures logs from WAF to monitor blocked actions.**
4. **Metric Filters: Identifies patterns in the logs (e.g., blocked IPs) and creates metrics.**
5. **CloudWatch Alarms: Monitors the metric and triggers an alarm when a threshold is met.**
6. **Amazon SNS: Sends notifications (e.g., email) when the alarm is triggered.**

Step-by-Step Implementation

Step 1: Configure Application Load Balancer (ALB)

1. **Go to the EC2 Console.**
2. **Under Load Balancing, select Load Balancers.**
3. **Click Create Load Balancer and choose Application Load Balancer.**
4. **Configure the ALB:**
    - **Provide a name.**
    - **Select Internet-facing for public access.**

- Add at least two availability zones for high availability.

5. Set up the Listener:
    - Add an HTTPS listener and associate a security group.
6. Configure the Target Group:
    - Create a target group and register your instances or services.
7. Save and create the ALB.

Step 2: Configure AWS WAF and Enable Logging

1. Go to the AWS WAF Console.
2. Create or select a Web ACL.
3. Add rules to block malicious IPs (e.g., rate-based rules, IP sets).
4. Associate the Web ACL with the ALB created earlier.
5. Enable logging for the Web ACL:
    - Navigate to the Logging and Metrics tab.
    - Choose a CloudWatch Log Group as the destination.
    - Save the configuration.

Step 3: Create an SNS Topic for Notifications

1. Go to the Amazon SNS Console.
2. Click Create Topic.
3. Select Standard as the topic type.
4. Provide a name (e.g., WAF-IP-Blocked-Notifications).
5. Click Create Topic.
6. Create a Subscription:
    - Select the SNS topic you just created.
    - Click Create Subscription.
    - Choose Email as the protocol and enter the recipient's email address.
    - Confirm the subscription by clicking the link in the email.

Step 4: Create a CloudWatch Log Group (If Not Already Created)

1. Go to the CloudWatch Console.
2. Navigate to Logs > Log Groups.

3. Click Create log group.
4. Provide a name (e.g., WAF-Logs) and save.

Step 5: Create a Metric Filter in CloudWatch Logs

1. Go to the CloudWatch Console.
2. Navigate to Logs > Log Groups.
3. Select the log group where WAF logs are sent (e.g., WAF-Logs).
4. Click on the Metric filters tab and then Create metric filter.
5. Define the pattern:
    - Use the following pattern to detect blocked IPs:

```
{ $.action = "BLOCK" }
```

6. Click Next and configure the metric:
    - Filter Name: BlockedIPs
    - Metric Namespace: WAF
    - Metric Name: blockipcount
    - Metric Value: 1
7. Save the filter.

Step 6: Create a CloudWatch Alarm

1. Go to the CloudWatch Console.
2. Navigate to Alarms > Create Alarm.
3. Click Select Metric and browse to:
    - Namespace: WAF
    - Metric Name: blockipcount
4. Set the threshold:
    - Trigger the alarm when blockipcount >= 1.
5. Configure actions:
    - Select Send a notification to an SNS topic.
    - Choose the SNS topic created earlier (e.g., WAF-IP-Blocked-Notifications).
6. Save the alarm.

Step 7: Test the Configuration

1. **Trigger a WAF block event:**
    - **Use a custom WAF rule to block your own IP or send a request that matches the block condition.**
2. **Verify:**
    - **The WAF logs show the blocked IP.**
    - **The CloudWatch metric updates (e.g., blockipcount increases).**
    - **The CloudWatch alarm triggers.**
    - **An SNS notification is sent to the configured email address.**

Cost Analysis

Estimated Monthly Cost

Service	Cost per Unit	What It Covers	Estimated Cost
Application Load Balancer	$0.0225 per hour	ALB runtime	$16.20 (20 days x 12 hrs)
Data Processed (ALB)	$0.008 per GB	Traffic handled by the ALB	$2.00 (250 GB)
WAF (1 Web ACL)	$5.00 per month	Web ACL management	$5.00
WAF Requests	$0.60 per 1M requests	Requests evaluated by WAF	$3.00 (5M requests)
CloudWatch Logs	$0.50 per GB	Log ingestion	$3.00 (10 GB logs)
CloudWatch Log Storage	$0.03 per GB per month	Storing ingested logs	$0.30 (10 GB logs)
CloudWatch Metrics	$0.30 per metric per month	Custom metrics	$0.30
CloudWatch Alarms	$0.10 per alarm per month	Monitoring metrics	$0.10
Amazon SNS	$0.50 per 1M publish requests	Notifications sent	$0.50
Total			**$30.40**