**SOP for implementing WAF on AWS Cloudfront**

Implementing a Web Application Firewall (WAF) on Amazon CloudFront in AWS involves a few essential steps. The WAF helps protect your web applications from common web exploits and malicious traffic. Below is a step-by-step guide for implementing WAF on CloudFront:

Step 1: Create a Web ACL

* Go to the AWS Management Console and navigate to the AWS WAF & Shield service.
* Click on "Web ACLs" in the left-hand navigation panel.
* Click on the "Create web ACL" button.
* Provide a name for your Web ACL and optionally add a description.
* Choose the region for your WAF deployment.
* Under "Default action," select whether to allow or block all requests that don't match any rules.
* Click "Create web ACL" to create your Web ACL.

Step 2: Create WAF Rules

* In the Web ACL that you just created, click on "Add default rule."
* Choose the type of rule you want to create, such as "IP match conditions," "String match conditions," or "SQL injection match conditions."
* Configure the rule settings based on your security requirements.
* Click "Add rule" to create the WAF rule.

Step 3: Associate WAF with CloudFront

* Go to the AWS Management Console and navigate to the Amazon CloudFront service.
* Click on "Distributions" in the left-hand navigation panel.
* Select the CloudFront distribution for which you want to enable WAF.
* Click on the "Behaviors" tab and then click on "Create Behavior."
* In the "Create Behavior" window, enable "Web Application Firewall (WAF)."
* Choose the Web ACL that you created in Step 1 from the dropdown list.
* Optionally, set the "Default Behavior" for requests that don't match any WAF rules.
* Click "Create" to add the WAF association to the CloudFront distribution.

Step 4: Deploy the Changes

* After associating the WAF with CloudFront, click on the "Distribution Settings" tab.
* Scroll down to the "Distribution State" section and click on the "Deploy" button to deploy the changes.
* Choose the desired distribution method (either "Web" or "RTMP").
* Click "Yes, Edit" to confirm and deploy the changes.

Step 5: Test the WAF

* Wait for the CloudFront distribution to be deployed (status changes to "Deployed").
* Test the WAF by accessing your website through CloudFront and try triggering the rules you configured in the WAF.
* Verify that the WAF is blocking or allowing traffic based on the rule conditions.

Step 6: Monitor and Fine-Tune

* Monitor the WAF logs and metrics to ensure it's functioning as expected.
* Fine-tune the WAF rules based on your application's behavior and security requirements.