README-AWS WAF creation CloudFormation

Version History

SrNo	Version ID	Date	Author	Remark
1	1.0	19-Feb-2024	Umesh K N	First Version
2	2.0	29-May-2025	Shashank H M	Second Version (WAF template 4.0.6)

TABLE OF CONTENT

DOCUMENT OVERVIEW AND PURPOSE

This document covers step-by-step instructions to how to create WAF 4.0.6 version using CloudFormation templates.

OUTCOME

Creates WAF, S3 buckets to store logs, certain AWS protection list, log monitoring and couple of dashboards.

DIAGRAM (IF ANY)

PRE-REQUISITES

- An AWS Account with the user having the required permissions to execute the CloudFormation stack.
- A S3 bucket with the unique name to upload the provided templates.
- Relevant access to create S3 bucket and roles to create logs under it.

INSTALLATION GUIDE / EXECUTION COMMANDS

If you want to execute the template CLI, then use the below command:

1. To Create the Stack:

aws cloudformation create-stack --stack-name WAF-Test-CLI --template-url https://bucketforwaf.s3.ap-south-1.amazonaws.com/aws-waf-security-automations.template.yaml --parameters file://waf-parameters.json --capabilities CAPABILITY_NAMED_IAM --region ap-south-1

2. To Update the Stack:

aws cloudformation update-stack --stack-name WAF-Test-CLI --template-url https://bucketforwaf.s3.ap-south-1.amazonaws.com/aws-waf-security-automations.template.yaml --parameters file://waf-parameters.json --capabilities CAPABILITY_NAMED_IAM --region ap-south-1

3. To Delete the Stack:

aws cloudformation delete-stack --stack-name WAF-Test-CLI

CONFIGURATION

Resource Type

- **Endpoint Type**
  Choose appropriate value from the dropdown based on your requirement.
  Default: CloudFront

AWS Managed IP Reputation Rule Groups

- **Activate Amazon IP reputation List Managed Rule Group Protection:**

  Choose yes/no if you wish to enable Amazon IP reputation List Managed Rule Group Protection.

  Default: no

- **Activate Anonymous IP List Managed Rule Group Protection**

  Choose yes/no if you wish to enable Anonymous IP List Managed Rule Group Protection.

  Default: no

AWS Managed Baseline Rule Groups

- **Activate Core Rule Set Managed Rule Group Protection:**
  Choose yes/no if you wish to enable AWS Managed rules.

  Default: no

- **Activate Admin Protection Managed Rule Group Protection:**

  Choose yes/no if you wish to enable Admin Protection Managed Rule Group Protection.

  Default: no

- **Activate Known Bad Inputs Managed Rule Group Protection:**

  Choose yes/no if you wish to enable Known Bad Inputs Managed Rule Group Protection.

  Default: no

AWS Managed Use-case Specific Rule Groups

- **Activate SQL Database Managed Rule Group Protection:**

  Choose yes/no if you wish to enable SQL Database Protection.

  Default: no

- **Activate Linux Operating System Managed Rule Group Protection:**

  Choose yes/no if you wish to enable Linux Operating system Protection.

  Default: no

- **Activate POSIX Operating System Managed Rule Group Protection:**

  Choose yes/no if you wish to enable POSIX Operating system Protection.

  Default: no

- **Activate Windows Operating System Managed Rule Group Protection:**

  Choose yes/no if you wish to enable Windows Operating system Protection.

  Default: no

- **Activate PHP Application Managed Rule Group Protection:**

  Choose yes/no if you wish to enable PHP Application Protection.

  Default: no

- **Activate WordPress Application Managed Rule Group Protection:**

  Choose yes/no if you wish to enable WordPress Application Protection.

  Default: no

Custom Rule - Scanner & Probes

- **Activate Scanner & Probe Protection:**
  Choose appropriate values from the dropdown based on your requirement.
  Default: yes - AWS Lambda log parser

- **Application Access Log Bucket Name**
  Enter the S3 bucket name where you need to store logs. Logs would be created for the

options that you have selected – “yes” in the earlier options.
Eg: projname-waf-bucketlog => bucket name should be only in this format.

- **Application Access Log Bucket Prefix:**

  If you chose yes for the Activate Scanners & Probes Protection parameter, you can enter an optional user defined prefix for the application access logs bucket.

- **Is bucket access logging turned on:**

  Choose yes if you provided an existing application access log bucket above and the server access logging for the bucket is already turned on.

- **Error Threshold**
  Enter appropriate value based on your requirement.
  Default: 50

- **Keep Data in Original S3 Location**
  Choose yes/no value from the dropdown based on your requirement.
  Default: No

Custom Rule - HTTP Flood

- **Activate HTTP Flood Protection:**
  Choose appropriate values from the dropdown based on your requirement.
  Default: yes - AWS WAF rate-based rule

- **Default Request Threshold:**

  If you chose yes for the Activate HTTP Flood Protection parameter, enter the maximum acceptable requests per IP address per Five-minute period.

- **Request Threshold by Country:**

  If you chose Athena Log Parser to activate HTTP Flood Protection, you can enter a threshold by country following this JSON format {"TR":50,"ER":150}. These thresholds will be used for the requests originated from the specified countries, while the default threshold above will be used for the remaining requests.

- **Group By Requests in HTTP Flood Athena Query:**

If you chose Athena Log Parser to activate HTTP Flood Protection, you can select a group-by field to count requests per IP along with the selected group-by field. For example, if URI is selected, the requests will be counted per IP and URI. If you chose to deactivate this protection, ignore this parameter.

- **WAF Block Period**
  Enter appropriate value based on your requirement.
  Default: 240
- **Athena Query Run Time Schedule (Minute):**

Custom Rule - Bad Bot

- **Activate Bad Bot Protection:**
  Choose yes/no value from the dropdown based on your requirement.
  Default: yes
- **ARN of an IAM role that has write access to CloudWatch logs in your account:**

  Provide an optional ARN of an IAM role that has write access to CloudWatch logs in your account. If you leave it blank (default), a new role will be created for you.

Custom Rule - Third Party IP Reputation Lists

- **Activate Reputation List Protection:**
  Choose yes/no value from the dropdown based on your requirement.
  Default: yes

Legacy Custom Rules

- **Activate SQL Injection Protection:**
  Choose yes/no if you wish to activate SQL injection protection.
  Default: yes
- **Sensitivity Level for SQL Injection Protection:**

  Choose the sensitivity level used by WAF to inspect for SQL injection attacks. If you choose to deactivate SQL injection protection, ignore this parameter.
  Default: LOW

- **Activate Cross-site Scripting Protection:**
  Choose yes/no if you wish to activate Cross-site Scripting Protection.
  Default: yes

Allowed and Denied IP Retention Settings

- **Retention Period (Minutes) for Allowed IP Set**
  Enter appropriate value based on your requirement.
  Default: -1
- **Retention Period (Minutes) for Denied IP Set**
  Enter appropriate value based on your requirement.
  Default: -1
- **Email for receiving notification upon Allowed or Denied IP Sets expiration**
  Enter the email address to which a notification would be sent when Allowed / Denied IP sets expire.

Advanced Settings

- **Retention Period (Days) for Log Groups:**

  If you want to activate retention for the CloudWatch Log Groups, enter a number (1 or above) as the retention period (days)

OPTIONAL PARAMETERS OR CONDITIONS (IF ANY)

REFERENCES

- WAF : Guidelines for Implementing AWS WAF - AWS Whitepaper (amazon.com)

LIMITATIONS (IF ANY)

This template is specifically for WAF version 4.0.6. If you want to use an earlier version, you'll need to download the corresponding version and update the mapping section accordingly.

- For version 4.0.6, the KeyPrefix should be: security-automations-for-aws-waf/v4.0.6
- For earlier versions, the KeyPrefix should be: aws-waf-security-automations/<version>

APPENDIX

Sr No	**Acronym**	**Description**
1	IP	Internet protocol
2	WAF	Web Application Firewall
3	CLI	Command Line Interface