Westcon AWS
WAF Starter Kit
Deployment Guide

Westcon | powered by aws

AWS WAF Bundle – Implementation Guide v1.0

Table of Contents

Summary

This document provides an implementation guide to launch and maintain the AWS WAF bundle for AWS Distributors.

AWS Web Application Firewall (AWS WAF) helps protect web applications from common exploits that can affect application availability, compromise security, or consume excessive resources. AWS WAF allows you to define customizable web security rules, and control which traffic to allow to web applications and APIs deployed on Amazon CloudFront, an Application Load Balancer, or Amazon API Gateway.

Configuring WAF rules can be challenging, especially for organizations that do not have dedicated security teams. To simplify this process, this AWS WAF bundle can be used to deploy the AWS Managed Rules for AWS WAF. This is a managed service that provides protection against common application vulnerabilities or other unwanted traffic, without having to write your own rules.

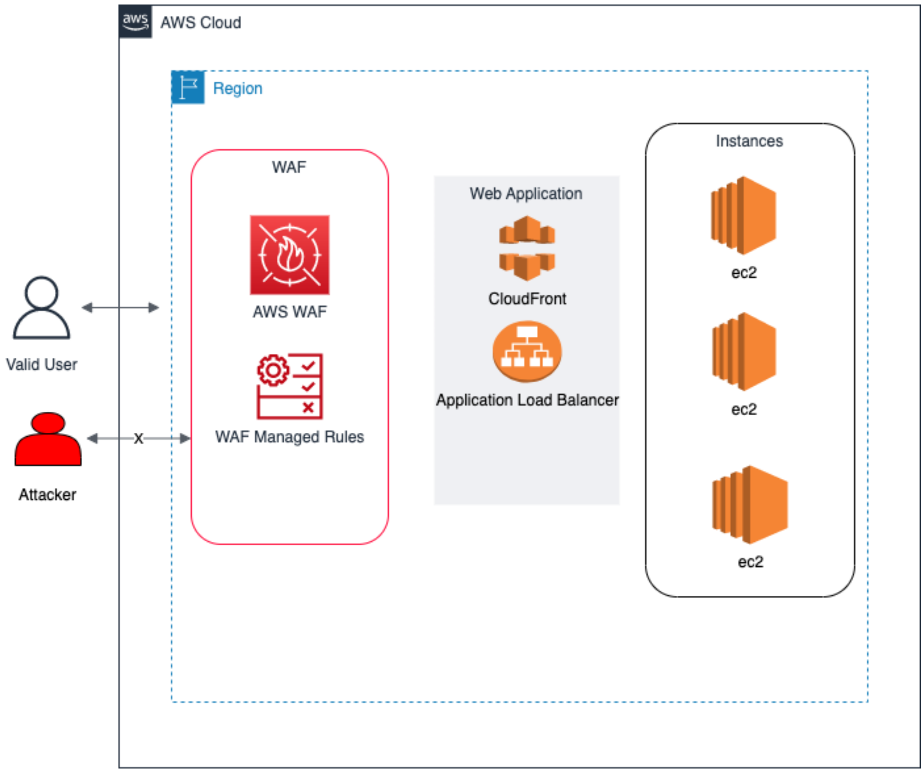
Mitigating false positives and testing rule group changes

Before using any managed rule group in production, test it in a non-production environment according to the guidance at Testing and tuning your AWS WAF protections. Follow the testing and tuning guidance when you add a rule group to your web ACL, to test a new version of a rule group, and whenever a rule group isn't handling your web traffic as you need it to.

Shared security responsibilities

AWS Managed Rules are designed to protect you from common web threats. When used in accordance with the documentation, AWS Managed Rules rule groups add another layer of security for your applications. However, AWS Managed Rules rule groups aren't intended as a replacement for your security responsibilities, which are determined by the AWS resources that you select. Refer to the Shared Responsibility Model to ensure that your resources in AWS are properly protected.

Architecture Overview



Cost

This bundle uses the following resources.

Resource Type	Price
Web ACL	$5.00 per month (prorated hourly)
Rule (customizable to either 1 or 2 managed rules)	$1.00 per month (prorated hourly)
Request	$0.60 per 1 million requests

NOTE: The above pricing information may be subject to change. Always check the official documentation for the latest costs. Official WAF pricing information is available here.

Template

This solution uses AWS CloudFormation to bootstrap AWS infrastructure and automate the deployment of Security Automations for AWS WAF on the AWS Cloud. The template is in the form of a "*WAF_Bundle_basic.yaml*" file provided along with this implementation guide.

Deployment

Prerequisites

This bundle is designed to work with web applications deployed with **Amazon CloudFront** or an **Application Load Balancer**. If you don't already have one of these resources configured, complete the applicable task before you launch this solution.

Step 1 – Launch the Stack

1. Sign in to the AWS Management Console and navigate to the CloudFormation.
2. Select the AWS Region you wish to launch the template in.
3. Click on “Create stack” and then “With new resources (standard)”.
4. On the **Specify template** page, verify that you selected and uploaded the correct template and choose **Next**.
5. On the **Specify stack details** page, assign a name to AWS WAF configuration in the **Stack name** field.
6. Under **Parameters**, review the parameters for the template, and modify them as necessary. To opt out of a particular feature, choose none or no as applicable.

   This solution uses the following default values.

Parameter	**Default**	**Description**
Stack Name	*<Requires input>*	The stack name cannot contain spaces and must be unique within your AWS account.
AWSDistributorName	<Requires input>	Enter the name of the AWS Distributor / Partner deploying this solution for the customer.
ActivateAWSManagedRulesParam	true	Choose true to turn on the component designed to add AWS Managed Rules to the top of the Web ACL priority list
ActivateReputationListsProtectionParam	true	Choose true to block requests from IP addresses on third-party reputation lists (supported lists: spamhaus, torproject, and emerging threats).
BundleName	AWS_WAF_Bundle_v1	Leave as is
EndpointType	Regional	Select the type of resource being used. ALB / API Gateway use Regional endpoint.

		Cloudfront uses CLOUDFRONT endpoint (for the Cloudfront endpoint, only the us-east-1 region is supported so ensure us-east-1 is selected as Region).
WebACLName	WebACL-WebApp1	Customize the name of the WebACL that will be created as required.

7. Choose **Next**.
8. On the **Configure stack options** page, you can specify tags (key-value pairs) for resources in your stack and set additional options, and then choose **Next**.
9. On the **Review** page, review and confirm the settings. Check the boxes acknowledging that the template will create AWS Identity and Access Management (IAM) resources and any additional capabilities required.
10. Choose **Create** to deploy the stack.

View the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a status of **CREATE_COMPLETE** in less than 5 minutes.

Step 2. Associate the web ACL with your web application

1. Update your Amazon CloudFront distribution(s) or Application Load Balancer(s) to activate AWS WAF and logging using the resources you generated in Step 1.
2. Open the AWS WAF console and choose the web ACL that you want to use.
3. On the **Associated AWS resources** tab, choose **Add AWS resources**.
4. Under **Resource type**, choose the CloudFront distribution or Application Load Balancer.
5. Select a resource from the list, then choose **Add** to save your changes.

Summary

This implementation guide provides basic details on launching and maintaining the AWS WAF Bundle. Additional configuration and/or additional rules may be applied on the provisioned WAF resources. Please consult the official WAF documentation for more details at:
https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html

Westcon | powered by aws

Have a question?

Contact us

NZ Cloud Sales: +64 9 477 7211
cloudsales.nz@westcon.com

AU Cloud Sales: +61 2 8412 1212
cloudsales.au@westcon.com

SG Cloud Sales: +65 6424 0570
cloudsales.sg@westcon.com

ID Cloud Sales: +62 21 8062 1470
cloudsales.id@westcon.com