WAF Service Delivery Technical Controls Calibration Guide

Table of Contents

Introduction

This calibration guide is intended for AWS partners who have applied or are interested in the Amazon Web Services (AWS) Web application Firewall (WAF) Service Delivery program. This guide only covers controls under the section of "AWS WAF Customer Reference Requirements" and the "Common Requirements" are addressed in a separate guide.

The calibration guide format is FAQs for each control. It is intended to provide clarity on the expected level of details for requested evidence. It helps partner improve application quality and reduce cycle time during the technical validation process. Additionally, partners can use the best practices in this technical guide to improve their AWS WAF related service offerings.

Each control has the following FAQs:

Why is this important?

This section explains why a particular control is essential to be implemented from an architectural point of view for efficient AWS WAF operation, security, migration etc.

What are the criteria for passing this control?

This section details the control and addresses question related to what level of information is needed to pass a particular control. It further describes the requirement so it easier for partner to provide the response needed in self-assessment to pass it swiftly.

Technical Enablement Resources

This section discusses how to implement the specific control using AWS services. Partner can implement a certain control using third party services; however, they should be able to justify that the service is adhering to the standards of the AWS and meeting the control.

What are good example responses (If applicable)?

This section provides good response examples that meet the control and displays the level of depth and expertise required in the assessment.

What are unacceptable/insufficient information responses (if applicable)?

This section is composed of response examples not meeting the requirement of the control.

WAF-001

Requirement

AWS WAF Use Case Description

Please provide the following as evidence:

- A description of WAF use case, e.g. application vulnerability protection, PCI compliance, DDoS protection, etc.
- Request volume
- Rule set implemented
- Process for deciding what rules to implement

Criteria for Passing

An adequate response to describing the WAF use case being demonstrated that covers but is not limited to application vulnerability protection, Distributed Denial of Service (DDoS) protection or Payment card industry (PCI) compliance.

The use case should capture incoming traffic on the application in order to design a solution which secures the application from malicious user, DDoS attacks, SQL injections etc. Additionally, partner must have a rule defining process to inspect the HTTP(s) web requests to take the necessary action in case of an attack.

Why is this important?

Diving deep into the use case description for developing a solution to secure applications from any unauthorized access helps the user understand how they can leverage this use case to mitigate risk to their own applications.

Technical Enablement Resources

How can you implement this?

Partner is aware of the customer's architecture and estimated traffic which helps them determine the right rules for implementing AWS WAF. AWS WAF rules can be accessed in the rule group or Web ACL where it is defined. There are two main categories:

- Managed rule groups created by AWS or AWS Marketplace sellers (updated automatically), and
- Custom rule groups, created and maintained by AWS customers

Partners need to have a defined process to discuss with the customer on the appropriate access to their content and decide rules like blocking IP Addresses, blocking traffic based on country of origination, string appearing in the request header, sql code in request which could be malicious etc. The partner can use data from the threat intelligence platform or labs to create AWS WAF rule groups (managed or custom) that help protect from malicious cyberattacks.

Additional Resources

- Managing your own rule groups

- Logging web ACL traffic
- AWS WAF intelligent threat mitigation

Good Example Response

WAF is used to protect API Gateway (both public and private) and CloudFront Distributions. Given the customer requirements, custom rule implementation was not needed and therefore we opted to leverage existing AWS managed rules. This also had the added benefit of automatic updates.

For API gateway we process a monthly average of 30,000 requests against the following ruleset.

- AWSManagedRulesAmazonIpReputationList
- AWSManagedRulesAnonymousIpList
- AWSManagedRulesBotControlRuleSet
- AWSManagedRulesAdminProtectionRuleSet
- AWSManagedRulesCommonRuleSet
- AWSManagedRulesKnownBadInputsRuleSet
- AWSManagedRulesPHPRuleSet
- AWSManagedRulesSQLiRuleSet

CloudFront is used to protect the front-end of the customer application and we saw a monthly average of 20,000 requests. The use case implemented WAF security automations and the following managed rules.

- AWSWAFSecurityAutomations-CloudFront-WhitelistRule
- AWSManagedRulesCommonRuleSet
- AWSWAFSecurityAutomations-CloudFront-BlacklistRule
- AWSWAFSecurityAutomations-CloudFront-HttpFloodRateBasedRule
- AWSWAFSecurityAutomations-CloudFront-ScannersAndProbesRule
- AWSWAFSecurityAutomations-CloudFront-IPReputationListsRule
- AWSWAFSecurityAutomations-CloudFront-BadBotRule
- AWSWAFSecurityAutomations-CloudFront-SqlInjectionRule
- AWSWAFSecurityAutomations-CloudFront-XssRule

Unacceptable Example Response

Our product provides both Marketplace Managed Rules and Custom Rules customers can implement in their account.

WAF-002

Requirement

Valid AWS WAF Workloads

Each case study needs to implement AWS WAF in one of the following workload types:

- AWS WAF in a compliance environment
- AWS WAF as part of a custom security application
- AWS WAF as a part of a DDoS mitigation strategy
- AWS WAF as a part of Security Research application
- AWS WAF Creation of Templatized Rulesets

Please provide the following as evidence:

- Primary Security Objective in implementing WAF
- Project outcomes and measurements of success
- Testing strategy for security objectives

Criteria for Passing

The partner is able to provide a comprehensive description of how AWS WAF is implemented for the selected workload type (above). For example,

- If this implementation is part of a compliance environment, then state which compliance program it supports and specifically which controls in the compliance program AWS WAF mitigates and it achieves this.
- For templatized rulesets, discuss how rules are auto-generated through the use of infrastructure-as-code and/or other automation technologies. Once these rulesets are created, what automation mechanisms exist to manage and maintain them going forward.

Evidence should be provided in the form of existing documentation or project artifacts.

Why is this important?

This enables us to determine whether the partner understands the capabilities of WAF to a sufficient depth to be able to implement in the scenarios mentioned above. Understanding our partner response to this requirement enables us to determine the impact of WAF on such use cases and thereby helping to shape future evolution of WAF.

Technical Enablement Resources

How can you implement this?

Partners need to understand the customer workload and use WAF for the threat detection and prevention of their application. They need to have discussions with customer about the prime objective, testing, monitoring & metrics to capture success which ensures that the workload is secure.

Additional Resources

- Guidelines for implementing AWS WAF

Good Example Response

In this case AWS WAF is part of a custom security design.

The design of the solution and implementation of AWS WAF are part of a customized environment for the customer, with the aim of ensuring security, service availability, filtering website traffic allowing regular user interaction, having real-time visibility of requests and obtaining security recommendations

Having clear the security objectives of the customer, we proceed with the implementation of the service, resulting in traffic detection, application of security rules (block or allow) and a dashboard that allows monitoring the activity with the option of obtaining greater detail through Amazon Cloud Watch.

The solution was tested with a full suite of functional, non-functional and penetration test cases to validate the security threat model.

Please refer to the following supporting documents as evidence:

1. Security_test_cases.pdf
2. Project_plan.pdf
3. Application_results.pdf

Unacceptable Example Response

The customer needed WAF for DDoS prevention.

WAF-003

Requirement

Automated Security Improvements

AWS WAF should take advantage of automated security improvements. This can be accomplished either by using managed security rules or by implementing a solution for updating the ruleset automatically with an AWS Lambda based solution (or something similar).

Please provide the following as evidence:

- Describe the implementation details to ensure solution stays up to date with new security threats

Criteria for Passing

Partner should be able to describe if they are using custom rules that those are regularly updated to prevent the new security threats. Partner needs to have monitoring enabled on WAF solution to ensure that it is preventing the traffic as expected.

Why is this important?

Partners should have automated mechanisms in place to determine whether the existing WAF rules are effective at defending against malicious actors / traffic. Although managed rules are updated by AWS automatically, the partner should maintain monitoring of these rules to determine if new security threats are circumventing existing managed rules. This policy should apply for existing custom rules as well.

Additional Resources

- https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing-activities.html
- https://docs.aws.amazon.com/whitepapers/latest/guidelines-for-implementing-aws-waf/testing-and-tuning.html
- https://docs.aws.amazon.com/whitepapers/latest/guidelines-for-implementing-aws-waf/monitoring-and-visibility.html

Good Example Response

By including rules managed by AWS we seek to take advantage of the updates made to these rules and not worry about doing manual tasks with some frequency. With the use of monitoring (CloudWatch metrics) on the WAF solution, subsequent evaluations will be made to review the need to include more managed rules. The managed rules used in this solution are part of the catalog of rules provided by AWS.

WAF-003 - Automated Security Improvements, pg. 3 to see the brief information about the automation for security improvements we have in place.

Unacceptable Example Response

We are using Marketplace managed rules.

Resources

Visit AWS Service Delivery Program Guide to get overview of the program.
Explore AWS Service Delivery Benefits to understand AWS Service Delivery benefits.
Find Amazon WAF Service Delivery checklist.
Visit How to build a microsite to understand on building a Practice/solution page
Check out How to build an architecture diagram to build an architecture diagrams.
Learn about Well Architected Framework on Well Architected Website

Notices