Implementing AWS WAF for Enhanced Web Security

Abid Jeem

March 13, 2025

1 Introduction

AWS WAF is a powerful, managed web application firewall service integrated natively with a range of AWS resources. By allowing the configuration of custom rulesets without requiring external software, AWS WAF offers scalable, dynamic protection for web applications against common exploits and threats.

2 Protected Resources

AWS WAF can safeguard multiple AWS services, including:

1. Application Load Balancers (ALBs)
2. Amazon CloudFront Distributions (Content Delivery Network)
3. Amazon API Gateway APIs (API Management)
4. AWS AppSync GraphQL APIs (GraphQL Service)
5. Amazon Cognito User Pools (Identity and Access Management)
6. Amazon ECS Containers (Elastic Container Service)

3 Core Components of AWS WAF

The functionality of AWS WAF is based on three key components:

1. **Web Access Control Lists (ACLs)**: Collections of rules that determine the handling of incoming web requests.
2. **Rules**: Statements that define inspection criteria and specify actions (allow, block, or count) when requests meet the criteria.
3. **Rule Groups**: Reusable sets of rules, including both AWS managed and custom-defined groups.

4 Configuration Process

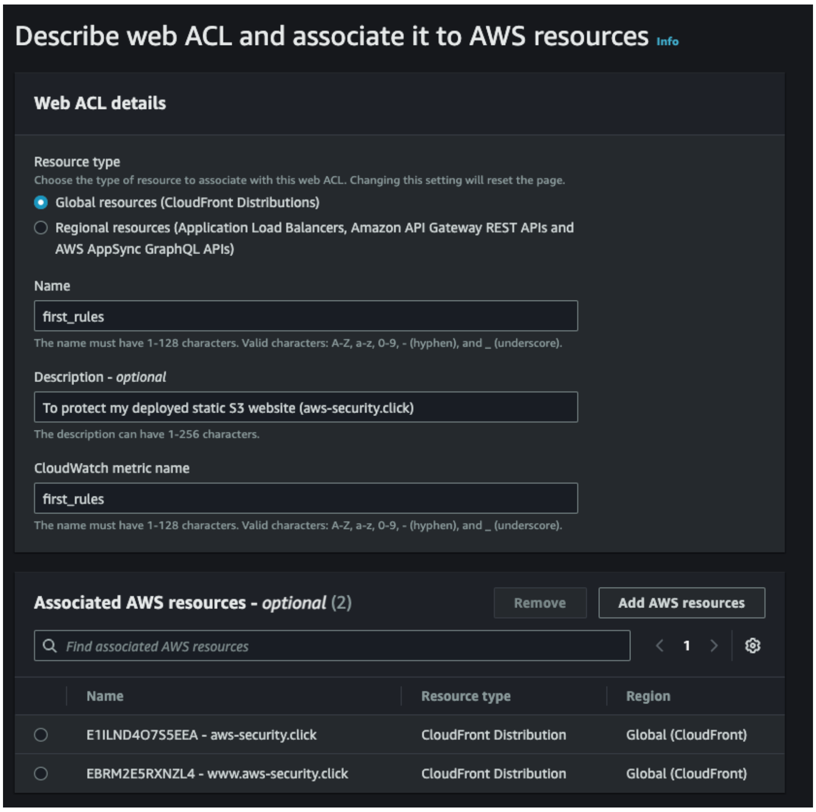
The implementation of AWS WAF involves several steps, each demonstrating careful planning and technical acumen.

4.1 Creating a Web ACL

1. Navigate to the AWS WAF service in the AWS Management Console and click on "Create Web ACL".

2. Assign a name to your Web ACL (e.g., `first_rules`) and configure the corresponding CloudWatch metric name.

3. Add your target resource, such as a CloudFront Distribution, to the Web ACL.



Describe web ACL and associate it to AWS resources Info

Web ACL details

Resource type

Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

● Global resources (CloudFront Distributions)

○ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs and AWS AppSync GraphQL APIs)

Name

first_rules

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - *optional*

To protect my deployed static S3 website (aws-security.click)

The description can have 1-256 characters.

CloudWatch metric name

first_rules

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Associated AWS resources - *optional* (2)

	Name	Resource type	Region
○	E1ILND4O7S5EEA - aws-security.click	CloudFront Distribution	Global (CloudFront)
○	EBRM2E5RXNZL4 - www.aws-security.click	CloudFront Distribution	Global (CloudFront)

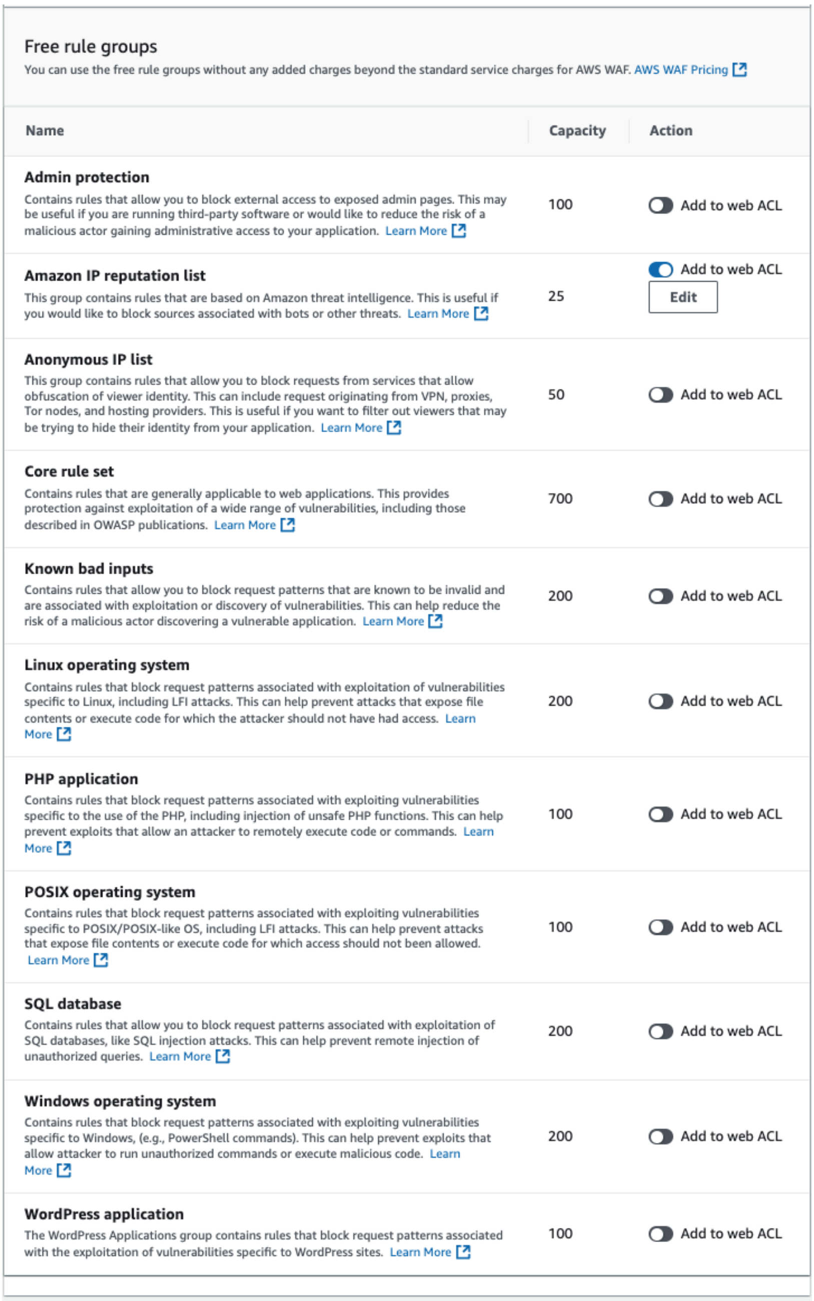
Figure 1: AWS WAF Console - Creating a Web ACL.

4.2 Creating Rules

1. Click on "Add Rules" and select "Add managed rule groups". This presents a list of pre-configured rules from AWS and trusted partners.

2. For this implementation, choose the Free Rule Groups. Toggle "Add to Web ACL" for the Amazon Reputation IP list.

3. The managed rule is added, consuming a specific portion of your Web ACL capacity (e.g., 25 out of 5000 units).



Free rule groups

You can use the free rule groups without any added charges beyond the standard service charges for AWS WAF. AWS WAF Pricing

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. Learn More	100	○ Add to web ACL
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats. Learn More	25	● Add to web ACL Edit
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application. Learn More	50	○ Add to web ACL
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. Learn More	700	○ Add to web ACL
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. Learn More	200	○ Add to web ACL
Linux operating system Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. Learn More	200	○ Add to web ACL
PHP application Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands. Learn More	100	○ Add to web ACL
POSIX operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not been allowed. Learn More	100	○ Add to web ACL
SQL database Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Learn More	200	○ Add to web ACL
Windows operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands). This can help prevent exploits that allow attacker to run unauthorized commands or execute malicious code. Learn More	200	○ Add to web ACL
WordPress application The WordPress Applications group contains rules that block request patterns associated with the exploitation of vulnerabilities specific to WordPress sites. Learn More	100	○ Add to web ACL

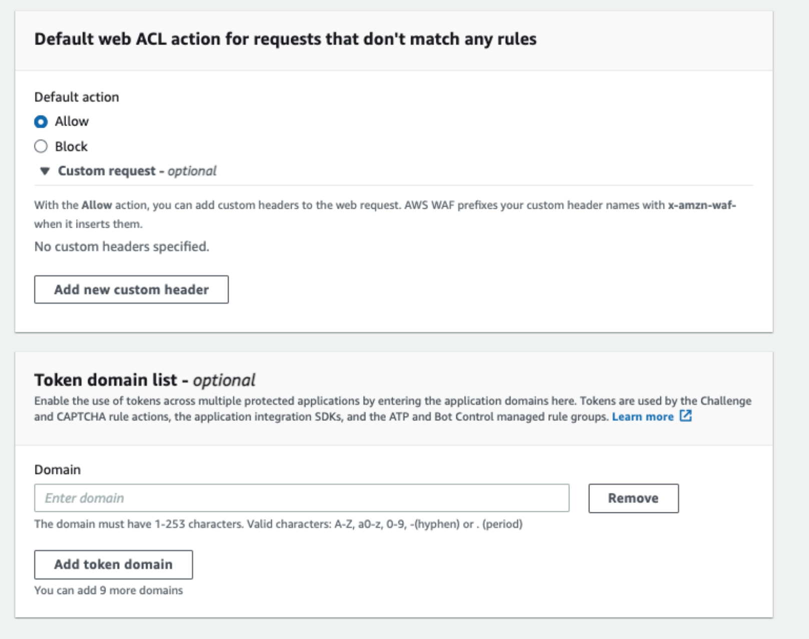
Figure 2: Selecting Managed Rule Groups in AWS WAF.

4.3 Configuring Rules

1. Set the **Default Web ACL Action** to *Allow* for any requests that do not match the configured rules.

2. Optionally, configure a custom header for allowed requests. AWS WAF automatically prefixes these headers with `x-amzn-waf-`.

3. Configure CAPTCHA challenges for suspected bot activity, and add additional domains to the *Token Domain List* to prevent repetitive verification.



Default web ACL action for requests that don't match any rules

Default action

● Allow

○ Block

▼ **Custom request** - *optional*

With the **Allow** action, you can add custom headers to the web request. AWS WAF prefixes your custom header names with **x-amzn-waf-** when it inserts them.

No custom headers specified.

Token domain list - *optional*

Enable the use of tokens across multiple protected applications by entering the application domains here. Tokens are used by the Challenge and CAPTCHA rule actions, the application integration SDKs, and the ATP and Bot Control managed rule groups. Learn more

Domain

Enter domain

The domain must have 1-253 characters. Valid characters: A-Z, a0-z, 0-9, -(hyphen) or . (period)

You can add 9 more domains

Figure 3: Configuring Rule Actions and Custom Headers in AWS WAF.

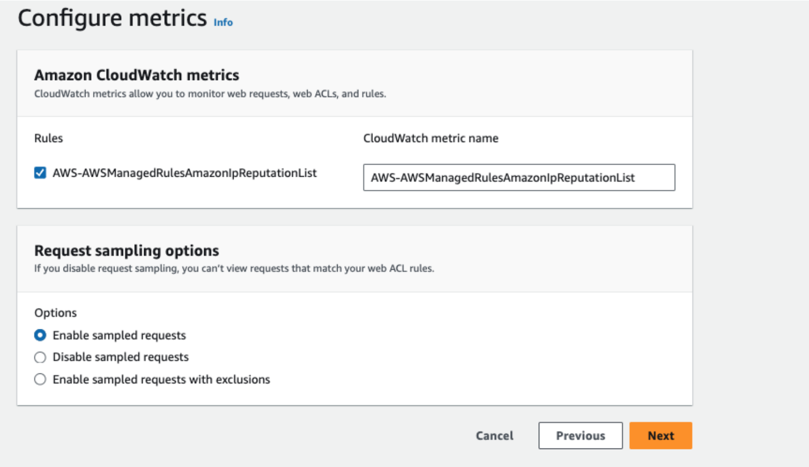
4.4 Setting Rule Priorities

- Establish rule priorities to ensure that the first matching rule is the one applied. This is crucial to maintain data integrity, such as ensuring that rule counts are registered before a request is blocked.

4.5 Configuring CloudWatch Metrics

1. AWS CloudWatch monitors and provides metrics for your resources.

2. For this project, the default configuration is maintained, leveraging the free tier's metrics for ongoing monitoring.



Configure metrics Info

Amazon CloudWatch metrics

CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.

Rules	CloudWatch metric name
☑ AWS-AWSManagedRulesAmazonIpReputationList	AWS-AWSManagedRulesAmazonIpReputationList

Request sampling options

If you disable request sampling, you can't view requests that match your web ACL rules.

Options

● Enable sampled requests

○ Disable sampled requests

○ Enable sampled requests with exclusions

Figure 4: Defining Rule Priorities in AWS WAF.

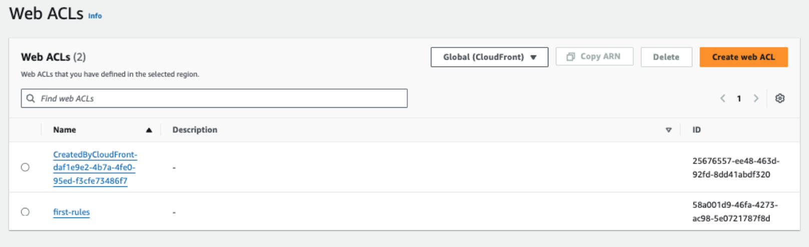
4.6 Review and Finalization

1. Review all configuration settings.
2. Click "Create Web ACL" to deploy your WAF settings.

4.7 Post-Deployment Monitoring

After deployment, the Web ACL dashboard displays useful data, such as:

- Requests per 5-minute interval.
- Sample requests and rule hit counts.
- Detailed metrics for each rule (e.g., the Amazon Reputation IP list).



Web ACLs (2)

Web ACLs that you have defined in the selected region.

	Name	Description	ID
○	CreatedByCloudFront-daf1e9e2-4b7a-4fe0-95ed-f3cfe73486f7	-	25676557-ee48-463d-92fd-8dd41abdf320
○	first-rules	-	58a001d9-46fa-4273-ac98-5e0721787f8d

Figure 5: AWS WAF Dashboard - Post-Deployment Monitoring.

5 Additional AWS WAF Features

AWS WAF also offers advanced capabilities, including:

- **BOT Control:** Enhanced detection and mitigation of automated traffic.
- **Application Integration SDKs:** Improved telemetry and bot detection.
- **Customizable IP Sets and Regex Pattern Sets:** For refined, rule-based protection.
- **Custom Rule Groups:** Allowing for tailored security policies.
- **OWASP Top 10 Protections:** Add-on features that secure against common web vulnerabilities.

6 Conclusion

This document illustrates a systematic approach to deploying AWS WAF, highlighting the integration of security best practices with AWS's robust services. By configuring a Web ACL, creating and prioritizing rules, and monitoring via CloudWatch, this implementation not only secures web applications but also demonstrates technical expertise and attention to detail—qualities highly valued in today's cloud-driven IT environments.