AWS WAF A web application firewall that helps protect web applications from attacks by allowing you to configure rules that **allow, block, or monitor (count) web requests** based on conditions that you define.

- These conditions include:
  - IP addresses
  - HTTP headers
  - HTTP body
  - URI strings
  - SQL injection
  - cross-site scripting.

Features

- WAF lets you create rules to filter web traffic based on conditions that include IP addresses, HTTP headers and body, or custom URIs.
- You can also create rules that block common web exploits like SQL injection and cross site scripting.
- For application layer attacks, you can use WAF to respond to incidents. You can set up proactive rules like *Rate Based Blacklisting* to automatically block bad traffic, or respond immediately to incidents as they happen.
- WAF provides real-time metrics and captures raw requests that include details about IP addresses, geo locations, URIs, User-Agent and Referers.
- AWS WAF can parse request body JSON content to inspect specific keys or values in the JSON content with WAF rules. This helps you protect your APIs by checking for valid JSON structure, inspecting the JSON content for common threats against your application, and reducing false positives by inspecting only the keys or values in the JSON content.
- **AWS WAF Security Automations** is a solution that automatically deploys a single web access control list (web ACL) with a set of AWS WAF rules designed to filter common web-based attacks. The solution supports log analysis using Amazon Athena and AWS WAF full logs.

Conditions, Rules, and Web ACLs

- You define your conditions, combine your conditions into rules, and combine the rules into a web ACL.

- **Conditions** define the basic characteristics that you want WAF to watch for in web requests.
- You combine conditions into **rules** to precisely target the requests that you want to allow, block, or count. WAF provides two types of rules:
    - **Regular rules** – use only conditions to target specific requests.
    - **Rate-based rules** – are similar to regular rules, with a rate limit. Rate-based rules count the requests that arrive from a specified IP address every five minutes. The rule can trigger an action if the number of requests exceed the rate limit.
- **WAF Managed Rules** are an easy way to deploy pre-configured rules to protect your applications common threats like application vulnerabilities. All Managed Rules are automatically updated by AWS Marketplace security Sellers.
- After you combine your conditions into rules, you combine the rules into a **web ACL**. This is where you define an action for each rule—allow, block, or count—and a default action, which determines whether to allow or block a request that doesn't match all the conditions in any of the rules in the web ACL.
- You can insert HTTP headers to a user request when WAF allows the request to reach your application. You can use the custom HTTP headers to validate the requests made to your application passed through WAF, and configure your application to only allow requests that contain the custom header values that you specify. You can also insert headers so your application can process the request differently based on the presence of the header, or log the header in your application logs for reporting and analytics.
- WAF lets you configure the HTTP status code and the response body returned to the user when a request is blocked.

AWS WAF Pricing

- WAF charges based on the number of web access control lists (web ACLs) that you create, the number of rules that you add per web ACL, and the number of web requests that you receive.
-