## AWS WAF (Web Application Firewall)

AWS WAF is a web application firewall designed to protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF works by allowing you to monitor HTTP and HTTPS requests forwarded to Amazon CloudFront, an Application Load Balancer (ALB), API Gateway, or AWS App Runner services.

---

## 1. Core Components of AWS WAF

### Web ACL (Web Access Control List)

- A Web ACL is a core component that acts as a set of rules to filter traffic. It defines how requests to your application are handled based on IP addresses, specific request headers, URI strings, SQL injection attacks, cross-site scripting (XSS), and more.
- A Web ACL consists of:
    - **Rules**: Each rule contains conditions and filters that define what traffic is allowed or blocked.
    - **Rule Actions**: These determine whether to **Allow**, **Block**, or **Count** requests that match the rule's criteria.

### Rules and Rule Groups

- **Rules**: These are the building blocks that define the conditions under which a request is allowed or blocked. AWS WAF supports several types of rules:
    - **IP Set Match**: Allows or blocks based on IP addresses.
    - **String Match**: Filters requests based on the presence of strings in the request URI, headers, or other parts.
    - **Regex Match**: Uses regular expressions to match complex patterns in requests.
    - **Size Constraints**: Blocks or allows requests based on the size of a particular part of the request (such as the size of the body).
    - **Rate-based Rules**: Throttles requests when a specified rate limit is exceeded.
    - **Managed Rule Groups**: Predefined, regularly updated rulesets provided by AWS or third-party vendors to protect against common attacks like SQL injection, XSS, and bad bots.

### Conditions

- Conditions define the criteria that requests must meet to trigger a rule. Some of the conditions include:
    - **IP addresses or ranges** (IP sets).
    - **Country of origin**.

    - **Headers** like `User-Agent`, `Referer`, etc.
    - **Cookies** and query strings.
    - **URI path** or HTTP methods.

---

## 2. How AWS WAF Works

AWS WAF inspects incoming traffic to applications and compares the requests against defined rules. Based on the evaluation, it will either:

- **Allow**: Forward the request to the application.
- **Block**: Block the request entirely.
- **Count**: Only log the request without affecting its flow.

**Request Filtering**

- AWS WAF can analyze requests for specific patterns in multiple parts of the HTTP/HTTPS request such as:
    - **Header**: Analyzes HTTP headers for specific string patterns or size constraints.
    - **Body**: Checks the contents of the HTTP body for specific patterns or malicious content.
    - **URI Path**: Examines the path component of a request to detect malicious file access attempts or unwanted URLs.

**Rate-based Rules**

- Rate-based rules automatically block IP addresses when requests exceed a defined threshold within a five-minute period. These are useful for rate limiting and mitigating Distributed Denial of Service (DDoS) attacks.
- Once the rate limit is exceeded, the rule applies the action for that IP address until the rate drops below the threshold.

**Custom Rules**

- You can define custom rules tailored to your specific application needs, such as blocking a range of suspicious IP addresses or allowing only certain HTTP methods (like GET and POST).

---

## 3. Managed Rules

AWS WAF offers **Managed Rule Groups**, which provide predefined rules that protect applications from:

- **OWASP Top 10 Attacks**: The most common web vulnerabilities, such as SQL injection, cross-site scripting, and cross-site request forgery (CSRF).
- **Common Vulnerability Exploits**: Rules that detect and block malicious actors attempting to exploit known vulnerabilities in web applications.
- **Bad Bots**: Managed rules to detect and block automated bot traffic that might be scraping data, brute-forcing credentials, or performing other malicious activities.

Managed Rule Groups are continuously updated by AWS or third-party vendors (like F5, Fortinet, or Trend Micro), helping you stay protected from the latest threats without having to manually configure new rules.

---

## 4. Integration with AWS Services

AWS WAF integrates natively with several AWS services, including:

- **Amazon CloudFront**: Protects your applications at the edge by blocking malicious traffic before it reaches your origin servers.
- **Application Load Balancer (ALB)**: Protects applications running behind an ALB by inspecting incoming traffic.
- **Amazon API Gateway**: Secures APIs by filtering requests before they reach the backend.
- **AWS App Runner**: Protects containerized applications deployed using App Runner.

---

## 5. Monitoring and Logging

AWS WAF provides several monitoring and logging mechanisms:

- **Amazon CloudWatch**: You can monitor AWS WAF metrics like request counts, blocked requests, allowed requests, and more.
- **AWS WAF Logs**: AWS WAF can send full logs of web requests to **Amazon Kinesis Data Firehose**, which can then be sent to **Amazon S3**, **Amazon Redshift**, or **Amazon Elasticsearch Service** for further analysis.
- **AWS CloudTrail**: AWS WAF configuration changes are tracked by AWS CloudTrail, giving you a complete audit trail.

---

## 6. Use Cases

AWS WAF is suitable for a variety of scenarios:

- **Blocking Common Exploits**: Preventing SQL injection and cross-site scripting (XSS) attacks.
- **DDoS Mitigation**: Protecting against layer 7 (application layer) DDoS attacks by rate limiting requests.
- **Bot Mitigation**: Blocking malicious bots while allowing legitimate traffic.
- **Custom Filtering**: Creating specific rules for your application's needs, such as blocking access to specific URLs or parameters.
- **Compliance**: Enforcing compliance by ensuring that only approved traffic types are allowed to your application.

---

## 7. Pricing

AWS WAF pricing is based on three components:

1. **Web ACL Charges**: You are charged for each Web ACL created.
2. **Rule Charges**: There is a charge per rule (or rule group) associated with a Web ACL.
3. **Request Charges**: You are charged based on the number of web requests inspected by AWS WAF.

AWS offers a **free-tier** where the first 10,000 requests inspected per month are free.

---

## 8. Best Practices

- **Use Managed Rule Groups**: These are regularly updated to protect against new and evolving threats, reducing the effort needed to maintain rule sets.
- **Use Rate-Based Rules**: Protect applications from sudden spikes in traffic, such as bot attacks or brute-force attempts.
- **Monitor WAF Logs**: Constantly review logs to fine-tune rules and monitor for new attack patterns.
- **Enable CloudWatch Alarms**: Set alarms to alert you when thresholds, such as unusual traffic spikes, are met.
- **Minimize Latency**: Use CloudFront and ALB integration to ensure that traffic inspection by AWS WAF does not introduce unnecessary latency.