1. What is a Web ACL?

- A **Web ACL** is a collection of rules that define how AWS WAF should inspect and handle incoming requests to a specific web application or resource.
- It acts as a filtering mechanism by allowing, blocking, or counting the requests based on defined conditions (such as IP addresses, headers, query strings, or patterns in the request body).
- A Web ACL can be associated with resources like **Amazon CloudFront**, **Application Load Balancers (ALB)**, **Amazon API Gateway**, or **AWS App Runner**.

---

2. Components of a Web ACL

Rules

- Rules are the building blocks of a Web ACL, defining the specific traffic filtering logic.
    - **Custom Rules**: User-defined rules tailored for specific use cases.
    - **Managed Rules**: Predefined rules provided by AWS or third-party vendors that protect against common threats like SQL injection, XSS, and bot attacks.
    - **Rule Groups**: Collections of rules that can be managed together. You can either create your own rule groups or use managed rule groups from AWS Marketplace.

Actions

- Every rule in a Web ACL has an associated action that determines how AWS WAF handles matching requests:
    - **Allow**: The request is allowed to reach the resource.
    - **Block**: The request is blocked before reaching the resource.
    - **Count**: The request is counted and logged but not blocked or allowed, useful for monitoring the effect of the rule before fully deploying it.

Default Action

- A Web ACL has a default action that applies to any requests that do not match any rules.
    - **Allow**: If no rules match, the request is allowed.
    - **Block**: If no rules match, the request is blocked.

---

3. Rule Evaluation Process in Web ACL

When a Web ACL processes a request:

1. **Evaluate Rules in Order**: Rules are evaluated in the order they are listed. AWS WAF checks each request against the first rule in the Web ACL, then the second, and so on.
2. **Matching Condition**: If a request matches the conditions of a rule, the action defined by that rule is applied immediately (allow, block, or count).
3. **Short-circuiting**: If a rule specifies an action (like block or allow), AWS WAF stops evaluating any further rules.
4. **No Match**: If no rules match, the default action (allow or block) is applied.

---

4. Types of Rules within a Web ACL

There are several types of rules that can be configured within a Web ACL to match specific criteria:

IP Set Match

- Filters requests based on the IP address or range of the incoming request. For example, you can allow requests from trusted IPs or block requests from malicious IP ranges.

String Match

- Inspects requests for specific strings in headers, query strings, URI paths, or bodies. This can be used to allow or block traffic based on specific keywords or patterns.

Regex Match

- Uses regular expressions to search for complex patterns in requests. This is useful for detecting malicious payloads hidden in request parameters.

Size Constraint

- Evaluates the size of certain parts of the request (such as headers or body). For example, you can block requests that exceed a certain size, which could be an indicator of malicious payloads.

Rate-based Rules

- These rules track the rate of incoming requests from individual IP addresses and can throttle or block IPs that exceed a specified request rate (e.g., more than 1000 requests within a 5-minute window). This is particularly useful for preventing DDoS or brute force attacks.

5. Web ACL Association

You must associate a Web ACL with a resource (such as a CloudFront distribution, an Application Load Balancer, API Gateway, or App Runner). Once associated:

- All traffic passing through that resource is inspected and filtered according to the Web ACL's rules.
- You can apply a single Web ACL to multiple resources, ensuring consistent security policies across different applications.

---

6. Logging and Monitoring for Web ACL

AWS WAF Logs

- Web ACLs can be configured to log request details for analysis. The logs capture information about each request, including:
    - The action taken (allow, block, or count).
    - The matching rule.
    - Request details like IP address, URI path, headers, and more.

Logs can be stored in **Amazon S3**, streamed to **Amazon Kinesis Data Firehose**, or sent to **Amazon CloudWatch** for real-time monitoring and analysis.

CloudWatch Metrics

- AWS WAF automatically sends metrics related to Web ACLs to **Amazon CloudWatch**. These metrics can help you monitor the effectiveness of your rules, such as:
    - Number of allowed or blocked requests.
    - Request rates (e.g., total number of requests per minute).
    - Rule-specific metrics to determine how often certain rules are triggered.

CloudWatch Alarms

- You can create alarms based on CloudWatch metrics to notify you of unusual traffic patterns, such as an unexpected spike in blocked requests, which could indicate an ongoing attack.

---

7. Best Practices for Web ACL Configuration

1. Use Managed Rules for Quick Setup

- AWS provides **Managed Rule Groups** that contain predefined rules for common attacks like SQL injection or cross-site scripting (XSS). These can be deployed quickly without requiring custom configurations.

2. Implement Rate-based Rules

- For rate-limiting, use **rate-based rules** to protect your applications from traffic spikes that might indicate a DDoS attack or brute-force login attempts.

3. Use Counting Mode for Testing Rules

- When deploying new rules, use the **Count** action to monitor how many requests would have been blocked or allowed. This allows you to fine-tune the rules without immediately affecting live traffic.

4. Combine Custom and Managed Rules

- Use a combination of **Managed Rule Groups** for general protection and **Custom Rules** for application-specific scenarios, such as blocking certain IP ranges or specific request patterns unique to your application.

5. Monitor and Fine-tune

- Regularly monitor Web ACL logs and metrics to adjust rules as needed. For example, if a certain rule blocks too much legitimate traffic, you can refine it based on the logged request details.

---

8. Pricing Considerations

The cost of using Web ACLs in AWS WAF is based on three main factors:

1. **Web ACL Charges**: You are charged for the number of Web ACLs you create.
2. **Rule Charges**: Each rule added to a Web ACL incurs a cost.
3. **Request Charges**: AWS charges based on the number of requests processed by AWS WAF.

---

9. Use Cases for Web ACL

- **Application Protection**: Apply a Web ACL to filter out malicious traffic targeting web applications, such as SQL injection or cross-site scripting attacks.
- **API Protection**: Protect APIs hosted on Amazon API Gateway by blocking unwanted traffic and rate-limiting requests from abusive clients.
- **Bot Mitigation**: Block traffic from known malicious bots while allowing good bots (e.g., search engine crawlers) using AWS's Managed Bot Control.
- **DDoS Prevention**: Throttle or block requests from IP addresses that are flooding your site with too many requests in a short time.
