AWS WAF

Topics : AWS
Written on December 09, 2023

Amazon Web Services (AWS) Web Application Firewall (WAF) is a managed web application firewall service that helps protect your web applications from common web exploits and malicious traffic. AWS WAF allows you to define customizable web security rules to filter and block malicious requests before they reach your web applications.

1. **Web Application Firewall:**
    - AWS WAF is designed to protect web applications from common threats, such as SQL injection, cross-site scripting (XSS), and other OWASP Top Ten vulnerabilities.
2. **Rules and Conditions:**
    - AWS WAF enables you to create rules and conditions to control access to your web applications. Rules are sets of conditions that define how to inspect and filter web requests.
3. **Rule Actions:**
    - You can define actions to be taken when a web request matches a rule. Actions include allowing the request, blocking the request, or counting the request without taking any other action.
4. **Managed Rules:**
    - AWS WAF provides managed rule sets that are pre-configured to protect against common threats. These rule sets are regularly updated to address emerging security threats.
5. **Rate-Based Rules:**
    - AWS WAF supports rate-based rules that help protect against volumetric attacks, such as DDoS attacks. Rate-based rules allow you to limit the number of requests from a client IP address within a specified time period.
6. **IP Reputation Lists:**
    - You can use IP reputation lists to block requests from specific IP addresses known for malicious activities. AWS WAF provides managed IP reputation lists, and you can also create custom lists.

7. **GeoMatch Conditions:**
    - GeoMatch conditions allow you to block or allow requests based on the geographic location of the client IP address. This can be useful for enforcing regional access controls.
8. **WebACLs (Web Access Control Lists):**
    - WebACLs are sets of rules that you can associate with a CloudFront distribution or an Application Load Balancer (ALB) to control incoming web traffic. WebACLs allow you to define the order in which rules are evaluated.
9. **Logging and Monitoring:**
    - AWS WAF integrates with AWS CloudWatch to provide detailed logging and monitoring of web requests and security events. You can use CloudWatch Metrics and Alarms to gain insights into your web application's security.
10. **Integration with AWS Services:**
    - AWS WAF seamlessly integrates with other AWS services, such as Amazon CloudFront, AWS Application Load Balancer (ALB), and Amazon API Gateway. This allows you to protect your applications at the edge or within your infrastructure.
11. **Custom Rules with AWS Lambda:**
    - AWS WAF allows you to create custom rules using AWS Lambda functions. This gives you the flexibility to implement custom logic for inspecting and blocking requests based on your specific requirements.
12. **Security Automations and AWS Marketplace:**
    - AWS WAF integrates with AWS Security Automations for automated responses to security events. Additionally, you can explore the AWS Marketplace for third-party WAF solutions and rule sets.