WAF & Shield

AWS Certified Security Specialty SCS-C02

WAF (Web Application Firewall)

The Amazon Web Application Firewall (WAF) service is used to protect web applications from common attacks at the Layer 7 application layer (which includes HTTP).

WAF safeguards applications from attacks such as SQL Injection and Cross-Site Scripting (XSS). However, WAF is not designed to protect against DDoS attacks; for that, we use AWS Shield. We will discuss Shield in more detail later.

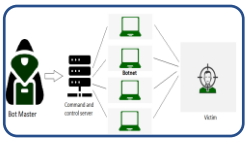
Additional Section:

SQL Injection

targets databases by injecting malicious SQL queries through input fields, like login forms. Attackers manipulate the database to extract, modify, or delete sensitive information. For instance, an unvalidated input could allow access to all user data.

Cross-Site Scripting (XSS)

attacks involve injecting malicious scripts into websites. These scripts can steal session cookies or redirect users to harmful sites. For example, a script may capture sensitive user information and send it to the attacker.



DDoS (Distributed Denial of Service)

A DDoS attack floods a server with excessive traffic from multiple sources, overwhelming its resources and causing service disruption. This is often executed via botnets, making it difficult to stop.

It provides protection using a Web ACL (Access Control List), which contains rules that define how requests are handled.

Types of Rules:

1. **IP Filtering:** Filtering IP addresses.
2. **HTTP Headers/Body:** Inspecting the components of requests.
3. **Geo Match:** Allowing or blocking requests based on geographic location.
4. **Rate-Based Rules:** Tracking the number of requests to identify suspicious activity.
5. **Managed Rules:** Providing over 190 pre-configured rules from AWS or vendors, such as:
    - Baseline Rule Groups: For general threat protection.
    - Use-case Specific Rule Groups: For protection against specific threats (e.g., SQL Injection or WordPress).
    - IP Reputation Rule Group: Blocking requests based on the reputation of the IP address.
    - Bot Control: Blocking and managing requests from bots.

AWS Shield

AWS Shield is a managed DDoS (Distributed Denial of Service) protection service designed to safeguard AWS infrastructure from various types of DDoS attacks.

Types of AWS Shield:

1. **AWS Shield Standard:**

- Cost: Free and automatically enabled for all AWS customers.
- Protection Against:
    - ❖ SYN & UDP floods
    - ❖ Reflective attacks
    - ❖ Attacks on Layer 3 and Layer 4 (network and transport layers)

2. **AWS Shield Advanced:**

- Cost: Approximately $3,000 per month per organization.
- Advanced Protection: Provides enhanced security against complex DDoS attacks targeting services such as:
    - ❖ Amazon EC2
    - ❖ Elastic Load Balancing
    - ❖ Amazon CloudFront
    - ❖ Global Accelerator
    - ❖ Route 53
- Additional Features:
    - ❖ 24/7 access to the AWS DDoS Response Team for real-time assistance during attacks.
    - ❖ Protection against potential high costs incurred from DDoS attacks.
    - ❖ Automatic mitigation of Layer 7 DDoS attacks, including the dynamic creation and deployment of WAF (Web Application Firewall) rules to counteract threats.