Amazon WAF Use Case

Amazon WAF Client Project: Enhancing Web Application Security

GENERAL CHARACTERISTICS

Intent	To protect a financial services company's online banking platform against web application attacks by using Amazon Web Application Firewall (WAF).
Scope	Deployment of Amazon WAF to filter malicious web traffic, prevent DDoS attacks, and ensure compliance with PCI DSS regulations.
Level	System-level.
Client	Confidential (Financial Services Company).
Last Update	[Today's Date]
Status	Finalized.
Stage	Implementation and Monitoring.

ACTORS

Primary Actor	Web Application Security Engineer
Secondary Actors	Solution Architect, Network Engineer, IT Security Team.

PREREQUISITES

Static Preconditions	- AWS account with the necessary permissions. - Amazon WAF, AWS Shield, and AWS CloudWatch services enabled.
Dynamic Preconditions	- Web application traffic pattern analysis. - Security and compliance requirements for PCI DSS and GDPR.
Assumptions	- The client's web application is hosted on AWS infrastructure. - WAF can effectively block malicious traffic patterns and comply with regulatory standards.

TRIGGERS

Trigger Event	The client needs to protect their online banking platform against rising cyber threats, including DDoS, SQL injection, and cross-site scripting (XSS).

Amazon WAF Use Case

EXPECTED OUTCOME

Success Postcondition	The client's online banking platform is fully protected from web application attacks, achieving PCI DSS compliance.
Failed Postcondition	Web application vulnerabilities are exploited, leading to potential downtime or data breach incidents.

OPERATIONS AND CONCEPTS

Operations	1. Deployed Amazon WAF to filter malicious web traffic and prevent unauthorized access. 2. Configured managed WAF rules to block common threats such as SQL injection and XSS. 3. Integrated AWS Shield for additional DDoS protection. 4. Set up real-time monitoring and alerts using Amazon CloudWatch for malicious activity. 5. Enabled AWS Config and CloudTrail for compliance tracking and auditing. 6. Conducted regular security tests and audits to validate the solution.
Concepts	- Amazon WAF: Managed firewall that protects web applications from common exploits. - AWS Shield: Protection against DDoS attacks for applications hosted on AWS. - CloudWatch: Monitoring service to track performance and security metrics. - CloudTrail: AWS service for logging and auditing API activity. - PCI DSS Compliance: Standards for securing payment card data in the banking sector.

MAIN SUCCESS SCENARIO

Step 1	Assessed the client's web application and security needs, focusing on threat vectors such as SQL injection and DDoS attacks.
Step 2	Deployed Amazon WAF to protect the online banking platform from web application vulnerabilities.
Step 3	Configured AWS WAF to block common attack patterns, including SQL injection, cross-site scripting (XSS), and bots.

Amazon WAF Use Case

Step 4	Integrated AWS Shield to enhance protection against volumetric DDoS attacks.
Step 5	Set up real-time traffic monitoring and alerting using Amazon CloudWatch to detect suspicious activity.
Step 6	Enabled AWS Config and CloudTrail to ensure auditability for PCI DSS compliance and maintain security logs.
Step 7	Conducted penetration testing to simulate attack attempts and verify the effectiveness of the WAF solution.
Step 8	Delivered a secure and compliant web application firewall solution, ensuring the availability and integrity of the online banking platform.