Scholarship #1 Group #2

Azure WAF (Web Application Firewall) Scenario

Scenario Overview: A company, *GlobalRetail Corp*, operates a web application serving customers worldwide. Due to increasing security concerns and malicious traffic from various sources, the company has decided to implement a Web Application Firewall (WAF) solution to protect the application.

The company's security policy mandates that access to the application should be restricted to users from a specific country, and any traffic originating from outside this country should be blocked. Additionally, the WAF should be configured to detect and prevent bad requests, such as SQL injections or cross-site scripting (XSS) attacks, and to route traffic based on URL patterns for specific application services.

As an Azure Administrator, you are tasked with designing and implementing a WAF solution in Azure that meets these requirements. The solution will be deployed in a single Azure region and must demonstrate security and traffic management features.

Goals:

1. **Implement a WAF Solution**: Design and implement an Azure WAF to protect the web application from malicious traffic, with deployment in a single region.

2. **Country-Specific Access Control**: Configure the WAF to restrict access to the application based on geographical location, allowing traffic only from a specified country.

3. **Bad Request Prevention**: Ensure that the WAF is capable of detecting and blocking bad requests, including common web vulnerabilities like SQL injection, XSS, and more.

4. **Traffic Routing Based on URL**: Implement a routing solution that directs traffic to different back-end services based on the URL path requested by the user.

Student Notes:

- **Architectural Design**: You must design the solution around the company's requirements, selecting the best Azure services for implementing the WAF in a single region.

- **Country-Specific Access**: Design a policy to limit access based on country origin.

- **Bad Request Detection**: Ensure that the WAF is configured to detect and block common attack vectors such as SQL injection, XSS, and other threats. Demonstrate how the WAF responds to and prevents malicious requests.

- **Traffic Routing**: Design a solution to route incoming traffic to different application services based on specific URL patterns (e.g., /api/*, /admin/*). Consider how this routing can be efficiently managed and integrated into the WAF configuration.

- **Monitoring and Alerts**: Set up monitoring for the WAF and application traffic, with alerts configured for any detected security violations or blocked requests. Ensure the WAF logs can be analyzed for insight into traffic patterns and potential attacks.

Important Considerations:

- **Security and Performance**: Your design must prioritize security while ensuring the performance of the application is not compromised.

- **Cost Management**: Consider the cost implications of deploying a WAF in a single region, ensuring that your design is cost-effective without sacrificing security or availability.

Expectations:

- **Design Flexibility**: You have the freedom to select and configure the appropriate Azure services for this scenario. Justify your choices in terms of security, performance, and cost efficiency.

- **WAF Configuration**: Demonstrate a well-configured Azure WAF that meets the company's requirements for geographical restrictions, bad request blocking, and URL-based traffic routing.

- **Country Access Control**: Successfully block traffic from outside the designated country and allow only the selected country to access the application.

- **Bad Request Prevention**: Show how the WAF can identify and block malicious requests, ensuring the web application is protected from common vulnerabilities.

- **Traffic Management**: Implement URL-based routing, directing requests to different services based on the URL path.

In this scenario, students are expected to demonstrate their knowledge of Azure WAF, security policies, and traffic routing through a secure, efficient, and compliant design.