Home / Dashboard / My Courses / AWS Certified Security Specialty / Web Application Firewall (WAF) - Quiz / Report

← Back to the **Course**

Level: Advanced

AWS Certified Security Specialty

Web Application Firewall (WAF) - Quiz

Completed on **Sun, 27 Feb 2022**

1st
Attempt

0/5
Marks Obtained

0.00%
Your Score

0h 0m 3s
Time Taken

FAIL
Result

Domain wise Quiz Performance Report

Join us on Slack community

No.	Domain	Total Question	Correct	Incorrect	Unattempted
1	Other	5	0	0	0
Total	All Domains	5	0	0	0

Review the Answers

Filter By All Questions

Question 1

Unattempted

Domain: Other

A company is planning to host an application that will consist of the following layers.

A set of EC2 Instances hosting the web layer.

A database set on an RDS Instance.

S3 static websites that have global customers.

You need to ensure that you use the AWS WAF service as a defensive firewall against your system. Which of the following would you need to have to ensure this integration is possible? Choose 2 answers from the options given below.

A. Place an Application Load Balancer in front of the EC2 Instances. right

B. Place a Network Load Balancer in front of the EC2 Instances.

C. Place a Cloudfront distribution to serve the contents in the S3 bucket. right

D. Place a Cloudfront distribution in front of the database instance.

Explanation:

Answer – A and C

This is mentioned in the AWS Documentation.

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, CloudFront or an Application Load Balancer responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You also can configure CloudFront to return a custom error page when a request is blocked.

Option B is invalid because the WAF service supports the Application Load Balancer.

Option D is invalid because the CloudFront distribution should be placed in front of the S3 static websites.

For more information on Web Application Firewall, please visit the below URL

https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html

Ask our Experts

⊕ View Queries

View Queries

Question 2 Unattempted

Domain: Other

A company is hosting a web application that is sitting behind an Application Load Balancer. You use a WAF web ACL to protect the Application Load Balancer against SQL injection and other types of web layer attacks. You need to enable logging to get detailed information about the traffic that is analyzed by your web ACL. Which of the following would you need to have in place for this requirement to be fulfilled?

Choose 2 options.

A. Enable the web ACL logging in the AWS WAF Console. right

B. Use ALB access logs to get detailed information about WAF deny rules.

C. Create an Amazon Kinesis Data Firehose for the WAF logging. right

D. Place a Cloudfront distribution behind the ELB.

Explanation:

Answer – A and C

This is mentioned in the AWS Documentation.

You can enable logging to get detailed information about the traffic that is analyzed by your web ACL. Information contained in the logs includes the time that AWS WAF received the request from your AWS resource, detailed information about the request, and the action for the rule that each request matched.

To get started, you set up an Amazon Kinesis Data Firehose. As part of that process, you choose a destination for storing your logs. Next, you choose the web ACL that you want to enable logging for. After you enable logging, AWS WAF delivers logs through the firehose to your storage destination.

> Option B is incorrect since access logs for the ALB only say that the request was blocked because of WAF - 403 error code. However, it doesn't provide information on the WAF rules.
>
> Option D is incorrect since you don’t necessarily need to add the Cloudfront distribution for getting the logging information.

For more information on Web Application Firewall logging, please visit the below URL

https://docs.aws.amazon.com/waf/latest/developerguide/logging.html

Ask our Experts

View Queries

Question 3 Unattempted

Domain: Other

A company is hosting a web application that is sitting behind an Application Load Balancer. The IT Security team needs to respond to possible layer 7 DDoS attacks in the most efficient time possible. Which of the following 2 actions can help achieve this?

A. Use the AWS WAF service and set up ACLs to respond to the DDoS attacks. right

B. Use the AWS Shield Advanced service to protect against the DDoS attacks. right

C. Enable AWS Shield and engage the AWS DDoS Response Team (DRT).

D. Use AWS GuardDuty.

Explanation:

Answer: A and B

AWS Docs provides the following details.

If DDoS alarms in CloudWatch indicate a possible layer 7 attacks, you have two options.

· Investigate and mitigate the attack on your own: If you determine that activity represents a DDoS attack, you can create your own AWS WAF rules to mitigate the attack. AWS WAF is included with AWS Shield Advanced at no additional cost. AWS provides pre-configured templates to get you started quickly.

· If you are an AWS Shield Advanced customer, you also have the option of contacting the AWS Support Center: If you want assistance in applying mitigations, you can contact the AWS Support Center. Critical and urgent cases are routed directly to DDoS experts. With AWS Shield Advanced, complex cases can be escalated to the DRT, which has deep experience in protecting AWS, Amazon.com, and its subsidiaries.

Option C is incorrect because AWS Shield is enabled by default and you need to enable AWS Shield Advanced to engage AWS DDoS Response Team (DRT).

Option D is incorrect because GuardDuty detects unauthorized and unexpected activities in your AWS environment. It does not help to respond to layer 7 DDoS attacks.

For more information on responding to DDoS attacks, please visit the below URL https://docs.aws.amazon.com/waf/latest/developerguide/ddos-responding.html

Ask our Experts

⊕ View Queries 👍 👎

Question 4 Unattempted

Domain: Other

A company is hosting a web application that is sitting behind an Application Load Balancer. There is a plan to use the AWS WAF service to protect the application from various sorts of attacks. There is also a requirement to prevent traffic from a specific country. How can this be achieved?

A. Create an IP Match Condition in the WAF web ACL.

B. Create a Geographic Match Condition rule and add the rule in the WAF web ACL. right

C. Create a Geographic Match Condition and add the condition in the WAF rule group. Activate the rule group.

D. Create a Geographic Match Condition in WAF web ACL and add the ACL in the WAF rule. Activate the rule.

Explanation:

Answer - B

This is mentioned in the AWS Documentation.

If you want to allow or block web requests based on the country that the requests originate from, create one or more geo match conditions. A geo match condition lists countries that your requests originate from. Later in the process, you specify whether to allow or block requests from those countries when you create a web ACL.

Option A is incorrect since this is used to allow or block requests based on the IP addresses that they originate from.

Option C is incorrect because the rule group should be added to the web ACL. The rule group itself cannot be activated.

Option D is incorrect because the Geographic Match Condition should be created in a rule group instead of the web ACL, and you cannot add a web ACL to a rule. The description of the option is inaccurate.

For more information on working with Web ACL geo conditions, please visit the below URL

https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-geo-conditions.html

Ask our Experts

⊕ View Queries 👍 👎

Question 5 Unattempted

Domain: Other

Your company hosts multiple web applications in AWS EC2 and the AWS WAF service is used to protect the applications against the attacks in the HTTP(S) layer 7. To meet the company's security policies, you need to ensure that the same protection rules are applied for all the WAF ACLs. Which of the following would help to achieve this requirement?

A. Purchase managed rule groups in AWS Marketplace and configure all WAF ACLs to use the rule groups.

B. Create custom rule groups in AWS WAF and configure all WAF ACLs to use the rule groups. right

C. Create a WAF template that contains the required rules. Use the template for the WAF ACLs.

D. Create the WAF conditions that include the required rules. Apply the conditions in all the WAF ACLs.

Explanation:

Answer - B

Option A is incorrect because there is no need to purchase rules in AWS Marketplace. This is not a cost-efficient method.

Option B is CORRECT because rule groups in AWS WAF can be created with the required conditions that are used for all the WAF ACLs.

Option C is incorrect because AWS WAF does not have the concept of the template. Rule groups should be used in this scenario.

Option D is incorrect because WAF rule groups should be created with the required conditions. For any WAF ACL, you can apply the rule groups.

Ask our Experts

⊕ View Queries

👍 👎

Finish Review

Certification

Cloud Certification

Java Certification

PM Certification

Big Data Certification

Company

Become Our Instructor

Support

Discussions

Blog

Business

Support

Contact Us

Help Topics

Join us on Slack!

Join our open **Slack community** and get your queries answered instantly! Our experts are online to answer your questions!

WHIZLABS © 2022, Whizlabs Education INC.