Best practices for Amazon CloudFront, AWS WAF, and Shield

Contents

Introduction

In the present times, software applications are in high demand. However, the intensity of cyber-attacks and hacking has also increased with the same speed. Customers not only want applications that serve their purpose but are secure, well-monitored, and protected concerning the attacks. To come up with such an application additional layers of security added in your architecture are the key.

This article covers the three amazing tools you can use to increment the security layers on your applications providing your customers with fast and secure results. These tools include Amazon CloudFront, AWS WAF, and AWS shield.

Let's take a look at them one by one.

Overview

Each of these tools is responsible for one additional security layer to your architecture. Following is a short description of each of them:

Amazon CloudFront

Amazon CloudFront is responsible for the secure and fast delivery of content to your end-users. It also comes in hand with the features of securing your application by making use of the compliance standards such as ISO 27001, ISO 9001, and a lot more. It distributes the content delivery among the edges around the globe. The users can access the content via the closest edge to them, making the content delivery faster. It keeps the origin of applications secured by setting up the edges as the primary source of content delivery.

AWS WAF

AWS WAF allows you to create a firewall to protect against DDoS attacks. These attacks are based on the wastage of resources in such a way that they are no longer available for the end-users. The attacks can be of few minutes, such as short-lived attacks or exponential ones such as the larger DDoS attacks. The main job of the Web Application Firewall is to categorize the customer-specific requests so that the application resources can be saved from the common attacks.

AWS Shield

AWS Shield adds a third layer of security to your application making it highly secure from DDoS attacks. It also allows you to visualize the changes so that you can take the relevant steps towards them. There are two versions of AWS Shield available, such as standard and advanced. AWS Standard Shield does not hold any additional cost. Whereas the AWS Advanced Shield comes in hand with the extensive features and incremented cost.

Requirements

This section highlights the security and accessibility features that you should use from each of these tools.

Amazon CloudFront

With Amazon CloudFront you can set up the conditions and restrictions towards the accessibility of content in the following ways:

1. ***Configure CloudFront for HTTPS:***

You can configure your CloudFront in a way that your users use HTTPS to access the content. And also utilize it for the retrieval of objects from the origin. By this configuration, you can encrypt the communication from both ends, such as the request from the user and the retrieval of objects from the origin.

2. ***Choosing the Security Policy:***

If you opt for the HTTPS configuration, you need to select one of the security policies. These policies are responsible for setting up the minimum SSL/TLS requirements so that the request from the users fulfilling those could be catered only. It also chooses the cipher that CloudFront will use to encrypt and decrypt the data during the communication.

3. ***Choosing the domain type:***

You need to choose if you want to use your domain name in the files or the one with the CloudFront involved in it. After making the key choice of a domain type, you can follow the right steps to make it work.

4. ***Signed URLs or Signed Cookies***

CloudFront allows you to put a restriction in place for the users to access your content. This restriction can be in the form of a signed URL or signed cookies. CloudFront analyses the request and if it fulfils the criteria of the one set by you, it allows the content access.

5. ***Access Restriction to Amazon S3***

For better security, you need to restrict the access of your users to the Amazon S3. For that, you ought to create an Origin Access Identity which is responsible for retrieving the data from the origin and make it accessible to the users. It is necessary to ensure that the URLs provided to the user do not allow them direct access to the Amazon S3 bucket.

6. ***Access Restriction to Application Load Balancer***

The access of content via Application Load Balancer allows the utilization of CloudFront functionalities. So, you need to restrict the access of your users to it for making the best use of CloudFront features.

7. ***Geo-Blocking***

Amazon CloudFront allows you to restrict content access from certain geographical locations. You can make use of this feature by built-in CloudFront geo-blocking functionality or third-party applications.

8. ***Field-Level Encryption***

Encrypting the data at the closest edge from which the user requests is the best possible way to ensure the security of sensitive data throughout the application. Field-level encryption is the feature that provides you with the aforementioned functionality.

AWS WAF And AWS Shield

Following are the security restrictions and conditions you can impose using AWS WAF and AWS Shield:

1. ***Protecting your data.***

To protect your data, you need to be conscious of your AWS account and its credentials. For this purpose, you can use Multi-Factor Authentication and SSL/TSL for communication. Encryption solutions, APIs, and advanced managed security services are the key.

2. ***AWS IAM***

Access to AWS WAF and AWS Shield requires the credentials of the account that are permitted to access the AWS resources. So, authenticate your accounts to be linked with them.

3. ***Monitoring***

Monitoring the data allows you to recover from multipoint failure. Collection and analysis of data from the AWS resources is an essential part of making the best use of AWS WAF and Shield.

4. ***Compliance Validation***

You can ensure that your system is following the compliance standards. The standards are dependent upon the sensitivity and approaches of your data processing. Third-party auditors are responsible for setting up the audit reports that you can download and analyse.

5. ***AWS Security Token Service***

The user requests should hold the signed key along with them. These IDs are linked with the Identity Access Management principles. You can also make use of temporary credentials for secure requests.

Best Practices

Following are the ten best practices you can utilize to make your application infrastructure secure and sound:

1. You can introduce the three layers of security on your application architecture by the use of AWS Cloud Front, AWS WAF, and AWS Shield to keep your system secured from all sorts of DDoS attacks.
2. Keeping the data in transition encrypted can play a significant role in ensuring security. It validates that no data is disclosed throughout the process of data communication and transfer.
3. You can make use of the built-in functionality of CloudFront, WebSocket Support that allows you to improve the user performance for real-time applications. It reduces the latency and delay in communication and can be beneficial for the scenarios like trading or gaming.
4. Making the security metrics visible is a key functionality of improving the overall security of the application. CloudWatch metrics, Sample web requests, and full logs are the functionalities of AWS WAF that can help you with this.
5. You can make use of the AWS Shield Lambda Engagement to notify the DDoS Response Team who can help you out with the direct reply to your problem in the case of an emergency. These emergencies include sudden DDoS attacks.
6. With the AWS Advanced shield, you can use the functionality of the Global Threat Environment Dashboard that holds the record of all the anomalies being handled by the AWS. It gives you insights and allows you to make an understanding about the possible attacks.

7. You can analyse your web traffic using the functionality of VPC flow logs. It allows you to view all the IP traffic that is involved in the communication from and to your network in the AWS virtual private cloud.
8. Utilizing the Elastic IPs by registering them as Protected Resources (if you are registered for AWS Advanced Shield), you can reduce the time to mitigate an attack as these attacks are detected quickly.
9. For improving the security of your origin, you can allow the AWS Lamba functionalities to automatically update the rules of security groups leading to allow the traffic from Amazon CloudFront only.
10. You can make use of Network Access Control Lists to filter out the traffic and control levels of the network reducing the chances of attacks.

Amazon CloudFront along with the AWS WAF and AWS Shield can highly improve the security of your application by keeping the communication between the user and application encrypted and providing comprehensive protection against DDoS attacks.

References

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

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

https://medium.com/@Excellarate/web-application-security-using-aws-waf-and-aws-shield-e92c38ebad14

https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/

https://www.slideshare.net/AmazonWebServices/best-practices-for-security-at-scale

https://stackarmor.com/protecting-against-a-distributed-denial-of-service-ddos-attack-using-aws/

https://pilotcoresystems.com/insights/eight-benefits-of-combining-aws-cloudfront-with-waf-and-shield