

Deploying a Secure Static Website on AWS with WAF Protection

Abid Jeem

March 12, 2025

1 Introduction

This document outlines the step-by-step process of deploying a secure static website on AWS using Amazon S3, Route 53, CloudFront, and AWS WAF. Screenshots are included to illustrate each stage of the deployment.

2 Setting Up Route 53

What is Route 53?

- A scalable DNS and domain name registration service.
- Allows the creation of endpoints for routing user requests to specific applications.


3 Enabling CloudFront with HTTPS

3.1 Why CloudFront?

- Enables HTTPS with caching for better security and performance.
- Requires an SSL/TLS certificate from Amazon Certificate Manager (ACM).

3.2 Requesting an SSL Certificate

1. Navigate to **Certificate Manager** in AWS.
2. Request a public certificate using DNS validation.
3. Use RSA 2048-bit encryption for security.
4. Once validated, create DNS records in Route 53 by clicking the automated option in ACM.



Request public certificate

Domain names
Provide one or more domain names for your certificate.

Fully qualified domain name [Info](#)

[Remove](#)

[Remove](#)

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Figure 1: SSL Certificate request process in ACM.

4 Configuring CloudFront

1. Navigate to CloudFront and create a new distribution.
2. Set the **Origin Domain** by copying the "Static Website Hosting" endpoint from S3.
3. Under **Viewer Protocol Policy**, select **Redirect HTTP to HTTPS**.
4. In **Custom SSL Certificate**, choose the previously created certificate.
5. Under **Alternative Domain Name (CNAME)**, enter the **www** version of your static site.
6. Enable **AWS WAF** for additional security.

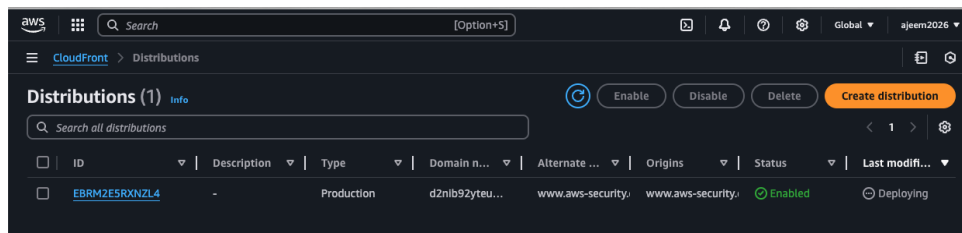


Figure 2: CloudFront distribution setup with HTTPS.

5 Creating Non-WWW Distribution

1. Repeat the CloudFront setup process for the non-www version of the website.
2. Now, both www and non-www versions have distributions.

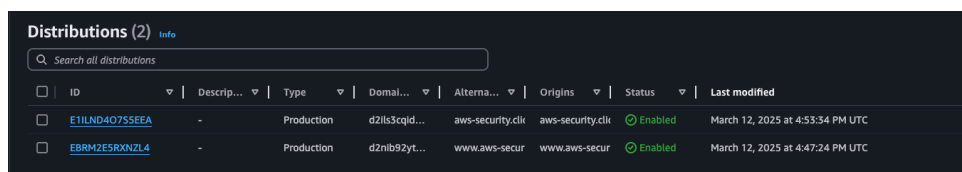


Figure 3: CloudFront distributions for both www and non-www versions.

6 Final Configurations: Securing with HTTPS and Updating Route 53

6.1 Enforcing HTTPS in S3

1. Navigate to S3 and edit the **Static Website Hosting** settings.
2. Change the protocol from HTTP to HTTPS.

6.2 Updating Route 53 Records

1. Find the two CNAME records in Route 53.
2. Locate the **A** record and edit it.
3. Change **Route traffic to** from **Alias to S3 website endpoint** to **Alias to CloudFront distribution**.
4. Select the correct distribution from the system-suggested options. Repeat this process for other.

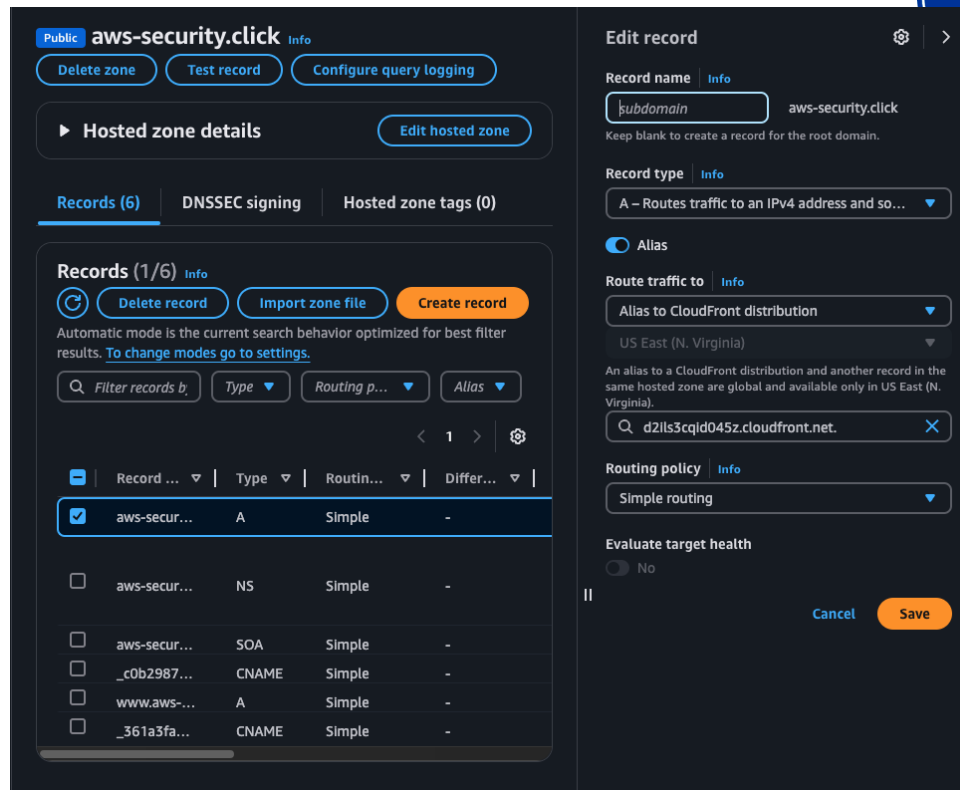


Figure 4: Updating Route 53 records to point to CloudFront.

7 Conclusion

By following these steps, I have successfully deployed a secure static website using AWS S3, Route 53, CloudFront, and AWS WAF. This setup ensures:

- Secure HTTPS access using CloudFront and ACM.
- Optimized routing via Route 53.
- Protection against threats with AWS WAF.

This project showcases my ability to architect, deploy, and secure cloud-based applications, demonstrating my expertise in AWS infrastructure and security.