Customize 403 error pages from Amazon CloudFront Origin with Lambda@Edge

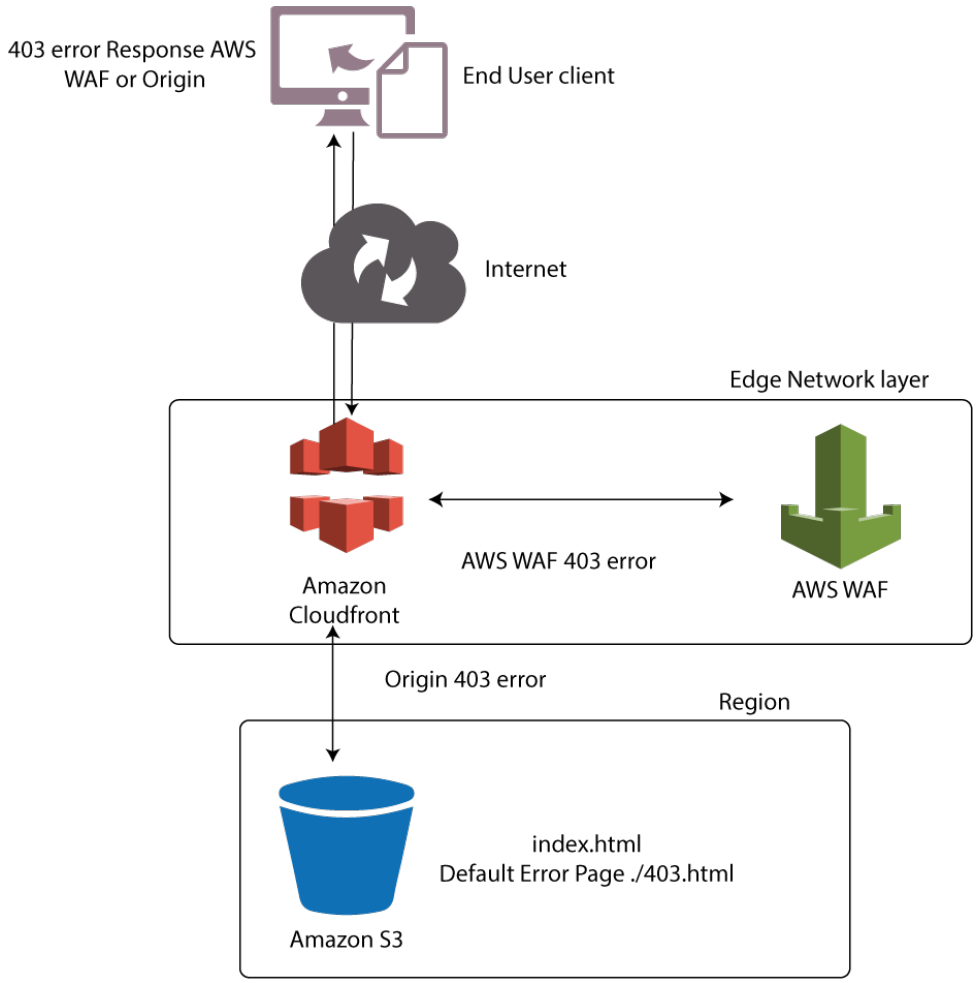
Description:

AWS Web Application Firewall (AWS WAF) is commonly used to protect HTTP and HTTPS requests forwarded to Amazon CloudFront. When you are using this approach, default 403 error pages do not distinguish whether the error came from AWS WAF or the CloudFront Origin.

As an AWS WAF and Amazon CloudFront user, you may want to customize your end-user experience for the HTTP 403 error based on whether the request was blocked by AWS WAF (unauthorized access) or by the Origin (page not found at the Origin).

Scenario:

A customer has set up an AWS WAF on Amazon CloudFront distribution. Currently, the customer is unable to show their end-users' client a custom error page based on whether the request is blocked by AWS WAF (AWS WAF 403 error) or whether the requested resource is forbidden by the Origin (Origin 403 error)**.**

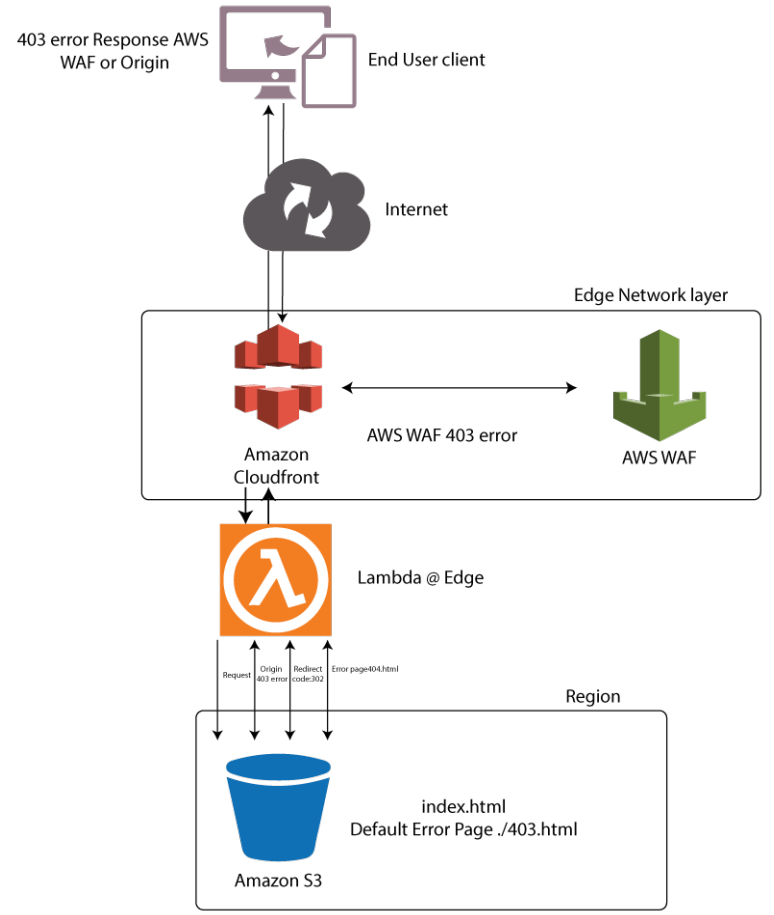


Current infrastructure

Challenge/Requirement:

Use Lambda@Edge functions to display customized error pages or mask 4XX error pages, based on where the error originated.

Reference Solution Architecture:


403 error Response AWS WAF or Origin
End User client
Internet
Edge Network layer
AWS WAF 403 error
Amazon Cloudfront
AWS WAF
Lambda @ Edge
Request
Origin 403 error
Redirect code:302
Error page404.html
Region
index.html
Default Error Page ./403.html
Amazon S3