**# cloudfront-sg-ip-update**

This repository will help you to update Cloudfront and WAF ip address into security group

**Steps to implement solution.**

1. Ready Lambda code with s3 bucket. Bu default i put Ireland region.

* If you are working with Other region. Create one s3 bucket and upload code.zip file and make it public accessible.

1. Execute template cloudfront-ip-update.yml and fill parameters. VPC, S3 bucket and object.

* This Cloudformation will create 4 security group. 2 for https (global and Region) and 2 for http (global and region), lambda function, IAM role for lambda

1. Manually test lambda function to update latest IP into Security group.

* Test Lambda fucntion by following Event sample.

{

"Records": [

{

"EventVersion": "1.0",

"EventSubscriptionArn": "arn:aws:sns:EXAMPLE",

"EventSource": "aws:sns",

"Sns": {

"SignatureVersion": "1",

"Timestamp": "1970-01-01T00:00:00.000Z",

"Signature": "EXAMPLE",

"SigningCertUrl": "EXAMPLE",

"MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",

"Message": "{\"create-time\": \"yyyy-mm-ddThh:mm:ss+00:00\", \"synctoken\": \"0123456789\", \"md5\": \"7fd59f5c7f5cf643036cbd4443ad3e4b\", \"url\": \"https://ip-ranges.amazonaws.com/ip-ranges.json\"}",

"Type": "Notification",

"UnsubscribeUrl": "EXAMPLE",

"TopicArn": "arn:aws:sns:EXAMPLE",

"Subject": "TestInvoke"

}

}

]

}

* you find in logs that test has been failed due to md5 checksum. Copy updated md5 from Error logs (Ex. "got 2e967e943cf98ae998efeec05d4f351c expected") and update into Event logs.

1. change your region to N.Virginia(us-east-1) and update sns subcription with following steps and detail.

* go to sns service (N.virginia region only)
* Subscription
* Create
* Topic Arn - arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged
* Protocol - AWS Lambda
* Paste Endpoint of Lambda function created by template
* Create

**Hint:-** you can find lambda function arn in from Cloudformation stack output section.