**MY EXPERIENCE: UPDATE AWS SECURITY GROUP FIREWALLS USING AUTOMATION WITH AWS LAMBDA**

Earlier this year, I led a project aimed at enhancing an organization’s security by automating the update of AWS security group firewalls. The primary goal was to ensure that only traffic originating from Amazon CloudFront and AWS WAF IP ranges could access the company’s Amazon EC2 instances. This approach was necessary to prevent malicious requests from bypassing AWS WAF security rules and directly accessing the instances, which would pose a significant security and compliance risk.

The challenge arose from the dynamic nature of AWS IP ranges, which changes frequently. However, AWS notifies users of these changes via a public SNS topic, providing the service IP ranges in JSON format. In this regard, updating the security groups manually every time AWS releases new IPs is impractical and prone to errors. Thus, a more automated and reliable solution was needed.

To address this problem, I designed and implemented a solution that leveraged the integration between Amazon SNS and AWS Lambda. The key objective was to automate the process of updating security groups with the new IPs released by AWS, ensuring continuous protection without manual intervention.

I started by subscribing an SNS topic to AWS’s IP range notification service. This ensured that our system would receive updates whenever there were changes in the AWS service IP ranges. The SNS topic was configured to trigger an AWS Lambda function whenever a new notification was published.

I developed the Lambda function using Python 3.7, focusing on parsing the JSON data received from the SNS topic. The function extracted the relevant IP ranges for CloudFront and AWS WAF from the JSON data. Once the IP ranges were identified, the Lambda function updated the Security Groups accordingly. This involved adding new IP ranges to the security group rules while removing any outdated entries.

To ensure that the Lambda function had the necessary permissions, I configured IAM roles and policies with the least privilege principle. These roles allowed the function to read the SNS messages, update the security group rules, and log its activities for monitoring and debugging purposes using CloudWatch.

This automated solution significantly enhanced the organization's security posture. By ensuring that only traffic originating from the CloudFront and AWS WAF IP ranges could access the backend EC2 instances, we effectively prevented potential security breaches that could bypass WAF rules. Additionally, the automation eliminated the need for manual updates, reducing the potential for human error and saving valuable time.