**Project**

**Info Security Sec A**

Aftab Arshad 22-11367

Shafay Ahmed 22-10198

Ali Asghar 21-10479

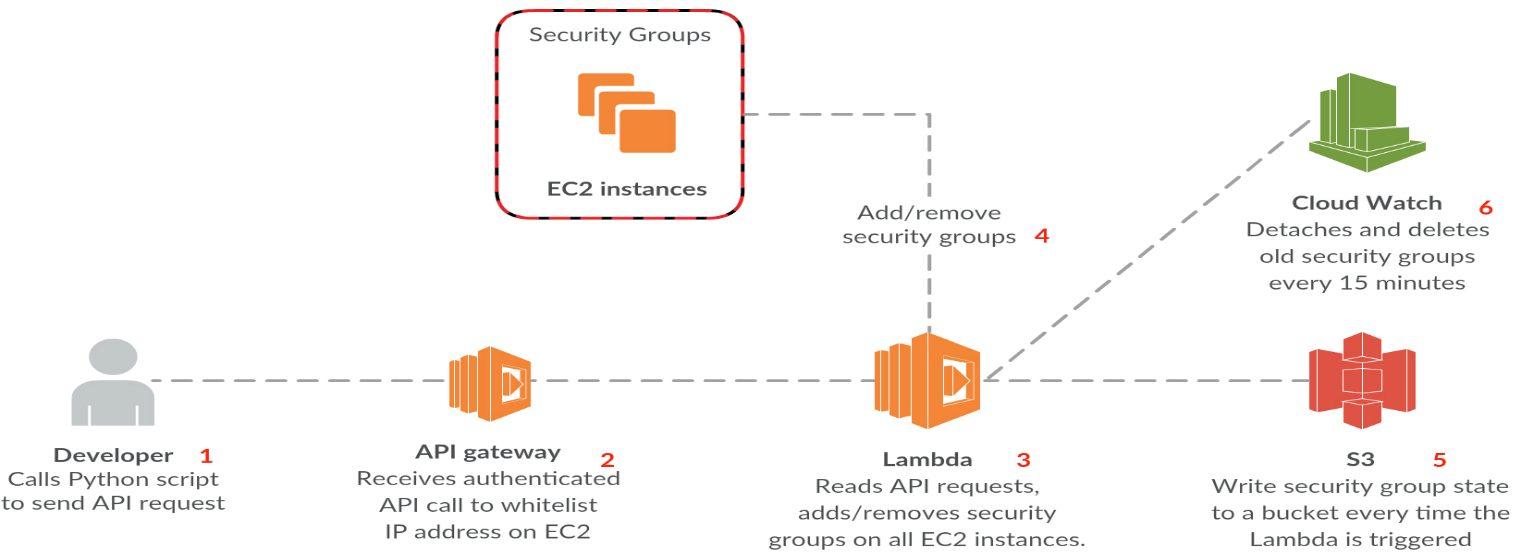
**aws-lambda-firewall-api**

Using a simple API request, you may create temporary security groups on your EC2 instances. Furthermore, you may simply audit your security groups by using automated reports sent to S3.

**Description**

The Lambda firewall can be utilized in critical areas where stringent control over security groups is required. Users with a valid API gateway key can request to whitelist an IP address for a set period of time without needing to enter the console. When a security group expires, it is automatically disconnected and deleted from the EC2 instances. You no longer have to manually add or remove security groups, which is especially handy for users who have many breakout IP addresses.

The steps how the Lambda firewall can be used are shown:



Aside from security group administration, the Lambda firewall will also publish the status of security groups to an S3 folder so that all security groups can be readily seen. This makes it very simple to inspect and verify which ports are exposed to the outside world at any given moment.

**Installation**

You need to install two things in order for the firewall to work;

1. Add the Lambda function to your account with handler "lambda\_function.handler" and configure it with proper IAM permissions to run, see "lambda\_function.py".

2. Set the correct bucket name in the lambda function to write logs to S3 - you can skip this by entering a blank bucket name.

3. Create an API gateway and map the correct GET parameters to the Lambda function.

4. Create API keys for users in the API gateway and deploy the gateway to production.

5. Next, create a trigger in CloudWatch so the Lambda function is called every 15 minutes to remove expired security groups.

6. Configure a valid API key and the correct Lambda URL in "firewall\_client.py" and distribute it to your users.

Make sure to use and enable CloudWatch logs if the Lambda function does not work.

Usage

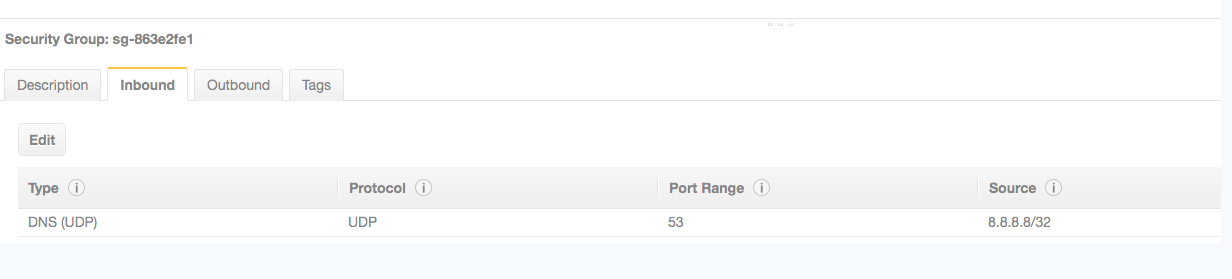
- Security groups are added by the firewall\_client which can be called manually by your users.

- Rules are removed when the function is called by the API gateway or when a valid API call is received.

If all steps are completed, users can whitelist an IP address and port simply by running "firewall\_client.py" with the correct parameters. If these are skipped, default values are used;

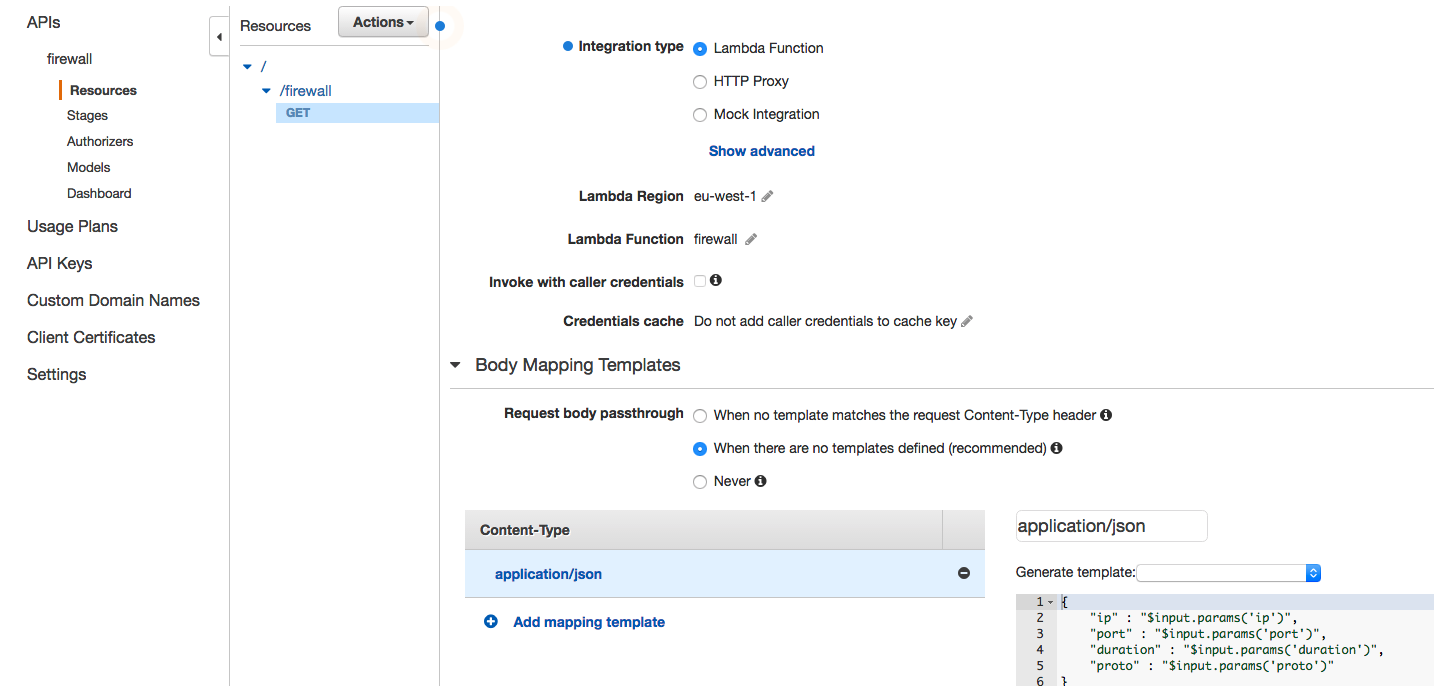
C:\Users\Ahmed\Desktop\aws-lambda-firewall-master\aws-lambda-firewall-master\docs\4.png

You should now see a new security group associated with all your EC2 instances;



The security group's name defines the source IP address that is whitelisted. The description includes two types of timestamps: the first two values reflect when the security group was established, and the final two define when it should be removed.

Configure the body templates of your API gateway as follows;



```json

{

"ip" : "$input.params('ip')",

"port" : "$input.params('port')",

"duration" : "$input.params('duration')",

"proto" : "$input.params('proto')"

}

```

Your API gateway method should look as follows;

