04 Security

July 2, 2020

1 AWS Sheild

AWS Sheild is a managed DDoS (Distributed Denial of Serives) protection that safeguard web applications running on AWS.

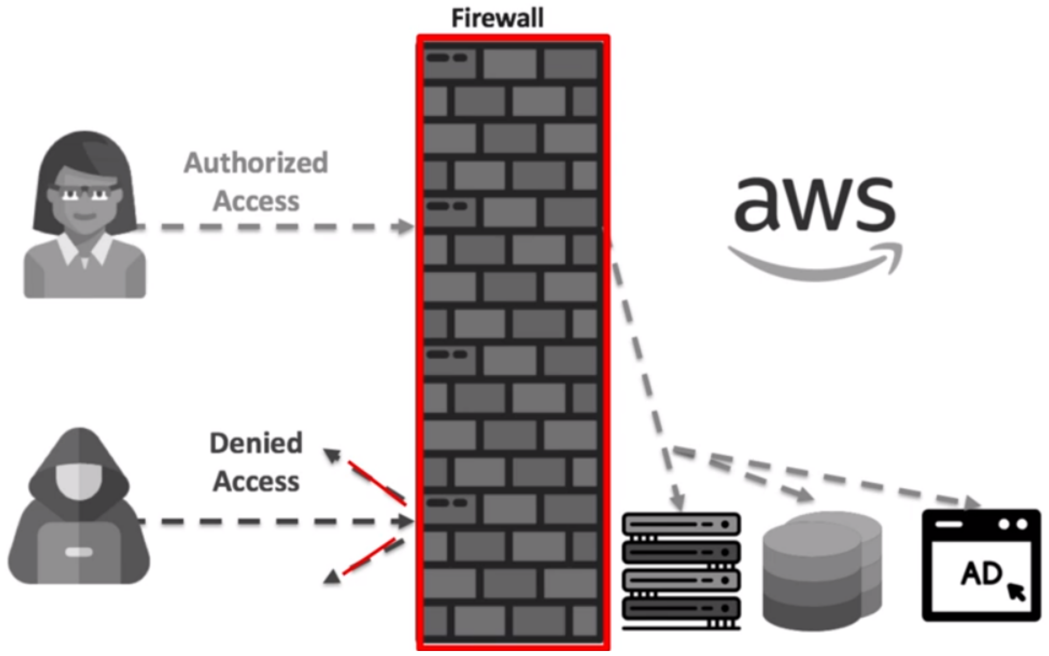
DDoS is basically when you make an application unavaiable by overwhelming it with traffic from multiple sources. When a server is overwhelmend, it crashes and can no longer serve requests

AWS Sheild is something you get out automatically, even for the free teir

2 AWS WAF

AWS WAF provides a firewall that protects your web applications

WAF can stop common web attacks by reviewing the data being sent to your application and stopping well-known attacks



Fire Walls Stop: - SQL Injection - Cross-site scripting - Reviewing Data Sent - Stopping well-known attacks

3 IAM

Identity and Access Management is an AWS service that allows us to configure who can access our AWS account, services or even applications running in our accoutn. IAM is a global service and is automatically available across ALL regions

4 Users

- We need to varify users
- make sure they can only see specific data
- the concept is called least privileged access

4.1 Account

- email account used to create account is root level
- root account has access to everything and must be secured

5 IAM User

- IAM User is an entity you create
- It represents a user/service
- The IAM User consists of a user name and access credentials

6 IAM Group

- is a collection of users
- grants premission for a collection of users

7 IAM Role

- is an identity
- the identity grants premissions
- these are not assoicated wit a user or group
- roles can be attached to a user and he can assume it temporarily

8 Policy

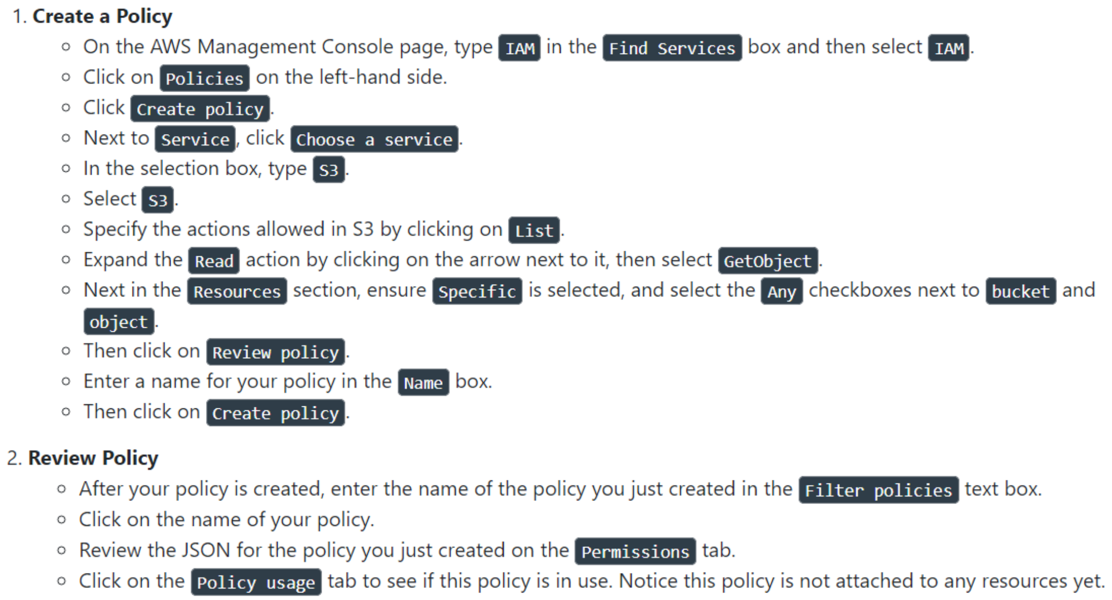
- Policy is a way to define granular premissions
- can be attached to users, groups and roles
- there are predefined policies you can use

9 EC2 Security Group

- Not a part of IAM
- Also not IAM security group
- EC2 security groups are associated with an EC2 instance

- they act as an built-in firewall for your virtual servers

10 IAM Lab



1. **Create a Policy**
   - On the AWS Management Console page, type `IAM` in the `Find Services` box and then select `IAM`.
   - Click on `Policies` on the left-hand side.
   - Click `Create policy`.
   - Next to `Service`, click `Choose a service`.
   - In the selection box, type `S3`.
   - Select `S3`.
   - Specify the actions allowed in S3 by clicking on `List`.
   - Expand the `Read` action by clicking on the arrow next to it, then select `GetObject`.
   - Next in the `Resources` section, ensure `Specific` is selected, and select the `Any` checkboxes next to `bucket` and `object`.
   - Then click on `Review policy`.
   - Enter a name for your policy in the `Name` box.
   - Then click on `Create policy`.
2. **Review Policy**
   - After your policy is created, enter the name of the policy you just created in the `Filter policies` text box.
   - Click on the name of your policy.
   - Review the JSON for the policy you just created on the `Permissions` tab.
   - Click on the `Policy usage` tab to see if this policy is in use. Notice this policy is not attached to any resources yet.