Lab 2 - Security Groups

Protect Your EC2 Instance with a Security Group

1. Objective

> Understand what AWS Security Groups are, why they're critical to EC2 security (stateful firewalls), and how they protect against brute-force and other network-level attacks. Then create or attach a Security Group that restricts SSH (port 22) access to just your own public IPv4 address.

2. Prerequisites

- An AWS Free Tier account with EC2 permissions
- A running Linux EC2 instance (or know how to launch one)
- A computer with internet access and a modern browser

3. Environment Setup

1. **Log in** to the AWS Management Console.
2. Navigate to the **EC2 Dashboard** in your chosen Region.
3. If you don't already have an instance:
   - Launch a **t2.micro** Amazon Linux 2 instance. Usually for playing around, people recommend the Virginia region or us-east-2 since it charges less (still you are on the free tier but just so you know that different regions can cost more or less)
   - Note its **Instance ID** and **Public IPv4** address.

4. Tasks

1. **Define Security Groups**
   In a short paragraph, describe:
   - What a Security Group is.
   - How stateful filtering works (inbound vs. outbound).
2. **Discover Your Public IP**

   ```
   curl https://checkip.amazonaws.com
   ```

   Record the returned address as `<YOUR_PUBLIC_IP>`.
3. **Create a Security Group**

- In the EC2 console, select **Security Groups** → **Create security group**.
- Name: `ssh-access-yourname`
- Description: “Restrict SSH to my IP”
- VPC: the same one as your EC2 instance
- Add an **Inbound rule**:
  - **Type**: SSH
  - **Port**: 22
  - **Source**: `<YOUR_PUBLIC_IP>/32`
- Leave Outbound at its default.
- Click **Create**.

4. **Attach to Your EC2 Instance**
   - Select your instance, then **Actions** → **Networking** → **Change security groups**.
   - Deselect any “0.0.0.0/0 SSH” group.
   - Select `ssh-access-yourname` and **Save**.
5. **Verify Access**
   - From your terminal:

     ```
     ssh -i /path/to/your-key.pem ec2-user@<EC2_PUBLIC_IP>
     ```

   - Confirm successful SSH login.
   - From a different network (e.g., mobile tether), attempt the same SSH command—confirm it’s blocked.

5. Commands and References

- **AWS CLI: Create & Authorize SG**

```
aws ec2 create-security-group \
  --group-name ssh-access-yourname \
  --description "Restrict SSH to my IP" \
  --vpc-id vpc-xxxxxxxx

aws ec2 authorize-security-group-ingress \
  --group-name ssh-access-yourname \
  --protocol tcp \
  --port 22 \
  --cidr YOUR_PUBLIC_IP/32
```

- **AWS CLI: Attach SG to Instance**

```
aws ec2 modify-instance-attribute \
  --instance-id i-0123456789abcdef0 \
  --groups sg-0123456789abcdef0
```

- **AWS Docs**
  - Security Groups for Your VPC: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html
  - create-security-group CLI reference: https://docs.aws.amazon.com/cli/latest/reference/ec2/create-security-group.html

6. Submit the Completed Lab

- **Screenshot** of either:
  - Your Security Group's Inbound rule, or
  - The EC2 instance's Security Groups tab
  (Mask any sensitive details like private keys or full IPs.)
- **Reflection** (1–2 sentences):
  - What you built (SG rules + attachment).
  - Any challenges encountered (finding IP, SSH issues, console navigation).

7. Further Reading and Resources for Study

AWS Security Groups Tutorials

- AWS Official Documentation: "Security Groups for Your VPC" https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html
- DigitalOcean: "How To Configure AWS Security Groups" https://www.digitalocean.com/community/tutorials/how-to-configure-aws-security-groups
- Linuxize: "AWS EC2 Security Groups Tutorial" https://linuxize.com/post/aws-ec2-security-groups/
- FreeCodeCamp: "Beginner's Guide to AWS Security Groups" https://www.freecodecamp.org/news/aws-security-groups-beginners-guide/

IPv4 Addressing for Beginners

- Cloudflare Learning Center: "What Is an IP Address? A Beginners Guide to IPv4 & IPv6" https://www.cloudflare.com/learning/ddos/glossary/internet-protocol-address-ip/
- DigitalOcean: "Introduction to IP Addressing" https://www.digitalocean.com/community/tutorials/an-introduction-to-ip-addresses

- HowToGeek: “IPv4 Addressing Explained: Netmasks, CIDR, and Classful Addressing” https://www.howtogeek.com/412719/what-is-cidr-and-how-does-it-work/
- FreeCodeCamp: “IP Addressing & Subnetting for Beginners” https://www.freecodecamp.org/news/ip-addressing-and-subnetting-for-beginners/