AIM: To study and Implement Security as a Service on AWS / Azure

THEORY:

- **Security as a Service:**
  - A business model called SECaaS, or Security as a Service, offers security to IT companies on a subscription basis. A superior security platform is provided by the outsourced approach, which lowers the total cost of ownership than the business could supply on its own.
  - With the use of cloud computing, security for the company is maintained by an outside party. For the necessary computational and storage resources to run their websites and apps, many enterprises rely on security services.
  - SECaaS is impressed by the "Security as a Service (SaaS)" model as applied to implement security kind services and doesn't need on-premises hardware, avoiding substantial capital outlays.
  - These security services typically embody authentication, antivirus, anti-malware/spyware, intrusion detection detection, penetration testing and security event management, among others. Security groups are fundamental to network security in AWS. They control how traffic is allowed into or out of our EC2 machine.

- **SECaaS as Service Provider:**
  No security platform is perfect, since they all have a number of weaknesses. Nothing provides services that are in line with our demands. Lack of complete control over security alternatives, susceptibility to shared technology, data breach, poor architecture, resource allocation, and many other issues may be problems associated with the outsourcing approach.

  Selecting efficient SECaaS suppliers is crucial to addressing these ongoing difficulties. Partnering with the right SECaaS requires experience and produces optimum production with a better profit.

  Focus on the following while choosing a provider :

1. It should be assured that the security team is available to respond to any system-related issues and inquiries.
2. To be able to respond to any potential threats, the provided solution must be adaptable.

3. It needs to be strong.
4. Following an investigation into the security issues, service suppliers must propose an exact resolution.
5. Endpoint and workload protection given through the cloud should be offered by IT providers.
6. Cloud security should be addressed by vendors.

SECaaS vendors work with organizations to develop security measures, verify acceptable frameworks and review financial commitments.

Benefits of SECaaS:

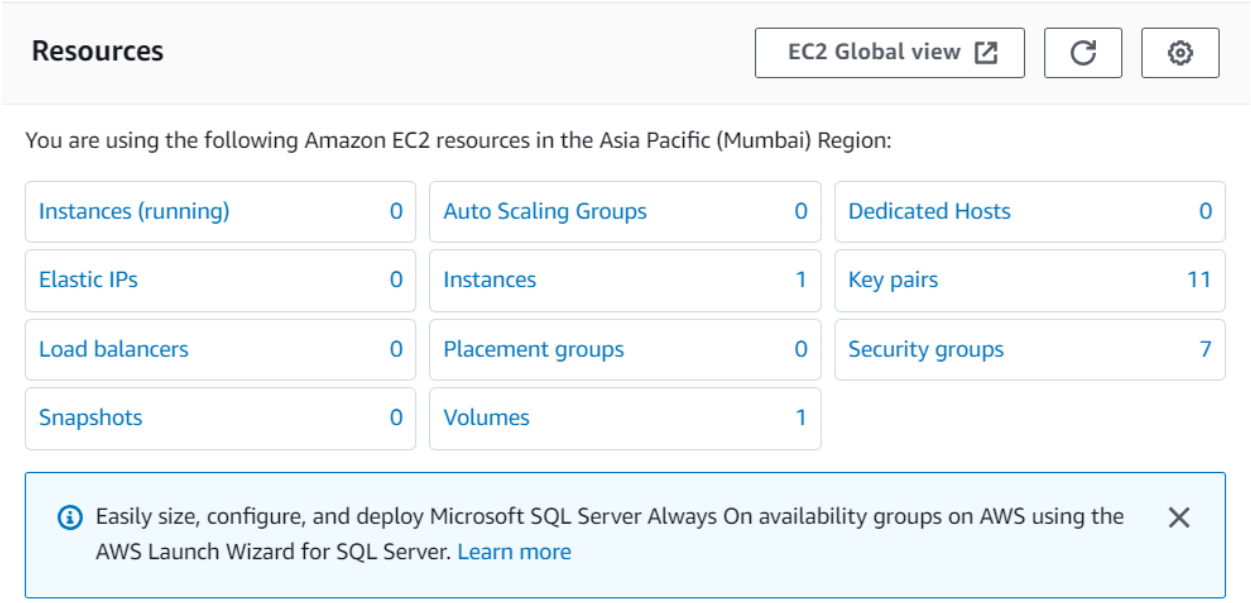
- The organization's resources are constantly provided with greater security.
- Offers the latest version of antivirus software that is compatible with cutting-edge technologies.
- At a reasonable cost, the company may hire qualified security personnel. To secure the company's data, they will provide the finest service possible.
- The IT team's ability to administer and monitor security procedures inside the firm is facilitated by the use of a web interface or having access to a management dashboard, both of which need greater security expertise.
- When a user accesses data without a valid business reason, it may be determined that they are doing so.
- A web interface that allows internal management of various activities as well as a view of the protective configuration and ongoing actions.
- Faster delivery of security services.
- It is economical. Since no new hardware or security license renewals are required. Instead, it may be upgraded or replaced with a newer model as required at a reduced cost.

Examples of SECaaS :

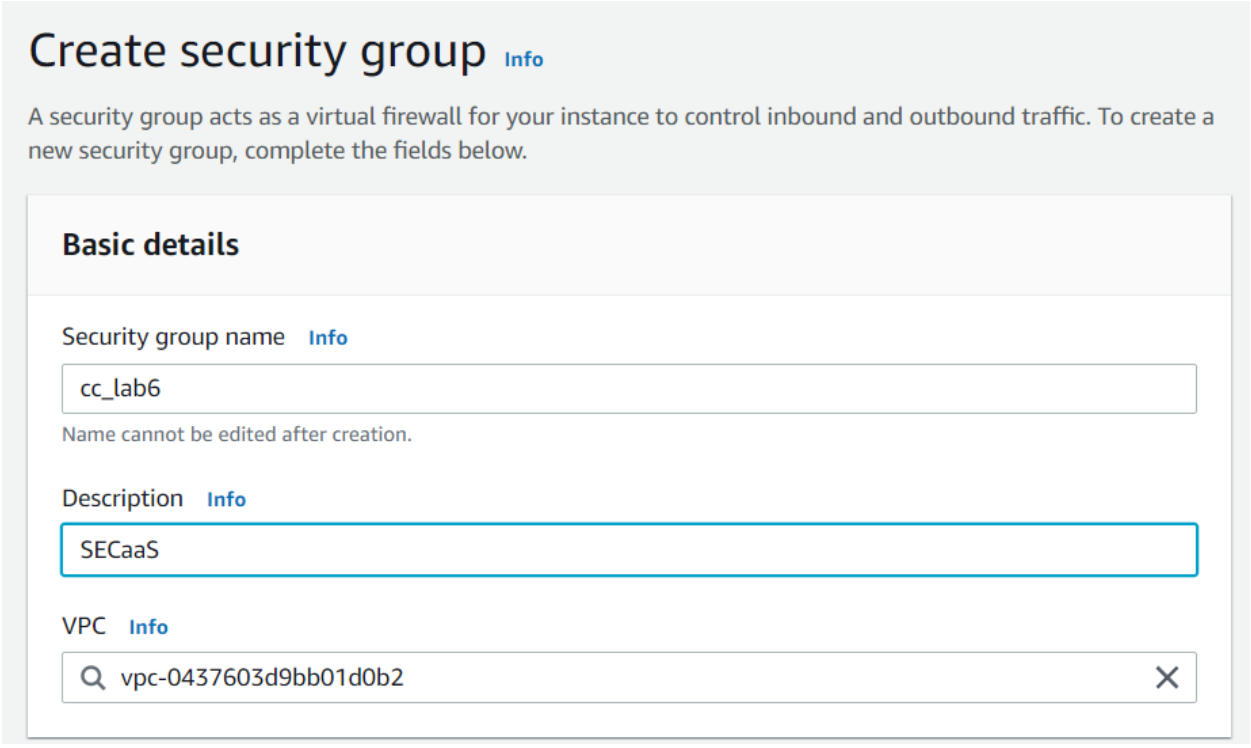
1. Every danger is continuously monitored on a regular basis by SECaaS.
2. Cyber security is handled by security analysts.
3. Threat intelligence reacts right away to any malfunctions that compromise security.
4. To minimize the impact on the system, sophisticated techniques identify the infection.
5. The automations respond to spam and viruses automatically and eliminate them.

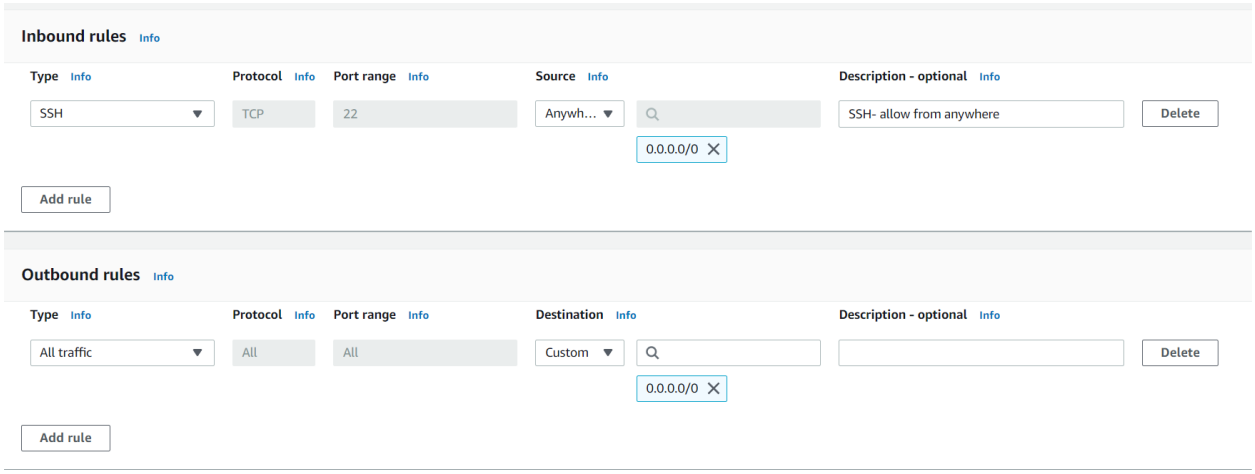
OUTPUT:

1. Open EC2 where you have created instances before. Click on the Security group. Once you click on security groups, you can see many groups which are by default created when you created EC2 instances.

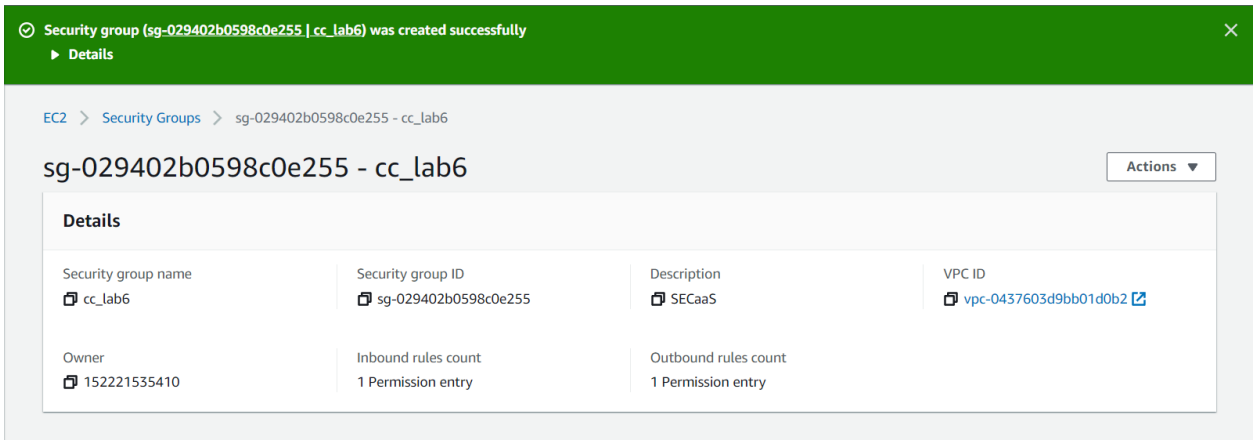


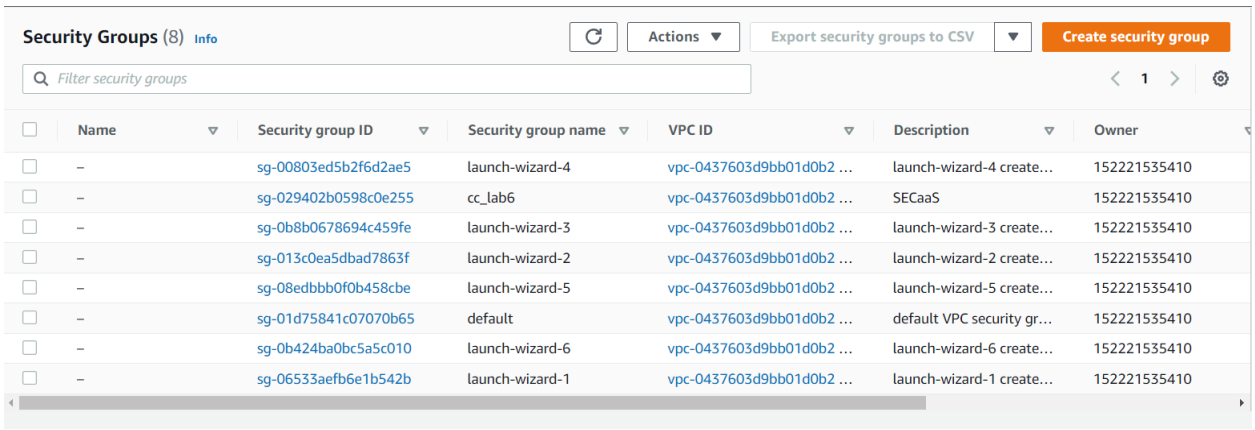
2. Click on create security group. Enter details. Set inbound & outbound rules. By default, outbound rule allows all traffic but inbound rules need to be set. Add tag is optional.





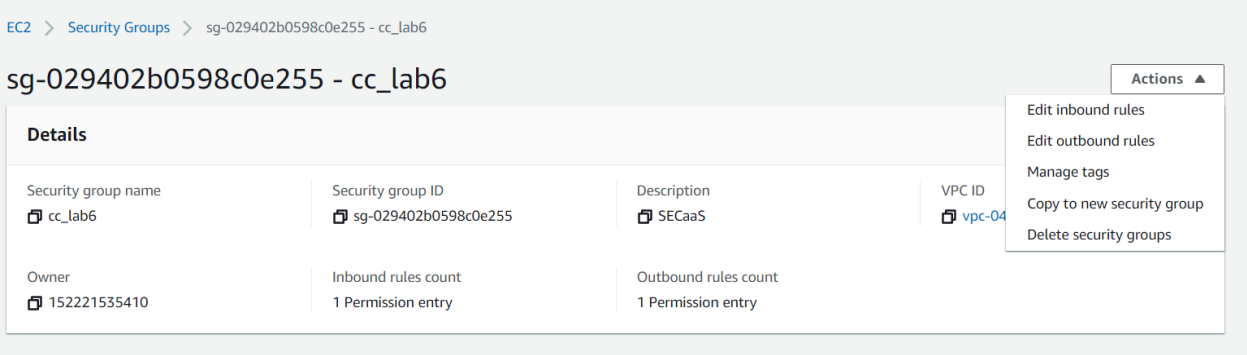
3. After entering all details click on ‘create security group’ button at the bottom and group is created successfully.





Security Group has been created.

4. When you click on this security group, it will give you all information about inbound
   and outbound rules and tags. Also you can change these rules and add new ones too.



CONCLUSION:

We have studied about SECaaS and created one.