NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Security Groups

Cloud Infrastructure Engineering

Nanyang Technological University & Skills Union - 2022/2023

Course Content

- Quick Check-In
- Dive into the basics of Security Groups
- Explore the importance of Security Groups
- Explore creating your own Security Groups
- Implement best practices when using Security Groups

Time	What	How or Why
7:15pm - 7:45pm	Part 1 - Presentation	Overview of Security Groups
7:45pm - 7:55pm	Break	
7:55pm - 8:15pm	Part 2 - Presentation	Best Practices for Security Groups
8:15pm - 8:55pm	Part 3 - Activity	Hands-on Creating Security Groups
8:55pm - 9:05pm	Break	
9:05pm - 10:00pm	Assignment & Wrap Up	

Recap

- Who?
  - Users, Groups, Roles & Permissions
- Why IAM?
  - Security, Compliance, Confidentiality
- Types of Policies
  - Identity-Based Policies
  - Resource-Based Policies
  - Permissions Boundaries
  - Organizations’ SCPs
  - Access Control Lists (ACLs)
  - Session Policies

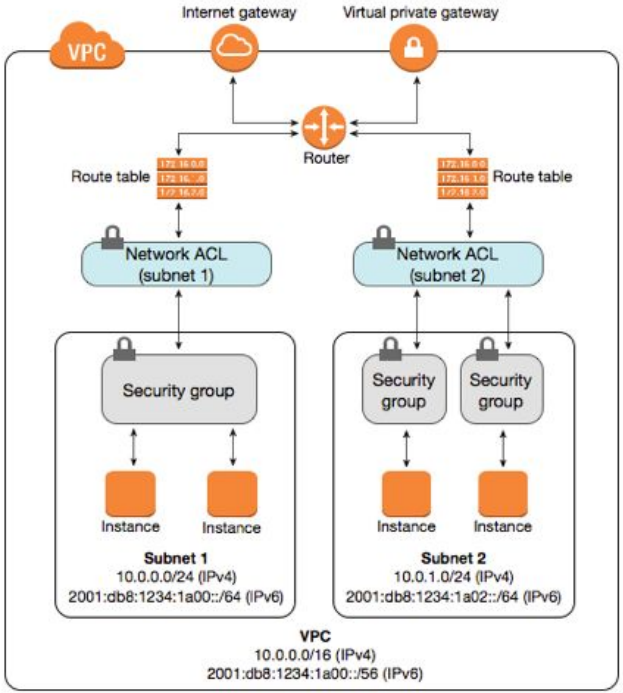
Self Study Check-In

Q1) By default, new security groups start with only an outbound rule that allows all traffic to leave the resource. True or False?

Q2) How important is security groups? Explain

Lesson Overview

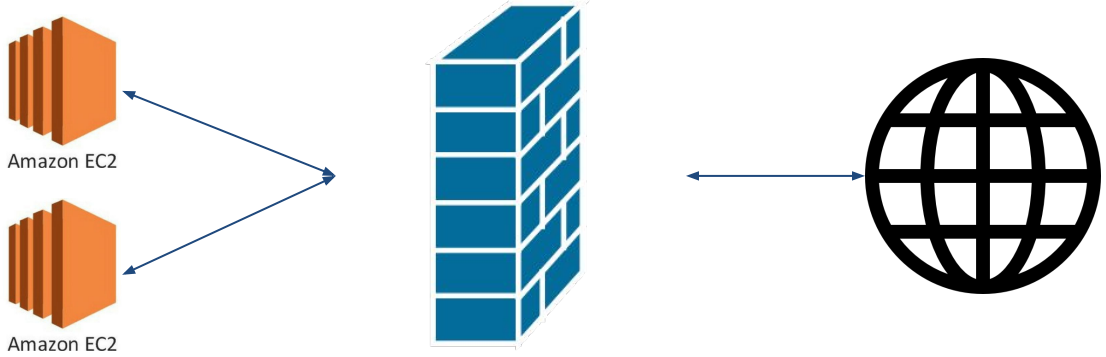
Big Overview - General



Big Overview - Security Groups

A **security group controls the traffic that is allowed to reach and leave the resources that it is associated with**. Think ***Firewall Rules***.

For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

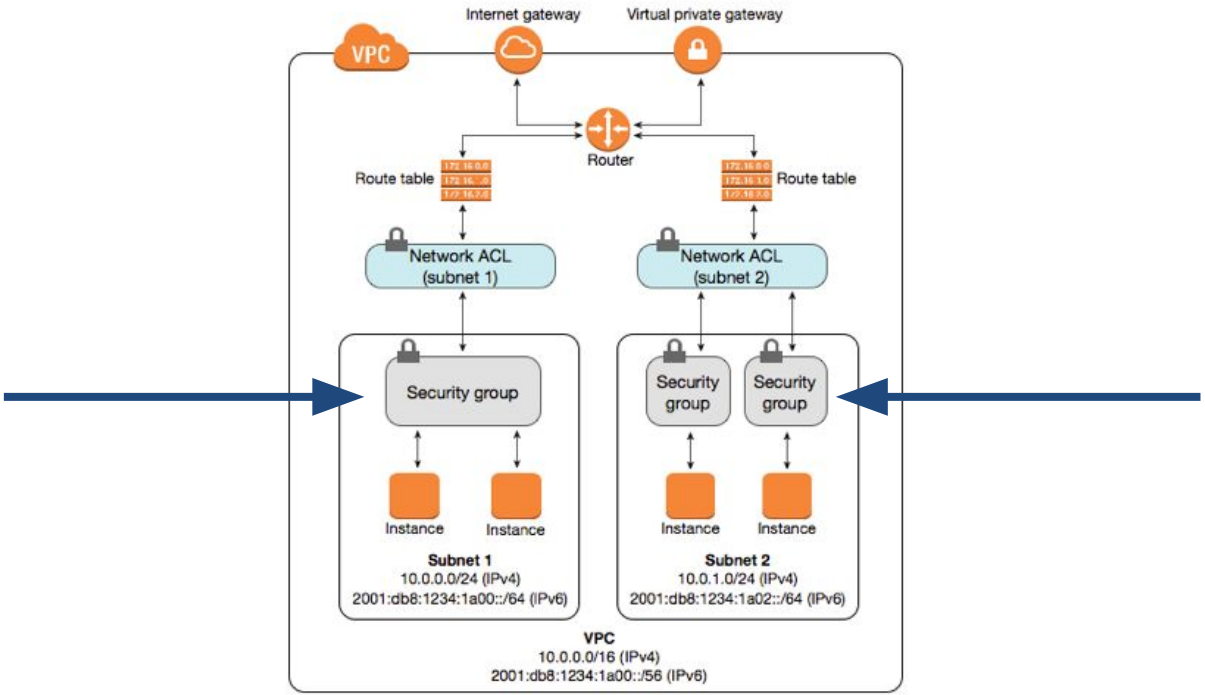


Big Overview - Security Groups

When you create a VPC, it comes with a ***default security group***. You can **create additional security groups** for each **VPC**. You can associate a security group only with resources in the VPC for which it is created.

For each security group, you add **rules** that control the traffic based on protocols and port numbers. There are separate sets of rules for **inbound** traffic and **outbound** traffic.

Big Overview - Security Groups



Big Overview - VPC

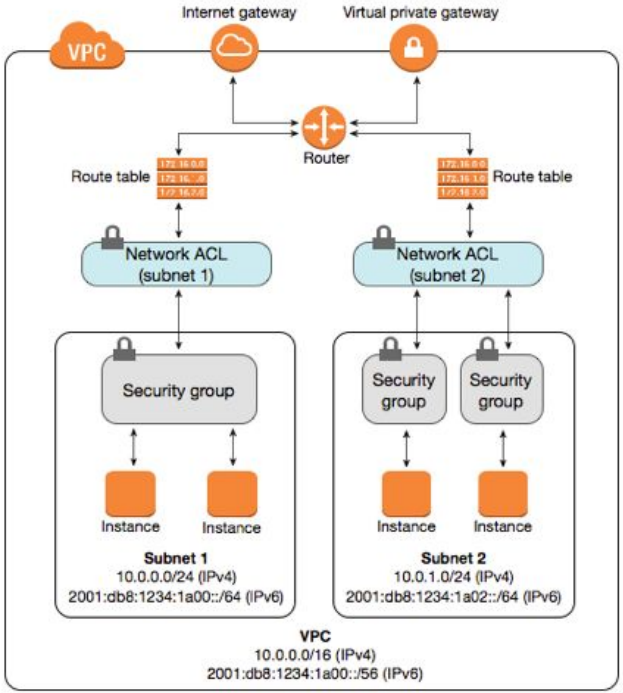
Hold Up - What is a VPC?

A Virtual Private Cloud - **virtual network** that closely **resembles a traditional network** that you'd operate in your own data center.

A VPC can span **multiple availability zones** in one region.

After you create a VPC, you can add subnets.

Big Overview - VPC



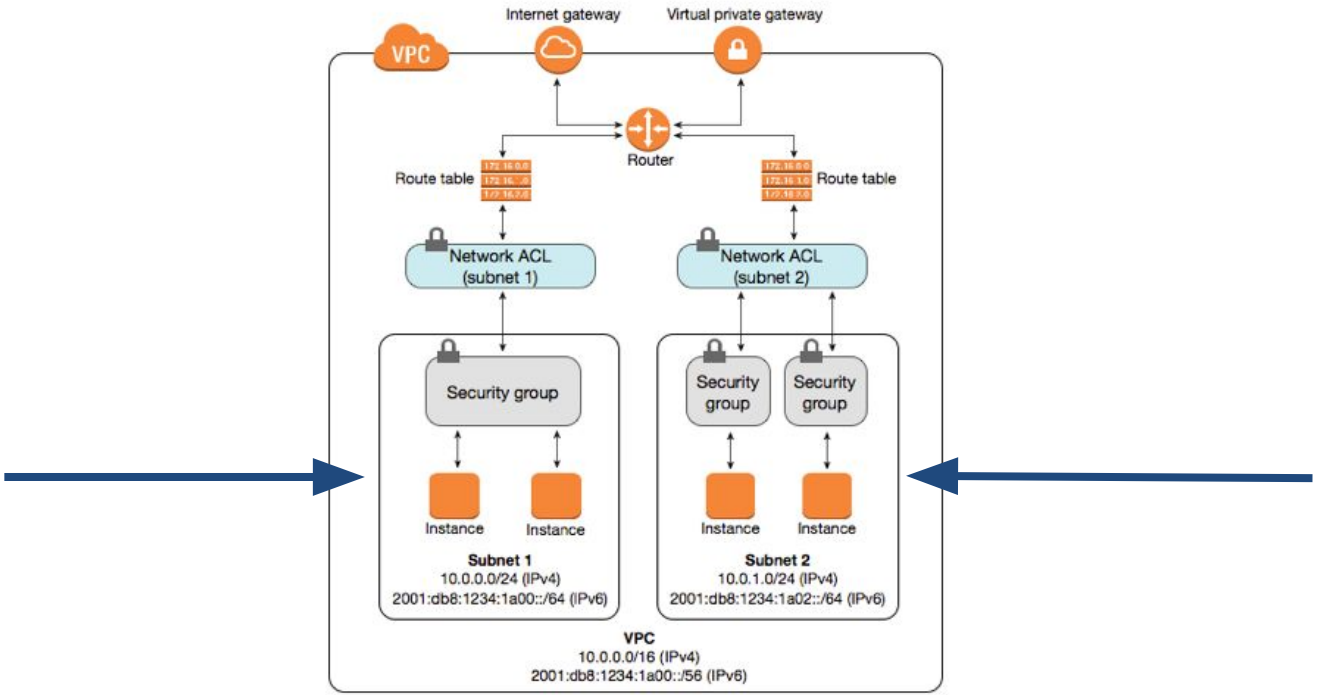
Big Overview - Subnets

Hold Up - What is a Subnet?

A Subnet - **range of IP addresses in your VPC**.

A subnet must reside in a **single Availability Zone**. After you add subnets, you can deploy AWS resources in your VPC.

Big Overview - Subnets



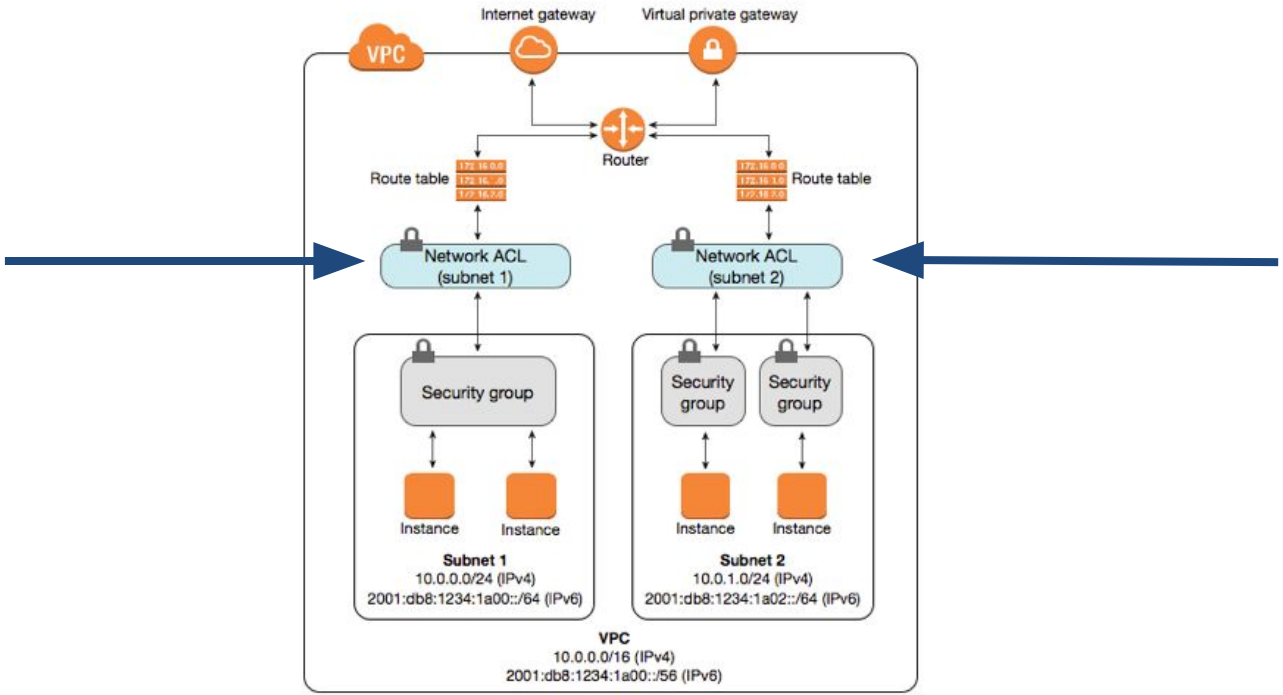
Big Overview - NACLs

Hold Up - What is a Network ACL?

A NACL - **allows or denies specific inbound or outbound traffic at the *subnet* level.**

You can use the default network ACL for your VPC, or you can create a custom network ACL for your VPC with rules that are similar to the rules for your security groups in order to add an additional layer of security to your VPC.

Big Overview - NACLs



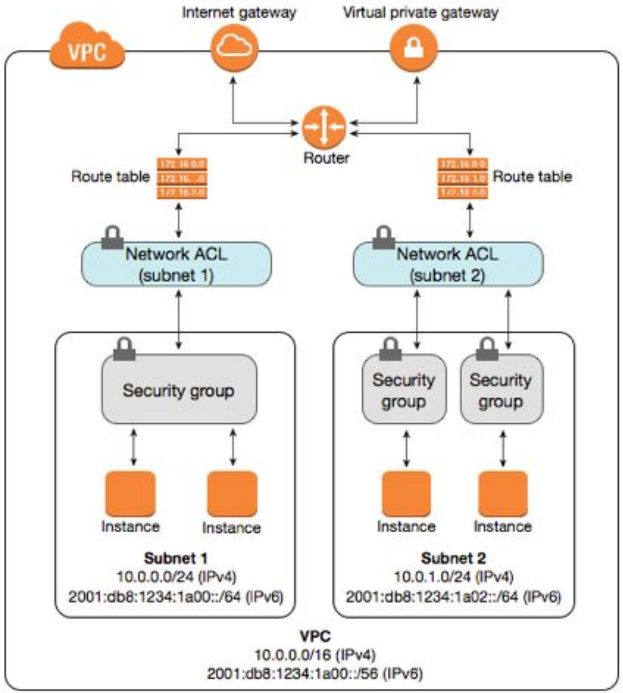
Big Overview - SGs vs NACLs

NACL	Security Groups
Firewall or protection for the subnet	Firewall to protect EC2 instances.

MUST READ:

https://www.knowledgehut.com/tutorials/aws/nacl-vs-security-groups

Big Overview



Also look at:

- Route Tables
- Routers
- Internet Gateways (IGW)
- NAT Gateways
- Virtual Private Gateways

What Are Security Groups?

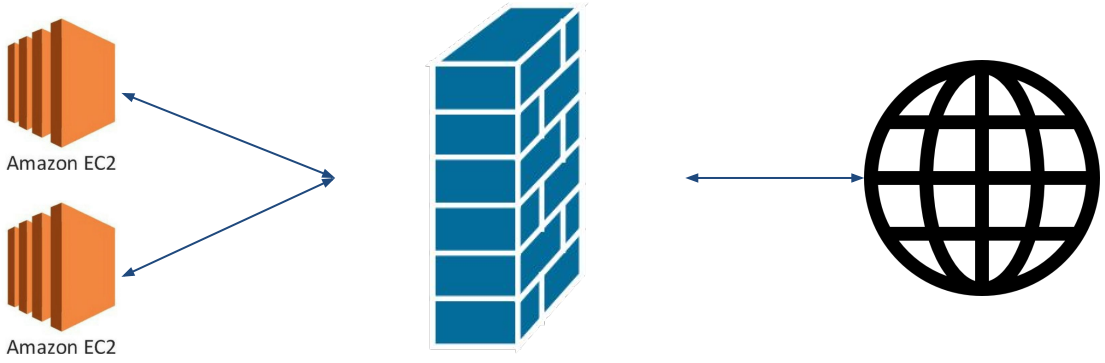
What Are Security Groups?

AWS provides a wide range of IT infrastructure, on-demand, and scalable cloud computing services.

As such, many clients will trust the platform if it **allows for strong levels of security** regarding cloud workloads and projects — and where **network traffic can be filtered appropriately.**

What Are Security Groups?

To maintain and provide this level of security, **AWS is built with security groups that support some degree of control of network traffic associated with EC2 instances**.



What Are Security Groups?

A security group is an **AWS firewall solution** that performs one primary function: to **filter incoming and outgoing traffic from an EC2 instance**.

It accomplishes this filtering function at the **TCP and IP layers, via their respective ports, and source/destination IP addresses**.

Let’s Recap

Question	Your Answer
What is TCP? Explain on your own word	Answer here
What is the difference between HTTP and HTTPS?	Answer here
What is IPv4 and IPv6? What are the differences?	Answer here

Functions of Security Groups

Every Security Group works **similar to a firewall** as it carries a set of rules that filter traffic entering and leaving the EC2 instances.

Security groups are associated with the EC2 instances and offer **protection at the ports and protocol access level**.

The firewall possesses a ‘Deny rule,’ but the **security group has default a “Deny All”** that allows data packets to be dropped if no rule is assigned to them from the source IP.

Functions of Security Groups

Also, when compared to a NACL, **security groups form the first layer of defense at the instance level** in a cloud computing environment whereas **NACLs provides a second layer of protection at the subnet level.**

When creating a security group, **each group will be assigned** to a **particular VPC**.

It's important to note that when creating a security group, you should ensure that it is **assigned to the correct VPC** protect to avoid errors.

Rules Guiding AWS Security Groups

Rules Guiding AWS SG

AWS Security Groups have a set of rules that filter traffic in two ways: **inbound** and **outbound**.

To further break this down, each rule is made up of four principal components:

- Type,
- Protocol,
- Port Range, and
- Source.

There is also a space for a description as well.

Default AWS SG

aws | Services | Search [Option+S] | Singapore | luqmannurhakimtaj

Resource Groups & Tag Editor

- AMIs
- AMI Catalog
- **Elastic Block Store**
  - Volumes
  - Snapshots
  - Lifecycle Manager
- **Network & Security**
  - Security Groups
  - Elastic IPs
  - Placement Groups
  - Key Pairs
  - Network Interfaces
- **Load Balancing**
  - Load Balancers
  - Target Groups
- **Auto Scaling**
  - Launch Configurations
  - Auto Scaling Groups

Security Groups (1/1) Info

Actions | Export security groups to CSV | Create security group

Filter security groups

Name	Security group ID	Security group name	VPC ID	Description	Owner
–	sg-6c6d2826	default	vpc-88a264ee	default VPC security gr...	0253280

sg-6c6d2826 - default

Details | Inbound rules | Outbound rules | Tags

Details

Security group name	Security group ID	Description	VPC ID
default	sg-6c6d2826	default VPC security group	vpc-88a264ee

Owner	Inbound rules count	Outbound rules count
025328071091	3 Permission entries	1 Permission entry

New AWS SG

aws | Services | Search [Option+S] | Singapore | luqmannurhakimtaj

Resource Groups & Tag Editor

Basic details

Security group name Info

MySSHSecurityGroup

Name cannot be edited after creation.

Description Info

Allow Access for EC2 Instances SSH

VPC Info

vpc-88a264ee

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
SSH	TCP	22	My IP	103.252.202.164/32		Delete

Add rule

Breaking Down Security Groups

The **rule** allows for selection of the **common type of protocols** such as HTTP, SSH, etc., and it opens a drop-down menu were all the protocols are listed.

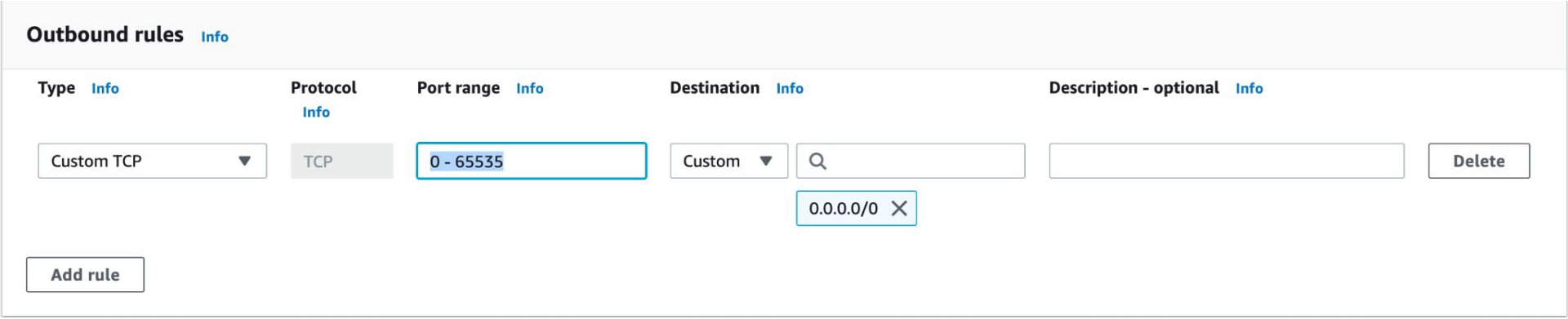
Protocols are automatically selected to be the **TCP**. However, it can be changed to UDP, ICMP as well as assigns a corresponding association to IPv4 or IPv6.

Types of Security Groups Rules

- All TCP
- Custom TCP
- All UDP
- Custom UDP
- SSH
- HTTP
- HTTPS
- Many, many more

Breaking Down Security Groups

Port Range is also pre-filled, but you can decide to **choose the port range** of your choice depending on the protocol. Nonetheless, there will be times when you will have to use the **custom port range number**.



Breaking Down Security Groups

Source (**custom IP**) this can be a **particular IP address or a subnet range**. However, you can grant access using the anywhere source IP (0.0.0.0/0) value. Allowing access through the anywhere source can turn out to be a mistake every AWS user **should avoid**.

Activity

- Open AWS Console
- Create a new EC2 instance with a **new security group**:
  - Name: “<Name>SSHSecurityGroup”
  - Description: “Security Group To Allow SSH from my VPC”
  - VPC: < Choose Any >
  - Inbound Rules:
    - Type: SSH
    - Protocol: TCP
    - Source: My IP
- Assuming another teammate has set up the right keypair for this instance, can he/she access the VM with the above configuration? How can you edit your security group to allow this?

Best Security Groups Practices

Avoid Incoming Traffic Through (0.0.0.0/0)

One common mistake is to allow inbound traffic from (0.0.0.0/0). It could end up **exposing sensitive cloud information to outside threats.**

Though the security group performs its initial layer filtering when all inbound traffic is allowed but ultimately allows for **many risks during the process**.

Avoid Incoming Traffic Through (0.0.0.0/0)

Avoid this as much as possible

Security Group: sg-ca43a5b7

Description | **Inbound** | Outbound | Tags

Edit

Type	Protocol	Port Range	Source
All traffic	All	All	0.0.0.0/0

Avoid Incoming Traffic Through (0.0.0.0/0)

Instead, try specific types, port ranges and source/destination IPs

Inbound rules | Outbound rules | Tags

Inbound rules (1/1)

Manage tags | Edit inbound rules

Filter security group rules

1

IP version	Type	Protocol	Port range	Source	Description
IPv4	SSH	TCP	22	103.252.202.164/32	–

Delete Unused Security Groups

There is no need to keep a security group not assigned to an EC2 instance.

Ensure that all unused SG's are deleted to keep the working environment clean and less at risk to link the AWS to the outside world.

Delete Unused Security Groups

Delete Security Groups

Are you sure you want to delete these security groups?

sg-be41a7c3 - Webserver_SG
sg-ca43a5b7 - AllOpen_SG

Note that the following security groups **cannot be deleted**:

These security groups are **associated with one or more instances**. Terminate the instances, or associate them with different security groups (VPC only). View your associated instances.

sg-2e40a653 - Web_SG

These security groups are **referenced by one or more other security groups**. Delete the other security groups, or remove their references. View your referencing security groups.

sg-50b6572d - Application_SG

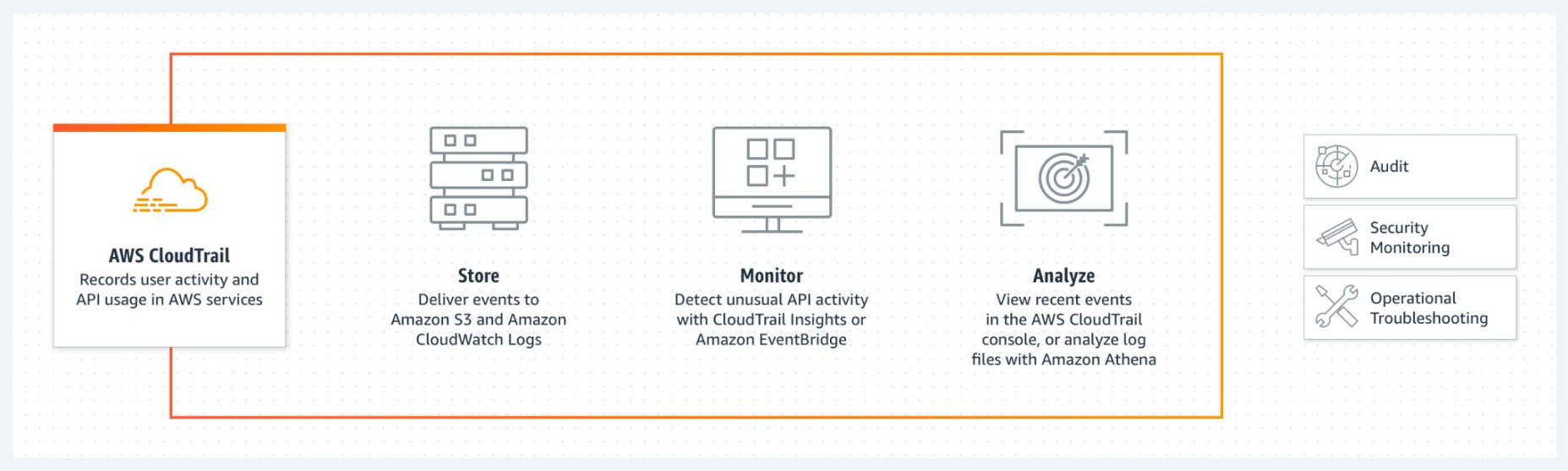
Cancel **Yes, Delete**

Enable Tracking & Alerts

AWS comes with some unique set of tools that allows its user to **keep track of working information**. The **AWS Cloudtrail** is a cloud tool that enforces the compliance of AWS.

It's apparent that the right deployment of Security Groups and Network access control lists will go a long way in providing first and second layer form of security for an AWS account.

Enable Tracking & Alerts



Activity

- Once done with your assignment, delete the Security Group

Activity

Learner:

- Clean up AWS.
- Remove/delete/terminate all service/ resources that created.

Instructor

- Clean up AWS.
- Remove/delete/terminate all service/ resources that created.
- Check the AWS account after learner clean up.

What’s Next?