sg-exampro

Security Groups

A virtual firewall that controls the traffic to and from EC2 Instances

Security Groups – Introduction

Security Groups acts as a **virtual firewall** at the instance level

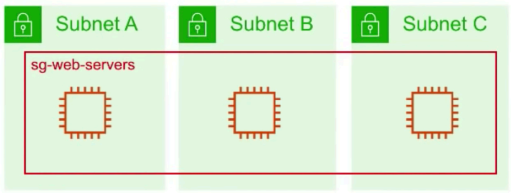
Security Groups are associated with EC2 instances

provide security at the **protocol** and **port** access level.

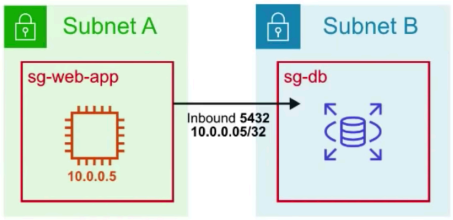
Each Security Group contains a set of rules that filter traffic coming **into (inbound) and out of (outbound)** EC2 instances.

There are no 'Deny' rules. **All traffic is blocked by default** unless a rule specifically allows it.

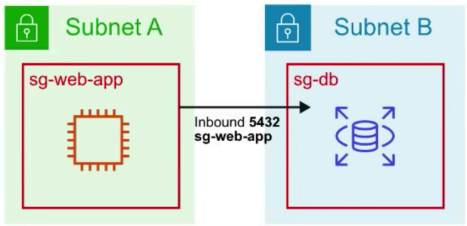
Multiple Instances across multiple subnets can belong to a **Security Group.**



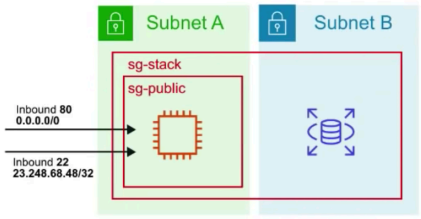
Security Groups – Use Case



You can specify the source to be an IP range or
A specific ip (/32 is a specific IP Address)



You can specify the source to be another security group



An instance can **belong to multiple Security Groups**, and rules are **permissive** (instead of restrictive). Meaning if you have one security group which has no Allow and you add an allow to another than it will Allow.

Security Groups – Limits

You can have **upto 10,000 Security Groups in a Region** (default is 2,500)

You can have **60 inbound rules** and **60 outbound rules** per security group

16 Security Groups per Elastic Network Interface (ENI) (default is 5)

Security Groups *CheatSheet*

- Security Groups acts as a firewall at the instance level
- Unless allowed specifically, all **inbound traffic** is **blocked by default**.
- All **Outbound traffic** from the instance is **allowed by default.**
- You can specific for the source to be either an IP range, single Ip Address or another security group
- Security Groups are **STATEFUL** (if traffic is allowed inbound it is also allowed outbound)
- Any changes to a Security Group take effect immediately.
- EC2 Instances can belong to multiple security groups
- Security groups can contain multiple EC2 Instances.
- You **cannot block specific IP addresses** with Security Groups, for this you would need a Network Access Control List (NACL)
- You can have upto 10,000 Security Groups per Region (default 2,5000)
- You can have 60 inbound and 60 outbound rules pre Security Group
- You can have 16 Security Groups associated to an ENI (default is 5)