

AWS Certified Cloud Practitioner
Training Bootcamp

Security Groups Basics 101

Security Groups (SG) Basics

- AWS security groups act as a virtual firewall for your EC2 instances to control inbound and outbound traffic
- Security groups enforce security at the instance level, not the subnet; different EC2 instances can have different SGs applied
- In a SG you add rules that control inbound traffic to instances and separate rules that control outbound traffic



**Security
Group**

Security Groups (SG) Basics

Create Security Group

Security group name ⓘ

Description ⓘ

VPC ⓘ vpc-9353d9e9 (default) ⌵

Security group rules:

Inbound

Outbound

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
This security group has no rules				

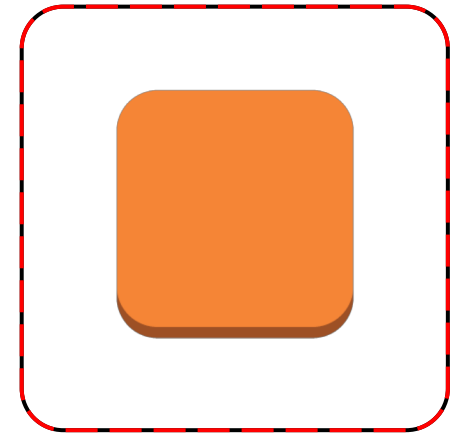
Add Rule

Cancel

Create

Security Groups (SG) Basics

- When you first create a security group, it has no inbound rules => no traffic is permitted to EC2
- When defining rules, you can only specify allow rules and no deny rules
- By default, all outbound traffic is permitted
- What rules can you actually define in a SG ?



**Security
Group**

Security Groups (SG) Basics

■ Inbound Rules:

Edit inbound rules ✕

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH ⌵	TCP	22	Custom ⌵ 0.0.0.0/0	e.g. SSH for Admin Desktop ✕

Add Rule

■ Outbound Rules:

Edit outbound rules ✕

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Destination ⓘ	Description ⓘ
All traffic ⌵	All	0 - 65535	Custom ⌵ 0.0.0.0/0	e.g. SSH for Admin Desktop ✕

Add Rule

AWS Certified Cloud Practitioner
Training Bootcamp

Thank you