



## Short Interview questions on Security Group

### Q1: What is a Security Group in AWS?

**A:** A virtual firewall that controls inbound and outbound traffic for EC2 instances.

---



### Q2: Are Security Groups stateful or stateless?

**A:** They are **stateful** — if you allow inbound traffic, the response is automatically allowed.

**Stateful** = "If I let someone in, I'll automatically let them back out."

No need to write a matching outbound rule for every inbound rule.

#### Example (Linux EC2 via SSH):

-  You create an **inbound rule** to allow SSH:
  - Protocol: TCP
  - Port: 22
  - Source: 0.0.0.0/0 (anyone)
-  You **don't add any outbound rule** for port 22.

 Still, when you connect via SSH, the response from the EC2 instance goes back to you.

#### Why?

Because the Security Group is *stateful* — it remembers that there was an **incoming connection**, so it **automatically allows the response back**, even if the outbound rule is not explicitly defined for that port.

---

### ◆ Q3: What are the key components of a Security Group rule?

**A:** Protocol (TCP/UDP), Port range, and Source (for inbound) or Destination (for outbound).

---

#### ◆ Q4: Can you block traffic using a Security Group?

A: No, Security Groups can **only allow** traffic, not explicitly deny it.

---

#### ◆ Q5: How many Security Groups can be attached to one EC2 instance?

A: Up to **five** Security Groups per instance (default soft limit).

---

#### ◆ Q6: What happens if you don't specify a Security Group while launching an instance?

A: The instance is associated with the **default Security Group**, which typically allows **all traffic within the same group**.

Every VPC in AWS comes with a default Security Group. By default, this Security Group has a set of rules. A key default inbound rule is one that **allows all inbound traffic from sources that are also associated with this same default Security Group**. This is often referred to as "self-referencing" rule.

- Imagine two instances, A and B, in a VPC.
  - You launch them without specifying a Security Group.
  - Both A and B get the default Security Group.
  - The default group allows traffic from itself.
  - So, Instance A can talk to Instance B on any port or protocol.
  - Instance B can talk to Instance A on any port or protocol.
  - Both can also send traffic anywhere outside.
- 

#### Q7: Difference between Security Groups and Network ACLs?

A: Security Groups are **instance-level** and **stateful**, while NACLs are **subnet-level** and **stateless**.

How to set outbound traffic in security group, explain with example.

- Security Groups can indeed **block outbound traffic**.
- You can specify rules to allow outbound traffic **only to particular destinations**.

**How to do it:**

When you configure the **outbound rules** for a Security Group, instead of keeping the default rule that allows all outbound traffic (destination 0 . 0 . 0 . 0 / 0), you remove it and add specific rules.

In these specific outbound rules, you define:

- The **protocol** (e.g., TCP, UDP, ICMP).
- The **port range** (e.g., 80 for HTTP, 443 for HTTPS, or all ports).
- The **destination**. This is where you specify *only* the IP address, CIDR block, or even another Security Group ID that the instance is allowed to send traffic to.

### Example:

Let's say you have an EC2 instance that only needs to send traffic to a database server with the IP address 172 . 31 . 10 . 5 on port 3306 (MySQL/Aurora).

Your outbound rules for the instance's Security Group would look like this:

- **Type:** Custom TCP Rule
- **Protocol:** TCP
- **Port Range:** 3306
- **Destination:** 172 . 31 . 10 . 5 / 32 (using /32 to specify a single IP address)

With only this rule, the instance can only send TCP traffic on port 3306 to 172 . 31 . 10 . 5. Any other outbound traffic (to other IPs or other ports on 172 . 31 . 10 . 5) would be implicitly denied.

### What is the primary function of a Security Group in AWS?

- A) Monitoring EC2 traffic
- B) Assigning IP addresses
- C) Acting as a virtual firewall
- D) Launching EC2 instances

✓ Correct Answer: C

---

### Security Groups in AWS are:

- A) Stateless
- B) Stateful
- C) Immutable
- D) Temporary

✓ Correct Answer: B

---

**Which of the following can you configure in a Security Group rule?**

- A) MAC address
- B) Availability Zone
- C) Protocol, Port, and Source/Destination
- D) EC2 instance name

 **Correct Answer: C**

---

**4:**

**Which of the following is true about outbound rules in a Security Group?**

- A) They are disabled by default
- B) You must explicitly allow all outbound traffic
- C) They allow all outbound traffic by default
- D) Outbound rules are not configurable

 **Correct Answer: C**

---