VPC Basics

05 January 2026 08:14 PM

Why is there a **range of IP addresses**?

An IP address range exists because networks are designed to support **multiple devices**, not just one.

1. Every device on a network (PC, phone, server, printer) requires a **unique IP address**.
2. Instead of assigning addresses individually and arbitrarily, networks allocate them from a **defined block (range)**.
3. This range is determined by the **subnet mask / CIDR prefix**.

Example

Network: 192.168.1.0/24
IP range: 192.168.1.1 – 192.168.1.254

1. .0 → Network address (identifies the subnet)
2. .255 → Broadcast address (used to reach all devices)
3. Remaining addresses → Usable for hosts

The range ensures:

1. No IP conflicts
2. Organized addressing
3. Scalability

Key rule

1. If two devices are in the same IP range (same subnet), they can talk directly.
2. If they are in **different ranges**, routing is required.

A subnet is:

1. A **logical boundary**
2. A method of **grouping IP addresses**
3. A way to **limit broadcasts**

When two devices are in the **same subnet**:

1. Communication happens **directly at Layer 2 (Ethernet)**
2. **No router is involved**
3. IP is used for identification; **MAC addresses are used for delivery**
4. **Link**

In AWS networking, **Security Groups are stateful firewalls**. This property directly explains why **return traffic is automatically allowed**.

1. Meaning of stateful

A **stateful** firewall **tracks the state of a connection**.

This means it remembers:

1. Who initiated the connection
2. Source IP and destination IP
3. Source port and destination port
4. Protocol (TCP/UDP/ICMP)

Once a connection is **permitted in one direction**, the firewall **automatically allows the response traffic**, even if no explicit rule exists for it.

2. How Security Groups handle traffic

Example: outbound request

You allow an EC2 instance to make an outbound HTTP request.

Outbound rule

Allow: TCP 80 → 0.0.0.0/0

The instance sends a request to a web server.

Return traffic (automatic)

i. The response comes **from the web server**
ii. Uses **source port 80**
iii. Returns to the **ephemeral port** on the instance

Even if **no inbound rule allows port 80**, the response is allowed because:

i. The connection was **initiated by the instance**
ii. The security group tracks the session state