How Data Flows From AWS

05 January 2026 11:25 PM

EC2 → Internet Flow with TCP Handshake Included

Assumption:

1. Protocol = **TCP** (e.g., HTTPS on port 443)

1. DNS Resolution

EC2 resolves google.com using **VPC DNS Resolver** and obtains a **public IP address**.
(No connection yet — DNS is separate from TCP.)

2. TCP SYN (Connection Initiation)

1. EC2 application initiates a TCP connection
2. EC2 sends a **TCP SYN packet**
    1. Source IP: EC2 private IP
    2. Source port: Ephemeral port (e.g., 49152)
    3. Destination IP: Google public IP
    4. Destination port: 443
3. Packet exits via the **ENI**

3. VPC Route Table Evaluation

1. Destination IP is outside VPC CIDR
2. Route table forwards packet to **NAT Gateway**

4. NAT Gateway – Source NAT (SNAT)

1. NAT Gateway:
    1. Replaces **source private IP → public Elastic IP**
    2. Keeps source port (or remaps if needed)
2. TCP state is **tracked** by the NAT Gateway

5. Internet Gateway

1. Packet passes through **Internet Gateway**
2. IGW enables **internet routability** (no NAT performed here)

6. AWS Edge Network

1. Packet exits AWS via **edge infrastructure**
2. Traverses public internet

7. Destination Server Receives SYN

1. Google server receives **TCP SYN**
2. Responds with **TCP SYN-ACK**

8. Return Path (SYN-ACK)

1. SYN-ACK arrives at the **public IP (EIP)**
2. AWS routes it back to the **NAT Gateway**

9. NAT Gateway – Reverse NAT

1. NAT Gateway:
   1. Translates destination public IP → EC2 private IP
   2. Restores correct source/destination ports

10. Packet Reaches EC2 ENI

1. Packet enters EC2 through the ENI
2. **Security Group inbound rules are evaluated**
   1. Allowed because:
      I. It is **return traffic**
      II. Security groups are **stateful**

11. TCP ACK (Handshake Completion)

1. EC2 sends **TCP ACK**
2. ACK follows the same outbound path:
   1. ENI → NAT Gateway → IGW → Internet
3. **TCP three-way handshake is now complete**

12. Connection Established

1. TCP connection is **established**
2. Application data (HTTP request/response) flows over the same path
3. NAT Gateway maintains session state until timeout

13. Connection Termination (Later)

1. FIN / ACK exchange occurs
2. NAT Gateway clears translation state after idle timeout

Where the TCP Handshake Happens (Summary)

Step	TCP Action
2	SYN (EC2 → Internet)
8	SYN-ACK (Internet → EC2)
11	ACK (EC2 → Internet)
12	Connection established

Important AWS-Specific Points (Exam-Critical)

1. NAT Gateway is **stateful**
2. Security Groups are **stateful**
3. Return traffic is **automatically allowed**
4. Internet Gateway does **not** perform NAT
5. ARP and MAC addressing are **internal only**