Networking

Smart Internz

Networking

- **Definition:** Networking involves connecting devices and systems to share resources, exchange data, and enable communication.

Components:

- **Hardware:** Routers, switches, hubs, modems, and network interface cards (NICs).
- **Protocols:** Rules for data transmission, e.g., TCP/IP, HTTP, FTP.
- **Cabling & Wireless:** Physical (Ethernet) or wireless (Wi-Fi, Bluetooth) mediums for data transmission.

Types of networks

- **LAN (Local Area Network):** Connects devices in a small area (e.g., home or office).
- **WAN (Wide Area Network):** Spans large areas (e.g., the Internet).
- **MAN (Metropolitan Area Network):** Covers a city or campus.

Smart Internz

Key Concepts

- **IP Addressing:** Unique identifiers for devices.
- **DNS:** Converts domain names into IP addresses.
- **Firewalls:** Protect networks by filtering traffic.

Networking basics

- One way to think about networking is to think about sending a letter.
- When you send a letter, you provide the following three elements:
- The letter, inside the envelope
- The address of the sender in the from section
- The address of the recipient in the to section

IP addresses

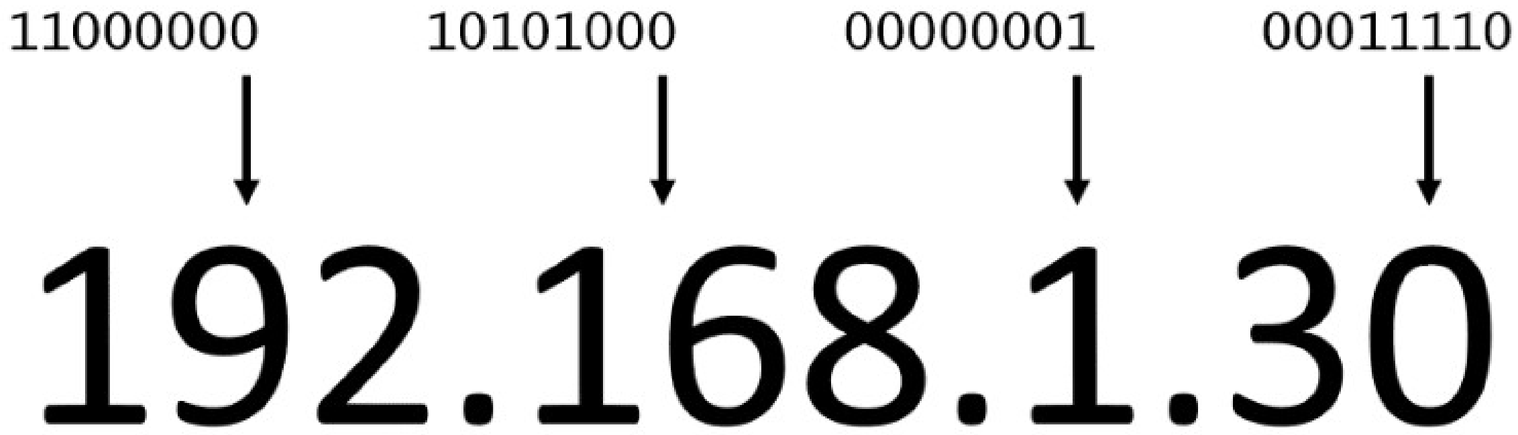
- An IP address is like a mailing address for computers, used to route messages to the correct location.
- Instead of using words like street or city, an IP address is made up of bits (0s and 1s).
- A 32-bit address is common and consists of 32 digits written in binary.
- Example: 11000000 10101000 00000001 00011110 is a binary 32-bit address.

Networking basics

- One way to think about networking is to think about sending a letter.
- When you send a letter, you provide the following three elements:
- The letter, inside the envelope
- The address of the sender in the from section
- The address of the recipient in the to section

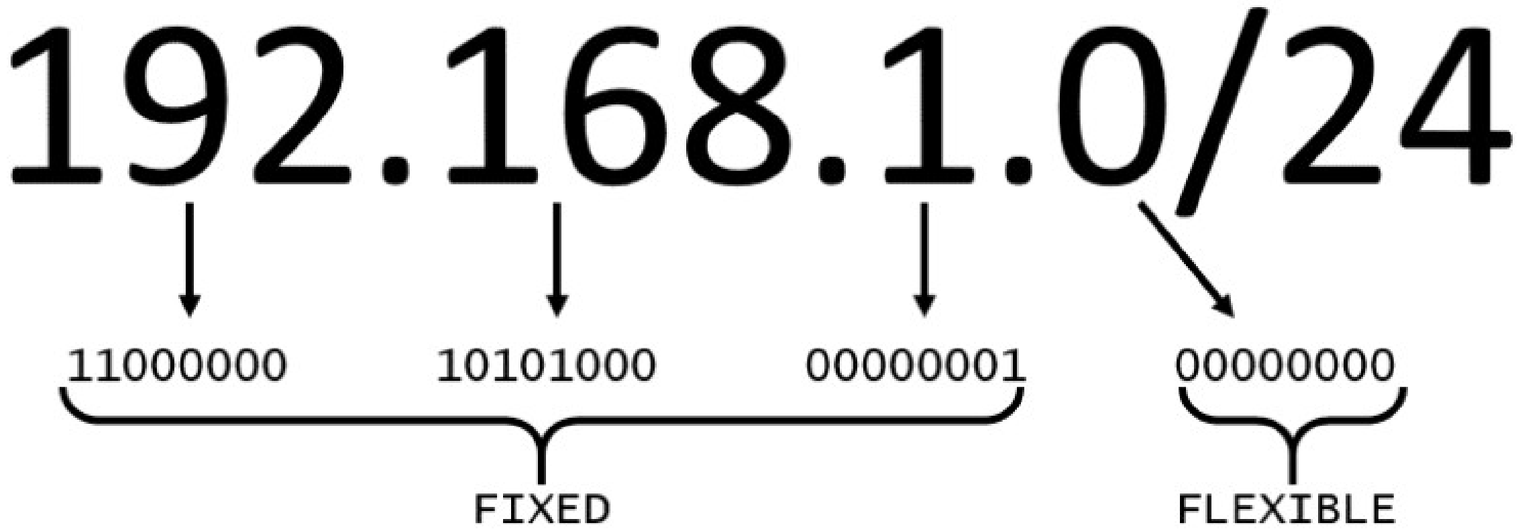
IPv4 notation

- IPv4 addresses are typically written in decimal format rather than binary.
- A 32-bit address is divided into four 8-bit groups called octets, each converted to decimal and separated by periods.
- The result is a standard IPv4 address, used to identify a single computer on a network.
- For working with networks, Classless Inter-Domain Routing (CIDR) is used to manage IP address allocation efficiently.

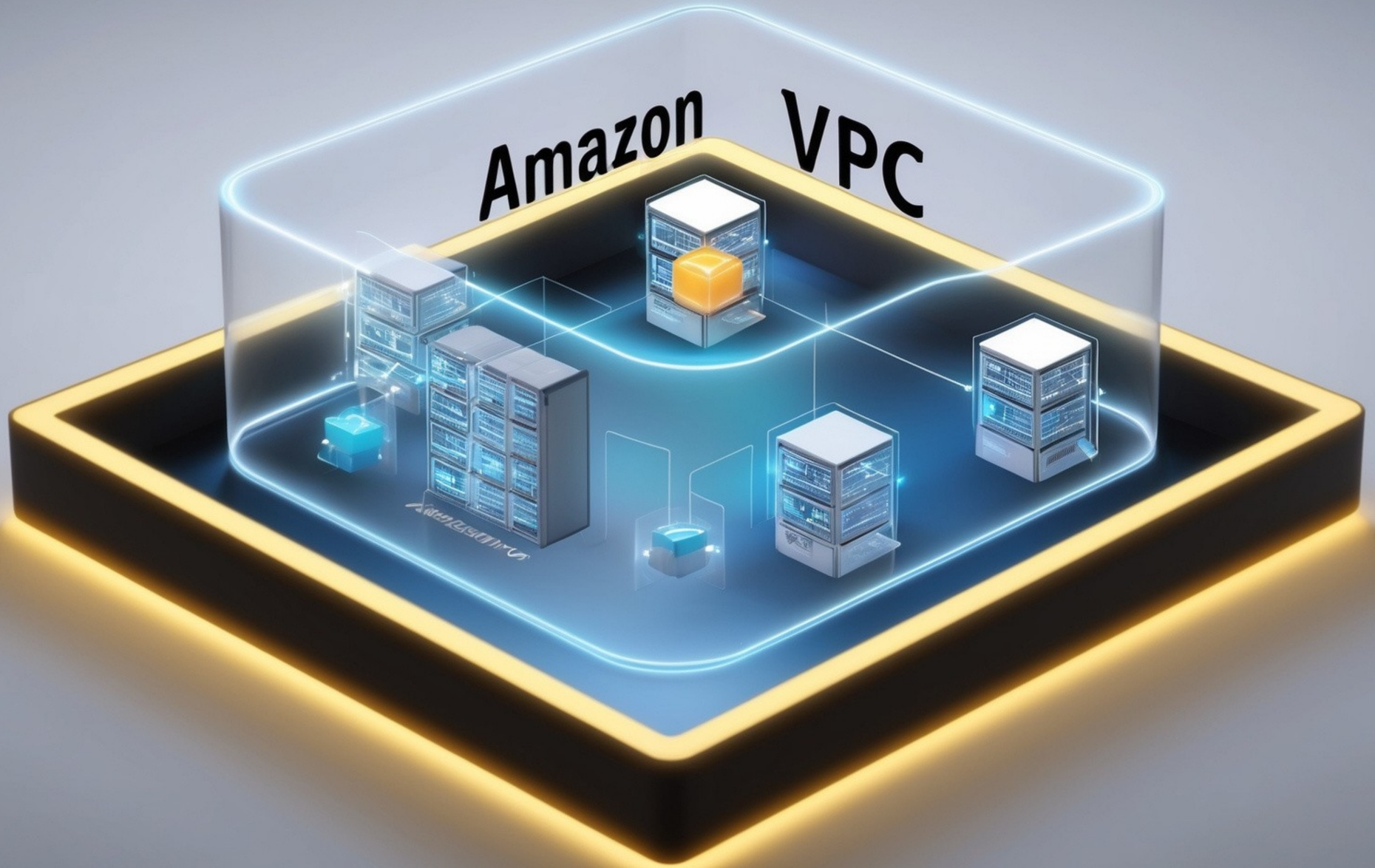


192.168.1.0/24

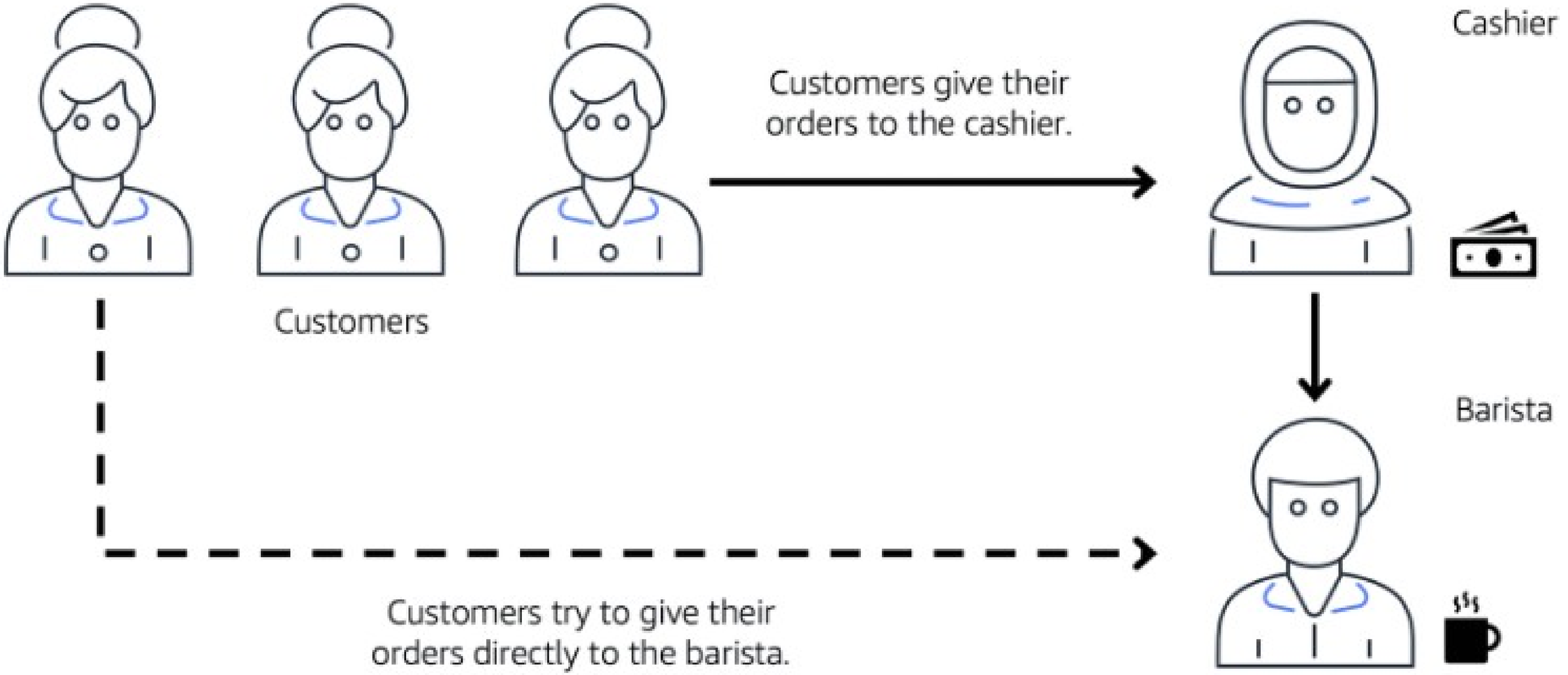
- CIDR notation represents a range of IP addresses in a compressed format.
- It starts with a base IP address followed by a / and a number, which specifies how many bits are fixed.
- Example: In 192.168.1.0/24, the first 24 bits are fixed, leaving 8 flexible bits, allowing for 256 IP addresses.

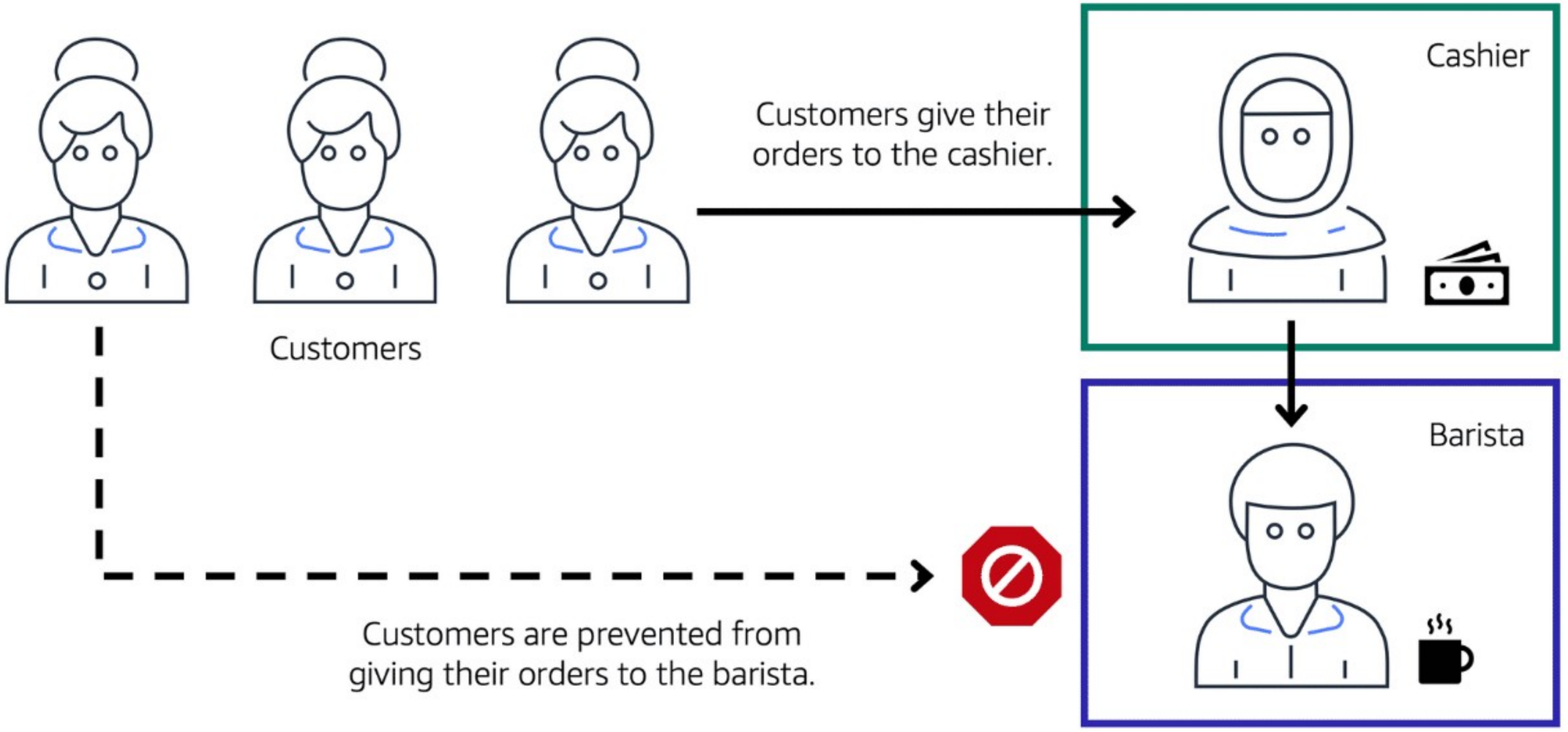


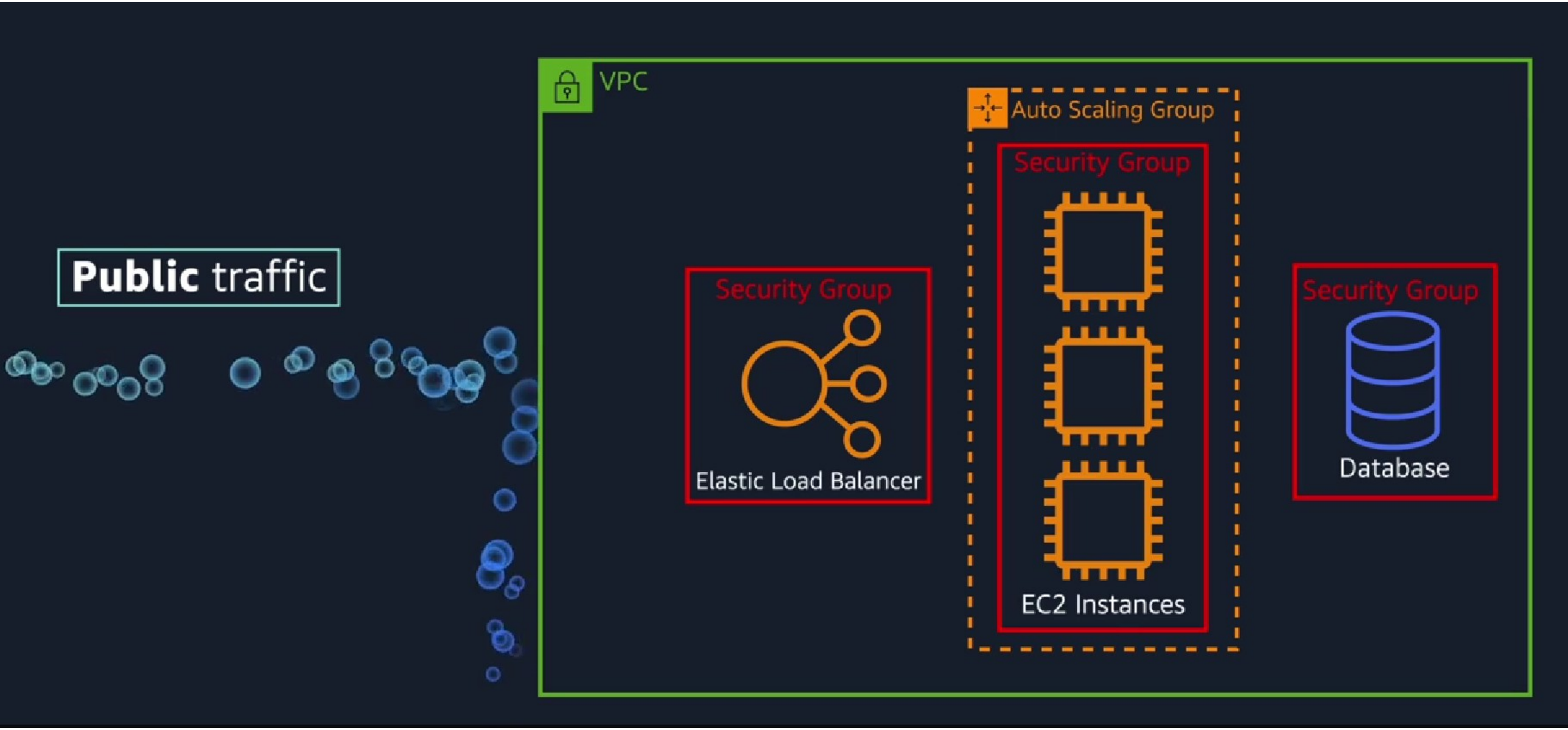
- The smaller the number after the /, the larger the range of IP addresses (e.g., /16 allows more addresses than /24).
- In AWS, the smallest IP range is /28 (16 IP addresses), and the largest is /16 (65,536 IP addresses).
- CIDR is essential for defining network sizes and ranges when working in the AWS Cloud.


Amazon VPC

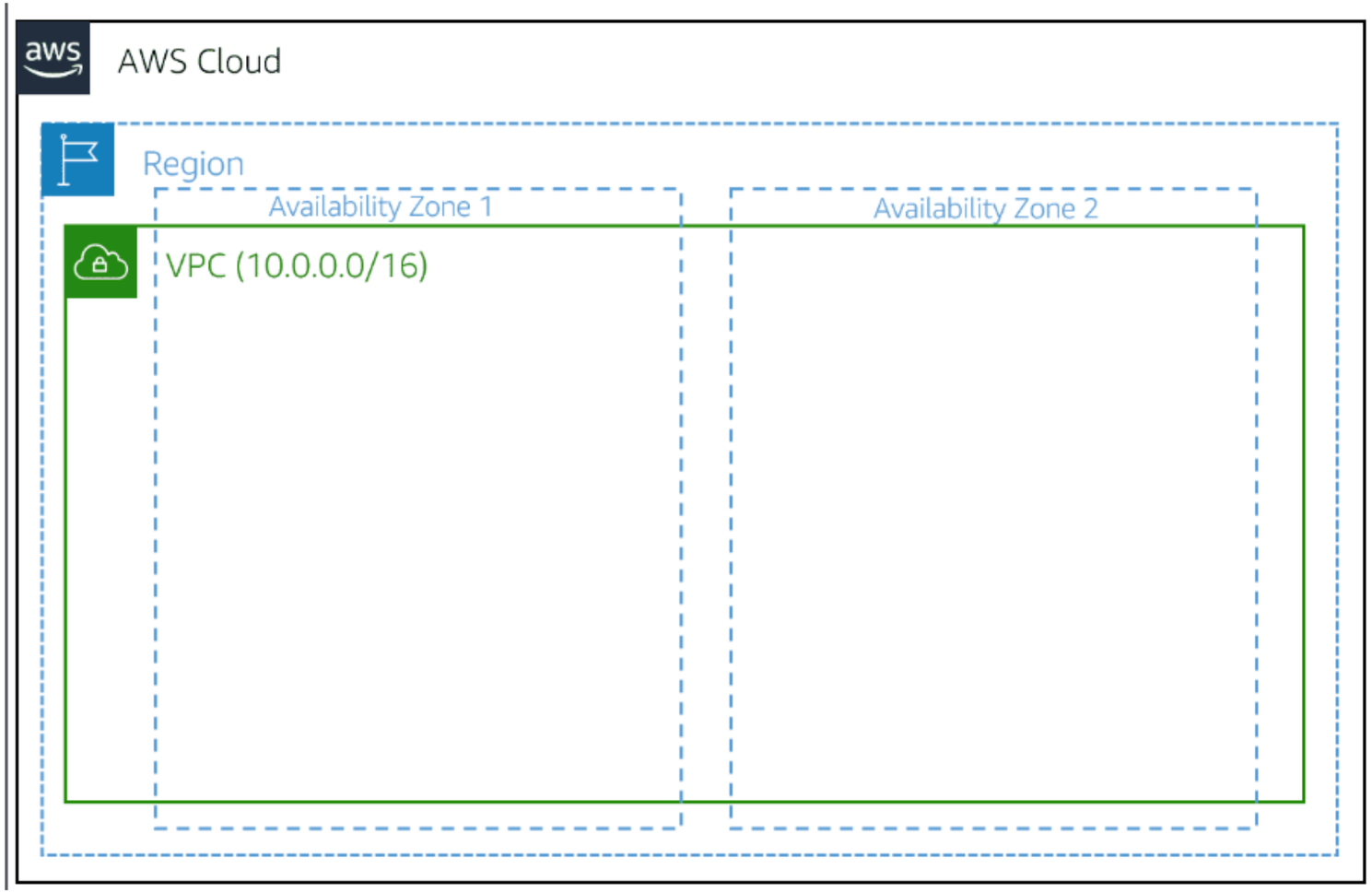
Amazon VPC


Cashier
Customers give their orders to the cashier.
Customers
Barista
Customers try to give their orders directly to the barista.


Customers give their orders to the cashier.
Cashier
Customers
Barista
Customers are prevented from giving their orders to the barista.


Public traffic
VPC
Auto Scaling Group
Security Group
Security Group
Elastic Load Balancer
EC2 Instances
Security Group
Database

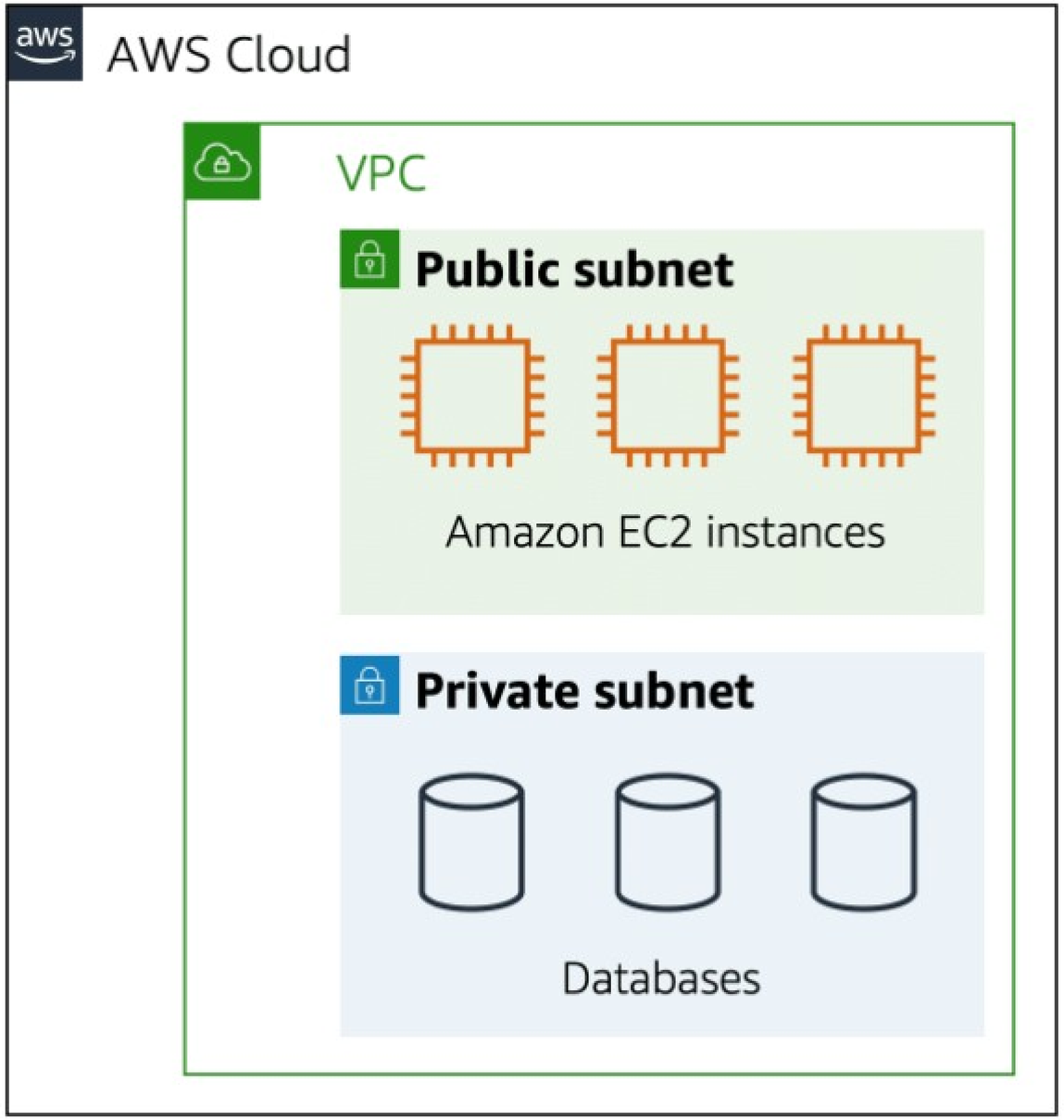
- Amazon VPC creates an isolated virtual network in the AWS Cloud, similar to a traditional data center network.
- When creating a VPC, you define its name, region, and IP range in CIDR notation.



Smart Internz

Subnets

Subnets are smaller networks within a VPC, like VLANs in traditional networks.



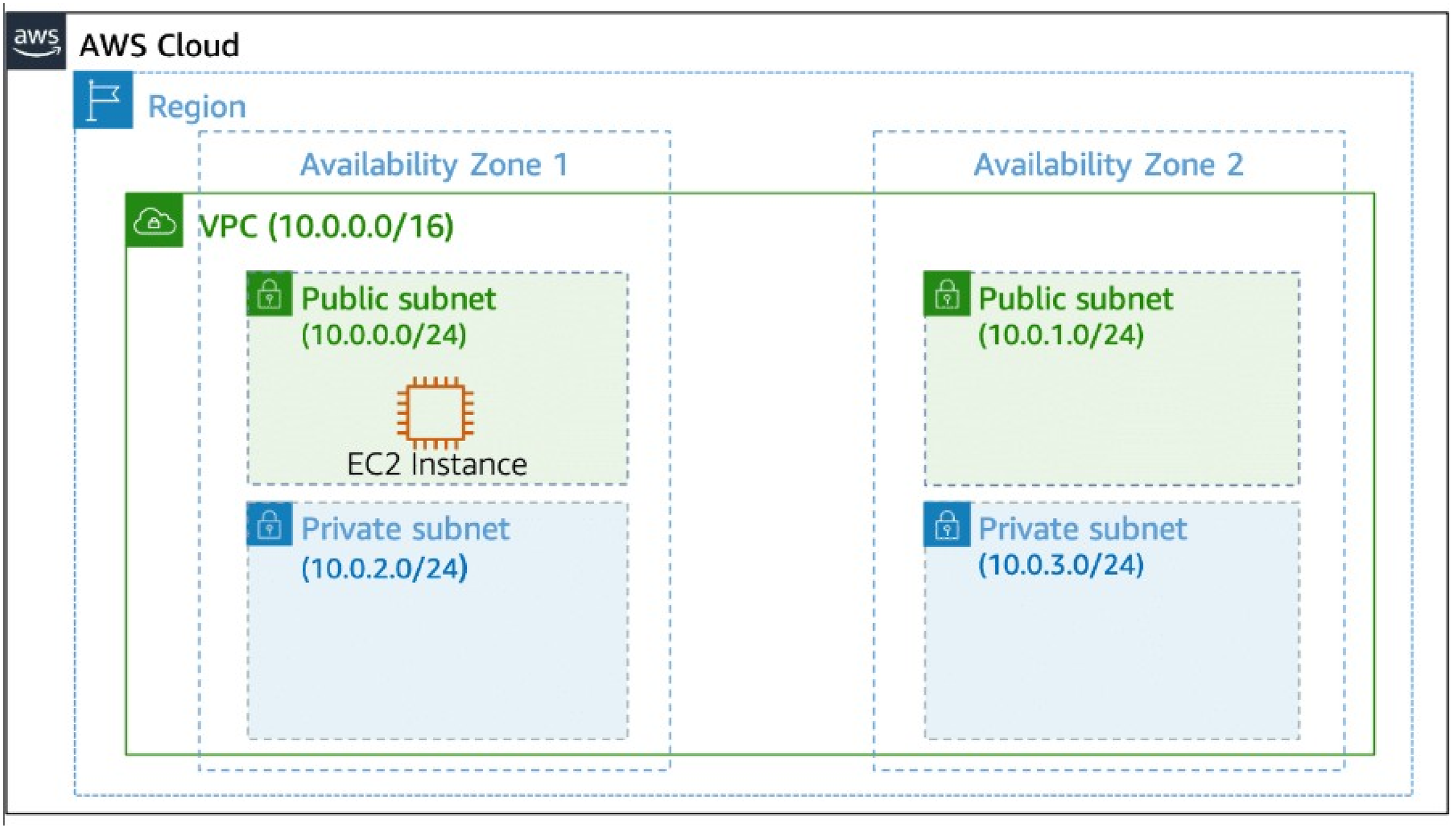
- **Public subnets** contain resources that need to be accessible by the public, such as an online store's website.

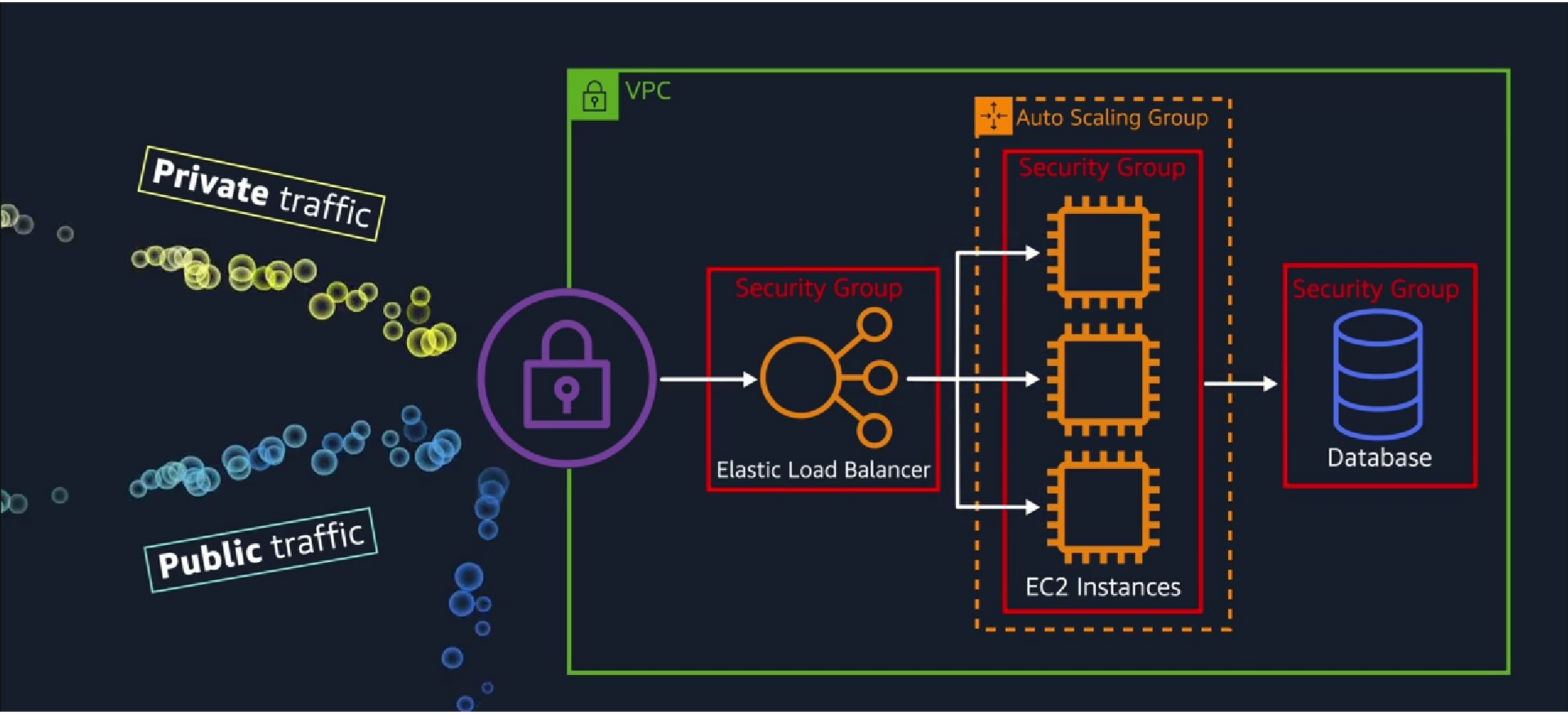
- **Private subnets** contain resources that should be accessible only through your private network, such as a database that contains customers' personal information and order histories.

Smart Internz

When you create a subnet, you must specify the following:

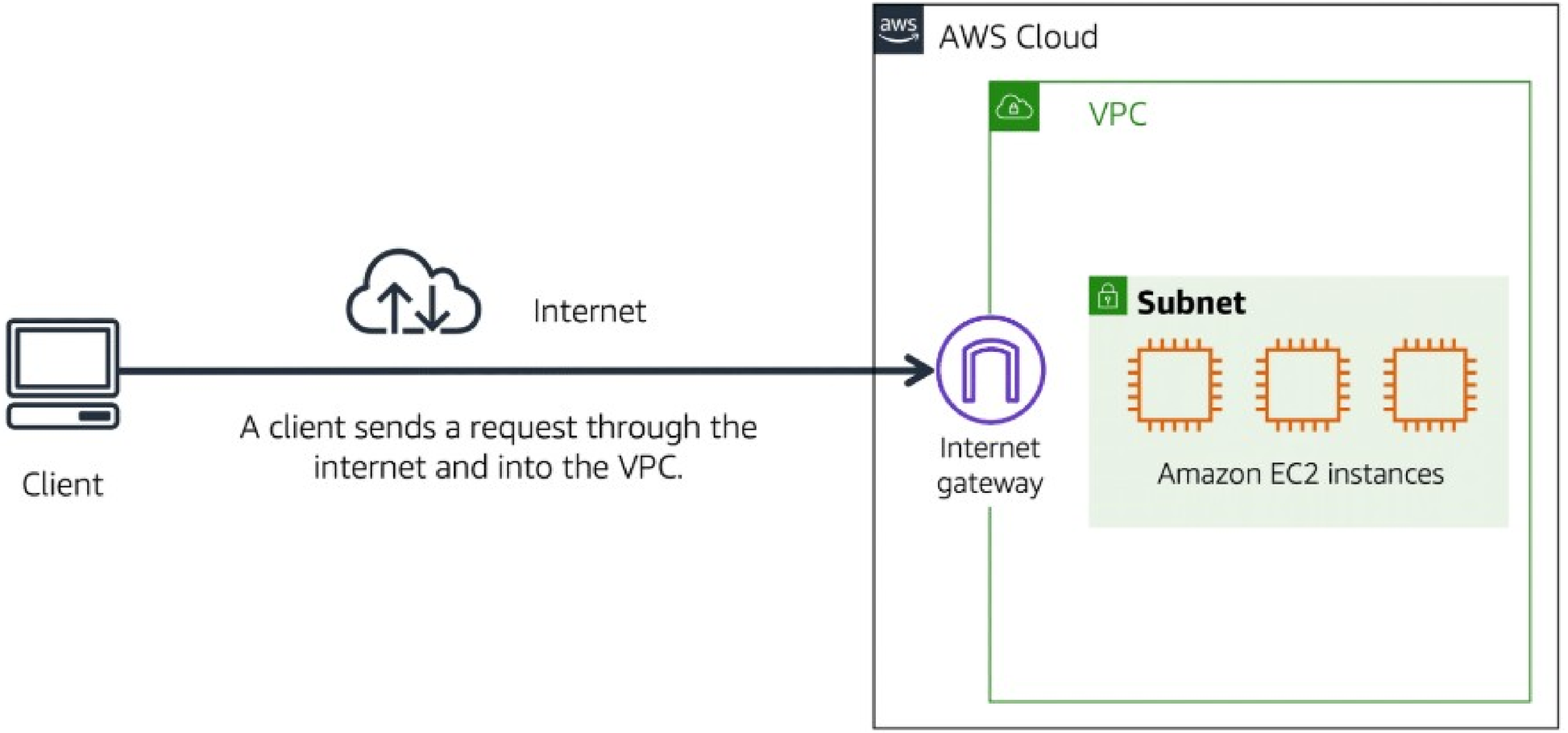
- VPC that you want your subnet to live in—in this case: VPC (10.0.0.0/16)
- Availability Zone that you want your subnet to live in—in this case: Availability Zone 1
- IPv4 CIDR block for your subnet, which must be a subset of the VPC CIDR block—in this case: 10.0.0.0/24
- When you launch an EC2 instance, you launch it inside a subnet, which will be located inside the Availability Zone that you choose.


AWS Cloud
Region
Availability Zone 1
Availability Zone 2
VPC (10.0.0.0/16)
Public subnet
(10.0.0.0/24)
EC2 Instance
Public subnet
(10.0.1.0/24)
Private subnet
(10.0.2.0/24)
Private subnet
(10.0.3.0/24)


Private traffic
Public traffic
VPC
Auto Scaling Group
Security Group
Security Group
Elastic Load Balancer
EC2 Instances
Security Group
Database

Internet gateway

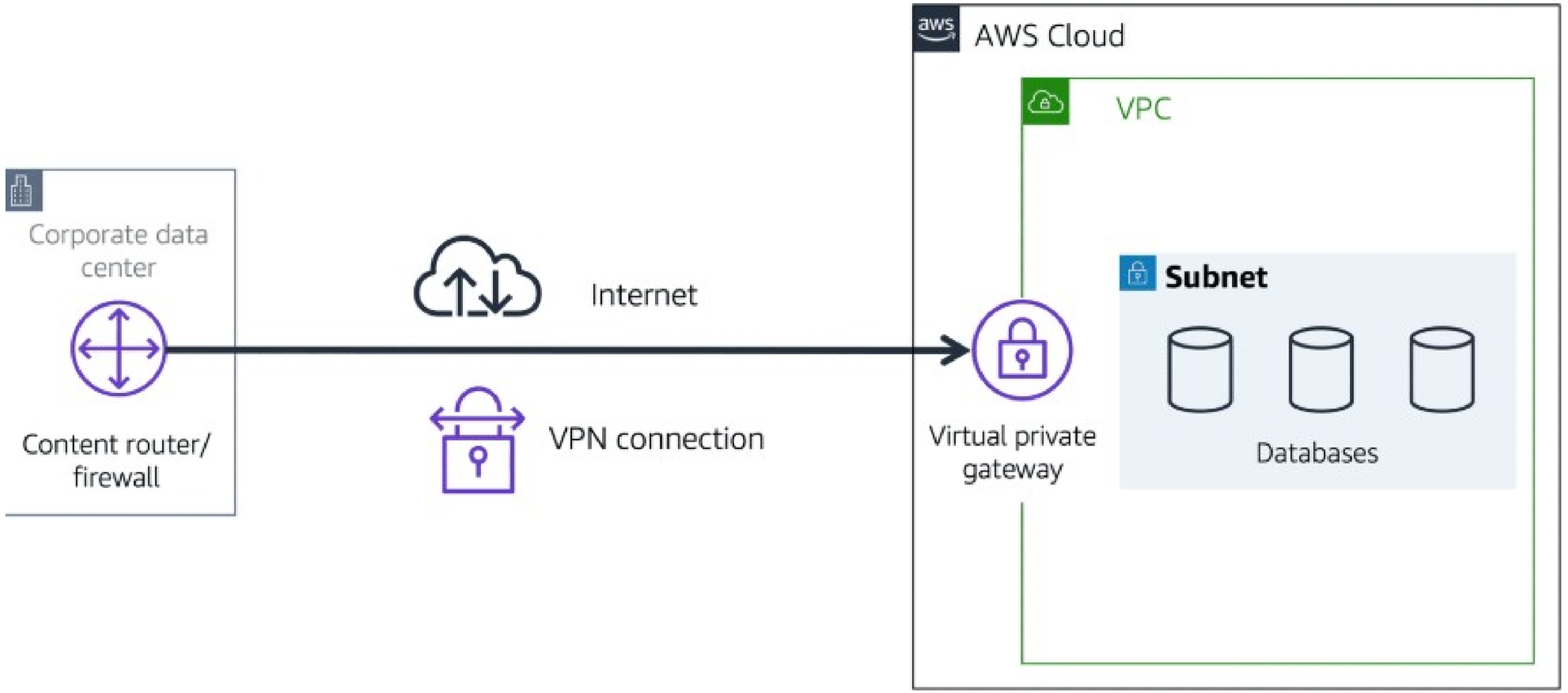
To allow public traffic from the internet to access your VPC, you attach an internet gateway to the VPC.



Smart Internz

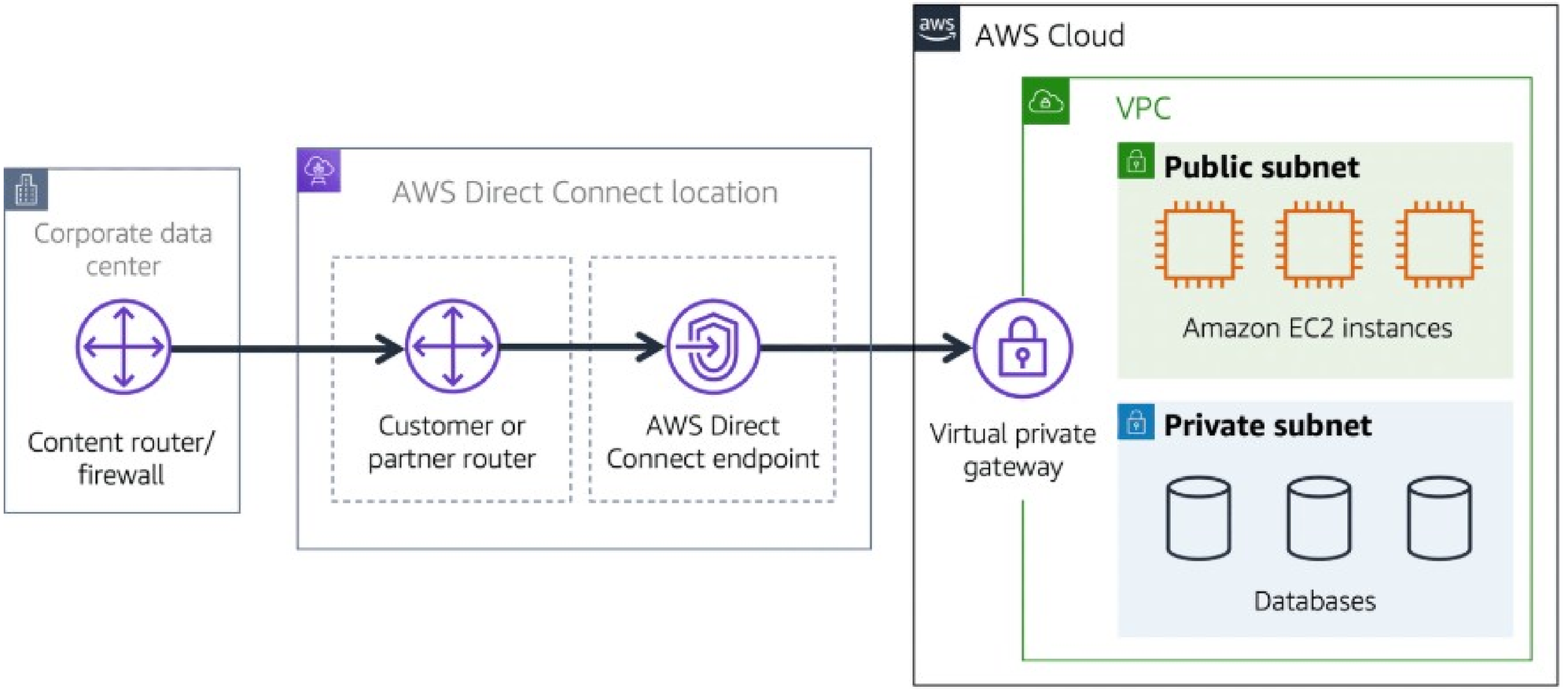
What if you have a VPC that includes only private resources?

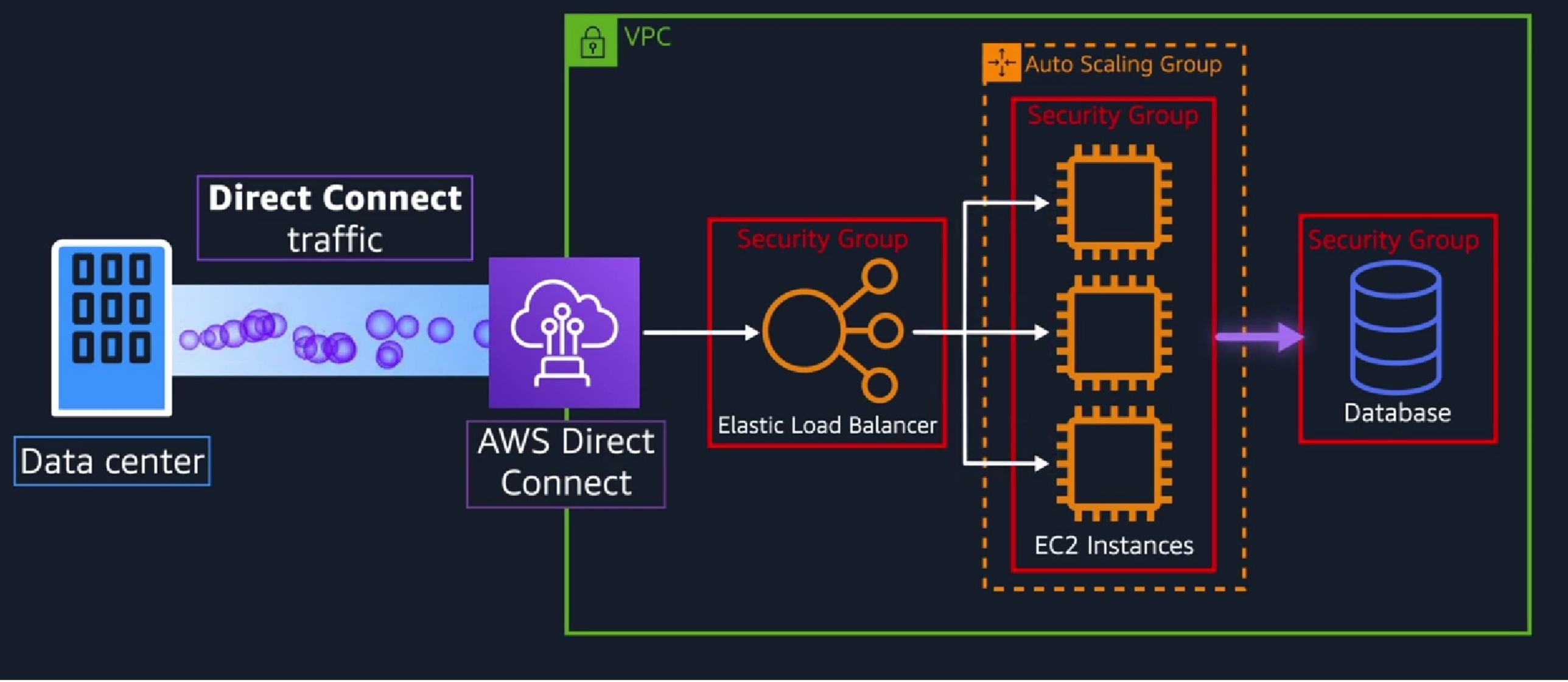
To access private resources in a VPC, you can use a virtual private gateway.



AWS Direct Connect

AWS Direct Connect is a service that lets you to establish a dedicated private connection between your data center and a VPC.

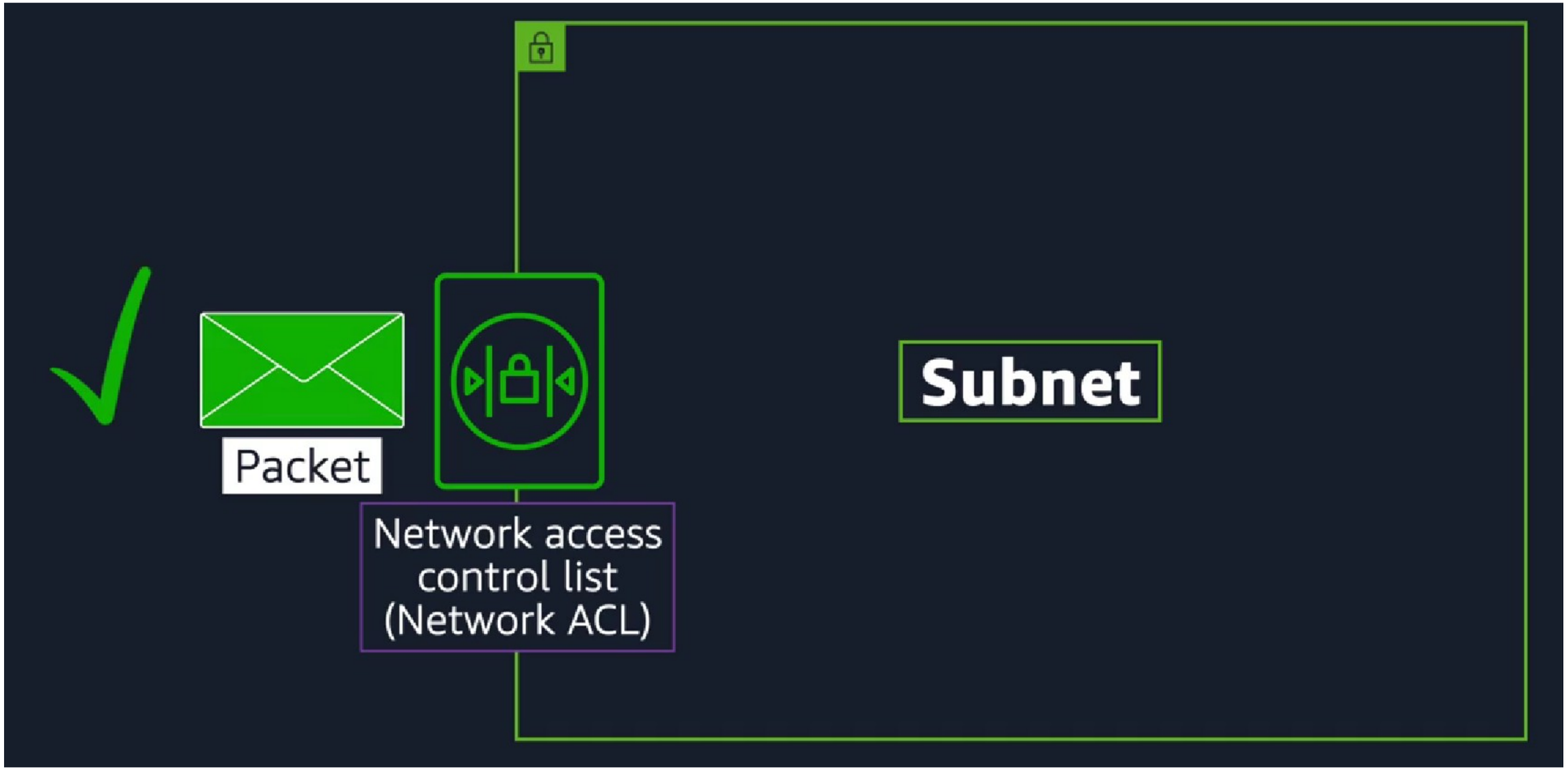




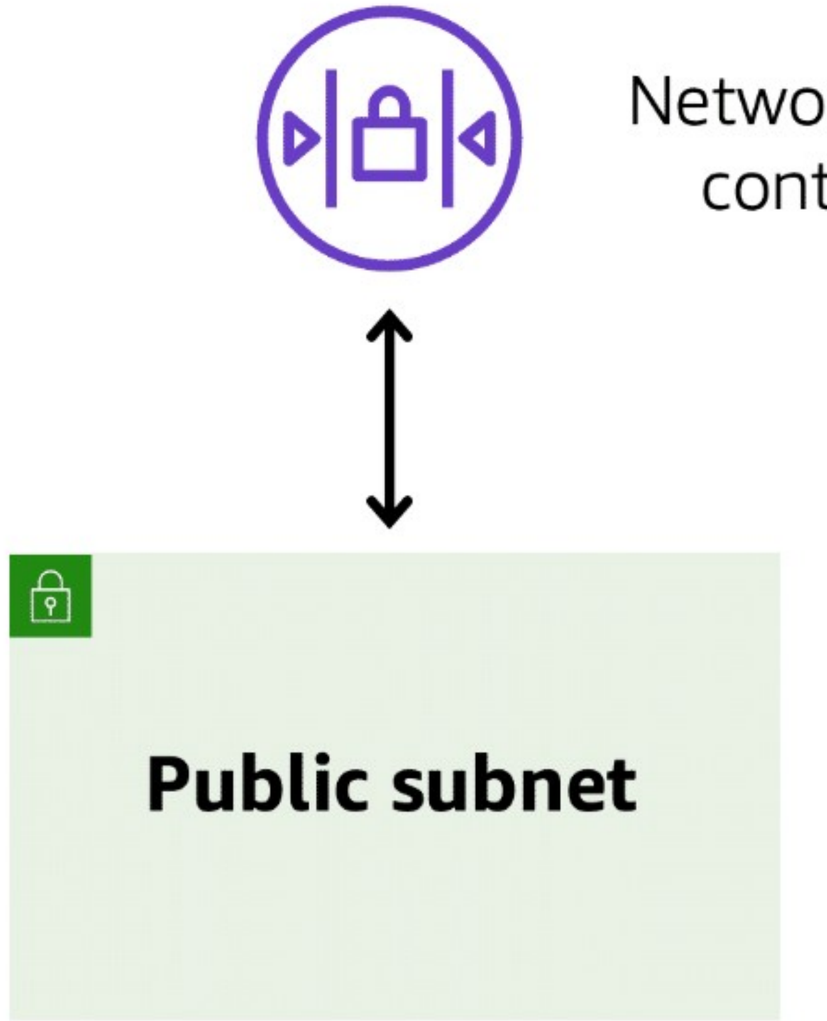
The private connection that AWS Direct Connect provides helps you to reduce network costs and increase the amount of bandwidth that can travel through your network.

Network traffic in a VPC

When a customer requests data from an application hosted in the AWS Cloud, this request is sent as a packet. **A packet** is a unit of data sent over the internet or a network.

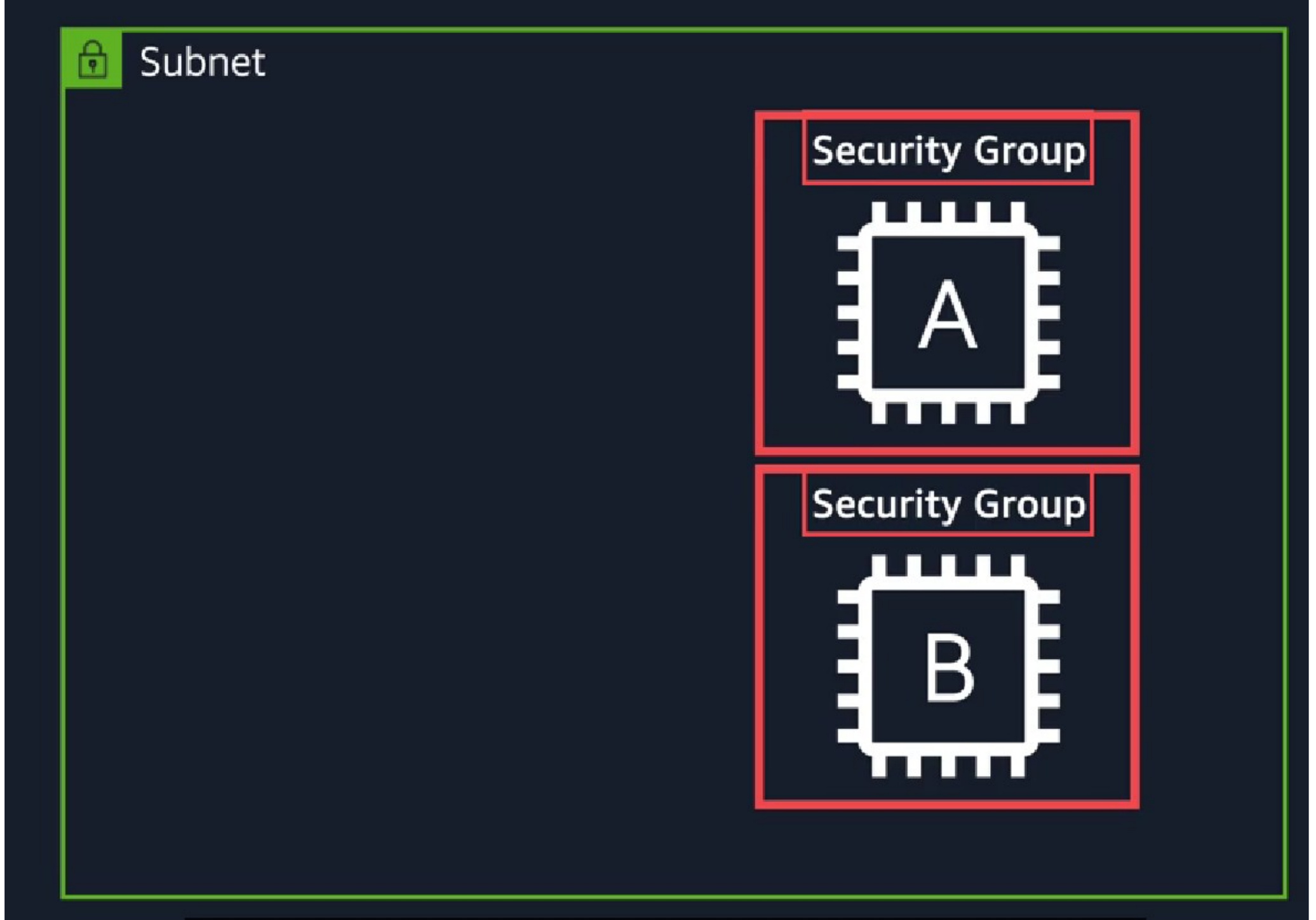


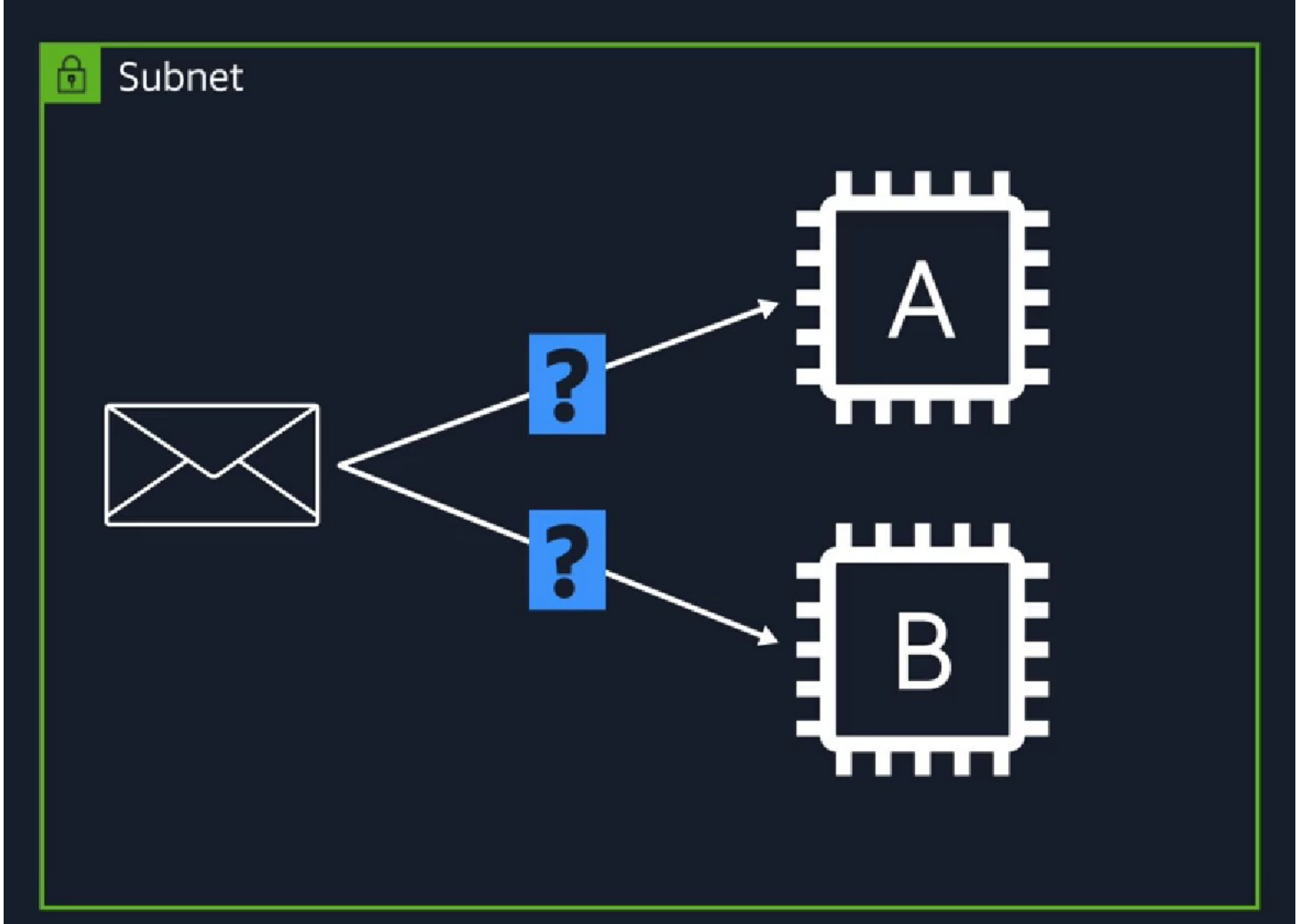
The VPC component that checks packet permissions for subnets is a network access control list (ACL)



Stateless packet filtering

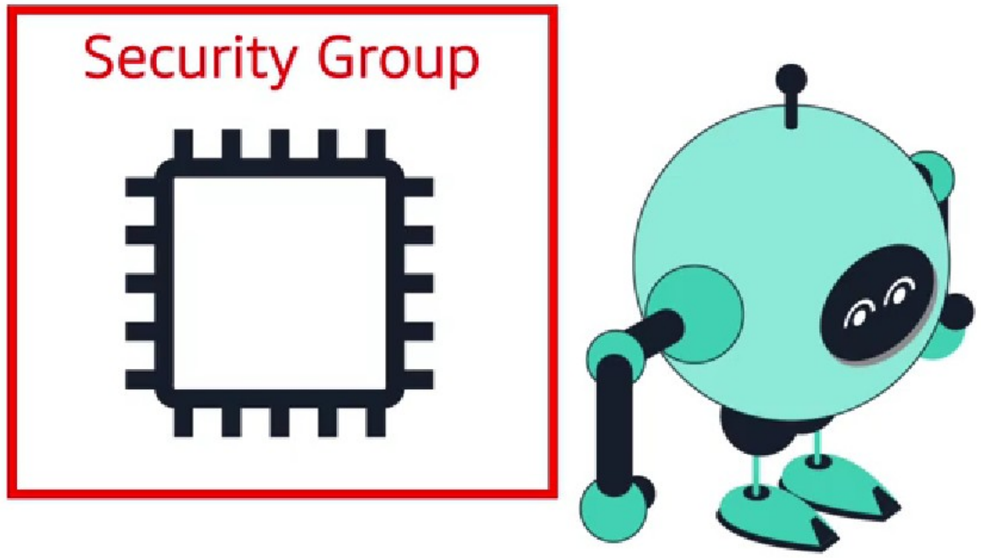
Network ACLs perform stateless packet filtering.
They remember nothing and check packets that cross the subnet border each way:
Inbound
Outbound.


Subnet
Security Group
A
Security Group
B


Subnet
?
?
A
B

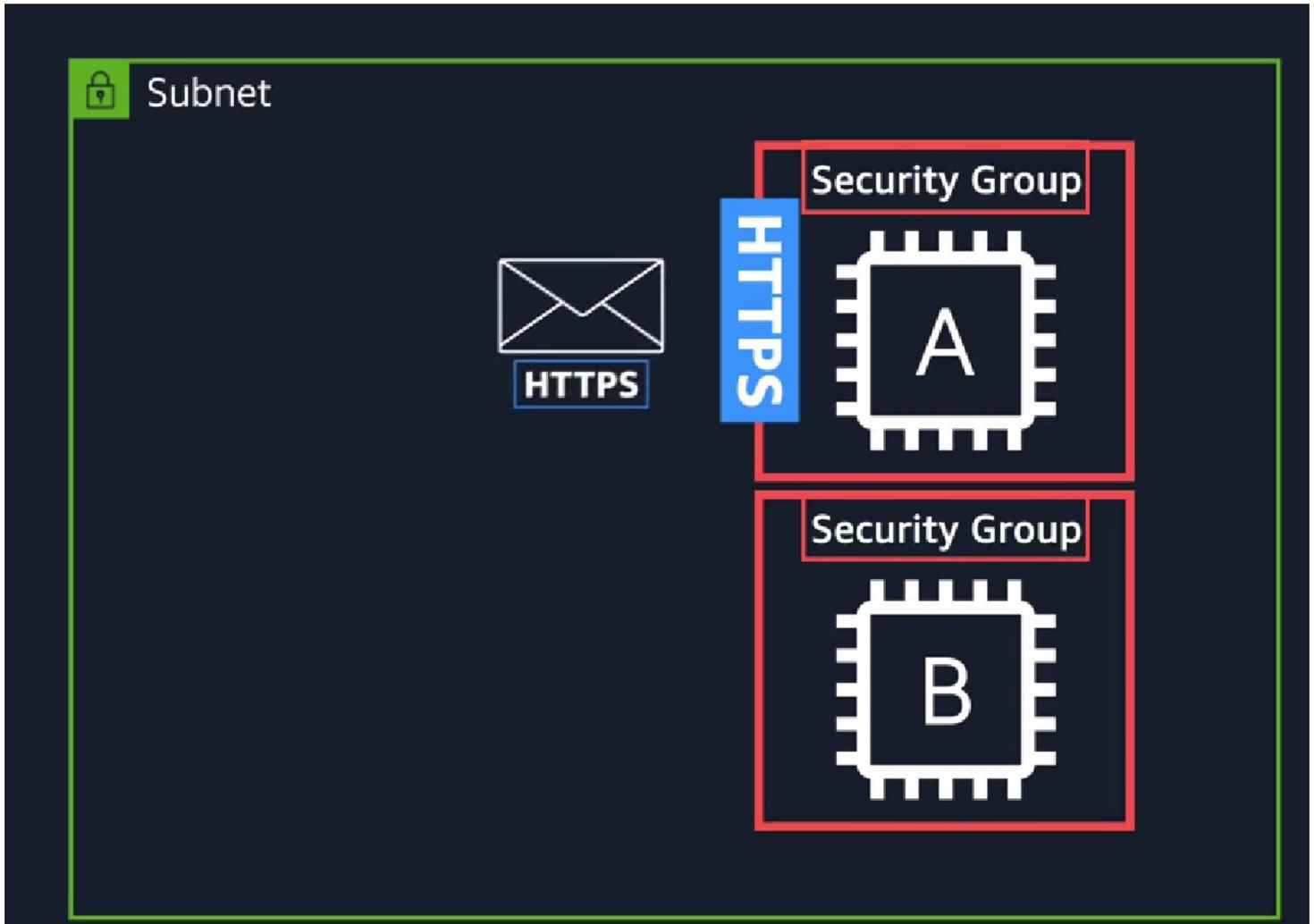
Security Group

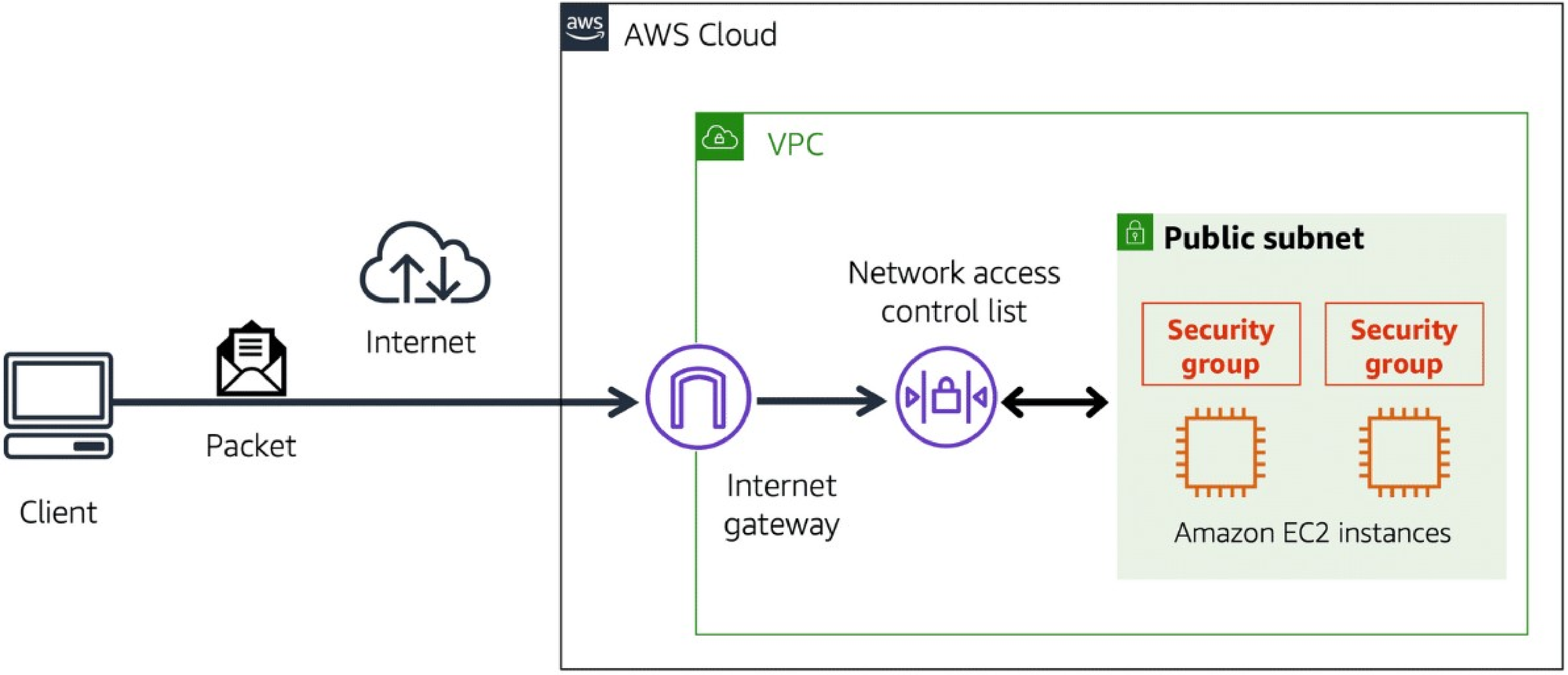
Stateful

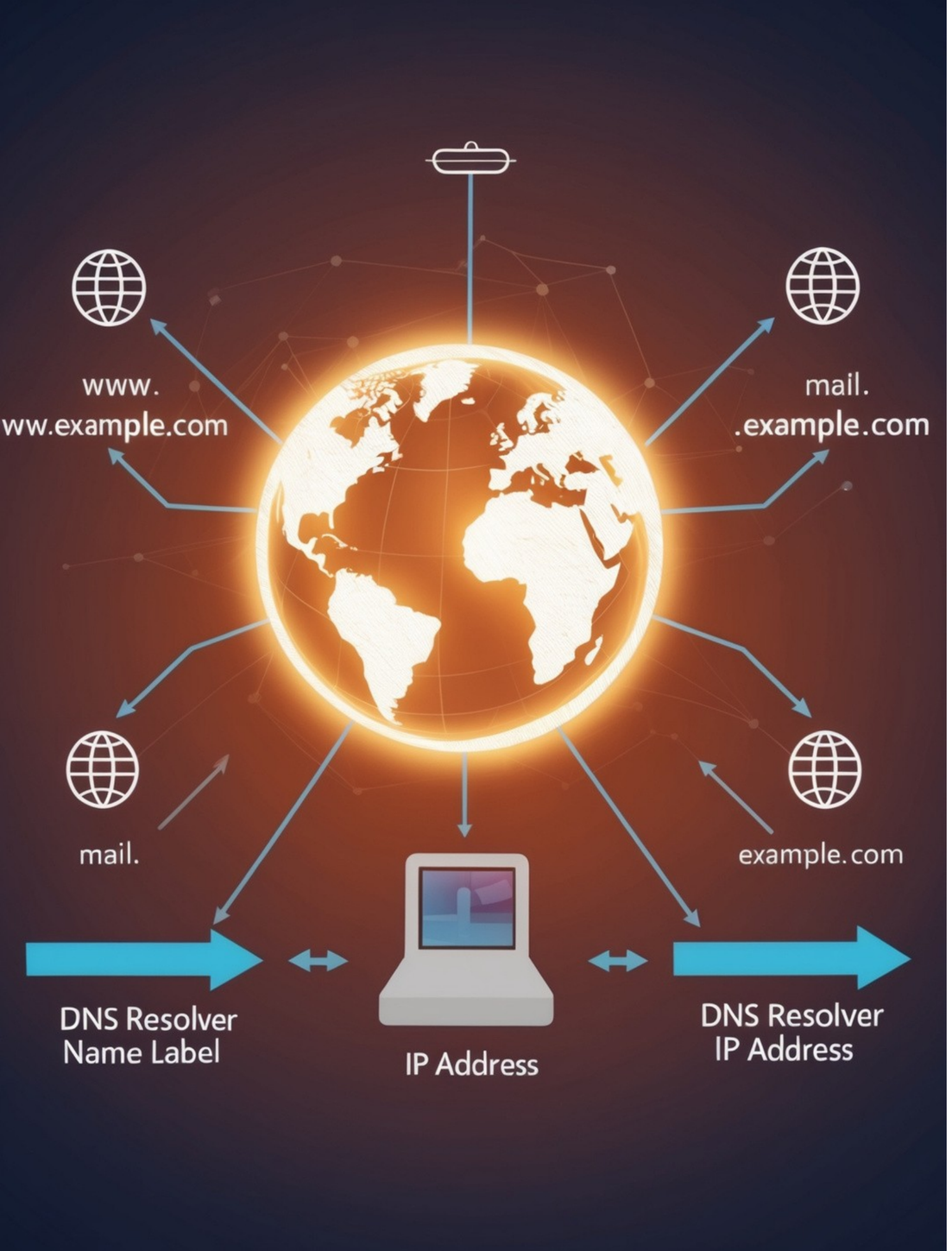


- A **Security group** is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance.
- By default, a security group denies all inbound traffic and allows all outbound traffic.

You can add custom rules to configure which traffic should be allowed;
any other traffic would then be denied

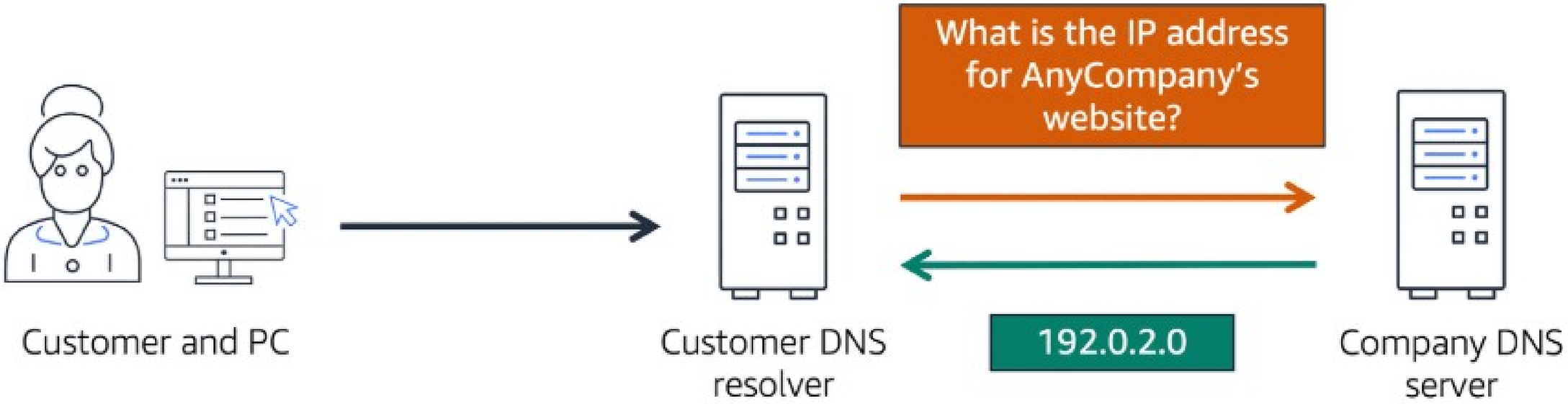



AWS Cloud
VPC
Public subnet
Network access control list
Security group
Security group
Internet
Packet
Client
Internet gateway
Amazon EC2 instances



Domain Name System (DNS)

- DNS is the internet's phone book, translating domain names into IP addresses.
- DNS resolution involves the customer’s DNS resolver communicating with the company’s DNS server.
- This process ensures customers can access websites by entering domain names in their browsers.

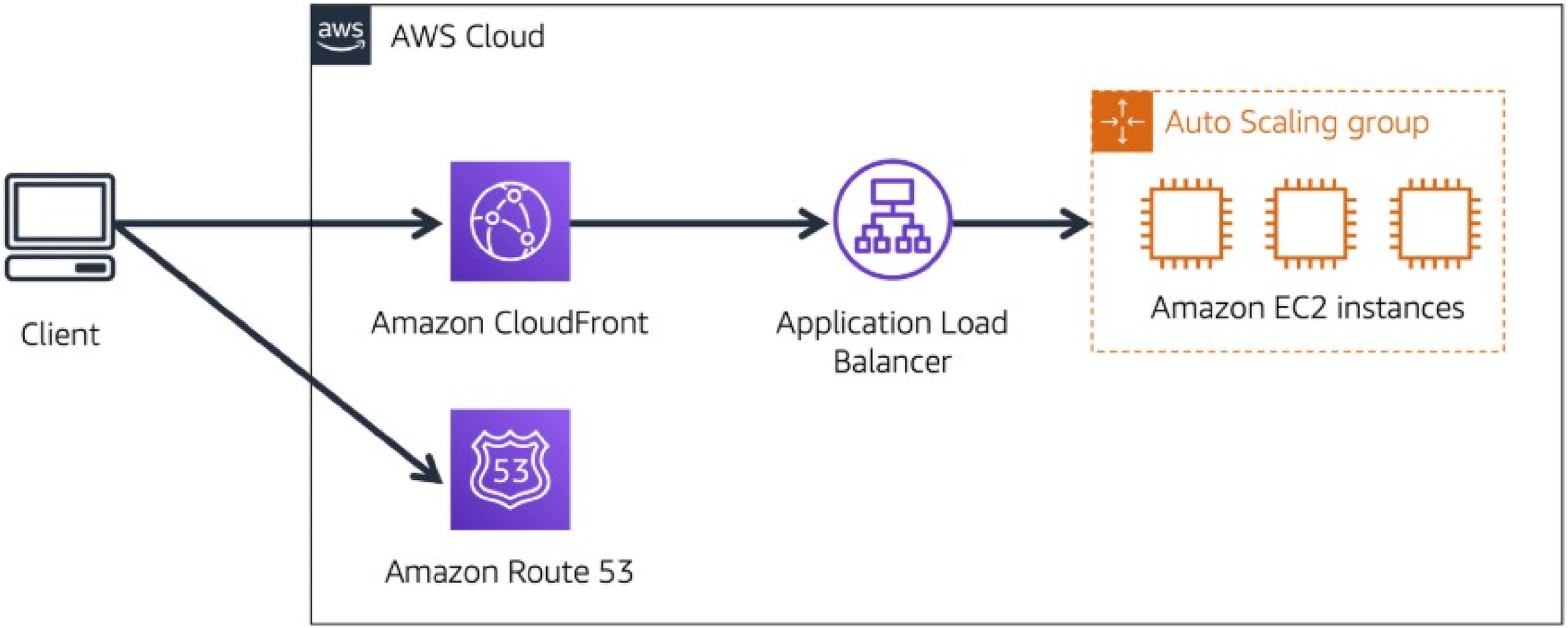


A client connects to a DNS resolver looking for a domain. The resolver forwards the request to the DNS server, which returns the IP address to the resolver.

Amazon Route 53

- Amazon Route 53 routes users to AWS or external resources.
- Connects requests to EC2 instances and load balancers.
- Manages DNS records and registers/transfers domains.
- Centralizes domain management for ease and reliability.

How Amazon Route 53 and Amazon CloudFront deliver content



- **Customer Request:** User visits Any Company's website to access the application.
- **DNS Resolution:** Amazon Route 53 identifies the website's IP address (e.g., 192.0.2.0) and returns it to the user.
- **Edge Location:** The request is routed to the nearest edge location via Amazon CloudFront.
- **Application Routing:** CloudFront connects to an Application Load Balancer, which directs the request to an Amazon EC2 instance.