Cloud-Native Networking Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

VPC a logically isolated section of the AWS Cloud where you can launch AWS resources

Region the geographical location of your network

AZ the data center of your AWS resources

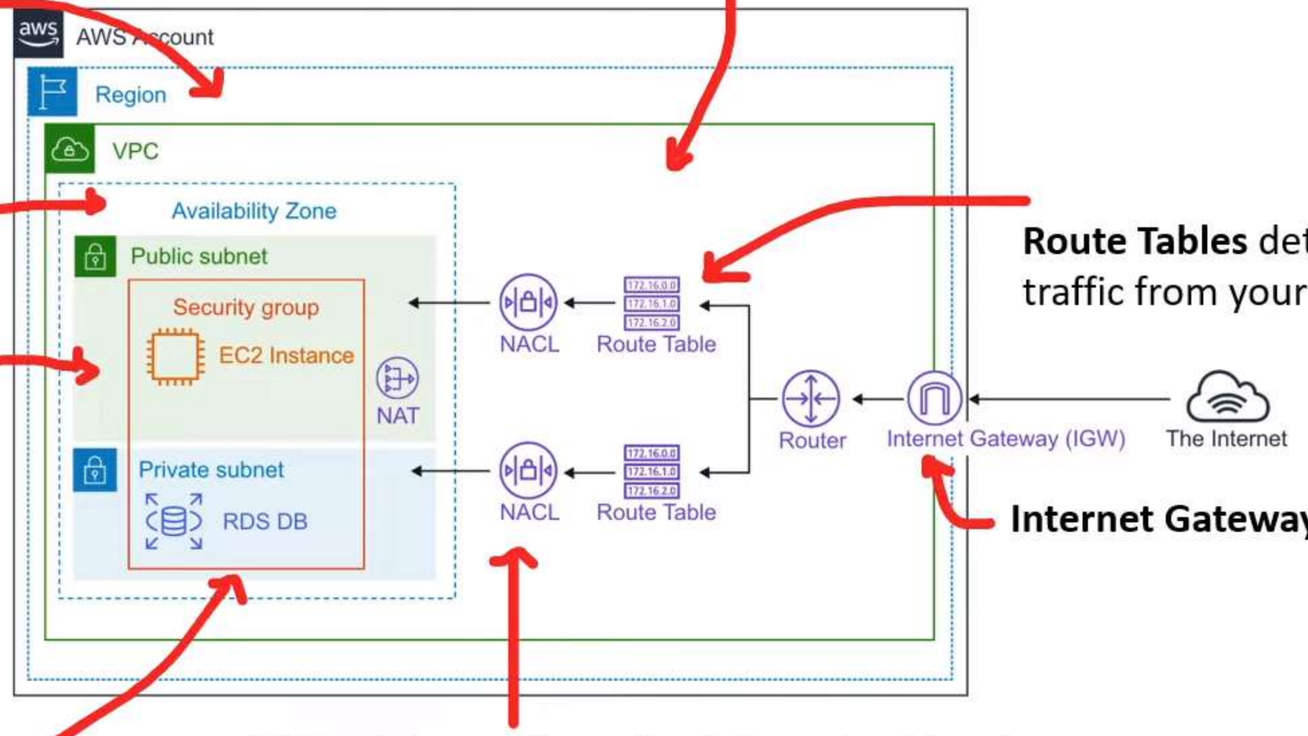
Route Tables determine where network traffic from your subnets are directed

Subnets a logical partition of an IP network into multiple, smaller network segments

Internet Gateway Enable access to the Internet

Security Groups Acts as firewall at the instance level

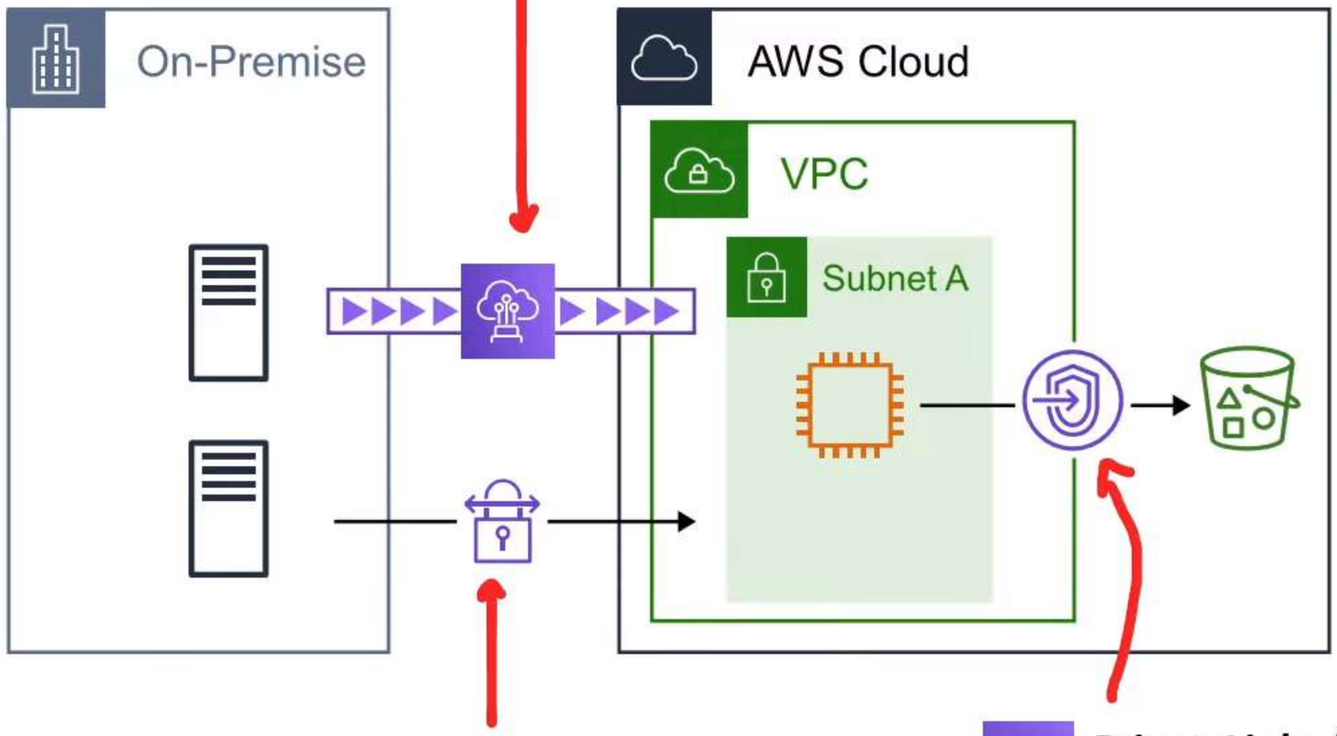
NACLs Acts as a firewalls at the subnet level



Enterprise/Hybrid Networking

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

DirectConnect dedicated gigabit connection from on-premise data-center to AWS (a very fast connection)



AWS Virtual Private Network (VPN) a secure connection between on-premise, remote offices, mobile employees.

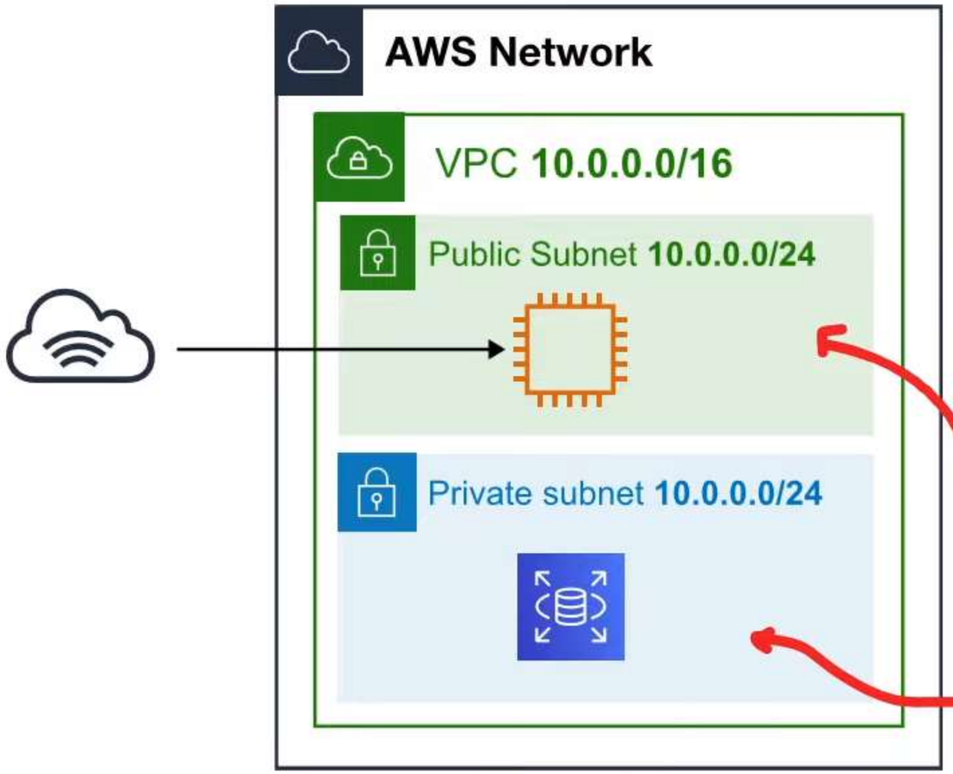
PrivateLinks (VPC Interface Endpoints) keeps traffic within the AWS network and not traverse the internet to keep traffic is secure.

Virtual Private Cloud (VPC) and Subnets

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Virtual Private Cloud (VPC) is a logically isolated section of the AWS Network where you launch your AWS resources. You choose a **range of IPs using CIDR Range**

CIDR Range of **10.0.0.0/16 = 65,536** IP Addresses



Subnets a logical partition of an IP network into multiple smaller network segments. **You are breaking up your IP range for VPC** into smaller networks.

Subnets **need to have a smaller CIDR range than to the VPC** represent their portion.
eg Subnet CIDR Range 10.0.0.0/24 = 256 IP Addresses

A Public Subnet is one that can reach the internet

A Private Subnet is one that cannot reach the internet

Security Groups vs NACLs

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Network Access Control Lists (NACLs)

Acts as a virtual **firewall at the subnet level**

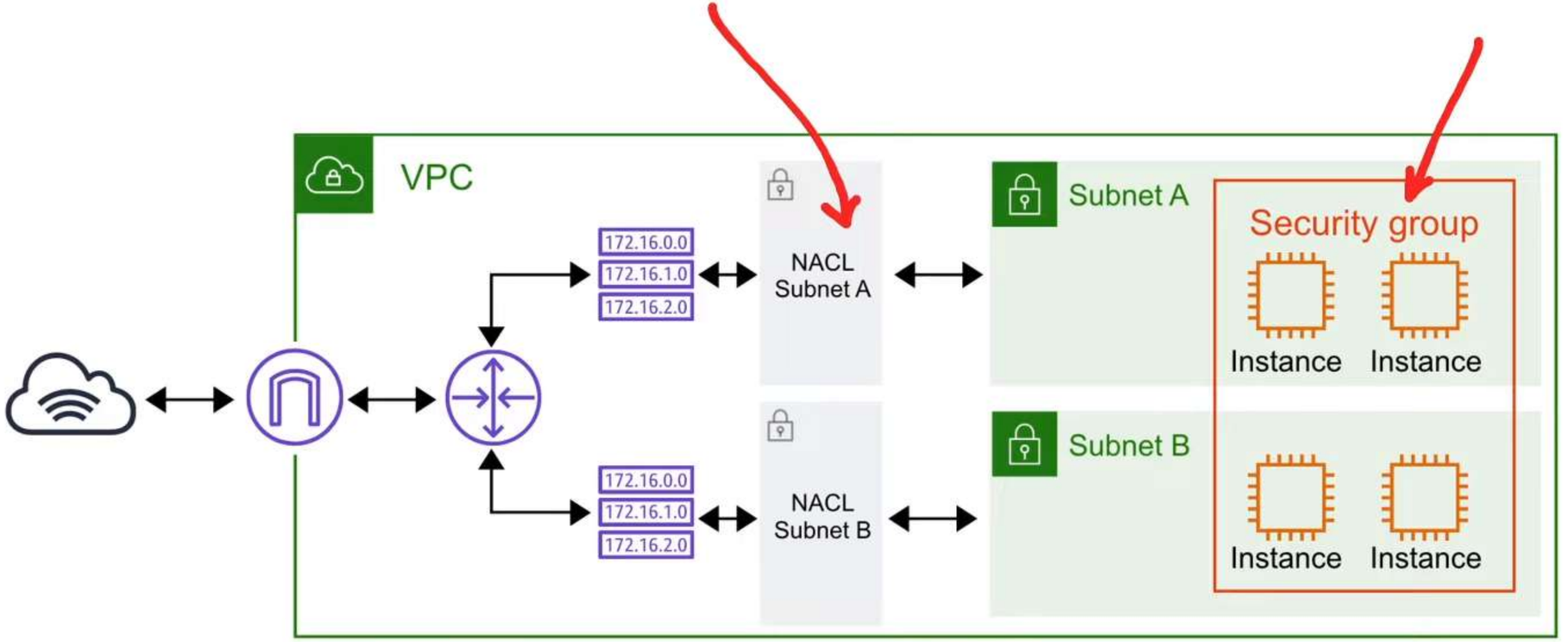
You create **Allow and Deny rules**.

eg. Block a specific IP address known for abuse

Security Groups

Acts as a virtual **firewall at the instance level**

Implicitly denies all traffic. **You create only Allow rules.**

eg. Allow an EC2 instance access on port 22 for SSH

eg. You cannot block a single IP address.