Virtual Private Cloud (VPC)

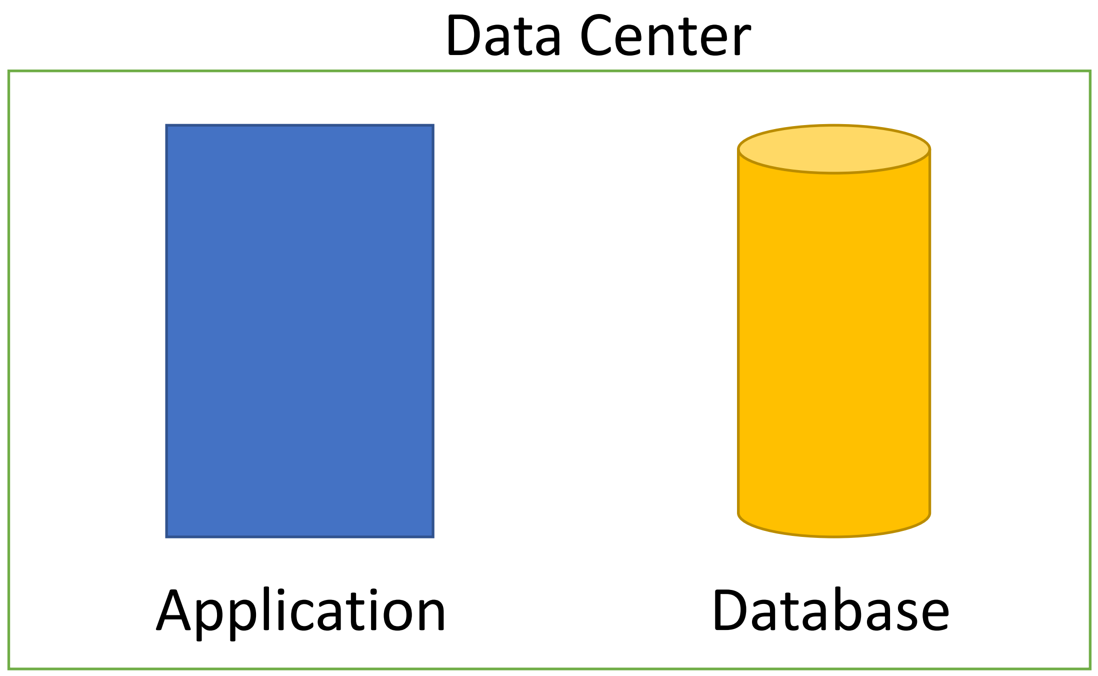
Why VPC

- Who can Access the application and database ?

- Can anyone from internet directly connect to the database ?

How do we create your own Private Network in Cloud

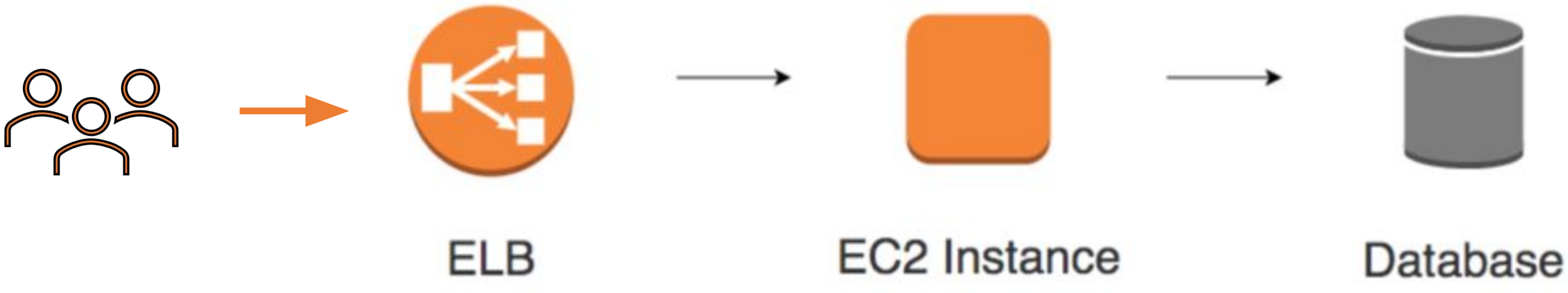
- **AWS VPC**



AWS VPC

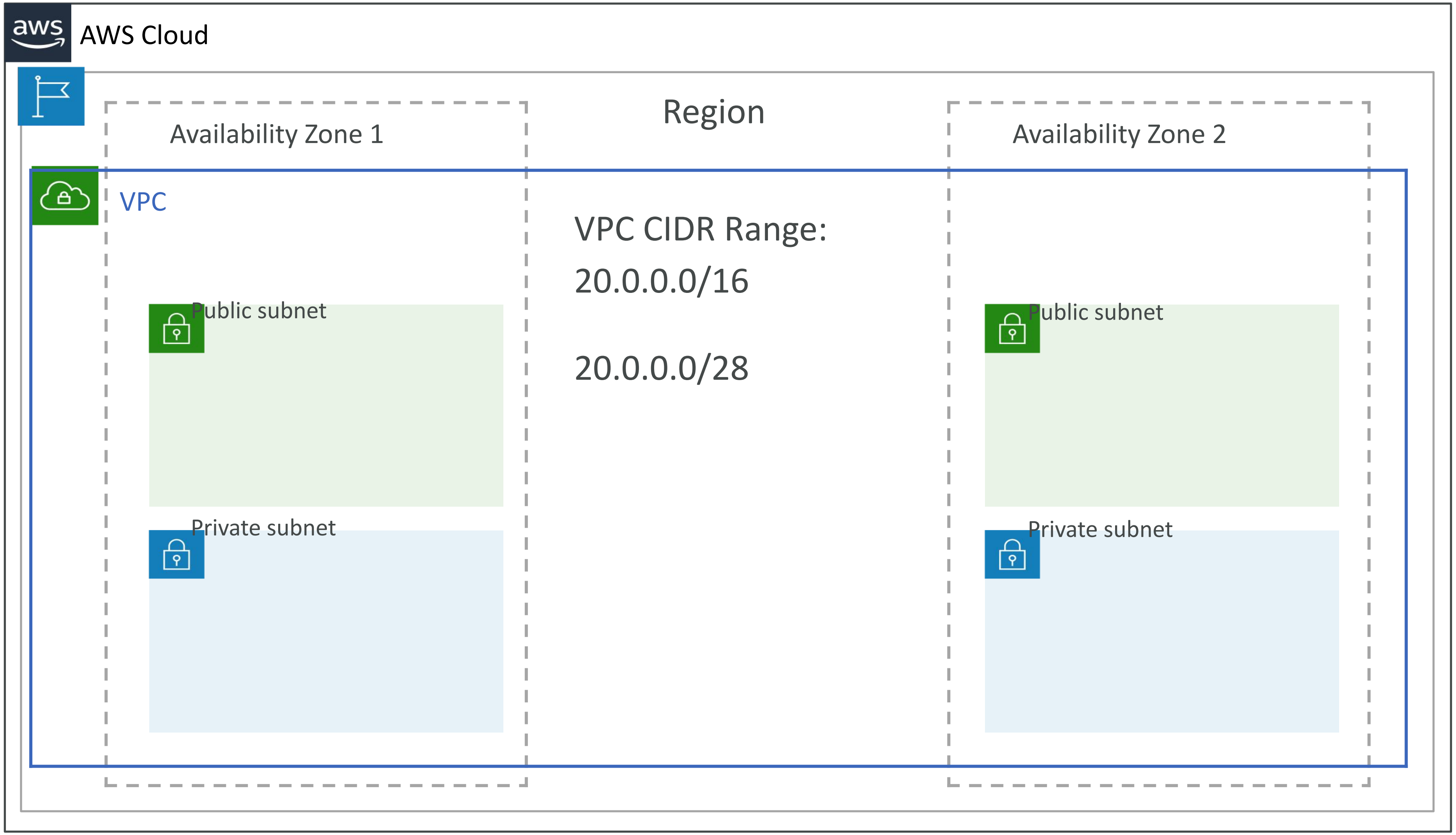
- It is our own isolated network in AWS cloud
- Network traffic within a VPC is isolated (not visible) from all other Amazon VPCs and other resources in AWS
- We control all the traffic coming in and going outside a VPC
- Create all your AWS resources (compute, storage, databases etc) within a VPC
- Secure resources from unauthorized access AND Enable secure communication between your cloud resources

AWS VPC



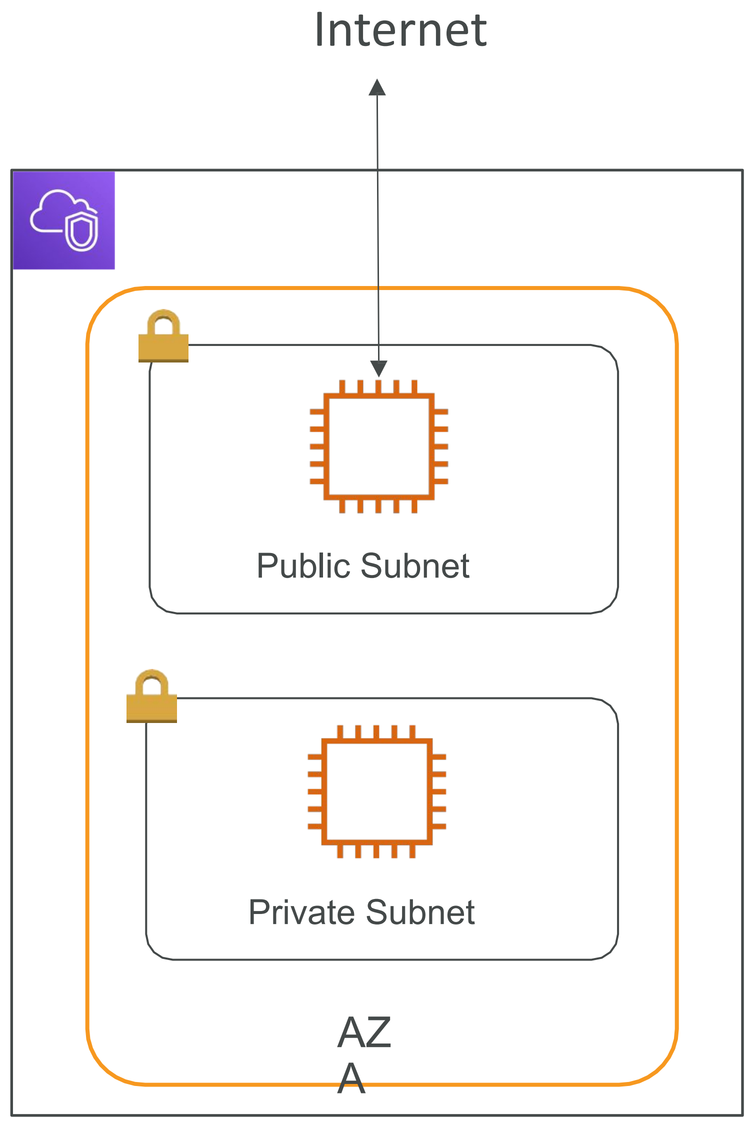
- Public Elastic Load Balancers are accessible from internet (public resources)
- Databases or EC2 instances should NOT be accessible from internet
- ONLY applications within your network (VPC) should be able to access them (private resources)
- How do you separate public resources from private resources inside a VPC?

AWS VPC -Diagram



AWS VPC

- VPC - Virtual Private Cloud: private network to deploy your resources (regional resource)
- Subnets allow you to partition your network inside your VPC (Availability Zone resource)
- A public subnet is a subnet that is accessible from the internet
- A private subnet is a subnet that is not accessible from the internet
- To define access to the internet and between subnets, we use Route Tables.



AWS VPC

CIDR (Classless Inter-Domain Routing) Blocks

- Resources in same network use similar IP address to make routing easy:
  - Example: Resources inside a specific network can use IP addresses from 69.208.0.0 to 69.208.0.15

- How do you express a range of addresses that resources in a network can have?
- CIDR block

- A CIDR block consists of a starting IP address(69.208.0.0) and a range(/28)
- Example: CIDR block 69.208.0.0/28 represents addresses from 69.208.0.0 to 69.208.0.15 – a total of 16 addresses

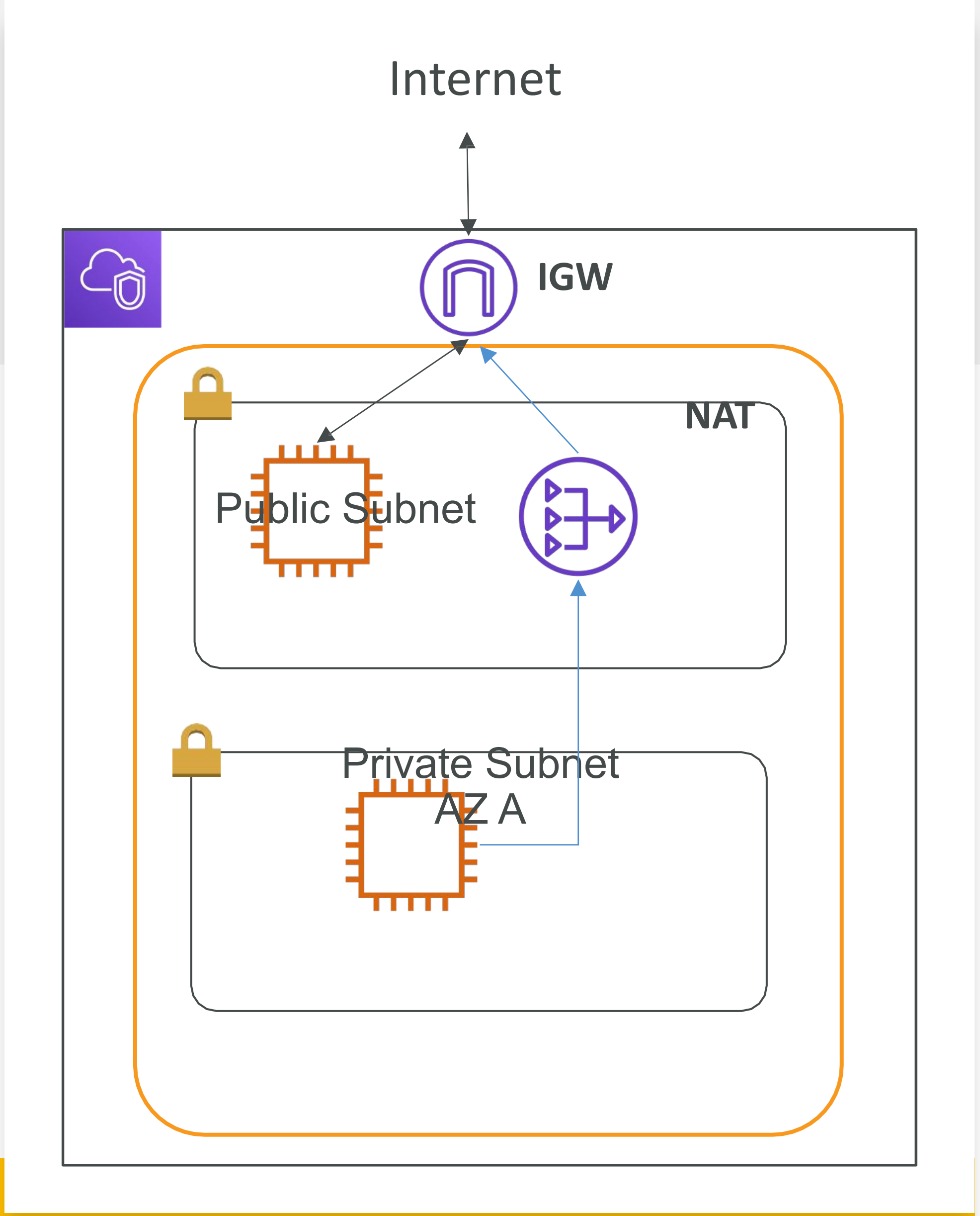
- Tip: 69.208.0.0/28 indicates that the first 28 bits (out of 32) are fixed.
- Last 4 bits can change => 2 to the power 4 = 16 addresses

AWS VPC

Internet Gateway & NAT Gateways

- Internet Gateways helps our VPC instances connect with the internet
- Public Subnets have a route to the internet gateway.

- NAT Gateways (AWS-managed) & NAT Instances (self-managed) allow your instances in your Private Subnets to access the internet while remaining private
- Three Options:
  - NAT Instance: Install a EC2 instance with specific NAT AMI and configure as a gateway
  - NAT Gateway: Managed Service
  - Egress-Only Internet Gateways: For IPv6 subnets



AWS VPC Network ACL & Security Groups

NACL (Network Access control List)

A firewall which controls traffic from and to subnet

Can have ALLOW and DENY rules

Are attached at the Subnet level

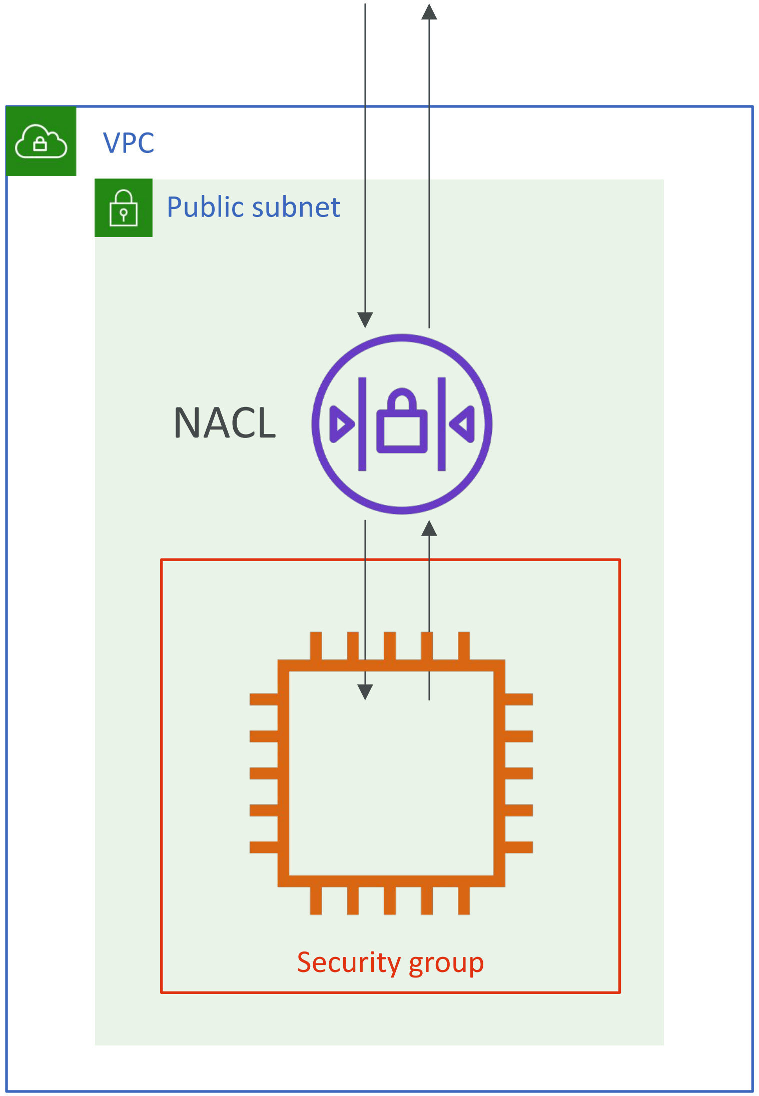
Rules only include IP addresses

Security Groups

A firewall that controls traffic to and from an EC2 Instance

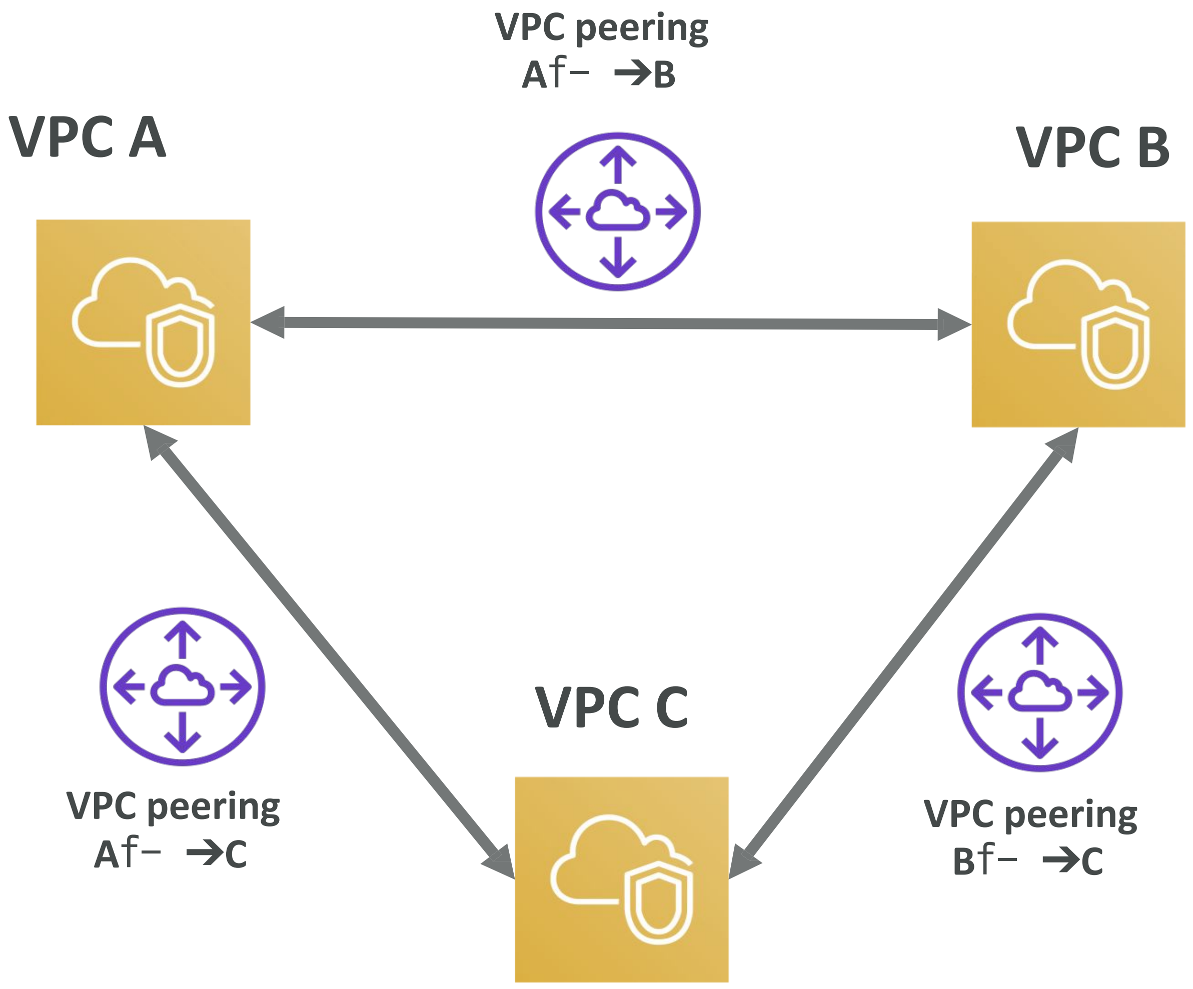
Can have only ALLOW rules

Rules include IP addresses and other security groups



AWS VPC
- VPC Peering

- Connect two VPC, privately using AWS' network
- Make them behave as if they were in the same network
- Must not have overlapping CIDR (IP address range)
- VPC Peering connection is not transitive (must be established for each VPC that need to communicate with one another)



VPC peering
Af– →B

VPC A

VPC B

VPC C

VPC peering
Af– →C

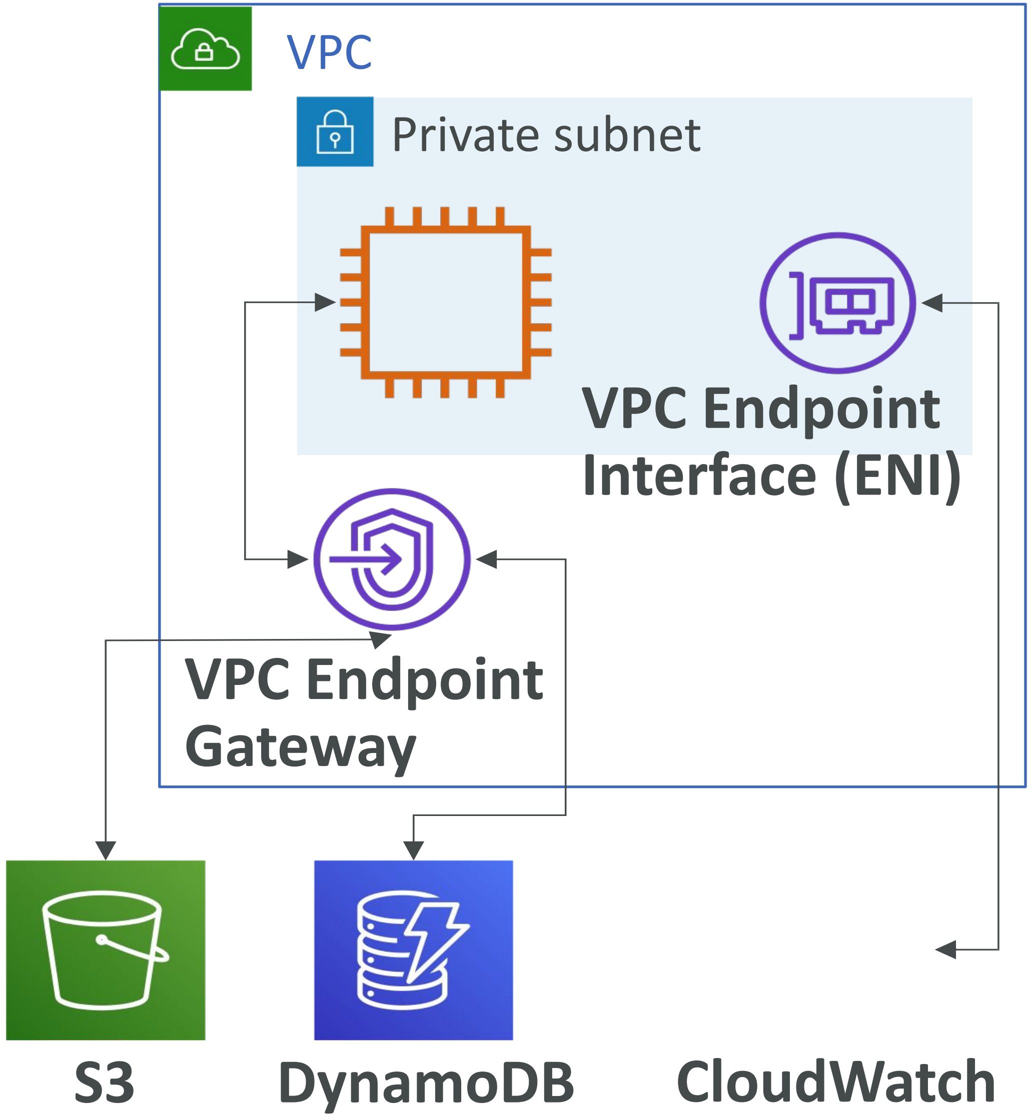
VPC peering
Bf– →C

AWS VPC
- VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- This gives you enhanced security and lower latency to access AWS services

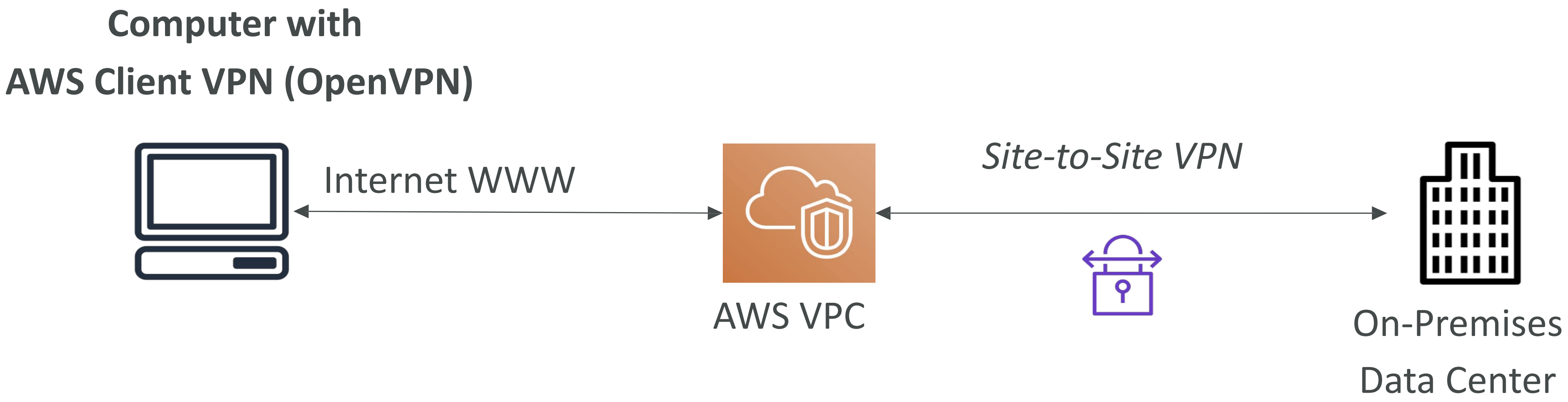
<span></span>

VPC Endpoint Gateway: S3 & DynamoDB
VPC Endpoint Interface: the rest



AWS VPC
- AWS Client VPN

- Connect from your computer using OpenVPN to your private network in AWS and on-premises
- Allow you to connect to your EC2 instances over a private IP (just as if you were in the private VPC network)
- Goes over public Internet



AWS VPC :Summary

- VPC: Virtual Private Cloud
- Subnets: Tied to an AZ, network partition of the VPC
- Internet Gateway: at the VPC level, provide Internet Access
- NAT Gateway / Instances: give internet access to private subnets
- NACL: Stateless, subnet rules for inbound and outbound
- Security Groups: Stateful, operate at the EC2 instance level or ENI
- VPC Peering: Connect two VPC with non overlapping IP ranges, nontransitive