

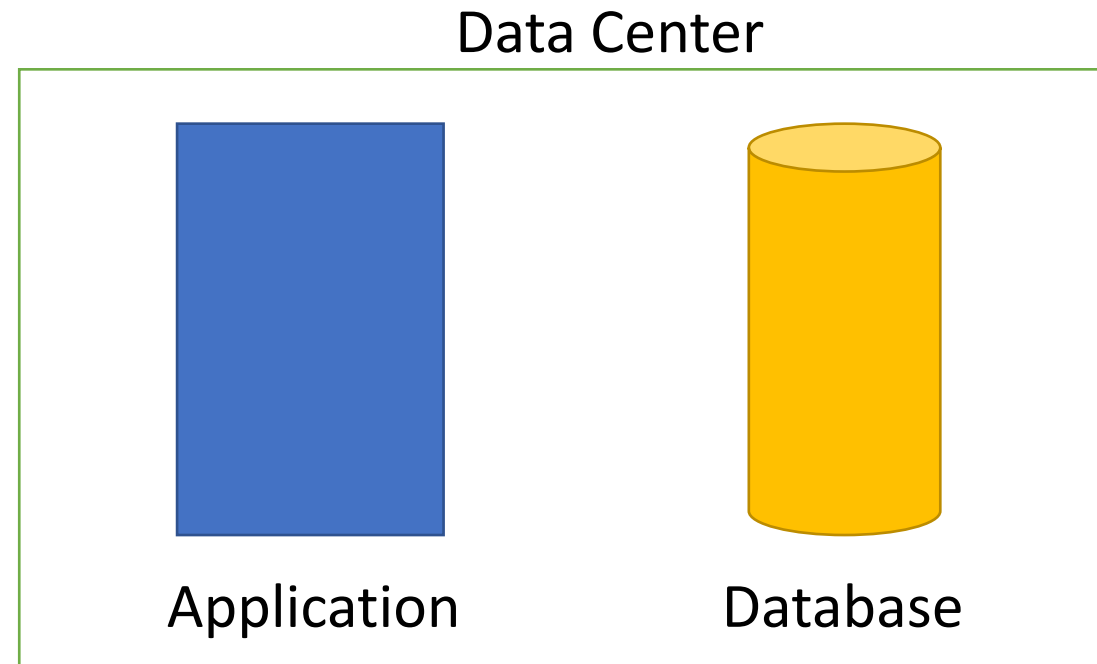
Virtual Private Cloud (VPC)

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 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



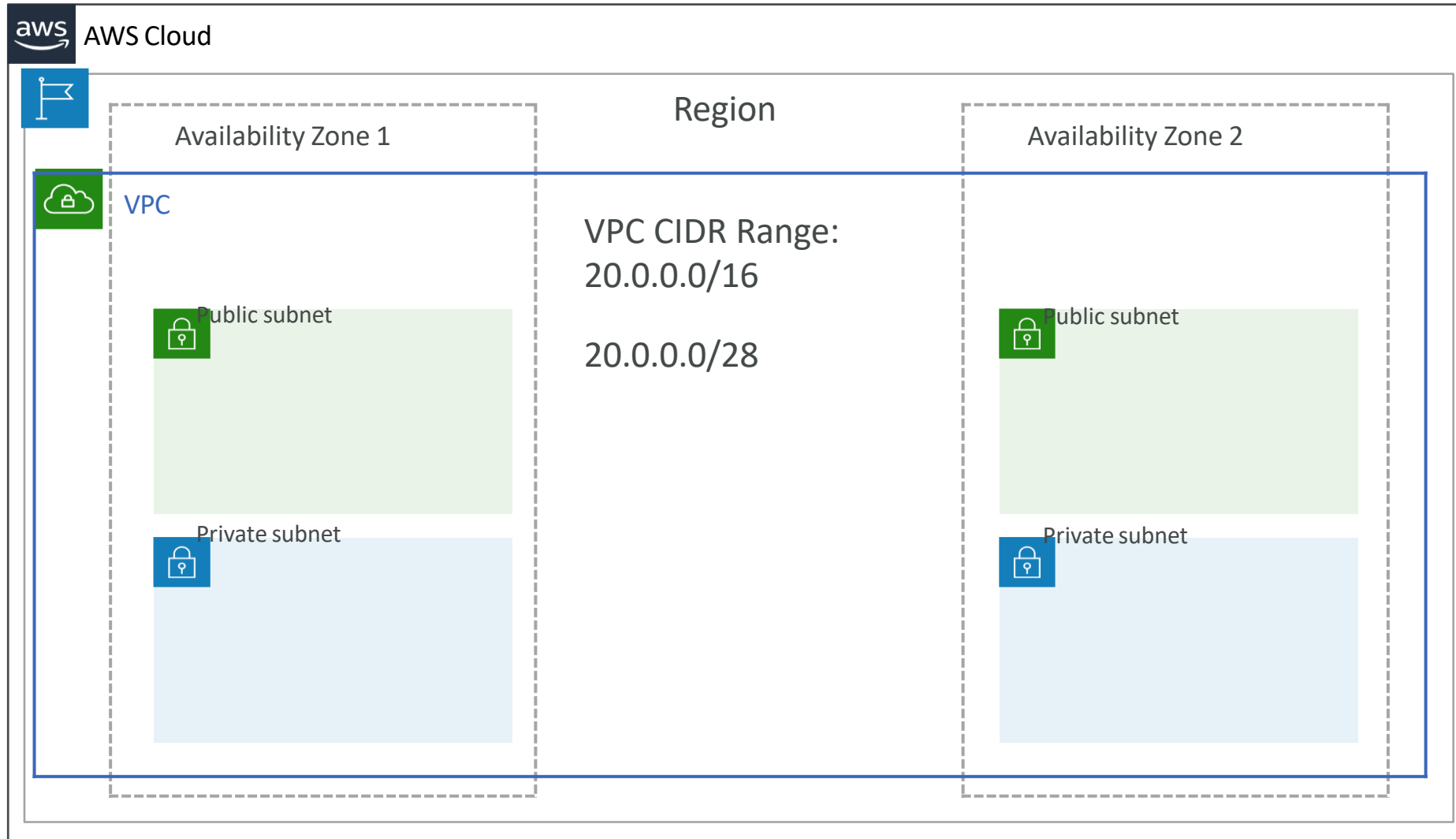
 Public Elastic Load Balancers are accessible from internet (public resources)

 Databases or EC2 instances should NOT be accessible from internet

 ONLY applications within your network (VPC) should be able to access them (private resources)

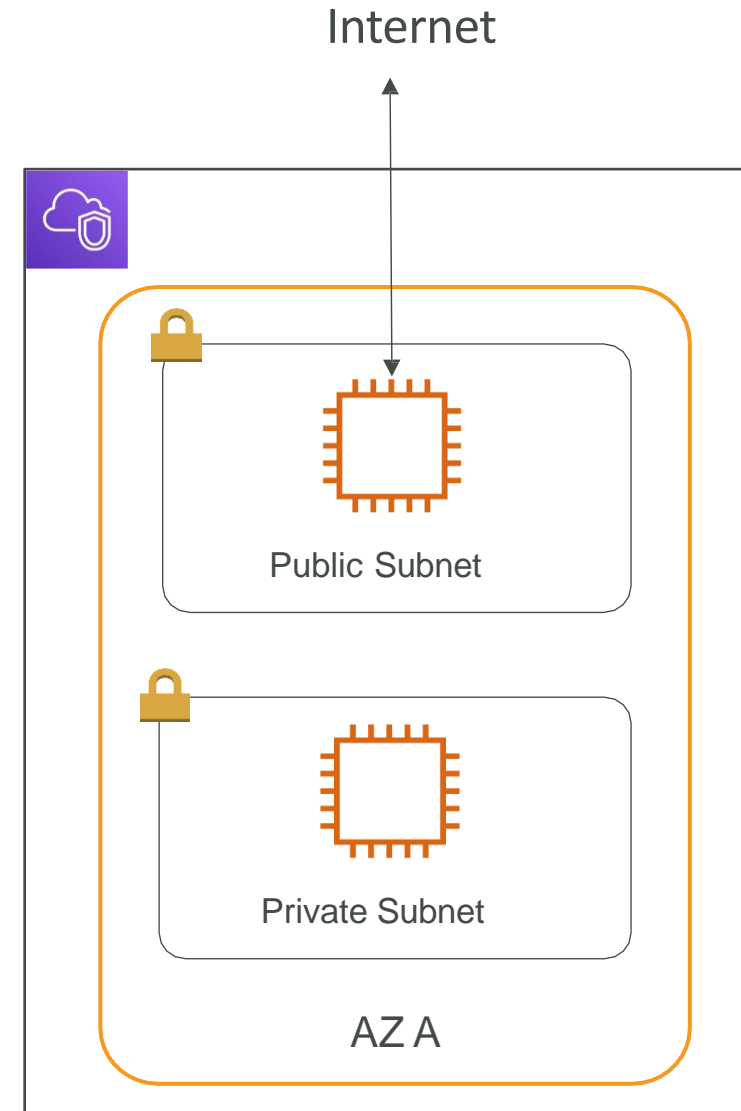
 How do you separate public resources from private resources inside a VPC?

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

Addressing for Resources - IP address

- **Two IP address formats:**
 - IPv4 (Internet Protocol version 4 - numeric 32 bit)
Example : 127.255.255.255
 - IPv6 (Internet Protocol version 6 - alphanumeric 128 bit)
Example : 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 - IPv4 allows a total of 4.3 billion addresses
 - We are running out of the IPv4 address space => IPv6 is introduced as an extension
 - To check the Network address, use the below tool link
 - <https://cidr.xyz/>
-

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

CIDR (Classless Inter-Domain Routing) Blocks - VPC CIDR Blocks

CIDR	Start Range	End Range	Total addresses	Bits selected in IP address
69.208.0.0/24	69.208.0.0	69.208.0.255	256	01000101.11010000.00000000.*****
69.208.0.0/25	69.208.0.0	69.208.0.127	128	01000101.11010000.00000000.0*****
69.208.0.0/26	69.208.0.0	69.208.0.63	64	01000101.11010000.00000000.00*****
69.208.0.0/27	69.208.0.0	69.208.0.31	32	01000101.11010000.00000000.000*****
69.208.0.0/28	69.208.0.0	69.208.0.15	16	01000101.11010000.00000000.0000****
69.208.0.0/29	69.208.0.0	69.208.0.7	8	01000101.11010000.00000000.00000***
69.208.0.0/30	69.208.0.0	69.208.0.3	4	01000101.11010000.00000000.000000**
69.208.0.0/31	69.208.0.0	69.208.0.1	2	01000101.11010000.00000000.0000000*
69.208.0.0/32	69.208.0.0	69.208.0.0	1	01000101.11010000.00000000.00000000

Subnet Calculator tools

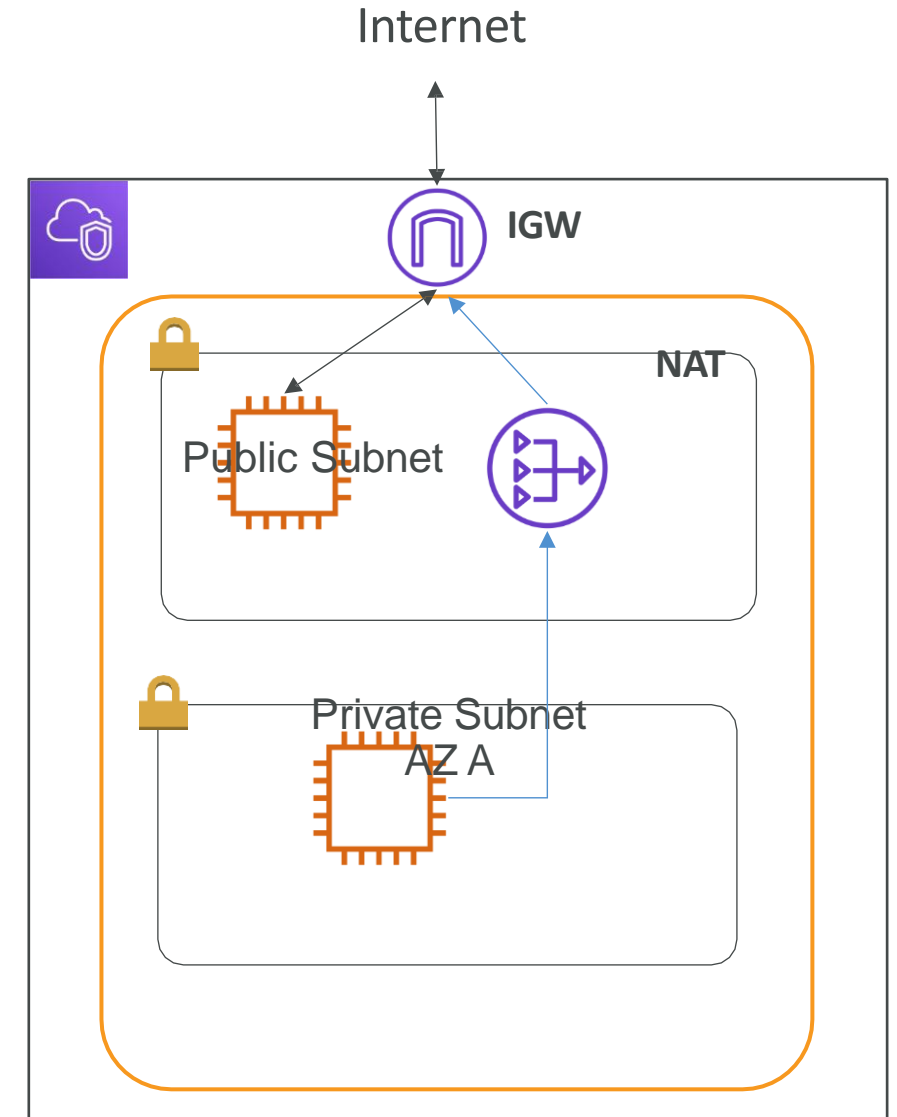
<https://www.davidc.net/sites/default/subnets/subnets.html>

<https://www.site24x7.com/tools/ipv4-subnetcalculator.html>

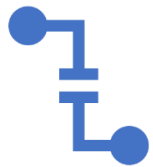
AWS VPC

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



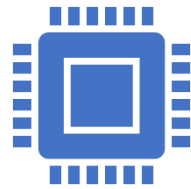
NACL (Network Access control List)

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

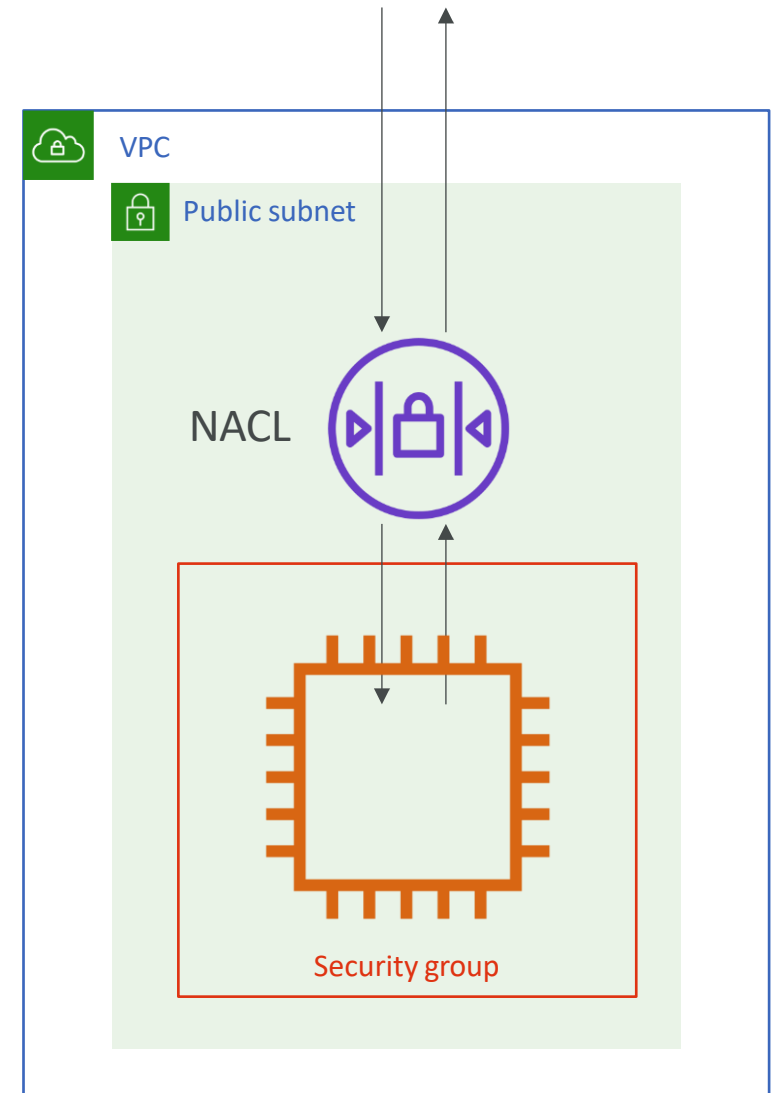


Security Groups

A firewall that controls traffic to and from an EC2 Instance

Can have only ALLOW rules

Rules include IP addresses and other security groups



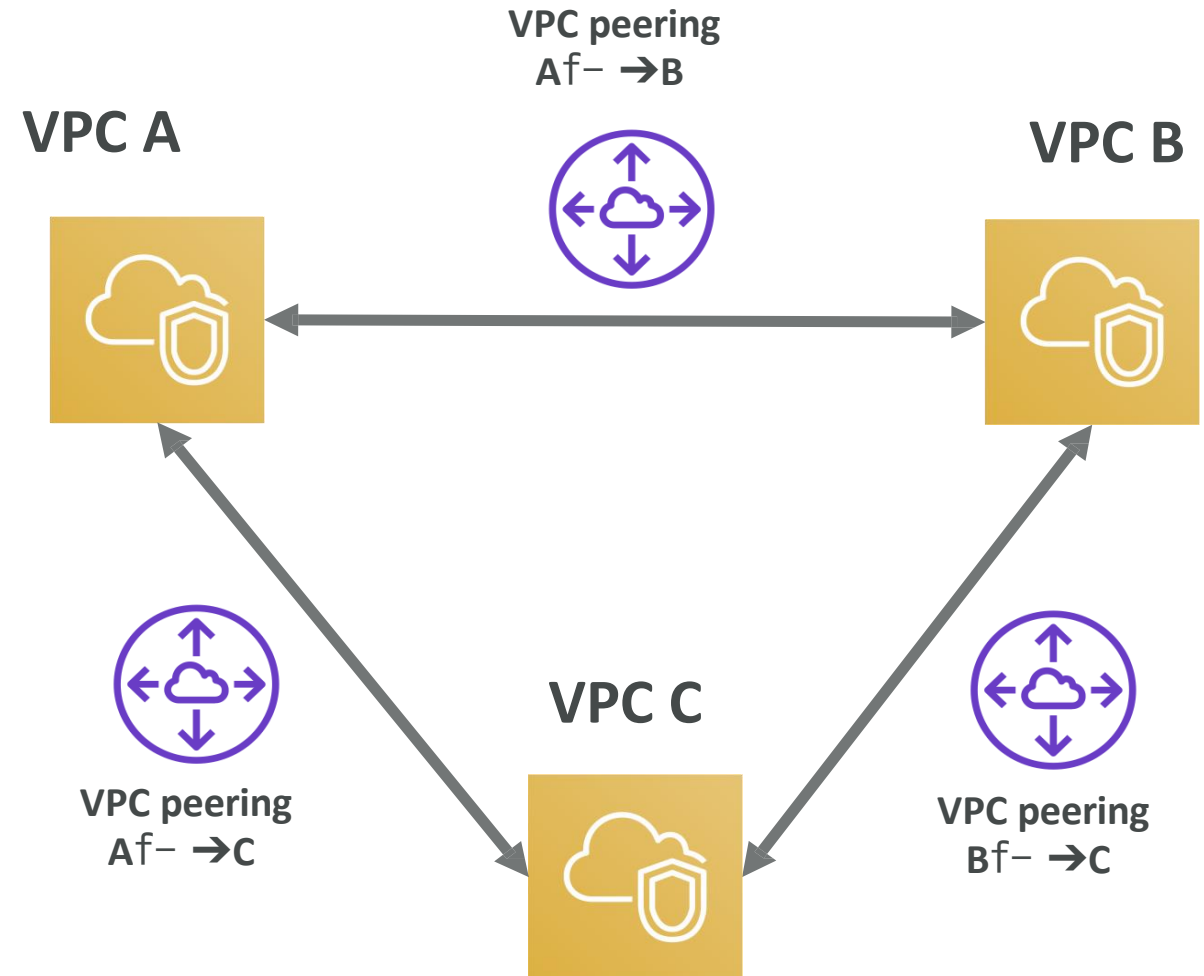
Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group)

AWS VPC Network ACL & 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)



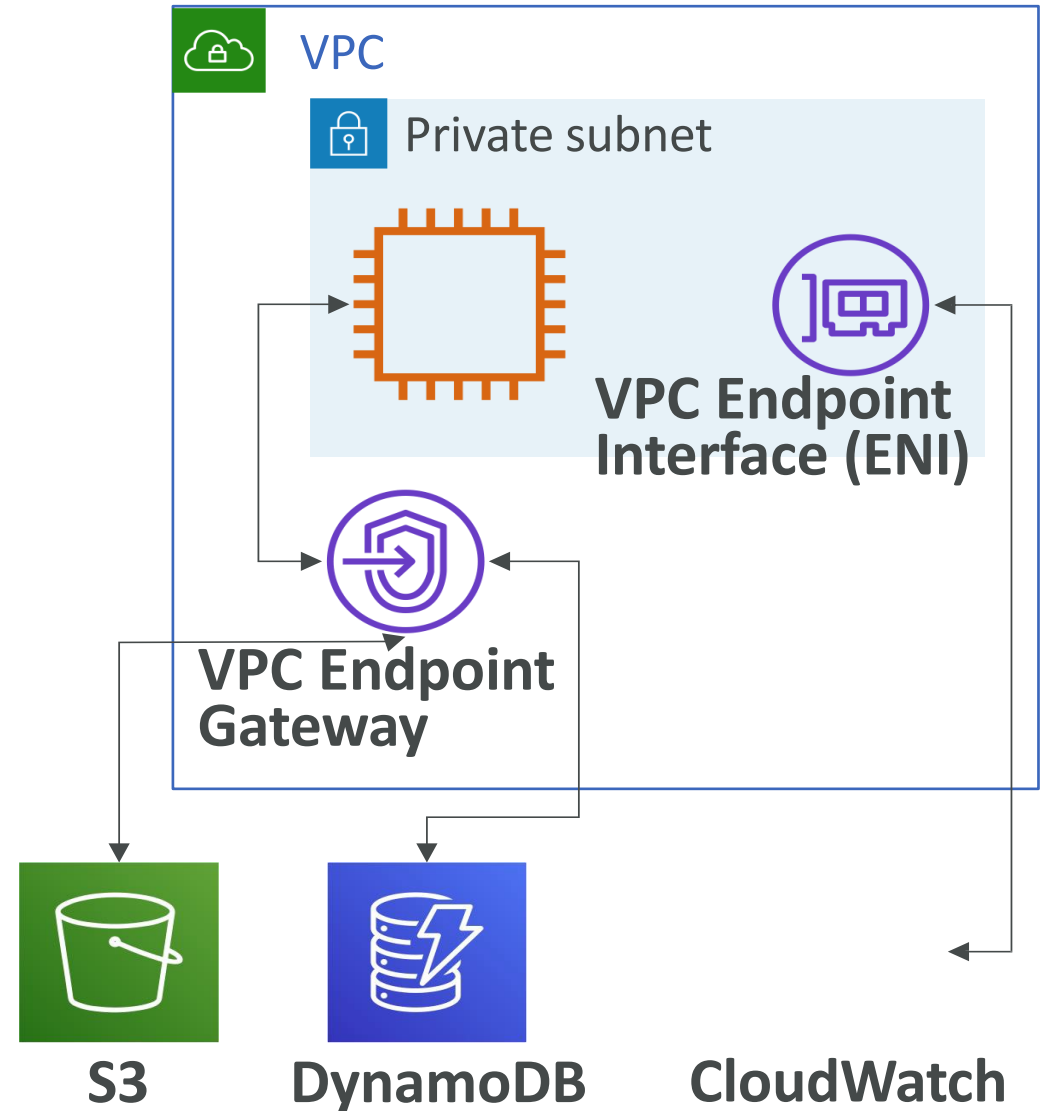
AWS VPC

- 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

VPC Endpoint Gateway: S3 & DynamoDB

VPC Endpoint Interface: the rest

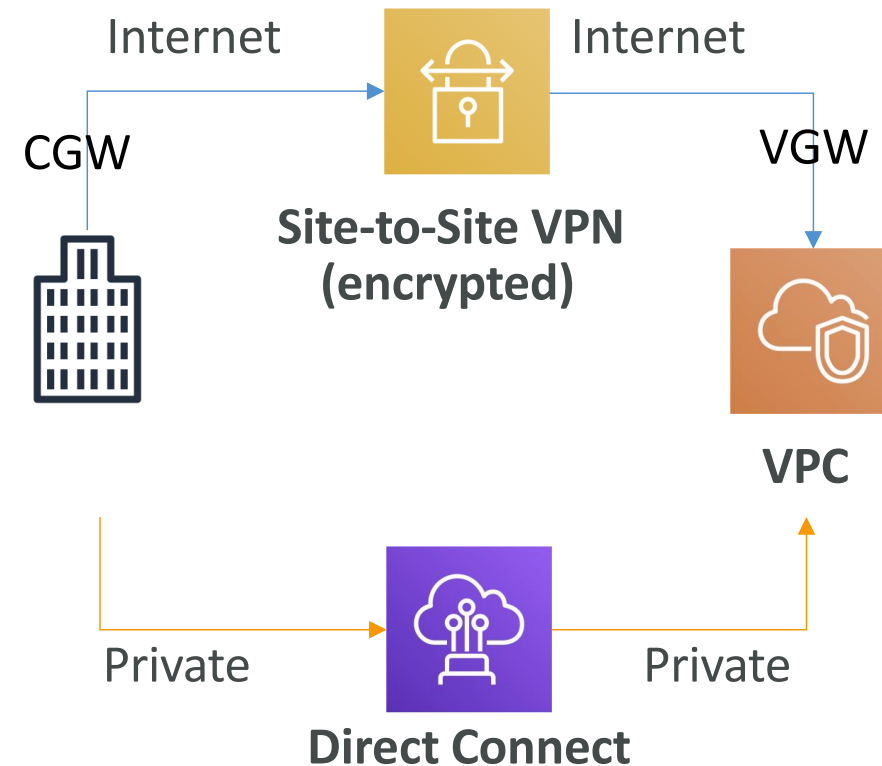


AWS VPC

- Site to Site VPN & Direct Connect

- Site to Site VPN
 - Connect an on-premises VPN to AWS
 - The connection is automatically encrypted
 - Goes over the public internet

On-premises: must use a Customer Gateway (CGW)
AWS: must use a Virtual Private Gateway (VGW)
- Direct Connect (DX)
 - Establish a physical connection between on-premises and AWS
 - The connection is private, secure and fast
 - Goes over a private network
 - Takes at least a month to establish

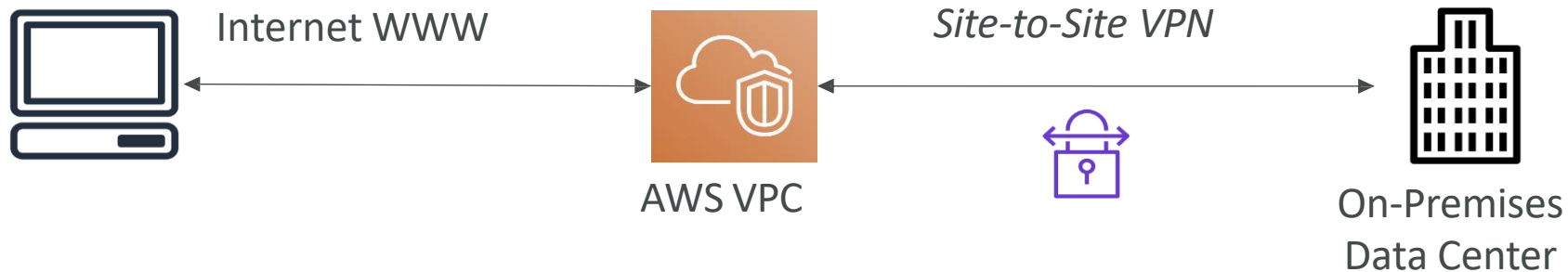


AWS VPC

- 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

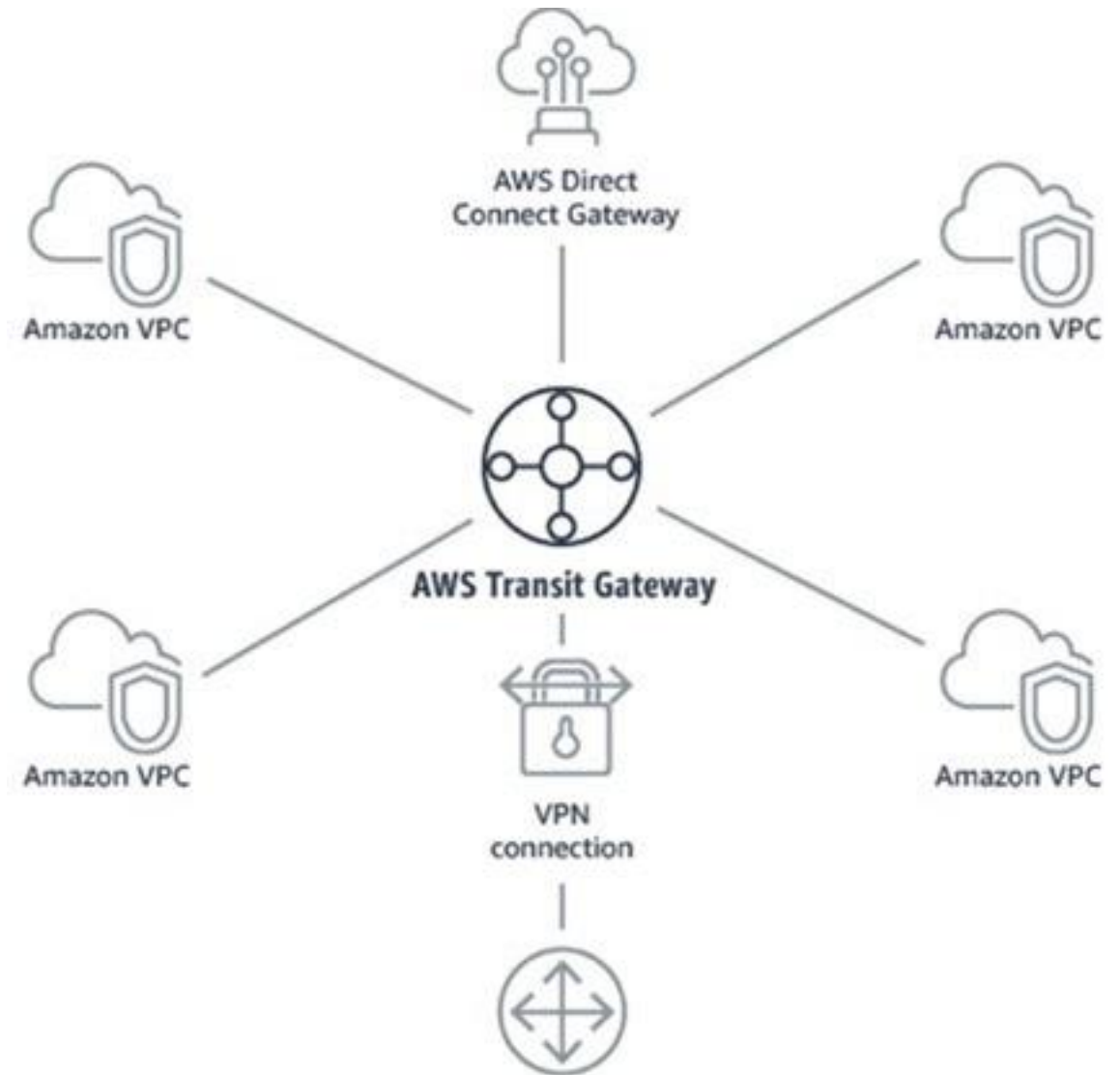
Computer with
AWS Client VPN (OpenVPN)



AWS VPC

- Transit Gateway

- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- One single Gateway to provide this functionality
- Works with Direct Connect Gateway, VPN connections



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