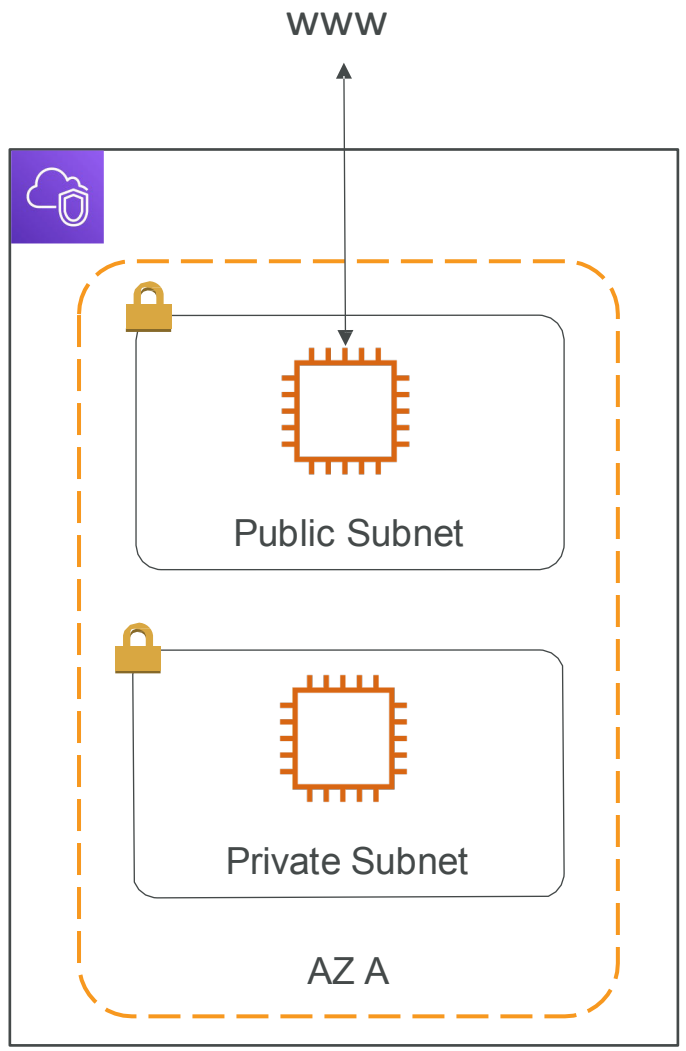
VPC Section

VPC

- Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network
- You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

Subnets

- 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.
- A route table contains a set of rules, called routes, that determine where network traffic from your subnet or gateway is directed.



CIDR

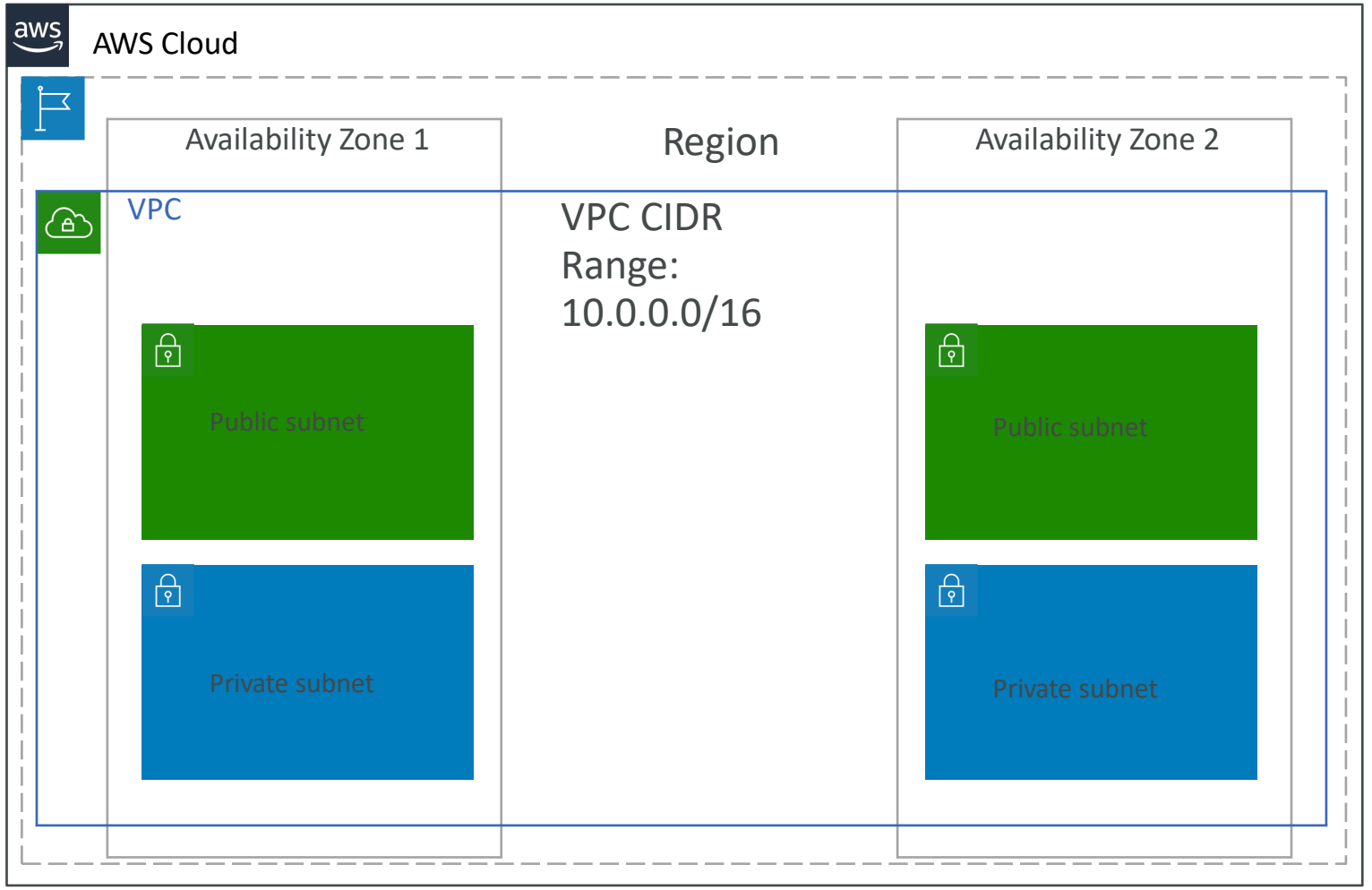
- Classless Inter-Domain Routing is a method for allocating IP addresses

  Ex: The IPv4 block 192.168.100.0/22 represents the 1024 IPv4 addresses
  from 192.168.100.0 to 192.168.103.255.
  I.e. 2^ (32-22) = 2^10 = 1024 IPv4 addresses.

- The first four IP addresses and the last IP address in each subnet CIDR block are not available to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

  1. 10.0.0.0: Network address.
  2. 10.0.0.1: Reserved by AWS for the VPC router.
  3. 10.0.0.2: Reserved by AWS for mapping to the Amazon-provided DNS.
  4. 10.0.0.3: Reserved by AWS for future use.
  5. 10.0.0.255: Network broadcast address.

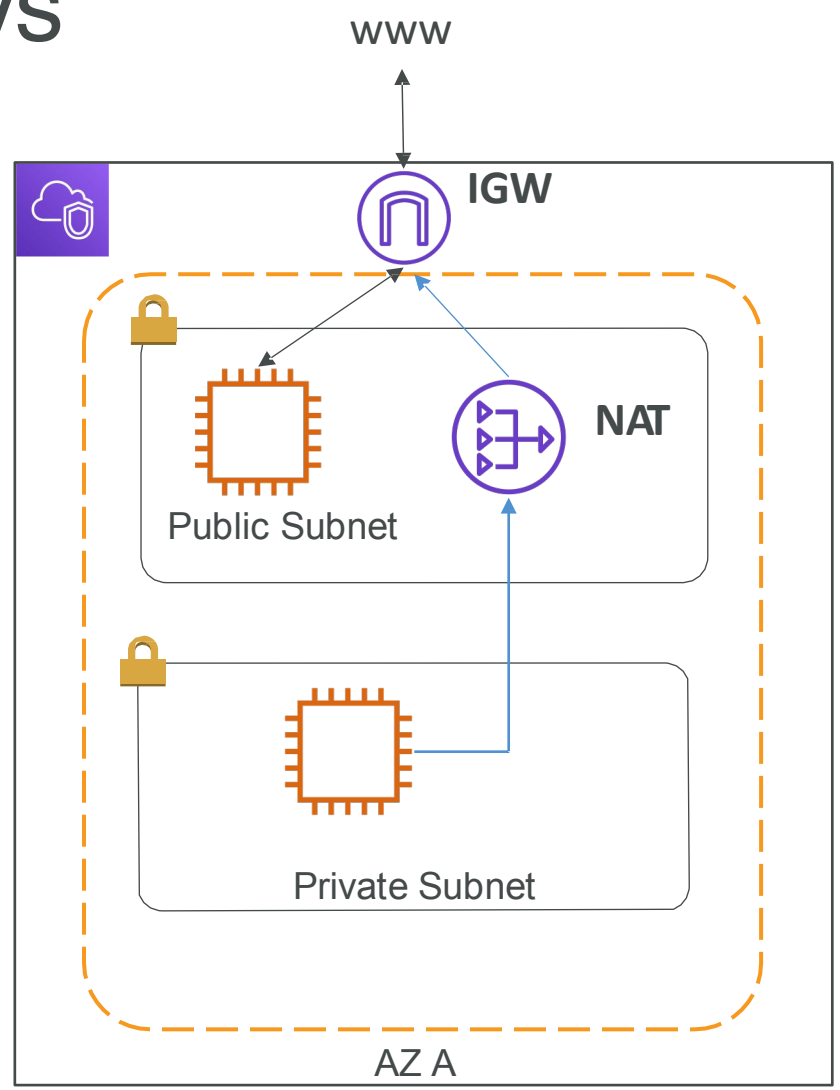
VPC Diagram


aws
AWS Cloud
Availability Zone 1
Region
Availability Zone 2
VPC
VPC CIDR
Range:
10.0.0.0/16
Public subnet
Private subnet
Public subnet
Private subnet

Internet Gateway & NAT Gateways

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

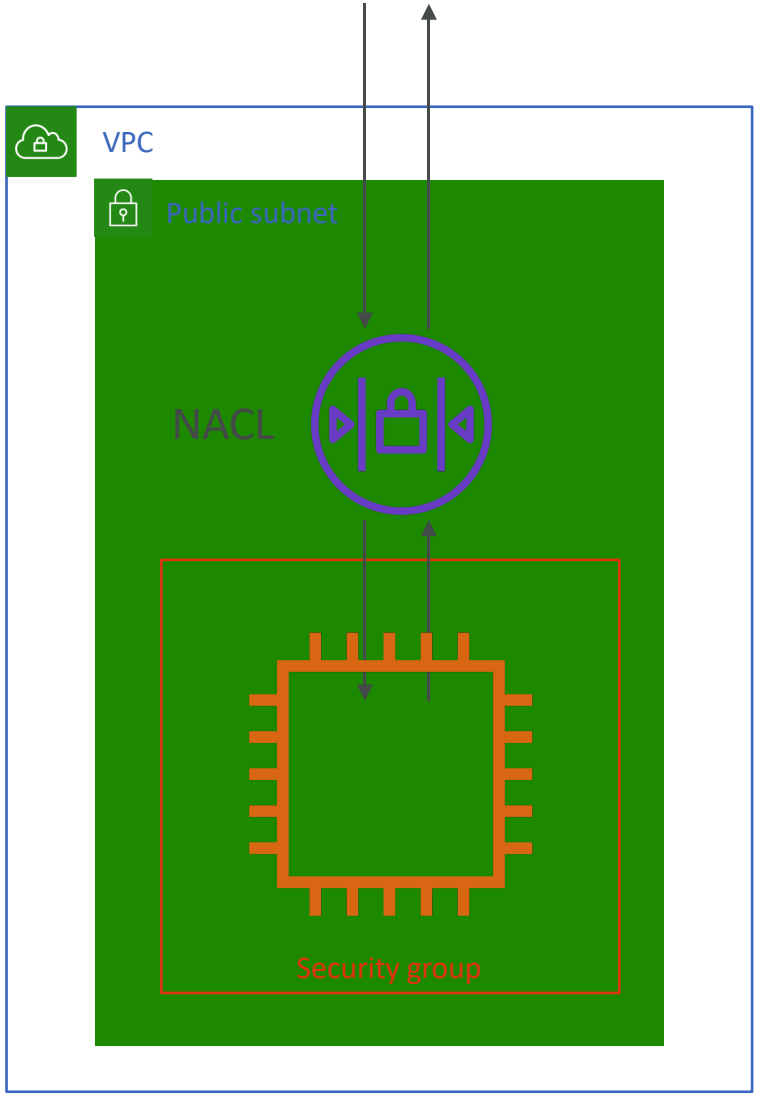
- NAT Gateways (AWS-managed) & NAT Instances (self-managed) allow your instances in your Private Subnets to access the internet while remaining private



Network ACL & Security Groups

- NACL (Network ACL)
  - A virtual firewall at subnet level
  - Can have ALLOW and DENY rules
  - Rules only include IP addresses

- Security Groups
  - A virtual firewall at instance level
  - Can have only ALLOW rules
  - Rules include IP addresses and other security groups



Network ACLs vs 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)

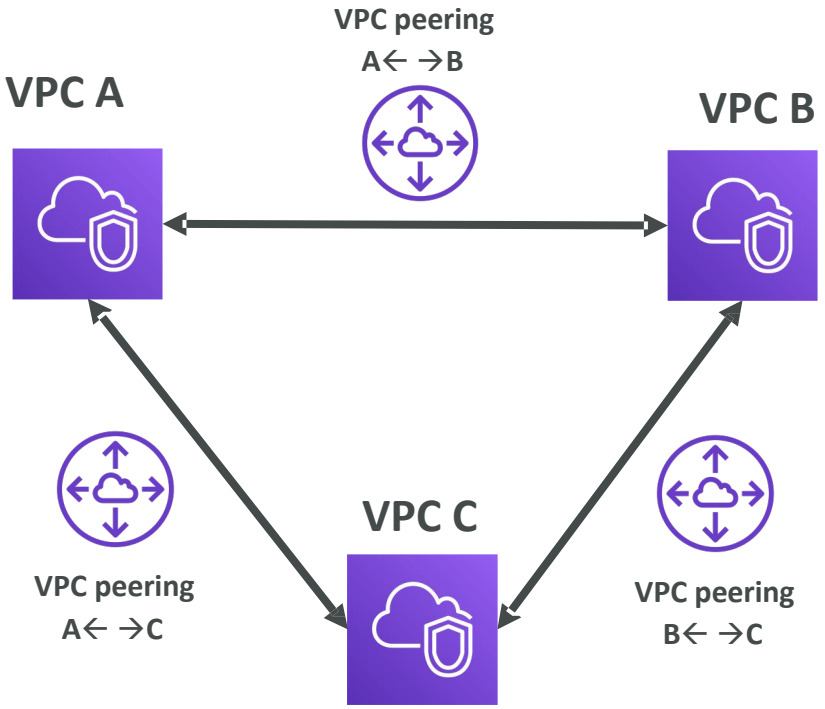
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison

VPC Flow Logs

- Capture information about IP traffic going into your interfaces:
  - VPC Flow Logs
  - Subnet Flow Logs
  - Elastic Network Interface Flow Logs
- Helps to monitor & troubleshoot connectivity issues. Example:
  - Subnets to internet
  - Subnets to subnets
  - Internet to subnets
- Captures network information from AWS managed interfaces too: Elastic Load Balancers, ElasticCache, RDS, Aurora, etc...
- VPC Flow logs data can go to S3 / CloudWatch Logs

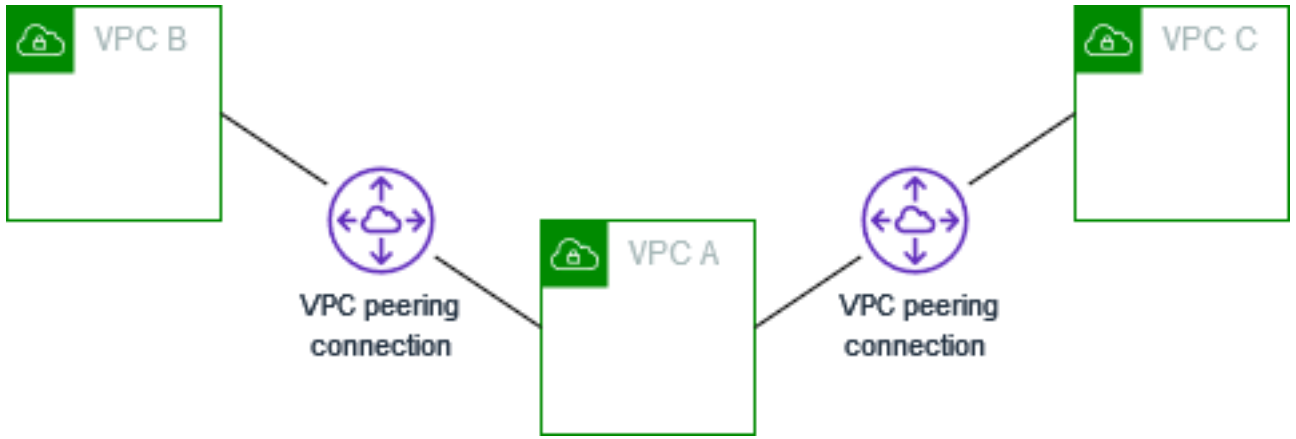
VPC Peering

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
- Instances in either VPC can communicate with each other as if they are within the same network.
- You can create a VPC peering connection between your own VPCs, or with a VPC in
- another AWS account.
- The VPCs can be in different regions (also known as an inter-region VPC peering connection).



VPC Peering Conditions

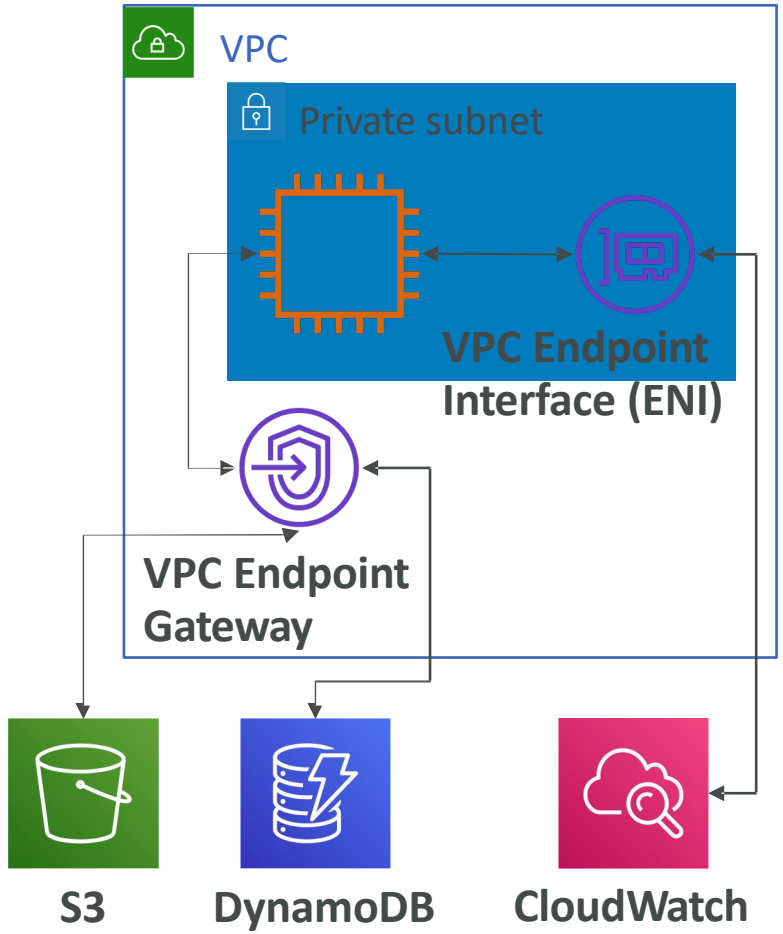
- CIDR blocks shouldn’t overlap
- Transitive peering relationships are not supported. i.e In the image VPC B Does not have connection with VPC C
- If the VPCs are in different regions, inter-region data transfer costs apply.
- You cannot have more than one VPC peering connection between the same two VPCs at the same time.



VPC Endpoints

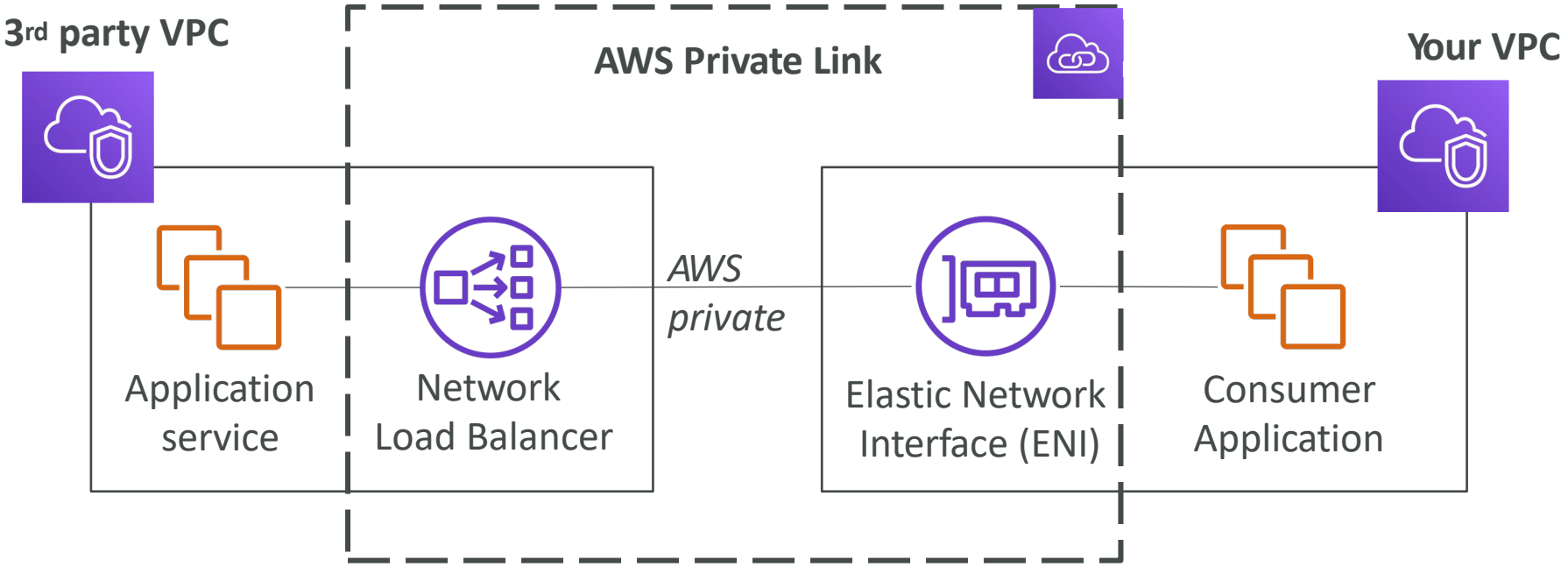
- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- This gives you enhanced security and lower latency to access AWS services

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



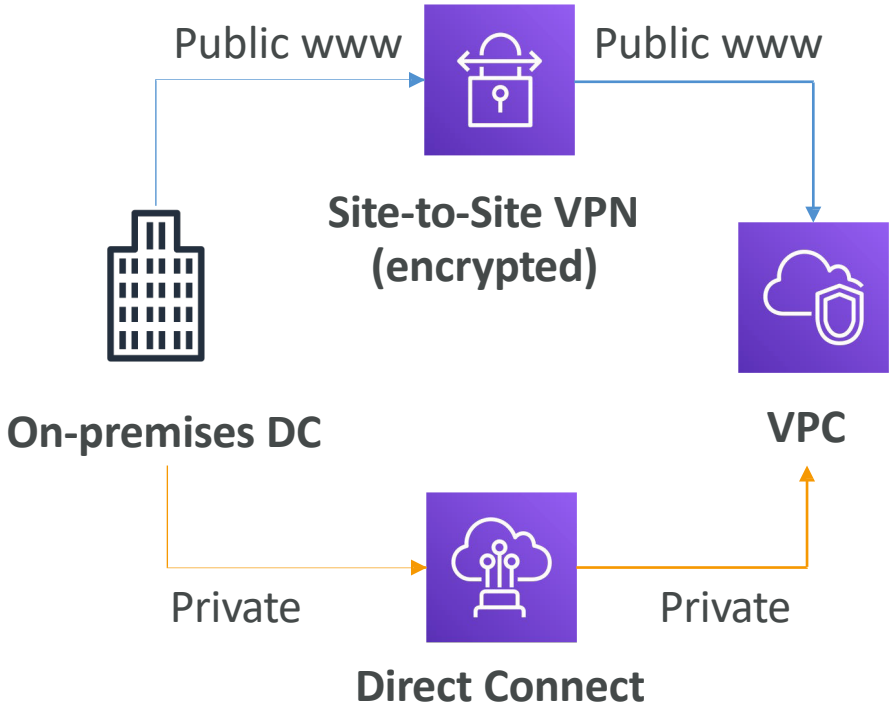
AWS PrivateLink (VPC Endpoint Services)

- Most secure & scalable way to expose a service to 1000s of VPCs
- Does not require VPC peering, internet gateway, NAT, route tables…
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)



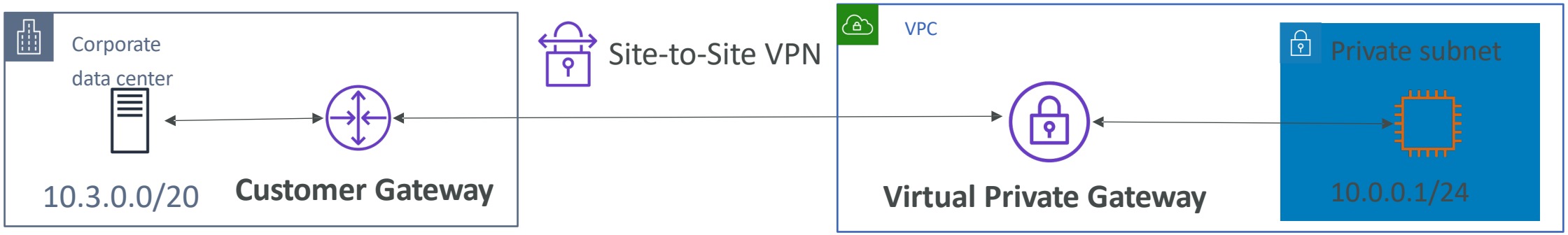
Site to Site VPN & Direct Connect

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



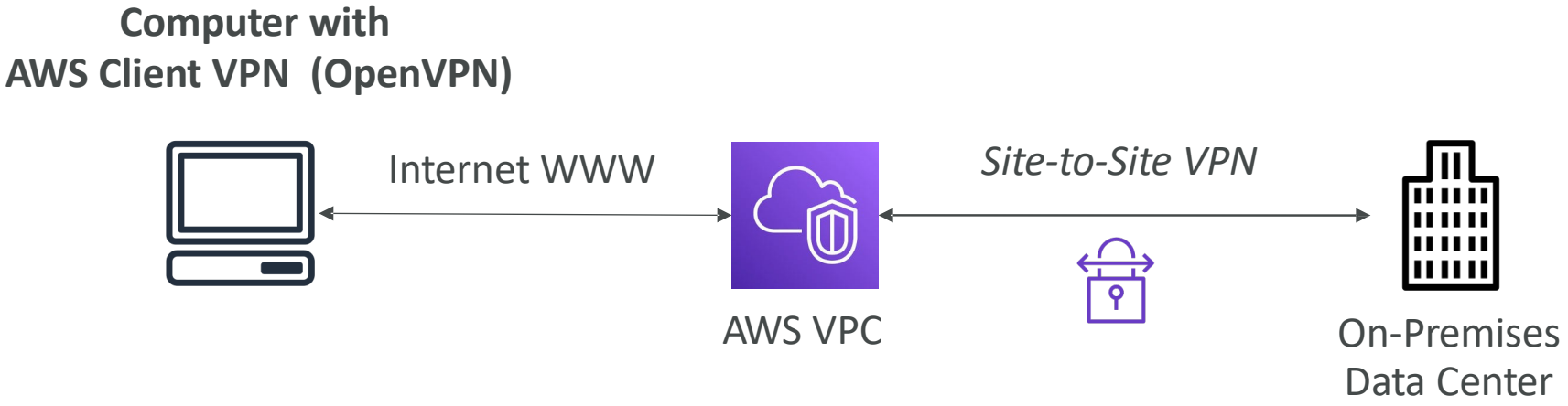
Site-to-Site VPN

- On-premises: must use a Customer Gateway (CGW)
- AWS: must use a Virtual Private Gateway (VGW)

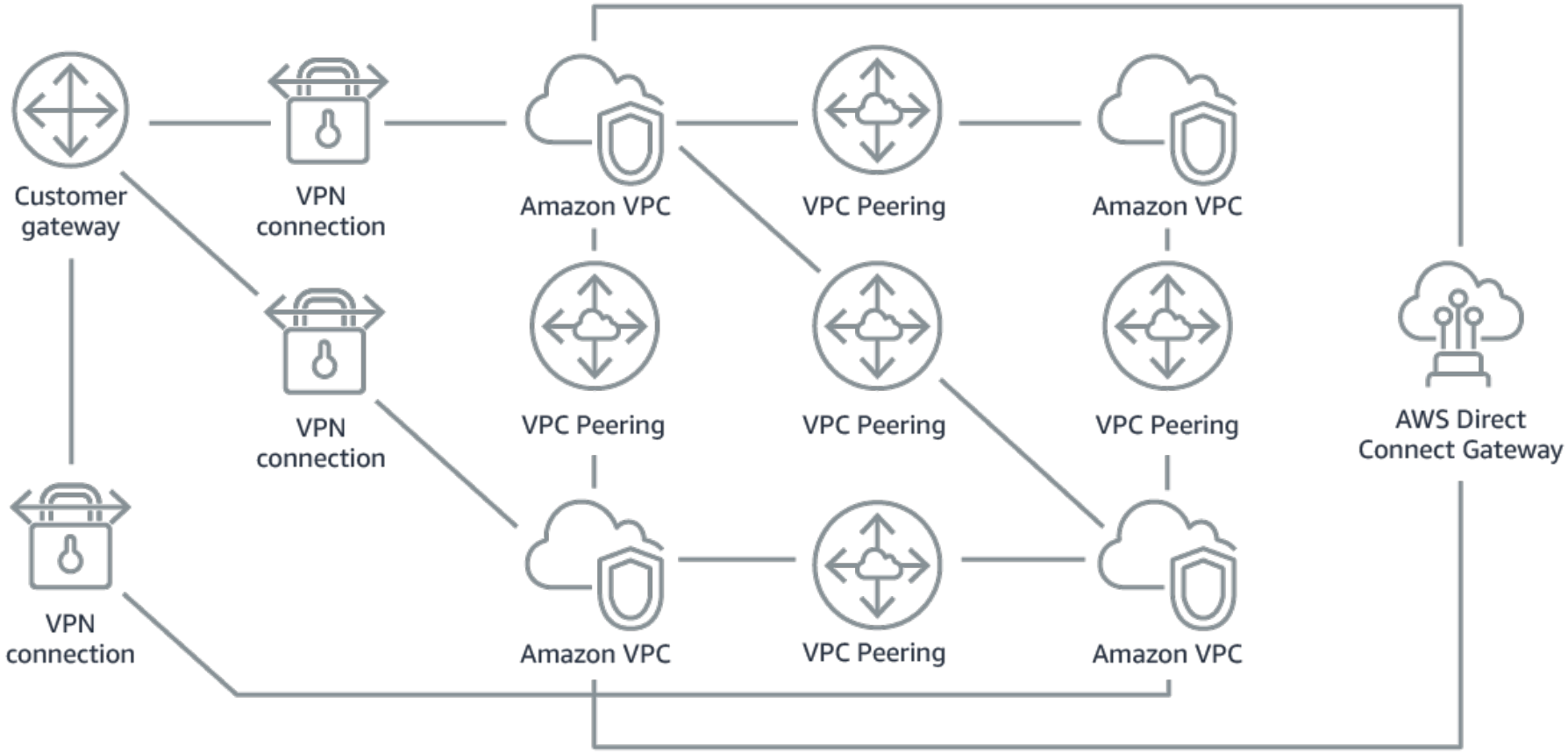


AWS Client VPN

- 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

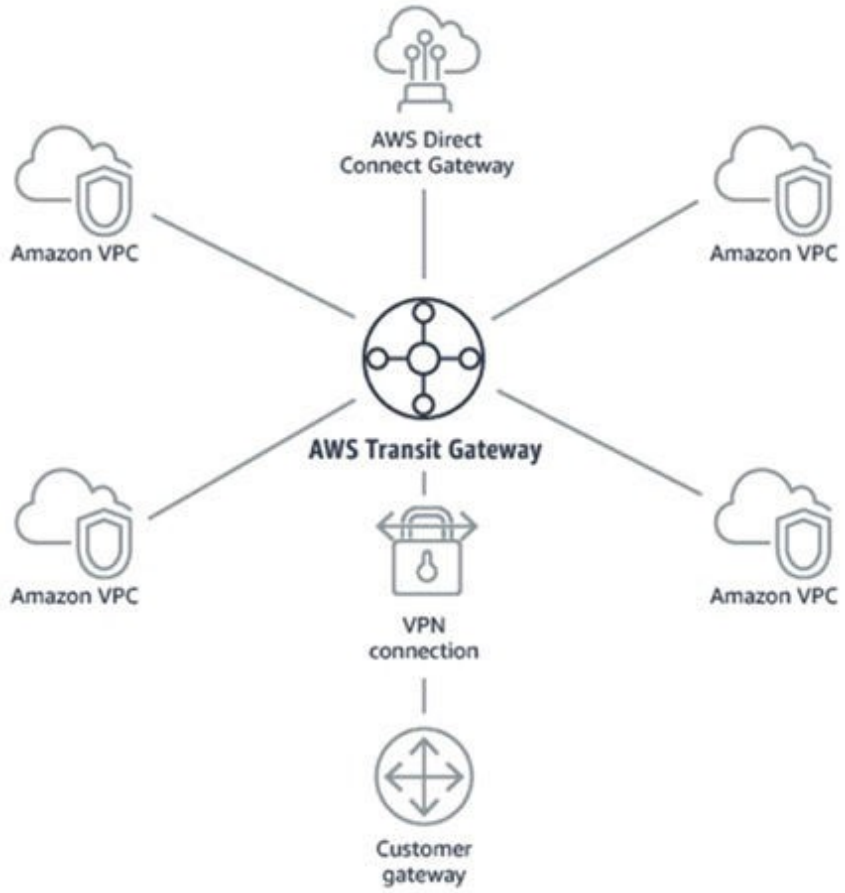


Network topologies can become complicated



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



VPC Quota or VPC limitations

- **5** VPC per region
- **5** IGW per region
- Subnet per VPC **200**
- IPv4 CIDR blocks per VPC **4**
- Elastic IP addresses per Region **5**
- Internet gateways per Region **5**
- NAT gateways per Availability Zone **5**
- Network ACLs per VPC **200**
- Rules per network ACL **200**

VPC Closing Comments

- 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

VPC Closing Comments

- VPC Endpoints: Provide private access to AWS Services within VPC
- PrivateLink: Privately connect to a service in a 3rd party VPC
- VPC Flow Logs: network traffic logs
- Site to Site VPN: VPN over public internet between on-premises DC and AWS
- Client VPN: OpenVPN connection from your computer into your VPC
- Direct Connect: direct private connection to AWS
- Transit Gateway: Connect thousands of VPC and on-premises networks together