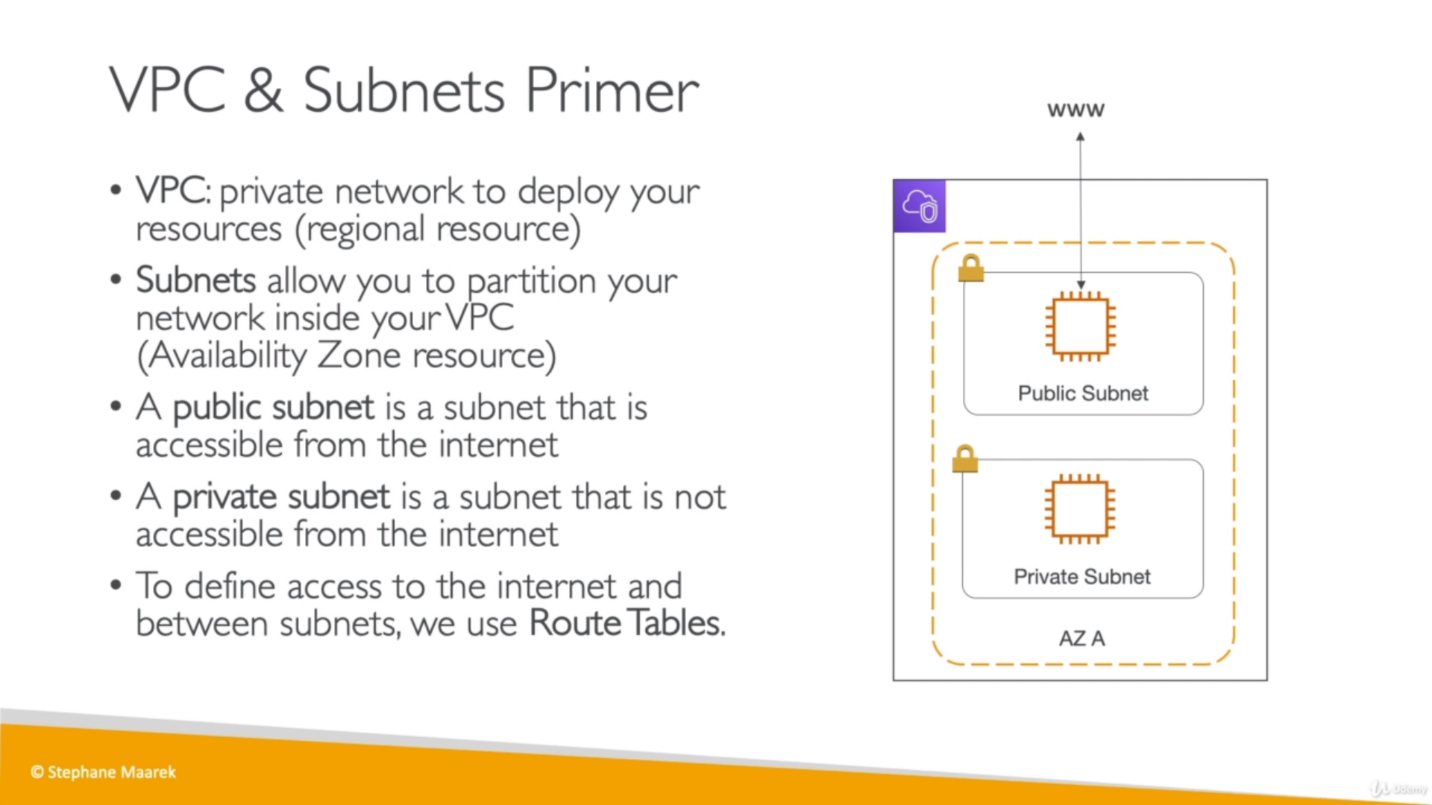
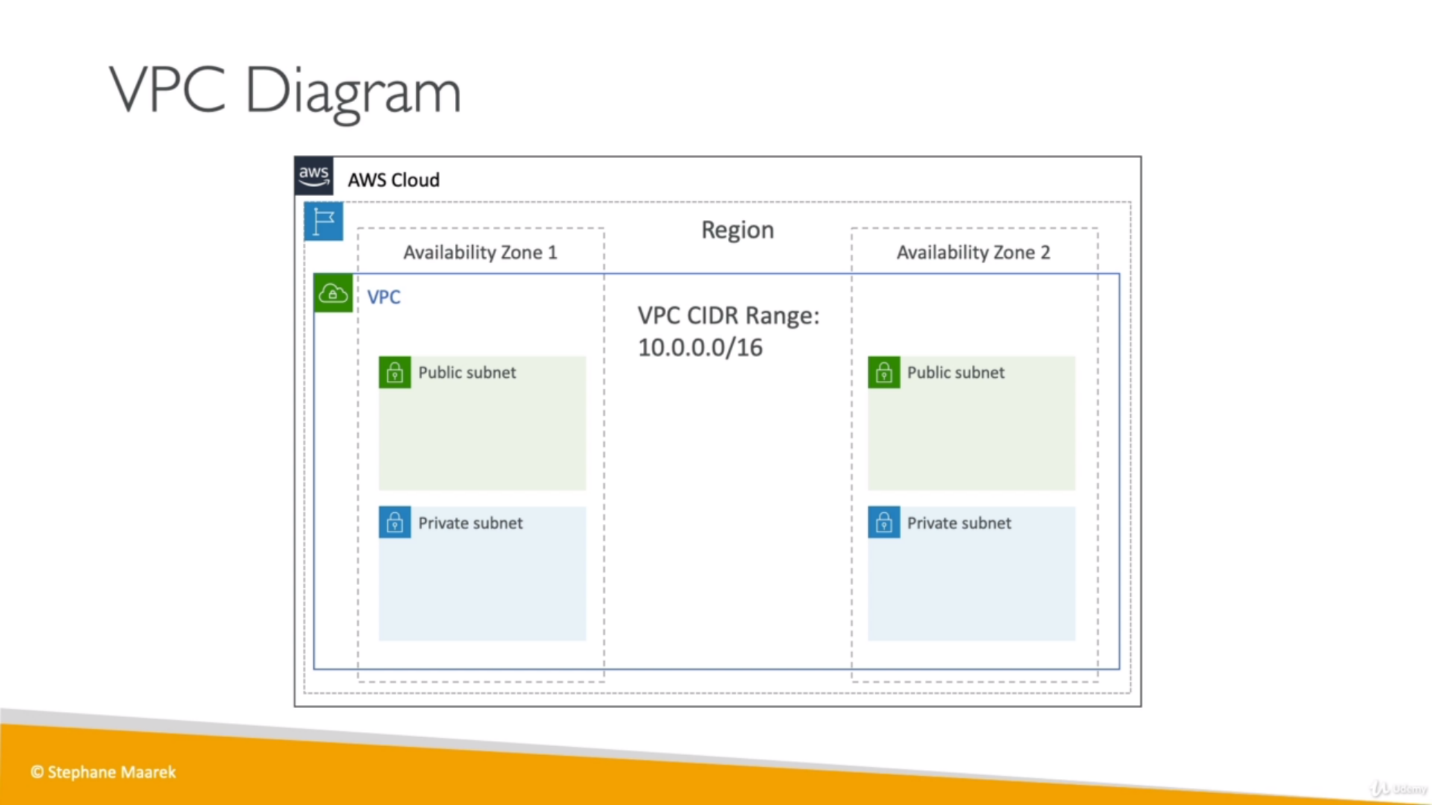
**VPC and Subnet**

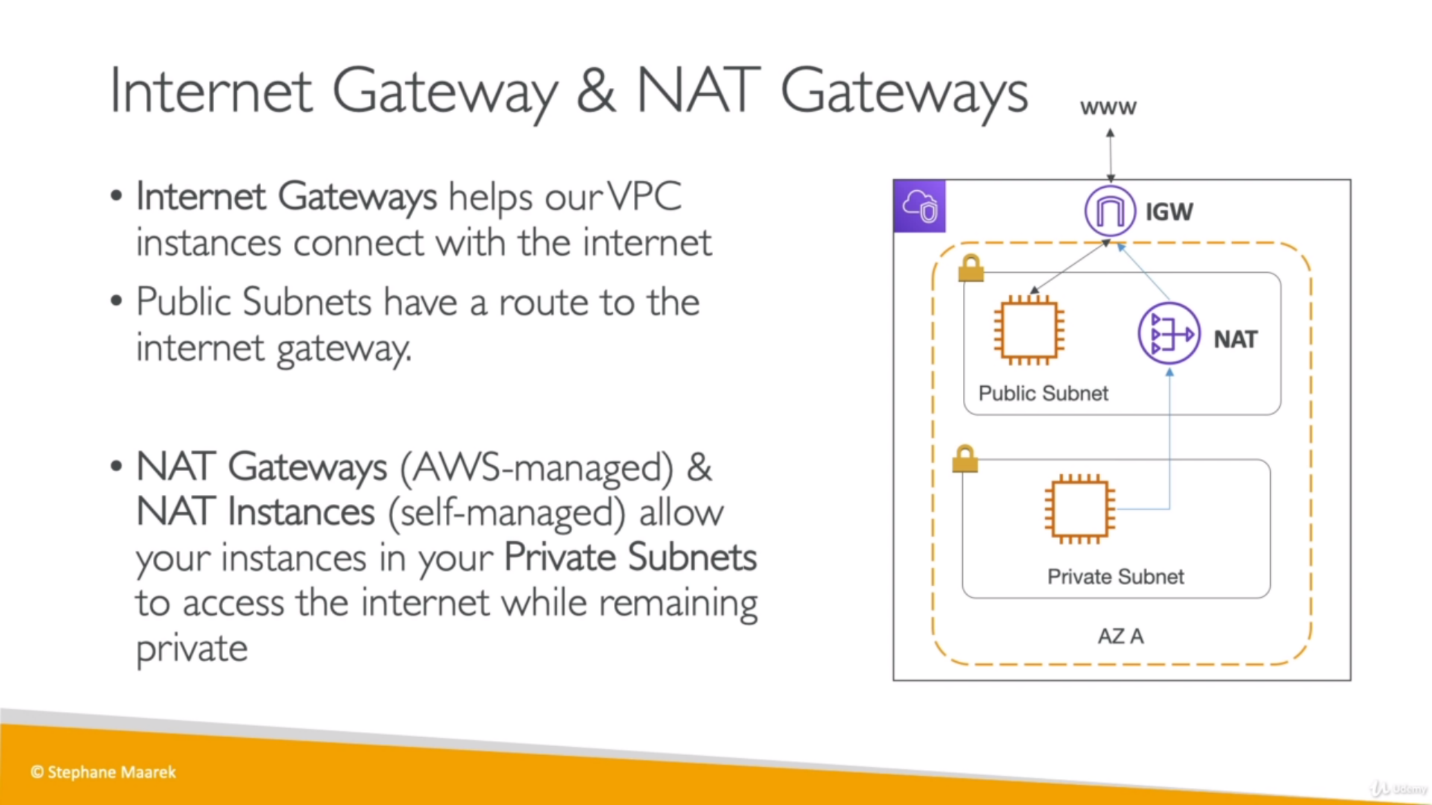
**Topics: VPC, Subnet, Internet and NAT gateway, NACL, Flow logs, Peering, Endpoints, Site to Site VPN, Direct Connect(DX)**

**Virtual Private Cloud :** it is based on region. One default VPC per region in AWS. Region will have multiple AZs and there can be multiple private/public subnet per AZ.





**Internet and NAT (network address translation) Gateways:**

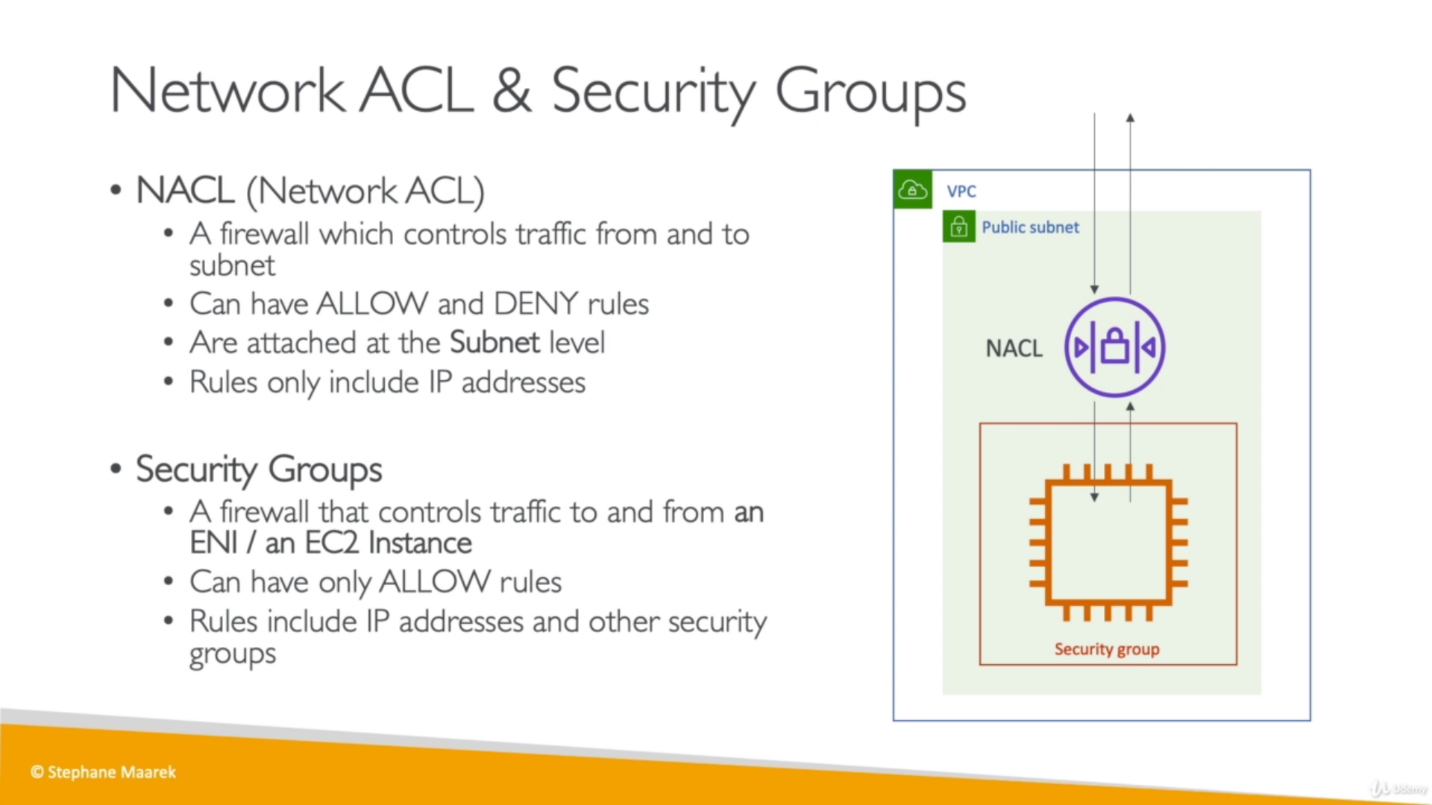


Private subnet instance + NAT G + Internet G = connect with Internet

Public subnet instance + Internet G = connect with Internet

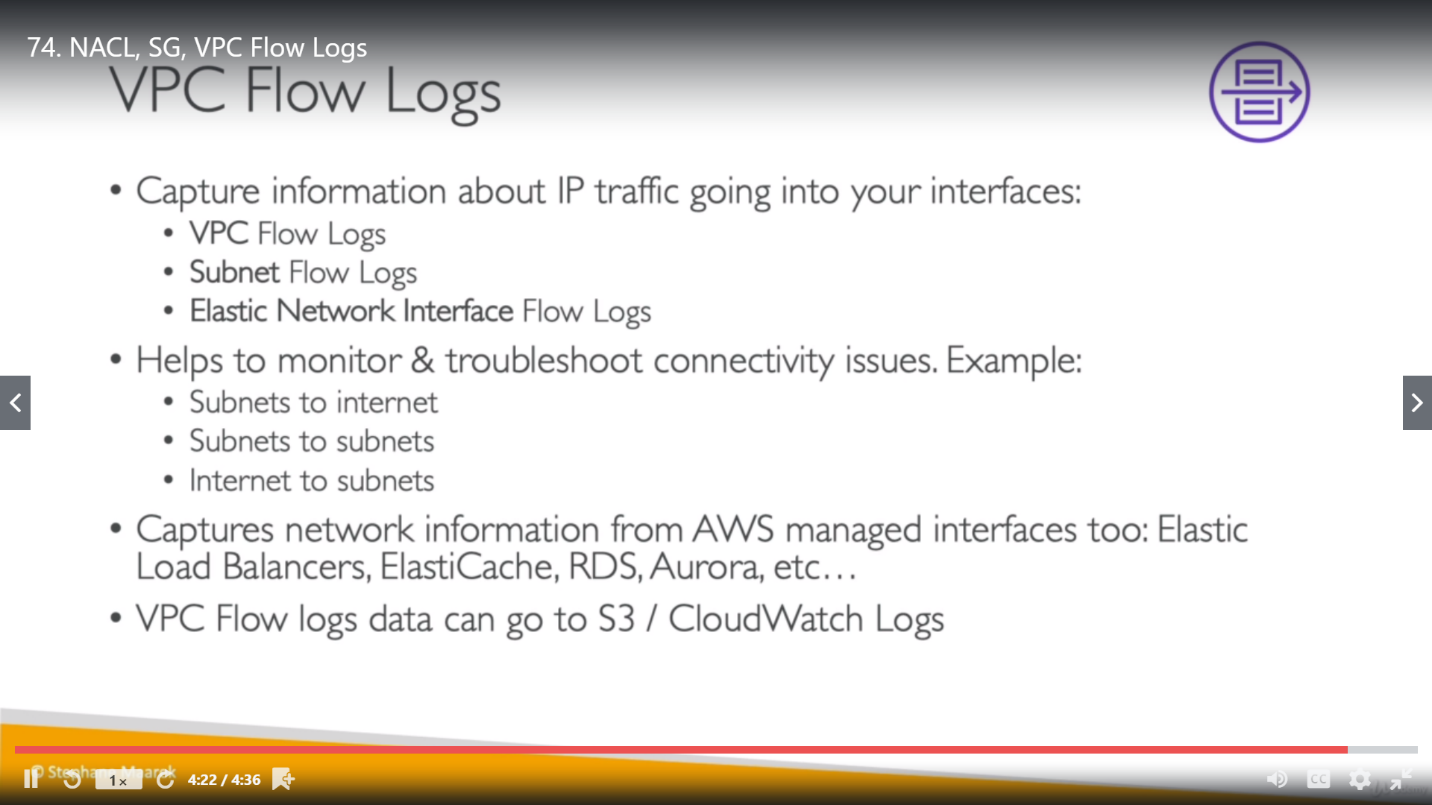
**NACL (Network Access Control List) and security group:**

A **network** access control list (**ACL**) is an optional layer of security for our VPC that acts as a firewall for controlling traffic in and out of one or more subnets based on IP addresses based rules.



Below table not need to remember:





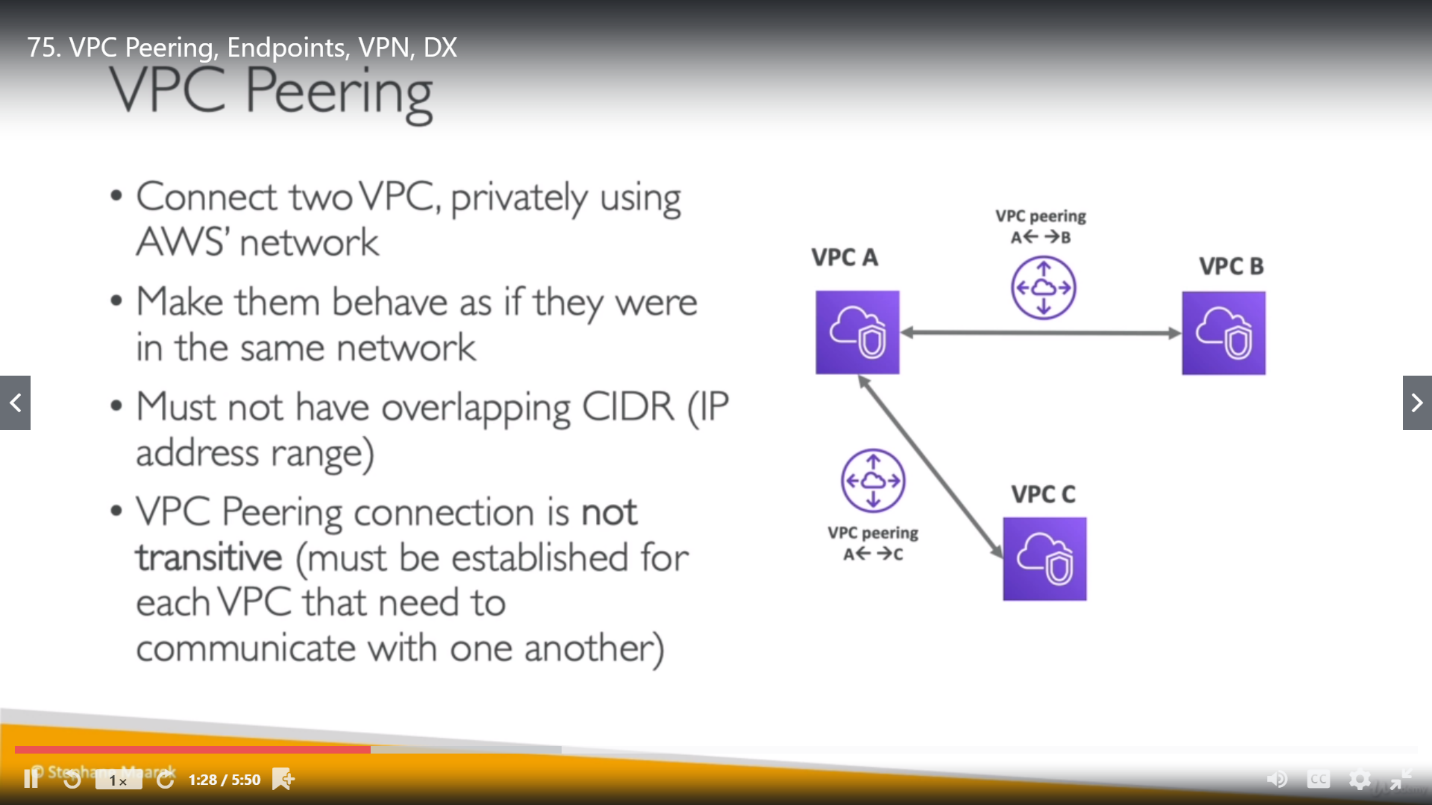
**VPC Peering:**

[Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/userguide/) (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

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).

IP ranges defined for each VPC should not be overlapped that mean both VPC should not have instance with same IP.

If VPC A have connection with VPC B and VPC C, then VPC B and VPC C can’t talk to each other.



**VPC Endpoints:**

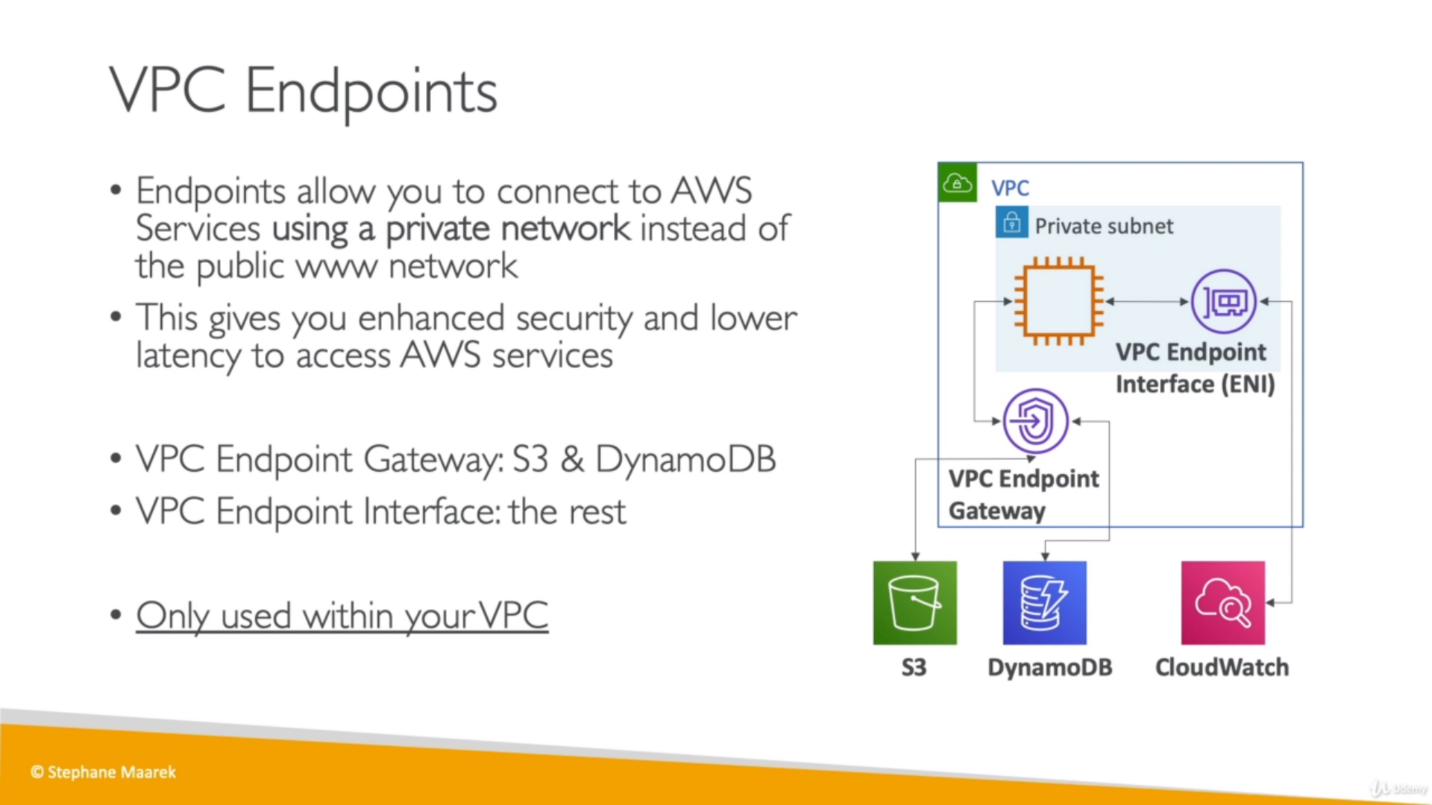
VPC Endpoint are useful whenever we need to access an AWS services from VPC instances (both are locally for AWS, there is no connection with outside world/internet). Instances in our VPC do not require public IP addresses to communicate with resources in the service. Traffic between our VPC and the other service does not leave the Amazon network. Endpoints are virtual devices. There are two types of VPC endpoints**: *interface endpoints***and***gateway endpoints*.**

**An**[**interface endpoint**](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html) is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service.

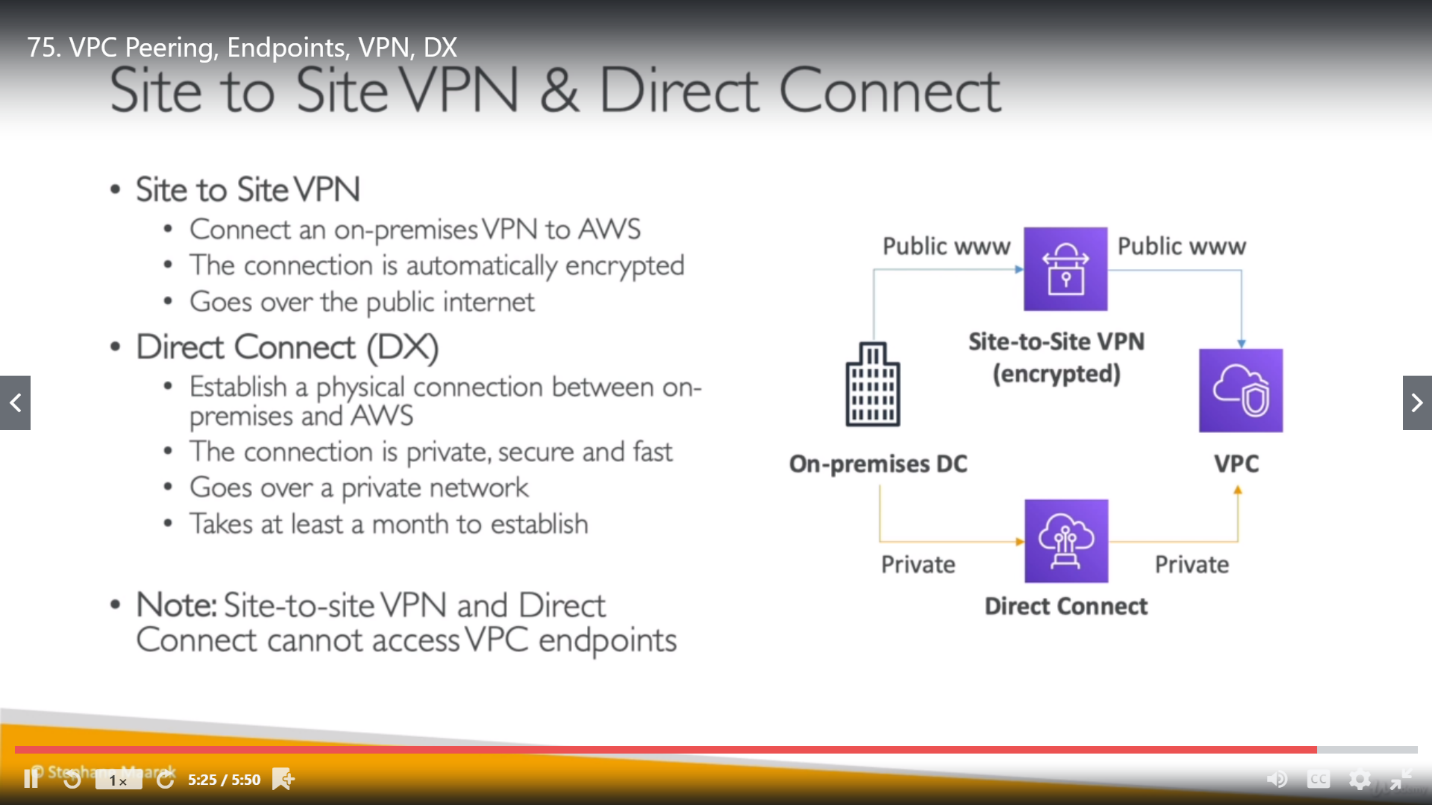
Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses. It supports a lot of services as EC2, CloudWatch etc. (In simple language, our VPC EC2 instance can communicate to any AWS service except S3 and DynamoDB using Interface endpoint)

We know **Route Table** is used to connect VPC subnet with Internet. **A**[**gateway endpoint**](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html) is a gateway that we specify as a target for a route in our route table for traffic destined to a supported AWS service. The following AWS services are supported:

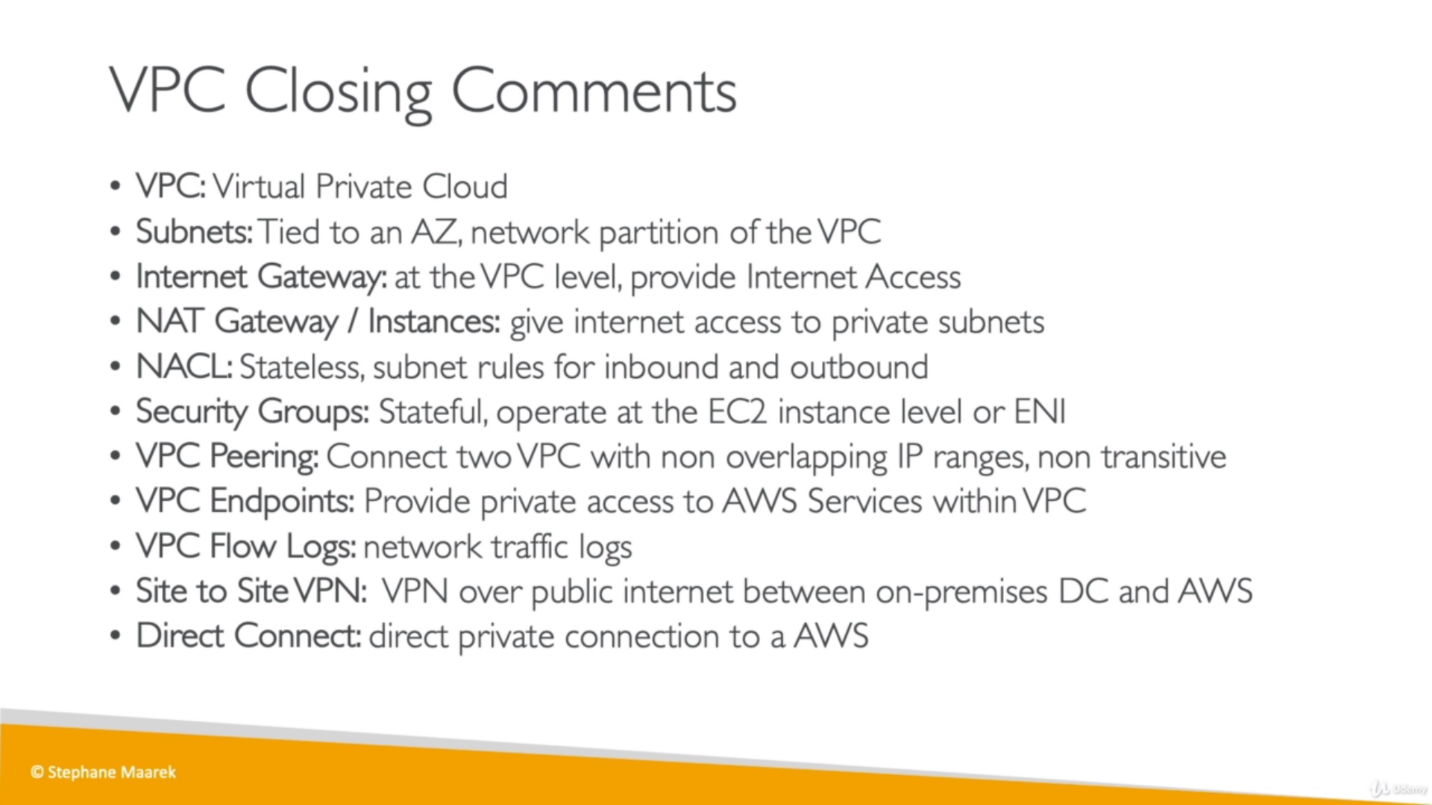
* Amazon S3
* DynamoDB



**Site to Site VPN and Direct Connect(DX):** These two concepts are used to connect on premises VPN with VPC. Site to Site is public connection other side DX is private.



VPC endpoints are for connecting VPC instances with other AWS services and above two (Side to Side VPN and Direct connect) are methods to connect our VPN with VPC.



**3 tier architecture**

