AWS PrivateLink

It was mentioned in a previous section that there are two different types of VPC endpoints: **Gateway VPC Endpoints** and **Interface VPC Endpoints**. Since we have already spent a section discussing Gateway VPC Endpoints, I find it to be worth spending a section discussing the other type of VPC endpoint too.

Now, the main differentiator that we can use to distinguish between Interface VPC Endpoints and Gateway VPC Endpoints are its use of AWS PrivateLink and the range of services covered by it. Let us start with the second one because it is in my opinion, the more important one. Unlike Gateway VPC Endpoints which are limited to the S3 and DynamoDB services, Interface VPC Endpoints allow us to create a private and secure connection with any publicly available AWS service (well technically, any service that supports PrivateLink, which is almost all of them) like EC2, ECS, RDS and all the others that we have discussed in prior sections.

Secondly, Interface VPC Endpoints create these secure connections by utilizing private IP addresses via a service called AWS PrivateLink which allows the service to act as a bridge between VPCs, AWS services and on-premises networks without ever having to expose the infrastructure and traffic to the public internet.

Therefore, whenever we wish to connect one AWS service to another, say EC2 to SNS (Will be discussed in later sections), then utilizing interface VPC endpoints is usually the most convenient way of doing so, especially when privacy and not exposing the resources to the public internet is a major concern.