AWS Certified Solutions Architect - Associate

Module 7
Virtual Private Cloud

Agenda

- What is VPC
- Features
- Components
- Private & Public Subnet
- VPN
- VPC Security
- ACL Rules
- VPC peering
- Hands-on lab

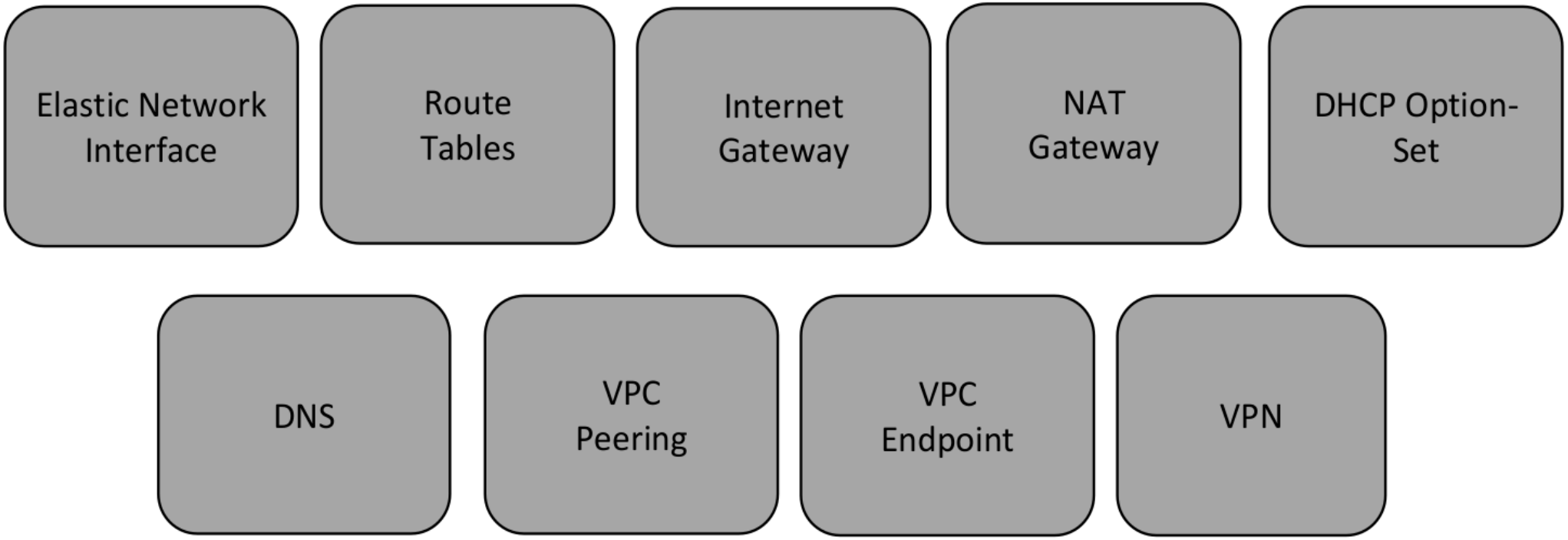
What is VPC

- **Amazon Virtual Private Cloud (VPC) enables you to launch AWS resources into a virtual network that you've defined.**
- **It is logically isolated from other virtual networks in the AWS cloud.**
- **You can configure your VPC; you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings.**
- **You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.**

Features

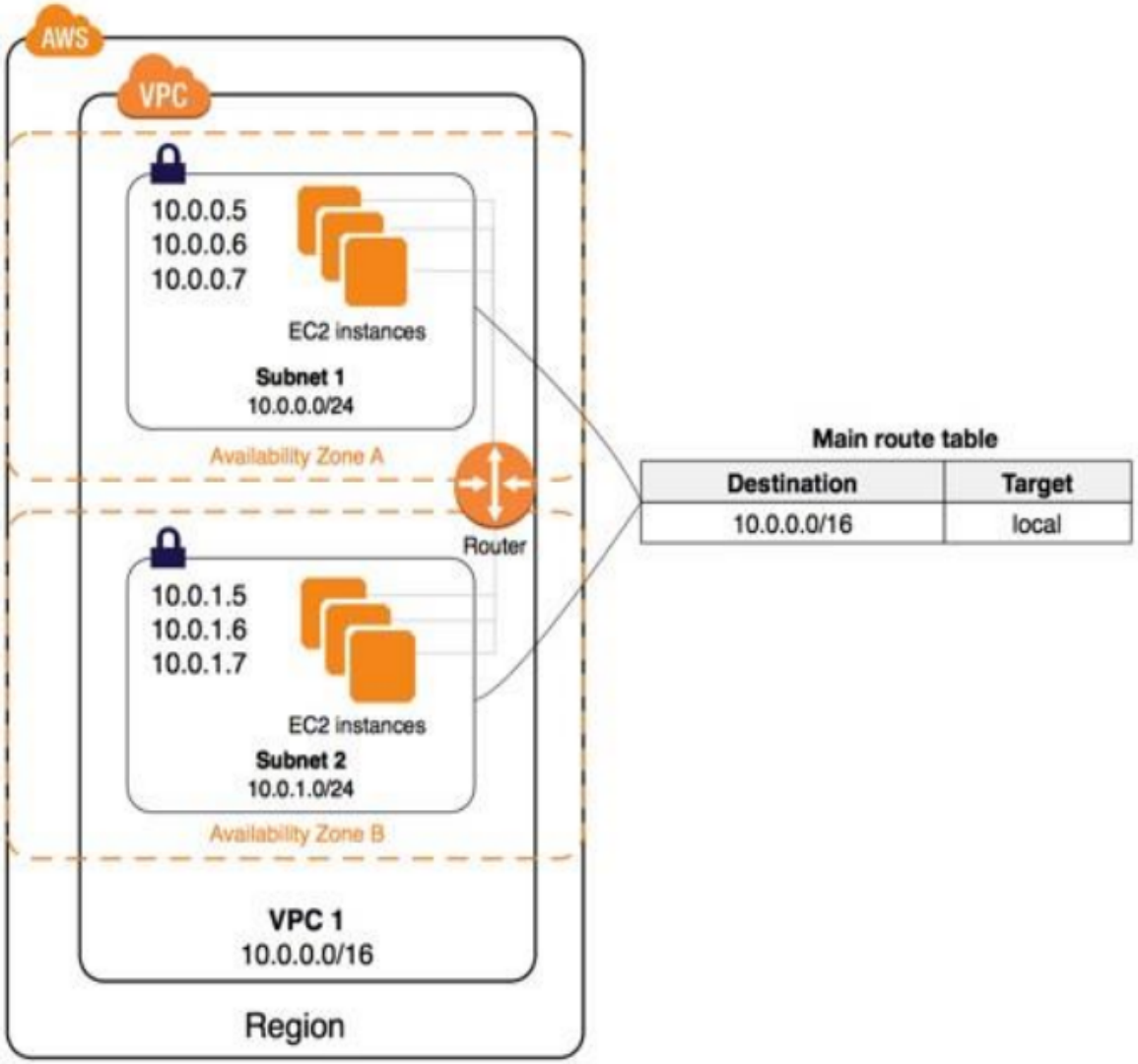
- **Attach one or more network interfaces to your instances.**
- **Assign static private Ipv4 addresses to your instances**
- **Run your instances on single-tenant hardware.**
- **Assign multiple IP addresses to your instances.**
- **Access control lists (ACL).**
- **Egress & Ingress filtering.**

Components


Elastic Network Interface
Route Tables
Internet Gateway
NAT Gateway
DHCP Option-Set
DNS
VPC Peering
VPC Endpoint
VPN

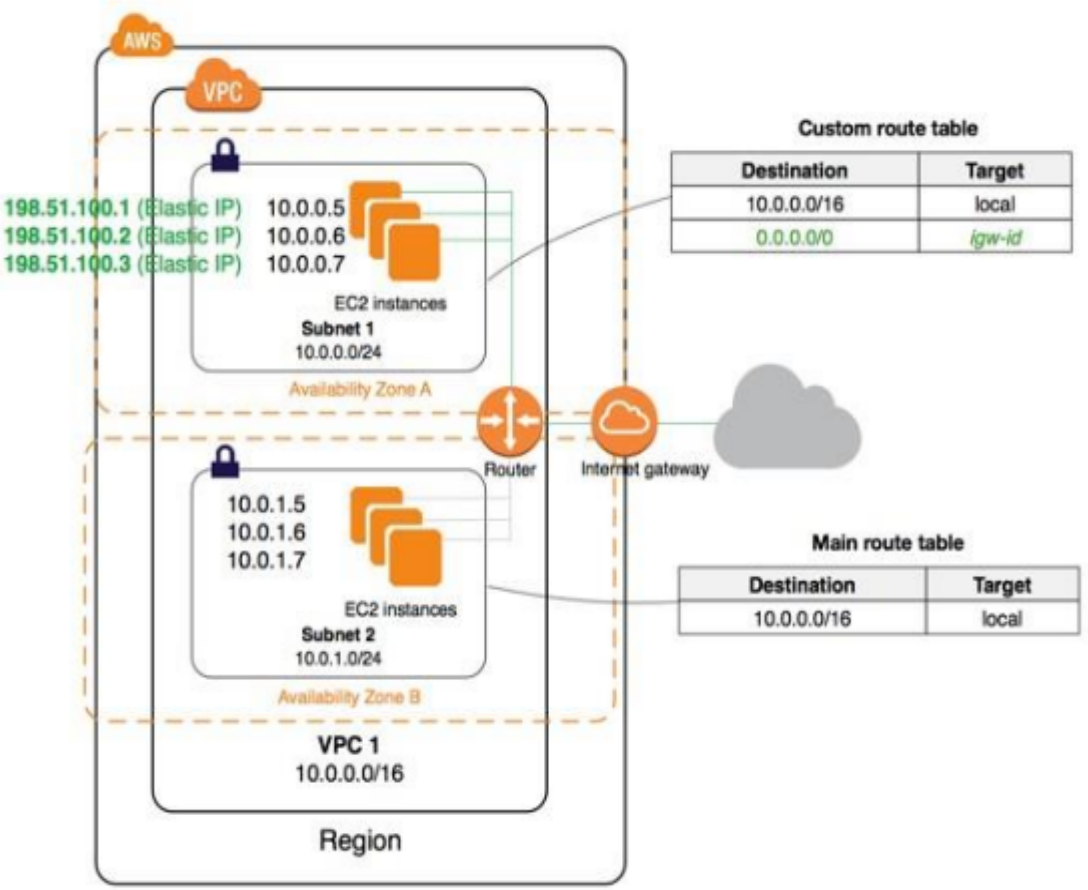
VPC – Private Subnet

- **If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet.**
- **By default, each instance has a private address, but no public address and these instances can communicate with each other, but can't access the Internet.**



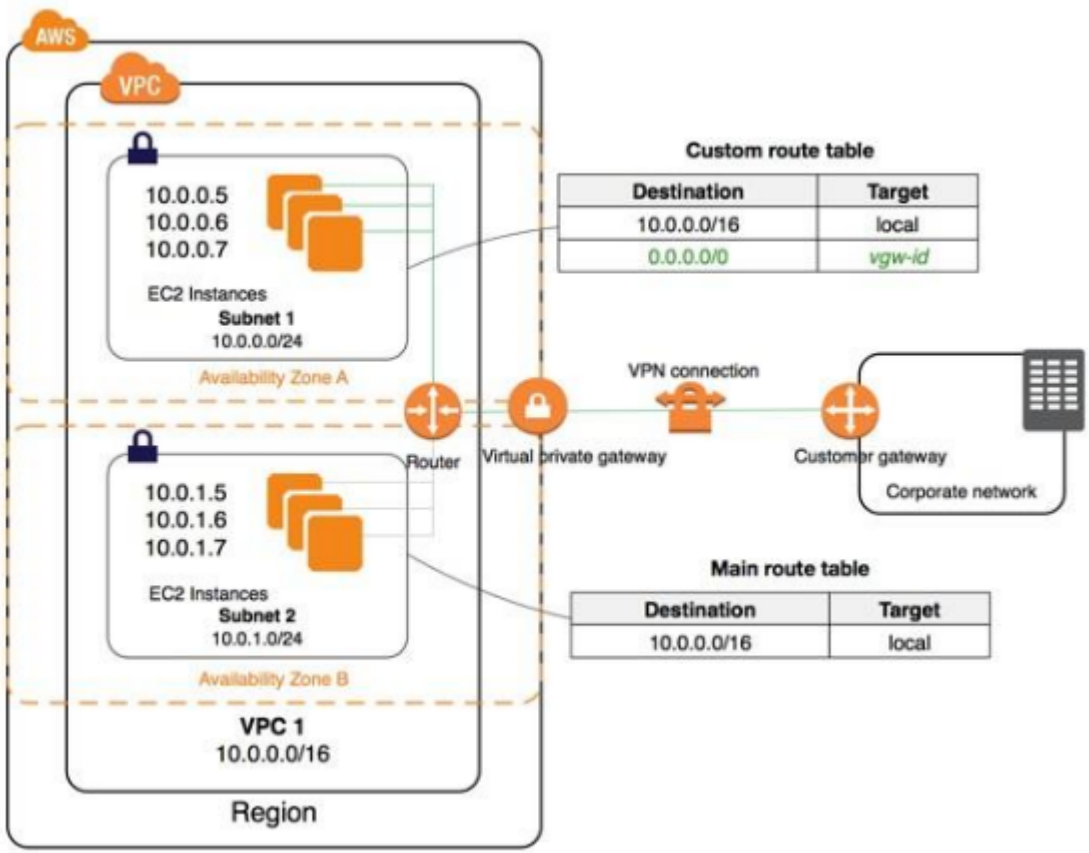
VPC – Public Subnet

- A public subnet is a subnet that has access to the Internet through an Internet gateway.
- Each instance has a private address and public address.
- These instances can communicate with each other, and access the Internet.



VPC – VPN

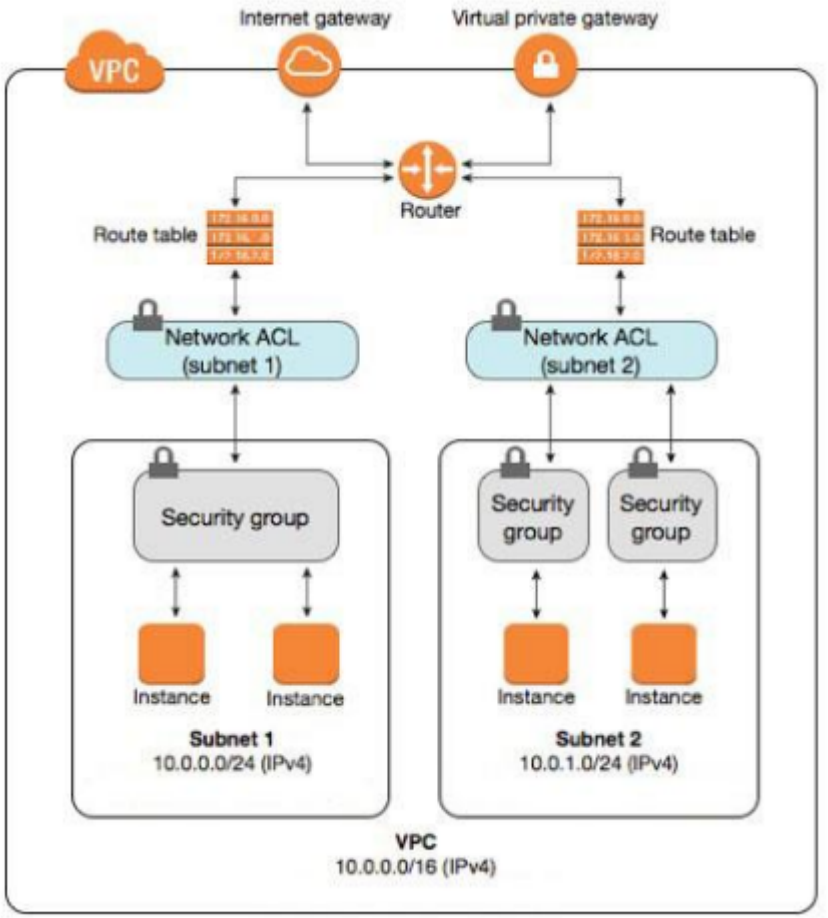
- Connect VPC to corporate data center using VPN connection
- This makes the AWS cloud an extension of your data center.
- VPN connection consists of a virtual private gateway and a customer gateway.



VPC - Security

VPC provides features to increase and monitor the security for your VPC:

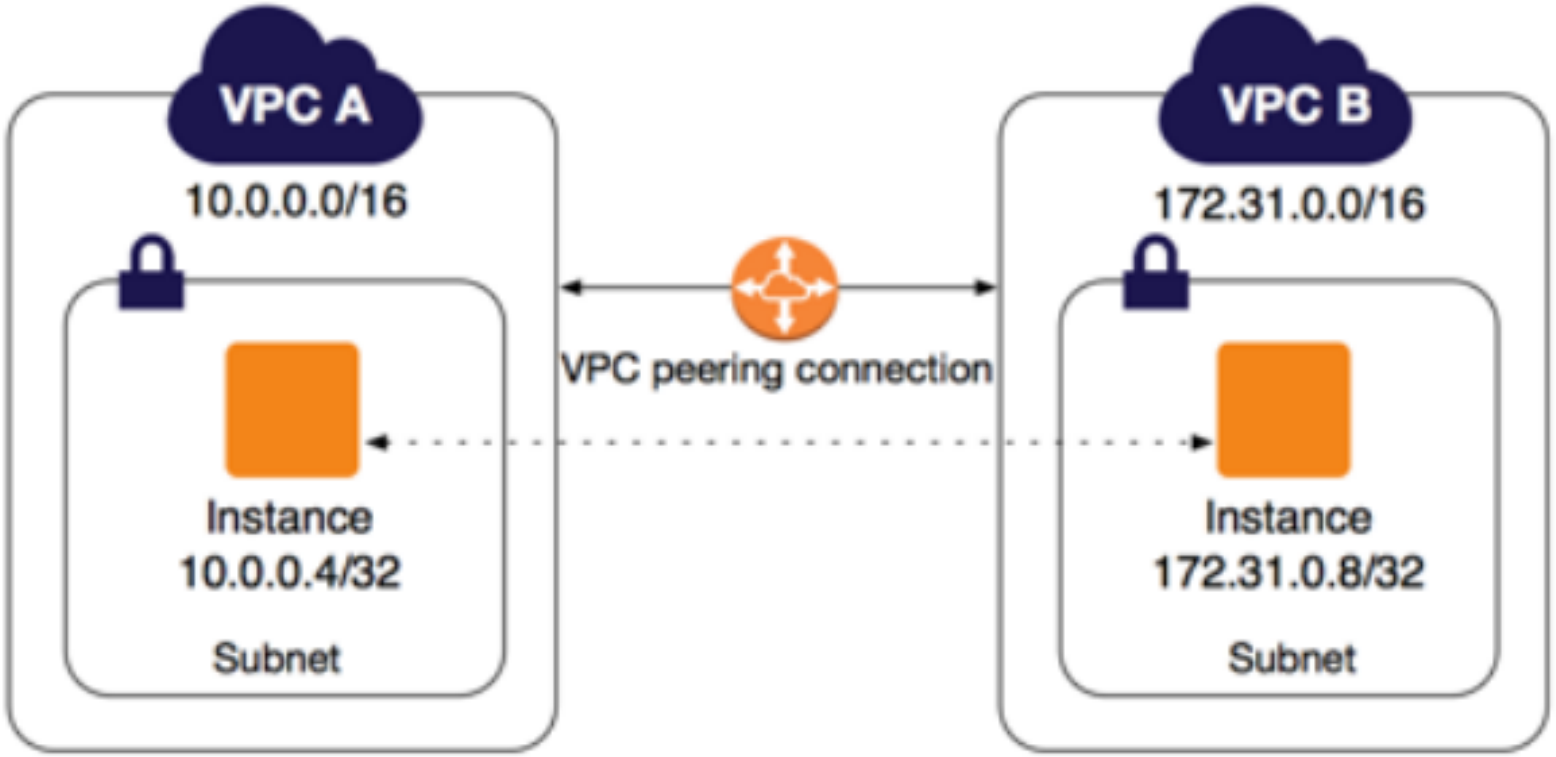
- **Security Groups**
- **Network Access Control Lists (ACLs).**



VPC: Peering

- **VPC peering is a networking connection between two VPCs that enables you to route traffic between them.**
- **Instances in either VPC can communicate with each other as if they are within the same network.**
- **Create a VPC peering connection between own VPCs, or with a VPC in another AWS account.**
- **In both cases, the VPCs must be in the same region.**

VPC – Peering


VPC A
10.0.0.0/16
VPC B
172.31.0.0/16
VPC peering connection
Instance
10.0.0.4/32
Subnet
Instance
172.31.0.8/32
Subnet

Hands-on Lab