This study guide demonstrates the lesson from *Introduction to AWS VPCs – Networking in the Cloud.*
My full AWS Architect Associate course can be found here:
https://www.udemy.com/course/ultimateaws/?referralCode=7ED214B795C444141361

AWS Virtual Private Cloud (VPC) Study Guide

Overview of VPC

An AWS Virtual Private Cloud (VPC) is a virtual network dedicated to your AWS account, providing a logically isolated section of the AWS cloud where you can launch AWS resources. By default, a VPC is isolated from other virtual networks and the internet, ensuring no traffic can enter or exit without explicit configuration.

Key Components and Concepts

- **Region and Availability Zones**: A VPC is created within a specific AWS region and can span multiple Availability Zones (AZs), allowing for the creation of highly available and resilient architectures.
- **CIDR Range**: When creating a VPC, you must define a Classless Inter-Domain Routing (CIDR) block, determining the IP address range available within the VPC. The largest range you can choose is /16, offering a substantial number of private IP addresses.
- **Subnets**: Within a VPC, you can create subnets, which are segments of the VPC's IP address range located within a specific Availability Zone. Subnets can be public (accessible from the internet) or private (isolated from the internet), depending on their intended use, such as hosting web servers or databases.
- **Internet Gateway (IGW)**: An internet gateway is a VPC component that allows communication between resources in your VPC and the internet. It's necessary for enabling internet access in public subnets.
- **VPN and AWS Direct Connect**: For secure connections between your on-premises data center and your VPC, AWS provides VPN connections and AWS Direct Connect, offering encrypted internet-based connections and dedicated physical connections, respectively.
- **Network ACLs and Security Groups**: Network Access Control Lists (ACLs) and Security Groups act as firewalls for controlling traffic into and out of subnets and EC2 instances, respectively. While Network ACLs apply at the subnet level affecting all resources within, Security Groups apply to individual instances, offering granular control.

Security and Network Traffic Control

- **Network ACLs**: Are associated with subnets, controlling all inbound and outbound traffic passing through the subnet. They offer another layer of security, supplementing Security Groups.

- **Security Groups**: Act on individual instances, allowing you to specify permissible traffic for each instance, providing customizable security at a more granular level.

Practical Applications

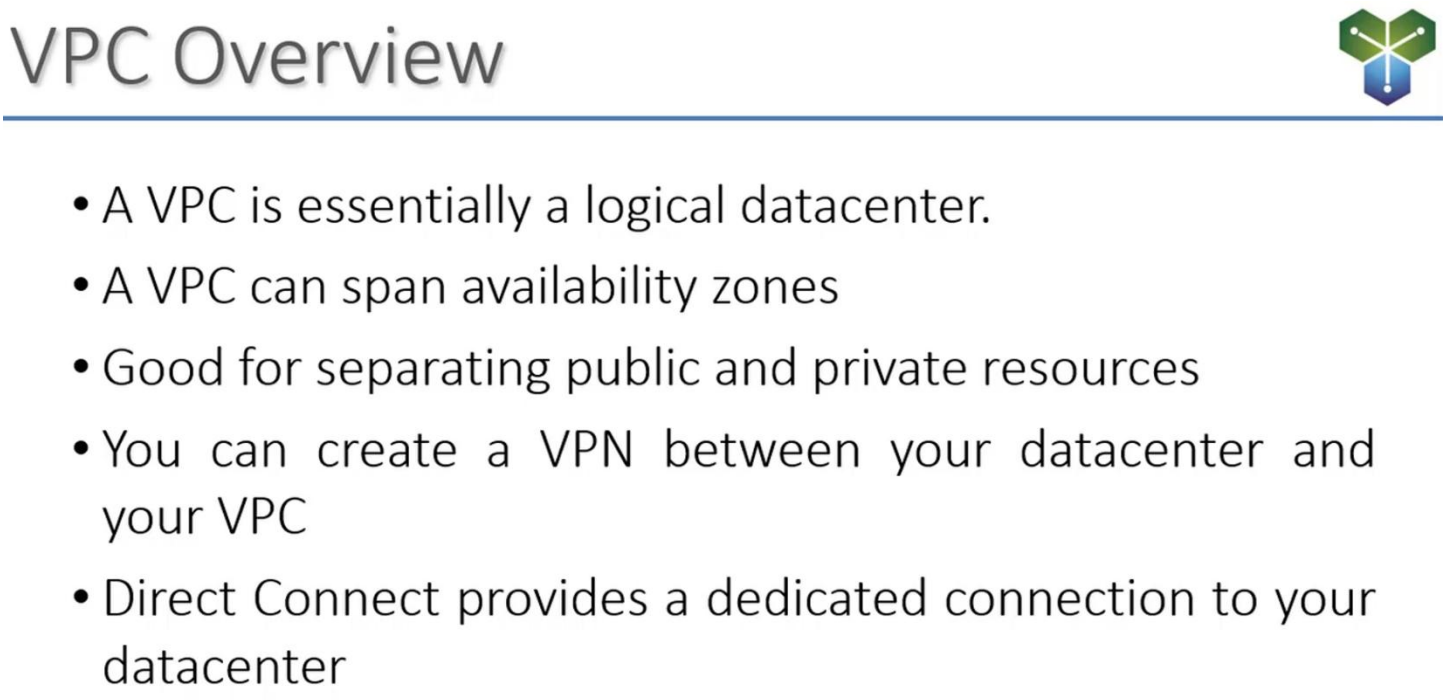
AWS VPC enables you to build a network architecture within AWS that mimics a traditional network you might operate in your own data center but with the benefits of AWS infrastructure. It's instrumental in:

- **Creating Isolated Networks**: For sensitive applications or data, ensuring they are not accessible from the internet.
- **Hosting Public-facing Services**: Like websites, by configuring public subnets and internet gateways.
- **Interconnecting with On-premises Data Centers**: Securely, using VPN or AWS Direct Connect, for hybrid cloud scenarios.

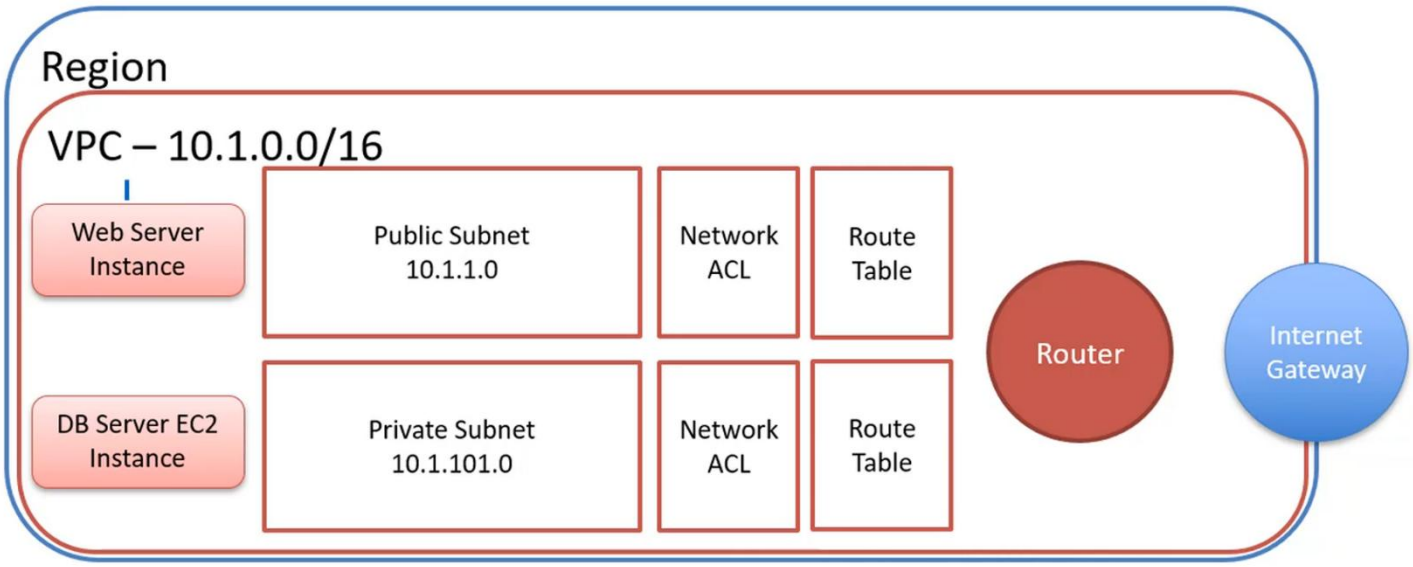
Conclusion

Understanding and effectively utilizing AWS VPC components like subnets, internet gateways, VPNs, Network ACLs, and Security Groups are fundamental for architecting secure, scalable, and highly available environments on AWS. By controlling network traffic at both the subnet and instance levels, AWS VPC provides the tools necessary to design complex networks tailored to an organization's specific needs.

See slides below:



VPC Diagram



For more details see my full AWS Architect Associate course:
https://www.udemy.com/course/ultimateaws/?referralCode=7ED214B795C444141361