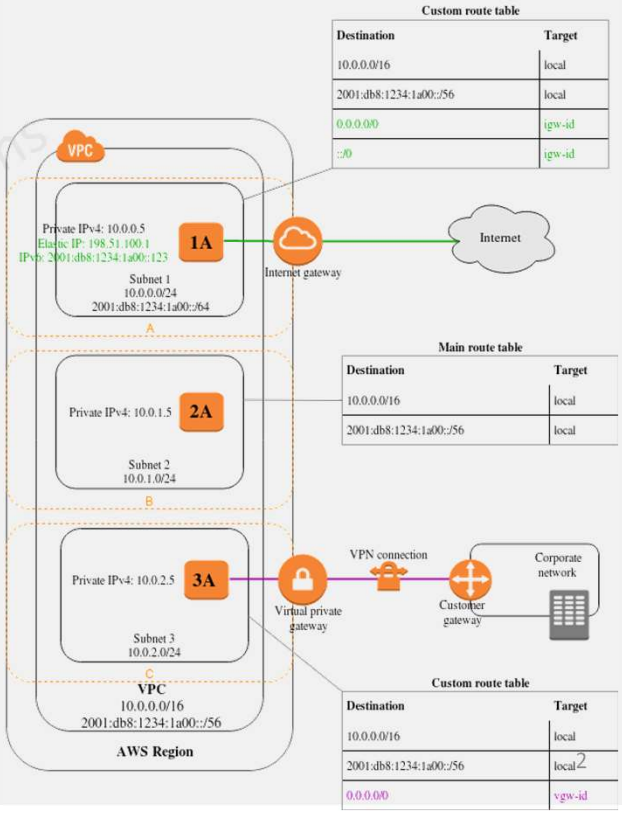
CLOUD COMPUTING APPLICATIONS

VPC: Advanced VPC

Prof. Reza Farivar

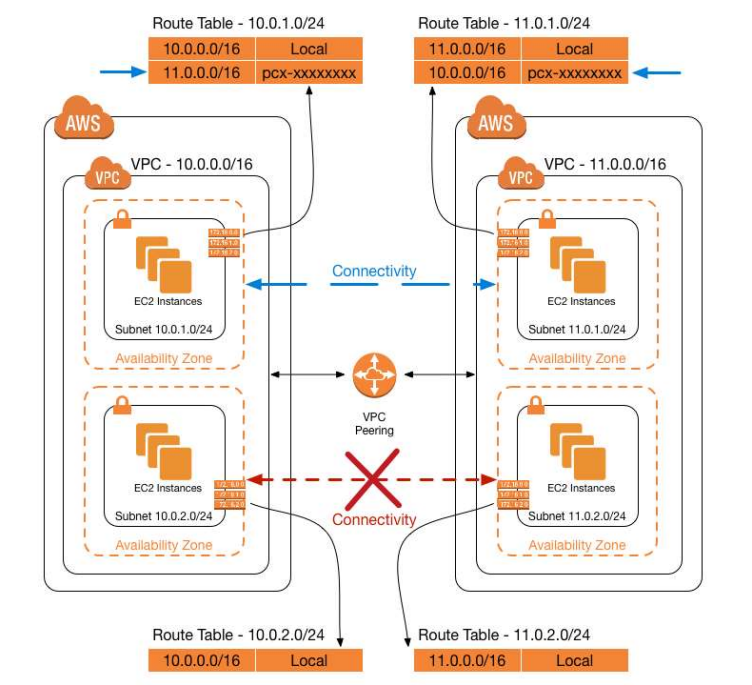
Virtual Private Gateway

- If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway for a Site-to-Site VPN connection, the subnet is known as a *VPN-only subnet*
- In this diagram, subnet 3 is a VPN-only subnet
- Concepts
  - **VPN connection**: A secure connection between your on-premises equipment and your VPCs.
  - **VPN tunnel**: An encrypted link where data can pass from the customer network to or from AWS.
    - Each VPN connection includes two VPN tunnels which you can simultaneously use for high availability.
  - **Customer gateway**: An AWS resource which provides information to AWS about your customer gateway device.
  - **Customer gateway device**: A physical device or software application on your side of the Site-to-Site VPN connection.
  - **Virtual private gateway**: The VPN concentrator on the Amazon side of the Site-to-Site VPN connection. You use a virtual private gateway or a transit gateway as the gateway for the Amazon side of the Site-to-Site VPN connection.
  - **Transit gateway**: A transit hub that can be used to interconnect your VPCs and on-premises networks. You use a transit gateway or virtual private gateway as the gateway for the Amazon side of the Site-to-Site VPN connection.
- As of 2020, VPN connections into AWS are IPV4 only
- It is recommended that you use non-overlapping CIDR blocks for your networks



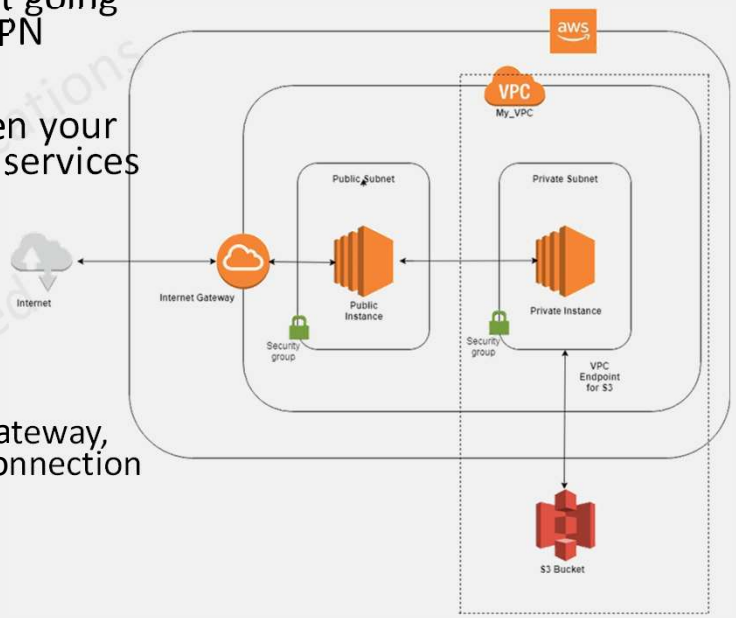
VPC Peering

- VPC peering can be used to make communication between VPCs within the same account, different AWS accounts, or any two VPCs within the same region or different regions
- Initially, VPC peering was supported only within the same region, but later AWS added support for VPC peering across regions
- The two VPCs cannot have CIDR blocks that overlap with each other.



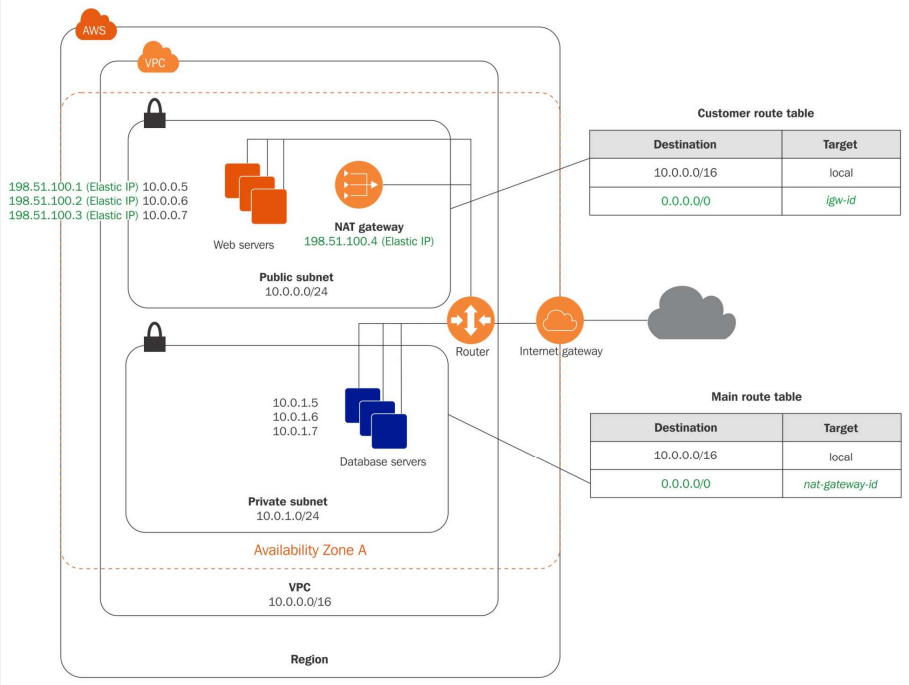
VPC Endpoints

- Generally, AWS services are different entities and do not allow direct communication with each other without going through either an IGW, a NAT gateway/instance, a VPN connection, or AWS Direct Connect
- A VPC endpoint enables private connections between your VPC and supported AWS services and VPC endpoint services
  - S3
  - DynamoDb
- AWS PrivateLink
  - Private IP addresses
  - Traffic does not leave the Amazon network
  - Does not require an internet gateway, virtual private gateway, NAT device, VPN connection, or AWS Direct Connect connection



** Interesting reading: https://www.bluematador.com/blog/s3-endpoint-connectivity-in-aws-vpc*

VPC with Private and Public Subnets



Routing in VPC vs. Physical Network

- Physical Ethernet Network
  - Link Layer
    - Lowest layer in the Internet Protocol
      - Layer 2 in OSI model
  - In a physical traditional network, this layer uses MAC address and ARP messaging (to discover unknown MAC addresses)
- VPC Network
  - Amazon backend intercepts any MAC ARP request
  - Looks up routing tables, and returns the destination without implementing ARP