Course and Labs

Design Network in AWS

Mohanraj Shanmugam

Course and Labs

Topic 3: AWS Connectivity

Mohanraj Shanmugam

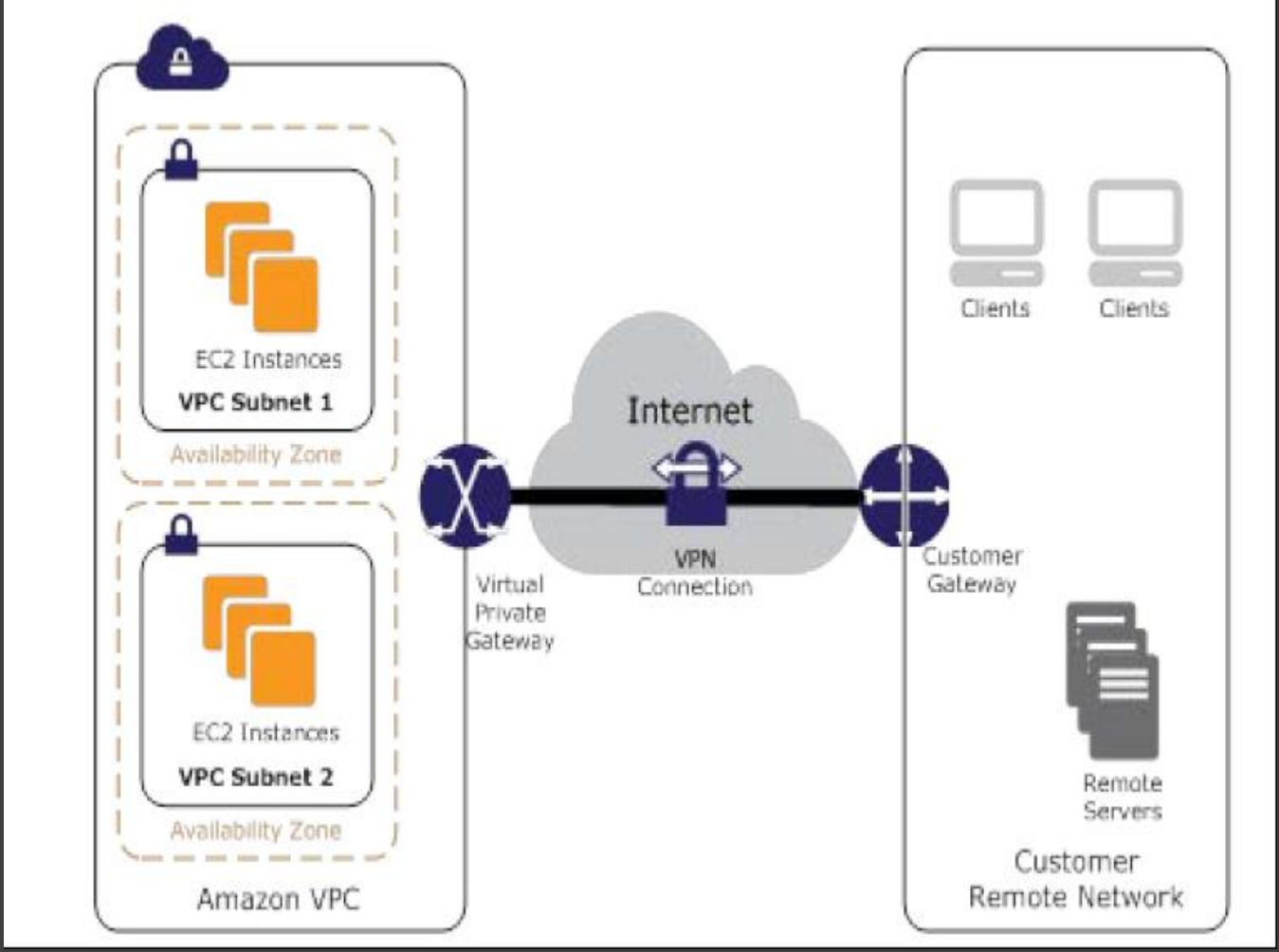
Routing and Private Connections

- Amazon VPC provides multiple network connectivity options for you to leverage depending on your current network designs and requirements.
- These connectivity options include leveraging either the Internet or an AWS Direct Connect connection as the network “backbone” and terminating the connection into either AWS or user managed network endpoints.
- Additionally, with AWS, you can choose how network routing will be delivered between Amazon VPC and your networks, leveraging either AWS or user-managed network equipment and routes.

User Network–to–Amazon VPC Connectivity Options

- Hardware VPN
  - Describes establishing a hardware VPN connection from your network equipment on a remote network to AWS-managed network equipment attached to your Amazon VPC
- AWS Direct Connect
  - Describes establishing a private, logical connection from your remote network to Amazon VPC, leveraging AWS Direct Connect.
- **AWS Direct Connect + VPN**
  - Describes establishing a private, encrypted connection from your remote network to Amazon VPC, leveraging AWS Direct Connect.
- **AWS VPN CloudHub**
  - Describes establishing a hub-and-spoke model for connecting remote branch offices.
- **Software VPN**
  - Describes establishing a VPN connection from your equipment on a remote network to a user-managed software VPN appliance running inside an Amazon VPC.

Hardware VPN



Amazon VPC provides the option of creating an IPsec, hardware VPN connection between remote customer networks and their Amazon VPC over the Internet

Consider taking this approach when you want to take advantage of an AWS-managed VPN endpoint that includes automated multi–data center redundancy and failover built into the AWS side of the VPN connection.

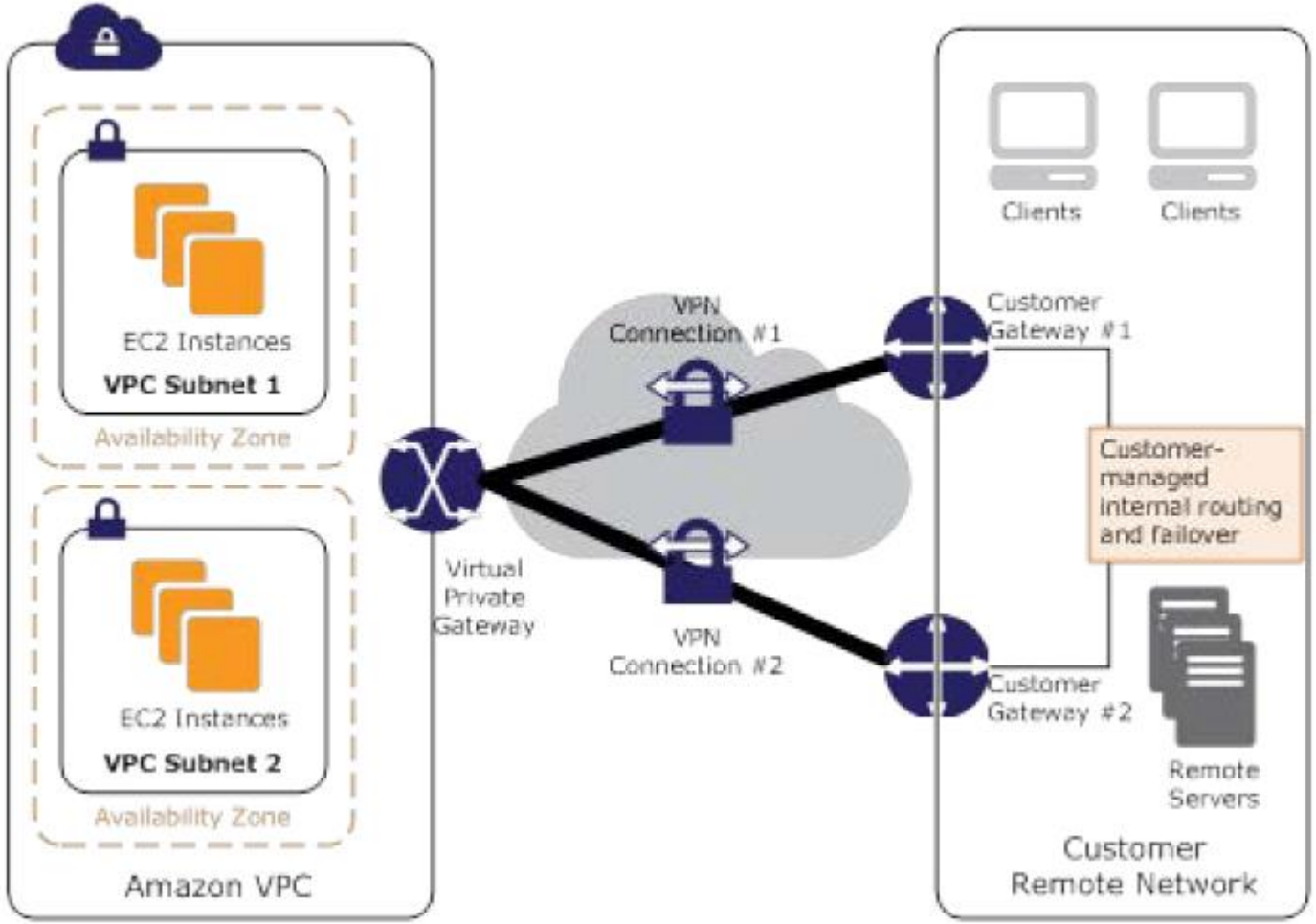
Reuse existing VPN equipment and processes

Reuse existing Internet connections

AWS-managed endpoint includes multidata center redundancy and automated failover

Supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies

Hardware VPN



- The Amazon virtual private gateway (VGW) represents two distinct VPN endpoints, physically located in separate data centers to increase the availability of your VPN connection.
- The VGW also supports and encourages multiple user gateway connections so you can implement redundancy and failover on your side of the VPN connection
- Both dynamic and static routing options are provided to give you flexibility in your routing configuration.
- Both dynamic and static routing options are provided to give you flexibility in your routing configuration.
- With dynamic routing, you can also specify routing priorities, policies, and weights (metrics) in your BGP advertisements and influence the network path between your network(s) and AWS.
- It is important to note that when BGP is used, both the IPSec and the BGP connections must be terminated on the same user gateway device, so it must be capable of terminating both IPSec and BGP connections.

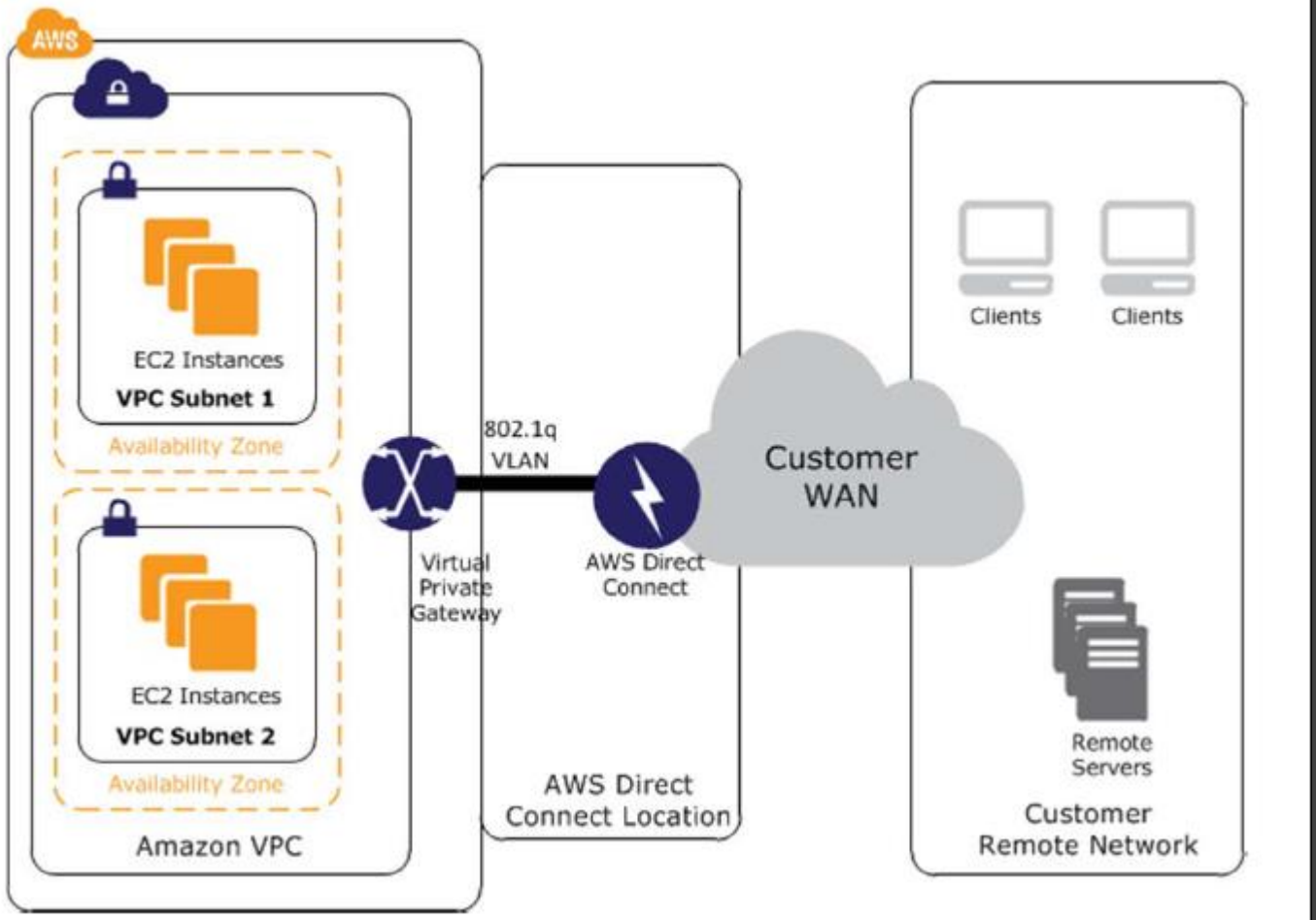
Limitation of Hardware VPN

- Network latency, variability, and availability are dependent on Internet conditions
- Customer-managed is responsible for implementing redundancy and failover (if required)
- Customer device must support single-hop BGP (when leveraging BGP for dynamic routing)

AWS Direct Connect

- AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to Amazon VPC.
- Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment.
- This private connection can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
- AWS Direct Connect lets you establish 1 Gbps or 10 Gbps dedicated network connections (or multiple connections) between AWS networks and one of the AWS Direct Connect locations.

AWS Direct Connect



- It uses industry-standard VLANs to access Amazon Elastic Compute Cloud (Amazon EC2) instances running within an Amazon VPC using private IP addresses.
- You can choose from an ecosystem of WAN service providers for integrating your AWS Direct Connect endpoint in an AWS Direct Connect location with your remote networks.
- AWS Direct connect Location

https://aws.amazon.com/directconnect/faqs/

AWS Direct connect Partner Locations

https://aws.amazon.com/directconnect/partners/

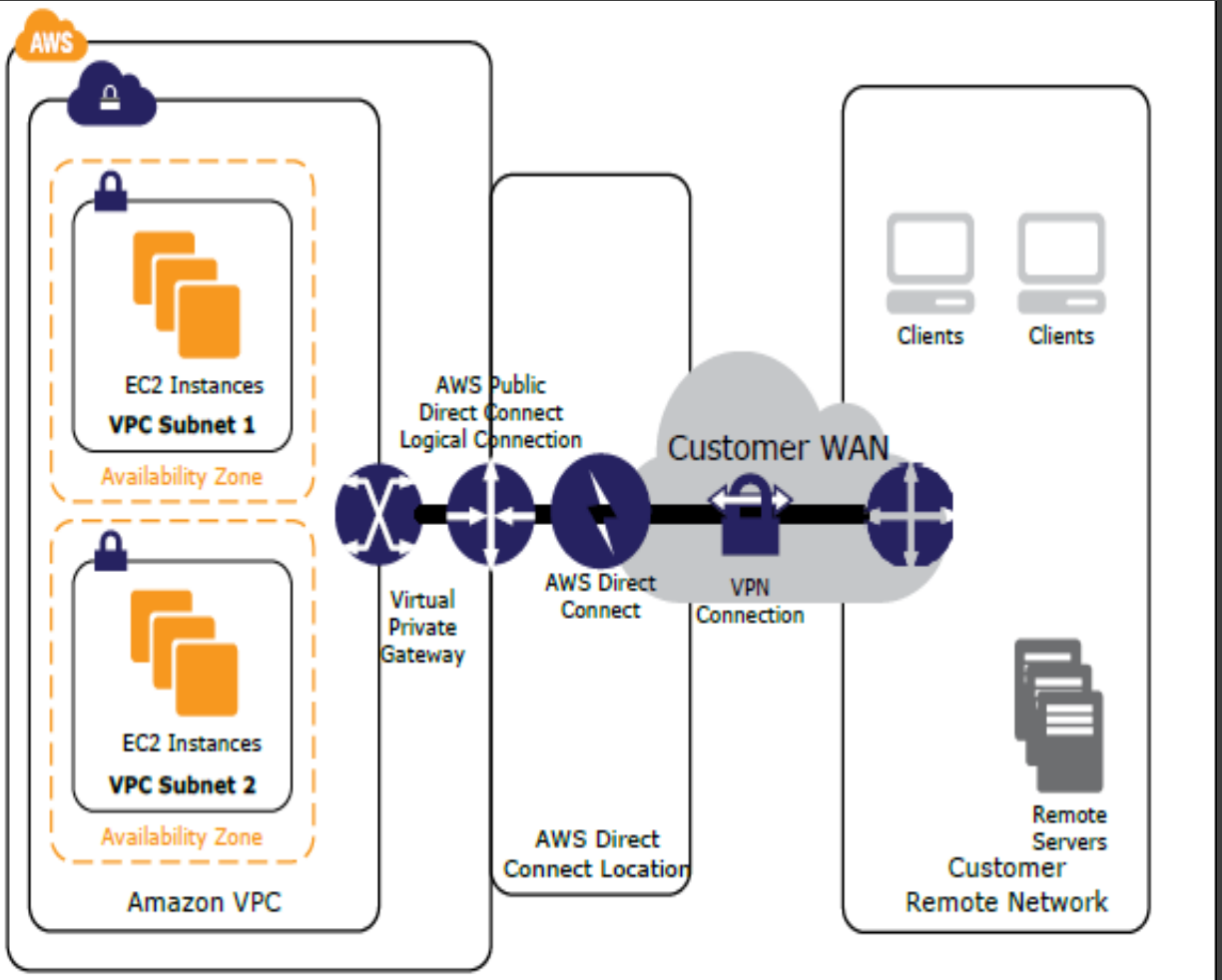
AWS Direct Connect

- When to use AWS Direct Connect
  - Working with Large Data Sets
  - Real-time Data Feeds
  - Hybrid Environments
- Pricing
  - Pricing is per port-hour for all AWS Direct Connect locations.
  - Data Transfer In is $0.00 per GB in all locations.
  - Data Transfer Out is cost per GB per month
  - http://aws.amazon.com/directconnect/pricing/

AWS Direct Connect

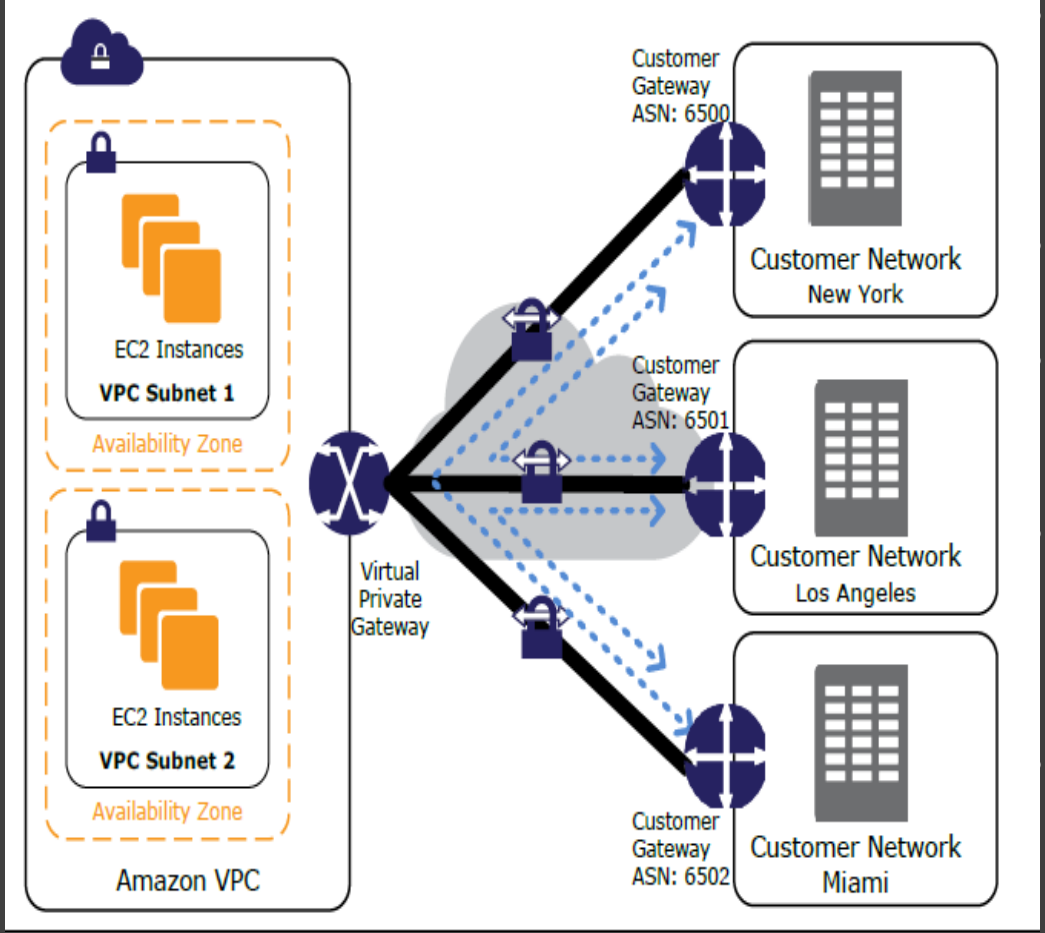
- To use AWS Direct Connect, you simply:
  - Decide on an AWS Direct Connect location, how many connections you would like to use, and the port size. Multiple ports can be used simultaneously for increased bandwidth or redundancy.
  - Use the AWS Management Console to create your connection request(s).
  - If you are connecting from a remote location, you can work with an APN Partner supporting Direct Connect or a network carrier of your choice.
  - Once your request is confirmed, you will receive an email which contains a Letter of Authorization – Connecting Facility Assignment (LOA-CFA).
  - Provide the LOA-CFA to an APN Partner or your service provider who will establish the connection on your behalf.
  - Once the connection is up, use the AWS Management Console to configure one or more virtual interfaces to establish network connectivity.

AWS Direct Connect + VPN



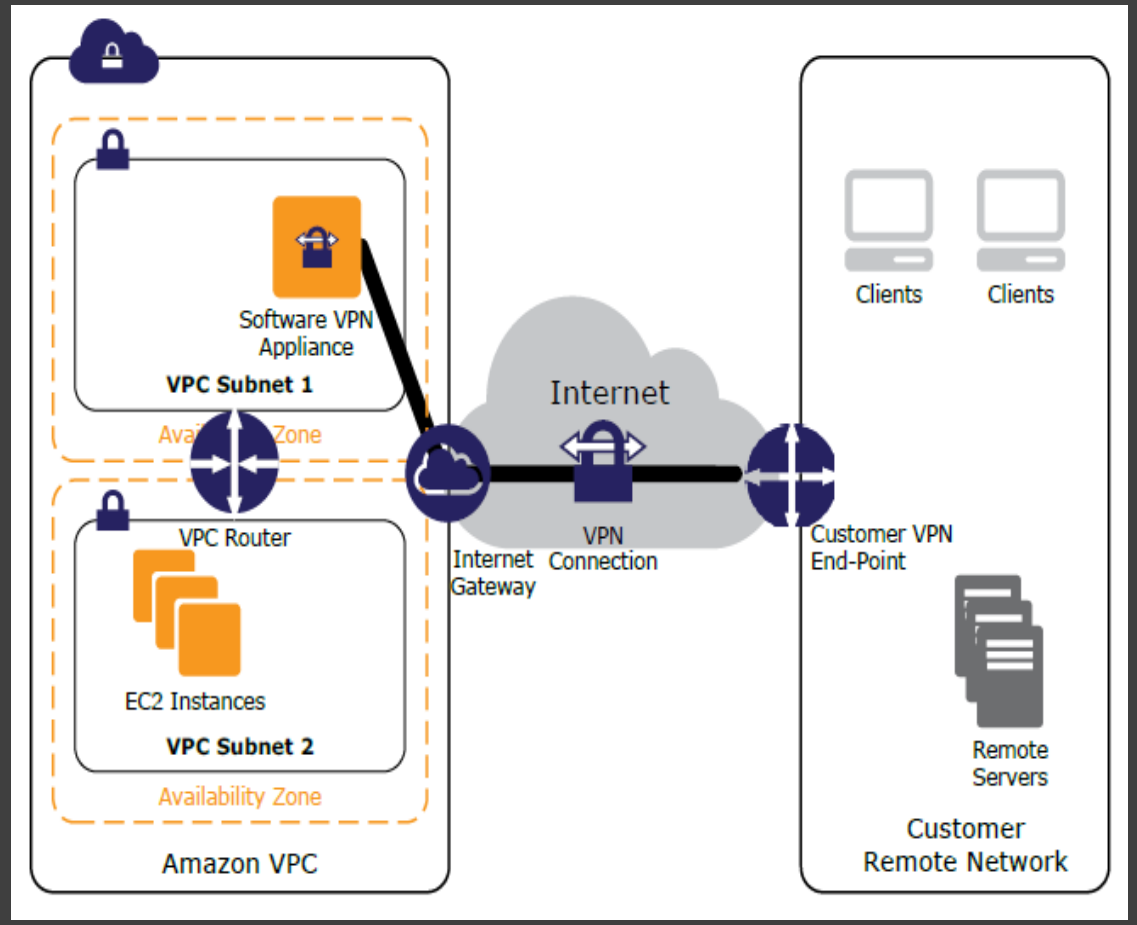
- AWS Direct Connect + VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC hardware VPN.
- This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than Internet-based VPN connections.
- This solution combines the AWS-managed benefits of the hardware VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection.

AWS VPN CloudHub



- You can securely communicate from one site to another using the AWS VPN CloudHub.
- The AWS VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC.
- Use this design if you have multiple branch offices and existing Internet connections and would like to implement a convenient, potentially low cost hub-and-spoke model for primary or backup connectivity between these remote offices.
- blue dashed lines indicating network traffic between remote sites being routed over their AWS VPN connections.
- AWS VPN CloudHub leverages an Amazon VPC virtual private gateway with multiple gateways, each using unique BGP autonomous system numbers (ASNs).
- Your gateways advertise the appropriate routes (BGP prefixes) over their VPN connections. These routing advertisements are received and readvertised to each BGP peer so that each site can send data to and receive data from the other sites.
- The remote network prefixes for each spoke must have unique ASNs, and the sites must not have overlapping IP ranges. Each site can also send and receive data from the VPC as if they were using a standard VPN connection.

Software VPN



- Amazon VPC offers you the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network.
- This option is recommended if you must manage both ends of the VPN connection either for compliance purposes or for leveraging gateway devices that are not currently supported by Amazon VPC's hardware VPN solution.
- You can choose VPN products from well-known security companies like Check Point, Astaro, OpenVPN Technologies, and Microsoft, as well as popular open source tools like OpenVPN, Openswan, and IPsec-Tools.
- It is your responsibility for you to manage the software appliance, including configuration, patches, and upgrades.
- Implement in a HA Architecture to avoid any single point of Failure

Amazon VPC-to-Amazon VPC Connectivity Options

Course and Labs

- Use these design patterns when you want to integrate multiple Amazon VPCs into a larger virtual network.
- This is useful if you require multiple VPCs due to security, billing, presence in multiple regions, or internal charge-back requirements to more easily integrate AWS resources between Amazon VPCs.
- You can also combine these patterns with the UsCustomer Network-–to–-Amazon VPC Connectivity Options for creating a corporate network that spans remote networks and multiple VPCs.
- VPC connectivity between VPCs is best achieved when using nonoverlapping IP ranges for each VPC being connected. For example, if you'd like to connect multiple VPCs, make sure each VPC is configured with unique Classless Inter-Domain Routing (CIDR) ranges. Therefore, we advise you to allocate a single, contiguous, nonoverlapping CIDR block to be used by each VPC.

Amazon VPC-to-Amazon VPC Connectivity Options

- VPC Peering
- Software VPN
- Software-to-hardware VPN
- Hardware VPN
- AWS Direct Connect

VPC Peering

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP 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 within a single region.
- AWS uses the existing infrastructure of a VPC to create a VPC peering connection
- it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

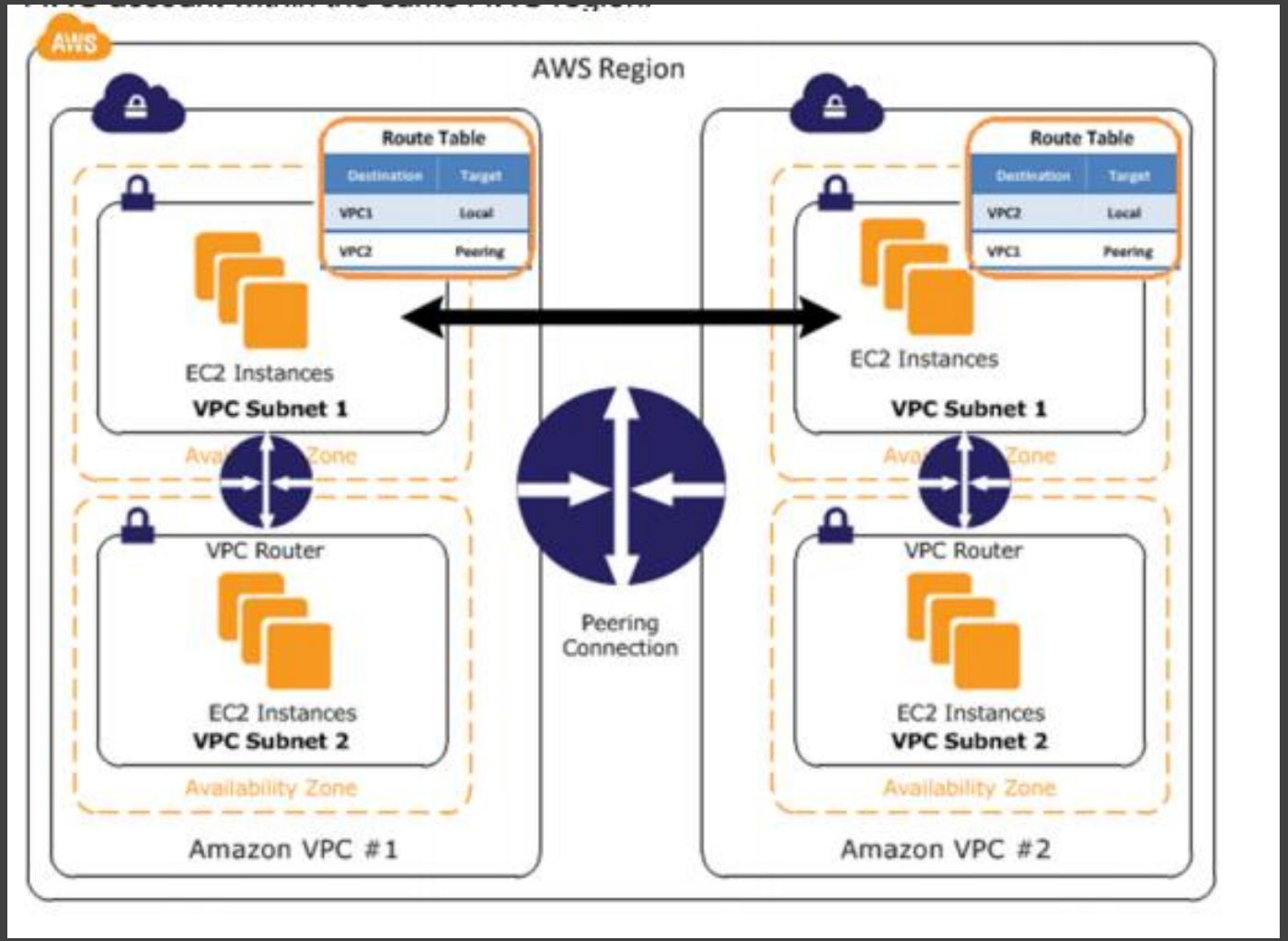
VPC Peering

- A VPC peering connection can help you to facilitate the transfer of data
- for example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network.
- You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

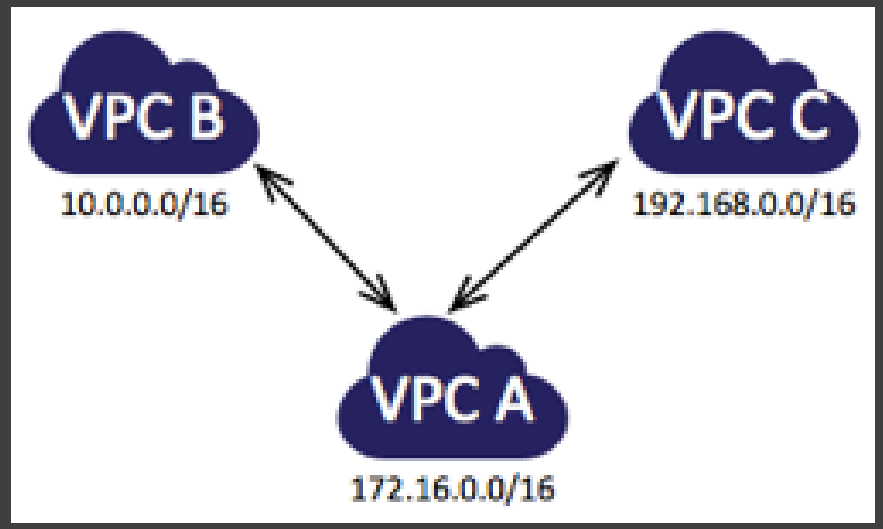
VPC Peering Basics

- To establish a VPC peering connection, the owner of the *requester VPC* (or *local VPC*) sends a request to the owner of the *peer VPC* to create the VPC peering connection.
- . The peer VPC can be owned by you, or another AWS account, and cannot have a CIDR block that overlaps with the requester VPC's CIDR block.
- The owner of the peer VPC has to accept the VPC peering connection request to activate the VPC peering connection.
- To enable the flow of traffic between the peer VPCs using private IP addresses, add a route to one or more of your VPC's route tables that points to the IP address range of the peer VPC.
- The owner of the peer VPC adds a route to one of their VPC's route tables that points to the IP address range of your VPC.
- You may also need to update the security group rules that are associated with your instance to ensure that traffic to and from the peer VPC is not restricted.

VPC Peering Basics

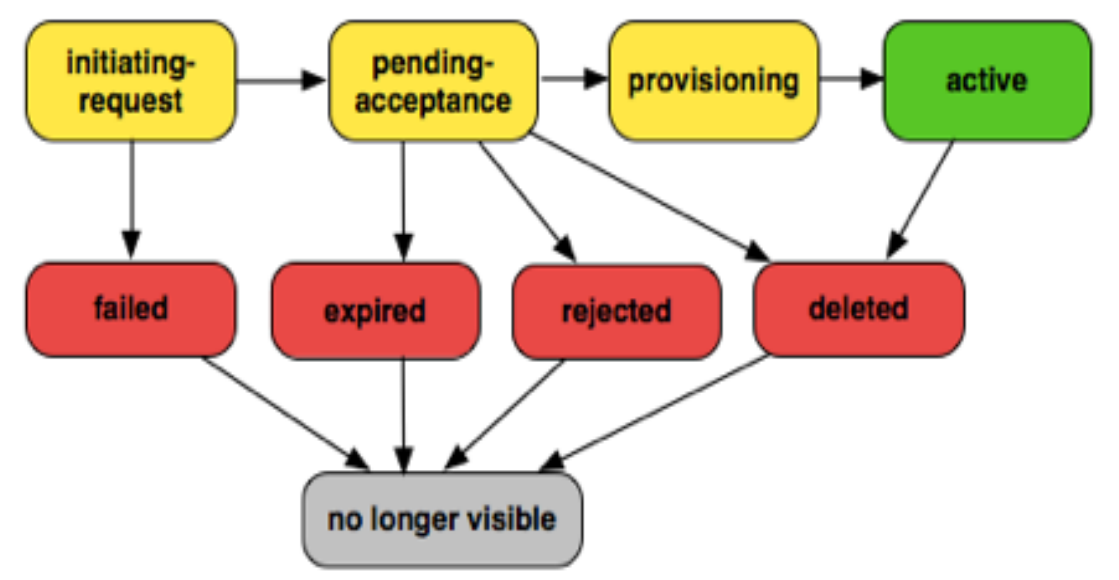


VPC Peering Basics



- A VPC peering connection is a one to one relationship between two VPCs.
- You can create multiple VPC peering connections for each VPC that you own, but transitive peering relationships are not supported
- you will not have any peering relationship with VPCs that your VPC is not directly peered with.
- example of one VPC peered to two different VPCs. There are two VPC peering connections: VPC A is peered with both VPC B and VPC C. VPC B and VPC C are not peered, and you cannot use VPC A as a transit point for peering between VPC B and VPC C. If you want to enable routing of traffic between VPC B and VPC C, you must create a unique VPC peering connection between them.

VPC Peering Connection Lifecycle



- A VPC peering connection goes through various stages starting from when the request is initiated. At each stage, there may be actions that you can take, and at the end of its lifecycle, the VPC peering connection remains visible in the VPC console and API

VPC Peering Connection Lifecycle

- **Initiating-request**: A request for a VPC peering connection has been initiated. At this stage, the peering connection may fail or may go to `pending-acceptance`.
- **Failed**: The request for the VPC peering connection has failed. During this state, it cannot be accepted or rejected. The failed VPC peering connection remains visible to the requester for 2 hours.
- **Pending-acceptance**: The VPC peering connection request is awaiting acceptance from the owner of the peer VPC. During this state, the owner of the requester VPC can delete the request, and the owner of the peer VPC can accept or reject the request. If no action is taken on the request, it will expire after 7 days
- **Expired**: The VPC peering connection request has expired, and no action can be taken on it by either VPC owner. The expired VPC peering connection remains visible to both VPC owners for 2 days.

VPC Peering Connection Lifecycle

- **Rejected**: The owner of the peer VPC has rejected a `pending-acceptance` VPC peering connection request. During this state, the request cannot be accepted. The rejected VPC peering connection remains visible to the owner of the requester VPC for 2 days, and visible to the owner of the peer VPC for 2 hours. If the request was created within the same AWS account, the rejected request remains visible for 2 hours.
- **Provisioning**: The VPC peering connection request has been accepted, and will soon be in the `active` state.
- **Active**: The VPC peering connection is active. During this state, either of the VPC owners can delete the VPC peering connection, but cannot reject it.
- **Deleted**: An `active` VPC peering connection has been deleted by either of the VPC owners, or a `pending-acceptance` VPC peering connection request has been deleted by the owner of the requester VPC. During this state, the VPC peering connection cannot be accepted or rejected. The VPC peering connection remains visible to the party that deleted it for 2 hours, and visible to the other party for 2 days. If the VPC peering connection was created within the same AWS account, the deleted request remains visible for 2 hours.

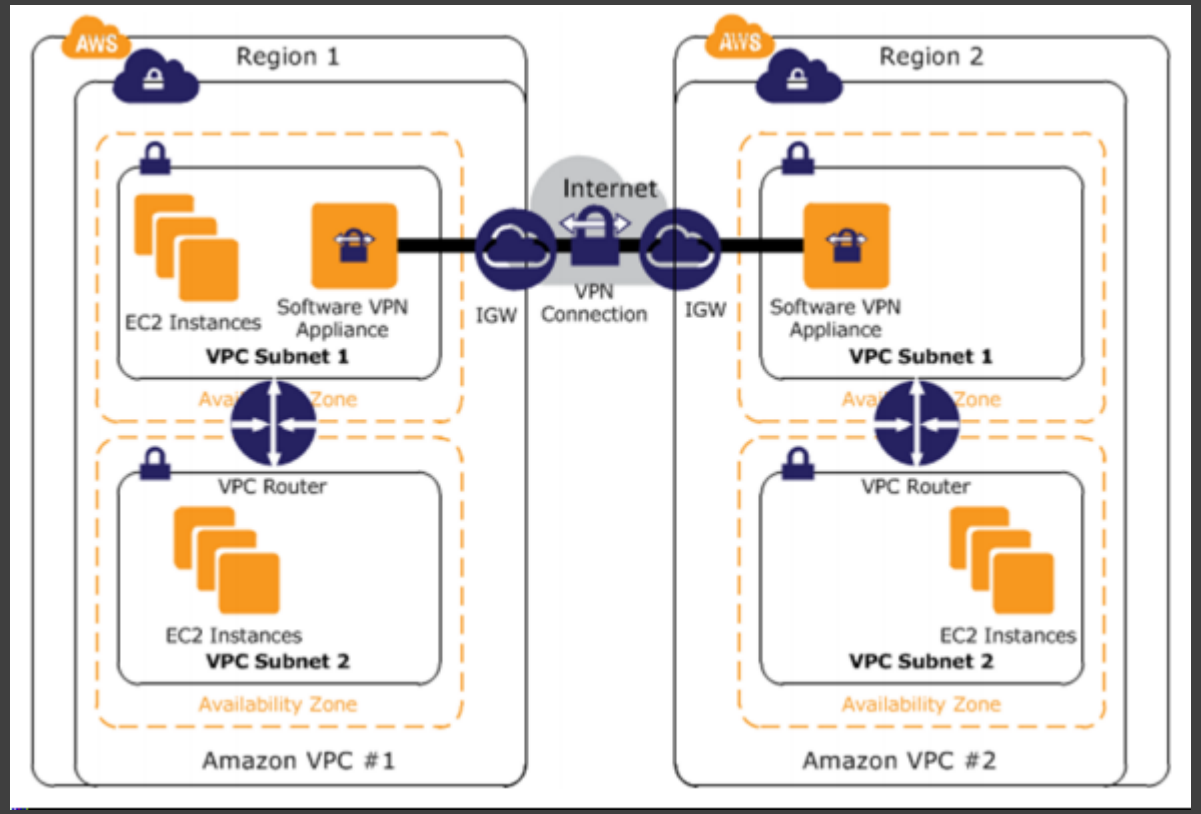
VPC Peering Limitations

- To create a VPC peering connection with another VPC, you need to be aware of the following limitations and rules:
  - You cannot create a VPC peering connection between VPCs that have matching or overlapping CIDR blocks.
  - You cannot create a VPC peering connection between VPCs in different regions.
  - You have a limit on the number active and pending VPC peering connections that you can have per VPC. For more information about VPC limits, see Amazon VPC Limits.
  - VPC peering does not support transitive peering relationships; in a VPC peering connection, your VPC will not have access to any other VPCs that the peer VPC may be peered with. This includes VPC peering connections that are established entirely within your own AWS account.
  - You cannot have more than one VPC peering connection between the same two VPCs at the same time.

VPC Peering Limitations

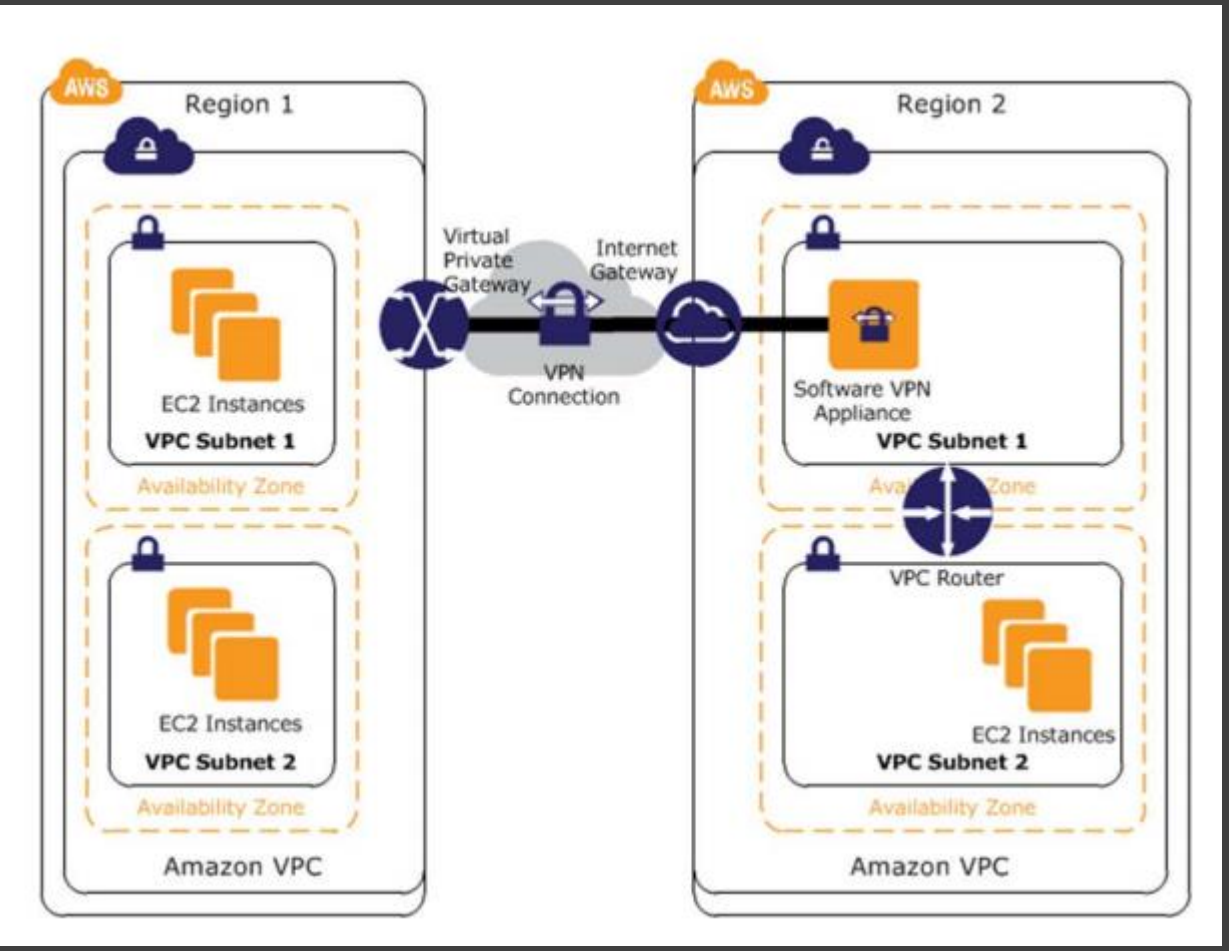
- The Maximum Transmission Unit (MTU) across a VPC peering connection is 1500 bytes.
- A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs. For more information about placement groups, see Placement Groups in the *Amazon EC2 User Guide for Linux Instances*.
- Unicast reverse path forwarding in VPC peering connections is not supported. For more information, see Routing for Response Traffic in the *Amazon VPC Peering Guide*.
- You cannot reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group. Instead, reference CIDR blocks of the peer VPC as the source or destination of your security group's ingress or egress rules.
- An instance's public DNS hostname will not resolve to its private IP address across peered VPCs.

Software VPN



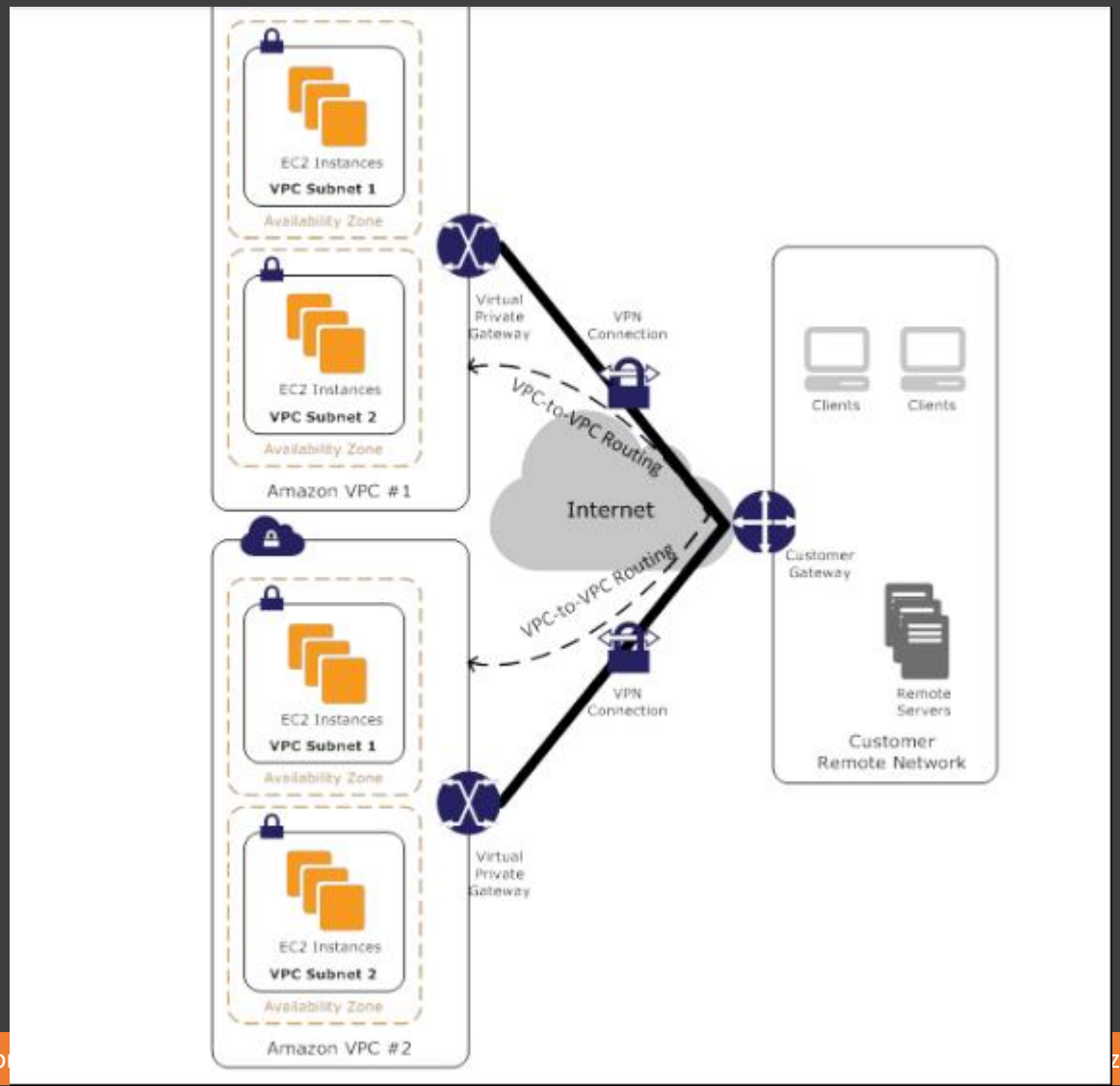
- Amazon VPC provides network routing flexibility.
- This includes the ability to create secure VPN tunnels between two or more software VPN appliances to connect multiple VPCs into a larger virtual private network so that instances in each VPC can seamlessly connect to each other using private IP addresses.
- This option is recommended when you want to connect VPCs across multiple AWS regions and manage both ends of the VPN connection using your preferred VPN software provider
- This option uses an Internet gateway attached to each VPC to facilitate communication between the software VPN appliances

Software-to-Hardware VPN



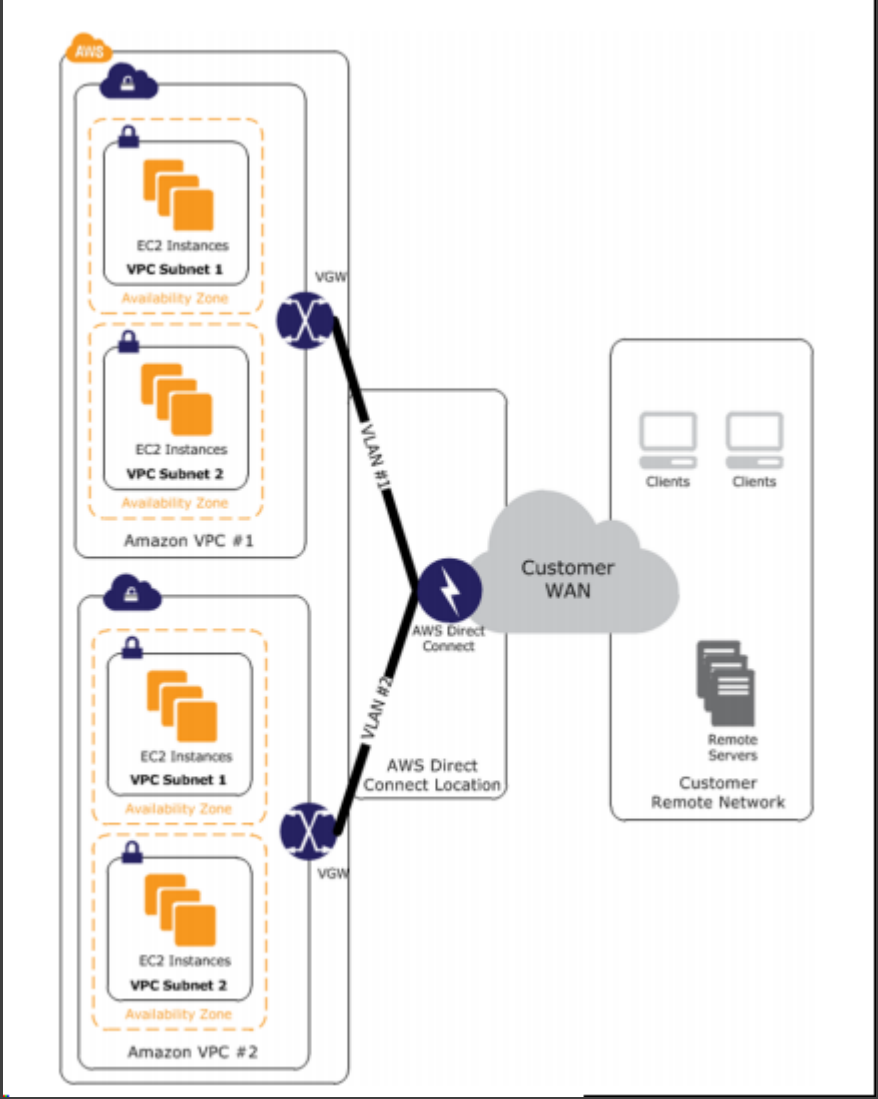
- Amazon VPC provides the flexibility to combine the hardware VPN and software VPN options to connect multiple VPCs.
- With this design, you can create secure VPN tunnels between a software VPN appliance and a virtual private gateway to connect multiple VPCs into a larger virtual private network, allowing instances in each VPC to seamlessly connect to each other using private IP addresses.
- This option is recommended when you want to connect VPCs across multiple AWS regions and would like to take advantage of the AWS-managed hardware VPN endpoint including automated multidata center redundancy and failover built into the VGW side of the VPN connection.
- This option uses a virtual private gateway in one Amazon VPC and a combination of an Internet gateway and software VPN appliance in another Amazon VPC

Software-to-Hardware VPN



- Amazon VPC provides the option of creating a hardware IPsec VPN to connect your remote networks with your Amazon VPCs over the Internet. You can leverage multiple hardware VPN connections to route traffic between your Amazon VPCs
- We recommend this approach when you want to take advantage of AWS-managed VPN endpoints including the automated multidata center redundancy and failover built into the AWS side of each VPN connection.
- the Amazon VGW represents two distinct VPN endpoints, physically located in separate data centers to increase the availability of each VPN connection.
- Amazon VGW also supports multiple customer gateway connections allowing you to implement redundancy and failover on your side of the VPN connection
- This solution can also leverage BGP peering to exchange routing information between AWS and these remote endpoints. You can specify routing priorities, policies, and weights (metrics) in your BGP advertisements to influence the network path traffic will take to and from your network(s) and AWS
- This solution can also leverage BGP peering to exchange routing information between AWS and these remote endpoints. You can specify routing priorities, policies, and weights (metrics) in your BGP advertisements to influence the network path traffic will take to and from your network(s) and AWS

AWS Direct Connect



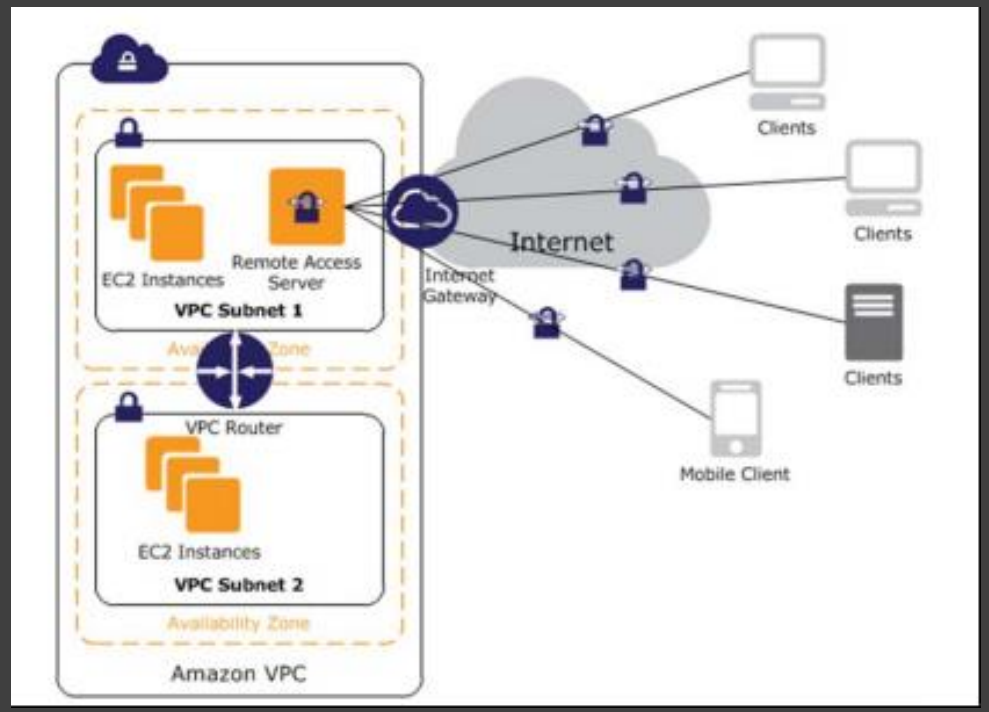
- AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to your Amazon VPC or among Amazon VPCs. This option can potentially reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than the other VPC-to-VPC connectivity options.
- You can divide a physical AWS Direct Connect connection into multiple logical connections, one for each VPC. You can then use these logical connections for routing traffic between VPCs
- you can connect AWS Direct Connect locations in other regions using your existing WAN providers and leverage AWS Direct Connect to route traffic between regions over your WAN backbone network.
- We recommend this approach if you're already an AWS Direct Connect customer or would like to take advantage of AWS Direct Connect's reduced network costs, increased bandwidth throughput, and more consistent network experience
- . AWS Direct Connect can provide very efficient routing since traffic can take advantage of 1 GB or 10 GB fiber connections physically attached to the AWS network in each region. Additionally, this service gives you the most flexibility for controlling and managing routing on your local and remote networks, as well as the potential ability to reuse AWS Direct Connect connections.

Internal User-to-Amazon VPC Connectivity Options

Course and Labs

- Internal user access to Amazon VPC resources is typically accomplished either through your network–to-Amazon VPC options or the use of software remote-access VPNs to connect internal users to VPC resources
- With the former option, you can reuse your existing on-premises and remote-access solutions for managing end-user access, while still providing a seamless experience connecting to AWS hosted resources.
- With software remote-access VPN, you can leverage low cost, elastic, and secure Amazon Web Services to implement remote-access solutions while also providing a seamless experience connecting to AWS hosted resources
- In addition, you can combine software remote-access VPNs with your network-to-Amazon VPC options to provide remote access to internal networks if desired. This option is typically preferred by smaller companies with less extensive remote networks or who have not already built and deployed remote access solutions for their employees.

Software Remote-Access VPN



- You can choose from an ecosystem of multiple partners and open source communities that have produced remote-access solutions that run on Amazon EC2.
- Remote-access solutions range in complexity, support multiple client authentication options (including multifactor authentication) and can be integrated with either Amazon VPC or remotely hosted identity and access management solutions (leveraging one of the network-to-Amazon VPC options) like Microsoft Active Directory or other LDAP/multifactor authentication solutions.
- As with the software VPN options, the customer is responsible for managing the remote access software including user management, configuration, patches and upgrades. Additionally, please note that this design introduces a potential single point of failure into the network design as the remote access server runs on a single Amazon EC2 instance

VPC Endpoints

- A VPC endpoint enables you to create a private connection between your VPC and another AWS service without requiring access over the Internet, through a NAT device, a VPN connection, or AWS Direct Connect. Endpoints are virtual devices.
- They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and AWS services without imposing availability risks or bandwidth constraints on your network traffic.
- Currently, we support endpoints for connections with Amazon S3 within the same region only.
- An endpoint enables instances in your VPC to use their private IP addresses to communicate with resources in other services.
- Your instances do not require public IP addresses, and you do not need an Internet gateway, a NAT device, or a virtual private gateway in your VPC. You use endpoint policies to control access to resources in other services. Traffic between your VPC and the AWS service does not leave the Amazon network.