
aws
certified
Solutions
Architect
Professional
DOLFINed

AWS VIRTUAL PRIVATE CLOUD (VPC)

YOU CAN DO IT TOO!

VPC REFRESHER

VPC IP Addressing

AWS Virtual Private Cloud (VPC)

VPC IP Addressing

- The CIDR block is the range of IP addresses that you choose for the VPC when you create it
- Once the VPC is created, you can NOT change its main CIDR block range
  - But you can expand the VPC CIDR block by adding additional CIDR blocks
  - Some restrictions apply
- If you need a different main CIDR block range, create a new VPC
- The different subnets within a VPC can NOT overlap (basic TCP/IP rule)

AWS Virtual Private Cloud (VPC)

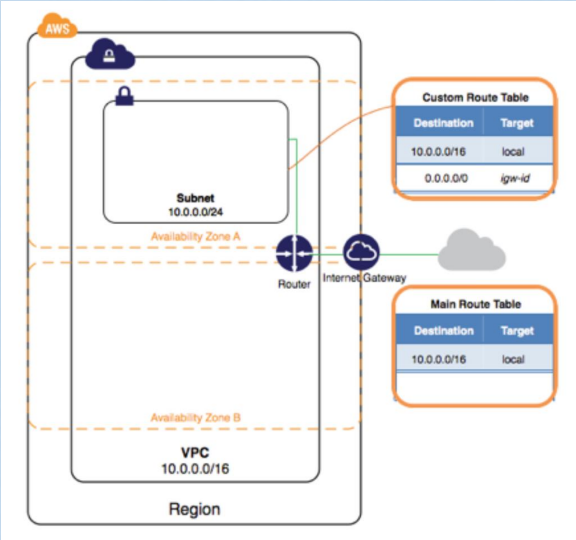
AWS Reserved IP's in each subnet

- First 4 IP addresses in each subnet and the last one are reserved by AWS
  - Ex. If the subnet is 10.0.0.0/24
    - 10.0.0.0 is the base network
    - 10.0.0.1 VPC router
    - 10.0.0.2 DNS related
    - 10.0.0.3 Reserved for future use
    - 10.0.0.255 last IP

AWS Virtual Private Cloud (VPC)

Internet Gateway

- Is the gateway through which your VPC communicates with the internet, and with other AWS services
- Is a horizontally scaled, redundant, and highly available VPC component
- It performs NAT (static one-to-one) between your Private IPv4 addresses in your VPC and the allocated Public (or Elastic) IPv4 addresses
- It supports both IPv4 and IPv6
- You can not SSH or connect to it, it is fully managed by AWS



Source: aws.amazon.co

AWS Virtual Private Cloud (VPC)

Public Subnet vs. Private Subnet

- Public Subnet means:
  - Its VPC has an Internet gateway attached to it
  - It is associated with a route table that has an entry for a default route pointing at the VPC's Internet gateway
    - Destination 0.0.0.0/0 Target: igw-1234

- Any subnet that does not satisfy either or both of the conditions above is considered a private subnet by AWS definition
  - Private subnet means, it is not accessible from the Internet since it has not Public Internet IP addresses configured.

AWS Virtual Private Cloud (VPC)

Elastic IP addresses

- Elastic IPs are Internet routable IP addresses that you can have allocated to your VPC, and will continue being allocated to your VPC until you decide to release them back to AWS
- Some AWS services (example NAT gateway) require an Elastic IP address to function
- You have 5 Elastic IP addresses per region (Soft limit that you can change by contacting AWS)
- Public IPv4 addresses on the other hand, are DHCP based (dynamically allocated) to your Compute, and are released back to AWS if you stop your compute instance.

AWS Virtual Private Cloud (VPC)

Elastic IP addresses – AWS Charges

- You are not charged for a used Elastic IP, but if you are not using it.
  - Example if when an Elastic IP is attached to a stopped EC2 instance (virtual server) or detached and left un-used you start to be charged

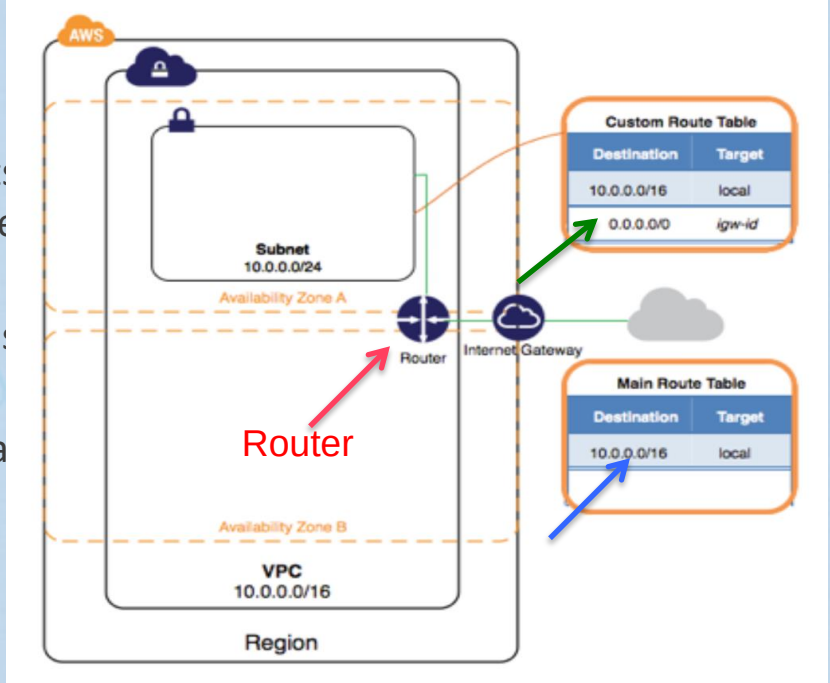
- If you have attached more than one Elastic IP address to a running EC2 instance, you get charged for all except one (the one you are entitled to use for free)

Implied Router / Route Tables

AWS Virtual Private Cloud (VPC)

Implied Router

- It is the central VPC routing function,
- It connects the different AZ's together and connects the VPC to the Internet Gateway (and Virtual Private Gateway when configured)
- Each subnet will have a route table the router uses to forward traffic within the VPC
- The route tables can also have entries to externa destinations



Source: aws.amazon.co

Review Topic : VPC Security

NACLs vs. Security Groups

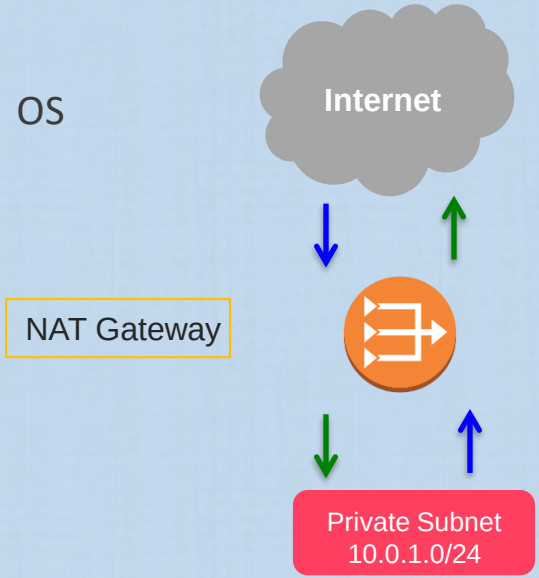
Security Group	Network ACL
Operates at the instance level (first layer of defense)	Operates at the subnet level (second layer of defense)
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so you don't have to rely on someone specifying the security group)

Source: aws.amazon.com

Review Topic : VPC

NAT Gateway

- Is an AWS managed service (Highly available, redundant..etc)
  - Customer does not need to worry about patching or OS updates
- Can not be assigned a security group
- AWS is responsible for its security/patching…etc
- Can scale to 10s of Gbps throughput
- Works only with an Elastic IP, can Not use a Public IP to do its function
  - NAT instances can work with Public and Elastic IP addresses

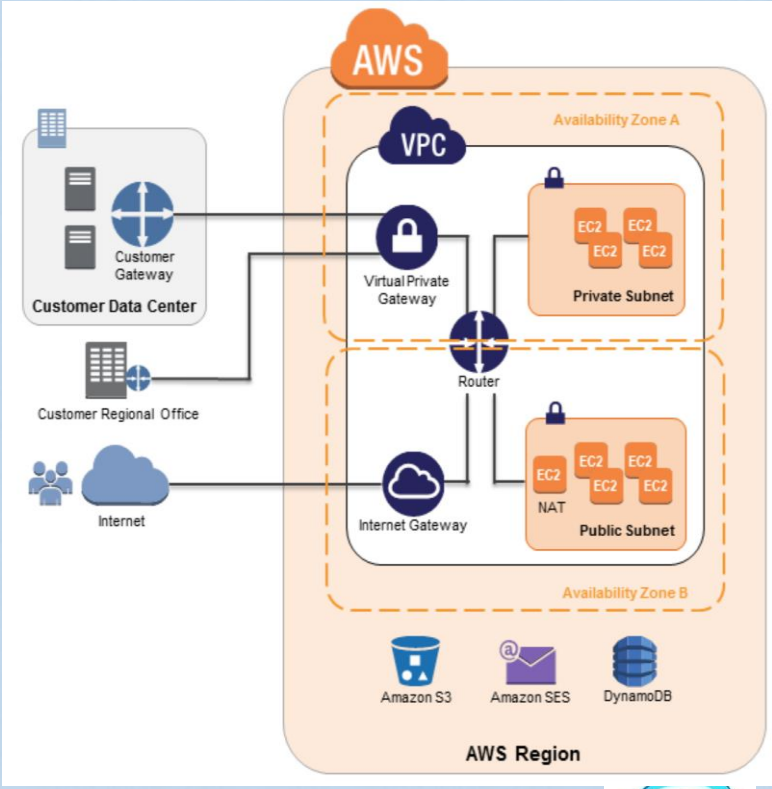


Virtual Private Networks (VPN)

Review Topic : VPC

Virtual Private Networks (VPN)

- A secure connection over the Internet or Direct Connect between On-Premise and AWS
- VPN connections are quick, easy to deploy, and cost effective
- A VGW is required on the VPC side, and a Customer gateway on the client's data center (locations) side
- An Internet routable IP address is required on your Customer gateway
- Two tunnels are configured for each VPN connection for redundancy
- You can NOT use the NAT gateway in your VPC through the VPN connection



Source: aws.amazon.com

AWS Virtual Private Cloud (VPC)

Enabling Dynamic Route Propagation

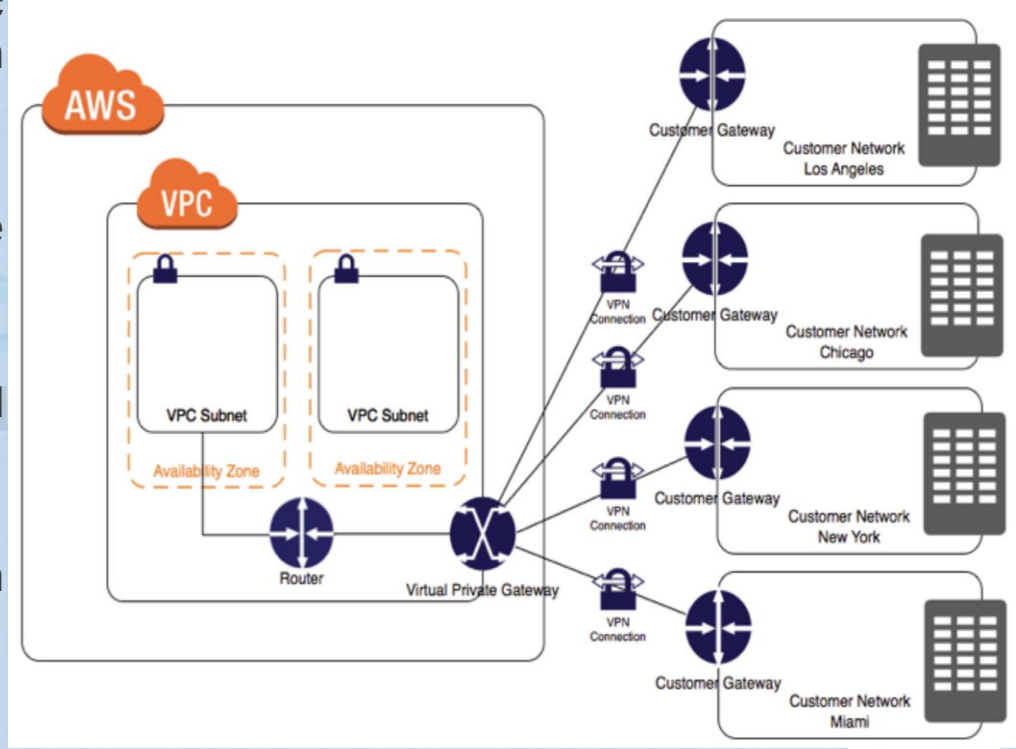
- To allow the VPC subnet(s) to communicate with the on premise subnets, you need to update the route table(s) of the subnet(s) in the VPC to point to the VGW

- Alternatively, you can enable route propagation in these route tables such that, routes the VGW learns over the VPN connection, are dynamically propagated to the route table pointing at the VGW as the next hop (Target)
  - Less manual tasks

AWS Virtual Private Cloud (VPC)

AWS VPN CloudHub

- You can **have up to 10 IPSec** connections per VGW (soft limit can be increased by contacting AWS)
- VPN based Hub and Spoke connectivity to a common VGW
- Can mix DX connections (explained next) with VPN connections
- Spokes can communicate with each other and with the VPC



Source: aws.amazon.com

AWS Virtual Private Cloud (VPC)

VPN – Allowed IP Prefixes

Which IP prefixes can receive/send traffic through the VPN connection?

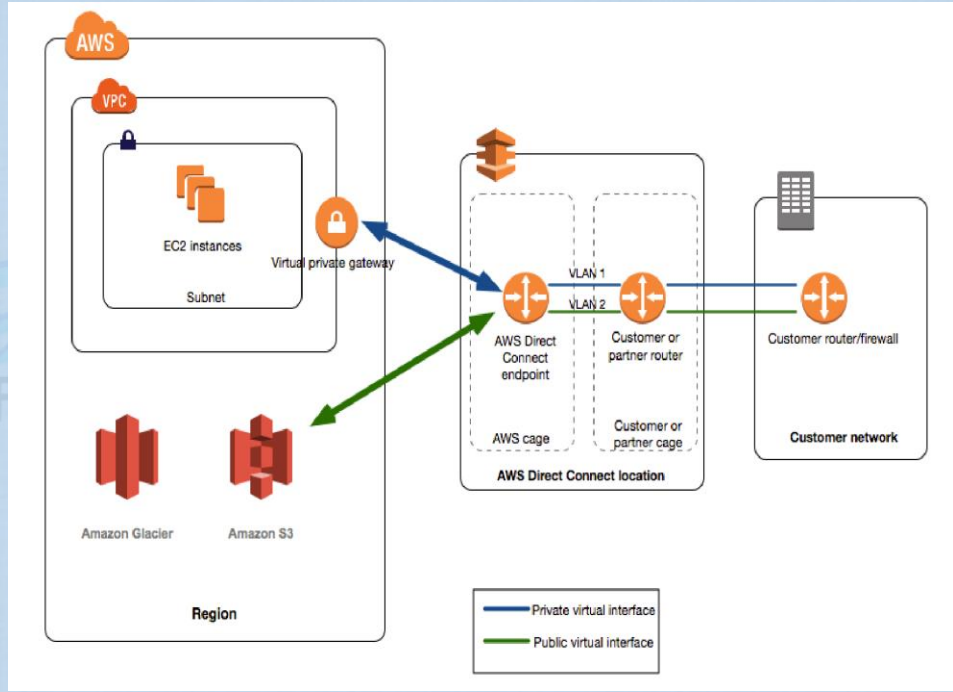
- Only IP prefixes that are known to the virtual private gateway,
- VGW learns about these prefixes through Static or BGP routing
- VGW does not route any other traffic destined outside of the received BGP advertisements, static route entries, or its attached VPC CIDR
- You can NOT access Elastic IPs on your VPC side using the VPN tunnel established, Elastic IPs in AWS can only be accessed from the Internet
- You can NOT use a NAT gateway in your VPC over the VPN connection

DIRECT CONNECT DX

VPC Direct Connect (DX)

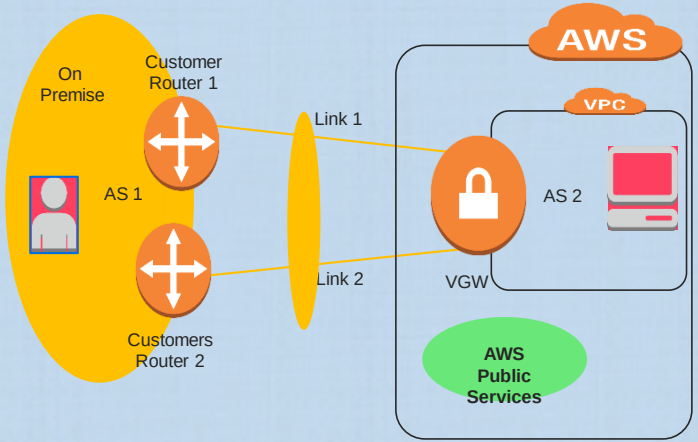
AWS Direct Connect (DX)

- It is a direct connection (not internet based) **and provides for higher speeds (bandwidth), less latency and higher performance** than Internet
- Border Gateway Routing Protocol must be used to route between then two ends of the DX connection.
- Customer Router must be capable of 802.1Q and BGP
- You can use the connection to establish Private Virtual Interfaces (VIFs) to connect to a VPC in the region (via the VPC's VGW)
- You can establish multiple Private VIFs to multiple VPCs in a region (one per VPC)
- You can establish Public VIF to connect to any public AWS endpoints in ANY region
- Supports both IPv4 and IPv6 (requires public VIFs)
- All networking traffic remains on the AWS global network backbone, regardless of whether you access public AWS services or a VPC in another Region.
- Any data transfer out of a remote Region is billed at the remote Region data transfer rate.



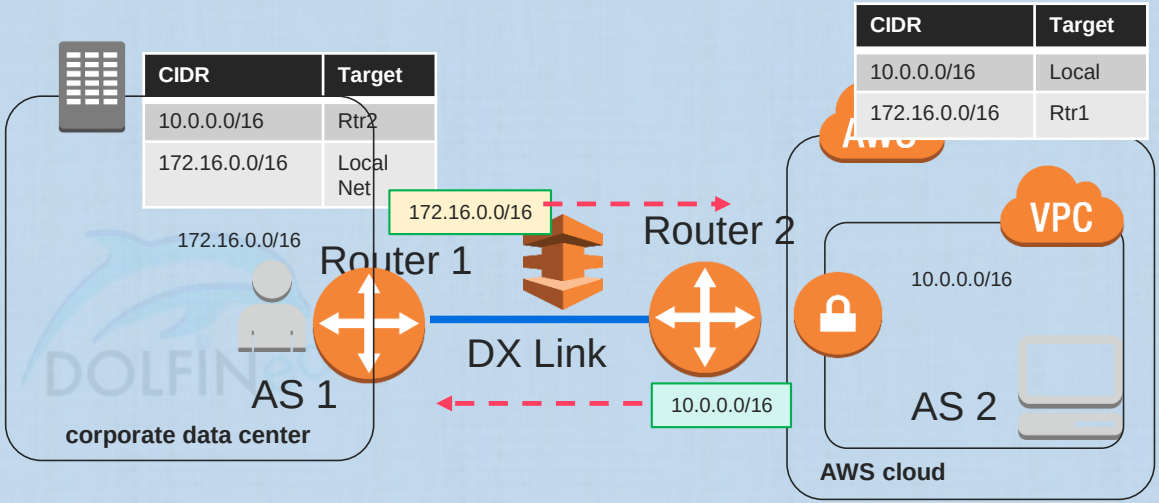
Link Aggregation Groups - LAGs

- A link aggregation group (LAG) is a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection.
  - All connections in a LAG operate in active/active mode.
- You can create a LAG from existing connections, or you can provision new connections. After you've created the LAG, you can associate existing connections (whether standalone or part of another LAG) with the LAG.
- The following rules apply:
  - All connections in the LAG must use the same bandwidth.
  - You can have a maximum of four connections in a LAG.
  - All connections in the LAG must terminate at the same AWS Direct Connect endpoint.



BGP and Hybrid Connectivity

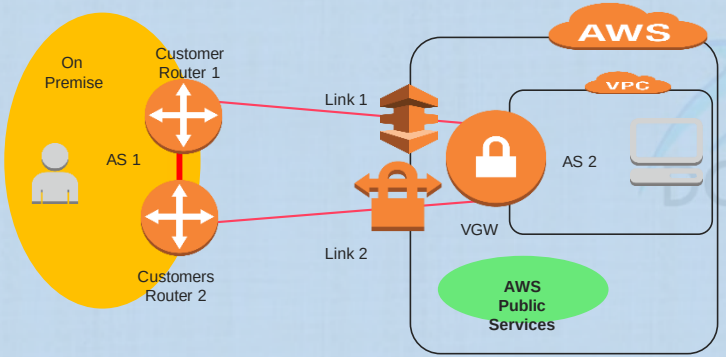
- BGP between Corporate Data Center and AWS VPC configured using a direct connect link
- BGP setup, Routing updates are propagated dynamically
- Each side builds its own route table based on these updates and BGP communities configured, if any.
- BGP is the only routing option on Direct connect links
- You can only have one default route (0.0.0.0/0) per routing table
- Route propagation can be used to have the VGW send the Customer side routes to the respective VPC private or vpn-only subnet's route table
  - As an alternative you can manually configure entries in the



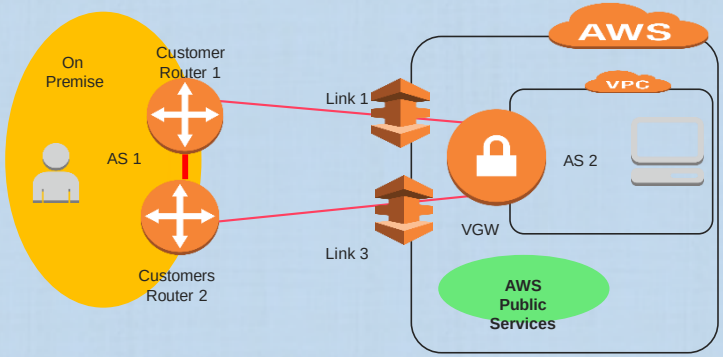
AWS Direct Connect HA

- Can be achieved by two Direct connection connections
  - By manipulating BGP, they can be in Active/Active or Active/Standby configuration

- A VPN connection can also be used as the standby or backup connection if the Direct connect one fails



Failover



Active/Active Or Failover

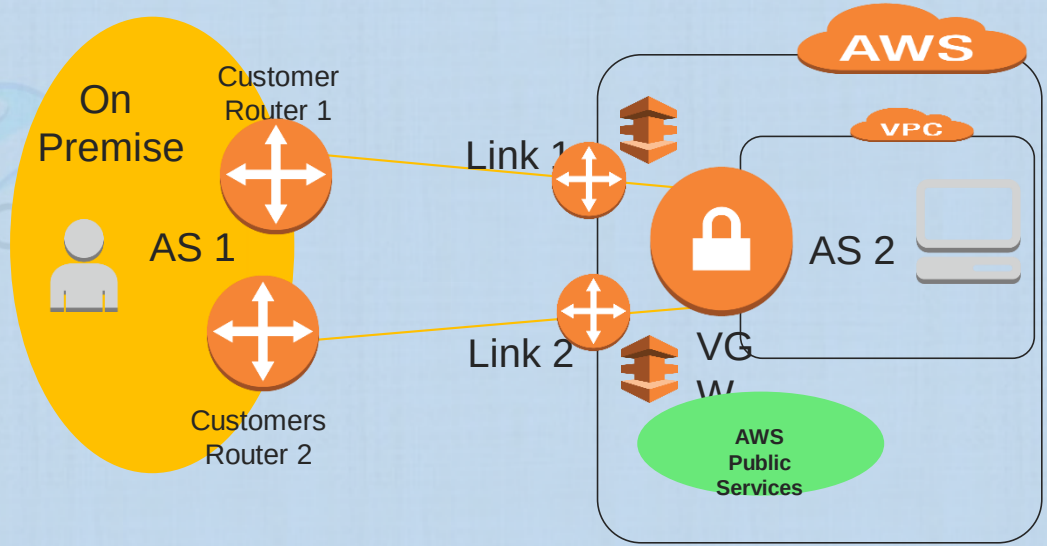
VPC Direct Connect (DX)

- BGP Communities
- DX Routing Manipulation

Border Gateway Protocol (BGP) – Communities and Attributes

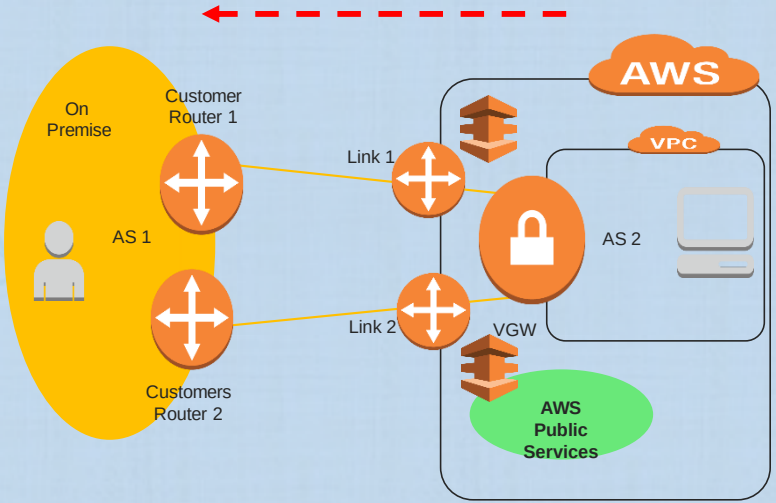
- AWS Direct Connect applies inbound and outbound routing policies for a public AWS Direct Connect connection.

- **Inbound Policies:**
  - Client must own the public prefixes and they must be registered as such.
  - Traffic must be destined to Amazon public prefixes.
    - Transitive routing between connections is not supported.
  - AWS Direct Connect performs inbound packet filtering to validate that the source of the traffic originated from your advertised prefix.



AWS Direct Connect – BGP Communities in Outbound Policies – AWS Side

- AWS Direct Connect advertises all local and remote AWS Region prefixes where available and includes on-net prefixes from other AWS non-Region points of presence (PoP) where available; for example, CloudFront and Route 53.
  - No access to non-Amazon prefixes (i.e no access to the global internet over the direct links).
- AS_PATH is used to determine the routing path, and **AWS Direct Connect is the preferred path** for traffic sourced from Amazon (Preference over HA VPN links)
- Only public ASNs are used internally for route selection.
- AWS Direct Connect advertises prefixes with a minimum path length of 3.
- AWS Direct Connect advertises all public prefixes with the well-known NO_EXPORT BGP community.
  - The prefixes advertised by AWS Direct Connect must not be advertised beyond the network boundaries of your connection.



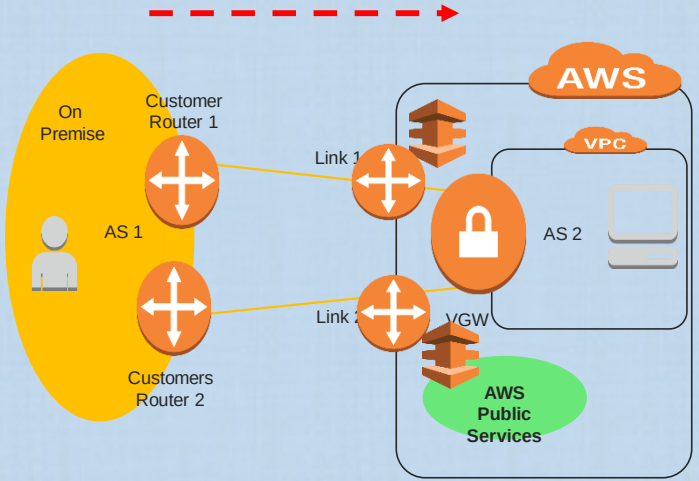
AWS Direct Connect – BGP Communities – On Premise side

Scope BGP Communities

- BGP community tags can be applied on the public prefixes that you advertise to Amazon to indicate how far to propagate your prefixes in the Amazon network
  - For the local AWS Region only, all Regions within a continent, or all public Regions.
  - If community tags are applied, prefixes are advertised to all public AWS Regions (global) by default.

Local Preference BGP Communities

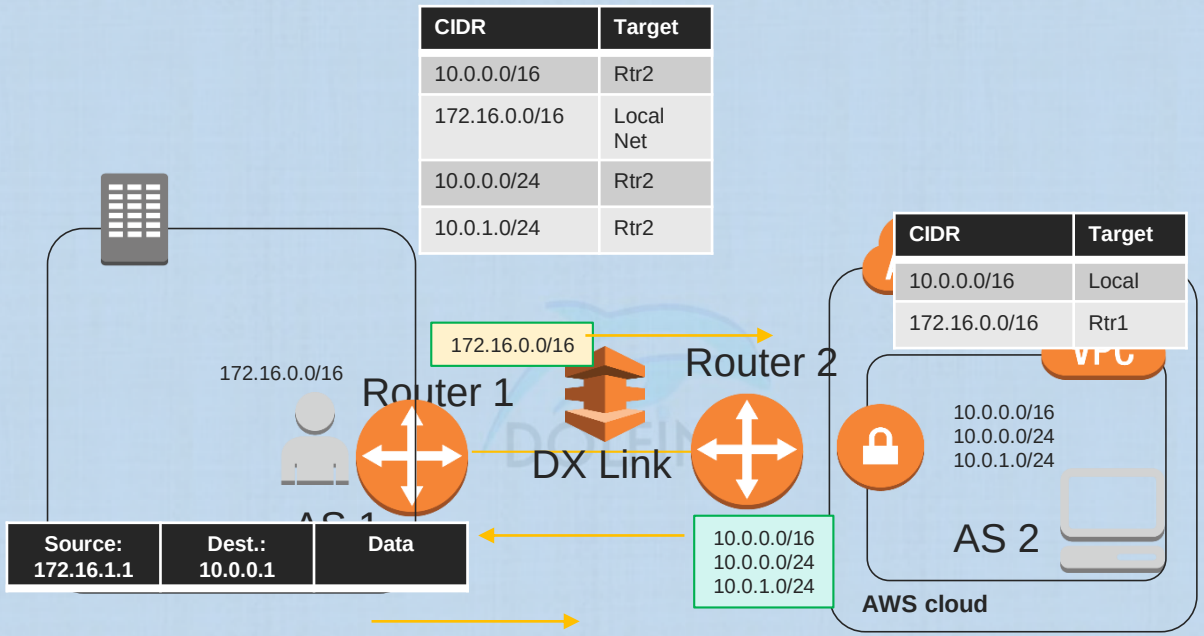
- **Local preference BGP community tags are supported for private virtual interfaces, and transit virtual interfaces.**
- Local preference BGP community tags can be used to achieve load balancing and route preference for incoming traffic(sourced from AWS).
- For each advertised prefix over a BGP session, a community tag can be applied to indicate the priority of the associated path for returning traffic.
- To load balance traffic across multiple AWS Direct Connect connections, apply the same community tag across the prefixes for the connections.
- To support failover across multiple AWS Direct Connect connections, apply a community tag with **a higher preference to the prefixes for the primary or active virtual interface.**



VPC Direct Connect (DX)

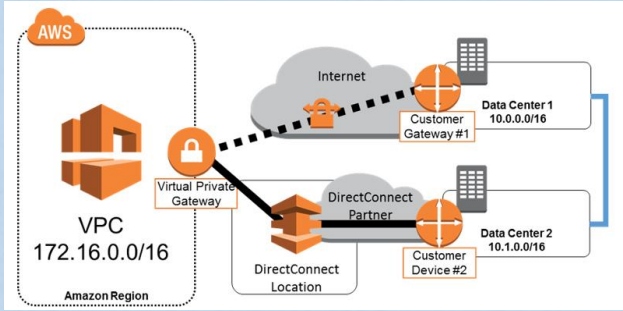
- **Route Priority Processing**

Routing Processing – Longest Prefix Match

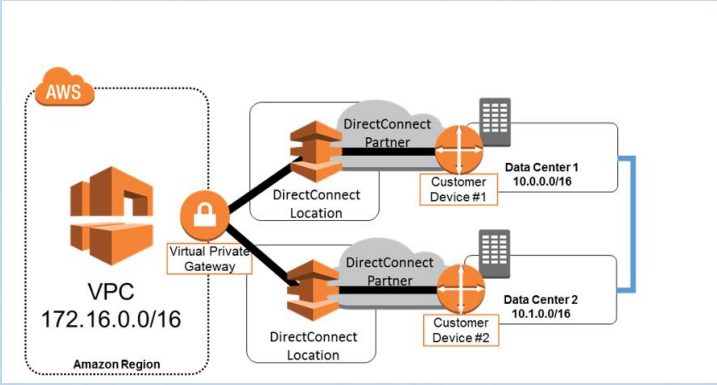


Route Tables and Route Priority - From AWS to On Premise

- Route tables determine where network traffic is directed.
- A route(s) must be added in the VPC route table (for the CIDRs on premise that will be reached from the VPC), the VGW will be the Target (next hop)
  - This is true for both VPN and Direct Connect VPC connectivity
- Alternatively, route propagation can be enabled for the route table to automatically propagate the on premise CIDRs (received via BGP or configured by Static routes on the VGW (VPN case) to the table.



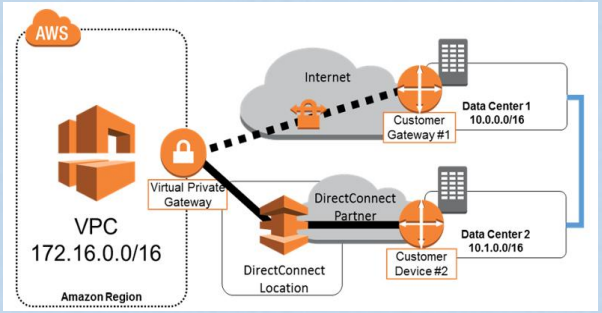
- If overlapping routes within a Site-to-Site VPN connection and longest prefix match cannot be applied, then AWS prioritize the routes as follows, from most preferred to least preferred:
  - BGP propagated routes from an AWS Direct Connect connection
  - Manually added static routes for a Site-to-Site VPN connection
  - BGP propagated routes from a Site-to-Site VPN connection

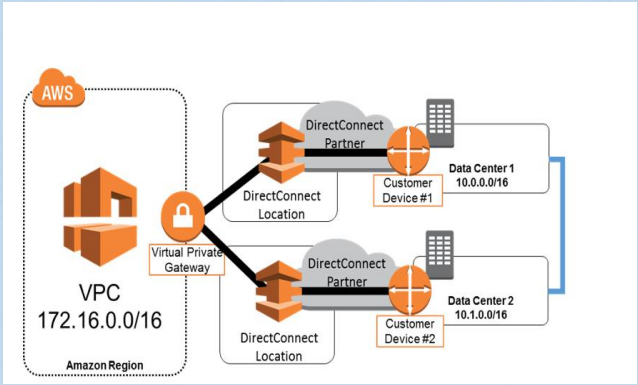


Traffic Forwarding - From AWS to On Premise

- When a virtual private gateway (VGW) receives routing information, it uses **path selection** to determine how to route traffic to your remote network.
- First it applies **Longest prefix match** applies;
- If all routes are of equal length (subnet mask) then, the following rules apply:
  - If any propagated routes from a Site-to-Site VPN connection or AWS Direct Connect connection **overlap** with the local route for your VPC,
    - Forwarding will use the local route is most preferred even if the propagated routes are more specific.
  - If any propagated routes from a Site-to-Site VPN connection or AWS Direct Connect connection have the same destination CIDR block as other existing static routes, AWS prioritizes the static routes whose targets are an Internet gateway, a virtual private gateway, a network interface, an instance ID, a VPC peering connection, a NAT gateway, or a VPC endpoint.

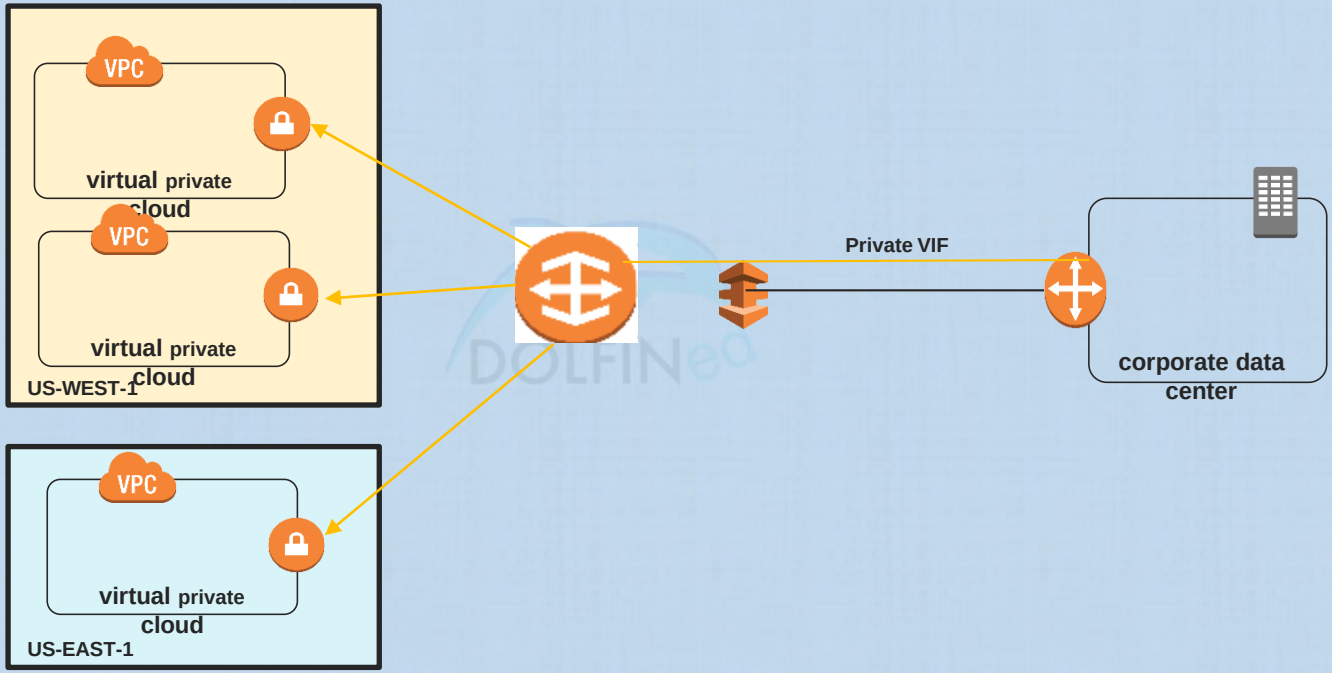
- Only IP prefixes that are known to the virtual private gateway, whether through BGP advertisements or static route entry, can receive traffic from your VPC.
  - The virtual private gateway does not route any other traffic destined outside of received BGP advertisements, static route entries, or its attached VPC CIDR.





DIRECT CONNECT GATEWAY

AWS Direct Connect Gateway – Why do we need it?

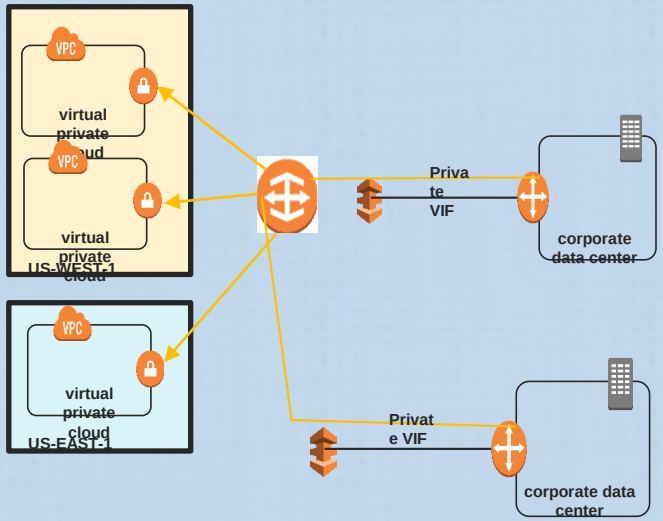


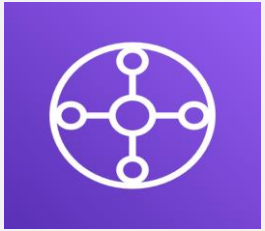
AWS Direct Connect Gateway

- A Direct Connect gateway is a globally available resource.
  - You can create the Direct Connect gateway in any public Region and access it from all other public Regions.
- Use AWS Direct Connect gateway to connect your VPCs.
- You associate an AWS Direct Connect gateway with either of the following gateways:
  - A virtual private gateway(s) of the VPC(s) you need to connect to
  - A transit gateway when you have multiple VPCs in the same Region
- Create a private virtual interface (Private VIF) for your AWS Direct Connect connection to the Direct Connect gateway.
  - You can attach multiple private virtual interfaces to your Direct Connect gateway (from different locations or from different DX links connected to different Customer Gateways).
- You can associate a VGW from one account with a Direct Connect Gateway from another account, by creating association proposal from the Direct Connect Gateway in one account to the VGW in the other account.

AWS Direct Connect Gateway - Limitations

- The VPCs to which you connect through a Direct Connect gateway cannot have overlapping CIDR blocks.
- You cannot create a public virtual interface to a Direct Connect gateway.
- A Direct Connect gateway supports communication between attached private virtual interfaces and associated virtual private gateways only.
- The following traffic flows are not supported:
  - Direct communication between the VPCs that are associated with the Direct Connect gateway.
  - Direct communication between the virtual interfaces that are attached to the Direct Connect gateway.
  - Direct communication between a virtual interface attached to a Direct Connect gateway and a VPN connection on a virtual private gateway that's associated with the same Direct Con
- You cannot associate a virtual private gateway with more than one Direct Connect gateway and you cannot attach a private virtual interface to more than one Direct Connect gateway.
- A virtual private gateway that you associate with a Direct Connect gateway must be attached to a VPC





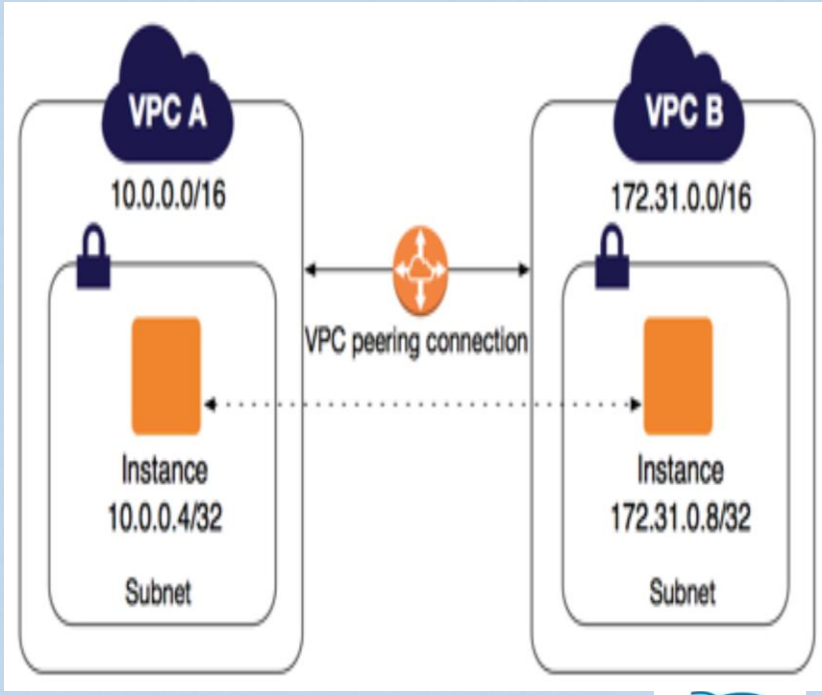
VPC PEERING & TRANSIT GATEWAY

VPC Peering

Review Topic : VPC

VPC Peering

- By default a VPC can not communicate with any other VPC through Private IPv4 addresses, even if the other VPC belongs to the same AWS account.
- To allow two VPCs to communicate you need to configure a VPC Peering connection
- A VPC peering connection is a highly available networking connection between two VPCs that enables routing traffic between them using private IPv4 addresses or IPv6 addresses.
- Instances in either VPC can communicate with each other as if they are within the same network.

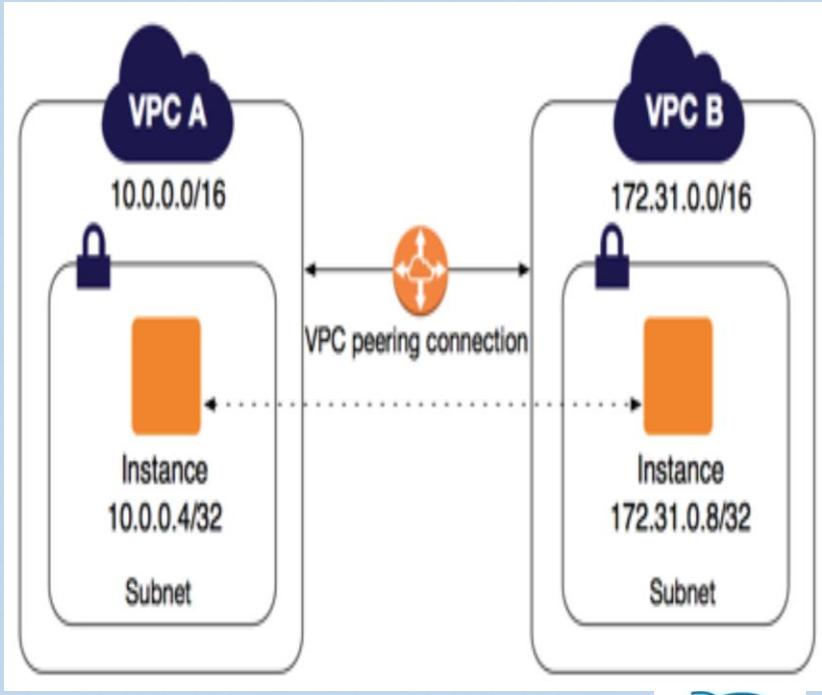


Source: aws.amazon.com

Review Topic : VPC

VPC Peering

- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within the same region, or between AWS regions.
- There is no single point of failure in the VPC Peering connection, so you need not worry about creating two VPC Peering connections for redundancy or high availability.
- For the connection to be established:
  - There MUST not be any overlapping IP ranges between the two VPCs
  - Request from a VPC has to be initiated
  - An accept from the other VPC has to be done
  - Routing and Security Groups/NACLs has to be updated to allow traffic both ways

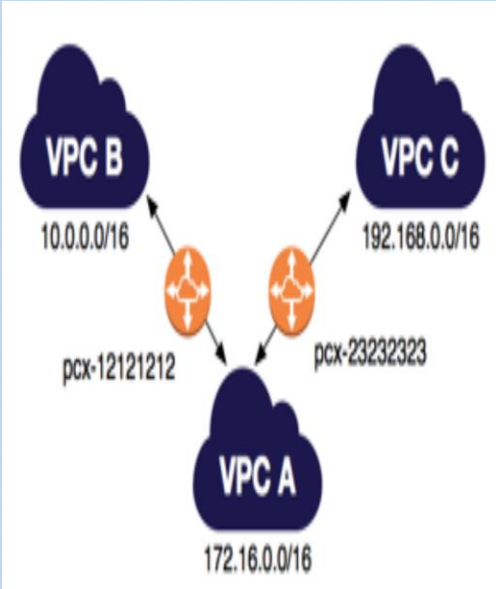


Source: aws.amazon.com

Review Topic : VPC

VPC Peering

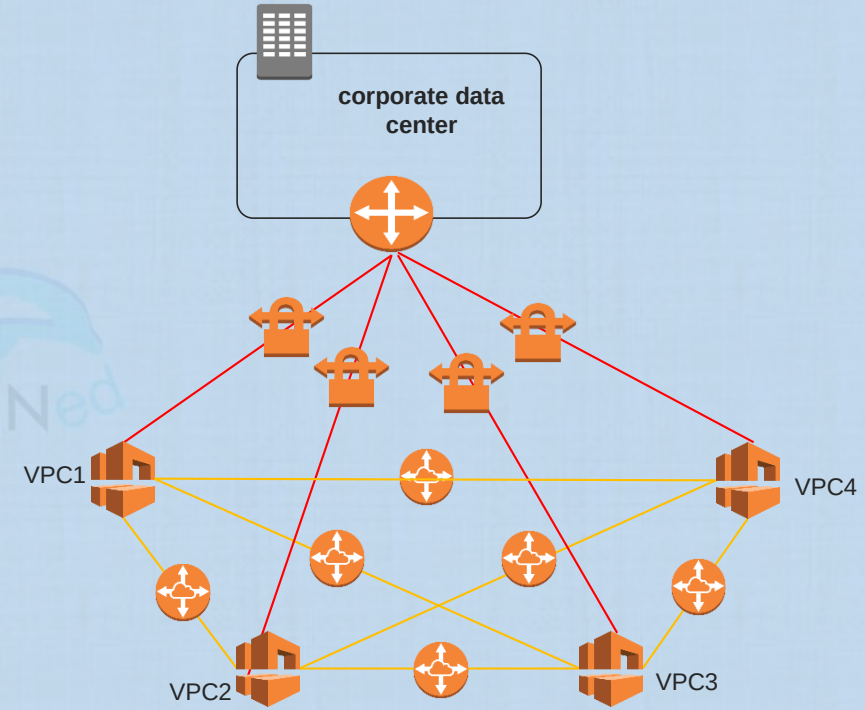
- You can reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group rules.
- A VPC peering connection is a one to one relationship between two VPCs. You can create multiple VPC peering connections for each VPC that you own
- Transitive peering relationships are not supported:
  - You do not have any peering relationship with VPCs that your VPC is not directly peered with.
- You cannot have more than one VPC peering connection between the same two VPCs at the same time.



Source: aws.amazon.com

AWS VPC Peering - Limitations

- VPC Peering is non transitive
- To allow 4 VPCs to talk to each other,
  - You need a full mesh among them
    - That is n (n-1) / 2 VPC peerings
    - 6 peering connection are required
    - What if these were 20 or 30 VPCs

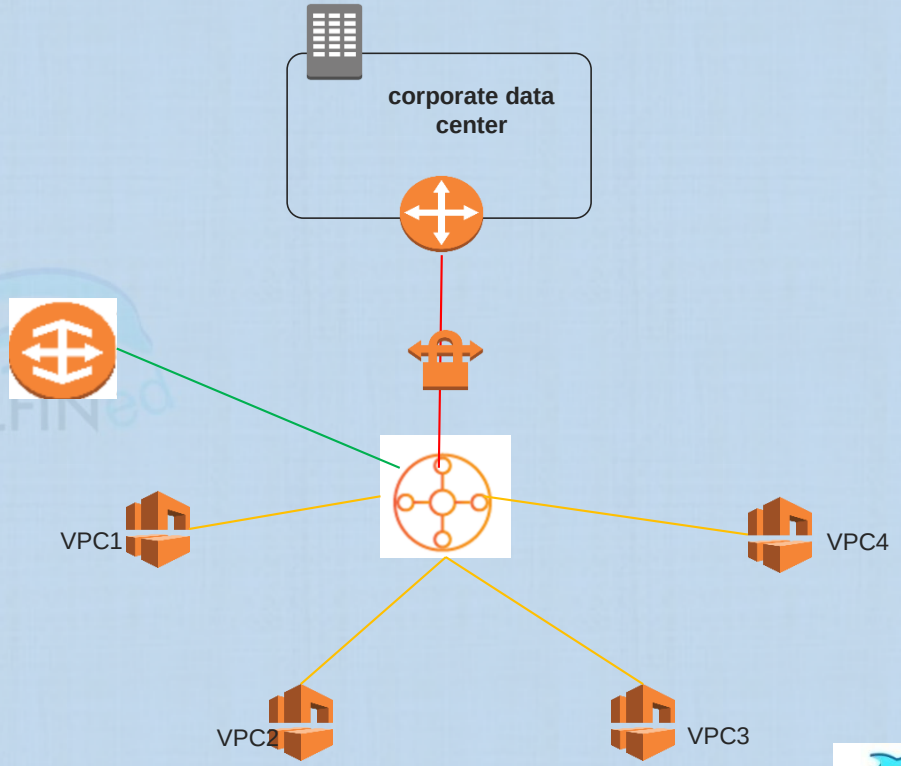


AWS Transit Gateway

- **Routing Use cases**

AWS Transit Gateway

- A *transit gateway* is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks.
- It is a regional resource
- VPCs can communicate with one another, and with On-premise CIDR blocks by default.
- This can be changed by creating multiple route tables, associated different VPCs with different routing tables to limit/control who talks to whom
- A Transit Gateway can be associated across accounts.



AWS Transit Gateway Concepts

- **Attachment**
  - A VPC, an AWS Direct Connect gateway, or a VPN connection can be attached to a transit gateway.

- **Transit gateway route table**
  - A transit gateway has a default route table and can optionally have additional route tables.
  - A route table includes dynamic and static routes that decide the next hop based on the destination IP address of the packet.
  - The target of these routes could be a VPC or a VPN connection.
  - By default, the VPCs and VPN connections that are attached to a transit gateway are associated with the default transit gateway route table.

AWS Transit Gateway

- **Associations**
  - Each attachment is associated with exactly one route table.
  - Each route table can be associated with zero to many attachments.

- **Route propagation**
  - A VPC or VPN connection can dynamically propagate routes to a transit gateway route table.
  - With a VPC, you must create static routes to send traffic to the transit gateway.
  - With a VPN connection, routes are propagated from the transit gateway to your on-premises router using Border Gateway Protocol (BGP).

AWS Transit Gateway

- It supports RAM, hence, it can be shared between accounts
- It is enabled per AZ
- Regional resource
- It supports IPv6
- Questions:
  - Can I use security groups as sources?
  - Limits:
    - 5 Transmit Gateways per VPC
    - 50 Gbps per VPC
    - 1.25 Gbps per VPN attachment

AWS VPC Peering Routing Use Case

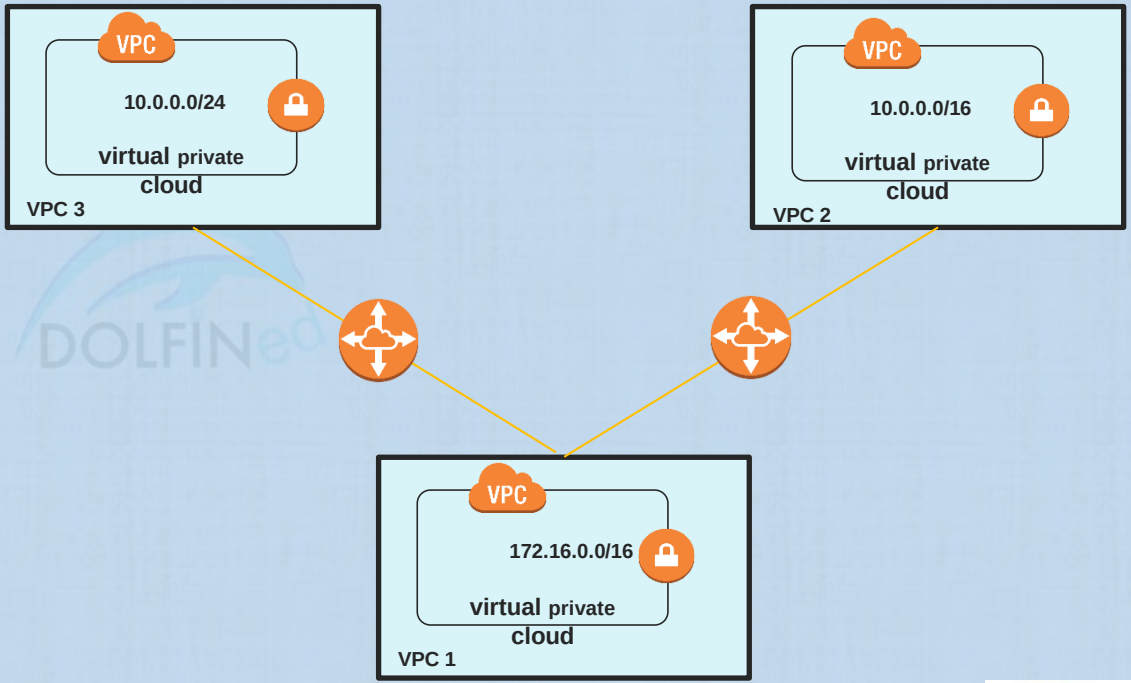
- VPC1 is peering with VPC2 and VPC3

- VPC 1 CIDR : 172.16.0.0/16
- VPC2 CIDR : 10.0.0.0/16
- VPC3 CIDR : 10.0.0.0/24

- You need to connect to a DB server in VPC3 from VPC1, the DB server has the IP address 10.0.0.1

- How can you achieve this?

- Answer: Configure a static route in the route table of the subnet(s) in VPC1 that needs to connect to the DB server in VPC3, using 10.0.0.0/24 as destination



AWS Elastic Compute Cloud (EC2)

- EC2 Optimized Instances and Enhanced Networking
- Placement Groups

Review Topic : Elastic Compute Cloud

EC2 – EBS optimized instances

- EBS optimized EC2 instances enable the full use of an EBS volume's provisioned IOPS
  - They deliver dedicated performance between EC2 instances and their attached EBS volumes
  - Are designed to work with all EBS volume types
    - This is all about high performance data transfer between EC2 instances and their attached EBS volumes
- For supported instance types, SR-I/OV provides:
  - Higher packet per second (PPS) performance for data transfers
  - Lower latency
  - Very low network Jitter
- EC2 enhanced networking can be enabled on EBS-backed or Instance Store-backed instances
- EC2 enhanced networking can function across Multi-AZ

Review Topic : Elastic Compute Cloud

EC2 – Placement Group Types

Cluster Placement groups

- Clustering of EC2 instances in a single availability zone
- EC2 instances in the cluster can use the full 10Gbps speeds, and 100Gbps aggregate speed without any oversubscription
- Use for application that require low latency and/or high throughput between nodes
- Use SR-I/OV (Single Root I/O Virtualization) based enhanced networking instances for placement groups
- It can also be created across a VPC peering connections

Spread Placement Groups:

- Launched each instance in the group in a different rack
- Can be in a single or multiple Availability zones in the same region
- Maximum of 7 running instances per AZ per group
- If the request fails because of insufficient capacity, try again later

Review Topic : Elastic Compute Cloud

EC2 – Placement Group Types

Partition Placement Groups:

- AWS tries to launch your group instances into different logical entities called partitions
- Partition is launched in a separate rack to minimize the impact of a failure
- Partition placement groups can be in a single or multiple availability zones in the same region
- Maximum of 7 partitions per AZ
- Ideal for Hbase, HDFS, and Cassandra
- You get visibility into which Instances are in which partitions
- If the request fails because of insufficient capacity, try again later

AWS Elastic Compute Cloud (EC2)

EC2 Bastion Hosts

EC2 – Bastion Hosts (for Linux instances)
Remote Desktop (for Windows Instances)

- For inbound, secure, connectivity to your VPC to manage and administer public and/or private EC2 instances, you can use a bastion host (or a jump box/stone).
  - The Bastion host is an EC2 instance, whose interfaces will have a security group allowing inbound SSH access for Linux EC2 instances or inbound RDP access for windows instances
  - Bastion hosts can have auto-assigned public IP addresses or Elastic IP addresses (Elastic IPs are better for security reasons and to fix the IP address)
  - Using Security groups you can further limit which IP CIDRs can access the Bastion Host.
  - Once logged to the Bastion host, you can connect via RDP (Windows) or SSH (Linux) to the EC2 instance(s) you desire to manage

AWS Elastic Compute Cloud (EC2)

EC2 ENI

Review Topic : Elastic Computer Cloud (EC2)

Elastic Network Interfaces (ENI) - Attributes

- Each Elastic Network Interface can have up to:
  - A description
  - One Primary IPv4 addresses
  - **One or more secondary IPv4 addresses**
    - Secondary IPv4 addresses can be re-assigned to another instance in failure scenarios if you allow it
  - One Elastic IP address corresponding to each IPv4 address (via NAT)
  - One Public IPv4 address (automatically assigned)
  - One of more IPv6 addresses
  - **Up to 5 Security groups**
  - A MAC address
  - **A source/destination check flag**

Review Topic : Elastic Computer Cloud (EC2)

Secondary IP addresses - Benefits

- You can configure secondary IPv4 addresses to your EC2 instance's Interfaces and ENIs

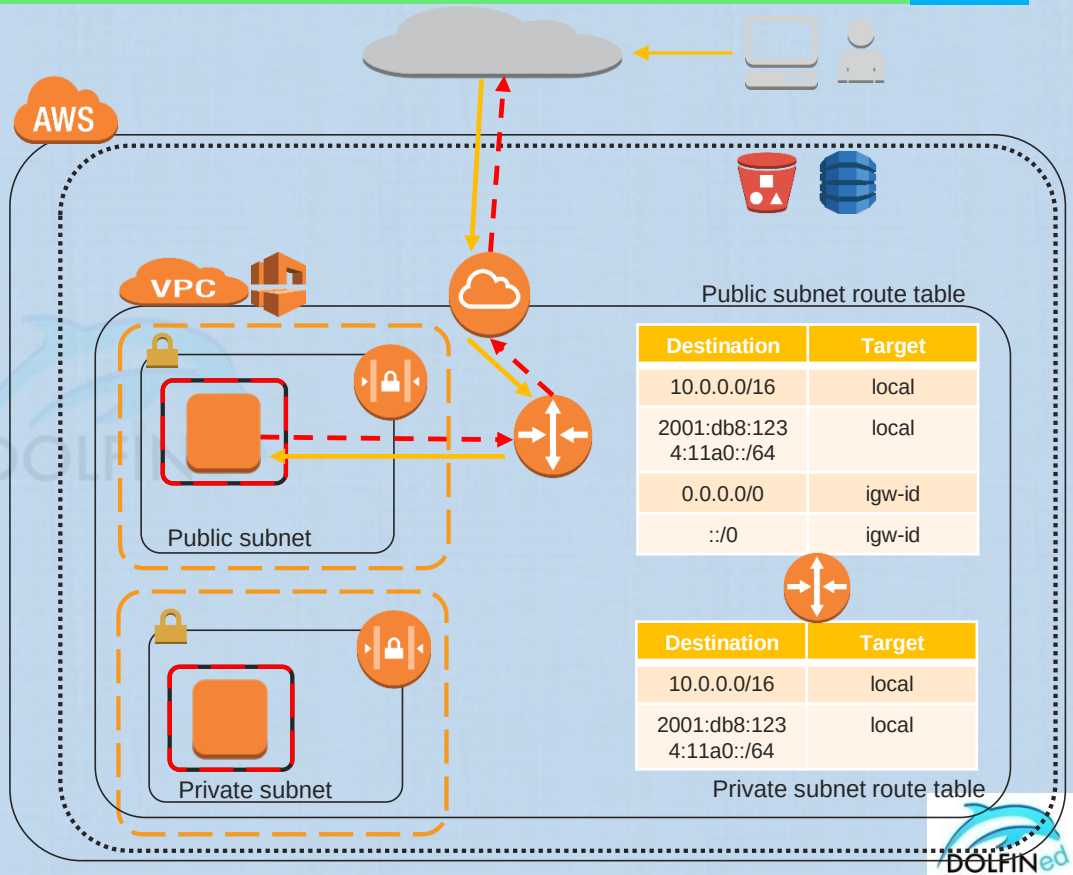
- To attach a network interface (ENI) in a subnet to EC2 instance in another subnet, **they both "MUST" be in the same AWS Region and same AZ**

- It can be useful to assign multiple IP addresses to an EC2 instance in your VPC to do the following:
  - Hosting multiple websites on a single server (multiple SSL certificates each associated with one IP address)
  - Security and network appliances use in your VPC
  - *Redirecting internal traffic to a standby EC2 instance in case your primary EC2 instance fails,*
    - *This can be achieved by moving (reassigning) the secondary IPv4 address from the failed instance to the standby one*

IPV6 EGRESS ONLY INTERNET GATEWAY

IPv6 and the Internet Gateway

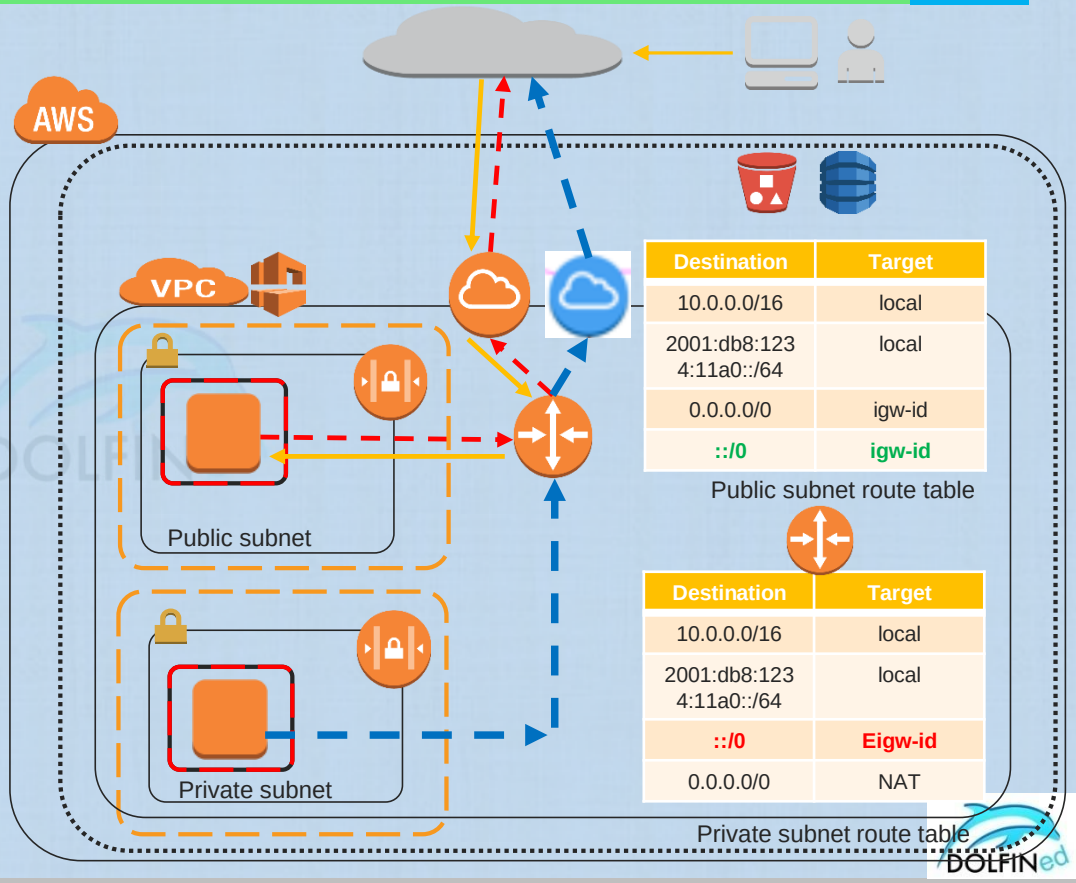
- As in IPv4, an instance with an IPv6 address in a public subnet can connect to the Internet through the Internet gateway.
- Clients on the Internet can initiate a connection to such an instance as well.
- IPv6 addresses are globally unique, which means IPv6 addresses are public IP addresses (no Private address notion)



IPv6 and Egress-only Internet Gateway

- To prevent initiating traffic to your IPv6 addressed instances from the internet, yet allow the instance to access the internet (initiate traffic)
  - An egress-only Internet gateway will be required.
  - Create anegress-only Internet gateway in the VPC,
  - Add a route to the respective route table, directing all ::/0 (All IPv6 traffic destined to the Internet) pointing to the egress-only Internet gateway.
- You can't associate a security group with it
- Use NACLs to protect your instances

- The egress-only Internet gateway is stateful:
  - It forwards traffic from the instances in the subnet to the Internet or other AWS services,
  - It then sends the response back to the instances.



AWS VPC ENDPOINTS

VPC Endpoints

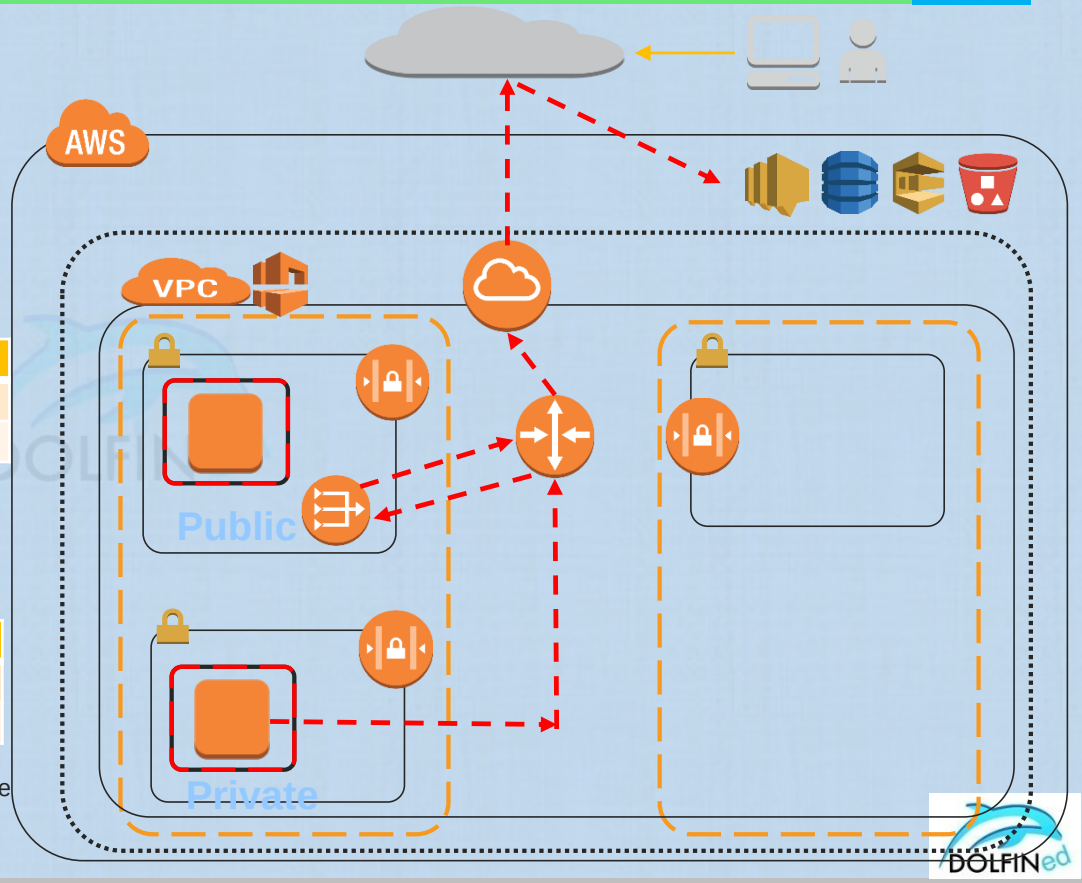
Without VPC Endpoints, EC2 instances/Apps access to AWS services requires to go over the internet (IGW), VPN connections, or NAT gateways, or Public IP addresses.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Igw-id

Public subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NATgw-id

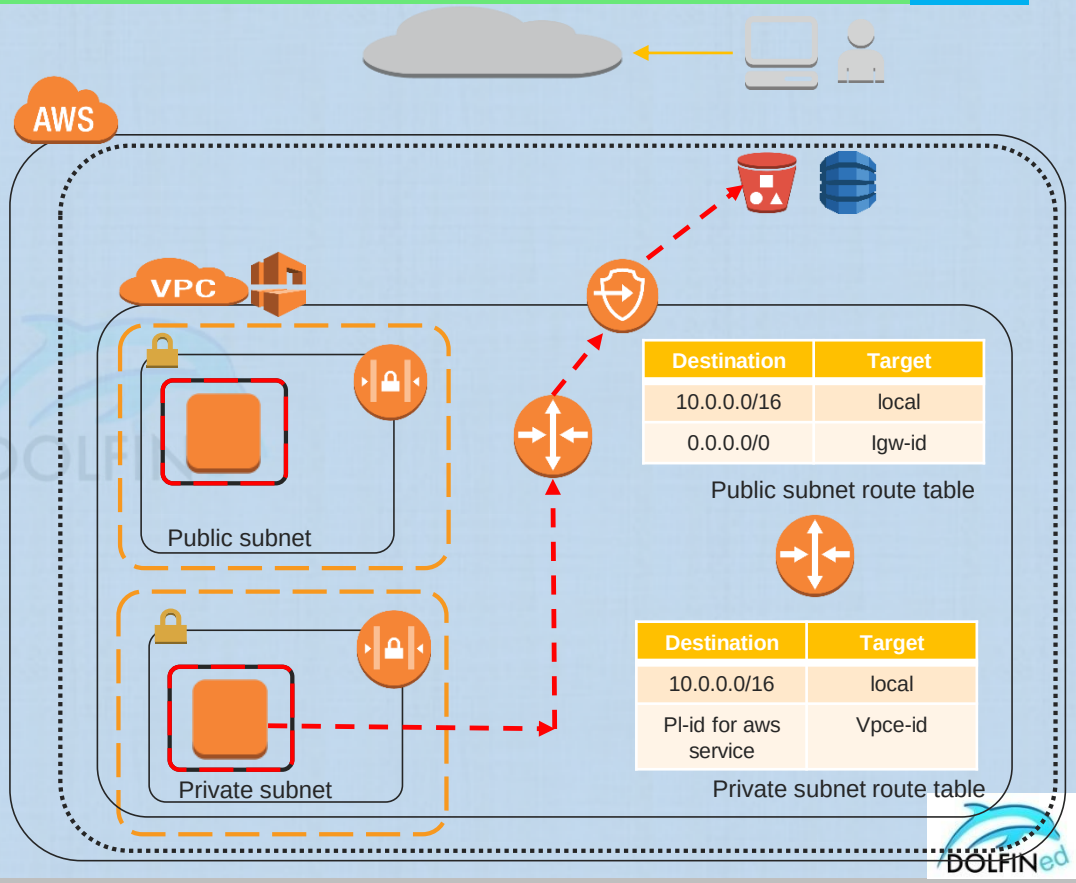
Private subnet route table



VPC Endpoints

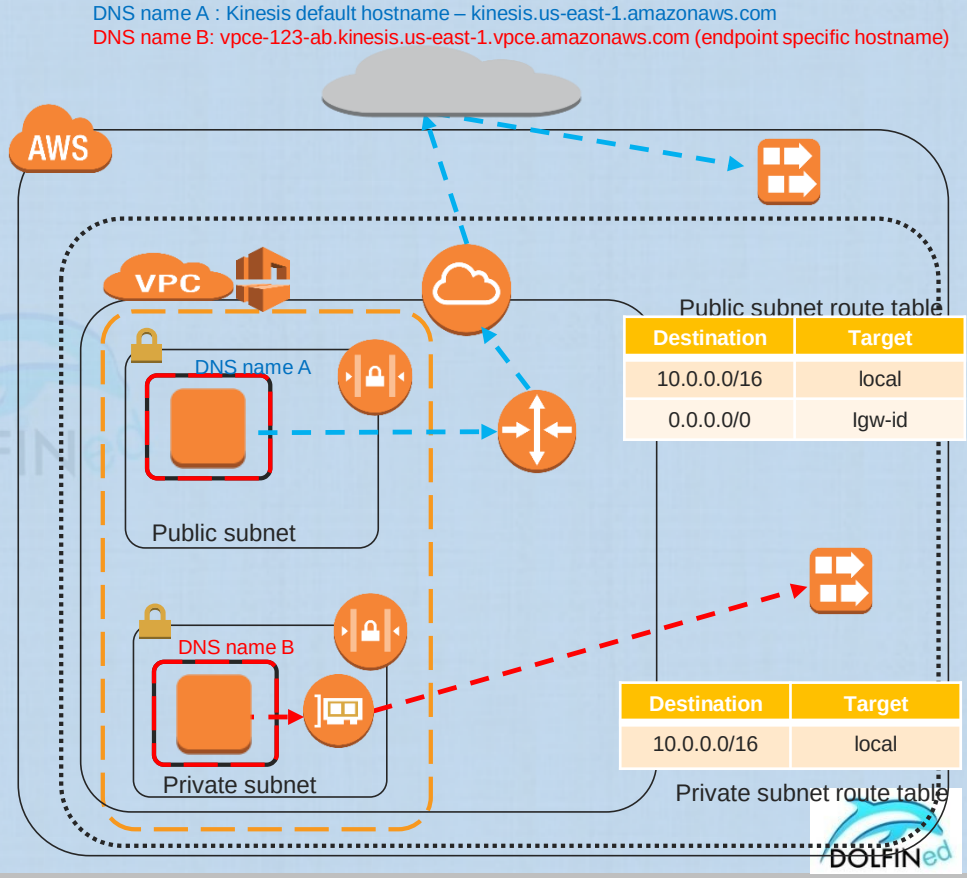
With VPC Endpoints, EC2 instances/Apps can leverage higher performance, and more secure connections to connect, via its private IP addresses,to AWS services without the need to go over the internet (IGW), VPN connections, or NAT gateways, or Public IP addresses.

- Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components.
  - they allow communication between instances in the VPC and services without imposing availability risks or bandwidth constraints on network traffic.
- There are two types of VPC endpoints: ***interface endpoints*** **and** ***gateway endpoints***



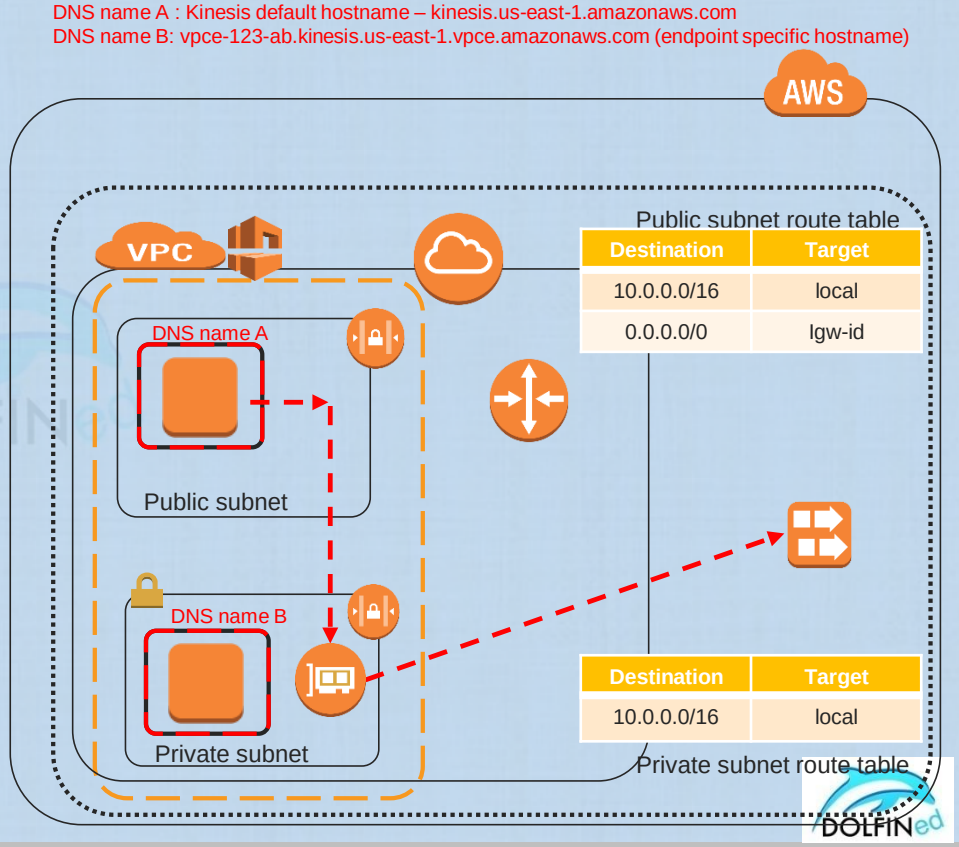
Interface VPC Endpoints (AWS PrivateLink)

- An Interface endpoint is an ENI with a private IP address that serves as an entry point for traffic destined to a supported service.
- AWS will create an ENI per subnet you specify
  - Not highly available, you need to configure it in multiple subnets in multiple AZs
- It allows the connection to services that are powered by AWS PrivateLink.
  - These services include:
    - Some AWS services,
    - Services hosted by other AWS customers and partners in their own VPCs (endpoint services), and
    - Supported AWS Marketplace partner services.
- The owner of the service is the service provider, and you, as the principal creating the interface endpoint, are the service consumer.
- Relies on DNS resolution and is not based on Route table entries.



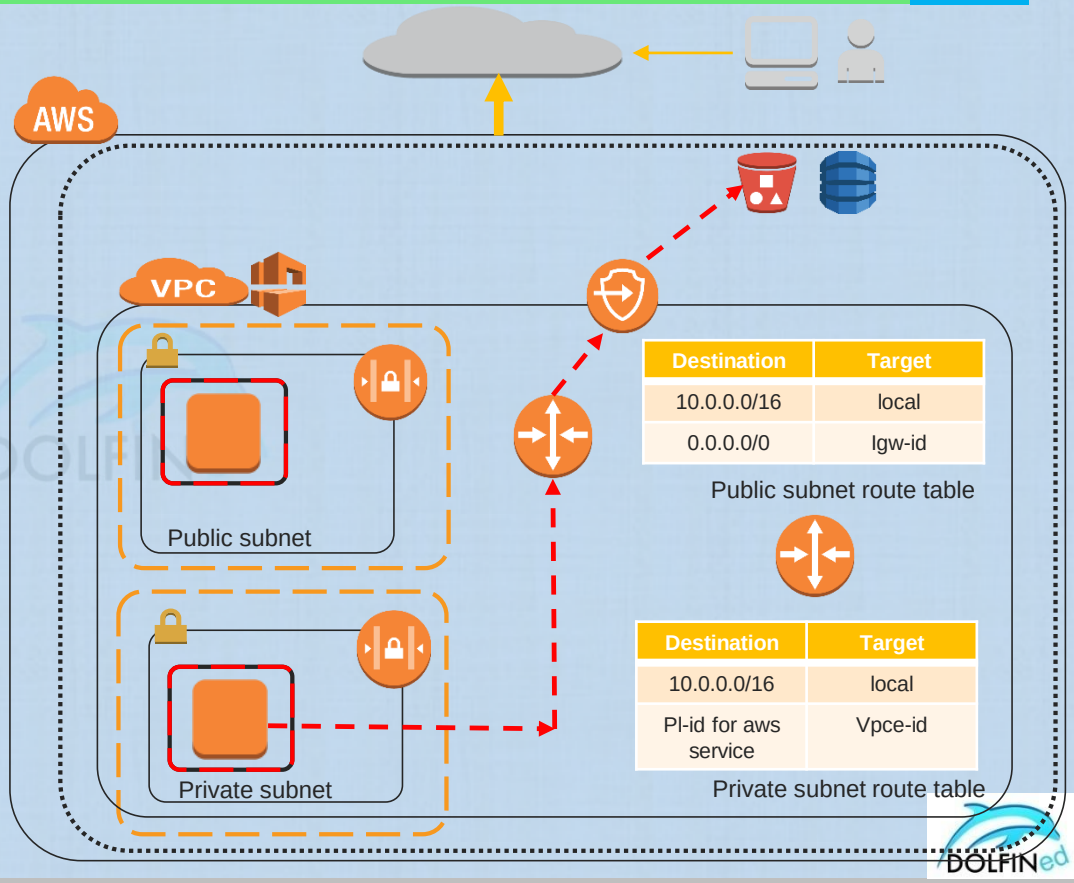
Interface VPC Endpoints – Private DNS

- It associates a private hosted zone with your VPC.
  - The hosted then will have a record set for the default Service's DNS name that resolves to the private IP addresses of the interface Endpoints created in the VPC.
  - This allow to use the service's default DNS hostname instead of the endpoint-specific DNS hostnames to make requests to the service.
  - This way applications in the VPC that were configured to use the default services DNS hostnames, they can continue to use that and be routed to the Interface endpoints.



Gateway Endpoints

- A gateway endpoint is a gateway that is a target for a specified route in route table you specify
- It is used for traffic destined to a supported AWS service. The following AWS services are supported:
  - Amazon S3
  - DynamoDB
- An endpoint policy can be configured to control who can access and permissions on Services accessed by the gateway
- Endpoints are supported within the same region only.
- It does not require security groups to be configured
- It is redundant and highly available
- Only one is required per VPC and can be accessed from different Subnets/Azs



VPC FLOW LOGS
& DHCP OPTION SETS

VPC Flow Logs

- VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.
- Flow logs can help you with several tasks;
  - To troubleshoot why specific traffic is not reaching an instance, which in turn helps you diagnose overly restrictive security group rules.
  - You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.
- You can create a flow log for a VPC, a subnet, or a network interface.
  - If you create a flow log for a subnet or VPC, each network interface in the VPC or subnet is monitored.
- Flow log data can be published to Amazon CloudWatch Logs and Amazon S3.
  - After you've created a flow log, you can retrieve and view its data in the chosen destination.
- CloudWatch Logs charges apply when using flow logs, whether you send them to CloudWatch Logs or to Amazon S3.
- Flow logs do not capture real-time log streams for your network interfaces.

VPC DHCP Options Sets

- You can use an on-premise DNS for your AWS VPC environment, you can also use Route 53 as the DNS for your On-premise environment
- The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network.
- The options field of a DHCP message contains the configuration parameters.
- Some of those parameters are the domain name, domain name server, and the netbios-node-type.
- You can configure DHCP options sets for your virtual private clouds (VPC).