AWS Virtual Private Cloud – VPC

- **AWS VPC – Virtual Private Cloud is a virtual network dedicated to the AWS account. It is logically isolated from other virtual networks in the AWS cloud.**
- VPC allows the users complete control over their virtual networking environment, including the selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways.
- VPC allows you to use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.
- VPC is a regional service and it spans all of the AZs in the Region. Availability zones (AZ) are multiple, isolated locations within each Region.
  - **VPC needs a set of IP addresses in the form of a Classless Inter-Domain Routing (CIDR) block** *for e.g, 10.0.0.0/16, which allows 2^16 (65536) IP address to be available*
  - Allowed CIDR block size is between
    - /28 netmask (minimum with 2^4 – 16 available IP address) and
    - /16 netmask (maximum with 2^16 – 65536 IP address)
  - CIDR block from private (non-publicly routable) IP address can be assigned
    - 10.0.0.0 – 10.255.255.255 (10/8 prefix)
    - 172.16.0.0 – 172.31.255.255 (172.16/12 prefix)
    - 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)
  - Each VPC is separate from any other VPC created with the same CIDR block even if it resides within the same AWS account

- Connection between your VPC and corporate or home network can be established, however, the CIDR blocks should be not be overlapping *for e.g. VPC with CIDR 10.0.0.0/16 can communicate with 10.1.0.0/16 corporate network but the connections would be dropped if it tries to connect to 10.0.37.0/16 corporate network cause of overlapping IP addresses*.

Subnets

- Subnet spans a single Availability Zone, distinct locations engineered to be isolated from failures in other AZs, and cannot span across AZs
- Subnet can be configured with an Internet gateway to enable communication over the Internet, or virtual private gateway (VPN) connection to enable communication with your corporate network
- Subnet can be Public or Private and it depends on whether it has Internet connectivity i.e. is able to route traffic to the Internet through the IGW

- Instances within the Public Subnet should be assigned a Public IP or Elastic IP address to be able to communicate with the Internet

Subnet Sizing

- CIDR block assigned to the Subnet can be the same as the VPC CIDR, in this case you can launch only one subnet within your VPC
- CIDR block assigned to the Subnet can be a subset of the VPC CIDR, which allows you to launch multiple subnets within the VPC
- CIDR block assigned to the subnet should not be overlapping
- CIDR block size allowed is between
  - /28 netmask (minimum with 2^4 – 16 available IP address) and
  - /16 netmask (maximum with 2^16 – 65536 IP address)
- AWS reserves 5 IPs address (first 4 and last 1 IP address) in each Subnet which are not available for use and cannot be assigned to an instance. *for e.g. for a Subnet with a CIDR block 10.0.0.0/24 the following five IPs are reserved*
  - *10.0.0.0: Network address*
  - *10.0.0.1: Reserved by AWS for the VPC router*
  - *10.0.0.2: Reserved by AWS for mapping to Amazon-provided DNS*
  - *10.0.0.3: Reserved by AWS for future use*
  - *10.0.0.255: Network broadcast address. AWS does not support broadcast in a VPC, therefore the address is reserved.*
- VPC supports IPv4 and IPv6 addressing and has different CIDR block size limits for each
- IPv6 CIDR block can be optionally associated with the VPC
- VPC IPv4 CIDR block cannot be modified once created i.e. cannot increase or decrease the size of an existing CIDR block.
- However, **secondary CIDR blocks can be associated with the VPC to extend the VPC**

IP Addresses

Instances launched in the VPC can have Private, Public, and Elastic IP addresses assigned to them and are properties of ENI (Network Interfaces)

- Private IP Addresses
  - Private IP addresses are not reachable over the Internet, and can be used for communication only between the instances within the VPC
  - All instances are assigned a private IP address, within the IP address range of the subnet, to the default network interface
  - Primary IP address is associated with the network interface for its lifetime, even when the instance is stopped and restarted and is released only when the instance is terminated

    - Additional Private IP addresses, known as secondary private IP address, can be assigned to the instances and these can be reassigned from one network interface to another
- Public IP address
    - Public IP addresses are reachable over the Internet, and can be used for communication between instances and the Internet, or with other AWS services that have public endpoints
    - Public IP address is assigned from AWS pool of IP addresses and it is not associated with the AWS account and hence is released when the instance is stopped and restarted or terminated.
- Elastic IP address
    - Elastic IP addresses are static, persistent public IP addresses that can be associated and disassociated with the instance, as required
    - Elastic IP address is allocated to the VPC and owned by the account unless released.
    - A Network Interface can be assigned either a Public IP or an Elastic IP. If you assign an instance, that already has a Public IP, an Elastic IP, the public IP is released
    - Elastic IP addresses can be moved from one instance to another, which can be within the same or different VPC within the same account
    - Elastic IPs are charged for non-usage i.e. if it is not associated or associated with a stopped instance or an unattached Network Interface

Elastic Network Interface (ENI)

- Each Instance is attached to a default elastic network interface (Primary Network Interface eth0) and cannot be detached from the instance
- ENI can include the following attributes
    - Primary private IP address
    - One or more secondary private IP addresses
    - One Elastic IP address per private IP address
    - One public IP address, which can be auto-assigned to the network interface for eth0 when you launch an instance, but only when you create a network interface for eth0 instead of using an existing ENI
    - One or more security groups
    - A MAC address
    - A source/destination check flag
    - A description
- ENI's attributes follow the ENI as it is attached or detached from an instance and reattached to another instance. When an ENI is moved from one instance to another, network traffic is redirected to the new instance.
- Multiple ENIs can be attached to an instance and is useful for use cases:

- Create a management network.
- Use network and security appliances in your VPC.
- Create dual-homed instances with workloads/roles on distinct subnets.
- Create a low-budget, high-availability solution.

Route Tables

- Route table defines rules, termed as routes, which determine where network traffic from the subnet would be routed
- Each VPC has an implicit router to route network traffic
- Each VPC has a Main Route table and can have multiple custom route tables created
- Each Subnet within a VPC must be associated with a single route table at a time, while a route table can have multiple subnets associated with it
- Subnet, if not explicitly associated to a route table, is implicitly associated with the main route table
- Every route table contains a local route that enables communication within a VPC which cannot be modified or deleted
- Route priority is decided by matching the most specific route in the route table that matches the traffic
- Route tables need to be updated to define routes for Internet gateways, Virtual Private gateways, VPC Peering, VPC Endpoints, NAT Devices, etc.

Internet Gateways – IGW

- An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in the VPC and the Internet.
- IGW imposes no availability risks or bandwidth constraints on the network traffic.
- An Internet gateway serves two purposes:
  - To provide a target in the VPC route tables for Internet-routable traffic,
  - To perform network address translation (NAT) for instances that have been NOT been assigned public IP addresses.

NAT Gateway

- AWS NAT – Network Address Translation devices, launched in the public subnet, enables instances in a private subnet to connect to the Internet but prevents the Internet from initiating connections with the instances.
- Instances in private subnets would need an internet connection for performing software updates or trying to access external services.

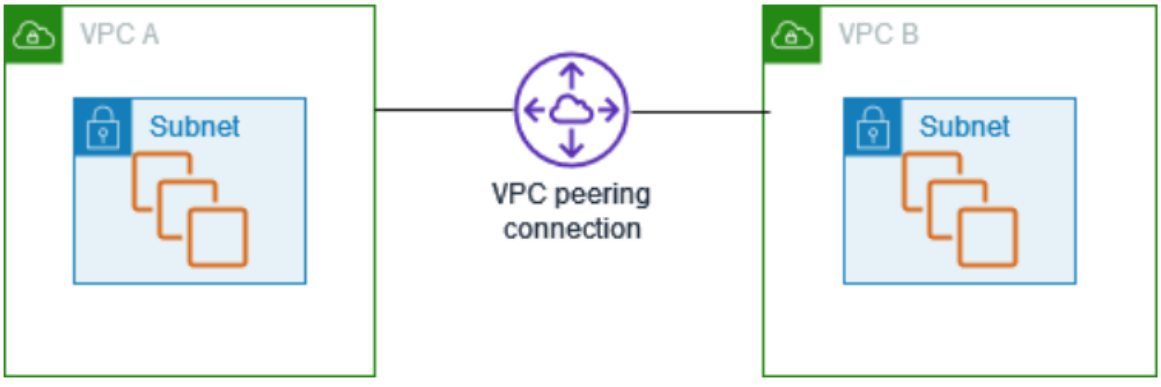
- NAT instance prevents instances to be directly exposed to the Internet and having to be launched in a Public subnet and assigning of the Elastic IP address to all, which are limited.
- NAT device routes the traffic, from the private subnet to the Internet, by replacing the source IP address with its address and it translates the address back to the instances' private IP addresses for the response traffic.
- AWS allows NAT configuration in 2 ways
  - NAT Gateway, managed service by AWS
  - NAT Instance
- NAT gateway is an AWS managed NAT service that provides better availability, higher bandwidth, and requires less administrative effort.
- A NAT gateway supports 5 Gbps of bandwidth and automatically scales up to 100 Gbps. For higher bursts requirements, the workload can be distributed by splitting the resources into multiple subnets and creating a NAT gateway in each subnet.
- Public NAT gateway is associated with One Elastic IP address which cannot be disassociated after its creation.
- Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone.
- A NAT gateway supports the TCP, UDP, and ICMP protocol
- NAT gateway cannot send traffic over VPC endpoints, VPN connections, AWS Direct Connect, or VPC peering connections. The private subnet's route table should be modified to route the traffic directly to these devices.

VPC Peering

- A VPC peering connection is a networking connection between two VPCs that enables routing of traffic between them using private IPv4 addresses or IPv6 addresses.
- VPC peering connection
  - can be established between your own VPCs, or with a VPC in another AWS account in the same or different region.
  - is a one-to-one relationship between two VPCs.
  - supports intra and inter-region peering connections.
- With VPC peering,
  - Instances in either VPC can communicate with each other as if they are within the same network
  - AWS uses the existing infrastructure of a VPC to create a 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
  - All inter-region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global AWS backbone, and never traverses

the public internet, which reduces threats, such as common exploits, and DDoS attacks.

- VPC peering does not have any separate charges. However, there are data transfer charges.



VPC Peering Limitations & Rules

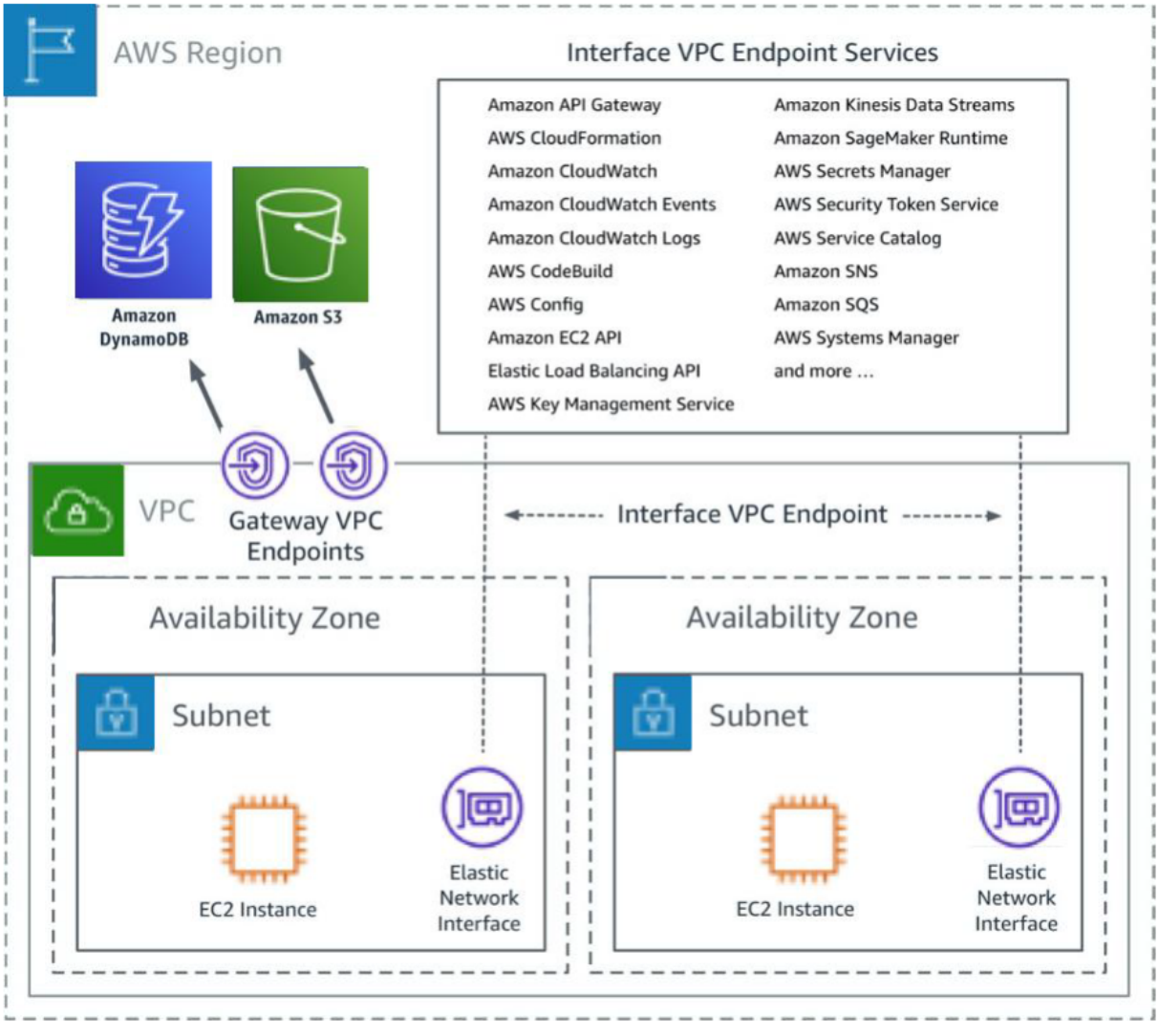
1. Does not support Overlapping or matching IPv4 or IPv6 CIDR blocks.
2. Does not support transitive peering relationships i.e. the VPC does not have access to any other VPCs that the peer VPC may be peered with even if established entirely within your own AWS account

- VPC Peering can be applied to create shared services or perform authentication with an on-premises instance
- This would help create a single point of contact, as well limiting the VPN connections to a single account or VPC

AWS VPC Endpoints

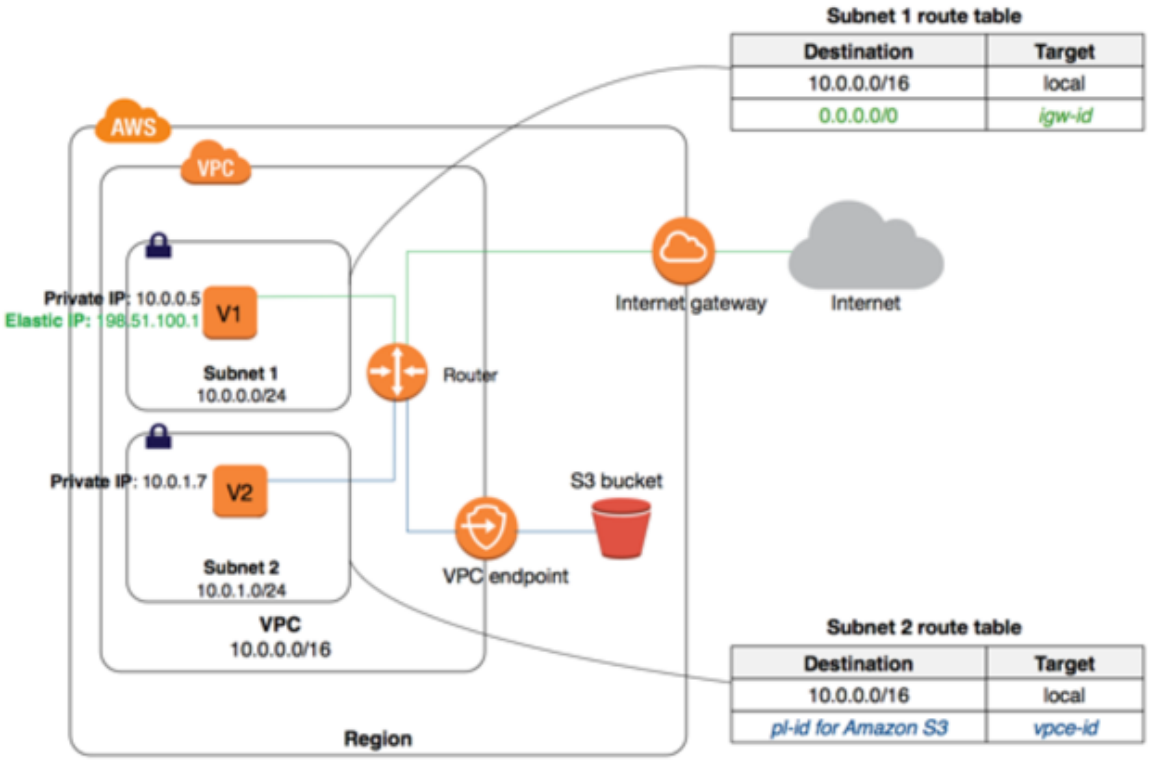
- VPC Endpoints enable the creation of a private connection between VPC to supported AWS services and VPC endpoint services powered by PrivateLink using its private IP address
  - Endpoints do not require a public IP address, access over the Internet, NAT device, a VPN connection, or AWS Direct Connect.
- Traffic between VPC and AWS service does not leave the Amazon network
- Endpoints are virtual devices, that are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in the VPC and AWS services without imposing availability risks or bandwidth constraints on your network traffic.

- AWS currently supports the following types of Endpoints
  - VPC Gateway Endpoints
  - VPC Interface Endpoints

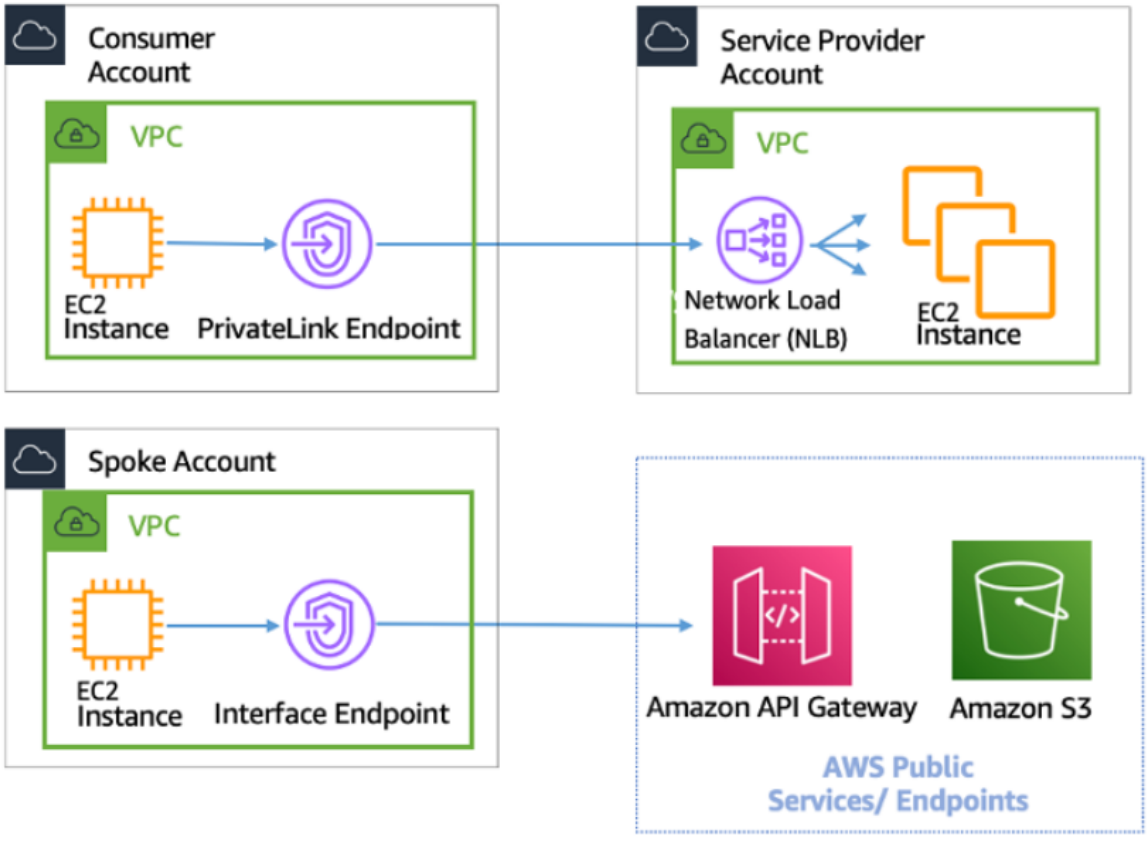


VPC Gateway Endpoints

- A VPC Gateway Endpoint is a gateway that is a target for a specified route in the route table, used for traffic destined for a supported AWS service.
- Gateway Endpoints currently supports S3 and DynamoDB services
- Gateway Endpoints do not require an Internet gateway or a NAT device for the VPC.
- Gateway endpoints do not enable AWS PrivateLink.
- VPC Endpoint policy and Resource-based policies can be used for fine-grained access control.



VPC Interface Endpoints – PrivateLink



- VPC Interface endpoints enable connectivity to services powered by AWS PrivateLink.
- Services include AWS services *like CloudTrail, CloudWatch, etc.*, services hosted by other AWS customers and partners in their own VPCs (referred to as endpoint services), and supported AWS Marketplace partner services.
- Interface Endpoints only allow traffic from VPC resources to the endpoints and not vice versa
- PrivateLink endpoints can be accessed across both intra- and inter-region VPC peering connections, Direct Connect, and VPN connections.
- VPC Interface Endpoints, by default, have an address like vpce-svc-01234567890abcdef.us-east-1.vpce.amazonaws.com which needs application changes to point to the service.
- Interface Endpoints can be used to create custom applications in VPC and configure them as an AWS PrivateLink-powered service (referred to as an *endpoint service*) exposed through a Network Load Balancer.
- Custom applications can be hosted within AWS or on-premises (via Direct Connect or VPN)

AWS VPC VPN

- AWS VPN connections are used to extend on-premises data centers to AWS.
- VPN connections provide secure IPSec connections between the data center or branch office and the AWS resources.
- AWS Site-to-Site VPN or AWS Hardware VPN or AWS Managed VPN
  - Connectivity can be established by creating an IPSec, hardware VPN connection between the VPC and the remote network.
  - On the AWS side of the VPN connection, a Virtual Private Gateway (VGW) provides two VPN endpoints for automatic failover.
  - On the customer side, a customer gateway (CGW) needs to be configured, which is the physical device or software application on the remote side of the VPN connection

AWS Direct Connect – DX

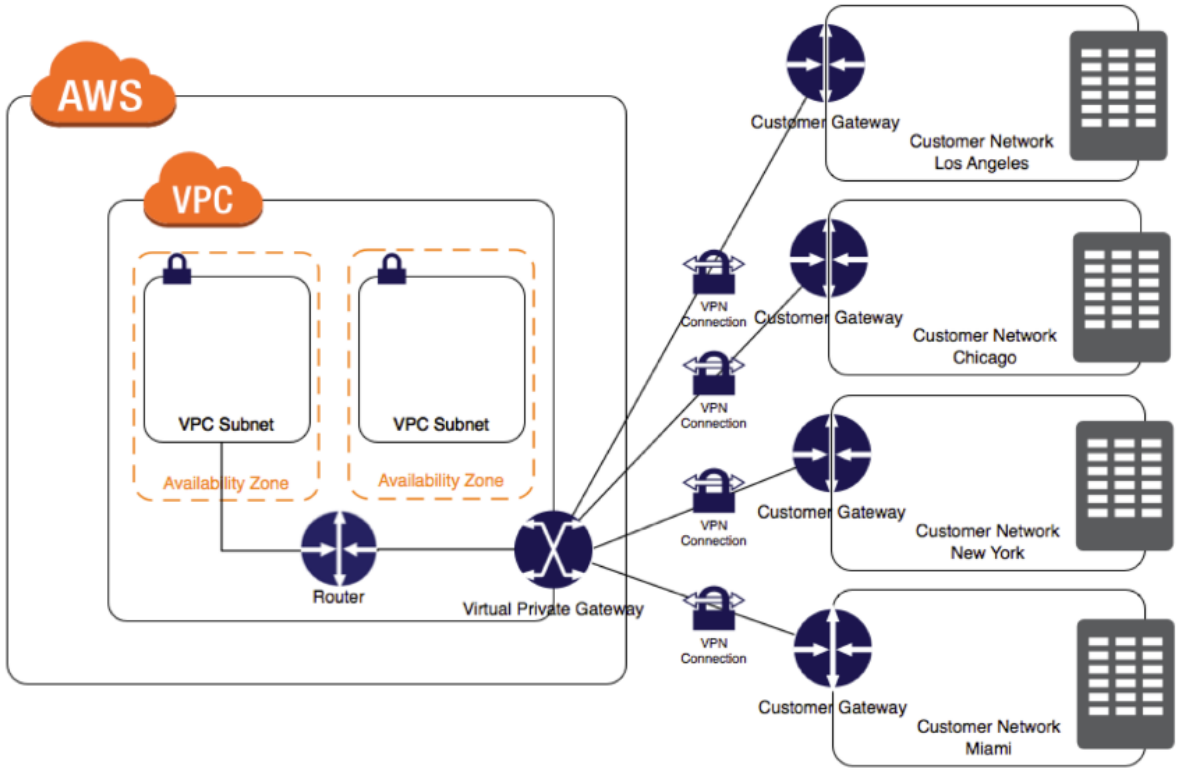
- AWS Direct Connect is a network service that provides an alternative to using the Internet to utilize AWS cloud services
- DX links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable with one end of the cable connected to your router, the other to an AWS Direct Connect router.
- Connections can be established with
  - Dedicated connections – 1Gbps, 10Gbps, and 100Gbps capacity.
  - Hosted connection – Speeds of 50, 100, 200, 300, 400, and 500 Mbps can be ordered from any APN partners supporting AWS DX. Also, supports 1, 2, 5 & 10 Gbps with selected partners.
- Virtual interfaces can be created directly to public AWS services (e.g. S3) or to VPC, bypassing internet service providers in the network path.
- Each AWS DX location enables connectivity to all AZs within the geographically nearest AWS region.
- DX supports both the IPv4 and IPv6 communication protocols.

Direct Connect Advantages

- **Reduced Bandwidth Costs**
  - All data transferred over the dedicated connection is charged at the reduced data transfer rate rather than Internet data transfer rates.
  - Transferring data to and from AWS directly reduces the bandwidth commitment to the Internet service provider
- **Consistent Network Performance**
  - provides a dedicated connection and a more consistent network performance experience than the Internet which can widely vary.
- **AWS Services Compatibility**
  - is a network service and works with all of the AWS services like S3, EC2, and VPC

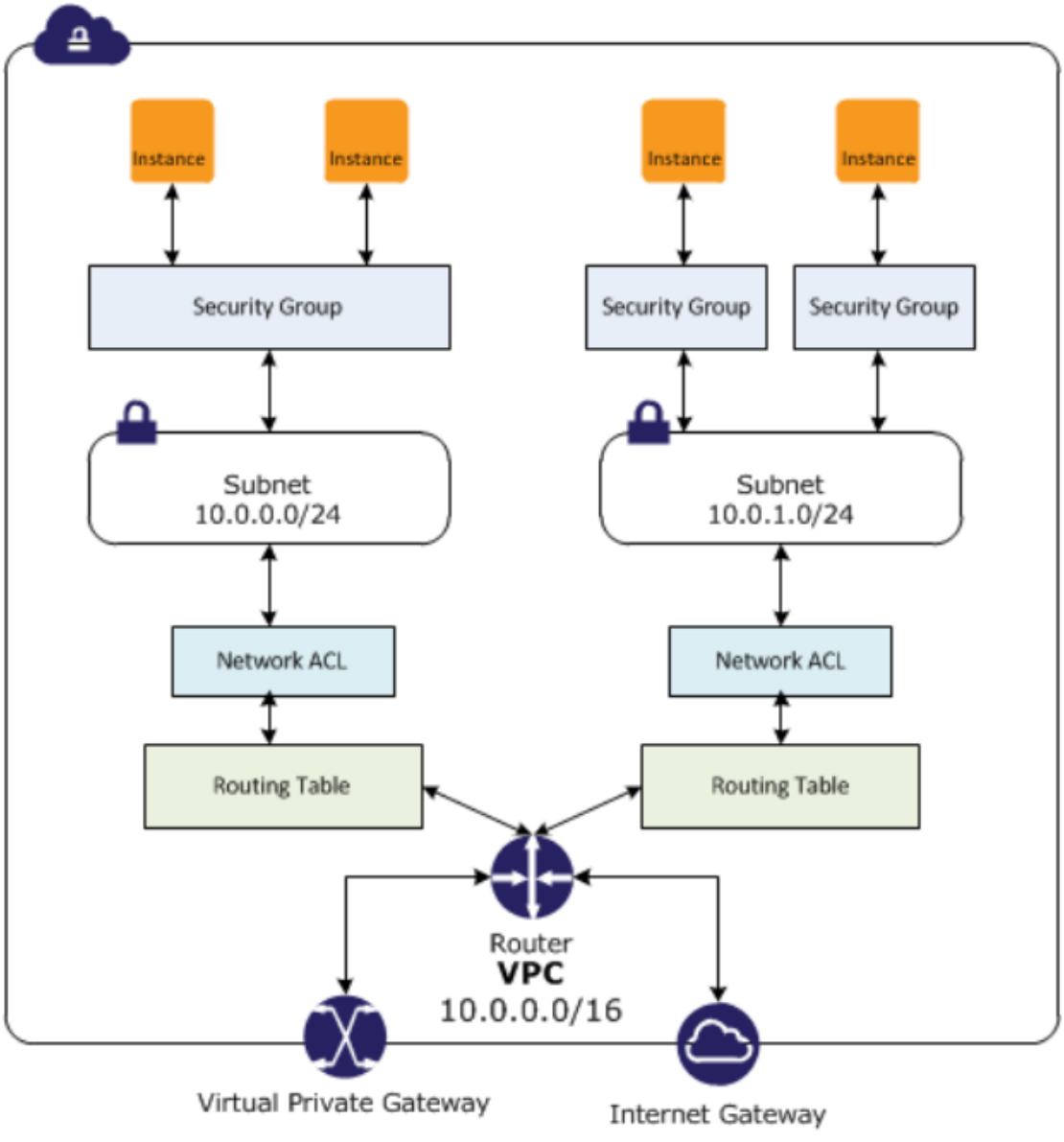
- **Private Connectivity to AWS VPC**
  - Using DX Private Virtual Interface a private, dedicated, high bandwidth network connection can be established between the network and VPC
- **Elastic**
  - can be easily scaled to meet the needs by either using a higher bandwidth connection or by establishing multiple connections.

Multiple Site-to-Site VPN Connections



AWS VPC Security Group vs NACLs

- In a VPC, both Security Groups and Network ACLs (NACLS) together help to build a layered network defence.
- **Security groups** – Act as a **virtual firewall** for **associated instances**, controlling both inbound and outbound traffic at the instance level
- **Network access control lists (NACLs)** – Act as a firewall for **associated subnets**, controlling both inbound and outbound traffic at the subnet level



Security Groups

- Acts at an Instance level and not at the subnet level.
- Each instance within a subnet can be assigned a different set of Security groups
- An instance can be assigned 5 security groups with each security group having 60 rules.
- allows separate rules for inbound and outbound traffic.
- allows adding or removing rules (authorizing or revoking access) for both Inbound (ingress) and Outbound (egress) traffic to the instance
  - **Default** Security group allows **no external inbound traffic** but allows inbound traffic from instances with the same security group

    - **Default** Security group **allows all outbound traffic**
    - New Security groups start with only an outbound rule that allows all traffic to leave the instances.
- can **specify only Allow rules, but not deny rules**
- can grant access to a specific IP, CIDR range, or to another security group in the VPC or in a peer VPC (requires a VPC peering connection)
- are **evaluated as a Whole or Cumulative bunch of rules** with the most permissive rule taking precedence *for e.g. if you have a rule that allows access to TCP port 22 (SSH) from IP address 203.0.113.1 and another rule that allows access to TCP port 22 from everyone, everyone has access to TCP port 22.*
- are **Stateful –** responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules, and vice versa. Hence an Outbound rule for the response is not needed
- Instances associated with a security group **can't talk to each other** unless rules allowing the traffic are added.
- are associated with ENI (network interfaces).
- are associated with the instance and can be changed, which changes the security groups associated with the primary network interface (eth0) and the changes would be applicable immediately to all the instances associated with the Security Group.

Network Access Control Lists – NACLs

- A Network ACLs (NACLs) is an optional layer of security for the VPC that acts as a **firewall for controlling traffic in and out of one or more subnets**.
- are not for granular control and are assigned at a Subnet level and are **applicable to all the instances in that Subnet**
- has separate inbound and outbound rules, and each rule can either **allow or deny traffic**
    - Default ACL allows all inbound and outbound traffic.
    - The newly created ACL denies all inbound and outbound traffic.
- **A Subnet can be assigned only 1 NACL** and if not associated explicitly would be associated implicitly with the default NACL
- can associate a **network ACL with multiple subnets**
- is a numbered list of rules that are **evaluated in order** starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL *e.g. if you have a Rule No. 100 with Allow All and 110 with Deny All, the Allow All would take precedence and all the traffic will be allowed.*
- are **Stateless**; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa) *for e.g. if you enable Inbound SSH on port 22 from*

the specific IP address, you would need to add an Outbound rule for the response as well.

VPC Flow logs

- VPC Flow Logs help capture information about the IP traffic going to and from network interfaces in the VPC and can help in monitoring the traffic or troubleshooting any connectivity issues.
- Flow log data can be published to CloudWatch Logs, S3, and Kinesis Data Firehose.
- Flow log can be created for the entire VPC, subnets, or each network interface. If enabled, for the entire VPC or subnet all the network interfaces within that resource are monitored.
- Flow log can be configured to capture the type of traffic (accepted traffic, rejected traffic, or all traffic).
- Flow logs do not capture real-time log streams for network interfaces.
- Flow log data is collected outside of the path of the network traffic, and therefore does not affect network throughput or latency.