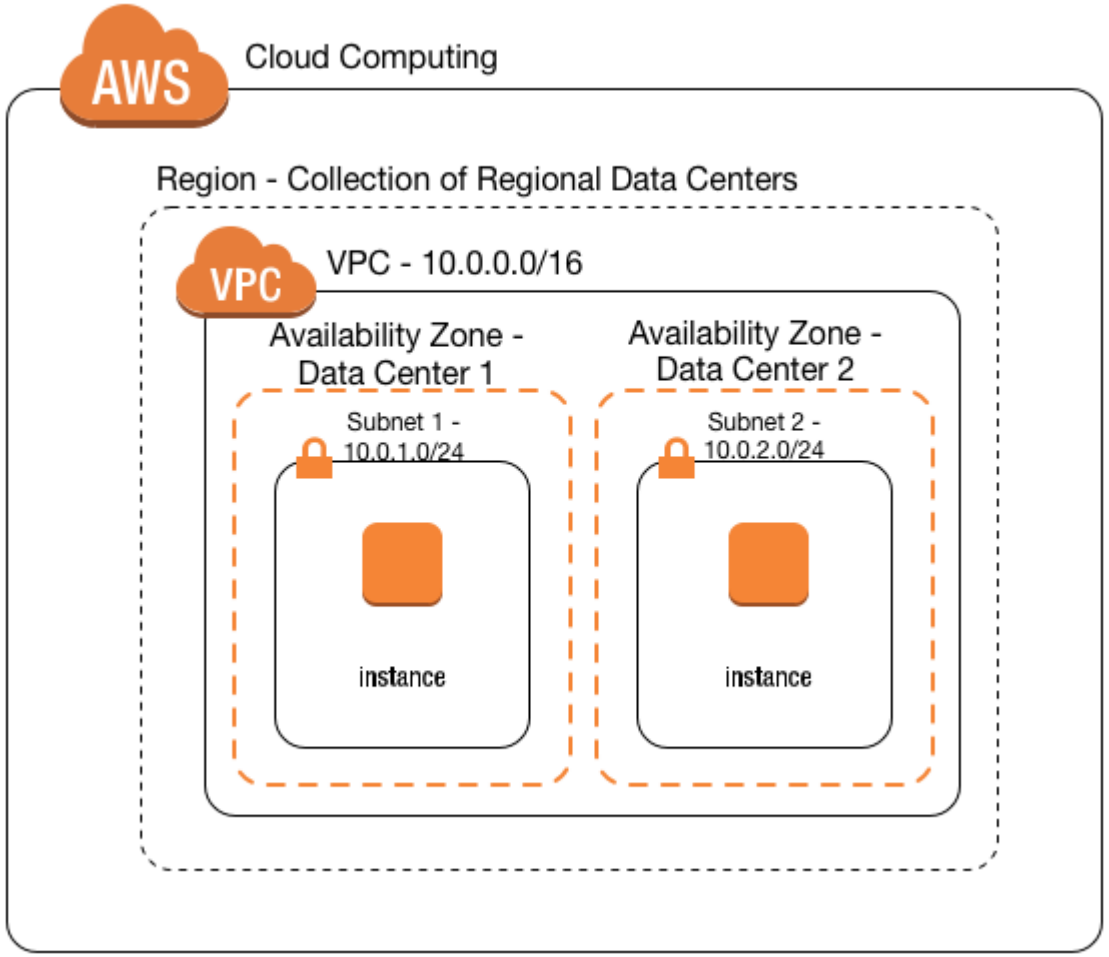
Virtual Private Cloud

- AWS Virtual Private Cloud
- VPC Components
- VPC Types
- Implied Router
- Route Tables
- VPC IP Addressing
- Internet Gateway
- Public Subnet vs. Private Subnet
- Elastic IP addresses
- Security Groups
- Network Access Control Lists
- NAT Instance
- NAT Gateway
- VPC Flow Logs
- VPC Peering
- Transit Gateway
- Virtual Private Gateways
- Customer Gateways
- Virtual Private Networks
- AWS Direct Connect

AWS Virtual Private Cloud (VPC)

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ug.pdf

- Is a virtual network or data center inside AWS for one client, or a department in an enterprise
- The AWS client has full control over resources & virtual compute instances (virtual servers) hosted inside that VPC
- Is similar to having your own data center inside AWS
- Logically isolated from other VPCs on AWS
- You can have one or more IP address subnets inside a VPC
- A VPC is confined to an AWS region and does not extend between regions



VPC Components

- CIDR and IP address subnets
- Implied Router
- Route tables
- Internet gateway
- Security Groups
- Network Access Control Lists (N. ACLs)

VPC Types

A Default VPC

– Created in each AWS region when an AWS account is created

– Has default CIDR, Security Group, N ACL, and route table Settings

– Has an Internet Gateway by default

A Custom VPC

– Is a VPC an AWS account owner creates

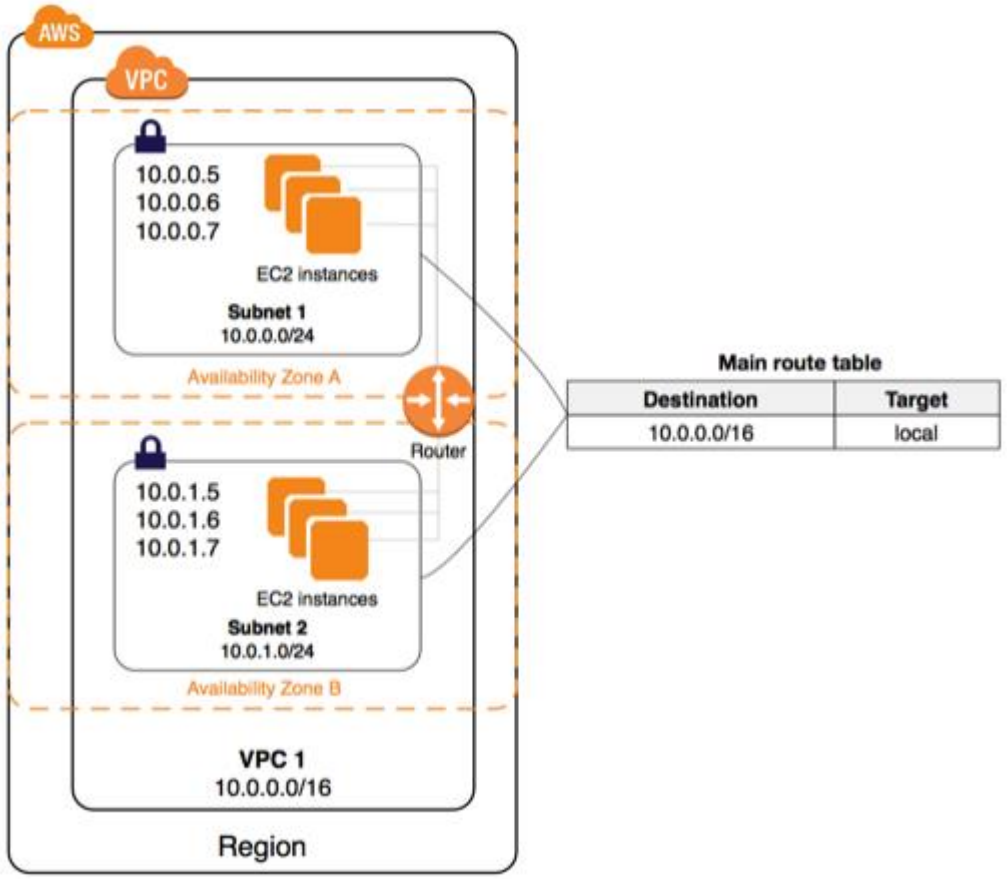
– AWS user creating the custom VPC can decide the VPC CIDR block

– Has its own default security group, N ACL, and Route tables

– Does not have an Internet Gateway by default, one needs to be created if needed

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 that the router uses to forward traffic within the VPC
- The route tables can also have entries to external destinations



Route Tables

- Each Subnet MUST be associated with only one route table at any given time
- If you do not specify a subnet-to-route-table association, the subnet (when created) will be associated with the main (default) VPC route table. You can change the subnet association to another route table when/as needed
- You can also edit the main (default) route table if you need, but you can **NOT delete the Main (default) route table**
- However, you can make a custom route table manually become the main route table, then you can delete the former main, as it is no longer a main route table
- Every route table in a VPC comes with a default rule that allows all VPC subnets to communicate with one another
- You can NOT modify or delete this rule

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 Reserved IP's in each subnet

First **4 IP addresses** in each subnet and the **last one** is 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

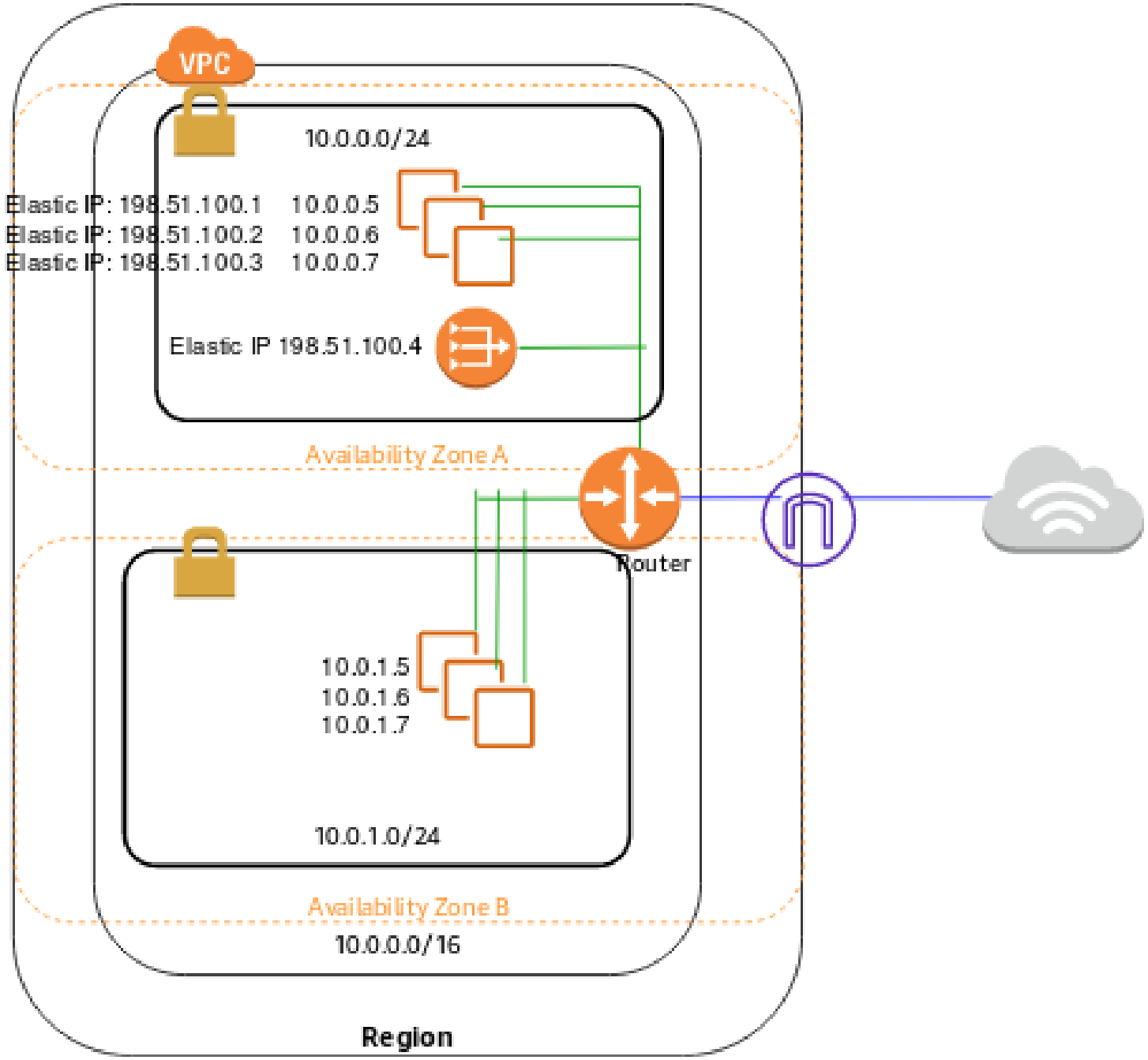
10.0.0.3 Reserved for future use

10.0.0.255 last IP

RFC 1918 range	Example CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	192.168.0.0/20

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


VPC
10.0.0.0/24
Elastic IP: 198.51.100.1 10.0.0.5
Elastic IP: 198.51.100.2 10.0.0.6
Elastic IP: 198.51.100.3 10.0.0.7
Elastic IP 198.51.100.4
Availability Zone A
Router
10.0.1.5
10.0.1.6
10.0.1.7
10.0.1.0/24
Availability Zone B
10.0.0.0/16
Region

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

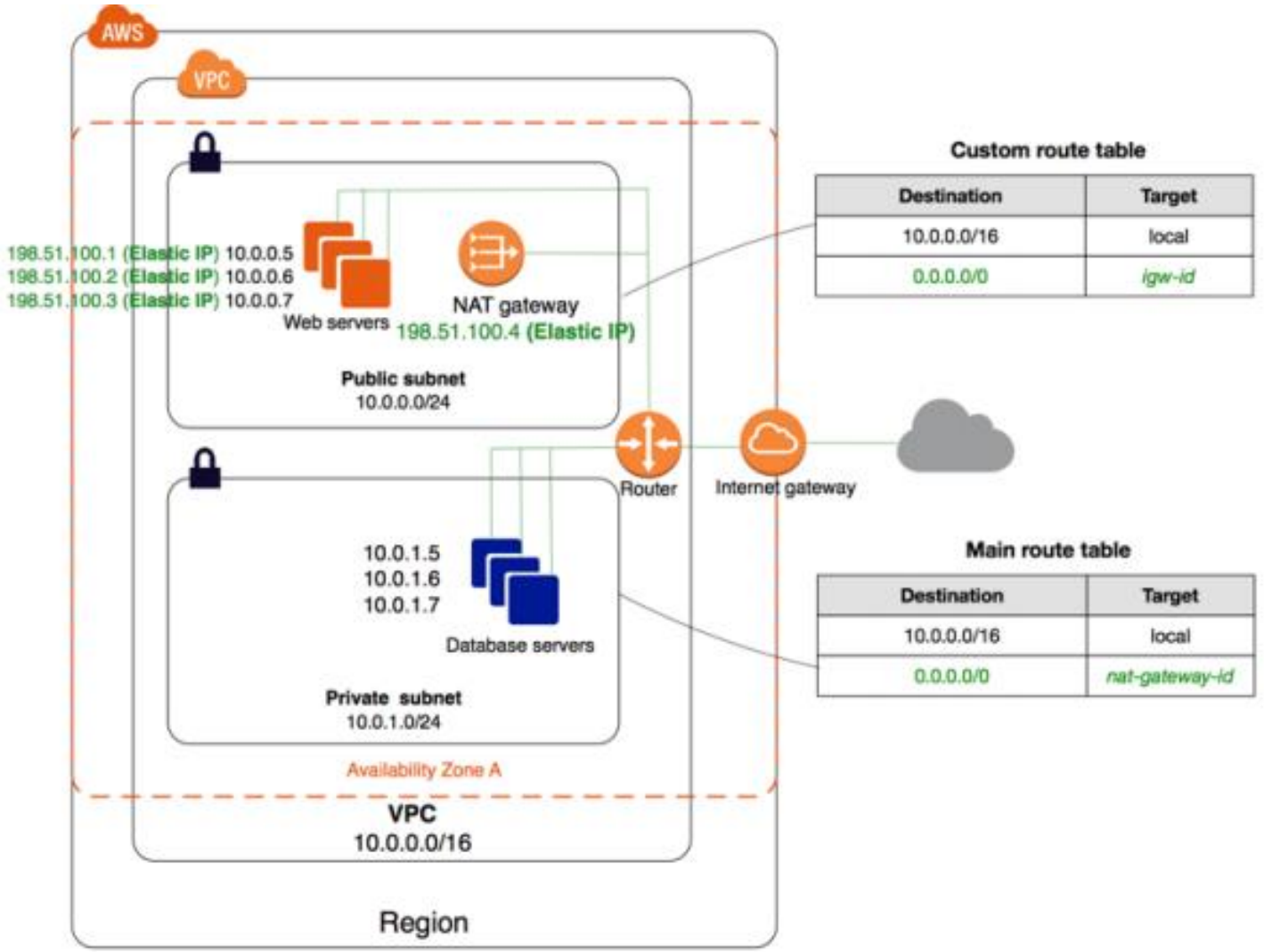
Destination 0.0.0.0/0 Target: igw-1234

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

– **Private subnet means**, it is not accessible from the Internet since it has no Public Internet IP addresses configured.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-gateway-id

VPC with public and private subnets (NAT)



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.

Security Groups

- A security group is a virtual firewall
- It controls traffic at the virtual server (EC2 Instance) level
  - Specifically at the virtual Network Interface level
- Up to 16 (5 is the default) security groups per EC2 instance interface can be applied
- **Stateful**, return traffic, of allowed inbound traffic, is allowed, even if there are no rules to allow it
- Can only have permit rules, can NOT have deny rules
- Implicit deny rule at the end
- All rules are evaluated to find a permit rule

Security Groups

- You can use Security Group names as the source or destination in other security group rules
- You can use the security group name as the source in its own inbound security group rules
- Any Virtual Server Instance(EC2) created without specifying a security group for it (during its creation), will be assigned the VPC default security group
- Each VPC created will have a default Security Group created for it, you can NOT delete a default Security group
- **Security groups are VPC resources**, hence, different EC2 instances, in different Availability Zones, belonging to the same VPC, can have the same security group applied to them
- **Changes to security groups take effect immediately**

Default and non-Default Security Groups

A default security group

– Is the one created by AWS when the default VPC is created, or when you create your own Custom VPC and it will have (by default)

- Inbound rules allowing Instances assigned the same security group to talk to one another
- All outbound traffic is allowed

A Custom (non-default) security group

– Is the one you create under a default or non-default VPC, and by default it will have

- No inbound rules – basically all inbound traffic is denied by default
- All outbound traffic is allowed by default

Network Access Control Lists (N.ACLs)

- It is a function performed on the implied router (The implied VPC router hosts the Network ACL function)
- It functions at the **Subnet Level**
- N. ACLs are "**Stateless**". Outbound traffic for an allowed inbound traffic, must be "explicitly" allowed too
- You can have **"permit" and "deny"** rules in a NACL
- NACL is a set of rules, each has **a number**
- NACL rules are checked for a "permit" from lower numbered rules until either a permit is found, or an explicit/implicit deny is reached
- You can insert rules (based on the configured rule number spacing) between existing rules, hence, it is recommended to leave a number range between any two rules to allow for edits later.
- N. ACLs end with an explicit deny any, which you can NOT delete
- A subnet must be associated with a N. ACL, if you do not specify the N. ACL, the subnet will get associated with **the default N. ACL** automatically

Network Access Control Lists (N.ACLs)

- You can create your own custom N. ACL, you do not have to use the default one
- A default N.ACL allows all traffic inbound and outbound
- A custom (non-default) N. ACL blocks/denies all traffic inbound and outbound by default.

For NACLs:

- Inbound in NACL means coming from outside the subnet destined to the subnet.
- Outbound means going out of the subnet.

For Security Groups

- Inbound for security group means inbound from outside the instance destined to the instance.
- Outbound means going out of the instance's ENI.

If you are facing any issues regarding communication between EC2 instances in a VPC, always look for the security setting of security groups and N ACLs relevant to the communication path (Source instance on which subnet and to Destination instance on which subnet).

NAT Instance

- NAT instance is required to enable the private subnet EC2 Instances to get to the internet
  - Hence, the NAT instance MUST be configured in a **public subnet**
  - EC2 instances with Public/Elastic IP addresses do not need to go through NAT instances to access the Internet
- NAT instance need to be assigned a security group
- No traffic initiated from the Internet can access the private subnet through the NAT instance
  - Only responses to traffic initiated from the private subnets are allowed through NAT instances
- Only admin SSH traffic can be allowed to the NAT instance (or RDP if Windows)

NAT Gateway

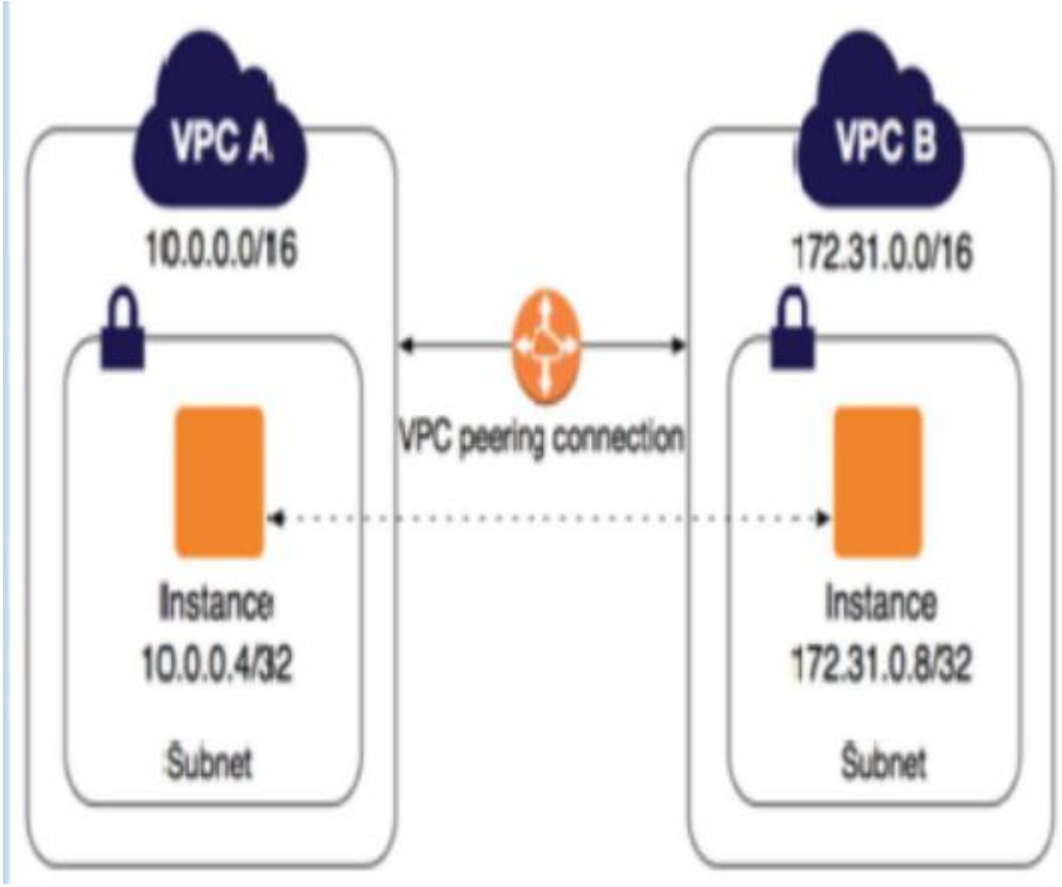
- Is an AWS managed service (Highly available, redundant..etc)
  - Customer does not need to worry about patching or OS updates
- Can not be assigned a security group
- AWS is responsible for its security/patching…etc
- Can scale to 10s of Gbps throughput
- Works only with an Elastic IP, can Not use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

VPC Flow Logs

- VPC Flow Logs enables you to capture information about the IP traffic going to and from network interfaces in your VPC.
- Flow log data can be published to Amazon CloudWatch Logs or Amazon S3.
- Flow logs can help you with a number of tasks, such as:
  - Diagnosing overly restrictive security group rules
  - Monitoring the traffic that is reaching your instance
  - Determining the direction of the traffic to and from the network interfaces

VPC Peering

- By default VPCs can not communicate with each other.
- To allow VPC to communicate each other, we need to setup a vpc peering connection.
- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account
- The VPCs can be in different regions

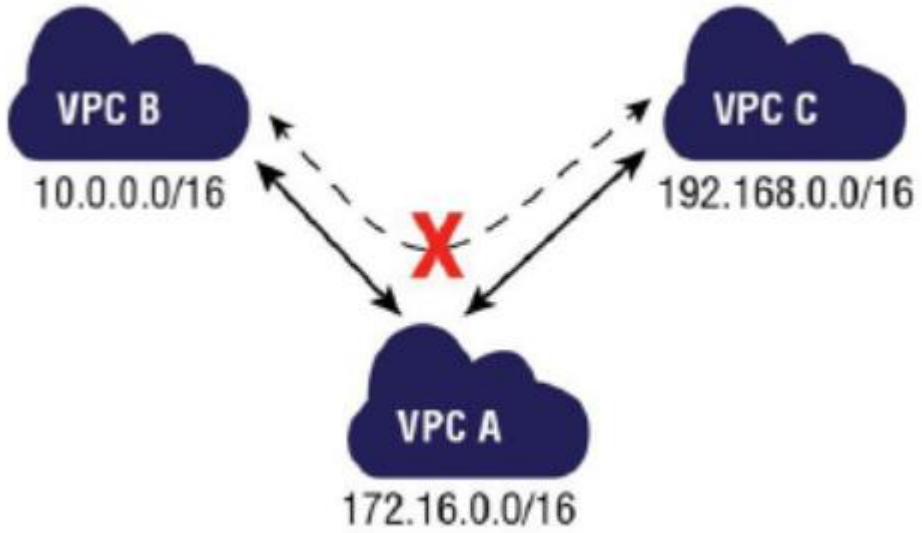


VPC Peering

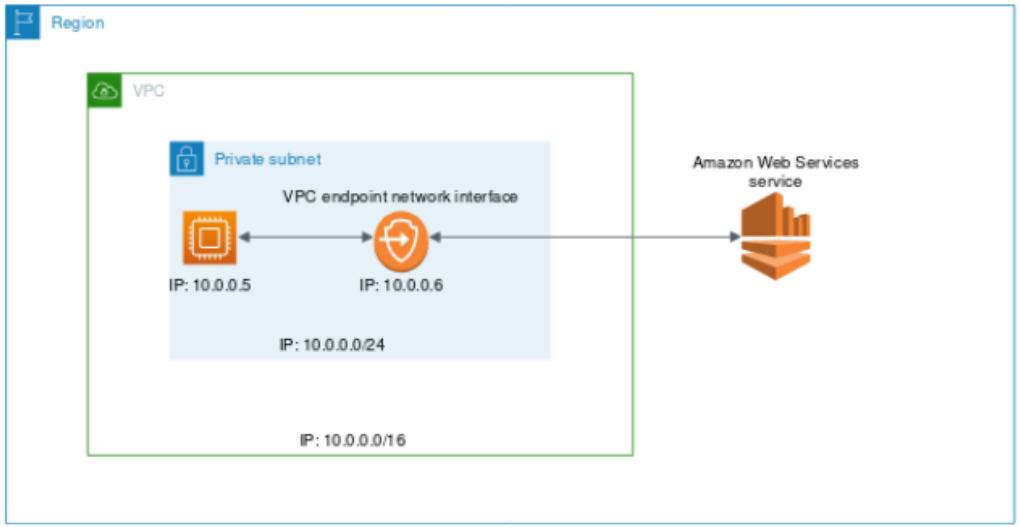
- Peering connections are created through a request/accept protocol.
- If the peer Amazon VPC is within the same account, it is identified by its VPC ID.
- If the peer VPC is within a different account, it is identified by Account ID and VPC ID.
- The owner of the peer Amazon VPC has one week to accept or reject the request.
- Routing, SG/NACL need to be updated according to communicate the traffic.

VPC Peering

- An Amazon VPC may have multiple peering connections, and peering is a one-to-one relationship between Amazon VPCs.
- Peering connections do not support transitive routing.
- You cannot create a peering connection between Amazon VPCs that have matching or overlapping CIDR blocks.



VPC endpoints



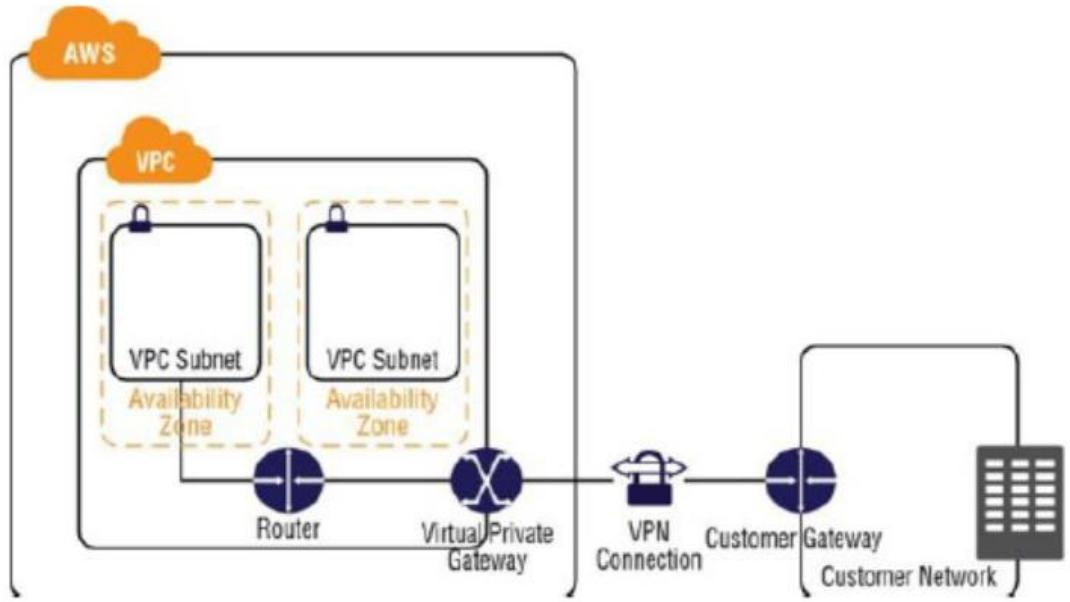
- A VPC endpoint enables you to securely connect your VPC to another supported AWS services.
- Traffic between your VPC and the other service does not leave the Amazon network.
- A VPC endpoint does not require an internet gateway, virtual private gateway, NAT device, VPN connection, or AWS Direct Connect connection.
- Instances in your VPC do not require public IP addresses to communicate with resources in the service.

Virtual Private Gateways (VPGs), Customer Gateways (CGWs) and Virtual Private Networks (VPNs)

- You can connect an existing data center to Amazon VPC using either hardware or software VPN connections.
- Virtual Private Gateway (VPG) are VPN concentrator on AWS side of the VPN connection between the two networks.
- Customer Gateway (CGW) represents a physical device or a software application on the customer's side of the VPN connection.
- After these two elements of VPC have been created, it is last step to create VPN tunnel
- VPN tunnel is established after traffic is generated from customer's side of VPN connection.

VPN

- Following are the important points to understand about VPGs, CGWs, and VPNs
  - The VPG is the AWS end of the VPN tunnel.
  - The CGW is a hardware or software application on the customer's side of the VPN tunnel.
  - You must initiate the VPN tunnel from the CGW to the VPG.
  - VPGs support both dynamic routing with BGP and static routing.
  - The VPN connection consists of two tunnels for higher availability to the VPC.



AWS Direct Connect

- AWS Direct Connect is a cloud service solution to establish a dedicated network connection from your premises to AWS.
- Establish a private connection between AWS and your datacenter.
- Speed up to 100 Gbps.