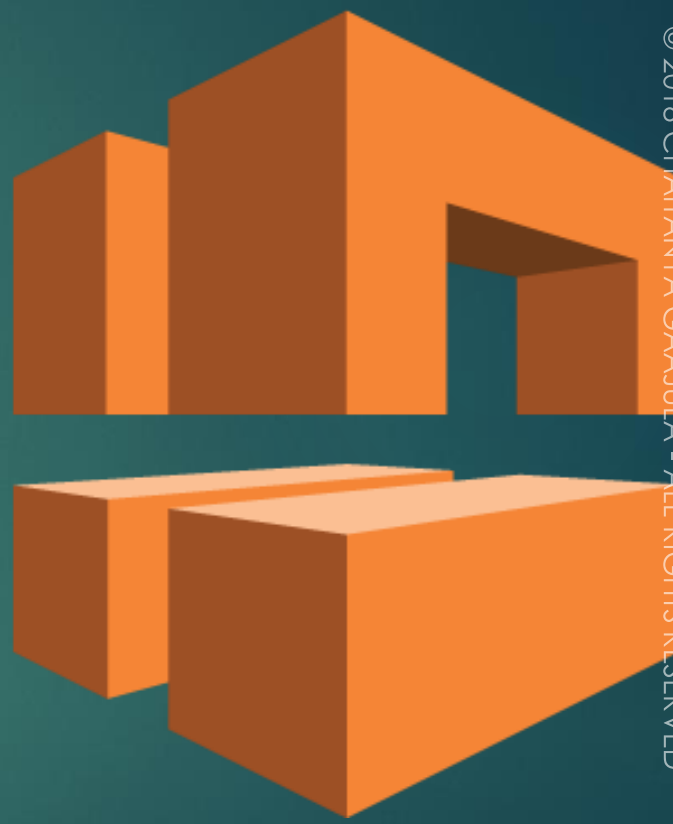
Virtual Private Cloud

Agenda

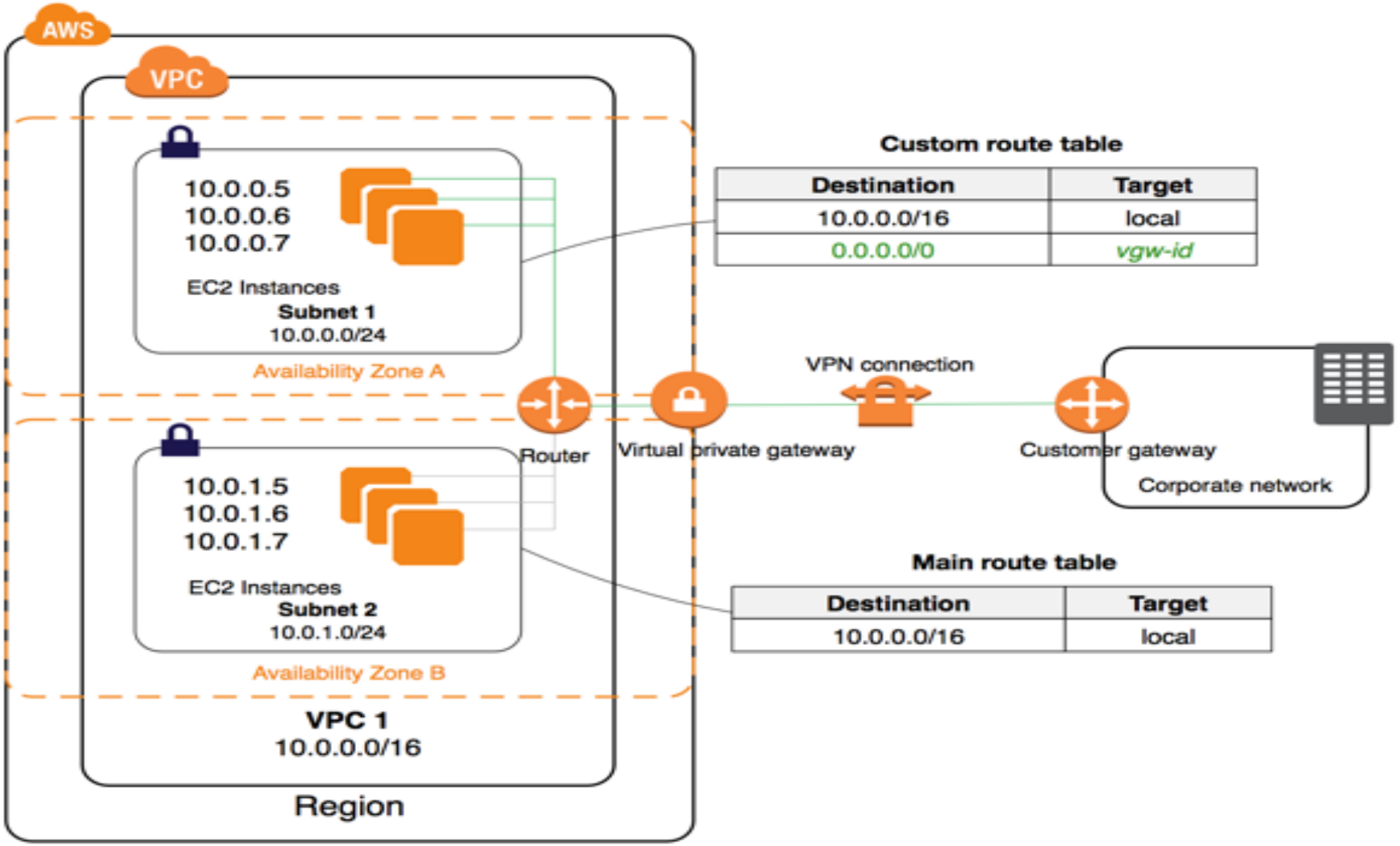
- What is VPC
- VPC Features / Components / Types
- Public and Private Subnet
- VPC Security
- Security Groups and ACL Rules
- Flow Logs
- VPC Limitations
- VPC Peering
- Quiz
- Hands-On Lab



What is VPC

- Amazon Virtual Private Cloud (VPC) enables you to launch AWS resources into a virtual network that you've defined.
- A Virtual Private Cloud is a virtual network dedicated to your AWS account.
- It is logically isolated from other virtual networks in the AWS cloud.
- You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.
- You can configure your VPC; you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings.
- Use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.

Overview of VPC



VPC Features

- Attach one or more network interfaces to your instances
- Assign multiple IP addresses to your instances
- Assign static private IPv4 addresses to your instances
- Access control lists (ACL)
- Run your instances on single-tenant hardware
- Egress & Ingress filtering

AWS VPC: Types

Default VPC

Non-Default VPC

Default Vs Non-Default VPC's

Characterisitics	Default VPC	Non-Default VPC
Public IP Address	Instance receives Public IP Address by default	Instance does not receive Public IP Address by default
Private IP Address	Instance receives a static IP private address from the range of default VPC	Instance receives a static IP private address from the range of VPC
DNS Hostnames	Are enabled by default	Are disabled by default
Accessing the internet	Instance can access the internet	Instances cannot access the internet
Internet Gateway	It is attached to the default VPC and the default subnet has a route to IGW	Depends on how it was created

AWS VPC: Components

- Subnets
- Route Tables
- Internet Gateway
- NAT Gateway
- Security Groups
- ACL's
- VPC Peering
- VPN

Route Tables

- A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.
- Each subnet in your VPC must be associated with a route table
- The table controls the routing for the subnet.
- A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Internet Gateway

An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet.

Uses:

- Provides a target in your VPC route tables for Internet-routable traffic
- Performs network address translation (NAT) for instances that have been assigned public IPv4 addresses.
- An Internet gateway supports IPv4 and IPv6 traffic.

Private, Public and Elastic IP address

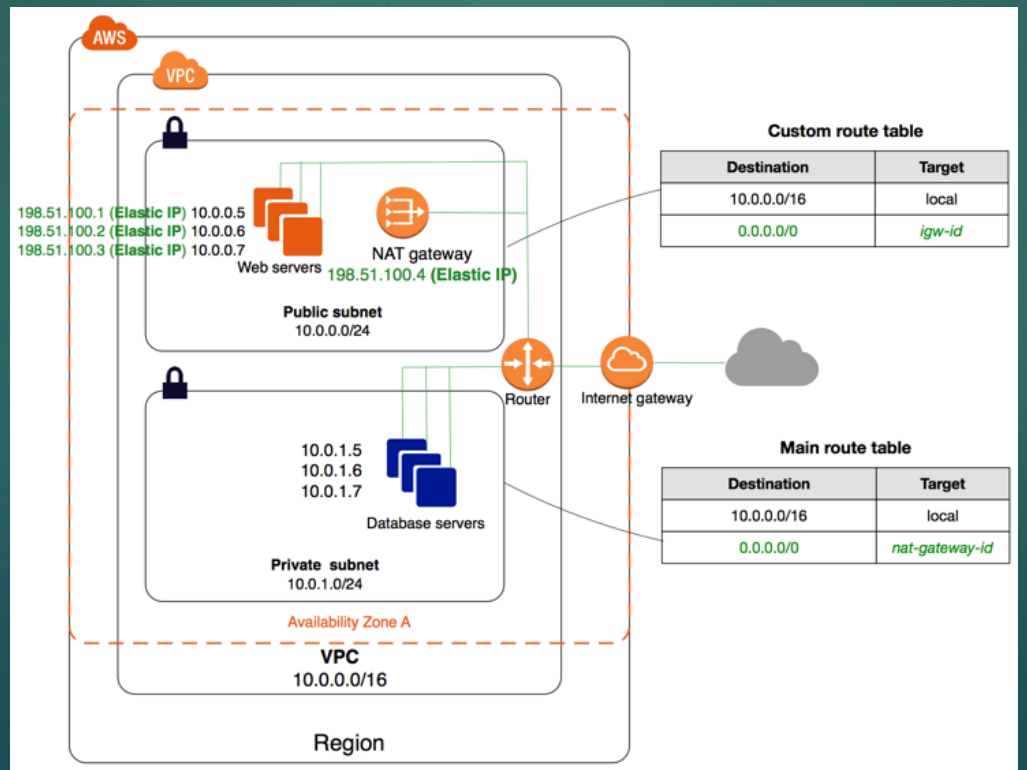
- A private IPv4 address is an IP address that's not reachable over the Internet. Private IPv4 addresses are used for communication between instances in the same network

- A public IP address is an IPv4 address that's reachable from the Internet. You can use public addresses for communication between your instances and the Internet.

- An Elastic IP address is a static public IPv4 address that could be allocate to AWS account. KIt could be associated to and from instances as required, and it's allocated to the account until you choose to release it

NAT Device

- NAT device helps to enable instances in a private subnet to connect to the Internet (for example, for software updates) or other AWS services, but prevent the Internet from initiating connections with the instances.
- A NAT device forwards traffic from the instances in the private subnet to the Internet or other AWS services, and then sends the response back to the instances.

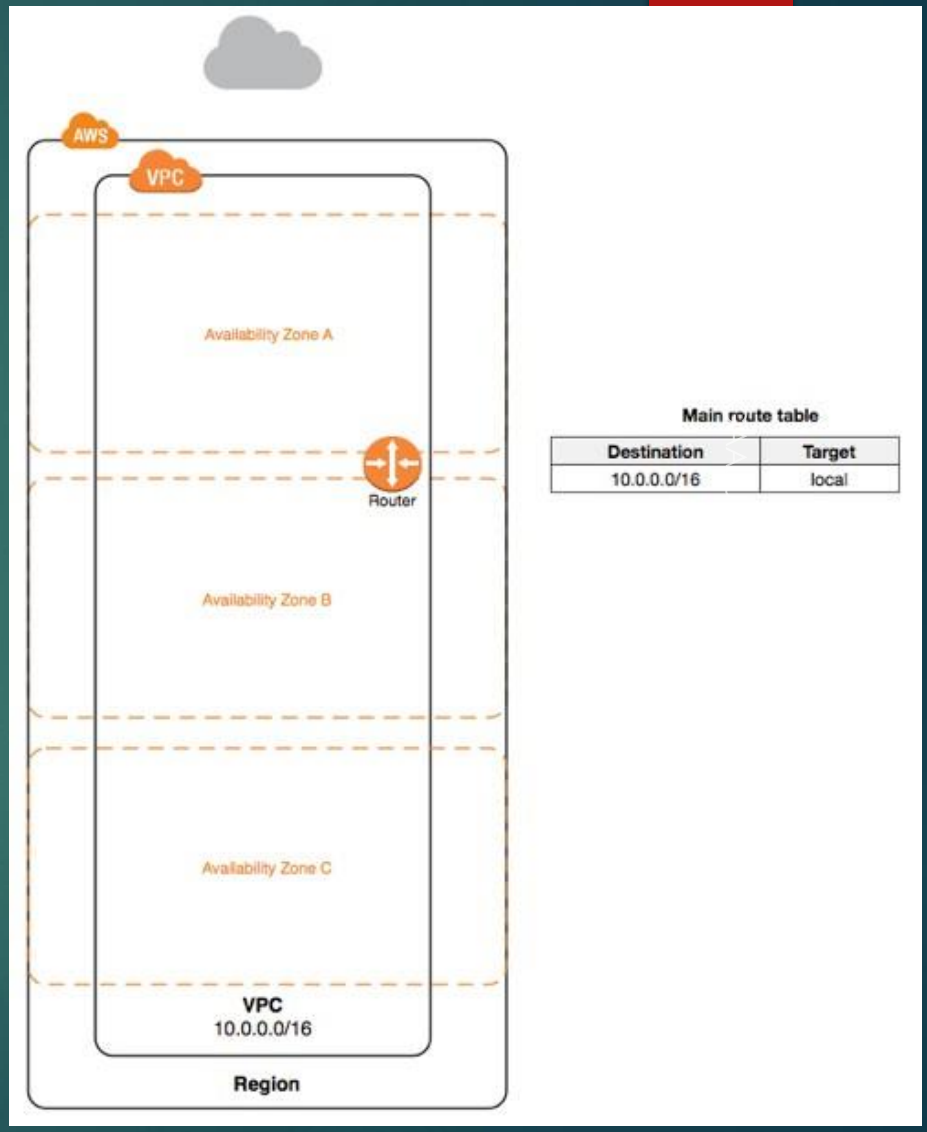


Nat Gateway and Nat Instances

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Supports bursts of up to 10Gbps.	Depends on the bandwidth of the instance type.
Maintenance	Managed by AWS.You do not need to perform any maintenance.	Managed by you, for example, by installing software updates or operating system patches on the instance.
Performance	Software is optimized for handling NAT traffic.	A generic Amazon Linux AMI that's configured to perform NAT.
Cost	Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.	Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size.
Type and size	Uniform offering; you don't need to decide on the type or size.	Choose a suitable instance type and size, according to your predicted workload.

AWS VPC: VPC and Subnet

- Specify a range of IP addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block.
- Example, 10.0.0.0/16. This is the primary CIDR block for your VPC.
- Allowed block size is between a /16 netmask and /28 netmask.
- For subnet, specify the CIDR block for the subnet, which is a subset of the VPC CIDR block.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.
- Use http://www.subnet-calculator.com/cidr.php

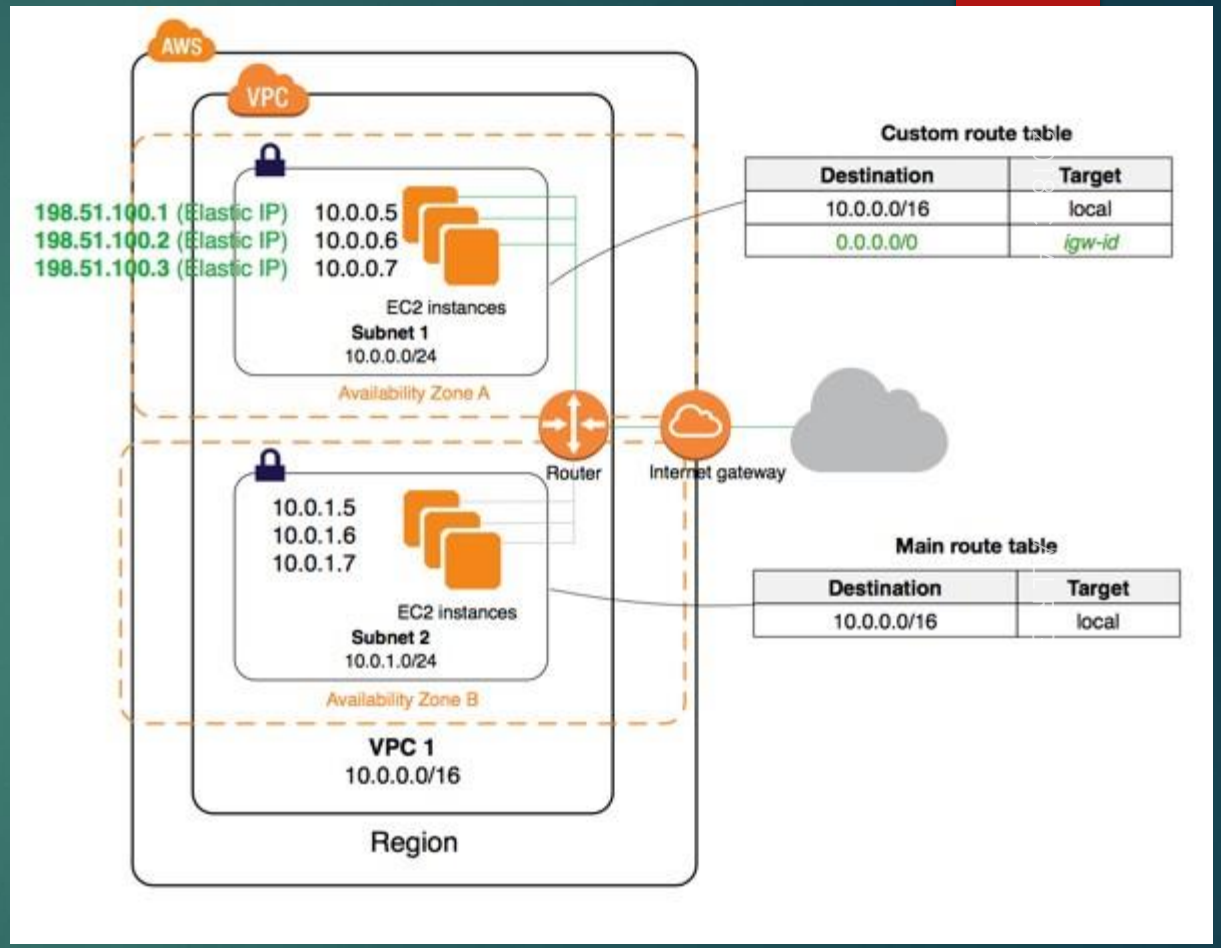


Subnet Mask Classes

Address Class	Value in First Octet	Classful Mask (dotted decimal)	Classful Mask (prefix notation)
A	1 - 126	255.0.0.0	/8
B	128 - 191	255.255.0.0	/16
C	192 - 223	255.255.255.0	/24
D	224 - 239	N/A	N/A
E	240 - 255	N/A	N/A

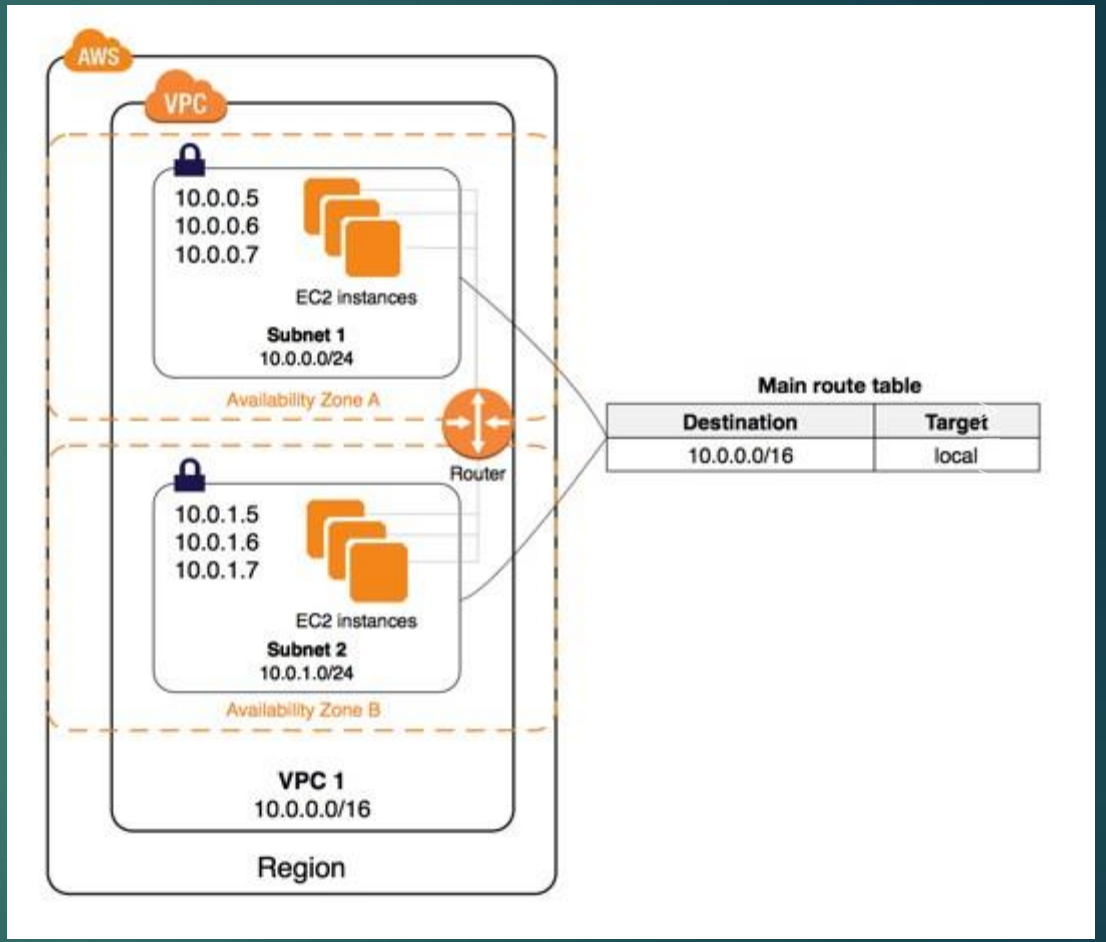
AWS VPC: Public Subnet

- A public subnet is a subnet that has access to the Internet through an Internet gateway.
- Each instance has a private address and public address.
- These instances can communicate with each other, and access the Internet.



AWS VPC: Private Subnet

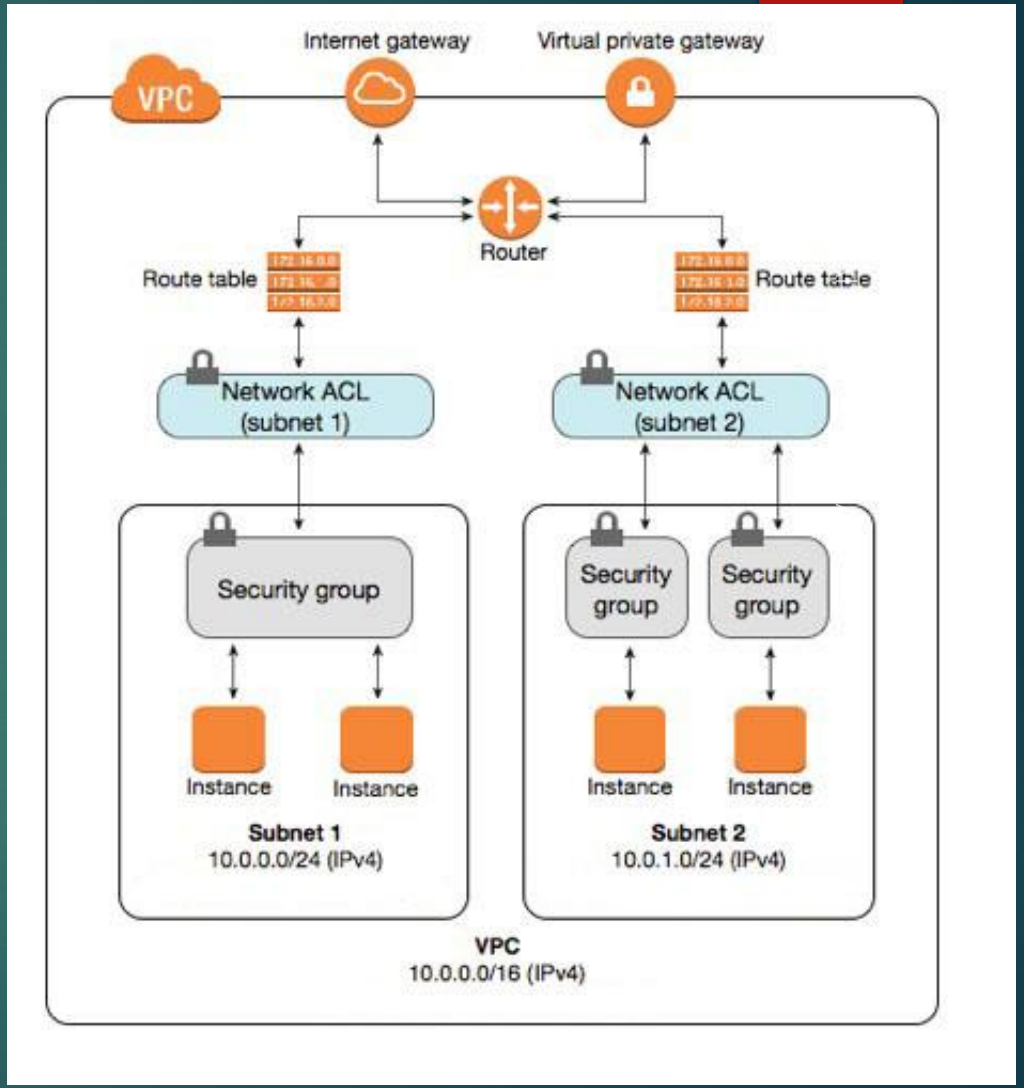
- If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet.
- By default, each instance has a private address, but no public address.
- These instances can communicate with each other, but can't access the Internet.



AWS VPC: Security

- VPC provides features to increase and monitor the security for your VPC:
  - **Security Groups**
  - **Network Access Control Lists (ACLs)**
  - **Flow Logs**

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	Is stateless
Evaluate all rules before deciding whether to allow traffic	Process rules in number order when deciding whether to allow traffic



AWS VPC: ACL Rules

Inbound ACL Rule						
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/ Deny**	**Comments**
100	HTTP	TCP	80	0.0.0.0/0	Allow	Allows inbound HTTP traffic from any IP address
110	HTTPS	TCP	443	0.0.0.0/0	Allow	Allows inbound HTTPS traffic from any IP address
120	RDP	TCP	3389	192.0.2.0/2	Allow	Allows inbound RDP traffic from IP address range
130	Custom TCP	TCP	32768-6553	0.0.0.0/0	Allow	Allows inbound return traffic from the Internet [ephemeral port]
*	All Traffic	All	All	0.0.0.0/0	Deny	Denies all inbound IP traffic not already handled by a preceding rule

Outbound ACL Rule						
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/ Deny**	**Comments**
100	HTTP	TCP	80	0.0.0.0/0	Allow	Allows outbound IP HTTP traffic from the subnet to the Internet
110	HTTPS	TCP	443	0.0.0.0/0	Allow	Allows outbound IP HTTPS traffic from the subnet to the Internet
120	Custom TCP	TCP	32768-6553	50.0.0.0/0	Allow	Allows outbound responses to clients on the Internet [ephemeral port]
*	All Traffic	All	All	0.0.0.0/0	Deny	Denies all outbound IP traffic not already handled by a preceding rule

AWS VPC: Flow Logs

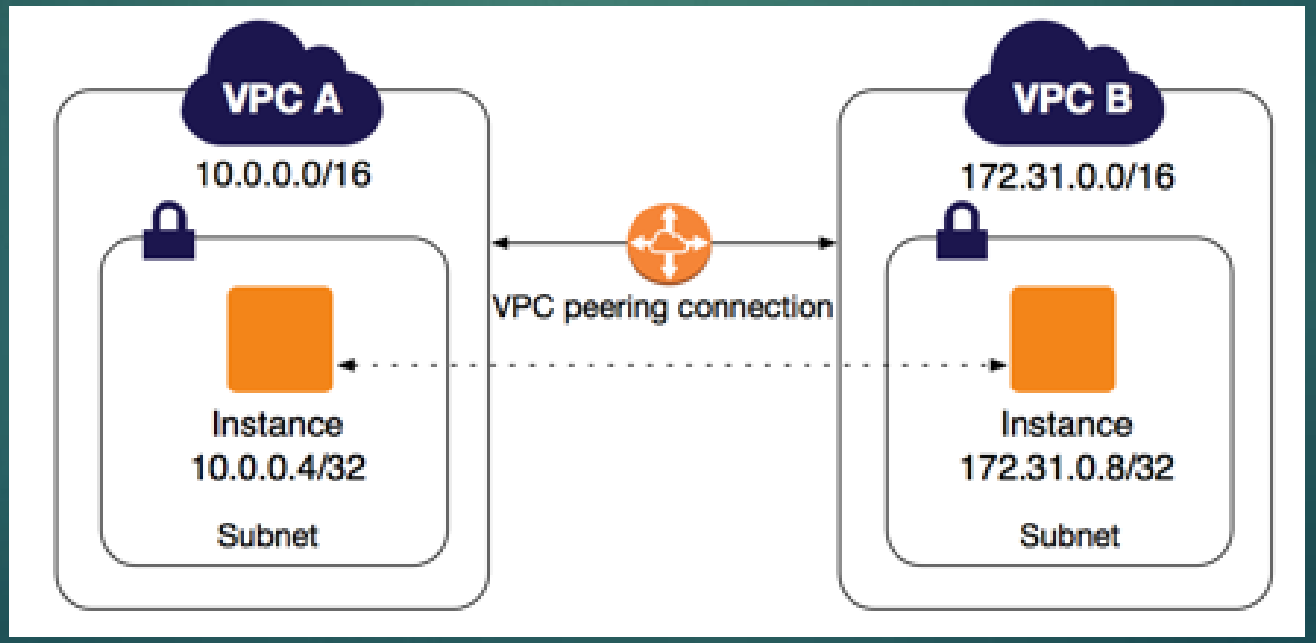
- VPC Flow Logs enables you to capture information about the IP traffic going to and from network interfaces in your VPC.
- Flow log data is stored using Amazon CloudWatch Logs.
- After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.
- You can create a flow log for:
  - VPC
  - Subnet
  - Network Interface
- Flow log format:
  - version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log- status

AWS VPC: Limitations

Resource	Default Limit
VPCs per region	5
Subnets per VPC	200
Internet gateways per region	5
NAT gateways per Availability Zone	5
Virtual private gateways per region	5
Network ACLs per VPC	200
Rules per network ACL	20
Route tables per VPC	200
Routes per route table	50
Active VPC peering connections per VPC	50
VPN connections per region	50

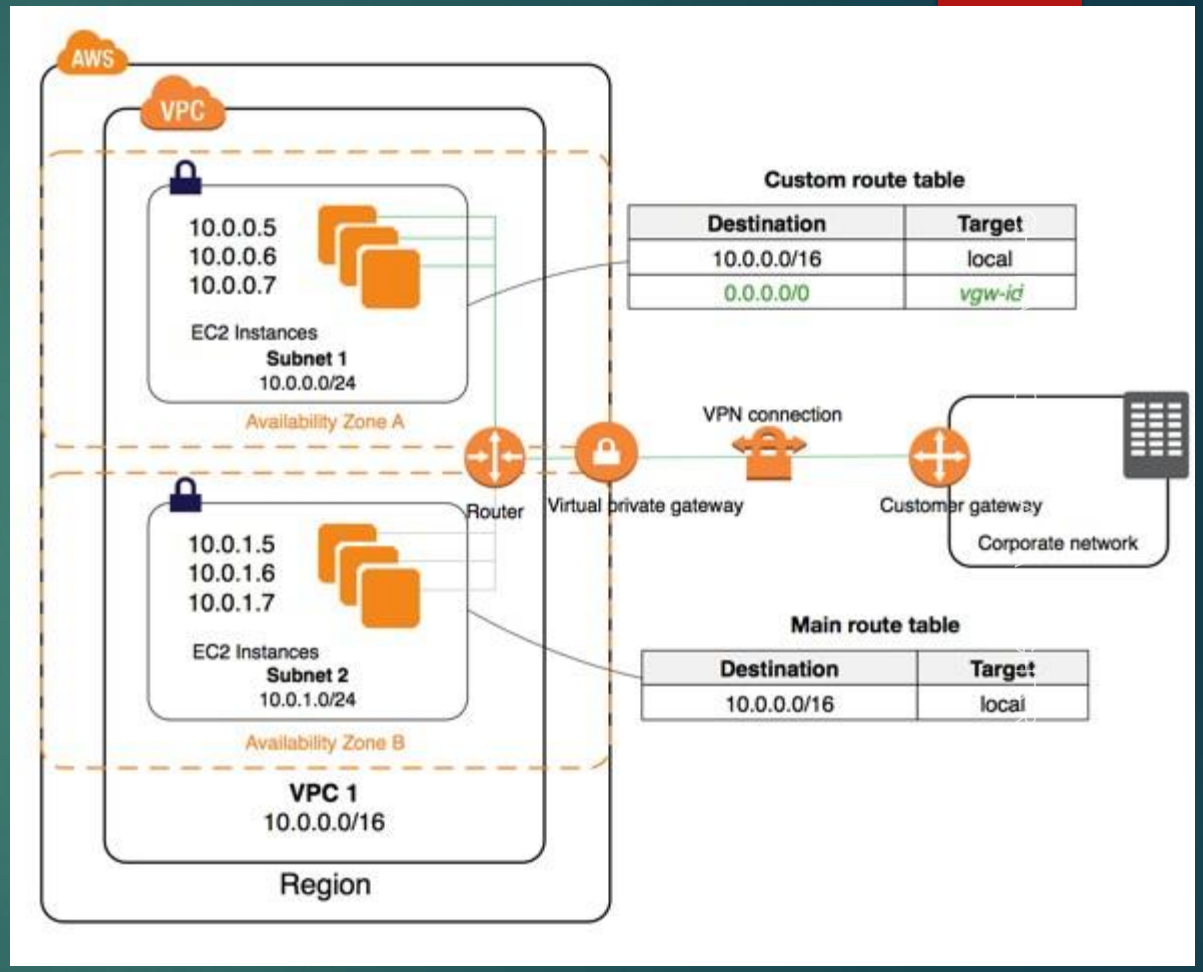
AWS VPC: Peering

- VPC peering is a networking connection between two VPCs that enables you to route traffic between them.
- Instances in either VPC can communicate with each other as if they are within the same network.
- Create a VPC peering connection between own VPCs, or with a VPC in another AWS account.
- In both cases, the VPCs must be in the same region.



AWS VPC: VPN

- Connect VPC to corporate data center using VPN connection
- This makes the AWS cloud an extension of your data center.
- VPN connection consists of a virtual private gateway and a customer gateway.



Hands-On Lab

Hands-on Lab

- Create a VPC using private address ranges CIDR block
- Create Public & Private subnet
- Manage Internet Gateway
- Manage Subnet settings
- Launch an Instance in Public & Private subnet
- Configure Web server in Public subnet
- Manage ACL
- Manage NAT Gateway

Thank You