AWS Foundation

VIRTUAL PRIVATE CLOUD (VPC)

Agenda

1. Introduction to VPC
2. Components of VPC
3. Security in VPC
4. Subnets
5. VPC Peering
6. VPC Endpoint
7. Transit Gateway and Direct Connect
8. VPN and Flow Logs
9. VPC Reachability Analyzer

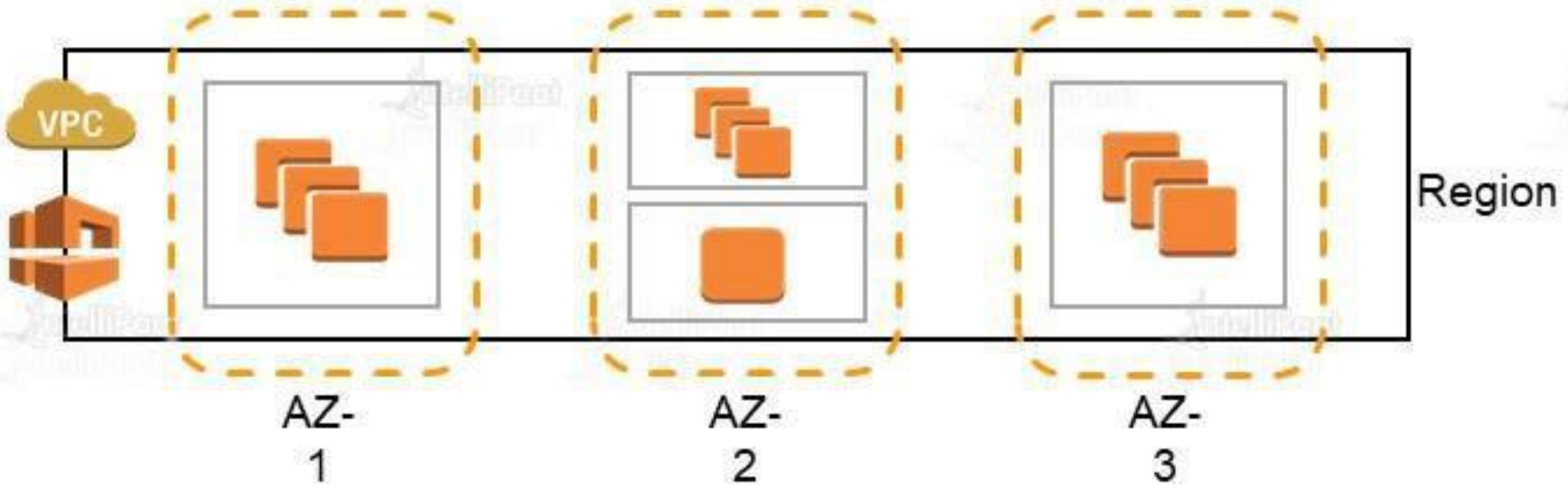
What is AWS VPC

What is a VPC ?

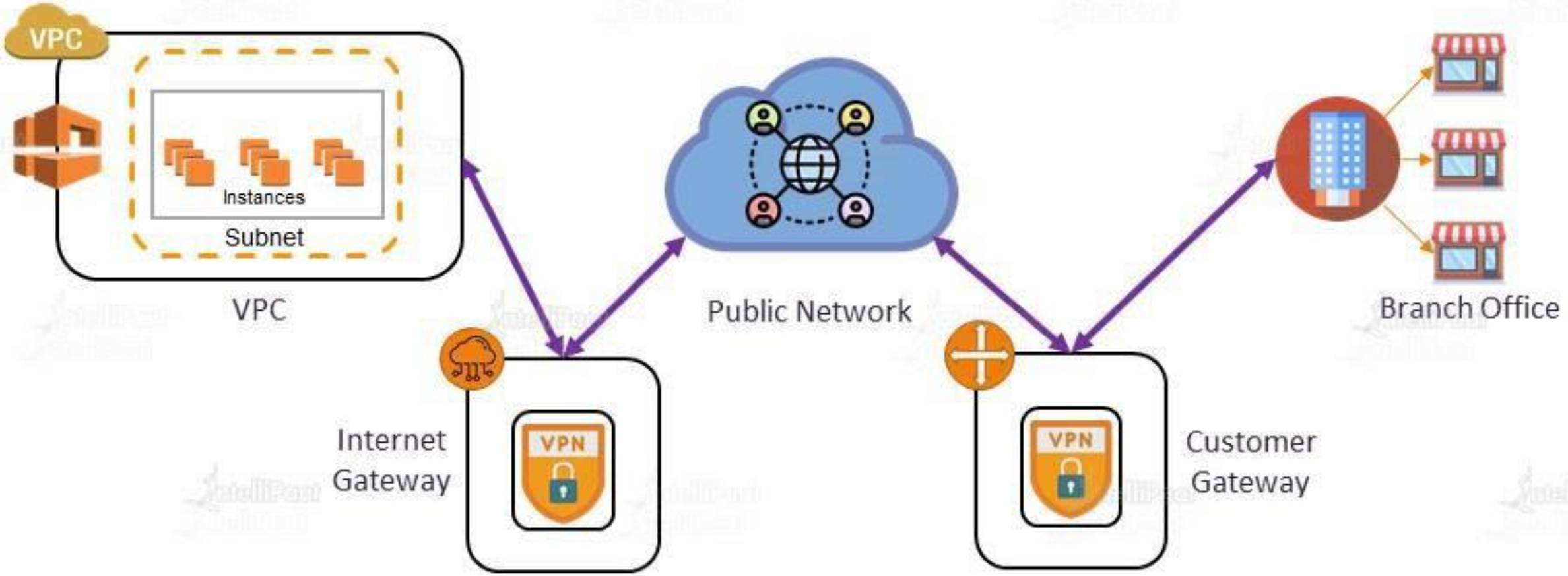
Virtual Private Cloud

Amazon VPC – Lets you create a logically isolated section of the AWS cloud where you can launch AWS services in the Virtual Network which you defined.

VPCs span all Availability Zones in a Region



What is a VPC ?



IP Addresses and CIDR Notations

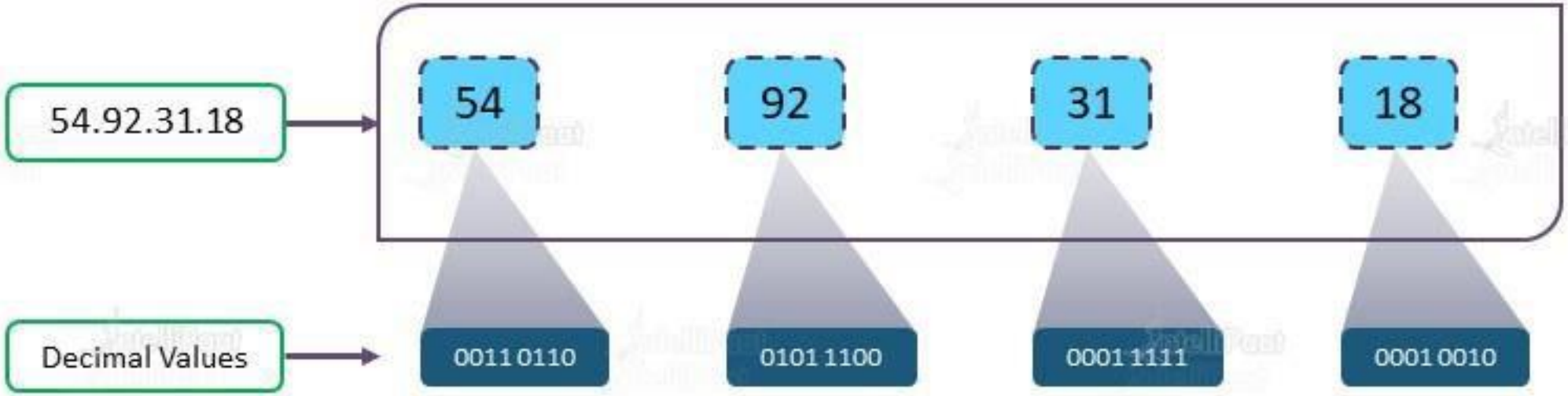
IP Addressing

A Sample IP Address

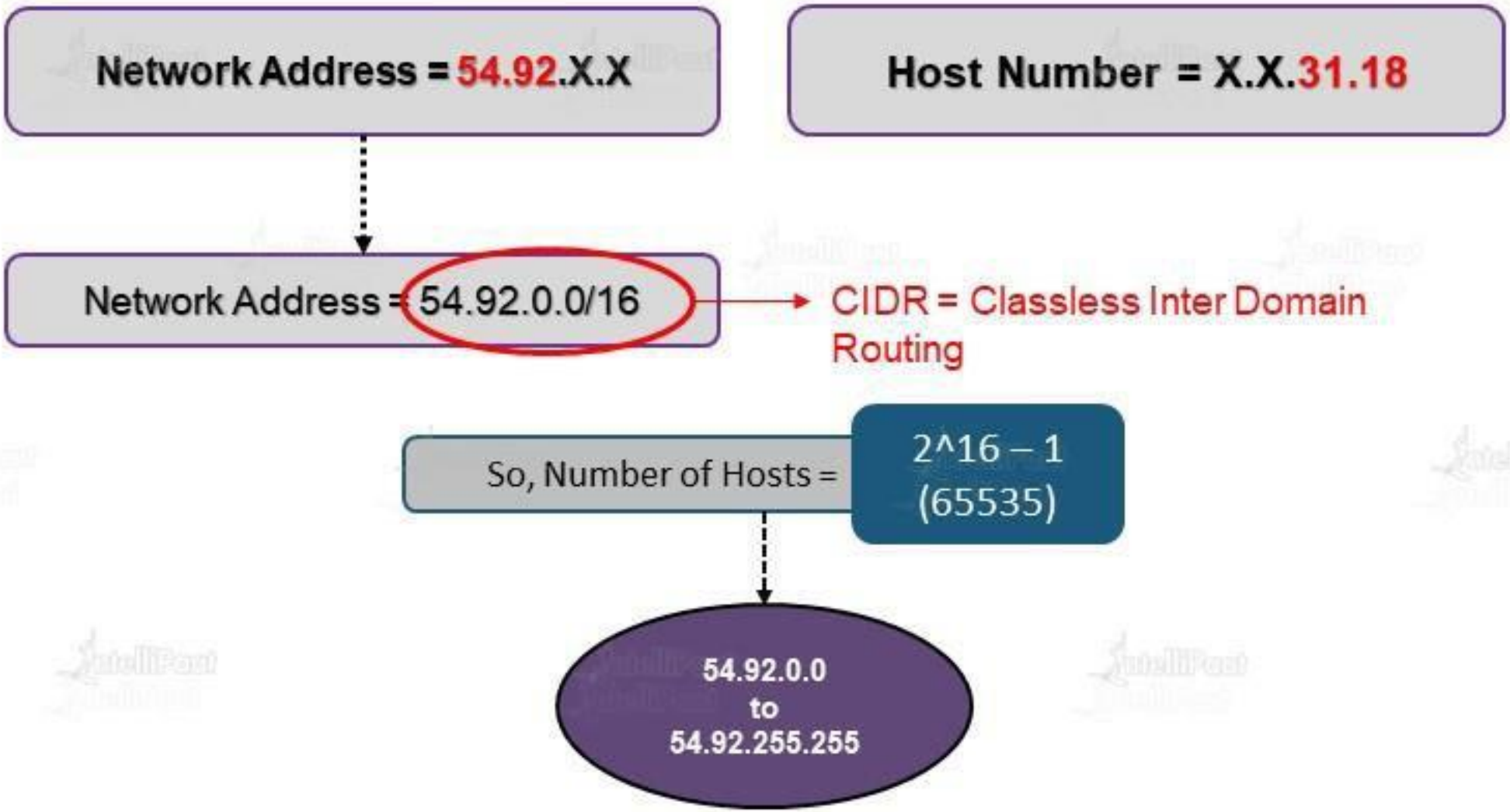
54.92.31.18

- What is an IP Address?

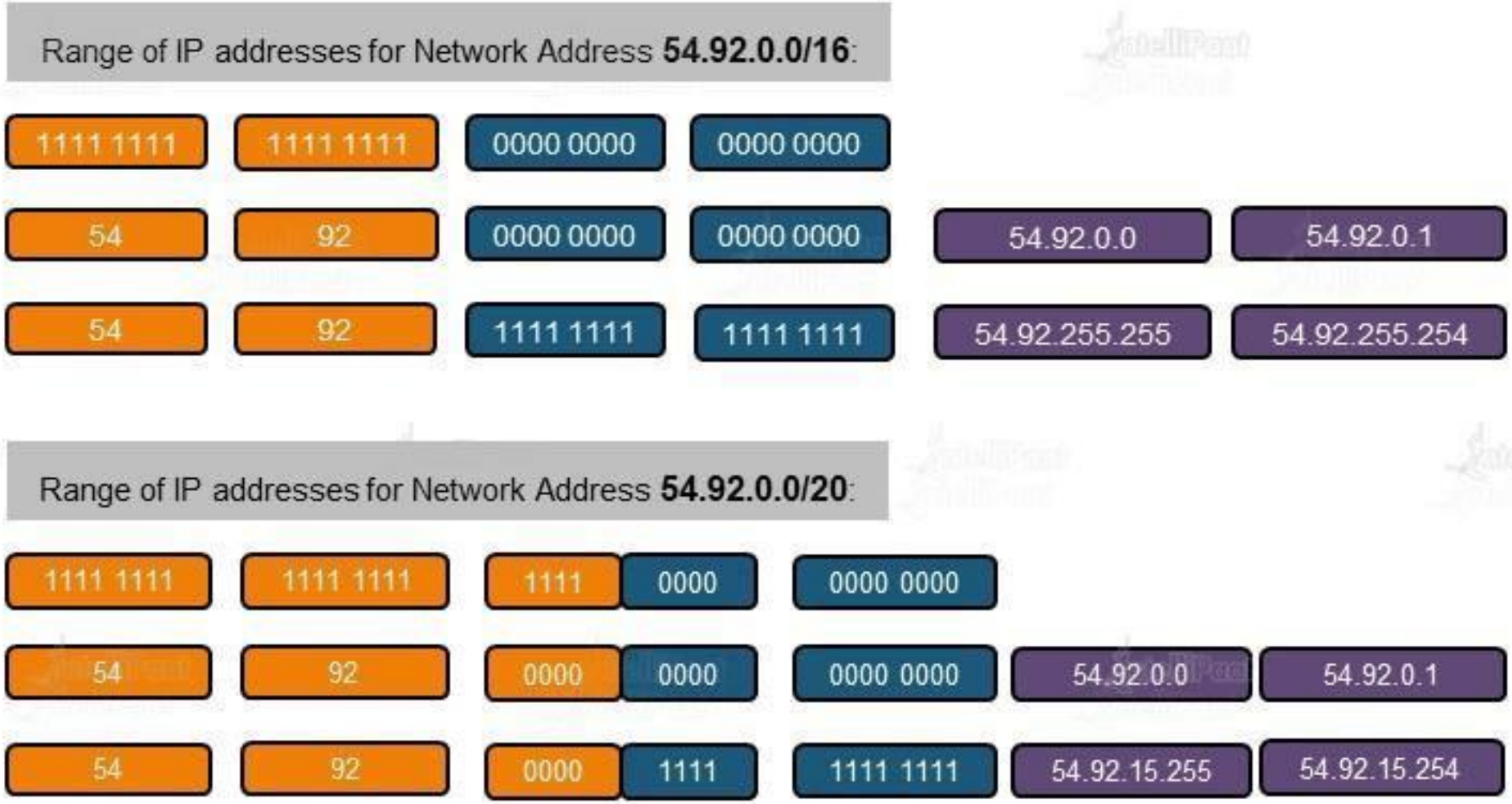
Unique string of numbers assigned to a computer using the Internet Protocol to communicate over a network



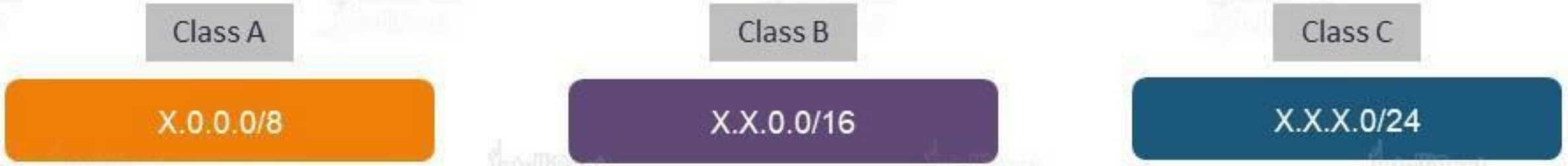
IP Addressing



IP Address for CIDR

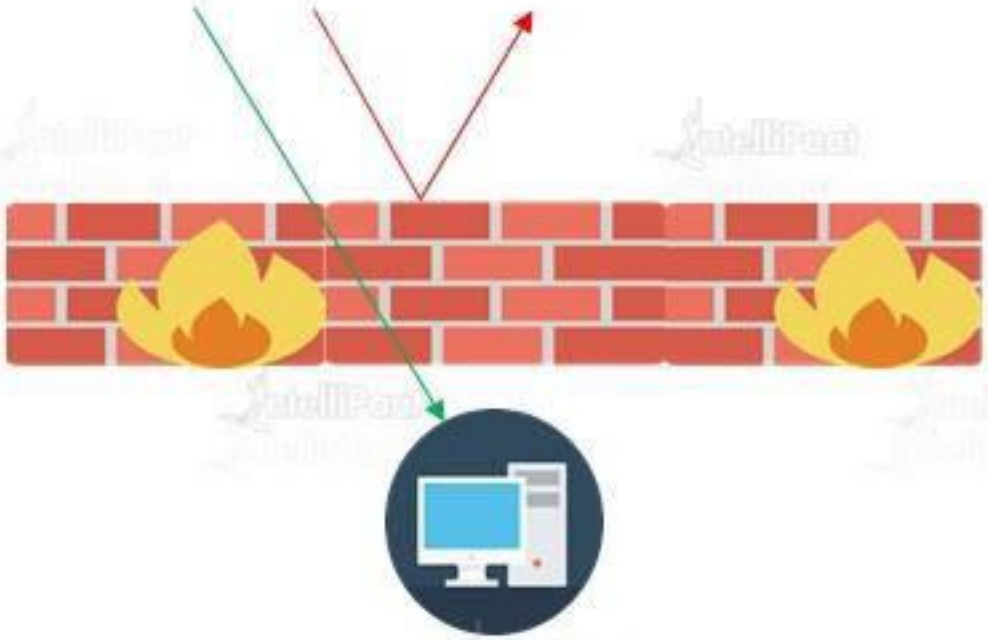


CIDR Classes



Firewall

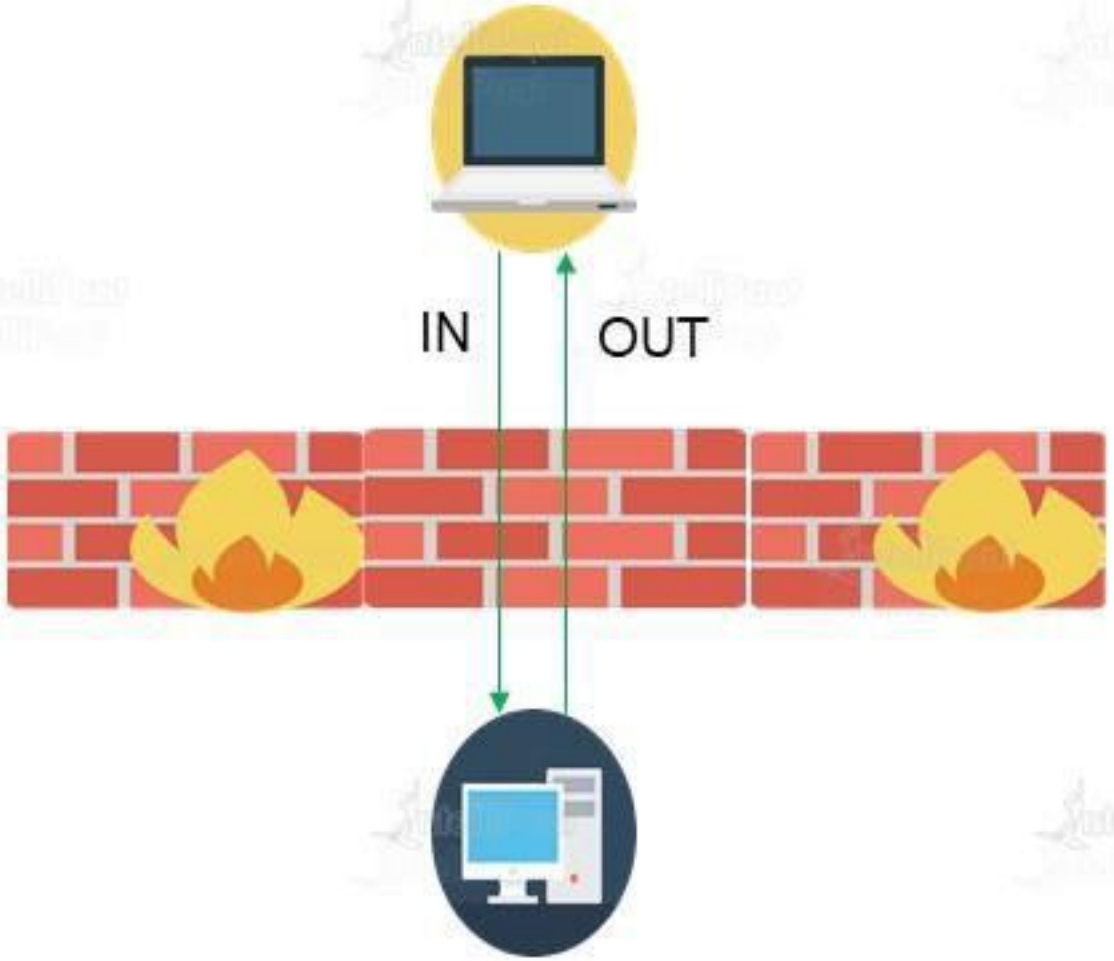
- Firewall is a system made to prevent unauthorized traffic to and from your PRIVATE network/computer/server by Allowing or Denying those traffic.
- Allowing and denying traffic are mentioned by Rules, also called firewall rules.



Firewall

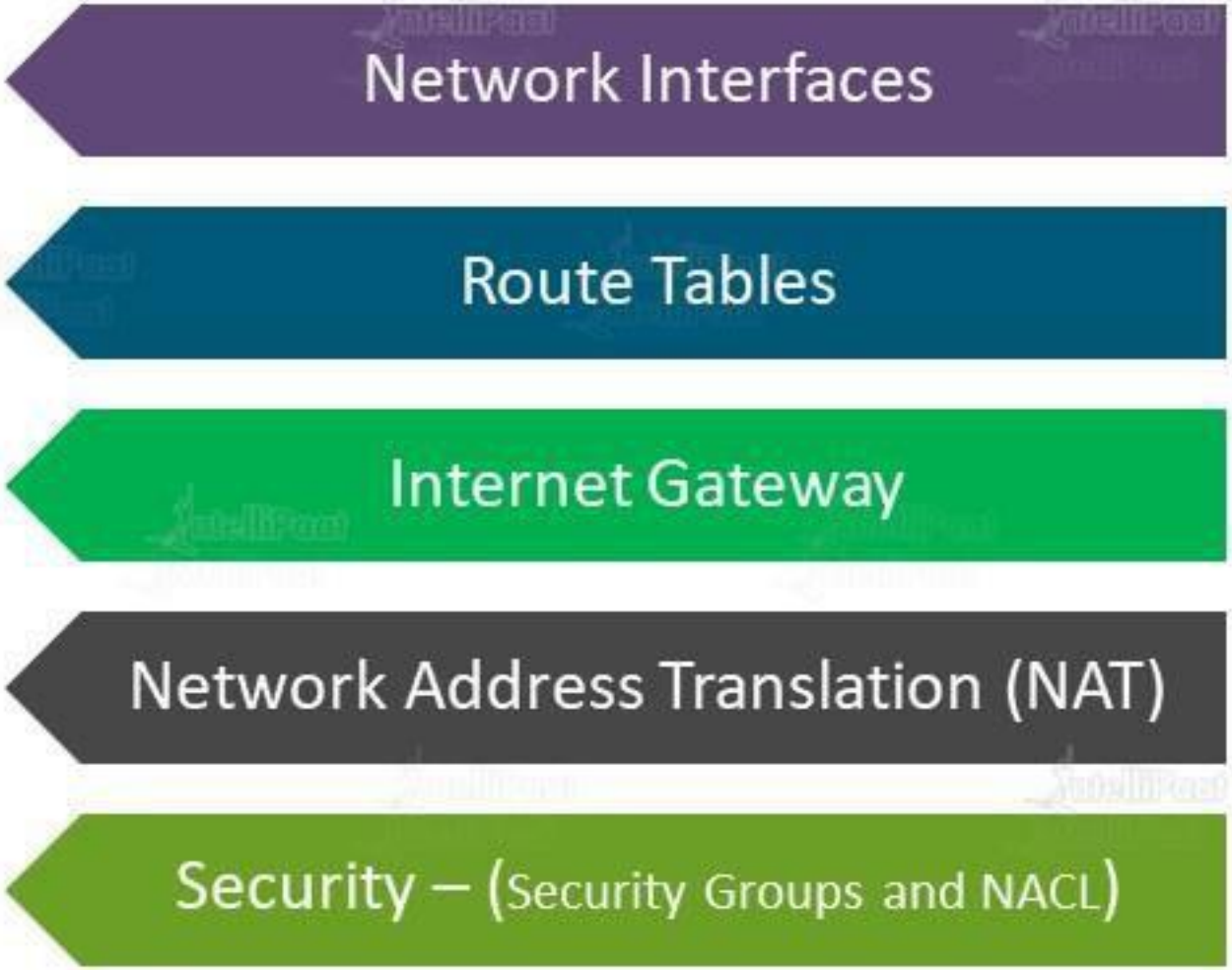
Types

- **Stateful:** No additional rules are needed for response traffic.
- **Stateless:** Rules have to be mentioned for both request and response.



Components of VPC

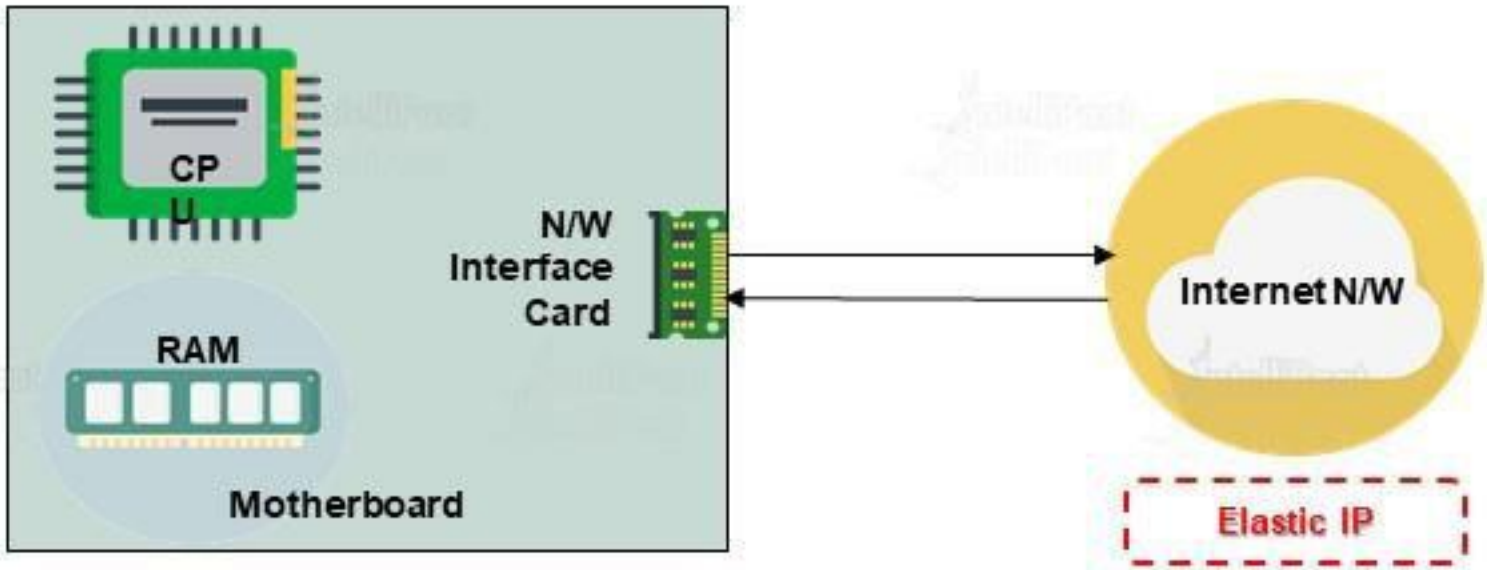
Components of VPC



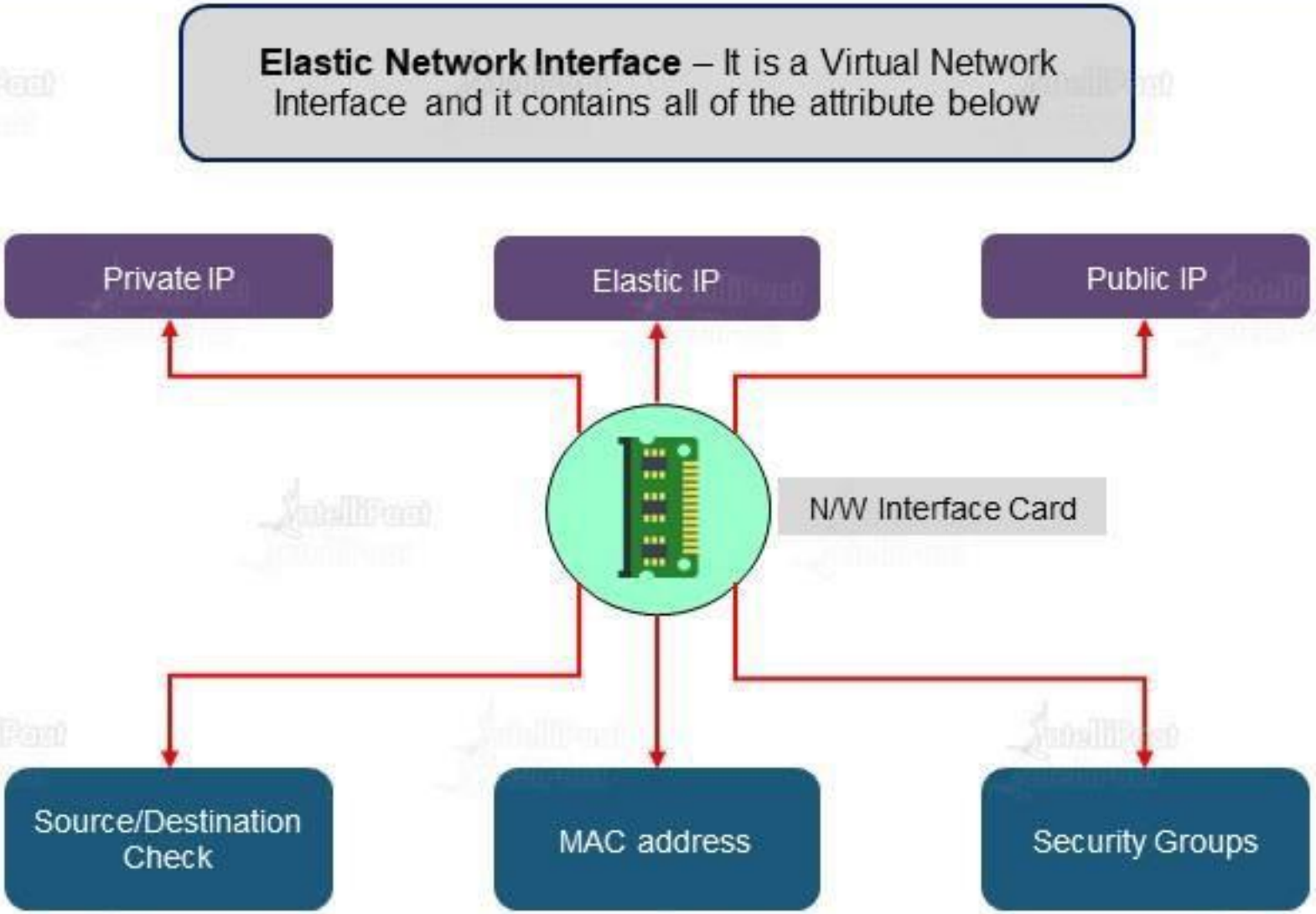
Network Interfaces

Network Interface

- Interface between a computer and an internet network.
- Network IO happens via N/W interface cards
- N/W interfaces contain – Elastic IP, Public IP, Private IP, Security Groups



Network Interfaces

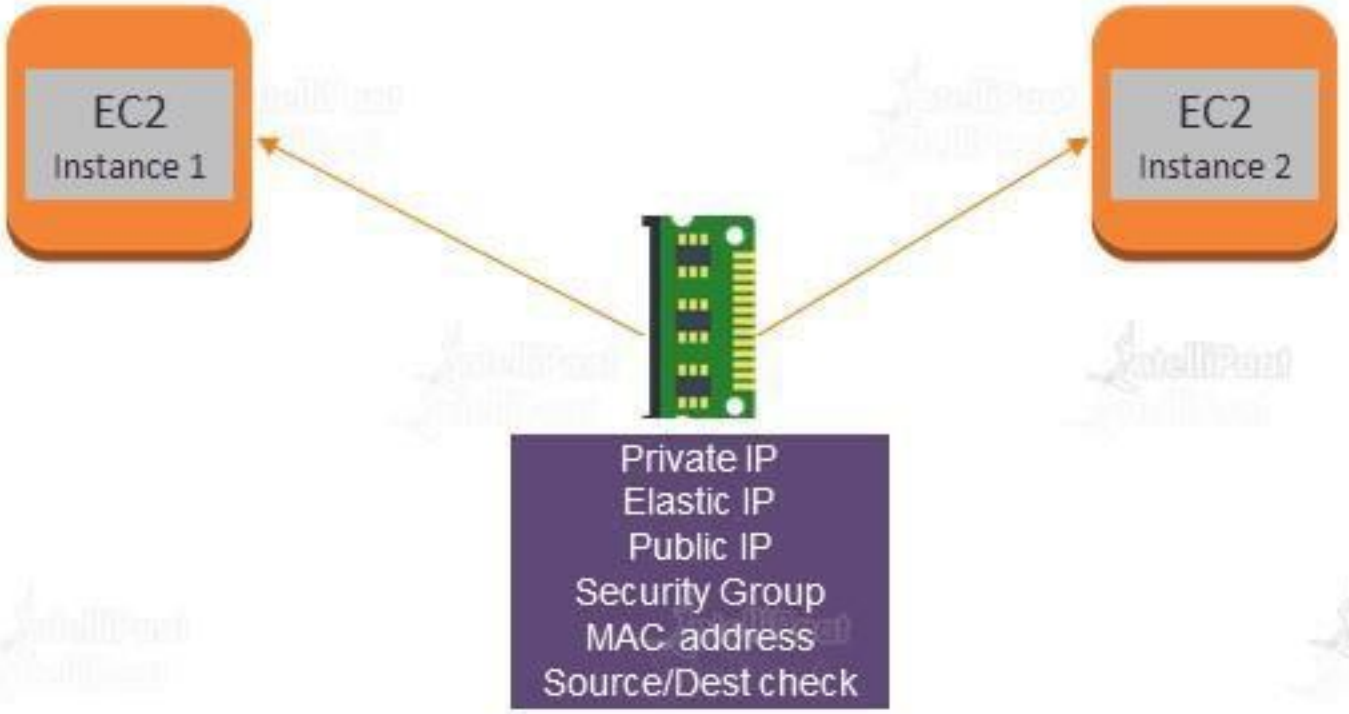


Network Interfaces

Elastic Network Interface

Network interface can be:

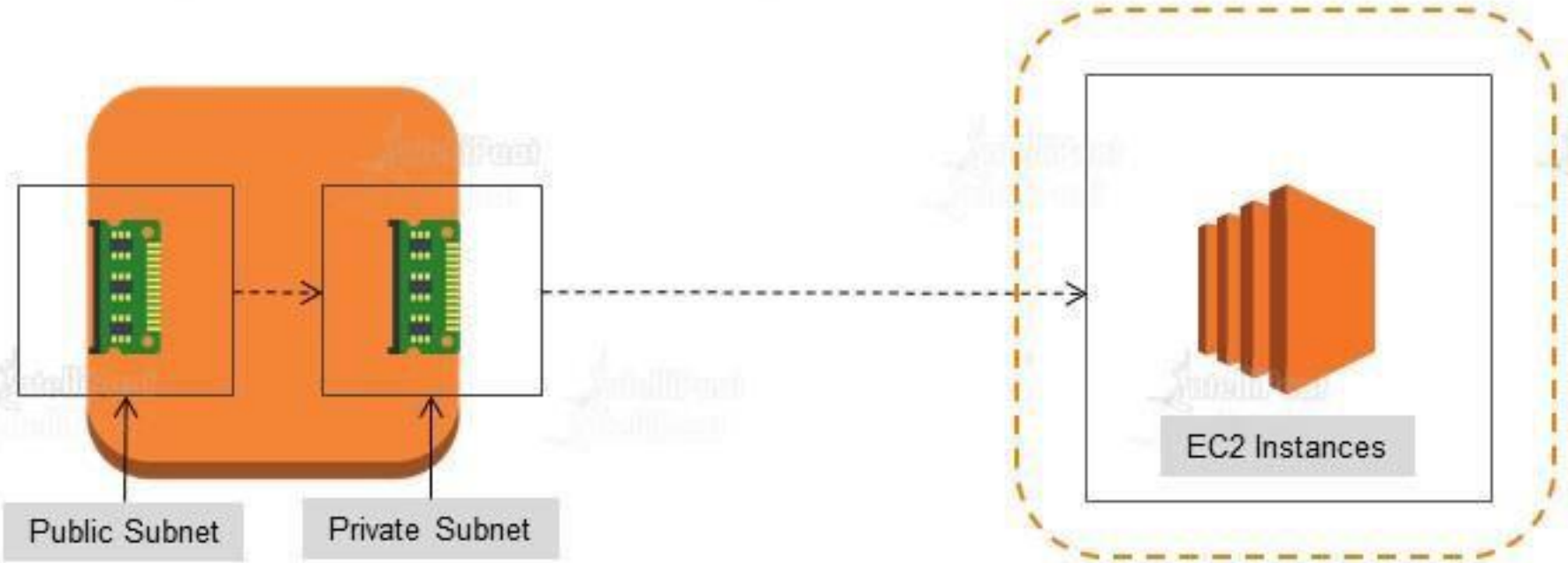
- Created to an Instance
- Attached to an Instance
- Detached from an Instance
- Re-attached to another instance.



Network Interfaces

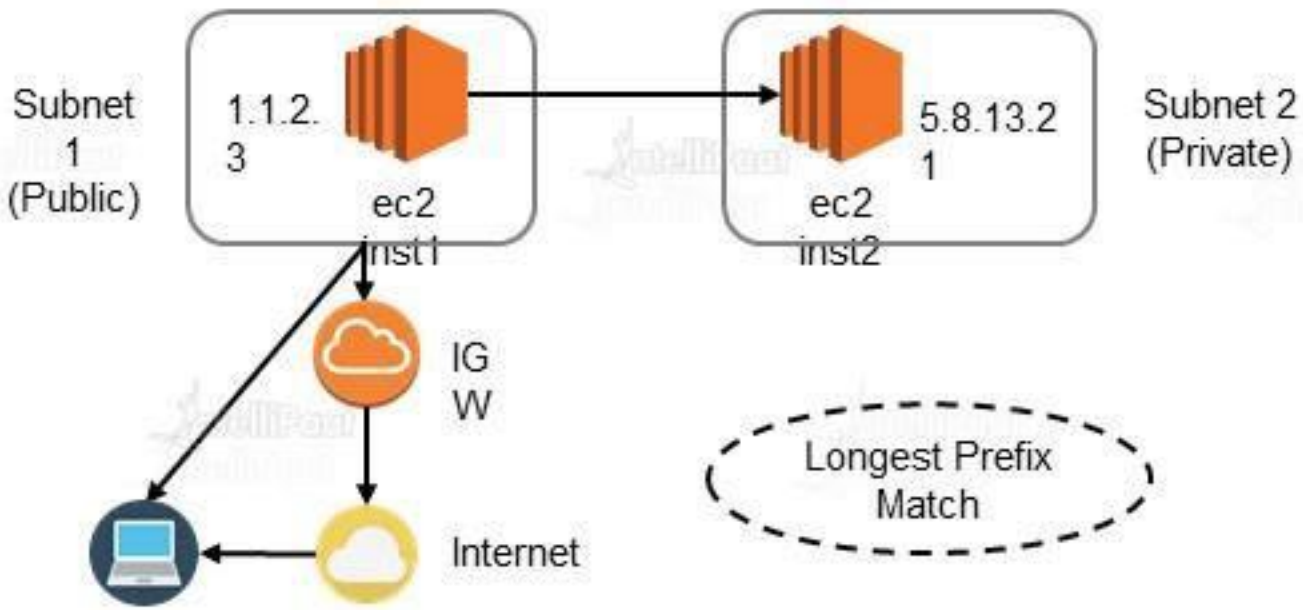
Multiple IP Addresses

- Network interface can have an additional Secondary IP address attached to it.
- IP address can be assigned to n/w interfaces attached to a running or stopped instance.



Route Tables

- Route table tells a machine/network where traffic is directed.
- Directions are defined by "routes" in Route Tables.
- Each subnet must be associated with a Route.
- All VPCs come with an implicit router and a main route table which can be modified.



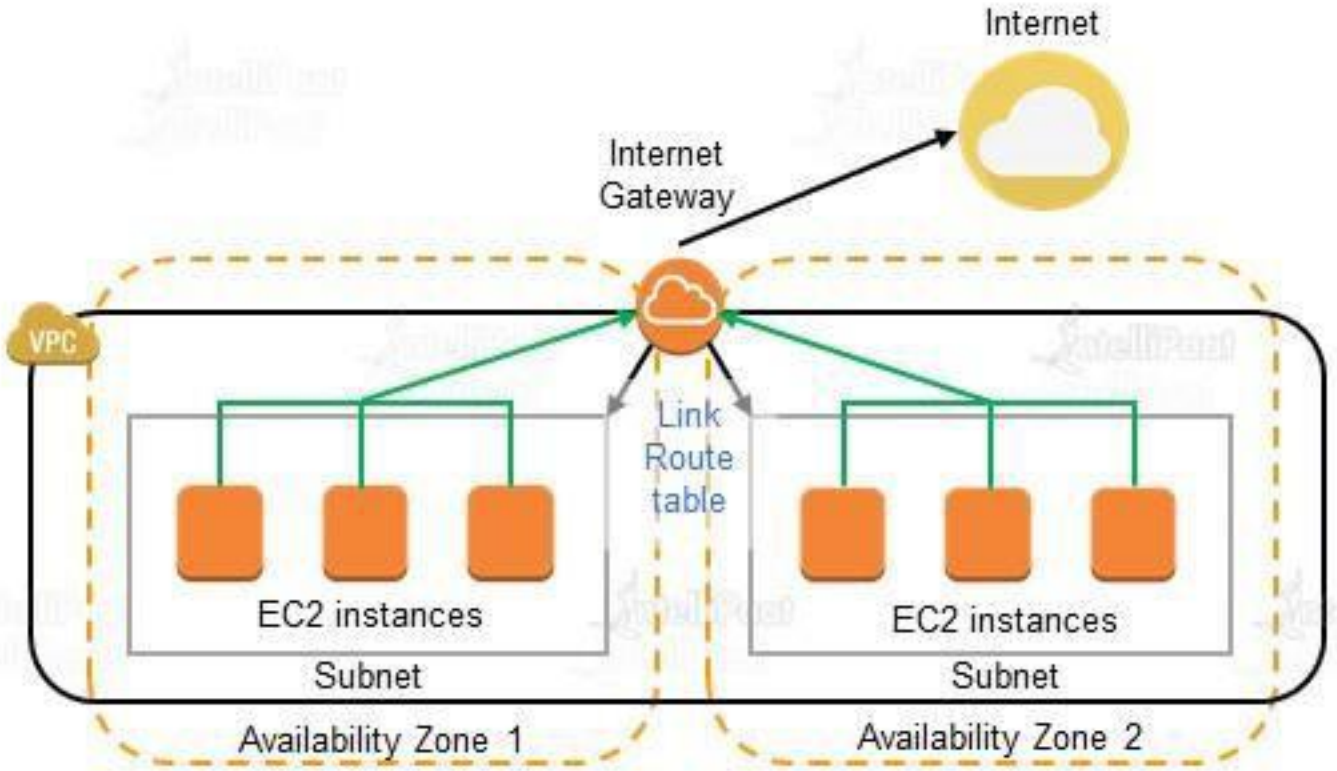
Destination	Target
5.8.13.21	Local
0.0.0.0/0	IGW
6.4.2.1/32	IGW

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

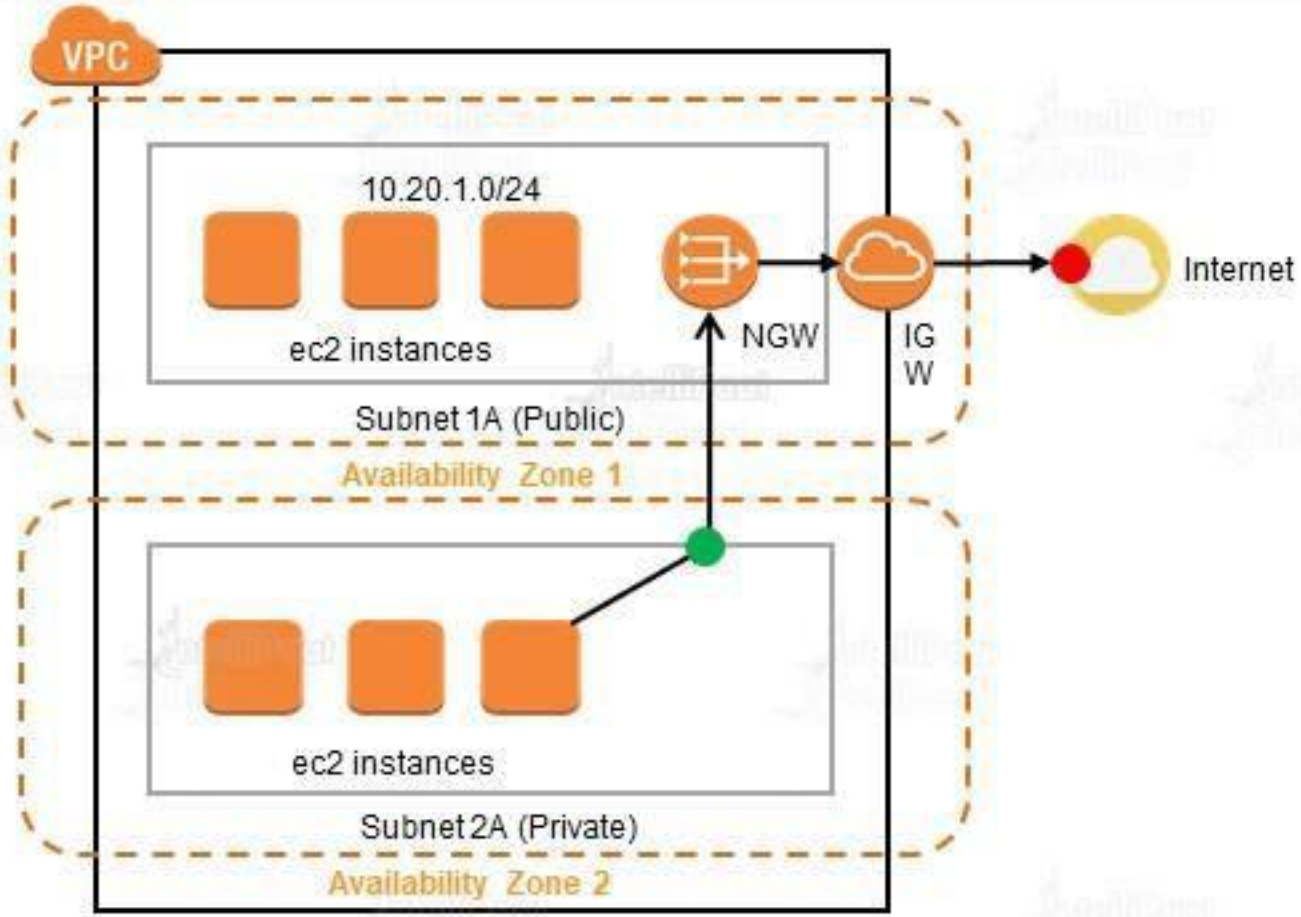
Purpose of an Internet Gateway

- Created to an Instance
- Attached to an Instance
- Detached from an Instance
- Re-attached to another instance.



Network Address Translation

- Internet cannot initiate any connection to the instances via NAT.
- NAT devices enable instances in the Private Subnet to connect to Internet and brings responses back to the instances.
- NAT devices are created in Public Subnet.



Destination	Target
10.20.1.0/24	Local
0.0.0.0/0	NAT gateway

Network Address Translation

NAT Gateway vs NAT Instance

NAT Gateway	NAT Instance
Implemented with redundancy.	Failover has to be managed manually using scripts.
Supports Burst up to 10 Gbps.	Depends on the bandwidth of the instance type.
Entirely managed by AWS.	Has to be managed by the customer.
No size.	Instance type and size can be selected.
Only NACLs can be used to filter traffic.	Both Security Groups and NACLs can be used.
Elastic IP has to be associated.	Both Elastic IP and Public IP can be used.

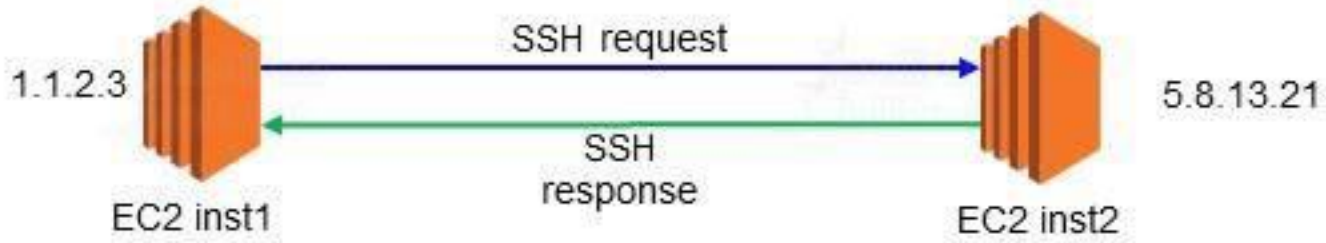
IntelliPaat

Security in VPC

Security

Security Groups

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic



Outbound EC2 inst1

Type	Protocol	Port	Destination
SSH	TCP	22	5.8.13.21

TO 5.8.13.21

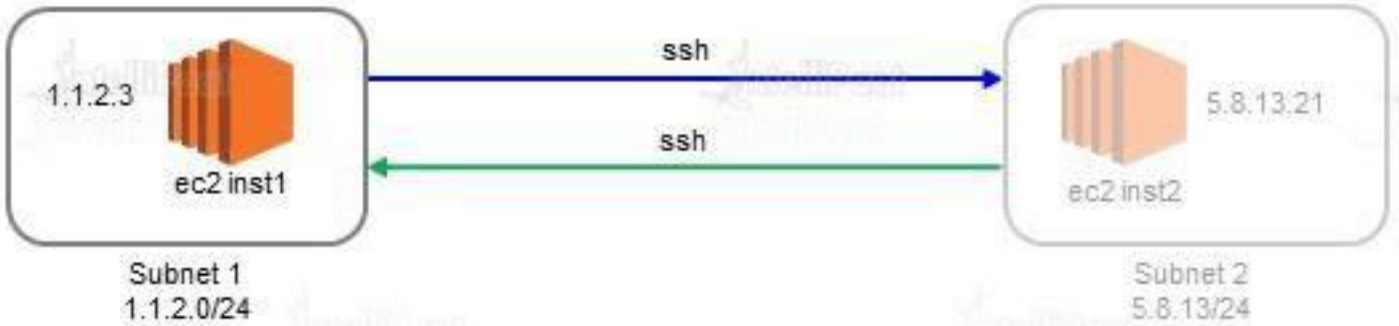
Inbound EC2 inst2

Type	Protocol	Port	Source
SSH	TCP	22	1.1.2.3

FROM 1.1.2.3

Security

Network ACLs



- Network Access Control Lists
- Optional layer of security for your VPC that acts as a firewall
- Controls traffic in and out of one or more subnets

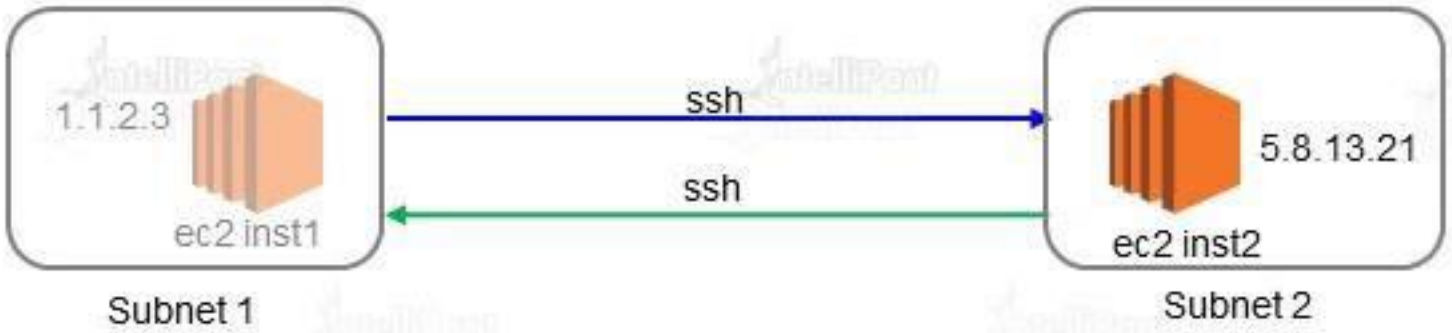
subnet1	Rule No.	Type	Protocol	Port	Destination	Allow/Deny
Outbound	100	SSH	TCP	22	5.8.13.0/24	ALLOW
Outbound	200	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

subnet1	Rule No.	Type	Protocol	Port	Source	Allow/Deny
Inbound	50	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
Inbound	100	SSH	TCP	1024-65535	5.8.13.0/24	ALLOW

subnet1	Rule No.	Type	Protocol	Port	Source	Allow/Deny
Inbound	100	SSH	TCP	1024-65535	5.8.13.0/24	ALLOW
Inbound	200	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Security

Network ACLs

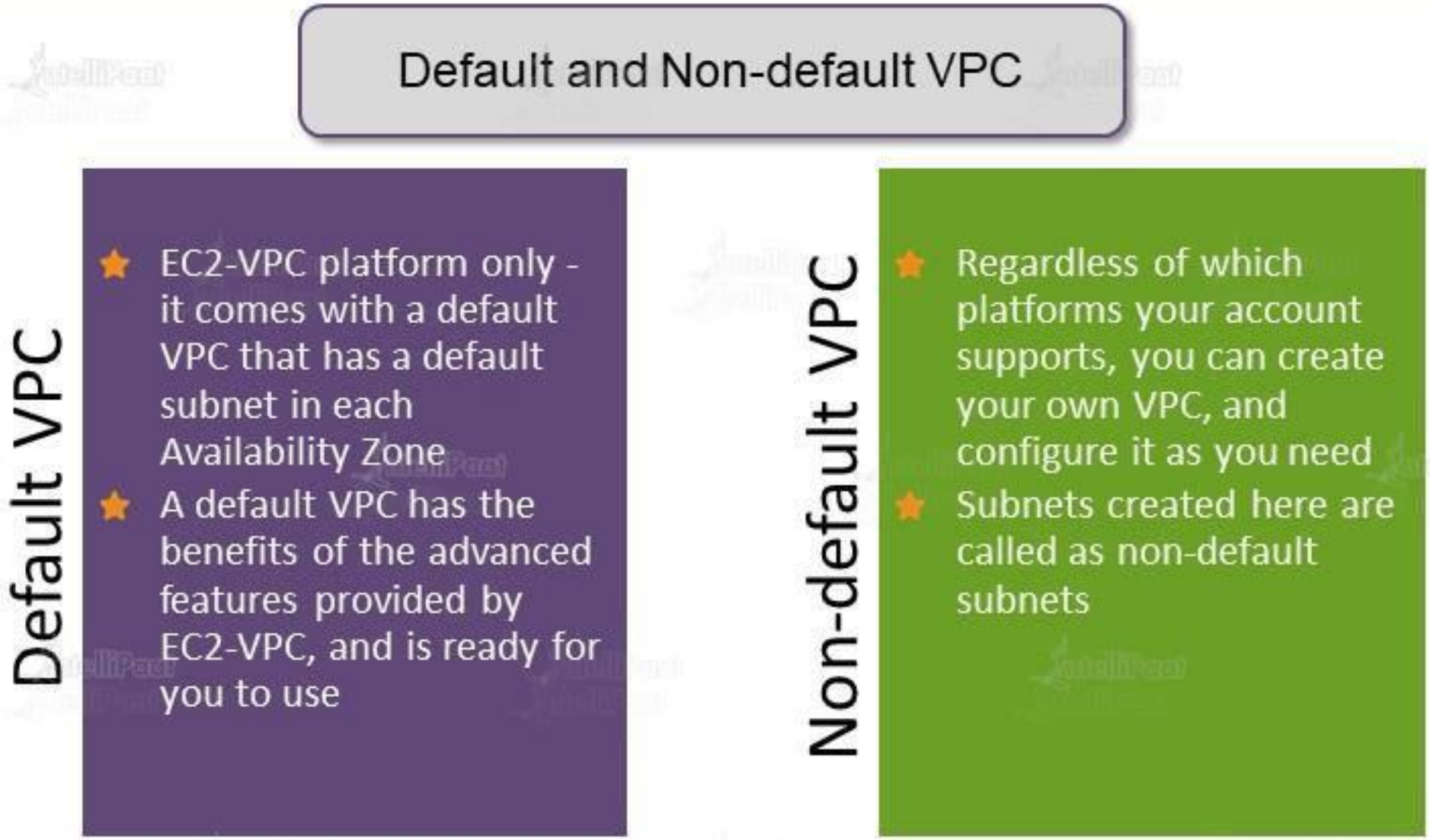


Type – inst1	Rule No.	Type	Protocol	Port	Source	Allow/Deny
Inbound	100	SSH	TCP	22	1.1.2.0/24	ALLOW
Inbound	200	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Type – inst1	Rule No.	Type	Protocol	Port	Destination	Allow/Deny
Outbound	100	SSH	TCP	1024-65535	1.1.2.0/24	ALLOW
Outbound	200	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Types of VPC

Types of VPC

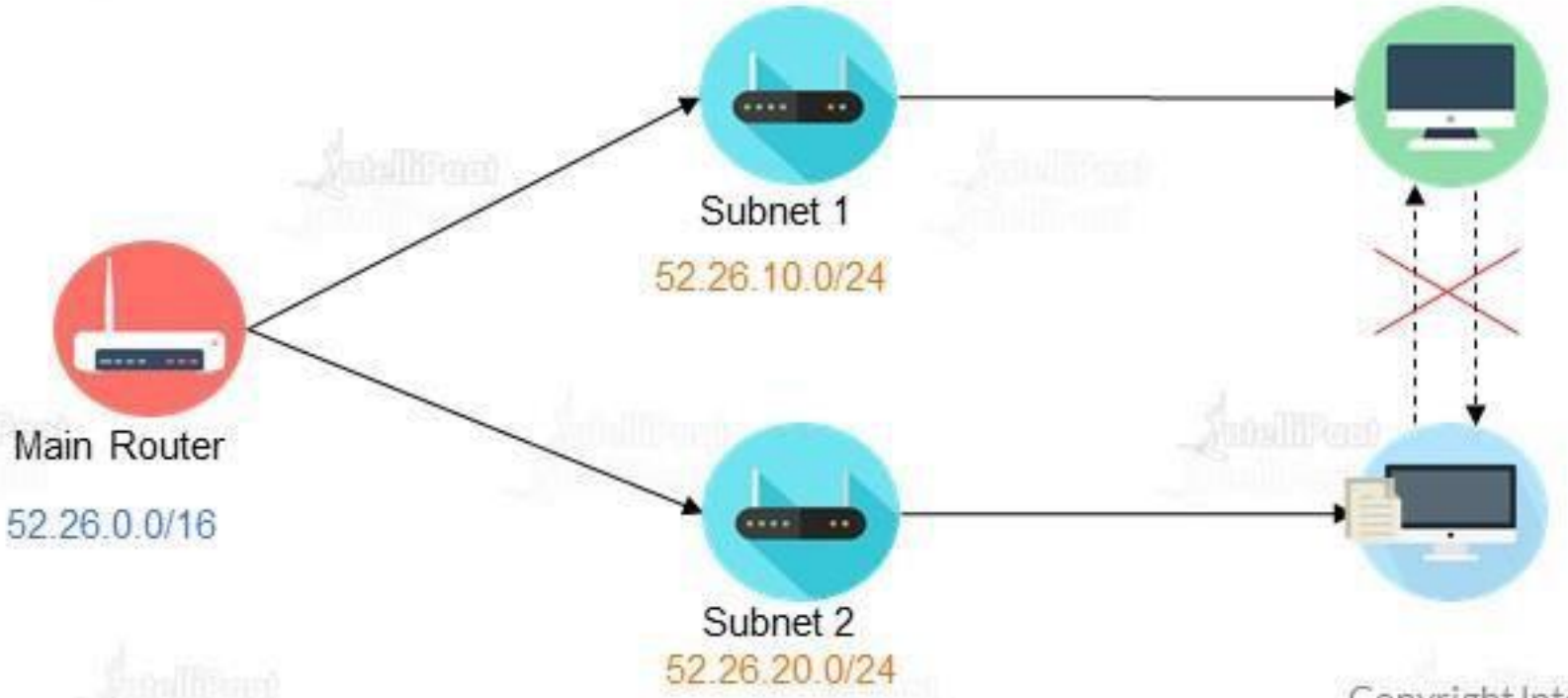


IntelliPaat

Subnets

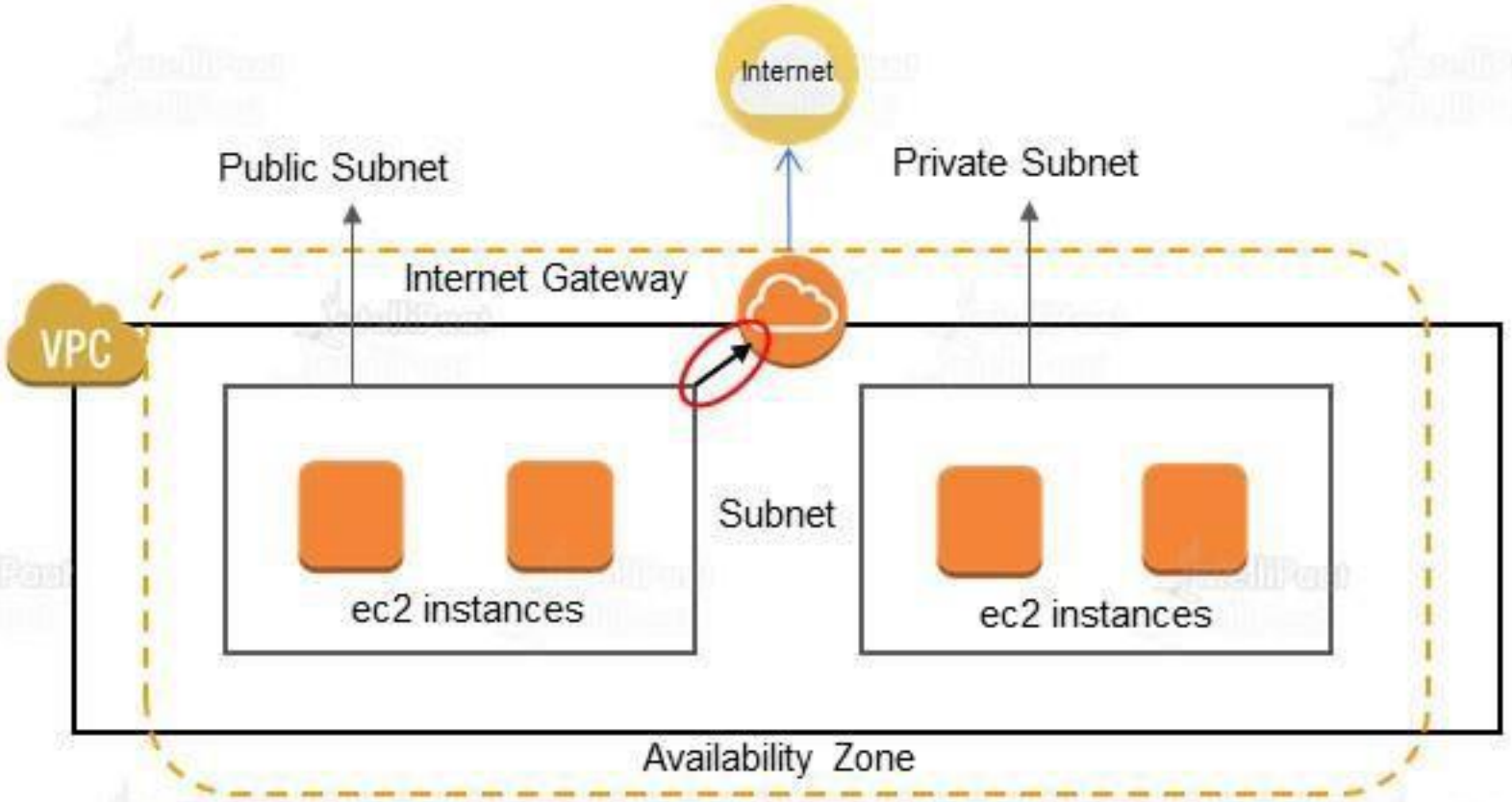
Subnets

- Subnet is dividing a large network into multiple smaller logical networks.
- Each subnet is a separate network on its own. Machines in one subnet cannot talk to machines in other subnet directly. Route through the main router has to be taken.



Subnets

- Public Subnet has internet gateway associated with it.
- Private subnet does not have any route to Internet Gateway.

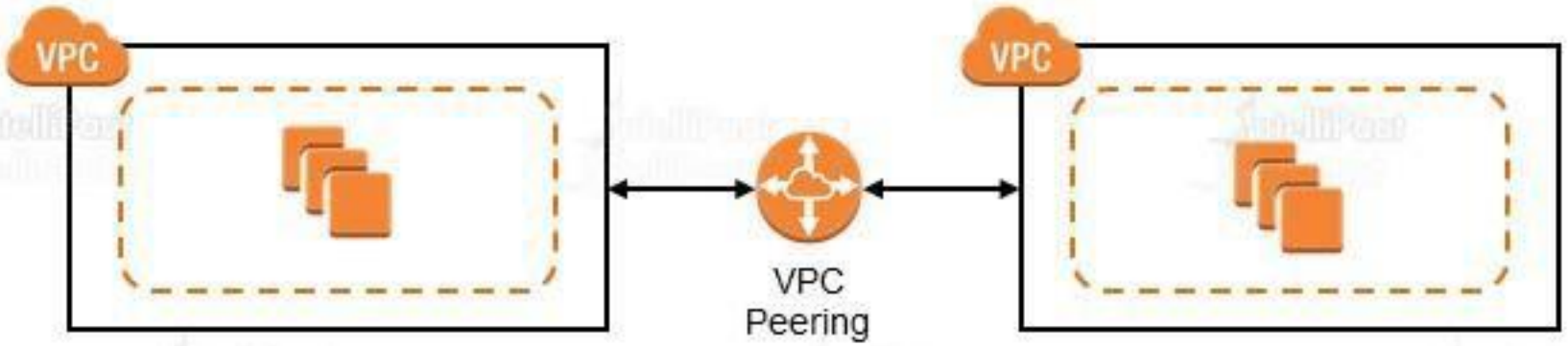


VPC Peering

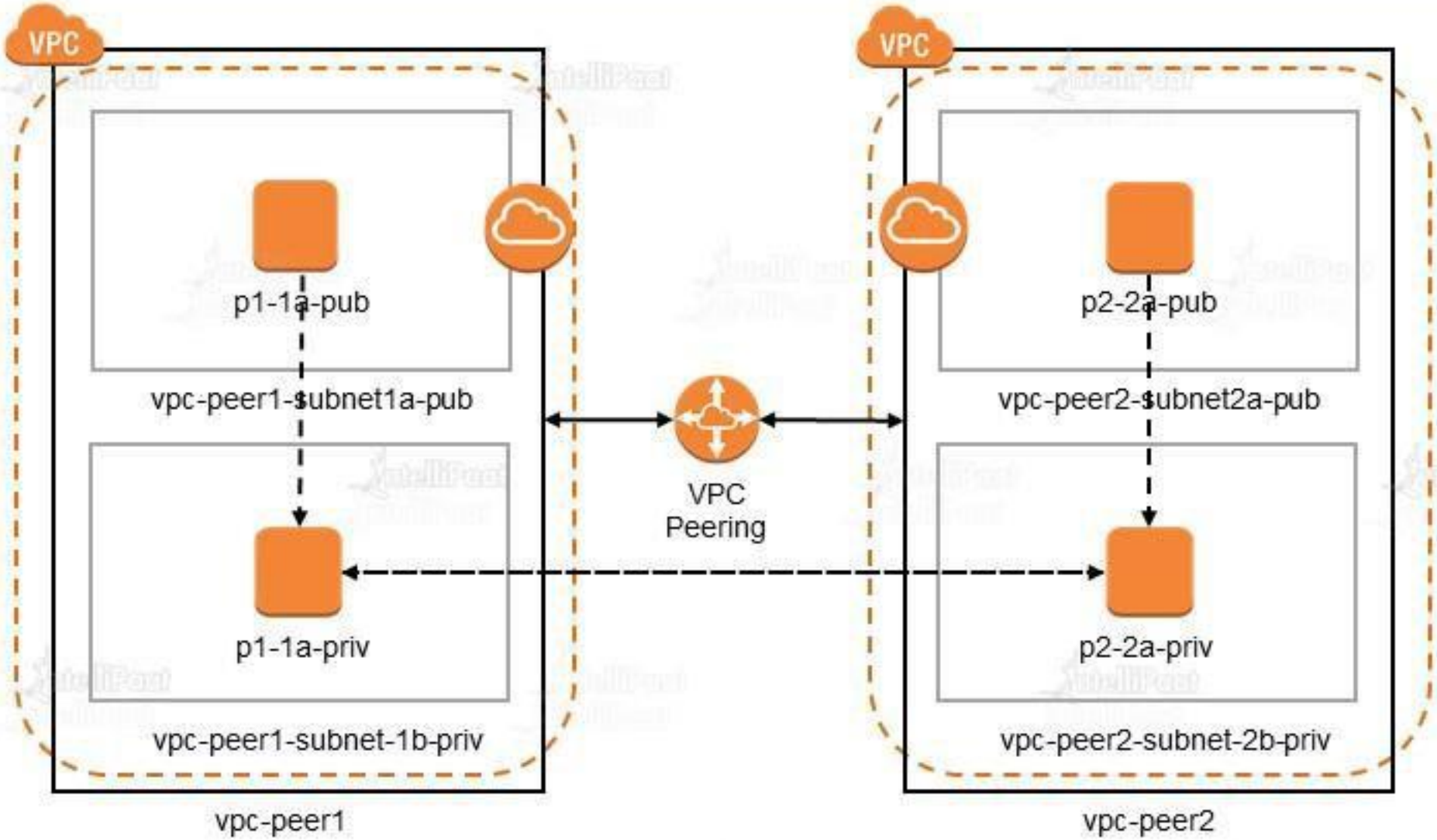
VPC Peering

VPC Peering

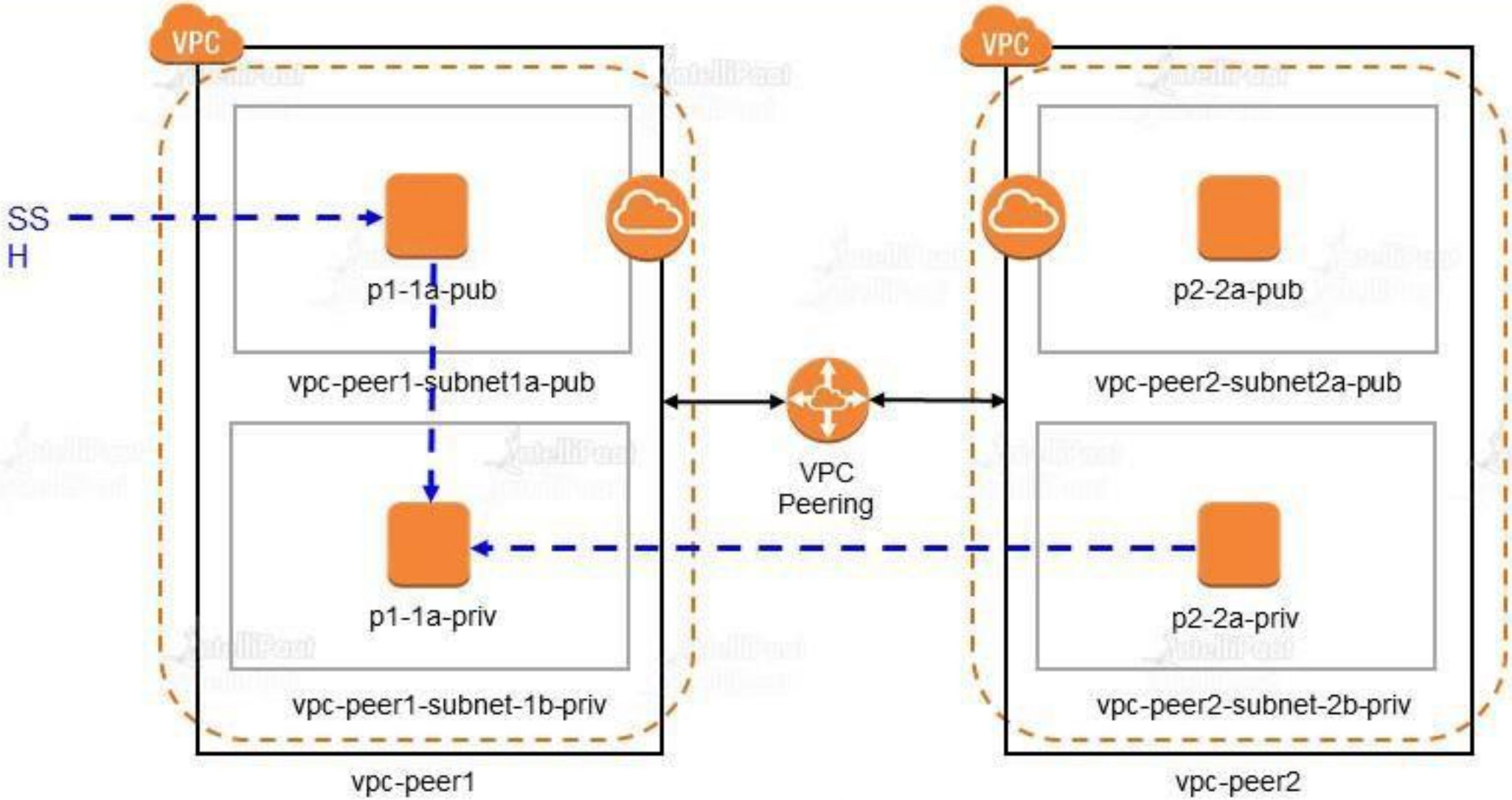
- Network connection between two VPCs which enables traffic flow between them using Private IP addresses.
- Peering connections can be created between VPCs in the same or different accounts and between VPCs in the same or different regions.



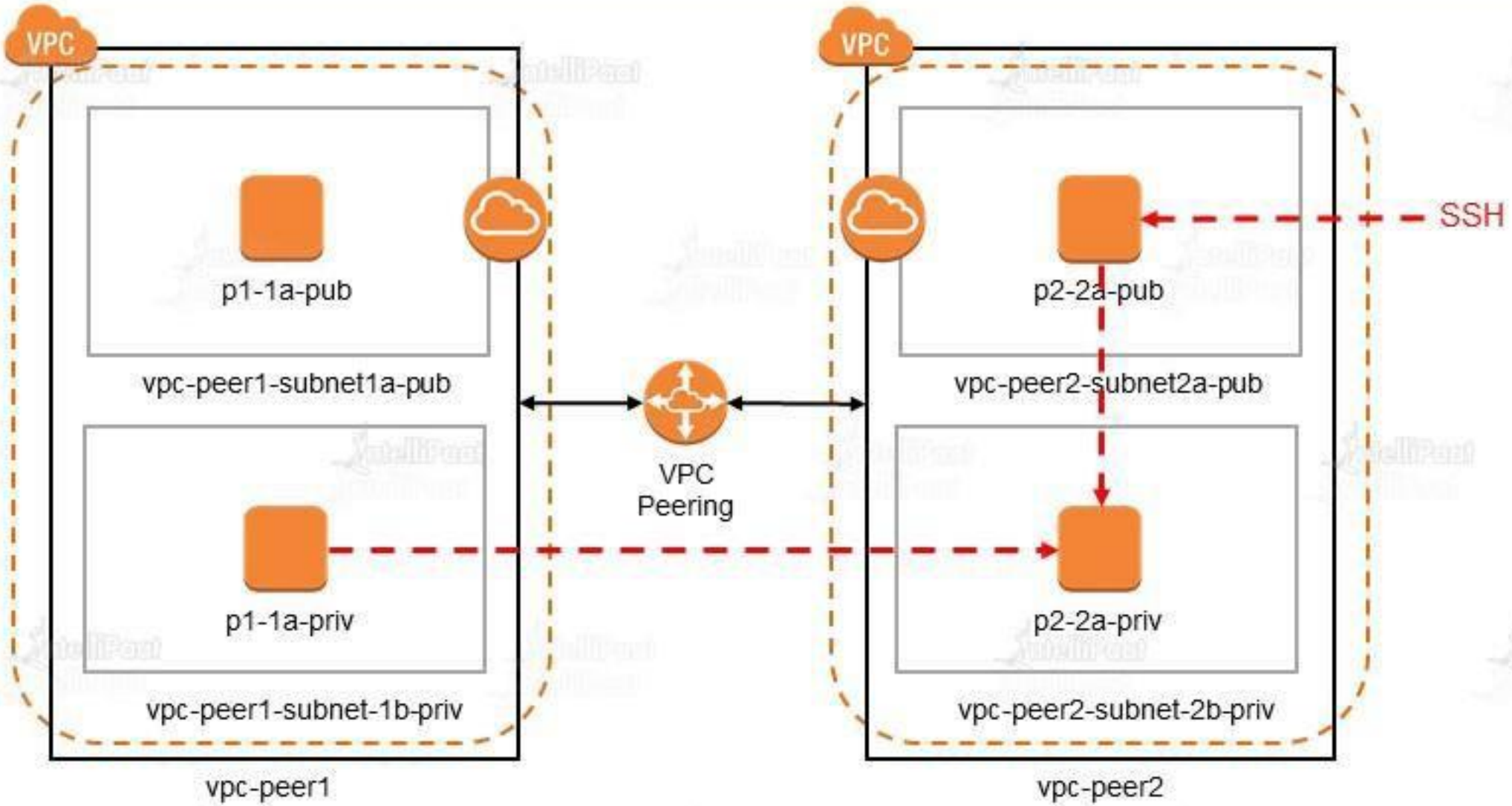
VPC Peering



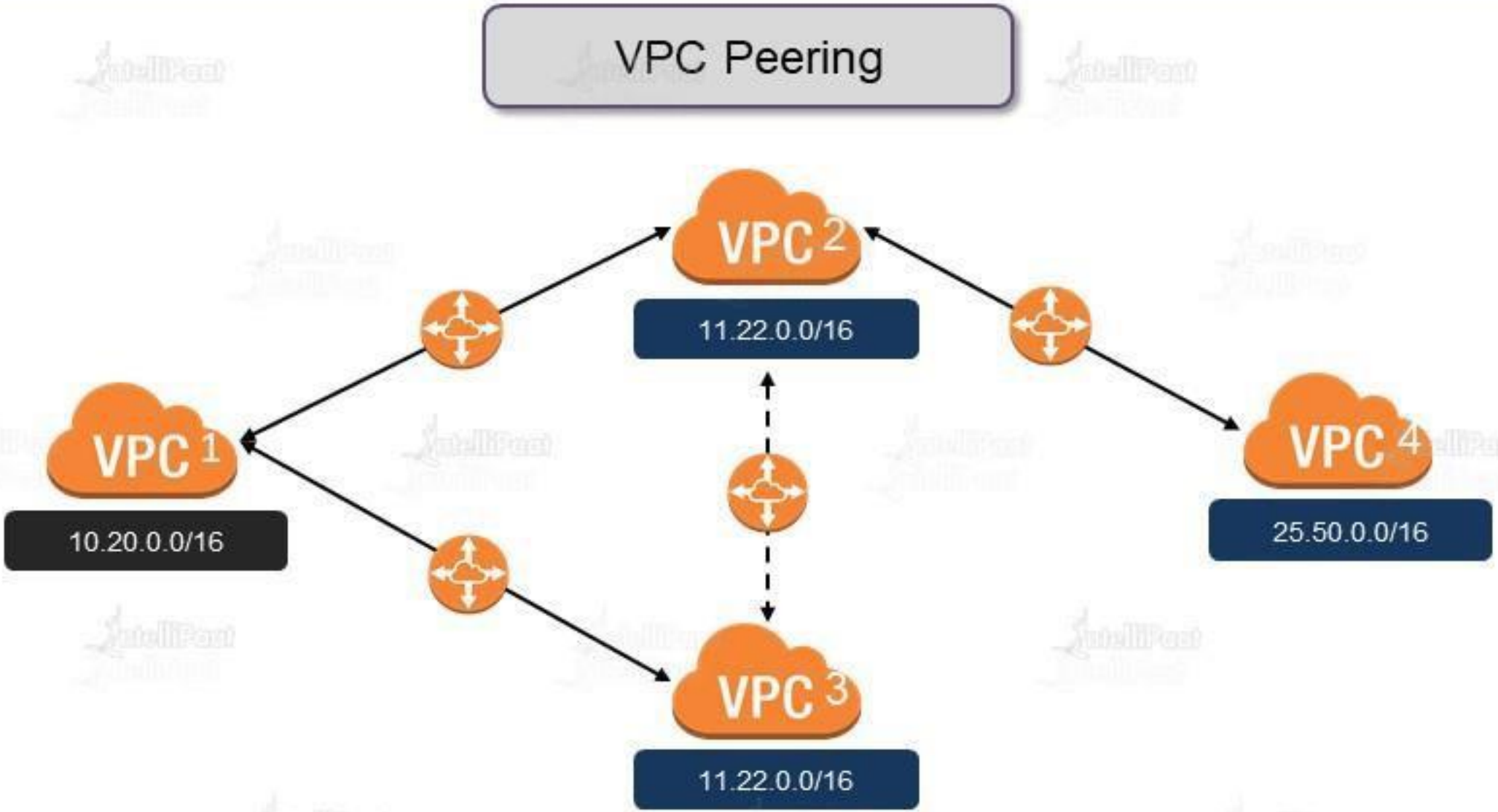
VPC Peering



VPC Peering



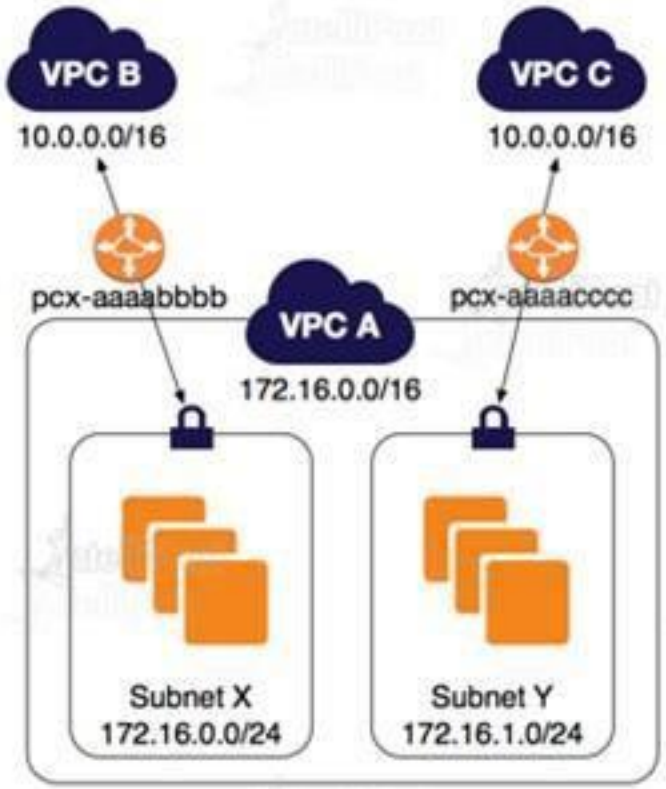
VPC Peering



VPC Peering

VPC Peering Scenarios

Two VPCs (with same n/w address) peered with 2 subnets in the same VPC.

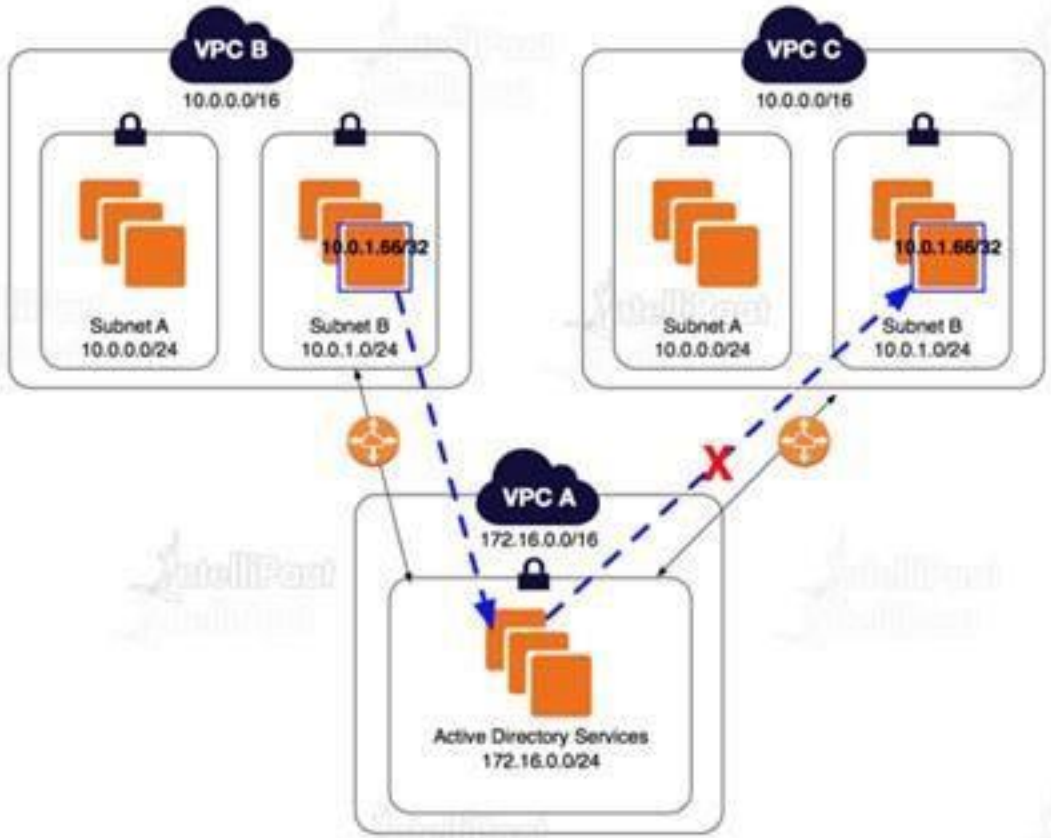


Route Table	Destination	Target
Subnet X in VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
Subnet Y in VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	172.16.0.0/24	pcx-aaaabbbb
VPC C	10.0.0.0/16	Local
	172.16.1.0/24	pcx-aaaacccc

VPC Peering

VPC Peering Scenarios

Two VPCs peered with specific subnets.



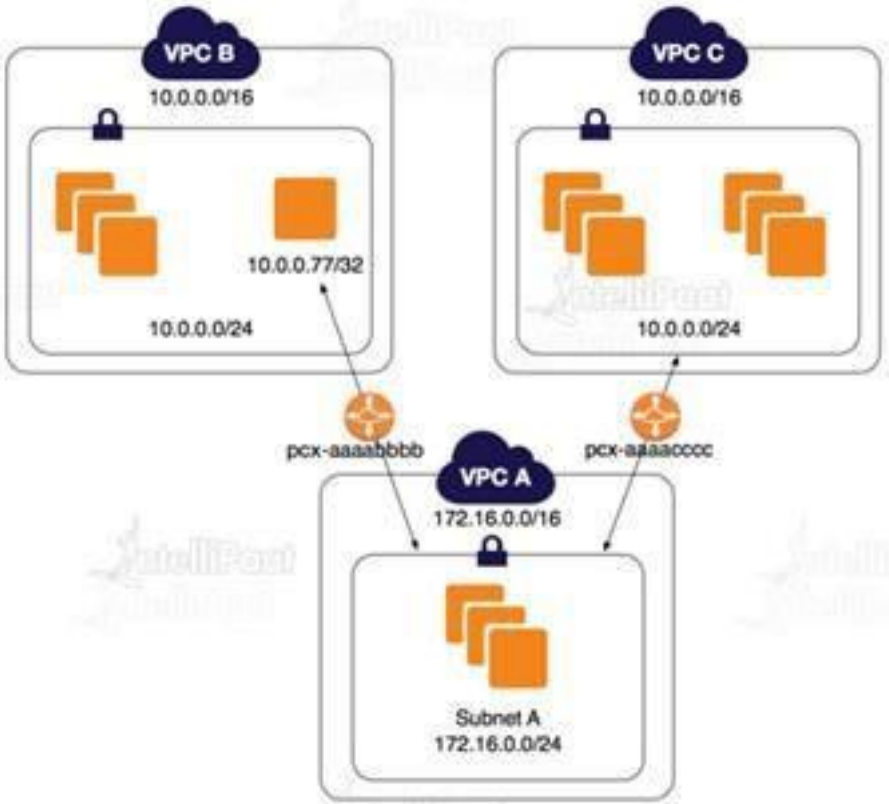
Route Table	Destination	Target
Subnet B in VPC B	10.0.0.0/16	Local
	172.16.0.0/24	pcx-aaaabbbb
VPC A	172.16.0.0/24	Local
	10.0.0.0/16	pcx-aaaacccc

Destination	Target
172.16.0.0/16	Local
10.0.1.0/24	pcx-aaaabbbb
10.0.0.0/24	pcx-aaaacccc

VPC Peering

VPC Peering Scenarios

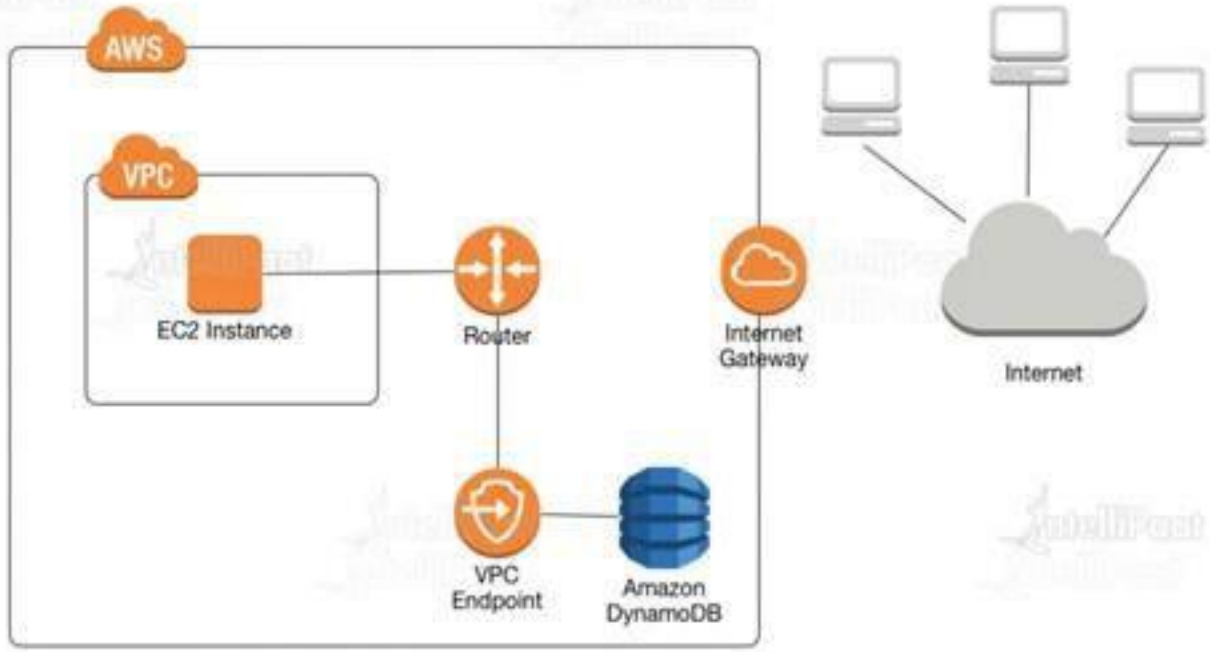
One VPC peered with two VPCs using Longest Prefix Match.



Route Table	Destination	Target
VPC A	172.16.0.0/16	Local
	10.0.0.77/32	pcx-aaaabbbb
	10.0.0.0/16	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaabbbb
VPC C	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaacccc

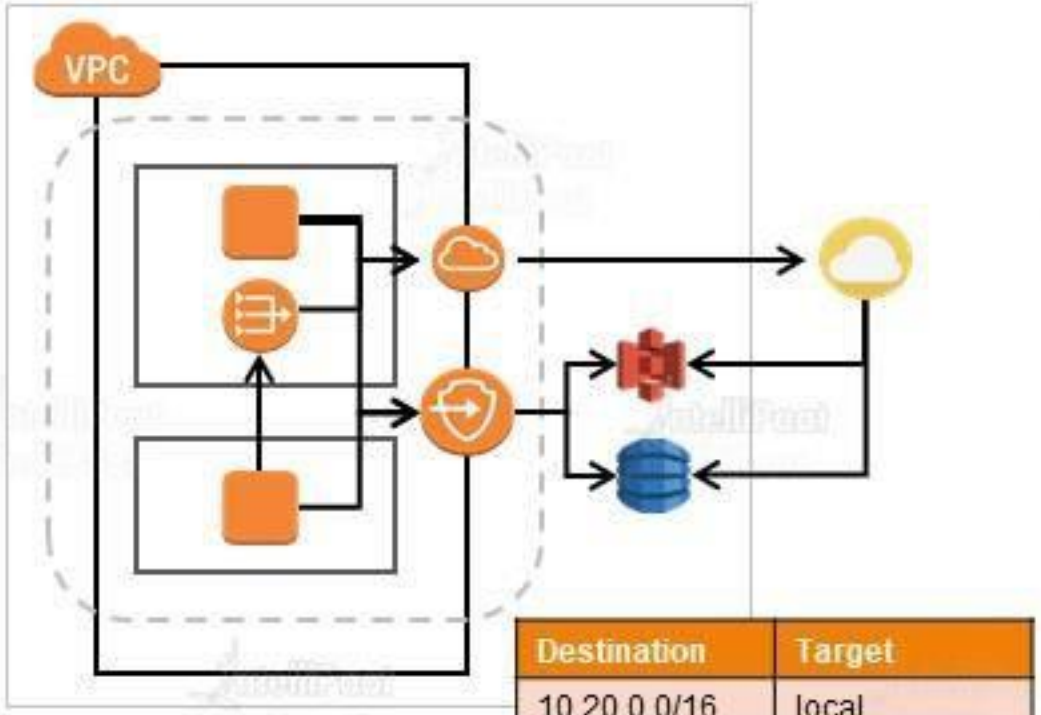
VPC Endpoints

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.



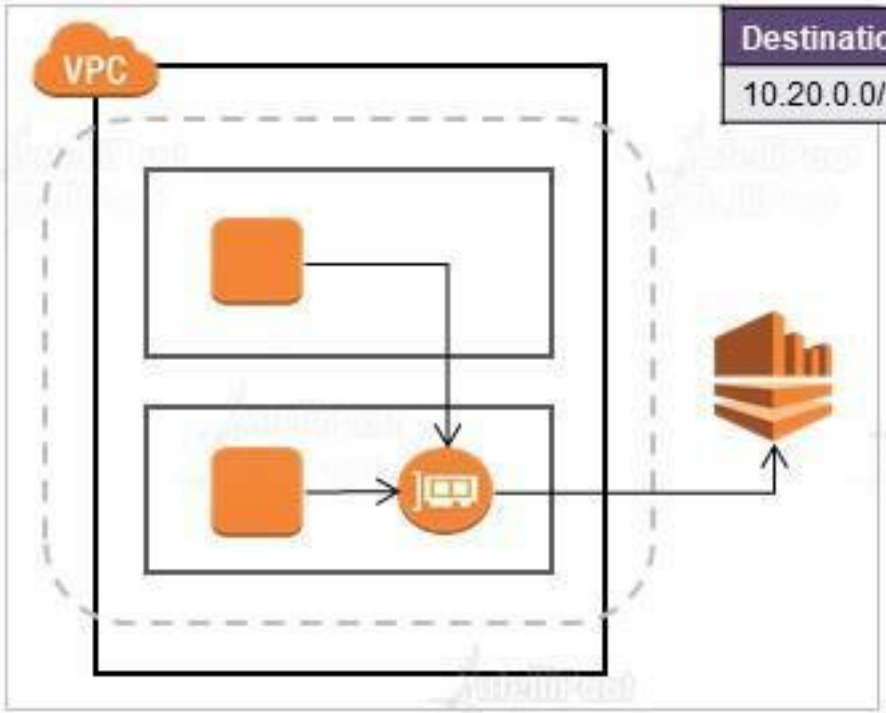
VPC Endpoints

Gateway Endpoint.



Destination	Target
10.20.0.0/16	local
To S3	vpce-id

Interface Endpoint – Powered by PrivateLink.



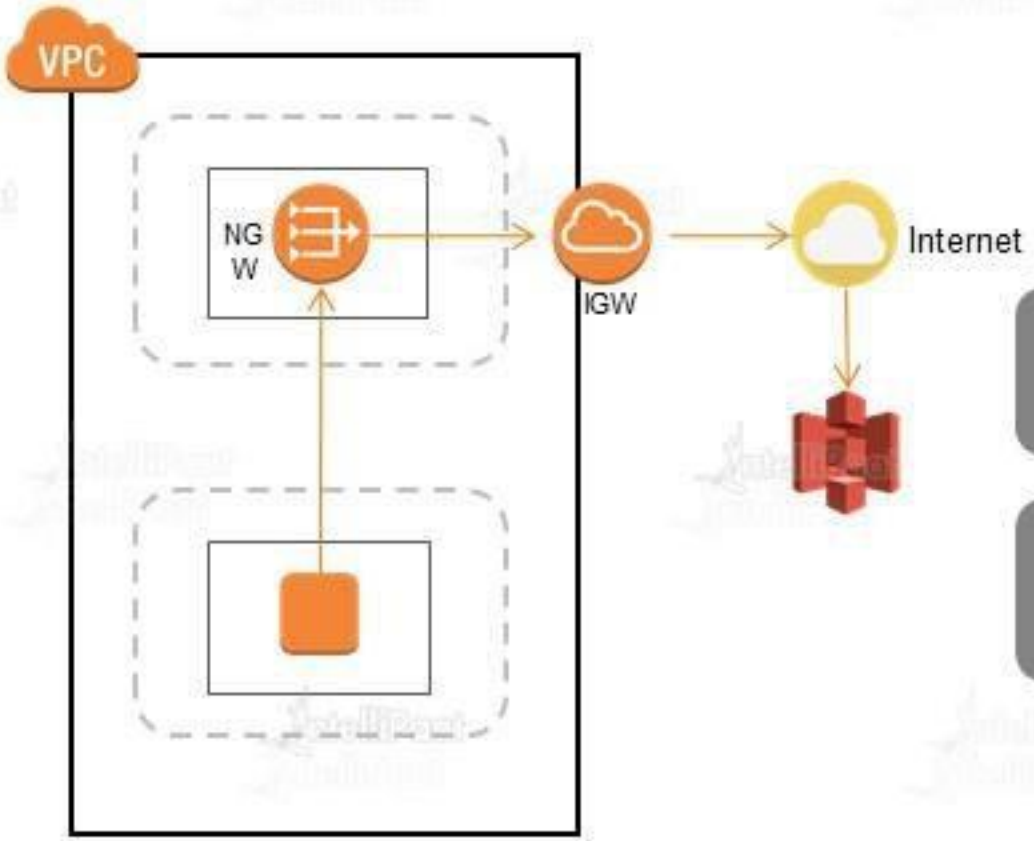
Destination	Target
10.20.0.0/16	local

VPC Pricing

VPC Pricing

- Free tier: Entirely free except for VPN and NAT Gateway.
- Only VPN connection and NAT Gateway are priced.
- VPN: $0.05 per VPN connection per hour.
- NAT Gateway: $0.045 per hour, $0.045 per GB of data processed per hour.
- Visit https://aws.amazon.com/vpc/pricing/ for details.

VPC Pricing



Data Transfer OUT:
From EC2 To

- S3 in same region = FREE
- EC2, ENI in different AZ = $0.010/GB.

NAT GTW running price (monthly) = $0.045*24*30 = $32.4

Data Transfer out to S3 = $0

NAT GTW data processing price for 200 GB = $0.045*200 = $9.0

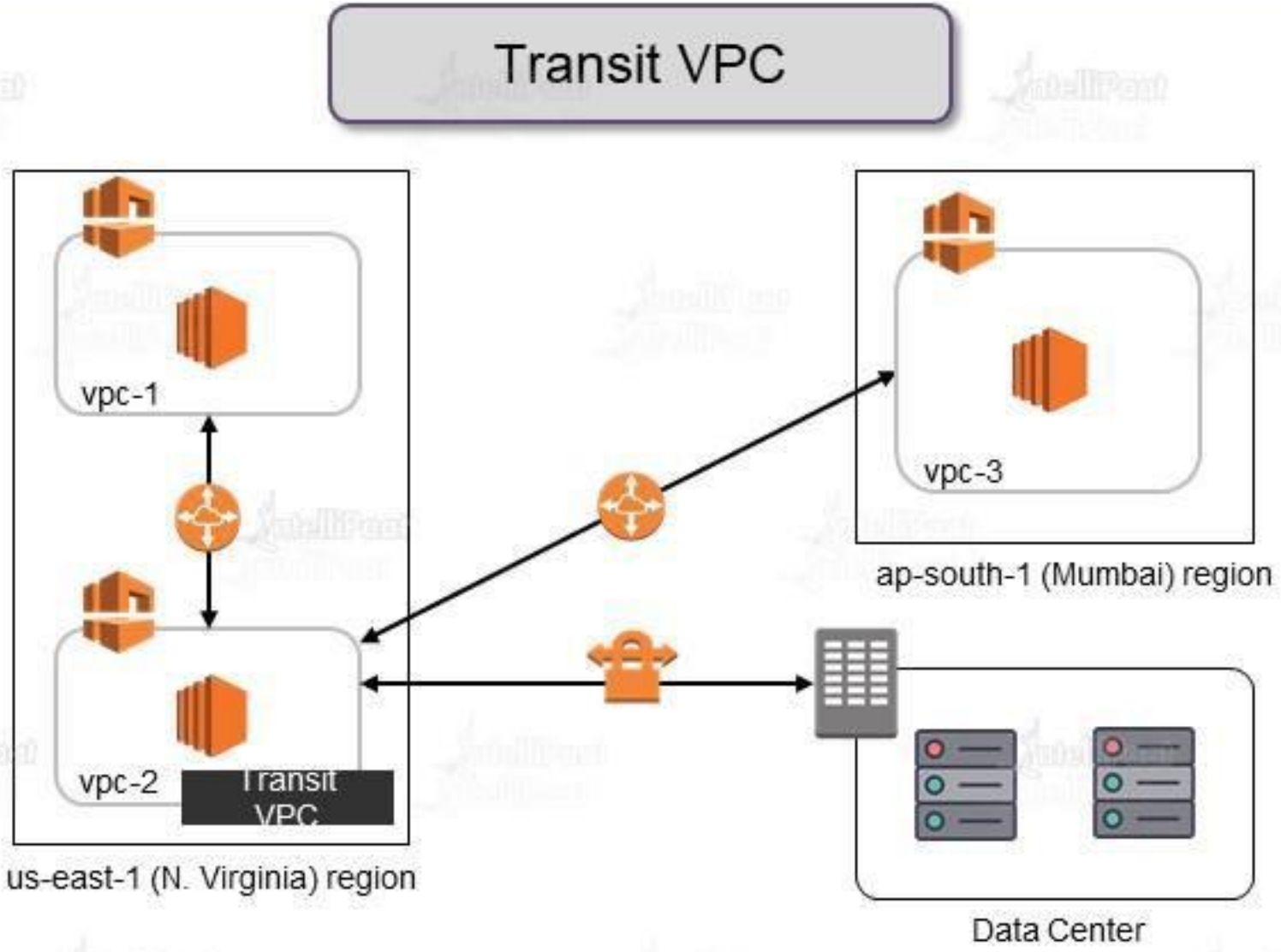
Data Transfer out to NAT = 200*$0.010 = $2.0

Total Price = 32.4 + 9 + 2 = $43.4/month

IntelliPaat

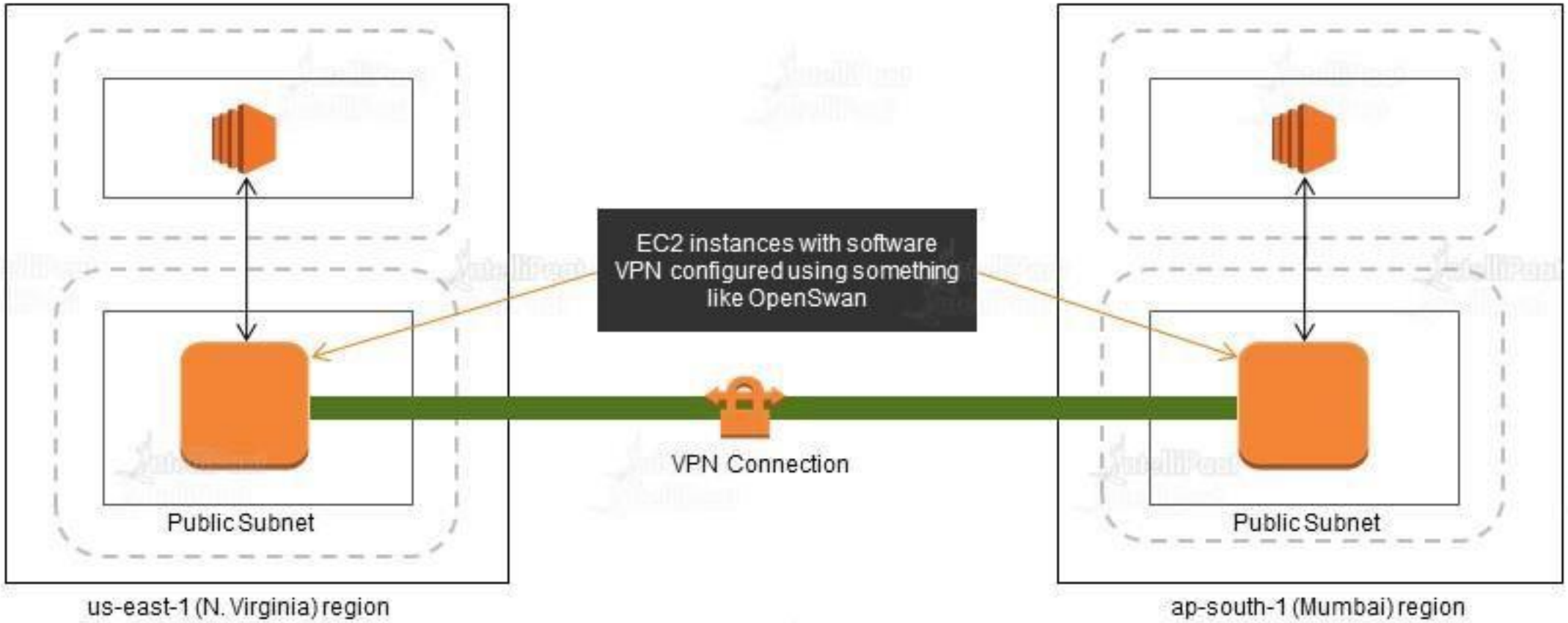
Design Patterns

Design Patterns



Design Patterns

Multi-region VPC connectivity



AWS Transit Gateway

AWS Transit Gateway

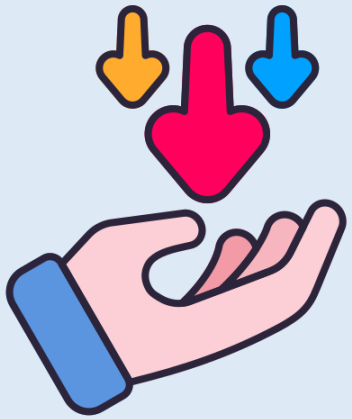
AWS Transit Gateway is a central hub that connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks. This simplifies your network and eliminates complicated peering relationships. It functions as a cloud router, establishing new connections only once.

IntelliPaat

AWS Transit Gateway Vs VPC Peering

Advantages of AWS Transit Gateway

- When compared to VPC peering, there is more visibility (network manager, CloudWatch metrics, and flow logs).
- Fine-grained routing is possible with TGW Route Tables per attachment.
- The number of regions determines the complexity.



Disadvantages of AWS Transit Gateway

- Each additional hop will add latency.
- Potential bottlenecks in regional peering connections.
- Pricing is based on hourly rates for attachments, data processing, and data transfer.

Advantages of VPC Peering

- Only data transfer is charged for.
- There is no bandwidth restriction.

Disadvantages of AWS Transit Gateway

- Each VPC adds to the network's complexity.
- When compared to TGW, there is less visibility (only VPC flow logs) and it is more difficult to maintain route tables.

Benefits of AWS Transit Gateway

- Improved connectivity
- improved visibility and control
- enhanced security
- Multicasting that is adaptable

Creation of AWS Transit Gateway

- Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
- In the Region selector, choose the Region that you used when you created the VPCs.
- On the navigation pane, choose Transit Gateways.
- Choose Create transit gateway.
- (Optional) For Name tag, enter a name for the transit gateway. This creates a tag with "Name" as the key and the name that you specified as the value.
- (Optional) For Description, enter a description for the transit gateway.

Creation of AWS Transit Gateway

- For Amazon side Autonomous System Number (ASN), enter the private ASN for your transit gateway. This should be the ASN for the AWS side of a Border Gateway Protocol (BGP) session.
  The range is from 64512 to 65534 for 16-bit ASNs.
  The range is from 4200000000 to 4294967294 for 32-bit ASNs.
  If you have a multi-Region deployment, we recommend that you use a unique ASN for each of your transit gateways.

- Choose Create transit gateway. When the gateway is created, the initial state of the transit gateway is pending.

IntelliPaat

AWS Direct Connect

AWS Direct Connect

The **AWS Direct Connect** cloud service provides the quickest connection to your AWS resources. Your network traffic remains on the AWS global network and is never exposed to the public internet while in transit. This reduces the possibility of encountering bottlenecks or unexpected increases in latency.

Benefits of AWS Direct Connect

- Create hybrid networks.
- Extend your current network
- Control large datasets

Creation of AWS Direct Connect

Creation of AWS Direct Connect

To create a new connection

1. Open the AWS Direct Connect console at

   https://console.aws.amazon.com/directconnect/v2/home.

2. On the AWS Direct Connect screen, under Get started, choose Create a connection.
3. On the Create Connection pane, under Connection settings, do the following:
   - For Name, enter a name for the connection.
   - For Location, select the appropriate AWS Direct Connect location.

.

Creation of AWS Direct Connect

On the Create Connection pane, under Connection settings, do the following:

- For On-premises, select Connect through an AWS Direct Connect partner when you use this connection to connect to your data center.

- (Optional) Configure MAC security (MACsec) for the connection. Under Additional Settings, select Request a MACsec capable port. MACsec is only available on dedicated connections.

Creation of AWS Direct Connect

On the Create Connection pane, under Connection settings, do the following:

- (Optional) Add or remove a tag.
- [Add a tag] Choose Add tag and do the following:
    - For Key, enter the key name.
    - For Value, enter the key value.
- [Remove a tag] Next to the tag, choose Remove tag.
- Choose Create Connection.

IntelliPaat

AWS VPN

AWS VPN

AWS Virtual Private Network solutions connect your on-premises networks, remote offices, client devices, and the AWS global network in a secure manner. AWS VPN is made up of two components: AWS Site-to-Site VPN and AWS Client VPN. To protect your network traffic, each service offers a highly available, managed, and elastic cloud VPN solution.

AWS VPN

Types of VPN

01 AWS Client VPN

02 Site to Site VPN

IntelliPaat

AWS Client VPN

AWS Client VPN

AWS Client VPN is a fully-managed, elastic VPN service that scales up and down automatically based on user demand. Because it is a cloud VPN solution, you do not need to install and manage hardware or software-based solutions, nor do you need to guess how many remote users you will support at the same time.

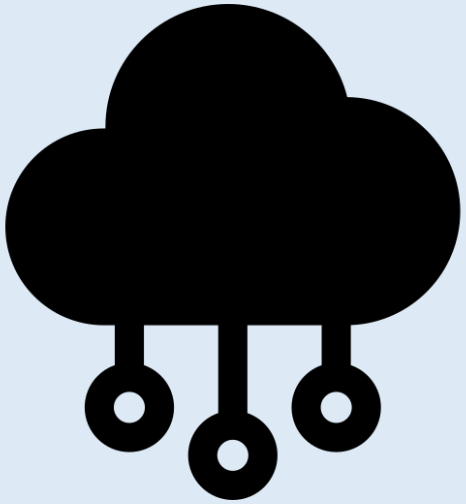
IntelliPaat

AWS Site-to-Site VPN

AWS Site-to-Site VPN

The AWS Site-to-Site VPN service establishes a secure link between your data centre or branch office and your AWS cloud resources. The Accelerated Site-to-Site VPN option, which works with AWS Global Accelerator, provides even better performance for globally distributed applications.

AWS Site-to-Site VPN



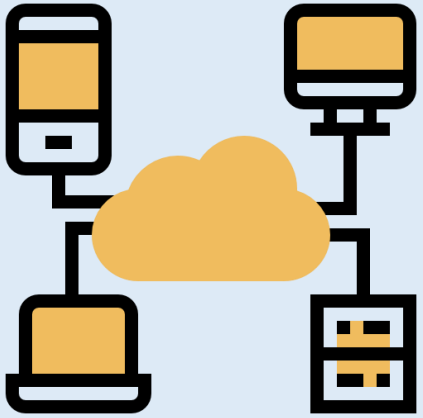
Creating AWS Site to Site AWS

- Step 1: Create a customer gateway
- Step 2: Create a target gateway
- Step 3: Configure routing
- Step 4: Update your security group
- Step 5: Create a Site-to-Site VPN connection
- Step 6: Download the configuration file
- Step 7: Configure the customer gateway device

VPC Flow Logs

VPC Flow Logs

VPC Flow logs allow you to monitor and analyze IP address traffic to and from network interfaces within your VPC. If you have a content delivery platform, for example, flow logs can profile, analyze, and predict customer patterns of content access, as well as track down top talkers and malicious calls.

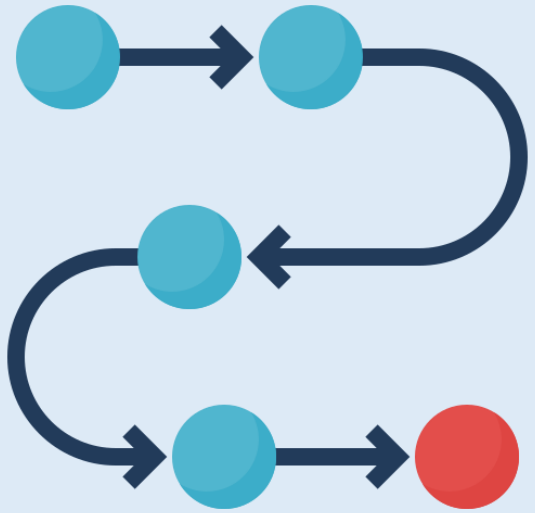


Getting Started with VPC Flow Logs

You can use VPC Reachability Analyzer to determine whether a destination resource in your virtual private cloud (VPC) is reachable from a source resource. To get started, you specify a source and a destination. For example, you can run a reachability analysis between two network interfaces or between a network interface and a gateway.

Getting Started with VPC Flow Logs

- Step 1: Create and analyze a path
- Step 2: View the results of the path analysis
- Step 3: Change the network configuration and analyze the path
- Step 4: Delete the path



Benefits of AWS VPC Flow Logs

- Flow log data can be published to CloudWatch Logs and S3, and then queried or analyzed from either platform.
- You can investigate why specific traffic is not reaching an instance, which aids in the diagnosis of overly strict security group rules.
- Flow logs can be used as an input to security tools to monitor traffic to your instance.
- You can analyze and identify the account and Region where you receive the most traffic for applications that run in multiple AWS Regions or use multi-account architecture.

VPC Flow Logs

Creation of VPC Flow Logs

To create a flow log using the console

1. Do one of the following:
    - Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/. In the navigation pane, choose Network Interfaces. Select the checkbox for the network interface.
    - Open the Amazon VPC console at https://console.aws.amazon.com/vpc/. In the navigation pane, choose Your VPCs. Select the checkbox for the VPC.
    - Open the Amazon VPC console at https://console.aws.amazon.com/vpc/. In the navigation pane, choose Subnets. Select the checkbox for the subnet.

Creation of VPC Flow Logs

- Choose Actions, Create flow log.
- For Filter, specify the type of traffic to log. Choose All to log accepted and rejected traffic, Reject to log only rejected traffic, or Accept to log only accepted traffic.
- For Maximum aggregation interval, choose the maximum period of time during which a flow is captured and aggregated into one flow log record.
- For Destination, choose Send to CloudWatch Logs.

.

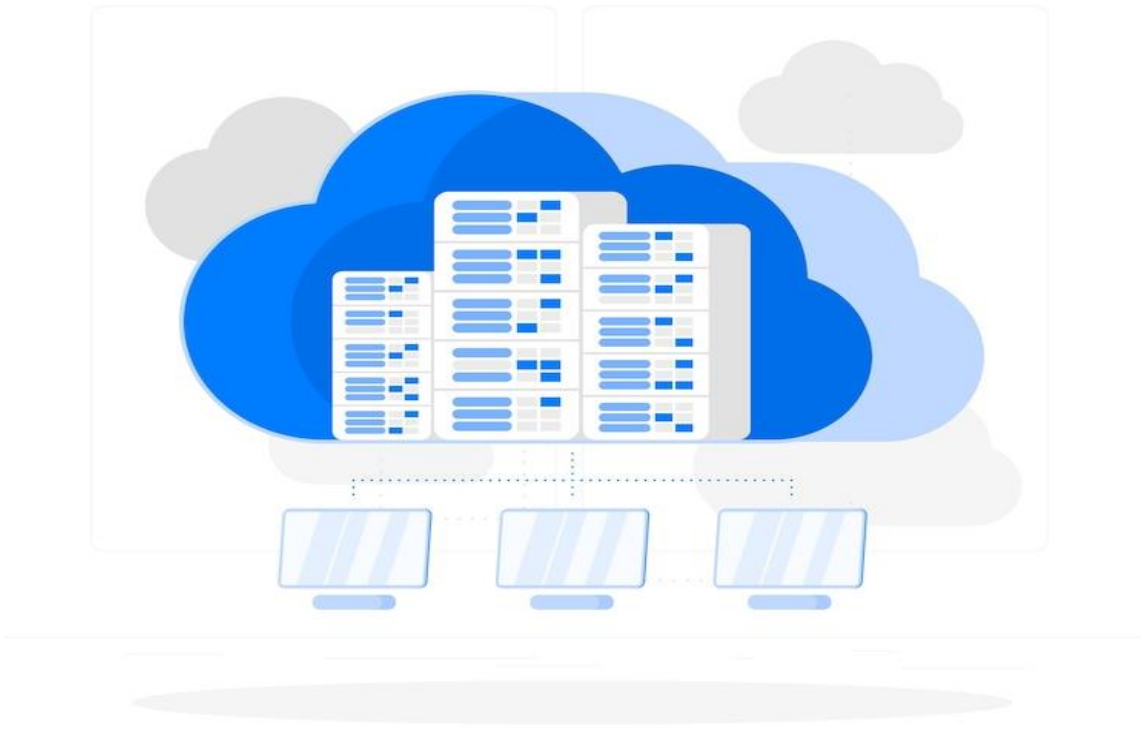
Creation of VPC Flow Logs

- For Destination log group, choose the name of the destination log group that you created.
- For IAM role, specify the name of the role that has permissions to publish logs to CloudWatch Logs.
- For Log record format, select the format for the flow log record.
    i. To use the default format, choose AWS default format.
    ii. To use a custom format, choose Custom format and then select fields from Log format.
- (Optional) Choose Add new tag to apply tags to the flow log.
- Choose Create flow log.

VPC Reachability Analyzer

VPC Reachability Analyzer

VPC Reachability Analyzer is a configuration analysis tool that allows you to perform connectivity testing in your virtual private clouds between a source resource and a destination resource (VPCs). Reachability Analyzer generates hop-by-hop details of the virtual network path between the source and the destination when the destination is reachable.



Use Cases of VPC Reachability Analyzer

- Troubleshoot network misconfiguration-related connectivity issues.
- Check that your network configuration corresponds to your intended connectivity.
- As your network configuration changes, automate the verification of your connectivity intent.

.

India : +91-7847955955

US : 1-800-216-8930 (TOLL FREE)

support@intellipaat.com

24X7 Chat with our Course Advisor