IntelliPaat

AWS Foundation

Introduction to VPC

Agenda

1. WHAT IS AMAZON VPC
2. IP ADDRESS AND CIDR NOTATIONS
3. DEMO 1: VPC
4. COMPONENTS OF VPC
5. DEMO 2: NAT GATEWAY
6. SECURITY IN VPC
7. DEMO 3: SECURITY
8. TYPES OF VPC
9. SUBNETS
10. VPC PEERING
11. VPC ENDPOINTS
12. VPC PRICING
13. DESIGN PATTERNS

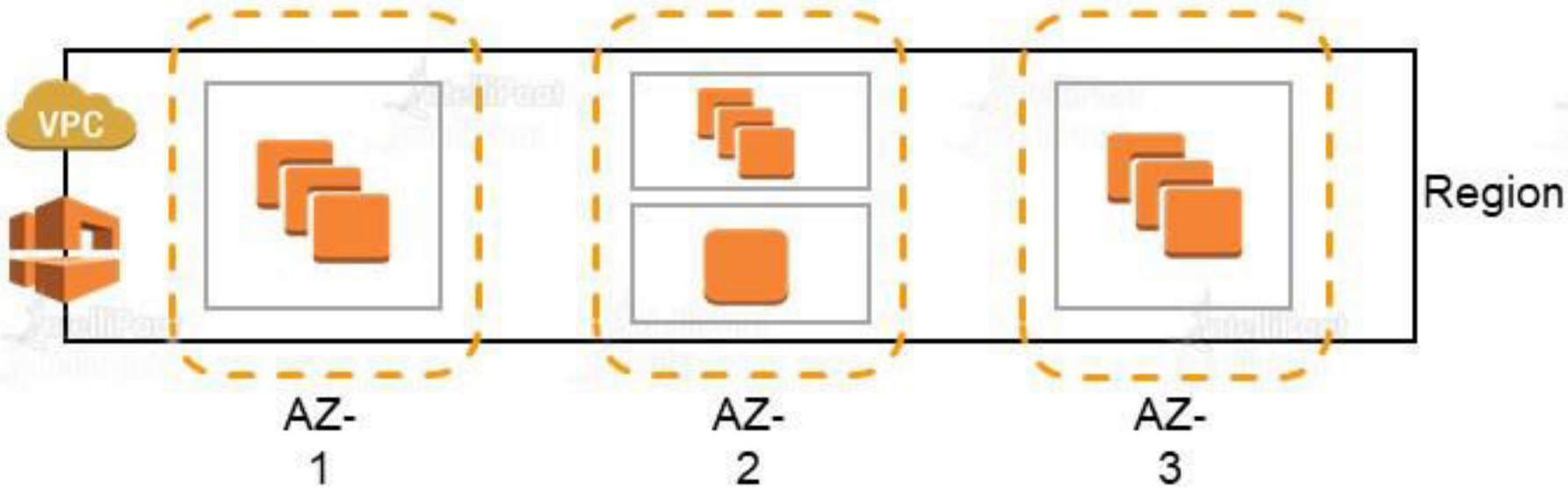
What is Amazon VPC

What is Amazon VPC

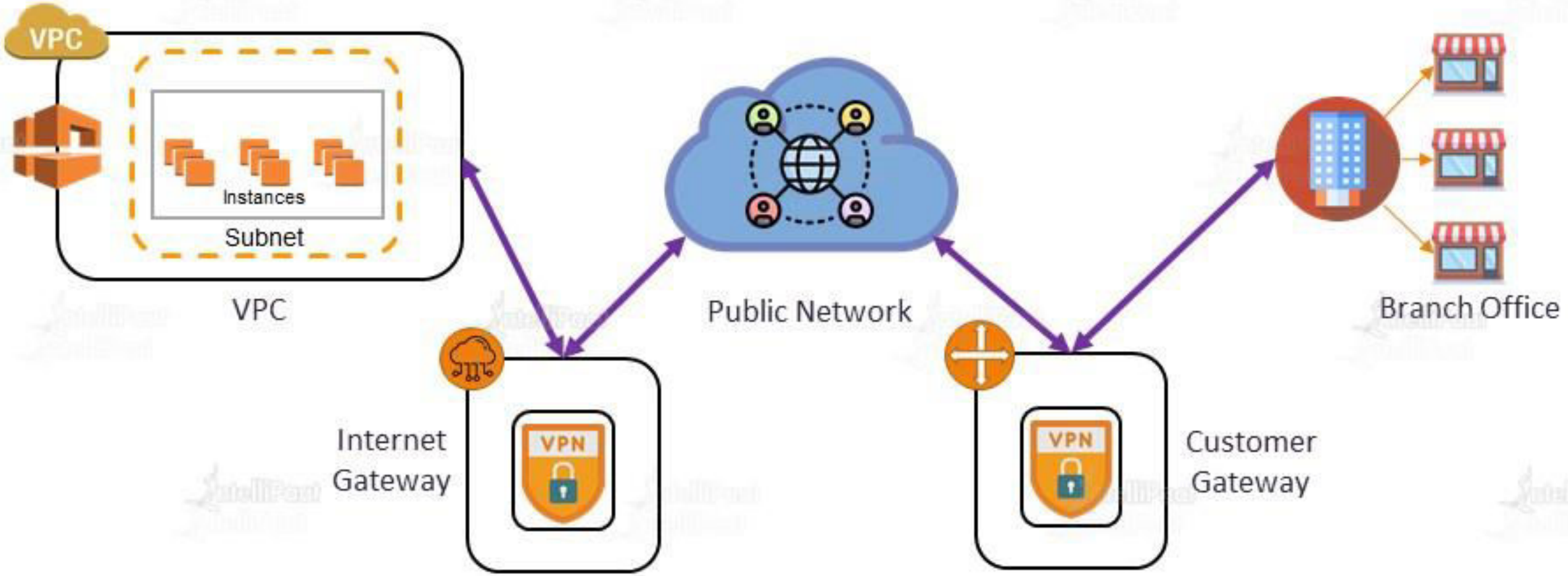
Virtual Private Cloud

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 Amazon VPC



IP Address and CIDR Notations

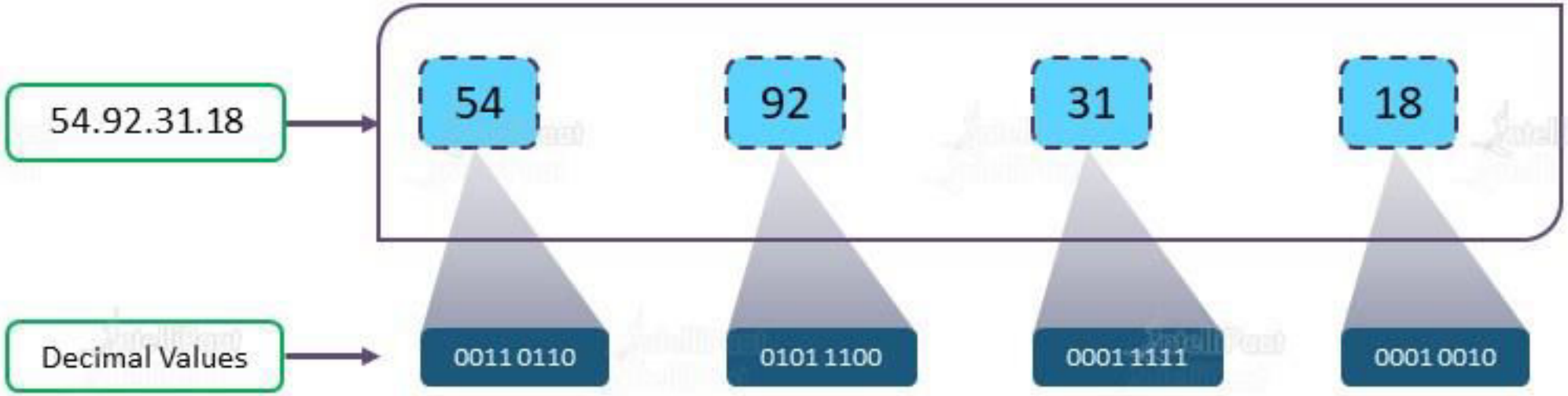
IP Addressing

A Sample IP Address

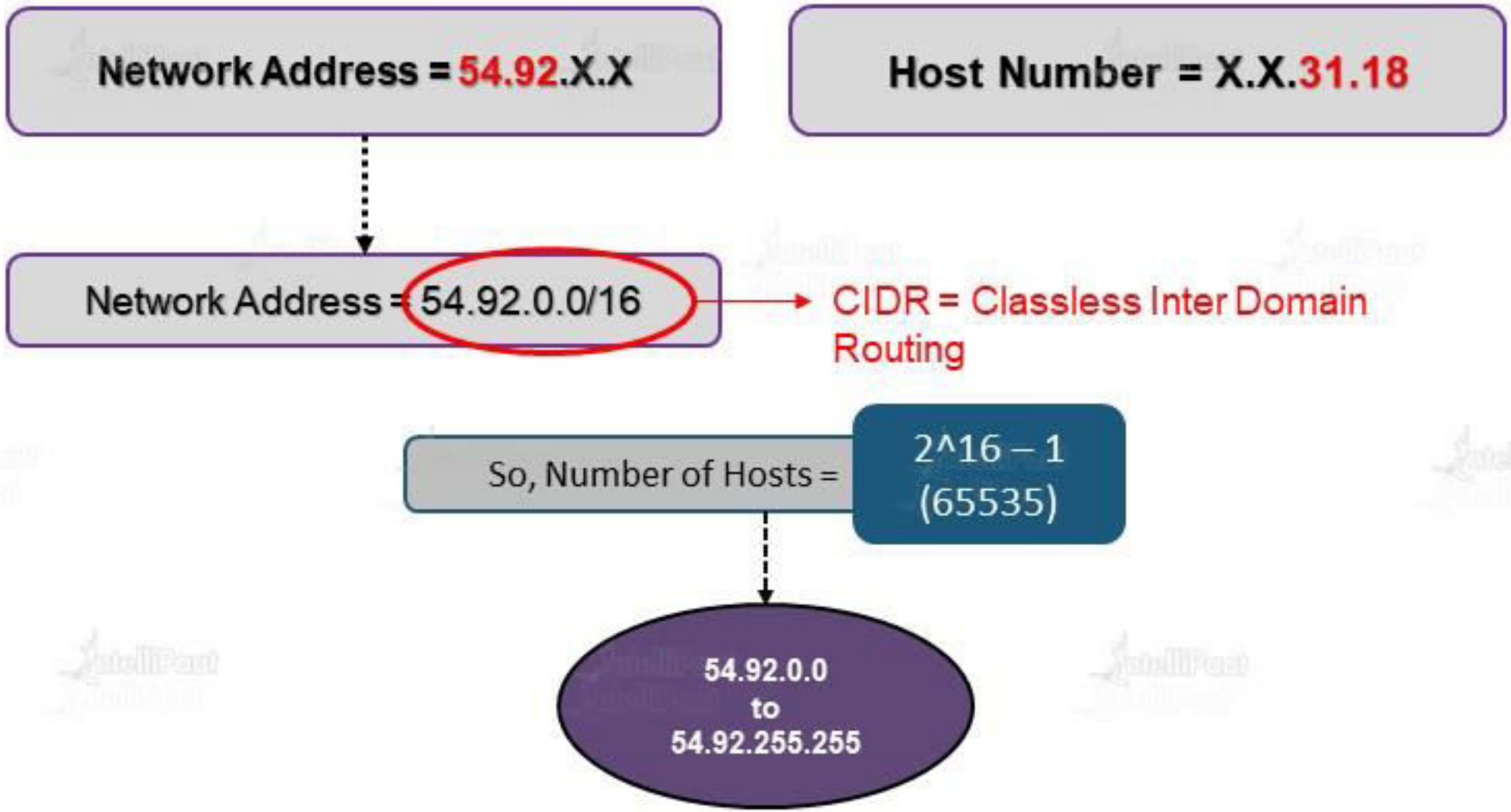
54.92.31.18

- 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 range for CIDR

Range of IP addresses for Network Address **54.92.0.0/16**:

1111 1111	1111 1111	0000 0000	0000 0000		
54	92	0000 0000	0000 0000	54.92.0.0	54.92.0.1
54	92	1111 1111	1111 1111	54.92.255.255	54.92.255.254

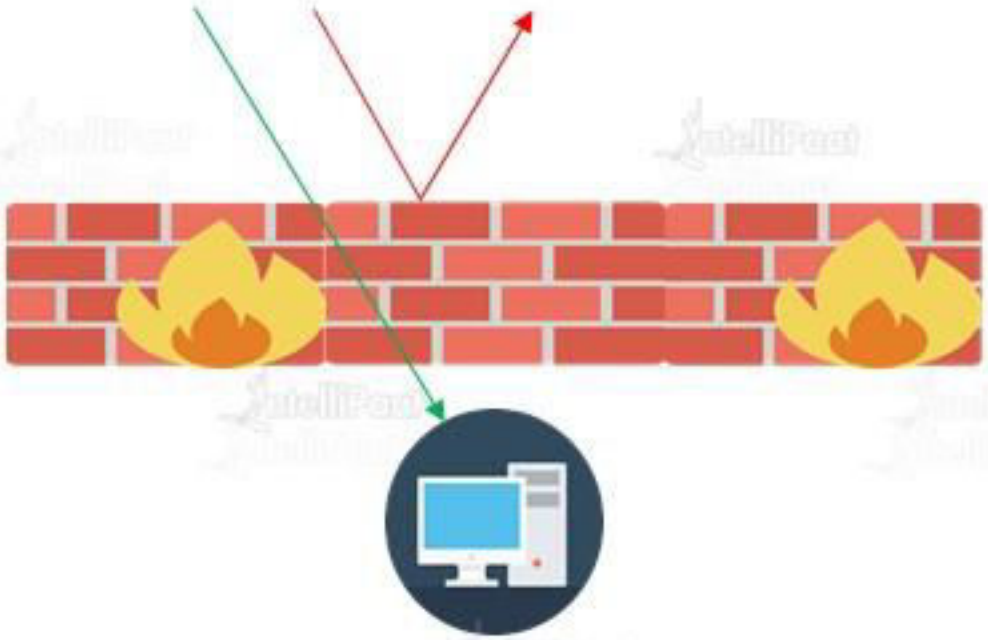
Range of IP addresses for Network Address **54.92.0.0/20**:

1111 1111	1111 1111	1111	0000	0000 0000		
54	92	0000	0000	0000 0000	54.92.0.0	54.92.0.1
54	92	0000	1111	1111 1111	54.92.15.255	54.92.15.254

CIDR Classes

Firewall

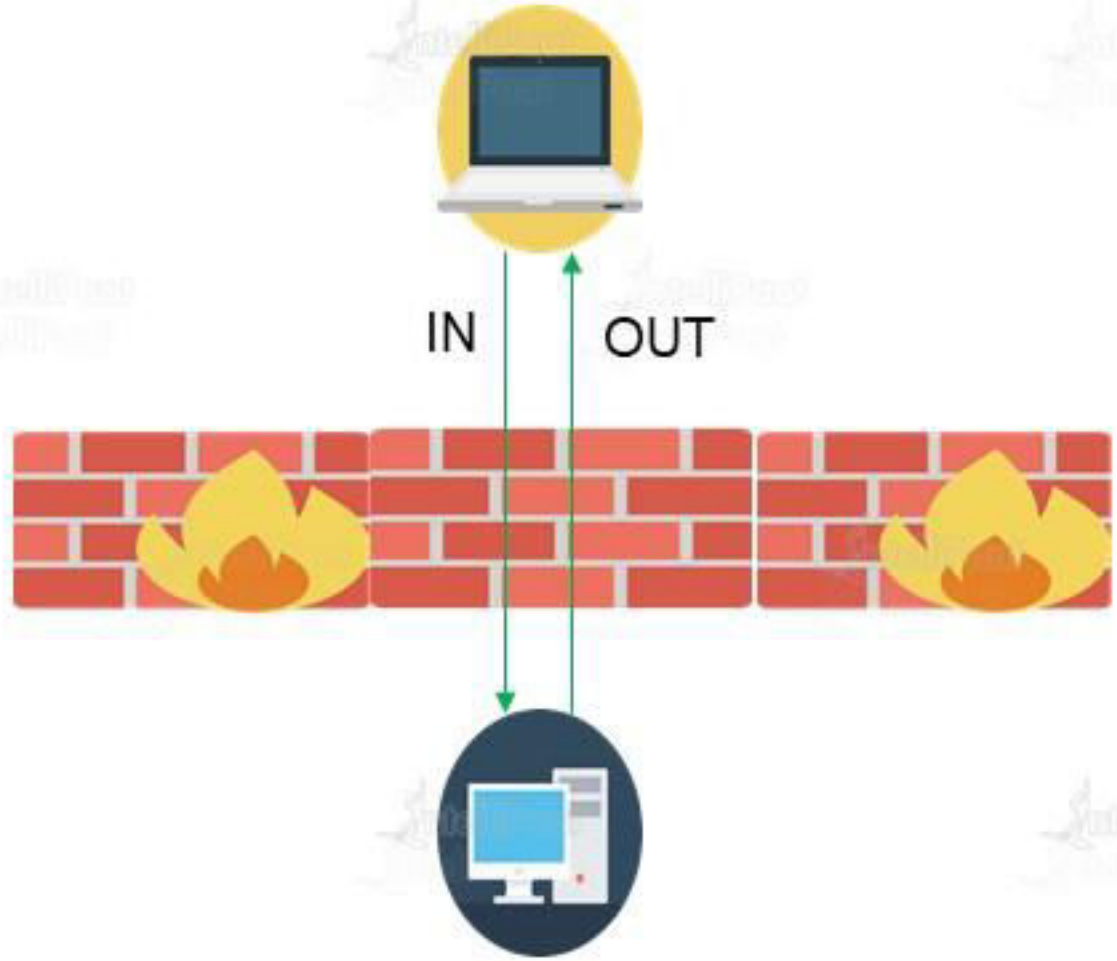
- Firewall is a system made to prevent unauthorized traffic to and from your PRIVATE network/computer/server by Allowing or Denying those traffic.
- Allowing and denying traffic are mentioned by Rules, also called firewall rules.



Firewall

Types

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



Demo 1: VPC

Demo 1: VPC

Creating VPC and Subnets

1) Create VPC with CIDR block 24.8.0.0/20 (myVPC) in the Region N. Virginia.

2) Create 3 subnets in the VPC created above. All 3 subnets should be in different Availability Zones.
   1) myVPC-subnet-1A
   2) myVPC-subnet-1B
   3) myVPC-subnet-1C

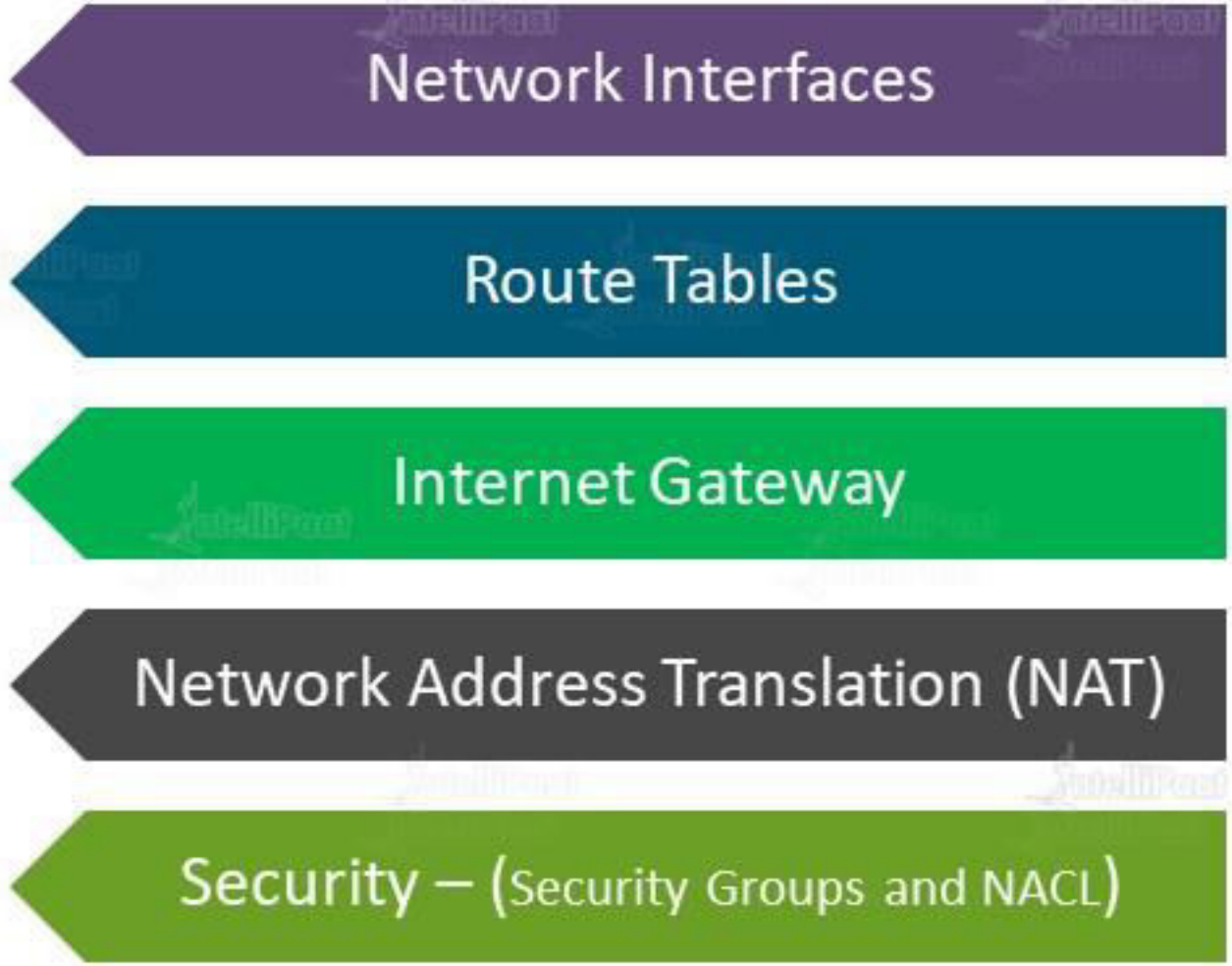
3) myVPC-subnet-1A should be PUBLIC subnet. myVPC-subnet-1B, myVPC-subnet-1C should be PRIVATE subnets.

4) Launch two EC2 instances in each of the subnets 1A and 1B created above.

5) Launch one instance in the subnet 1C.

Components of VPC

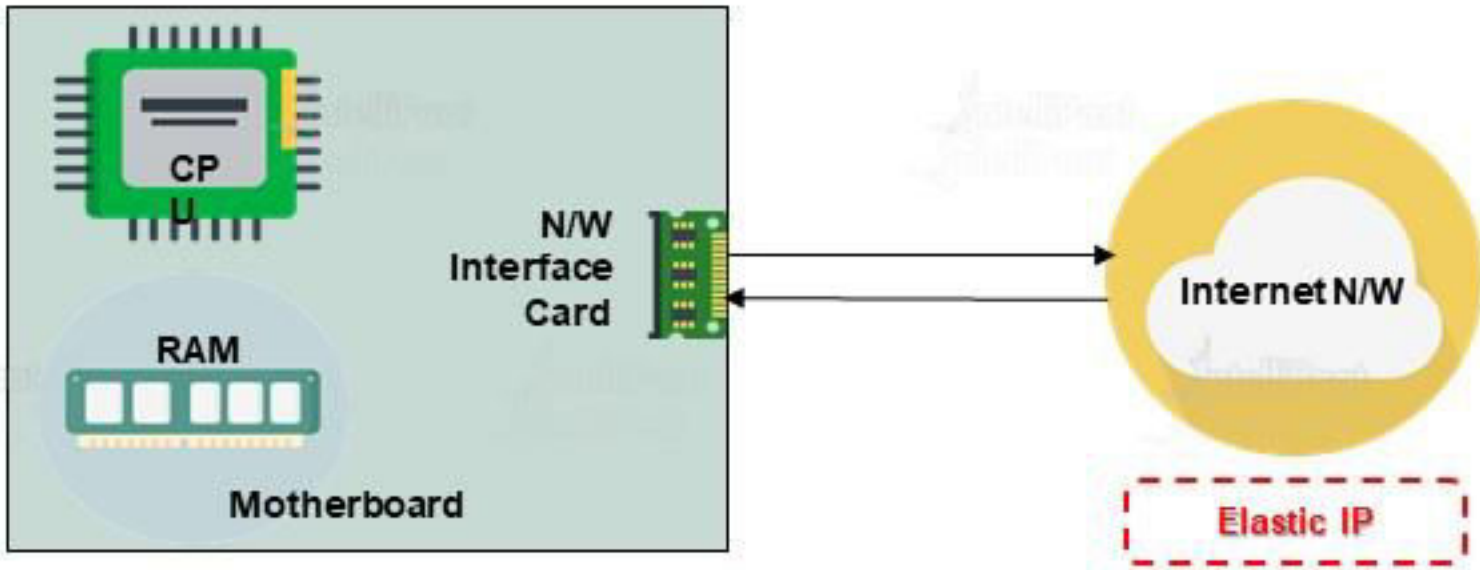
Components of VPC



Network Interfaces

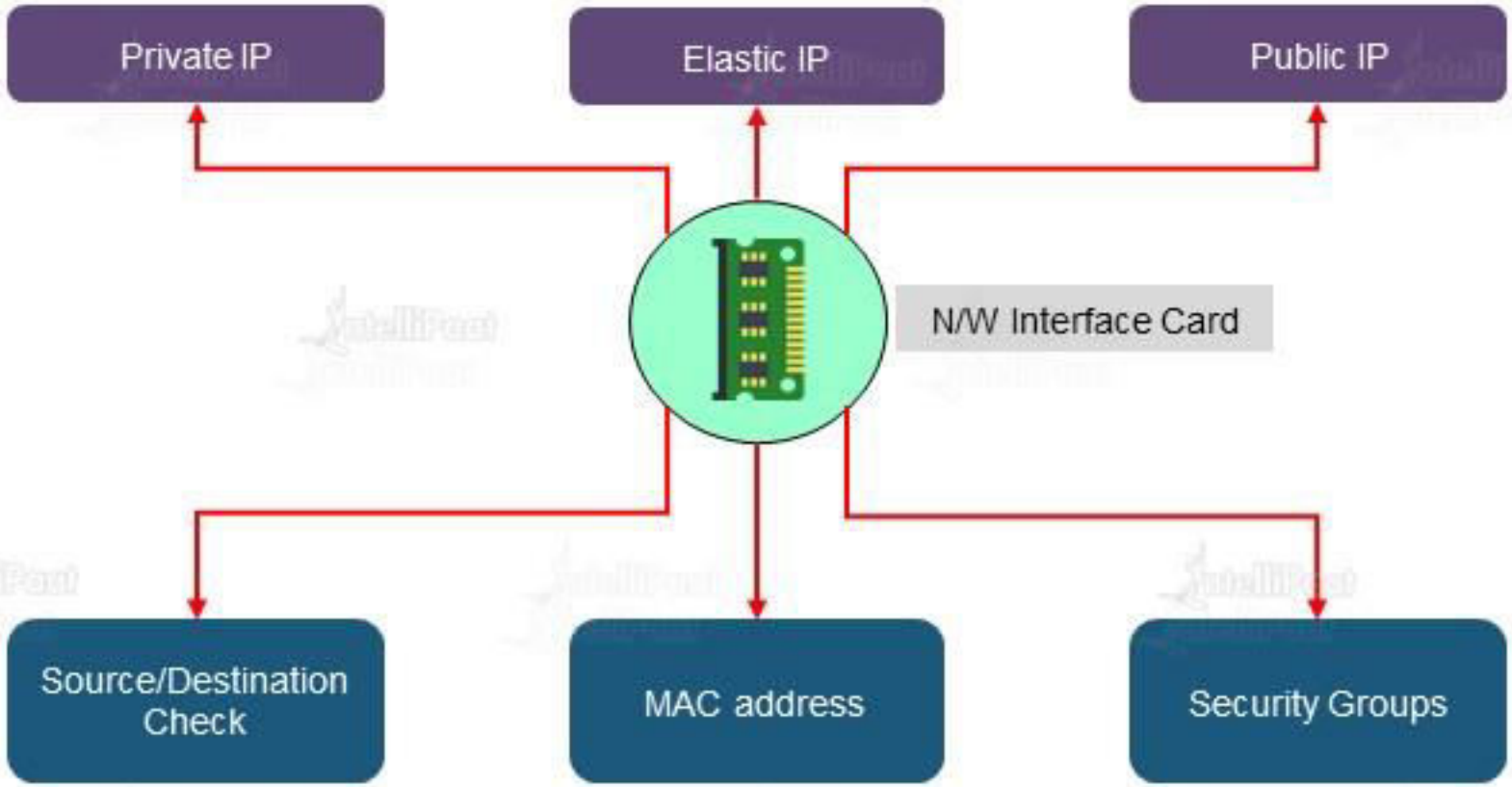
Network Interface

- 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

Elastic Network Interface – It is a Virtual Network Interface and it contains all of the attribute below

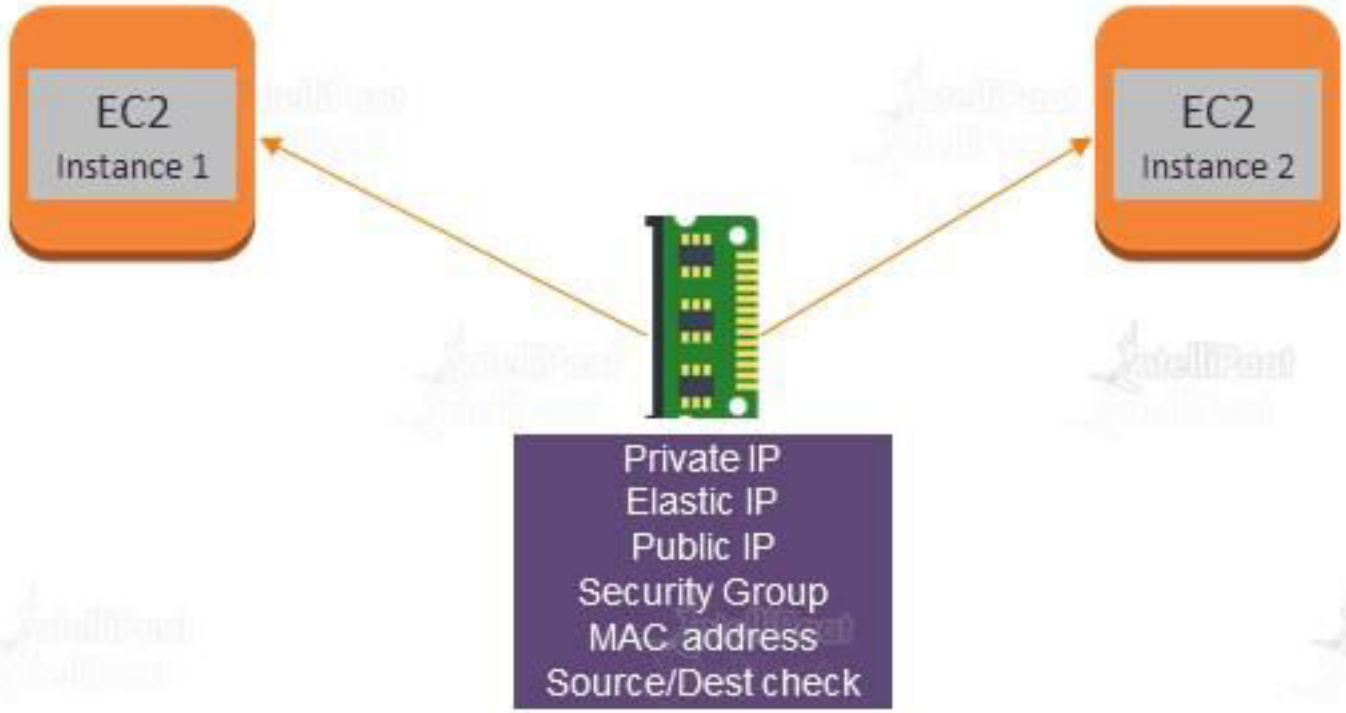


Network Interfaces

Elastic Network Interface

Network interface can be:

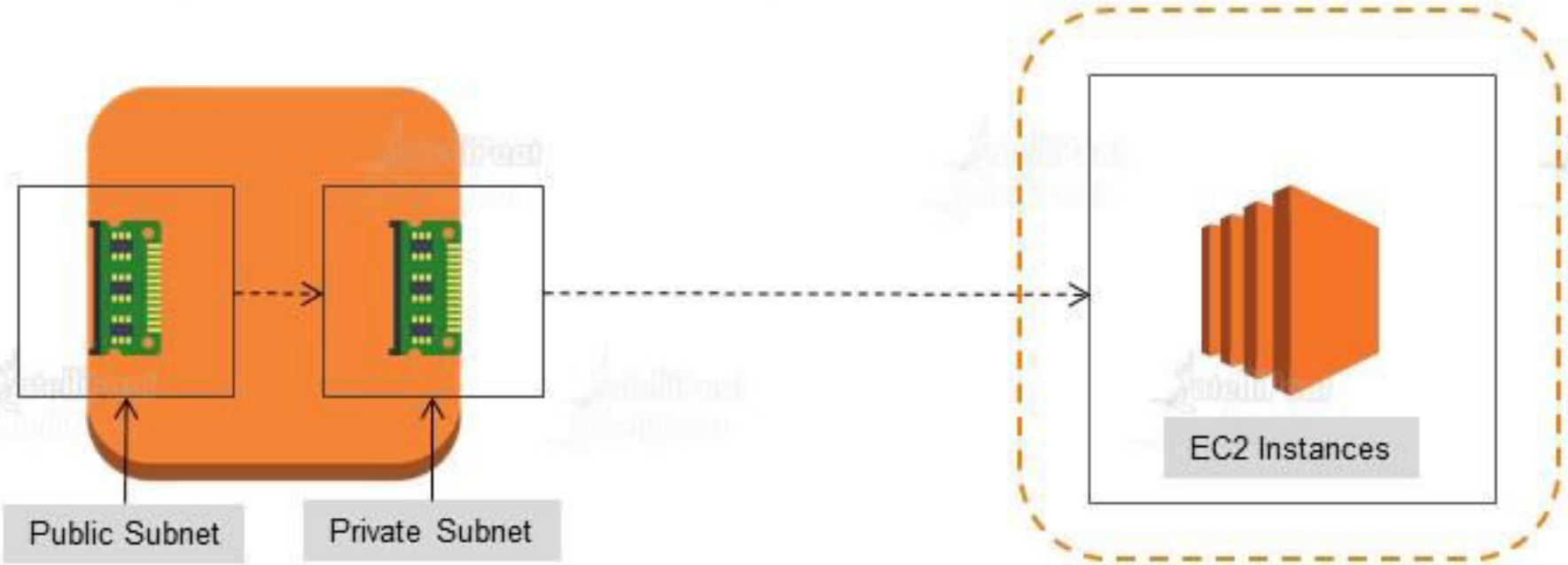
- Created to an Instance
- Attached to an Instance
- Detached from an Instance
- Re-attached to another instance.



Network Interfaces

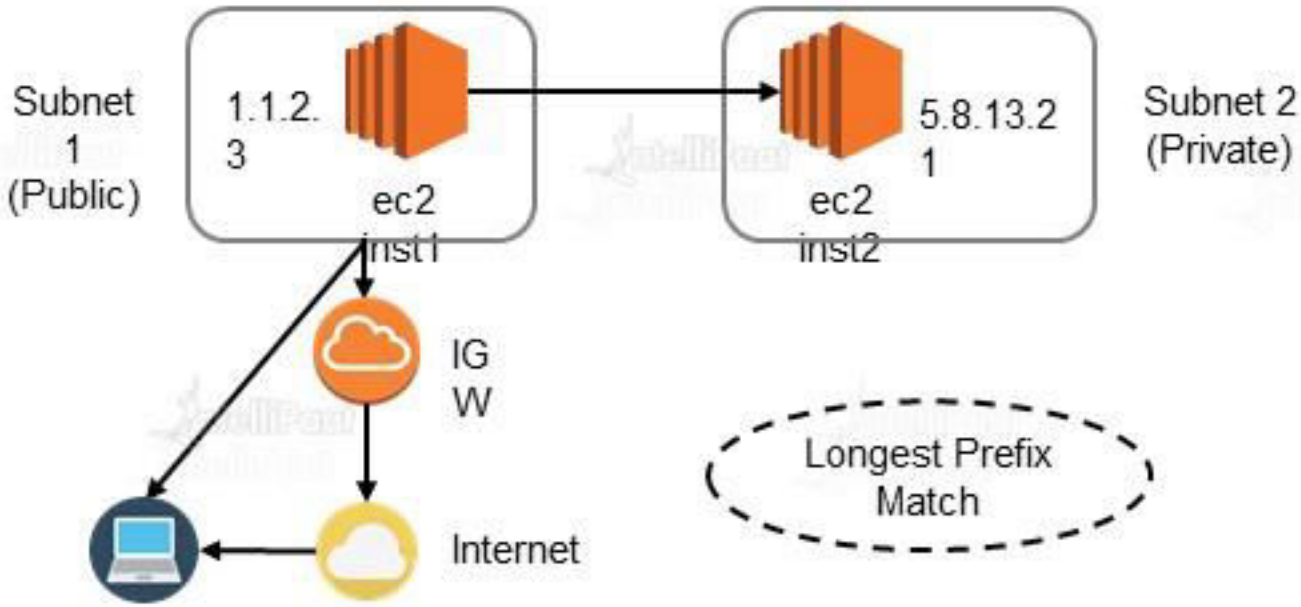
Multiple IP Addresses

- 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.



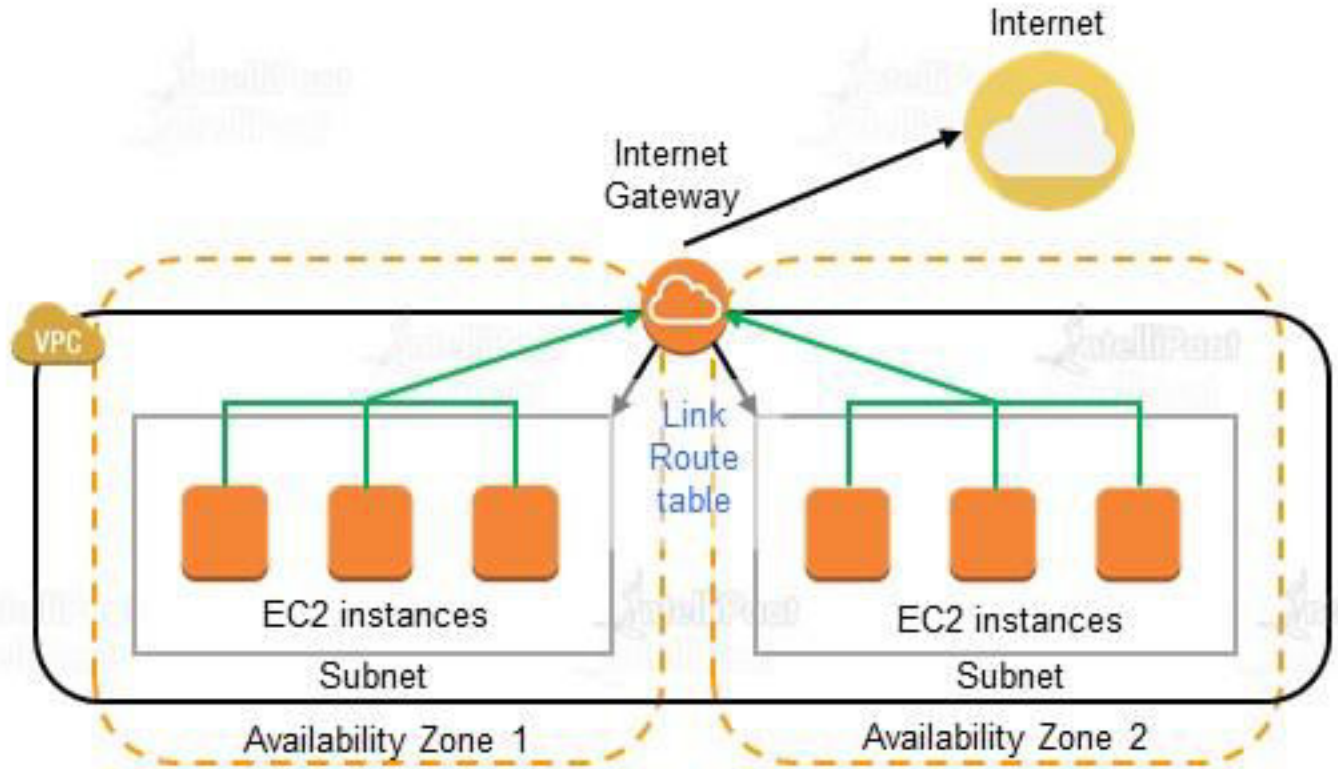
Destination	Target
5.8.13.21	Local
0.0.0.0/0	IGW
6.4.2.1/32	IGW

Internet Gateways

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

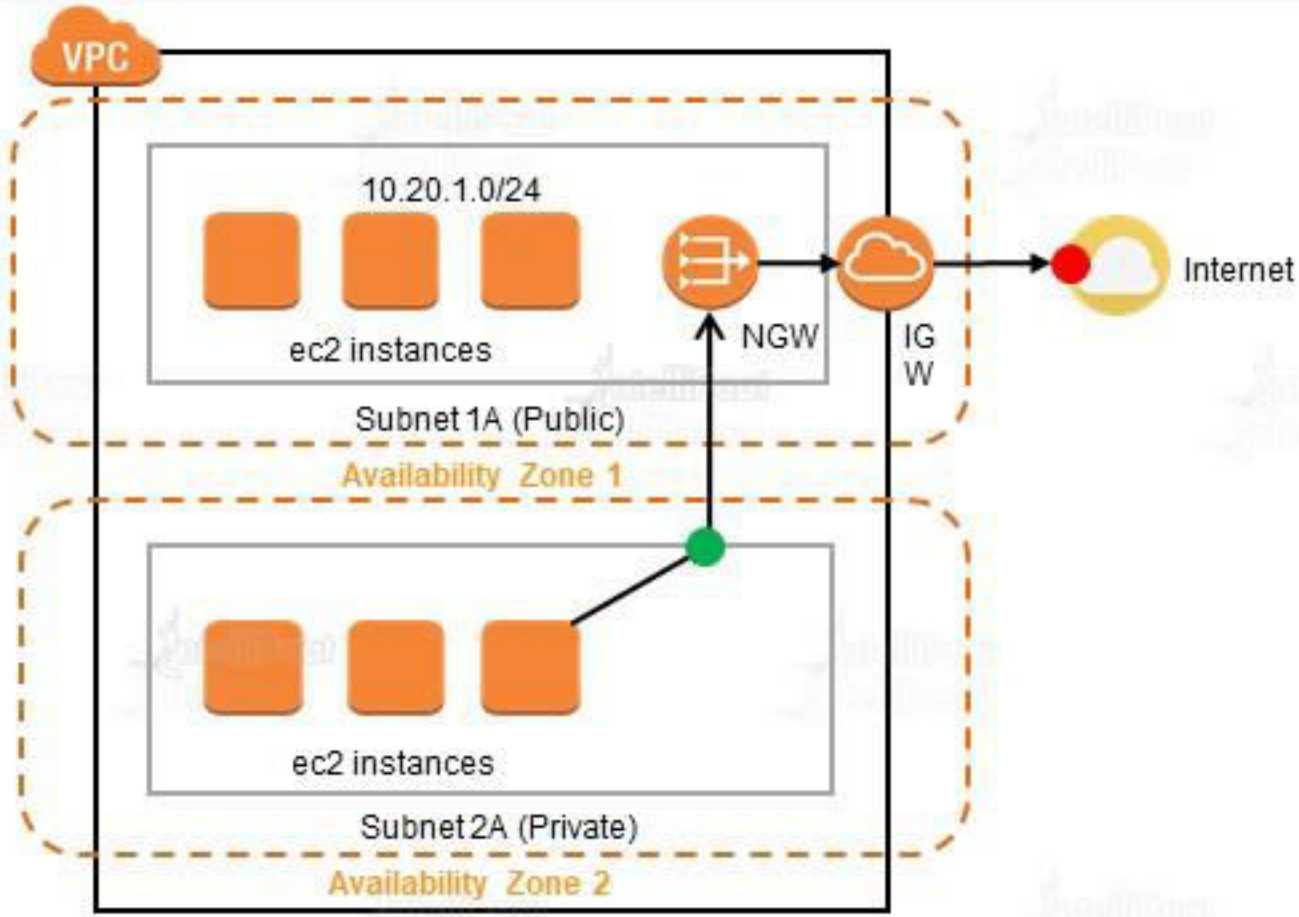
Purpose of an Internet Gateway

- 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.

Demo 2: NAT Gateway

Demo 2: NAT Gateway

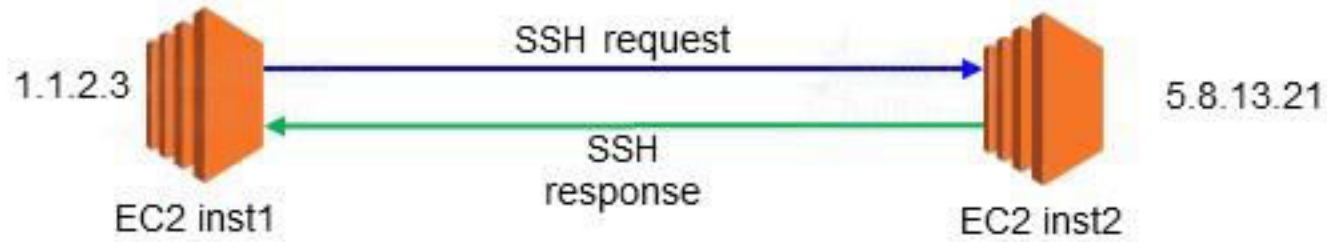
SG and NACL – 3 Tier Architecture

1) Use the public and private subnet which was created in the previous demo.
2) Spin up 1 instance each on public and private subnets – "pub" and "priv".
3) Setup NACLs to control traffic. "pub" should be able to ssh to "priv".
4) Try to install "httpd" service using command "sudo yum install -y httpd".
5) Create and attach a NAT gateway to pubic subnet.
6) Modify route tables and N/W ACL rules to allow "priv" to install httpd from internet.
7) Attach a public IP to "priv".
8) Try to ssh to priv from local machine. Failure shows that NAT does not allow request from internet to go into instances in private subnet.

Security in VPC

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

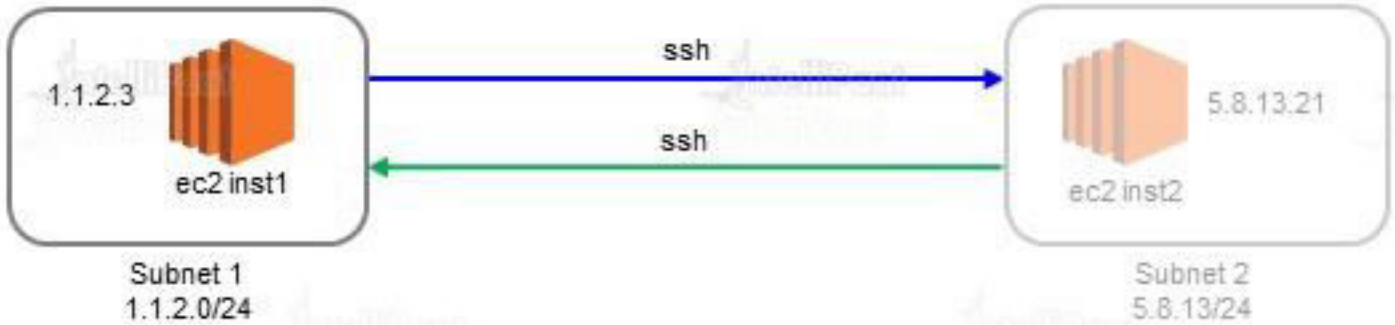
Inbound EC2 inst2

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

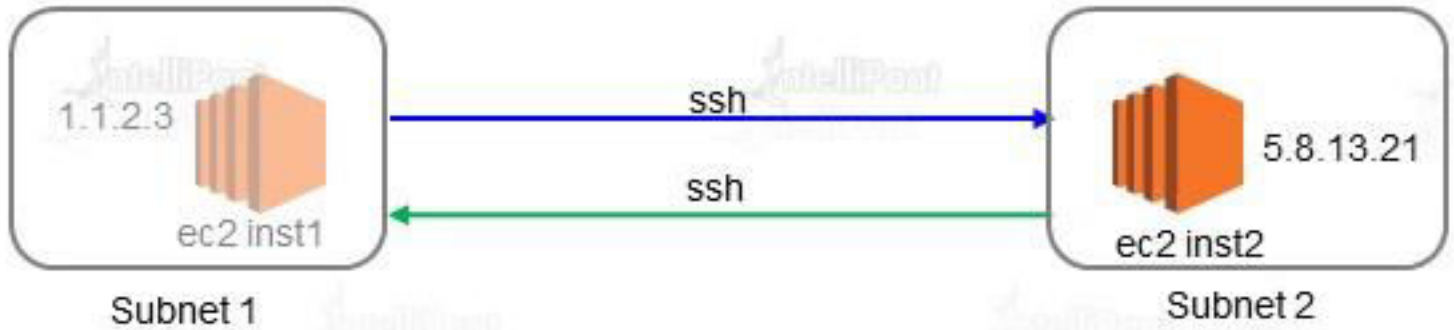
subnet1	Rule No.	Type	Protocol	Port	Destination	Allow/Deny
Outbound	100	SSH	TCP	22	5.8.13.0/24	ALLOW
Outbound	200	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

Demo 3: Security

Demo 3: Security

SG and NACL – 3 Tier Architecture

1) Create a VPC – "3tier-architecture" with CIDR 10.20.0.0/16. Create 3 subnets – 1 public - web and 2 private – app and db.
2) Launch "web1" and "web2" instances in Subnet "web".
3) Launch "app1" and "app2" in Subnet "app".
4) Launch "db1" in Subnet "db".
5) "web1" and "web2" are basic httpd web servers and should be connectable from internet on ports 22 (SSH) and 80 (HTTP). Test it.
6) "app1" and "app2" should only be connectable from "web1" and "web2" using Private IP addresses over port 22 (SSH).
7) "db1" should be connectable only from "app1" and "app2" using Private IP address over port 22 (SSH).

Types of VPC

Types of VPC

Default and Non-default VPC

Default VPC

- EC2-VPC platform only - it comes with a default VPC that has a default subnet in each Availability Zone
- A default VPC has the benefits of the advanced features provided by EC2-VPC, and is ready for you to use

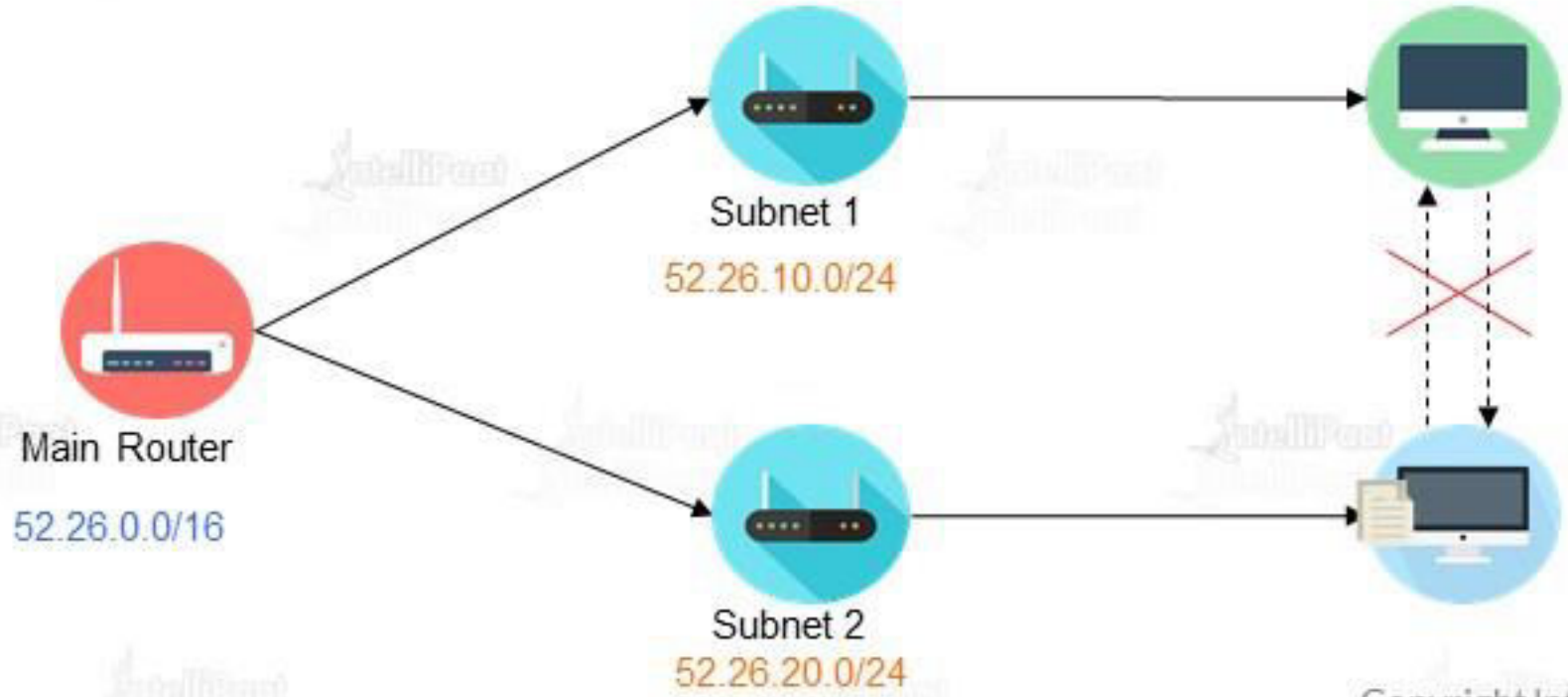
Non-default VPC

- Regardless of which platforms your account supports, you can create your own VPC, and configure it as you need
- Subnets created here are called as non-default subnets

Subnets

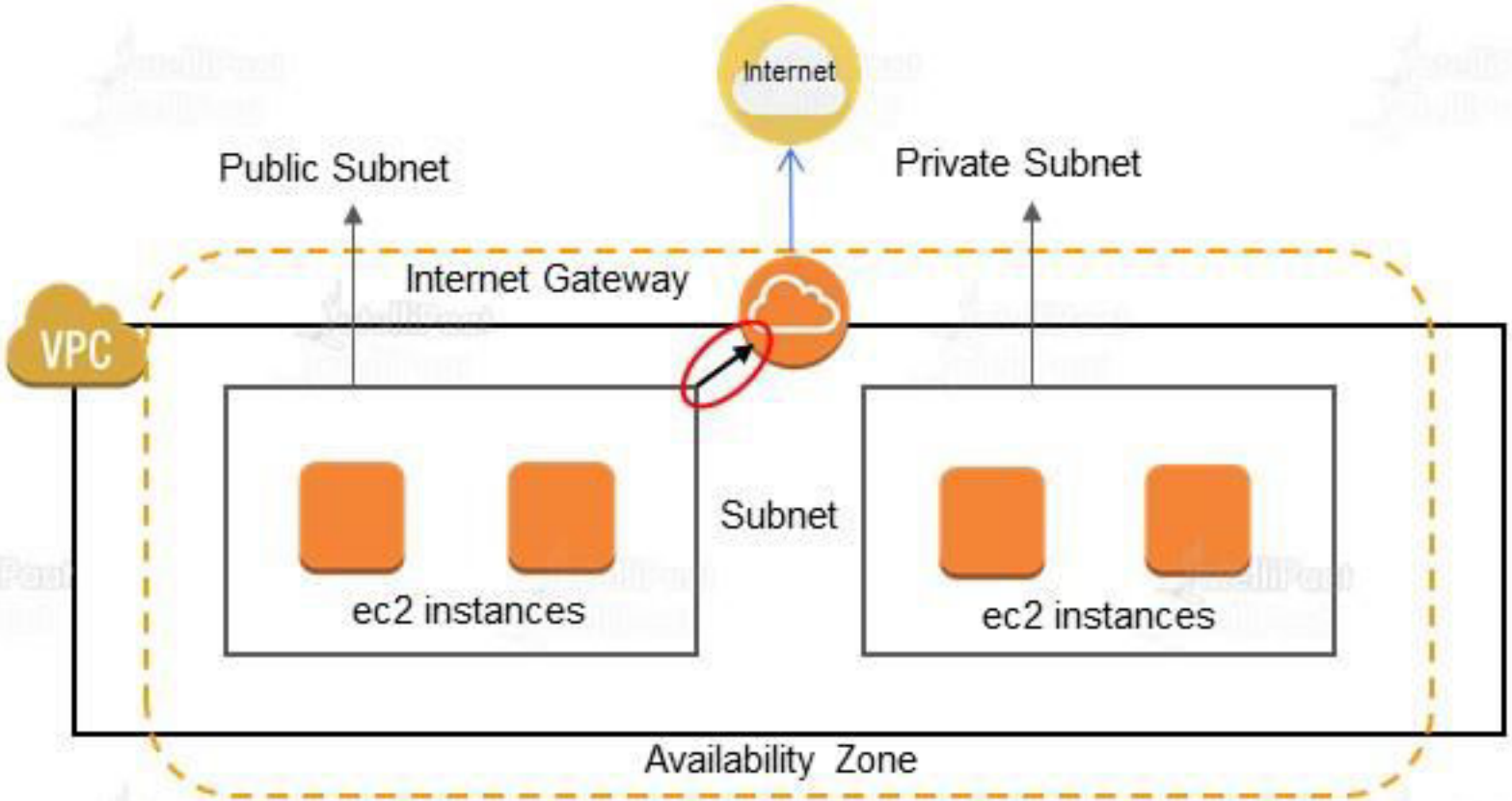
Subnets

- 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.



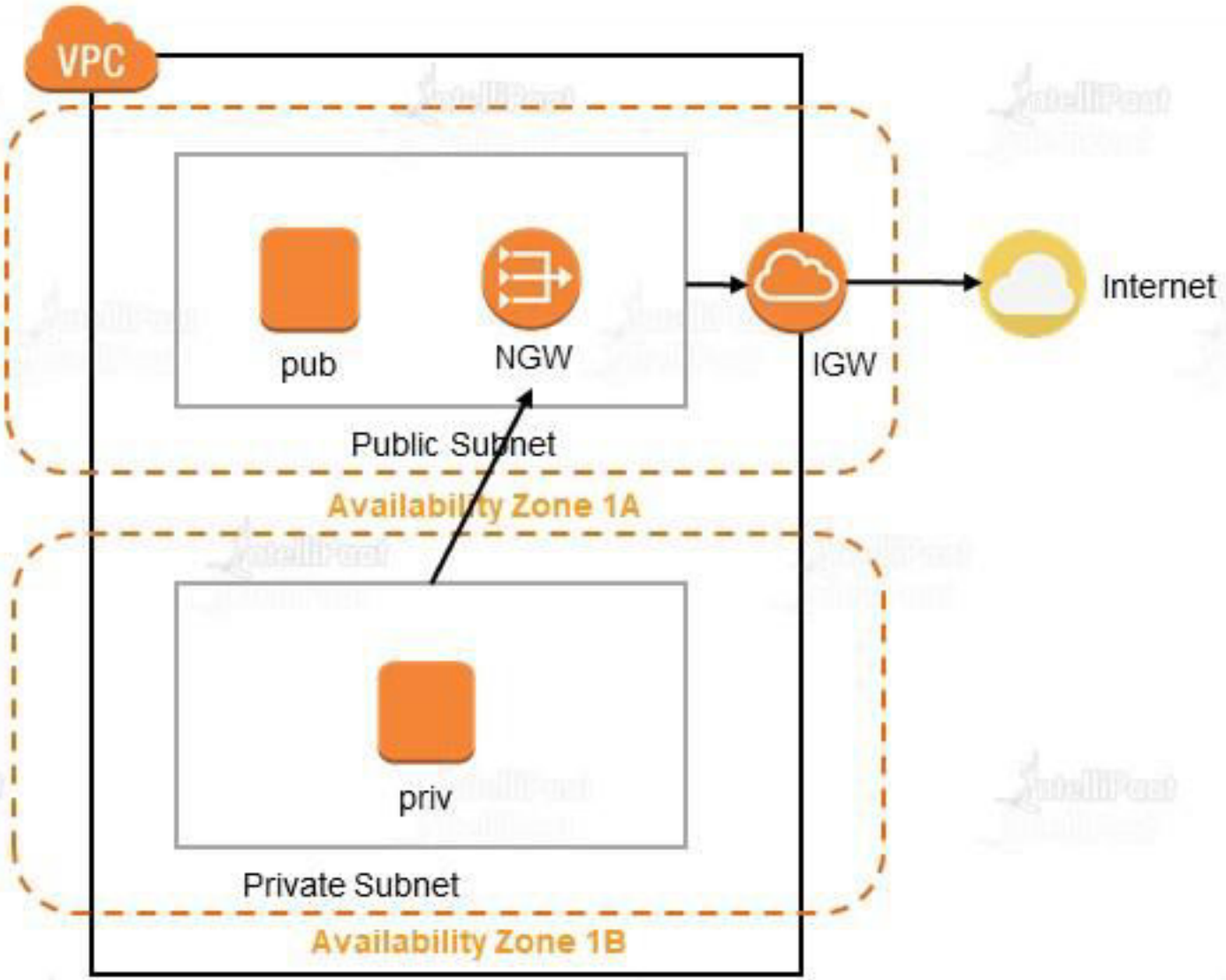
Subnets

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



Demo 4: VPC Architecture

Demo 4: Architecture

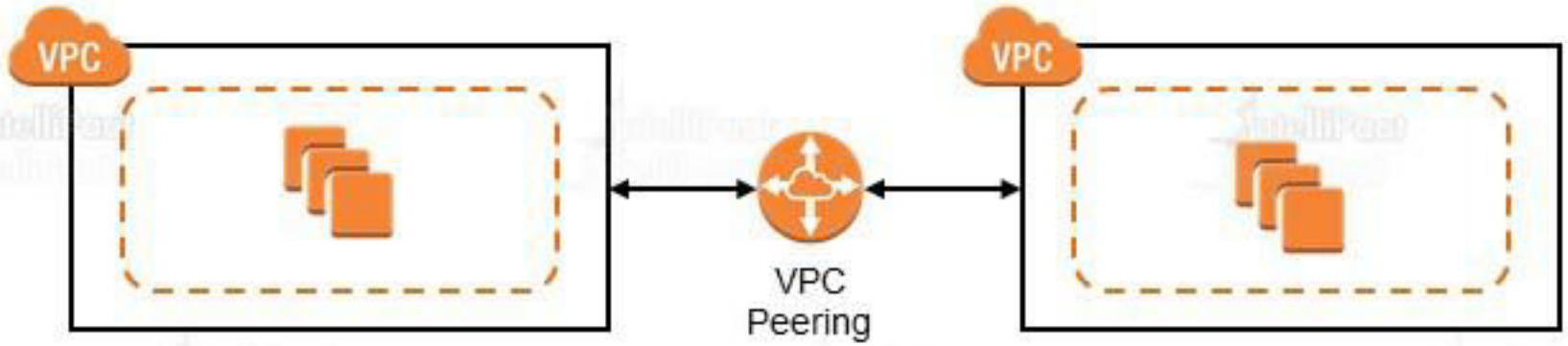


VPC Peering

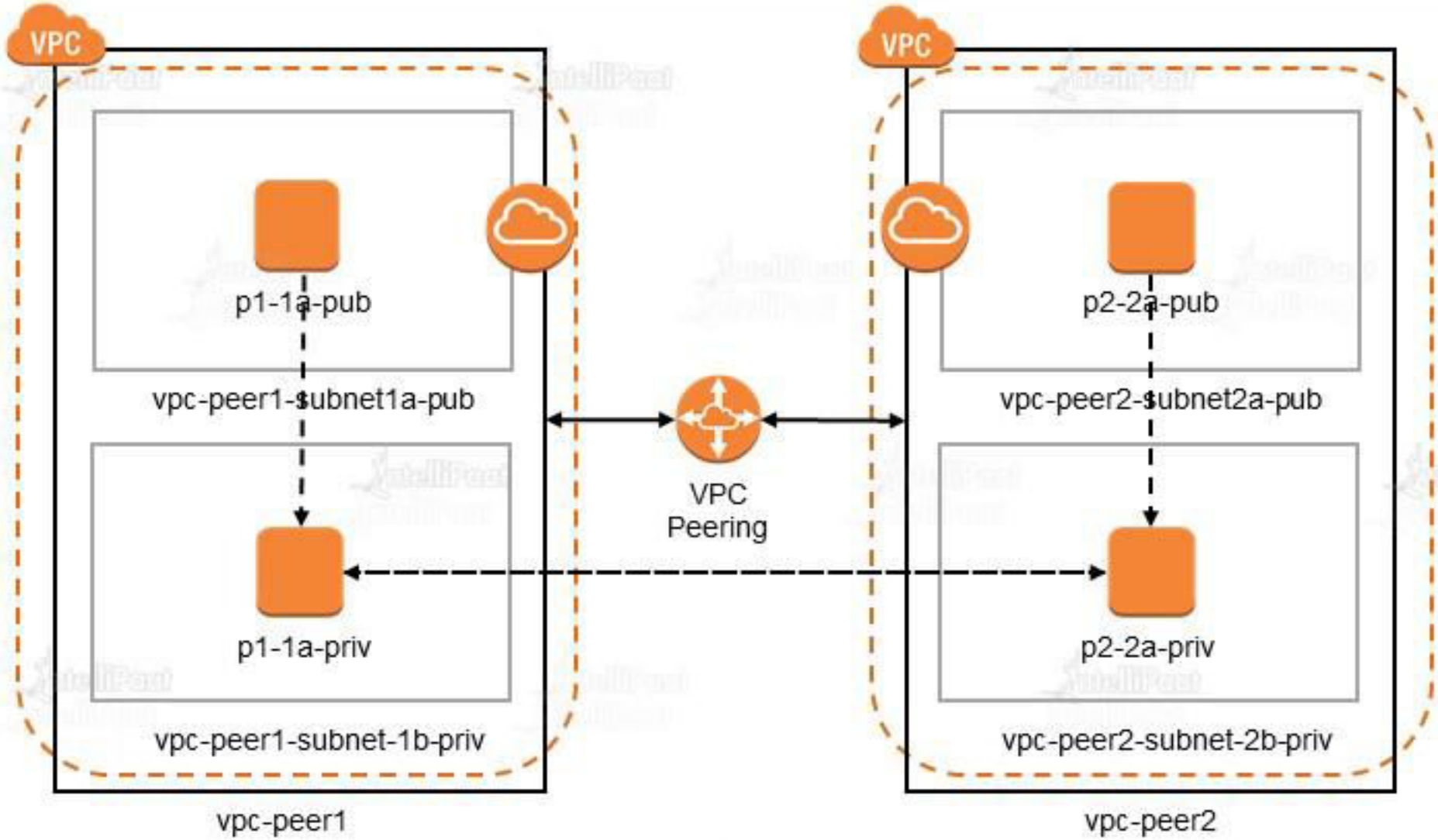
VPC Peering

VPC Peering

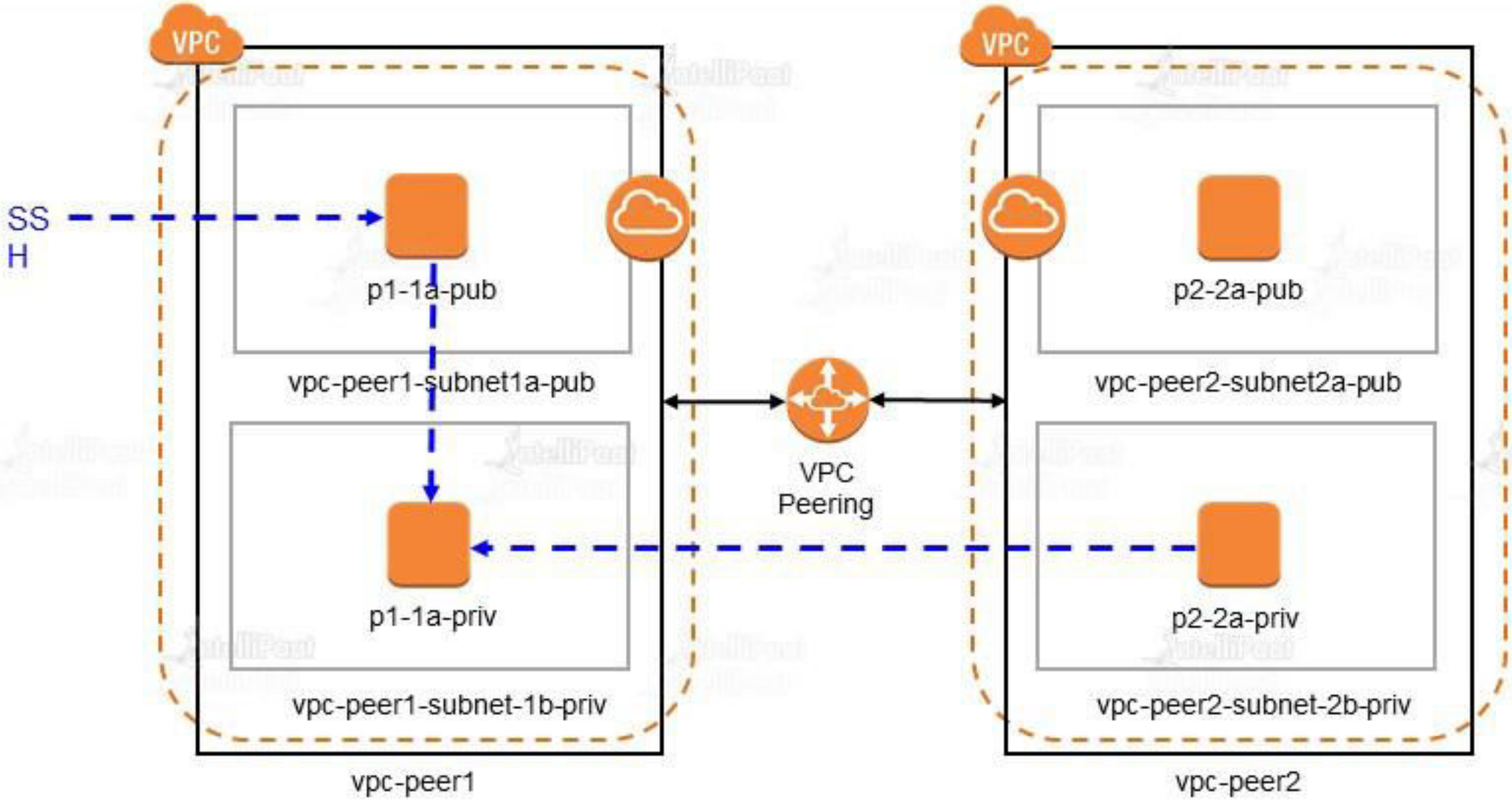
- Network connection between two VPCs which enables traffic flow between them using Private IP addresses.
- Peering connections can be created between VPCs in the same or different accounts and between VPCs in the same or different regions.



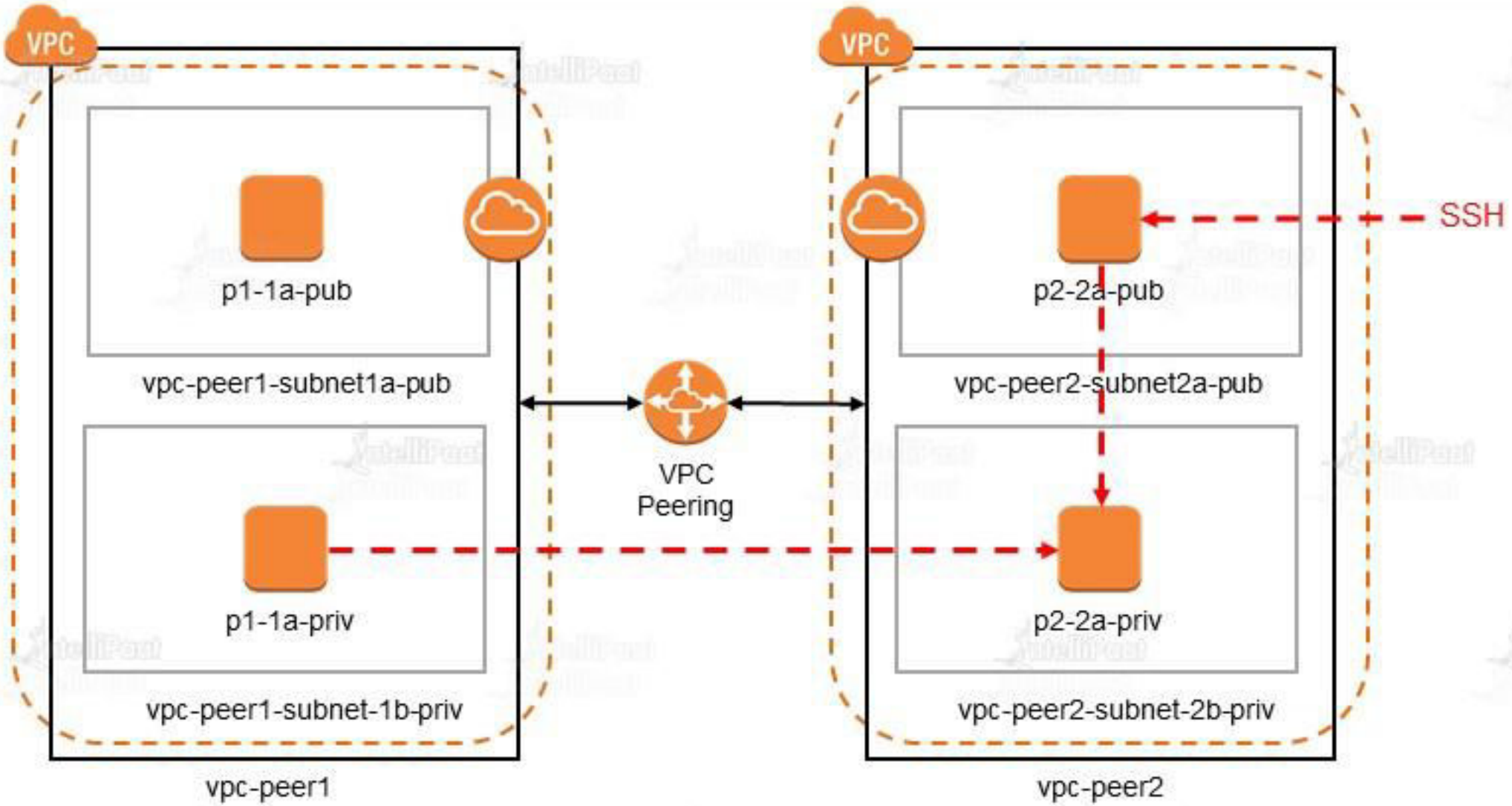
VPC Peering



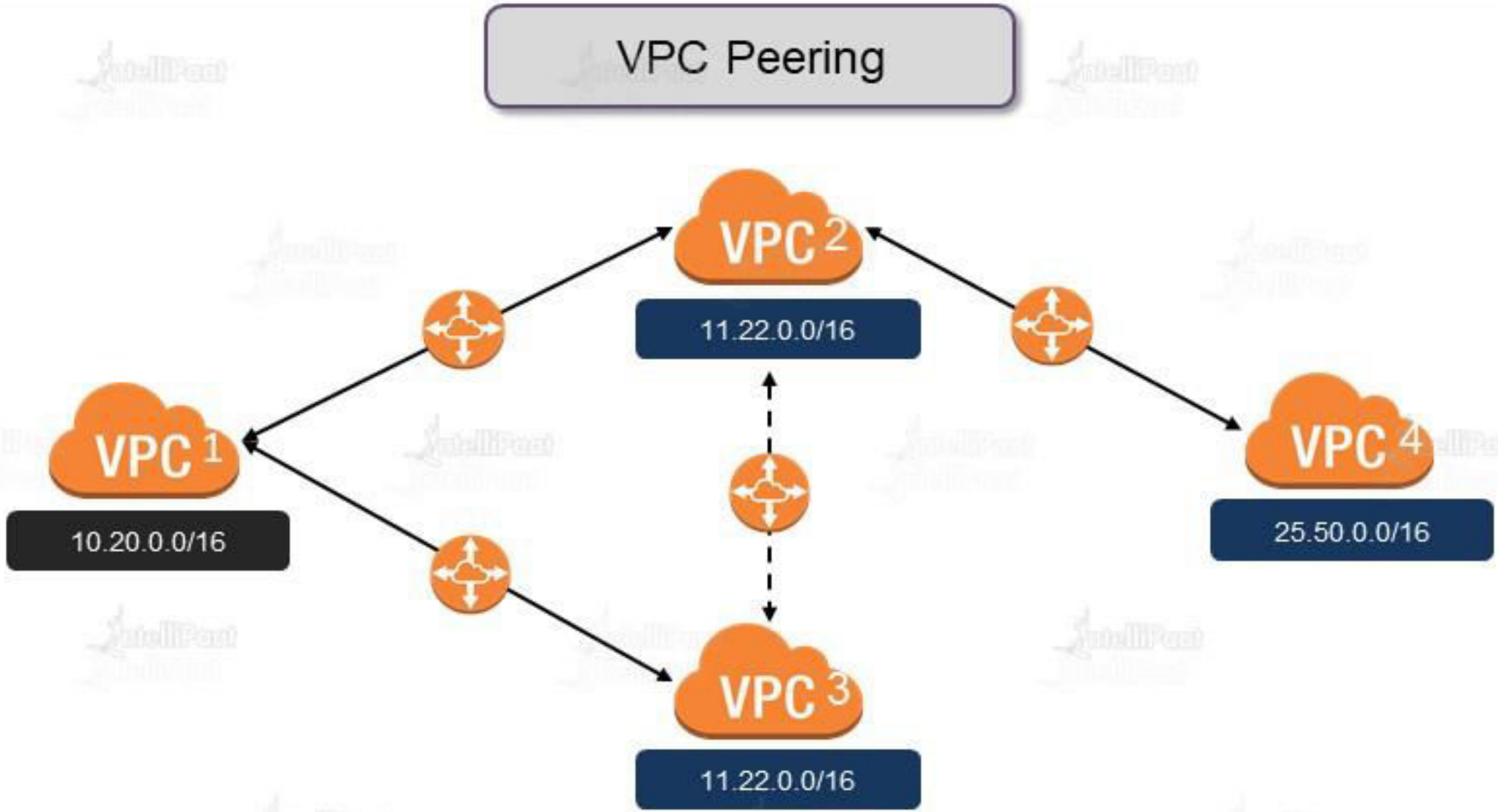
VPC Peering



VPC Peering



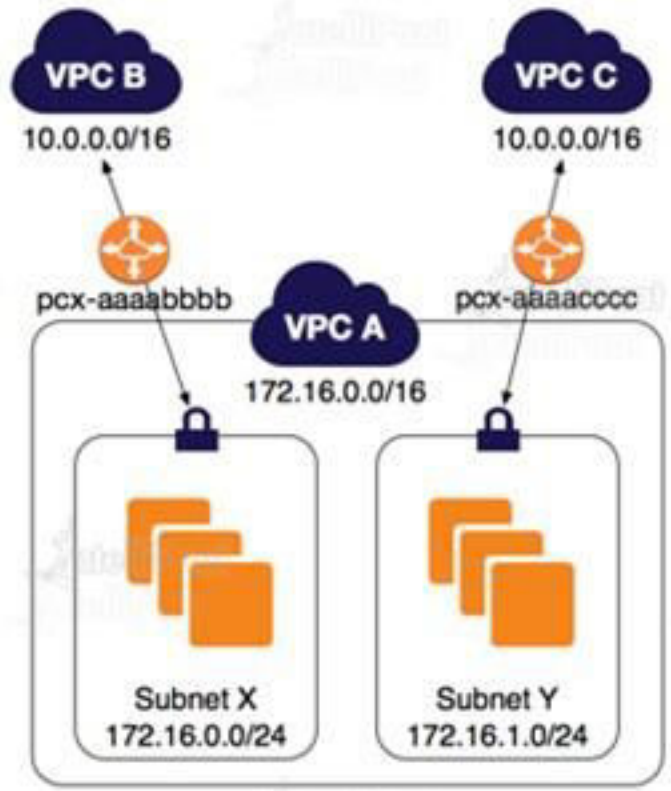
VPC Peering



VPC Peering

VPC Peering Scenarios

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

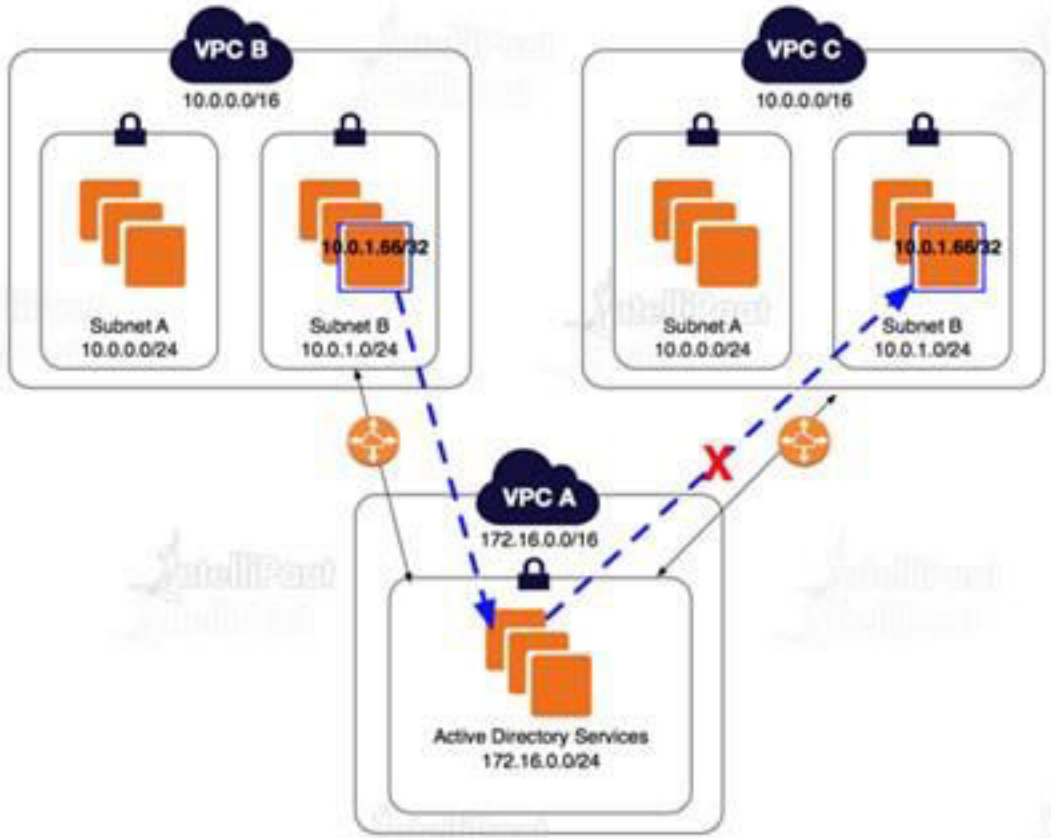


Route Table	Destination	Target
Subnet X in VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
Subnet Y in VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	172.16.0.0/24	pcx-aaaabbbb
VPC C	10.0.0.0/16	Local
	172.16.1.0/24	pcx-aaaacccc

VPC Peering

VPC Peering Scenarios

Two VPCs peered with specific subnets.



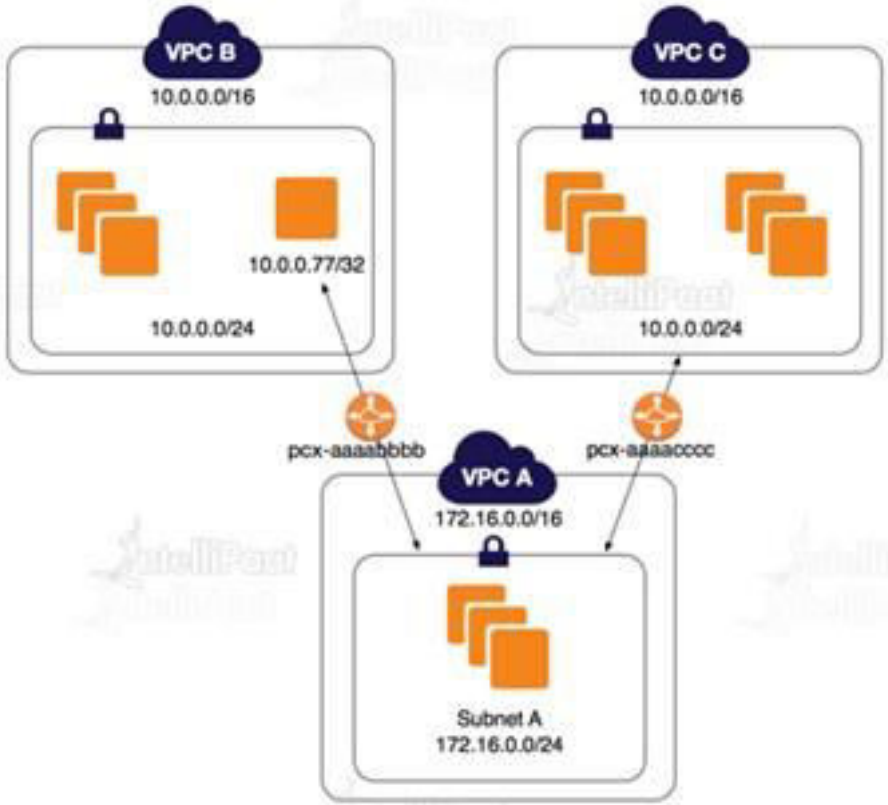
Route Table	Destination	Target
Subnet B in VPC B	10.0.0.0/16	Local
	172.16.0.0/24	pcx-aaaabbbb
VPC A	172.16.0.0/24	Local
	10.0.0.0/16	pcx-aaaacccc

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

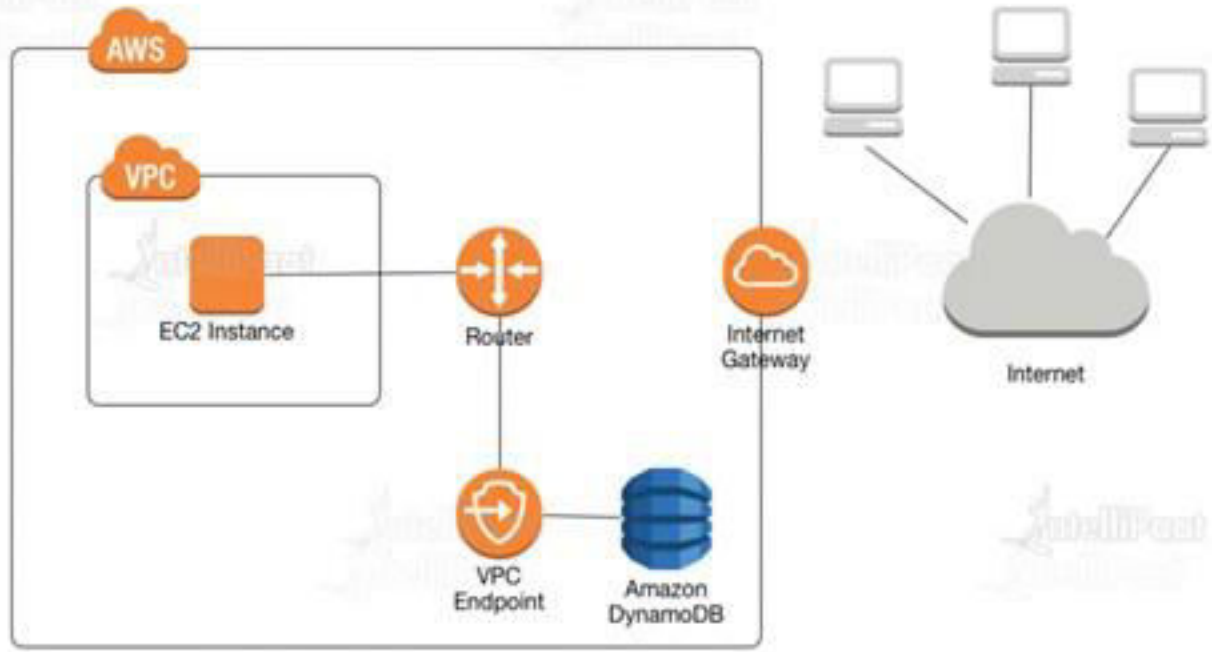
One VPC peered with two VPCs using Longest Prefix Match.



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

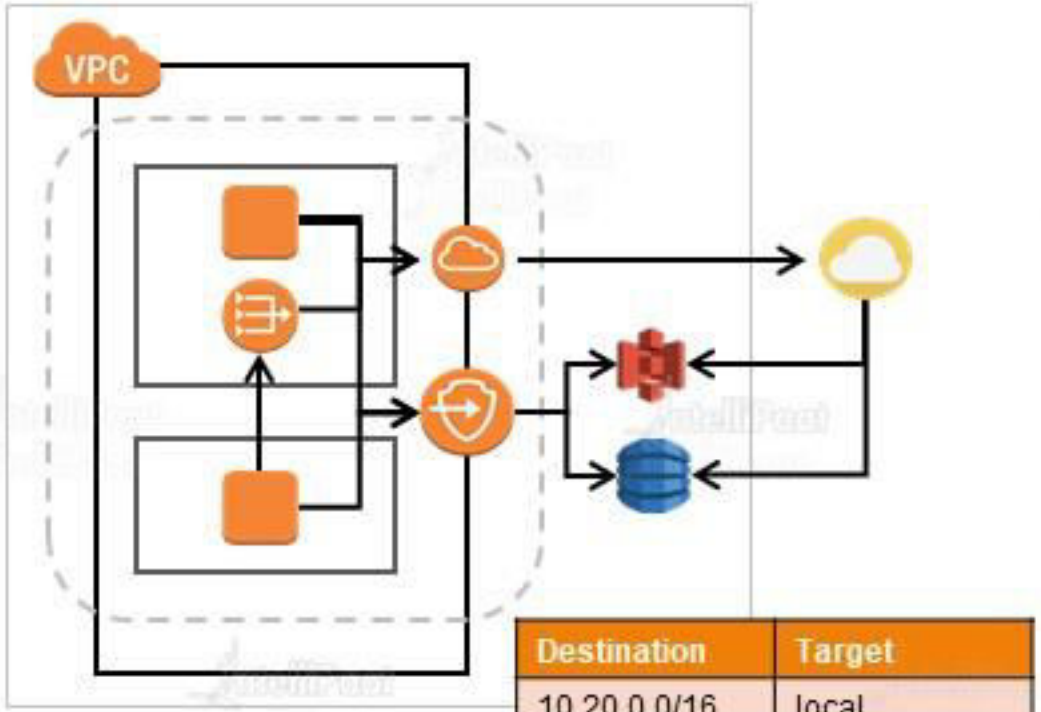
VPC Endpoints

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.



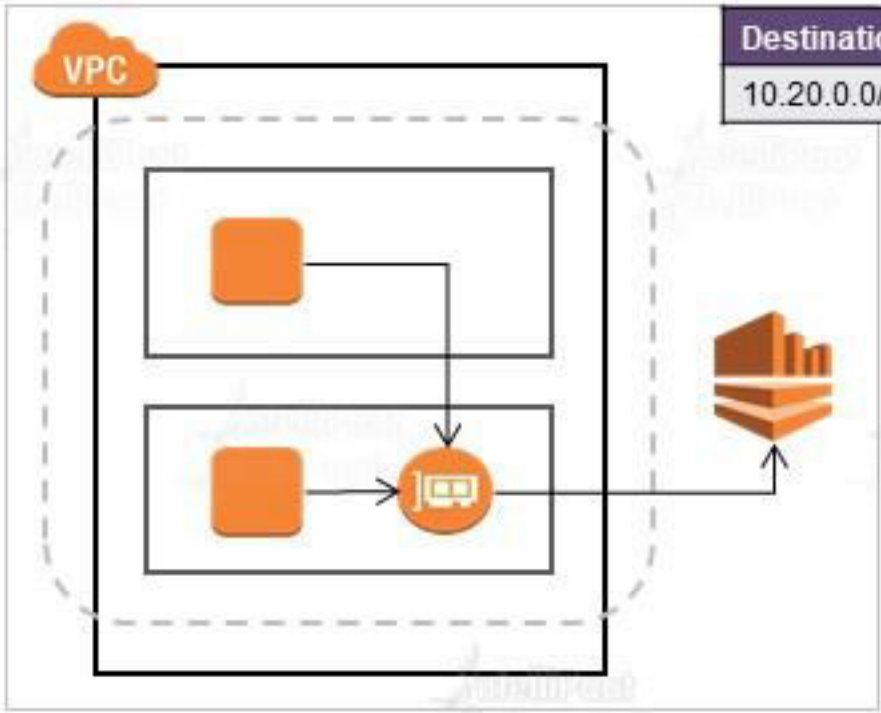
VPC Endpoints

Gateway Endpoint.



Destination	Target
10.20.0.0/16	local
To S3	vpce-id

Interface Endpoint – Powered by PrivateLink.



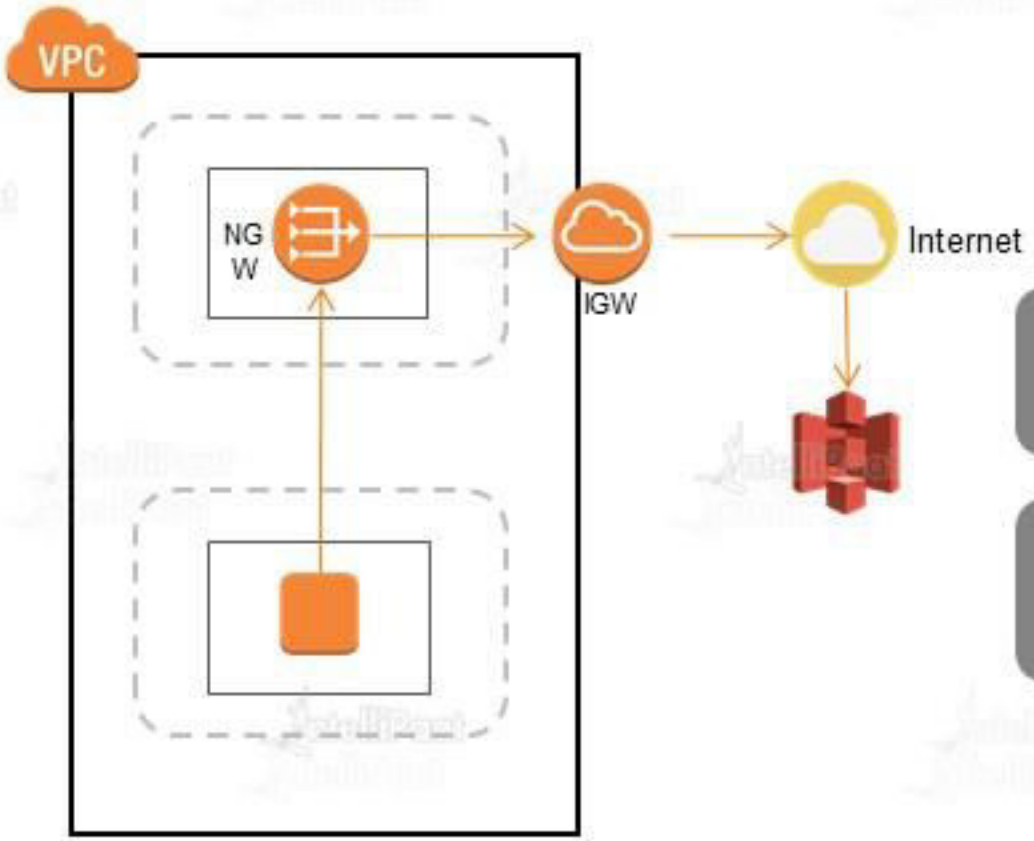
Destination	Target
10.20.0.0/16	local

VPC Pricing

VPC Pricing (us-east-1)

- 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 (us-east-1)



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

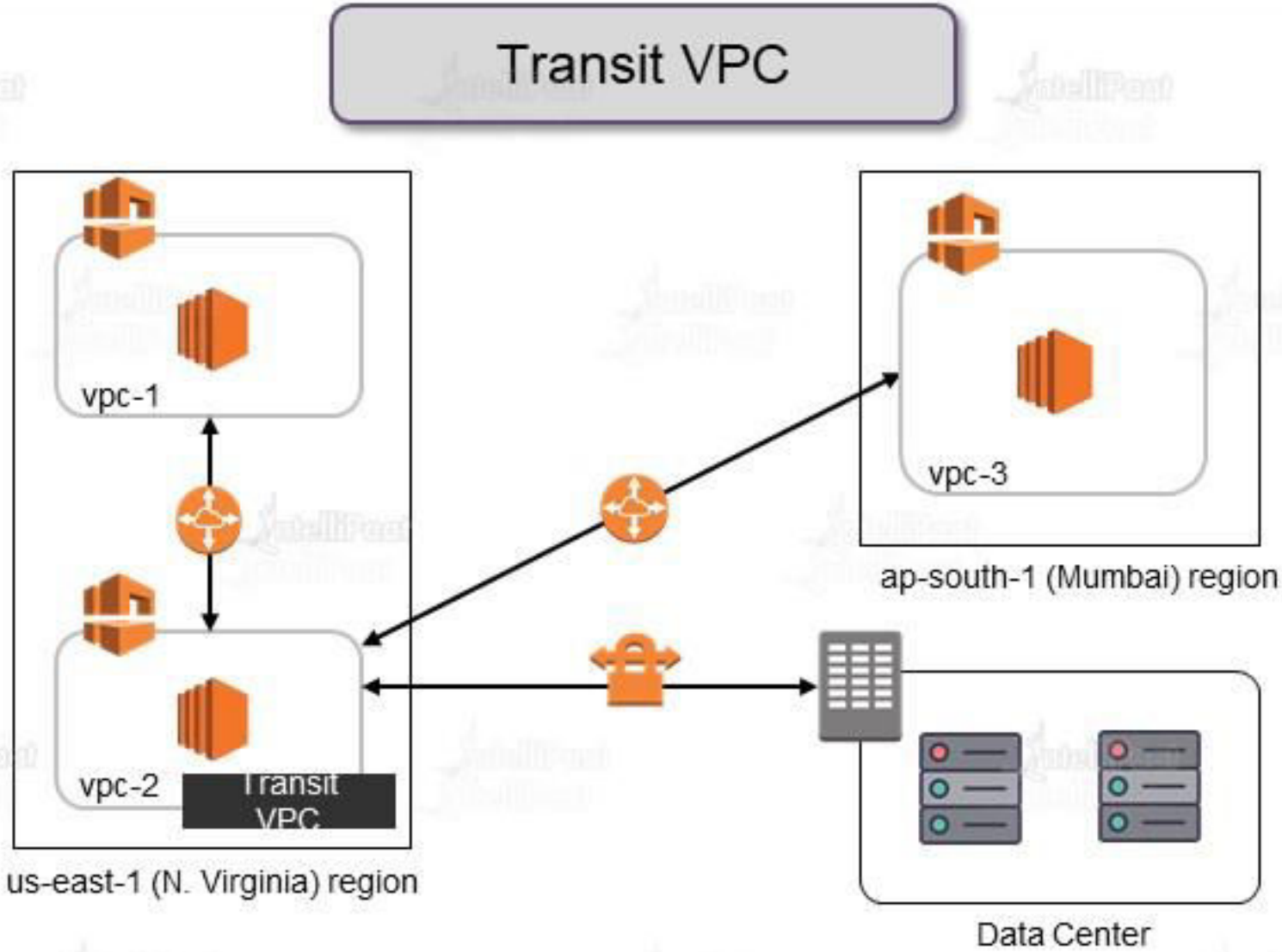
NAT GTW data processing price for 200 GB = $0.045*200 = $9.0

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

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

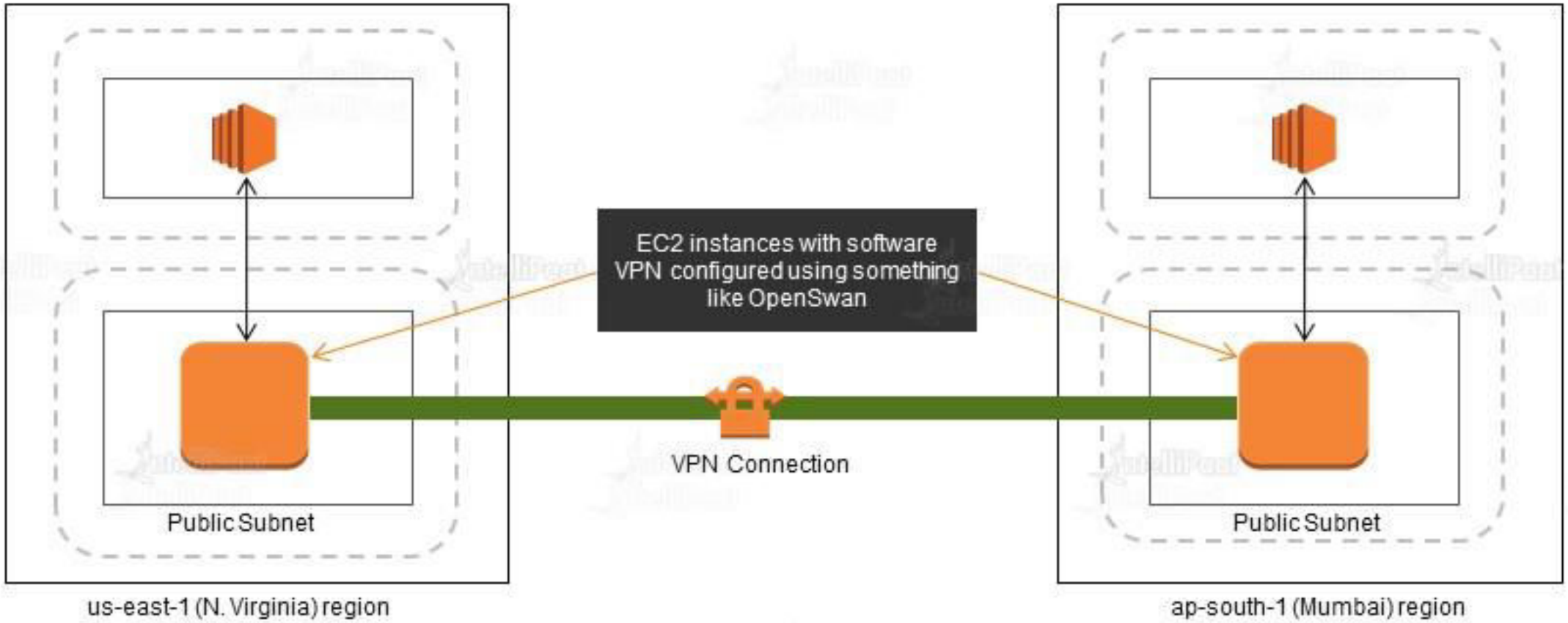
Design Patterns

Design Patterns



Design Patterns

Multi-region VPC connectivity



India : +91-7847955955

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

support@intellipaat.com

24X7 Chat with our Course Advisor