1. Bastion Host Between two Instance In two VPC Public subnets

**VPC A 172.16.0.0/16** Region(virginia)

EC2\_machine

Subnet\_Public -172.16.0.0/17

ROUTE Table:

|  |  |
| --- | --- |
| Destination | Target |
| 172.16.0.0/16 | local |
| 0.0.0.0/0 | IGW\_A |

NACL \_VPC A

|  |  |
| --- | --- |
| Type | Source |
| All Traffic | 0.0.0.0/0(in and out) |

EC2\_security group

|  |  |
| --- | --- |
| Type | source |
| SSH | My\_IP |

**VPC B** **10.0.0.0/16** Region(virginia)

Subnet Public 10.0.0.0/17

EC2\_Machine

ROUTE Table:

|  |  |
| --- | --- |
| Destination | Target |
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | IGW\_B |

NACL \_VPC A

|  |  |
| --- | --- |
| Type | Source |
| All Traffic | 0.0.0.0/0(in and out) |

EC2\_security group

|  |  |
| --- | --- |
| Type | source |
| SSH | VPC\_A\_subnet\_public(EC2 public IP) |

Simple Bastion Host in one VPC

**VPC 10.0.0.0/16**

Subnet Public 10.0.0.0/17

EC2\_machine

Subnet Private 10.0.128.0/17

EC2\_machine

ROUTE Table:

|  |  |
| --- | --- |
| Destination | Target |
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | IGW |

NACL \_VPC

|  |  |
| --- | --- |
| Type | Source |
| All Traffic | 0.0.0.0/0(in and out) |

Public Subnet EC2\_security group:

|  |  |
| --- | --- |
| Type | source |
| SSH | My IP |

Private Subnet EC2\_security group:

|  |  |
| --- | --- |
| Type | source |
| SSH | VPC\_subnet\_public(EC2 private IP) |

My Note (Bastion Host and VPC Peering):

* In Bastion Host “we connect to EC2 Instances in different VPC’S under PUBLIC SUBNET”. Those Instances should be in One Region (Intra Region) or Different Regions (Inter Region) we will connect but “we can’t connect to EC2 Instances in Different VPC’S under PRIVATE SUBNET” for this we will go to “VPC PEERING CONCEPT”. Whereas EC2 two Instances in one VPC under Public\_subnet and Private\_Subnet can able to connect via Bastion Host.

Simple VPC Peering in Inter Region (Check Non-overlapping CIDR Blocks)

VPC\_A : 172.16.0.0/16 (Region Virginia)

EC2\_Machine

Public Subnet 172.16.0.0/17

IGW\_A

ROUTE Table:

|  |  |
| --- | --- |
| Destination | Target |
| 172.16.0.0/16 | local |
| 0.0.0.0/0 | IGW\_A |
| 10.0.0.0/16 | Peering connection |

NACL \_VPC\_A :

|  |  |
| --- | --- |
| Type | Source |
| All Traffic | 0.0.0.0/0(in and out) |

Public Subnet EC2\_security group:

|  |  |
| --- | --- |
| Type | source |
| SSH | My IP |

Note:

+ Peering request Accepted in Ohio Region.

VPC\_B: 10.0.0.0/16 (Region Ohio)

private Subnet 10.0.0.0/17

EC2\_Machine

ROUTE Table:

|  |  |
| --- | --- |
| Destination | Target |
| 10.0.0.0/16 | local |
| 172.16.0.0/16 | Peering connection |

NACL \_VPC\_B :

|  |  |
| --- | --- |
| Type | Source |
| All Traffic | 0.0.0.0/0(in and out) |

Private Subnet EC2\_security group:

|  |  |
| --- | --- |
| Type | source |
| SSH | VPC\_A Public\_subnet (EC2 private IP) |

Note :

Intra Region Peering means peering one region. Both VPCS In One Region( ex: Virginia).

**NAT Instance:**

1. While creating NAT Instance select “Exiting NAT AMI”
2. NAT\_instance - go to Actions and select Networking - Click on Change Source/destination check – Active “Stop”.

**VPC – 172.16.0.0/16**

|  |  |
| --- | --- |
| Destination | Target |
| **172.16.0.0/16** | **local** |
| 0.0.0.0/0 | **IGW** |

**Private Route**

**Public Route**

IGE

Public Subnet 172.16.0.0/17

Private Subnet 172.16.128.1/17

EC2

EC2

|  |  |
| --- | --- |
| Type | Source |
| SSH | Private IP of EC2 Inst in private subnet |
| All ICMP IPv4 | Private IP of EC2 Inst in private subnet |

|  |  |
| --- | --- |
| Type | source |
| SSH | My IP |

|  |  |
| --- | --- |
| Destination | Target |
| **172.16.0.0/16** | **local** |
| 0.0.0.0/0 | **NAT\_Instance** |

|  |  |
| --- | --- |
| Type | source |
| SSH | My IP |

|  |  |
| --- | --- |
| Type | Source |
| SSH | Only EC2 instance private IP in Public Subnet |

NAT Instance