# Bastion Host process

# Creating VPC

resource "aws\_vpc" "VPC" {

   cidr\_block = "10.0.0.0/16"

  tags = {

    Name = "main"

  }

}

# Creating Public Subnet

resource "aws\_subnet" "PU" {

  vpc\_id     =  aws\_vpc.VPC.id

  cidr\_block = "10.0.1.0/24"

  tags = {

    Name = "PU"

  }

}

# Craeting Private Subnet

resource "aws\_subnet" "PR" {

  vpc\_id     =  aws\_vpc.VPC.id

  cidr\_block = "10.0.2.0/24"

  tags = {

    Name = "PR"

  }

}

# Creating IG

resource "aws\_internet\_gateway" "IGW" {

  vpc\_id = aws\_vpc.VPC.id

  tags = {

    Name = "IGW"

  }

}

# Creating Route tale for PU Instance

resource "aws\_route\_table" "RT" {

vpc\_id = aws\_vpc.VPC.id

route {

    cidr\_block = "0.0.0.0/0"

    gateway\_id = aws\_internet\_gateway.IGW.id

}

tags = {

    Name = "PURT"

  }

}

# Route table attachment

resource "aws\_route\_table\_association" "RTA" {

  subnet\_id      = aws\_subnet.PU.id

  route\_table\_id = aws\_route\_table.RT.id

}

# Creating Security group for Pu Instnace

resource "aws\_security\_group" "SG" {

  name        = "allow\_tls"

  vpc\_id      = aws\_vpc.VPC.id

  tags = {

    Name = "dev\_sg"

  }

 ingress {

    description      = "TLS from VPC"

    from\_port        = 80

    to\_port          = 80

    protocol         = "tcp"

    cidr\_blocks      = ["0.0.0.0/0"]

  }

ingress {

    description      = "TLS from VPC"

    from\_port        = 22

    to\_port          = 22

    protocol         = "TCP"

    cidr\_blocks      = ["0.0.0.0/0"]

  }

ingress {

    description      = "TLS from VPC"

    from\_port        = 443

    to\_port          = 443

    protocol         = "TCP"

    cidr\_blocks      = ["0.0.0.0/0"]

  }

egress {

    from\_port        = 0

    to\_port          = 0

    protocol         = "-1"

    cidr\_blocks      = ["0.0.0.0/0"]

  }

  }

# Creating Elastic IP

resource "aws\_eip" "EIP" {

  instance = aws\_instance.ec2.id

  domain   = "vpc"

}

# Creating NAT Gateway

  resource "aws\_nat\_gateway" "nat" {

  allocation\_id = aws\_eip.EIP.id

  subnet\_id     = aws\_subnet.PU.id

  tags = {

    Name = "gw NAT"

  }

  }

# Creating Public EC2 Instance with Pulic IP address

resource "aws\_instance" "ec2" {

    ami = var.ami

    instance\_type = var.instance\_type

    key\_name = var.key\_name

    subnet\_id = aws\_subnet.PU.id

    vpc\_security\_group\_ids = [aws\_security\_group.SG.id]

    associate\_public\_ip\_address = true

    tags = {

      Name = "Pu"

    }

  }

  # Creating Route tale for Private Instance and attach to NAT

resource "aws\_route\_table" "PVRT" {

vpc\_id = aws\_vpc.VPC.id

route {

    cidr\_block = "0.0.0.0/0"

     nat\_gateway\_id = aws\_nat\_gateway.nat.id

}

tags = {

    Name = "PVRT"

  }

}

# Private Route table attachment

resource "aws\_route\_table\_association" "PVRTA" {

  subnet\_id      = aws\_subnet.PR.id

  route\_table\_id = aws\_route\_table.PVRT.id

}

# Creating Private EC2 Instance without IP address

resource "aws\_instance" "ec23" {

    ami = var.ami

    instance\_type = var.instance\_type

    key\_name = var.key\_name

    subnet\_id = aws\_subnet.PR.id

    vpc\_security\_group\_ids = [aws\_security\_group.SG.id]

    tags = {

      Name = "Pr"

    }

  }