Prashant Lakhera
Mar 14, 2019 · 3 min read · Listen

100 Days of DevOps — Day 32-Introduction to NAT Gateway

Welcome to Day 32 of 100 Days of DevOps, Focus for today is NAT Gateway

> What is NAT Gateway

NAT gateway enables instance in Private Subnet to connect to the internet or other AWS services but prevent the internet from initiating a connection with those instances.

> **How NAT works**

- *NAT device has an Elastic IP address and is connected to the Internet through an internet gateway.*
- *When we connect an instance in a private subnet through the NAT device, which routes traffic from the instance to the internet gateway and routes any response to the instance*
- *NAT maps multiple private IPv4 addresses to a single public IPv4 address.*

NAT gateway doesn't support IPv6 traffic for that you need to use Egress only gateway.

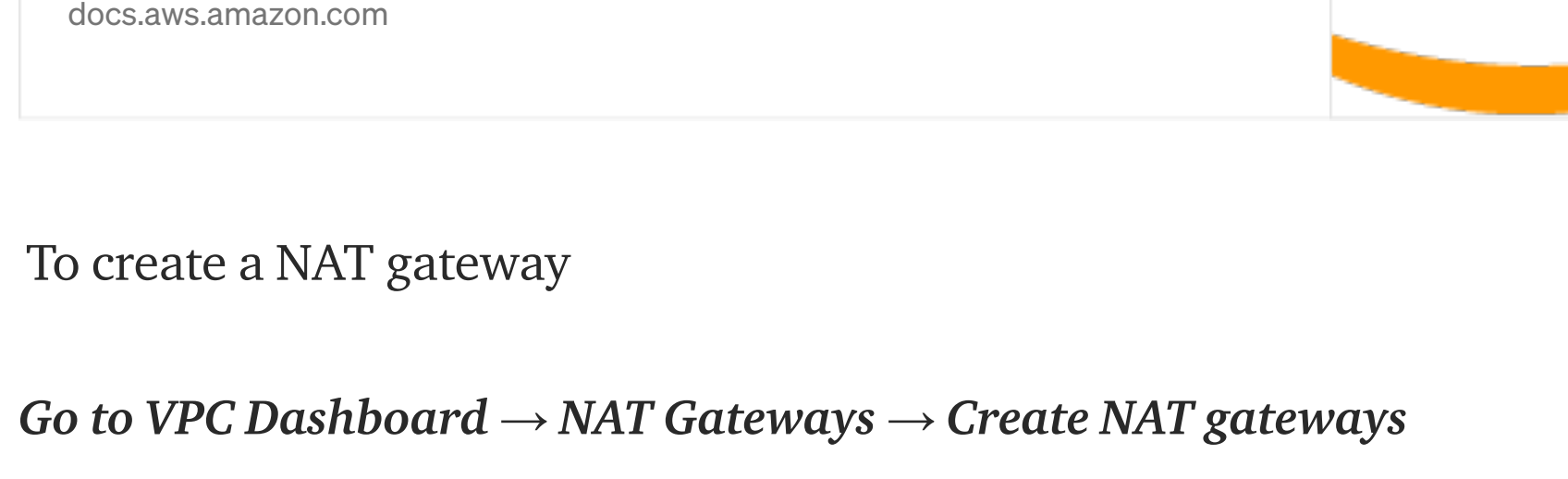
> **NOTE:** IPv6 traffic is separate from IPv4 traffic, route table must include separate routes for IPv6 traffic.

More info

Comparison of NAT Instances and NAT Gateways — Amazon Virtual Private Cloud
Compare NAT gateways and NAT instances.
docs.aws.amazon.com

> To create a NAT gateway

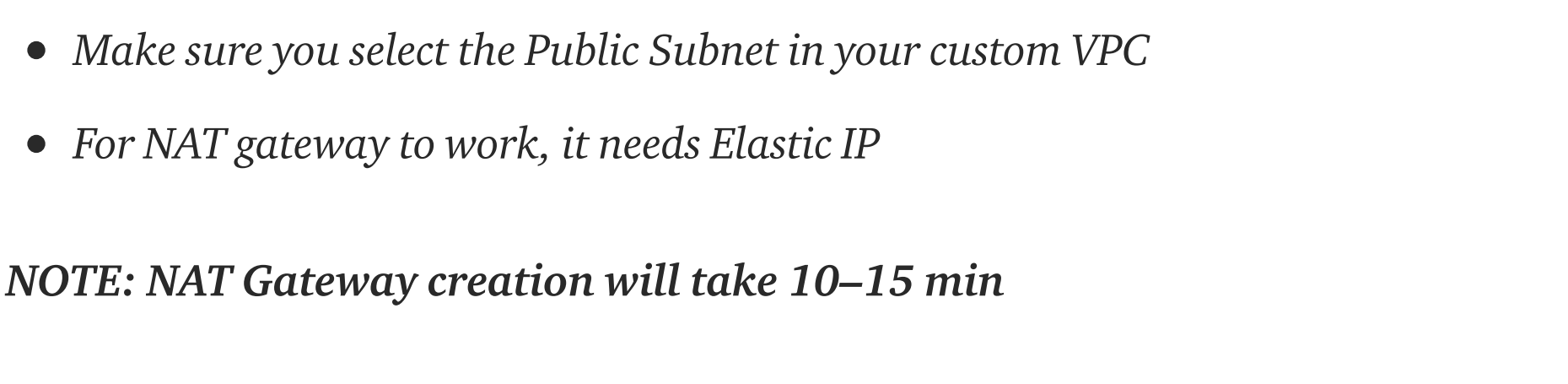
Go to VPC Dashboard → NAT Gateways → Create NAT gateways



- *Make sure you select the Public Subnet in your custom VPC*
- *For NAT gateway to work, it needs Elastic IP*

NOTE: NAT Gateway creation will take 10–15 min

- *Once the NAT gateway is available, add it to your default Route table*



The advantage of NAT Gateway

- *NAT gateway is highly available but we need it per availability zone.*
- *Can scale up to 45Gbps*
- *Managed by AWS*

Limitation of NAT Gateway

- *You can associate exactly one Elastic IP address with a NAT gateway. You cannot disassociate an Elastic IP address from a NAT gateway after it's created. To use a different Elastic IP address for your NAT gateway, you must create a new NAT gateway with the required address, update your route tables, and then delete the existing NAT gateway if it's no longer required.*
- *You cannot associate a security group with a NAT gateway. You can use security groups for your instances in the private subnets to control the traffic to and from those instances.*
- *You can use a network ACL to control the traffic to and from the subnet in which the NAT gateway is located. The network ACL applies to the NAT gateway's traffic*

Most of the code is the same as VPC Code

100daysofdevops/100daysofdevops
Contribute to 100daysofdevops/100daysofdevops development by creating an account on GitHub.
github.com

- *Some additions*

```
#Adding Elastic IP for NAT gateway

resource "aws_eip" "test_eip" {
  vpc = true
}

#Adding NAT Gateway

resource "aws_nat_gateway" "test_nat_gw" {
  allocation_id = "${aws_eip.test_eip.id}"
  subnet_id     = "${aws_subnet.public_subnet.0.id}"
}
```

nat_gateway.tf hosted with ❤ by GitHub view raw

As well as we need to tell associate NAT gateway to Private Route Table

```
# Private Route Table

resource "aws_default_route_table" "private_route" {
  default_route_table_id = "${aws_vpc.main.default_route_table_id}"
  route {
    nat_gateway_id = "${aws_nat_gateway.test_nat_gw.id}"
    cidr_block = "0.0.0.0/0"
  }

  tags {
    Name = "my-private-route-table"
  }
}
```

private_route_table_nat.tf hosted with ❤ by GitHub view raw

Complete Teraform Code

100daysofdevops/100daysofdevops
Contribute to 100daysofdevops/100daysofdevops development by creating an account on GitHub.
github.com\

Looking forward from you guys to join this journey and spend a minimum an hour every day for the next 100 days on DevOps work and post your progress using any of the below medium.

- *Twitter: @100daysofdevops OR @lakhera2015*
- *Facebook: https://www.facebook.com/groups/795382630808645/*
- *Medium: https://medium.com/@devopslearning*
- *Slack: https://devops-myworld.slack.com/messages/CF41EFG49/*
- *GitHub Link:https://github.com/100daysofdevops*

Reference

100 Days of DevOps — Day 0
D-day is just one day away and finally, this is a continuation of the post(I posted a month earlier)
medium.com