Centralized IPv4 and IPv6 Egress using NAT Gateways and NAT66 Instances

These step by step instructions describe how to setup the Centralized IPv4 and IPv6 Egress using NAT Gateways and NAT66 Instances solution illustrated in Centralizing outbound Internet traffic for dual stack IPv4 and IPv6. Before proceeding, make sure to complete the steps described in Baseline Architecture. The following diagrams outline the network architecture and the corresponding route tables we're going to setup:

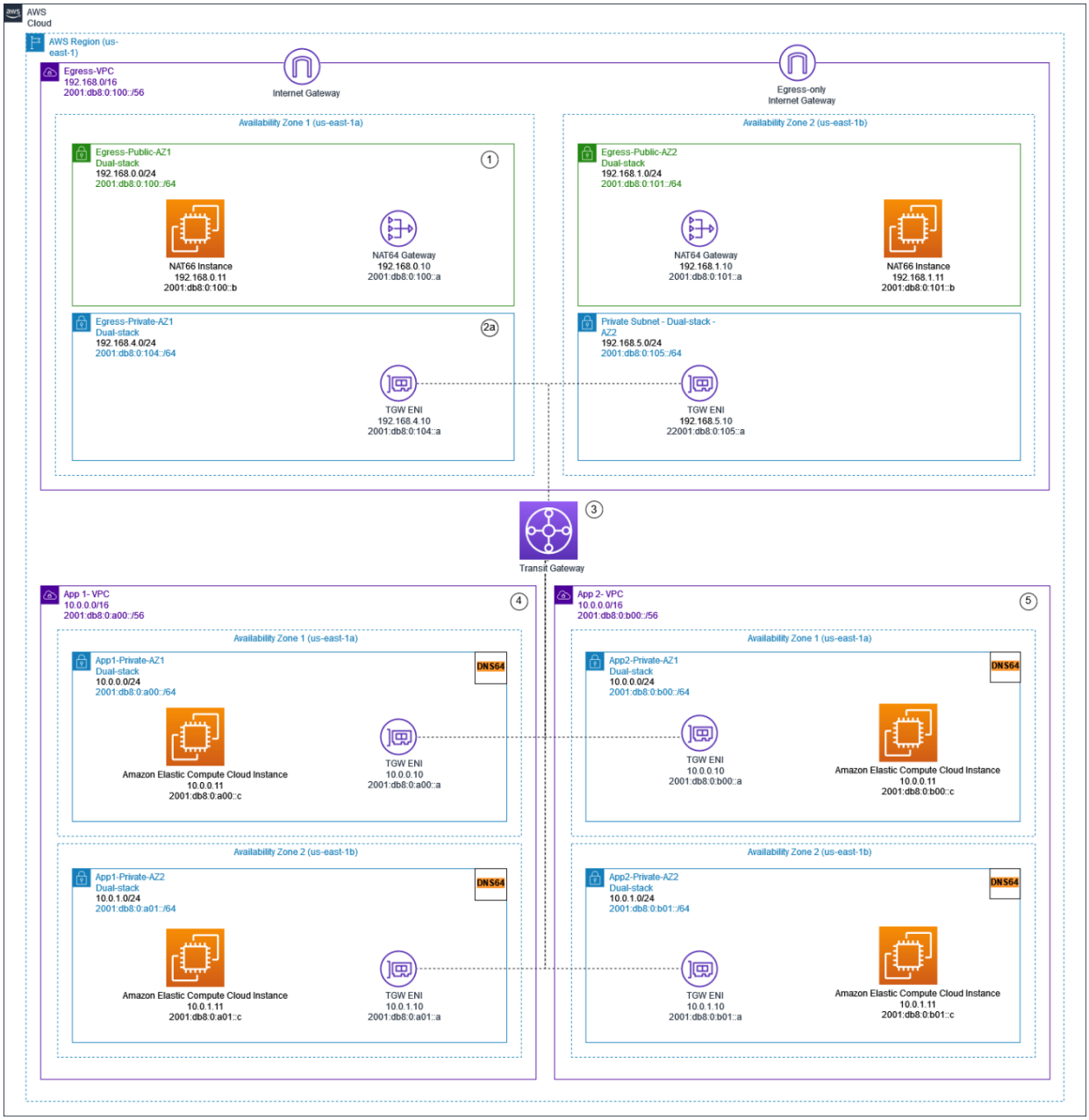

Figure 1: Centralized IPv4 and IPv6 Egress using NAT Gateways and NAT66 Instances

1	Egress VPC Public Subnet - Dual-stack
ROUTE	NEXT HOP
192.168.0.0/16	local
2001:db8:0:100::/56	local
2001:db8:0:a00::/56	Transit GW
2001:db8:0:b00::/56	Transit GW
::/0	Egress Only Internet GW
0.0.0.0/0	Internet GW

2a	Egress VPC Private Subnet - Dual-stack - AZ1
ROUTE	NEXT HOP
192.168.0.0/16	local
2001:db8:0:100::/56	local
::/0	NAT Instance ENI AZ1
64:ff9b::/96	NAT Gateway

2b	Egress VPC Private Subnet - Dual-stack - AZ2
ROUTE	NEXT HOP
192.168.0.0/16	local
2001:db8:0:100::/56	local
::/0	NAT Instance ENI AZ2
64:ff9b::/96	NAT Gateway

3a	Transit Gateway App-RouteTable
ROUTE	NEXT HOP
64:ff9b::/96	Transit GW Attachemnt Egress VPC
::/0	Transit GW Attachemnt Egress VPC

3b	Transit Gateway Egress-RouteTable
ROUTE	NEXT HOP
2001:db8:0:a00::/56	Transit GW Attachemnt App VPC 1
2001:db8:0:b00::/56	Transit GW Attachemnt App VPC 2

4	App 1 VPC
ROUTE	NEXT HOP
10.0.0.0/16	local
2001:db8:0:a00::/56	local
::/0	Transit Gateway
64:ff9b::/96	Transit Gateway

5	App 2 VPC
ROUTE	NEXT HOP
10.0.0.0/16	local
2001:db8:0:b00::/56	local
::/0	Transit Gateway
64:ff9b::/96	Transit Gateway

Figure 2: Route Tables configuration for Centralized NAT64 and NAT66 Egress using NAT Gateways and NAT66 Instances

Egress VPC Setup

1. Create two new route tables in Egress-VPC. For Name tags, use Egress-Private-AZ1-RT and Egress-Private-AZ2-RT.
2. Add a new route in the route table Egress-Private-AZ1-RT, with the destination set to ::/0. Associate the route with the EC2 instance nat-az1. For more information, see Adding and Removing Routes from a route table. Then edit the subnet association and add the Egress-Private-AZ1 subnet to this route table.
3. Add a new route in the route table Egress-Private-AZ2-RT, with the destination set to ::/0. Associate the route with the EC2 instance nat-az2. For more information, see Adding and Removing Routes from a route table. Then edit the subnet association and add the Egress-Private-AZ2 subnet to this route table.

Application VPCs and Transit Gateway Setup

1. Choose Transit Gateway Route tables and select App-RouteTable. Choose Routes, Create route, enter the ::/0 route, and choose the attachment: Egress-Attachment. This covers the 64:ff9b::/96 range for NAT64
2. In the left navigation pane, choose Route Tables and edit the default route tables associated with App1-VPC and App2-VPC, adding a ::/0 route and set TGW-Internet as the target.

NAT66 Instances Setup

1. Create a security group with the following characteristics (where not specified you can leave the default values. For more information, see Create a security group):
    a. Security group name: nat-sg.
    b. Description: Security group for the NAT EC2 instances.

c. VPC: Egress-VPC.
d. Inbound rules:
    i. Click on Add rule.
    ii. Specify as Type Custom TCP, Port Range 443 and Source 2001:db8:0:102::/64 (Egress-Private-AZ1).
    iii. Repeat steps i. to ii. but specify as source 2001:db8:0:103::/64 (Egress-Private-AZ2).
    iv. Repeat i. to iii. for any additional port you would like to allow outbound connections to.

2. Create an EC2 instance with the following characteristics (where not specified you can leave the default values. For more information, see Launch an instance):
    a. Name: nat-az1.
    b. Amazon Machine Image (AMI): select Quick Start then Amazon Linux.
    c. Instance type: t3.small.
    d. Key pair (login): choose the appropriate value for your use case (it is recommended to make use of AWS Systems Manager Session Manager, therefore to select Proceed without a key pair).
    e. VPC: Egress-VPC.
    f. Subnet: Egress-Public-AZ1.
    g. Firewall (security groups): select Select existing security group then nat-sg.
    h. User data:

```
#!/usr/bin/env bash
#
# NAT66 EC2 instance user data script.

# Error messages
trap 'echo "Aborting due to errexit on line $LINENO. Exit code: $?" >&2' ERR

# Strict mode
set -Eeuo pipefail

# Set $IFS to only newline and tab
IFS=$'\n\t'

# Set kernel parameters
sysctl -w net.ipv6.conf.all.forwarding=1
sysctl -w net.ipv6.conf.eth0.accept_ra=2

# Persist kernel parameters
cat <<EOF > /etc/sysctl.d/10-nat66.conf
net.ipv6.conf.all.forwarding = 1
net.ipv6.conf.eth0.accept_ra = 2
EOF

# Set ip6tables rules
ip6tables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
ip6tables -A FORWARD -i eth0 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
ip6tables -A FORWARD -i eth0 -o eth0 -j ACCEPT

# Persist ip6tables rules
ip6tables-save > /etc/sysconfig/ip6tables

# Install iptables-services
```

```
yum install -y iptables-services

# Enable ip6tables
systemctl enable ip6tables

# Start ip6tables
systemctl start ip6tables
```

3. Go to the EC2 console, select Instances from the menu on the left then nat-az1.
4. Click on Actions, Networking then Change source/destination check**.**
5. Select Stop then click on Save.
6. Repeat steps 2. to 6. to create an additional instance with Name equal to nat-az2 and Subnet equal to Egress-Public-AZ2.