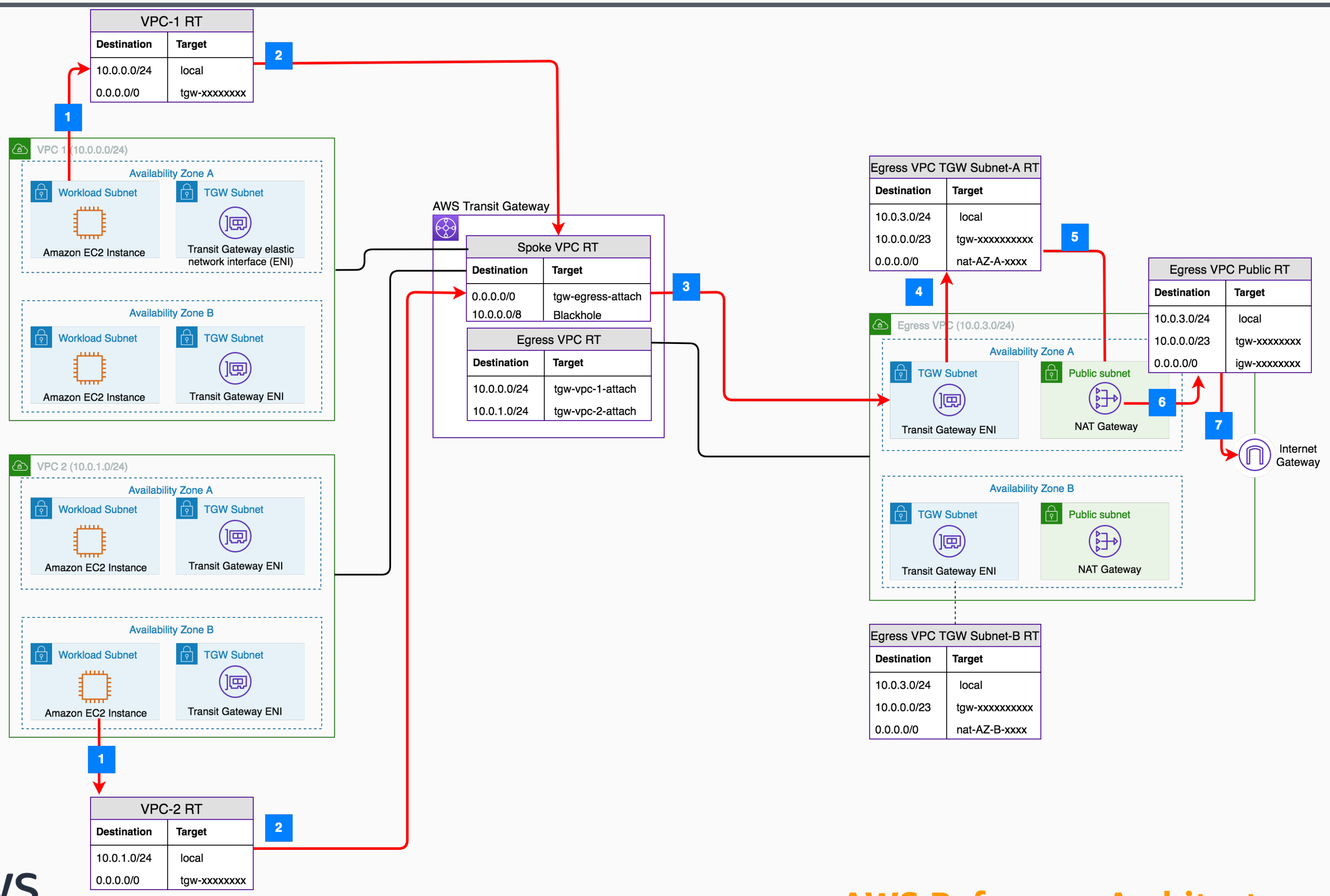
Architecture for Centralized Internet Egress with NAT Gateway – Inter-VPC Communication Disabled

Use NAT Gateway and AWS Transit Gateway to create high availability centralized internet egress for all Amazon Virtual Private Clouds (VPCs) while isolating inter-VPC traffic.



VPC-1 RT

Destination	Target
10.0.0.0/24	local
0.0.0.0/0	tgw-xxxxxxxx

VPC-2 RT

Destination	Target
10.0.1.0/24	local
0.0.0.0/0	tgw-xxxxxxxx

Spoke VPC RT

Destination	Target
0.0.0.0/0	tgw-egress-attach
10.0.0.0/8	Blackhole

Egress VPC RT

Destination	Target
10.0.0.0/24	tgw-vpc-1-attach
10.0.1.0/24	tgw-vpc-2-attach

Egress VPC TGW Subnet-A RT

Destination	Target
10.0.3.0/24	local
10.0.0.0/23	tgw-xxxxxxxxxx
0.0.0.0/0	nat-AZ-A-xxxx

Egress VPC Public RT

Destination	Target
10.0.3.0/24	local
10.0.0.0/23	tgw-xxxxxxxx
0.0.0.0/0	igw-xxxxxxxx

Egress VPC TGW Subnet-B RT

Destination	Target
10.0.3.0/24	local
10.0.0.0/23	tgw-xxxxxxxxxxx
0.0.0.0/0	nat-AZ-B-xxxx

1 Traffic from the **Amazon Elastic Compute Cloud (Amazon EC2)** instance in the workload subnet attempts to reach the internet. The subnet's route table routes to **AWS Transit Gateway** via the default route (0.0.0.0/0).

2 Traffic enters **Transit Gateway** on the VPC-**Transit Gateway** attachment. It is routed to the egress VPC via the default route in the **Transit Gateway** route table.

3 Traffic enters the egress VPC on the **Transit Gateway** attachment subnet.

4 This subnet's route table routes the traffic to the Network Address Translation (NAT) gateway in that Availability Zone (AZ) via the default route.

5 Traffic enters the NAT gateway, and the source IP is now changed to NAT gateway IP.

6 When exiting the NAT gateway, the traffic looks up the public subnet route table and gets routed to the internet gateway.

7 The traffic leaves for the internet.

See also: Creating a single internet exit point from multiple VPCs Using AWS Transit Gateway

AWS Reference Architecture