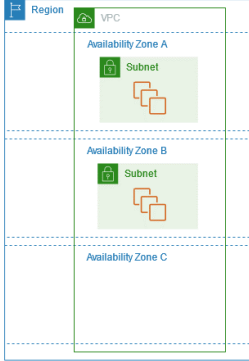
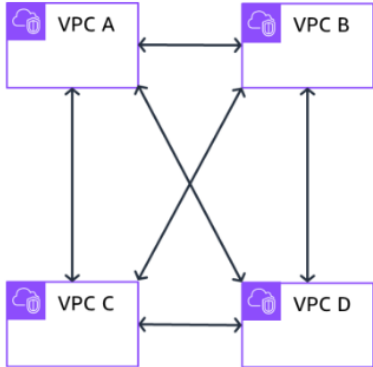
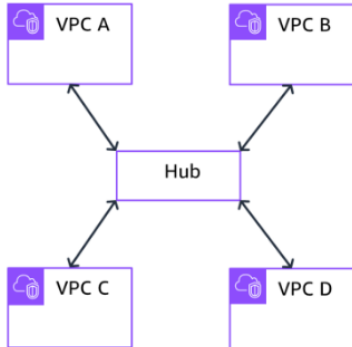


NETWORKING

A. Vocabulary

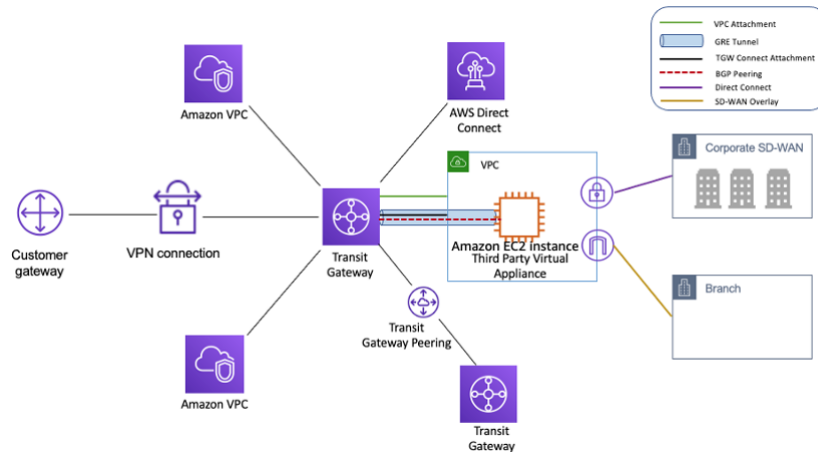
Regions	Isolated from other regions. Greatest possible fault tolerance and stability (us-east-1).
Availability Zone (AZ)	Isolated locations within a region (us-east-1a). VPC can cross multiple AZ. 

B. Network design

	Full mesh architecture Work for small number of VPC Does not expand well Number of connections $N(N-1)/2$
	Hub and Spoke architecture Central hub manages connectivity Works for large number of VPC Number of connections N More latency due to Hub

C. Transit Gateway

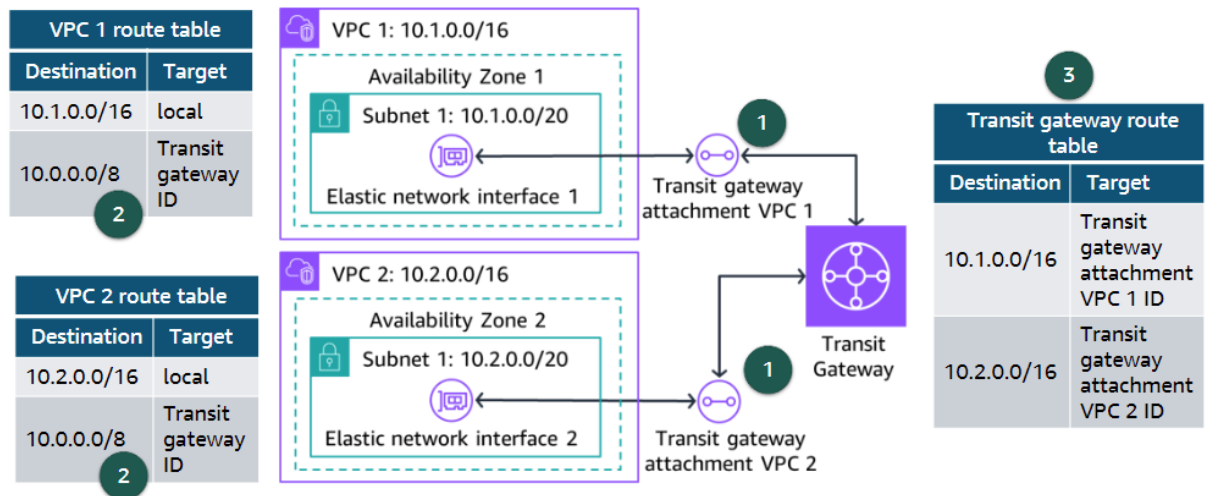
Transit Gateway provides Hub and Spoke design for connecting VPC and on-premises networks.






Hub and spoke design with AWS Transit Gateway

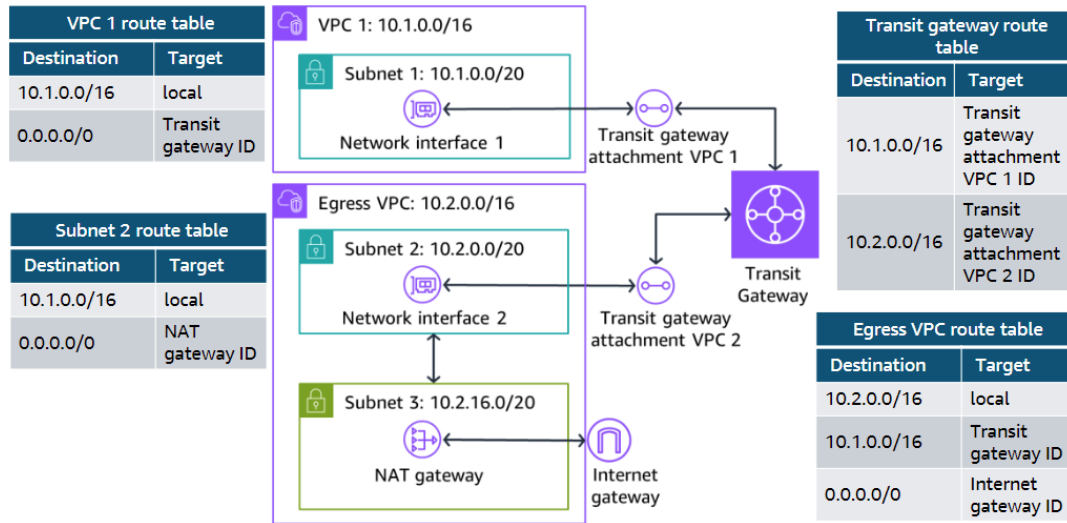
Manages service	Yes (high availability and scalability).
Charges	Per hour for the number of connections and the amount of traffic.
Routing	<u>Dynamic</u> Requires routers to discover routing paths <u>Static</u> Routes configured before traffic can be routed
IP addresses	IPv4 and IPv6
Logs	Transit Gateway Flow Logs to CloudWatch, Amazon S3, Kinesis Data Firehose

Example – No Internet Access



1. Connect the VPC to the **Transit Gateway**  using a **Transit Gateway Attachment**  through an **Elastic Network Interface**  (like a network card).
2. Add a route for the Transit Gateway. In this case, 10.0.0.0/8 includes 10.X.0.0/16 (10.0.0.0/8 -> 10.0.0.0/10.255.255.255 / 10.X.0.0/16 -> 10.X.0.0/10.X.255.255). [Use this tool](#)
3. Configure the Transit Gateway route table to route the traffic to the correct VPN.

Example – With Internet Access



Internet access is obtained using the **NAT Gateway** in the PUBLIC subnet 3. The **NAT Gateway** is **NOT** in a separate VPC.

VPC 1 and VPC 2 route table sends all traffic 0.0.0.0/0 (except local one) to:

- Transit Gateway for VPC 1
- NAT Gateway for VPC 2

The **Transit Gateway** is responsible to route the traffic between VPC 1 and VPC 2.

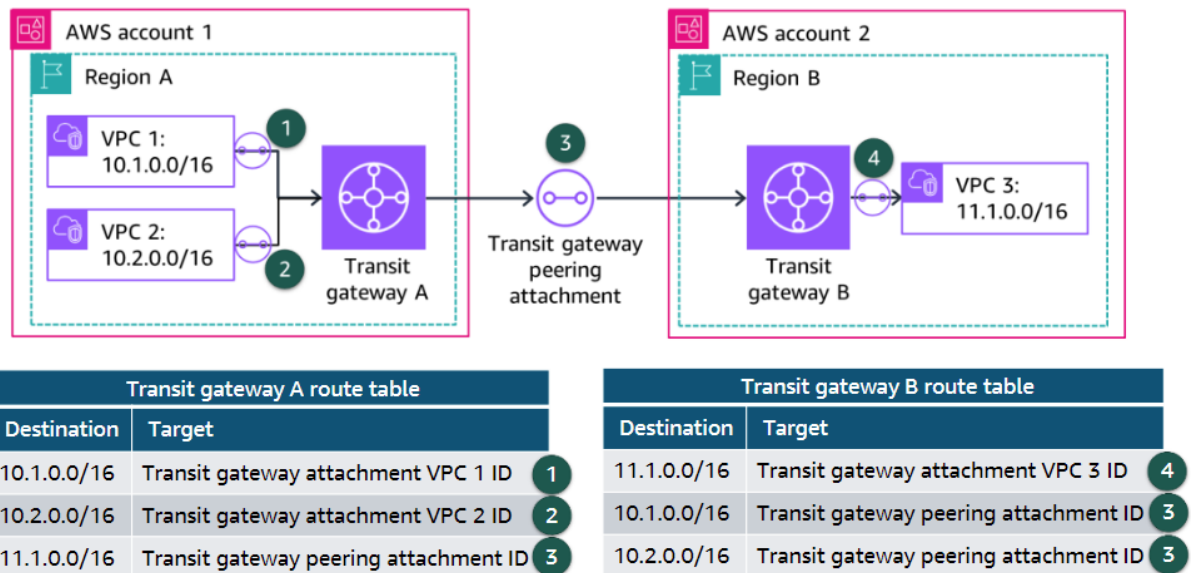
The **NAT Gateway** routes VPC 1 traffic back to the **Transit Gateway**, and all other traffic 0.0.0.0/0 to the **Internet Gateway**.

This design is cheaper and simpler to use.

For redundancy, you can run a NAT Gateway for each Availability zone.

D. Peering

If you need network traffic to flow between AWS Regions or different AWS accounts, you can create a transit gateway peering connection between transit gateways. Traffic **DOES NOT** traverse the public internet (more secure)



VPC 1 and VPC 2 belongs to a different region and account than VPC 3.

Transit Gateway A routing (same idea for B):

- 10.X.0.0/16 to the corresponding VPC
- 11.1.0.0/16 to the **Transit Gateway B**.

E.