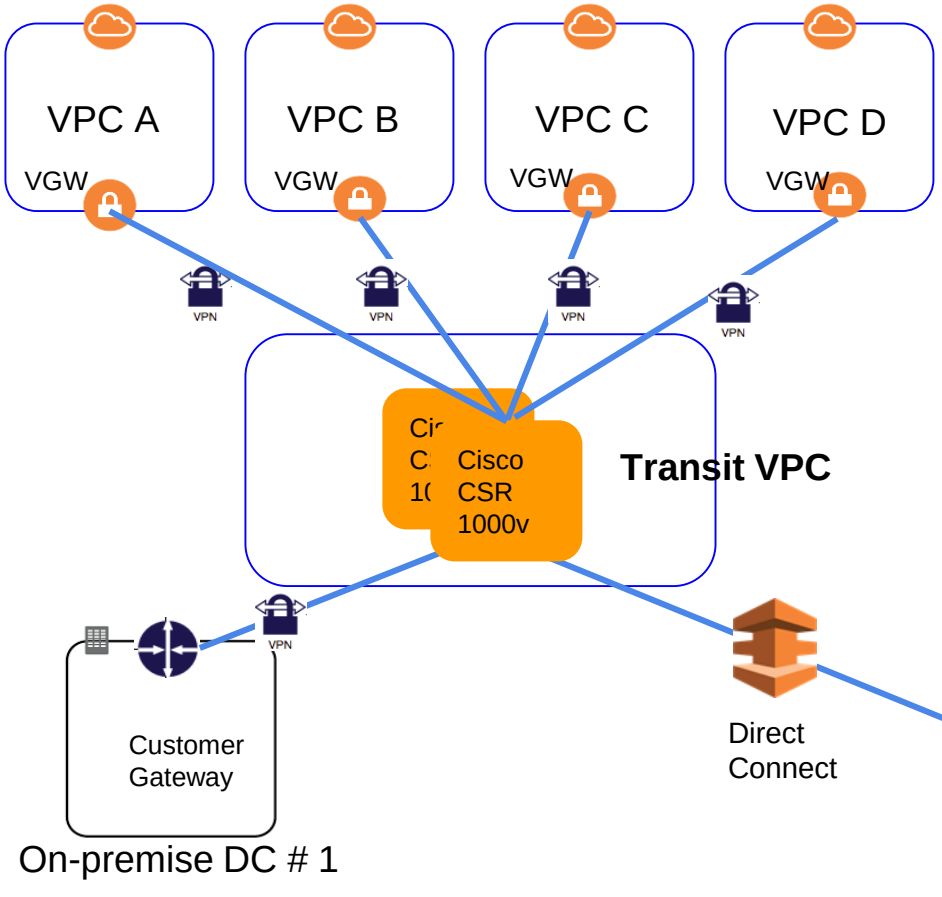
Transit Gateway

Solution 1 : Transit VPC (Introduced in 2016)



HUB AND SPOKE TOPOLOGY

- Simplifies Network
- Need fewer connections
- Reduces overall cost of physical network devices
- Reduces time and efforts
- Allows deploying IPS/IDS

The problem with VPC peering & Transit VPC

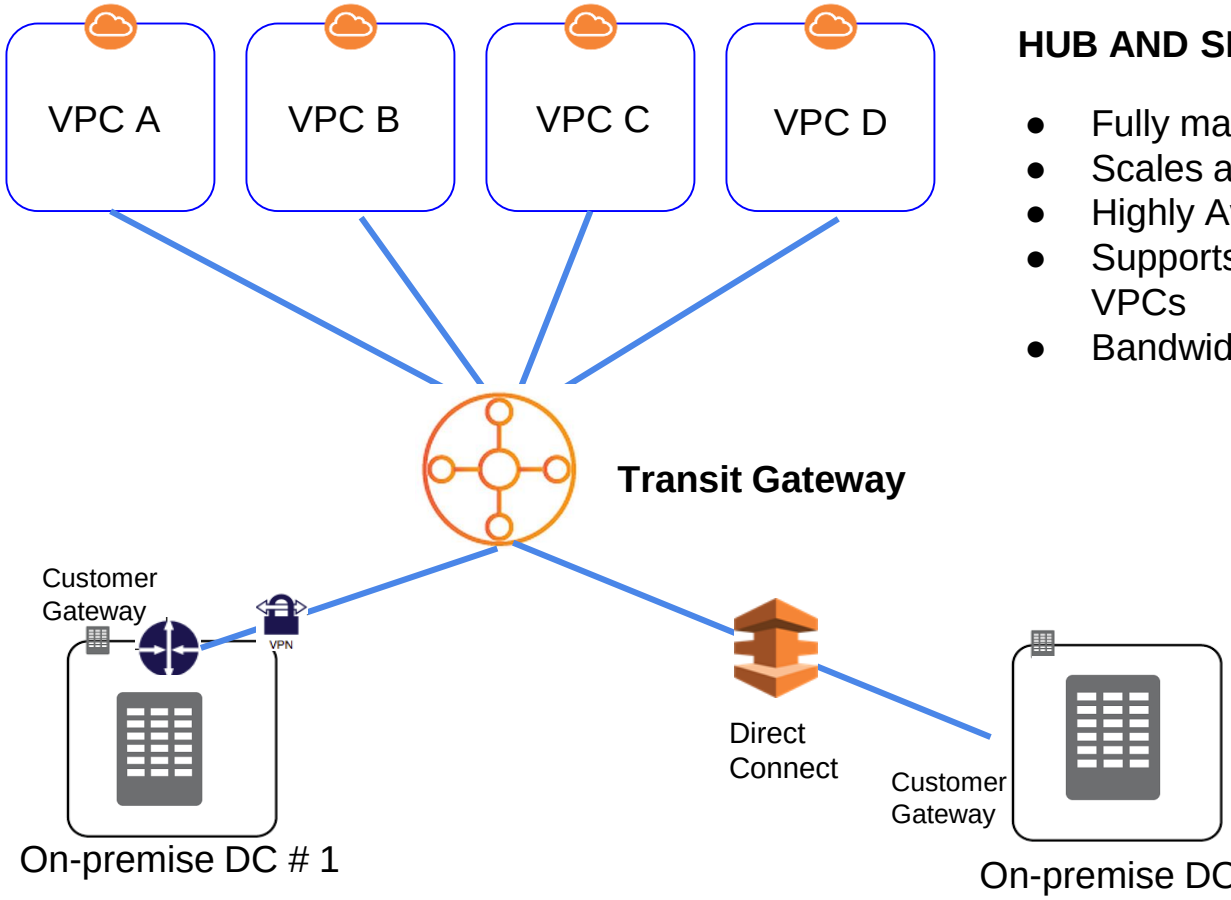
VPC Peering:

- Point-to-point connection between VPCs
- Non transitive traffic flow
- Separate connection for each VPC for on-premise VPN or Direct Connect

Transit VPC:

- Instance based (Cisco CSR 1000V)
- Additional EC2 cost
- Software Licensing cost
- Availability issues
- Bandwidth limitations of EC2

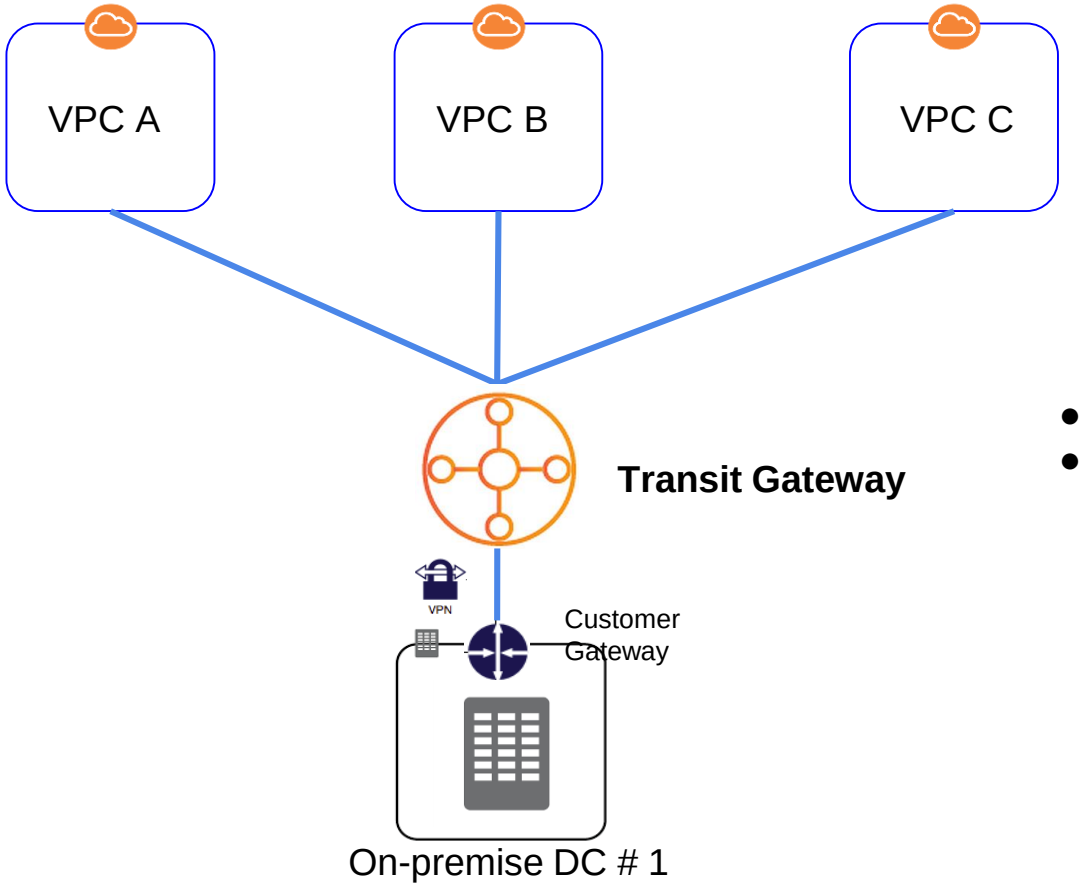
Solution 2: Transit Gateway (2018 Re:Invent)



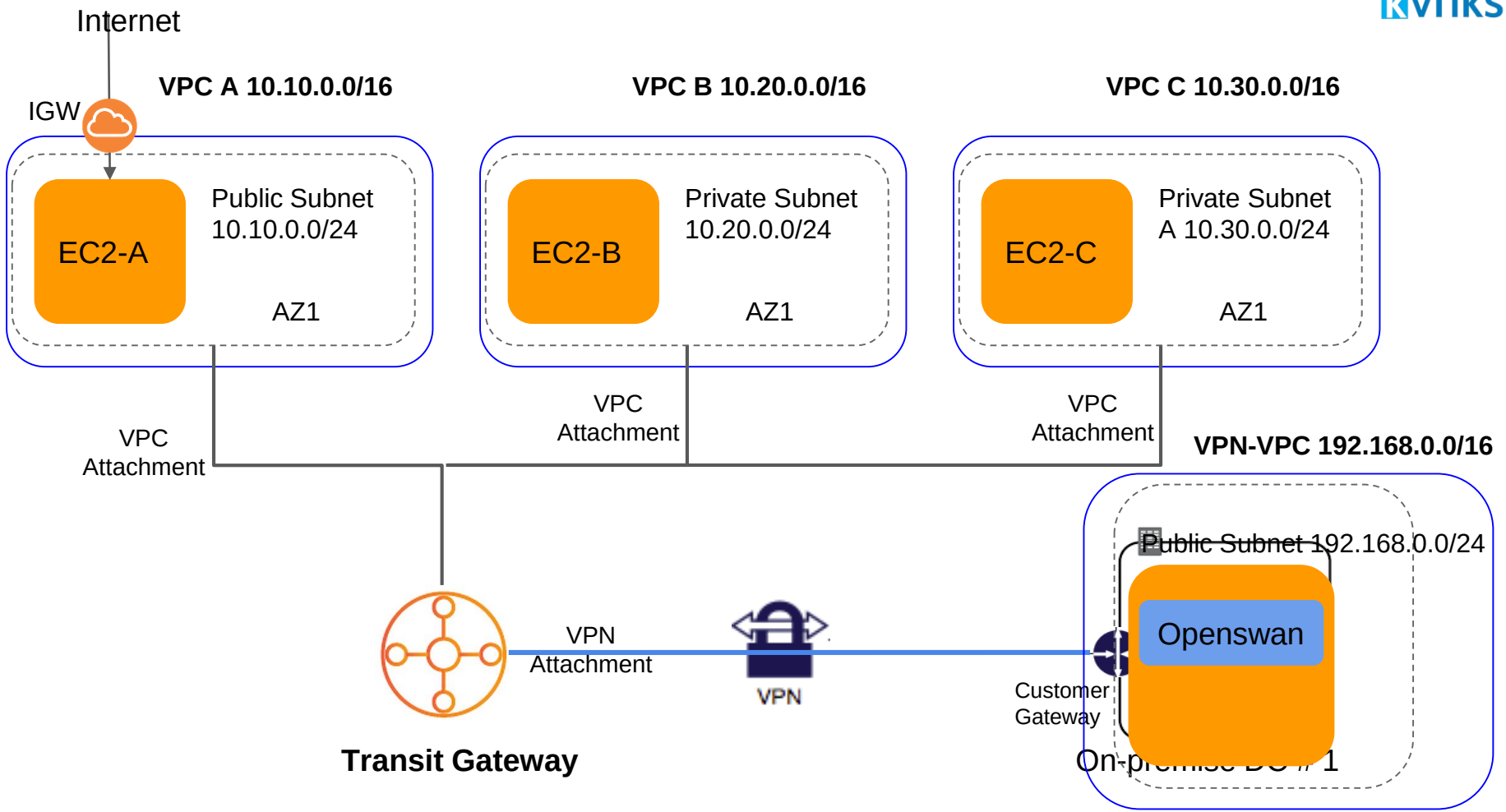
HUB AND SPOKE TOPOLOGY

- Fully managed gateway
- Scales automatically
- Highly Available
- Supports attaching upto 5000 VPCs
- Bandwidth upto 50 gbps

Exercise: Setup Transit Gateway



- 3 VPCs in same AWS Region
- VPN connection



Steps - Part 1 - Inter VPC communication

1. Create VPC-A (10.10.0.0/16) with single Public Subnet in Region A (Mumbai)
2. Create VPC-B (10.20.0.0/16) with single Private Subnet in Region A
3. Create VPC-C (10.30.0.0/16) with single Private Subnet in Region A
4. Create VPC-VPN (192.168.0.0/16) with single Public Subnet in Region B (N.Virginia)
5. Launch EC2 instance in each of the subnets created above. Total 4 EC2 instance. Make sure you open Security group rule for ICMP inbound for source 10.0.0.0/8 (for all other VPCs)
6. Login to EC2-A (ssh using Public IP) and try to ping EC2-B, EC2-C or EC2-VPN Private IPs. This does not work.
7. Create a Transit Gateway in Region A
8. Create 3 Attachments for VPC-A, VPC-B and VPC-C
9. Modify the VPC-A Subnet, VPC-B Subnet and VPC-C Subnet to route traffic to destination 10.0.0.0/8 through transit gateway
10. Verify that, now traffic starts flowing from EC2-A to EC2-B and EC2-C over Private IP address
11. Congratulations !!
12. Extend the VPC-A CIDR by attaching one more CIDR e.g 10.40.0.0/16
13. Verify in Transit Gateway Route table that this new route is automatically propagated

Steps - Part 2 - VPN communication

1. For same Transit Gateway, create a VPN attachment
2. Provide the IP address of EC2-VPN for Customer Gateway.
3. Choose Static Route
4. After creation of Site-to-Site VPN connection, Download the VPN configurations for Openswan.
5. Login to EC2-VPN over SSH using Public IP
6. Setup the VPN using OpenSWAN (Refer Site-To-Site VPN document)
7. After successfully configuring ipsec, start the ipsec service
8. Verify that in Region A, Site-to-Site VPN shows that 1 Tunnel is UP
9. Try to ping to EC2-VPN from EC2-A. This does not work as there is no route in VPC-A Subnet Route table
10. Add a route for destination 192.168.0.0/16 in the Route table of VPC-A Public subnet RT
11. Now the traffic starts flowing to EC2-VPN from EC2-A. Congratulations !!
12. Ping EC2-A from EC2-VPN. This does not work as you might not have open SG of EC2-A
13. Open the SG for inbound ICMP for source 192.168.0.0/16.
14. Now traffic also flows from EC2-VPN to EC2-A i.e from On-premise to AWS VPC
15. Be happy..you just did it :). Don't forget to terminate everything that you created for this exercise.