Class 11

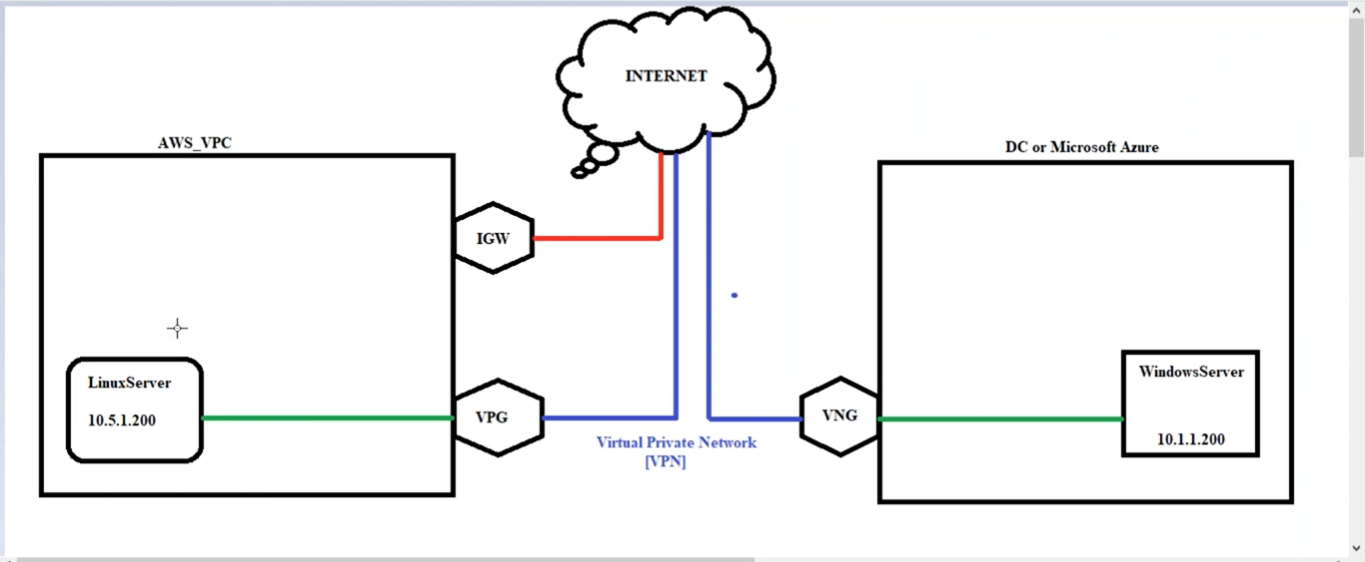
VPN: virtual private network [This is also called Site-to-site VPN]

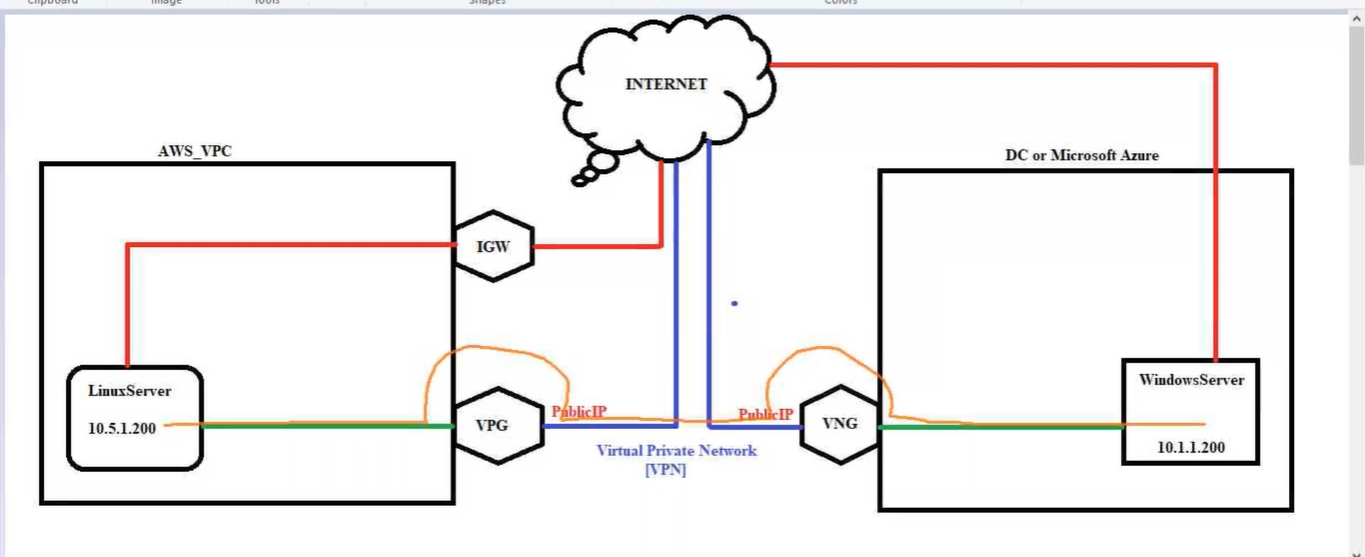
VPN connection is only to just **connect two DC centers** and access data,

To move the servers, we have **migration concept**

VPG: virtual private gateway

* virtual private gateway is used to connect server in AWS to server in other Data Center
* To use VPG no need to use Public IPs,
* in real-time we don’t use Public IPs, because we don’t expose our server to internet
* we connect our laptop to AWS server using VPN
* connection b/n VPG and other data center is called VPN





* Connection between two servers in two Data Centers is through VPG & VNG using Public IP,
* Servers use Private IP’s, but VPG & VNG are connected using their Public IP
* **VPN** connect is established between VPG & VNG using their Public IP

Lab:

**Azure**

1, create server with ip 10.1.1.200 and VNG (virtual network gateway same as VPG in AWS cloud), routing table that divert to AWS server

* login to server in azure

**AWS**

2, VPC and subnets and routing table already setup

Ec2 -> Instance -> subnet1 -> 10.0.1.200 ->

#!/bin/bash

yum update -y

yum install nginx -y

service ngnix start

* login to server in aws -> putty -> ec2-user@DNS -> sudo su –
* [root@ip-10-0-1-200 ~]# hostname Dheeraj-Server (this command is used to display name “Dheeraj-Server”)
* [root@Dheeraj-Server ~]# (like this in place of server Public IP)

3, [create VPG and attach it to VPC]

VPC -> VIRTUAL PRIVATE NETWORK (VPN) -> Virtual Private Gateways -> Name tag: AWSB26-VPG & Amazon default ASN -> RC -> Attach to VPC (our vpc)

4, Route Tables: [edit AWS subnet route of our aws server to Azure VPC (10.1.0.0/16) towards VPG]

VPC Dashboard -> Route Tables -> Routes -> Edit routes -> 10.1.0.0/16 (Azure VPC IP) & vgw-0a6568f6df681f3ec

* Now make the connection between VPG & VNG

VPC -> VIRTUAL PRIVATE NETWORK (VPN) -> Customer Gateways -> Name: AZURE-VNG & IP Address: (copy past Azure VNG Public IP) --- to connect VPG to VNG

* Now we must copy AWS VPG Public in Azure, for getting VPG IP go to (to get VPG Public IP)

VPC -> VIRTUAL PRIVATE NETWORK (VPN) -> Site-to-Site VPN Connections -> Create VPN Connection-> Static IP prefix: (Azure VPC)

* Now download file and upload in Azure

VPC -> VIRTUAL PRIVATE NETWORK (VPN) -> Site-to-Site VPN Connections -> Download Configuration

* Now go to both server and ping each other ip’s
* Under -> Site-to-Site VPN Connections (we can see connection of Azure in Tunnel 1 & Tunnel 2)

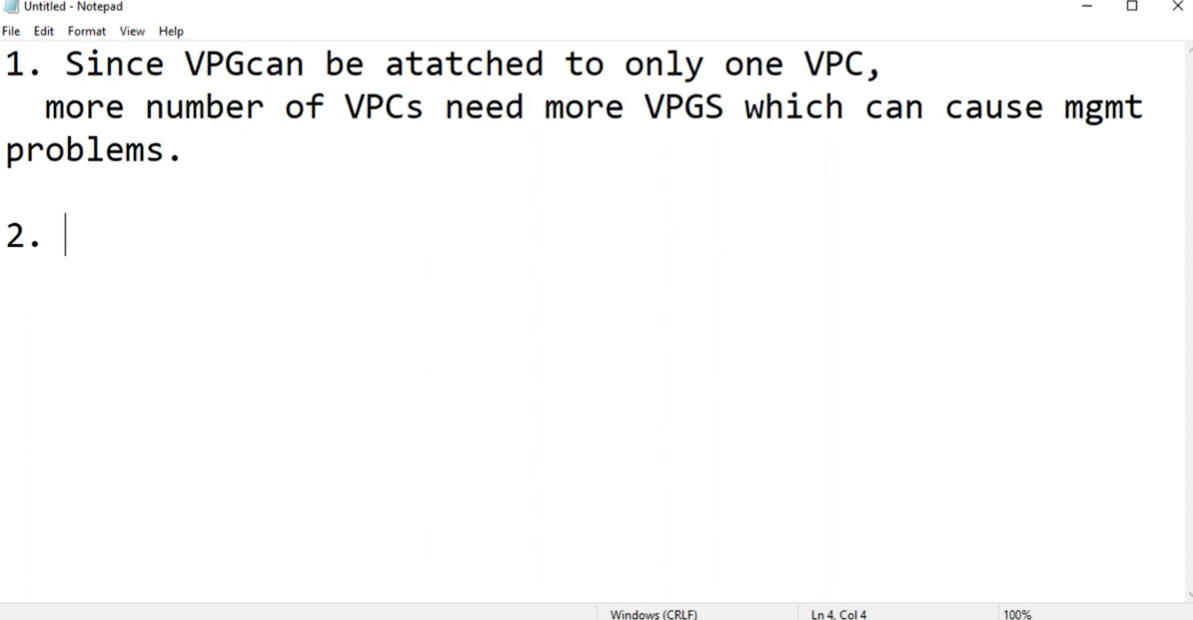
Workflow: **[VPG** (attach to VPC)**, Route table** (to azure server on VPG)**, Customer Gateways** (to create VPG public IP)**, Site-to-Site VPN Connections -> Create VPN Connection & Download Configuration]**

Here we have the problem: -

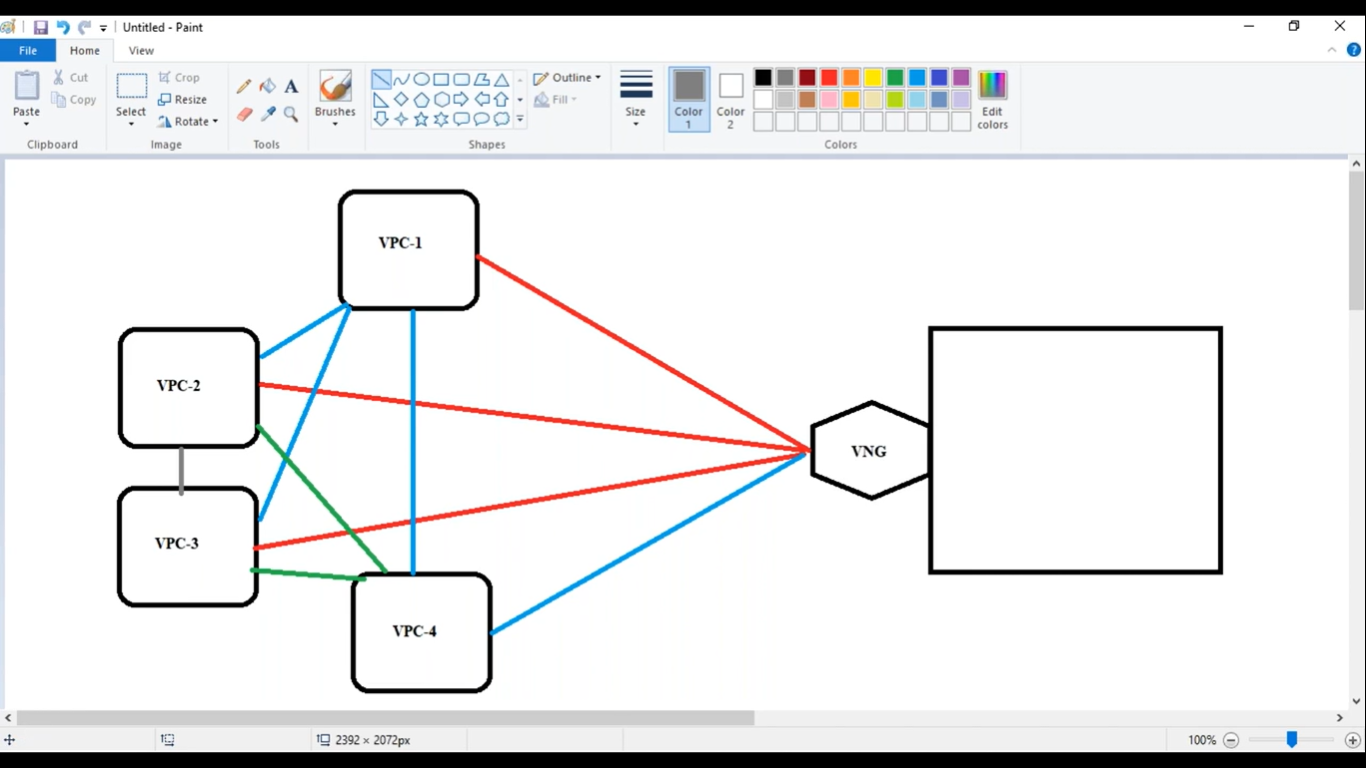
Problem is if we have more than VPC’s, we must create VPG’s for every VPC, that leads to maintenance problem.

We can solve this by “Transit Gateway” – in place of VPG we create only one Transit Gateway for all VPC’s

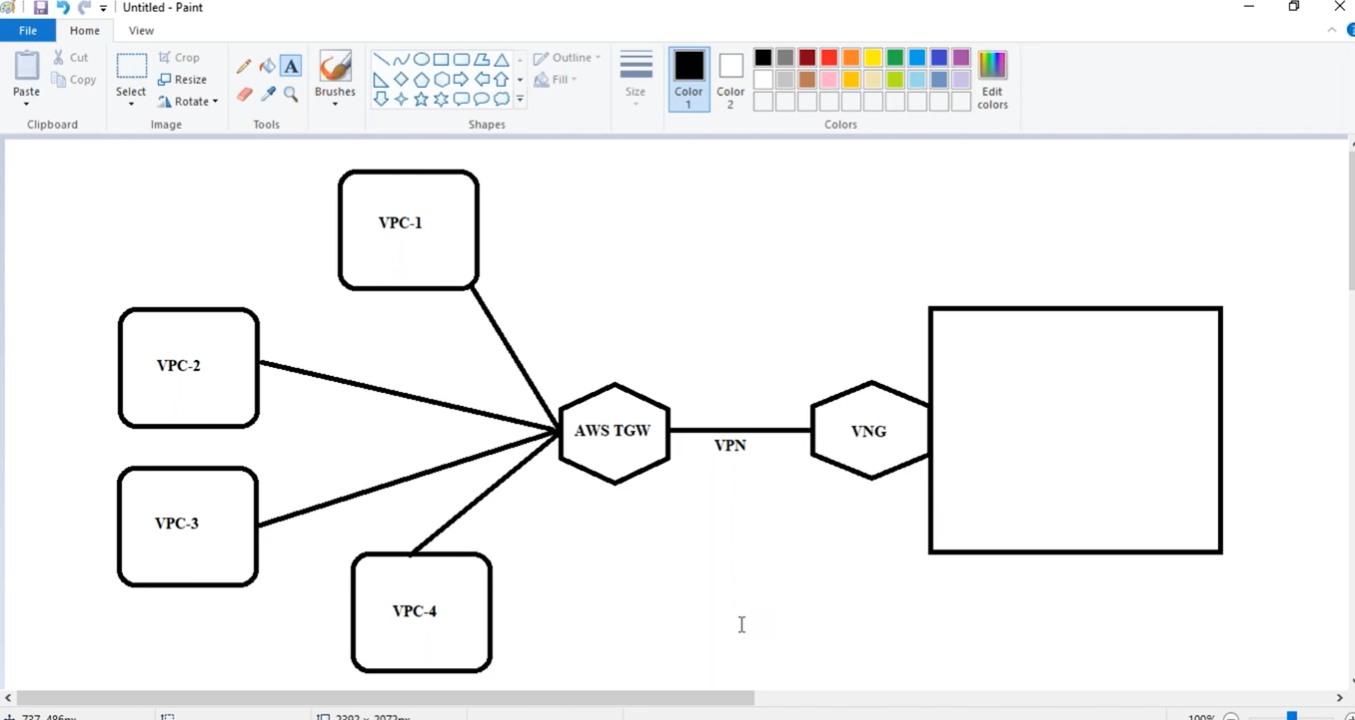
**Problem: -**

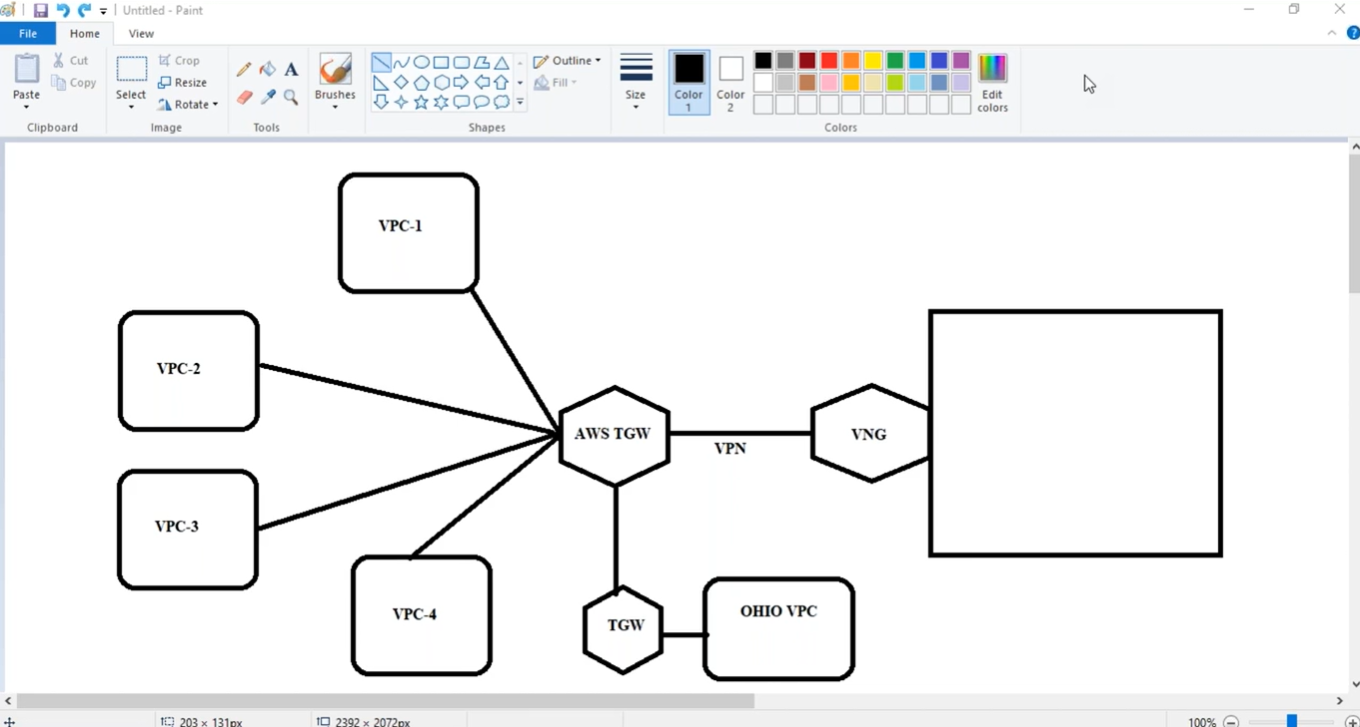


**Vpc peering and site to site connection problem**



**Solution using Transit Gateway**





**We have one more VPN: - called “Point-to-site VPN or Client VPN Endpoints”**

Point to site VPN, is used to connect our laptop directly to Office or AWS cloud without internet