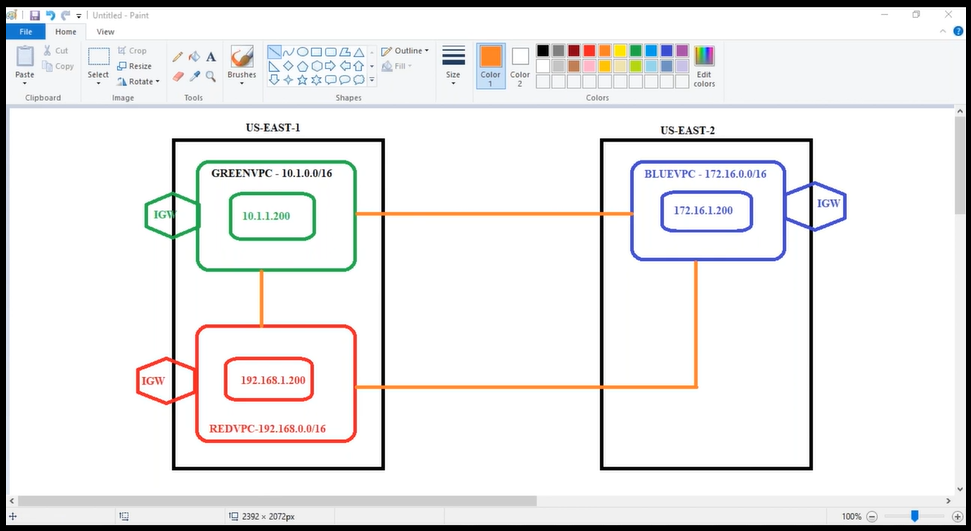
6. vpc peering (enabling connection between two vpc’s)

US-EAST-1(Virginia) & US-EAST-2(Ohio) - Regions



Vpc – subnet – igw – routing table – security groups and then server (ec2 instance) [for green,red,blue servers]

Create vpc “peering connection” (same region)

|

Green-to-Red (Accept)

|

Edit routing table (green and give red vpc ip range & same with red)

|

Putty ping

Import key pairs:

Goto first region where we have a key pair

|

Putty

|

Command “ec2-metadata” copy it

|

Go to key pairs-> import->past

Create vpc “peering connection” (other region)

|

Green-to-blue (Accept on both sides)

Blue-to-Red (Accept on both sides)

|

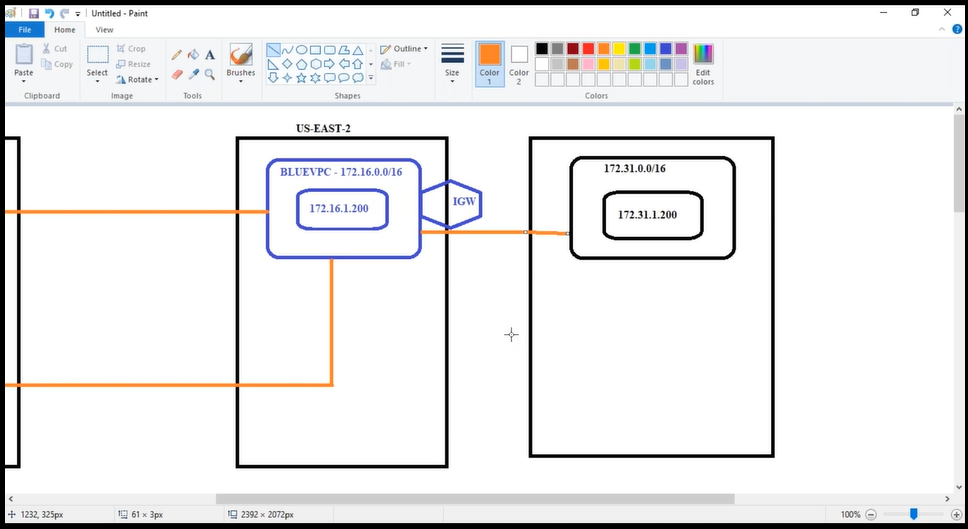
Edit routing table (in green vpc RT, give blue vpc ip range & same with blue)

Edit routing table (in red vpc RT, give blue vpc ip range & same with red)

|

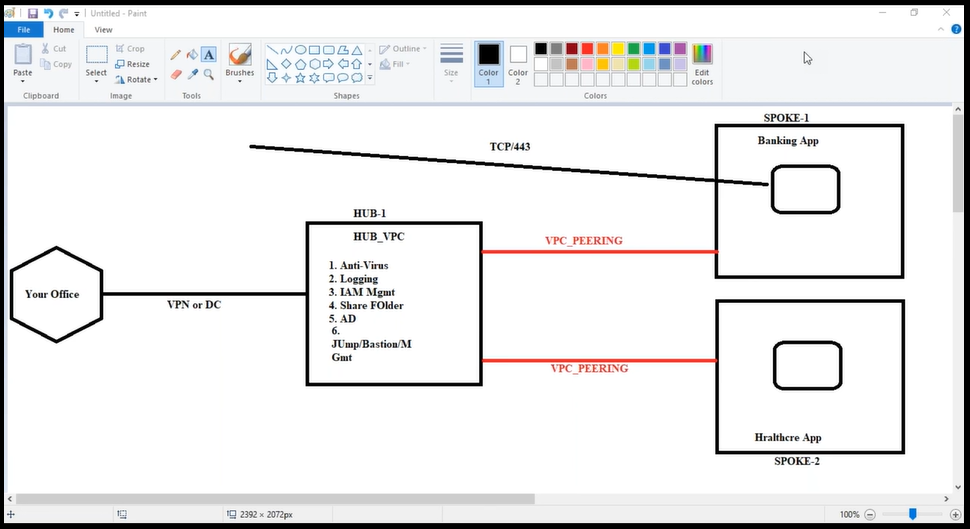
Putty ping

Same with different accounts and different regions



[Delete all servers for not to bill]

* So finally, where do we use Vpc peering?



🡺Tcp/433 is Custer ip to see banking app, done by internet gateway

----------------------------------------------------------------------------------

Hub – we can manage centrally

We first login into Hub Vpc server and go to spoke Vpc servers [that is the reason we create vpc peering in real time]

------

**Interview question**: Explain about your infrastructure?

We are having Multi account architecture {eg, aws accounts: [dheerajpalvai@gmail.com](mailto:dheerajpalvai@gmail.com), dheeraj.nc24@gmail.com} ,

We are using “Hub & Spoke”.

We have a Hub vpc also called as shared vpc, and all the shared servives are like

1, Anti-virus

2, logging(logs)

3, IAM management(Identity and access management)

4, shared folder

5, AD (Active Directory)

6, Jump/Bastion/Management

Every thing is there in hub vpc or shared vpc , from there we manage every other VPC

Google “pci dss aws”

