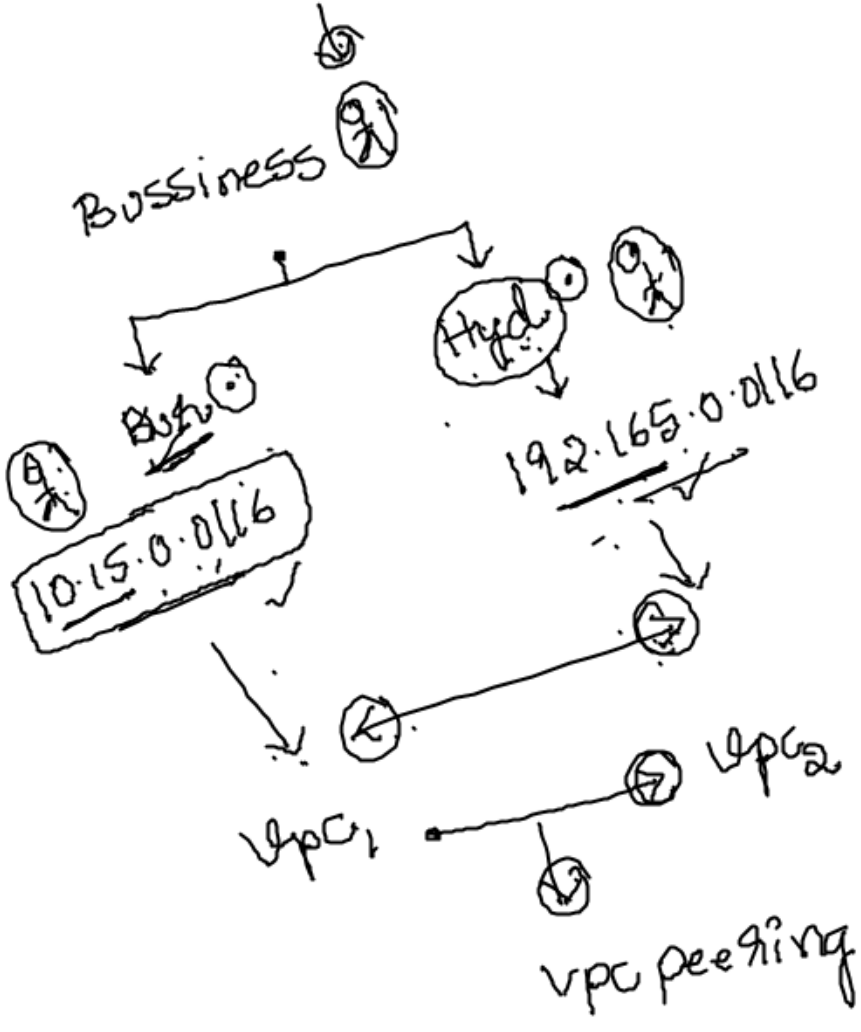
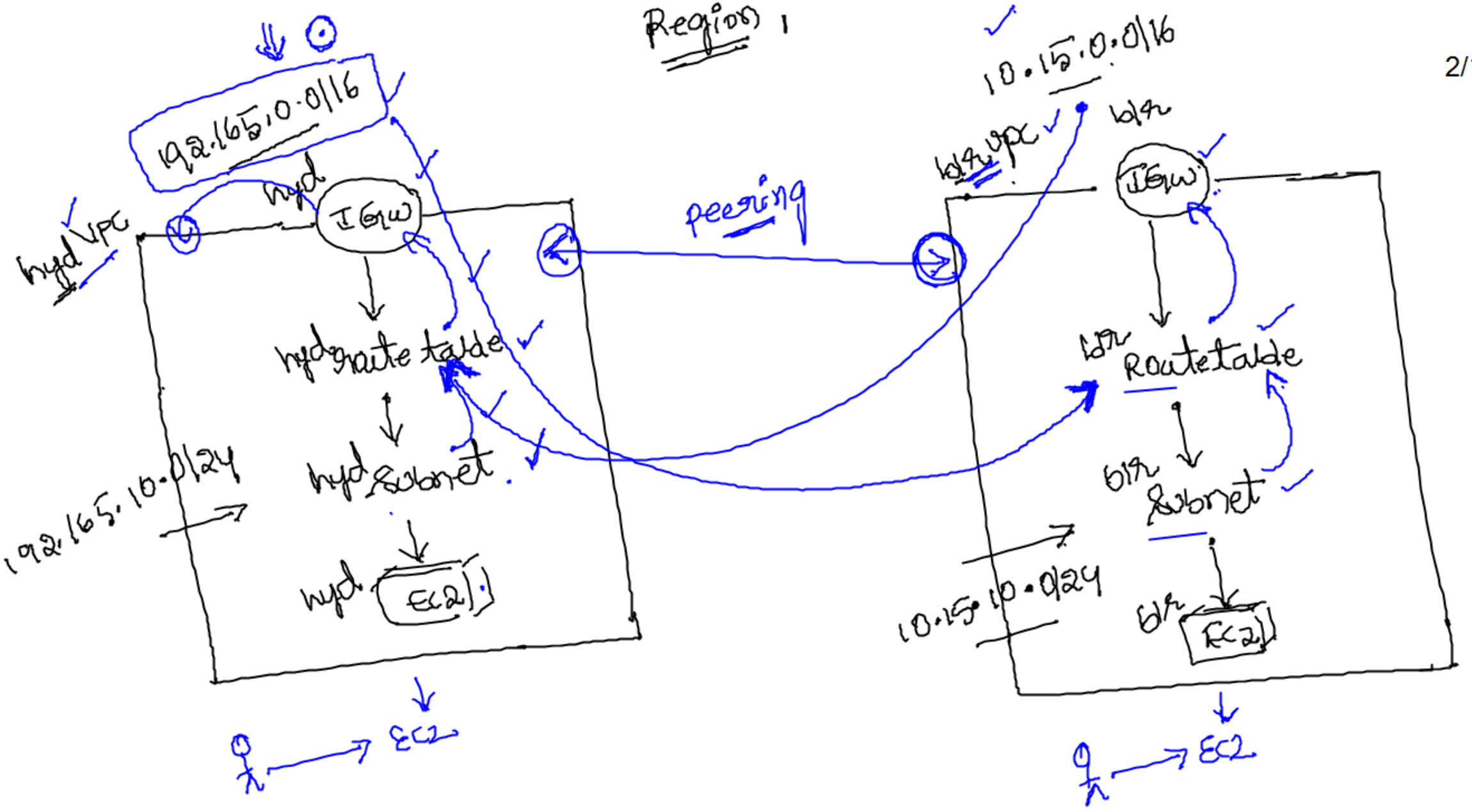
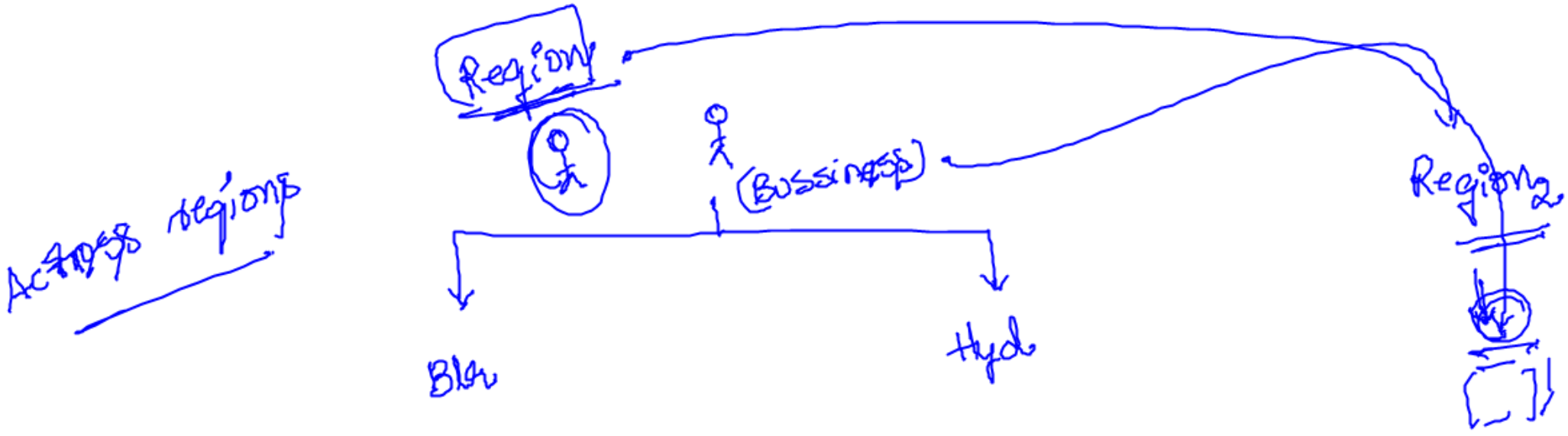
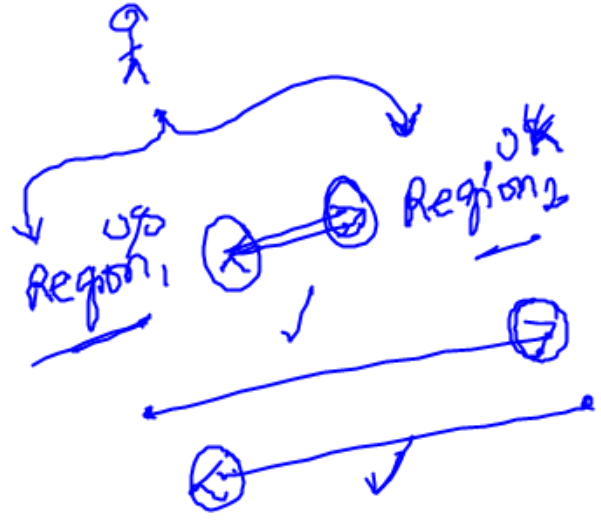
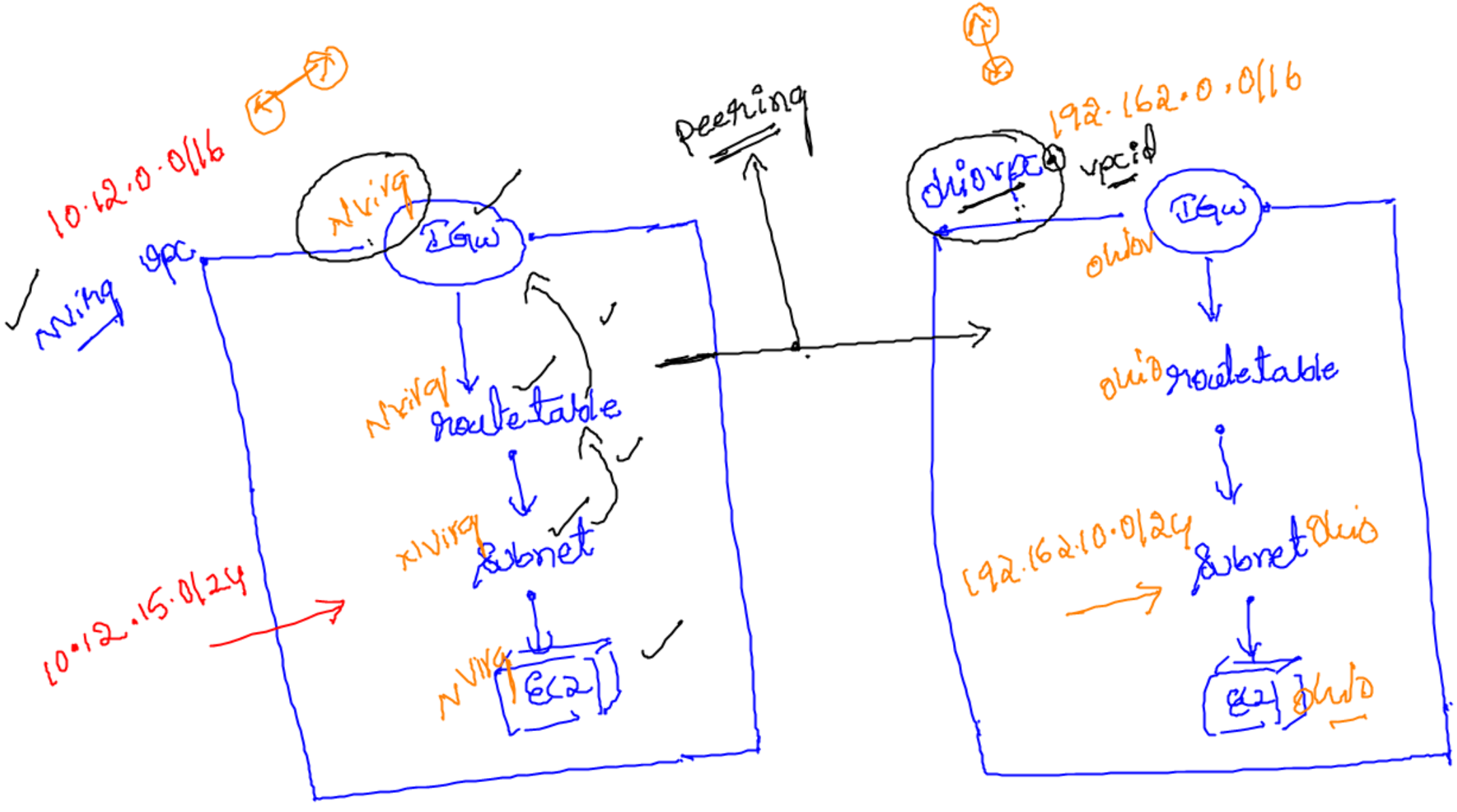
Vpc

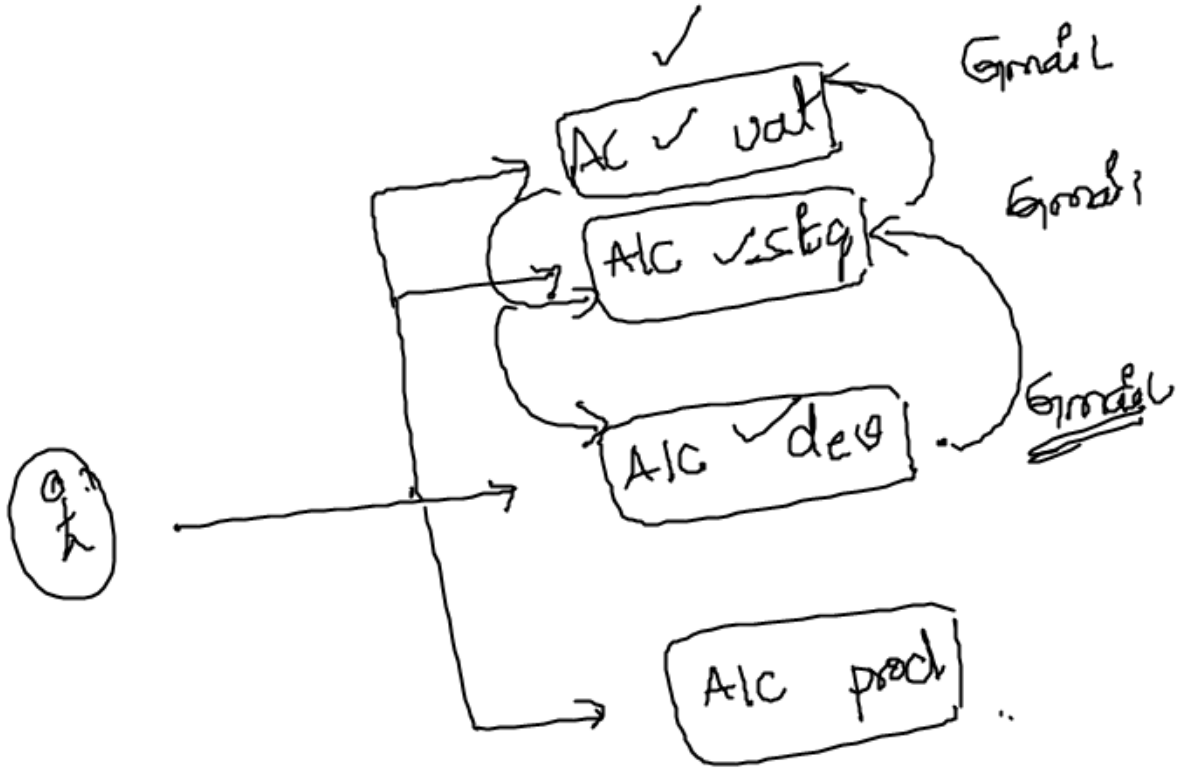

Bussiness
Hyd
Bglr
10.15.0.0/16
192.165.0.0/16
vpc1
vpc2
vpc peering


Region 1
192.165.0.0/16
hyd
hyd VPC
IGW
peering
10.15.0.0/16
blr
blr VPC
IGW
hydroutetable
hyd subnet
192.165.10.0/24
hyd
EC2
EC2
Routetable
blr
subnet
10.15.10.0/24
blr
EC2
EC2


Region1
Across regions
(Bussiness)
Region2
Blr
Hyd


UK
US
Region1
Region2

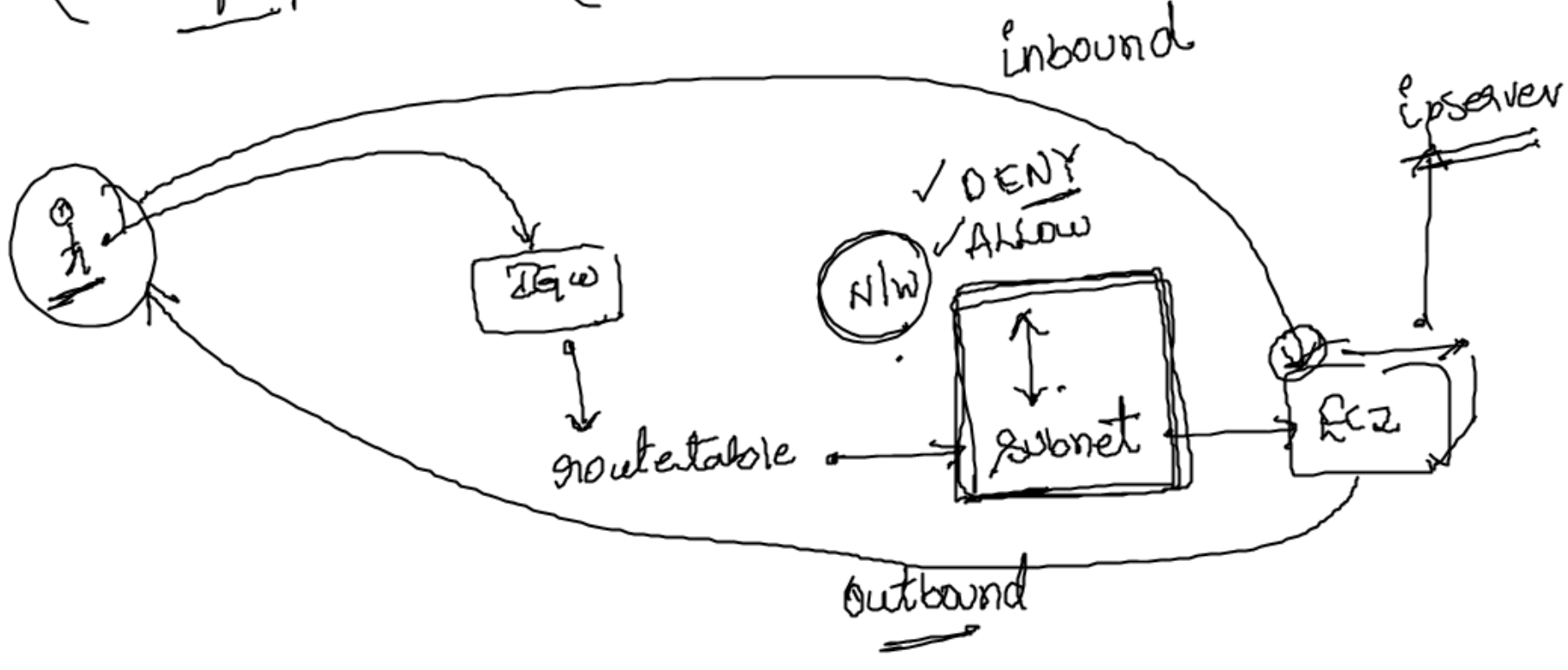

10.12.0.0/16
nvirg
vpc
nvirg
IGw
nvirg
routetable
nvirg
subnet
10.12.15.0/24
nvirg
EC2
peering
192.162.0.0/16
ohiovpc
vpcid
IGw
ohiov
ohio
routetable
192.162.10.0/24
subnet
ohio
EC2
ohio

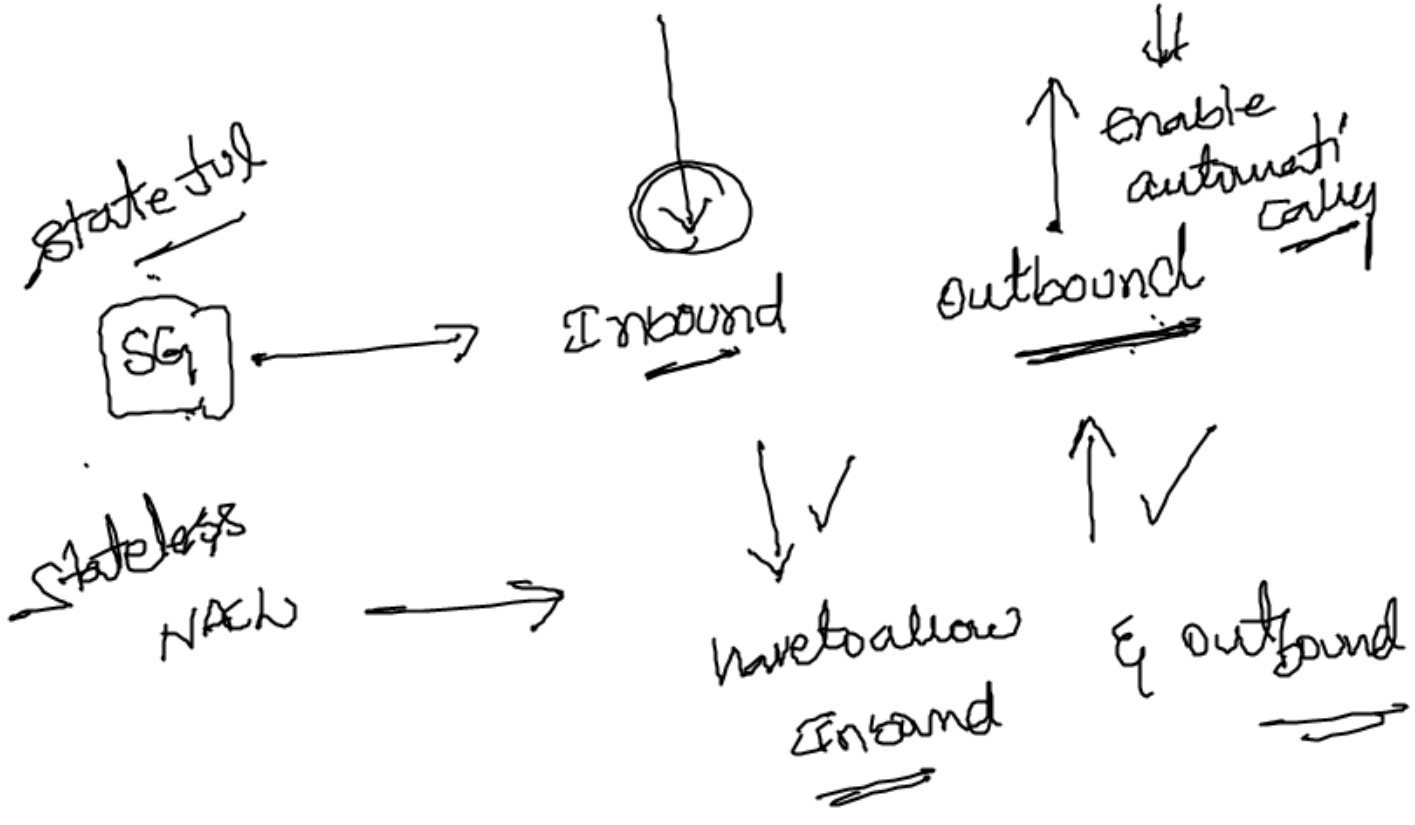

Gmail
Gmail
Gmail
Alc val
Alc stg
Alc dev
Alc prod

95%

(security group)

NACL
(Network Access Control List)




stateful
SG
Inbound
outbound
enable
automati
cally
Stateless
NACL
have to allow
Inbound
& outbound

NOTE:-

(SSh)

"ping"

Security group

(Icmp packets)

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

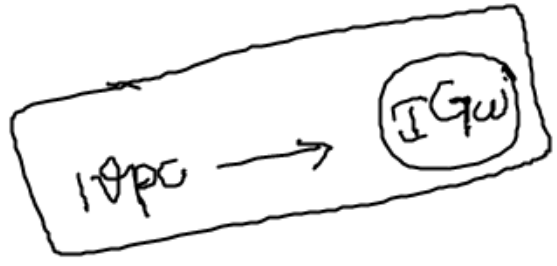
Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH	TCP	22	Custom 0.0.0.0/0		Delete
All ICMP - IPv4	ICMP	All	Custom 0.0.0.0/0		Delete

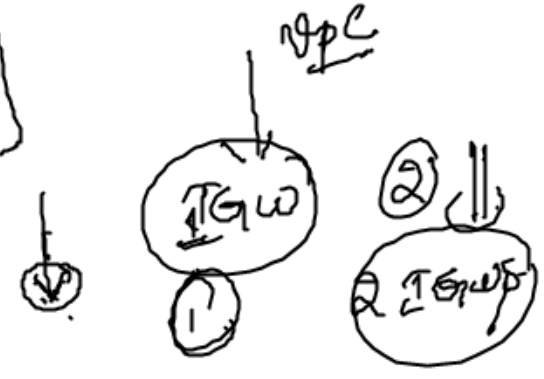
ping

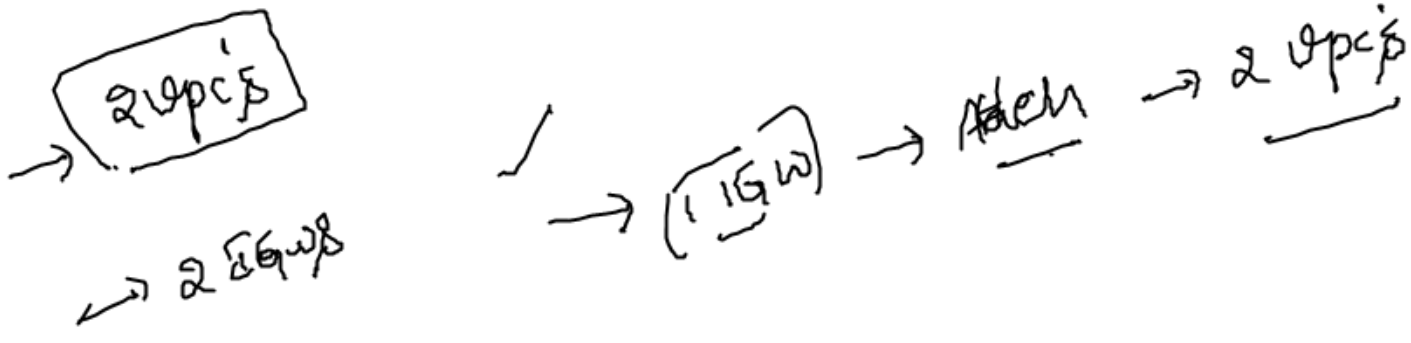
Add rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a ne[Ctrl]e created with the new details. This will cause traffic that depends on that rule to

R1
R2
R3


1 vpc
IGW


vpc
IGW
1
2
2 IGWs


2 vpcs
2 IGWs
1 IGW
Attach
2 vpcs