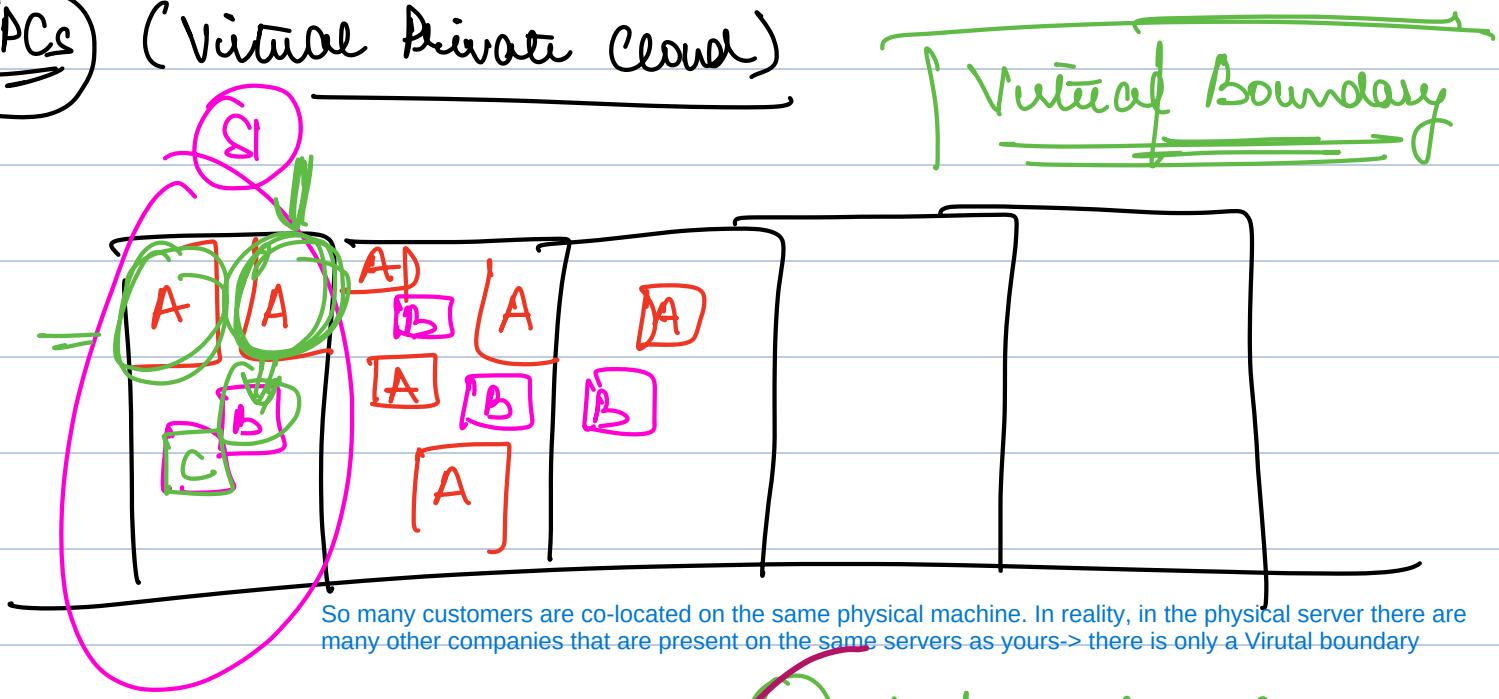
→ VPC

→ Security Groups

→ Domain Names (Route 53)

A company is assigned a part of the Amazon's machine -> A or B

VPCs (Virtual Private Cloud)



So many customers are co-located on the same physical machine. In reality, in the physical server there are many other companies that are present on the same servers as yours-> there is only a Virutal boundary

One company may also have many services. Now a company might need a level of isolation for each of these services

✓ (1) No physical isolation

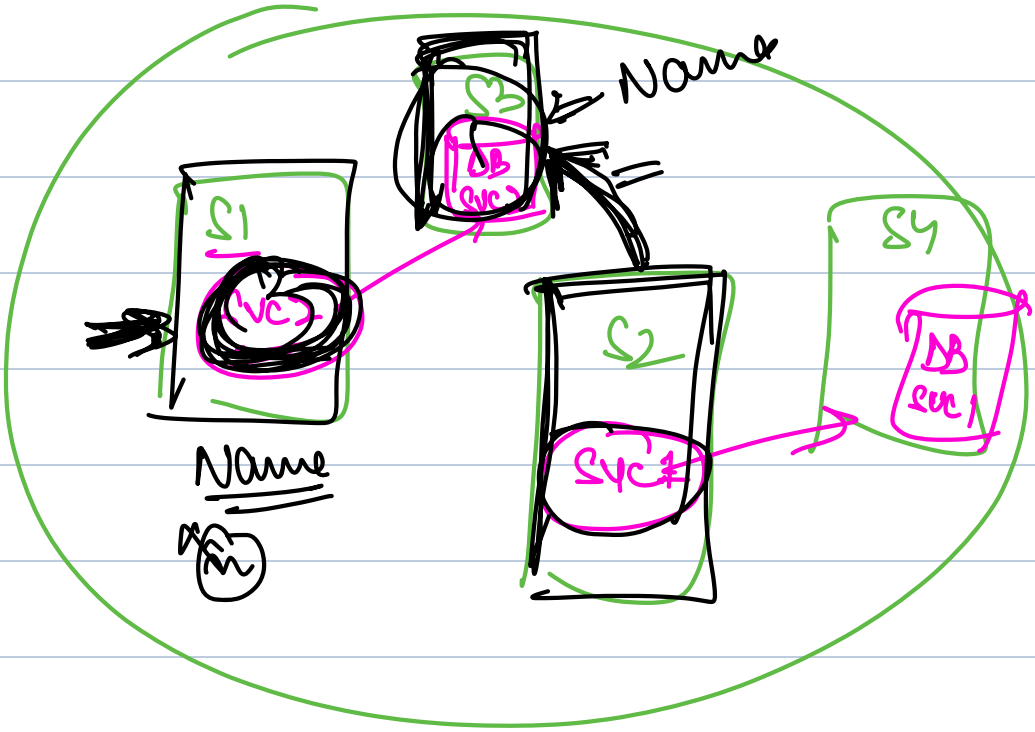
↳ only virtual isolation

1 company => Many Services

↳ level of isolation for each of services

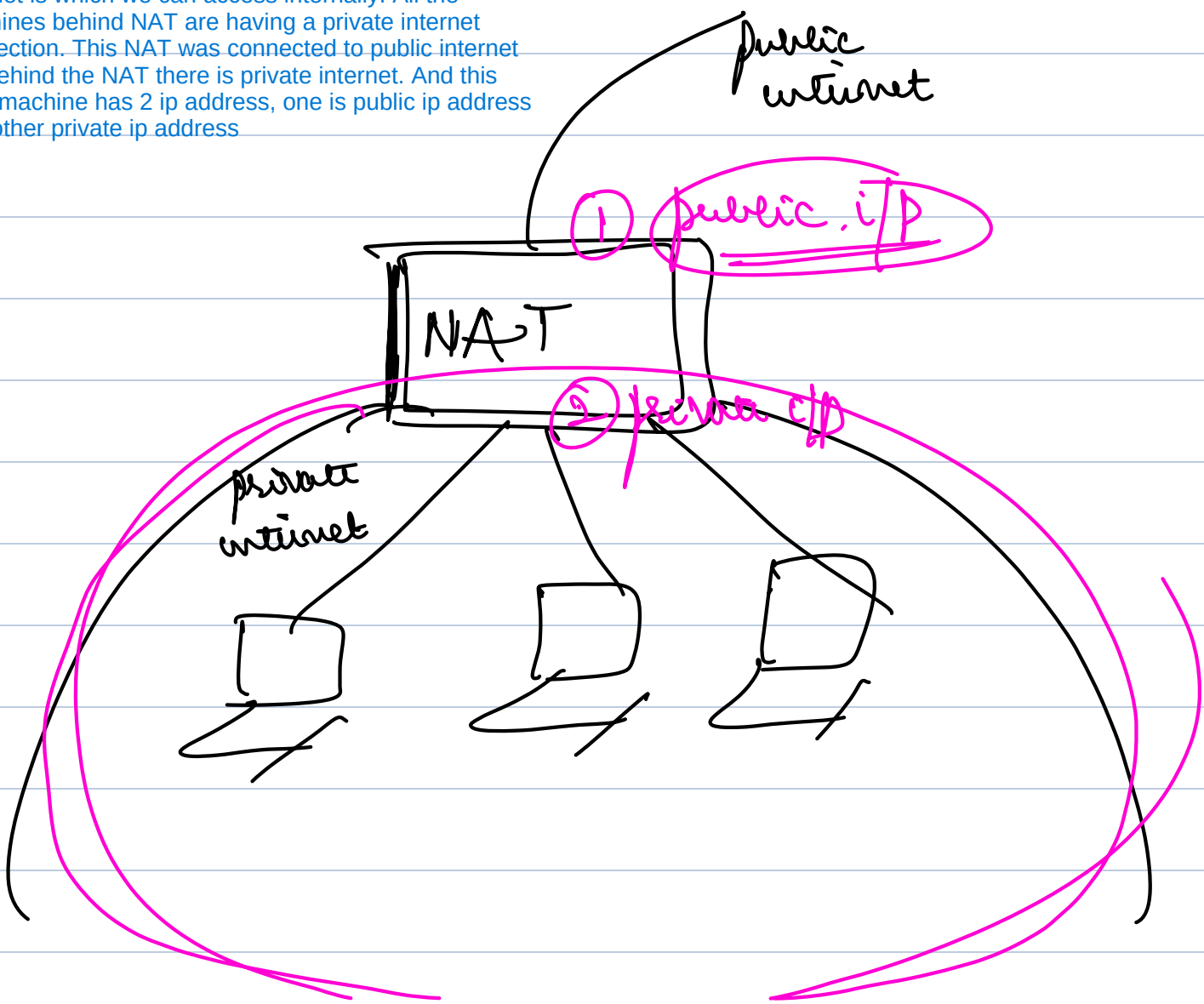
What do you mean by level of isolation for each services. Lets suppose for one company there are server 1, S1, server 2, S2, S3, S4 hosted at one particular location.
In the server 4 you are hosting db, S3 again Db and S1, S2 -> some other service. S1 is connecting with S3, S2 with S3

Now if S2 access the data of S3, and change code which has business constraint applied by S1 -> suppose Name should not start with 'N' and S2 changed for names starting with 'N' then there will be an issue. hence AWS provides level if isolation for each servers irrepescetive of the physical machine kept at the same location



① AWS ka
ek account
create a
VPC

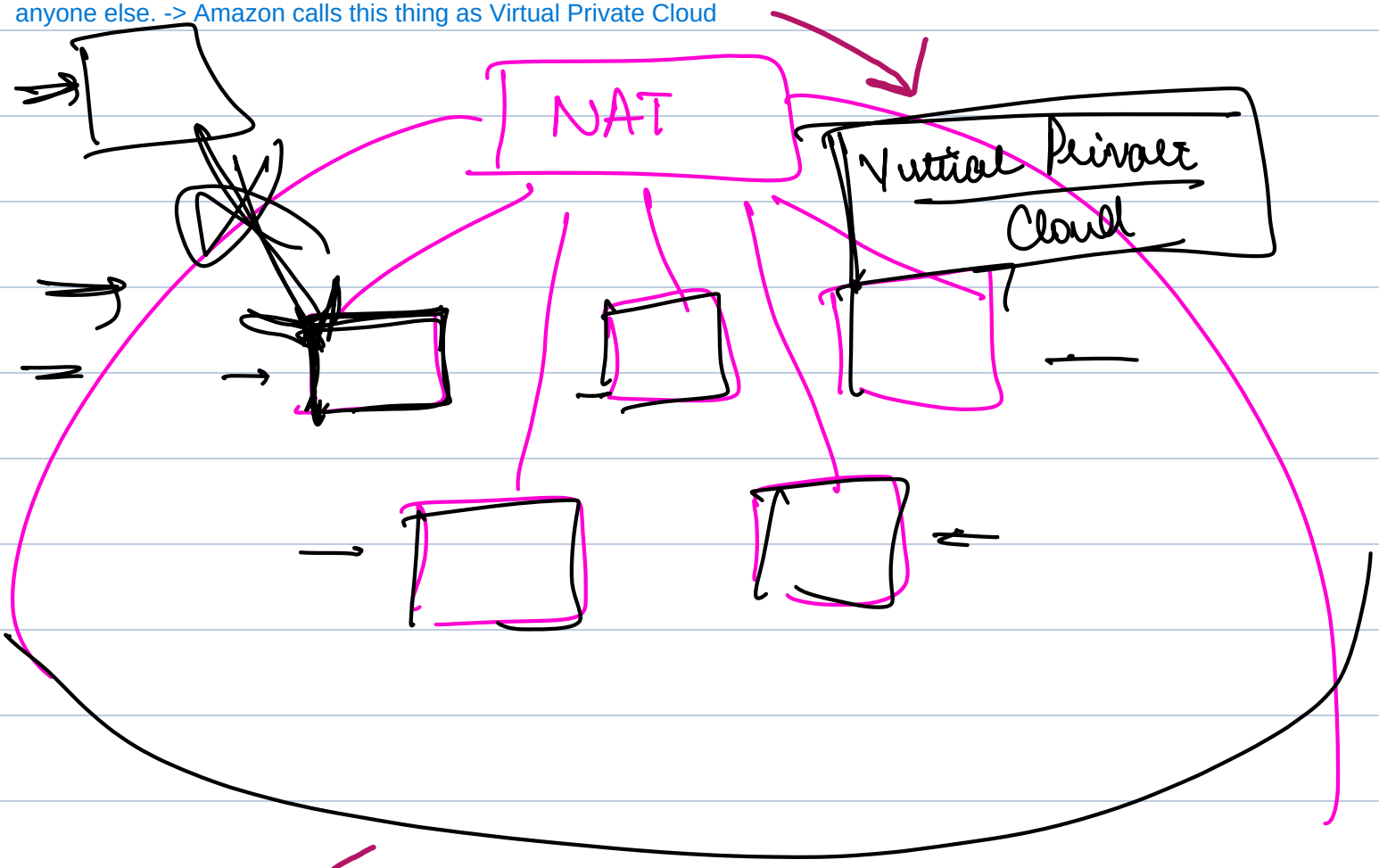
So far we have heard about private internet, A private internet is which we can access internally. All the machines behind NAT are having a private internet connection. This NAT was connected to public internet but behind the NAT there is private internet. And this NAT machine has 2 ip address, one is public ip address and other private ip address



Amazon will put all of your machines in a private NAT

Whenever you create a AWS a/c, now AWS may have physical core location of multiple different companies but Amazon will try to provide you no physical but virtual isolation -> this means Amazon will put all of your machines in a private NAT

So AMzon for each a/c will be creating a kind of a NAT and all of the virtual servers that you are creating, all of them are only connected to this NAT and these servers coz that are a part of NAT private network they can only talk to each other and not anyone else. -> Amazon calls this thing as Virtual Private Cloud



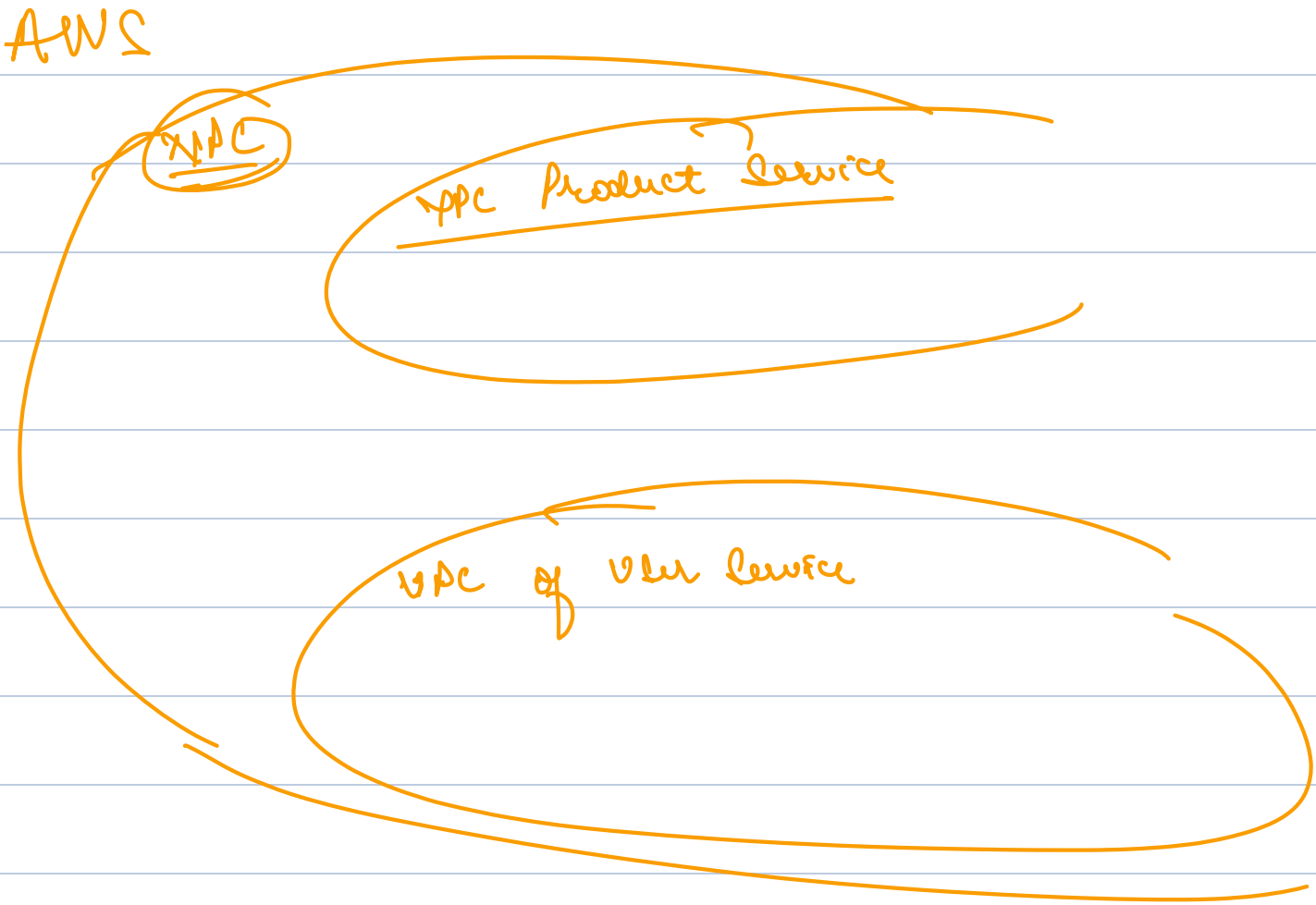
By default, a machine can only be accessed from other machines of their VPC.

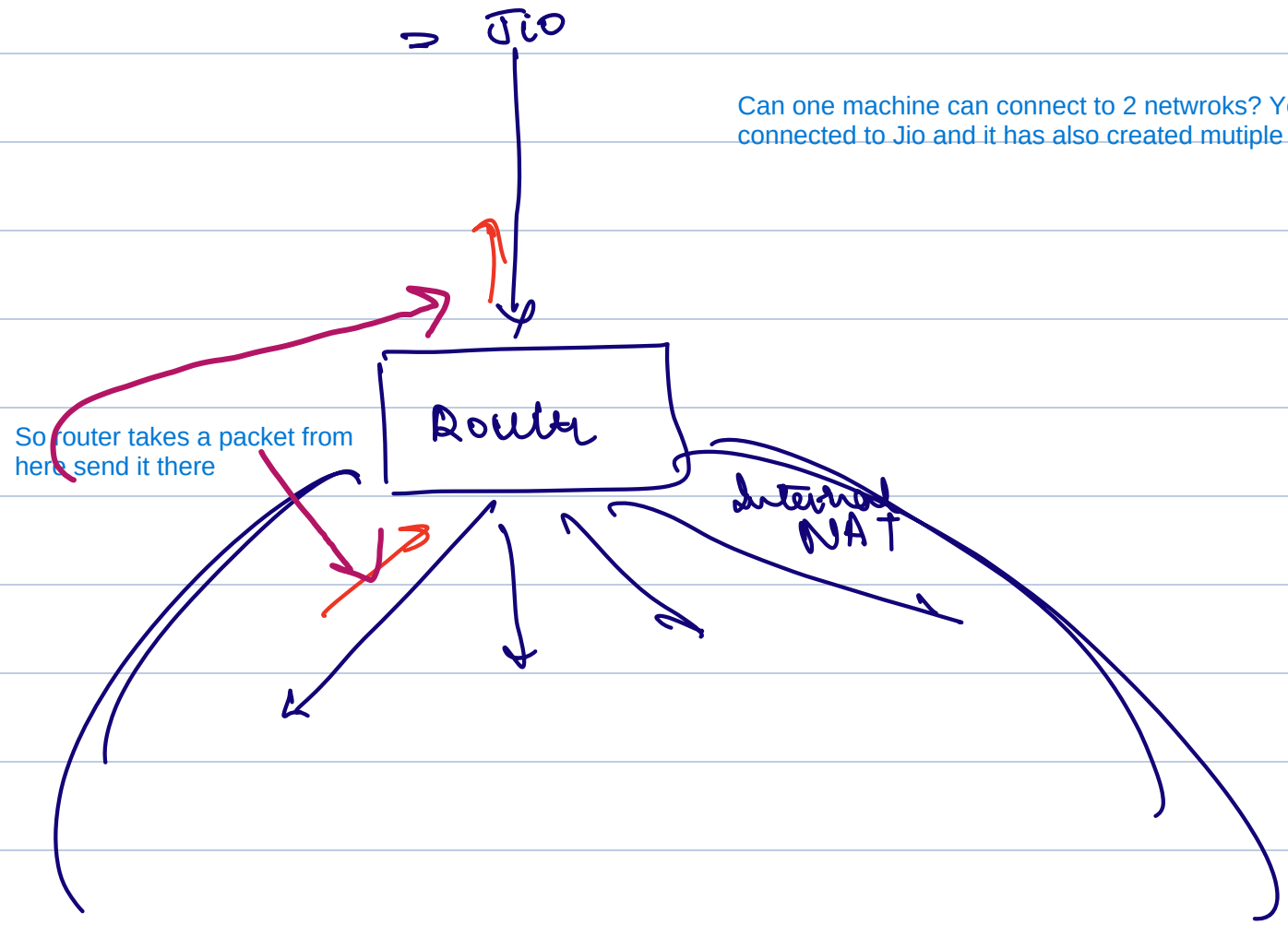
This is said Virtual Private CLoud coz physically the machines can be kept near to each other but Virtually they are isolated.

By default with a AWS a/c you get one 1VPC

1. 1 VPC as a part of your account
2. Create More VPC's as you need.

You create an AWS a/c you get a VPC, you can create more VPC - ProductService, another for USerService

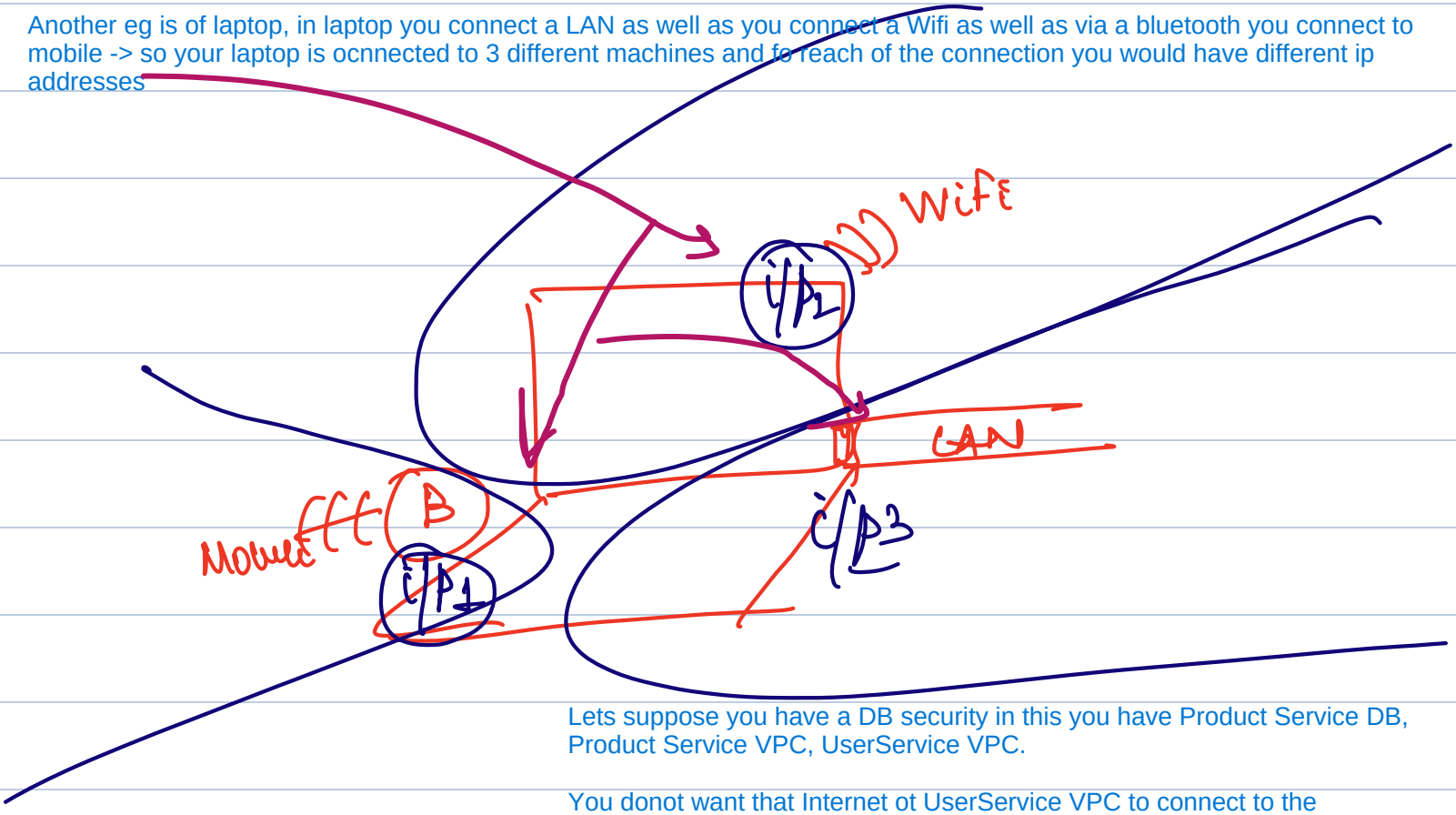




Can one machine can connect to 2 netwroks? Yes Eg Router is connected to Jio and it has also created mutiple internal net.

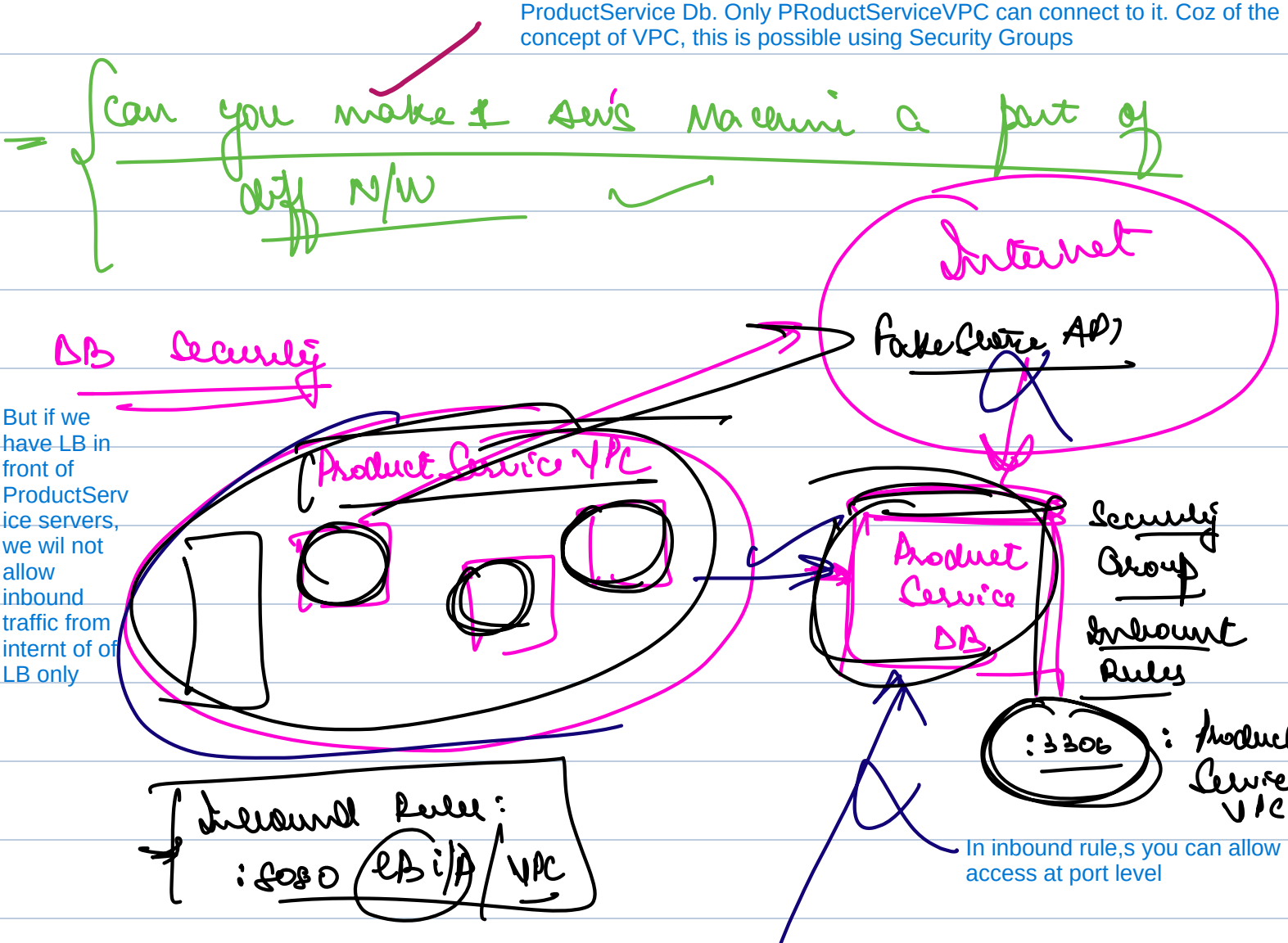
So router takes a packet from here send it there

Another eg is of laptop, in laptop you connect a LAN as well as you connect a Wifi as well as via a bluetooth you connect to mobile -> so your laptop is ocnnected to 3 different machines and fo reach of the connection you would have different ip addresses

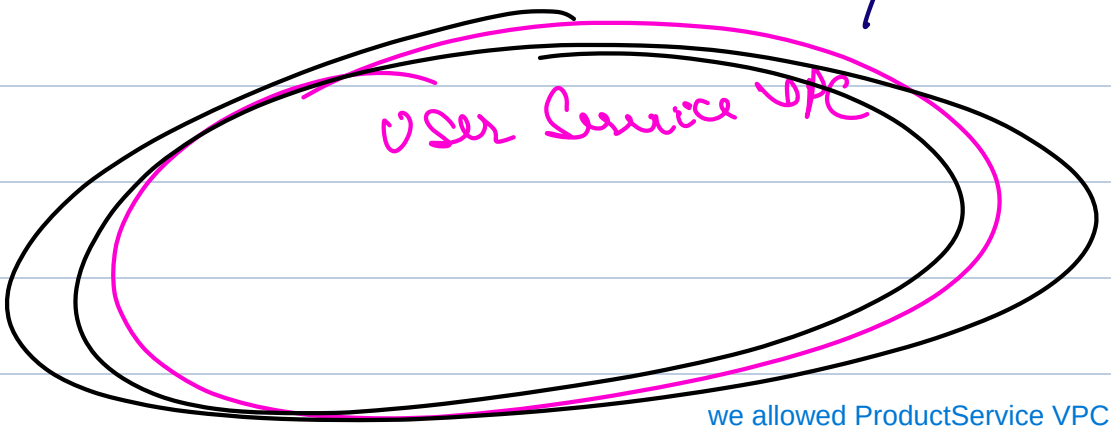


Lets suppose you have a DB security in this you have Product Service DB, Product Service VPC, UserService VPC.

You donot want that Internet ot UserService VPC to connect to the ProductService Db. Only PRoductServiceVPC can connect to it. Coz of the concept of VPC, this is possible using Security Groups



But if we have LB in front of ProductService servers, we wil not allow inbound traffic from internt of of LB only

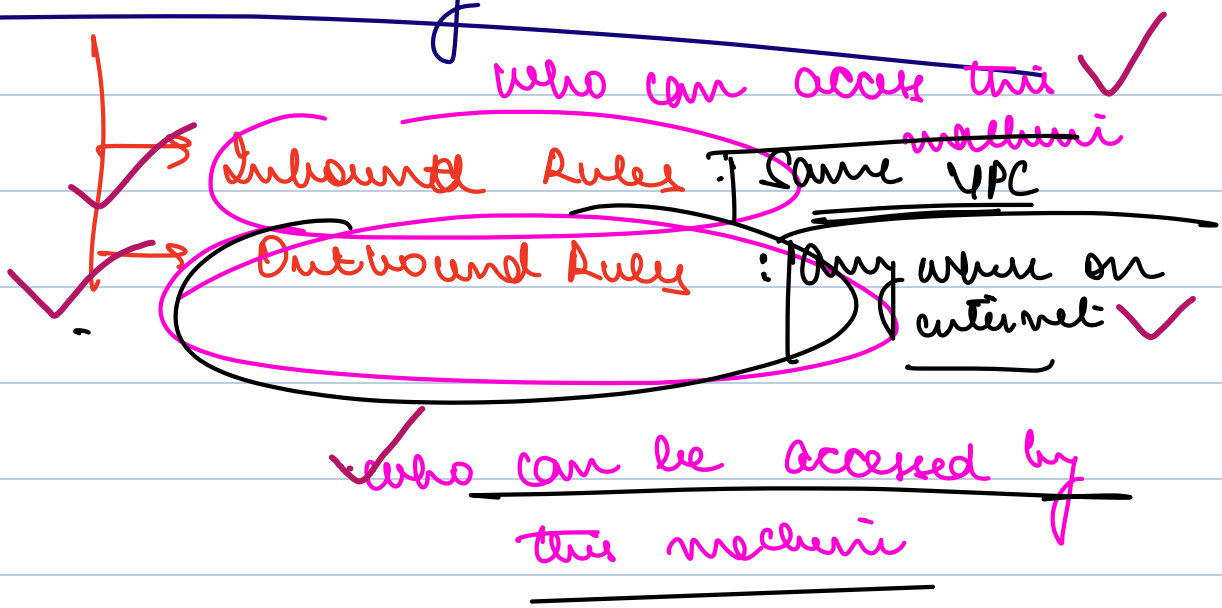


we allowed ProductService VPC to access the internet -> here we are defining outbound rules, who could be accessed by this machine. eg is FakeStoreAPI and we want our ProductService API to access FakeStoreAPI

And Inbound rules are for same VPC-> anyone on the same VPC

Security Groups

Associated to every machine



LB

Inbound Rules

: 80 ⇒ anywhere from internet.

Outbound Rules

: ____

For LB you can say the inbound rule is anywhere from the internet.

Lets say you want to host a website with the name, Abhinav.com, first of all you have to buy this domain. How they will buy, they will buy via broker (also called Domain Registrar) Eg of these are godaddy, Porkbun, NameCheap

Using our own domain name

Lets say

ICANN

Buy this domain

via a Broker (domain registrar)

GoDaddy, PorkBun, NameCheap

Naman.dev

Host the content that needs to be present on your domain

Paid hosting providers

Free hosting providers

Free Hosting

Wordpress

Wix.com

GitHub Pages (only static pages)

Github only allows host the static html pages not dynamic server

Paid Hosting

(AWS)

(DigitalOcean)

Is there any connection b/w these yet? No

Any issues?

You own the domain name

You have the content

But lets say someone, a user is trying to access our domain name

naman.dev ⇒ i/p

Eg when someone will open naman.dev -> there is no such connection that will show them the content present at ip of eg Github pages

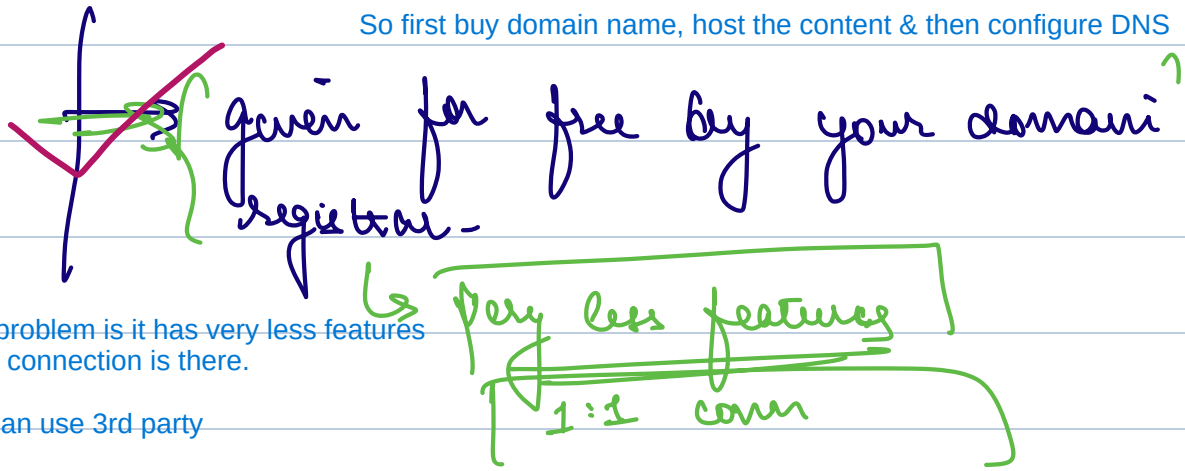
mail.naman.dev ⇒ i/p

blog.naman.dev ⇒ i/p

⇒ Configure the DNS

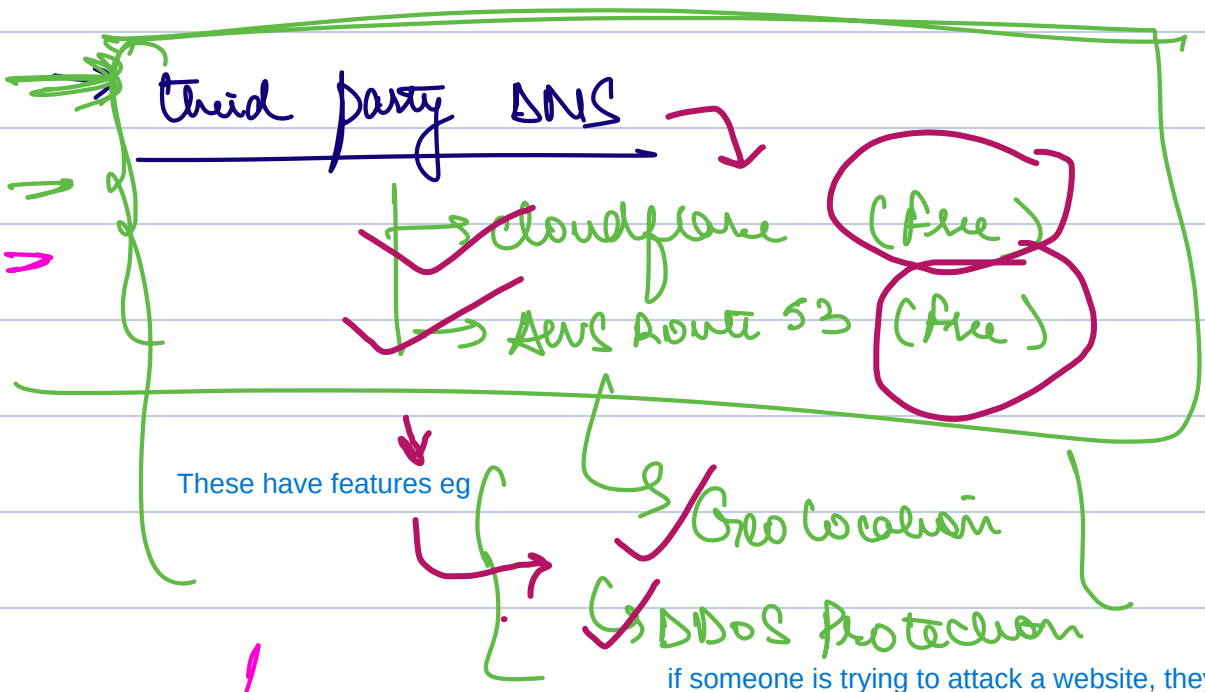
Similarly if someone there would be an ip address of mail.naman.dev or blog.naman.dev. Where is the ip address present for this domain? DNS. You have to configure DNS.

So first buy domain name, host the content & then configure DNS



but the problem is it has very less features only 1:1 connection is there.

or you can use 3rd party



These have features eg

- Geolocation
- DDoS Protection

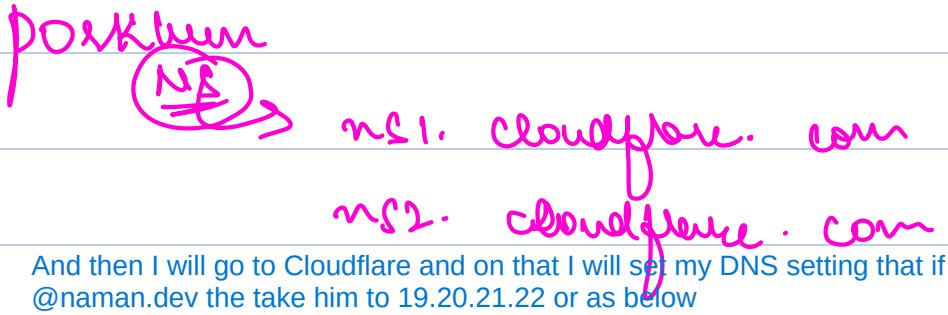
if someone is trying to attack a website, they will try to protect you

If you are using 3rd party DNS, you have tell Domain registrar that you are not going to use their DNS service-> b configuring NS setting (where you specify ip address of 3rd party DNS,

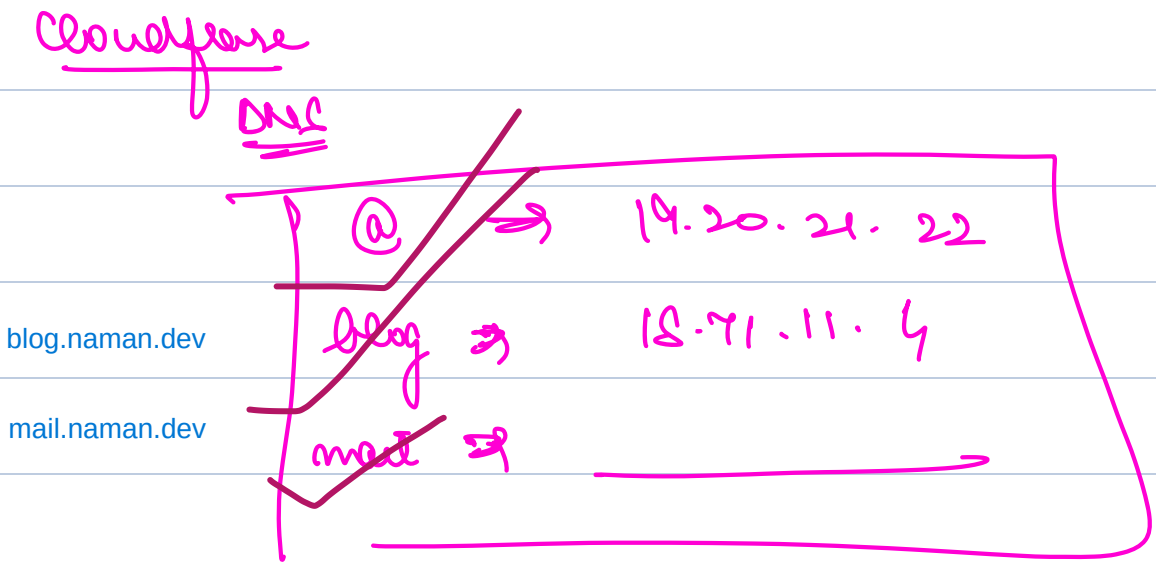
in your domain reg you configure "NS" setting: where you specify i/p

address of third party DNS

Eg I will go to Porkbun and I will say hey my servers are: NS -> ns1.cloudflare.com



And then I will go to Cloudflare and on that I will set my DNS setting that if someone opens suppose @naman.dev the take him to 19.20.21.22 or as below



Cloudflare will assign a proxy ip addresss noone can know my real ip address of my server

So Now I will change my domain name NS(name servers) to Route 53. In Route 53 the first step is to setup your domain name and domain name in Route 53 is called a hosted zone.

i am moving cloudflare domain name servers to route 53 domain name servers