VPC-1

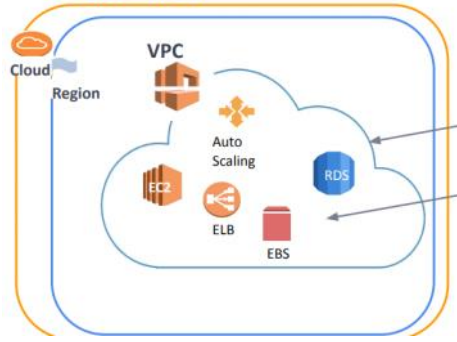
Saturday, August 10, 2024 4:22 PM

Ec2 gibi bu isin bel kemiklerinden birisi.
Daha cok tumgen gelim sekliyle ogrenecegiz bu isi.

1 Introduction to VPC

Introduction to VPC

What is VPC?



Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define.

Mantiksal izole edilmis alan demek. Yani AWS bize launch ettigimiz resourcelarimizi, diger recourcelarda olabilir veya diger aws kullanicilari da olabilir, bunlardan ayirmak icin kullandigi sanal bir cit alani olusturmus.
Her resource vpc bazli br resource degildir. Istisnalar vardir ama hemen hemen cogu resource vpc bazlidir, bir network area icerisinde uretilir.

Burada s3-dynamodb ye ulasmak icin aws enviromentin disina cikiyoruz ve sonra tekrar internetle aws icinde bu servislere baglaniyoruz. Yani apartmanda yan komsuya gitmek icin apartmandan cikip sonra tekrar apartmana girip komsuma gidiyorum.

services using HTTP protocol

S3, Dynamodb nonvpc resourcelardir. Yani vpc otesi servislerdir.

Ama buradaki gibi vpc endpointlerle apartmanin disina cikmama gerek kalmadan yan komsuma gidebiliyorum

2 VPC Basic Components

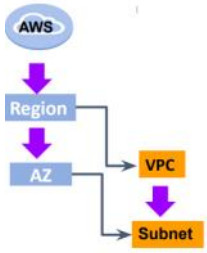
Ama biz herzaman bir resource yaratirken bir vpc icinde yaratiriz.

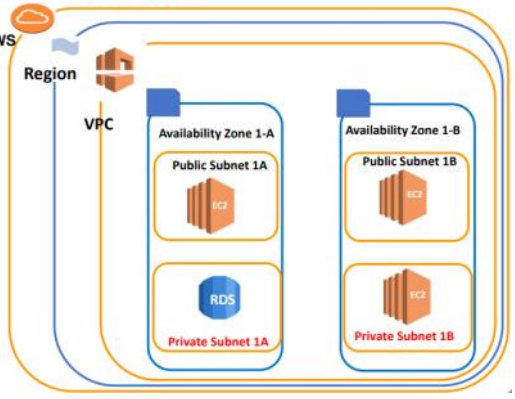
Her resource bir networke dahil ediliyor aslinda yukaridaki rds ornegindeki gibi

VPC Basic Components

- VPC Region (AZ)
- VPC Subnets
- VPC CIDR
- Elastic Network Interfaces
- Internet Gateway
- Route Table
- Security Group and Network ACL

Region,VPC, AZ and Subnets





CLARUSWAY

VPC regiaon bazli ve subnetler de AZ bazlidir
hiyerarsik olarak.
VPC yi bir region bazli seciyoruz ve daha sonra onun bazi companentleri oluyor. Alt aglari subnetler oluyor. Bu subnetleri de Azlere bagli olarak yaratiyoum

VPC CIDR

10.0.0.0/16= **65,536** IPs in Range
10.0.1.0/24= **256** IPs in Range
10.0.1.0/32= **1** IP in Range

- CIDR refers to Classless Inter-Domain Routing.
- It is a set of Internet protocol (IP)
- standards that is used to create unique identifiers for networks.

- As the Size Block/Netmask (/16,24,32) increases, the number of IP located in CIDR Block decreases.

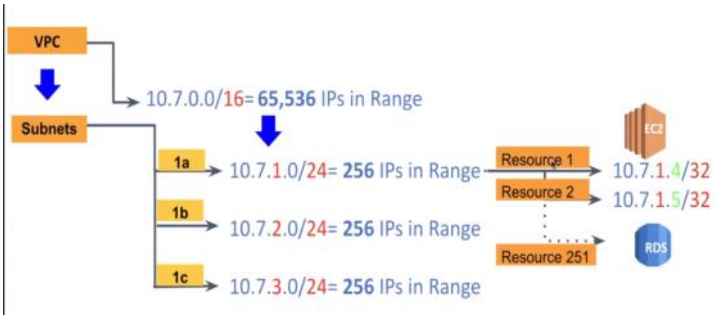
Her VPC de CIDR blogu olur. Bu onun tanitici adres blogudur.
IP adres demeti gibi dusunebiliriz.
Sag tarafta subnetmasklar bulunur.
VPC yi bir IP demeti gibi dusunebiliriz. Bizim resoucelarimiz icin yaratilmis mantiksal bir alan ise CIDR da bu alanlarin icinde yaratilacak olan resourcelara verilecek Iplerin oldugu deposu.

3. **Private Address Space**

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

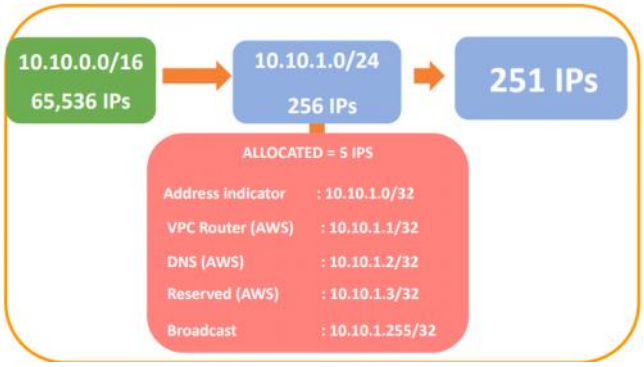
10.0.0.0	-	10.255.255.255 (10/8 prefix)
172.16.0.0	-	172.31.255.255 (172.16/12 prefix)
192.168.0.0	-	192.168.255.255 (192.168/16 prefix)

Burada bu ozel alanlar kullanilacak Ipleri cercevelemisler. Yani diyor ki 10.0.0.0 da 10 alinmis siz digerleri uzerinde oynayabilirsiniz. Ilk 8 oktet alinmis.
0 lar hostlara verebilecegim IP variasyon kismi.



Burada mesela VPC ye 10.0.0.0/16 atanmis. Bu su demek: VPC ye 65.536 tane IP atanmis. Ama bunu kaba taslak kullanmiyoruz. Icerde bir subnet yaratip onunla kullaniyoruz. Biz bir resource yarattimizda VPC icindeki bir subnette yaratiyoruz. Biz bu IP demetlerini VPC altinda bolunmus subnetler gibi, subnetler altindaki CIDR lara bolustutuyoruz.
Mesela 10.7.1.0 p blogunda olusturdugumuz bir resourcea 10.7.1.4/32 CIDR verilmis.

VPC CIDR

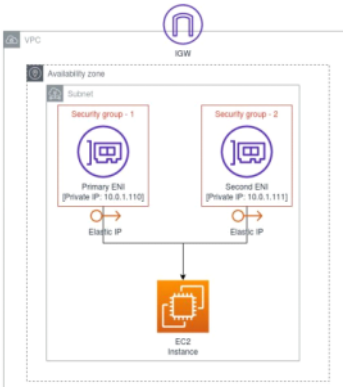


VPC nin CIDR icin dagittigi IP lerin hepsini biz kullanamiyoruz.
Kirmizi kutucuktakiler kendi rezerve ettigi Ipler bu yuzden onlar haricindekileri kullanabiliyoruz.

Elastic Network Interface

An *elastic network interface* is a logical networking component in a VPC that represents a virtual network card. It can include the following attributes:

- A primary private IPv4 address from the IPv4 address range of your VPC
- One or more secondary private IPv4 addresses from the IPv4 address range of your VPC
- One Elastic IP address (IPv4) per private IPv4 address
- One public IPv4 address
- One or more IPv6 addresses
- One or more security groups
- A MAC address
- A source/destination check flag
- A description



Bilgisayarlardaki ethernet kartinin sanal PC deki karsiligina Elastic Network Interface diyoruz.
Public IP, private IP, MAC dresi vs bizim instancemizin baglanmasini saglayan ara aparattir.
Yani bir EC2 ya trafigi ona bagladigimiz ethernet kartiyla bagliyoruz.
Bir birden fazla interface baglayabiliriz.
Primary ENI dedigimiz ayrilamaz, cunku security gruplarla iliskilendiriliyo.
Secondar ENI ise ec2 ariza verdigi zaman birincil ethernet kartida onunla birlitke arizalanir ama bu second ENI trafigi alir baska bir yerden tekrar kendisi devam ettirir. Yani ayn EC2 ya gidecek mektuplar bu sefer ikincil ENI uzerinden devam eder. Bu ancak ayni AZ icinde gecerlidir.
Elastic Network Interface kartlari availability zone bazlidir.

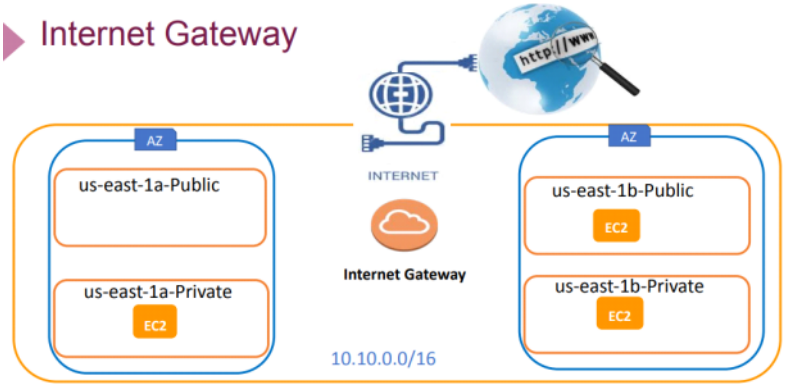
Elastic Network Interface

ENI → ENA → EFA

ENI	ENA	EFA
• Upto 10 GBPS • VMDq • TCP/IP • Multiple ENI/instance • Traffic can traverse across subnets • VPC Networking, General purpose • Default	• Upto 25 GBPS • SR-IOV • TCP/IP • Single setting/per instance • Traffic can traverses across subnets • Low latency apps • Optional on supported instance type	• Upto 100 GBPS • OS-Bypass • SRD • One EFA per instance • OS Bypass traffic is limited to single subnet and is not routable • HPC and ML Apps • Optional on supported instance type

SINAVDA CIKABILIR!!!
ENA-EFA adaptor olarak gecer. ENI interface, digerleri adaptor.
EFA fabric adaptor, ENA network adaptor.
ENA hizli trafikler icin
EFA ise HPC ve ML apps icin yani daha yuksek performans gerektiren durumlar icin.
Machine learning icin EFA kullanilir mesela.
ENA ve EFA her instanceta yok. Bizim standart instancelarimiz ENI kullanir.
Daha cok IP baglanmasi gerekiyosa mesela ENA ya da EFA
SINAVDA YA ENI ILE EFA GELIR YA ENI ILE EFA GELIR!!!

Internet Gateway

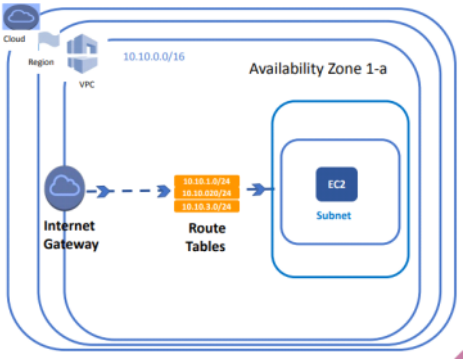


- **Internet Gateway** is a VPC component that provides communication between resources in your VPC and the internet.

VPCnin internet gecisini saglayan da internet gatewaydir.
Yani modem gibi.
Her VPC nin disariya cilan bir modemi var.
Dolayisiyla bu bizim resourcelarimizin publige acik olmasini sagliyor. Ama mesela ben disariya ulasayim ama disarisi ulasamasin istiyorsak bunun inbound/outboundlari ayarlanarak internet gateway ile ayar yapilmis olunur.
Internet gateway VPC nin gecirgenligini saglarken, Elastic etwork Interface ise bizim EC2muzun internet gecirgenligini sagliyor.
Internet gateway olacak ki biz public Ipmizle internete baglanabilelim.

Route Table

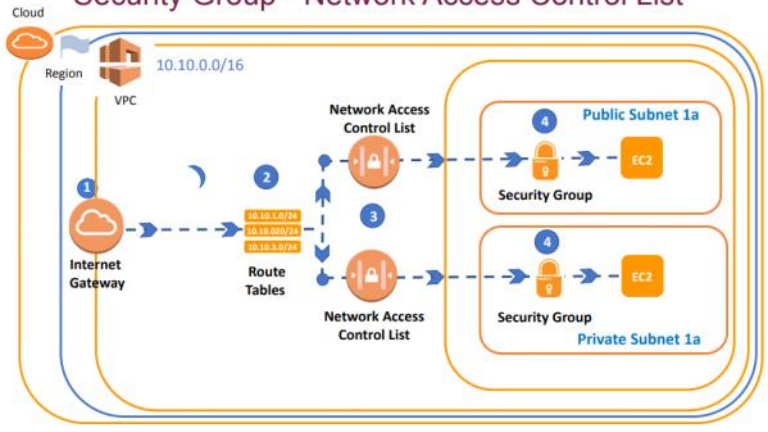
- Route Table is a set of rules, that is used to determine where VPC traffic is directed.



CLARUSWAY

Icerisinde rotalama yapar.
Subnetlerin baglandigi bir componenttir.
Icerideki ve disaridaki trafigin akis kurallarinin bulundugu yerdir.
Inbound ve outbound hukumlerinin verildigi yer.
Route table esittir pasaport.
Route table uzerindeki izinler de vizemiz..

Security Group - Network Access Control List



Security group bizim EC2 based bir component ve bu bizim EC2larimiza bir koruma saglar. Iceriye girecek ve disariya cikacak trafigi kontrol eder.
Regionlarin altinda VPC ler var ve onlarin altinda subnetler var ve biz bu subnetler altinda resourcelarimizi yaratiyoruz dedik.
EC2 larimizin giris cikilarini kontrol eden security gruplar oldugu gibi subnetlerimizdeki giris cikislarimizi da kontrole eden Network Access Control listlerdir. Bunlarin anatomik yapisi biraz daha farkli security grouplardan.

Network ACLs & Security Groups

- Network ACLs are subnet-based security components.
- It controls the traffic in and out of subnets.

- Security Groups are instance-based security components,
- They are used for determining which traffic will access the instance.

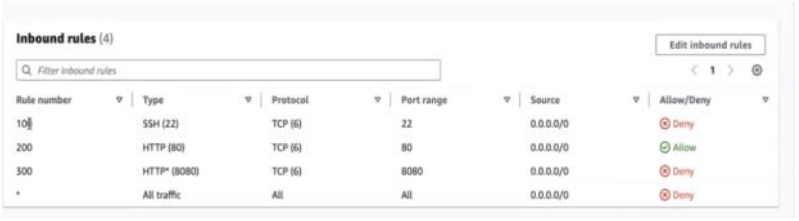
- Instance in subnet is affected by rules of both Security Groups and Network ACLs

CLARUSWAY

Network ACLs bir subnet bazli compenenttir.
Bu hiyerarsik bir yapi oldugundan dolayi, security grouplar ayni zamanda Network ACLlerin tabi oldugu kurallara tabii olmak zorundadirlar.

	Security Group	Network Access Control List
Rules	It supports only **Allow Rules**	It supports **both Allow and Deny** rules
Default by AWS	By default, **inbound** rules are **Denied**, **outbound** rules are **Allow**	By default, all the rules are **Allowed**
* **Newly Created by User**	By default, **inbound** rules are **Denied**, **outbound** rules are **Allow**	By default, all the rules are **Denied*** until you add rules.
Add Rule	You need to add the rule which you'll **Allow**	You need to add the rule which you can **either Allow or Deny it**.
Stateful/Stateless	It is a **Stateful** means that any changes made in the inbound rule will be automatically reflected in the outbound rule	It is a **Stateless** means that any changes made in the inbound rule will not reflect the outbound rule
Association	1. It is **instance-based** 2. Instances can associate with **more than one** Security Groups	1. It is **subnet-based** 2. Subnets can **associate with only one** Network ACL

Security groupta sadece allow olan izinler var.
Ama Network ACL te allowda deny da var. Bu bir ust tabaka bir guvenlik.



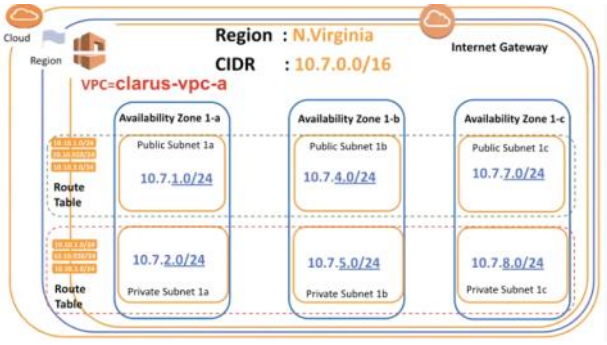
Inbound rules (4)

Edit inbound rules

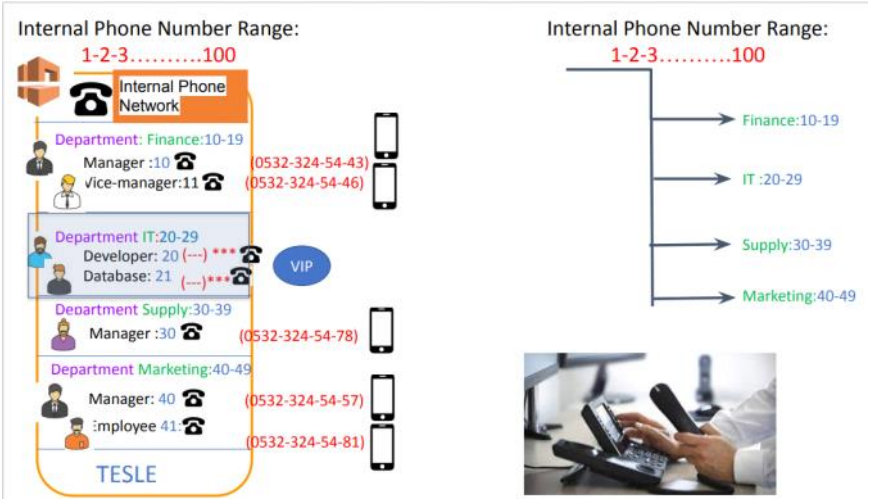
Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	Deny
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
300	HTTP* (8080)	TCP (6)	8080	0.0.0.0/0	Deny
*	All traffic	All	All	0.0.0.0/0	Deny

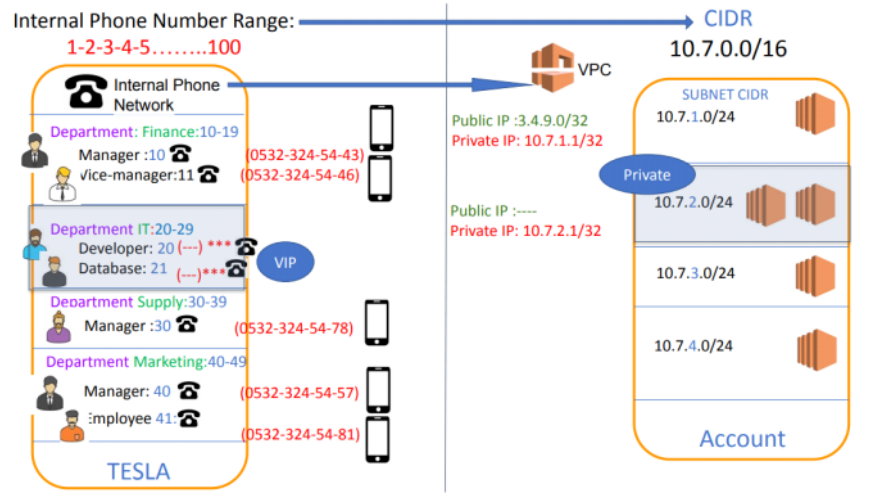
Kucuk numaradan itibaren siralamaya baslar. Ismi ozellikle girmesinler listesinde olanlar deny ile belirtilir. Bu bir ust duzey guvenlik listesidir. Ayni sekilde normalde security groupta outbound ruleda all traffic varken burada girenler ve cikanlar tek tek belirtilir. Cunku inbound ve outbound rulelar birbiriyle konusmazlar. Haberlesmezler. O yuzden tek tek belirtmek gerekir burada kurallari. Bu demek oluyor ki guvenlik tedbirleri ust seviyede.
Securtiy groupta durum farkli. Ikisi de birbiriyle konustugu icin iki tarafta ayri ayri belirtmeye gerek yok. Iceri girebilen all traffic disari cikabilir orada.
SINADA CIKABILIR!!!: yeni yaratilan bir access control liste default olarak inbound rulelar denied ve outbound rulelar allow olarak yaratilir.



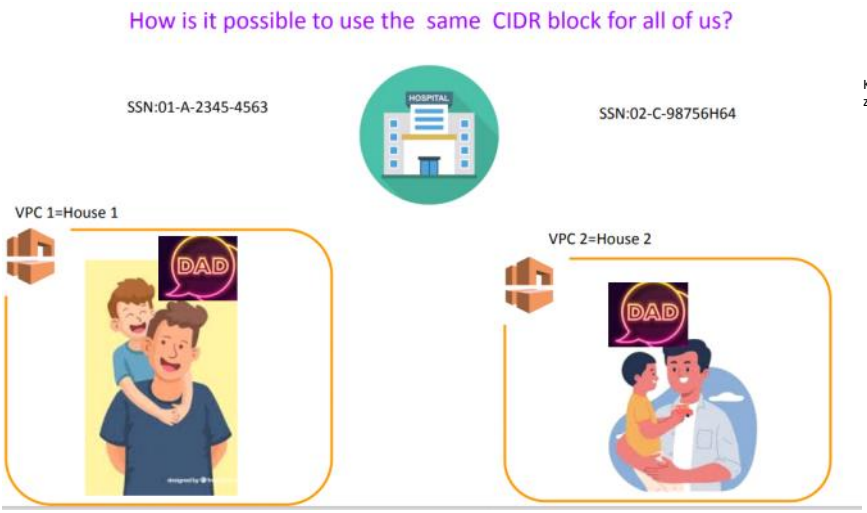
Biz VPC adi buradaki gibi olan bir vpc olusturup altina 2 ayri publiv ve private route table olusturduk.
Bunlari 3 ayri zoneda olusturup her zoneda bir public ve bir private subnet olusturduk.



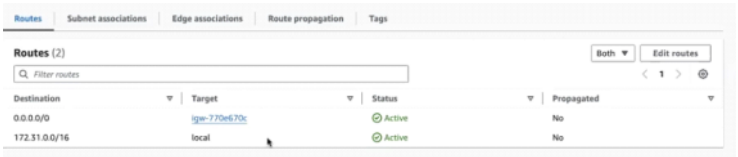
1-100 sentral numarasi var.
Her kati bir departmana bolduk .
Bu sentral numaralriyla sirket icerisinde istedigin seyler gorusebileceksin.
Her kati departman numaralarini bir siraya gore bolduk. Yani numaralrina baktigimiz zaman hangi departmandan oldugunu anlayabiliyoruz.
Icteki konusmayi bu sekilde dahili telefonlarla yapiyoruz.
Birde disaridaki isleri halletmek icin her bir calisana bir cep telefonu veriyoruz.
Dolayisiyla herkesin masasinda bir cep telefonu ve bir dahili telefon var.
Guvenligi onemli olan telefonlar icin ise sadece masabasi telefon vreiyorum. VIP grubu icin eger disari ile bir irtibat saglamasi gerekiyorsa once santrali arar ve daha sonra santralden disariya baglanirlar.



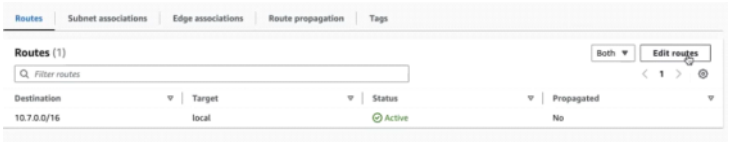
Santal telefon numaralari = CIDR
Internal Phone Network = VPC nin sectigi subnet numaralari
Public IP = cep telefonlari
Private IP= santral numaralari
Departmanlar = subnetler



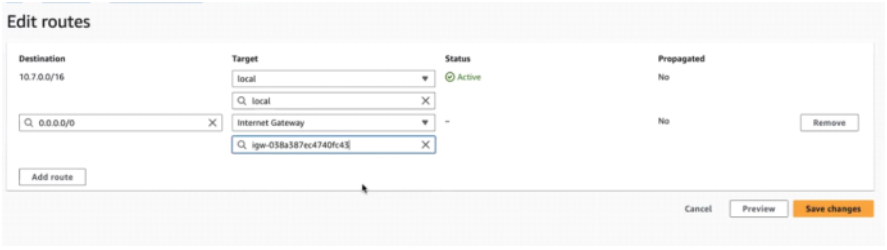
Kendi VPC lerinde dad diye seslenebilirler ma amesela hastaneye gittiklerinde bir tc numarasi vermek zorundalar gibi bir mantik ayni CIDR blogunu kullanmak.



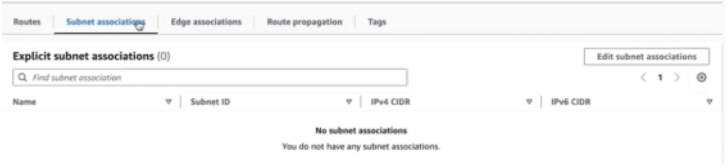
Burada disari cikmak icin targetin igw ve local icin targetin local oldugunu gosteren pasaport vize olayini gormus oluyoruz. Yani disa baglanmak icin ihtiyacimiz olan gatewayi gosteriyor.



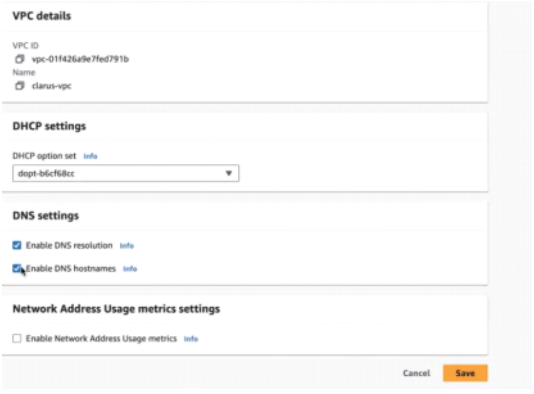
Yeni olusturdugumuz rote tableda sadece local izin var. Disari izin yok. Onun icin bir izin ayarlamamiz lazim.
Bunu da edit kismindan yapiyoruz.



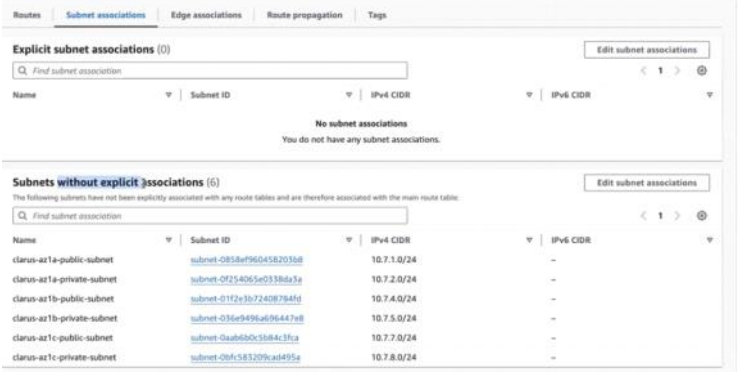
Editte bu bilgileri girip bir gatewaye baglamis oluyoruz. Degisiklikleri kaydedince artik disari baglanti da gerceklesmis oluyor.



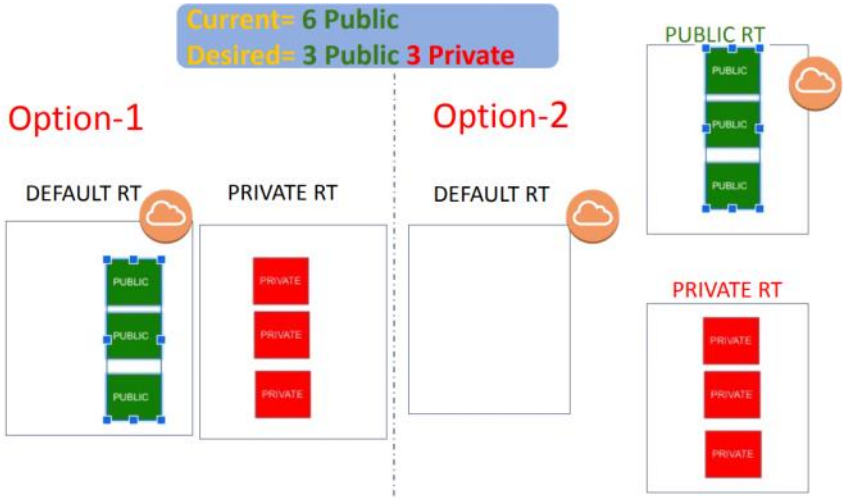
Subnet kismi ilk etapta bos.



VPC iceriklerini guncellesidigimde bizim hostnamei enable yapmamiz lazim.
Bununla VPC icindeki resoucelara bir DNS name tanimlamis oluyoruz.

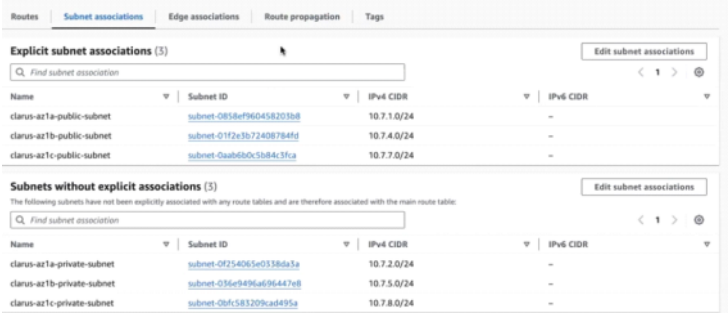


Subnet ekledigimde tum subnetler without explicit olarak kaydedilir otomatik olarak isiminin private public olmasi bir seye yaramaz.
Explicit demek dogrudan demek. Inplicit ise dolayli demek.
Bunlarida hangi route tablea bagli oldugu ile alakali private ya da public hale getiriyoruz.



Bunun icin de bu yolu takip edecegiz. Ya ilk ya 2.
Aws best practise ise soyle der:Publicleri tek bir route icinde topla. Her private subnet icin ise private bir route table yap.

Biz bu kismi editleyerek dogrudan bir association yapiyoruz.



Sonra bu sekilde publicler igw ile bagli privatelar hala ayni yerde default olarak duruyor. Onlari da private routeta explicit association ile baglayaagiz.