# 申请VPC

## VPC概念

官网文档：

https://docs.aws.amazon.com/zh\_cn/AmazonVPC/latest/UserGuide/VPC\_Introduction.html

Virtual Private Cloud (VPC) 虚拟私有云是仅适用于您的 AWS 账户的虚拟网络。

AWS默认可以创建5个VPC 它在逻辑上与 AWS 云中的其他虚拟网络隔绝。

好处：安全性更高，隔离效果更好，使架构更加清晰，方便管理等

可在 VPC 中启动 AWS 资源，如 Amazon EC2 实例。您可以通过修改 VPC 的 IP 地址范围来配置 VPC，创建子网并配置路由表、网关和安全设置。

子网是您的 VPC 内的 IP 地址范围。您可以在指定子网内启动 AWS 资源。对必须连接 Internet 的资源使用公有子网，而对将不会连接到 Internet 的资源使用私有子网。

注意:AWS可用区分布，

如果A账户东京区域可用区A在地点A，B账户东京区可用区可能也在地点A

Aws所有账户的信息的可用区，是有交互的。并不是所有的A可用区都在A地点，B可用区都在B地点

VPC是由若干个子网构成，VPC是可以跨可用区，子网不可以跨可用区，一个可用区可以有多个子网

默认一个VPC的子网是互通的

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| VPC | 子网 | 可用IP | 可用区 | 业务分布 |  |  |
| 172.29.0.0/16 | 172.29.10.0/24 | 254 | ap-northeast-1a | 业务A | 业务B | 私有子网 |
|  | 172.29.20.0/24 | 254 | ap-northeast-1b | 业务A | 业务B | 私有子网 |
|  | 172.29.30.0/24 | 254 | ap-northeast-1c | 业务A | 业务B | 私有子网 |
|  | 172.29.40.0/24 | 254 | ap-northeast-1a | 业务C | 业务D | 私有子网 |
|  | 172.29.50.0/24 | 254 | ap-northeast-1b | 业务C | 业务D | 私有子网 |
|  | 172.29.60.0/24 | 254 | ap-northeast-1c | 业务C | 业务D | 私有子网 |

EC2-VPC

安全组- ACL

这样每个业务可以分别使用三个可用区 做负载高可用

每个可用区最好都有公有子网，私有子网

对于单一子网，如果使用IP过多，可能IP数量不够

路由表下面包含路由和子网互联

路由包含：

local：本地默认同一vpc互通

igw：Internet网关，设置此网关后，此路由表内的机器在配置弹性IP（公有子网）后，可直接上互联网

vgw：在设置与其他云厂商的专线后，这里设置互通的VPC网段

pcx：与aws其他VPC设置的对等连接的VPC网段

nat：NAT网关，设置后，属于私有子网的EC2实例就可以上互联网

子网互联：

一般用户与其他VPC的某个子网互联

因为默认的VPC（192.168.0.0/16）都是内网互通的。而A路由表（192.168.10.0/2）的机器需要与VPC（172.29.20.0/24）相连的话，

子网，通俗来说，

公有子网就是通过弹性IP上网的EC2实例，

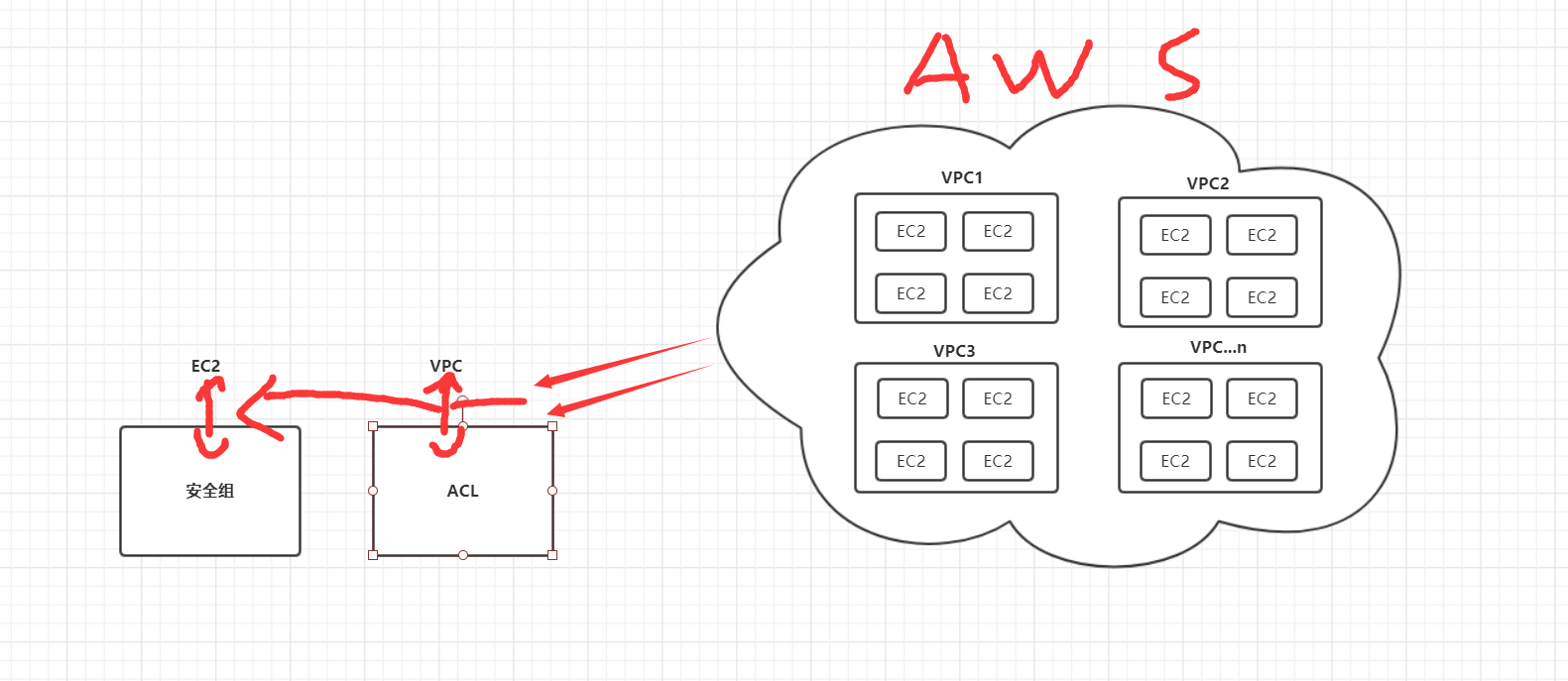
私有子网是没有弹性IP，而通过NAT的形式来上网的EC2实例

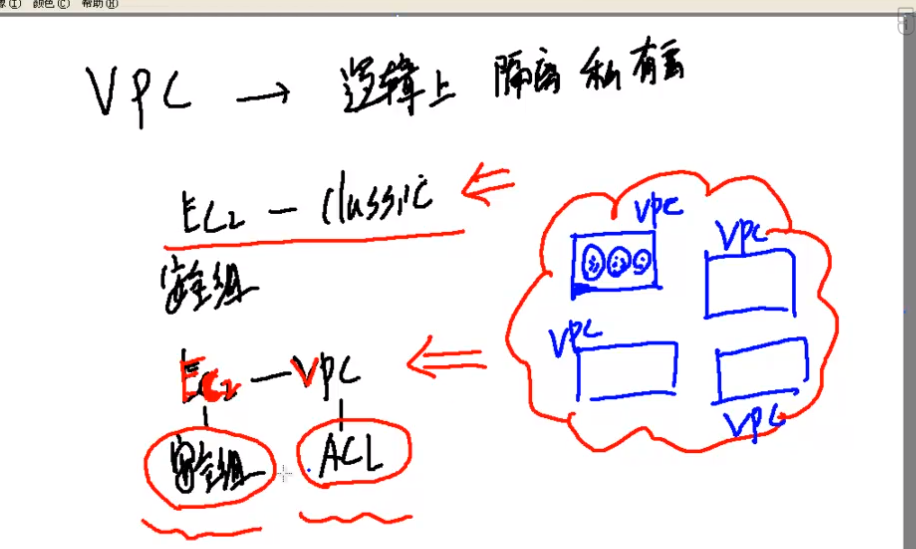
Amazon混合云

将EC2加入VPC

VPC经典

EC2 -classic 安全组





# 将EC2加入VPC

子网

路由表

网关

创建VPC

## 子网

## 子网划分

每个可用区分配一个子网，

三个可用区 a b c 分别是 192.168.1.0/24 192.168.2.0/24 192.168.3.0/24

这样每个业务可以分别使用三个可用区 做高可用

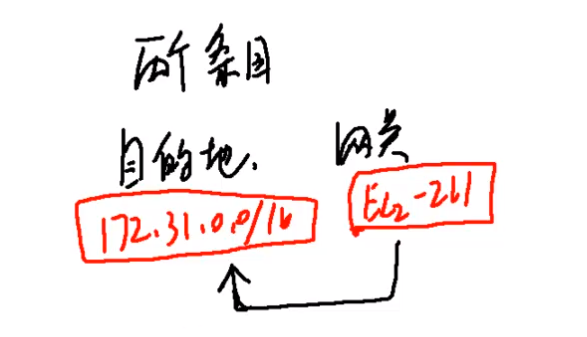
每个可用区最好都有公有子网，私有子网

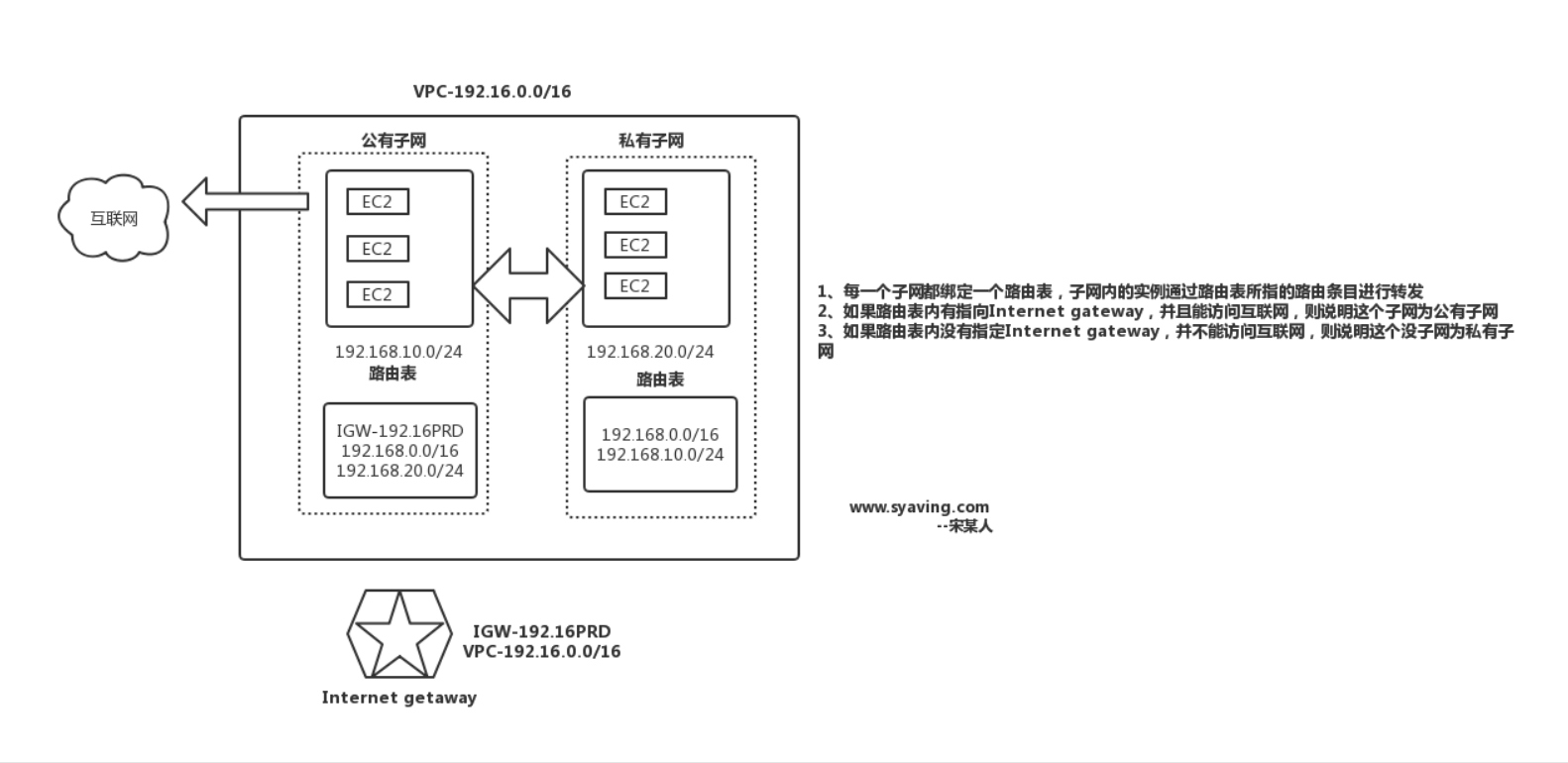
对于单一子网，如果使用IP过多，可能IP数量不够

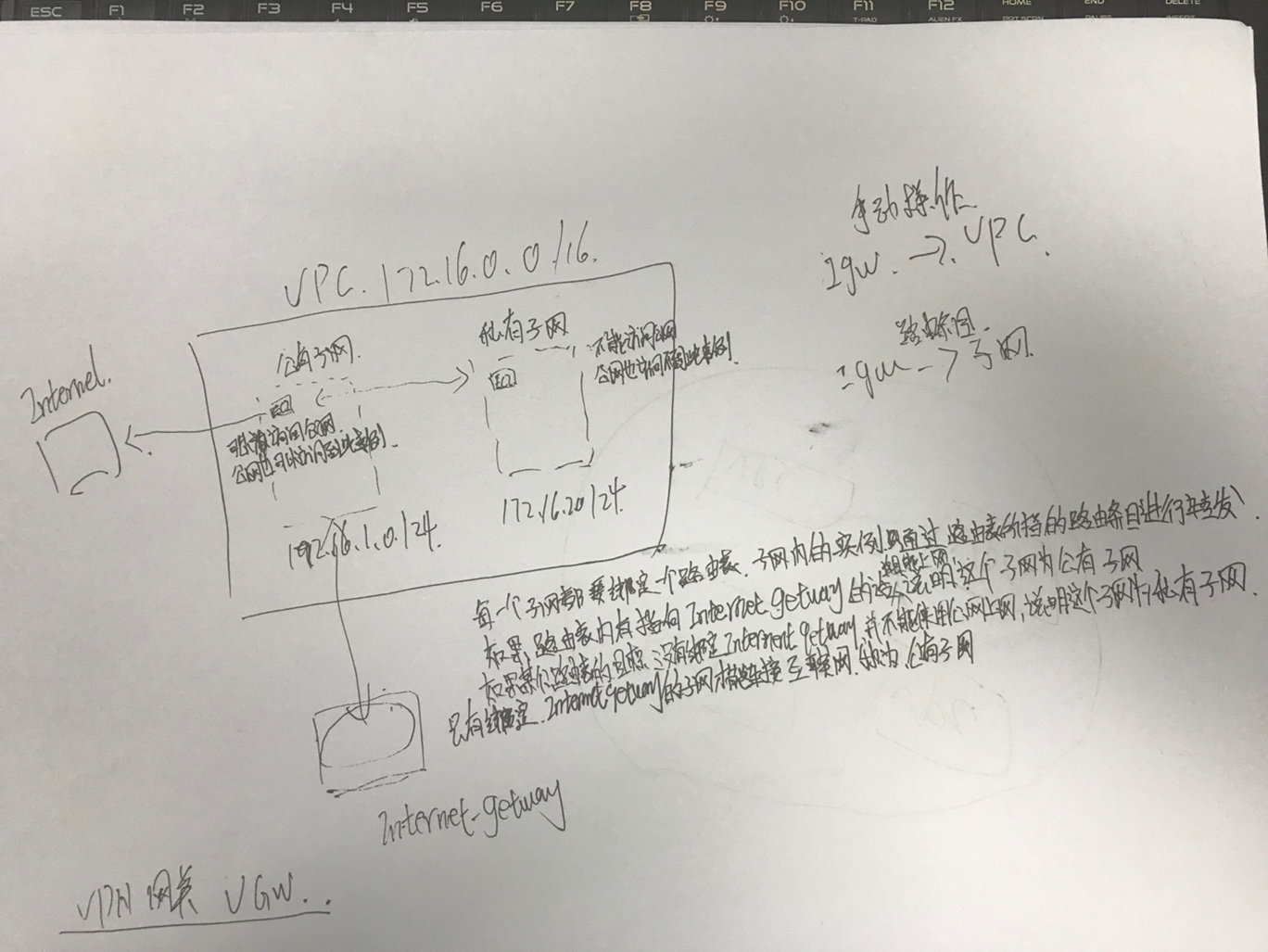
## 路由表

由两个条目构成

目的地 网关







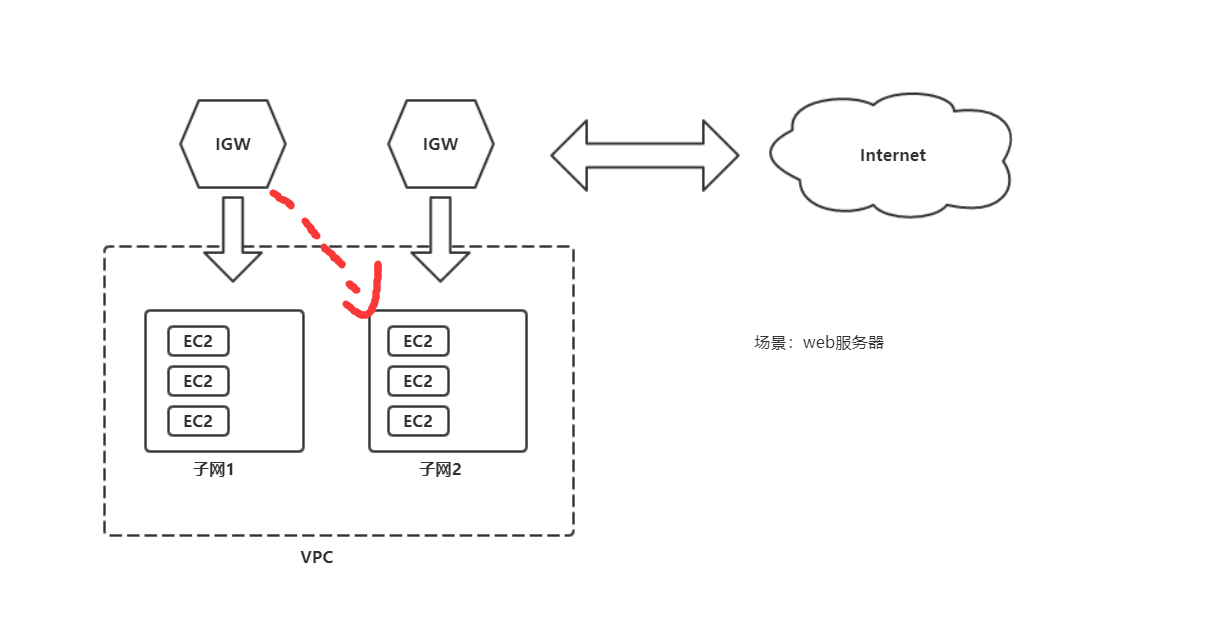
# VPC经典场景

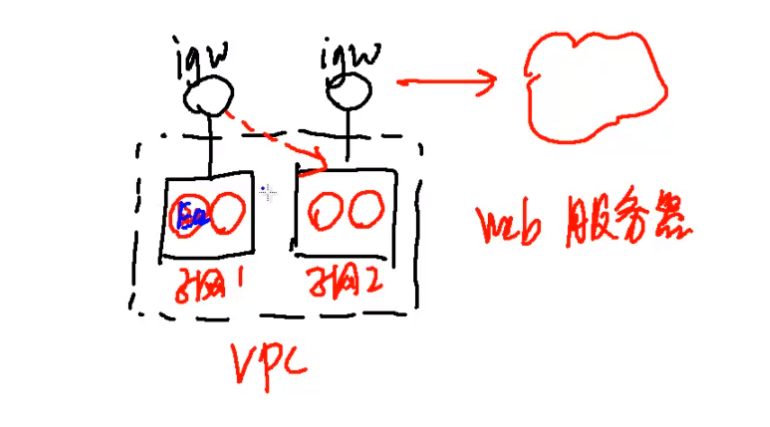
* 只有公共子网的VPC
* 有公共子网和私有子网的VPC
* 有公共子网和私有子网，且使用VPN的 VPC
* 只有私有子网的VPC

## 只有公共子网的VPC

子网内配有Internet网关

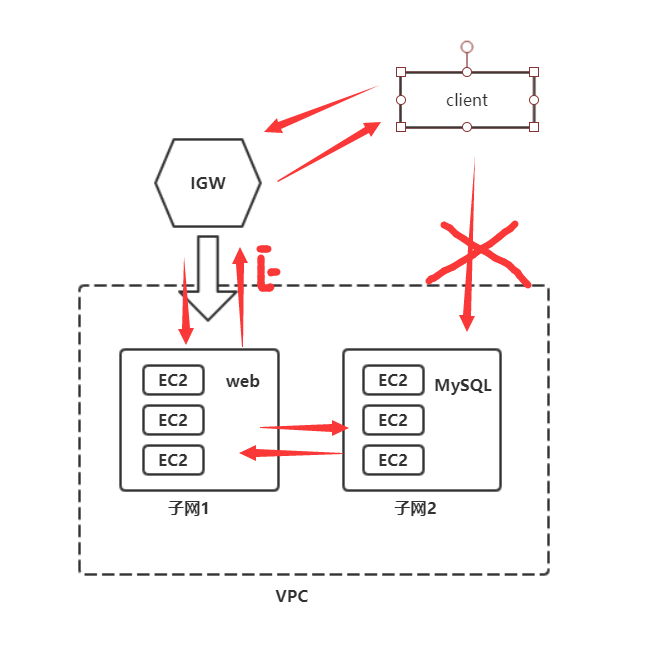
配置NAT实例，也可以访问互联网。但是有限制。实例可以访问Internet 但是Internet访问不到实例

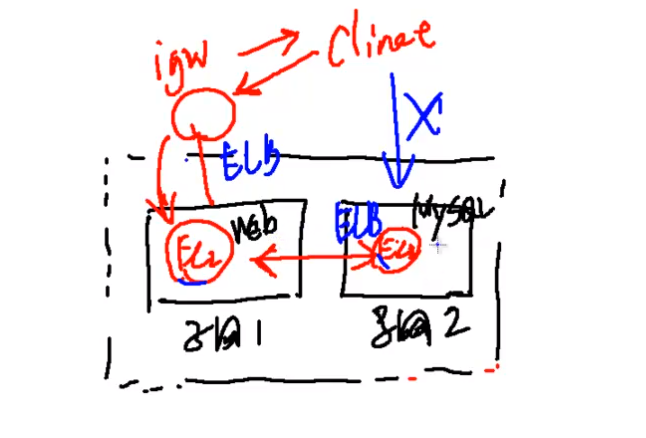




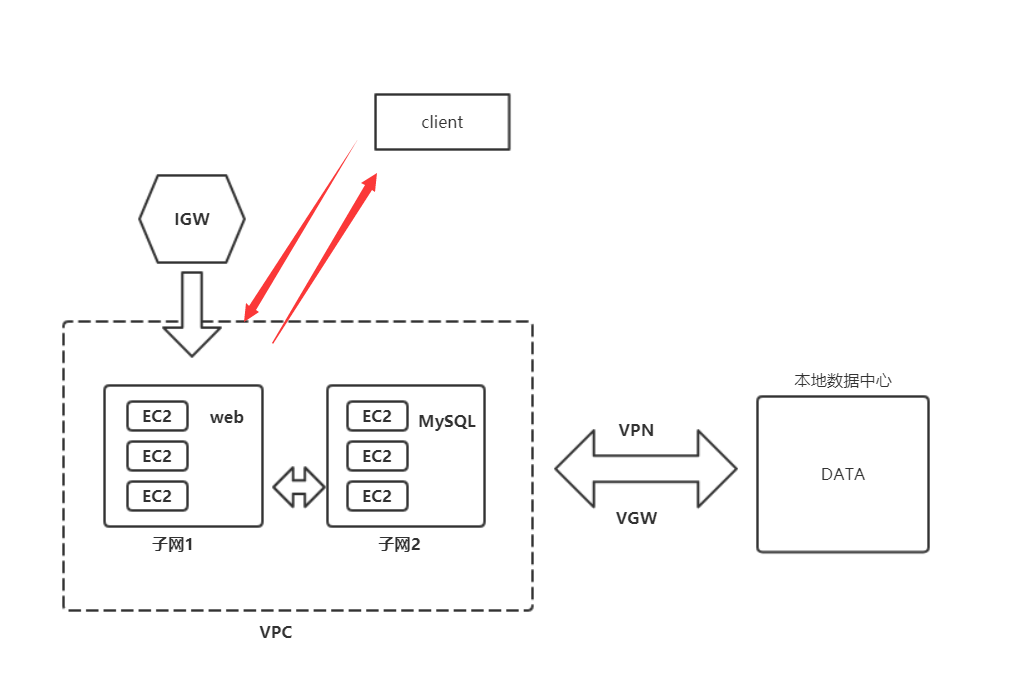
## 有公共子网和私有子网的VPC

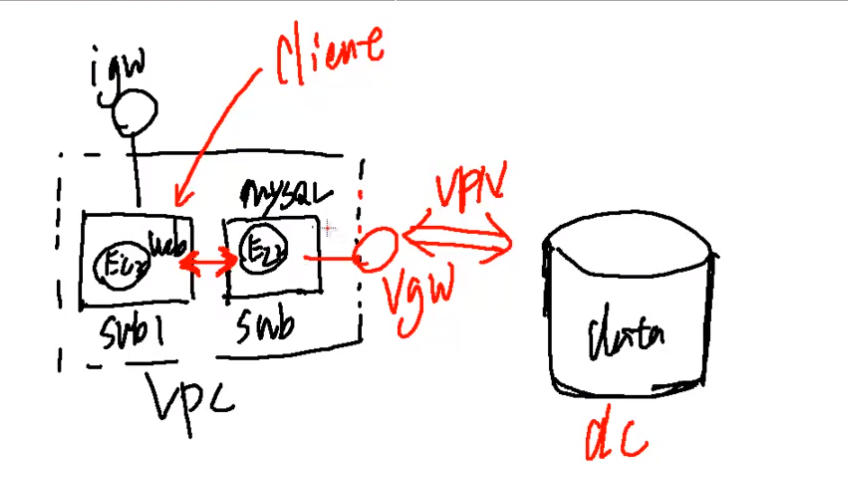
动态数据的网站



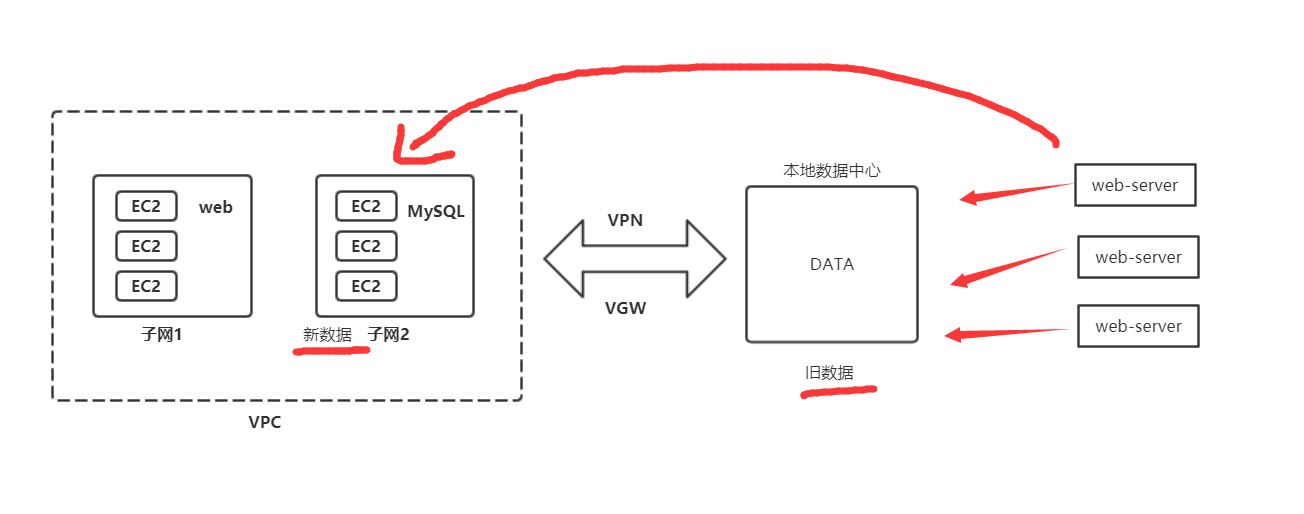


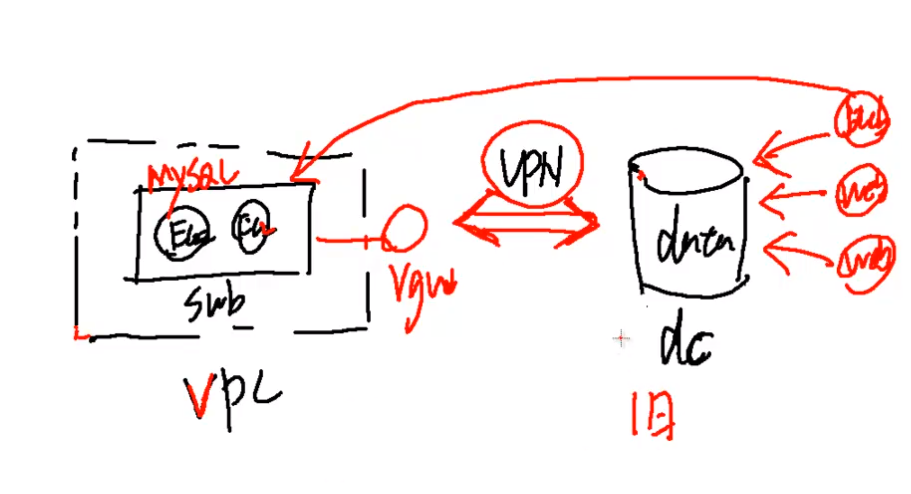
## 有公共子网和私有子网，且使用VPN的 VPC





## 只有私有子网的VPC





# 变更VPC

## 怎么把默认VPC下的实例迁移到新建的VPC中?

默认是不可以的

处理方法：

做快照 还原过去 不能直接迁

内网也不能变

创建的时候就要定好在那个子网里了

不支持虚拟机直接迁移到其他网络

那就是 vpc可以变， 里面的子网 内网 是无法改变的

AWS现在是支持更改网段地址

但是第一次分配的主网段地址

不能调

只能增加新的网段

如果想从某个子网/VPC 把机器迁到另外一个子网/VPC，就用快照还原的方式

没有直接改网络地址的方案

是的，就是增加了一个新的CIDR可以分配

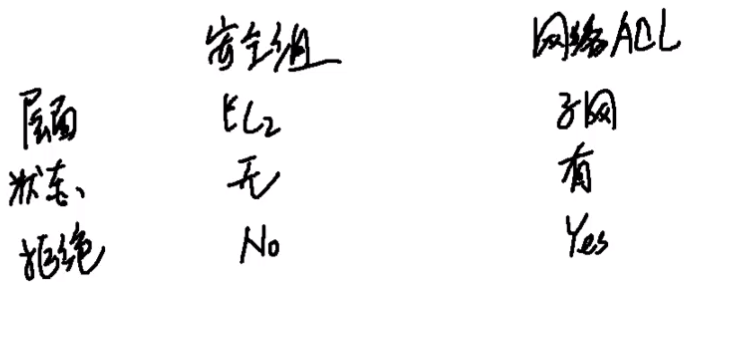
比如原来是172.0.0.0/16的VPC，你再增加一个172.1.0.0/16的网段，可以放到一个VPC里了

IP地址不会不够用了



acl跟子网结合

安全组跟实例结合



# EC2上网设置

1、如果有弹性IP的话，加上igw 才能上网

2、如果没有弹性IP，加上nat才能上网 ，设置nat的时候，nat应该绑定到公有子网上，如果绑定到私有子网是无法上网的。