1. **VPC概念**
   1. 在云概念中，我们会做计算虚拟化、存储虚拟化、网络虚拟化。

其中网络是相当重要的环节。网络的发展史从传统网络-网络虚拟化-SDN网络三步发展。

传统网络：就是一个交换机加路由器，你用手机连上WIFI。传统网络适用于物理机房里。

网络虚拟化：我们发现传统网络用在云不可能，云上好多租户，每个租户都有好多虚拟出来的计算服务器、存储服务器等等。所以这些虚拟出来的服务器本身就是虚拟的东西，它们的网络怎么连？而且租户要是都用一个网络，别人通过这个网络攻击我怎么办？所以云端每个账号是隔离。传统网络的物理隔离，一个人一台路由器，谁跟谁的网络都不同，这是最好的，但在云计算都是虚拟化的情况下，没法用。所以阿里云是逻辑隔离的，通过一些逻辑手段，租户们是可以连在一台交换机上的，但我们可以对每个租户做一些属性配置，租户间是不能互联的。

在云上，每天有千万个用户在用，而且一天少则几万，多则十几万的用户要么走了，要么新注册，我不可能天天手动的给人配置物理的传统网络，不实际。在云计算中有重要的一个概念，比如阿里云的机房里一台服务器的性能太高，你一个人租一台用不完，没关系，我帮你吧一台服务虚拟成多台，我直接从平台把虚拟机分给不同人，虚拟机各自的网络，也是通过逻辑隔离的网络虚拟化。

SDN网络：软件定义网络，我通过网络帮你定义出来不同的网络属性，这是针对云的网络定义方式。

* 1. 阿里云网络产品

专有网络VPC、负载均衡SLB、NAT网关、弹性公网EIP、VPN网关、共享带宽、共享流量包、高速通道、云托付、全球加速。

* 1. VPC介绍

网络产品中，最最重要的一个产品是VPC，是基于阿里云建立的一个隔离网络环境，专有网络之间逻辑上彻底隔离。

VPC提供了两个能力：1.用户可以自定义网络拓扑，包括选择自由IP range，划分网段、配置路由表和网关等。 2.通过专线或VPC与原有数据中心相连，云上云下使用一个网络地址规划，实现平滑上迁移云。

VPC最大的作用是做网络隔离的。VPC规划包括了IP段、网段、路由表和网关。

* 1. VPC技术

首先将网络虚拟化技术，网络虚拟化技术引入了Overlay技术和引入SDN技术。

特点：

1.VM（ecs）IP灵活分配：VMIP地址与物理网络拓扑解耦；VM的IP可以根据业务需要分配。

2.VM ip地址可以从寻址功能变为标记：承载VM虚机的物理机坏了，VM迁移时，IP地址不变；当手动迁移时，不需要配置物理交换机。

3.多租户：租户间相互隔离；租户可以自行设置安全策略

4.转发逻辑由自学习转为集中控制：OVS有控制平面同一管理；路由信息由控制器集中控制

5.消除大二层网络问题：二层网络由实变虚，不再仅仅是vlan；消除arp广播域，去除二层环路；简化VM配置，减少网络故障

**VPC的组成部分**是由私网网段、一个路由器和至少一个交换机组成。VPC中有几个组件：1.私网网段。每个VPC都要规划好私网网段，尤其是VPC之间互联时，网段规划更要注意，网段不能冲突。 2.路由器：是实现不同网络之间互通的。是私有网络的枢纽。交换机是网络之内的。路由器对外连接，交换机内部互联 3.交换机：连同同一网络下不同设备，互相通讯。4.路由表，最大的功能是为数据包转发提供依据

* 1. VPC中的一些概念

VRouter与Vswitch（路由与交换机）

路由表：**路由表**（routing table）或称**路由择域信息库**（RIB, Routing Information Base），是一个存储在[路由器](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8/108294)或者联网计算机中的电子表格（文件）或类数据库。路由表存储着指向特定[网络地址](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%9C%B0%E5%9D%80/9765459)的路径（在有些情况下，还记录有路径的路由度量值）。路由表中含有网络周边的[拓扑](https://baike.baidu.com/item/%E6%8B%93%E6%89%91/573536)信息。路由表建立的主要目标是为了实现[路由协议](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%8D%8F%E8%AE%AE/202634)和[静态路由](https://baike.baidu.com/item/%E9%9D%99%E6%80%81%E8%B7%AF%E7%94%B1/100778)选择。主要是提供数据包转发依据的。

安全组：控制内部通讯的范围，也叫虚拟防火墙。

防火墙：限定访问范围的工具。

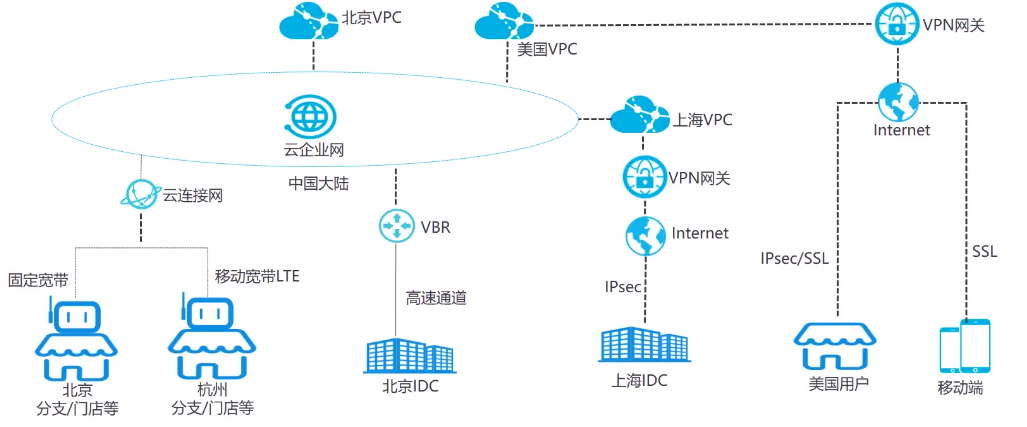
小结思考：1.VPC由哪些组件构成？

答：虚拟路由器（Vrouter）虚拟交换机（Vswitch），路由表共同构成。

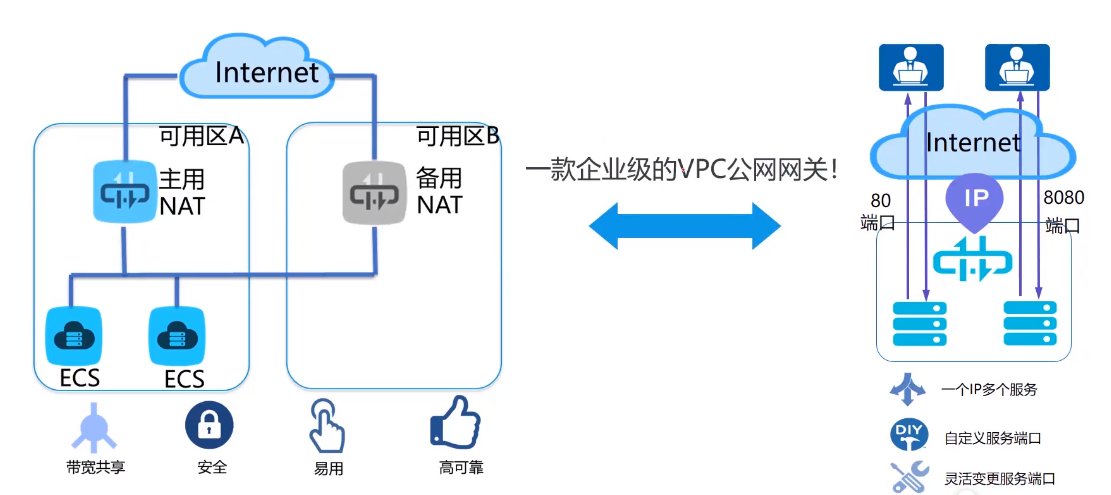
2.VPC中路由表有什么用。

为数据包转发提供依据，比如有哪儿到哪儿，应该怎么转。通过修改路由表，实现数据包的控制，比如哪些能走，哪些方向应该怎么走，限制网络连接的情况。

1. **VPC组件**
   1. 弹性公网IP（EIP）。就是可以动态绑定和解绑的，可独立持有的公网IP。特点是：一个公网IP，全球可达；优质的BGP线路和带宽，享受和淘宝、天猫同品质公网；可用于VPC中的ECS/NAT/SLB。ECS有了公网IP，才可以连接互联网。缺点是一个EIP只能给一个人用
   2. 云企业网CEN。是提供一种快速架构混合云和分布式业务的全球网络，协助用户打造一张具有企业级规模和通信能力的上云之路。最大的好处是可以把不同的VPC，都加入CEN中，这样不同的VPC就可以互通了，而且不仅可以加Vpc，还可以把专线、智能基础网关、高速都加进来，这些东西是你在家里面或公司，将网络与阿里云网络接起来。

。

* 1. VPN网关。是基于internet，通过加密通道将企业数据中心，企业办公网络，互联网终端，连接上阿里云专有网络，并符合安全可靠要求的服务。 就像在海康上班时，公司的OA/CRM/SPS等办公网站和软件，都需要在公司的WiFi或网线才能登陆，如果在外办公，则需要用笔记本的VPN输入账号密码，通过互联网连接到海康的内部网络，使用系统。 VPN分为IPsec-VPN，适用于大型公司，是企业上云用的，比如站对站的VPN连接；SSL-VPN,也就是我在海康时个人电脑上装的软件，是点对站访问。
  2. NAT网关。是共享上网用的。解决的是弹性公网IP成本太高问题，比如你有十台ECS上网，就需要买十个弹性IP，成本就高了。但如果你是企业，有很多ECS，那就买个NAT网关。好处是内部不管多少人上网，反正你只要买一个NAT网关就都可以上网了。



小结思考：可以提供阿里云中资源访问internet的网络产品有哪些，各有什么特点？

答：一个是弹性公网IP，也就是EIP， 它可是使资源上网，但缺点是一个IP只能绑定一个资源，如果共同上网时，费用会大。

第二个是NAT网关，优点是多人共同上网时，可以共享同一个IP连接互联网，可以大大节省IP地址的成本。

1. **VPC的规划与使用**
   1. **VPC的规划**

一般VPC的规划一般会考虑一下几个问题

问题一：应该使用几个VPC

问题二：应该使用几个交换机

问题三：应该使用什么网段

问题是：VPC与VPC之间，或本地数据中心如何互通

问题一思考：1.单个VPC适合简单部署，适于对网路方面没有特别多特殊需求的情况下使用； 2.是否有多地域部署系统要求，你有几个地域，则至少有几个VPC，是多VPC 3.各系统之间是否有VPC隔离的需要，比如将技术部和销售部之间的通信进行权限的限制，如果有也需要多VPC 4.多VPC之间是通过云企业网互联（**高速通道产品已经基本淘汰**）



问题二思考：1.尽量使用至少两台，并且每台交换机部署在不同可用区下 2.应用的不同部分使用不同交换机，比如前端服务和数据库服务使用不同交换机。

问题三思考：1.规划VPC网段：在云上只有一个VPC且不需要和本地IDC互联时，可选择私网网段中任意一个网段或子网；但如果云上有多个VPC，或者VPC与本地IDC是混合云架构时，建议使用上面这些标准网段的子网作为VPC网段，掩码建议不超过16位。 2.规划交换机网段：交换机的网段大小在16位到29位网络掩码之间，可提供8-65536个地址；每个交换机的第一个和最后三个IP地址为系统保留地址 （也就意味着如果有是个ECS需要上网，需要规划14个地址因为有4个是系统自留不让用的）；交换机网段的确定还需要考虑交换机下ECS的数量。

问题四思考：1.当用户有VPC互通或本地IDC互通需求时，确保VPC网段与互通的网络的网段不冲突；2.在多VPC情况下，建议遵循以下规则：尽可能做到不同VPC的网段不同，不同VPC可以使用标准网段的子网段增加VPC可用网段；如果不能做到不同VPC网段不同，则必须做到不同交换机网段不同。

* 1. **VPC使用常见问题**
     1. 每个VPC可以有多少个路由器? 每个VPC有，且只能有一个路由器，每个路由维护一个路由表。
     2. 如何选择交换机网段？交换机的网段必须遵守从属VPC的网段，如果交换机网段和从属VPC网段相同，VPC内就只能创造一个交换机。 阿里云VPC提供了192.168.0.0/16，172.12.0.0/12，10.0.0/8以及它的子网供用户使用。



小结思考：规划VPC时至少使用几台交换机，为什么？

答案：至少是两个。而且不同交换机需要放在同一region的不同的zone下，可以提高SLB的性能，包括有效防止可用区故障导致的单点故障。

1. **VPC的管理**
   * 1. VPC的访问控制

安全组：虚拟防火墙，具备状态检测保过滤功能。安全组用于设置单台或多台ecs的网络访问控制，它是重要的网络安全隔离手段，用于云端划分安全域。

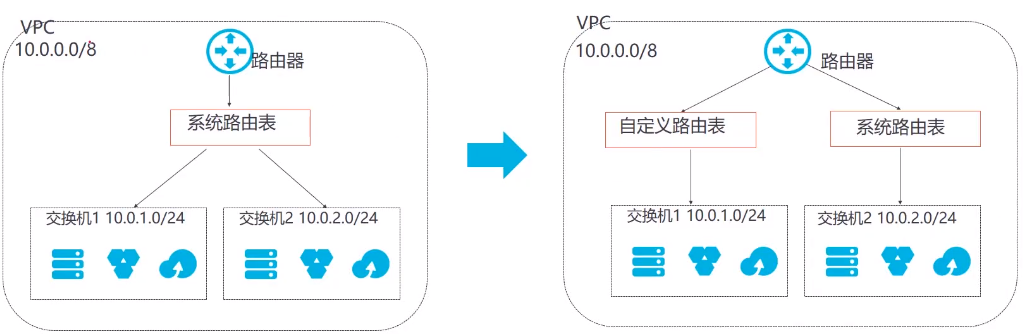
安全组是逻辑上的分组，他是同一Region内具有相同安全需求并且相互信任的ecs组成。每个ecs至少一个安全组。同一安全组内，默认实例互通；不同安全组之间，默认不互通。但可以手动授权两个安全组之间相互访问。

特别注意：安全组应该是白名单，所以需要尽可能最少的开放和暴露端口，以及配置公网IP。

安全组分为入方向和出方向，如果访问控制设置冲突时，优先级高的一方生效；如两方优先级一样，则“拒绝”规则生效。

* + 1. VPC的路由管理

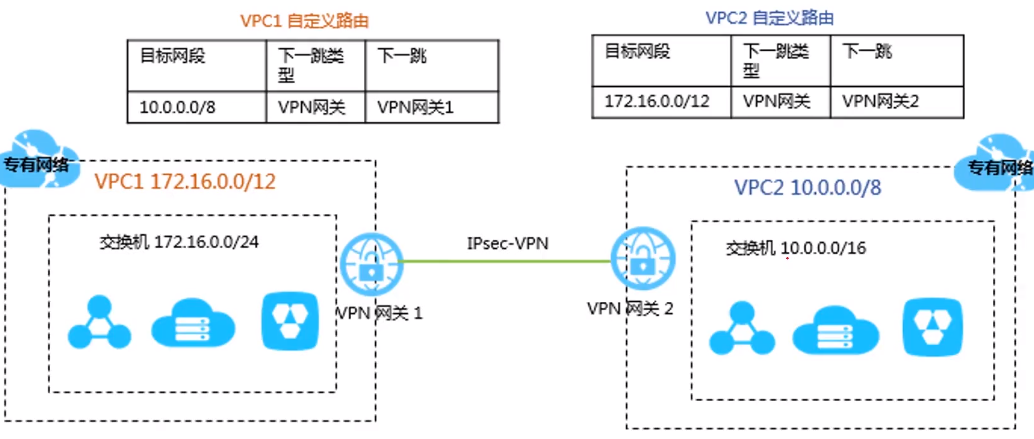
创建VPC后，系统会自动为用户创建一个默认的路由表，并为其添加系统路由来管理专有网络的流量。一个VPC有且只有一张路由表和路由器，用户不能手动创建或删除默认路由表。但可以自己添加自定义路由表。



路由表在专有网络管理控制台，单机路由表，选择地域，点击管理或点击路由表的ID连接，进行操作。

* + 1. VPC的互联

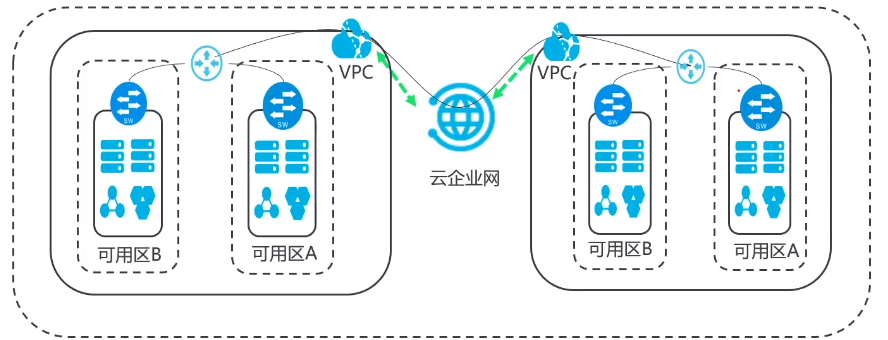
**互联方式一**：**VPN网关** 适用场景，在公司里面或出差时自己电脑拨号，连接到阿里云。两个VPC互联。



多个VPC的互联时，需要给每个VPC购买一个VPN网关，两个VPC之间通过VPN网关拨号连接。

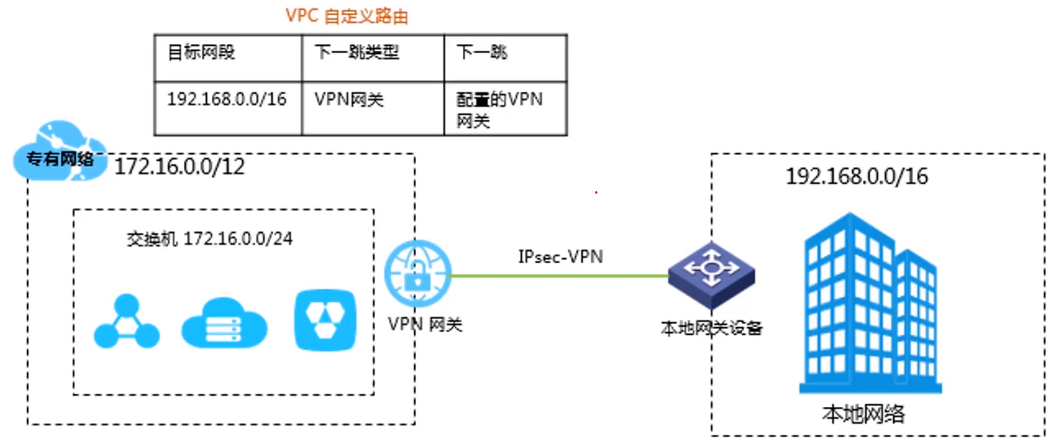
**互联方式二：云企业网 （主推）**

云企业网(Cloud Enterprise NETwork，CEN)。在VPC之间或VPC与本地IDC之间，搭建私网通信通道，通过自动路由分发及学习，提高网络的快速收敛及跨网络通信的质量和安全性，实现全网资源的互通。



最大的好处是解决VPN网关可以让两个VPC互联，但当有3个以上VPC时，VPC是点到点的，建议用云企业网后，路由表是自动选取自动分发的，把VPC加进来后，VPC直接互相连接。

**互联方式三：本地网络连接阿里云VPC 建议用VPN网关**



适用于公司里面的IDC通过拨号，连接到阿里云当中。直接在阿里云购买VPN网关，本地购买网关设备。需要在阿里云VPN网关中，指定一个路由，路由目的地是你公司的内网；之后在公司的网关设备上完成网关的指派。这样就可以实现地与云的互通。

小结思考：VPC之间的安全如何规划？ 安全规划主要是白名单的功能，是虚拟防火墙，实现的之间的一些连接，利用安全组的方式，实现访问的限制。安全组内部是可以相互访问，安全组之间则需要通过手动设置。