阿里云云计算ACP认证培训

网络与VPC

为了无法计算的价值 | 阿里云

课程目标

学完本课程，您将能够：

了解专有网络VPC的产生背景以及优势；

了解专有网络VPC及相关组件的概念和使用方法；

掌握专有网络VPC的使用场景和最佳实践。

目录

网络与VPC背景

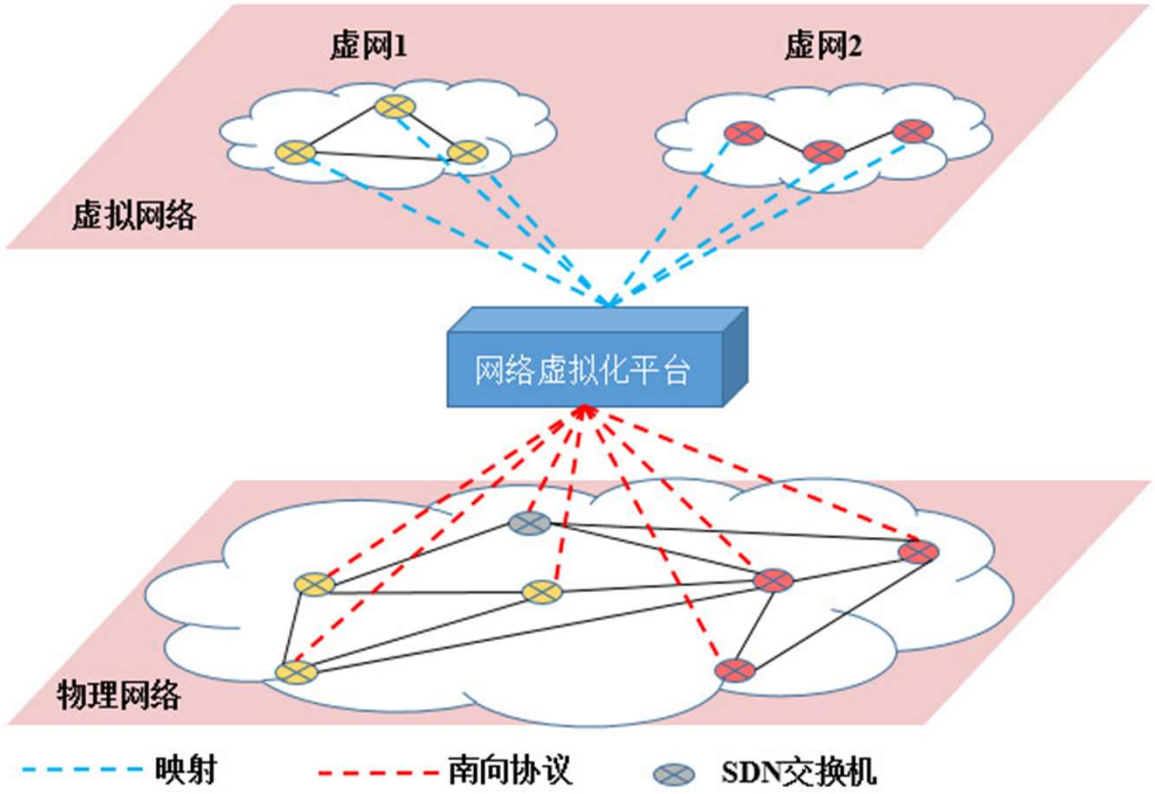
传统网络

↓

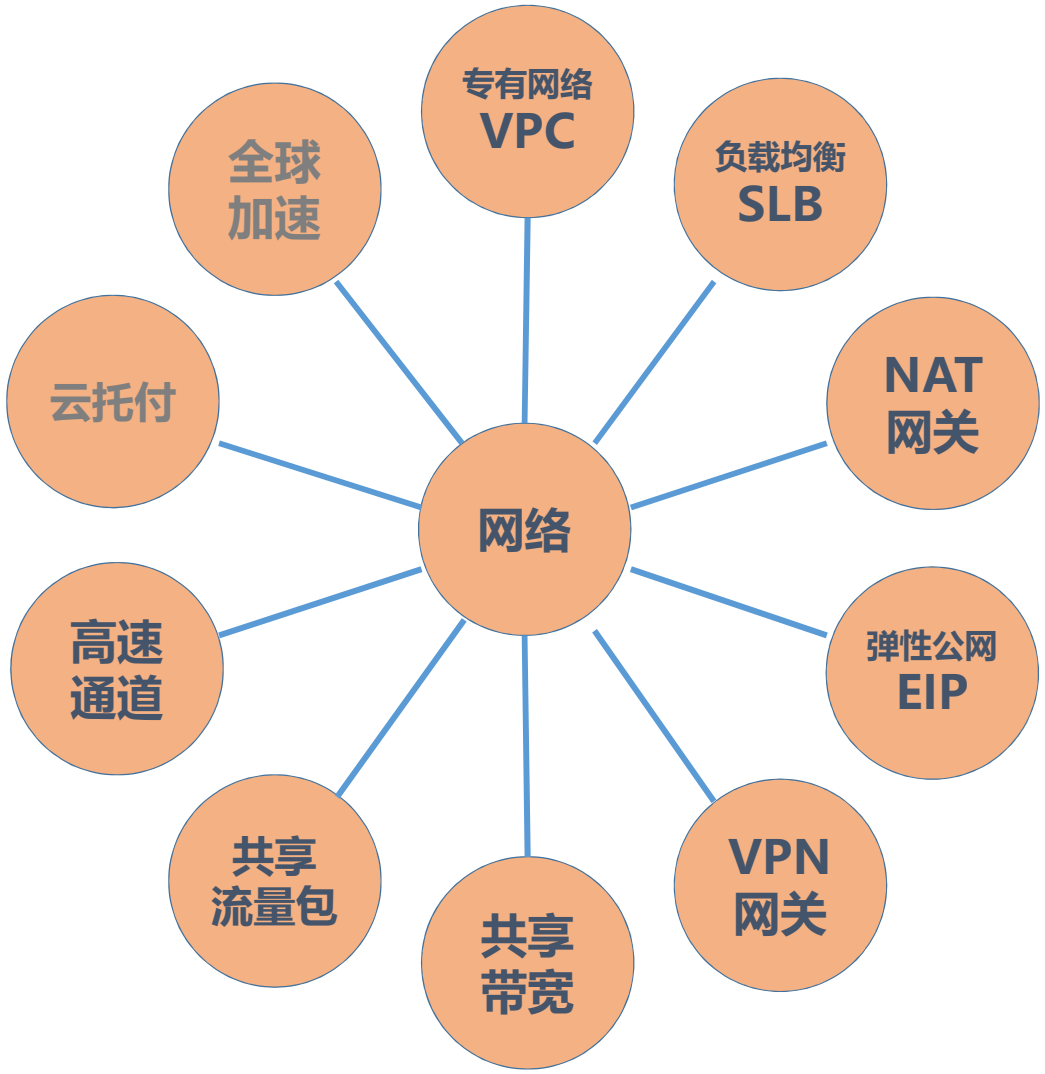
网络虚拟化

↓

SDN网络

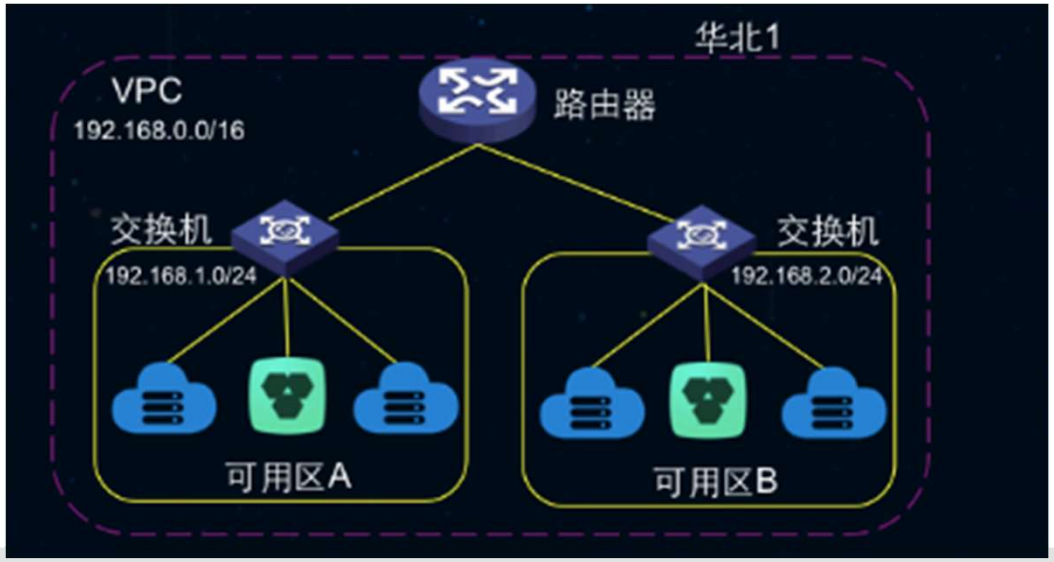


网络产品概览

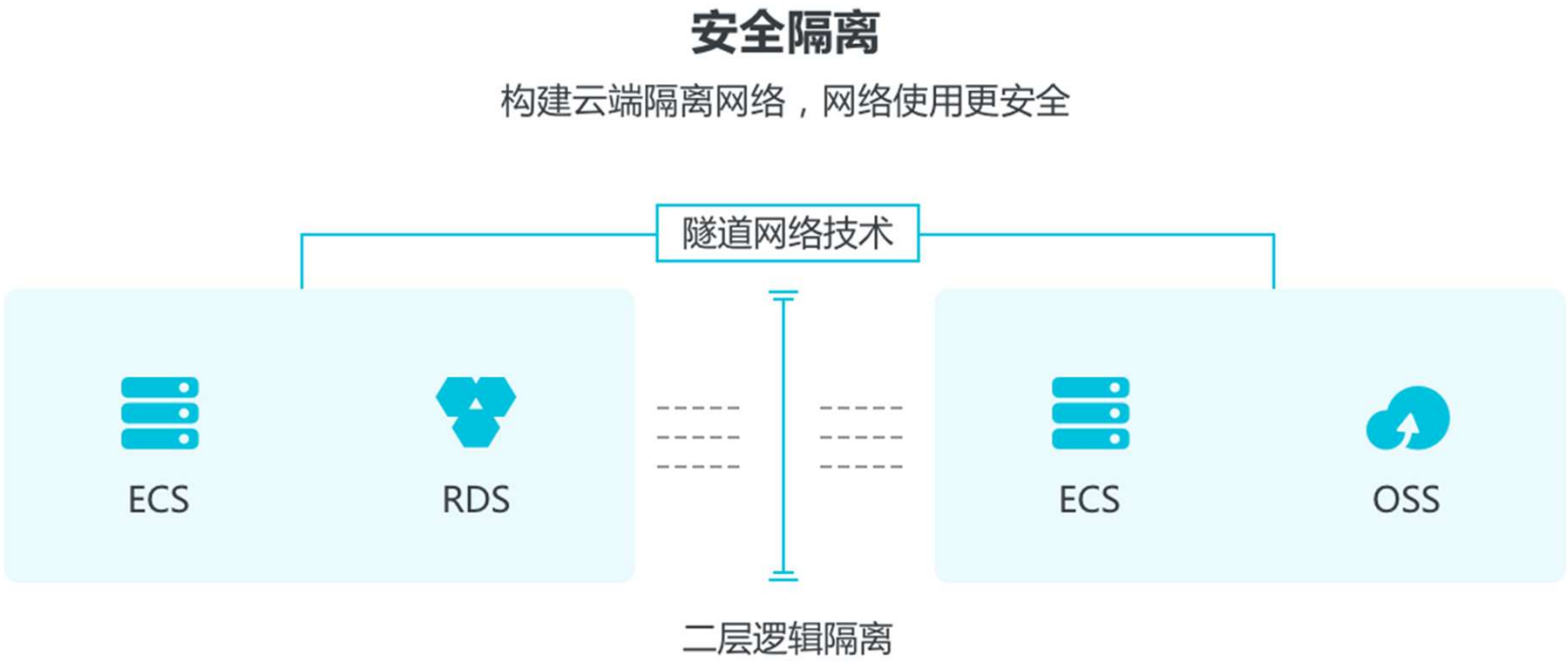

网络
专有网络
VPC
负载均衡
SLB
NAT
网关
弹性公网
EIP
VPN
网关
共享
带宽
共享
流量包
高速
通道
云托付
全球
加速

专有网络VPC

- 专有网络VPC（Virtual Private Cloud）是基于阿里云构建的一个隔离的网络环境，专有网络之间逻辑上彻底隔离。VPC 主要提供了两个能力：
- 用户可以自定义网络拓扑，包括选择自有 IP 地址范围、划分网段、配置路由表和网关等；
- 通过专线或VPN与原有数据中心连接，云上和云下的资源使用同一个网络地址规划，实现应用的平滑迁移上云。



专有网络VPC特点



专有网络VPC特点

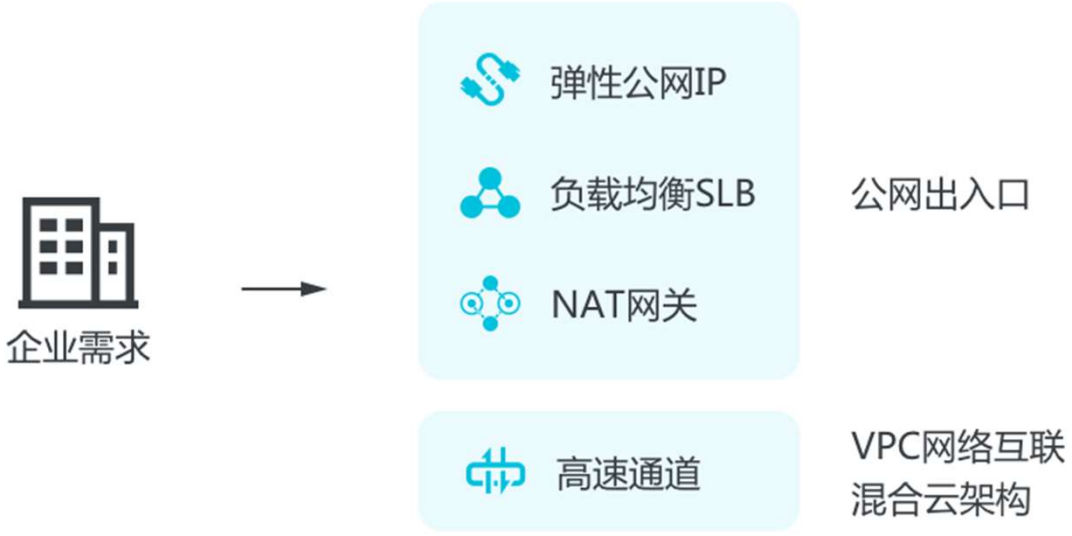
灵活

自主网络规划管理，灵活掌控网络部署

专有网络VPC特点

易扩展

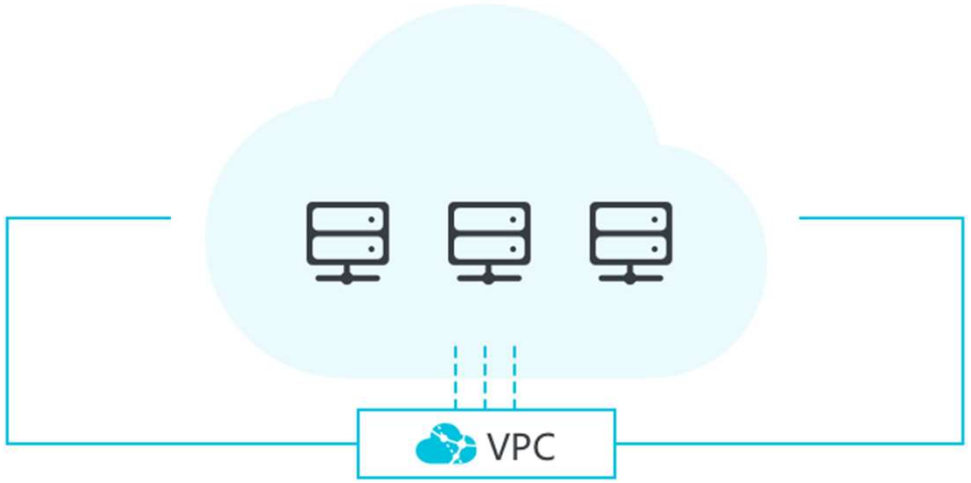
使用NAT网关可管理公网出入口，结合高速通道实现混合云架构



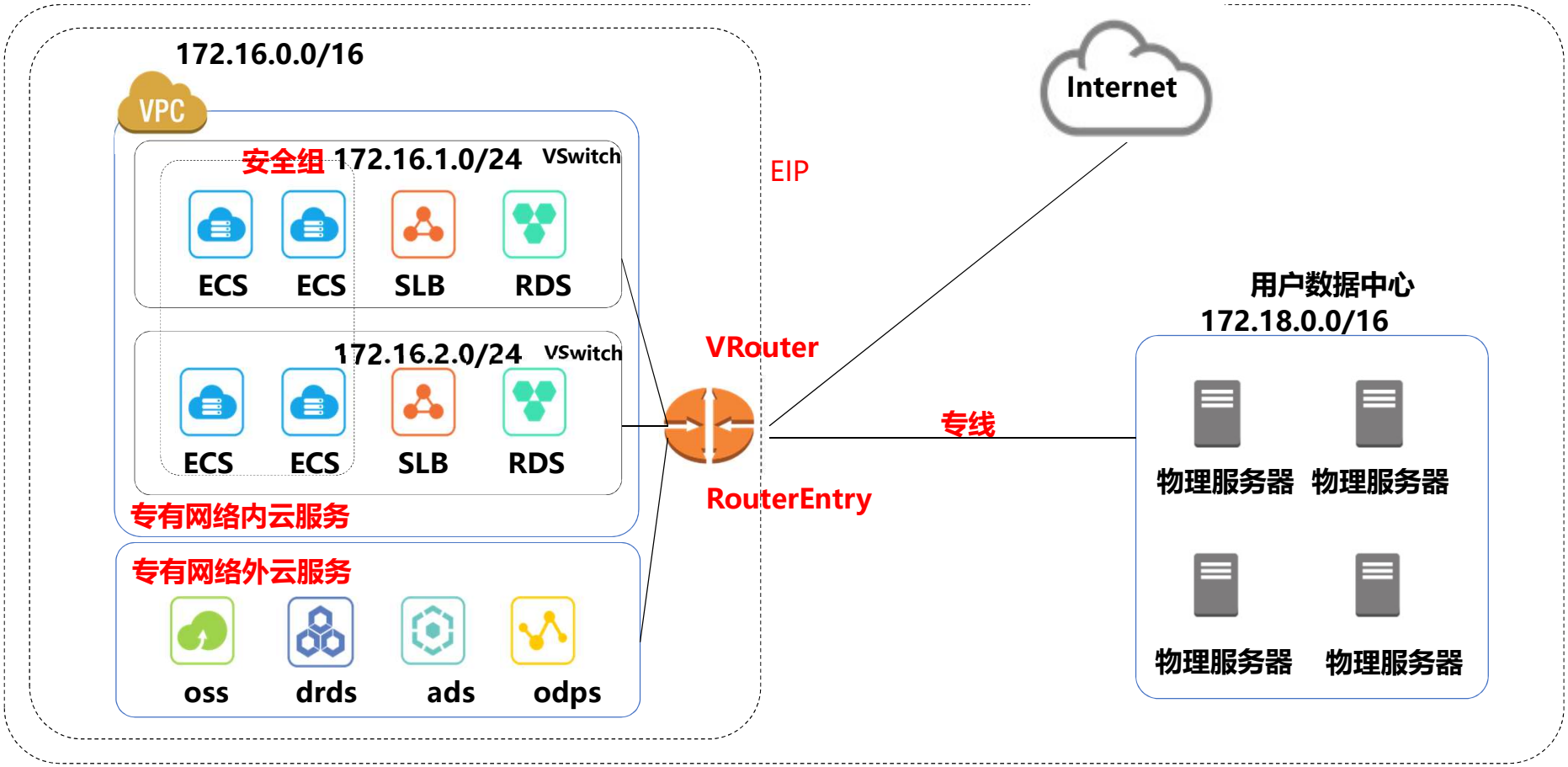
专有网络VPC特点

完全免费

完全免费，体验云上专有网络

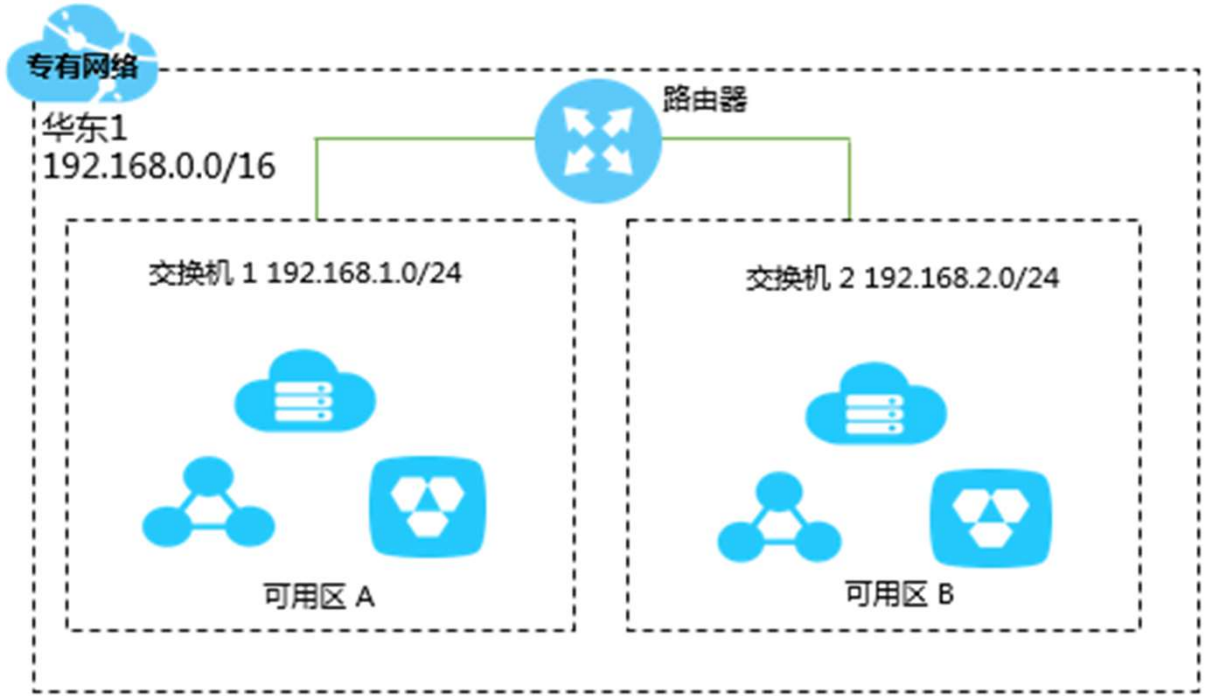


专有网络VPC产品架构



路由器与交换机

- 路由器和交换机是VPC的两个基础组件



- 路由器（VRouter）可以连接VPC内的各个交换机，同时也是连接VPC和其他网络的网关设备。
- 每个专有网络创建成功后，系统会自动创建一个路由器。每个路由器关联一张路由表。
- 交换机（VSwitch）是组成专有网络的基础网络设备，用来连接不同的云产品实例。

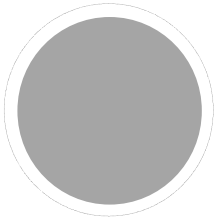
路由表与路由条目

路由表

创建专有网络时，系统会为该专有网络自动创建一个路由器和一张路由表

选路规则

路由表采用最长前缀匹配原则作为流量的路由选路规则。

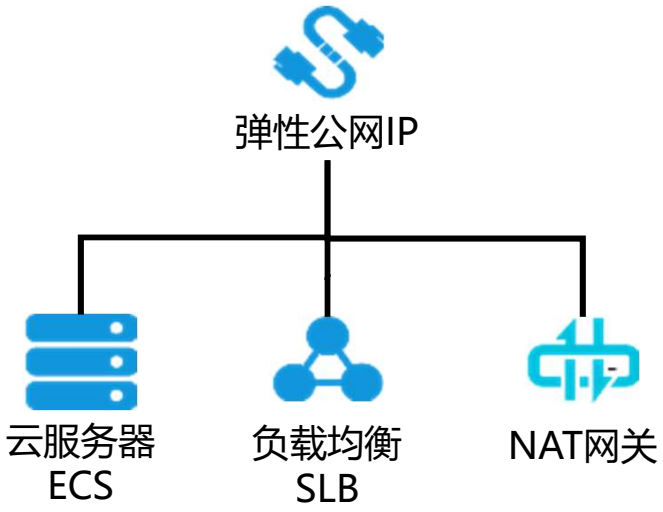


路由条目

路由表中的每一项是一条路由条目，路由条目指定了网络流量的导向目的地，由目标网段、下一跳类型、下一跳三部分组成。路由条目包括系统路由和自定义路由；

弹性公网IP

弹性公网IP（Elastic IP Address，简称EIP），独立的公网IP资源，可以绑定到阿里云专有网络VPC类型的ECS、NAT网关、私网负载均衡SLB上，并可以动态解绑，实现公网IP和ECS、NAT网关、SLB的解耦，满足灵活管理的要求。



灵活

独立的公网IP资源，可以灵活地对ECS、NAT网关、私网负载均衡SLB绑定和解绑

高可用

基于高可用的底层架构实现，无单点故障，并支持跨可用区容灾

低成本

支持按使用流量付费，包年包月价格更优惠

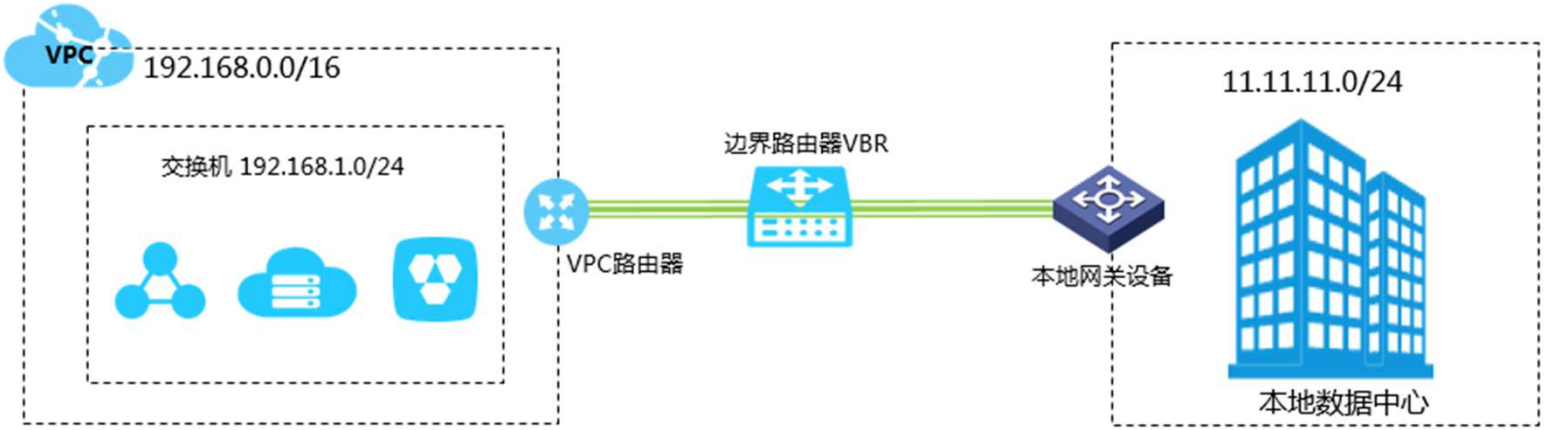
简单

开通即用，带宽变更实时生效

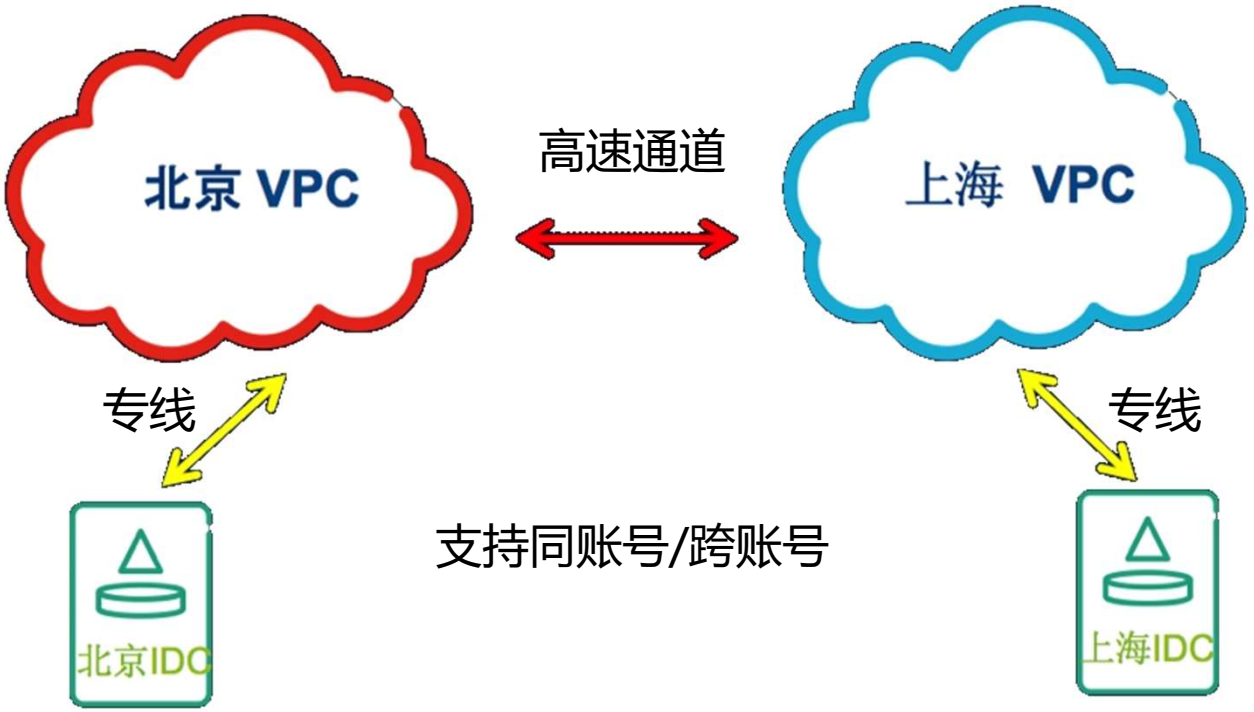
高速通道

高速通道是一款为用户提供网络互连能力的产品，为用户实现高速、稳定、安全的私网互通。

高速通道可实现云下IDC接入阿里云、IDC与云上VPC互通以及云上VPC之间跨地域互通的能力。

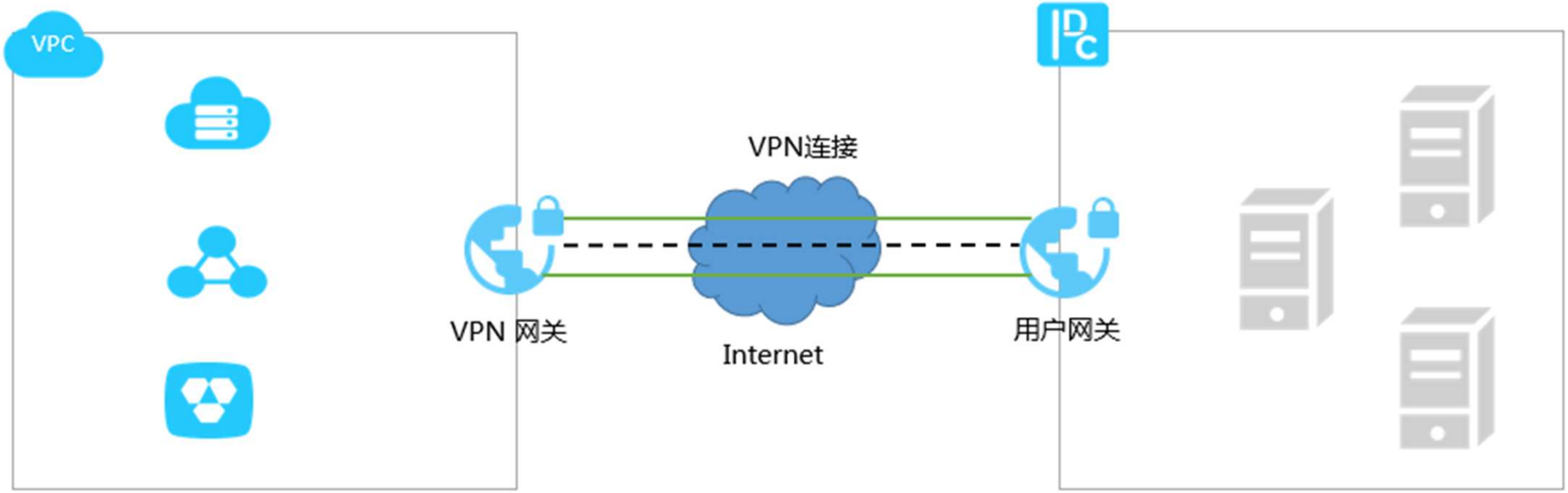


高速通道应用场景



VPN网关

VPN网关（VPN Gateway）是一款基于Internet，通过加密通道将企业数据中心、企业办公网络、或internet终端和阿里云专有网络（Virtual Private Cloud）安全可靠连接起来的服务。



注意：阿里云VPN网关在国家相关政策法规内提供服务，不提供访问Internet功能。

高速通道与VPN对比

比较点	使用公网打通VPC通信	使用高速通道打通VPC通信
通信质量与可用性	远距离公网通信质量受各种因素影响，时延稳定性、丢包率难以保证。	阿里云优质基础设施为更好的链路质量和可用性提供保障： •保证时延抖动不超过20% •保证封包成功率不低于99.8% •可用性不低于99.95 % •丢包率低于0.2%
成本	使用公网进行通信需要支付昂贵的公网流量费用或者带宽费用。	跨地域之间带宽费用相对低廉。 同地域之间VPC互连免费。
安全性	通过公网传输存在被监听窃取的风险。	基于阿里云虚拟网络技术实现，不同通信链路相互隔离，安全性高。

NAT网关

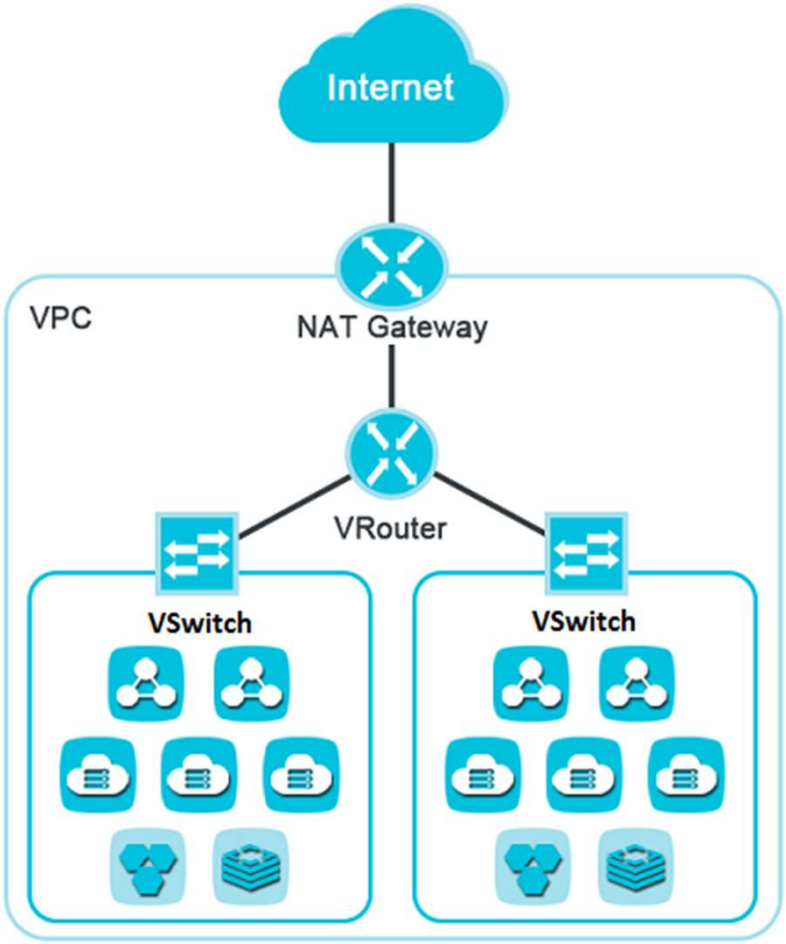
NAT网关（NAT Gateway)是一款企业级的VPC公网网关，提供SNAT和DNAT功能，支持多IP，支持共享带宽，具备TGbps级别的集群转发能力和Region级别的高可用性（跨可用区的容灾）。

灵活易用的转发能力

高性能

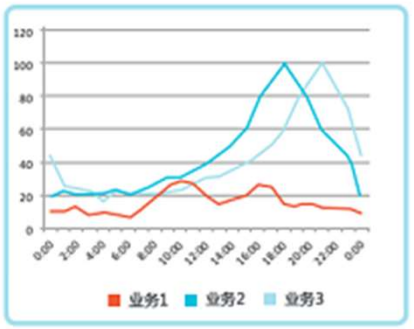
高可用

共享带宽



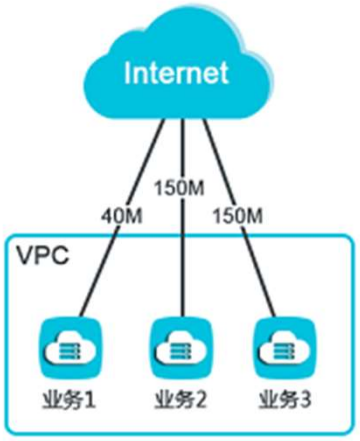
共享公网带宽

各自购买公网宽带

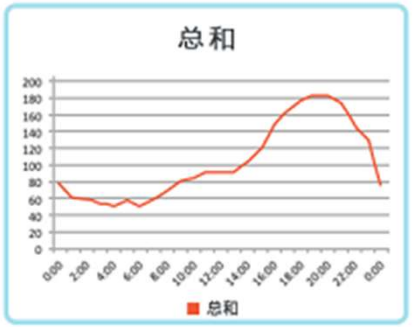


- 业务1：峰值30 MB，峰值出现时间不稳当；
  为了应对可能的突发高峰，要购买40 MB的带宽。
- 业务2：峰值100 MB，出现在18:00左右；
  为了应对突发高峰，要购买150 MB的带宽。
- 业务3：峰值100 MB，出现在21:00左右；
  为了应对突发高峰，要购买150 MB的带宽。

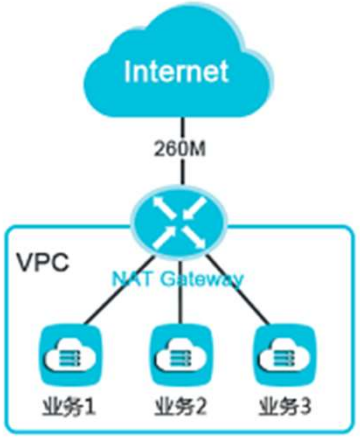
总计需要购买340 MB的带宽。



用NAT网关来共享带宽

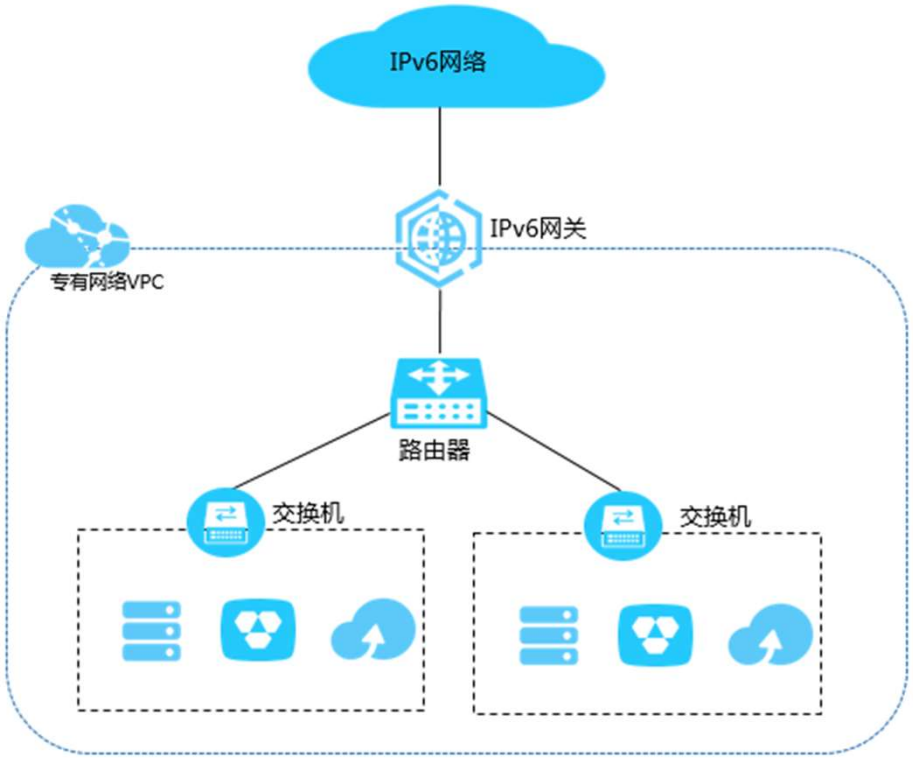


- 在共享带宽模式下，
  三个业务的总计峰值约为180 MB。
- 考虑到可能的流量高峰，
  购买一个260 MB的共享带宽包就可满足业务需要。



IPV6网关

- IPv6网关（IPv6 Gateway）是专有网络（VPC）的一个IPv6互联网流量网关。
- 您可以通过配置IPv6互联网带宽和仅主动出规则，灵活定义IPv6互联网出流量和入流量。



- **高可用：**IPv6网关提供跨可用区级的高可用能力，帮您打造极致稳定的IPv6公网网关服务。
- **高性能：**单个IPv6网关实例可提供万兆级吞吐量，满足超大业务IPv6公网需求。
- **灵活管理公网通信：**您可以通过调整公网带宽和设置仅主动出规则，灵活设置IPv6地址的公网访问权限。

设置EIP网卡可见模式

- 弹性公网IP本质上是一个NAT IP。
- 由于普通模式（NAT模式）下的公网IP存在于网关设备，并不在ECS实例的网卡上，所以在操作系统内看不到公网IP，只能看到网卡上的私网IP。
- **EIP网卡可见模式**功能使EIP在网卡上可见，解决了上述问题：
  - EIP替换辅助弹性网卡的私网IP，辅助弹性网卡将变为一个纯公网网卡，私网功能不再可用。
  - EIP在操作系统内部的弹性网卡上可见，可直接通过**ifconfig**或**ipconfig**获取网卡上的公网IP地址。
  - EIP可支持全部IP协议类型，支持FTP、H.323、SIP、DNS、RTSP、TFTP等协议。

目录

VPC的网络规划

问题一，应该使用几个VPC?

问题二，应该使用几个虚拟交换机?

问题三，应该选择什么网段?

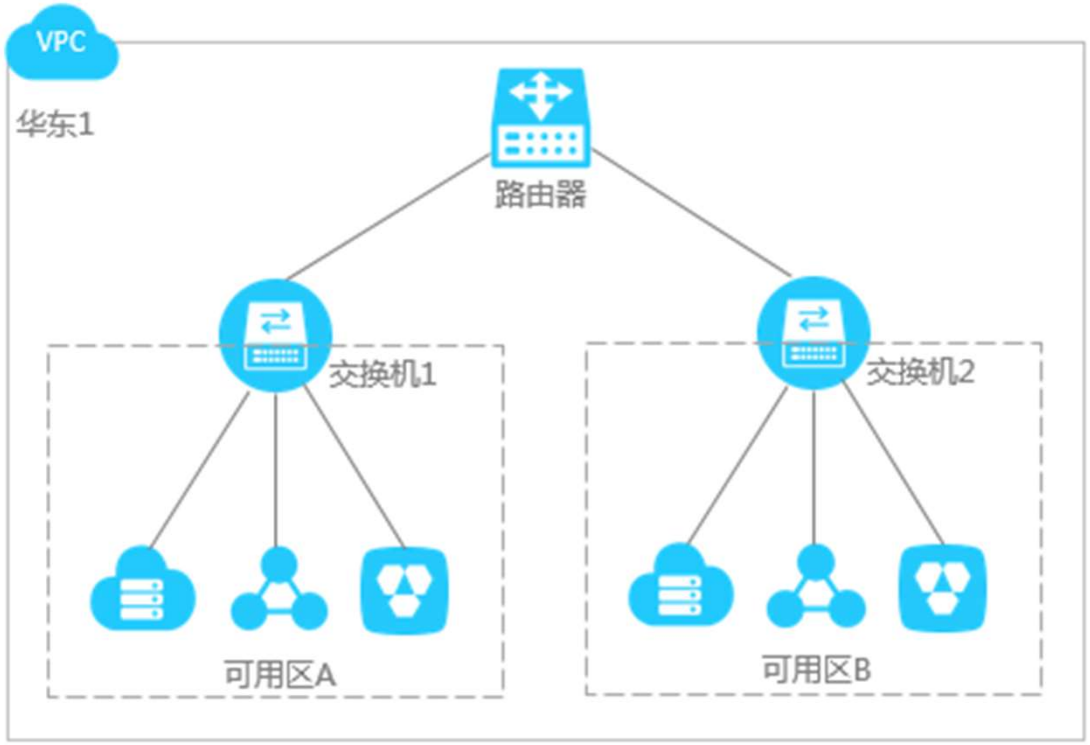
问题四，考虑一个比较复杂的业务系统，云上存在多个VPC且需要和云下IDC互通，如何规划网段?

网络规划--我应该使用几个VPC?

- 单个VPC

1）没有多地域部署系统的要求

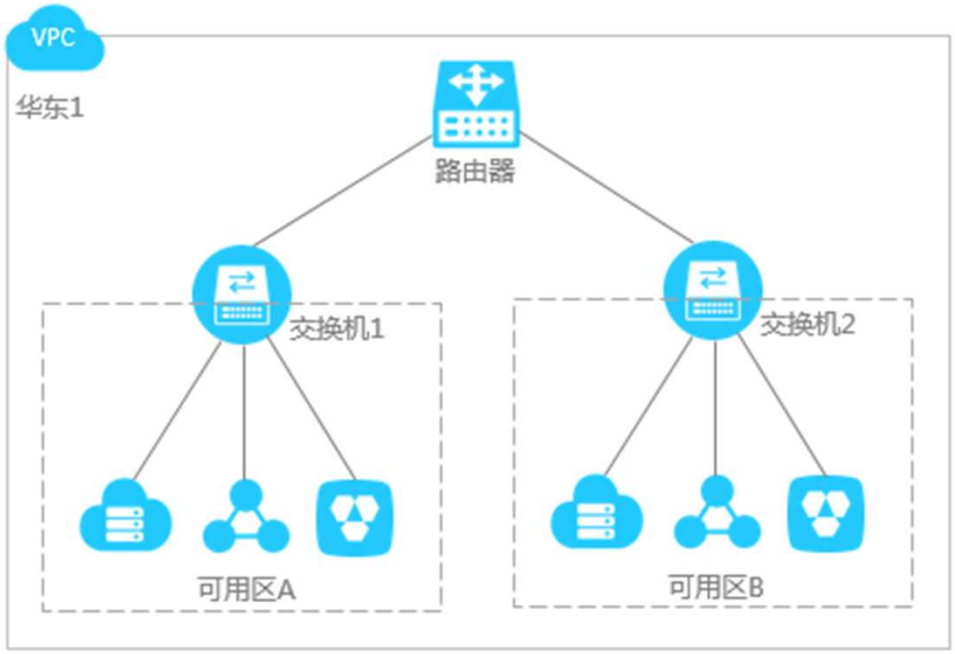
2）各系统之间也不需要通过VPC进行隔离

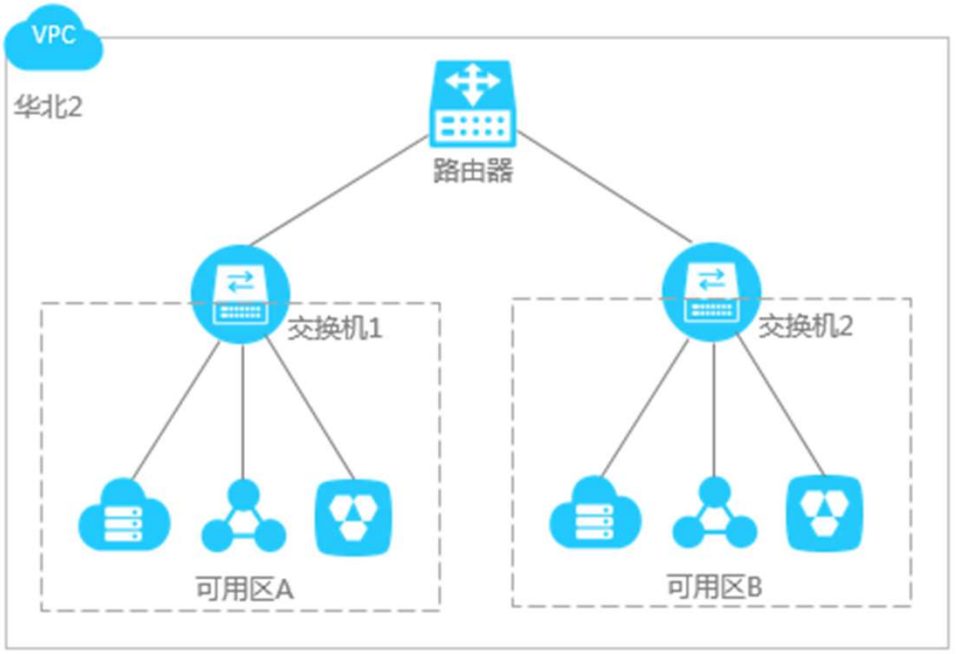


网络规划--我应该使用几个VPC?

- 多个VPC

多地域部署系统

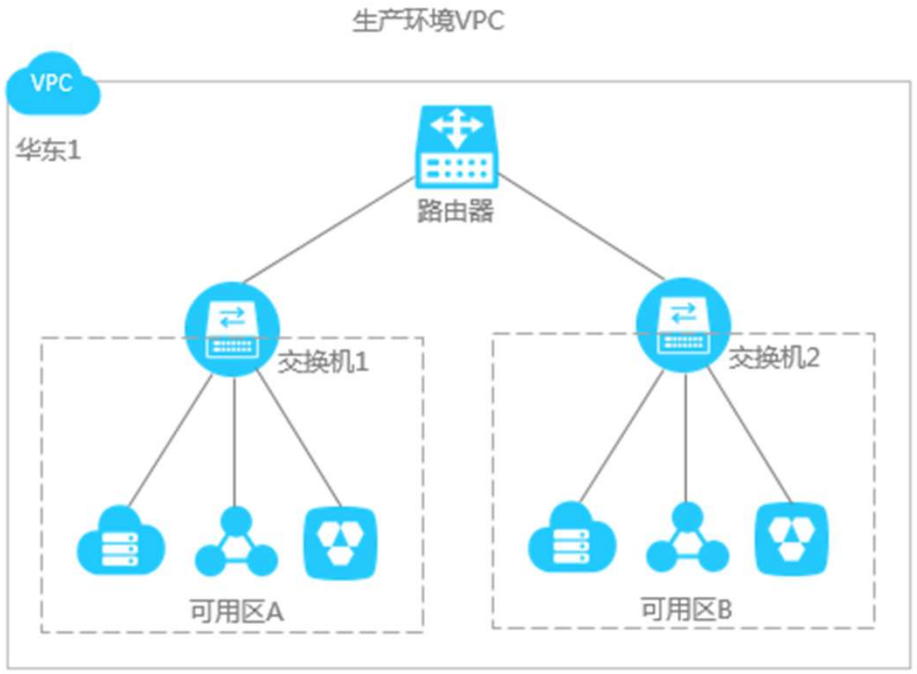


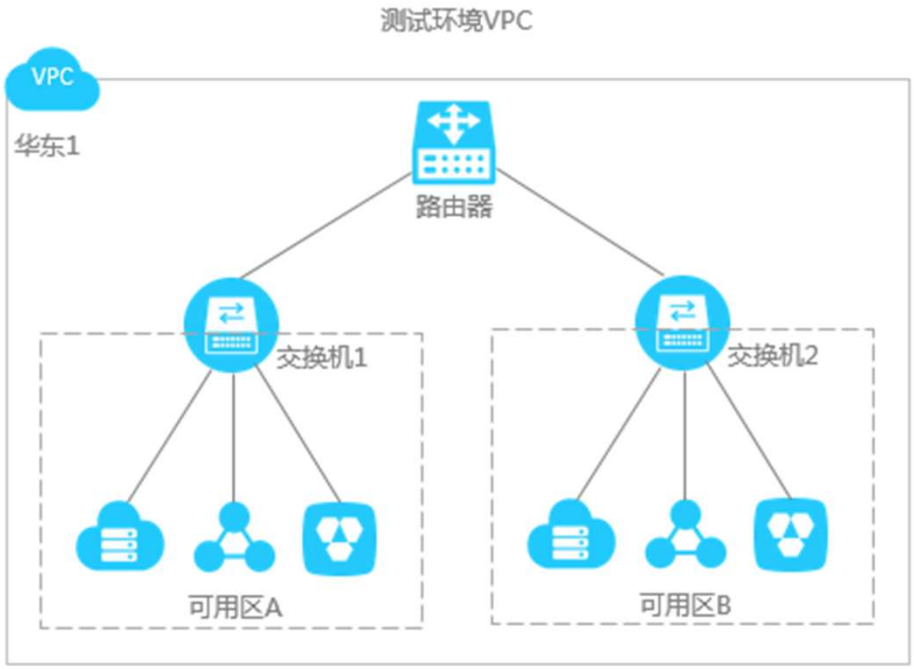


网络规划--我应该使用几个VPC?

- 多个VPC

多业务系统隔离

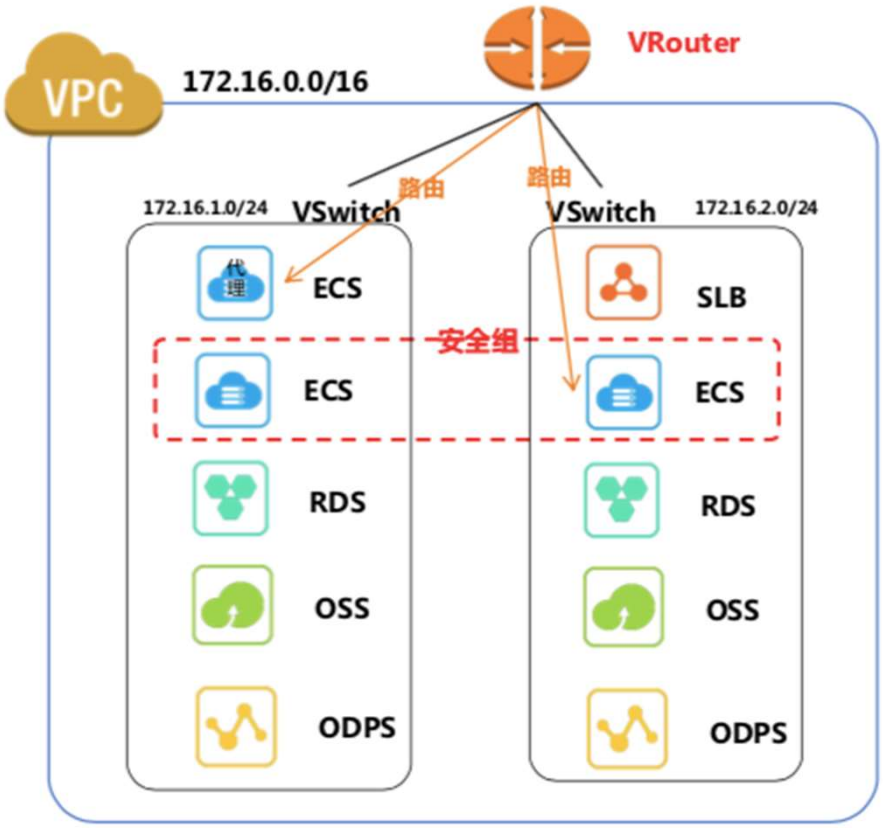




网络规划--应该使用几个虚拟交换机?

- 即使只使用一个VPC，也尽量使用至少两个虚拟交换机，并且两个虚拟交换机分布在不同可用区，做到跨可用区容灾。

- 使用多少个虚拟交换机还和系统规模和系统规划有关。



网络规划--应该选择什么网段

- **VPC网段**

网段	可用IP地址数量	备注
192.168.0.0/16	65532	去除系统占用地址，掩码必须在16到29之间
172.16.0.0/12	1048572	去除系统占用地址，掩码必须在16到29之间
10.0.0.0/8	16777212	去除系统占用地址，要考虑经典网络配置，掩码必须在16到29之间

（1）只有一个VPC并且不需要和本地IDC互通时，可以选择上表中的任何一个网段或其子网。

（2）VPC网段的选择还需要考虑到是否使用了经典网络。（10.0.0.0/8）

（3）如果有多个VPC，或者有VPC和线下IDC构建混合云的需求，，掩码建议不超过16位。

网络规划--应该选择什么网段

- **交换机网段**

（1）交换机的网段的大小在16位网络掩码与29位网络掩码之间；

（2）交换机的网段可以和其所属的VPC网段相同，或者是其VPC网段的子网;

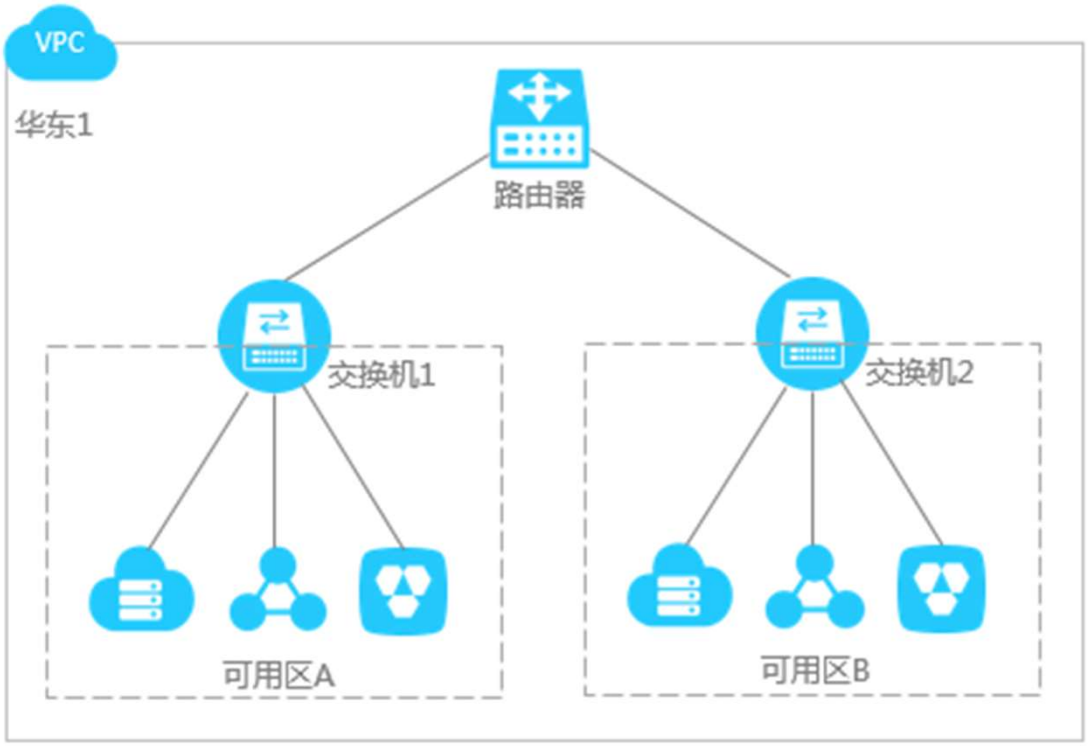
（3）每个交换机的第一个和最后三个IP地址为系统保留地址。

（4）ClassicLink功能允许经典网络的ECS和192.168.0.0/16，10.0.0.0/8，172.16.0.0/12这三个VPC网段的ECS通信。

（5）虚拟交换机网段的确定还需要考虑该交换机下容纳主机的数量；

网络规划--应该选择什么网段

小型的基础架构的VPC网络规划实践：



举例：

VPC网段：192.168.0.0/16

交换机1：192.168.0.0/24

ECS-11：192.168.0.2

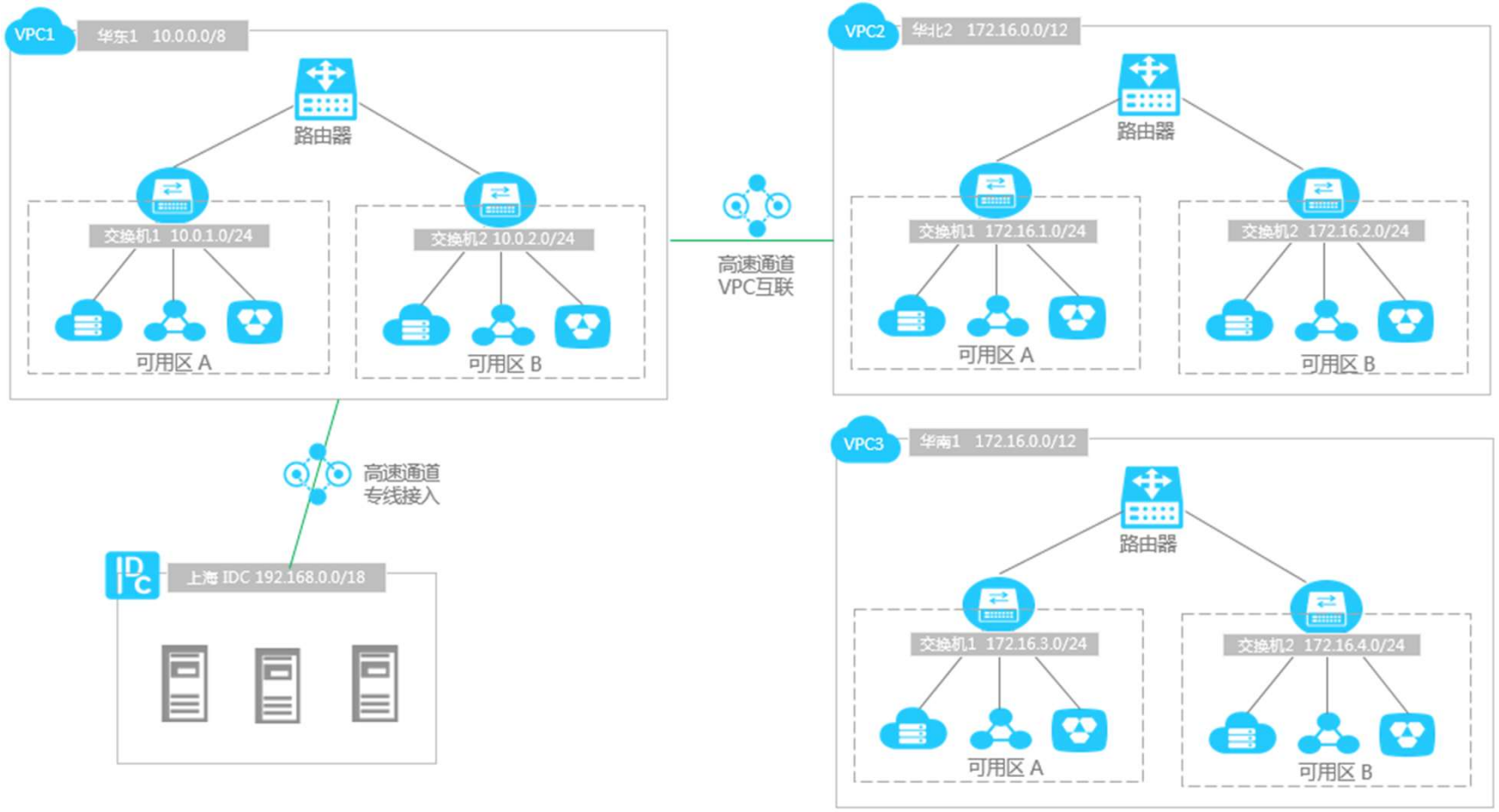
ECS-12：192.168.0.3

交换机2：192.168.1.0/24

ECS-21：192.168.1.11

ECS-22：192.168.1.12

网络规划--多VPC与IDC互通的网段规划



目录

VPC的访问控制

- **ECS——安全组**

安全组是一种虚拟防火墙，具备状态检测包过滤功能——网络安全隔离手段，用于在云端划分安全域；

  - 当访问控制规则冲突时，优先级高的规则生效，优先级相同时，“拒绝”的规则生效
  - 安全组应作为白名单使用，且遵循“最小授权”原则

- **云数据库 RDS 版——白名单**

用户可定义允许访问 RDS 的 IP 地址，指定之外的 IP 地址将被拒绝访问，云服务器的IP地址加入到需要访问的RDS的白名单后，云服务器才能访问RDS实例；

- **负载均衡——白名单**

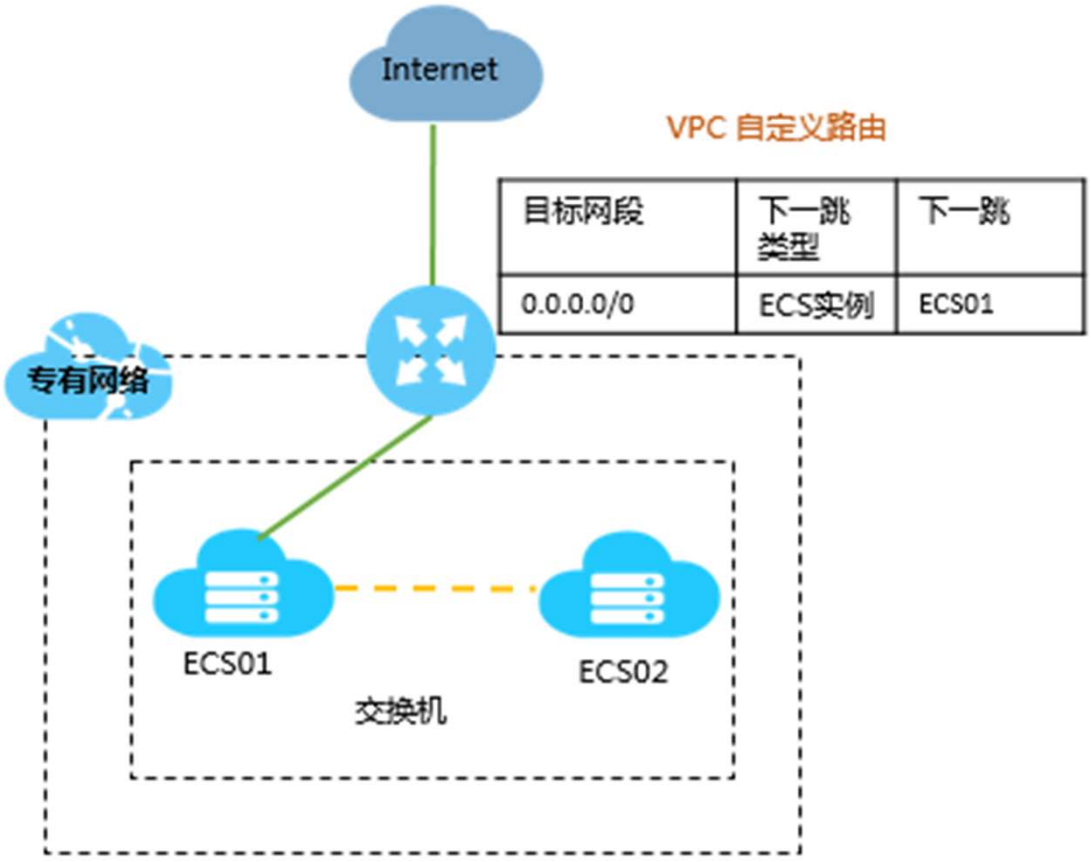
用户可定义允许访问 SLB 的 IP 地址，指定之外的 IP 地址将被拒绝访问，适用于应用只允许特定 IP 访问的场景；

目录

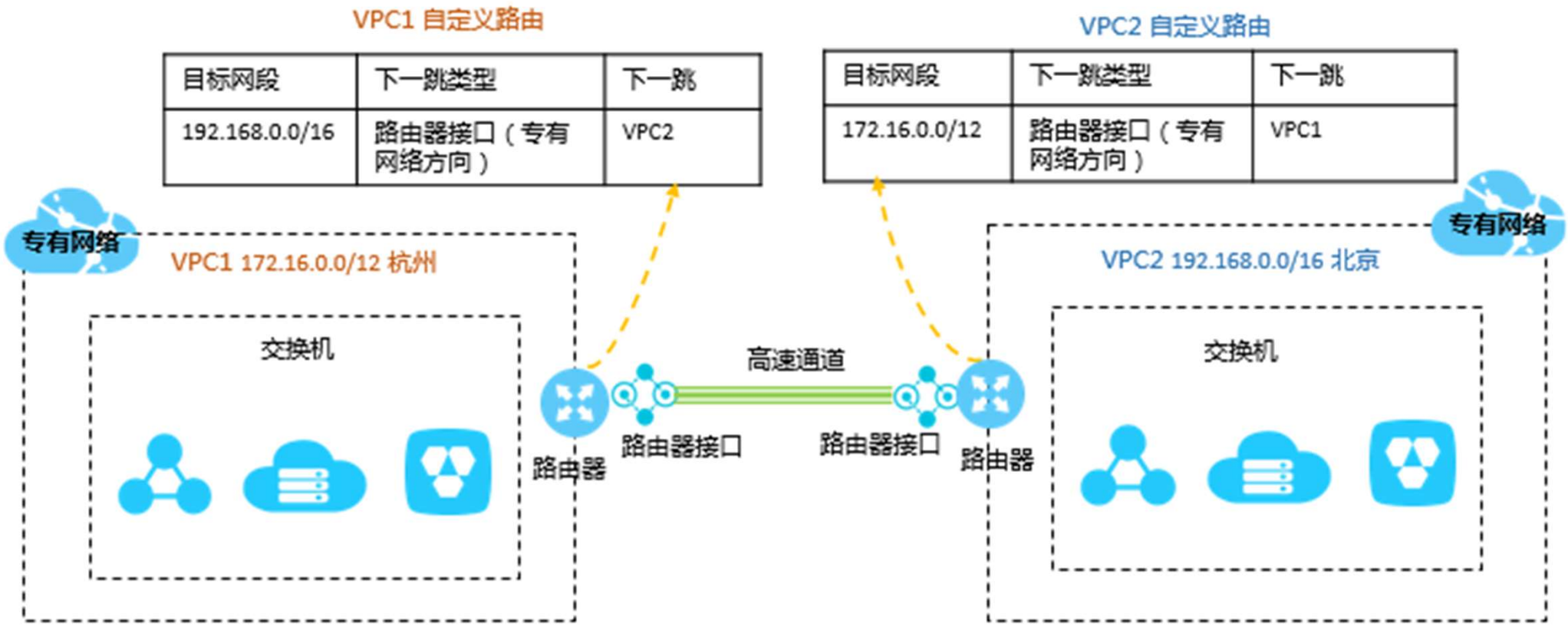
VPC的路由表和路由条目

- VPC内网路由
- VPC互连--高速通道连接两个VPC
- VPC互连-- VPN网关连接两个VPC
- 高速通道物理专线连接专有网络和本地网络
- VPN网关连接专有网络和本地网络

路由表和路由条目——VPC内网路由



路由表和路由条目——VPC互连（高速通道）



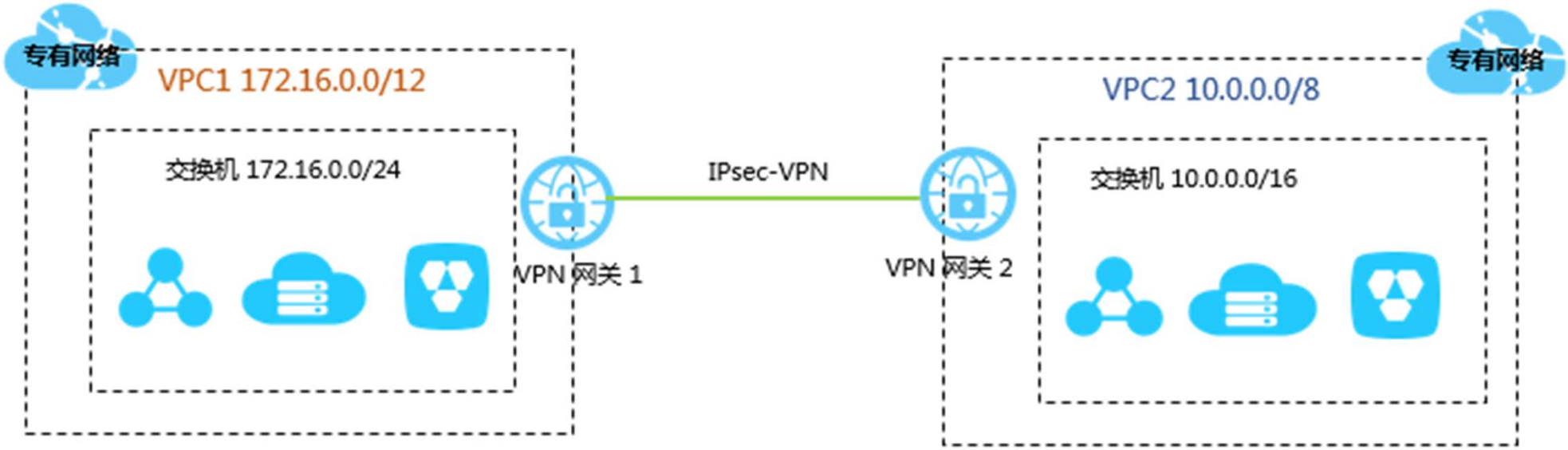
路由表和路由条目——VPC互连（VPN网关）

VPC1 自定义路由

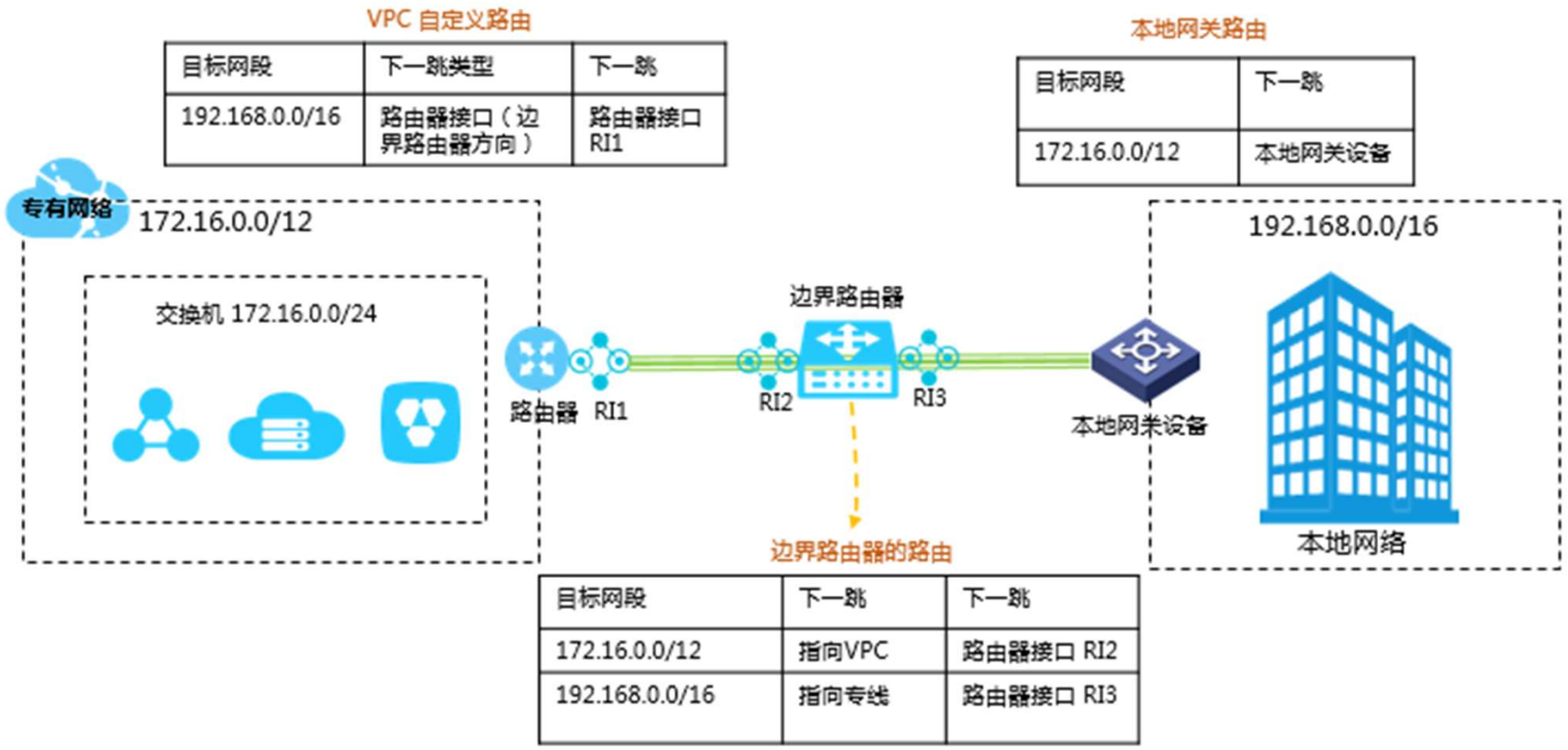
目标网段	下一跳类型	下一跳
10.0.0.0/8	VPN网关	VPN网关1

VPC2 自定义路由

目标网段	下一跳类型	下一跳
172.16.0.0/12	VPN网关	VPN网关2



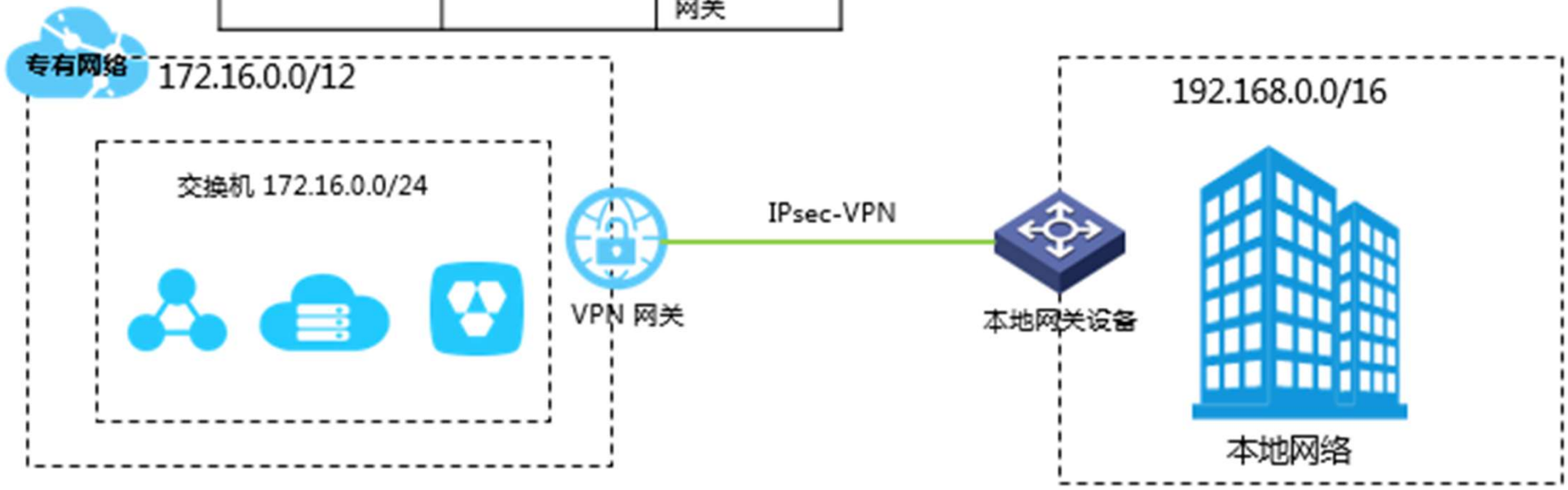
路由表和路由条目——连接本地网络（高速通道）



路由表和路由条目——连接本地网络（VPN网关）

VPC 自定义路由

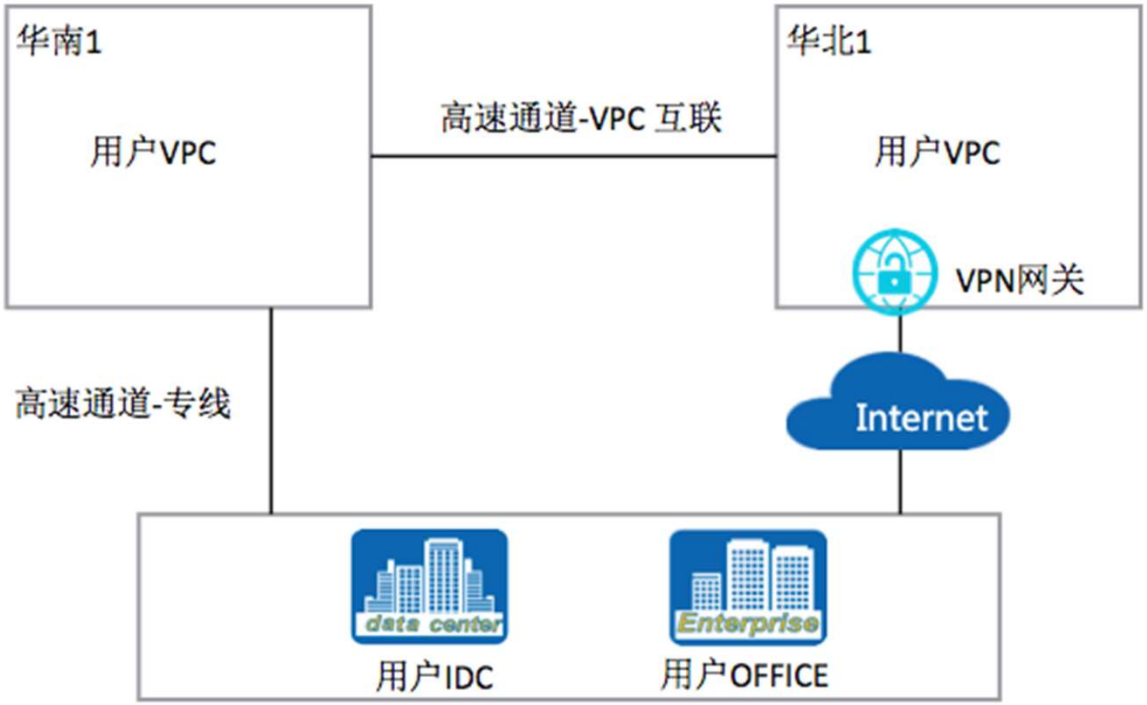
目标网段	下一跳类型	下一跳
192.168.0.0/16	VPN网关	配置的VPN网关



目录

最佳实践：基于VPC构建混合云

混合云是目前应用比较多的一种形态，它将用户线下IDC和云上VPC连接起来，既保护了用户线下IDC的现有投资，又充分利用了云的弹性，低成本等优势。



小结

1. 什么是专有网络VPC，它有什么特点?
2. 简述专有网络VPC产品的基本概念，如VRouter、VSwitch、路由表等。
3. 在VPC上如何管理ECS、SLB和RDS?
4. 云上/云下连入VPC有哪些方式，它们之间的区别各是什么?
5. NAT网关的功能和应用场景是什么?

为了无法计算的价值 | 阿里云