专有网络 VPC

最佳实践

最佳实践

专有网络VPC（Virtual Private Cloud）是阿里云推荐使用的网络类型，越来越多的用户选择使用VPC，可以说VPC是现在用户上云第一个考虑的产品。使用VPC主要有如下两个优势：

网络隔离

VPC基于隧道技术，实现数据链路层的隔离，为每个租户提供一张独立、隔离的安全网络。不同专有网络之间内部网络完全隔离，只能通过对外映射的IP（弹性公网IP和NAT IP）互联。

网络管理

您可以完全掌控自己的虚拟网络，例如选择自己的IP地址范围、划分网段、配置路由表和网关等，从而实现安全而轻松的资源访问和应用程序访问。此外，您也可以通过专线或VPN等连接方式将您的专有网络与传统数据中心相连，形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。

访问专有网络VPC获取更多信息。

在考虑使用VPC的时候，首先遇到的一个问题就是如何进行VPC网络规划？您可以从以下几个问题入手规划和设计的您专有网络架构。

问题一，应该使用几个VPC？

问题二，应该使用几个虚拟交换机？

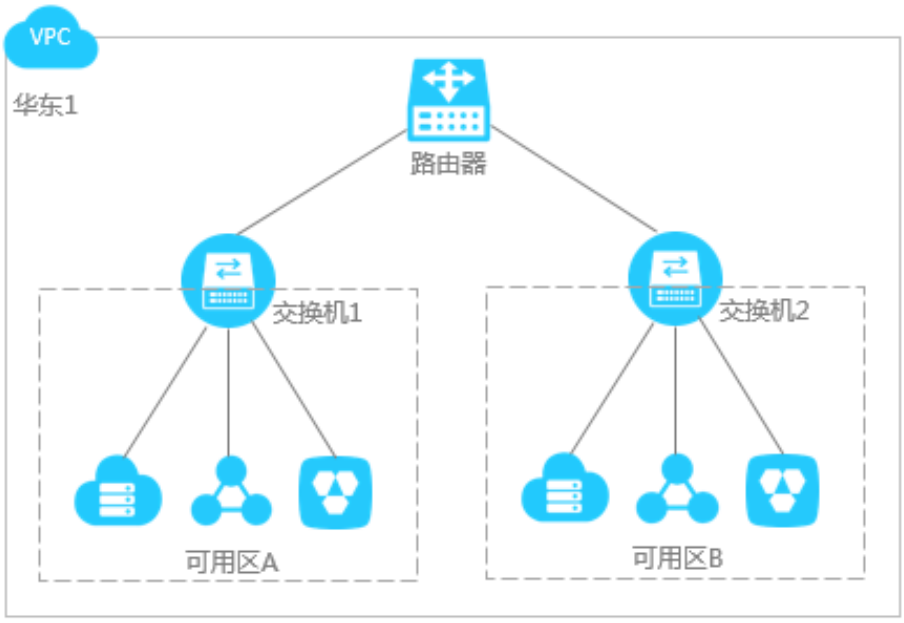
问题三，应该选择什么网段？

问题四，云上多个VPC，且需要和云下IDC互通，如何规划网段？

问题一，应该使用几个VPC？

单个VPC

如果您没有多地域部署系统的要求且各系统之间也不需要通过VPC进行隔离，那么推荐使用一个VPC。目前，单个VPC内运行的云产品实例可达10000个，这样的容量基本上可以满足您的需求。

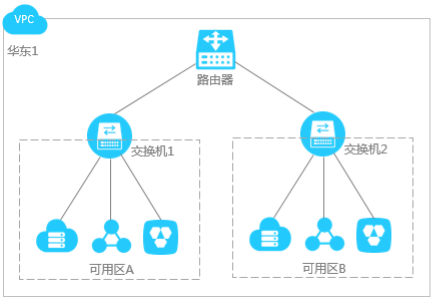


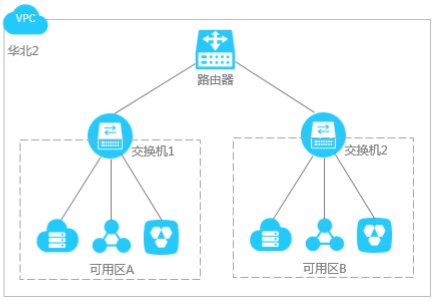
多个VPC

如果您有如下任何一个需求，都推荐您使用多个VPC。

有多地域部署系统的要求

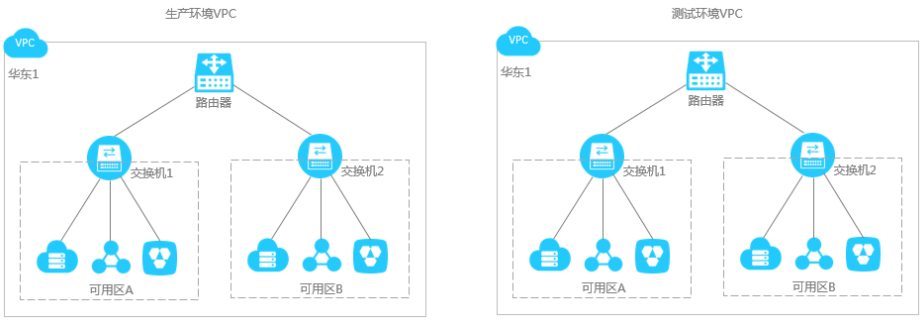
VPC是地域级别的资源，是不能跨地域部署的。当您有多地域部署系统的需求时，就必然需要使用多个VPC，如下图所示。使用多个VPC，怎么能内网互通呢？基于阿里巴巴骨干网构建的高速通道产品能轻松实现跨地域，跨国VPC间的互通。





多业务系统隔离

如果在一个地域的多个业务系统需要通过VPC进行严格隔离，比如生产环境和测试环境要严格进行隔离，那么也需要使用多个VPC，如下图所示。



问题二，应该使用几个虚拟交换机？

首先，即使只使用一个VPC，也尽量使用至少两个交换机，并且将两个交换机分布在不同可用区，这样可以实现跨可用区容灾。

同一地域不同可用区之间的网络通信延迟很小，但也需要经过业务系统的适配和验证，系统调用复杂加上系统处理时间，跨可用区调用也可能产生期望之外的延迟。建议进行系统优化和适配，能够容忍这种延迟，在高可用和低延迟之间找到平衡。

> 可用区是指在同一地域内，电力和网络互相独立的物理区域，在同一地域内可用区与可用区之间内网互通。

其次，使用多少个交换机还和系统规模、系统规划有关。如果前端系统都可以被公网访问并且都有主动访问公网的需求，考虑到容灾，可以考虑将不同的前端系统，部署在不同的交换机下，而后端系统部署在另外的交换机下。

问题三，应该选择什么网段？

在创建VPC和交换机时，您必须以无类域间路由块 (CIDR block) 的形式为您的专有网络划分私网网段。

VPC网段

目前阿里云默认提供如下三个标准私网网段供您选择。

网段	可用主机数	备注
192.168.0.0/16	65532	去除系统占用地址
172.16.0.0/12	1048572	去除系统占用地址
10.0.0.0/8	16777212	去除系统占用地址

注意：如有除此之外的特殊网段要求，也可以提工单或者通过客户经理申请开通。

您可以根据以下建议规划VPC网段，VPC创建成功后，网段无法再修改：

您可以使用这些网段及其子网作为VPC的网段。

如果可能有多个VPC，或者VPC和线下IDC有构建混合云的需求，建议使用上面这些标准网段的子网作为VPC的网段，掩码建议不超过/16。

如果云上只有一个VPC并且不需要和线下IDC互通，那么选择以上任何一个网段或其子网均可，您可以可自由选择。

VPC网段的选择还需要考虑到是否使用了经典网络。经典网络的网段是10.0.0.0/8，如果您在云上使用了经典网络，并且计划将经典网络的主机和VPC网络打通（阿里云正计划提供ClassicLink功能，以实现将经典网络迁移到VPC），那么，建议您选择非10.0.0.0/8作为VPC的网段。

ClassicLink功能可以允许经典网络的ECS和192.168.0.0/16，10.0.0.0/8，172.16.0.0/12 三个VCP网段的主机通信，但只能和10.0.0.0/8中的特定交换机的网段通信，即如果经典网络的ECS要和使用了10.0.0.0/8的VPC网段的主机通信，那么该主机必须是某个特定的10.0.0.0/8下的子网，具体子网还未确定。因此，如果您有ClassicLink功能的需求，建议选择非10.0.0.0/8的网段作为VPC的网段。

交换机网段

您可以根据以下建议规划交换机网段，同样，交换机创建成功后，网段无法再修改：

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，可提供8~65536个地址。做这个限制的原因是/16掩码也能支持65532个主机，规模足够大了，没必要更大，而小于/29有太小，没有意义。

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。比如VPC的网段是192.168.0.0/16，那么该VPC下的虚拟交换机的网段可以是192.168.0.0/16，也可以是192.168.0.0/17，一直到192.168.0.0/29。

注意：如果您的交换机网段和所属VPC网段相同，您只能在该VPC下创建一台交换机。

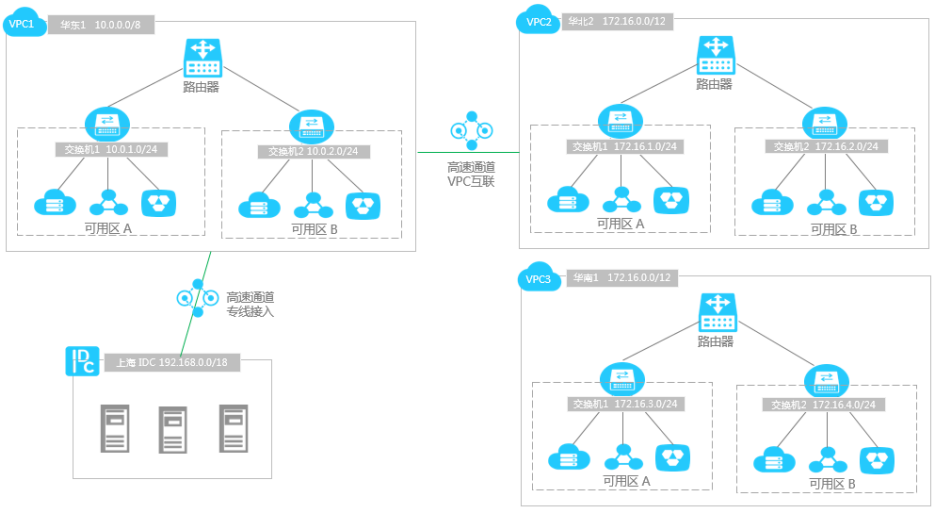
每个交换机的第一个和最后三个IP地址为系统保留地址。以 192.168.1.0/24 为例，192.168.1.0、192.168.1.253、 192.168.1.254和192.168.1.255这些地址是系统保留地址。

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。

问题四，云上多个VPC且和云下IDC需要互通，如何规划网段？

如下图所示，比如您在华东1、华北2、华南1三个地域分别有三个VPC，并且华东1和华北2两个地域的VPC需要通过高速通道（VPC互联功能）实现私网互通，华南1地域的VPC暂时没有和其它地域通信需求，但未来也可

能和华北2的VPC私网通信。另外，您在上海还有一个自建IDC，需要通过高速通道（专线功能）和华东1的VPC私网互通。



由于VPC与VPC之间，VPC和线下IDC之间需要互通的IP段不能相同，因此，上图中上海IDC、华东1 VPC1、华北2 VPC2要使用不同的网段，而华南1暂时没有和其它VPC之间互通的需求，因此，可以使用和华北2相同的网段，但考虑到将来华南1有和华北2可能有私网互通的需求，华南1 VPC3中的两个交换机的网段和华北2 VPC2中交换机的网段规划使用不同的网段，也就是说VPC网段一样，但交换机的网段不一样。

阿里云VPC互通要求要求地址不能冲突，指的是交换机的网段不能一样，但VPC的网段可以一样。当然尽量规划不同VPC的网段不一样。

因此，在多VPC需要互通并且和线下IDC需要互通的情况下，建议遵循如下网段规划原则：

> 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来增加VPC可用的网段数。
>
> 如果不能做到不同VPC的网段不同，则尽量保证不同VPC的交换机网段不同。
>
> 如果也不能做到交换机网段不同，则保证要通信的交换机网段不同。

此外，如果线下IDC网段已经确定无法修改，云上VPC的网段也已经确定无法修改，但有线下IDC和和VPC的通信需求，阿里云正在规划专线网关功能，可以解决这一问题。

阿里云的专有网络目前没有网络的访问控制，当前在专有网络中进行访问控制，依赖各个云产品的访问控制能力。本文将介绍云服务器 ECS 、云数据库 RDS 、负载均衡的访问控制功能。

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。安全组用于设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分安全域。

隔离机制

安全组是一个逻辑上的分组，这个分组是由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。每个实例至少属于一个安全组，在创建的时候就需要指定。同一安全组内的实例之间网络互通，不同安全组的实例之间默认内网不通。可以授权两个安全组之间互访。

一个VPC类型的ECS实例只能加入本VPC的安全组。您可以随时授权和取消安全组规则。您的变更安全组规则会自动应用于与安全组相关联的ECS实例上。

安全组可以根据出入方向的规则设置对安全组内部实例的出入方向网络流量进行访问控制。

入方向：授权/拒绝某个IP或CIDR通过某个协议类型访问安全组内部实例指定的端口范围。

出方向：授权/拒绝安全组内部实例通过某个协议访问某个IP或CIDR的指定的端口范围。

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。

配置规则

安全组应作为白名单使用，且遵循“最小授权”原则。例如，用于运维管理的跳板机，该类实例一般具备很强的内网网络访问权限，需要暴露在公网并允许SSH登录。这类实例的风险较高，建议进行单独管理。安全组规则可以这样设计：

在跳板机实例所在的安全组中拒绝（deny）所有地址（0.0.0.0/0）对于该实例所有协议（all）端口（-1/-1）的访问（Ingress）。

在该安全组中允许（allow）某运维人员的IP地址（xx.xx.xx.xx）对于该实例通过ssh（tcp，22端口）的方式登录（Ingress）跳板机。

由于相同安全组中的ECS内网互通，需要将不同业务环境、不同访问控制需求的服务器规划在不同的安全组中：

提供公网服务的和内网服务放置在不同的安全组。

不同应用使用不同的安全组。

不同的部署环境使用不同的安全组。

当需要专有网络中的服务器内网互通时，有两种方式:

可以配置安全组之间互相授权

也可以通过设置安全组规则对特定地址段的出入方向授权来实现。

当安全组数量较少或网络规划不严格规划时，前者的配置相对简单。当安全组数量随着业务部署的复杂度增加时，在合理的规划服务器地址段的基础上，对地址段的授权能够有效的降低安全组的配置和管理成本。

更多安全组的配置可以参考：安全组介绍、安全组实践（一）、安全组实践（二）、安全组实践（三）。

云数据库 RDS 版——白名单

基于云数据库RDS版的白名单功能，您可定义允许访问RDS的IP地址，指定之外的IP地址将被拒绝访问。在专有网络中使用RDS产品时，需要将云服务器的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。

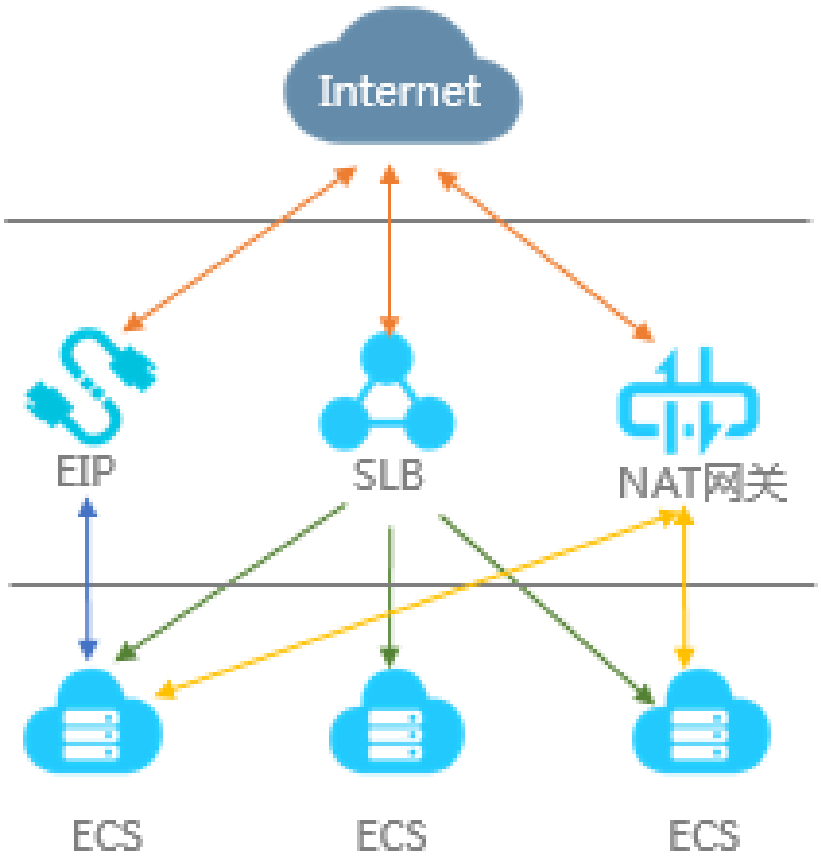
更多云数据库RDS版白名单的配置可以参考云数据库RDS版设置白名单。

负载均衡——白名单

您可以为负载均衡监听设置仅允许哪些IP访问，适用于应用只允许特定IP访问的场景。负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务。通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。一般对于外网或内网用户开放访问。当服务仅对指定用户开放，或仅用于内部访问时，通过白名单功能可以有效的对服务进行访问控制。在配置白名单时，将需要通过负载均衡服务访问后端服务器的用户IP地址或专有网络内部的云服务IP地址加入到负载均衡服务监听的访问控制白名单即可。

更多负载均衡白名单的配置可以参考负载均衡设置访问控制。

目前阿里云虚拟网络为您提供了以下几种不同形态的公网类产品：负载均衡（SLB），弹性公网IP (EIP)，NAT网关。这几种产品分别适用于不同的场景，您可通过这几种产品实现VPC资源与公网的互通。



产品	功能	场景关键词	计量计费特性
负载均衡	支持入方向的端口映射（DNAT）。您可在后端添加服务器，并设置相应的调度策略。负载均衡将把公网流量分发到后端的服务器上，同时您可根据业务的访问量对后端服务器进行动态增减，做到灵活的扩容和缩容。并且，负载均衡会提供健康检查服务，自动屏蔽异常状态的后端服务器，保证系统高可用。负载均衡适用于对可用性要求高的、需要多台ECS承载同一业务的应用场景。	DNAT + 负载均衡 七层转发/四层转发 健康检查/高可用	预付费：按带宽 后付费：按带宽/按流量
NAT网关	支持入方向的端口映射（DNAT）和出方向的SNAT功能，支持带宽包，能够明显得降低带宽成本。	DNAT（IP映射/端口映射） SNAT（ECS访问互联网） 共享带宽	后付费：按带宽
EIP	能够动态的绑定到VPC类型的ECS上，为	SNAT+DNAT 一个EIP只能绑定一个	预付费：按带宽 后付费：按带宽/按流

	每台ECS提供独立使用的公网IP地址和带宽。	ECS	量

注意：负载均衡的DNAT可支持一个“负载均衡 IP+端口”映射到多个“ECS IP+端口”上，NAT网关的DNAT只支持一个“公网IP+端口”映射到一个“ECS IP+端口”上，即负载均衡是基于端口进行负载均衡的，而NAT网关的DNAT本身没有负载均衡的能力。

使用建议：

如果有多台ECS，需要基于端口做流量分担，就需要使用负载均衡。

如果多台ECS需要主动访问公网，建议使用NAT网关，配置SNAT表。

如果有多台ECS需要对外提供公网服务，且希望有多个公网IP，又不需要基于端口做负载均衡，建议使用NAT网关，配置端口转发表。

如果希望多公网IP又希望共享带宽，建议使用NAT网关，可以提供多个公网IP共享带宽，提高带宽利用率，降低成本。

如果极少量ECS需要对公网提供服务又希望主动访问公网，可以使用EIP，直接将EIP绑定到VPC ECS即可，不再需要进行其它配置。

典型场景与解决方案

下面针对几种典型的场景来介绍如何选择产品，假设您购买的都是VPC类型的ECS。

需要对外提供服务

对外提供带有负载均衡的七层服务

无公网IP的ECS主动访问互联网

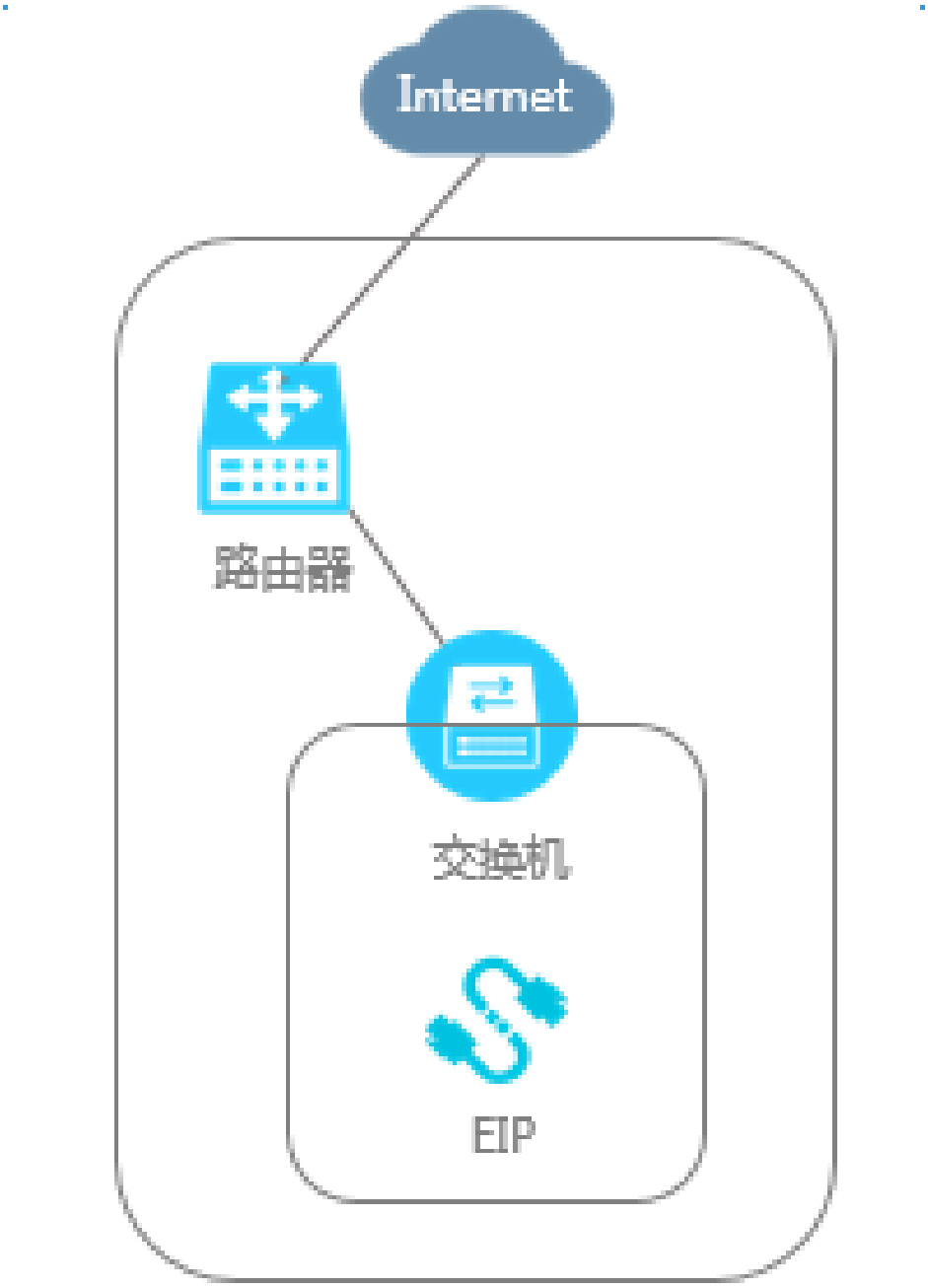
抓取类业务

多个公网服务共享带宽

需要对外提供服务

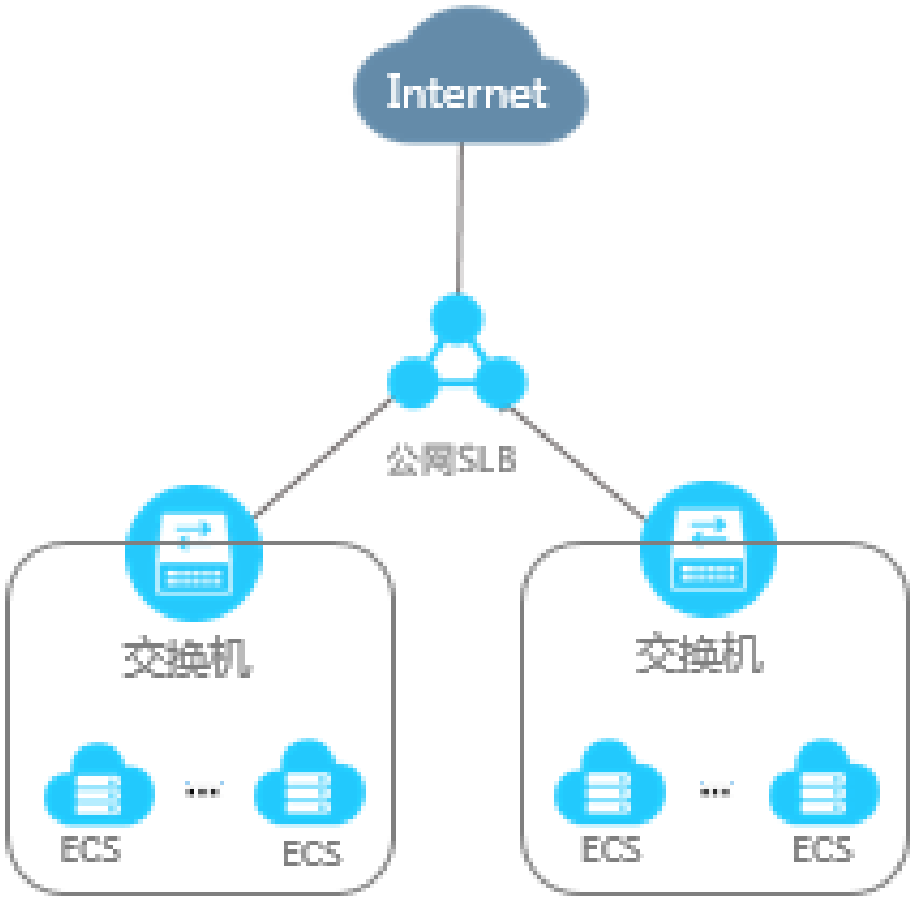
单台ECS对外提供服务

您只存在单一应用，并且业务较小的时候，单台ECS即可满足您的需求，应用程序、数据库、文件都部署在该ECS上面。为这台ECS绑定一个公网EIP即可对外提供服务。



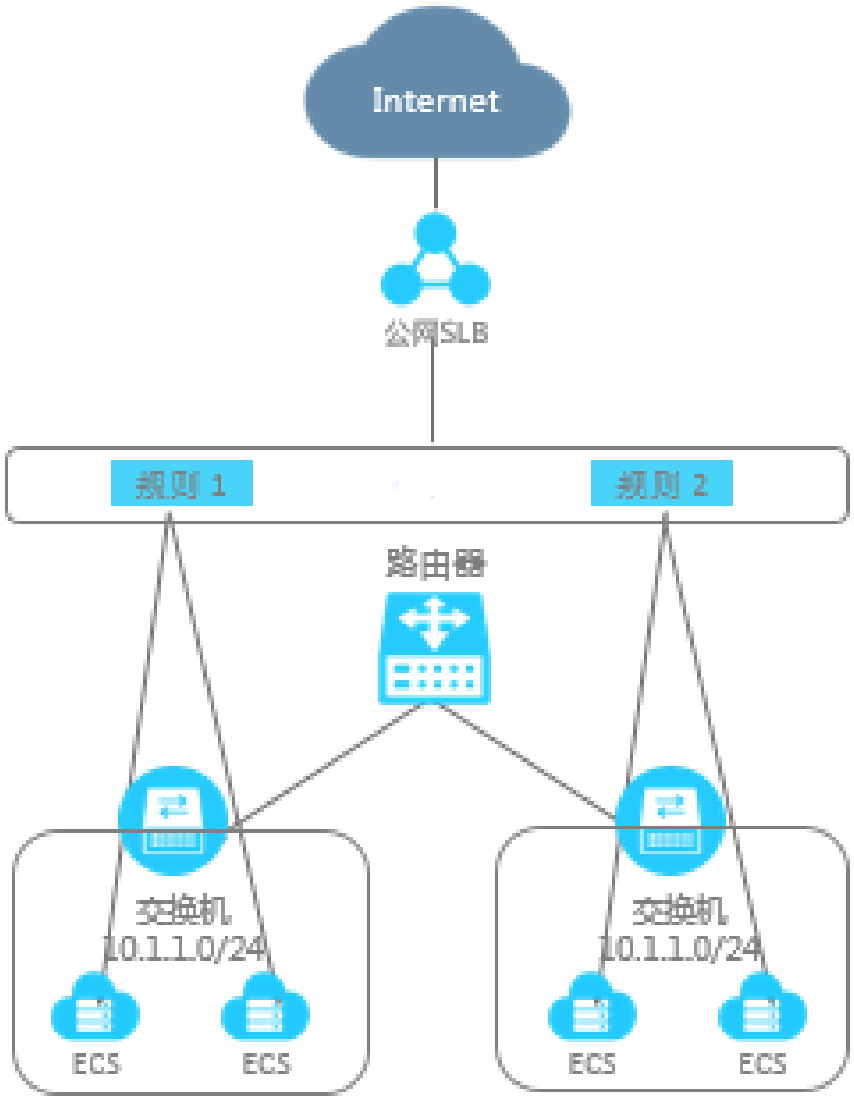
对外提供带有负载均衡的四层服务

当业务流量较大，需要对外提供服务，一台ECS已经不能支撑这么大的访问流量，需要多台ECS才能支持。您只需要最简单的负载均衡功能，不需要更高级的七层转发等功能。此时，您可选择公网负载均衡实例、创建四层（TCP/UDP）监听、后端挂载多台ECS来搭建整个业务架构。



对外提供带有负载均衡的七层服务

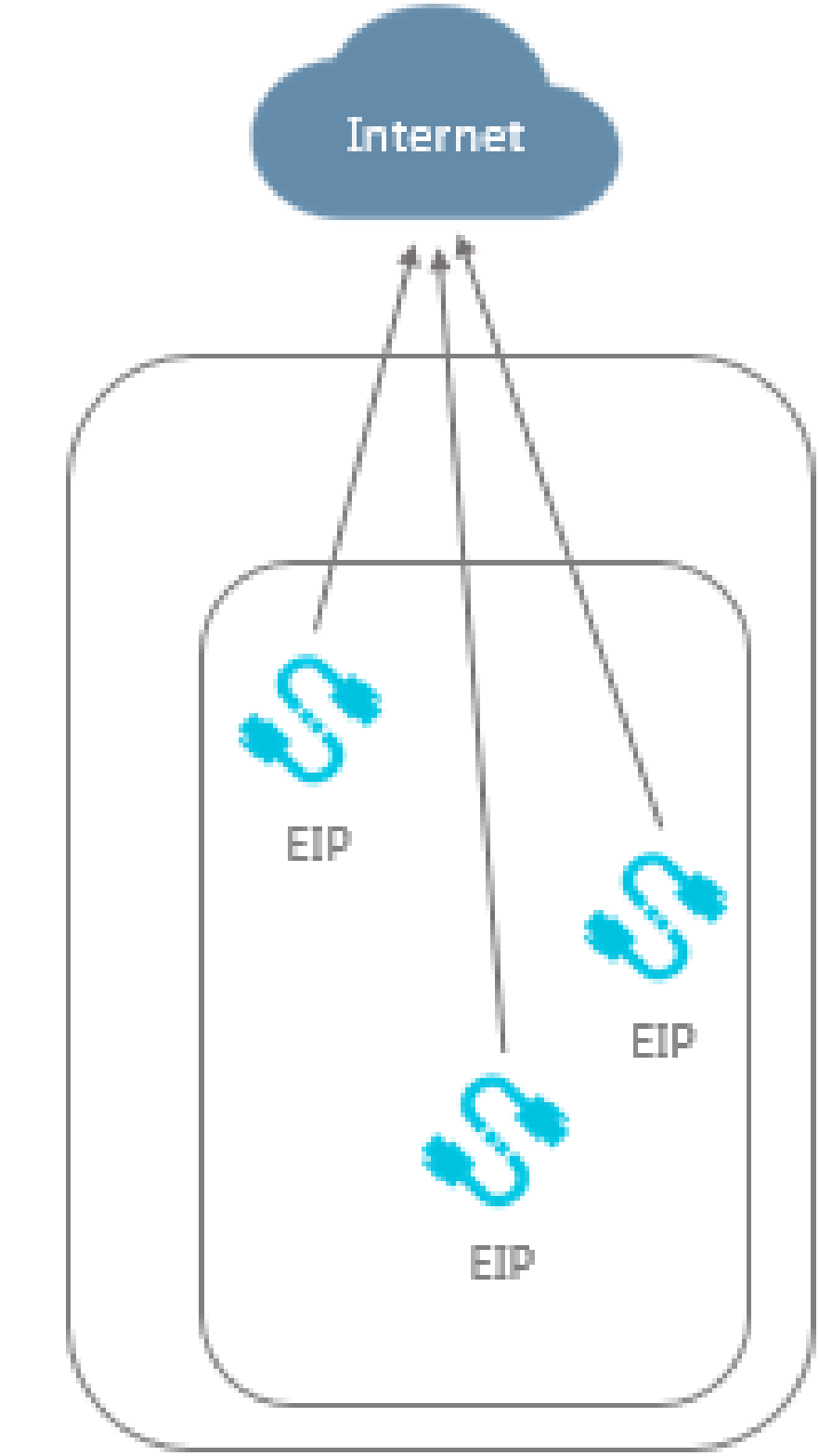
业务流量较大，需要对外提供服务，一台ECS已经不能支撑这么大的访问流量，需要多台ECS才能支持。用户需要用到“按域名或按URL转发”或者数据安全传输等七层功能。此时，您可选择公网负载均衡实例、创建七层（HTTP/HTTPS）监听、后端挂载多台ECS来搭建整个业务架构。



无公网IP的ECS主动访问互联网

挂载EIP

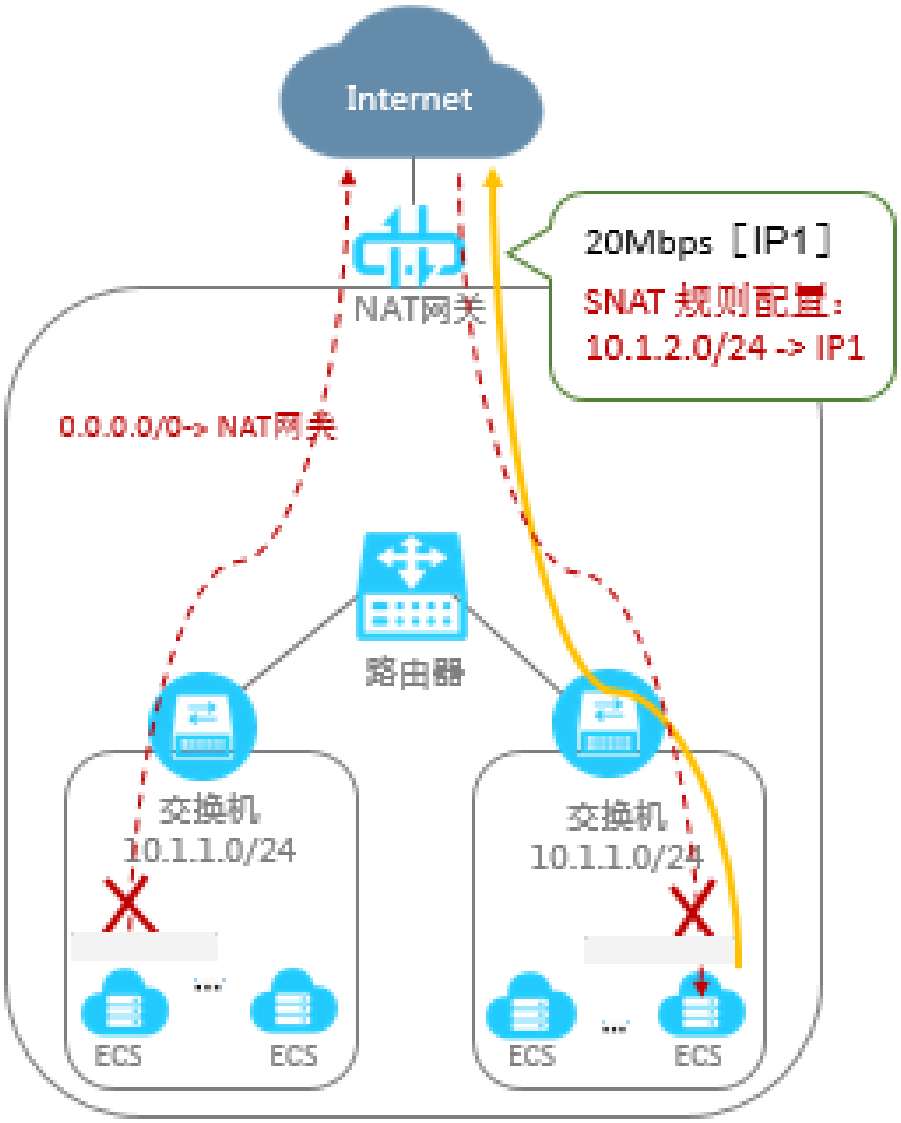
当您的ECS较少的时候，可针对每台ECS分别绑定一个EIP，可通过各自的EIP实现公网的访问。



使用NAT网关

若您访问的公网ECS数量特别多时，分别对每个ECS进行EIP绑定十分繁琐。此时建议使用NAT网关的

SNAT功能。您首先创建一个带有公网IP和公网带宽的NAT网关，在NAT网关上配置相应的SNAT规格，允许特定交换机下的所有ECS访问公网。在NAT网关上配置自定义路由，将某个虚拟交换机下的访问公网的数据转发至NAT网关。



抓取类业务

场景概述

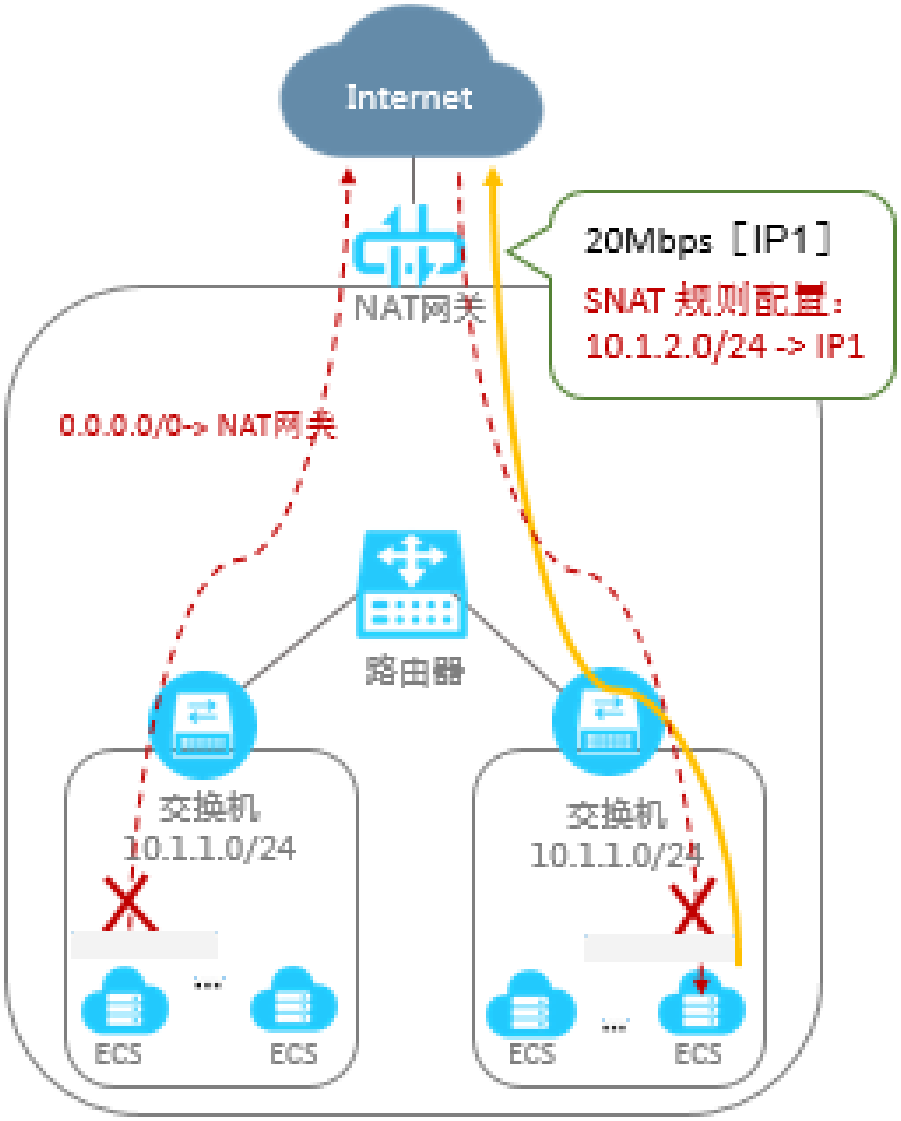
您需要根据既定的抓取目标，有选择的访问万维网上的网页与相关链接，获取所需要的信息按照一定的规则从网络中去定向抓取相关网页资源进行分析。爬虫业务需要保证公网IP的可用性，当IP被攻击时可以方便的更改该公网IP。

核心需求

您将保有多台VPC ECS，分别负责抓取不同的数据，并且这些ECS都有访问公网（SNAT）的需求，当这些IP被攻击时，需要随意更换出口IP。

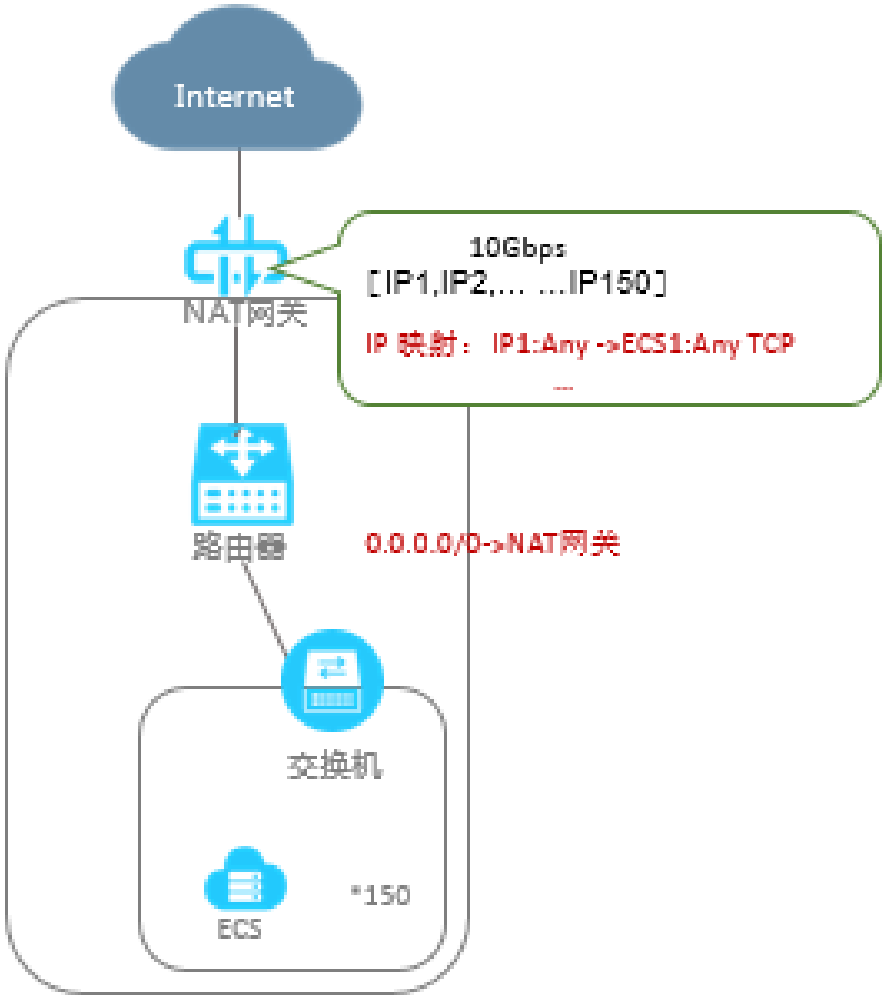
解决方案

多台ECS通过VRouter接入NAT网关，可针对某个VSwitch下的网段配置统一的SNAT规则，多台ECS都可以通过一个公网IP去访问公网。当该公网IP被攻击时，您可直接修改SNAT规则配置修改出口IP。



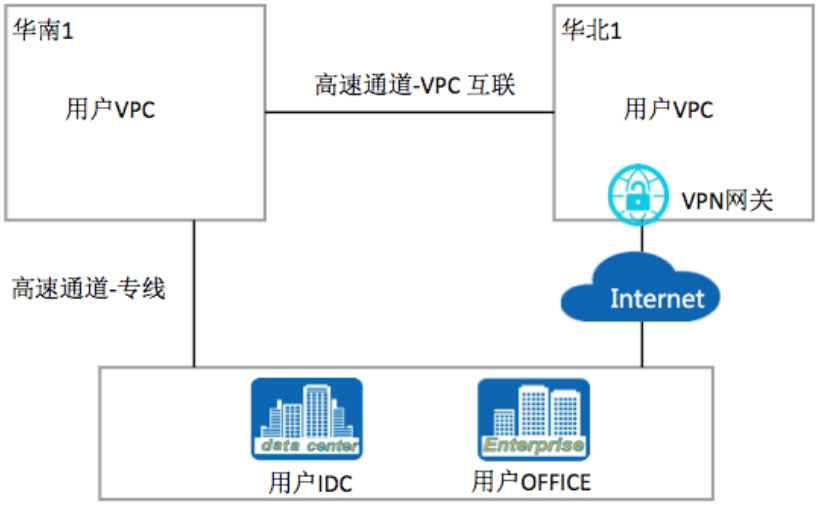
多个公网服务共享带宽

您的业务发展快，并存在多个应用，可将不同的应用部署在不同的子网中独立的进行管理。若子网内的每个ECS都是相对独立的业务模块，可使用NAT网关的端口转发功能进行IP映射，并针对这些ECS共享带宽。



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，既保护了您线下IDC的现有投资，又充分利用了云的弹性，低成本等优势。

如下图所示，阿里云通过高速通道和VPN网关两个产品为用户提供了混合云构建方案。



高速通道产品有两个核心功能，一是高速通道-物理专线，即将线下IDC和云上VPC连接起来，二是高速通道 - VPC互联，将两个VPC连接起来；混合云主要使用高速通道-物理专线功能。

VPN网关基于Internet，通过加密通道将企业数据中心，企业办公网络等和阿里云专有网络（VPC）安全可靠连接起来。

在VPN网关的支持下，企业可以在几分钟内完成企业数据中心与阿里云VPC之间的互联，大幅降低了企业成本的同时，还获得数据传输安全性。

这两个产品的简单对比如下，您可以根据自己的需要选择使用相应的产品。

产品	使用链路	网络质量	价格	交付时间
高速通道 - 专线	专线	高	较高	长，一般超过30天
VPN 网关	Internet	较低	较低，约专线的40%	短，约10分钟

高速通道 - 专线

高速通道 - 专线的接入方式有两种，一种是用户自行通过运营商接入，另一种是通过阿里云合作伙伴接入。阿里云有多家合作伙伴，全国超过300个城市提供接入能力。合作伙伴的接入点已经和阿里云专线打通，用户只需要将自己IDC通过专线接入到当地合作伙伴的接入点即可。因此，建议选择阿里云合作伙伴接入。

物理专线接入说明：

通过合作伙伴接入方法

登陆到高速通道控制台，选择物理专线，点击右上角的**申请专线接入**，也可以直接访问 阿里云专线接入合作伙伴。

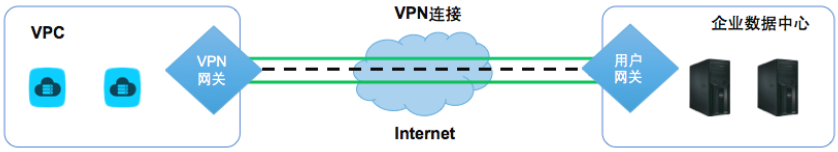
在合作伙伴申请页面，可以看到阿里云专线合作伙伴列表及联系方式，直接用合作伙伴联系即可，如下图所示。

通过运营商自行接入

具体操作参考通过运营商自行接入操作指南。

VPN网关

通过VPN网关可以非常快速的将线下IDC和云上VPC连接起来。VPN网关主要有三个核心概念和组件，几个组件的关系如下图所示。



VPN网关：用户在阿里云创建的IPSec VPN网关。

VPN网关是用户在阿里云专有网络（VPC）创建的IPSec VPN网关，与用户侧的用户网关配合使用。可在阿里云专有网络（VPC）和用户侧的企业数据中心基于Internet建立安全可靠的加密通信。一个VPN网关可以有多个VPN连接。

注意：VPN网关只能在专有网络（VPC）中使用，不能在经典网络中使用。

用户网关：用户企业数据中心VPN服务网关。

用户网关是用户侧企业数据中心的VPN服务网关。用户可将用户网关的信息注册到云上，然后将用户网关和VPN网关连接起来。一个用户网关可以与多个VPN网关进行连接。

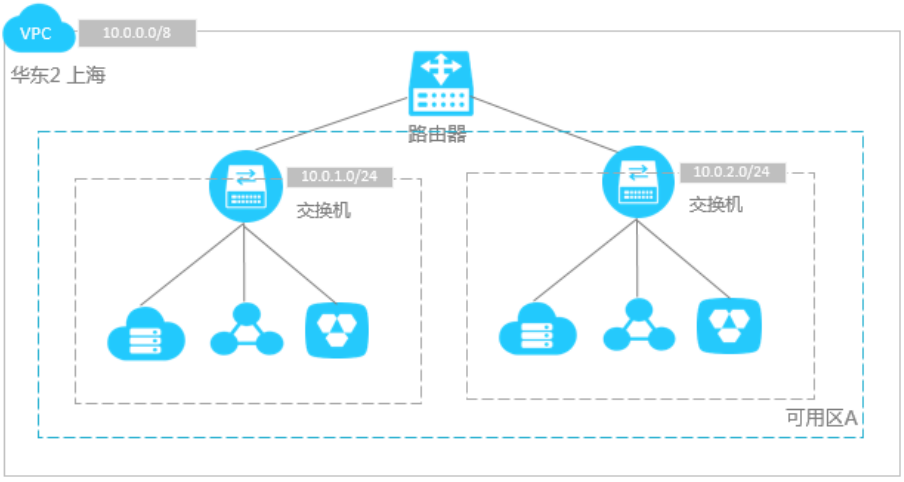
VPN连接：通过用户网关和VPN网关建立的加密VPN通道。

VPN连接是指VPN网关和用户网关建立连接后的VPN通道。只有VPN连接建立后，用户IDC才能用云上VPC进行加密通信。目前VPN连接支持IPSec加密协议，可满足绝大多数VPN连接的需求。

具体配置可以参考VPN网关部署实践。

应用场景

在阿里云上管理您的专属网络，创建专有网络、交换机，并在该专有网络中创建云产品实例（如ECS、RDS、SLB等）并使用。假设地域规划为上海，使用上海可用区A上的云产品资源。



网络规划

地域为华东2(上海)，可用区为华东2可用区A

专有网络网段为10.0.0.0/8

将两个应用部署在两个交换机中，分别对公网和私网提供服务，子网网段分别是10.0.1.0/24、10.0.2.0/24

在两个交换机中分别部署私网ECS、公网SLB、私网RDS

操作步骤

登录专有网络管理控制台，地域选择华东 2 (上海)。

单击**创建专有网络**，弹出**创建专有网络**对话框，填写如下信息。

- 专有网络名称：VPC_A
- 网段：10.0.0.0/8

在专有网络VPC_A中，创建两个交换机。

在上海地域的专有网络列表，选择VPC_A的管理链接，进入**专有网络基本信息**页面。

在左侧导航栏，选择**交换机**，单击**创建交换机。**

在弹出**创建交换机**对话框，填写下面的信息完成交换机1的创建。

名称：业务网络A

可用区：华东2可用区A

i. 网段：10.0.1.0/24

创建交换机2，同样在专有网络VPC_A下创建交换机。

名称：业务网络B

网段：10.0.2.0/24

可用区：华东2可用区A

配置公网业务的云产品部署。

打开名称为“业务网络A”的交换机页面，单击**创建实例**下拉菜单，分别创建ECS1、ECS2、RDS1、SLB1。

登录负载均衡控制台，通过后端服务器的配置，将两台ECS实例添加到公网负载均衡实例下。

进入实例管理页面，选择某一实例的管理链接进入后端服务器配置界面，进入实例详情页

。

在左侧导航选择**后端服务器**，然后单击**未添加的服务器**页签，将ECS1和ECS2添加到公网SLB1实例下。

配置私网业务的云产品部署。

打开名称为“业务网络B”的交换机页面，单击**创建实例**下拉菜单，分别创建ECS3、ECS4、RDS2、SLB2。

登录负载均衡控制台，通过后端服务器的配置，将两台ECS实例添加到公网负载均衡实例下。

进入实例管理页面，选择某一实例的管理链接进入后端服务器配置界面，进入实例详情页。

在左侧导航选择**后端服务器**，然后单击**未添加的服务器**页签，将ECS3和ECS4添加到公网SLB2实例下。

API

涉及的相关API文档如下：

VPC

创建专有网络

新建交换机

ECS

- 创建实例

负载均衡

创建负载均衡实例

添加后端服务器

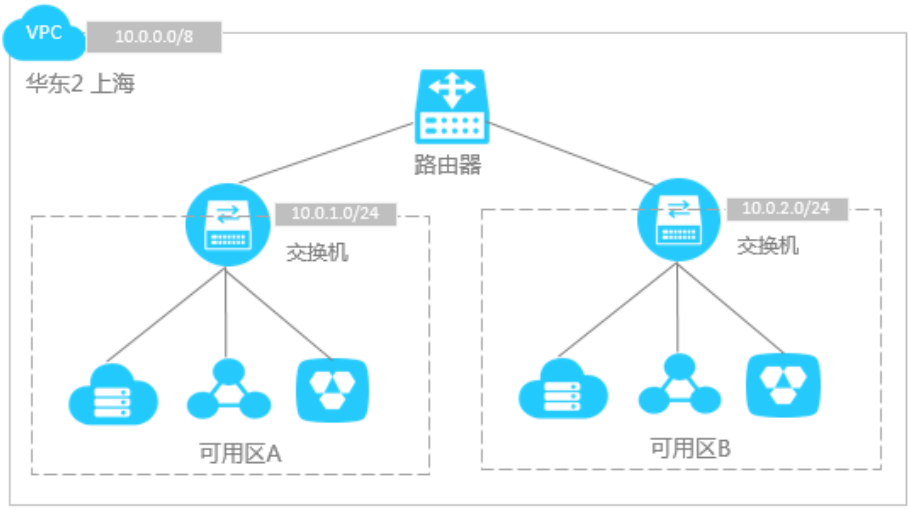
RDS

- 创建RDS实例

应用场景

您可以通过将资源部署在处于不同可用区的交换机中，实现利用阿里云可用区进行容灾。本文以地域华东2 为例，可用区使用华东2的可用区A和可用区B，进行跨可用区的资源部署。

当阿里云华东2可用区A机房发生异常时，仍能够通过部署在华东2可用区B机房的备服务器提供服务。



网络规划

- 地域：华东 2，可用区：华东2可用区A、华东2可用区B
- 专有网络网段为10.0.0.0/8
- 将两个应用部署在两个不同可用区的交换机中，子网网段分别是10.0.1.0/24、10.0.2.0/24
- 在两个不同可用区的交换机中分别部署ECS、负载均衡、RDS

操作步骤

登录专有网络管理控制台https://vpc.console.aliyun.com/#/vpc/cn-shanghai/list，地域选择**华东2**。

单击**创建专有网络**，弹出**创建专有网络**对话框，填写如下信息。

- **专有网络名称**：VPC_B
- **网段**：10.0.0.0/8

在专有网络VPC_B中，创建两个交换机。

i. 在华东2地域的专有网络列表，选择VPC_B的**管理**链接，进入**专有网络基本信息**页面。

ii. 在左侧导航栏，单击**交换机**，然后单击**创建交换机**，弹出**创建交换机**对话框，填写下面的信息完成交换机1的创建。

- **名称**：业务网络主
- **可用区**：华东2可用区A
- **网段**：10.0.1.0/24

iii. 创建交换机2，同样在专有网络VPC_B下创建交换机。

- **名称**：业务网络备
- **网段**：10.0.2.0/24
- **可用区**：华东2可用区B

配置业务相关云产品部署。

i. 在交换机列表的**业务网络主**中创建如下云产品实例ECSx2、RDSx1，作为服务的主服务器和数据库。单击**创建实例**下拉菜单，分别创建ECS1、ECS2、RDS1。

ii. 在交换机列表的**业务网络备**中创建如下云产品实例ECSx2、RDSx1，作为服务的备服务器和数据库。单击**创建实例**下拉菜单，分别创建ECS3、ECS4、RDS2。

iii. 在地域华东2(上海)下创建两台公网负载均衡，选择主可用区为华东2可用区A，备可用区为华东2可用区B，并将两个交换机下的四台ECS实例分别添加到公网负载均衡实例下。创建和配置负载均衡的具体方法，请参考 负载均衡快速入门。

API

涉及的相关API文档如下：

VPC

创建专有网络

新建交换机

ECS

- 创建实例

负载均衡

创建负载均衡实例

添加后端服务器

RDS

- 创建RDS实例

VPC内如何使用云产品

如何选择使用专有网络

专有网络VPC（Virtual Private Cloud）是隔离的私有网络。默认情况下，VPC之间是无法通过私网通信的，VPC内的ECS也无法访问公网或者被公网访问，并且VPC不能通过私网访问经典网络。但是阿里云产品一般都提供公网访问能力和专有网络访问能力，95%以上的云产品都已经支持VPC。

> **注意**：需要内部访问的云产品一定要使用相同的网络类型。比如ECS是使用VPC类型的，要通过私网访问负载均衡和RDS实例，那么该负载均衡和RDS实例则也必须使用VPC类型的，否则无法访问。

针对不同的云产品，您选择使用专有网络VPC的方式也不同：

通过购买页提供网络类型选择

这种方式以实例型云产品为主，如ECS，RDS，负载均衡等，这种云产品一般在购买页提供了网络类型选择，选择专有网络的网络类型即可。这些实例购买后，会获得一个VPC类型的实例或访问域名，本质上都是用户VPC地址段内的一个IP地址。

下图是ECS购买页面的网络类型选择。

下图是RDS购买页面的网络类型选择。

下图是负载均衡购买页面的网络类型选择。

通过控制台提供VPC私网访问方式

比如表格存储、容器服务、E-MapReduce、文件存储等云产品，您可以在表格存储控制台针对表格存储实例设置VPC访问域名。容器服务和E-MapReduce通过控制台创建集群的时候可以选择网络类型。文件存储产品在控制台提供专有网络VPC类型的挂载点。需要注意相关产品控制台的设置。

通过文档方式提供VPC私网访问方式

比如日志服务、对象存储等云产品，您可以查看以下相关云产品帮助文档：

日志服务的VPC访问入口说明

对象存储的VPC访问入口说明

如何切换专有网或经典网络

阿里云近期会陆续提供从经典网络迁移到VPC的解决方案，相关文档会更新的官方网站。

对于部分实例型云产品，云产品提供了网络切换的功能，比如RDS等数据库产品，可以在控制台进行网络类型的切换，从经典网络切换到VPC网络。

对于ECS产品，后续也会提供从经典网络切换到VPC网络的能力。

对于负载均衡产品，目前不支持将经典网络实例切换为VPC网络的实例，您可以重新购买一个VPC类型的实例并挂载VPC ECS。

注意：还有一些云产品不需要支持VPC，比如CDN，态势感知这样的云产品。