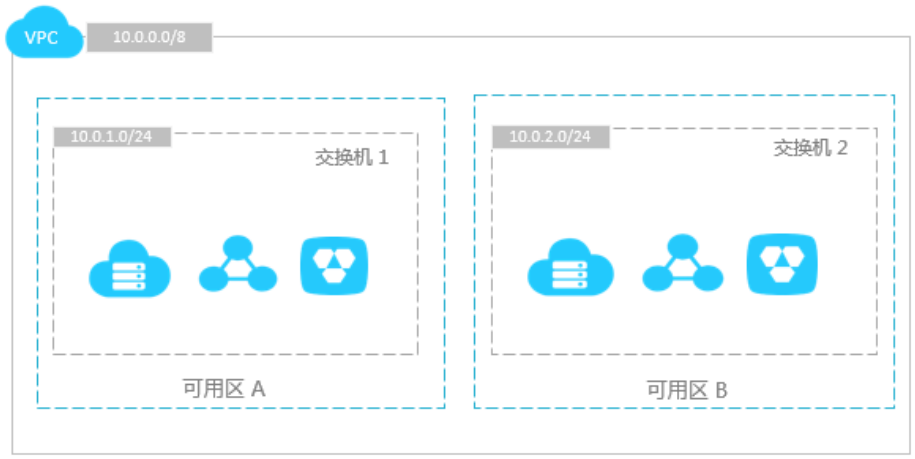
专有网络 VPC

产品简介

产品简介

专有网络VPC（Virtual Private Cloud）是您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。您能够在自己定义的虚拟网络中使用阿里云资源。

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。



默认专有网络和交换机

当您在创建一个云服务实例时，如果您没有提前创建专有网络和交换机，您可以使用系统提供的默认专有网络配置。在实例创建后，一个默认的专有网络和交换机也会随之创建好。

默认专有网络和交换机说明

默认专有网络	默认交换机

每个地域的默认专有网络唯一。	每个可用区的默认交换机唯一。
默认专有网络的网络掩码是16位，如172.31.0.0/16，最多可提供65536个私网IP地址。	默认交换机的网络掩码是20位，如172.16.0.0/20，最多可提供4096个私网IP地址。
默认专有网络不占用阿里云为您分配的专有网络配额。	默认交换机不占用专有网络中可创建交换机的配额。
默认专有网络由阿里云为您创建，您自行创建的均为非默认专有网络。	默认交换机由阿里云为您创建，您自行创建的均为非默认交换机。
默认专有网络与非默认专有网络的操作方式与规格限制一致。	默认交换机与非默认交换机的操作方式与规格限制一致。

专有网络和经典网络

阿里云提供如下两种网络类型：

经典网络

经典网络类型的云产品，统一部署在阿里公共基础内，规划和管理由阿里云负责，更适合对网络易用性要求比较高的客户。

专有网络

专有网络是一个可以自定义隔离专有网络， 您可以自定义这个专有网络的拓扑和IP地址，适用于对网络安全性要求较高和有一定的网络管理能力的客户。

经典网络和专有网络的功能差异如下表所示。

经典网络和专有网络的区别

功能	经典网络	专有网络
二层逻辑隔离	不支持	支持
自定义私网网段	不支持	支持
私网IP规划	经典网络内唯一	专有网络内唯一，专有网络间可重复
私网互通	账号内相同地域内互通	专有网络内互通，专有网络间隔离
隧道技术	不支持	支持
自定义路由器	不支持	支持
路由表	不支持	支持
交换机	不支持	支持
SDN	不支持	支持

自建NAT网关	不支持	支持
自建VPN	不支持	支持

背景信息

随着云计算的不断发展，对虚拟化网络的要求越来越高，比如弹性（scalability）、安全性（security）、可靠性（reliability）和私密性（privacy），并且还有极高的互联性能（performance）需求，因此催生了多种多样的网络虚拟化技术。

比较早的解决方案，是将虚拟机的网络和物理网络融合在一起，形成一个扁平的网络架构，例如大二层网络。随着虚拟化网络规模的扩大，这种方案中的ARP欺骗、广播风暴、主机扫描等问题会越来越严重。为了解决这些问题，出现了各种网络隔离技术，把物理网络和虚拟网络彻底隔开。其中一种技术是用户之间用VLAN进行隔离，但是VLAN的数量最大只能支持到4096个，无法支撑公共云的巨大用户量。

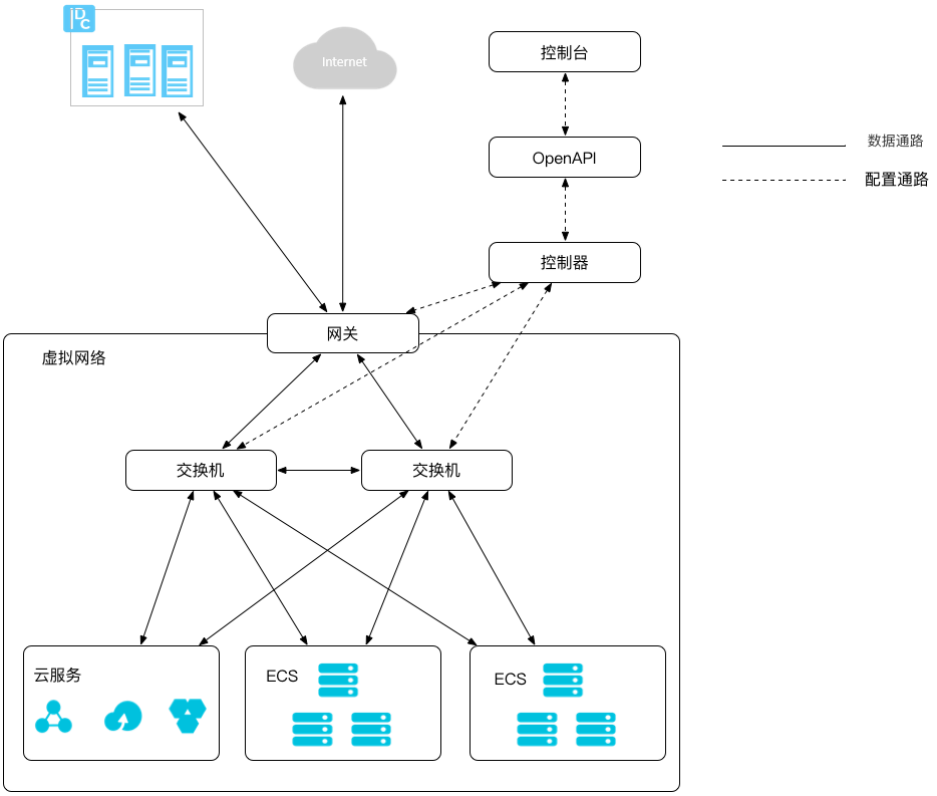
原理描述

基于目前主流的隧道技术，专有网络（Virtual Private Cloud，简称VPC）隔离了虚拟网络。每个VPC都有一个独立的隧道号，一个隧道号对应着一个虚拟化网络。一个VPC内的ECS（Elastic Compute Service）实例之间的传输数据包都会加上隧道封装，带有唯一的隧道ID标识，然后送到物理网络上进行传输。不同VPC内的ECS实例因为所在的隧道ID不同，本身处于两个不同的路由平面，所以不同VPC内的ECS实例无法进行通信，天然地进行了隔离。

基于隧道技术和软件定义网络（Software Defined Network，简称SDN）技术，阿里云的研发在硬件网关和自研交换机设备的基础上实现了VPC产品。

逻辑架构

如下图所示，VPC包含交换机、网关和控制器三个重要的组件。



交换机和网关组成了数据通路的关键路径，控制器使用自研的协议下发转发表到网关和交换机，完成了配置通路的关键路径。整体架构里面，配置通路和数据通路互相分离。交换机是分布式的结点，网关和控制器都是集群部署并且是多机房互备的，并且所有链路上都有冗余容灾，提升了VPC产品的整体可用性。

交换机和网关性能在业界都是领先的。自研的SDN协议和控制器，能轻松管控公共云成千上万张虚拟网络。

专有网络VPC（Virtual Private Cloud）帮助您基于阿里云构建出一个隔离的网络环境。除了给您提供一个独立的虚拟化网络，阿里云还为每个VPC提供独立的路由器和交换机组件。您可以完全掌控自己的虚拟网络，包括私网IP地址范围、子网网段和路由配置等。

专有网络

专有网络是您基于阿里云创建的自定义私有网络，不同的专有网络之间彻底逻辑隔离。您可以在自己的专有网络内创建和管理云产品实例，比如ECS，SLB和RDS。

在创建专有网络时，您需要以CIDR block的形式指定专有网络内使用的私网网段。关于CIDR block的相关信息，请参见维基百科上的Classless Inter-Domain Routing条目说明。

您可以使用下表中标准的私网网段及其子网作为VPC的私网地址。

VPC可用的私网IP地址

网段	可用私网IP数量（不包括系统保留）
192.168.0.0/16	65532
172.16.0.0/12	1048572

10.0.0.0/8	16777212

专有网络创建成功之后，网段无法修改。建议使用比较大的网段，尽量避免后续扩容。系统不会根据VPC的网段来创建系统路由，所以使用比较大的地址范围来创建VPC，不会影响业务的正常使用。

交换机

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。创建专有网络之后，您可以通过添加交换机为专有网络划分一个或多个子网，每个专有网络的交换机数量不能超24个。

在专有网络中创建交换机时，您必须也要以CIDR block的形式为其指定网段。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。更多网络规划的信息，参考VPC网络规划。

> 注意：交换机不支持组播和广播。

IP地址

IP地址使VPC中的资源能够相互通信以及与Internet上的资源进行通信，是您访问云产品实例以及云产品实例对外提供服务的主要方式。在阿里云专有网络中，会出现如下几种类型的IP地址：

私网IP

私网IP是在专有网络中创建实例时分配的IP地址，例如专有网络类型云服务器ECS实例的私网IP、专有网络类型负载均衡实例的私网IP、专有网络类型云数据库实例的私网IP等。私网IP无法通过Internet访问，但可以用于专有网络中云产品实例之间的通信，例如ECS实例之间私网互访、ECS实例与其它云服务（OSS、RDS）之间私网互访、提供私网负载均衡服务等。

与经典网络中的系统统一分配的内网IP地址不同，专有网络的私网IP地址是根据实例所属的交换机网段分配的。所以某个实例的私网IP地址在专有网络中唯一，分配给云产品实例的私网IP可以在该实例属性中查看。

公网IP

公网IP是在专有网络中创建ECS实例时分配的公网IP地址。您可以通过该公网IP访问公网或者提供公网服务。

> **注意**：公网IP不是必选项。在创建专有网络类型的ECS实例时，您可以选择不分配公网IP。

弹性公网IP

弹性公网IP（Elastic IP Address，简称 EIP），是可以独立购买和持有的公网IP地址资源，能动态绑

定到不同的ECS实例上，绑定和解绑时不影响实例运行。

弹性公网IP是一种NAT IP。它实际位于阿里云的公网网关上，通过NAT方式映射到了被绑定ECS实例的私网网卡上。因此，绑定了弹性公网IP的ECS实例可以直接使用这个IP进行公网通信，但是在网卡上并不能看到这个IP地址。

注意：在阿里云各项资源中，目前只有ECS实例支持绑定弹性公网IP。

路由器

路由器（VRouter）是专有网络的枢纽。作为专有网络中重要的功能组件，它可以连接VPC内的各个交换机，同时也是连接VPC与其它网络的网关设备。

路由器支持静态路由，同时支持专线接入VPC场景的负载分担、等价、主备等路由配置方式。

创建VPC时，系统会自动为VPC创建一个路由器和一个路由表。您不可以直接删除专有网络的路由器或路由表，但可以在路由表中添加新的路由条目，来转发流量。当删除VPC后，关联的路由器和路由表也会随之删除。

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，路由条目包括系统路由和自定义路由。

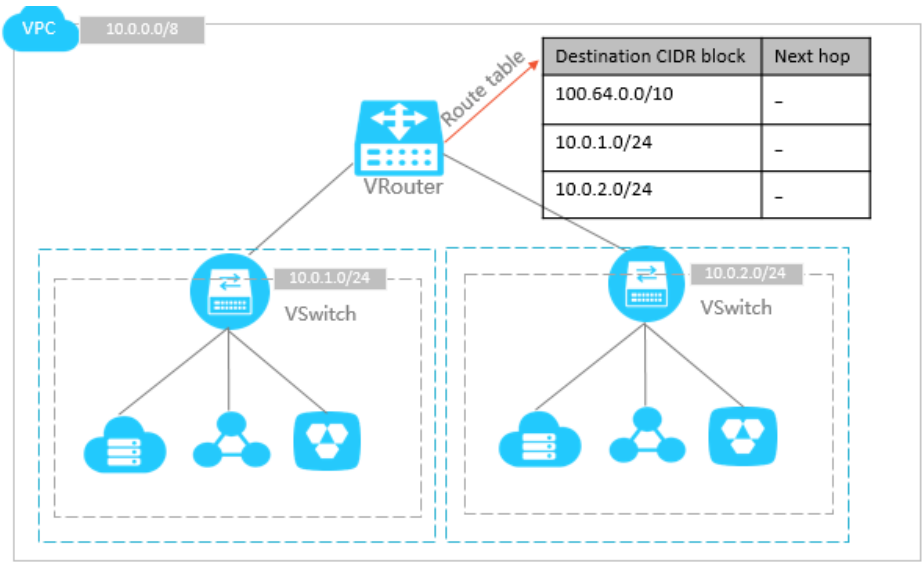
系统路由

创建VPC时，系统会自动添加一条目标网段为100.64.0.0/10的系统路由条目，用于VPC内的云产品通信。

另外，系统也会为创建的交换机自动添加一条以交换机网段为目标网段的系统路由。

自定义路由

您可以根据需要，添加自定义路由。详情参考管理路由表。



阿里云的专有网络具有如下明显优势：

安全隔离

- 不同用户的云服务器部署在不同的专有网络里。
- 不同专有网络之间通过隧道ID进行隔离。专有网络内部由于交换机和路由器的存在，所以可以像传统网络环境一样划分子网，每一个子网内部的不同云服务器使用同一个交换机互联，不同子网间使用路由器互联。
- 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。
- 由于使用隧道封装技术对云服务器的IP报文进行封装，所以云服务器的数据链路层（二层MAC地址）信息不会进入物理网络，实现了不同云服务器间二层网络隔离，因此也实现了不同专有网络间二层网络隔离。
- 专有网络内的ECS使用安全组防火墙进行三层网络访问控制。

访问控制

- 灵活的访问控制规则。
- 满足政务，金融的安全隔离规范。

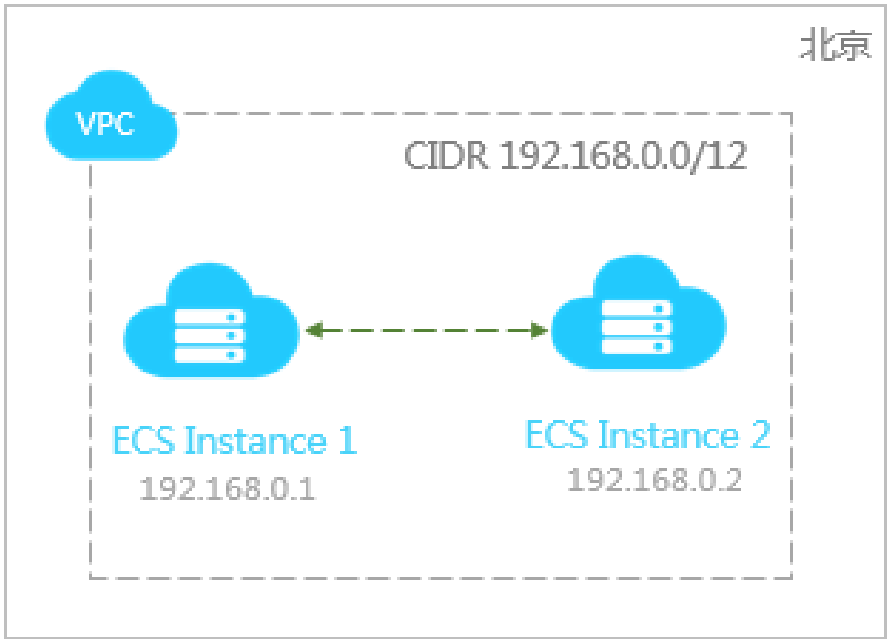
软件定义网络

- 按需配置网络设置，软件定义网络。
- 管理操作实时生效。

丰富的网络连接方式

- 支持软件VPN。
- 支持专线连接。

专有网络是完全隔离的网络环境。默认情况下，相同专有云网络内的ECS和云服务可以进行私网通信，但VPC与VPC之间、VPC与经典网络或公网不能互通。您可以使用弹性公网IP、高速通道、NAT、VPN网关或公网负载均衡等公网产品实现专有网络间的通信。

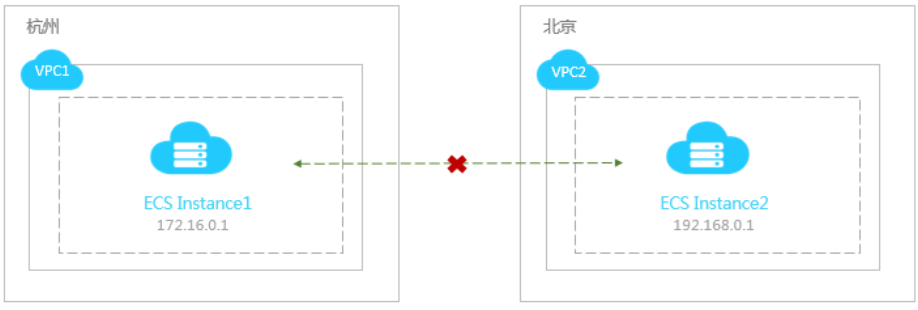


本文介绍了如下情况的VPC通信：

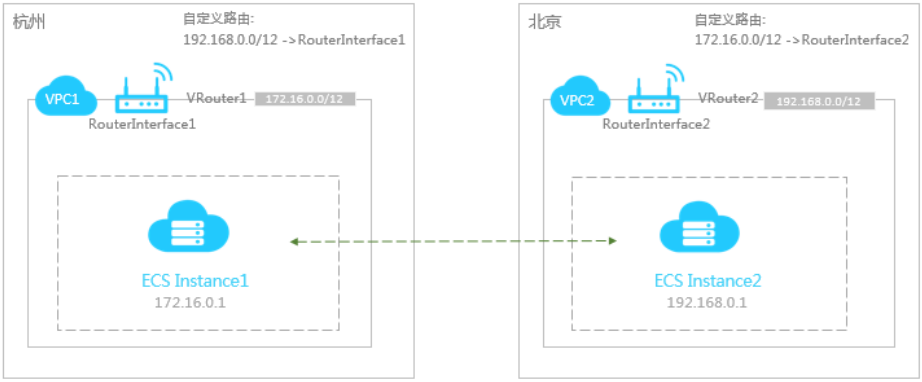
- VPC与VPC通信
- VPC与经典网络通信
- VPC与Internet通信
- VPC与本地IDC通信

VPC与VPC通信

默认情况，不同专有网络间的ECS不能直接进行私网通信。

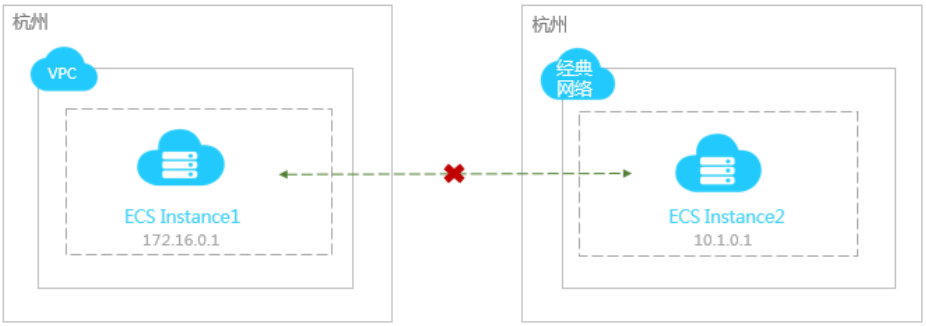


您可以使用高速通道的路由器接口，在两侧VPC的路由器上分别创建路由器接口，以及自有的骨干传输网络来搭建高速通道，轻松实VPC之间安全可靠、方便快捷的通信。配置详情参考同账号下专有网络内网互通。



VPC与经典网络通信

如下图所示，专有网络内的ECS不能访问经典网络的ECS或者云服务。



VPC访问经典网络

VPC与经典网络可以通过公网IP进行通信。只要VPC和经典网络中的ECS实例或云实例的公网IP符合下表中的任意一一条要求，专有网络就可以访问经典网络的云服务。

网络	配置要求
VPC	- 创建ECS实例时为其分配了一个公网IP。 - 在ECS实例上绑定一个弹性公网IP。 - 在ECS实例上配置NAT网关（SNAT）。
经典网络	- ECS实例有可用的公网IP。 - 该ECS实例被添加到一个公网负载均衡实例中。此时专有网络的云服务通过访问公网负载均衡的服务地址将请求转发给后端ECS实例。

经典网络访问VPC

反之，经典网络也可以通过公网IP访问VPC，只要VPC中的ECS实例或云服务也配置了公网IP。

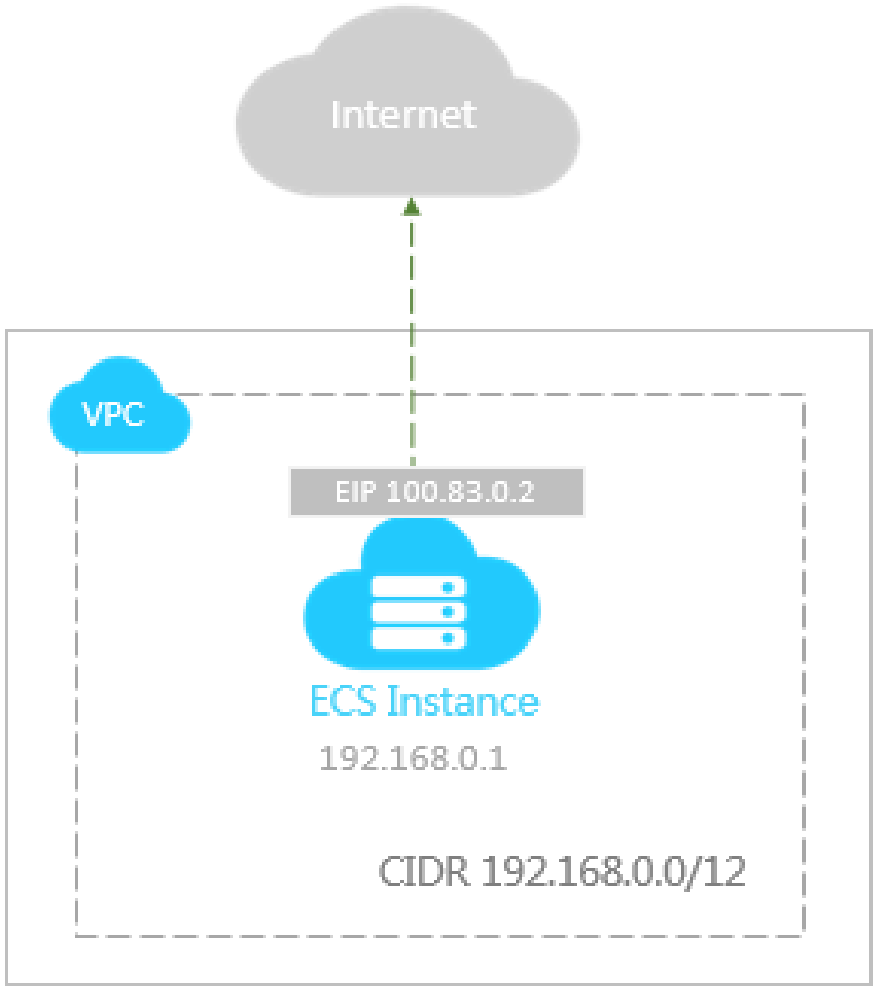
网络	配置要求
经典网络	- ECS实例有可用的公网IP。
VPC	- 创建ECS实例时为其分配了一个公网IP。 - 在ECS实例上绑定一个弹性公网IP。 - 在ECS实例上配置NAT网关（DNAT）。 - 该ECS实例被添加到一个公网负载均衡实例中。此时来自公网的请求可以经过公网负载均衡实例转发给后端ECS服务器。

VPC与Internet通信

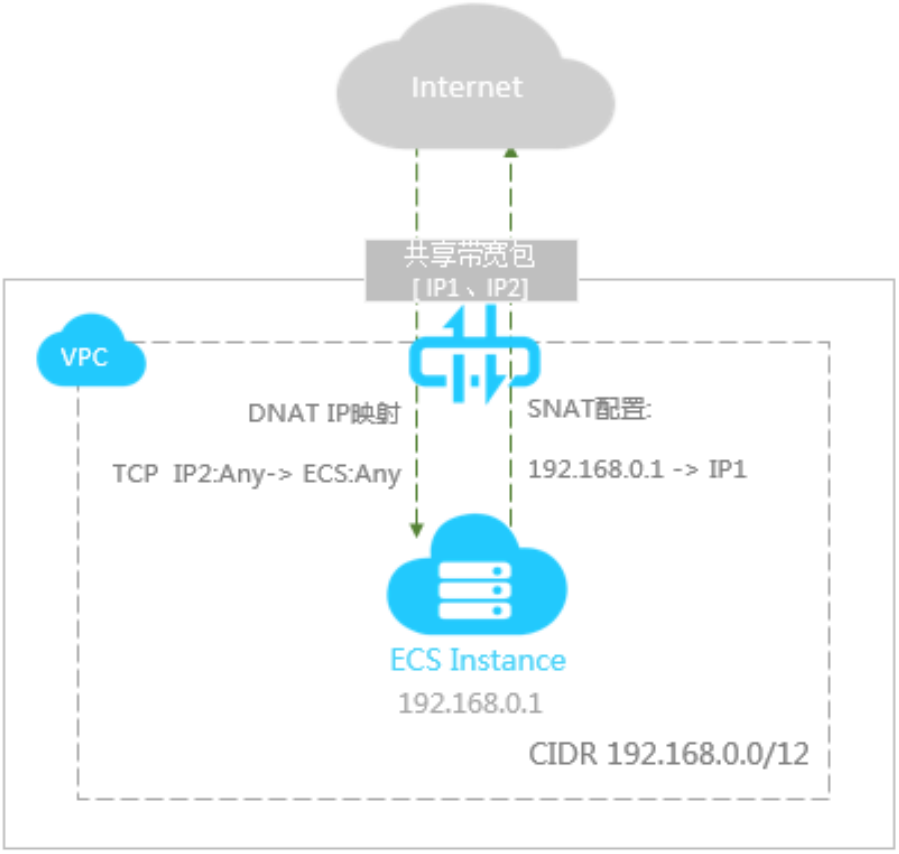
默认情况下，专有网络内的ECS不能与公网互通。您可以通过以下途径中的一种打通VPC与公网的通信：

为专有网络中的ECS实例分配公网IP，实现专有网络与公网的通信。详情参考分配公网IP。

您可以通过在ECS上绑定弹性公网IP，实现专有网络与公网的互通。详情参考弹性公网IP。



在专有网络的ECS上设置NAT网关，实现专有网络与公网的互通。详情参考端口映射和SNAT设置。



注意： 如果您有多台ECS需要和公网互通，您可以使用NAT网关的共享带宽包，一个带宽包内的所有ECS实例共享带宽，以节省您的费用。

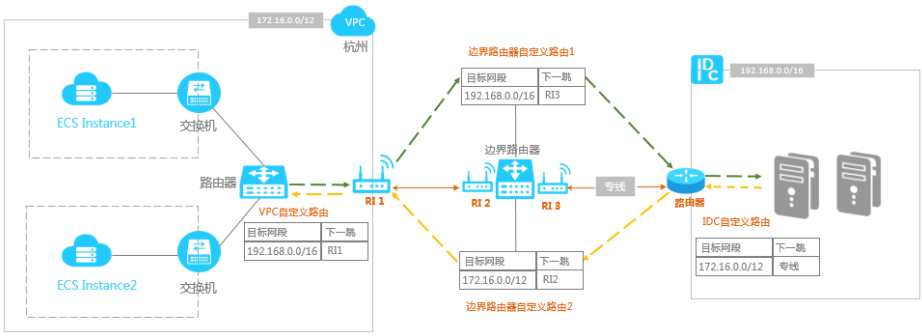
专有网络的ECS实例添加到一个公网负载均衡实例中。详情参考配置公网负载均衡。

注意：此情形下，专有网络中的ECS实例不能访问公网，只能接收负载均衡转发的公网请求。

VPC与本地IDC通信

默认情况下，本地IDC网络中心和专有网络之间不能通信，您可以通过以下途径打通本地IDC与VPC之间的通信：

您可以使用高速通道的物理专线来连通本地IDC到阿里云的专线接入点，并建立虚拟边界路由器作为VPC到IDC的数据转发桥梁。详情参考专线接入。



您可以使用VPN网关来实现本地IDC网络中心与专有网络的互通，详情参考搭建VPN网关。

术语	英文	说明
专有网络	VPC	专有网络是您基于阿里云创建的自定义私有网络，不同的专有网络之间彻底逻辑隔离。您可以在自己创建的专有网络内创建和管理云产品实例，例如ECS，SLB，RDS等。
交换机	VSwitch	交换机是组成专有网络的基础网络设备。它可以连接不同的云产品实例。在专有网络内创建云产品实例时，必须指定云产品实例所连接的交换机。
路由器	VRouter	路由器是专有网络的枢纽。它可以连接专有网络的各个交换机，同时也是连接专有网络与其它网络的网关设备。路由器根据具体的路由条目的设置来转发网络流量。
路由条目	Route Entry	路由表中的每一项是一条路由条目。路由条目定义了通向指定目标网段的网络流量的下一跳地址。路由条目包括系统路由和自定义路由两种类型。
路由表	Route Table	路由表是指路由器上管理路由条目的列表。

专有网络

限制项	普通用户限制说明	例外申请方式
单个账号的专有网络个数	10个	工单
专有网络可选的网段范围	192.168.0.0/16，172.16.0.0/12，10.0.0.0/8以及它们的子网	工单

单个专有网络的路由器个数	1个	没有例外
单个专有网络的交换机个数	24个	没有例外
单个专有网络的路由表个数	1个	没有例外
单个路由表的路由条目数量	48条	工单
单个专有网络容纳云产品数量	10,000个	没有例外

路由器和交换机

分类	限制说明
路由器	- 每个VPC有且只有1个路由器。 - 路由器不支持BGP和OSPF等动态路由协议。 - 每个路由器有且只有1个路由表。 - 路由表的路由条目会影响VPC中的所有云产品实例。目前不支持指定交换机和云产品实例的源地址策略路由。
交换机	- VPC的交换机不支持二层广播和组播。 - 交换机本身对云产品实例数量没有限制。它能够容纳多少实例，取决于所在专有网络当前的云产品实例数量，即10,000减去当前已保有的云产品数量。 - 交换机的网段不可以进行修改。

专有网络ECS实例的迁移限制

您可以在VPC网络中将ECS实例从某一路由器下的一台交换机转移到另一台交换机，但不支持以下操作：

- ECS实例不支持跨路由器切换。
- ECS实例不支持网络类型之间的切换，不支持从专有网络迁移到经典网络和不支持从经典网络迁移到专有网络。

发布时间	发布内容
2015年08月4日	全网开放，功能包括专有网络（VPC）、路由器（VRouter）、路由表（RouteTable）、交换机（VSwitch）
2015年12月28日	专有网络支持资源访问控制服务(RAM)

2016年03月29日	全文整改和优化
2016年03月30日	默认专有网络功能上线