专有网络 VPC

用户指南

用户指南

默认VPC和交换机

默认VPC和交换机

当创建一个云产品实例时，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。详情参考使用默认专有网络创建ECS实例。

默认专有网和交换机的配置如下表所示。

默认专有网络VPC	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
默认专有网络的网段掩码是16位，如172.31.0.0/16，最多可提供65536个私网IP地址	默认交换机的网段掩码是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

搭建专有网络

创建VPC

前提条件

确保您已经做好了网络规划包括创建几个VPC、VPC的网段、需要几个交换机以及其他规划，详情参考**网络规划**。

操作步骤

登录**专有网络管理控制台**。

在左侧专有网络导航栏，单击**专有网络**。

选择专有网络的地域。

在专有网络列表页面，单击右上角的**创建专有网络**。

在**创建专有网络**对话框，输入以下信息，然后单击**创建VPC**。

配置	**说明**
专有网络名称	输入专有网络的名称。
描述（可选）	添加描述。
网段	选择专有网络的网段。 - 您可以使用阿里云提供的三个标准私网网段（10.0.0.0/8 、172.16.0.0/12、192.168.0.0/16 ）及其子网作为VPC的网段。 **注意** ：如果要使用标准网段的子网作为VPC的网段，需要使用Open API去创建VPC。 - 如果有多个VPC，或者VPC和本地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并且不需要和本地IDC互通，那么选择以上任何一个网段或其子网。 - 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），建议您不要使用10.0.0.0/8作为VPC的网段。 - **注意**：如有除此之外的特殊网段要求，您可拨打客服电话或在阿里云管理控台提交提交在线工单进行咨询。

相关操作

创建交换机

交换机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，详情参考创建交换机。

管理路由表

成功创建VPC后，系统会默认为该VPC创建一个路由器和路由表。您可以在路由表中，添加自定义路由条目，详情参考管理路由表。

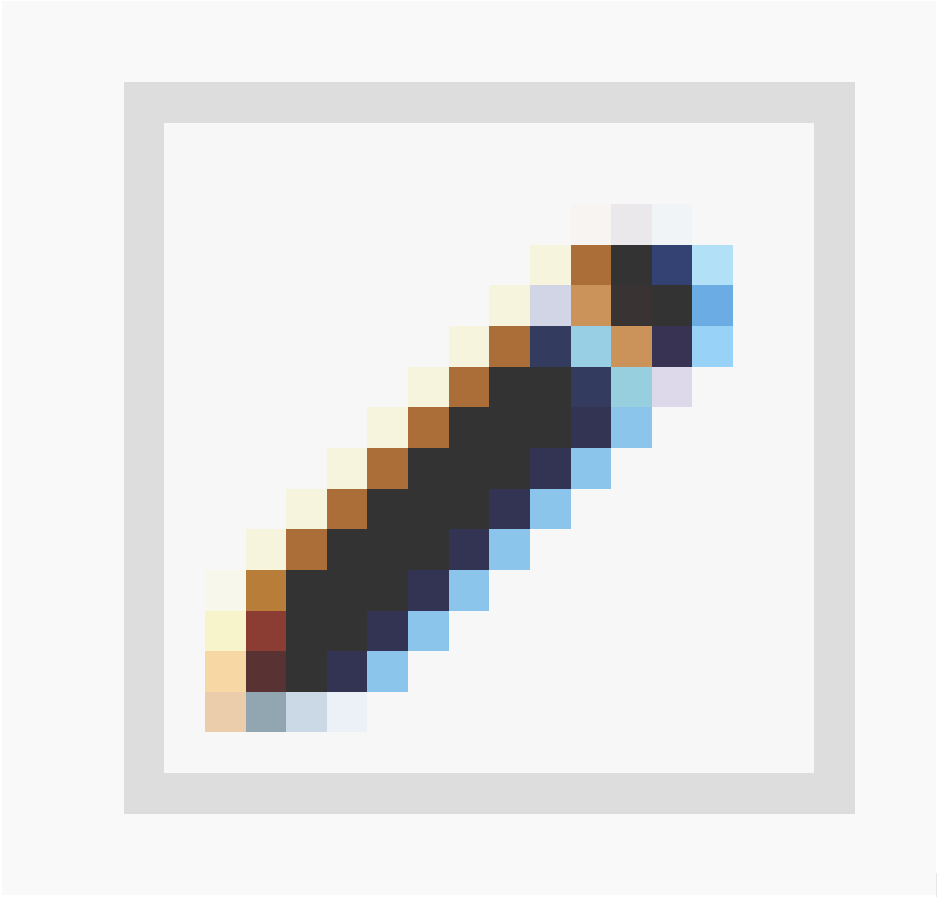
删除VPC

在专有网络列表页面，单击**删除**，在**删除专有网络**对话框中单击**确定**删除该VPC。

注意：删除专有网络之前，需要先释放或移走专有网络内的所有实例资源。

修改VPC名称

将鼠标移至VPC ID区域，单击



图标，修改VPC名称。

相关API

创建VPC

删除VPC

查询专有网络列表

修改专有网络属性

创建交换机

前提条件

网络规划

创建专有网络

操作步骤

登录**专有网络管理控制台**。

在左侧导航栏，单击**专有网络**。

选择专有网络的地域。

在专有网络列表页面，单击目标专有网络的ID链接。

在专有网络详情导航栏，单击**交换机**。

单击**创建交换机**，输入以下信息，然后单击**确定**。

交换机创建成功后，系统会为该交换机创建一条路由条目。这个系统路由条目的目标网段是交换机的网段。

配置	**说明**
专有网络	显示要创建的交换机所属的专有网络ID。
专有网络网段	显示当前专有网络的网段。 您可以单击**显示二进制**，以二进制的形式查看网段。
名称	输入交换机的名称。
可用区	选择交换机的可用区。 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。建议您将交换机部署在不同可用区内，这样可以实现跨可用区容灾。
网段	输入交换机的网段。 - 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，可提供8-65536个地址。 - 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。
可用IP数	显示指定网段下可用的IP地址数量。
描述（可选）	添加交换机描述。

相关操作

创建专有网络云服务

在**交换机列表**页面，单击**创建实例**，选择您要在该专有网络子网内创建的云服务器实例。详情参考在VPC中创建云产品实例。

修改交换机

在**交换机列表**页面，单击**编辑**修改交换机的名称和描述；或者将鼠标移至交换机ID上，单击出现的铅笔图标，修改交换机的名称。

删除交换机

在**交换机列表**页面，单击**删除**，在**删除交换机**对话框中单击**删除**该交换机。

注意：删除交换机之前，确保您已经将该交换机下的云服务转移或释放。

相关API

创建交换机

删除交换机

查询交换机列表

修改交换机属性

管理路由表

概述

路由器是专有网络的枢纽。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。

创建VPC时，系统会自动为VPC创建一个路由器和一个路由表。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。路由表根据具体的路由条目的设置来转发网络流量。

> **注意**：您不可以直接创建或删除路由器和路由表。当您删除了一个VPC后，系统会将该VPC关联的路由器和路由表删除。

路由条目包括系统路由和自定义路由两种类型。

系统路由

您不可以修改或删除系统路由。

创建专有网络时，系统会自动创建一条系统路由条目。

该系统路由条目的目标网段为100.64.0.0/10，VPC中的云产品使用该网段提供服务。

创建交换机时，系统也会创建一条对应的系统路由条目。

该路由条目的目标网段为所创建交换机的网段，用于VPC内的云产品实例的通信。

自定义路由条目

您可以创建和删除自定义路由条目。每个路由表最多只能创建48个自定义路由条目。

> 注意：一般情况下，系统路由条目已经可以满足需求。只有当您有特殊场景需求时，才需要添加自定义路由条目。在添加自定义路由条目前，请规划好您的网络部署。

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。最长前缀匹配是指当路由表中有多条条目可以匹配目的IP时，采用掩码最长（最精确）的一条路由作为匹配项并确定下一跳。

某专有网络的路由表如下表所示。

目标网段	下一跳类型	下一跳	路由条目类型
100.64.0.0/10			系统
192.168.0.0/24			系统
0.0.0.0/0	Instance	i-12345678	自定义
10.0.0.0/24	Instance	i-87654321	自定义

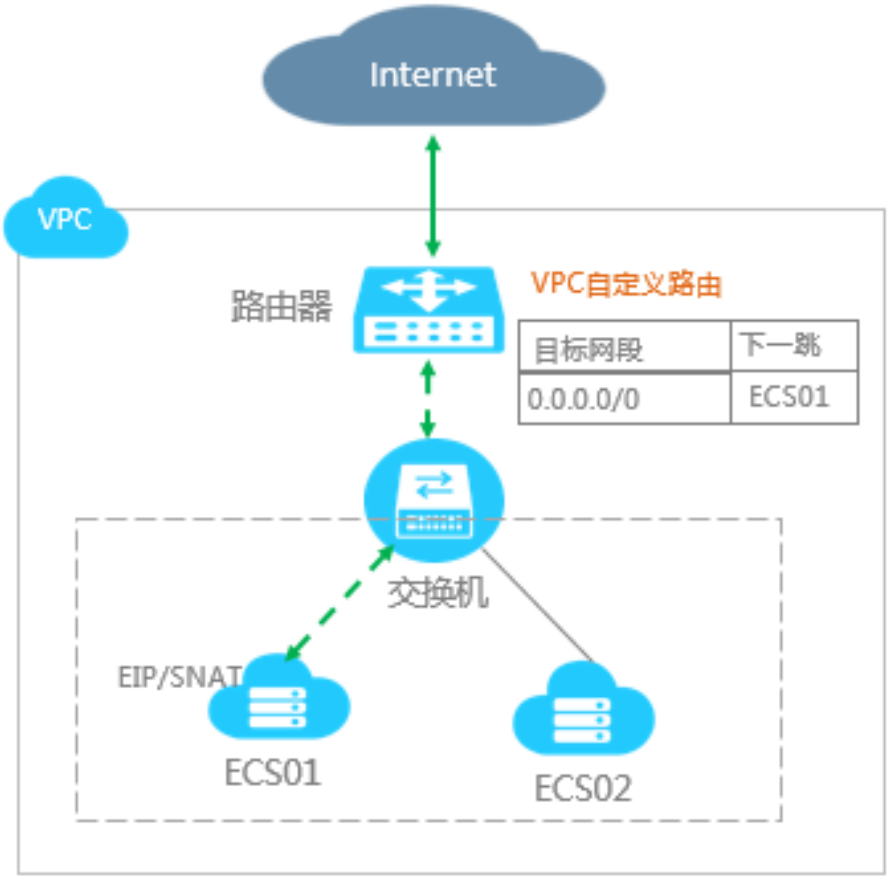
目标网段为100.64.0.0/10和192.168.0.0/24的两条路由均为系统路由条目，前者为系统保留的地址段，后者为专有网络中为交换机配置的系统路由条目。

目标网段为0.0.0.0/0和10.0.0.0/24的两条路由为自定义路由，表示将访问0.0.0.0/0地址段的流量转发至ID为i-12345678的ECS实例，将访问10.0.0.0/24地址段的流量转发至ID为i-87654321的ECS实例。根据最长前缀匹配规则，在该专有网络中，访问10.0.0.1的流量会转发至i-87654321，而访问10.0.1.1的流量会转发至i-12345678。

自定义路由条目规划

VPC内网路由

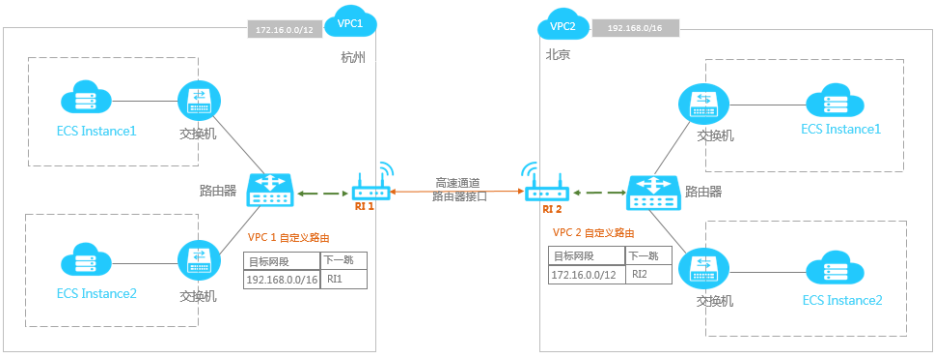
如下图所示，比如您在一个VPC内创建了两个ECS实例，分别为ECS01和ECS02。ECS01绑定了一个弹性公网IP, 为ECS01提供访问Internet的代理服务。当您想将ECS02的请求都路由到ECS01进行公网访问时，可以添加一条自定义路由。



目标网段	下一跳类型	下一跳
0.0.0.0/0	ECS实例	ECS01

VPC互通

如下图所示，比如您有两个VPC，分别为VPC1（网段：172.16.0.0/12）和VPC2（网段：192.168.0.0/16）。如果您想让两个VPC之间互通，您需要使用高速通道产品，购买一个路由器接口，将VPC1设置为本端，VPC2设置为对端。购买完成后，系统会分别在发起端和接受端创建两个互为对端的路由器接口（RI1和RI2）。最后要实现两个VPC互通，您需要添加如下路由条目。



VPC1的路由配置

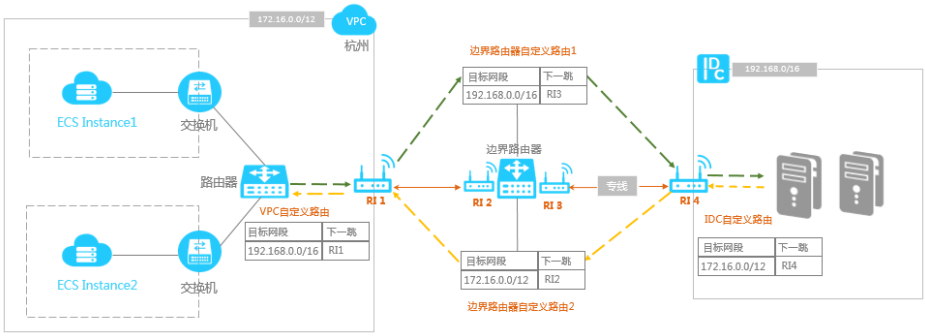
目标网段	下一跳类型	下一跳
192.168.0.0/16	路由器接口（普通路由）	RI1

VPC2的路由配置

目标网段	下一跳类型	下一跳
172.16.0.0/12	路由器接口（普通路由）	RI2

VPC与本地IDC互通

如下图所示，比如您有一个网段为172.16.0.0/12的VPC，在北京有一个网段为192.168.0.0/16的IDC。当您想打通VPC与本地IDC的通信时，您需要在高速通道产品中申请物理专线接入，并配置边界路由器，然后创建一个路由器接口连接边界路由器和VPC，最后需要添加如下路由。



VPC端的路由配置

目标网段	下一跳类型	下一跳
192.168.0.0/16	路由器接口（普通路由）	RI1

边界路由器的路由配置

目标网段	下一跳类型	下一跳
192.168.0.0/16	指向专线	RI3
172.16.0.0/12	指向VPC	RI2

IDC端的路由配置

目标网段	下一跳类型	下一跳
172.16.0.0/12	—	RI4

添加自定义路由条目

登录**专有网络管理控制台**。

在左侧专有网络导航栏，单击**专有网络**。

选择专有网络的地域。

在专有网络列表页面，单击需要添加路由的专有网络ID。

在专有网络详情页面的左侧菜单栏，单击**路由器**，然后单击**添加路由**。

在**添加路由**对话框，配置以下信息，单击**确定**。

配置	说明
目标网段	指定该路由的目标网段。 您可以输入一个IP地址或者一个CIDR形式的网段。如果您输入了一个IP地址，默认使用32位子网掩码。
下一跳类型	选择下一跳类型。 - ECS实例：将来自目标网段的请求转发到ECS实例。 - 路由器接口：将来自目标网段的转发到指定的路由器接口。请求会经过该路由器接口路由到对应的对端路由器接口。 - VPN网关：将来自目标网段的请求路由到指定的VPN网关。
下一跳	根据您选择的下一跳类型，指定具体的下一跳。 **注意**：如果您选择了等价路由，需要选择2-4个实例作为路由下一跳，且作为下一跳的路由器接口实例的对端路由器类型必须为边界路由器。

专有网络中的ECS安全组设置

当您创建专有网络类型的ECS实例时，可以使用系统提供的默认安全组规则，也可以选择VPC中已有的其它安全组。安全组是一种虚拟防火墙用来控制ECS实例的出站和入站流量，详情参见**安全组**。

本文档介绍了常用的专有网络内ECS实例的安全组设置。

案例 1：内网互通

同一VPC内的相同安全组下的ECS实例，默认互通。

不同VPC内的ECS实例，无法互通。首先需要使用高速通道或VPN网关打通两个VPC之间的通信，然后确保两个VPC内的ECS实例的安全组规则允许互相访问，如下表所示。

安全组规则	规则方向	授权策略	协议类型	端口范围	授权类型	授权对象	优先级
VPC 1中的ECS实例的安全组配置	入方向	允许	Windows：RDP	3389/3389	地址段访问	输入要登录访问该ECS实例的私网IP。 如果允许任意ECS实例登录，填写0.0.0.0/0。	1
			Linux：SSH(22)	22/22			
			自定义TCP	自定义			
VPC 2中的ECS实例的安全组配置	入方向	允许	RDP	3389/3389	地址段访问	输入要登录访问该ECS实例的私网IP。 如果允许任意ECS实例登录，填写0.0.0.0/0。	1
			Linux：SSH(22)	22/22			
			自定义TCP	自定义			

案例 2：屏蔽、拦截、阻断特定IP或特定端口的访问

您可以通过配置安全组屏蔽、拦截、阻断特定IP或特定端口对专有网络ECS实例的访问。

安全组	规则方	授权策	协议类	端口范	授权类	授权对	优先级

规则	向	略	型	围	型	象	
拒绝特定IP地址段对ECS实例所有端口的入站访问	入方向	拒绝	全部	-1	地址段访问	屏蔽的IP地址段，采用CIDR格式，如10.0.0.1/32。	1
拒绝特定IP地址段对ECS实例TCP 22端口的入站访问	入方向	拒绝	SSH(22)	22/22	地址段访问	屏蔽的IP地址段，采用CIDR格式，如10.0.0.1/32。	1

案例 3：只允许特定IP远程登录到实例

如果您为VPC中的ECS实例配置了公网IP如NAT网关，EIP等，您可以根据具体情况，添加如下安全组规则允许Windows远程登录或Linux SSH登录。

安全组规则	规则方向	授权策略	协议类型	端口范围	授权类型	授权对象	优先级
允许Windows远程登录	入方向	允许	RDP	3389/3389	地址段访问	如果允许任意公网IP登录，填写0.0.0.0/0。 如果只允许特定IP远程登录，填写指定的IP地址。	1
允许Linux SSH登录	入方向	允许	SSH	22/22	地址段访问	如果允许任意公网IP登录，填写0.0.0.0/0。 如果只允许特定IP远程登录，填写指定的	1

						IP地址。	

案例4：允许从公网访问专有网络ECS实例部署的HTTP/HTTPS服务

如果您在专有网络的ECS实例上部署了一个网站，通过EIP、NAT网关对外提供服务，您需要配置如下安全组规则允许用户从公网访问您的网站。

安全组规则示例	规则方向	授权策略	协议类型	端口范围	授权类型	授权对象	优先级
允许来自HTTP 80端口的入站访问	入方向	允许	HTTP	80/80	地址段访问	0.0.0.0/0	1
允许来自HTTPS 443端口的入站访问	入方向	允许	HTTPS	443/443	地址段访问	0.0.0.0/0	1
允许来自TCP 80端口的入站访问	入方向	允许	TCP	80/80	地址段访问	0.0.0.0/0	1

在VPC中创建云产品实例

概述

您可以直接在专有网络的交换机下创建云产品实例，比如ECS、RDS或SLB。

前提条件

您已经创建了专有网络和交换机。

操作步骤

登录专有网络管理控制台。

在左侧专有网络导航栏，单击**专有网络**。

选择地域，然后单击目标专有网络的ID链接，进入**专有网络基本信息**页面。

在左侧菜单栏，单击**交换机**，打开**交换机列表**页面。

单击目标交换机的**创建实例**选项，然后单击要创建的实例类型。

在实例购买页面选择实例的配置，完成购买流程后，实例即成功创建在所选交换机下。

VPC中的访问控制

阿里云的专有网络目前没有独立的访问控制策略。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。比如ECS通过设置安全组来进行访问控制，SLB和RDS通过白名单来进行访问控制。

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。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。

当您创建专有网络类型的ECS实例时，可以使用系统提供的默认安全组规则。您可以更改默认安全组的规则，但无法删除默认安全组。

默认安全组1：出方向允许所有访问，入方向可以选择允许访问ICMP协议所有端口和TCP协议的 22、3389、80、443端口。

当使用非默认专有网络和交换机创建ECS实例时，您可以选择此默认安全组规则。

默认安全组2： 出方向允许所有访问，入方向只开放TCP协议的22和3389端口，以及ICMP协议所有端口。

当使用默认专有网络和交换机创建ECS实例时，您可以选择此默认安全组规则。

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）。

RDS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。

SLB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。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。

VPC内设置私网隔离

默认情况下，VPC内的不同交换机下的ECS实例可以通过系统路由相互访问。您可以通过配置安全组规则，使其互相隔离。

本操作以网段为172.16.0.0/12的VPC为例，在该VPC下有三个交换机分别为VS1（172.16.1.0/24）、VS2（172.16.2.0/24）和VS3（172.16.3.0/24）。

每个交换机下分别创建一个云服务器ECS实例，如下图所示。这三个ECS实例都加入了默认安全组2内，出方向允许所有访问，入方向只开放TCP协议的22和3389端口，以及ICMP协议所有端口。

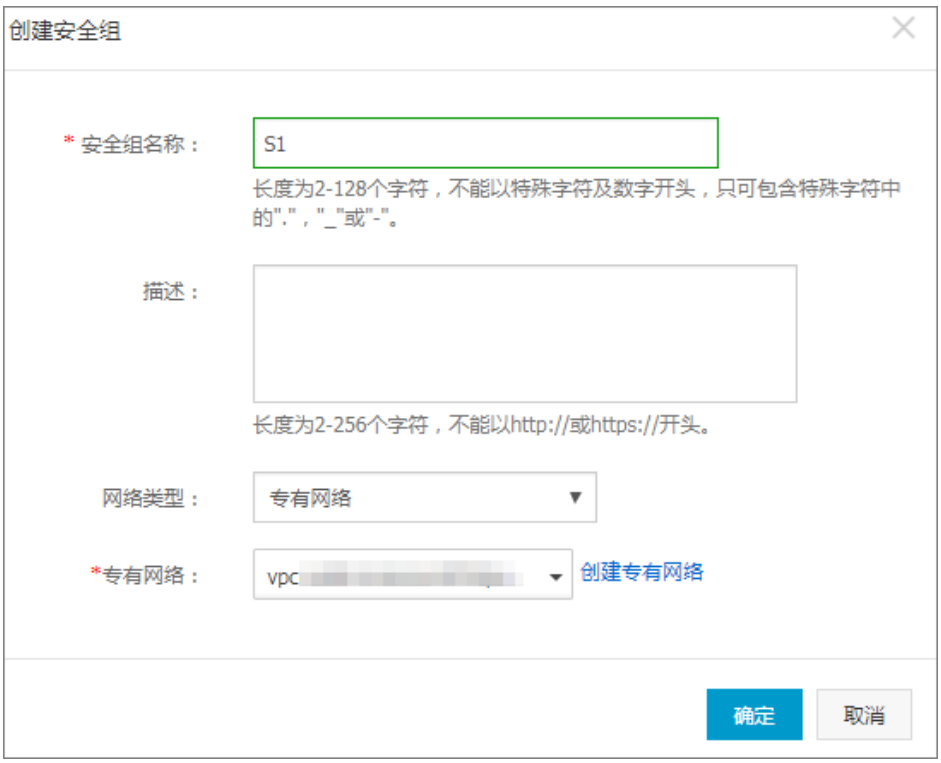
默认情况下，这三个ECS实例可以私网互通。您可以通过将这三个ECS实例加入到不同的安全组内实现VPC内私网隔离。

操作步骤

登录云服务器ECS管理控制台。

在左侧导航栏，单击**网络和安全** > **安全组**，然后单击**创建安全组**。

在**创建安全组**对话框，输入安全组名称，网络类型选择**专有网络**，然后指定ECS实例所在的专有网络。单击**确定**。



单击**立即设置规则**，分别添加如下三条入方向授权规则：

规则1：开放ICMP协议所有端口。优先级可以设置100。数字越大，优先级越低。

规则2：拒绝全部来自交换机2（网段为172.16.2.0/24）的访问，优先级设为1。

规则3：拒绝全部来自交换机3（网段为172.16.3.0/24）的访问，优先级设为1。

在ECS实例列表页面，找到位于交换机1（网段为172.16.1.0/24）中的ECS实例，然后单击实例ID链接，进入详情页面。

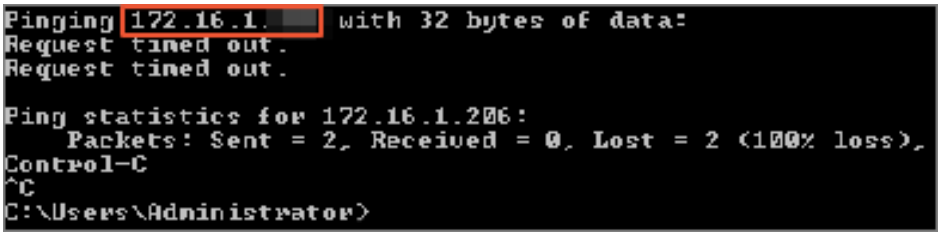
在左侧导航栏，单击**本实例安全组**。

该实例目前只关联了一个VPC内的默认安全组。

单击**加入安全组**，然后在**ECS实例加入安全组**对话框中选择刚创建的安全组S1，单击**确定**。

单击默认安全组对应的**移出**，将该ECS实例从默认安全组中移出。

此时其它两个ECS实例（交换机1和交换机2中的ECS实例）已经无法通过私网访问这个ECS实例了。



重复上述步骤为另外两个交换机下的ECS实例分别创建两个安全组，然后将它们从默认安全组内移出，使三个交换机内的ECS实例两两不能互访。

VPC内的公网访问

分配公网IP

如果VPC中的ECS实例有访问公网服务的需求，在创建ECS实例时，您可以选择为其分配一个公网IP。

如下图所示，创建ECS实例时，选择好ECS实例所属的专有网络和交换机后，在配置公网IP时选择**分配**。这样，ECS实例创建后，系统会为该ECS实例自动分配一个公网IP。

注意：

如果您没有选择分配公网IP，还可以通过绑定弹性公网IP实现公网访问。

此公网IP不能与ECS实例解绑。

更多关于创建ECS实例的信息参考**创建Linux实例**或**创建Windows实例**。

创建成功后，您可以在实例列表页面查看ECS实例的公网IP。可以用分配的公网IP连接ECS实例，执行 ping命令，测试公网访问。

绑定弹性公网IP

如果您在创建ECS时没有**分配公网IP**，您也可以通过绑定弹性公网IP的方法实现VPC内的ECS访问公网服务。

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，绑定和解绑时无需停机。更多详细信息参考**弹性公网IP概述**。

操作步骤

登录弹性公网IP管理控制台。

单击**申请弹性公网IP**。

在购买页面完成购买配置，单击**立即购买**，完成支付。

关于弹性公网IP的价格和计费方式，参考**EIP计费说明**。

注意：确保弹性公网IP的地域和要绑定的ECS实例所属的地域相同。

购买完成后，返回弹性公网IP列表页面，然后单击目标EIP的**绑定**选项。

在**绑定弹性公网IP**对话框，选择要绑定的ECS实例，然后单击**确认**。

注意：只有处于运行中和已停止状态的ECS实例可以绑定弹性公网IP，并且该ECS实例没有已分配的公网IP或其它EIP。

当绑定成功后，您的ECS实例就可以通过该EIP访问公网了。当不需要访问公网时，您也可以随时解绑、释放该EIP。详情参考管理弹性公网IP。

配置NAT网关

NAT网关（NAT Gateway）是一款企业级的VPC公网网关，提供NAT代理（SNAT、DNAT）、10Gbps级别的转发能力、以及跨可用区的容灾能力。更多详细信息参考NAT网关产品简介。

您可以通过使用NAT网关的SNAT功能为VPC内无公网IP的ECS实例提供访问Internet的代理服务。

操作步骤

登录VPC管理控制台。

在专有网络左侧导航栏，单击**NAT网关**，然后单击**创建NAT网关**。

在NAT网关购买页，配置购买信息，单击**立即购买**，完成支付。

关于NAT网关的计费方式，参考NAT网关价格总览。

购买完成后，返回NAT网关页面，找到创建的NAT网关，然后单击**购买带宽包**。

NAT网关上可以放置多个公网IP。为了方便您进行多个应用间带宽的复用，NAT网关支持多个IP共享一份购买的带宽。NAT网关上的公网IP和公网带宽，被抽象为共享带宽包。

在**带宽包**页面，单击**购买带宽包**。

在共享带宽包购买页面，配置购买信息，单击**立即购买**完成支付。

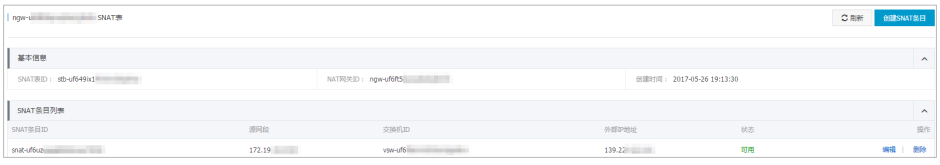
返回NAT网关页面，单击SNAT表链接，进入SNAT表页面。

在SNAT表页面，单击**创建SNAT条目**。

在**创建SNAT条目**窗口，配置如下信息，然后单击**确定**。

- **交换机**：选择ECS实例所属的交换机。
- **外部IP地址**：选择要提供外网服务的IP地址。

当该SNAT路由条目状态为**可用**时，源网段（交换机）下的ECS实例就可以通过分配的外部IP地址访问Internet了。



如下图所示，该ECS实例所在的交换机已经配置了一条SNAT条目，在该ECS实例内可以访问公网。您可以在ECS实例上执行 ping命令，测试公网访问。

公网访问VPC

分配公网IP

当您有从公网访问VPC中的云服务的需求时，可以在创建ECS实例时为其分配一个公网IP。

如下图所示，创建ECS实例时，选择好ECS实例的专有网络和交换机后，在配置公网IP时选择**分配**，创建成功后，系统会自动分配一个公网IP给专有网络中的ECS实例。更多关于创建ECS实例的信息参考创建Linux实例或创建Windows实例。

创建成功后，系统会自动分配一个公网IP。您可以执行 ping命令测试是否可以从公网访问该ECS实例。

弹性公网IP

如果您在创建ECS时没有分配公网IP，您也可以通过绑定弹性公网IP的方法实现从公网访问VPC中的云服务的需求。

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，绑定和解绑时无需停机。更多详细信息参考弹性公网IP概述。

操作步骤

登录弹性公网IP管理控制台。

单击**申请弹性公网IP**。

在购买页面完成购买配置，单击**立即购买**，完成支付。

关于弹性公网IP的价格和计费方式，参考弹性公网IP价格总览。

> 注意：弹性公网IP的地域和要绑定的ECS实例所属的VPC的地域相同。

购买完成后，返回弹性公网IP列表，找到购买的EIP，然后单击**绑定**。

在绑定弹性公网IP窗口，选择要绑定的ECS实例，单击**确认**。

> 注意：只有处于运行中和已停止状态的ECS实例可以绑定弹性公网IP，并且该ECS实例没有已分配的公网IP。

当绑定成功后，您就可以从公网通过该EIP访问VPC中的ECS实例了，当您不需要从公网访问云服务时，您也可以随时解绑、释放该EIP。详情参考管理弹性公网IP。

配置DNAT

NAT网关（NAT Gateway）是一款企业级的VPC公网网关，提供NAT代理（SNAT和DNAT）、10Gbps级别的转发能力和跨可用区的容灾能力。更多详细信息参考NAT网关产品简介。

您可以使用NAT网关的DNAT功能，将一个公网IP映射给专有网络中的ECS。配置后，公网IP收到的数据将按照您自定义的映射规则，转发给VPC内的ECS。

操作步骤

登录VPC管理控制台。

在专有网络左侧导航栏，单击**NAT网关**，然后单击**创建NAT网关**。

在NAT网关购买页，配置购买信息，单击**立即购买**，完成支付。

关于NAT网关的计费方式，参考NAT网关价格总览。

购买完成后，返回NAT网关页面，找到创建的NAT网关，然后单击**购买带宽包**。

NAT网关上可以放置多个公网IP。为了方便您进行多个应用间带宽的复用，NAT网关支持多个IP共享一份购买的带宽。NAT网关上的公网IP和公网带宽，被抽象为共享带宽包。

在**带宽包**页面，单击**购买带宽包**。

在共享带宽包购买页面，配置购买信息，单击**立即购买**完成支付。

购买完成后，返回NAT网关页面，找到创建的NAT网关，然后单击**设置DNAT**。

在DNAT表页面，单击**创建DNAT条目**，在创建DNAT条目窗口配置以下信息。

配置	说明
公网IP地址	选择一个可用的公网IP。 **注意**：不可重用SNAT条目中已使用的公网IP。
私网IP地址	指定要映射的专有网络ECS实例的私网IP。您可以通过以下两种方式指定私网IP： - 自填：输入要映射的专有网络ECS实例的私网IP。 - 从ECS对应IP进行选择：从专有网络ECS实例列表中选择要映射的ECS实例。系统会自动填充私网IP。

端口设置	选择映射方式： - 所有端口：该方式属于IP映射，等同于为所选的ECS实例配置了一个弹性公网IP。该ECS实例可以接收来自公网任何端口、任何协议的请求。选择所有端口后，无需再配置公网端口、私网端口和协议类型。 - 具体端口：该方式属于端口映射。配置后，NAT网关会将收到的指定协议的[私网IP:私网端口]的数据发向指定的[公网IP:公网端口]，并将来自[公网IP:公网端口]指定协议的数据发送给指定的[私网IP:私网端口]。选择具体端口后，需要配置公网端口、私网端口和协议类型。

单击**确定**，创建成功后，当端口转发条目的状态为**可用**时， 就可以从公网访问该ECS实例了。

配置公网负载均衡

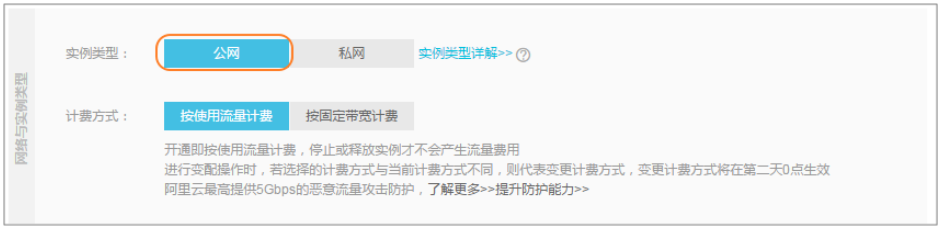
负载均衡（Server Load Balancer）是将访问流量根据转发策略分发到后端多台云服务器（Elastic Compute Service，简称 ECS）的流量分发控制服务。更多详细信息，查看负载均衡产品简介。

您可以创建一个公网负载均衡实例，然后将VPC ECS实例添加到负载均衡实例中作为后端服务器来接收负载均衡监听转发的请求。这样，VPC中的ECS实例就可以通过负载均衡对外提供服务了。

说明：本操作以两台部署了Aphache静态网页的ECS实例为例。

操作步骤

参考创建负载均衡实例，创建一个公网类型的负载均衡实例，即**实例类型**选择**公网**。



实例创建成功后，系统会为公网负载均衡实例分配一个公网IP地址。您可以用该IP地址提供服务。

添加后端服务器。

在负载均衡实例管理页面，单击目标负载均衡实例的ID链接，进入负载均衡详情页面。

在左侧导航栏，单击**服务器** > **后端服务器**。

单击**未添加的服务器**页签，选择专有网络类型的ECS实例，单击**添加**，权重设置为100。

配置监听。

在负载均衡详情页面，单击**监听**，然后单击**添加监听**。

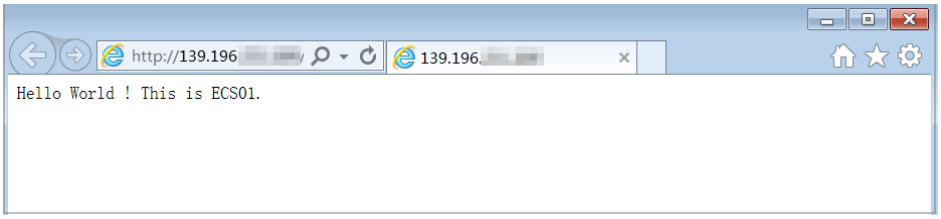
根据您的需要参考下图配置监听规则，单击**下一步**。

更多监听配置参考监听配置。

配置健康检查，选择TCP监听，使用默认值。单击**下一步**，完成配置。

完成配置后，当负载均衡实例的状态为**运行中**，并且后端服务器的ECS实例检查正常时，负载均衡实例就开始按照设置的监听规则进行流量请求转发了。

如下图所示，在浏览器中打开负载均衡的公网IP地址就可以访问后端添加的ECS实例上的服务了。

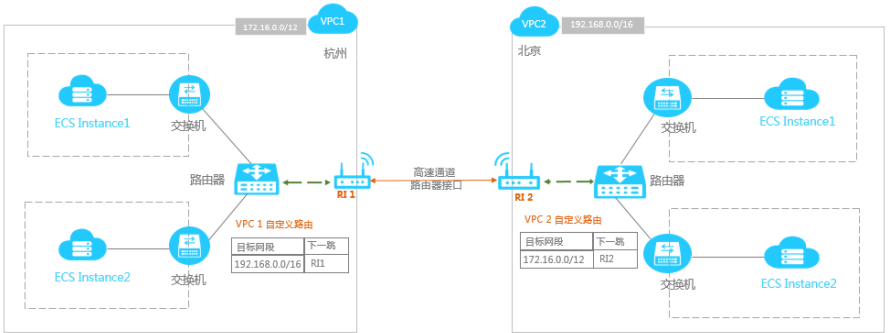


VPC互连

高速通道

高速通道可以实现任意地域内两个专有网络之间的私网通信，既可以避免绕行公网带来的网络质量不稳定问题，又可以避免数据在传输过程中被窃取的风险。

如下图所示，比如您有两个VPC，分别为VPC1（网段：172.16.0.0/12）和VPC2（网段：192.168.0.0/16）。如果您想让两个VPC之间互通，您需要使用高速通道产品，购买一个路由器接口，将VPC1设置为本端，VPC2设置为对端。购买完成后，系统会分别在发起端和接收端创建两个互为对端的路由器接口（RI1和RI2）。最后要实现两个VPC互通，您需要添加如下路由条目。



VPC1的路由配置

目标网段	下一跳类型	下一跳
192.168.0.0/16	路由器接口	RI1

VPC2的路由配置

目标网段	下一跳类型	下一跳
172.16.0.0/12	路由器接口	RI2

具体配置详情参考：

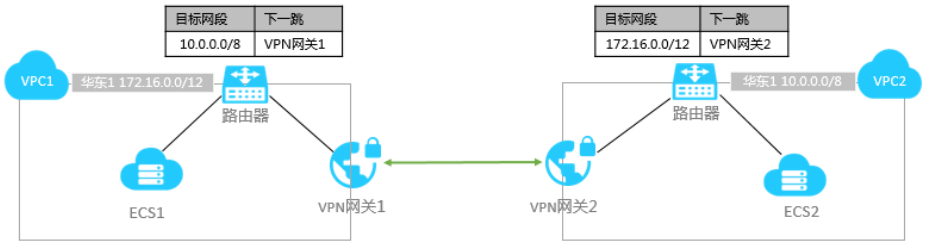
同账号下专有网络内网互通

跨账号下专有网络之间内网连通

VPN网关部署

阿里云VPN网关是基于Internet建立加密隧道进行通信。配置简单，耗时短，可以非常快速地将两个VPC连接起来。

您可以通过部署VPN网关，使两个VPC之间能够私网互通。首先为每个VPC创建一个VPN网关和一个用户网关，再创建VPN连接建立VPN通道，最后分别在两个VPC内添加一个自定义路由条目。配置详情参考配置VPC到VPC连接。

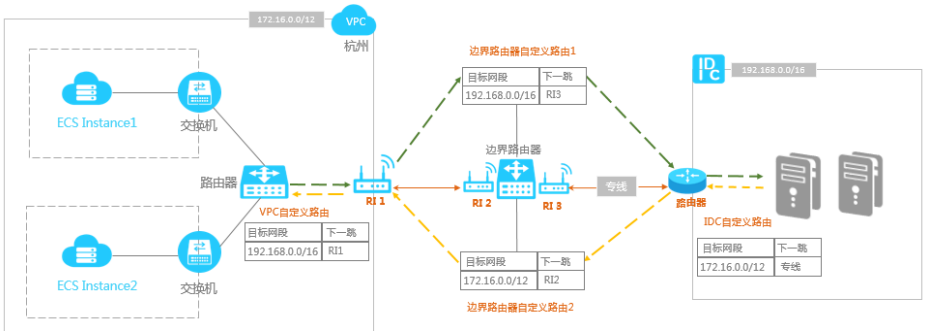


VPC与线下IDC互连

专线接入

您可以通过高速通道的专线接入功能实现VPC与线下IDC的互通。

假设您在杭州有一个网段为172.16.0.0/12的VPC环境，在北京有一个线下IDC环境。当您有的VPC中的云服务有访问线下IDC的需求时，您可以使用物理专线承载VPC和IDC之间的通信，如下图示。



操作步骤

申请物理专线

物理专线是连通线下IDC到阿里云的专线接入点。您可以自行接入，也可以通过阿里云合作伙伴接入。

创建边界路由器

创建边界路由器作为VPC到IDC的数据转发桥梁。创建成功后，系统会自动把边界路的路由器接口（上图中的RI3）通过专线和IDC相关联。

创建路由器接口

创建路由器接口连接VPC和边界路由器。在创建路由器接口时，把边界路由器选为本端，VPC选为对端。创建成功后，系统会在边界路由器和VPC之间创建两个互为对端的路由器接口，如上图中的RI1和RI2。

配置路由

最后您还需要在VPC和边界路由器端配置如下路由：

VPC端的路由配置

目标网段	下一跳类型	下一跳
192.168.0.0/16	路由器接口	RI1

边界路由器的路由配置

目标网段	下一跳类型	下一跳
192.168.0.0/16	专线	RI3
172.16.0.0/12	VPC	RI2

IDC端的路由配置

用户线下的路由设备需要配置一条指向物理专线的路由。

具体配置详情，参考**物理专线接入**。

搭建VPN网关

阿里云VPN网关是基于Internet建立加密隧道进行通信，比建立专线的方式更简单，耗时更短，可以非常快速地将企业数据中心和云上VPC连接起来，构建混合云。

规划和准备

在部署VPN网关前，请做好网络规划：

线下IDC和云上VPC的私网IP地址段规划**不能相同**，否则无法通信。

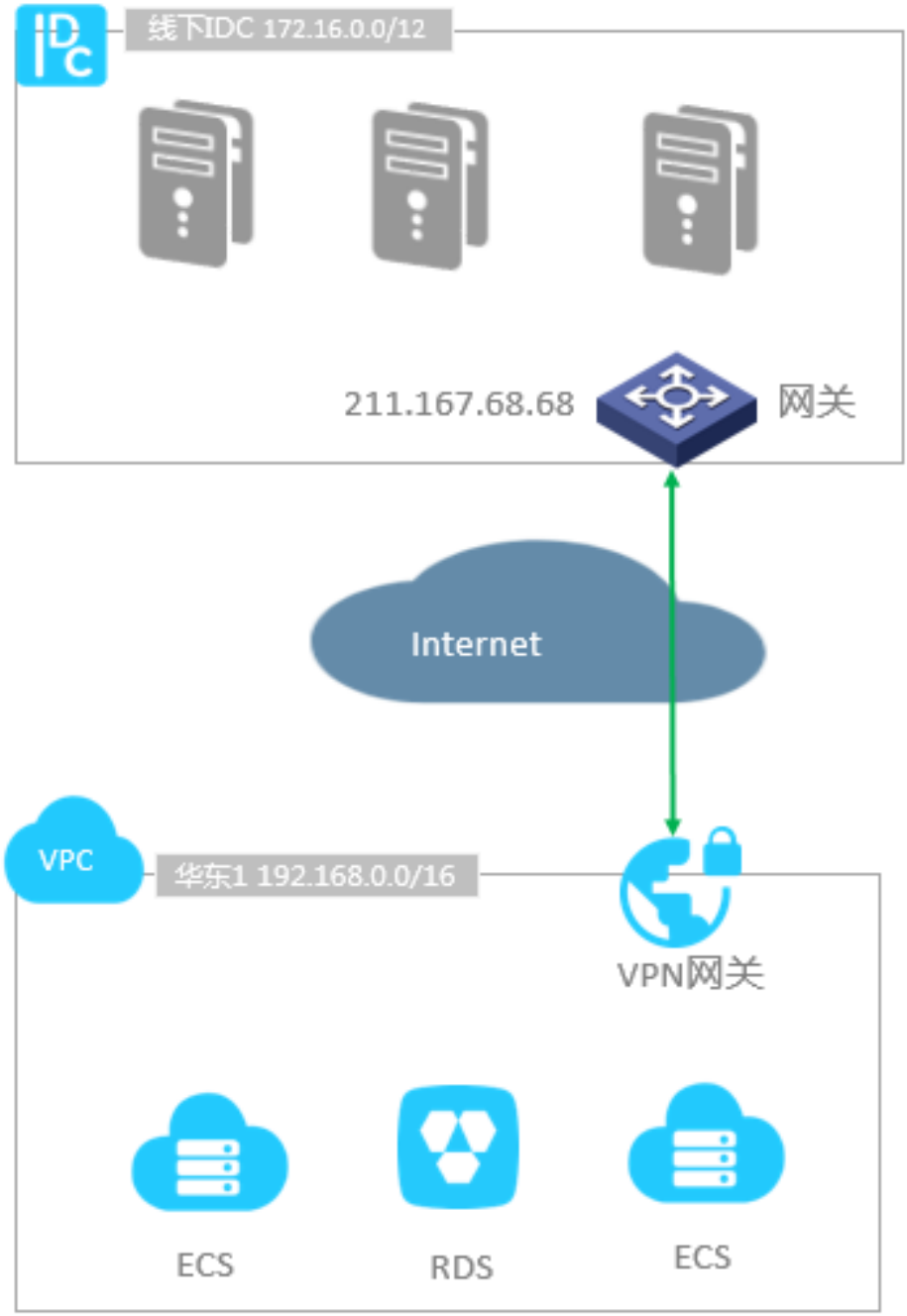
规划VPN网关所在的VPC和交换机，即云上VPN网关的网络环境。

确定线下IDC的网关设备，用哪个设备和云上VPC互联。阿里云VPN网关支持标准的IKEv1和IKEv2协议。因此，只要支持这两种协议的设备都可以和云上VPN网关互联，比如Cisco ASA、Juniper、SonicWall、Nokia、IBM、Ixia等。

应用场景

本操作适用于使用VPN网关搭建一个VPC与线下IDC互通的混合云场景。

假设阿里云上的VPC网段是192.168.0.0/16，线下IDC的网段是172.16.0.0/12，线下IDC的网关设备公网IP地址是211.167.68.68。通过VPN网关将云上VPC和线下IDC打通，使VPC内云资源和IDC内的服务器可以私网通信。



操作步骤

步骤一 创建VPN网关

为云上VPC创建VPN网关。

步骤二 创建用户网关

用户网关是对线下IDC网关设备的一个简单抽象，就是把线下IDC网关设备的公网IP地址注册到系统中便于后续建立VPN连接。

步骤三 创建VPN连接

创建VPN连接将云上VPN网关和线下IDC的用户网关进行关联。

步骤四 在线下IDC网关设备中加载配置

在线下IDC网关设备中加载VPN网关的配置。

步骤五 设置路由

到这里VPN网关基本配置完毕，但是要让云上VPC内的ECS可以直接访问线下IDC内的服务器，还需要在云上VPC设置路由。

步骤六 测试访问

测试VPN网关配置是否生效。

步骤一 创建VPN网关

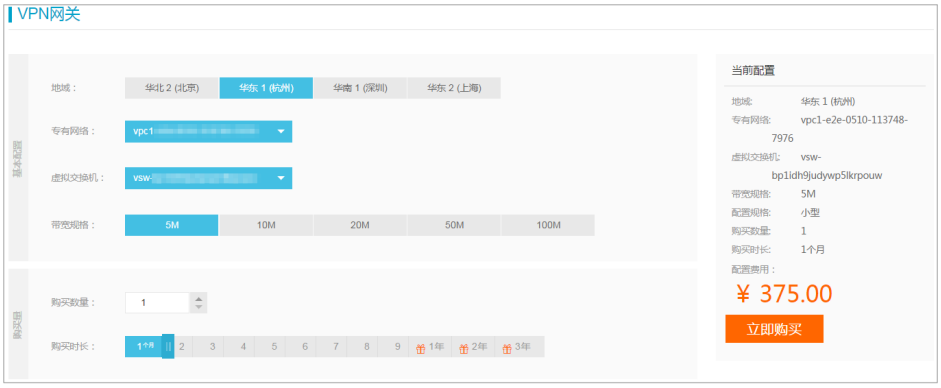
打开VPN网关页面，然后单击**创建VPN网关**。

在VPN网关购买页面，配置如下信息，然后单击**立即购买**，完成支付。

地域： 选择华东1（杭州）地域。该地域要和您的VPC地域相同。

专有网络和交换机： 选择要连接的VPC和交换机。

带宽规格：选择带宽规格，带宽规格指的是VPN网关所具备的公网带宽。



返回VPN网关页面，单击**华东1**地域，查看创建的VPN网关。

刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态就表明VPN网关完成了初始化，可以正常使用了。

步骤二 创建用户网关

打开用户网关页面，然后单击**创建用户网关**。

在**创建用户网关**对话框，输入线下IDC网关设备的公网IP地址，然后单击**提交**。

步骤三 创建VPN连接

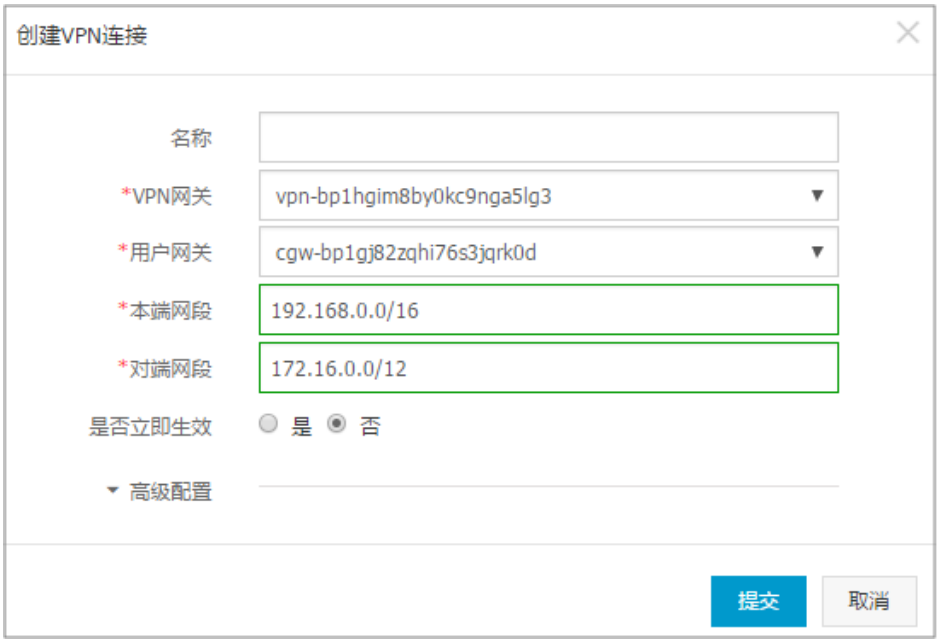
打开VPN连接页面，然后单击**创建VPN连接**。

在**创建VPN连接**对话框，输入以下信息，然后单击**提交**。

本端网段：云上VPC的网段，本教程中是192.168.0.0/16。

对端网段：线下IDC的网段，本教程中是172.16.0.0/12。

如果您想更改IKE和IPSec配置，单击**高级配置**进行修改。



步骤四 在线下IDC网关设备中加载配置

打开VPN连接页面，选择VPN连接的地域，本教程中选择**华东1**。

找到目标VPN连接，然后单击**下载配置**。

根据线下IDC网关设备的配置要求，将上述配置加载到IDC网关设备中。

注意：下载配置中的RemotSubnet和LocalSubnet与创建VPN连接时的本端网段和对端网段正好是相反的。因为从云上VPN网关角度看，对端是用户IDC的网段，本端是VPC网段；而从线下IDC的网关设备角度看，LocalSubnet就是指线下IDC的网段，RemotSubnet则是指云上VPC的网段。

步骤五 设置路由

登录VPC管理控制台。

在**专有网络列表**页面，找到VPN网关所属的VPC，单击该VPC的ID链接。

在VPC详情页面，单击**路由器**，然后单击**添加路由**。

在**添加路由**对话框，配置如下信息，单击**确定**。

目标网段：线下IDC的网段，本教程中是172.16.0.0/12。

下一跳类型：选择VPN网关。

VPN网关：选择创建好的VPN网关。

步骤六 测试访问

登录到云上VPC内找一台不带公网IP的ECS实例，并通过 ping 命令ping线下IDC内一台服务器的私网IP地址，验证通信是否正常。