目录

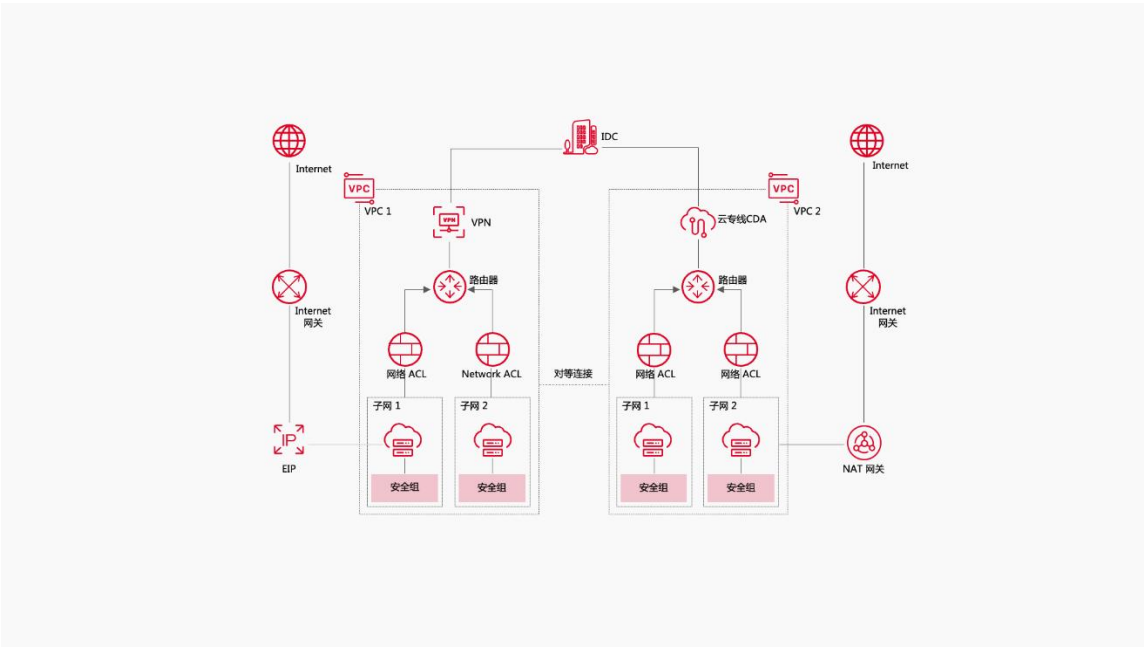
虚拟私有云产品简介

产品定义

本文为您介绍虚拟私有云（Virtual Private Cloud，VPC）产品的定义和产品架构。

虚拟私有云（Virtual Private Cloud，VPC）是您在天翼云上申请的隔离的、私密的网络环境。您能够在一个安全可控、隔离的网络环境中实现云资源的高效管理和利用。虚拟私有云具备丰富的产品特性，使得您可以自定义网络地址、路由表、安全组等。同时，虚拟私有云提供丰富的网络连接，可以满足云上虚拟私有云互访、公网访问、通过专线或者 VPN 与线下 IDC 互通等网络场景。

产品架构



虚拟私有云 VPC 产品架构可以分为：VPC、子网、路由表、访问控制、VPC 接入方式等。

VPC

在创建虚拟私有云时，需要设置虚拟私有云的网段。建议使用标准网段 10.0.0.0/8-28、172.16.0.0/12-28、192.168.0.0/16-28 作为 VPC 网段，多 VPC 互通场景或混合云场景需确保地址规划不能冲突。虚拟私有云之间通过隧道技术实现逻辑隔离，不同虚拟私有云之间默认隔离。VPC 网段创建后无法修改，请合理规划网络。您可以通过增加附加网段来满足 VPC 下多个网段的场景。如果标准网段不能满足您的网络规划需求，请提交工单申请其他网段。

子网

云资源（例如云服务器、物理机等）必须部署在子网内。您可以在虚拟私有云内创建一个或多个子网，但是子网的网段必须在虚拟私有云

网段范围内。同子网内网络默认互通，同 VPC 下不同子网之间默认互通。子网网段创建后无法修改，请合理规划网络。

路由表

路由表用于控制虚拟私有云的流量走向，路由表分为默认路由表和自定义路由表两种类型。默认路由表随着 VPC 自动创建，所有新建子网与默认路由表关联，不能创建也不能删除默认路由表，但可以在默认路由表中创建自定义路由规则。您可以选择创建自定义路由表，并将子网手动关联到自定义路由表中。对于部分可用区资源池，在 VPC 内创建自定义路由表，通过绑定自定义路由表和子网，实现子网内的云主机或物理机通信，从而更灵活地进行流量管理。在 VPC 内创建网关类型的自定义路由表，将其与 IPv4 网关绑定，这种路由表被称为网关路由表。网关路由表用来控制进入 VPC 的公网流量，可以将公网流量引流到 VPC 中的安全设备（例如虚拟防火墙）做统一安全防护。

访问控制

在虚拟私有云中，访问控制是保护云资源（云主机、物理机）免受未授权访问和攻击的关键配置之一。访问控制主要包括以下几个方面：

- 安全组是一种虚拟防火墙，用于控制云资源（云主机、物理机）的流量进出。在虚拟私有云中，您可以为每个安全组定义相应的规则，以允许或禁止特定 IP 地址或端口的流量进出。将适当的安全组规则应用于云资源（云主机、物理机）可以显著提高其安全性。

- 网络 ACL 是一种虚拟私有云中子网级别的流量防护策略，网络 ACL 可以通过为子网关联一个特定的 ACL 规则集来提供网络资源的安全性。

VPC 接入方式

天翼云提供了多种 VPC 连接方案，以满足用户不同场景下的诉求。

- 使用弹性 IP 或 NAT 网关，可以让虚拟私有云内的云主机或物理机与公网 Internet 进行互通。
- 在同一个区域内，使用对等连接功能可以让不同 VPC 之间的云主机或物理机互相访问。
- 通过虚拟专用网络 VPN、云专线功能将 VPC 和您的本地数据中心连通。

如何访问虚拟私有云

在天翼云中，提供了两种方式访问虚拟私有云。

- 管理控制台方式：管理控制台提供了一个 Web 界面，您可以使用直观的界面进行相应的操作。登录“控制中心”，选择“网络>虚拟私有云”。
- API 方式（Application Programming Interface）：用户可以使用云平台提供的 API 接口，来对虚拟私有云进行操作。可将虚拟私有云集成到第三方系统，用于二次开发，具体操作请参见《虚拟私有云 API 参考》。

产品优势

虚拟私有云产品为您提供优质的服务体验，本文带您了解虚拟私有云的产品优势。

简单易用

您可以通过控制台、API 等方式，快速创建、管理虚拟私有云，创建完成后，系统会自动为其创建默认路由表。您可以根据自己的应用需求轻松创建和配置虚拟私有云网络拓扑结构，包括子网、安全组、路由表等。

安全可靠

虚拟私有云之间通过隧道技术实现逻辑隔离，不同虚拟私有云之间默认不能通信。另外，我们还为您提供为您提供安全组、网络 ACL 等不同层面的网络访问控制方式，采用多重防护策略，让您的网络环境更安全。

灵活配置

虚拟私有云为您提供了强大的网络管理能力，您可以自定义网段，按需划分子网，并通过灵活配置路由表和路由规则，定制化地部署您的云上业务。并且支持云专线、VPN 等多种方式接入。

通过自定义私有网络，您可以按需划分子网来合理规划 IP 地址资源；通过配置路由表来管理私有网络的流量走向；通过配置安全访问控制策略来进行安全防护等。

互联互通

虚拟私有云提供丰富的接入方式，可以满足您在云上的通信需求：

- 访问其它虚拟私有云：默认情况下，两个虚拟私有云之间是不能通信访问的，通过对等连接使不同 VPC 之间的云主机或物理机互相访问。
- 访问 Internet：默认情况下，虚拟私有云与公网是不能通信访问的，通过弹性 IP、NAT 网关、弹性负载均衡等多种方式连接公网。
- 访问本地数据中心：您可以使用 VPN 连接、云专线来访问本地数据中心。

为企业提供多种连接选择，以满足云上多业务需求，助力轻松部署企业应用，同时减少企业 IT 运维成本。

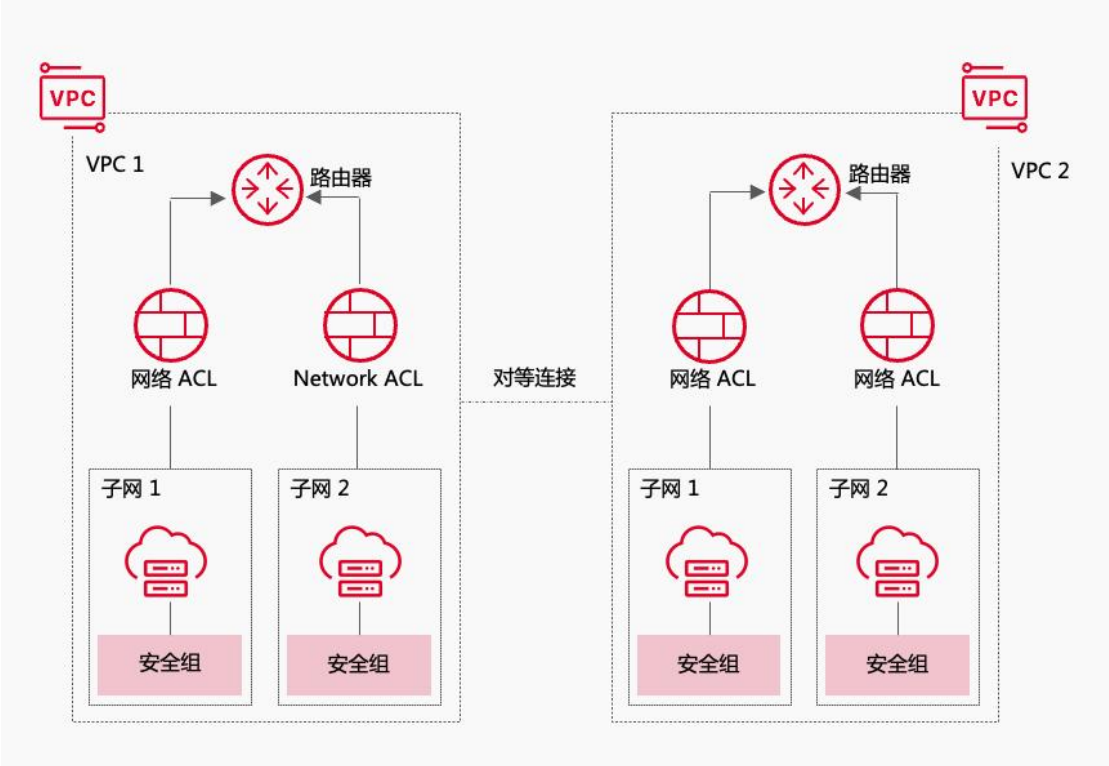
产品应用场景

虚拟私有云产品广泛应用于多种场景，本文带您更快了解虚拟私有云产品经典应用场景。

云上私有网络

场景说明

不同的 VPC 之间逻辑隔离。您可以将业务系统部署在天翼云上，构建云上的专属私有网络环境。如果您的实际应用中会有 Web 业务系统、APP 业务系统、数据库服务器、等各个不同的系统，这些系统之间通常需要做分层隔离。那么可以使用多个 VPC 进行业务隔离。或者您的生产环境和测试环境也是要严格进行隔离，那么也可以使用多个 VPC 进行业务隔离。当有互相通信的需求时，可以在两个 VPC 之间建立对等连接。



搭配使用

弹性云主机

Web 应用或网站托管

场景说明

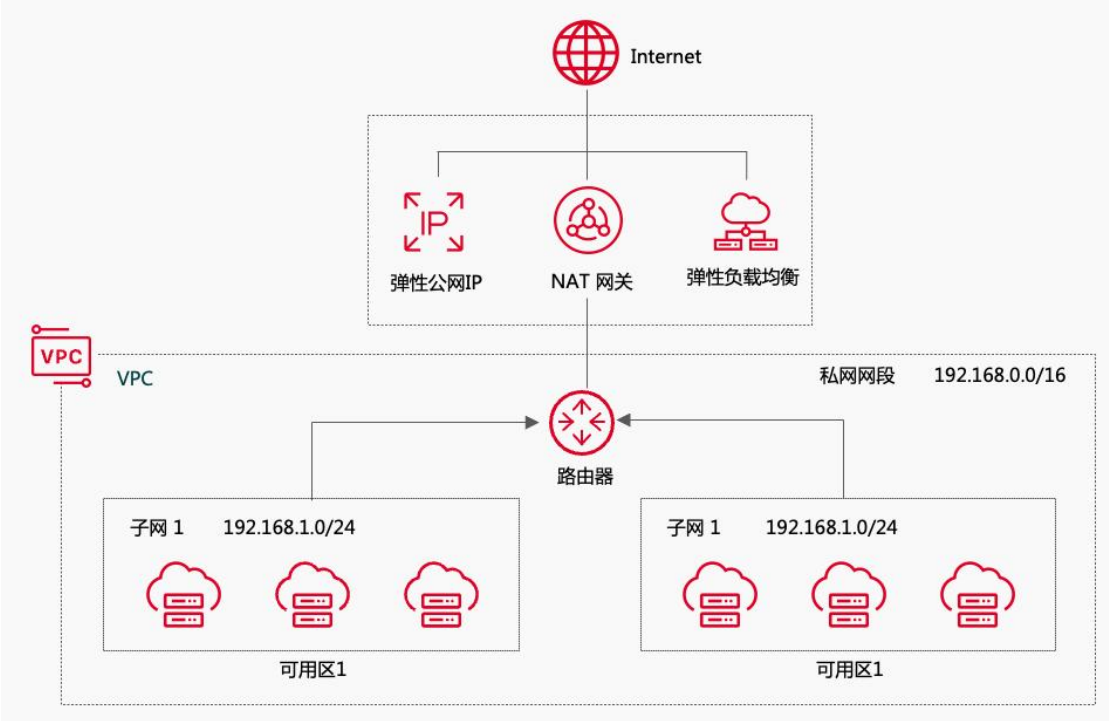
您可以将 Web 应用或网站等服务托管在 VPC 中的云服务器上，并通过弹性 IP 或 NAT 网关连接弹性云主机与 Internet，运行弹性云主机上部署的 Web 应用程序。当您有较多服务器来部署复杂业务、且公网流量较大时，可以使用负载均衡 CT-ELB。负载均衡 CT-ELB 可以实现自动分配云中多个弹性云主机实例间应用程序的访问流量，让您实现更高水平的应用程序容错能力。

VPC 内的云资源连接公网（Internet），可以通过如下云产品实现。

云产品	应用场景	描述	相关操作
弹性 IP	单个 ECS 连接公网	弹性 IP 是可以独立申请的公网 IP 地址，将弹性 IP 地址和子网中关联的弹性云主机绑定和解绑，可以实现 VPC 中的弹性云主机通过固定的公网 IP 地址与互联网互通。	云主机通过弹性 IP 访问互联网
NAT 网关（NAT Gateway）	多个 ECS 共享弹性 IP 连接公网	NAT 网关（NAT Gateway）是一种支持 IP 地址转换的网络云服务，能够为虚	NAT 网关操作指南

		拟私有云（Virtual Private Cloud，VPC）内的计算实例提供网络地址转换（Network Address Translation），分为 SNAT 和 DNAT 两个功能。通过 SNAT 可使多个弹性云主机共享使用弹性 IP 访问 Internet。通过 DNAT 可使多个弹性云主机提供互联网服务。NAT 网关是 VPC 内的一个公网流量的出入口，保护私有网络信息不直接对公网暴露。	
弹性负载均衡 (CT-ELB, Elastic	通过将访问流量均衡分发到多个 ECS 的方式	弹性负载均衡通过将访问流量自动分发到多台云主机，扩展应用系统对外的服务能	弹性负载均衡快速入门

Load Balancing)	对外提供服务，比如社交媒体等高并发访问场景	力，实现更高水平的应用程序容错性能。	



搭配使用

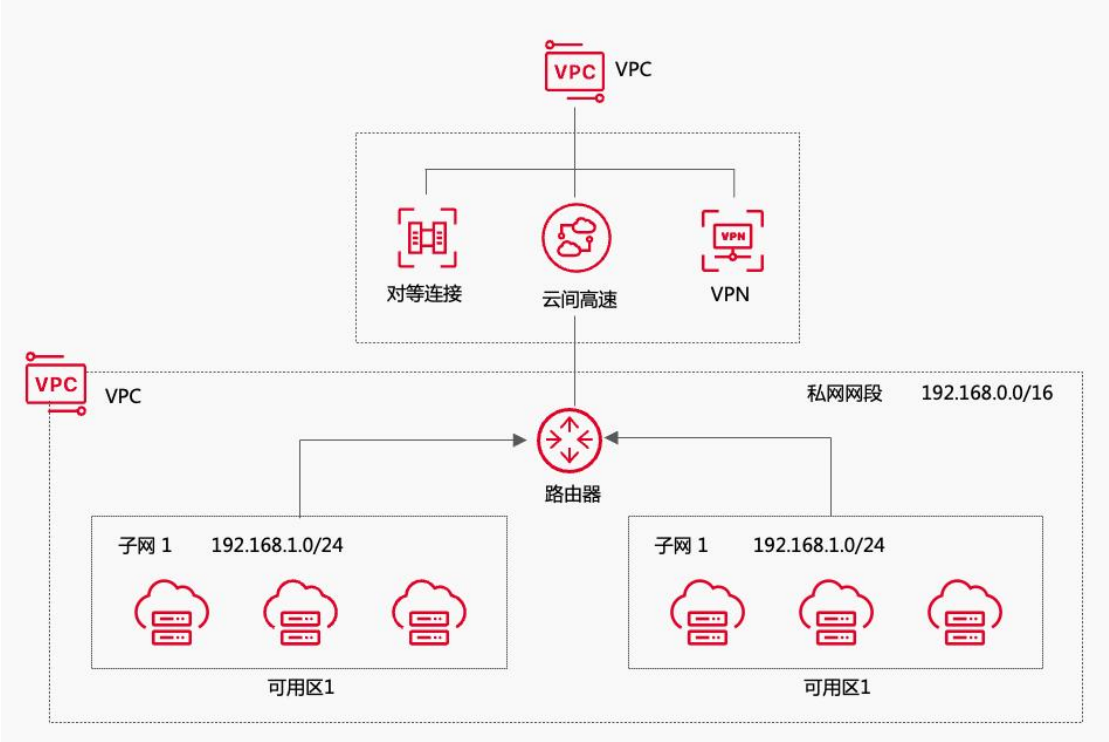
弹性云主机、弹性 IP、NAT 网关、弹性负载均衡

云上 VPC 连接

场景说明

对于相同或者不同区域下的 VPC 需要互通连接时，可通过如下表云产品实现。

云产品	应用场景	描述	相关操作
对等连接	同区域的不同 VPC 之间的互通	同一个区域的不同虚拟私有云，可以通过对等连接进行互连，同一帐号与不同帐号的连接方式略有差异。	同账号对等连接组网 跨账号对等连接组网
云间高速	跨区域的 VPC 互连	对于不同区域的 VPC，不区分是否同一帐号，都可以互连，跨区域连接实现云上网络。	跨区域通过云间高速互连
虚拟专用网络 VPN	不同区域 VPC 互连	基于 Internet 使用 IPsec 加密隧道将不同区域的 VPC 连接起来。具备成本低、配置简单、即开即用等优点。	使用 VPN 实现云上不同区域 VPC 互通



混合云部署

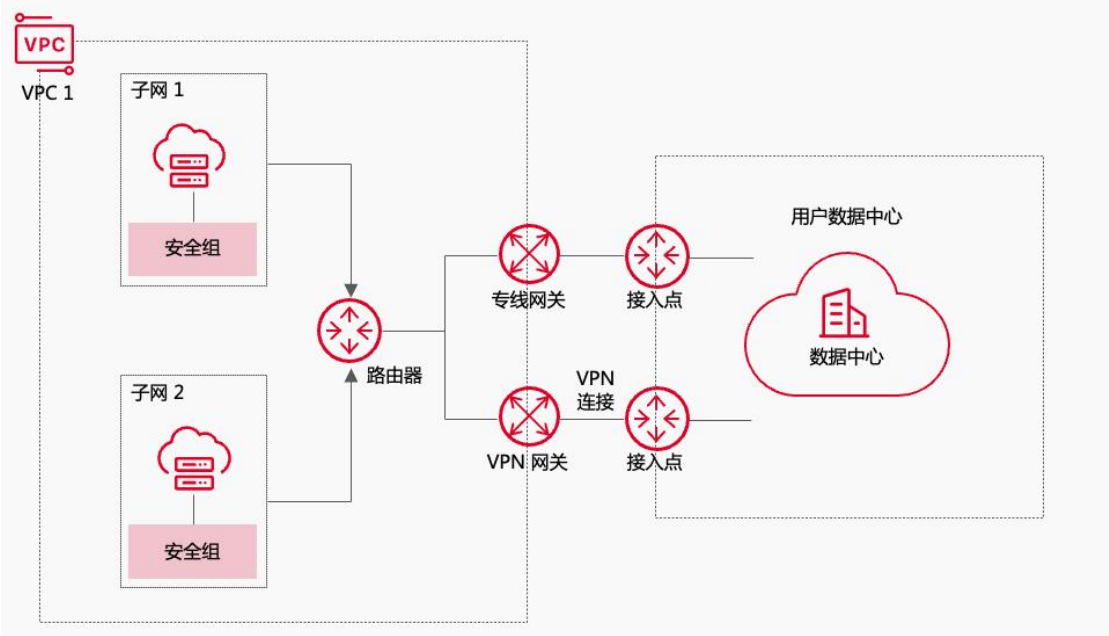
场景说明

对于自建本地数据中心（IDC）的用户，我们可以通过构建混合云架构，实现云上 VPC 与云下 IDC 之间的互连互通。

云产品	应用场景	描述	相关操作
虚拟专用网络 VPN	连接云上 VPC 与本地 IDC	VPN 连接（Virtual Private Network）用于搭建用户本地数据中心与天翼云 VPC 之间	通过 VPN 连接云下数据中心

		便捷、灵活，即开即用的 IPsec 加密连接通道，实现灵活一体，可伸缩的混合云计算环境。	
云专线 CDA	依托高性能网络布局和丰富链路资源，连接 VPC 与本地 IDC	天翼云云专线（CT-CDA，Cloud Dedicated Access），依托中国电信高性能网络布局和丰富链路资源，为用户本地数据中心与天翼云 VPC 之间提供高速、低时延、稳定安全的连接服务，灵活搭建云上云下	通过云专线实现客户站点与 VPC 互通 通过云专线实现客户站点与云上多个 VPC 互通

		专属通道，实现可伸缩的混合云部署。	



搭配使用

弹性云主机 ECS、云专线、虚拟专用网络 VPN

基本概念

本文带您了解使用虚拟私有云产品过程中涉及的基本概念。

名词	说明
子网	子网（subnet）是指在一个大的网络范围内，为了更好地进行资源管理，而将网络划分成的小型网络。每个子网有一个唯一的 IP 地址序列，可用于分配给该子网中的主机和其他网络设备。子网是虚拟私有云中的一个 IP 地

	址段，虚拟私有云中的所有资源都必须部署在子网上。
路由表	路由表用于控制虚拟私有云的流量走向，路由表分为默认路由表和自定义路由表两种类型。默认路由表随着 VPC 自动创建，所有新建子网与默认路由表关联，不能创建也不能删除默认路由表，但可以在默认路由表中创建自定义路由规则。
虚拟 IP	虚拟 IP（Virtual IP Address，简称 VIP）是一个从子网中分配的一个内网 IP 地址，没有分配给真实弹性云主机网卡。虚拟 IP 地址拥有私有 IP 地址同样的网络接入能力，用户也可以像主私网 IP 地址一样通过虚拟 IP 去访问弹性云主机。 您可以通过将虚拟 IP 与主备弹性云主机绑定，根据是否需要访问公网可以为虚拟 IP 绑定一个弹性 IP，配合高可用软件（例如 Keepalived）使用，实现业务的高可用。
安全组	安全组是一个逻辑上的分组，为同一个虚拟私有云内具有相同防护需求的弹性云主机、物理机提供安全访问策略。安全组创建后，用户可以根据业务需求自定义防护规则，当弹性云主机、物理机加入该安全组后，即受到这些访问规则的保护。
ACL	网络 ACL 是一个子网级别的流量防护规则，您可以自定义配置网络 ACL 规则，并将网络 ACL 与子网关联，通过出方向/入方向规则管理出入子网的流量，实现对子网中

	云服务器实例流量的访问控制。 安全组对云主机、物理机等实例进行防护，网络 ACL 对子网进行防护，两者结合起来，可以实现更精细、更复杂的安全访问控制。
流量镜像	流量镜像（Traffic Mirror）功能可以将网络流量从一个或多个源端口复制到一个目标端口，以便进行分析、监控和调试。流量镜像主要是复制网卡上的流量并筛选出符合条件的报文，因此它可以在不影响网络性能的情况下，捕获和记录网络流量，帮助管理员诊断网络故障、检测网络攻击和优化网络性能。
IPv4 网关	IPv4 网关是连接虚拟私有云和公网的网络组件。虚拟私有云访问 IPv4 公网的流量经过 IPv4 网关，由 IPv4 网关实现路由转发以及私网地址到公网地址的转换，最终实现对公网的访问。
弹性网卡	弹性网卡是虚拟私有网络 VPC 中的虚拟网络接口，用于连接 ECS 与私有网络。弹性网卡可以灵活的绑定/解绑云服务器，实现云服务器和网络的解耦。
NAT 网关	NAT 网关（NAT Gateway）是一种支持 IP 地址转换的网络云服务，能够为虚拟私有云内的计算实例提供网络地址转换，天翼云 NAT 网关分为 SNAT 和 DNAT 两个功能，通过 SNAT 可使多个弹性云主机共享使用弹性 IP 访问 Internet。通过 DNAT 可使多个弹性云主机提供互

	联网服务。
对等连接	对等连接（VPC Peering Connection）是指两个同一区域内的 VPC 之间的网络连接。用户可以使用私有 IP 地址在两个 VPC 之间进行内网通信，就像两个 VPC 在同一个网络中一样。用户可以在自己帐号的 VPC 之间创建对等连接，也可以在自己账号的 VPC 与同一区域内其他帐号的 VPC 之间创建对等连接。
VPC 终端节点	VPC 终端节点（VPC Endpoint，CT-VPCEP）使您能够将 VPC 私密地连接到终端节点服务（天翼云服务、 用户私有服务），该连接使用天翼云内部网络进行连接，不再绕行公网，为您提供性能更加强大、更加灵活的网络。VPC 终端节点为您提供“终端节点服务”和“终端节点”两种资源。

产品使用限制

本文为您介绍使用虚拟私有云产品时的相关限制，请您务必仔细阅读后使用。

天翼云部分可用区资源池适用于以下规则，实际情况以控制台展现为准。

资源	配额	提升额度
单个资源池可创建的	10	提交工单

VPC		
单个 VPC 可创建的子网	10	提交工单
单资源池可以创建的安全组数量	100	提交工单
单资源池安全组规则数量	500	提交工单
单资源池可以创建的 ACL 数量	100	提交工单
单个 ACL 规则数量	20	提交工单
单个 VPC 下的虚拟 IP 数量	10	提交工单
单个云主机可以绑定的虚拟 IP 数量	10	提交工单
单个 VPC 下的路由表数量	50	提交工单
单个路由表下的路由条目数量	10	提交工单

天翼云部分地域资源池适用于以下规则，实际情况以控制台展现为准。

资源	**配额**	**提升配额**
单个资源池可创建的	5	提交工单

VPC		
单个 VPC 可创建的子网	5	提交工单
单资源池可以创建的安全组数量	100	提交工单
单资源池安全组规则数量	500	提交工单
单资源池可以创建的 ACL 数量	100	提交工单
单个 ACL 规则数量	20	提交工单
单个云主机可以绑定的虚拟 IP 数量	10	不可提交工单
单个 VPC 下的路由表数量	50	提交工单
单个路由表下的路由条目数量	10	提交工单

资源池区别

本文为您介绍使用虚拟私有云产品时的资源池区别，请您务必仔细阅读后使用。

虚拟私有云 VPC 在不同资源池有不同的能力，具体可以分为地域资源池、可用区资源池。

- 地域资源池是没有可用区概念的资源池，您的所有资源都在地域下的一个数据中心中。
- 可用区资源池分单可用区资源池和多可用区资源池。可用区资源池和地域资源池网络架构类似，但是能力有区别，具体见下表。多可用区资源池下，vpc 产品可以助您实现多地容灾、多活等业务模式。

  具体区别如下：

产品模块	**地域资源池**	**可用区资源池**	**重要差异**
VPC	支持	支持	
子网	支持	支持	
安全组	支持	支持	可用区资源池： 安全组具有 VPC 属性，创建时需指定某一 VPC，且每一个 VPC 系统都会创建一个默认安全组。 地域资源池： 安全组不具备 VPC 属性，创建时无需指定所属 VPC，每个资源池会存在一个默认安全组。
ACL	支持	支持	可用区资源池：

			ACL 创建时无需指定子网，一个 ACL 支持绑定多个子网。每个 ACL 都会存在默认规则，不支持修改、删除、停用。 地域资源池： ACL 创建时需指定子网，一个 ACL 支持绑定一个子网。无默认规则。
虚拟 IP	支持	支持	可用区资源池： 部分多可用区资源池虚拟 IP 解绑服务器时需先解绑备服务器，再解绑主服务器。实际资源池情况以控制台为准。 地域资源池： 虚拟 IP 解绑服务器时支持无序解绑，即无“先备后主”的顺序。
路由表	支持	支持	地域资源池不支持 VPC 默认路由表；访问专线、VPN、对等连接不需要在路由表中配置路由。
IPv4 网关	不支持	支持	可用区资源池： 云主机通过公网 IP 访问公网时需要配置指向 IPv4 网关的路由

			地域资源池： 云主机绑定公网 IP 后即可访问公网。
IPv6 网关	不支持	支持	可用区资源池：通过 IPv6 访问公网时，需要先开通 IPv6 网关，然后开通 IPv6 带宽。 地域资源池：双栈网卡开通 IPv6 带宽即可访问公网。
NAT 网关	支持	支持	可用区资源池下的云主机通过 NAT 网关访问公网需要配置指向 NAT 网关的路由，然后配置 NAT 规则。 地域资源池下的云主机配置 NAT 规则后即可访问公网。
网卡	支持	支持	可用区资源池：支持弹性网卡，网卡创建后可以和云主机解绑/绑定。 地域资源池：创建网卡时必须关联到云主机上，网卡可以随时从云主机删除。
流量镜像	不支持	支持	可用区资源池：仅多可用区支持此功能，实际情况以控制台为

			准。
VPC 终端节点	不支持	支持	可用区资源池： 仅多可用区支持此功能，实际情况以控制台为准。

虚拟私有云快速入门

入门准备

本文将为您介绍如何快速搭建 IPv4 网段或 IPv6 网段的私有网络，以及搭建前的准备工作。

网段类型分类

- IPv4：IPv4 是一个 32 位地址，由四个 8 位数字组成。创建 VPC 及子网时，默认创建的网段为 IPv4 类型。IPv4 网络无法访问 Internet 上的 IPv6 服务，并且 IPv4 网络不能为使用 IPv6 终端的用户提供访问服务。
- IPv6：IPv6 是一个 128 位地址，由八个 16 位的十六进制数字组成。当您需要访问 Internet 上的 IPv6 服务或为使用 IPv6 终端的用户提供访问服务时，需要在配置时开启 IPv6 功能，开启后，您将拥有 IPv4 和 IPv6 两个网段，满足客户 IPv4 和 IPv6 的服务需求。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您需要确保账号中有足够的余额，关于账号充值，请参考费用中心在线充值。

搭建 IPv4 私有网络

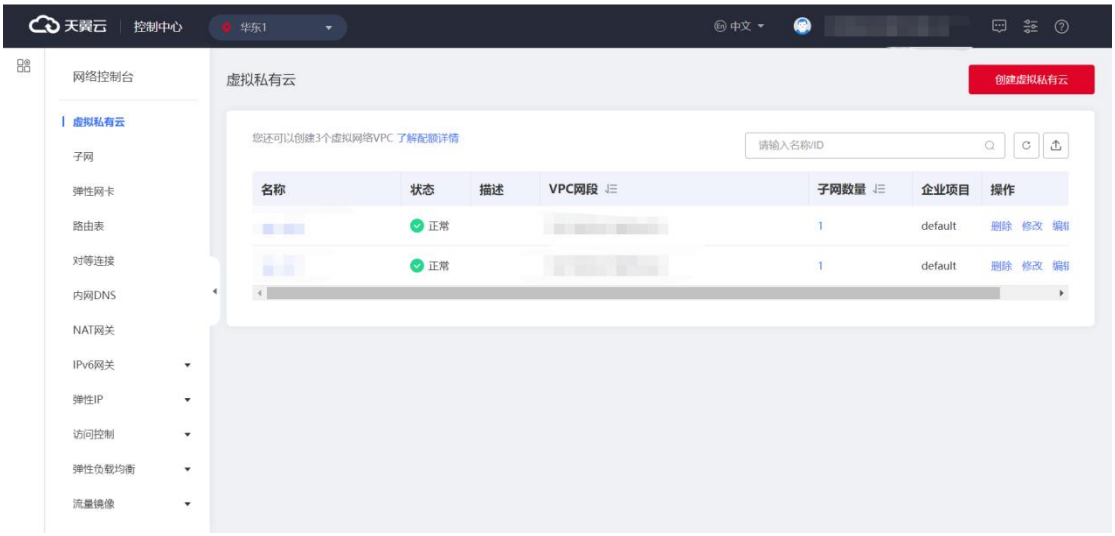
本文将帮助您搭建一个 IPv4 网段的 VPC，并为虚拟私有云中的弹性云主机实例绑定一个弹性 IP 进行公网访问。

操作步骤

创建 VPC 之前，您需要根据具体的业务需求规划 VPC 的数量、子网的数量和 IP 网段划分等。

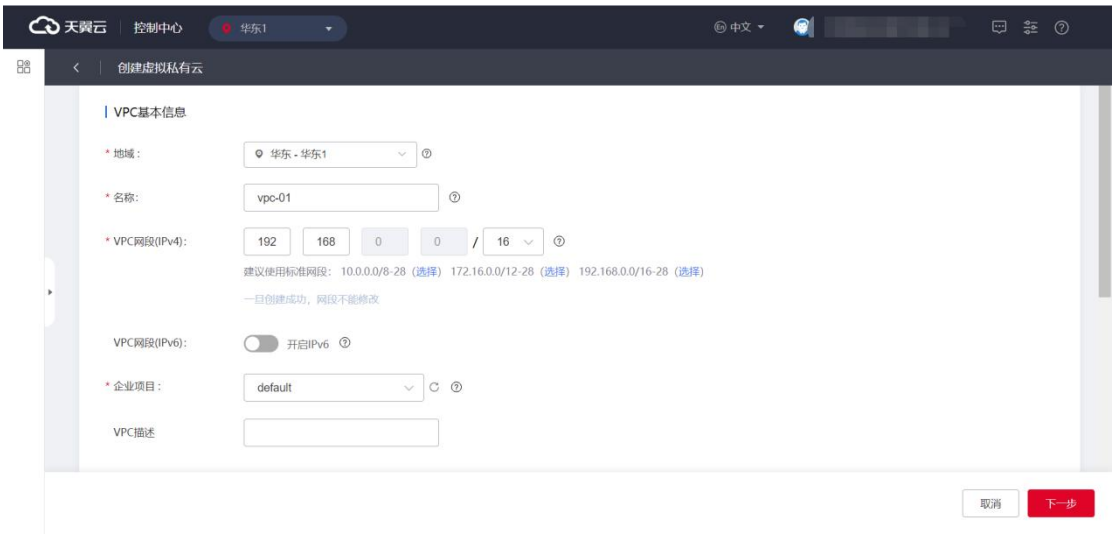
创建虚拟私有云和子网

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。



4. 点击“创建虚拟私有云”，进入“创建虚拟私有云”页面。

5. 在“创建虚拟私有云”页面，根据界面提示配置参数。



虚拟私有云具体参数说明如下：

参数名称	是否必填	含义	例子
地域	是	创建虚拟私有云的所属区域，建议就近选择靠近您业务的区域，可减少网络时延，提高访问	华东-华东 1

		速度	
名称	是	VPC 的名称，由数字、字母、中文、-、_组成，不能以数字、_和-开头	vpc-01
VPC 网段（IPv4）	是	虚拟私有云 VPC 的 IPv4 网段范围	192.168.0.0/16
VPC 网段（IPv6）	否	是否分配虚拟私有云 VPC 的 IPv6 地址	否
企业项目	是	当前 VPC 所属的企业项目	default
VPC 描述	否	自定义的 VPC 描述文案	用于政务网的 VPC

创建 VPC 时默认至少必须创建一个子网，配置信息如下：

子网具体参数说明如下：

参数名称	是否必填	含义	例子
子网名称	是	子网的名称，由数字、字母、中文、-、_组成，不能以数字、_和-开头	subnet-01
子网网段(IPv4)	是	子网的私有 IPv4 网段	192.168.0.0/24
网关(IPv4)	是	子网的网关地址，对于多可用区资源池，网关地址默认为.1,不	192.168.0.1

		可以指定其他地址； 对于单可用区资源池，网关地址默认为.1,可以指定其他地址。	
子网 IPv6 网段	否	是否分配子网的 IPv6 地址，只有该资源池支持 IPv6 网段，才会出现“开启 IPv6”选项，反之，则无此选项。	否
DNS 服务器地址	否	子网内的云主机访问公网时的 DNS 服务器地址，DNS 服务器默认地址自动填充，支持修改，但是不可以为空。	114.114.114.114,8.8.8.8
子网描述	否	自定义的子网描	

		述文案	

6. 点击“下一步”，进入资源详情页面，勾选我已阅读并同意相关协议《 天翼云虚拟私有云服务协议 》。
7. 点击“立即创建”，即可完成 VPC 和子网的创建。

购买弹性云主机

1. 在控制中心页面，在“计算”页签，点击“弹性云主机”，购买一个弹性云主机实例。详情请参见《弹性云主机用户指南》。
2. 网络：选择已创建的“vpc-01”及已创建的“subnet-01”子网。

3. 安全组：选择默认安全组“Sys-default”。 您也可以创建新的安全组并配置规则。详情请参见“创建安全组”、“添加安全组规则”。
4. 弹性 IP：默认选择“不使用”。

购买和绑定弹性 IP

弹性 IP（Elastic IP，EIP）是可以独立申请的公网 IP 地址，包括公网 IP 地址与公网出口带宽服务。您可以购买一个弹性 IP 并将其绑定到弹性云主机上，为其提供公网访问能力。如您已有弹性 IP，且处于未绑定状态，直接绑定弹性云主机即可。

1. 登录控制中心。
2. 在控制中心页面左上角点击  ，选择区域，本文我们选择华东 1。
3. 在控制中心页面，选择“网络 >弹性 IP”。
4. 单击“申请弹性 IP”。
5. 在弹性 IP 界面根据提示配置参数，参数说明如下：

参数名称	是否必填	含义	例子
地域	是	创建弹性 IP 的所属区域，建议就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	华东-华东 1
名称	是	弹性 IP 的名称，由数字、字母、中文、-、_组成，不能以数字、_和-开头。	eip-01
付费方式	是	付费方式分为以下两种：	按量付费

		• 包年/包月 • 按量计费	
计费类型	是	计费类型分为以下两种： • 按带宽计费 • 按流量计费	按带宽计费
带宽类型	是	付费方式分为以下两种： • 独享带宽 • 共享带宽	独享带宽
带宽	是	带宽大小，取数为整，步长为 1。	5Mbps
购买数量	是	弹性 IP 数量，支持修改。	1
企业项目	是	申请弹性 IP 时，可以将弹性 IP 加入已启用的企业项目	default

6. 点击“下一步”，进入弹性 IP 资源详情页面。
7. 确认资源规格无误后，勾选我已阅读并同意相关协议 《 天翼云弹性 IP 服务协议 》，点击确认下单。
8. 在目标弹性 IP 的列表页，在操作列，点击“绑定”“ 。

9. 在绑定弹性 IP 页面，选择要绑定的弹性云主机，点击“确定”，即可完成与弹性云主机的绑定。

测试公网连通性

绑定成功后，便可以从公网访问该弹性云主机。验证公网连通方法如下：

1. 您可以通过 SSH 密钥方式、VNC 等方式登录弹性云主机，具体请参见登录弹性主机。
2. 从外网 ping 该弹性云主机的弹性 IP 地址，验证公网通信是否正常。

搭建 IPv6 私有网络

本文将帮助您搭建一个 IPv6 网段的私有网络，并在 VPC 中创建一个带有 IPv6 地址的弹性云主机，使弹性云主机可以访问 Internet 上的 IPv6 服务。

操作步骤

创建 VPC 之前，您需要根据具体的业务需求规划 VPC 的数量、子网的数量和 IP 网段划分等。

创建虚拟私有云和子网

1. 登录控制中心。
2. 在控制中心页面左上角点击  ，选择区域，本文我们选择华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 点击“创建虚拟私有云”，进入“创建虚拟私有云”页面。
5. 在“创建虚拟私有云”页面，根据界面提示配置参数。VPC 配置时，请务必勾选“开启 IPv6”，如果开启 IPv6 功能配置后，将自动为子网分配 IPv6 网段，但您不能选择 IPv6 地址范围，子网下所有网卡关闭 IPv6 时，才能关闭子网 IPv6。

虚拟私有云具体参数说明如下：

参数名称	是否必填	含义	例子
地域	是	创建虚拟私有云的所属区域，建议就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	华东-华东 1
名称	是	VPC 的名称，由数字、字母、中文、-、_组成，不能以数	vpc-ipv6

		字、_和-开头	
VPC 网段(IPv4)	是	虚拟私有云VPC的IPv4 网段范围	192.168.0.0/16
VPC 网段(IPv6)	是	是否分配虚拟私有云 VPC 的 IPv6 地址	开启 IPv6
企业项目	是	当前VPC所属的企业项目	default
VPC 描述	否	自定义的VPC描述文案	用于政务网的VPC

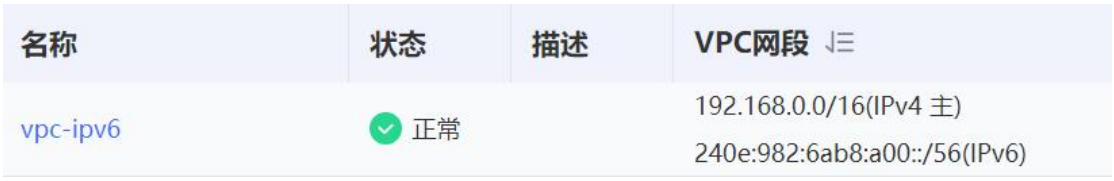
说明：对于地域资源池，VPC 上没有开启 IPv6 开关，仅在子网上有开启 IPv6 开关；实际产品能力以控制台展现为准。

子网具体参数说明如下：

参数名称	**是否必填**	**含义**	**例子**
子网名称	是	子网的名称，由数字、字母、中文、-、_组成，不能以数字、_和-开头	subnet-ipv6
子网网段(IPv4)	是	子网的私有IPv4 网段	192.168.0.0/24
网关(IPv4)	是	子网的网关地	192.168.0.1

		址，对于多可用区资源池，网关地址默认为.1，不可以指定其他地址； 对于单 AZ 资源池，网关地址默认为.1,可以指定其他地址。	
子网 IPv6 网段	是	是否分配子网的 IPv6 地址	开启 IPv6
DNS 服务器地址	否	子网内的云主机访问公网时的 DNS 服务器地址，DNS 服务器默认地址自动填充，支持修改，但是不可以为空。	114.114.114.114,8.8.8.8
子网描述	否	自定义的子网描述文案	

6. 点击“下一步”，进入资源详情页面，勾选我已阅读并同意相关协议《 天翼云虚拟私有云服务协议 》。
7. 点击“立即创建”，即可完成 VPC 和子网的创建。



购买弹性云主机

1. 在控制中心页面，在“计算”页签，点击“弹性云主机”，购买一个弹性云主机实例。详情请参见《弹性云主机用户指南》。
2. 网络：选择已创建的支持 IPv6 地址的 VPC，以及已创建的支持 IPv6 地址的子网。

3. 安全组：选择默认安全组。默认安全组的规则是在出方向上的 IPv4/IPv6 数据报文全部放行，入方向访问受限，安全组内的弹性云主机无需添加规则即可互相访问。
4. 弹性 IP：选择“不使用”。

5. 购买完成后，您可以在弹性云主机详情页查看自动分配的 IPv6 地址，也可以登录到弹性云主机，通过 ifconfig 查看分配的 IPv6 地址。

购买和加入共享带宽（可选）

默认 IPv6 地址只具备私网通信能力，如果您需要通过该 IPv6 地址访问 Internet 或被 Internet 上的 IPv6 客户端访问，您需要购买和绑定共享带宽。

如您已有共享带宽，可以不用重新购买，直接将 IPv6 地址加入共享带宽即可。

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在系统首页，选择“网络 > 弹性 IP”。
4. 在左侧导航栏，选择“弹性 IP > 共享带宽”。
5. 在页面右上角，单击“购买共享带宽”，按照提示配置参数。

测试公网连通性

您可以通过 SSH 密钥方式、VNC 等方式登录弹性云主机，ping 一个公网上的 IPv6 服务，验证连通性。验证公网通信是否正常。

虚拟私有云用户指南

虚拟私有云 VPC 管理

创建虚拟私有云

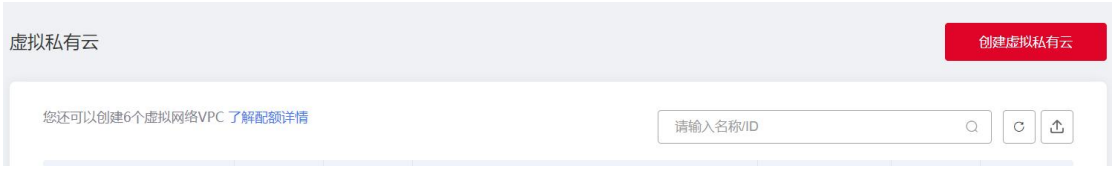
本文帮助您快速熟悉虚拟私有云 VPC 的创建。

操作场景

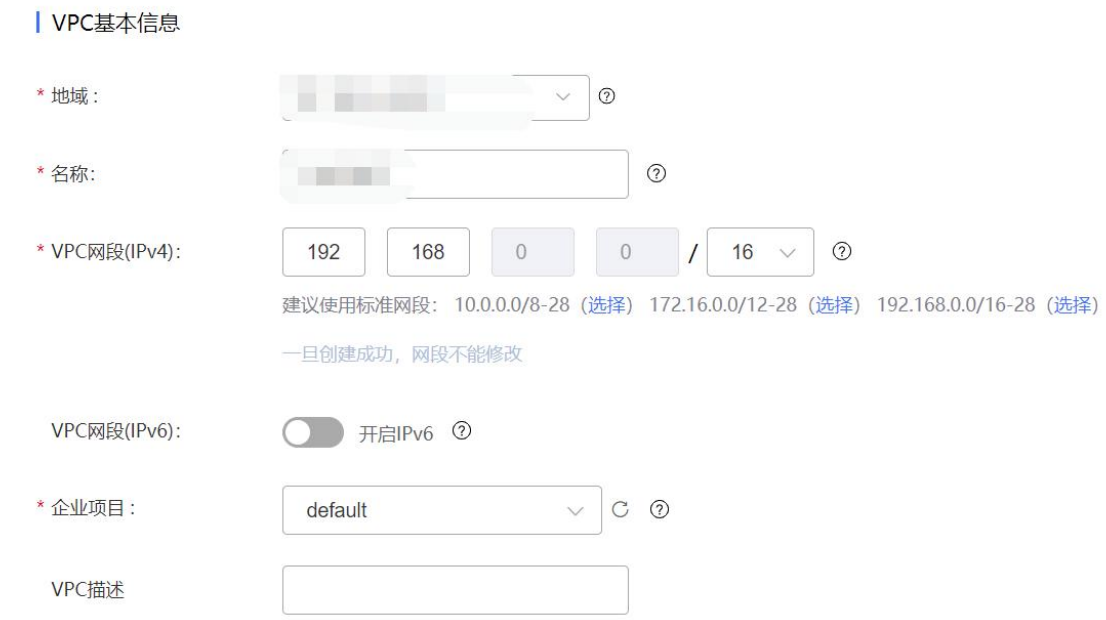
当需要为您的弹性云主机构建隔离的、用户自主配置和管理的虚拟网络环境时，首先要申请虚拟私有云。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在“虚拟私有云列表”界面，单击“创建虚拟私有云”。



5. 在“申请虚拟私有云”页面，根据界面提示配置参数。



参数	说明	取值样例
名称	VPC 名称	VPC-001
网段	VPC 的地址范围，VPC 内的子网地址必须在 VPC 的地址范围内。 目前支持网段范围： 10.0.0.0/8~28、 172.16.0.0/12~28、 192.168.0.0/16~28。 如果要使用其他网段，请申请工单。	192.168.0.0/16
子网名称	子网的名称。	Subnet-001
子网网段	子网的地址范围，需要在 VPC 的地址范围内。	192.168.0.0/24

网关	子网的网关，默认为子网内第一个可用 IP。	192.168.0.1
子网 IPv6 网段	开启 IPv6 功能后，将自动为子网分配 IPv6 网段，但您不能选择 IPv6 地址范围。	240e:980:1800:81::/64

修改虚拟私有云

本文帮助您快速熟悉虚拟私有云 VPC 的修改。

操作场景

如果您想通过 VPC 名称来区别不同的业务系统，您可以通过修改 VPC 名称来统一命名，本文主要帮助您了解如何修改虚拟私有云的名称。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在“虚拟私有云列表”界面，找到您需要修改的 VPC，在“操作”列，点击“修改”选项。

5. 根据界面提示修改 VPC 的名称。

删除虚拟私有云

本文帮助您快速熟悉虚拟私有云 VPC 的删除。

操作场景

如果您不再继续使用某个 VPC，您可以删除 VPC 来减少管理和维护的成本。

前提条件

虚拟私有云通常由于被子网、自定义路由或者其他服务资源使用而导致无法删除，需要您根据控制台的提示信息解除和 VPC 的关联，然后删除虚拟私有云。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在“操作”列，点击“删除”选项。

5. 根据弹框提示，点击“确认”按钮，即可删除。

虚拟私有云扩展网段

本文帮助您了解虚拟私有云内网网段的基本概念和使用说明。

基本概念

- VPC 主网段：VPC 创建时选择的网段被称为主网段。VPC 主网段随 VPC 创建、删除，不允许单独删除。
- VPC 扩展网段：VPC 创建后添加的平行网段被称为扩展网段。扩展网段和 VPC 主网段平行、使用方法相同。您可以在 VPC 扩展网段中创建子网、云主机等其他操作，和 VPC 主网段使用方法相同。

使用场景

- VPC 创建后，若主网段不够分配或者网络地址规划原因，需要增加其他网段时，您可以通过添加扩展网段来增加 VPC 的网段。
- 添加扩展网段后，您可以选择使用主网段或扩展网段来创建子网，但每个子网只能属于一个 VPC 网段。
- VPC 网段创建后不支持修改，子网网段创建后不支持修改，请提前做好网络规划。

约束与限制

- 一个 VPC 默认只能添加 2 个 IPv4 扩展网段；默认可以使用 10.0.0.0/8-28、172.16.0.0/12-28、192.168.0.0/16-28 三个标准私网网段及其子网段作为扩展网段。如果您想使用这三个标准私网网段之外的其他网段，请提交工单、开通权限后操作。
- 扩展网段不能和 VPC 的主网段有重叠。
- 主网段和扩展网段不能使用系统的预占地址段及其子网段，系统的预占地址段表格如下：

预占地址段	用途
0.0.0.0/8	RFC 保留
255.255.255.255/32	RFC 保留
127.0.0.0/8	RFC 保留
224.0.0.0/4	RFC 保留
240.0.0.0/4	RFC 保留
100.64.0.0/10	内部业务使用
198.19.128.0/20	内部业务使用

33.0.0.0/8	内部业务使用
169.254.0.0/16	内部业务使用
100:0:0:0::0/50	内部业务使用

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在虚拟私有云列表，找到您要修改扩展网段的 VPC，点击“编辑网段”，在编辑网段页面，根据您的业务需求编辑扩展网段。

子网管理

创建子网

本文帮助您快速熟悉子网的创建。

操作场景

申请虚拟私有云时会创建一个子网，当该虚拟私有云还需要添加其他子网时，可以通过以下两种方式创建新的子网来为 VPC 增加私有网络。

操作步骤

方式一：

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在“虚拟私有云列表”界面，选择需要创建子网的 VPC，并单击“子网”，在“子网”页签，单击“创建”按钮。

5. 在创建子网页面，根据界面提示配置参数，参数如下表所示：

参数	说明	取值样例
子网名称	子网的名称	Subnet-01
子网网段	子网的地址范围，需要在 VPC 的地址范围内	192.168.0.0/24
网关	子网的网关	192.168.0.1
开启 IPv6	开启 IPv6 功能后，将自动为子网分配 IPv6 网段，但您不能选择 IPv6	240e:980:1800:81::/64

	地址范围，subnet 下所有网卡关闭 IPv6 时，才能关闭子网 IPv6。	
DNS 服务器地址	DNS 服务器地址最多支持两个 IP，请以英文逗号隔开。	114.114.114.114 ,8.8.8.8

6. 单击“确定”按钮。

方式二：

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 单击“子网”，进入子网列表页面，单击“创建子网”按钮。

5. 在创建子网页面，根据页面提示配置参数。
6. 单击“确定”按钮。

修改子网

本文帮助您快速熟悉子网的修改。

操作场景

您可以修改子网的子网名称、子网 IPv6 网段、描述等信息，以满足业务中遇到的扩展网络规模等场景。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成子网的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击  ，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 单击“子网”，进入子网列表页面。
5. 单击目标子网“操作”列的“修改”选项，进入“修改子网”页面。
6. 在修改子网页面，根据界面提示进行参数修改。修改完毕单击“确认”按钮。

删除子网

本文帮助您快速熟悉子网的删除。

操作场景

当您不需要此子网的时候，可以进行删除操作。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成子网的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 单击“子网”，进入子网列表页面。
5. 单击目标子网“操作”列的“删除”选项，根据弹框提示进行删除。

   注意：该子网下有正在使用的虚拟 IP，不可删除。

查看子网

本文帮助您快速熟悉如何查看子网的子网网段、状态、DNS 服务器等信息。

操作场景

当您查看子网的相关联的 ACL、主机、虚拟 IP、路由等信息时，可以进行通过以下操作进行查看。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成子网的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 单击“子网”，进入子网列表页面。
5. 单击目标子网的子网名称，进入子网详情页。在详情页，可查看该子网的子网网段、状态、DNS 服务器等信息。

弹性网卡

本文帮助您快速熟悉弹性网卡基本知识。

弹性网卡基本知识

弹性网卡是虚拟私有网络 VPC 中的虚拟网络接口，用于连接 ECS 与私有网络。

每个弹性网卡可以包含以下主要属性：

- 专有网络 VPC、子网信息
- VPC 子网的 IPv4 地址范围内的一个主要私有 IPv4 地址

- VPC 子网的 IPv4 地址范围内的一个或者多个辅助私有 IPv4 地址
- 一个或多个公有 IPv4 地址
- 一个或多个 IPv6 地址
- □ 一个 MAC 地址
- □ 一个或多个安全组

网卡类型

网卡类型包括主网卡和辅助网卡。随着云主机、物理机服务器等实例一起创建的网卡称为主网卡。VPC 网络中的每个实例都有默认的主网卡，您无法独立创建和从实例卸载主网卡。您可以创建并额外绑定到实例上的网卡，称为辅助网卡，辅助网卡可以灵活的和实例解绑、绑定。

私有 IPv4 地址

每个弹性网卡都有一个子网地址范围内的私有 IPv4 地址，称为主私网地址。您可以在创建辅助弹性网卡时指定主私网地址，如果不指定，我们将为您随机分配。此外，您还可以为弹性网卡分配一个或者多个辅助私有 IPv4 地址，辅助私有 IP 地址在取消分配后可以回收，然后再分配给其他弹性网卡。

私有 IPv6 地址

如果虚拟私有网络 VPC 和子网开通了 IPv6 网段，您可以为弹性网卡分配一个辅助私有 IPv6 地址。辅助私有 IPv6 地址在取消分配后可以回收。VPC 内的 IPv6 地址支持 VPC 内网通信和公网通信，网卡绑

定 IPv6 带宽或者加入共享带宽后，可以使用 IPv6 来访问公网或被公网访问。

弹性公网 IP 地址

弹性网卡绑定一个或者多个弹性 IP，用于公网通信。使用弹性 IP 时会将网卡的私网 IP NAT 成为公网 IP，以此来访问公网或者被公网访问。

多队列

网卡多队列是指实例规格支持的最大网卡队列数。单台 ECS 实例 vCPU 处理网络中断存在性能瓶颈时，您可以将实例中的网络中断分散给不同的 vCPU 处理，从而提升性能。

修改内网 IP/切换 VPC

云主机、物理机的主网卡提供以下能力：修改为同子网下其他 IP、切换同 VPC 下的其他子网、切换至其他 VPC。

您可以通过修改云主机、物理机服务器的主网卡 IP 或者切换 VPC、子网来实现迁移功能，在网络规划存在冲突或者需要隔离某个服务器时，可以使用此功能。

注意：弹性网卡仅适用于可用区资源池，不同资源池列表见产品简介-资源池区别页面，实际情况以控制台展现为准。

创建弹性网卡

本文帮助您快速熟悉创建弹性网卡的相关操作。

操作场景

创建弹性网卡可用于实现灵活、高可用的网络方案配置。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经创建虚拟私有云 VPC、子网、弹性云主机。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 单击“弹性网卡”，进入弹性网卡列表页面。单击“创建弹性网卡”，进入创建弹性网卡界面。
5. 在创建弹性网卡详情页填写基本信息。弹性网卡具有子网属性，创建后只能挂载到对应子网的云主机、物理机实例上。可以通过分配辅助私网 IP 来实现单网卡多 IP。

参数	描述
名称	弹性网卡名称，由数字、字母、中文、-、_组成，不能以数字、_和-开头。
VPC	选择弹性网卡归属的 VPC，必填项。
子网	选择弹性网卡归属的子网，必填项。
主私网 IPv4	自动分配

地址	
辅助私网 IP	可以选择不设置、自动分配，或者指定地址。
安全组	选择弹性网卡所属安全组。

6. 填写基本信息后，点击“确定”按钮，弹性网卡创建成功。

修改弹性网卡基本信息、分配 IPv6、辅助私网 IP

本文帮助您快速熟悉如何修改弹性网卡的基本信息、分配 IPv6、辅助私网 IP。

操作场景

您可以根据业务需求修改弹性网卡的名称、安全组，管理辅助私网 IP。

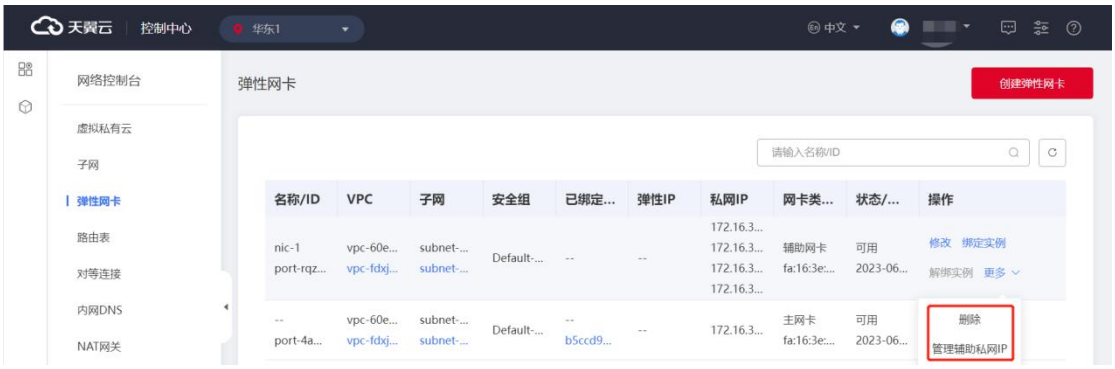
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经创建虚拟私有云 VPC、子网、弹性云主机。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 单击“弹性网卡”，进入弹性网卡列表页面。

5. 在弹性网卡列表页找到对应的弹性网卡，点击“修改”，填写名称、安全组、描述，点击“确定”即可完成修改。
6. 在目标弹性网卡的“操作”列，点击“管理辅助私网 IP”。



7. 在弹窗页面可以取消分配主私网 IPv6 地址，取消分配后 IPv6 地址回收。再次分配可以重新获得 IPv6 地址。您也可以分配新的辅助私网 IP（IPv4）或者取消分配。

   注意：分配辅助私网 IP 后，您需要登录服务器实例，在实例内部配置已分配的辅助私网 IP 地址。
8. 当您不需要此弹性网卡时，点击弹性网卡列表“删除”，即可删除该弹性网卡。

弹性网卡绑定/解绑云主机、物理机服务器等实例

本文帮助您快速熟悉如何绑定/解绑云主机、物理机服务器等实例。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经创建弹性网卡、云主机。

方式一：在弹性网卡页面操作

操作步骤：

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在弹性网卡列表页，点击“绑定实例”。

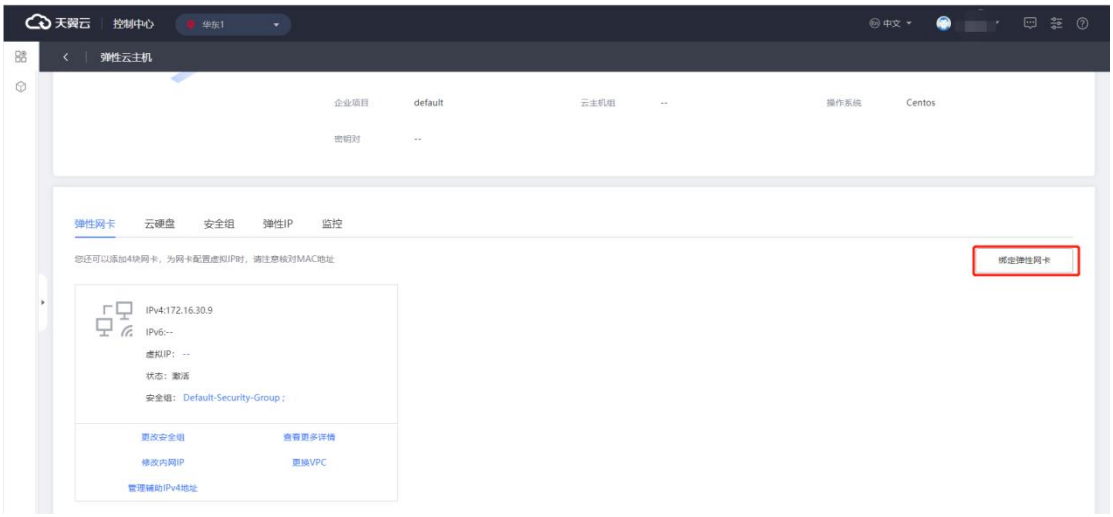
5. 在弹窗中选择需要绑定的云主机或者物理机服务器即可。

6. 在弹性网卡列表页，点击“解绑实例”。

7. 在解绑实例弹窗，点击“确定”即可。

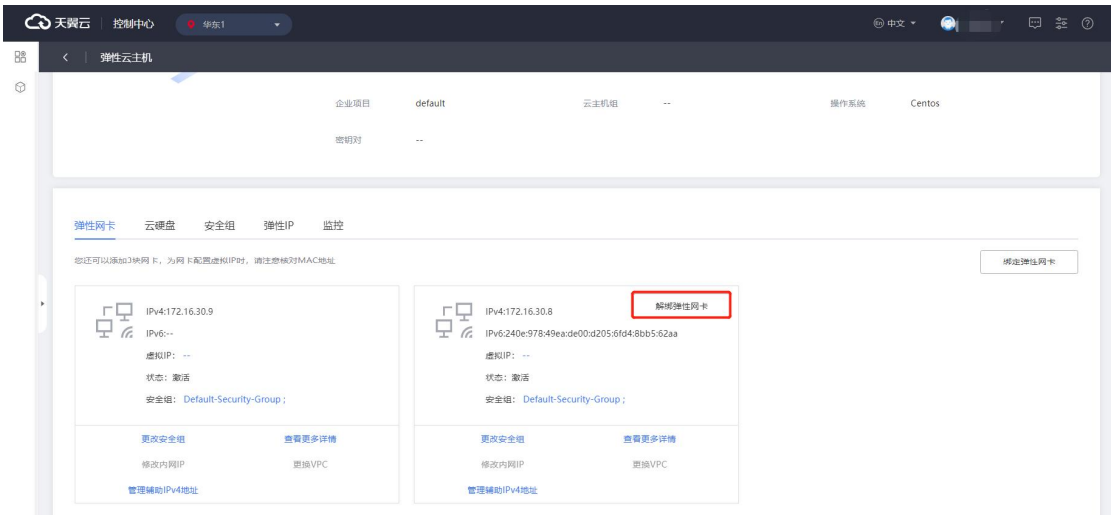
方式二：在云主机、物理机服务器页面操作

1. 打开云主机详情页，点击“绑定弹性网卡”。



2. 在绑定弹窗，选择需要的弹性网卡，点击“确定”即可。

3. 在云主机详情页，点击“解绑弹性网卡”。



4. 在解绑弹窗，点击“确定”即可。

实例内部配置已分配的辅助私网 IP 地址

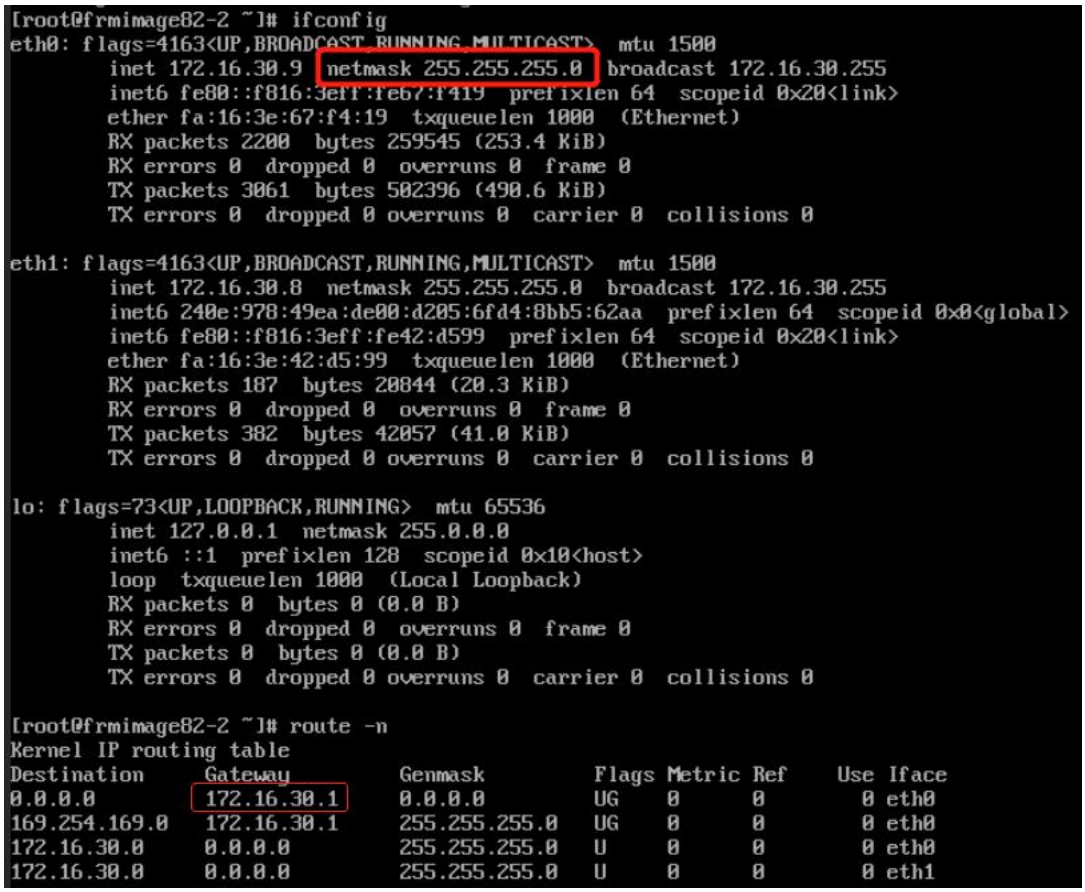
本文以 Linux 系统为例在实例内部配置辅助私网 IPv4 地址。

前提条件

已从控制台分配完成辅助私网 IPv4 地址。

操作步骤

1. 远程登录 ECS 实例。
2. 使用 ifconfig 命令查询子网掩码，并使用 route -n 命令查询默认网关。



3. 修改网络配置文件

如果配置单个私网 IPv4 地址，运行 vi /etc/sysconfig/network-scripts/ifcfg-eth0:0 命令，并添加相应的配置项。

配置项如下：

DEVICE=eth0:0

TYPE=Ethernet

BOOTPROTO=static

ONBOOT=yes

IPADDR=<分配的辅助私网 IPv4 地址 1>

NETMASK=<IPv4 子网掩码>

如果需要继续配置更多私网 IPv4 地址，递增 DEVICE 对应的序号并继续添加配置项即可。

例如运行 vi /etc/sysconfig/network-scripts/ifcfg-eth0:1 命令，添加配置项示例如下所示：

DEVICE=eth0:1

TYPE=Ethernet

BOOTPROTO=static

ONBOOT=yes

IPADDR=<分配的辅助私网 IPv4 地址 2>

NETMASK=<IPv4 子网掩码>

4. 根据操作系统类型运行相应的命令使配置生效

Cent OS 7：运行 service network restart 重启网络服务

Cent OS 8：运行 systemctl restart NetworkManager 命令重启网络服务。

运行 nmcli device reapply eth0 命令重连 eth0 网卡，或者运行 reboot 命令重启实例。

5. 运行 ifconfig 查看配置效果。

路由表

路由表概述

本文为您介绍路由表的定义、分类、路由规则等内容。

路由表由多条路由规则组成，用于控制虚拟私有云内子网的出流量走向。当您创建虚拟私有云后，系统会自动为您创建一张默认路由表，用来管理 VPC 的流量转发路径。每个子网只能关联一个路由表，一个路由表可以关联多个子网。您可以创建多个路由表，为不同流量走向的子网关联不同的路由表。

路由表分类

默认路由表

当您创建虚拟私有云时，系统会自动为其生成一个默认路由表。在创建子网时，如果您没有选择自定义路由表，子网会自动关联该默认路由表。您可以在默认路由表中添加、删除和修改路由规则，但无法删除该默认路由表。当您创建 VPN、专线、云间高速后，会在默认路

由表自动生成指向 VPN 网关、专线网关、云间高速网关的路由规则；您也可以在自定义路由表创建指向 VPN 网关、专线网关、云间高速网关的路由规则。

自定义路由表

您可以在虚拟私有云中创建自定义路由表。通过自定义路由表和子网进行绑定，可以实现更加精细化的网络流量管理。

自定义路由表可以被删除，并且可以关联子网用于管理子网出方向流量。

网关路由表

您在创建自定义路由表时选择网关类型，并将网关路由表和 IPv4 网关绑定，该路由表被称为网关路由表。网关路由表用来管理进入 IPv4 网关（公网网关）的流量，可以将公网流量转发到 VPC 中的安全设备（例如云防火墙）做统一安全防护。

使用路由表时，请注意以下事项：

- 一个 VPC 下会自动生成一张默认路由表，默认路由表无法删除，只能随 VPC 一起删除。
- 一个子网只能绑定一张路由表，子网的路由策略由其关联的路由表管理。多个子网可以绑定同一张路由表。
- 创建子网后，子网会自动关联默认路由表。
- 如果您需要将子网绑定的默认路由表更换成自定义路由表，直接将默认路由表与子网解绑，再换绑自定义路由表即可。

路由规则

路由表中的每一项是一条路由规则。路由规则由目标地址、下一跳类型、下一跳三部分组成。路由规则包括系统路由规则、自定义路由规则。

系统路由

系统路由系统默认创建，您不能修改系统路由。

目标网段	下一跳类型	下一跳	路由类型	描述	用途
VPC IPv4 网段	vpc.routing_table.local	local	系统	default routes with local	用于 VPC 内部互通
VPC IPv6 网段	vpc.routing_table.local	local	系统	default routes with local	用于 VPC 内部互通
0.0.0.0/0	IPv4 网关	IPv4 网关实例	系统	default routes with igw	用于访问公网
100.95.0.1/32	vpc.routing_table.	DNS 网关实例	系统	default routes with dnsgw	用于访问内网 DNS

	dnsgw				
fd00:ec2::250/128	vpc.routing_table.dnsgw	DNS 网关实例	系统	default routes with dnsgw	用于访问内网 DNS

自定义路由

您在默认路由表或者自定义路由表中手动创建的路由规则称为自定义路由。添加自定义路由时，下一跳类型及用途如下表：

下一跳类型	说明
云主机	将流量转发至 VPC 内的一台云主机实例的主网卡。
物理机	将流量转发至 VPC 内的一台物理机实例。
弹性网卡	将流量转发至指定的辅助弹性网卡。
虚拟 IP	将流量转发至虚拟 IP。
对等连接网关	将流量转发至 VPC 对等连接。
IPv4 网关	将流量转发至指定的 IPv4 网关；云主机绑定弹性 IP 后需要配置此路由才能访问公网。
NAT 网关	将流量转发至指定的 NAT 网关；配置此路由后，才能通过 NAT 网关做 SNAT 访问公网或者 DNAT 被公网访问时。
专线网关	将流量转发至专线网关，以此实现 VPC 和客户侧 IDC 通过专线网关互通；配置完成专线连接后，会自动同步目的地址为 IDC 侧 cidr 下一跳为专线网关的路由规则到默认路由表；不允许在默认路由表手动创建指向专线网关的路由规

	则。
VPN 网关	将流量转发至 VPN 网关，以此实现 VPC 和客户侧 IDC 的通过 VPN 网关互通；配置完成 VPN 连接后，会自动同步目的地址为 IDC 侧 cidr 下一跳为 VPN 网关的路由规则到默认路由表；不允许在默认路由表手动创建指向 VPN 网关的路由规则。
云间高速网关	将流量转发至云间高速网关；配置完云间高速后，会自动同步目的地址 下一跳为云间高速网关的路由规则到默认路由表；不允许在默认路由表手动创建指向云间高速网关的路由规则

路由转发规则

根据最长掩码匹配规则确定如何路由网络流量。同一张路由表下，自定义路由规则之间的目的网段不能相同；自定义路由规则和系统路由规则目的相同时，系统路由规则优先级低于自定义路由规则，默认优先匹配自定义路由规则。

创建路由表

本文将帮助您快速熟悉路由表的创建。

创建 VPC 后，系统会自动生成一张默认路由表，默认路由表只能随 VPC 一起删除，无法手动创建和删除，以创建自定义路由表为例。

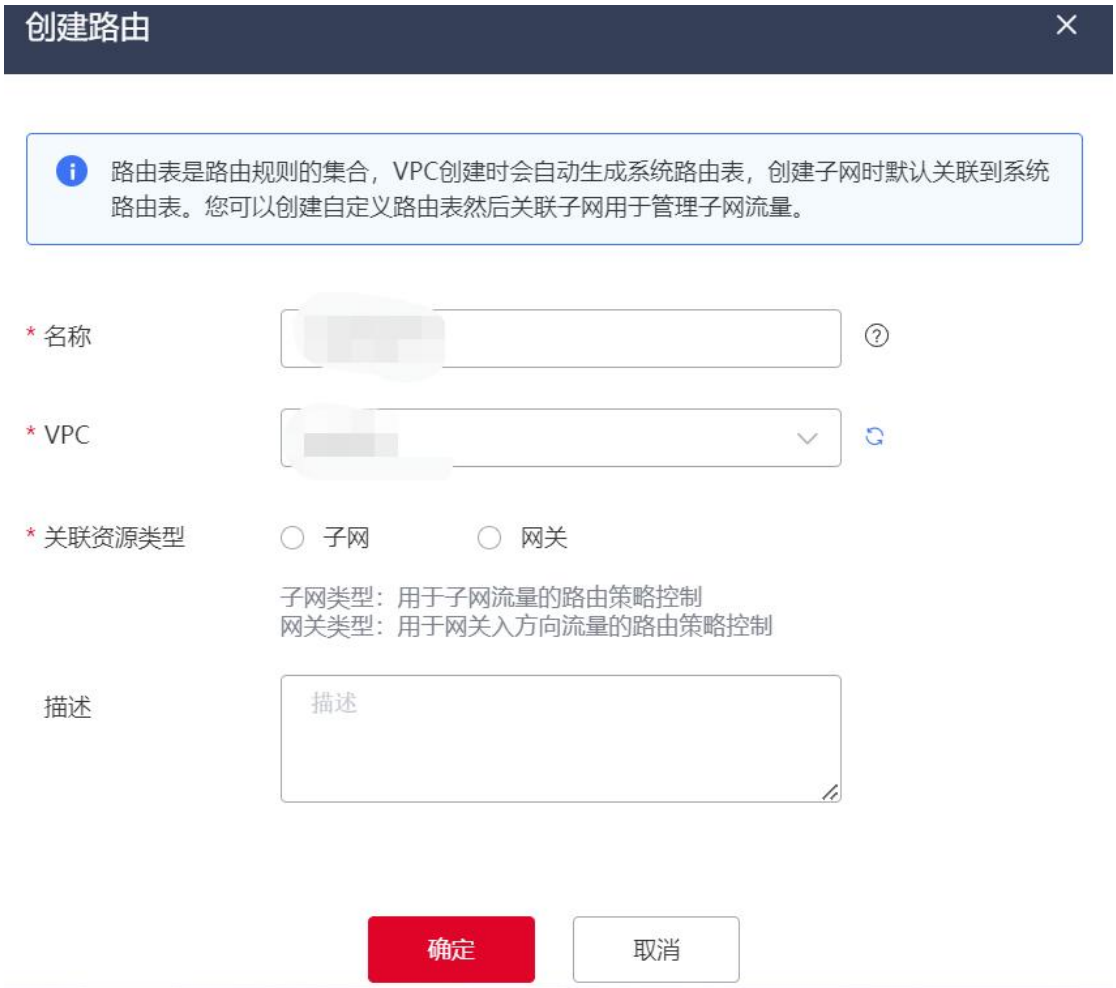
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 登录控制中心，并且已经完成虚拟私有云和子网的创建。

操作步骤

1. 进入“网络控制台”页面，点击“路由表”。

2. 在路由表列表页面，点击右上侧的“创建路由表”。



3. 在创建路由表页面，根据以下信息配置路由表，然后单击“确定”按钮。

参数	描述	举例说明
名称	路由表的名称，由数字、字母、中文、-、_组成，不能以数字、_和-开头。	router-01
VPC	选择路由表归属的VPC，必填项。	vpc-01
关联资源类型	子网类型：用于子网出方向流量的路由策略控	子网

	制；网关类型：用于网关入方向流量的路由策略控制。	
描述	路由表的描述信息，非必填项。	

创建路由规则

本文将帮助您快速熟悉路由表的创建。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 登录控制中心，并且已经完成虚拟私有云、子网和路由表的创建。

操作步骤

1. 进入“网络控制台”页面，点击“路由表”选项。
2. 找到对应的路由表，点击路由表名称，进入路由表详情页。

3. 在路由表详情页，找到“路由规则”页签，点击“创建”，进入创建路由规则详情页。

4. 在创建路由规则详情页，根据页面参数提示进行操作，具体参数表格如下：

参数	说明
IP 类型	可选择 IPV4、IPV6 两种不同的网络类型。
目的地址	网络流量传输到的 IP 地址范围。
下一跳类型	用于传输网络流量的云产品，例如：云主机。
描述	可选项

5. 点击“确定”按钮，即可完成路由规则的创建。

路由表关联子网

通过将路由表关联到某些子网，可以将子网的流量按照路由规则进行匹配转发。子网必须关联路由表后，才能进行正常的流量转发。本文将帮助您快速了解路由表如何关联子网。

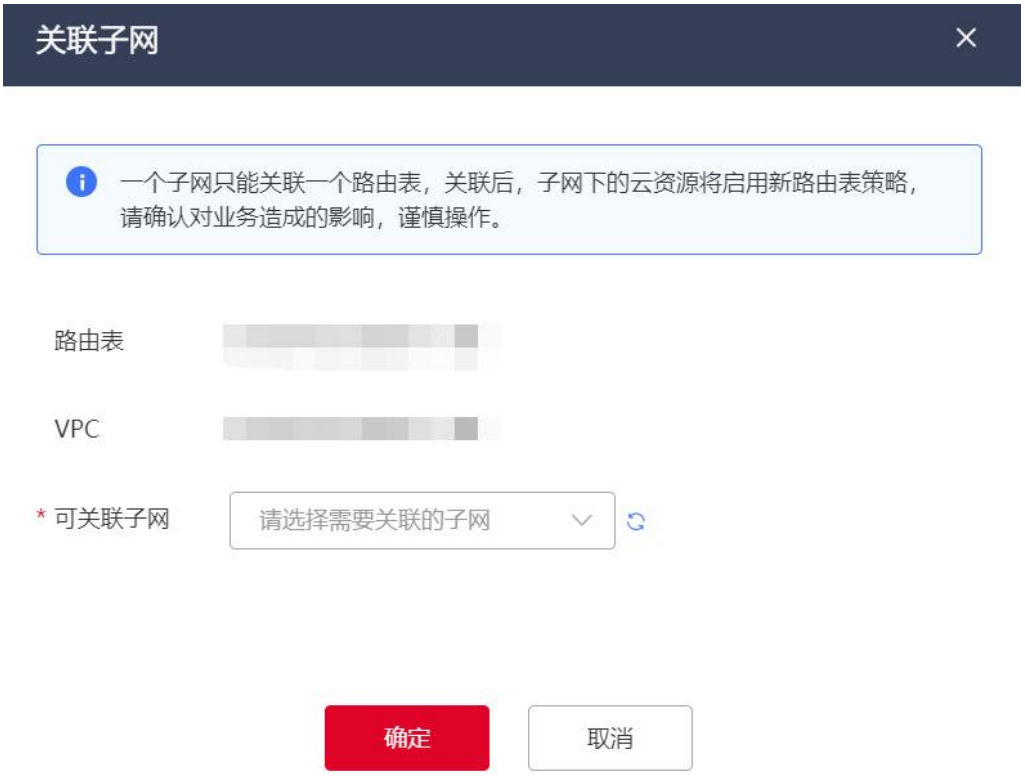
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 登录控制中心，并且已经完成虚拟私有云、子网、路由表和路由规则的创建。

操作步骤

1. 进入“网络控制台”页面，点击“路由表”选项。
2. 找到对应的路由表，点击路由表名称，进入路由表详情页。
3. 在路由表详情页，找到“关联子网”页签，点击“关联子网”，进入关联子网页面。

4. 在关联子网页面，选择可关联的子网，点击“确定”按钮即可。



5. 您也可以通过更换路由表，将子网从某个路由表换绑至其他路由表。

NAT 网关

产品定义

本文为您介绍 NAT 网关定义和产品架构等。

产品概述

NAT 网关（NAT Gateway）是一种支持 IP 地址转换的网络云服务，能够为虚拟私有云（Virtual Private Cloud，VPC）内的计算实例提供网络地址转换（Network Address Translation），分为 SNAT 和 DNAT 两个功能。通过 SNAT 可使多个弹性云主机共享使用弹性 IP 访问 Internet。通过 DNAT 可使多个弹性云主机提供互联网服务。NAT 网关是 VPC 内的一个公网流量的出入口，保护私有网络信息不直接对公网暴露。

产品基本概念

弹性 IP 地址

由天翼云提供的互联网协议地址，是互联网上可以被路由的地址。云上资源如果要对外提供服务，需要购买弹性公网地址并直接通过资源绑定或通过 NAT 网关规则绑定。

NAT（网络地址转换）

VPC 内的云上资源分配的是私网 IP，在互联网上私网 IP 不可被路由。如果 VPC 内的云上资源要与互联网互通或对互联网提供服务，则需要将云上资源的私网 IP 转换成可被路由的公网 IP，并对外进行发布。

DNAT（目的地址转换）

定义：通过 IP 映射或端口映射，将 IP 报文中的目的地址进行转换。

用户可以通过配置 NAT 网关 DNAT 规则实现 VPC 内多个云主机资源共享弹性 IP 对外提供服务。

SNAT（源地址转换）

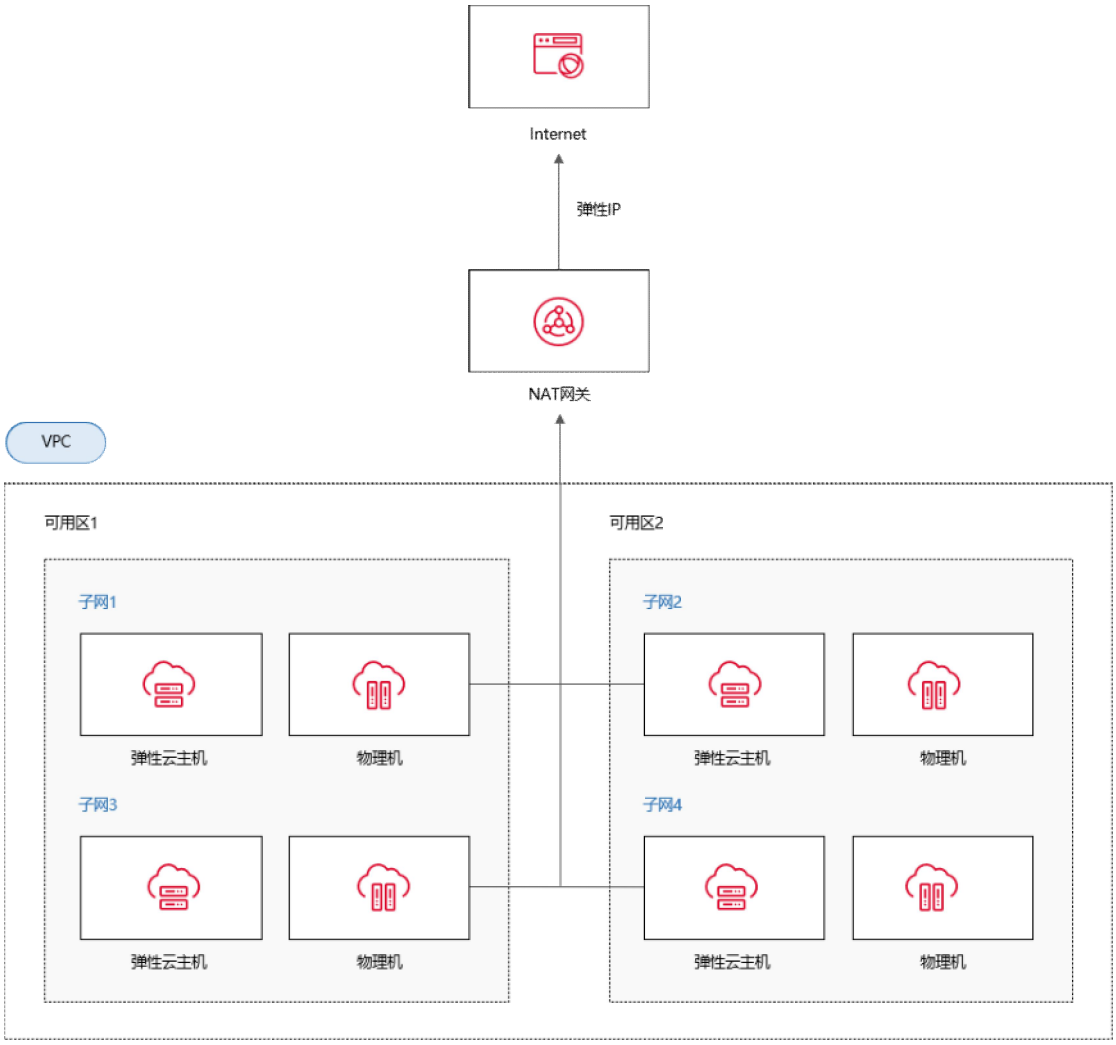
定义：将 IP 报文的源地址、源端口进行转换。

用户可以通过配置 NAT 网关 SNAT 规则，将云主机的私网 IP 转换成弹性公网 IP，使 VPC 内没有公网 IP 的云主机可以直接访问公网，实现 VPC 内多个云主机资源共享弹性 IP 主动访问 Internet。

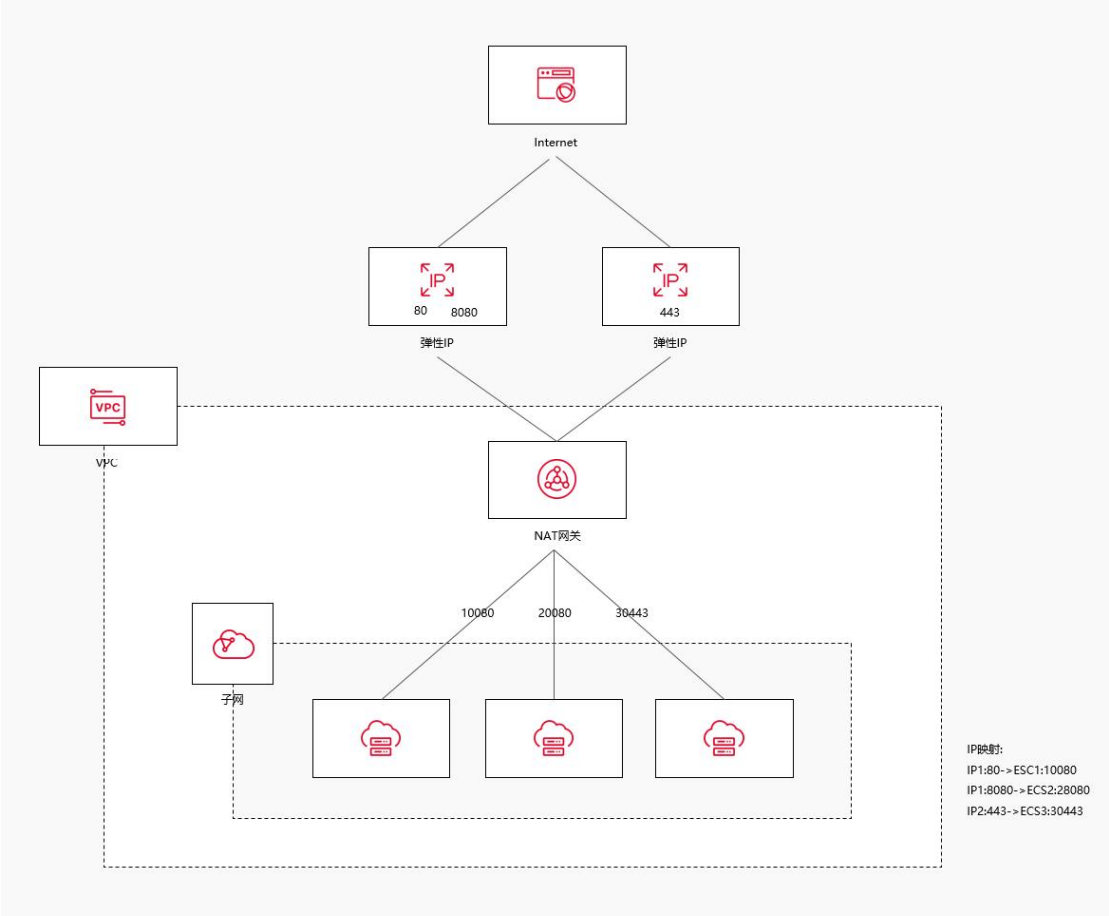
产品架构

NAT 网关分为 SNAT 和 DNAT 两个功能。

SNAT 功能通过绑定弹性公网 IP，实现私有 IP 向公有 IP 的转换，可实现 VPC 内跨可用区的多个云主机共享弹性公网 IP，安全，高效的访问互联网。



DNAT 将外网 IP、端口映射到 VPC 内的云主机内网 IP、端口，使得云主机上的服务可被外网访问。



NAT 网关如何和 IPV4 网关配合规划用户网络

背景信息

VPC 创建时，部分资源池默认会创建 IPv4 网关来统一管理进出 VPC 的公网流量，所有通过公网 IP 访问公网的流量都受到 Ipv4 网关的管理。IPv4 网关和 VPC 同生命周期，不允许单独删除 IPv4 网关。

在 VPC 中创建 NAT 网关后，在子网关联的路由表中增加一条目的地址为 0.0.0.0/0 指向 NAT 网关的路由规则后（部分资源池(如华东 1，华北 2 等)需要执行该步骤，以控制台为准），VPC 中的云主机可以通过 NAT 网关的 SNAT 或 DNAT 规则访问公网或对外提供服务。

注意事项

系统类型的路由规则不允许修改、删除；所有系统类型的路由规则优先级低于客户手动创建的路由规则。

在同一个子网内云主机同时绑定公网 IP 和 SNAT 规则时，由于指向 NAT 网关的路由优先级高于指向 IPv4 网关的系统路由，默认会通过 SNAT 访问公网，云主机绑定的 EIP 无法访问公网。因此，不建议同一个子网内的云主机同时绑定公网 IP 或者 NAT 网关。

操作步骤

具体操作步骤参见弹性 IP-如何通过弹性公网 IP 或 NAT 网关访问公网。

如何访问 NAT 网关

天翼云提供如下方式进行 NAT 网关的配置和管理：

- 控制台：天翼云提供 Web 化的服务管理平台，即控制台 OpenAPI：天翼云提供基于 HTTPS 请求的 API（Application programming interface）管理方式。

产品优势

NAT 网关产品为您提供安全可靠的公网服务，本文带您了解 NAT 网关的产品优势。

灵活部署

支持跨子网和跨 AZ 提供服务。NAT 网关可为同一个 VPC 的多个 AZ 的多个子网提供服务。 NAT 网关的规格、带宽和公网 IP，均可以按需配置。

简单易用

多种网关规格可灵活选择。对 NAT 网关进行简单配置后，即可使用，运维简单，即开即用，运行稳定可靠。

降低成本

多个计算实例共享使用弹性 IP。当您的私有 IP 地址通过 NAT 网关发送流量时，该软件将私有地址转换为公共地址。用户无需为计算实例访问 Internet 购买多余的弹性 IP 和带宽资源，多个计算实例共享使用弹性 IP，有效降低成本。

高性能

NAT 网关基于 DPDK 优化转发面性能，绕过协议栈直接从网卡驱动获取数据报文，直接将数据报文发送给用户态应用程序，不触发后续中断流程，减少了中断和内存拷贝的消耗，从而提升数据报文处理速度。

高可用

NAT 网关主备集群模式，单网元故障集群内状态同步，秒级故障收敛,具备高可用性。

功能特性

本文带您了解 NAT 网关的功能特性。

使用 SNAT 主动访问 Internet

使用 NAT 网关的 SNAT 功能，构建 VPC 主动访问公网出口，使 VPC 内没有弹性 IP 的资源可以直接访问公网，实现云内主机共享使用弹性 IP 访问 Internet。

使用 DNAT 面向 Internet 提供服务

使用 NAT 网关的 DNAT 端口级转换功能，使云上资源可轻松面向 Internet 提供服务，同时节省大量弹性公网 IP，保护云上私网网络结构。

可视化运维

结合弹性 IP 和 NAT 网关监控，可对出入网流量进行可视化主动运维。及时发现网络瓶颈，保障业务永续服务，让运维更简单。

应用场景

NAT 网关产品广泛应用云上 VPC 公网统一出口和面向 Internet 提供公网服务场景，本文带您更快了解 NAT 网关经典应用场景。

云上网络入口，面向 Internet 提供服务

场景说明

当 VPC 内的云主机需要面向公网提供服务时，可以使用 NAT 网关的 DNAT 功能，使云上资源可轻松面向 Internet 提供服务，同时节省大量弹性公网 IP，保护云上私网网络结构。

推荐配置

DNAT 功能绑定弹性 IP，可通过端口映射方式，NAT 网关会将会把访问该弹性 IP 的请求转换成指定的 IP 和端口转发到目标云主机实例上。

一个云主机配置一条 DNAT 规则，如果有多个云主机需要为公网提供服务，可以通过配置多条 DNAT 规则来共享一个或多个弹性 IP 资源。实现多个云主机共享弹性 IP 和带宽，精确的控制带宽资源，节省公网带宽资源。

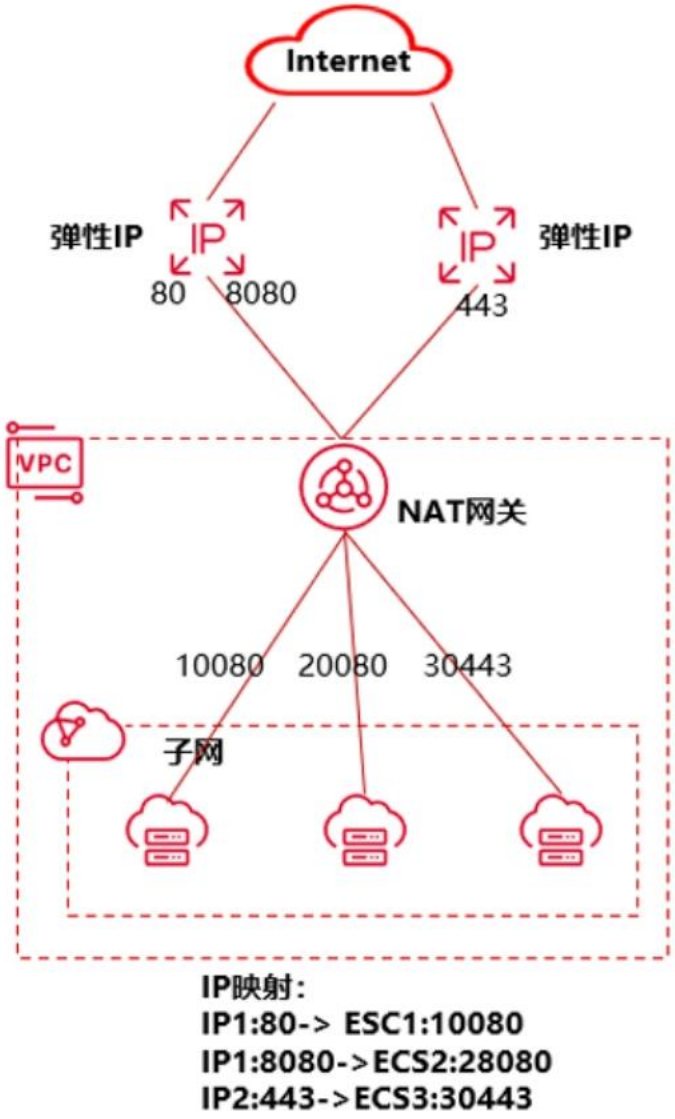
组网架构

使用 DNAT 为公网提供服务场景组网图如下图所示。图中示例的云主机类型均可以替换为弹性云主机、物理机的任何一个。例如：

弹性 IP1 的 80 端口，映射到云主机 ECS 1 的 10080 端口。

弹性 IP1 的 8080 端口，映射到云主机 ECS 2 的 20080 端口。

弹性 IP2 的 443 端口，映射到云主机 ECS 3 的 30443 端口。



构建 VPC 云上网络出口

场景说明

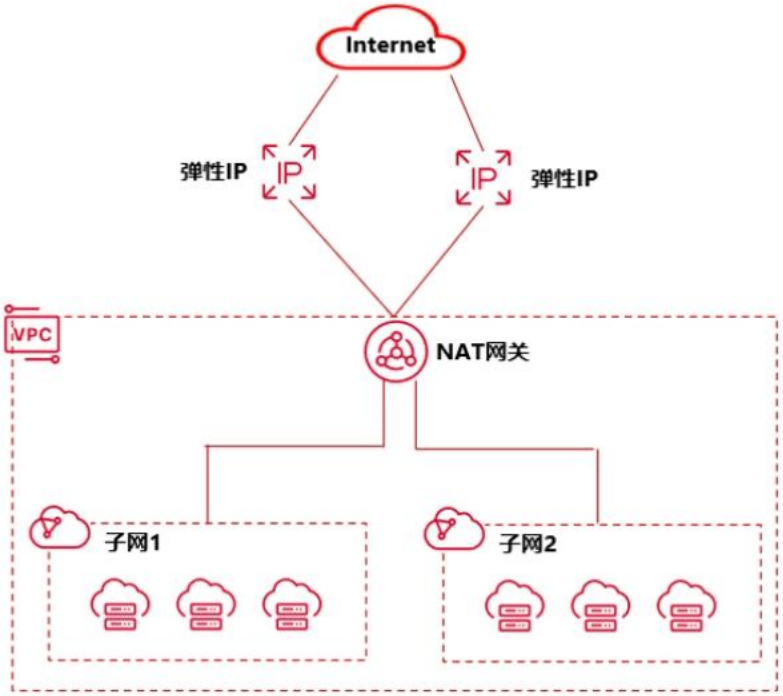
当 VPC 内的云主机需要主动访问 Internet，可以使用弹性 IP 绑定云主机实现。但是如果 VPC 内需要主动访问 Internet 的云主机过多时，为了节省弹性 IP 资源并且避免云主机 IP 直接暴露在公网上，可以使用 NAT 网关的 SNAT 功能，构建 VPC 主动访问公网出口。

推荐配置

VPC 中一个子网对应一条 SNAT 规则，一条 SNAT 规则配置一个弹性 IP。NAT 网关为您提供不同规格的连接数，根据业务规划，NAT 网关为您提供不同规格的连接数。您可以通过创建多条 SNAT 规则，来实现 VPC 内没有弹性 IP 的资源可以直接访问公网，多个云主机共享弹性公网 IP 资源访问 Internet。

组网架构

使用 SNAT 访问公网场景组网图如下图所示。



搭建高可用的 SNAT

场景说明

在 IT 系统中，往往存在绑定的弹性公网 IP 被攻击封堵的可能性。如果您想提高系统的高可靠性，可以在配置 SNAT 规则时，添加多个弹性公网 IP，当其中一个弹性公网 IP 被攻击封堵时，可以最大程度保障使用其他弹性公网 IP 的业务正常运行。

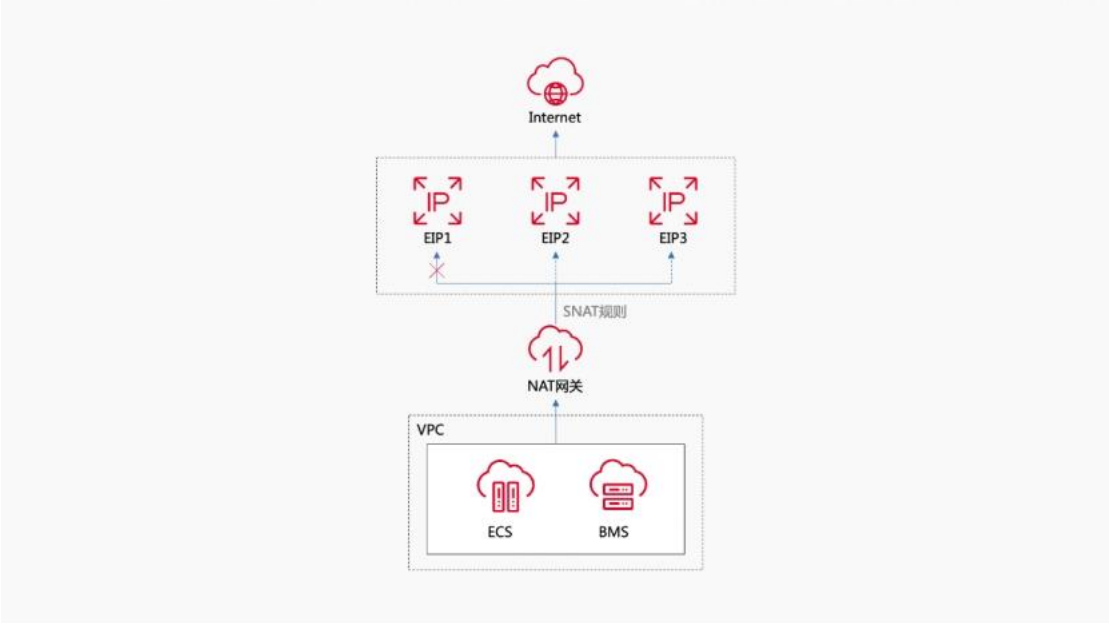
推荐配置

当 SNAT 规则上绑定了多个 EIP 时，系统会随机选择一个弹性公网 IP 访问公网。

部分资源池 SNAT 规则支持 EIP 地址池，每条 SNAT 规则支持添加 5 个弹性公网 IP，当 SNAT 规则中添加的弹性公网 IP 被攻击封堵或不可用时，需要手动从 EIP 池中删除。

组网架构

高可用 SNAT 的组网如图所示



多 NAT 网关实例

场景说明

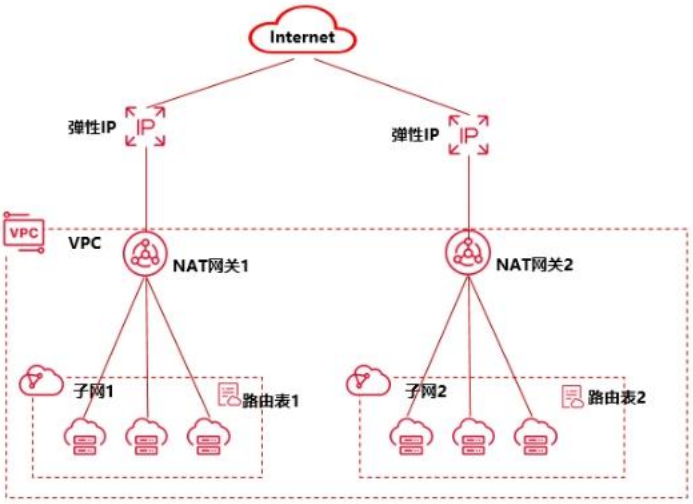
当单网关性能达到瓶颈，如 SNAT 支持最大 100 万连接，如果无法满足业务需求时，推荐使用多网关组成集群来横向扩展容量。

推荐配置

集群资源池支持多 NAT 实例组成集群，可横向扩充公网访问能力，需要一个 VPC 创建多个 NAT 网关，并使用自定义路由表和路由把流量分散到多个 NAT 网关，实现公网访问能力的横向扩容。

组网架构

NAT 网关集群组网如图所示



云间 NAT 网关高速访问互联网

场景说明

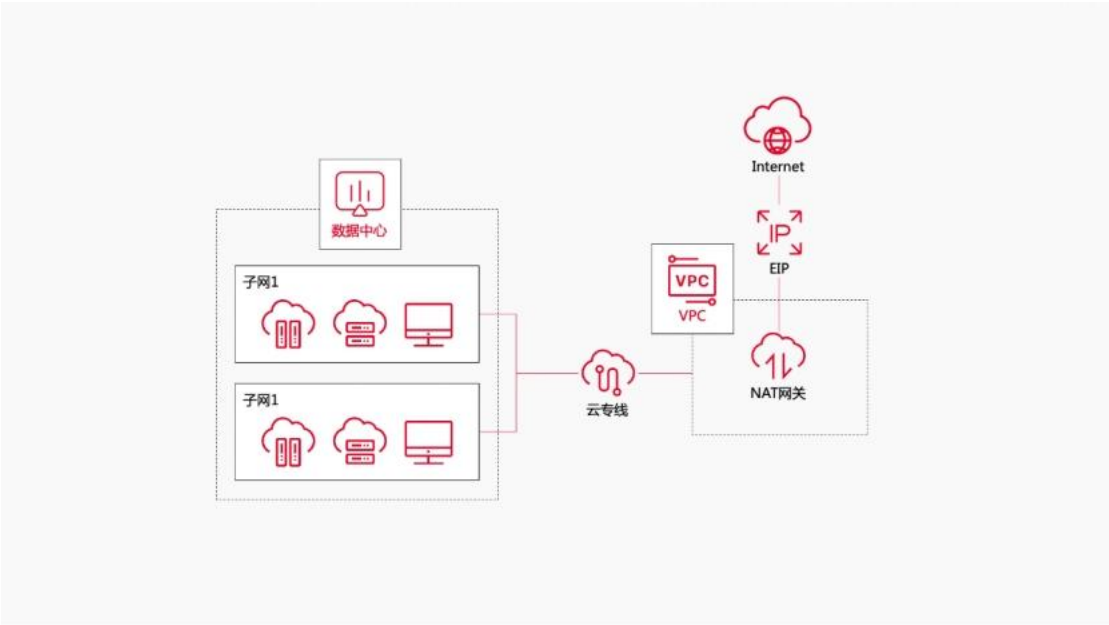
用户本地数据中心的服务器需要访问公网或为公网提供服务时，集群资源池 NAT 网关可为您提供高效、优质的网络服务。

推荐配置

可以通过开通云专线实现本地数据中心上云，然后购买公网 NAT 网关，通过配置 SNAT 规则实现访问公网。

组网架构

云间 NAT 网关高速访问互联网组网如图所示：



NAT 网关操作指导

本文介绍 NAT 网关的相关操作。

管理 NAT 网关

https://www.ctyun.cn/document/10026759/10166493

管理 SNAT 规则

https://www.ctyun.cn/document/10026759/10166496

管理 DNAT 规则

https://www.ctyun.cn/document/10026759/10166499

支持的监控指标

https://www.ctyun.cn/document/10026759/10166510

创建告警规则

https://www.ctyun.cn/document/10026759/10166504

查看监控指标

https://www.ctyun.cn/document/10026759/10166506

查看 NAT 网关后端实例对应的监控指标

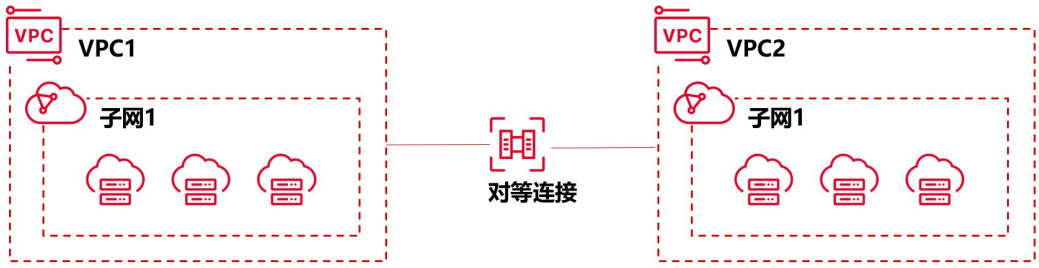
https://www.ctyun.cn/document/10026759/10166508

对等连接

对等连接是一个区域内两个 VPC 之间的网络连接，本文为您介绍对等连接产品的定义和相关操作。

产品简介

对等连接（VPC Peering Connection）是指两个同一区域内的 VPC 之间的网络连接。用户可以使用私有 IP 地址在两个 VPC 之间进行内网通信，就像两个 VPC 在同一个网络中一样。用户可以在自己帐号的 VPC 之间创建对等连接，也可以在自己账号的 VPC 与同一区域内其他帐号的 VPC 之间创建对等连接。



基本概念

虚拟私有云（VPC）

虚拟私有云为弹性云主机、物理机、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。

路由表

路由表是指虚拟私有云上管理路由条目的列表。

- 系统路由表 创建 VPC 后，系统会默认创建一张系统路由表来控制 VPC 的路由，VPC 内所有子网默认使用系统路由表。系统路由表不能创建也不能删除，但可以在系统路由表中创建自定义路由条目。
- 自定义路由表 支持创建 VPC 内自定义路由表，将自定义路由表和子网绑定，可更灵活地进行 VPC 网络管理。

对等连接

对等连接是两个 VPC 之间的网络连接，可以通过 VPC 对等连接，实现两个 VPC 之间私网互通。用户可以在自己帐号的 VPC 之间创建对等连接，也可以在自己账号的 VPC 与同一区域内其他帐号的 VPC 之间创建对等连接。

产品优势

对等连接产品为您提供灵活快捷的云上多 VPC 私网互联服务，本文带您了解对等连接的产品优势。

使用灵活，支持同账号、不同账号建连

支持在同一区域内的同一用户不同 VPC 之间、不同用户 VPC 之间以及公有云与专属云的 VPC 之间创建对等连接。

安全可控，自主授权

不同用户之间的 VPC 创建对等连接时，需要用户提供对端账户名和 VPC ID，且需要对端用户接受才可建立连接。

简单易用，配置灵活

天翼云提供 Web 管理平台，用户可登陆 Web 页面轻松实现连接创建、路由策略配置。

内网可达，无公网费用

使用对等连接的两个 VPC 通信时，通过资源池内部网络进行互通，不会绕行公网。

功能特性

本文带您了解对等连接的功能特性。

同账号对等连接

用户根据业务需求，在两个 VPC 之间创建对等连接。用户可以在自己账户内相同区域的两个 VPC 之间建立对等连接，也可以与其他账户内相同区域的 VPC 创建对等连接。

同账户内同区域的 VPC 之间创建对等连接，默认自动接受。

跨账号对等连接

跨账户同区域之间创建对等连接，需要对端账户同意,同意后建立对等连接。

对等连接管理

用户可通过天翼云控制台管理对等连接，支持查询、修改、删除操作。

路由管理

配置路由是两个 VPC 建立对等连接后互相通信的前提条件。同账号对等连接需在本账号下添加本端路由规则和对端路由规则，跨账号对等连接需分别在本账号下添加本端路由规则，在对端账号下添加对端路由规则。

产品应用场景

对等连接产品主要应用于云上同地域多 VPC 私网互连场景，本文带您更快了解对等连接经典应用场景。

灵活组建跨 VPC 网络、扩展资源

场景说明

同一区域内的不同业务部门资源需要互通时，可通过对等连接连通两个账号下的 VPC，实现同一区域内的云资源的内网访问。对等连接的建立过程需要双方互相确认，保障安全性。同时，伴随着业务的不断发展，当资源和网络架构已无法满足业务需求时，新业务下创建出的新 VPC 和云主机等资源，可以通过对等连接打通两个 VPC，轻松实现业务部署。

场景特点

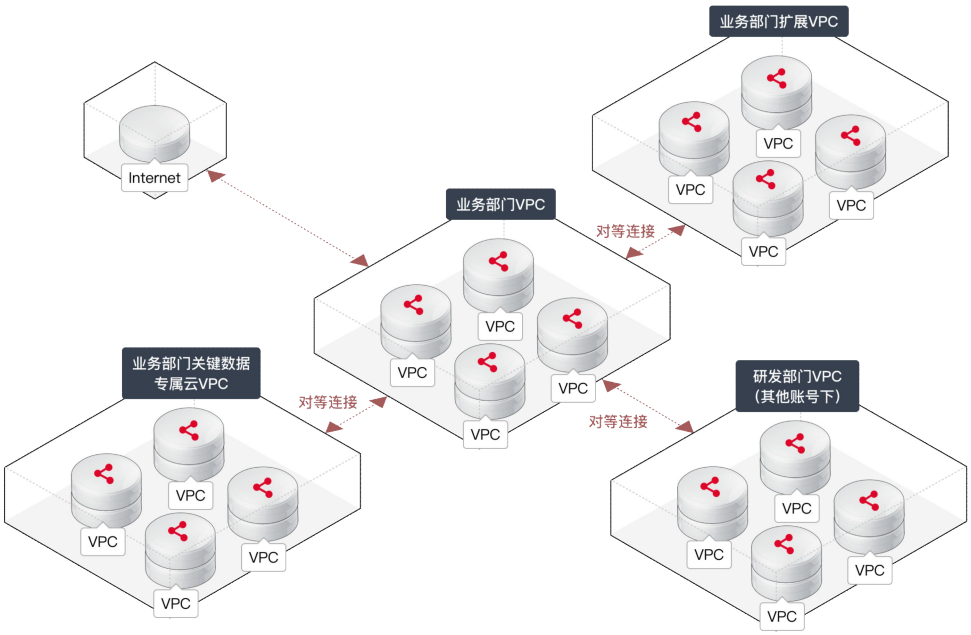
用户在使用不同账号进行资源订购及管理，默认情况下不同账号之间的资源无法通过内网访问。业务规模不断扩张，新建的 VPC 和计算资源需要和原有 VPC 实现互通访问。

产品优势

通过对等连接进行两个账号下的 VPC 的打通，从而实现云资源的内网访问。

打破不同 VPC 间相互隔离的业务现状，实现新老业务 VPC 的互通互联。

场景示意图如下：



构建安全可靠的混合云环境

场景说明

针对安全性要求较高的业务或核心业务，通过天翼云的专属云进行部署，而有互联网访问要求的业务，可以采用公有云进行部署。通过在专属云和公有云的 VPC 之间建立对等连接，从而实现两个 VPC 之间的内网互通。在保障安全性的情况下，最大限度降低企业成本投入。

场景特点

核心关键业务部署在专属云，有互联网访问需求的业务部署在共有云，业务上需要专属云和公有云进行互访。

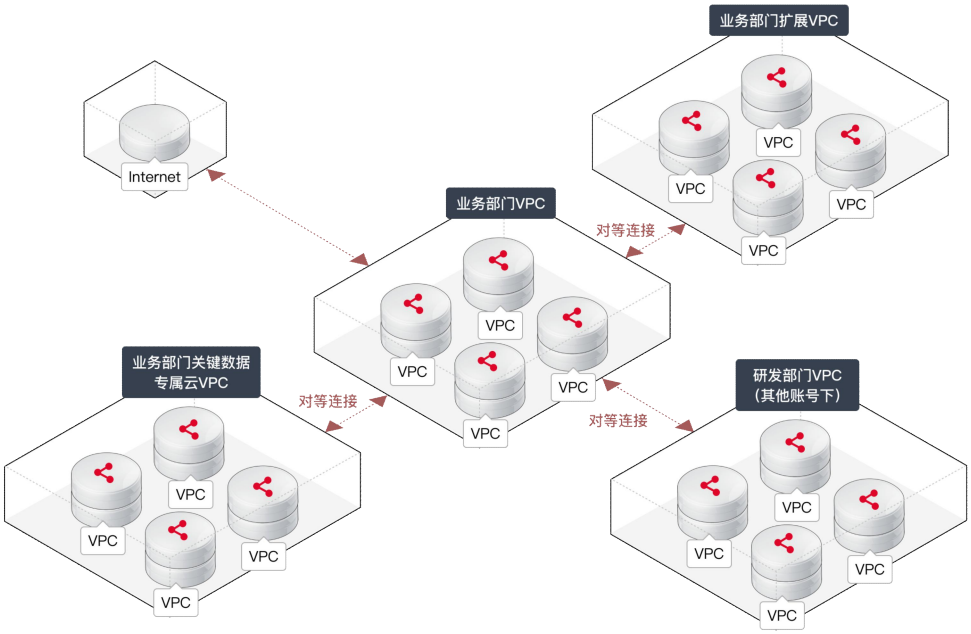
产品优势

通过对等连接打通专属云、公有云，实现不同形态云环境的互联互通。

配置简单、灵活，可以设置互访的网段，将有安全需求的业务，不提供对外访问。

通过对等连接实现两个 VPC 资源的内网互通，扩展了资源和网络架构。

场景示意图如下：



对等连接操作指导

本文介绍对等连接的相关操作。

创建对等连接

https://www.ctyun.cn/document/10026760/10037752

修改对等连接

https://www.ctyun.cn/document/10026760/10037753

删除对等连接

https://www.ctyun.cn/document/10026760/10037754

添加路由

https://www.ctyun.cn/document/10026760/10037755

删除路由

https://www.ctyun.cn/document/10026760/10037756

查看对等连接路由

https://www.ctyun.cn/document/10026760/10037757

IPv4 网关

IPv4 网关概述

本文将帮助您了解什么是 IPv4 网关，以及 IPv4 网关的使用限制、配额限制等内容。

什么是 IPv4 网关

IPv4 网关是连接虚拟私有云和公网的网络组件。虚拟私有云访问 IPv4 公网的流量经过 IPv4 网关，由 IPv4 网关实现路由转发以及私网地址到公网地址的转换，最终实现对公网的访问。

地域支持情况

天翼云部分资源池支持 IPv4 网关功能，实际情况以控制台展现为准。

使用限制

- VPC 创建后默认生成一个 IPv4 网关和指向 IPv4 网关的缺省路由规则。
- IPv4 网关当前仅支持 IPv4 流量。
- 一个 VPC 下只支持创建一个 IPv4 网关，且一个 IPv4 网关仅能关联一个 VPC。

- 一个 IPv4 网关仅能绑定一张网关路由表。
- VPC 删除时会连带删除 IPv4 网关。

配额限制

资源	默认限制	提升配额
单个 VPC 支持的 IPv4 网关个数	1 个	无法提升
单个 IPv4 网关支持的网关路由表个数	1 个	无法提升

IPv4 网关绑定路由表

本文将帮助您熟悉 IPv4 网关如何绑定路由表。

操作场景

创建 IPv4 网关后，云资源（云主机、物理机等）默认可以进行公网访问；如果您需要管理从公网进入 IPv4 网关的流量，需要关联网关型路由表进行流量规划。

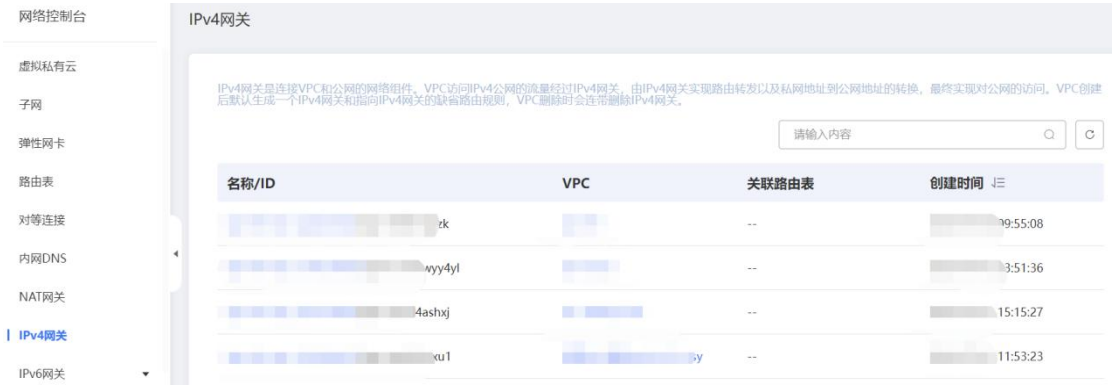
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 登录控制中心，并且已经完成虚拟私有云和 IPv4 网关的创建。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 进入“网络控制台”页面，点击“IPv4 网关”选项。



1. 找到需要绑定路由表的 IPv4 网关，点击该网关的名称，进入 IPv4 网关详情页。

2. 点击“绑定路由表”，在绑定路由表页面，选择网关类型的路由表。

3. 点击“确定”按钮，即可完成路由表的绑定。

VPC 终端节点

本文为您介绍 VPC 终端节点产品的定义和相关操作。

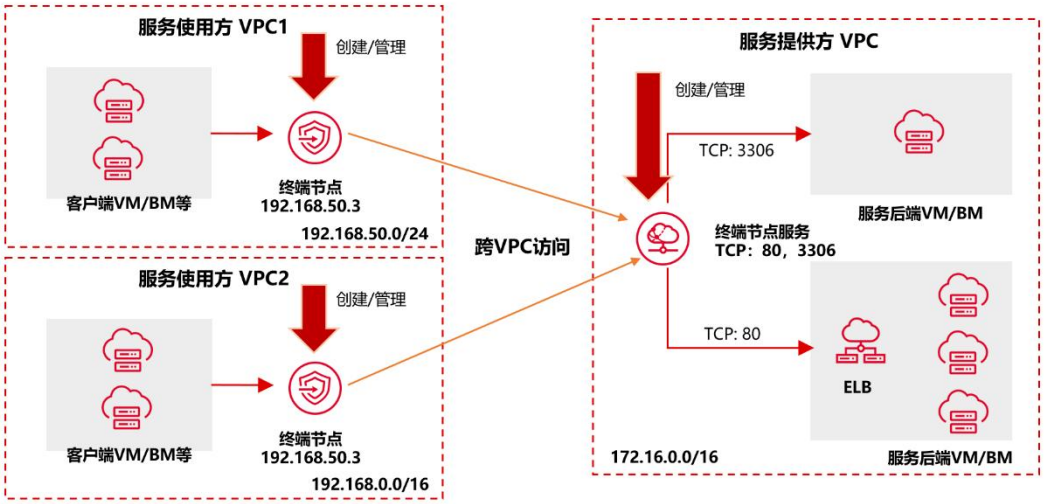
产品定义

本文为您介绍 VPC 终端节点产品的定义和产品架构。

VPC 终端节点（VPC Endpoint），能够将 VPC 私密地连接到终端节点服务（云服务、用户私有服务），使 VPC 中的云资源无需弹性 IP 就能够访问终端节点服务，提高了访问效率，为您提供更加灵活、安全的组网方式。

VPC 终端节点由“终端节点服务”和“终端节点”两种资源实例组成。

- 终端节点服务：指将云服务或用户私有服务配置为 VPC 终端节点支持的服务，可以被终端节点连接和访问。
- 终端节点：用于在 VPC 和终端节点服务之间建立便捷、安全、私密的连接通道。



基本概念

终端节点服务（Endpoint Service）

终端节点服务是可以被其他 VPC 通过创建终端节点建立私网连接的服务。终端节点服务由服务提供方创建和管理。

服务白名单（Service Whitelist）

服务白名单可以控制允许访问服务资源的用户范围。创建终端节点服务后，系统自动将服务所有者的天翼云账号 ID 添加到服务白名单中。服务白名单中的用户可以查询到该终端节点服务，也可以创建与该终

端节点服务连接的终端节点。如果希望其他账号下的 VPC 访问服务，需要将该天翼云账号 ID 添加到服务白名单中。

服务后端资源（ Service Resources ）

终端节点服务后端挂载的服务资源，实际部署开放的服务应用系统，可支持负载均衡，VIP，云主机和物理机等多种类型服务资源。

终端节点（Endpoint)

终端节点可以与终端节点服务相关联，以建立 VPC 通过私网访问外部服务的网络连接。终端节点由服务使用方创建和管理。根据终端节点连接的服务类型，可分为接口型和反向型。

终端节点访问控制（Endpoint Access Control List)

终端节点的访问控制能力，可以通过访问白名单方式，控制可通过终端节点访问服务的源主机信息。

产品优势

VPC 终端节点产品为您提供安全可靠的私网连接服务，本文带您了解 VPC 终端节点的产品优势。

性能优异

每个网关节点可提供百万级对话，满足多种应用场景需求。

即开即用

秒级创建，快速生效，迅速响应，方便用户即时使用。

使用灵活

无需弹性 IP，直连内网，使用更加灵活。

安全性高

用户能够通过终端节点私密地连接到终端节点服务，避免泄漏服务端相关信息所带来不可知的风险。

功能特性

本文带您了解 VPC 终端节点的功能特性。

VPC 终端节点为您提供“终端节点服务”和“终端节点”两种资源。

终端节点服务

终端节点服务（VPC Endpoint Service）指将云服务或用户私有服务配置为 VPC 终端节点支持的服务。终端节点服务通过专属网关，可以将 VPC 中的服务方便的提供给其它 VPC 中的资源使用，实现跨 VPC 的访问，而不必暴露服务端相关的网络信息，使您的访问更加安全、可靠。当前支持“接口”类型终端节点服务。

“接口”类型：包括系统配置的云服务、用户自己创建的私有服务和云服务商已创建的云服务。

用户可以通过终端节点服务快速的把服务发布到私网连接上，通过白名单授权管理可以灵活的管理可连接的用户信息，在保证安全的前提下灵活的通过私网共享服务

终端节点

终端节点（VPC Endpoint）在 VPC 和终端节点服务之间提供连接通道。您可以在 VPC 中创建自己的应用程序并将其配置为终端节点服务，同一区域下的其他 VPC 可以通过创建在自己 VPC 内的终端节点访问终端节点服务。

在同一区域中，通过购买终端节点可以实现所属 VPC 内云资源跨 VPC 访问终端节点服务。

终端节点与终端节点服务一一对应，访问不同类型终端节点服务的终端节点存在差异：

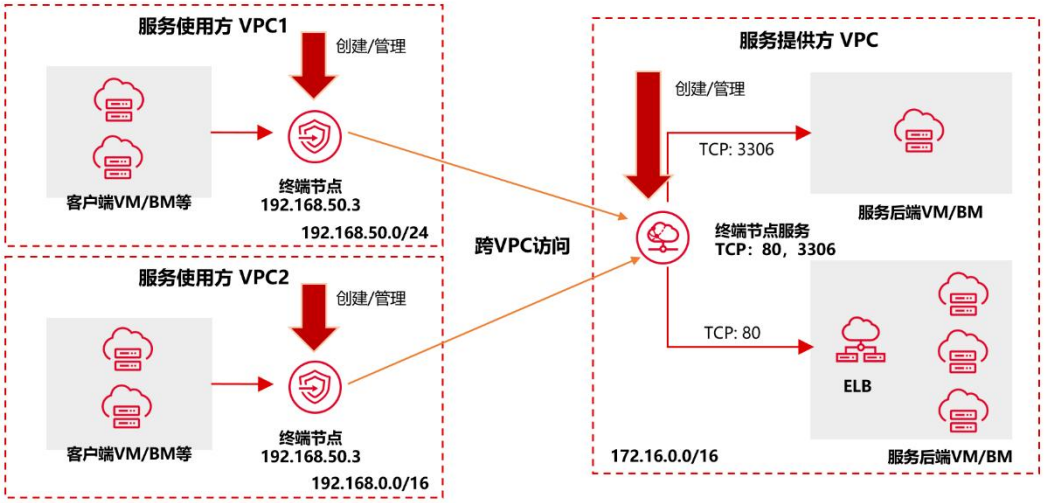
访问“接口”型终端节点服务的终端节点：是具备私有 IP 地址的弹性网络接口，作为“接口型”终端节点服务的通信入口。

产品应用场景

VPC 终端节点产品广泛应用于多种云上跨 VPC 的私网服务连接场景，本文带您更快了解 VPC 终端节点经典应用场景。

安全灵活的服务私网连接

通过 VPC 终端节点产品能够将 VPC 私密地连接到终端节点服务，用户无需做服务公网开放或配置复杂的路由打通私有网络，提高了访问效率，提供了更加灵活、安全的组网方式。



服务提供方

服务提供方在服务 VPC 内配置终端节点服务，服务后端资源可以是自己 VPC 内的云主机、负载均衡、裸金属、虚拟 IP。

当终端节点服务配置完成后，即可将己方后端资源对应的应用服务在云上进行共享。

针对不同账号间云服务共享场景，服务提供方可以配置白名单管控使用方的接入权限，安全可控。

服务使用方

其他 VPC 通过配置 VPC 终端节点与终端节点服务连接，用户访问对应终端节点的地址皆可访问对应的云服务 。

VPC 终端节点操作指导

本文介绍 VPC 终端节点的相关操作。

创建终端节点服务

https://www.ctyun.cn/document/10000119/10336783

查看终端节点服务

https://www.ctyun.cn/document/10000119/10336784

删除终端节点服务

https://www.ctyun.cn/document/10000119/10336785

连接管理

https://www.ctyun.cn/document/10000119/10336786

权限管理

https://www.ctyun.cn/document/10000119/10336788

端口映射

https://www.ctyun.cn/document/10000119/10336789

安全组

安全组概述

本文帮助您了解什么是安全组，安全组规则和一些安全组实践建议。

什么是安全组

安全组是一种网络安全防护机制，用于防止未经授权的访问和保护计算机网络免受恶意攻击。它是一种虚拟防火墙，用于限制入向和出向

网络流量。安全组工作在网络层和传输层，它通过检查数据包的源地址、目标地址、协议类型和端口号等信息来决定是否允许通过。安全组创建后，用户可以在安全组中定义各种访问规则，当弹性云主机加入该安全组后，即受到这些访问规则的保护。

不同资源池的安全组存在部分差异，如表 1 所示：

表 1 可用区资源池和地域资源池的差异

对比项	**多可用区资源池**	**地域资源池**
作用机制	“白名单”机制，即不匹配规则时，默认拒绝所有访问。	“白名单”机制，即不匹配规则时，默认拒绝所有访问。
创建安全组	需指定和 VPC 的关联关系	无需指定和 VPC 的关联关系
默认安全组	一个 VPC 一个默认安全组	一个资源池一个默认安全组
自定义模板安全组的默认规则	自定义模板类型的安全组不存在默认规则	每个自定义模板类型的安全组存在两条默认规则
默认安全组规则	存在默认安全组规则，具体规则以表 3 为准	存在默认安全组规则，具体规则以表 2 为准
安全组是否有状态	出/入方向均有状态	仅出向有状态

安全组模板	自定义、通用 Web 服务器、开放全部端口	自定义、通用 Web 服务器、开放全部端口

默认安全组：

- 对于地域资源池，系统会为每个用户默认创建一个安全组，多个 VPC 可以共用同一个安全组。默认安全组的默认规则可参考表 2“地域资源池默认安全组规则”。
- 对于可用区资源池，系统会为每个 VPC 默认创建一个安全组。一般来讲不同 VPC 之间是不同的业务，VPC 之间是相互隔离的，相同业务一般部署在一个 VPC。大多数情况下，不同的 VPC 由于业务的差异，所使用的安全组规则应该是不一样的。每个 VPC 自动建立一个默认安全组，可以满足用户不同业务需要不同安全组的场景。默认安全组的默认规则可参考表 3“可用区资源池默认安全组规则”。

安全组状态：

- 对于地域资源池来说，安全组出向是有状态的。如果您从实例发送一个出站请求，且该安全组的出站规则是放通的话，那么无论其入站规则如何，都将允许该出站请求的响应流量流入。
- 对于可用区资源池来说，安全组出/入方向均有状态的。如果您从实例发送一个出站请求，且该安全组的出站规则是放通的话，那么无论其入站规则如何，都将允许该出站请求的响应流量流入。

同理，如果该安全组的入站规则是放通的，那无论出站规则如何，都将允许入站请求的响应流量可以出站。

自定义安全组：

- 对于地域资源池来说，用户创建安全组时，模板类型为自定义的安全组会存在两条默认规则，即出向默认放通所有 IP 地址（0.0.0.0/0、::/0）流量的数据报文通过。
- 对于可用区资源池来说，用户创建安全组时，模板类型为自定义的安全组不存在默认规则，如未添加规则，则默认安全组出、入方向将均拒绝所有访问。

不同资源池列表见产品简介-资源池区别页面，实际情况以控制台展现为准。

安全组规则

为了更好地管理安全组的入出方向，您可以设置安全组规则，去控制云服务器的出入向流量。通过配置适当的规则，控制和保护加入安全组的弹性云服务器的访问。

- 安全组规则可分为入向规则和出向规则。入向规则用于控制流入服务器实例的流量，出向规则用于控制从服务器实例流出的流量。默认安全组会自带一些默认规则，您也可以自定义添加安全组规则。
- 安全组规则主要遵循白名单机制，具体说明如下：

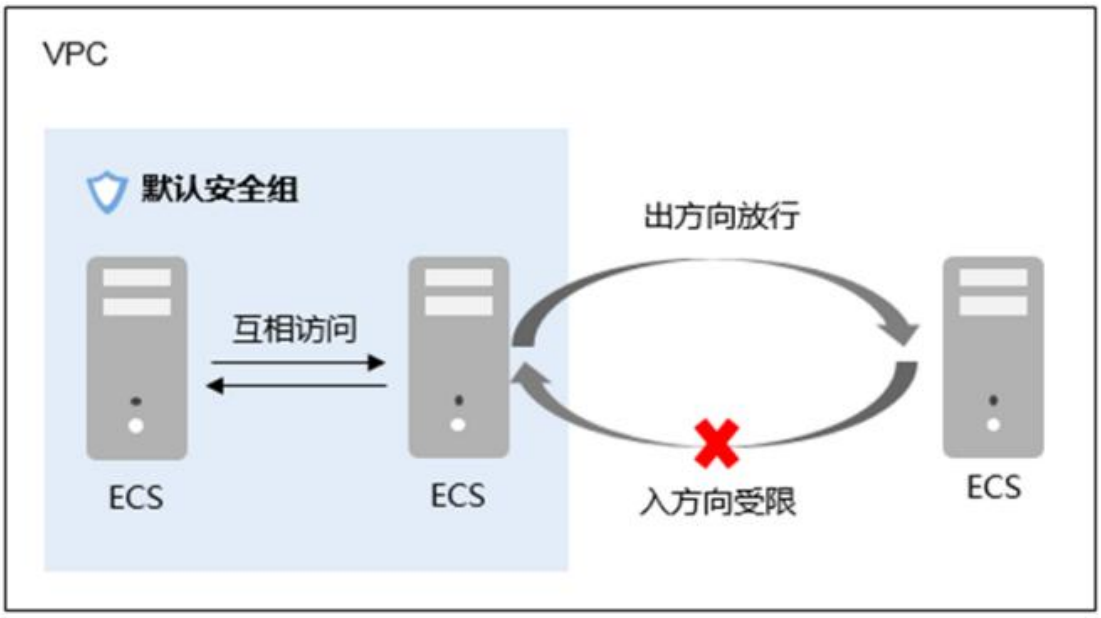
入方向规则：入方向指外部访问安全组内的云服务器的指定端口。当外部请求匹配上安全组中入方向规则的源地址，并且授权策略为“允

许”时，允许该请求进入，其他请求一律拦截。通常情况下，您一般不用在入方向配置授权策略为“拒绝”的规则，因为不匹配“允许”规则的请求均会被拦截。

出方向规则：出方向指安全组内的云服务器访问外部的指定端口。在出方向中放通全部协议和端口，配置全零 IP 地址，并且策略为“允许”时，允许所有的内部请求出去。0.0.0.0/0 表示所有 IPv4 地址，::/0 表示所有 IPv6 地址。

地域资源池：

对于地域资源池来说，系统会为每个用户默认创建一个安全组，默认安全组包含一系列默认规则，主要是在出方向上的数据报文全部放行，入方向访问受限，安全组内的云服务器无需添加规则即可互相访问。



默认安全组规则如下表 2：

表 2 地域资源池默认安全组规则

方向	授权	类型	协议	端口范	目的地址/源地址	说明

	策略			围		
出方向	允许	IPv4	Any	Any	0.0.0.0/0	允许所有 IPv4 类型的出站流量的数据报文通过。
出方向	允许	IPv6	Any	Any	::/0	允许所有 IPv6 类型的出站流量的数据报文通过。
入方向	允许	IPv4	Any	Any	默认安全组 ID (例如：sg-xxxxx)	仅允许安全组内的云服务器彼此通信，丢弃其他入站流量的全部数据报文。
入方向	允许	IPv6	Any	Any	默认安全组 ID (例如：sg-xxxxx)	仅允许安全组内的云服务器彼此通信，丢弃其他入站流量的全部数据报文。
入方向	允许	IPv4	TCP	22	0.0.0.0/0	允许所有 IP 地址通过 SSH 远程连接到 Linux 云服务器。
入方向	允许	IPv4	TCP	3389	0.0.0.0/0	允许所有 IP 地址通过 RDP 远程连接到 Windows 云服务器。
入方向	允许	IPv4	ICMP	Any	0.0.0.0/0	使用 ping 程序测试云服务器之间的通讯状况。

可用区资源池：

对于可用区资源池来说，系统会为每个 VPC 默认创建一个安全组，默认安全组包含一系列默认规则，主要是在出方向上的数据报文全部放行，入方向访问受限。

默认安全组规则如下表 3：

表 3 可用区资源池默认安全组规则

方向	授权策略	类型	优先级	协议	端口范围	目的地址/源地址	说明
出方向	允许	IPv4	100	Any	Any	0.0.0.0/0	允许所有 IPv4 类型的出站流量的数据报文通过。
出方向	允许	IPv6	100	Any	Any	::/0	允许所有 IPv6 类型的出站流量的数据报文通过。
入方向	允许	IPv4	99	ICMP	Any	0.0.0.0/0	使用 ping 程序测试云服务器之间的 IPv4 地址通讯状况
入方向	允许	IPv6	99	ICMP	Any	::/0	使用 ping 程序测试云服务器之间的 IPv6 地址通讯状况
入方向	允许	IPv4	99	TCP	22	0.0.0.0/0	允许所有 IPv4 地址通过 SSH 远程连接到 Linux 云服务器。
入方向	允许	IPv6	99	TCP	22	::/0	允许所有 IPv6 地址通过

							SSH 远程连接到 Linux 云服务器。
入方向	允许	IPv4	99	TCP	3389	0.0.0.0/0	允许所有 IPv4 地址通过 RDP 远程连接到 Windows 云服务器。
入方向	允许	IPv6	99	TCP	3389	::/0	允许所有 IPv6 地址通过 RDP 远程连接到 Windows 云服务
入方向	拒绝	IPv4	100	Any	Any	0.0.0.0/0	禁止所有 IPv4 类型的入站流量的数据报文通过。
入方向	拒绝	IPv6	100	Any	Any	::/0	禁止所有 IPv6 类型的入站流量的数据报文通过。

实践建议

以下是一些关于安全组的建议和实践经验，帮助确保您的云环境的安全性，您可根据具体需求和环境来制定适合的安全组策略：

- 原则上，安全组规则取最小权限原则，通过设置所需的端口和协议，限制对必要 IP 地址的访问。只允许最少必要的流量进出您的资源实例。
- 定期更新安全组规则，以适应您的业务需求的变化。不再需要的规则应被删除，根据业务变化添加新的安全组规则。

- 根据资源的安全需求，将资源实例划分为不同的安全组。通过多层级的安全组可以实现细粒度的安全控制，确保安全性与灵活性之间的平衡。
- 通过有规范的命名等方式有意识地规划和管理安全组规则，易于查找。
- 安全组应与其他安全措施如网络 ACL、防火墙等结合使用，以提供更全面的安全保护。
- 建议您不要直接修改线上环境使用的安全组，修改后的安全组会自动应用在 VPC 内的所有云服务器上，因此您可以先克隆一个安全组，在测试环境中进行调试，确保修改后云服务器之间的通讯正常，再将修改后的安全组同步到线上环境。

创建安全组

本文帮助您快速熟悉创建安全组的操作场景和操作流程。

操作场景

您可以创建安全组并定义安全组中的规则，将 VPC 中的弹性云主机划分成不同的安全域，以提升弹性云主机访问的安全性。建议您将不同公网访问策略的弹性云主机划分到不同的安全组。

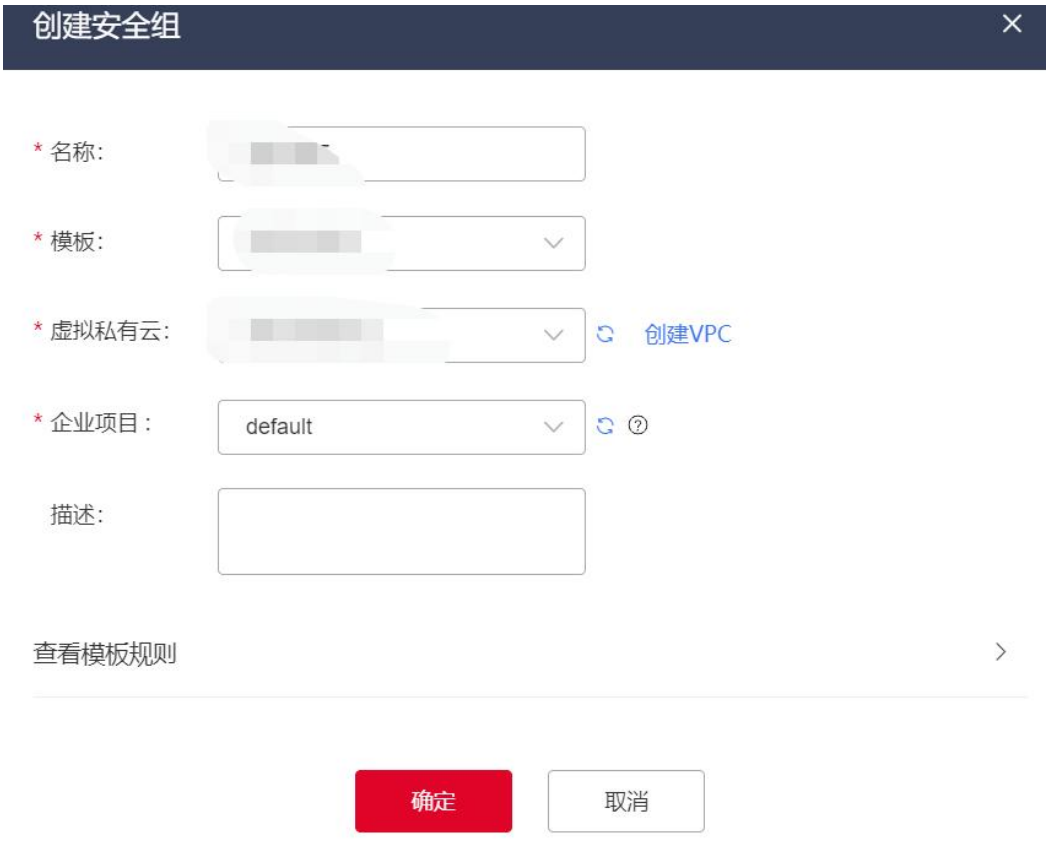
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。

5. 点击页面右上角“创建安全组”按钮，进入创建安全组页面。



6. 根据界面提示配置参数，设置安全组信息；参数说明如下：

配置	说明
名称	输入安全组的名称。
模板	模板自带安全组规则，方便您快速创建安全组。提供如下几种模板： • 自定义：用户自定义安全组规则。 • 通用 Web 服务器：默认放通 22、3389、80、443 端口和 ICMP 协议。 • 开放全部端口：开放全部端口有一定安全风险，请谨慎选择。
虚拟私有云	选择安全组所属的虚拟私有云，仅可用区资源池支持此选项。
描述	安全组的描述信息。
企业项目	创建安全组时，可以将安全组加入已启用的企业项目。

7. 点击“确认”按钮，即可完成安全组的创建。

x

注意事项：默认情况下，控制台已经为您提供了几种安全组规则模板，您可以跟据您的业务需求去选择规则模板，如果您需要自定义规则，可以参考“添加安全组规则”，添加规则时需要注意出入方向的差异。

添加安全组规则

本文帮助您快速熟悉添加安全组规则的操作场景和操作流程。

操作场景

安全组创建成功后，当您的云服务器需要与外部网络通讯时，您可根据业务需求自定义添加新的出方向、入方向安全组规则，这可以帮助保护服务器免受未经授权的访问。

入方向：指从外部访问安全组规则下的弹性云主机。

出方向：指安全组规则下的弹性云主机访问安全组外的实例。

安全组规则有数量限制，您应尽量保持规则的精简。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成安全组的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击  ，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，找到您需要添加规则的安全组名称，点击安全组名称，进入安全组详情页。

6. 点击“添加规则”，根据界面提示配置安全组规则，确定授权策略、优先级、协议类型、端口范围、源/目的地址等信息。

具体参数配置信息如下表：

参数	说明	取值样例
IP 版本	IPv4、IPv6	IPv4
授权策略	允许、拒绝	允许
优先级	安全组规则优先级可选范围为 1-100，默认值为 1，即最高优先级。优先级数字越小，	1

	级别越高。	
协议	网络协议，取值范围为：TCP，UDP，ICMP，All。	TCP
端口范围	安全组规则的端口范围，取值范围为：1～65535。	22 或 22-30
源地址/目的地址	源地址/目的地址：支持 IP 地址，地址格式：xxx.xxx.xxx.xxx/32（IPv4 地址）0.0.0.0/0（任意地址）； 支持安全组，表示源地址/目的地址为另外一个安全组。您可以选择当前帐号下，同一个区域内的其他安全组。当安全组 A 内有实例 a，安全组 B 内有实例 b，在安全组 A 设置入方向规则时，“策略”为允许，源地址选择安全组 B，则表示来自实例 b 的内网访问请求被允许进入实例 a。部分资源池源地址下拉框可选择安全组，实际情况以控制台展现为准。	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。	

7. 点击“确认”按钮。

操作指引

- 关于使用安全组时的一些常见类问题，可参考常见问题“安全类”。
- 关于配置安全组规则放通弹性云主机对应的常见端口，可参考文档“云主机的常用端口”。

Xx

快速添加多条安全组规则

本文帮助您快速熟悉快速添加多条安全组规则的操作场景和操作流程。

操作场景

安全组支持快速添加多条不同协议端口的安全组规则，可以用于 ping 云服务器之间的通讯情况、远程连接实例等场景，方便您快速创建多条具备相同授权对象、授权策略等信息的规则。

前提条件

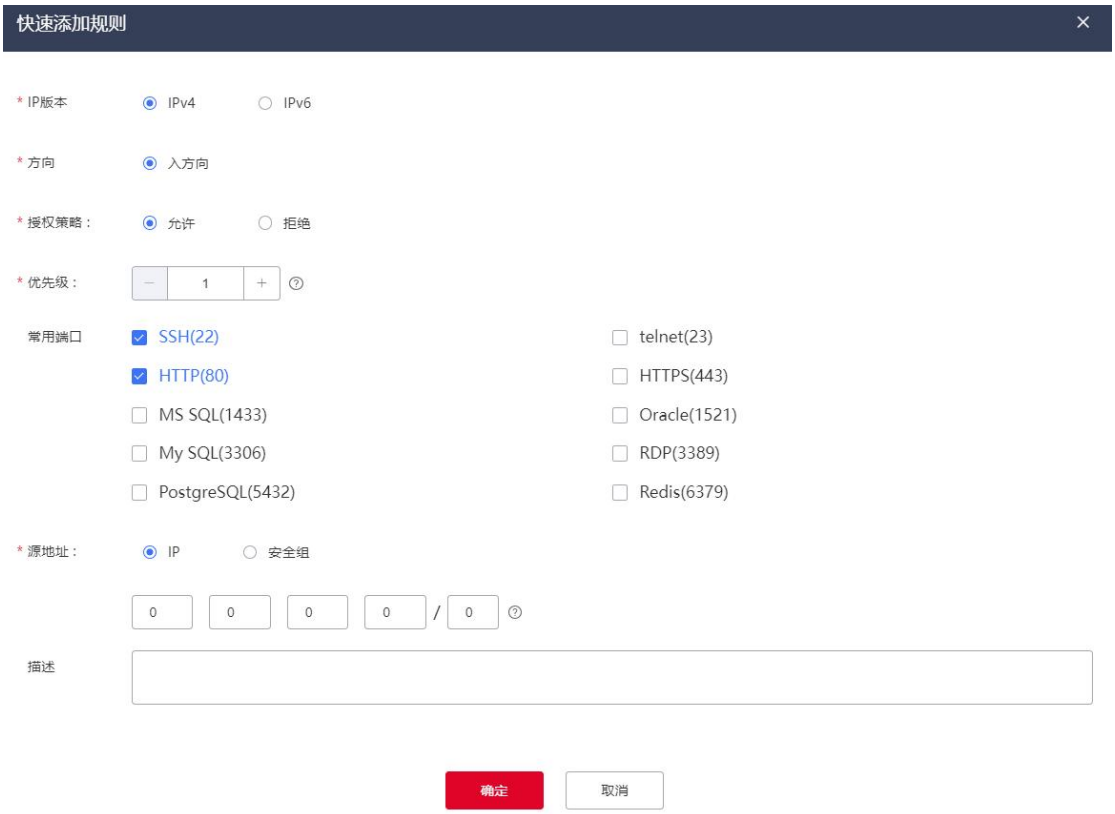
- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成安全组的创建。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，找到您需要添加规则的安全组名称，点击安全组名称，进入安全组详情页。

6. 在安全组详情页，点击“快速添加规则”，根据页面提示配置规则。



7. 点击“确定”按钮。

Xx

参数说明如下：

参数	说明	取值样例
IP 版本	IPv4、IPv6	IPv4
授权策略	允许、拒绝	允许
优先级	安全组规则优先级可选范围为 1-100，默认值为 1，即最高优先级。优先级数字越小，级别越高。	1
常用协议端口	提供一些常用的协议端口支持快速选择。	SSH (22)

源地址/目的地址	源地址/目的地址：支持 IP 地址，地址格式：xxx.xxx.xxx.xxx/32（IPv4 地址）0.0.0.0/0（任意地址），部分资源池源地址/目的地址支持安全组（可提工单申请）	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。	

复制安全组规则

本文帮助您快速熟悉复制安全组规则的操作场景和操作流程。

操作场景

复制功能支持利用已有的安全组规则，快速生成一个新的安全组规则。

复制时，您可以根据业务需求自定义修改目标规则。

前提条件

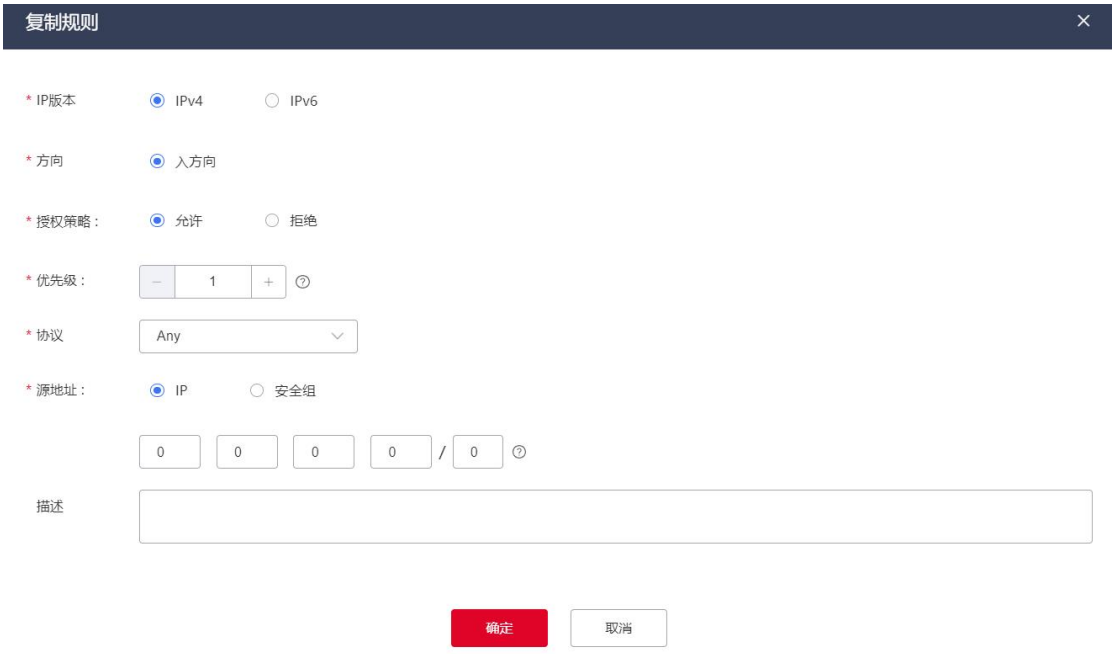
- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成安全组、安全组规则的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。

5. 在安全组列表页面，选择需要复制规则的安全组，单击安全组名称进入详情页，进入安全组详情页。
6. 在“安全组”详情界面，选择安全组规则所属方向，找到需要复制的安全组规则所在行。

7. 点击操作列的“复制”，进入复制安全组规则页面。



8. 根据业务需求修改目标安全组规则的相应参数。
9. 单击“确定”按钮，即可快速创建出安全组规则。关于安全组规则中参数的设置方法，请参考添加安全组规则。

修改安全组规则

本文帮助您快速熟悉修改安全组规则的操作场景和操作流程。

操作场景

当安全组规则创建成功后，针对不满足当前业务需求的访问控制规则，您可以选择修改规则操作，保障云服务器的安全及正常业务运行。

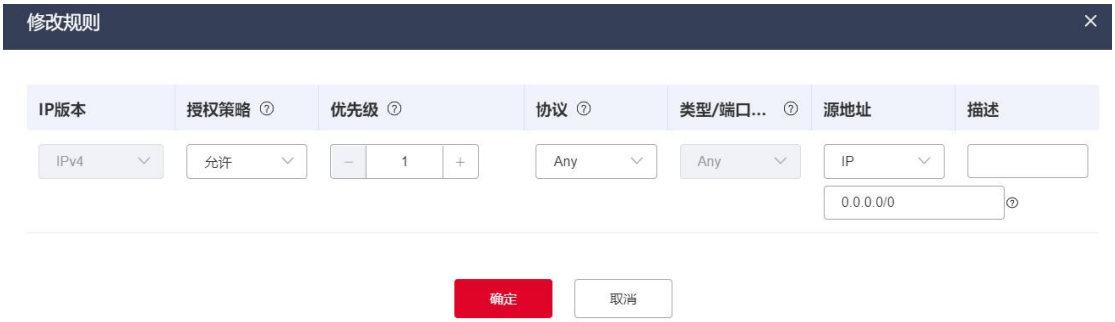
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成安全组、安全组规则的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要复制规则的安全组，单击安全组名称进入详情页，进入安全组详情页。
6. 在“安全组”详情界面，选择安全组规则所属方向，找到需要修改的安全组规则所在行。

7. 单击操作列的“修改”，根据页面提示信息进行修改。安全组规则参数的详细介绍，请参见添加安全组规则页面。



8. 点击“确定”按钮。修改完成后，安全组中的云服务器将根据修改后的规则进行行业务流量控制。

导入/导出安全组规则

本文帮助您快速熟悉导入/导出安全组规则的操作场景和操作流程。

操作场景

- 如果您根据业务场景需要在其他安全组中共用相同的安全组规则，可以利用安全组导入/导出功能将某个安全组的规则快速应用到另外一个安全组。
- 如果您想在本地备份一个安全组规则，可以利用安全组规则导出功能将待备份规则导出为本地文件。

约束与限制

- 导入安全组规则时，务必仔细检查规则的格式和内容，只能基于模板已有字段进行内容修改，不能新增字段和修改字段名称，否则会导入失败。
- 导入安全组规则时，若源地址/目的地址类型为安全组时，需确保安全组已存在且名称与 ID 正确，格式示例：格式为名称[id]，例如 sg-faae[b479ddae-618a-4e0a-bf14-cc66fca1355d]。（部分资源池可导入地址类型为安全组，实际情况以控制台展现为准）。
- 导入的规则应不超过 100 条，超过数量不允许导入。当存在重复安全组规则时，无法导入。
- 对于上传文件类型，选择本地的 CSV 格式。
- 在导入规则之前，建议先备份当前安全组的规则，以防止意外覆盖或错误的添加规则。
- 导入规则时，确保目标安全组已经存在，否则导入操作可能会失败。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成安全组、安全组规则的创建。

操作步骤

导入规则

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要导入安全组规则的安全组，单击安全组名称进入详情页，进入安全组详情页。
6. 在安全组详情界面，单击“导入规则”按钮，选择需要导入的文件；

7. 在导入规则界面，您可以选择“下载模板”，提前在模板中填好需要导入的安全组规则。模板中需要填写的规则字段，具体可以参考添加安全组规则页面。

8. 在弹窗中将会自动生成预览规则，如果存在导入失败的规则，您可以在预检查列查看失败原因。单击“确定”按钮，可以将文件中安全组规则导入安全组中。

导出规则

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要导出安全组规则的安全组，单击安全组名称进入详情页，进入安全组详情页。
6. 在安全组详情界面，单击“导出规则”按钮。
7. 单击“确定”按钮，可以将当前安全组规则导出成文件。

实例加入/移出安全组

本文帮助您快速熟悉实例加入/移出安全组规则的操作场景和操作流程。

操作场景

安全组是一种重要的网络安全防护策略，用于管理和控制虚拟机实例或云服务实例的网络访问。当您创建好安全组后，可以将云服务器加入到该安全组，使这些实例受到安全组的保护。您可以根据业务需求随时将安全组加入/移出云服务器中。

在安全组界面管理云服务器时，主要包含以下操作：

- 加入安全组 ：将云服务器加入到指定的安全组中，原先已加入云服务器中的安全组仍正常生效。
- 移出安全组 ：将云服务器从指定的安全组中移出，解除部分安全组与云服务器的绑定关系。

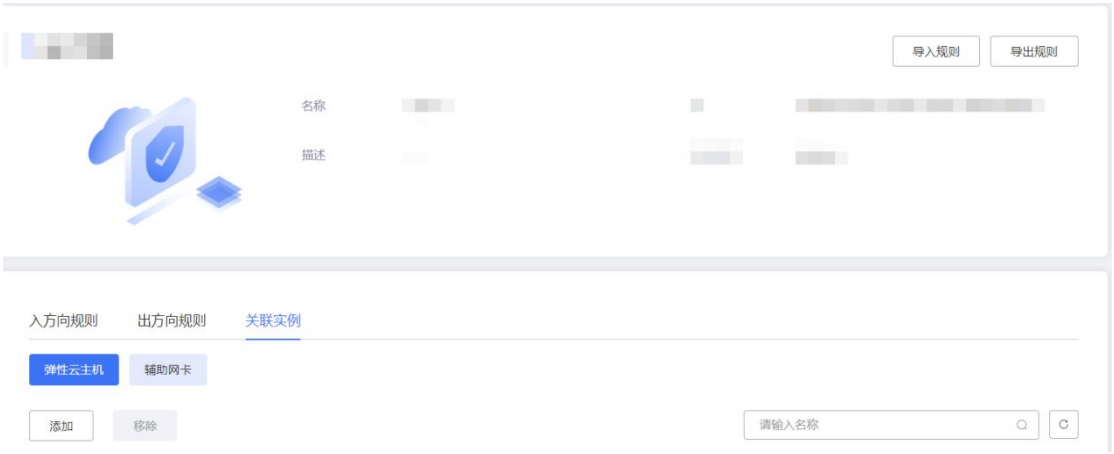
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成弹性云主机、安全组的创建。

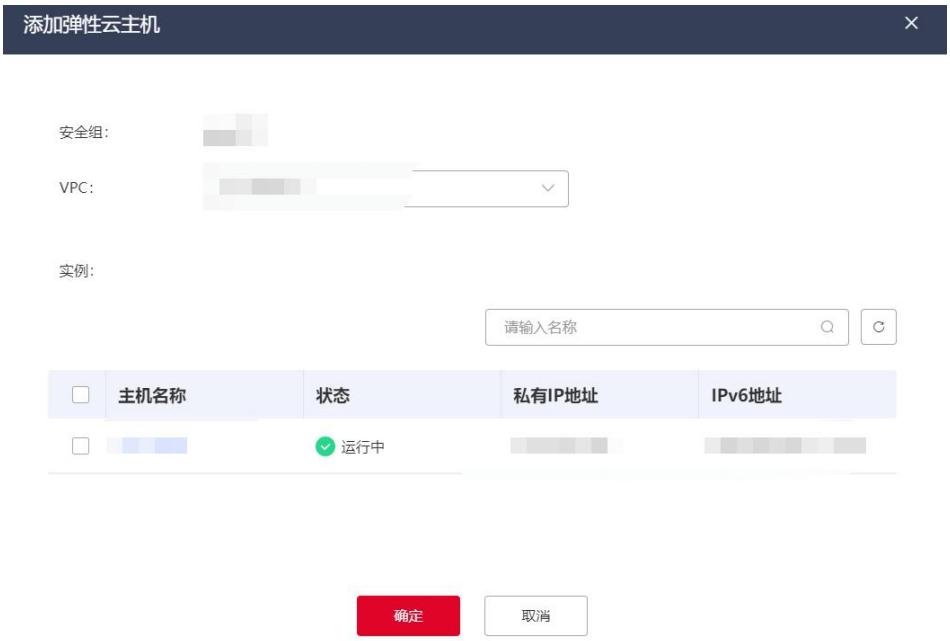
操作步骤

加入安全组

1. 登录控制中心。
2. 在控制中心页面左上角点击  ，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要操作的安全组，单击安全组名称进入详情页；
6. 在安全组详情界面，选择安全组规则所属方向，单击“关联实例”，您可以根据需要添加相应的云资源；



7. 在“弹性云主机”页签，单击“添加”，将一个或多个服务器加入到当前安全组中；



8. 在“辅助网卡”页签，单击“添加”，将一个或多个扩展网卡加入到当前安全组中；
9. 单击“确定”，即可调整云服务器与安全组之间的关联关系。
10. 加入完成后，该安全组中的规则将对新关联的云服务器生效。

移出安全组

说明

- 被移出的实例和安全组内其他实例间的网络不再互通，建议您在操作前充分测试，确保移出实例后业务可以正常运行。
- 为了更好的网络性能，建议单个实例关联的安全组不多于 5 个。
- 每个实例需要保证至少加入一个安全组。

步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要操作的安全组，单击安全组名称进入详情页。
6. 在安全组详情界面，选择安全组规则所属方向，单击“关联实例”，您可以根据需要移出相应的云资源。
7. 在“弹性云主机”页签，单击“移除”，将一个或多个服务器移出当前安全组中；
8. 在“辅助网卡”页签，单击“移除”，将一个或多个扩展网卡移出当前安全组中；
9. 单击“确定”，即可调整云服务器与安全组之间的关联关系。
10. 移出完成后，该安全组中的规则将不再对云服务器生效。

支持批量添加、移除操作：

- 同时勾选多个云服务器，单击列表上方的“移出”/“添加”，将多个服务器从当前安全组中全部移出/添加。
- 同时勾选多个辅助网卡，单击列表上方的“移出”/“添加”，将多个扩展网卡从当前安全组中全部移出/添加。

操作指引

- 更多安全组管理云服务器和辅助网卡的详细信息可参考“安全组与云服务器的关联管理”及“安全组与辅助网卡的关联管理”。
- 如果您的业务不再需要部分安全组或安全组规则，您可以删除安全组安全组规则，详情请参见“删除安全组”或“删除安全组规则”。
- 如果已有安全组已经不能满足您的业务需求，您可以自定义新的安全组，详情请参见“创建安全组”。

删除安全组规则

本文帮助您快速熟悉删除安全组规则的操作场景和操作流程。

操作场景

当您不再需要某些安全组规则去控制云主机之间的访问控制，您可以删除掉相应的安全组规则并创建新的规则。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成安全组、安全组规则的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要操作的安全组，单击安全组名称进入详情页。
6. 在安全组详情界面，选择安全组规则所属方向，找到需要删除的安全组规则所在行，单击操作列的“删除”；

7. 确认需要删除的安全组规则后，单击“确定”按钮。

   注：安全组规则批量删除功能正在内测中，实际支持资源池以控制台为准，可提工单申请开通。

删除安全组

本文帮助您快速熟悉删除安全组的操作场景和操作流程。

操作场景

当您的业务不需要部分安全组去控制云服务器网络流量时，您可以删除安全组，删除后，安全组及其规则将不再对云服务器生效。

约束与限制

- 系统会为每个用户默认创建一定的安全组，默认安全组不支持删除。
- 当安全组正和其他云服务器存在绑定关系时，例如弹性云主机、物理机服务、弹性网卡等，安全组将无法删除。您需要先将安全组与绑定的服务器解除关联，之后再重新执行删除操作。
- 当安全组被其他安全组引用为“源地址”或者“目的地址”时，安全组将无法删除。您需要先解除待删除安全组与引用安全组之间的关系，之后再重新执行删除操作。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成安全组的创建。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要删除的安全组。
6. 在待删除的安全组所在行操作列，单击“更多->删除”。

7. 确认删除的安全组信息，单击“确定”按钮。

克隆安全组

安全组支持快速克隆，方便将相同的安全组规则快速应用到不同区域的服务器上。本文帮助您快速熟悉克隆安全组的操作场景和操作流程。

操作场景

安全组支持跨区域克隆，您可以利用该功能备份安全组或安全组规则快速应用到不同区域的云资源上。

当您有如下需求时，可以利用克隆安全组的功能去实现：

- 您在区域 1 存在一个安全组 sgs1，此时区域 2 中的云资源（云主机、物理机等）需要配置与区域 1 中的安全组 sgs1 完全相同的

规则，您可以直接将安全组 sgs1 利用克隆功能快速创建相同的安全组到区域 2，而不需要在区域 2 中创建新的安全组。

- 如果您需要对云资源更换安全组规则，可以对原安全组做克隆操作，快速创建相同的新安全组作为备份资源。

约束与限制

克隆安全组时，只将原安全组出入方向规则克隆，云主机需另行关联。仅支持克隆源/目的地址是 IP 地址网段、本安全组的规则，如存在引用其他安全组的规则时，不支持克隆这条规则，实际情况以控制台展现为准。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成安全组的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要克隆的安全组。
6. 在待克隆的安全组所在行操作列，单击“更多->克隆”。

7. 在“克隆”弹窗中，根据界面提示配置参数，选取配置地域，修改名称；
8. 单击“确定”按钮，安全组克隆成功，可在目标区域查看克隆成功的安全组。

安全组与云服务器的关联管理

本文帮助您快速熟悉安全组与云服务器的关联管理。

操作场景

安全组是一种虚拟防火墙，为云服务器提供安全防控。根据您的业务需求，您可以自定义安全组与云服务器之间的关系，随时调整。

前提条件

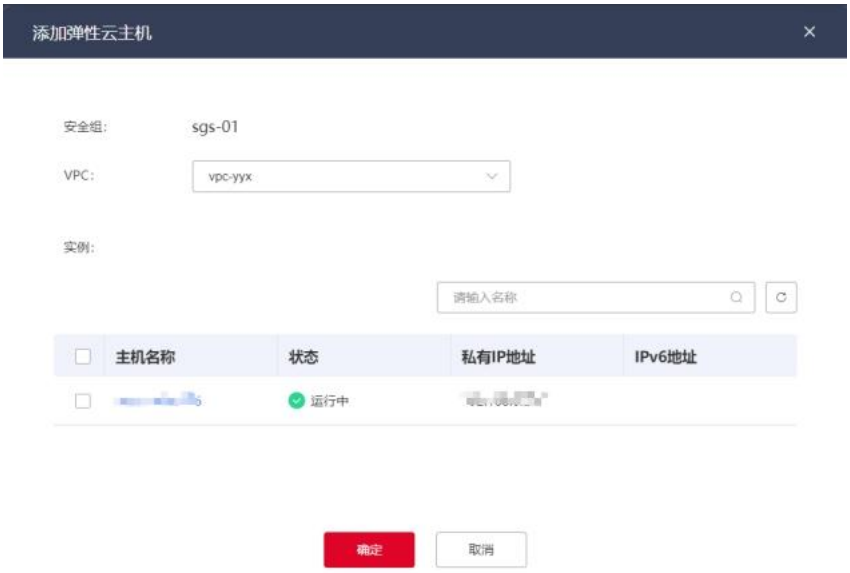
- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成弹性云主机、安全组的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。

3. 单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-安全组”选项。
5. 在安全组列表页面，选择需要调整关联关系的安全组，点击名称进入详情页。
6. 在安全组详情页，选择“关联实例”页签，可以管理云主机和安全组之间的关联关系。

7. 将云主机加入安全组：单击“弹性云主机”页签下的【添加】按钮。在添加云服务器的弹窗中，选择 VPC，选择需要添加的云服务器名称，单击确定。支持批量添加云服务器。



添加完成后，该安全组规则对所选择的云服务器自动生效。

注：为了更好的网络性能，建议一个云主机不超过 5 个安全组。

8. 将云主机移除安全组：

- 批量移除：单击“弹性云主机”页签下的【移除】按钮，在弹窗中选择需要移除的云服务器名称，支持批量解除云服务器和安全组的关系。
- 单次移除：选择需要移除的云服务器，单击其所在行的【移除】按钮，逐次解除云服务器和安全组之间的关系。

注：所选择的云服务器至少要属于一个安全组，否则就不允许移除。

- 对于地域资源池来说，在移除云服务器的弹窗中，需要先选择 VPC，再选择 VPC 下可移除的云服务器。
- 对于可用区资源池来说，可直接选择移除安全组所属的 VPC 下可移除的云服务器。

9. 更改安全组：选择需要更改安全组的云服务器，单击其所在行的【更改安全组】按钮，支持在云服务器的详情页里面调整云服务器与安全组之间的关系。

安全组与辅助网卡的关联管理

本文帮助您快速熟悉安全组与辅助网卡的关联管理。

操作场景

安全组防护云服务器的出入方向流量，但是您将云服务器与安全组关联后，只是针对主网卡做了防护。您可以根据业务需求，对每张网卡配置精准的安全组规则，从而对每张网卡的流量进行安全访问控制。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成弹性云主机、安全组的创建。

操作步骤

1. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
2. 单击“虚拟私有云”；进入网络控制台页面。
3. 在左侧导航栏，选择“访问控制-安全组”选项。
4. 在安全组列表页面，选择需要调整关联关系的安全组，点击名称进入详情页。
5. 在安全组详情页，选择“关联实例”页签，点击二级页签“辅助网卡”，可以管理网卡和安全组之间的关联关系。

6. 将辅助网卡加入安全组：单击“辅助网卡”页签下的【添加】按钮。在添加辅助网卡的弹窗中，选择 VPC，选择需要添加的辅助网卡名称，单击确定。支持批量添加辅助网卡。

添加完成后，该安全组规则对所选择的辅助网卡自动生效。

注：为了更好的网络性能，建议一个辅助网卡不超过 5 个安全组。

7. 将云主机移除安全组：

- 批量移除：单击“辅助网卡”页签下的【移除】按钮，在弹窗中选择需要移除的辅助网卡名称，支持批量解除辅助网卡和安全组的关系。
- 单次移除：选择需要移除的辅助网卡，单击其所在行的【移除】按钮，逐次解除辅助网卡和安全组之间的关系。

注：所选择的辅助网卡至少要属于一个安全组，否则就不允许移除。

- 对于地域资源池来说，在移除辅助网卡的弹窗中，需要先选择 VPC，再选择 VPC 下可移除的辅助网卡。
- 对于可用区资源池来说，可直接选择移除安全组所属 VPC 下可移除的辅助网卡。

8. 更改安全组：选择需要更改安全组的辅助网卡，单击其所在行的【更改安全组】按钮，支持在辅助网卡的详情页里面调整辅助网卡与安全组之间的关系。

查看弹性云主机的安全组

本文帮助您快速熟悉弹性云主机的安全组的查看的操作场景和操作流程。

操作场景

安全组主要是为了限制云主机/物理机的网络访问，保护云主机/物理机的安全。您可以查看云主机/物理机所关联的安全组的相关信息并根据业务需求做相应的调整。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成弹性云主机的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“计算”，单击“弹性云主机”；进入云主机控制台页面。

4. 在“弹性云主机”界面，选择需要操作的云主机，点击名称进入详情页；
5. 在弹性云主机详情页，选择“安全组”页签，查看弹性云主机所属的安全组详情；

6. 支持对安全组进行更改、编辑、删除等操作，同时可以查看安全组规则，对并规则进行添加、删除、修改等操作。

云主机的常用端口

本文为您介绍弹性云主机的常用端口，请您务必仔细阅读后使用。

场景说明

安全组端口的作用是限制云主机/物理机的网络访问，添加安全组规则时，您必须指定通信端口或端口范围，当存在外部请求时，安全组会根据您设置的端口限制进行匹配，允许或拒绝该访问的请求，这样可以增加云主机/物理机的安全性，防止未经授权的访问。

弹性云主机常用端口

您可以通过配置安全组规则放通弹性云主机对应的端口，配置规则方法请参见“添加安全组规则”页面，配置场景请参考“安全组配置示例”页面。具体弹性云主机常用端口如下表：

协议	端口	说明
FTP	21	FTP 服务上传和下载文件。

SSH	22	远程连接 Linux 弹性云主机。
Telnet	23	使用 Telnet 协议远程登录弹性云主机。
HTTP	80	使用 HTTP 协议访问网站。
POP3	110	使用 POP3 协议接收邮件。
IMAP	143	使用 IMAP 协议接收邮件。
HTTPS	443	使用 HTTPS 服务访问网站。
SQL Server	1433	SQL Server 的 TCP 端口,用于供 SQL Server 对外提供服务。
SQL Server	1434	SQL Server 的 UDP 端口，用于返回 SQL Server 使用了哪个 TCP/IP 端口。
Oracle	1521	Oracle 通信端口，弹性云主机上部署了 Oracle SQL 需要放行的端口。
MySQL	3306	MySQL 数据库对外提供服务的端口。
Windows Server Remote Desktop Services	3389	Windows 远程桌面服务端口，通过这个端口可以连接 Windows 弹性云主机。
代理	8080	8080 端口常用于 WWW 代理服务，实现网页浏览。如果您使用了 8080 端口，访问网站或使用代理服务器时，需要在 IP 地址后面加上：8080。安装 Apache Tomcat 服务后，

		默认服务端口为 8080。
NetBIOS	137、138、139	NetBIOS 协议常被用于 Windows 文件、打印机共享和 Samba。 137、138：UDP 端口，通过网上邻居传输文件时使用的端口。 139：通过这个端口进入的连接试图获得 NetBIOS/SMB 服务。

注意事项

部分运营商判断 25、135、139、444、445、5800、5900 等端口为高危端口，默认被屏蔽，建议您在使用过程中不要设置高危端口来承载业务，以防造成您的业务不通或部分资源损失。

安全组配置示例

安全组产品广泛应用于多种场景，本文带您更快了解安全组的经典应用场景。

不同安全组内的弹性云服务器内网互通

场景举例：

在同一个 VPC 内，用户需要将某个安全组内一台弹性云主机上的资源拷贝到另一个安全组内的弹性云主机上时， 用户可以将两台弹性云主机设置为内网互通后再拷贝资源。

安全组配置方法：

由于同一个 VPC 内，在同一个安全组内的弹性云服务器默认互通，无需配置。但是，在不同安全组内的弹性云服务器默认无法通信，此时需要添加安全组规则，使得不同安全组内的弹性云主机内网互通。在两台弹性云主机所在安全组中分别添加一条入方向安全组规则，放通来自另一个安全组内的实例的访问，实现内网互通，安全组规则如下所示。

协议	**方向**	**端口范围/ICMP 协议类型**	**源地址**
设置内网互通时使用的协议类型（支持 TCP/UDP/ICMP/All）	入方向	设置端口范围或者 ICMP 协议类型	IPv4 地址、IPv4 CIDR 或者另一个安全组的 ID

仅允许特定 IP 地址远程连接弹性云主机

场景举例：

为了防止弹性云主机被网络攻击，用户可以修改远程登录端口号，并设置安全组规则只允许特定的 IP 地址远程登录到弹性云主机。

安全组配置方法：

以仅允许特定IP地址(例如,192.168.20.2)通过SSH协议访问Linux操作系统的弹性云主机的 22 端口为例，安全组规则如下所示。

协议	方向	端口范围	源地址
SSH（22）	入方向	22	IPv4 地址、IPv4 CIDR 或者另一个安全组的 ID。 例如：192.168.20.2

SSH 远程连接 Linux 弹性云主机

场景举例：

创建好 Linux 弹性云主机后，为了通过 SSH 远程连接到弹性云主机，您可以添加安全组规则。

安全组配置方法：

协议	方向	端口范围	源地址
SSH（22）	入方向	22	0.0.0.0/0

RDP 远程连接 Windows 弹性云主机

场景举例：

创建好 Windows 弹性云主机后，为了通过 RDP 远程连接弹性云主机，您可以添加安全组规则。

安全组配置方法：

协议	方向	端口范围	源地址
RDP（3389）	入方向	3389	0.0.0.0/0

公网 ping 弹性云主机

场景举例：

创建好弹性云主机后，为了使用 ping 程序测试弹性云主机之间的通讯状况，您需要添加安全组规则。

安全组配置方法：

协议	方向	端口范围	源地址
ICMP	入方向	All	0.0.0.0/0

弹性云主机做 Web 服务器

场景举例：

如果您在弹性云主机上部署了网站，即弹性云主机作 Web 服务器用，希望用户能通过 HTTP 或 HTTPS 服务访问到您的网站，您需要在弹性云主机所在安全组中添加以下安全组规则。

安全组配置方法：

协议	方向	端口范围	源地址
TCP	入方向	80（HTTP）	0.0.0.0/0
TCP	入方向	443（HTTPS）	0.0.0.0/0

弹性云主机做 DNS 服务器

场景举例：

如果您将弹性云主机设置为 DNS 服务器，则必须确保 TCP 和 UDP 数据可通过 53 端口访问您的 DNS 服务器。您需要在弹性云服务器所在安全组中添加以下安全组规则。

安全组配置方法：

协议	方向	端口范围	源地址
TCP	入方向	53	0.0.0.0/0
UDP	入方向	53	0.0.0.0/0

使用 FTP 上传或下载文件

场景举例：

如果您需要使用 FTP 软件向弹性云主机上传或下载文件，您需要添加安全组规则。

安全组配置方法：

您需要在弹性云主机上先安装 FTP 服务器程序，再查看 20、21 端口是否正常工作。

协议	方向	端口范围	源地址
FTP	入方向	20-21	0.0.0.0/0

负载均衡健康检查：

对于负载均衡，为保证健康检查正常进行，需要确保服务器安全组已经放通 100.89.0.0/16 网段的地址。

网络 ACL

网络 ACL 的简介

本文带您了解什么是 ACL，以及 ACL 的基本特性。

网络 ACL 定义

网络 ACL 是一个子网级别的流量防护策略，您可以自定义设置网络 ACL 规则，并将网络 ACL 与子网绑定，实现对子网中云服务器实例流量的访问控制。通过出方向/入方向规则控制出入子网的流量数据。

地域资源池和可用区资源池的网络 ACL 存在部分区别，如表 1 所示：

表 1 地域资源池和可用区资源池的网络 ACL 的区别

对比项	地域资源池	可用区资源池
是否存在默认规则	不存在默认规则。	存在，每个 ACL 出/入方向各存在两条默认规则。 具体信息可参考“ACL 默认规则”。
创建 ACL 时是否需要指定子网	创建时需要指定子网。	创建时无需指定子网，可创建后再关联子网。
ACL 与子网之间的对应关系	一个子网支持关联一个 ACL。 一个 ACL 支持关联	一个子网支持关联一个 ACL。 一个 ACL 支持关联

	一个子网。	多个子网。
是否支持自定义源/目的地址	入方向规则不支持自定义目的地址。 出方向规则不支持自定义源地址。	出/入方向规则均支持自定义源/目的地址。

网络 ACL 基本信息

ACL 创建后，您可以添加 ACL 规则自定义访问控制策略，对于多可用区资源池来说，当 ACL 中没有明确的自定义规则时，系统会采用默认的规则。关联子网后，基于默认安全原则，网络 ACL 会默认拒绝所有出入子网的流量，直至添加放通规则。对于地域资源池来说，不存在默认规则，当不匹配规则时默认放通全部流量。

基本特性如下：

- 针对可用区资源池，网络 ACL 与子网之间是一对多的关系，即一个网络 ACL 可以对多个子网生效，而一个子网同一时间只能关联一个网络 ACL。
- 针对地域资源池，ACL 与子网是一对一的关系，即一个网络 ACL 只能对一个子网生效，而一个子网同一时间只能关联一个网络 ACL。
- 网络 ACL 只能在子网级别生效，不能对同一子网内的云主机实例间的流量实现过滤。
- 网络 ACL 支持多种策略，如允许、拒绝。

- ACL 规则的优先级数字越小则优先级越高。
- 对于可用区资源池来说，创建网络 ACL 后，自动创建出默认规则，它会拒绝所有未明确被允许的访问请求。默认规则为最低优先级，创建自定义规则后，按照优先级顺序执行规则。默认规则不支持修改、删除、启用/停用等操作。
- 对于可用区资源池来说，每个新创建的网络 ACL 最初都为未激活状态，直到您将 ACL 与子网关联后才可生效 ACL 内的规则，实现子网内的流量防控。
- 网络 ACL 是无状态的，即设置入方向规则的允许请求后，需要同时设置相应的出方向规则，否则可能会导致请求无法响应。您可以根据实际需求进行灵活的设置。

不同资源池列表见产品简介-资源池区别页面，实际情况以控制台展现为准。

安全组和网络 ACL 的区别

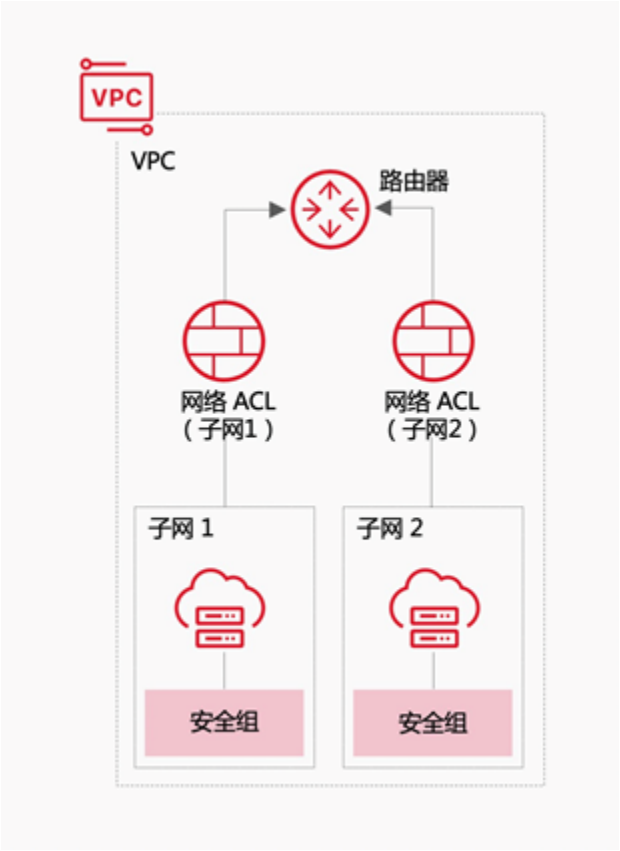
本文为您介绍下安全组和网络 ACL 的区别。

网络 ACL 和安全组的区别

ACL 和安全组都是用于控制资源访问权限的防护策略，与安全组不同的是 ACL 是一个子网级别的流量防护策略，您如果想在子网级别增加对资源的流量访问控制权限，可以自定义 ACL 规则，通过 ACL 与子网的绑定关系实现云服务器流量控制。尽管与安全组在实现和使用

场景上略有不同，但是二者可以结合实现更复杂、精细化的访问控制策略。

安全组和网络 ACL 如图所示：



下面是安全组和网络 ACL 的区别对比表格：

特性	安全组	网络 ACL

作用范围	云服务器级别。	子网级别。
作用机制	“白名单”机制，即不匹配规则时，默认拒绝所有访问。	“黑名单”机制，即不匹配规则时，默认允许所有访问。
支持协议	TCP/UDP/Any/ICMP。	TCP/UDP/ALL/ ICMP。
规则优先级	有，按照优先级顺序执行，数字越低优先级越高。 仅可用区资源池支持安全组规则优先级。	有，按照优先级顺序执行，数字越低优先级越高。
优先级生效顺序	多个规则冲突，同等优先级的情况下，拒绝优先于允许生效。	多个规则冲突时，优先级高的规则生效，优先级低的不生效。同等优先级时，拒绝优于允许生效。
规则是否支持启、停状态	无，只能添加、修改、删除规则。	有，可以启用或禁用规则。
规则数量限制	有，单用户单资源池可以	有，每个网络 ACL 最多

	添加 500 条规则。	可以有 20 条规则。
规则匹配方式	可以设置协议、端口、源/目的地址。 源/目的地址可以是IP地址形式，也可以是安全组形式。	可以设置协议、源端口、目的端口、源地址和目的地址。 地域资源池入向不支持自定义目的地址，出向不支持自定义源地址。
适用场景	适用于实例级别的安全控制，如 Web 服务器、数据库服务器等。	适用于子网级别的安全控制，如 VPC 内部通信、对外访问等。

总的来说，安全组和网络 ACL 都是重要的安全防护策略，但是它们的作用范围、规则数量限制、规则匹配方式、规则优先级、规则状态和适用场景等方面有所差异。您需要根据实际需求选择合适的产品来进行网络安全防护。

创建 ACL

本文帮助您快速熟悉 ACL 的创建。

使用场景

当您需要在子网级别对云主机/物理机的出入流量进行控制时，您可以将 ACL 与子网进行关联，通过 ACL 规则去控制访问流量

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在网络 ACL 列表页面，点击右上角的“创建网络 ACL”按钮，进入创建网络 ACL 页面。
6. 在创建网络 ACL 页面，根据以下信息配置网络 ACL，然后单击确定。

7. 配置信息如下：

配置	说明
ACL 名称	输入网络 ACL 的名称。
虚拟私有云	选择网络 ACL 所属的虚拟私有云。
子网	支持选择网络 ACL 所关联的子网，可用区资源池无需填写此项。
描述	输入网络 ACL 的描述。
企业项目	创建网络 ACL 时，可以将网络 ACL 加入已启用的企业项目。

注意事项：

1. 对于地域资源池来说，需要在创建 ACL 时指定 ACL 与子网的关联关系，一个 ACL 可关联一个子网；
2. 对于可用区资源池来说，创建 ACL 时无需指定与子网的关联关系，可以在创建后根据您的业务情况去关联，一个 ACL 可关联多个子网。

ACL 默认规则

本文帮助您快速熟悉 ACL 默认规则。

仅多可用区资源池支持默认规则，默认规则不支持修改、删除、启用/停用等操作。

网络 ACL 创建后包含默认的入方向规则和出方向规则：

- 入方向规则：拒绝所有入方向流量，优先级低于自定义 ACL 规则；
- 出方向规则：拒绝所有出方向流量，优先级低于自定义 ACL 规则。

创建 ACL 后会生成默认规则，默认规则如下：

入方向规则：

出方向规则：

ACL 默认规则拒绝出入方向的流量，且默认规则为最低优先级。

创建其他规则后，则将以创建的规则过滤网络流量。

添加 ACL 规则

本文帮助您快速熟悉添加 ACL 规则的操作场景和操作流程。

操作场景

当您需要按照自定义的策略来对出入子网的流量进行控制时，您可以自定义添加新的出方向、入方向 ACL 规则。

入方向：指从外部访问 ACL 规则下的子网内的云服务器。

出方向：指 ACL 规则下的子网内的云服务器访问 ACL 外的实例。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成网络 ACL 的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击  ，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，选择需要添加规则的 ACL。
6. 进入“ACL”详情界面，在入方向规则或出方向规则页签，单击“添加入方向/出方向规则”按钮。
7. 单击“增加一条规则”，可以依次增加多条规则。
8. 单击网络 ACL 规则操作列下的“复制”选项，复制已有的网络 ACL 规则。

9. 配置参数说明如下：

参数	说明
优先级	网络 ACL 规则的优先级，优先级的数值越小，表示优先级越高。--为默认的规则，优先级最低。*默认规则仅可用区资源池适用。
策略	选择入方向规则的授权策略：允许：允许访问子网中云服务器。拒绝：拒绝访问子网中云服务器。
协议	选择协议类型，支持以下几种协议：ALL：所有协议。ICMP：网络控制报文协议。TCP：传输控制协议。UDP：用户数据报协议。
源地址	此方向允许的源地址，默认值为 0.0.0.0/0，代表支持所有的 IP 地址。
目的地址	此方向允许的目的地址，默认值为 0.0.0.0/0，代表支持所有的 IP 地址。
源端口	源端口范围，取值范围是 1～65535 的数字。选择 TCP 或

范围	UDP 协议时必须填写。
目的端口范围	目的端口范围，取值范围是介于 1～65535 的数字。选择 TCP 或 UDP 协议时必须填写。
描述	网络 ACL 规则的描述信息，非必填项。

注意事项：

1. 对于地域资源池来说，创建 ACL 时需要指定子网与 ACL 的关联关系。添加规则时，入方向规则不支持自定义目的地址，出方向规则不支持自定义源地址。
2. 对于可用区资源池来说，添加规则时，出/入方向均支持自定义源/目的端口。

调整 ACL 规则优先级

本文帮助您快速熟悉调整 ACL 规则优先级的操作流程。

使用场景

ACL 规则可以设置优先级，默认规则为“--”，代表最低优先级。优先级的数值越小，优先级越高。当您需要将一些重要的规则放在 ACL 规则列表的顶部，以确保这些规则能够被最先匹配到并执行时，可以通过调整 ACL 规则的优先级实现。

默认规则为“--”，代表最低优先级。默认规则仅可用区资源池适用。

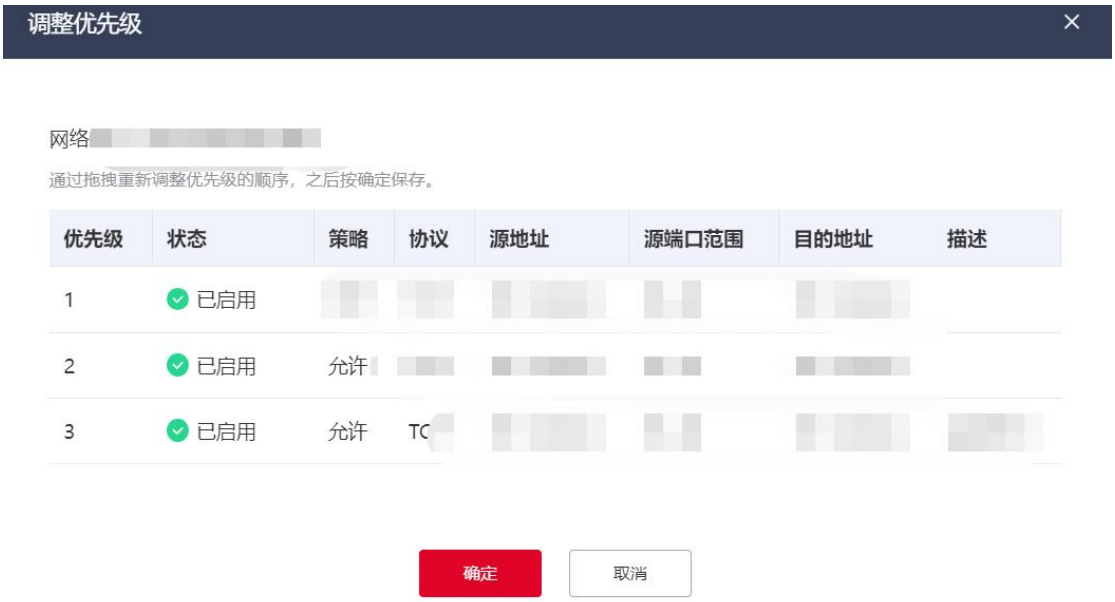
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成网络 ACL 的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，选择需要添加规则的 ACL。
6. 进入“ACL”详情页面，点击列表页的“调整优先级”按钮，进入调整优先级弹框界面；

7. 鼠标上下拖动 ACL 规则即可对优先级进行调整，然后单击“确定”。



修改 ACL 规则

本文帮助您快速熟悉 ACL 规则的修改操作流程。

使用场景

当您的应用场景发生变化时，可以修改 ACL 规则帮助您更好地控制网络访问，您需谨慎修改规则，确保修改后的规则能够满足实际需求并提高网络的安全性和可控性。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成网络 ACL 的创建。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，找到目标网络 ACL，单击网络 ACL 的名称。
6. 进入“ACL”详情页面，点击操作列的“修改”按钮。

7. 根据页面相关提示可以对 ACL 规则的配置信息进行修改。

8. 具体参数配置如下：

参数	**说明**
优先级	网络 ACL 规则的优先级，优先级的数值越小，表示优先级越高。--为默认的规则，优先级最低。*默认规则仅可用区资源池适用。
策略	选择入方向规则的授权策略：允许：允许访问子网中云服务

	器。拒绝：拒绝访问子网中云服务器。
协议	选择协议类型，支持以下几种协议：ALL：所有协议。ICMP：网络控制报文协议。TCP：传输控制协议。UDP：用户数据报协议。
源地址	此方向允许的源地址，默认值为 0.0.0.0/0，代表支持所有的 IP 地址。
目的地址	此方向允许的目的地址，默认值为 0.0.0.0/0，代表支持所有的 IP 地址。
源端口范围	源端口范围，取值范围是 1～65535 的数字。选择 TCP 或 UDP 协议时必须填写。
目的端口范围	目的端口范围，取值范围是介于 1～65535 的数字。选择 TCP 或 UDP 协议时必须填写。
描述	网络 ACL 规则的描述信息，非必填项。

注意事项：

1. 对于地域资源池来说，创建 ACL 时需要指定子网与 ACL 的关联关系。修改规则时，入方向规则不支持自定义目的地址，出方向规则不支持自定义源地址。
2. 对于可用区资源池来说，修改规则时，出/入方向均支持自定义源/目的端口。

停用/启用 ACL 规则

本文帮助您快速熟悉 ACL 规则的停用/启用操作流程。

使用场景

当您需要控制 ACL 规则是否生效时，可以通过停用/启用进行控制。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成网络 ACL 及规则的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，找到目标网络 ACL，单击网络 ACL 的名称。
6. 进入“ACL”详情页面，点击列表页的“停用/启用”按钮。

优先级	状态	策略	协议	源地址	源端口范围	目的...	目的端口...	描述	操作
1	已启用	允许	TCP	36.111.88.3...	1-65535	0.0.0.0/0	22-6789	36.111.88.33	修改 删除 停用
2	已停用	允许	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	1-65535		修改 删除 启用

7. 在弹窗中点击“确定”，可以对 ACL 规则进行停用/启用，停用后对应的 ACL 规则暂时不生效，启用后重新生效。

注意事项：

1. 对于多可用区资源池来说，默认规则不支持修改、删除、启用/停用等操作。

删除 ACL 规则

本文帮助您快速熟悉 ACL 规则的删除操作流程。

使用场景

当某个 ACL 规则已经不再需要时，可以将其删除以保持网络访问控制的简洁性和可维护性。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成网络 ACL 及规则的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，找到目标网络 ACL，单击网络 ACL 的名称。
6. 进入“ACL”详情页面，点击操作列的“删除”按钮，可以对 ACL 规则进行删除。

7. 支持批量删除多条网络 ACL 规则，单击列表上方的“删除”按钮，选择需要删除的网络 ACL 规则。

ACL 关联子网

ACL 支持和子网关联后对子网流量进行过滤防护，本文帮助您快速熟悉 ACL 关联子网的操作流程。

使用场景

ACL 创建成功后，需要和子网进行关联才可以对子网的流量进行过滤防护。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成网络 ACL 的创建。
- 仅可用区资源池支持，实际情况以控制台展现为准。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，找到目标网络 ACL，单击网络 ACL 的名称。
6. 进入“ACL”详情页面，点击列表页的“关联子网”。

7. 在弹出的关联子网页面，选择需要关联的子网，单击“确定”。

注意事项：

- 已被网络 ACL 关联的的子网将不会展示在其他 ACL 关联子网的弹窗中，如您需要更换 ACL 与子网之间的绑定关系，请先解除已绑定的 ACL 和子网，再进行重新关联。
- 仅可用区资源池支持在 ACL 创建后关联子网。
- 地域资源池需创建 ACL 时指定与子网的关联关系。
- 对于地域资源池来说，一个子网同一时间仅支持一个 ACL，一个 ACL 仅支持关联一个子网。
- 对于可用区资源池来说，一个子网同一时间仅支持一个 ACL，一个 ACL 支持关联多个子网。

ACL 取消关联子网

ACL 支持和子网关联后对子网流量进行过滤防护，本文帮助您快速熟悉 ACL 取消关联子网的操作流程。

使用场景

当您的 ACL 创建成功后，可根据自身业务需求，取消网络 ACL 与子网关联关系。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成网络 ACL 的创建。
- 仅可用区资源池支持，实际情况以控制台展现为准。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，找到目标网络 ACL，单击网络 ACL 的名称。
6. 进入“ACL”详情页面，点击列表页的“取消关联”。
7. 在弹窗中单击“确定”，取消子网与 ACL 的关联。

8. ACL 支持批量解绑多个子网，选择需要解除关联的子网，单击列表上方的“取消关联子网”，将多个子网同时从当前网络 ACL 中全部移出。

> **注意事项**：
>
> - 在地域资源池中，需要在创建 ACL 时指定子网与 ACL 的关联关系，不支持创建后解绑。如需解除绑定关系，请删除 ACL 后重建。

导入/导出 ACL 规则

ACL 规则支持批量导入和导出，本文帮助您快速熟悉 ACL 规则的导入/导出。

操作场景

当您需要将已有的 ACL 规则做本地备份时，您可以选择将网络 ACL 规则导出为本地文件。

当您需要复用已有的 ACL 规则到另一个 ACL 中，您可以选择导出和导入 ACL 规则。支持跨区域导入和导出。

建议您每次导入少于 20 条的规则，否则可能会影响性能。导入规则是在原有规则基础上进行新增，不会删除已有规则，请注意 ACL 规则的配额限制。相同规则不允许重复导入。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成网络 ACL 的创建。

操作步骤

导出 ACL 规则

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，找到目标网络 ACL，单击网络 ACL 的名称。
6. 进入“ACL”详情页面，点击详情页的“导出规则”。

导入 ACL 规则

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“访问控制-ACL”选项。
5. 在“ACL”界面，找到目标网络 ACL，单击网络 ACL 的名称。
6. 进入“ACL”详情页面，点击详情页的“导入规则”。

虚拟 IP

虚拟 IP 概述

本文帮助您快速熟悉虚拟 IP 的定义、特点、组网模式，以及应用场景等内容。

什么是虚拟 IP

虚拟 IP（Virtual IP Address，简称 VIP）是一个从子网中分配的内网 IP 地址，没有分配给真实弹性云服务器网卡。虚拟 IP 地址拥有私有 IP 地址同样的网络接入能力，用户也可以像主私网 IP 地址一样通过虚拟 IP 去访问弹性云服务器。

您可以通过将虚拟 IP 与主备弹性云服务器绑定，根据是否需要访问公网可以为虚拟 IP 绑定一个弹性 IP，配合高可用软件（例如 Keepalived）使用，实现业务的高可用。

注意：如未结合 Keepalived 使用，请谨慎删除与虚拟 IP 绑定的主服务器或者网卡，有可能会导致备服务器或网卡流量不通等现象。

特点介绍

虚拟 IP 具备如下网络特性：

- 虚拟 IP 可以动态的落在某一台云服务器上，某个云服务器可以通过 ARP 协议来宣告与虚拟 IP 之间的关系，更改绑定的服务器对象。
- 虚拟 IP 是从子网中分配的 IP 地址，仅支持绑定同属于一个子网下的资源。

组网模式

虚拟 IP 主要是搭配高可用软件，例如 Keepalived，用于弹性云服务器的主备切换。当主服务器发生故障时，虚拟 IP 将动态切换到备服务器上，备服务器会接管主服务器的业务，保证业务正常运行。

高可用性模式场景举例：为实现业务的高可用，避免单点故障，可以利用同一个虚拟 IP 结合不同的弹性云服务器实现“一主多备”的场景。当主服务器故障时，备服务器可以转为主服务器，继续对外提供服务。

以“一主一备”的场景为例，实现高可用性需要完成如下配置：

- 将一个虚拟 IP 绑定与同属于一个子网的两台云服务器做绑定。
- 将两台云服务器结合 Keepalived 使用，动态指定其中一台为主服务器，另一台为备服务器。具体操作文档可以参考虚拟 IP 结合 keepalived 实现主备双机高可用。

应用场景

结合弹性 IP 访问公网业务

- 当您需要对外提供高可用服务时，可以将弹性 IP 与虚拟 IP 绑定，实现面向公网的高可用性。

云内高可用私网服务

- 当您需要同一子网内的云服务器通过同一私网地址访问高可用服务，您可以将虚拟 IP 与云服务器相绑定，实现“一主多备”的场景。

使用限制

- 虚拟 IP 仅支持与同一子网下的服务器进行绑定；
- 一个虚拟 IP 仅支持绑定一个弹性 IP；
- 一个云主机/物理机绑定的虚拟 IP 数量建议不超过 10 个；
- IPv6 类型虚拟 IP 不支持绑定弹性 IP，如果需要访问公网，请在共享带宽界面添加该虚拟 IP。

申请虚拟 IP 地址

本文帮助您快速熟悉虚拟 IP 地址申请的操作方法。

操作场景

当需要设置虚拟 IP 地址为弹性云服务器所用时，可以通过在子网内申请虚拟 IP 地址的方式分配虚拟 IP 地址。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成 VPC、子网的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“子网”选项，点击需要创建虚拟 IP 的子网。
5. 进入子网详情界面，点击“虚拟 IP”页签，点击申请“虚拟 IP 地址”。

6. 在弹窗中配置相关信息，相关配置参数信息如下：

参数	说明
IP 类型	支持 IPv4 和 IPv6，IPv6 仅在子网支持 IPv6 的开放区域可配置

创建方式	选择虚拟 IP 地址的分配方式 自动分配：系统将自动分配 IP 地址。 手动分配：系统将根据您手动填写的地址分配 IP 地址。
备注	非必填信息

7. 单击“确定”按钮，即可完成虚拟 IP 地址的申请。

虚拟 IP 列表

本文帮助您快速熟悉虚拟 IP 地址查看的操作方法。

操作场景

当您需要查看虚拟 IP 绑定的弹性公网 IP、绑定的服务器类型时，可以通过查看虚拟 IP 列表，来获取相关信息。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成 VPC、子网的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。

4. 在左侧导航栏，选择“子网”选项，点击需要创建虚拟 IP 的子网。

5. 进入子网详情界面，点击“虚拟 IP”，即可查看虚拟 IP 列表。

6. 虚拟 IP 列表页字段如下：

列表项	**备注**
虚拟 IP 地址	已创建的虚拟 IP 地址
绑定的弹性 IP	如未绑定则显示--
绑定的服务器类型	云主机/物理机
绑定的云主机 (网卡)	显示云主机名称及网卡的内网 IP 地址
备注	--
操作	绑定弹性 IP (当处于已绑定时显示“解绑弹性 IP”）、绑定服务器、更多（解绑服务器、删除)

绑定弹性 IP

本文帮助您快速熟悉弹性 IP 绑定的操作方法。

操作场景

如果您想从公网服务访问同一个虚拟 IP 地址的多个弹性云服务器，您可以将弹性 IP 绑定到虚拟 IP 上，一个虚拟 IP 地址支持绑定一个弹性 IP。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成 VPC、子网的创建。
- 您需要提前申请好可用的弹性 IP，保证弹性 IP 和虚拟 IP 同属一个区域，且均处于可用状态。
- Xx

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“子网”选项，点击需要创建虚拟 IP 的子网。
5. 进入子网详情界面，点击“虚拟 IP”页签，在需要绑定弹性 IP 的虚拟 IP 地址所在行的操作列下，单击“绑定弹性 IP”。

6. 在弹窗中选择需要绑定的弹性 IP 地址。
7. 点击“确定”按钮。

   注意事项：

   - 绑定弹性 IP 为单选，每个弹性 IP 只能绑定一个虚拟 IP，且弹性 IP 绑定虚拟 IP 后不能再绑定其它云资源。
   - IPv6 类型虚拟 IP 不支持绑定弹性 IP，如果需要访问公网，请在共享带宽界面添加该虚拟 IP。

解绑弹性 IP

本文帮助您快速熟悉弹性 IP 解绑的操作方法。

操作场景

当虚拟 IP 不需要访问公网服务的时候，可以解除虚拟 IP 与弹性 IP 的绑定关系。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成 VPC、子网的创建。
- 您已完成虚拟 IP 与弹性 IP 的绑定。
- Xx

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“子网”选项，点击需要创建虚拟 IP 的子网。
5. 进入子网详情界面，点击“虚拟 IP”页签，在需要解绑弹性 IP 的虚拟 IP 地址所在行的操作列下，单击“解绑弹性 IP”。
6. 在弹窗中选择需要解绑的弹性 IP 地址。
7. 单击“确定”。

绑定服务器

本文帮助您快速熟悉服务器绑定的操作方法。

操作场景

当您需要通过虚拟 IP 去访问业务，实现业务的高可用，您可以选择将云服务器与虚拟 IP 绑定。

前提条件

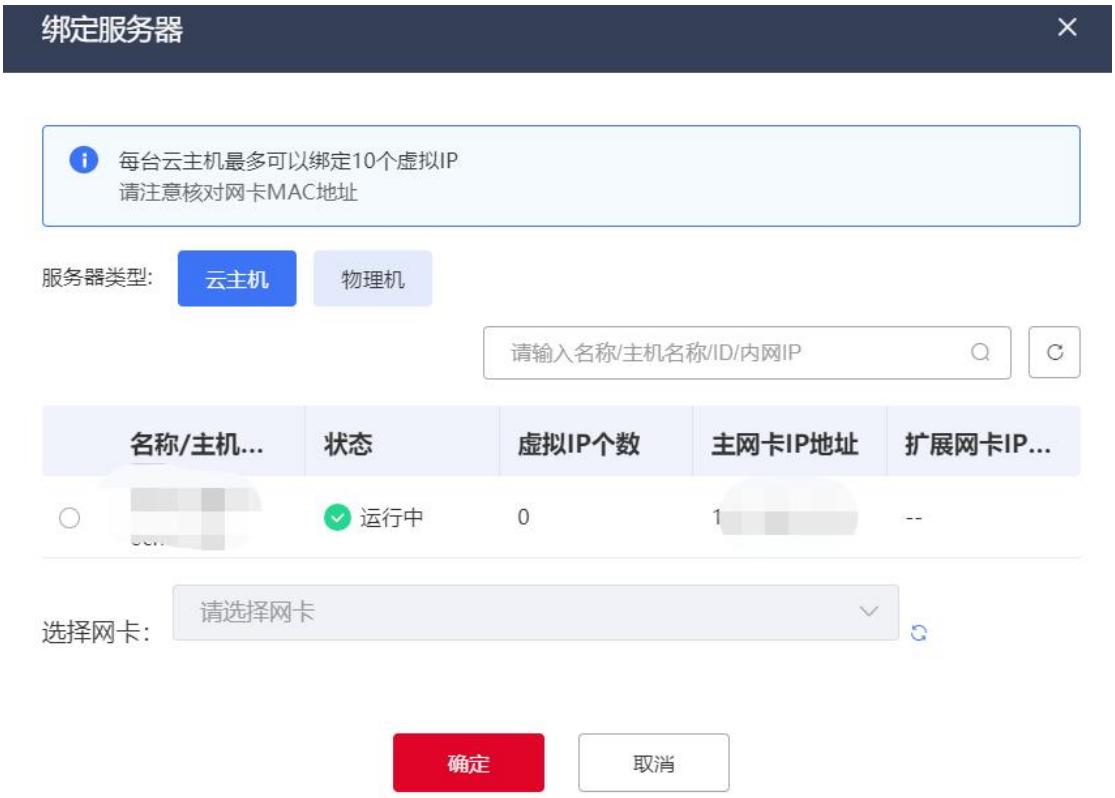
- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成虚拟 IP、弹性云主机的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。

3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“子网”选项，点击需要创建虚拟 IP 的子网。
5. 进入子网详情界面，点击“虚拟 IP”页签，在需要绑定服务器的虚拟 IP 地址所在行的操作列下，单击“绑定服务器”。

6. 在弹窗中选择需要绑定的“服务器类型”：云主机/物理机。



7. 选定服务器类型后选择需要绑定的网卡。
8. 单击“确定”按钮，即可完成服务器的绑定。

   注意事项：一个虚机 IP 支持绑定多个云服务器，同一个虚拟 IP 绑定的服务器类型只能是一种类型。

解绑服务器

本文帮助您快速熟悉服务器的解绑的操作方法。

操作场景

当您不需要云服务器通过已绑定的虚拟 IP 去访问服务的话，您可以选择解除虚拟 IP 和云服务器之间的绑定关系。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成虚拟 IP、弹性云主机的创建及绑定关系。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“子网”选项，点击需要创建虚拟 IP 的子网。
5. 进入子网详情界面，点击“虚拟 IP”页签，在需要解绑云服务器的虚拟 IP 地址所在行的操作列下，单击：“更多”，选择“解绑服务器”。
6. 在弹窗中选择需要解绑的“服务器类型”：云主机/物理机。
7. 选定服务器类型后选择需要解绑的网卡。

8. 单击“确定”按钮。

   注意事项：

   - 如果需要删除已绑定虚拟 IP 的云服务器，建议您先解绑服务器与虚拟 IP 的绑定关系。
   - 请谨慎删除与虚拟 IP 绑定的主服务器或者网卡，有可能会导致备服务器或网卡流量不通等现象。
   - 如果您解除辅助弹性网卡与云服务器之间的关系，不会解除您虚拟 IP 与辅助弹性网卡的绑定关系。

删除虚拟 IP

本文帮助您快速熟悉虚拟 IP 删除的操作方法。

操作场景

当您的业务不再需要虚拟 IP 时，您可以选择删除虚拟 IP。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成虚拟 IP 的创建。
- 删除虚拟 IP 前，您需要先解绑与虚拟 IP 绑定的资源，例如云主机、弹性 IP 等。具体操作方法请参考“解绑服务器”页面，“绑定/解绑弹性 IP”页面。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择广东-广东 6。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“子网”选项，点击需要创建虚拟 IP 的子网。
5. 进入子网详情界面，点击“虚拟 IP”页签，在需要删除的虚拟 IP 所在行的操作列下，点击“更多”，选择“删除”。
6. 删除虚拟 IP 前，用户必须先解绑弹性 IP、云主机、物理机，处于未绑定状态后才可以删除。
7. 在弹窗中确认信息无误后，点击“确定”。

流量镜像

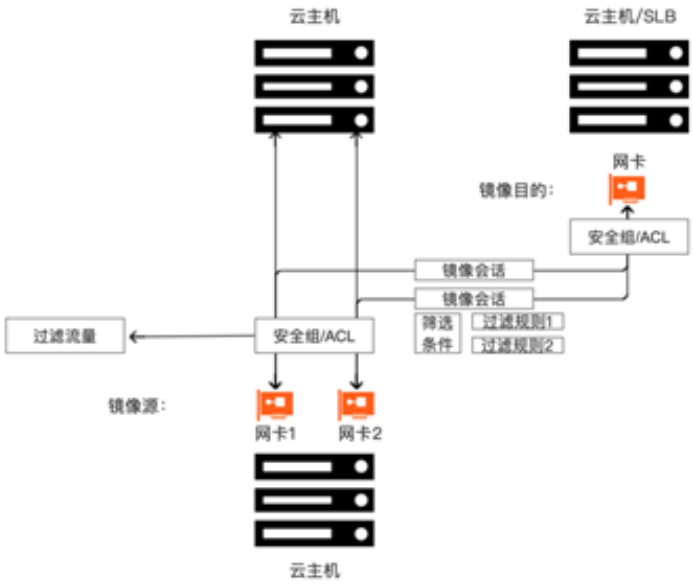
流量镜像概述

本文对流量镜像（Traffic Mirror）的定义、基本概念、功能特性及应用场景进行说明。

流量镜像的定义

流量镜像（Traffic Mirror）功能可以将网络流量从弹性网卡镜像到其他指定的云服务器的网卡上，以便于应用到内容检查、监控分析、问题排查等场景。流量镜像主要是镜像并筛选出符合条件的流量，因此它可以在不影响网络性能的情况下，捕获和记录网络流量，帮助管理员诊断网络故障、检测网络攻击等。

如图所示，云主机通过镜像会话将符合筛选条件的流量复制到镜像目的，然后可以利用分析设备对这些流量进行分析和监控。



基本概念

流量镜像功能用于复制并监控网络中的通信流量，以下是流量镜像的基本概念：

- 镜像源：需要镜像网络流量的实例，例如弹性网卡；
- 镜像目标：接收镜像后流量的实例；
- 镜像会话：通过特定筛选条件，将网络流量从镜像源复制到镜像目的；
- 筛选条件（Mirror Filter）：包含入方向规则和出方向规则，用来筛选在镜像会话中镜像的网络流量；
- 入方向规则和出方向规则：包含五元组信息和采集/不采集控制；
- 五元组：源网段、源端口、目的网段、目的端口和协议类型五个量组成的集合。

功能特性

筛选条件管理

- 创建/编辑/删除筛选条件，添加/编辑/删除筛选条件下的规则。

镜像会话管理

- 创建/编辑/删除镜像会话，管理会话的镜像源/目的/引用的筛选条件/启停。

流量镜像和计费

- 开启会话后，完成指定条件流量的镜像和转发。对镜像后的流量进行监控统计。

应用场景

安全场景：网络入侵检测

- 通过设置一定筛选条件，筛选出符合条件的流量，将复制到镜像目的中的网络流量发送到指定的监控设备上进行分析和监控。通过实时监控网络流量，及时发现和应对潜在的网络攻击行为。
- 例如，通过分析流量镜像数据来检测是否存在异常流量或异常行为，如大量的连接尝试、未经授权的访问、恶意软件传播等。

审计场景：金融或政府

- 在审计方面，流量镜像功能可以帮助您分析和监控网络中的数据流量。例如，可以透明地将实例流量镜像到统一审计平台进行分析，从而更好地了解网络的使用情况和安全状况，以满足审计需求。

网络运维场景：网络问题定位

- 利用流量镜像功能来检查网络问题，运维人员可以直接查看网络传输的内容，例如分析 TCP 的重传，来排查网络问题，而无需进

入虚拟机内部抓取报文。这样可以大大提高排查问题的效率和准确性。

产品使用限制

为保证流量镜像产品正常使用，在使用之前，请您务必仔细阅读以下使用限制。

- 每个用户在每个资源池最多可创建 10 个筛选条件，最多可创建 10 个会话。
- 一个会话只能添加一个源；一个源只能被加入一个会话。
- 一个会话只能添加一个目的；一个目的可以被加入最多 10 个会话。
- 一个网卡不能既作镜像源又作镜像目的。
- 一个会话只能添加一个筛选条件；一个筛选条件可以被最多 10 个会话引用。
- 一个筛选条件可以增加多个规则（出/入各 10 个）。
- 一个会话的源和目的必须归属同一个租户的同一个区域（Region）。
- 流量镜像的报文采用标准的 VXLAN 报文格式封装，当被镜像的报文长度加上 VXLAN 报文长度大于镜像源实例的 MTU 值时，系统会对报文进行截断。为了防止报文被截断，建议您在 IPv4

场景下，设置弹性网卡的 MTU 值比链路支持的 MTU 值至少小 50 字节。

- 流量镜像不采集 ACL 丢弃流量、安全组丢弃流量、QoS 丢弃流量和被过滤器过滤掉的流量。ACL 和安全组丢弃流量遵循以下规则：
  - 报文在从镜像源复制时，出方向不受安全组和网络 ACL 的限制。
  - 报文在复制至镜像目的时，入方向会受目的安全组和网络 ACL 策略的限制。
- 为了防止流量被安全组和 ACL 丢弃，需要在镜像目的所在安全组和网络 ACL 配置以下规则：
  - 安全组规则：入方向允许镜像源弹性网卡的 IP 访问目的端口为 4789 的 UDP 协议报文。
  - ACL 规则：入方向允许来自镜像源弹性网卡的 IP 和所有源端口的 UDP 协议报文。

支持地域

仅部分多 AZ 资源池支持，实际情况已控制台展示为准。

计费说明

本文对流量镜像产品计费进行说明。

公测期间免费。

创建筛选条件

本文对创建筛选条件的操作步骤进行说明。

使用场景

筛选条件是用于指定镜像的网络流量的规则，您可以设置筛选条件来复制符合条件的流量。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“流量镜像-筛选条件”选项。
5. 在筛选条件页面，点击右上角的“创建筛选条件”按钮。
6. 在创建筛选条件弹窗中，填写筛选条件的名称和描述。

7. 单击“确定”创建完成。
8. 点击筛选条件名称进入详情页，选择入方向规则或出方向规则，单击添加规则，根据弹窗内容添加入方向规则或出方向规则，配置完成后单击“确定”。入方向规则和出方向规则的相关参数如下表所示。

参数	**说明**
协议类型	选择需要镜像流量使用的协议类型，支持选择以下协议： ALL：所有协议 ICMP：网络控制报文协议 TCP：传输控制协议 UDP：用户数据报协议
源网段	设置网络流量的源地址网段
目的网段	设置网络流量的目的地址网段

源端口	输入网络流量的源端口范围 端口范围为 1~65535，使用正斜线（/）隔开起始端口和终止端口，格式为 20/30、80/80，-为不限制端口 当协议类型选择为 ALL 或者 ICMP 时，禁用端口输入框，显示“-”，表示不限制端口
目的端口	输入网络流量的目的端口范围 端口范围为 1~65535，使用正斜线（/）隔开起始端口和终止端口，格式为 20/30、80/80，-为不限制端口 当协议类型选择为 ALL 或者 ICMP 时，禁用端口输入框，显示“-”，表示不限制端口
策略	规则的采集策略： 采集：采集网络流量 不采集：不采集网络流量
优先级	规则的生效顺序。 添加规则时不支持添加优先级，添加后自动生成优先级，优先级不能重复，后添加的规则优先级默认最低。点击“调整优先级”按钮，支持拖拽修改已有规则优先级

注：

1. 筛选条件下无规则时默认不镜像流量。
2. 针对采集策略，不采集一般指不会对符合规则的网络流量进行采集，举例：若配置如下策略， 1、 ALL 0.0.0.0/0 - 0.0.0.0/0 - 不采集； 2、 ICMP 192.168.0.4/32 - 192.168.0.3/32 - 采集，则仍会对 192.168.0.4 的网络流量进行采集。

创建镜像会话

本文对创建镜像会话的操作步骤进行说明。

使用场景

通过创建镜像会话，可以将网络流量从一个网卡复制到另一个网卡，从而实现实时的网络监控和分析。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成筛选条件的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“流量镜像-镜像会话”选项。
5. 在镜像会话页面，点击右上角的“创建镜像会话”按钮。

6. 根据界面提示，配置名称、描述、VNI 参数，然后单击“下一步”，具体配置参数如下：

参数	说明
名称	输入镜像会话的名称 输入范围 2-32 位，支持大小写英文字母和数字，以英文字母开头。
描述	输入镜像会话的描述信息
VNI	指定一个 VNI 来区分不同的镜像流量，取值范围为 0~16777215。 支持自定义 VNI 的值。

7. 在关联筛选条件页面，列表展示所有筛选规则，选择一个筛选条件，然后单击“下一步”。

8. 在关联镜像源页面，列表展示所有网卡，选择需要镜像流量的网卡，然后单击“下一步”。

9. 在关联镜像目的页面，列表展示所有网卡，选择具体的网卡作为镜像目的，单击“下一步”。
10. 同一个网卡不能即作为镜像源又作为镜像目的。
11. 在确认信息界面对创建的信息进行确认，点击创建。
12. 配置完成后，单击“返回”或静待 5 秒后即可回到镜像会话展示界面。

启动镜像会话

本文对启动镜像会话的操作步骤进行说明。

使用场景

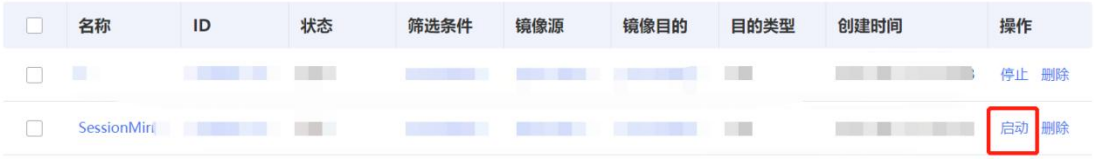
当您的镜像会话创建成功后，默认状态为未启动状态，当您需要开始镜像流量时，可选择启动镜像会话。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成镜像会话的创建。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“流量镜像-镜像会话”选项。
5. 在镜像会话页面，找到需要启动的镜像会话，然后在操作列单击“启动”按钮。



停止镜像会话

本文对停止镜像会话的操作步骤进行说明。

使用场景

当您的镜像会话启动成功后，您需要停止镜像流量时，可选择停止镜像会话。

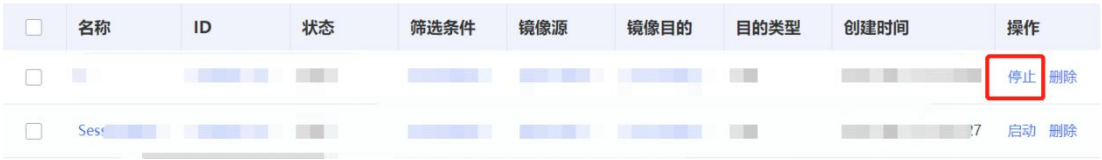
前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成镜像会话的创建及启动。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“流量镜像-镜像会话”选项。
5. 在镜像会话页面，找到需要启动的镜像会话，然后在操作列单击“停止”按钮。



6. 停止镜像会话将会终止您的镜像业务，请谨慎操作！

删除镜像会话

本文对删除镜像会话的操作步骤进行说明。

使用场景

当您不需要镜像业务时，您可以删除镜像会话，删除镜像会话之前，请先保证会话处于停止状态。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。
- 您已经完成镜像会话的创建。

操作步骤

1. 登录控制中心。

2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“流量镜像-镜像会话”选项。
5. 在镜像会话页面，找到需要删除的镜像会话，然后在操作列单击“删除”按钮。
6. 处于运行中的会话请先点击停止会话，在弹出的对话框，单击“确定”按钮。

删除筛选条件

本文对删除筛选条件的操作步骤进行说明。

使用场景

当您的删除筛选条件已不满足业务需求时，您可以选择删除，删除前请确保筛选条件已和镜像会话解除关联关系。

前提条件

- 注册天翼云账号，并完成实名认证。具体操作，请参见天翼云账号注册流程。

- 您已经完成筛选条件的创建，且解除筛选条件与镜像会话的绑定关系。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击，选择区域，本文我们选择华东-华东 1。
3. 依次选择“网络”，单击“虚拟私有云”；进入网络控制台页面。
4. 在左侧导航栏，选择“流量镜像-筛选条件”选项。
5. 在筛选条件页面，找到需要删除的筛选条件，然后在操作列单击“删除”按钮。

虚拟私有云常见问题

基础知识

什么是 CIDR?

CIDR 是一种用于对 IP 地址进行聚合和分配的方法。CIDR 使用前缀长度来表示 IP 地址的网络部分的位数，这样就可以更加灵活地分配 IP 地址，并实现对地址空间的高效利用。

CIDR 表示法

CIDR 使用一个斜线后跟一个数字来表示前缀长度。

例如，192.168.0.0/16 表示前 16 位为网络部分，剩余的位数为主机部分。

通过这种表示法，可以快速判断 IP 地址属于哪个网络。

如何选择 VPC 网段、子网网段？

您可以使用 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 及其子网段作为 VPC 的私网网段，网段掩码有效范围为 8~28 位。具体说明请参考，如何规划 VPC 网段、数量

如何选择子网网段

VPC 支持的网段为 10.0.0.0/8-28、172.16.0.0/12-28、192.168.0.0/16-28，子网的网段须在 VPC 网段范围内，且子网的掩码范围为：子网所在 VPC 掩码~28。如果使用的网段不在三个网段内，建议您提交工单申请。

不同子网之间网段不能相同、不能有交集

子网创建成功后，不支持修改网段，请提前合理规划好子网网段。

具体说明请参考，如何规划子网网段、数量

VPC 下的子网之间是否可以互通？

不同 VPC 之间默认逻辑隔离，同 VPC 下的不同子网默认互通。

同 VPC 下，主网段内的 ECS 实例与附加网段内的 ECS 实例是否可以互通？

同 VPC 下默认所有子网均可以互通，通过附加网段创建的子网和其他子网也可以互通。如果要禁止互通，可以通过安全组、ACL 来实现隔离。

不同 VPC 之间是否可以互通？

不同 VPC 之间默认逻辑隔离。可以通过对等连接、VPN、云间高速实现不同 VPC 之间的互通。

VPC 是否支持 VPN 接入？

VPC 支持本地数据中心 IDC 通过 VPN 接入，具体请参考 VPN 相关文档 https://www.ctyun.cn/document/10026758/10037859

VPC 是否支持专线接入？

VPC 支持本地数据中心 IDC 通过物理专线接入，具体请参考专线相关文档 https://www.ctyun.cn/document/10026762/10031161

操作类

本文汇总了使用虚拟私有云产品时常见的操作类问题。

子网间是否可以通信？

同 VPC 下不同子网之间默认互通，不同 VPC 之间默认逻辑隔离。

子网的网段是否可以修改？

不可以

子网的网段一旦创建，不能进行修改。

子网被相关资源占用时，会导致无法删除子网，如何排查相关资源？

虚拟私有云的子网被弹性云主机、物理机、虚拟 IP、NAT 网关、弹性负载均衡、路由表等资源使用时，子网无法删除。请根据子网信息排查子网中是否含有以上资源，先删除子网中的全部资源，再删除子网。

什么是安全组？

安全组是一种虚拟防火墙，用来控制弹性云服务器进出流量，加强弹性云服务器的安全保护。安全组创建后，用户可以在安全组中定义各种访问规则，当弹性云服务器加入该安全组后，即受到这些访问规则的保护。

安全组规则支持哪些协议？

安全组规则支持配置 TCP、UDP、ICMP 和 Any，Any 表示对所有协议生效。选择 TCP、UDP 协议时，配置允许该协议访问安全组的端口范围为 1-65535。当您选择 ICMP 协议时，可以在下拉列表中指定 ICMP 协议类型，此时默认类型是 Any。

安全组默认规则作用是什么？

安全组规则入方向表示从外部访问弹性云服务器，出方向表示弹性云服务器访问外部。弹性云服务器加入安全组后，如果安全组中没有任何规则，则弹性云服务器无法访问外部网络，同时外部网络也无法访

问弹性云服务器。安全组默认出方向规则表示弹性云服务器可以访问外部，默认入方向规则表示弹性云服务器可以被同一安全组内其他弹性云服务器访问。

需要注意的是，安全组不能解决网络故障或网络配置错误类问题。例如，因为网络原因，两个弹性云服务器之间本来就无法互相访问，即使配置了允许他们互相访问安全组规则，这两个弹性云服务器仍无法通信。

如何设置安全组规则？

安全组规则支持入方向和出方向。

针对入方向规则，限制源地址为安全组或者网段（CIDR），对于可用区资源池来说，源地址若为安全组，则仅可以选同一 VPC 下的安全组；对于地域资源池来说，源地址若为安全组，则可以选择该资源池内所有可用安全组。

针对出方向规则，限制目的地址为安全组或网段（CIDR），对于可用区资源池来说，目的地址若为安全组，则仅可以选择同一 VPC 下的安全组；对于地域资源池来说，目的地址若为安全组，则可以选择该资源池内所有可用安全组。源地址和目的地址是否支持安全组的情况以控制台展现为主。

安全组中多个安全组规则冲突时，安全组规则优先级哪个更高?

安全组添加的规则是白名单，多个安全组规则冲突，安全组取其并集生效。

两个相同优先级的安全组规则，一个规则拒绝、一个规则允许，哪条规则生效?

在安全组规则优先级相同的情况下，一个规则拒绝、一个规则允许，拒绝优于允许，默认拒绝（drop）规则生效。

筛选条件被镜像会话引用时支持修改吗?

支持。
筛选条件被引用时，也允许添加、编辑、删除出/入方向规则。

镜像会话中是否支持变更筛选条件?

支持。
仅停止状态支持变更筛选条件，运行中状态禁止变更。

使用限制类

本文汇总了使用虚拟私有云产品时常见的使用限制类问题。

虚拟私有云中可以使用哪些网段（CIDR）？

当前 VPC 支持的网段有：10.0.0.0/8-28、172.16.0.0/12-28、192.168.0.0/16-28。

一个用户下支持创建多少个 VPC?

默认情况一个用户支持创建 5 个 VPC，如果配额不满足实际需求，您可以提工单申请扩大配额。

子网可以使用的网段是什么?

子网的网段要在 VPC 的网段内部，VPC 提供三段私网网段，10.0.0.0/8-28、172.16.0.0/12-28 和 192.168.0.0/16-28，所以子网的网段也会在这些范围内。

虚拟私有云和子网的限额是多少?

用户最多可创建 5 个 VPC，每个 VPC 下最多可创建 5 个子网。

一个用户能拥有多少个安全组?

一个用户最多可以拥有 100 个安全组，500 条安全组规则。

虚拟 IP 的使用限制

每台云主机/物理机最多可以绑定 10 个虚拟 IP；虚拟 IP 绑定的云服务器类型是单一的，当虚拟 IP 绑定了云主机后不允许绑定物理机，同理，当虚拟 IP 绑定了物理机后，不允许绑定云主机。

每个用户可申请多少个镜像会话?

在默认情况下，每个用户每个资源池最多可拥有 10 个镜像会话。

每个用户可申请多少个筛选条件?

在默认情况下，每个用户每个资源池最多可拥有 10 个筛选条件。

每个网卡最多可被引用做镜像目的多少次?

在默认情况下，每个网卡做镜像目的最多被引用次数 10 次。

每个筛选条件下最多有多少个规则?

在默认情况下，每个筛选条件下最多可创建 10 条出方向规则、10 条入方向规则。

每个镜像会话中源和目的的限制数量是多少?

一个会话只能添加一个源；一个源只能被加入一个会话。

一个会话只能添加一个目的；一个目的可以被加入最多 10 个会话。

是否支持镜像不同租户不同区域的流量?

不支持。

一个会话的源和目的必须归属同一个租户的同一个区域。

源和目的是否可以为同一个网卡?

不可以。

一个网卡不能既作镜像源又作镜像目的。

流量镜像是否采集网络的全部流量?

不是。

流量镜像不采集 ACL 丢弃流量、安全组丢弃流量、QoS 丢弃流量和被过滤器过滤掉的流量。

镜像源和镜像目的如何受所在安全组和 ACL 的限制?

报文在从镜像源复制时，入方向受源的安全组和 ACL 限制，出方向不受安全组和网络 ACL 的限制

报文在复制至镜像目的时，入方向会受目的安全组和网络 ACL 策略的限制。

为了防止流量被安全组和 ACL 丢弃，需要在镜像目的所在安全组和网络 ACL 配置以下规则：

- 安全组规则：入方向允许镜像源网卡的 IP 访问目的端口为 4789 的 UDP 协议报文。

- ACL 规则：入方向允许来自镜像源网卡的 IP 和所有源端口的 UDP 协议报文。

路由类

本文汇总了使用虚拟私有云产品时常见的路由类问题。

路由表可以跨 VPC 存在吗？

不可以。

路由表由一系列路由规则组成，只能存在于某个 VPC 内，用于控制虚拟私有云的流量走向。

路由表收费吗？

不收费

默认路由表随着 VPC 自动创建，您也可以根据流量规划自定义路由表及路由规则。

默认路由表的作用是什么？

路由表用于控制虚拟私有云的流量走向。对于可用区资源池来说，

在新建 VPC 时，会默认生成一个默认路由表，每个 VPC 都会对应一个默认路由表。新建的子网也会关联到默认路由表下，您也可以创建自定义路由表，将子网关联到自定义路由表。

通用类

本文汇总了使用虚拟私有云产品时常见的通用类问题。

什么是配额?

为避免资源浪费，服务供应商限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个虚拟私有云。

如何查看我的配额?

11. 登录控制中心。
12. 在控制中心页面左上角点击，选择区域。
13. 在页面右上角，点击“我的配额”，进入服务配额页面。

服务	资源类型	已用配额	总配额
弹性云主机	实例数	0	200
	核心数	0	800
	RAM容量 (MB)	0	1,638,400
镜像服务	镜像	0	10
弹性伸缩服务	伸缩组	0	10
	伸缩配置	0	100
	ess_bandwidth_scaling_policy	0	10
云硬盘备份	备份数	0	720
云硬盘	磁盘数	0	400
	磁盘容量 (GB)	0	32,768
	快照数	0	2,000

14. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
15. 如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

1. 登录控制中心。
2. 在控制中心页面左上角点击  ，选择区域。
3. 在页面右上角，点击“我的配额”，进入服务配额页面。
4. 在服务配额页面，点击“申请扩大配额”按钮，进入新建工单页面。
5. 在新建工单页面，根据您的需求，填写相关参数。
6. 填写完毕后，勾选协议并单击“提交”。

不同 VPC 之间是否可以内网互通?

不同 VPC 之间逻辑上完全隔离，您可以使用对等连接、VPN 网关、云间高速等产品实现 VPC 内网互通。

VPC 如何访问公网服务

您可以使用弹性 IP 或者 NAT 网关访问公网，具体操作请参考如何使用弹性 IP 或者 NAT 网关访问公网页面。

公网可以访问 VPC 中的云服务吗?

您可以使用以下方法从公网访问 VPC 中的云服务：

- 默认分配弹性 IP
- 绑定已有弹性 IP
- 配置公网 NAT 网关

- 配置公网负载均衡

具体操作可参考常见公网访问方法页面。

对等连接有哪些限制?

- 配置对等连接时，不建议两端 VPC 的网段（CIDR）存在重叠，可能会造成路由冲突，导致配置不生效。
- 对等连接创建完成后，可以使用“ping”命令检查本端网络是否连通，不支持通过“ping”命令检查对端子网网关是否连通。
- 如果两个 VPC 的 CIDR 有重叠，建立对等连接时，只能针对子网建立对等关系。如果两个 VPC 下的子网网段有重叠，那么该对等关系可能不生效。建立对等连接时，请确保对等连接两端不包含重叠的子网。
- VPC A 与 VPC B、VPC C 分别建立对等连接，如果 VPC B 和 VPC C 的网段有重叠，那么 VPC A 中无法添加具有相同目的网段的路由。
- 两个 VPC 之间不能同时建立多个 VPC 对等连接。
- 不同区域的 VPC 不能创建对等连接。
- VPC1 与 VPC2 创建对等连接，默认情况下 VPC2 不能通过 VPC1 的 EIP 访问公网。
- 跨租户申请 VPC 对等连接，需要对端租户接受后，才能生效。同租户申请对等连接默认已接受。
- 为了安全起见，请不要接受来自未知帐号的对等连接申请。

- 对等连接双方帐号都有权限删除对等连接，一方删除对等连接后，对等连接的所有信息会被立刻删除，包括对等连接关联的路由信息。
- 对等连接建立后，需要在本端 VPC、对端 VPC 分别添加对方子网的路由才能通信。
- VPC 对等连接路由存在时，VPC 无法被删除。

为什么对等连接创建完成后不能互通？

问题描述

对等连接创建完成后，两个 VPC 还是不能互通。

排查思路：

对等连接配置错误

同一个区域的不同 VPC 之间内网不同，您可以通过配置对等连接实现内网互通，配置说明如下：

- 在 VPC1 和 VPC2 之间创建对等连接，需要连通 VPC1 的子网 A 和 VPC2 的子网 X。
- 对等连接的路由配置，在 VPC1 路由表中配置到子网 X 的路由，在 VPC2 的路由表中配置到子网 A 的路由，打通两个子网。
- 如果您的对等连接配置完成后，VPC 的子网网络仍然无法通信，请排查是否存在如下问题：
- 检查对等连接中 VPC 的子网是否存在重叠，VPC 内的子网网段如果存在重叠，可能会造成路由冲突，对等连接无效。

- 如果不存在 VPC 子网重叠的情况，请检查是否在 VPC 的路由表中配置了正确的路由，包括本端路由和对端路由。

配置建议：路由的目的地址为对端 VPC 子网的网段，比如 10.0.0.0/24，下一跳为“对等连接”。

网络配置错误

1. 确认弹性云主机使用的网卡安全组配置正确。

在弹性云主机详情页面中可以查看网卡使用的安全组。需要放通期望进行通信的对端 VPC 的子网网段。例如：对于 VPC 内的所有弹性云主机，网卡使用的安全组必须至少配置如下图的规则。

授权策略	类型	协议	端口范围/ICMP类型	远端	描述	操作
允许	IPv4	Any	Any	192.168.10.0/24		删除 修改 复制

2. 确认对等连接涉及的子网流量未被网络 ACL 拦截，否则需要放通对等连接涉及的网络 ACL 规则。
3. 多网卡场景下，请务必确认弹性云主机内部已经配置正确的策略路由，确保源 IP 不同的报文匹配各自的规则，从各自所在的网卡发出。
4. 操作步骤：例如，eth0 的 IP 地址为 192.168.1.10/24，eth1 的 IP 地址为 192.168.2.10/24，分别执行

   ping -I 192.168.1.10 192.168.1.1

   ping -I 192.168.2.10 192.168.2.1

   若都可以 ping 通，则双网卡策略路由配置无问题。

弹性云主机基本网络功能异常

1. 确认弹性云主机网卡已经正确分配到 IP 地址。

登录弹性云主机内部，使用命令 ifconfig 或 ip address 查看网卡的 IP 信息。

Windows 弹性云主机可以在命令行中执行 ipconfig 查看。

2. 从弹性云主机内部 ping 所在子网的网关，确认基本通信功能是否正常。

操作步骤：通常网关地址结尾为 1，可以在 VPC 详情页面中确认。

执行 ping 命令观察能否 ping 通即可。若无法 ping 通网关则需首先排查二三层网络问题。

对等连接的路由与专线、VPN 路由的目的地址有重叠

查看对等连接两端的 VPC 下是否有 VPN/云专线资源，排查路由规则的下一跳目的地址是否有重叠。

当对等连接的路由与云专线、VPN 路由的目的地址有重叠时，此时路由有可能失效。

路由已存在

如果添加对等连接路由时，报错“路由已存在”，请检查：VPN、云专线、对等连接等路由的目的地址是否已存在。若已存在则对等连接无法生效。

提交工单

如果上述方法均不能解决您的疑问，请提交工单寻求更多帮助。

您需从对等连接一端的弹性云主机使用 ping 命令向对端 VPC 下的弹性云主机发送 ICMP 报文，并向技术支持人员提供如下表格中的信息：

Item	说明	您的值
VPC1 ID	VPC1 的 ID	-
VPC2 ID	VPC2 的 ID	-
VM1 ID	VPC1 下的弹性云主机 ID	-
VM2 ID	VPC2 下的弹性云主机 ID	-
Subnet1 ID	VM1 所在子网 ID	-
Subnet2 ID	VM2 所在子网 ID	-
IP1	VM1 IP 地址	-
IP2	VM2 IP 地址	-

弹性云主机 IP 获取不到时，如何排查?

问题描述

用户无法查询到弹性云主机私网 IP 地址信息。

排查思路

本问题请按照以下思路进行排查处理。

步骤一：检查是否存在 dhclient 进程

1. 执行如下命令，检查是否存在 dhclient 进程。

```
ps -ef | grep dhclient
```

2. 若 dhclient 进程不存在，登录弹性云主机，尝试重启网卡或主动发起 DHCP 请求。

- Linux 系统：

  执行 dhclient ethx 命令。若不支持 dhclient 命令就执行 ifdown ethx;ifup ethx（ethx 代表弹性云主机网卡，如 eth0、eth1）。

- Windows 系统：先禁用网络连接，然后再重新启用。

3. 对于 DHCP Client 长期不发起请求的情况，例如：重启网卡后又复现，尝试使用以下方法配置静态 IP。

- Linux 系统：
- 执行以下命令，打开
- /etc/sysconfig/network-scripts/ifcfg-eth0 中的配置。
- 输入 vi /etc/sysconfig/network-scripts/ifcfg-eth0
- 修改/etc/sysconfig/network-scripts/ifcfg-eth0 中的配置。
- BOOTPROTO=static
- IPADDR=192.168.1.100 #IP 地址
- NETMASK=255.255.255.0 #掩码值
- GATEWAY=192.168.1.1 #网关地址
- 重启网络服务，执行以下命令：service network restart
- Windows 系统：在网络连接中选择“属性 > Internet 协议版本 4 > 属性”，手动输入 IP 地址、子网掩码和默认网关。

步骤二：检查弹性云主机日志

查看弹性云主机的 messages 日志（路径为/var/log/messages）排查问题。

通过网卡的 MAC 地址过滤日志，排查是否有进程影响 DHCP 获取 IP。

提交工单

如果上述方法均不能解决您的疑问，请提交工单寻求更多帮助。

您需要协助的运维操作：

请将弹性云主机的 ID、所在子网的 ID、VPC 的 ID 提供给技术支持。

二三层通信出现问题时，如何排查?

问题描述

用户云主机基本网络功能异常，无法完成基本通信。从弹性云主机内部 ping 所在子网的网关，无法 ping 通，则需首先排查二三层网络问题。

排查思路

本问题请按照以下思路进行排查处理。

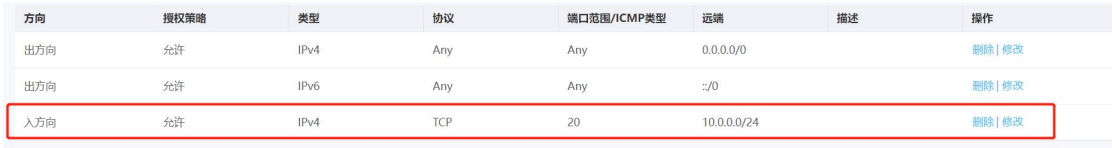
步骤一：检查弹性云主机是否获取到 IP

登录弹性云主机内部，使用命令 ifconfig 或 ip address 查看网卡的 IP 信息。Windows 弹性云主机可以在命令行中执行 ipconfig 查看。若弹性云主机没有获取到 IP，请参考弹性云主机 IP 获取不到时，如何排查?

步骤二：查看安全组是否放通

弹性云主机详情页面中可以查看网卡使用的安全组。需要包含期望进行通信的对端 VPC 的子网网段。

查看安全组是否放通，如下图。



方向	授权策略	类型	协议	端口范围/ICMP类型	远端	描述	操作
出方向	允许	IPv4	Any	Any	0.0.0.0/0		删除 | 修改
出方向	允许	IPv6	Any	Any	::/0		删除 | 修改
入方向	允许	IPv4	TCP	20	10.0.0.0/24		删除 | 修改

步骤三：查看网络 ACL 是否放通

虚拟私有云页面左侧导航栏选择网络 ACL，选择对等连接涉及的子网所关联的网络 ACL，并在网络 ACL 详情页查看对等连接涉及的子网是否已放通。

查看网络 ACL 是否放通，如下图。

提交工单

如果上述方法均不能解决您的疑问，请提交工单寻求更多帮助。

同一个 VPC 内的两台弹性云主机无法互通或者出现丢包等现象时，如何排查？

问题描述

同一个 VPC 内的两台弹性云主机无法互通或者出现丢包等现象。

排查思路

建议您从以下几个原因去排查问题，可以优先排查高频率原因。从而减少排查次数，快速找到根因。以下排查思路根据原因出现的概率从高到低进行排序。

ECS 网卡对应安全组规则未放通

排查弹性云主机网卡对应的安全组是否放通了出方向和入方向的协议的报文。

以入方向的 ICMP 报文为例，安全组规则需要包含下图中的任意一条规则。

若您的业务需要的是其他协议的报文，需放通相应协议的安全组规则。例如，测试的是 TCP 报文，则需检查安全组是否有规则放通出入方向的 TCP 协议。

ECS 网卡所在子网关联的网络 ACL 规则未放通

1. 查看弹性云主机的网卡是否处于网络 ACL 的关联子网中。
2. 在网络 ACL 列表中查看网络 ACL 的状态。

- 状态显示“已开启”，则表示网络 ACL 已经开启。执行第三步。
- 状态显示“未开启”，则表示网络 ACL 已经关闭。执行第四步。

3. 网络 ACL 关闭时，默认不放行出入方向所有协议。此时，请开启 ACL 并放通相应协议的报文或者是解除 ACL 与子网的关系并重新关联。
4. 单击网络 ACL 名称，分别在“入方向”和“出方向”的页签下添加相应协议的放通规则。

ECS 网卡内部网络配置问题

以下步骤以 Linux 系统为例，Windows 操作系统请检查系统防火墙限制。

1. 确认弹性云主机是否有多网卡配置。
2. 登录弹性云主机，执行以下命令，查看网卡是否创建且网卡获取私有 IP 地址。若无网卡信息或者无法获取私有 IP 地址，请联系技术支持。

   ifconfig
3. 执行以下命令，查看弹性云主机的 CPU 占用率是否过高，CPU 占有率超过 80%有可能会影响 ECS 通信。

   top
4. 执行以下命令，查看弹性云主机内容部是否有安全规则的其他限制。

   iptables-save
5. 执行以下命令，查看“/etc/hosts.deny”文件中是否包含了限制通信的 IP 地址。

   vi /etc/hosts.deny

如果 hosts.deny 文件里面包含了对端的 IP 地址，请将该 IP 从 hosts.deny 文件中删除并保存文件。

端口不通

1. 如果无法访问弹性云主机的特殊端口，请排查安全组规则以及网络 ACL 规则中是否对端口进行放行。
2. 在 Linux 弹性云主机内部通过以下命令查看弹性云主机内部是否监听该端口。如果未对该端口进行监听，可能会影响弹性云主机的通信。

   netstat -na | grep <端口号>

提交工单

如果上述方法均不能解决您的疑问，请提交工单寻求更多帮助。

弹性云主机如何切换 VPC 或者修改内网 IP 地址?

具体操作步骤请参考如何使用修改内网 IP、切换 VPC 页面。

DHCP 服务器租约默认时间是多长?

10 年。

筛选条件下无规则可以启动镜像会话吗?

筛选条件下无规则时，允许启动镜像会话，默认不镜像。

镜像会话源和目的缺失时会话是否可以运行?

缺失源和目的信息的镜像会话或资源释放导致源/目的被删除时，状态变为停止，禁止启动。

计费类

本文汇总了使用虚拟私有云产品时常见的计费类问题。

VPC 是否收费?

不收费。

VPC 是免费的，但用户在进行网络规划时，所涉及到的带宽或 VPN 按照收费标准计费。

流量镜像是否收费?

流量镜像公测期间免费提供服务。

安全类

本文汇总了使用虚拟私有云产品时常见的安全类问题。

什么条件下可以删除安全组?

- 删除安全组前，需要确保该安全组没有与任何云资源相关联。如果安全组被云资源（云主机、物理机、云数据库等）使用，请先释放对应云资源或者修改云资源使用的安全组，然后再尝试删除安全组。
- 删除安全组时，若该安全组被另一个安全组规则关联（例如“源地址”选择为该安全组），需先删除或修改关联的安全组规则，然后再尝试删除该安全组。
- 默认安全组不能删除。

弹性云主机加入安全组过后能否变更安全组?

可以。

变更安全组的详细操作，请参考实例加入/移出安全组页面。

您也可以选择在弹性云主机的详情页执行变更安全组的操作，具体请参考“查看弹性弹性云主机的安全组”页面。

安全组、ACL 服务是否收费?

安全组和 ACL 服务均免费。

变更安全组规则时，是否对原有流量实时生效?

安全组规则配置变更，对于原有流量可能不会立刻生效。用户需断开变更规则所影响的流量一段时间(约 120 秒)后，变更后的规则才能对流量生效。

如何判断安全组规则是否重复?

当您的协议、类型、端口范围、源/目的地址均相同时，将判断您的规则为重复规则，且不允许下发。当添加或导入规则时，如果安全组中已存在相同规则，则对应的规则将无法添加。

如何查看安全组关联的云服务器?

方法 1：在云服务器对应的管理控制台进行查看。

- 点击云服务器名称进入详情页，在安全组页签下查看云服务器关联的安全组详情。

方法 2：在安全组详情页的关联实例页签下查看云服务器。

- 点击目标的安全组名称进入详情页，在“关联实例”页签下查看该安全组所关联的云服务器，支持变更云服务器与安全组之间的关联关系。

无法访问公有云的某些端口时怎么办?

问题现象：访问公有云特定端口，在部分地区部分运营商无法访问，而其他端口访问正常。

问题分析：部分运营商判断如下表的端口为高危端口，默认被屏蔽无法访问。

协议	端口
TCP	42 135 137 138 139 444 445 593 1025 1068 1433 1434 3127 3128 3129 3130 4444 4789 5554 5800 5900 8998 9995 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 5554 9995 9996

解决方法：建议您修改敏感端口为其他非高危端口来承载业务。

为什么网络 ACL 添加了拒绝特定 IP 地址访问的规则，但仍可以访问?

网络 ACL 存在规则优先级。优先级的数值越小，表示优先级越高。针对可用区资源池来讲，“- -”表示默认规则，优先级最低。

多个网络 ACL 规则冲突，优先级高的规则生效，优先级低的不生效。

ACL 规则的优先级是默认生成的，先添加的规则默认优先级最高。优先级支持手动调整，您可在 ACL 详情中点击调整规则按钮，在弹窗中选择要调整的规则，拖拽到需调整的位置即可。

当您需要拒绝某个 IP 地址的访问时，可以将其优先级设置为最高优先级，拒绝特定 IP 地址访问的规则将优先生效。具体操作请参见调整 ACL 规则优先级。

为什么配置的安全组规则不生效?

问题现象：为云服务器配置的安全组规则未生效。

问题分析：当配置规则不生效时，建议从以下几个原因去排查问题，可以优先排查高频率原因。

- 安全组配置有误；
- 安全组规则与 ACL 规则的配置有冲突；
- 云服务器防火墙的限制。

安全组配置错误

当安全组规则配置有误时，无法满足期望的业务流量。您可以按照以下几点原因对安全组配置进行检查：

1. 安全组规则方向设置错误，例如将需要在入方向添加的规则添加到出方向规则下。
2. 安全组规则协议类型未选择正确。

3.对应端口为高危端口，在部分地区部分运营商无法访问，建议您修改敏感端口为其他非高危端口来承载业务。

4.对应端口未开通。在服务器中需要被正常监听的端口未放通。

- 例如，需要通过 TCP（80 端口）访问到您的服务器，可以在入方向规则放通 TCP，80 端口。您可以通过登录弹性云服务器查看安全组规则是否生效。
- 以 Linux 弹性云服务器为例，运行如下命令查看 TCP 80 端口是否被监听。

```
netstat -an | grep 80
```

5.对于地域资源池来说，需要保证云服务器属于同一 VPC。不同的 VPC 之间默认网络隔离，安全组需在网络互通的情况下生效。您可以使用对等连接等产品建立 VPC 连接互通，使得安全组能对不同 VPC 内云服务器的流量进行访问控制。

网络 ACL 规则与安全组规则冲突

安全组是一种虚拟防火墙，主要控制云服务器的进出流量，网络 ACL 是子网级别的安全防护，保障关联子网内的资源安全。

例如当您设置了安全组入方向规则放通 80 端口，同时设置的网络 ACL 规则包含拒绝 80 端口的规则，那么此安全组规则不生效。

具体配置细则您可以参考添加 ACL 规则或添加安全组规则。

云服务器防火墙限制

查看云服务器的防火墙是否限制了需要开放的端口。关于云防火墙的访问控制策略配置可参考添加防护规则。

提交工单

如果上述方法均不能解决您的疑问，请提交工单寻求更多帮助。

虚拟私有云最佳实践

如何规划 VPC 数量?

为了能够快捷的将业务迁移上云，您需要合理的规划 VPC 网络，本文帮助您更快了解如何规划 VPC 数量。

默认情况下，不同资源池的 VPC 之间内网不互通，同资源池的不同 VPC 内网不互通且是逻辑隔离的，同 VPC 下不同子网之间默认互通。规划虚拟私有云 VPC 的数量通常取决于业务需求和网络设计。以下是一些指导原则，可以帮助您规划 VPC 的数量：

- 规模和复杂性：VPC 的数量可以根据业务的规模和复杂性进行规划。当各业务之间没有网络隔离需求时，您可以只使用一个 VPC 即可。而对于有复杂网络需求的业务系统，可能需要多个 VPC 来满足不同的部门、项目或安全区隔的需求。

- 部门/项目隔离：如果组织有多个部门或项目，每个部门或项目可能需要独立的网络环境和资源。在这种情况下，可以为每个部门或项目创建一个独立的 VPC，以实现网络隔离和资源分离。
- 安全和合规性：某些组织可能有特定的安全或合规性要求，需要严格隔离敏感数据或资源。在这种情况下，可以使用多个 VPC 来创建安全区域，每个 VPC 可以具有独立的网络访问控制策略和安全规则。
- 地理位置和可用性：通过将 VPC 部署在多个地理位置或云服务提供商的区域中，即使一个地点或区域发生问题，其他区域的 VPC 仍然可以继续提供服务，确保业务的连续性和可用性。
- 性能和流量管理：根据网络流量的特点和负载要求，可以设计多个 VPC 来实现流量的管理和控制。例如，将不同类型的流量分离到不同的 VPC 中，以提供更好的性能和带宽控制。

需要注意的是，创建太多的 VPC 可能会增加管理复杂性和成本。因此，在规划 VPC 数量时要综合考虑组织的需求、管理能力和预算限制，根据组织需求和最佳实践进行详细的网络设计和 VPC 数量规划。

如何规划子网？

本文帮助您更快了解如何规划子网。

相关描述

子网是虚拟私有云内的 IP 地址块，可以将虚拟私有云的网段分成若干块，子网划分可以帮助您合理规划 IP 地址资源。虚拟私有云中的所有云资源都必须部署在子网内。同一个虚拟私有云下，子网网段不可重叠。

默认情况下，同一个 VPC 的所有子网内的云主机均可以进行内网通信，不同 VPC 的云主机不能进行内网通信。

注意事项

- 不同 VPC 的云服务器可通过创建对等连接通信。
- 子网创建成功后，不支持修改网段，请提前合理规划好子网网段。
- VPC 支持的网段为 10.0.0.0/8~28、172.16.0.0/12~28、192.168.0.0/16~28，子网的网段须在 VPC 网段范围内，且子网的掩码范围为：子网所在 VPC 掩码~28。如果使用的网段不在三个网段内，建议您提交工单申请。

如何划分子网用途

划分为公网子网和内网子网

- 建议您按照子网是否要访问公网进行分类，可以进行不同业务的隔离、方便运维管理。
- 如果子网下的云主机没有访问公网的场景，则规划为内网子网。

- 内网子网中的云主机不使用 NAT 网关、弹性 IP 等。如果子网下的云主机有访问公网的场景，则规划为公网子网。您可以使用 NAT 网关、弹性 IP 等访问公网。公网子网关联的路由表需要创建指向 IPv4 网关或者 NAT 网关的路由规则。

如何通过业务用途划分子网

- 建议在同一个 VPC 下的业务内可按照业务模块分别划分子网，例如子网 1 用于 Web 层，子网 2 用于逻辑层，子网 3 用于数据层，有利于结合网络 ACL 进行访问控制和过滤。
- 如果只是 VPC 的子网规划，不涉及和本地 IDC 的网络通信，则可以使用 VPC 网段中的子网段进行新建子网。
- 如果要通过 VPN/云专线与线下 IDC 进行互通，本端网段（子网网段）和对端网段（您的 IDC 侧子网网段）不能重叠，请合理规划 VPC 及子网网段。
- 在划分网段时还应考虑该网段的 IP 容量，即有多少可用的 IP 数。

如何规划路由策略?

本文帮助您更快了解如何规划路由策略。

路由表由一系列路由规则组成，用于控制 VPC 内子网的出流量走向。如果您无需对子网的流量走向进行特殊控制，默认 VPC 内网互通的情况下，则使用默认路由表即可，无需配置自定义路由策略；如果您需要对 VPC 内的网络流量走向进行特殊控制，则可以对路由表进行自定义路由配置。

规划路由策略是确保网络数据包按照预期的方式进行路由转发的过程。下面是规划路由策略的一般步骤：

1. 确定网络拓扑：了解网络的整体结构和拓扑图是规划路由策略的首要步骤。确定各个 VPC 之间的连接和子网的划分。
2. 定义路由目标：根据组织的需求和目标，确定不同子网或 VPC 之间的通信需求。确定哪些子网需要直接相互通信，哪些子网需要通过特定的网关或中转设备进行访问。
3. 划分路由域：将网络划分为逻辑上独立的路由域，通常以子网为单位。每个路由域内的主机可以直接通信，而不同路由域之间的通信需要经过路由器。
4. 配置路由策略：根据预定的网络拓扑和路由目标，配置各个路由器上的路由策略。路由策略定义了数据包在路由器之间的传输路径、下一跳和优先级等重要参数。需确保路由策略的一致性和正确性，避免发生路由环路或重复路由等问题。
5. 测试和优化：在应用路由策略之前，进行测试和验证以确保路由器之间的连通性和正确路由。根据需要，对路由策略进行优化，以提高路由的效率、可靠性和安全性。
6. 监控和维护：定期监控路由器的状态，检查路由表和路由策略的变化。根据需要，进行路由表的清理和优化，以确保网络的正常运行和良好的性能。

注意，路由策略的规划是一个复杂的过程，具体的步骤和配置方式会因网络规模和网络需求的不同而有所差异。

安全组最佳实践

本文介绍配置安全组及其规则的最佳实践。您可以通过配置安全组规则，允许或禁止安全组内的 ECS 实例对公网或私网的访问。

安全组实践建议

云上的安全组提供类似虚拟防火墙功能，用于设置单台或多台 ECS 实例的网络访问控制，是重要的安全隔离手段。创建 ECS 实例时，您必须选择一个安全组。您还可以添加安全组规则，对某个安全组下的所有 ECS 实例的出方向和入方向进行网络控制。

在使用安全组前，您应先了解以下实践建议：

- 最重要的规则：安全组应作为白名单使用。
- 开放应用出入规则时应遵循最小授权原则。例如，您可以选择开放具体的端口，如 80 端口。
- 不应使用一个安全组管理所有应用，因为不同的应用一定有不同的需求。对于分布式应用来说，不同的应用类型应该使用不同的安全组，例如，您应对 Web 层、Service 层、Database 层、Cache 层使用不同的安全组，暴露不同的出入规则。
- 避免为每台实例单独设置一个安全组，控制管理成本。
- 尽可能保持单个安全组的规则简洁。因为如果单个安全组规则过多，增加或者删除规则就变得很复杂，就会增加管理的复杂度。
- 天翼云的控制台提供了克隆安全组和安全组规则的功能。如果您想要修改线上的安全组和规则，您应先克隆一个安全组，再在克

隆的安全组上进行调试，避免直接影响线上应用。（部分资源池支持，可提工单申请克隆功能。）

安全组规则的属性

安全组规则主要是描述不同的访问权限，包括如下属性：

- Policy：授权策略，参数值可以是 accept（允许）或 drop（拒绝）。同等优先级，拒绝高于允许。
- Priority：优先级，规则优先级可选范围为 1~100，默认值为 1，即最高优先级。数字越大，代表优先级越低。
- IpProtocol：IP 协议，取值：tcp、udp、icmp、all。all 表示所有的协议。PortRange，IP 协议相关的端口号范围：

IpProtocol	取值为 tcp 或 udp	端口号取值范围为 1~65535。
IpProtocol	取值为 icmp 或 all	不限制端口。

- 安全组 TCP、UDP 报文分片后，分片不带有端口信息，需要将端口范围指定为 1-65535，不进行端口过滤。目前仅合肥 2 支持 UDP 大包分片后指定端口过滤功能，如有 UDP 大包分片，需要指定端口号过滤的需求，可联系客户经理开通此功能。
- 如果您想实现在不同安全组的资源之间的网络互通，您可使用安全组方式授权。对于内网访问，您可使用源安全组授权。

VPC 与外部网络连接

天翼云虚拟私有云提供丰富的接入方式，本文将会为您介绍 VPC 之间，VPC 与公网、本地数据中心互通的相关内容。

连接其他 VPC

您可以使用下表中的产品或功能，连接两个不同的虚拟私有云。

云产品	应用场景	描述
对等连接	同区域的 VPC 互连	对于同一区域的 VPC，可以通过对等连接进行互连，同一帐号与不同帐号的连接方式略有差异。
云间高速	跨区域的 VPC 互连	对于不同区域的 VPC，不区分是否同一帐号，都可以互连，跨区域连接实现云上网络。
虚拟专用网络 VPN	使用公网低成本连接跨区域 VPC	VPN 连接（Virtual Private Network）用于搭建用户本地数据中心与天翼云 VPC 之间便捷、灵活，即开即用的 IPsec 加密连接通道，实现灵活一体，可伸缩的混合云计算环境。

连接公网

您可以使用下表中的产品或功能，将 VPC 和公网（Internet）进行连接。

云产品	应用场景	描述
弹性 IP	单个 ECS 连接公网	弹性 IP 是可以独立申请的公网 IP 地址，将弹性 IP 地址和子网中关联的弹性云主机绑定和解绑，可以实现 VPC 中的弹性云主机通过固定的公网 IP 地址与互联网互通。
NAT 网关（NAT Gateway）	多个 ECS 共享弹性公网 IP 连接公网	NAT 网关能够为虚拟私有云内的计算实例提供网络地址转换服务，使多个弹性云主机可以共享使用弹性 IP 访问 Internet 或使多个弹性云主机提供互联网服务。
弹性负载均衡 (CT-ELB, Elastic Load Balancing)	通过将访问流量均衡分发到多个 ECS 的方式对外提供服务，比如社交媒体等高并发访问场景	弹性负载均衡通过将访问流量自动分发到多台云主机，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

连接本地数据中心

您可以使用下表中的产品或功能，将本地数据中心（IDC）和云上私有网络进行连接。

云产品	应用场景	描述
虚拟专用网络 VPN	使用公网低成本连接 VPC 与本地 IDC	基于 Internet 使用加密隧道将 VPC 与本地数据中心连接起来。具备成本低、配置简单、即开即用等优点。但它的网络质量依赖 Internet。
云专线	铺设物理专线高质量连接 VPC 与本地 IDC	使用物理专线将 VPC 与本地数据中心连接起来。具备低时延、高安全、专用等优点。适用对网络传输质量和安全等级要求较高的场景 。

常见公网访问方法

天翼云提供了丰富的解决方案，以满足 VPC 内的云主机/物理机实例与公网互联互通的需求。

公网产品分类

天翼云提供弹性 IP（EIP）、NAT 网关、弹性负载均衡（CT-ELB）等方式连接公网。

弹性 IP

弹性 IP 是可以独立申请的公网 IP 地址，将弹性 IP 地址和子网中关联的弹性云主机绑定和解绑，可以实现 VPC 中的弹性云主机通过固定的公网 IP 地址与互联网互通。

NAT 网关

NAT 网关能够为 VPC 内的弹性云主机提供 SNAT 和 DNAT 功能，通过灵活简易的配置，即可轻松构建 VPC 的公网出入口。

弹性负载均衡（CT-ELB）

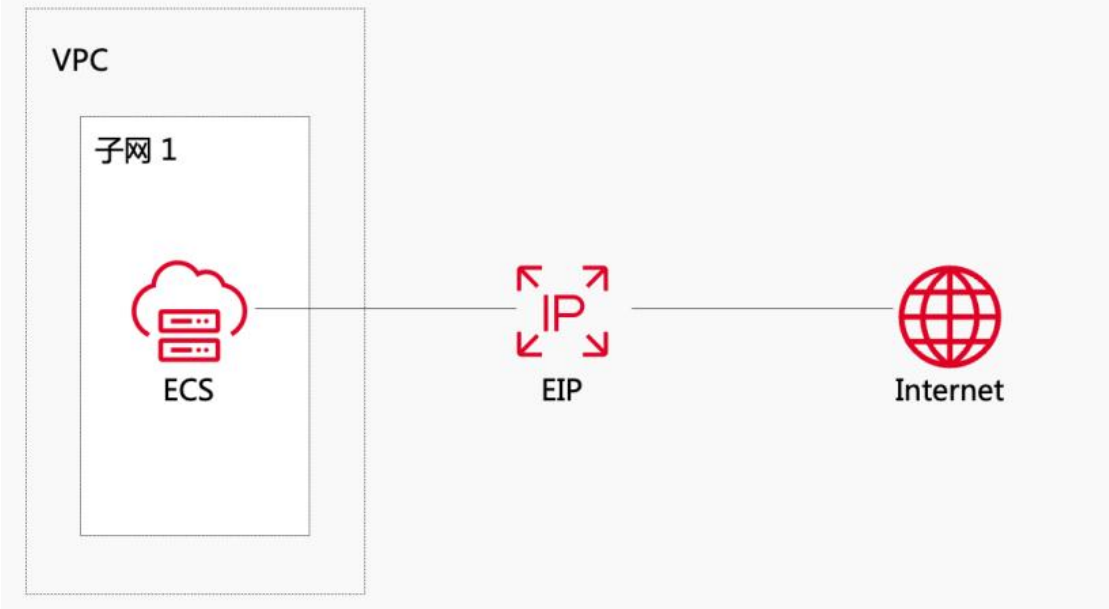
弹性负载均衡（CT-ELB ，Elastic Load Balancing）是一种分发控制网络流量的服务，通过预先设定的算法将访问流量自动分发到多台云主机，扩展应用系统对外的服务能力，实现更高水平的应用系统容错性能。

如何对外提供服务

单个弹性云主机对外提供服务

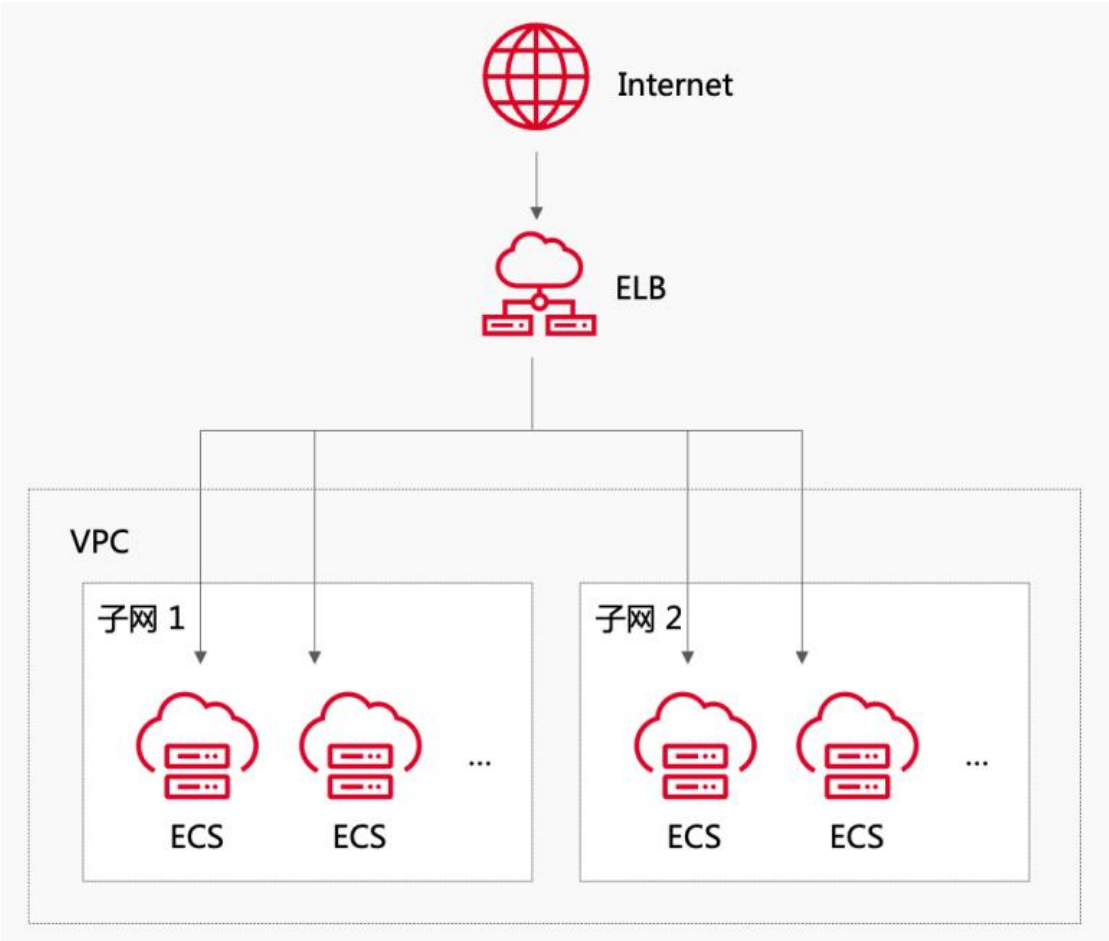
如果您要在 VPC 中的单个弹性云主机实例上提供对外服务，您可申请一个弹性 IP，绑定到弹性主机上，该弹性云主机即可连接公网提供服务。具体操作步骤如下：

1. 创建和配置弹性云主机实例：在天翼云管理控制台中创建弹性云主机实例，并选择合适的实例规格、操作系统和网络配置。确保为实例分配弹性 IP（EIP）以使其能够与外部网络通信。
2. 配置安全组：安全组是一种虚拟防火墙，用于控制进出弹性云主机实例的流量。为该弹性云主机实例创建一个安全组，并根据应用程序的需求配置入站和出站规则。
3. 配置网络 ACL：ACL 也可用于控制子网与外部网络之间的流量。确保对应的子网具有适当的入站和出站规则，以允许外部网络访问该实例提供的服务。
4. 配置路由策略：为了使外部网络能够访问该弹性云主机实例，需要相应的路由配置。
5. 配置 DNS 解析：将您使用的域名绑定到弹性云主机实例的弹性 IP 地址上，以便用户可以使用易记的域名访问您提供的服务。



通过负载均衡进行流量分发

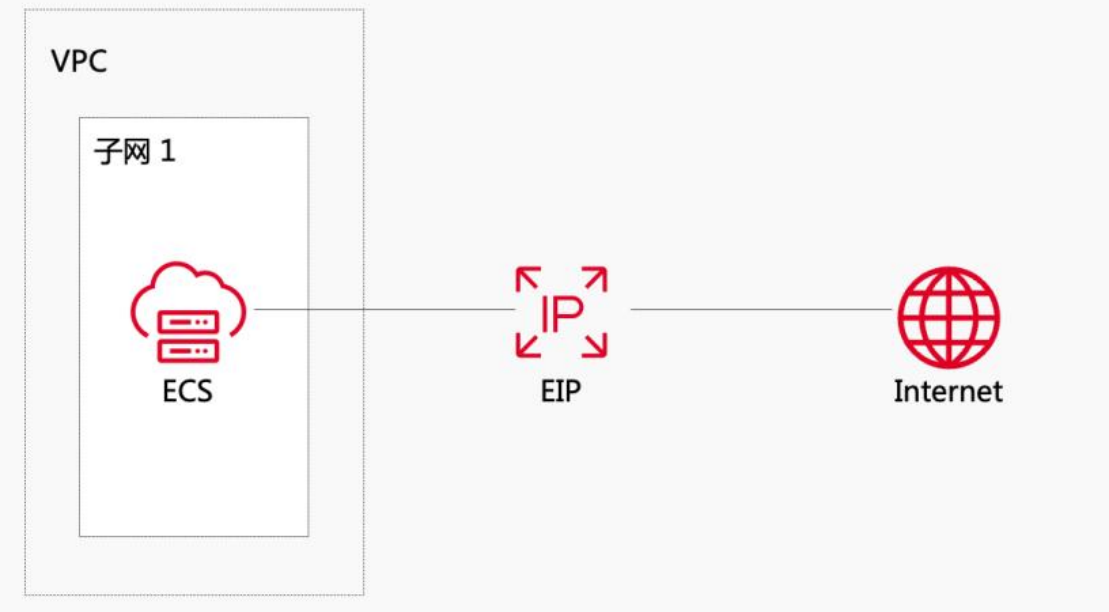
对于社交媒体热点事件、电商促销活动等高并发访问的场景，您可以通过 CT-ELB 将访问流量均衡分发到多台弹性云主机上，能够应对大量用户同时访问的需求。天翼云 CT-ELB 无缝集成了弹性伸缩服务，能够根据业务流量自动扩容，保证业务稳定可靠。



如何主动访问公网

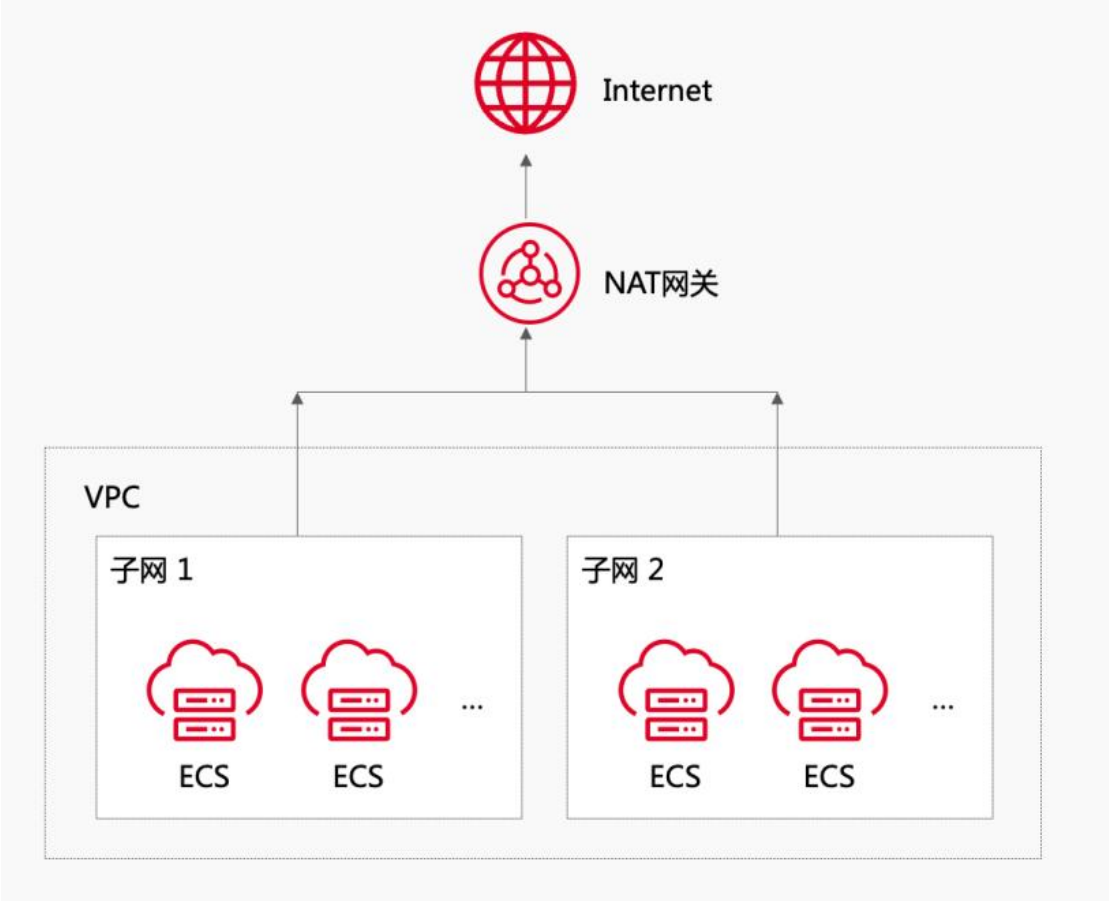
单个弹性云主机访问公网

- 当您的某台弹性云主机需要主动访问公网，可以为弹性云主机绑定弹性 IP，即可实现公网访问。



多个弹性云主机访问公网

- 如果您有多个弹性云主机实例需要访问公网，可以使用 NAT 网关服务，并将多个弹性云主机实例与 NAT 网关关联。按子网配置 SNAT 规则，轻松构建 VPC 的公网出口。对比弹性 IP 访问公网，在未配置 DNAT 规则时，外部用户无法通过公网直接访问 NAT 网关的公网地址，保证了弹性云主机的相对安全。



对于可用区资源池，云主机使用弹性 IP 或者 NAT 网关的操作方法可以参考如何使用弹性 IP 或者 NAT 网关访问公网页面。

如何修改内网 IP、切换 VPC

本文帮助您更快了解如何修改内网 IP、切换 VPC。

使用场景

当您遇到 VPC 中的两个实例 IP 地址冲突，或者在进行网络重构或迁移时，需要调整 VPC 网络架构、子网划分等，这可能会导致需要修改云主机内网 IP 或更换 VPC。

前提条件

- 弹性云主机处于关机状态。
- 只有主网卡支持修改内网 IP，必须先删除辅助网卡。
- 如果网卡绑定了虚拟 IP 或者 DNAT 规则，需要先解绑。
- 如果网卡上有 IPv6 地址，无法修改（包括 IPv4 和 IPv6 的）内网 IP 地址，请先删除 IPv6 地址。
- 如需修改弹性负载均衡后端服务器的内网 IP 地址，请先移出后端服务器组后再修改内网 IP。
- 如果弹性云主机作为静态路由的下一跳，必须先删除静态路由再修改内网 IP。

操作步骤

1. 登录控制中心。
2. 在控制中心页面左上角点击  ，选择区域，本文我们选择华东-华东 1。
3. 依次选择“计算”，单击“弹性云主机”，进入云主机控制台页面。
4. 在云主机列表，选择需要修改内网 IP 或者更换 VPC 的弹性云主机，在云主机详情页选择“弹性网卡”页签，点击“修改内网 IP”或者“更改 VPC”。

5. 在修改内网 IP 弹框页面或者更换 VPC 弹框页面，输入相关参数，点击“确定”按钮。

注意事项

- 修改内网 IP 会导致云主机网络中断，同时更改云主机子网、IP 地址、MAC 地址。
- 修改内网 IP 过程中，请勿操作云主机的弹性 IP，或对云主机做其他操作。
- 修改内网 IP 后，请重检查配置安全组、ACL、虚拟 IP 地址等配置。
- 修改内网 IP 后，请重新配置网络相关的服务、应用软件，例如虚拟 IP、静态路由表、ELB、NAT、DNS 等。

如何使用弹性 IP 或者 NAT 网关访问公网

本文帮助您更快了解如何使用弹性 IP 或 NAT 网关访问公网。

背景信息

对于多可用区资源池，客户可以通过手动配置路由的方式访问公网，实际情况以控制台展现为准。

VPC 创建时，默认会创建 IPv4 网关来统一管理进出 VPC 的公网流量，所有通过弹性 IP 访问公网的流量都受到 IPv4 网关的管理。IPv4 网关和 VPC 同生命周期，不允许单独删除 IPv4 网关。

创建子网路由表时，会默认生成 2 种类型的路由规则，目的网段为 VPC cidr、下一跳为 local 的系统路由；目的网段为 0.0.0.0/0、下一跳为 IPv4 网关的系统路由。因此，所有的子网默认具备通过 IPv4 网关访问公网的能力。

注意事项

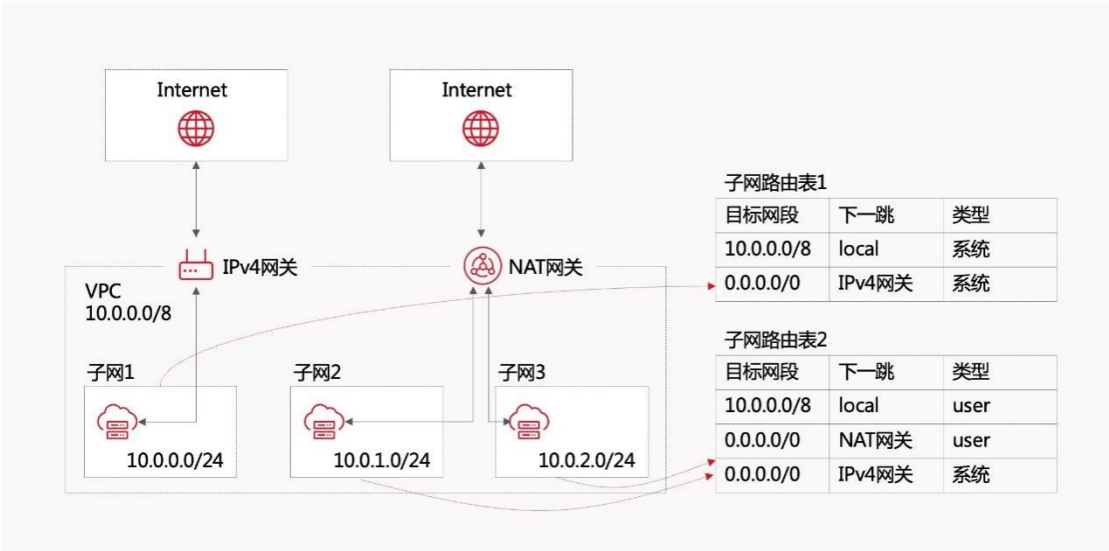
系统类型的路由规则不允许修改、删除；所有系统类型的路由规则优先级低于客户手动创建的 user 类型的路由规则。

在同一个子网内云主机同时绑定弹性 IP 和 SNAT 规则时，由于指向 NAT 网关的路由优先级高于指向 IPv4 网关的系统路由，默认会通过 SNAT 访问公网，云主机绑定的弹性 IP 无法访问公网。因此，不建议同一个子网内的云主机同时绑定弹性 IP 或者 NAT 网关。

示例如下：

VPC cidr：10.0.0.0/8

子网 1 cidr:10.0.0.0/24、子网 2 cidr:10.0.1.0/24、子网 3 cidr:10.0.2.0/24



操作步骤

云主机通过绑定弹性 IP 访问公网

配置方法

- 在创建子网路由表时已经默认生成了指向 IPv4 网关的缺省路由规则，所有的子网默认具备访问公网的能力。不需要再配置其他路由规则即可通过弹性 IP 访问公网。
- 子网 1 中的 ECS 可以通过弹性 IP 访问公网。

云主机通过 SNAT 访问公网

前提条件

- 在 VPC 内创建 NAT 网关实例。

配置方法

- 如果子网 2、子网 3 需要通过 SNAT 主动访问公网，需要在子网 2、子网 3 关联的路由表中增加一条目的地址为 0.0.0.0/0 指向 NAT 网关的路由规则。由于 user 类型的路由规则优先级高于系统类型的路由规则，这样可以保证可以通过 NAT 网关访问互联网。
- 从以上的例子可以看出，同一个子网内的云主机绑定弹性 IP 和 NAT 网关后，默认通过 NAT 网关访问公网，弹性 IP 无法访问公网。因此，不建议同一个子网内的云主机同时绑定弹性 IP 和 NAT 网关。

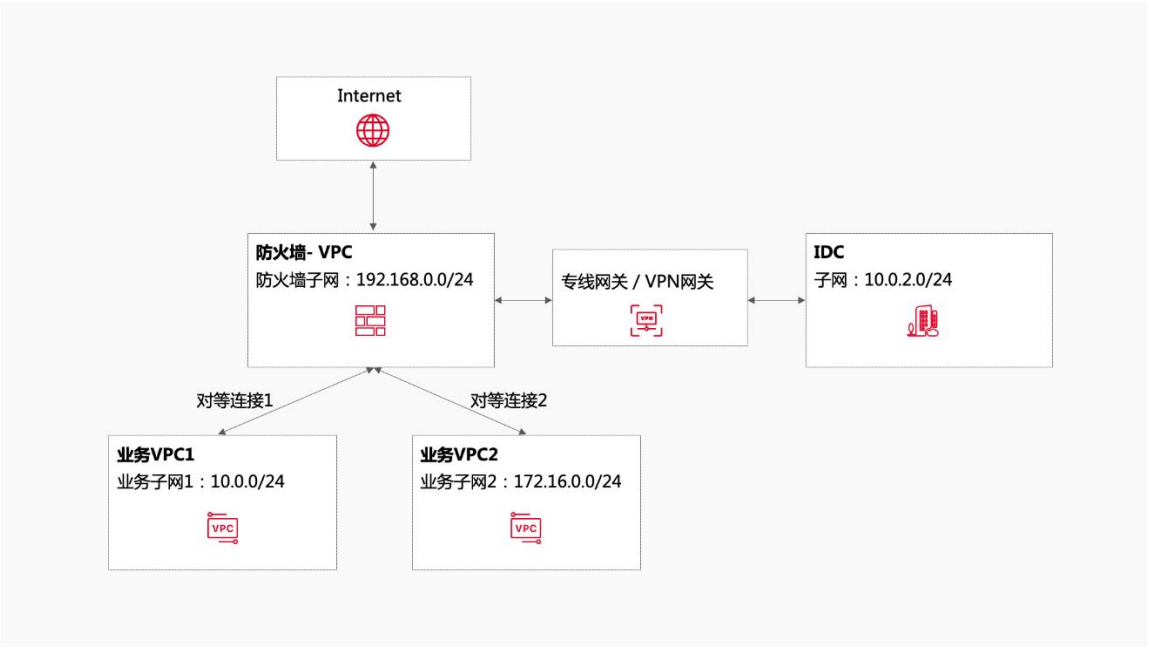
如何通过对等连接部署第三方公共防火墙

本文帮助您更快了解如何通过对等连接部署第三方公共防火墙。

注意事项

仅适用于多可用区资源池，实际情况以控制台展现为准，部署之前请检查资源池类型。

整体场景说明



前提条件

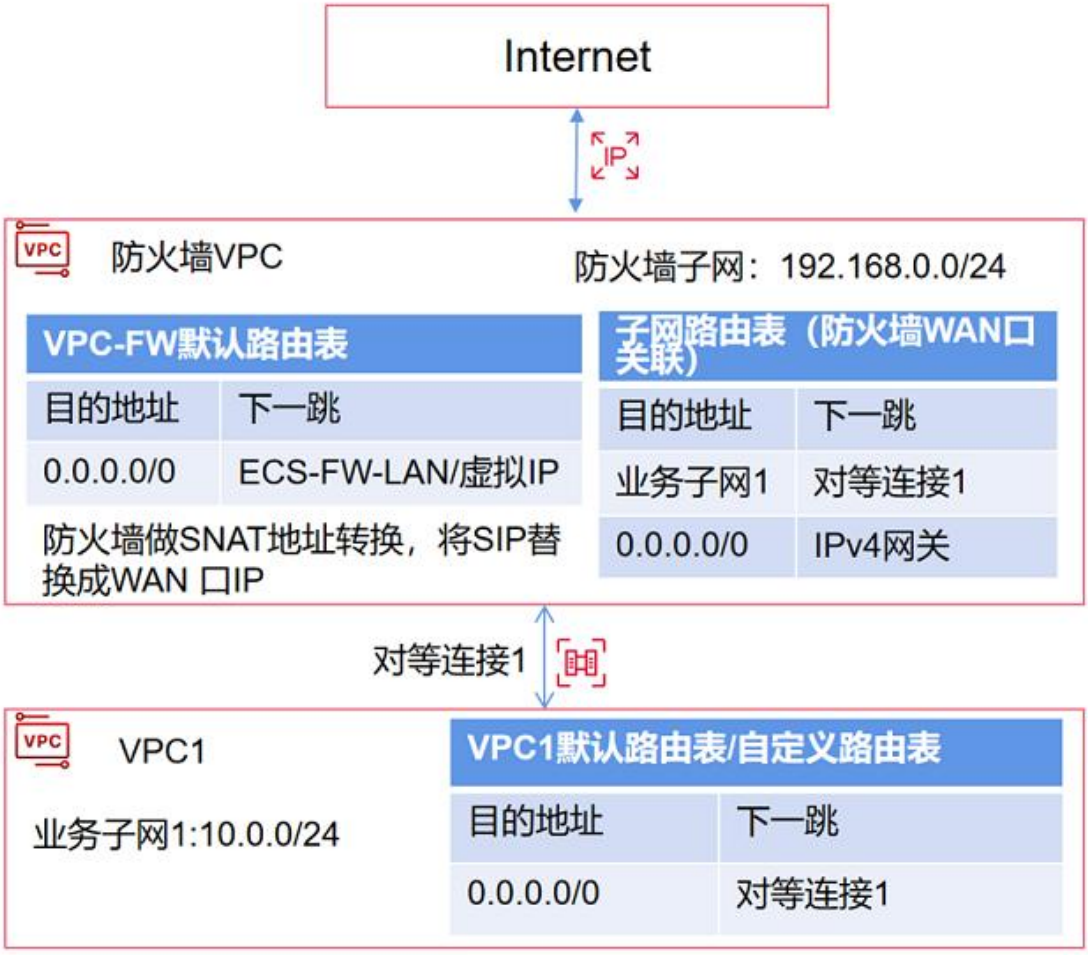
业务 VPC1 下的业务子网 1、业务 VPC2 下的业务子网 2、防火墙-VPC 下的防火墙子网三个网段不能重叠，否则建立对等连接后无法互通。

业务拓扑

- 业务 VPC1 为客户的业务主机所在的 VPC，业务主机的流量需要转发到防火墙 VPC 进行清洗。
- 客户的防火墙以云主机+防火墙镜像的方式部署在公共的防火墙 VPC。
- 业务 VPC1 和防火墙 VPC 建立对等连接 1；业务 VPC2 和防火墙 VPC 建立对等连接 2。

- 业务 VPC1 或者业务 VPC2 通过对等连接进入防火墙 VPC 进行流量清洗，然后防火墙 VPC 将流量转发至公网、线下 IDC；业务 VPC1 和业务 VPC2 互访的流量进入防火墙 VPC 进行清洗。

场景 1：访问公网的流量通过公共 VPC 防火墙进行清洗



基本场景介绍

对外访问的 EIP 绑定在防火墙的 WAN 口 IP 上。

防火墙做针对去 Internet 的做 SNAT，从而使得内部多个 VPC 共同使用 FW 上的 EIP 出公网。

业务 VPC 的 IP 地址不能重叠。

流量路径

从南往北，从业务 VPC1 到 Internet

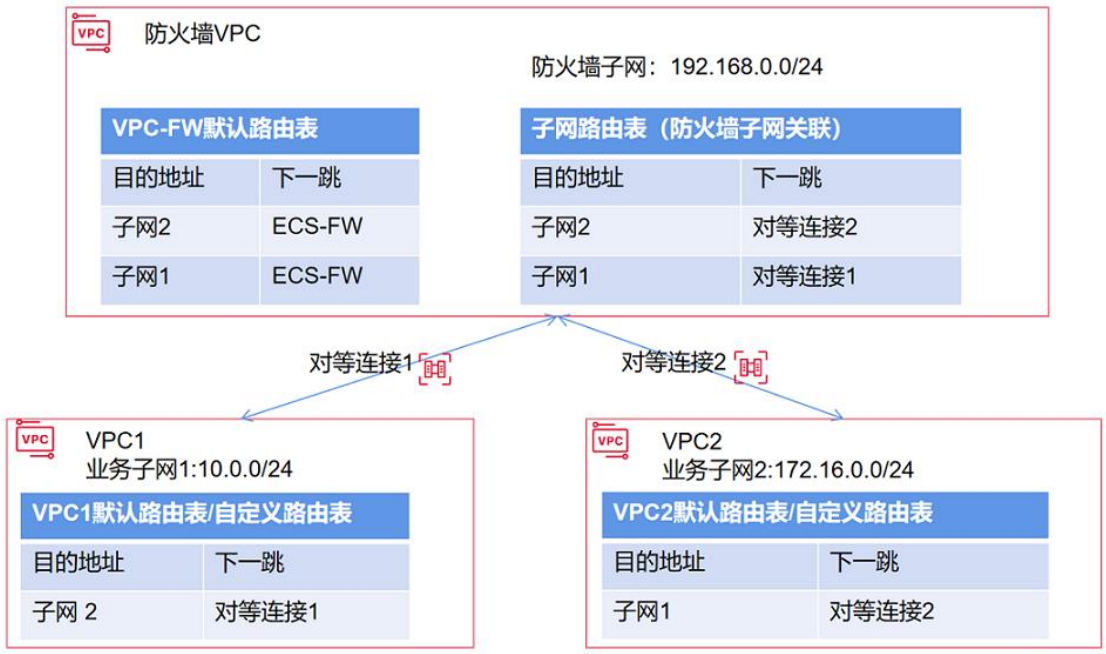
1. VPC1 的默认路由表或者自定义路由表均可。
2. 匹配 0.0.0.0/0，下一跳为对等连接。
3. VGW 虚拟网关将流量发给 VPC-FW。
4. VPC-FW 收到后匹配 VPC-FW 默认路由表，匹配 0.0.0.0/0 下一跳为 FW-LAN 口或者虚拟 IP 。
5. FW 做 SNAT 地址转换，将 SIP 替换成 WAN VIP， 并将流量从 FW-WAN 口送出。
6. FW WAN 口绑定了自定义子网路由表，匹配 0.0.0.0/0 下一跳为 IPv4 网关。
7. IPv4 网关收到报文后做 NAT 转换，将 SIP 从 FW 的 WAN VIP 替换成 EIP，送至 Internet。

从北往南，从 Internet 到 VPC1 的虚拟机

1. 流量的目的地址为 EIP，到达 IPv4 网关后，IPv4 网关将目的地址替换成 FW WAN 口 IP。
2. FW WAN 口收到后，做 NAT 转换，替换为 VPC1 的虚拟机 IP 地址。并从 FW LAN 口送出。
3. FW LAN 口绑定了子网自定义路由表，匹配 10.0.0.0/24，下一跳为对等连接。
4. VGW 虚拟网关收到后，送给 VPC1。

5. VPC1 默认路由表转发至虚拟机。

场景 2: 访问其他 VPC 的流量通过公共 VPC 防火墙进行清洗



基本场景介绍

业务子网 1 访问公网的流量进入防火墙 VPC 进行流量清洗。

业务 VPC1 下的业务子网 1:10.0.0.0/24。

防火墙 VPC 下防火墙云主机所在的子网：192.168.0.0/24。

操作步骤

1. 业务 VPC1 和防火墙 VPC 建立对等连接。
   - 在业务 VPC1 下的默认路由表或者自定义路由表下，创建路由规则如下：

     目的地址: 0.0.0.0，下一跳: 对等连接 1

     将子网 1 关联至默认路由表或者自定义路由表。

- 在防火墙 VPC 下创建自定义路由表(不能选择默认路由表)，并建立如下路由规则：

  目的地址业务子网 2 下一跳：对等连接 1

  将防火墙子网和自定义路由表做关联。

2. 业务 VPC2 和防火墙 VPC 建立对等连接。
   - 在业务 VPC2 下的默认路由表或者自定义路由表下，创建路由规则如下：

     目的地址：192.168.0.0/24（防火墙子网）下一跳：对等连接 2

     将子网 2 关联至默认路由表或者自定义路由表
   - 在防火墙 VPC 下的自定义路由表（不能选择默认路由表），并建立如下路由规则：

     目的地址：172.16.0.0/24（子网 2） 下一跳：对等连接 2

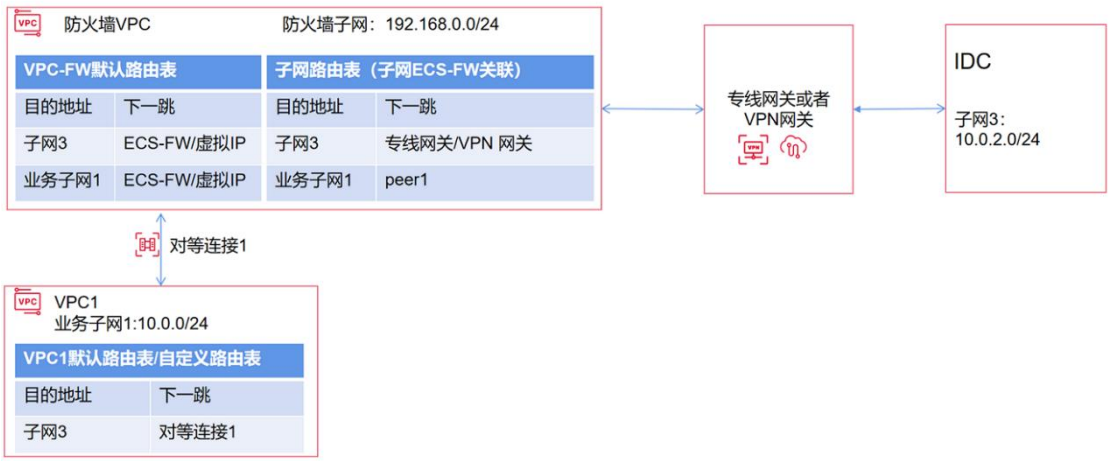
     将防火墙子网和自定义路由表做关联
3. 配置防火墙 VPC 的默认路由表，将流量引到防火墙云主机

   目的地址：172.16.0.0/24（子网 2） 下一跳：防火墙云主机或者虚拟 IP（虚拟 IP 绑定多个防火墙做高可用)

   目的地址：10.10.0.0/24（子网 1） 下一跳：防火墙云主机或者虚拟 IP（虚拟 IP 绑定多个防火墙做高可用)

   注意：防火墙子网不能关联默认路由表

场景 3：访问线下 IDC 的流量通过公共 VPC 防火墙进行清洗



基本场景介绍

业务子网 1 访问线下 IDC 子网 3 的流量进入防火墙 VPC 进行流量清洗。

业务 VPC1 下的业务子网 1:10.0.0.0/24。

防火墙 VPC 下防火墙云主机所在的子网：192.168.0.0/24。

线下 IDC 侧的子网 3:10.0.2.0/24。

操作步骤

1. 业务 VPC1 和防火墙 VPC 建立对等连接。
    - 在业务 VPC1 下的默认路由表或者自定义路由表下，创建路由规则如下：
    - 目的地址：10.0.2.0/24（子网 3），下一跳：对等连接 1。
    - 将子网 1 关联至默认路由表或者自定义路由表
    - 在防火墙 VPC 下创建自定义路由表（不能选择默认路由表），并建立如下路由规则：
    - 目的地址：10.0.0.0/24（子网 1），下一跳：对等连接 1。

- 将防火墙子网和自定义路由表做关联。

2. 配置防火墙 VPC 的默认路由表，将流量引到防火墙云主机，创建路由规则如下：
   - 目的地址 ：10.10.2.0/24（子网 3），下一跳：防火墙云主机或者虚拟 IP（虚拟 IP 绑定多个防火墙做高可用）。
   - 目的地址 ：10.0.0.0/24（子网 1），下一跳：防火墙云主机或者虚拟 IP（虚拟 IP 绑定多个防火墙做高可用）。
3. 在防火墙子网的自定义路由表配置路由，将流量引到专线网关/VPN 网关。
   - 在防火墙 VPC 下的自定义路由表中添加指向专线网关/VPN 网关的路由规则，具体如下：
   - 目的地址：10.0.2.0/24（子网 3），下一跳：专线网关/VPN 网关。
   - 将防火墙子网和自定义路由表做关联。注意，防火墙子网不能关联默认路由表。
   - 专线/VPN 配置完成后，系统会自动将目的地址为：子网 3；下一跳：为专线网关/VPN 网关；同步至默认路由表且无法删除，此时默认路由表未关联防火墙子网，不会真正进行引流。