弹性公网 IP

最佳实践

文档版本 01

发布日期 2025-01-17

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 公网访问

公网产品

公有云提供弹性公网IP（EIP）、NAT网关、弹性负载均衡（ELB）等方式连接公网。

- EIP

  EIP提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。拥有多种灵活的计费方式，可以满足各种业务场景的需要。

- ELB

  ELB将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用容错。为负载均衡器配置需要监听的端口信息以及弹性云服务器，通过监听器来检查后端弹性云服务器的运行状态，确保将请求发送到正常的弹性云服务器上，提高系统可用性。

- NAT网关

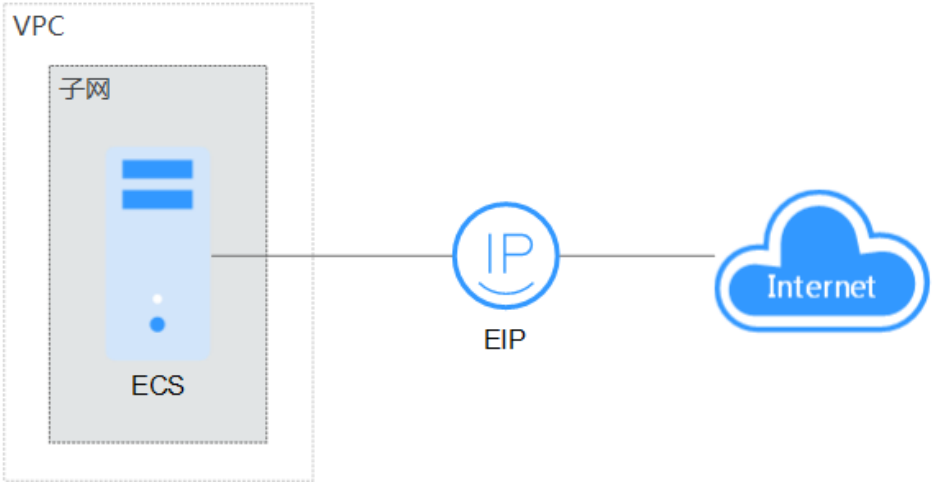
  NAT网关能够为VPC内的弹性云服务器提供SNAT和DNAT功能，通过灵活简易的配置，即可轻松构建VPC的公网出入口。

对外提供服务

- 单个ECS对外提供服务

  当您仅有单个应用服务，业务量较小时，您可申请一个EIP，绑定到ECS上，该ECS即可连接公网提供服务。

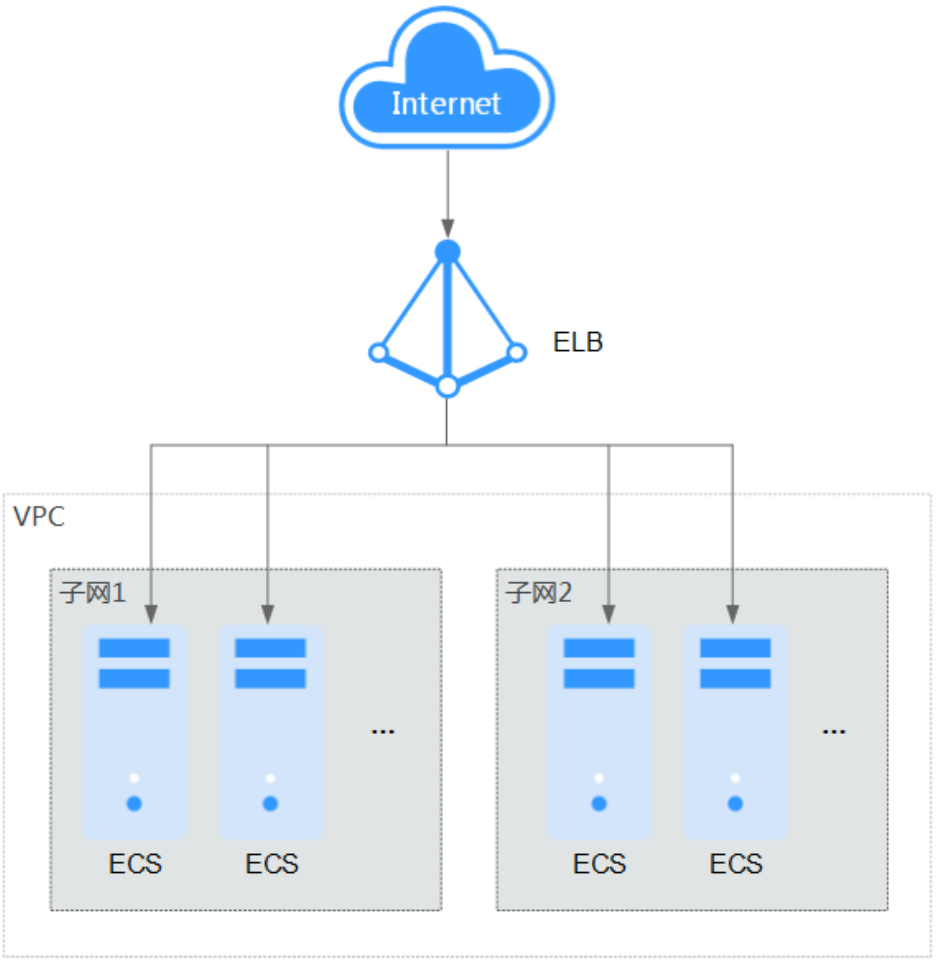
图 1-1 EIP



- 多个ECS负载均衡

  对于电商等高并发访问的场景，您可以通过ELB将访问流量均衡分发到多台弹性云服务器上，支撑海量用户访问。华为云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。

图 1-2 ELB

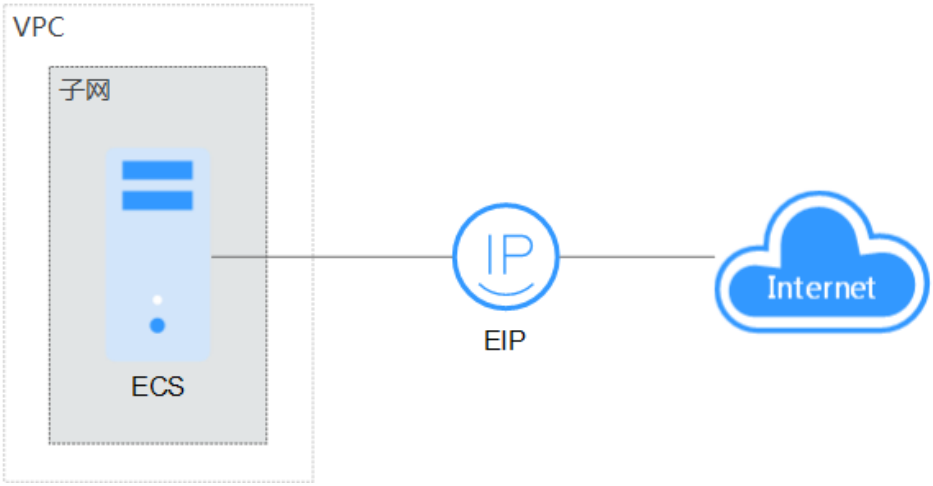


主动访问公网

- 单个ECS访问公网

  当您的某台ECS需要主动访问公网，可以为ECS绑定EIP，即可实现公网访问。华为云提供多种计费方式（按需等）供您选择，无需使用时支持灵活解绑。

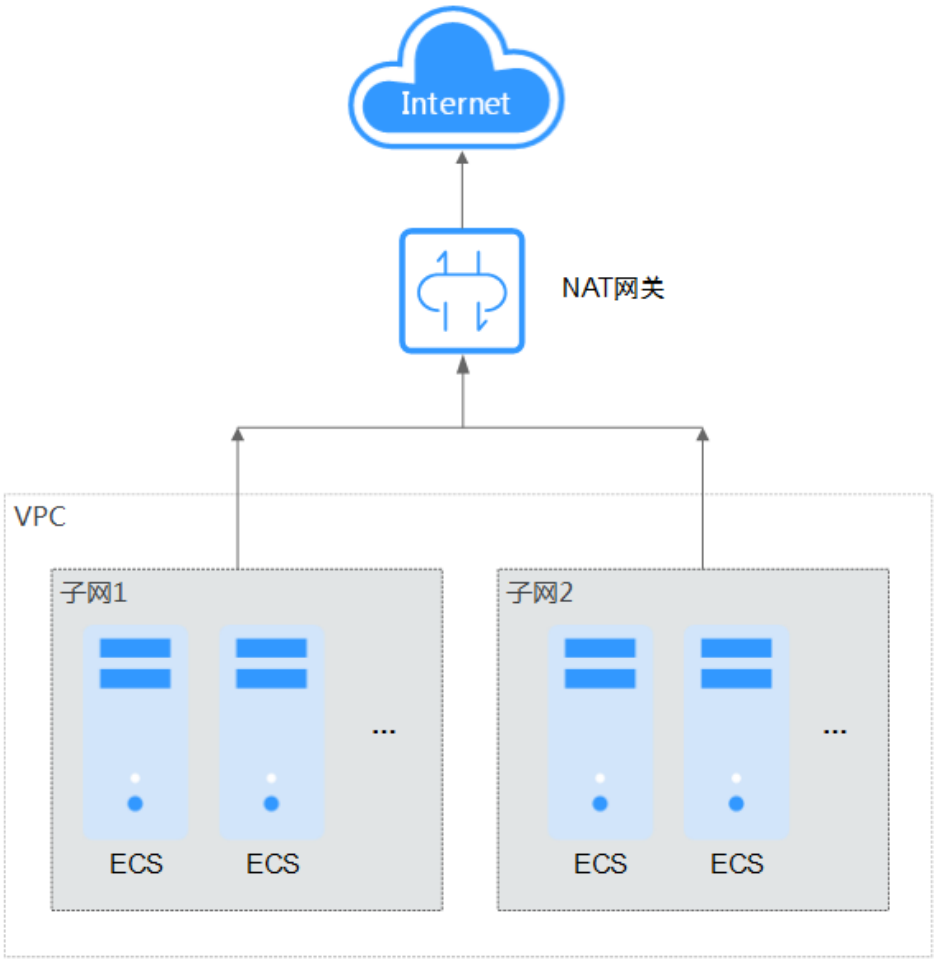
  图 1-3 EIP

- 多个ECS访问公网

  当您的VPC内ECS都有公网访问需求时，可以使用NAT网关服务，按子网配置SNAT规则，轻松构建VPC的公网出口。对比EIP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ECS的相对安全。

图 1-4 NAT 网关



2 节约公网成本

在您购买带宽产品之前一定要分析您业务系统的流量模型，以便选择适合的产品及计费模式。

独享带宽

如您需要保证单个弹性公网IP的带宽大小，建议您购买独享带宽。独享带宽只针对单个弹性公网IP进行限速，不受其他业务影响。

支持两种计费模式：

- 按带宽计费：针对流量使用较大且比较稳定的业务。
- 按流量计费：针对流量使用相对较小的业务，搭配共享流量包使用价格更优惠。

对于流量比较稳定，没有突发流量的系统可以考虑选择预付费的按带宽计费模式，可以比正常后付费按带宽计费享受更多价格优惠。

共享带宽

当您有大量业务在云上时，如果每个ECS单独使用一条独享带宽，则需要较多的带宽实例，并且总的带宽费用会较高，如果所有实例共用一条带宽，就可以节省企业的网络运营成本，同时方便运维统计。共享带宽是独立的带宽产品，支持将多个按需计费的弹性公网IP添加到共享带宽，对多个弹性公网IP进行集中限速。您可以将EIP绑定到ECS、NAT网关、ELB等产品，从而使这些产品使用共享带宽。

支持两种计费模式：

- 按带宽计费：如果您使用的弹性公网IP较多，并且错峰明显，使用共享带宽可以大幅节约成本。
- 按增强型95计费：如果您部署的业务经常有突发峰值，可以选择增强型95计费。既可以保证业务系统不受峰值带宽不够的影响，又可以避免带宽峰值设置过大带来的成本浪费。

共享流量包

共享流量包是公网流量的预付费套餐，价格比后付费流量更低，大大降低了公网流量成本。共享流量包购买后立即生效，自动抵扣**按需计费（按流量计费）**的EIP带宽产生的流量资费，使用简单，无需额外操作。

- 共享流量包适用哪些场景?

  对于按流量计费的带宽，启用共享流量包后，该带宽所产生的流量费用优先从共享流量包中进行抵扣。共享流量包全部使用完后，再按后付费流量进行结算。从节约成本的角度看，流量越大，节省的成本越多。

- 共享流量包使用说明
  - 只能抵扣同一区域产生的带宽流量，不支持跨区域抵扣。
  - 共享流量包包括动态和静态两种类型，分别抵扣全动态BGP和静态BGP产生的流量。
  - 共享流量包具有使用有效期（从购买开始计算1个自然月或1个自然年）。超过有效期后，没有使用完的流量无法继续使用。建议根据业务系统历史情况仔细评估需要多少共享流量包。
  - 共享流量包支持自动续费功能。如果您开通了自动续费功能，那么共享流量包到期前7天内，系统会尝试自动续费扣款，续费成功后，共享流量包中剩余的流量可以在新的有效期内继续使用。
  - 共享流量包全部使用完后，系统会自动按后付费流量进行结算，不会导致业务系统无法使用。

带宽加油包

带宽加油包用来临时调大带宽上限，适用于在有效期内的**包年/包月**独享带宽和共享带宽。当需要在一个时间段内临时调整带宽规格，您可以购买带宽加油包并设置有效期时间。使用带宽加油包不会影响业务中断，也不需要重启实例。

- 带宽加油包适用哪些场景?

  对于包年/包月的带宽，当某个时间段业务量激增（例如：双11），需要在这个时间段临时调整带宽规格，您可以通过购买带宽加油包，设置有效期时间来解决。

- 带宽加油包使用说明
  - 在购买带宽加油包时，如果您有未支付的带宽加油包订单，则无法购买新的带宽加油包。请取消未支付订单或支付订单后再购买新的带宽加油包。
  - 带宽加油包1天起售，购买后不能修改起始时间及带宽大小。
  - 带宽加油包是从购买时选择的有效期开始时间生效的，根据您设置的有效期时间，带宽加油包支持购买后立即生效。
  - 带宽加油包到期将自动失效，带宽恢复到原来的规格。
  - 在部分区域内，带宽加油包支持在有效期内叠加使用，具体以控制台显示为准。

    如果您购买带宽加油包后，带宽还是不能满足要求，可以再次购买带宽加油包叠加使用。

3 通过 EIP 实现线下 IDC 对外提供 IPv6 服务

应用场景

当已有的IPv4地址的弹性公网IP需要增加IPv6地址时，可以使用弹性公网IP（EIP）服务的IPv6转换功能即可将已有的IPv4地址映射为公网IPv6地址。开启IPv6转换后，将提供IPv4和IPv6弹性公网IP地址，原有IPv4业务可以快速为IPv6用户提供访问能力。

假设后端服务器在用户线下数据中心（IDC），现有IPv4服务无法快速上云，或短期内无法完成IPv6双栈改造，则可以使用IPv6 EIP快速对接线下IDC，对外提供IPv6能力，不必改造IDC内部IPv4网络，快速支持IPv6的用户接入，保证IPv4和IPv6用户的不同需求。

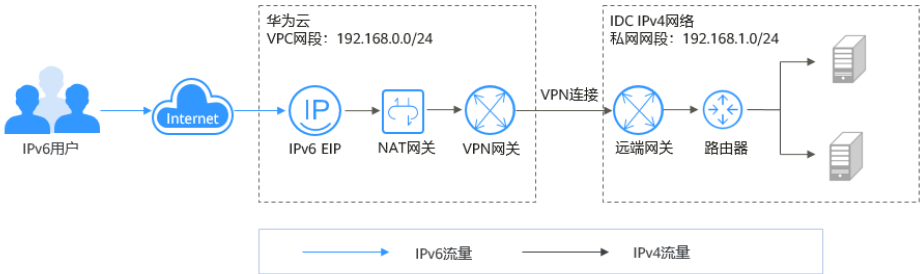
方案架构

1. 通过虚拟专用网络（VPN）将用户IDC与VPC连通。
2. 在VPC中搭建NAT网关，并绑定IPv6 EIP，对外提供公网IPv6服务。

说明

- IPv6 EIP只能作为服务端地址对外提供服务，无法主动访问IPv6地址。
- IDC的网段与云上VPC中的子网网段不能重叠，否则无法通信。

图 3-1 组网图



方案优势

不必改造IDC内部IPv4网络，就可以快速支持IPv6的用户接入，保证IPv4和IPv6用户的不同需求。

约束与限制

开启EIP的IPv6转换后，您需要在安全组的出方向和入方向中放通198.19.0.0/16网段的IP地址。因为IPv6弹性公网IP采用NAT64技术，入方向的源IP地址经过NAT64转换后，会将IPv6地址转换为198.19.0.0/16之间的某个IPv4地址，源端口随机，目的IP为本机的内部私有IPv4地址，目的端口不变。

表 3-1 安全组规则

方向	协议	端口和地址
入方向	全部	源地址：198.19.0.0/16
出方向	全部	目的地址：198.19.0.0/16

资源和成本规划

表 3-2 资源和成本规划

资源	资源名称	资源说明	数量
虚拟私有云（VPC）	VPC-Test01	在该VPC中购买EIP、NAT网关，VPC网段为：192.168.0.0/24	1
弹性公网IP（EIP）	EIP-IPv4&IPv6	IPv4地址的弹性公网IP,，需开启IPv6转换。	1
NAT网关	NAT-Test	需购买公网NAT网关，并绑定弹性公网IP。	1
VPN网关	VPN-GW-Test	VPN网关是VPC中建立的出口网关设备，通过VPN网关可建立VPC和IDC之间安全可靠的加密通信。	1
VPN连接	VPN-Test	VPN连接帮您快速构建VPN网关和远端网关之间的安全、可靠的加密通道。	1
用户线下数据中心（IDC）	IDC-Test	包含远端网关、路由器、后端服务器。该IDC私网网段为：192.168.1.0/24	1

操作流程

1. **购买EIP并开启IPv6转换。**
2. **配置VPN。**
3. **配置公网NAT网关。**

实施步骤

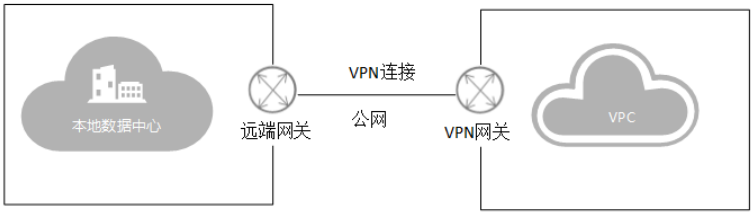
1. **购买EIP并开启IPv6转换**

   根据出公网的实际业务需求，购买相应带宽的弹性公网IP并勾选IPv6转换。

   具体操作请参见**申请弹性公网IP**。

2. **配置VPN**

   VPN由VPN网关和VPN连接组成，VPN网关提供了虚拟私有云的公网出口，与用户IDC的远端网关对应。

   a. 创建VPC。

      创建VPC，选择网段为192.168.0.0/24，IDC私有网段为192.168.1.0/24。

      IDC的网段与云上VPC中的子网网段不能重叠，否则无法通信。

      具体操作请参见**创建虚拟私有云和子网**。

   b. 创建VPN网关。

      虚拟私有云：选择**2.a**中创建的VPC。

      带宽大小：根据实际的业务需求，选择VPN连接需要的带宽大小。

      具体操作请参见**创建VPN网关**。

   c. 创建VPN连接。

      本端子网：选择网段，手动输入网段：192.168.0.0/24,198.19.0.0/16。

      远端网关：选择线下IDC的VPN远端公网IP。

      远端子网：选择线下IDC的私有网段192.168.1.0/24。

      具体操作请参见**创建VPN连接**。

      说明

      由于EIP开启IPv6转换后，源IP会被替换成198.19.0.0/16网段，因此需要将该网段加入到本端子网中。由于Console页面的校验，需要先填写VPC的子网，再填写198.19.0.0/16。

   d. 配置IDC侧VPN设备。

      完成云端的VPN配置后，需要对线下IDC侧的VPN设备进行相应配置，具体操作请参见**《虚拟专用网络管理员指南》**。

3. **配置公网NAT网关**

   购买公网NAT网关，通过添加DNAT规则，可以通过映射方式使您的云主机或通过VPN扩展到云上的主机为互联网提供服务。

   a. 购买公网NAT网关。

      虚拟私有云：选择**2.a**中创建的VPC。

      子网：选择**2.a**中创建的VPC下的子网。

      具体操作请参见**购买公网NAT网关**。

   b. 添加DNAT规则。

选择1中购买的EIP，并根据线下IDC的私网IP地址和端口，设置DNAT规则。例如选择具体端口及TCP协议，添加私网IP：192.168.1.22，绑定EIP。

具体操作请参见**添加DNAT规则**。

配置验证

操作完成后，就可以实现EIP服务的公网IPv6地址对外提供IPv6服务。

IPv6地址可以在EIP页面查询：

图 3-2 查看 IPv6 地址

使用具有访问公网能力的IPv6客户端，测试IPv6 EIP的IPv6地址的连通性。