虚拟私有云

产品介绍

文档版本 49

发布日期 2021-08-09

华为技术有限公司

版权所有 © 华为技术有限公司 2021。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

目 录

1 网络服务概述 1
1.1 华为云网络全景 1
1.2 网络规划和设计 8
1.3 网络安全 13
1.4 网络监控 17
2 什么是虚拟私有云 19
3 产品优势 21
4 应用场景 24
5 功能总览 29
6 约束与限制 34
7 与其他服务的关系 40
8 计费说明 42
9 权限管理 45
10 基本概念 48
10.1 子网 48
10.2 弹性公网 IP 48
10.3 路由表 49
10.4 安全组 52
10.5 对等连接 53
10.6 网络 ACL 55
10.7 虚拟 IP 57
10.8 弹性网卡 59
10.9 二层连接网关 60
10.10 IP 地址组 61
10.11 区域和可用区 61

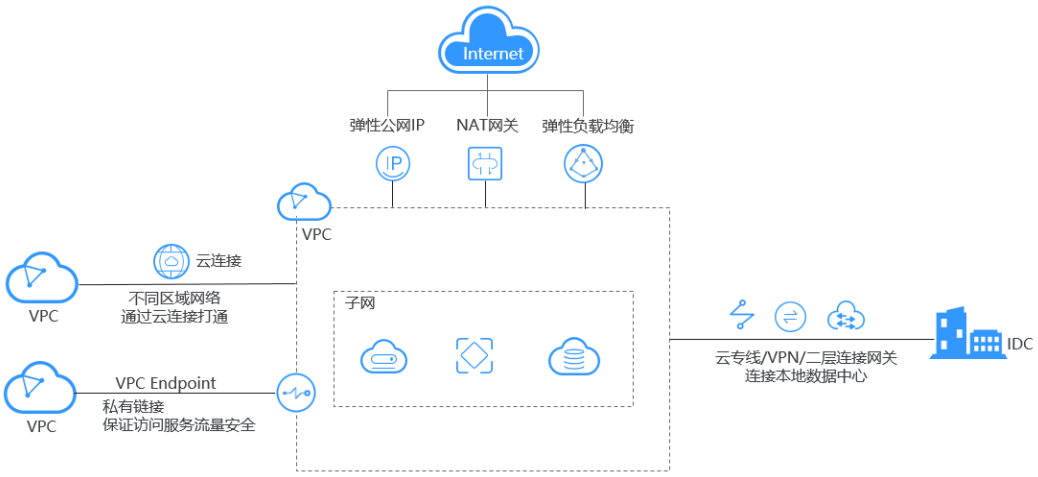
 版权所有 © 华为技术有限公司

1 网络服务概述

1.1 华为云网络全景

华为云拥有丰富的网络服务，提供安全、可扩展的云上网络环境，同时提供了高速、可靠的云上云下连接服务，能够方便的连接互联网和本地数据中心。

图 1-1 华为云网络全景



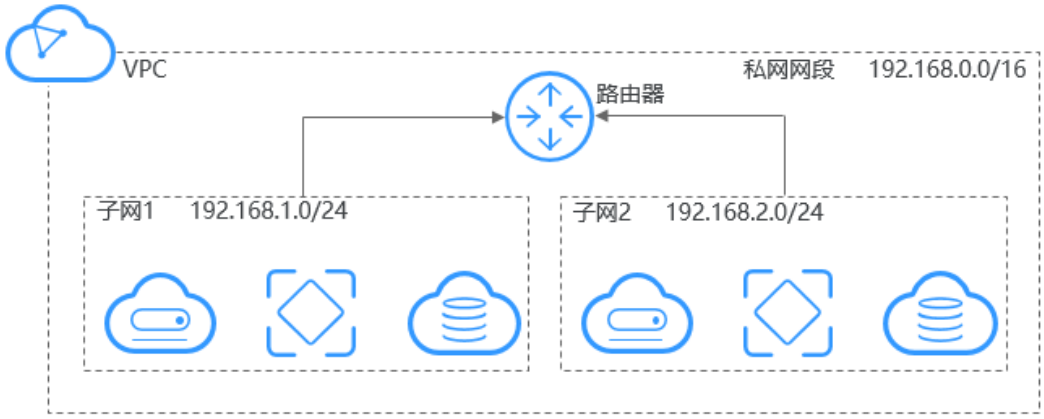
虚拟私有云 VPC

虚拟私有云（Virtual Private Cloud，以下简称VPC），为云服务器、云容器、云数据库等资源构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。

每个VPC由一个私网网段、路由表和至少一个子网组成。用户在创建VPC时需要指定私网网段，且云资源必须部署在子网内，系统会自动生成默认路由表，保证同一个VPC下的所有子网互通。

版权所有 © 华为技术有限公司

图 1-2 VPC



VPC为云上资源提供隔离的虚拟网络环境，同时VPC能配合其他网络服务也提供了强大的网络连接功能：

- 与互联网连接

  通过**弹性公网IP**，VPC中的资源都能与互联网连接通信；还可以通过**NAT网关**的网络地址转换能力，使得VPC内多个资源共享弹性公网IP。
- 与本地数据中心网络连接

  通过**云专线DC**、**虚拟私有网络VPN**、**L2CG**，可以构建VPC与本地数据中心的连接。
- 云上VPC相互连接

  通过**VPC对等连接**功能，VPC可以与同一个区域之间其他VPC之间建立对等连接。

  通过**云连接CC**服务，可以在不同区域的VPC之间建立高速、稳定的网络连接。

VPC的详细信息请参见**什么是虚拟私有云**。

弹性公网 IP

弹性公网IP（Elastic IP，简称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。

使用弹性公网IP，除了给公网IP固定带宽和流量外，还有如下三种套餐：

- 共享带宽

  共享带宽可以实现多个弹性公网IP共同使用一条带宽。提供区域级别的带宽共享及复用能力，同一区域下的所有已绑定弹性公网IP的弹性云服务器、裸金属服务器、弹性负载均衡等实例共用一条带宽资源。
- 共享流量包

  共享流量包是一款带宽流量套餐产品，使用方便，价格实惠。购买共享流量包后立即生效，并自动抵扣按需按流量计费的EIP带宽产生的流量资费，直到流量包用完或到期。
- 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。

EIP的详细信息请参见**什么是弹性公网IP**。

版权所有 © 华为技术有限公司

NAT 网关

公网NAT网关

NAT网关（NAT Gateway）能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器、云桌面）或者通过云专线/VPN接入虚拟私有云的本地数据中心的服务器，提供最高10Gbit/s能力的网络地址转换服务，使多个云主机可以共享弹性公网IP访问Internet或使云主机提供互联网服务。

NAT网关提供SNAT和DNAT功能：

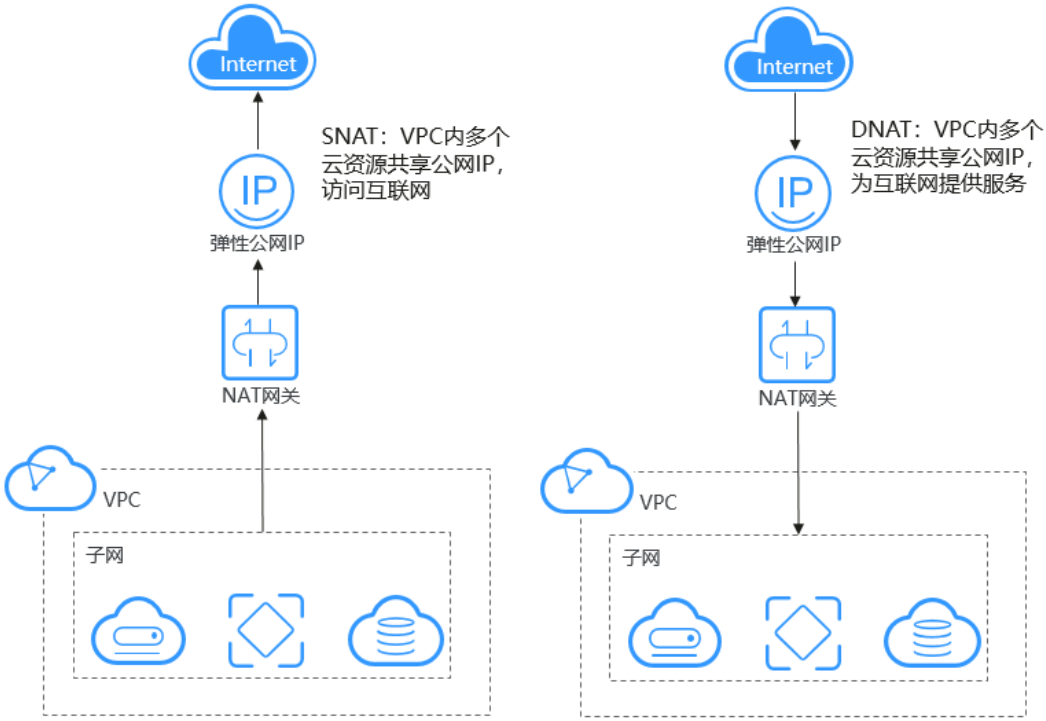
- SNAT

  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

  DNAT功能绑定弹性公网IP，可通过IP映射或端口映射两种方式，实现VPC内跨可用区的多个云主机共享弹性公网IP，为互联网提供服务。

图 1-3 公网 NAT 网关



私网NAT网关

私网NAT网关（Private NAT Gateway）能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器、云桌面）提供网络地址转换服务，使多个云主机可以共享私网IP访问用户本地数据中心（IDC）或其他虚拟私有云，同时，也支持云主机面向私网提供服务。

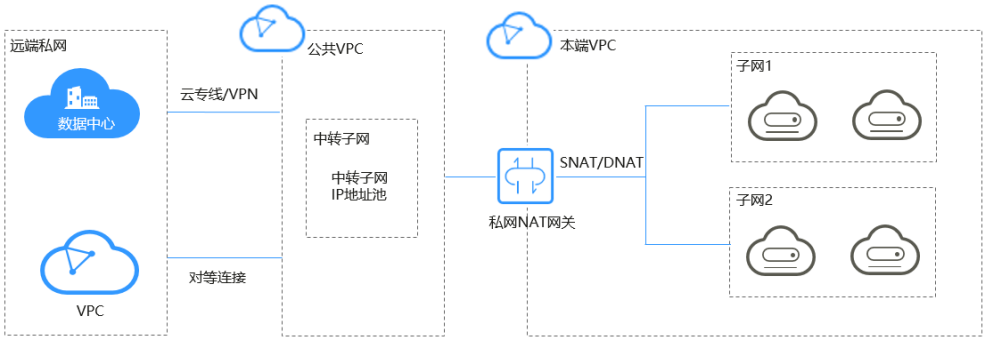
私网NAT网关支持大小网段灵活组网，IP网段可重叠，业务零改造，可降低企业上云的成本和风险。

私网NAT网关也分为SNAT和DNAT两个功能：

版权所有 © 华为技术有限公司

- SNAT功能通过绑定中转IP，可实现VPC内跨可用区的多个云主机共享中转IP，访问外部数据中心或其他VPC。
- DNAT功能绑定中转IP，可通过IP映射或端口映射两种方式，实现VPC内跨可用区的多个云主机共享中转IP，为外部私网提供服务。

图 1-4 私网 NAT 网关

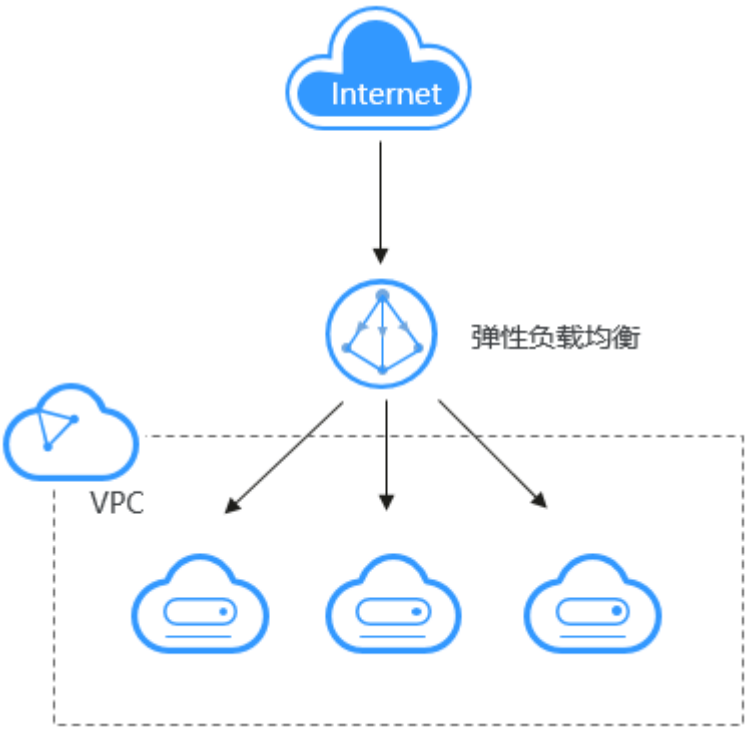


NAT网关的详细信息请参见**什么是NAT网关**。

弹性负载均衡 ELB

弹性负载均衡（Elastic Load Balance，简称ELB）是将访问流量根据转发策略分发到后端多台服务器的流量分发控制服务。弹性负载均衡可以通过流量分发扩展应用系统对外的服务能力，同时通过消除单点故障提升应用系统的可用性。

图 1-5 弹性负载均衡



版权所有 © 华为技术有限公司

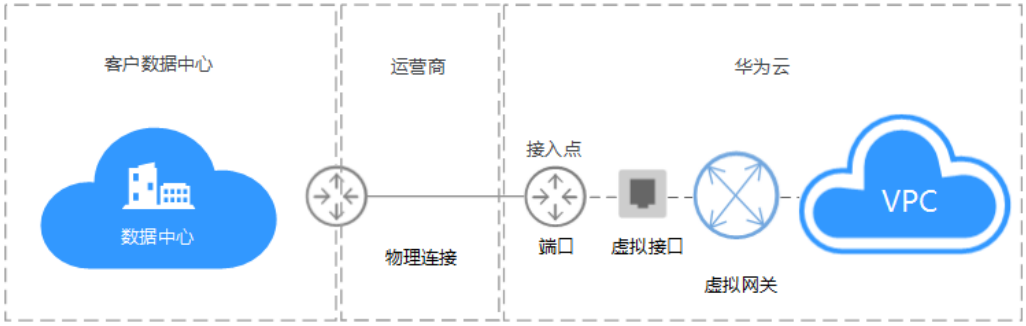
ELB的详细信息请参见**什么是弹性负载均衡**。

云专线 DC

云专线（Direct Connect）为用户搭建本地数据中心与云上VPC之间的专属连接通道，实现高速、稳定、安全可靠的混合云部署。

云专线是专用连接，流量不经过互联网。

图 1-6 云专线物理连接



云专线提供以下物理连接接入方式：

- 标准专线

  客户数据中心通过不同运营商专线，分别接入不同接入点，实现多链路多接入点互备，保障高可靠性。如果有特殊要求只能选择同一运营商，需确保不同物理路由。

  此方式独占华为云物理端口，您可以通过管理控制台自主申请物理连接。
- 托管专线

  用户本地数据中心通过合规运营商拉通专线，运营商和云专线接入点已做好专线预连接，运营商为用户分配上云连接。

  运营商和华为云连接端口是多租户共享的。

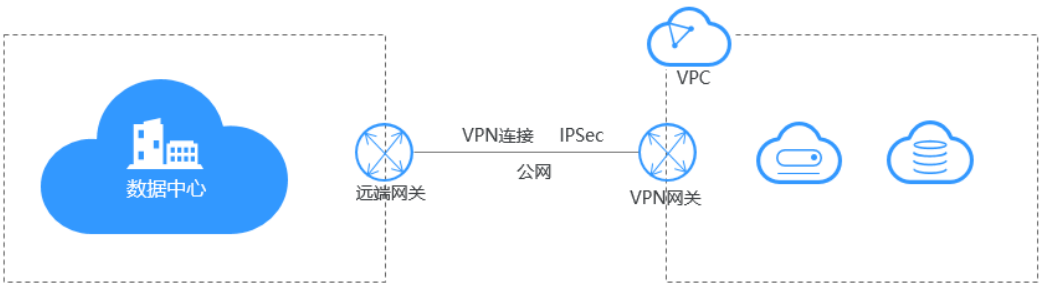
云专线的详细信息请参见**云专线产品概述**。

虚拟私有网络 VPN

虚拟专用网络（Virtual Private Network，以下简称VPN），用于在远端用户和VPC之间建立一条安全加密的公网通信隧道。当您作为远端用户需要访问VPC的业务资源时，您可以通过VPN连通VPC。

与云专线DC不同，VPN是在公网上构建的加密隧道网络，其流量经过互联网。

图 1-7 VPN 组网图



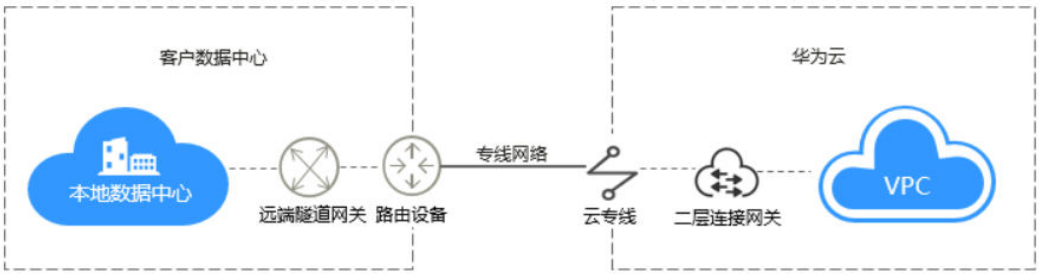
版权所有 © 华为技术有限公司

VPC 二层连接网关

二层连接网关（Layer 2 Connection Gateway，以下简称L2CG）是一种虚拟隧道网关，可基于云专线/VPN网络建立云上与云下之间的二层网络，解决云上和云下网络二层互通问题，允许您在不改变子网、IP规划的前提下将数据中心或私有云主机业务部分迁移上云。

通过云专线/VPN，建立的是云上与云下的三层网络通道，要求云上与云下子网网段不重叠。而当数据中心与云上子网网段相同，且需要云上与云下服务器在该相同子网网段互通时，您就可以通过二层连接网关来解决云上与云下二层网络通信问题。详细信息请参见**二层连接网关简介**。

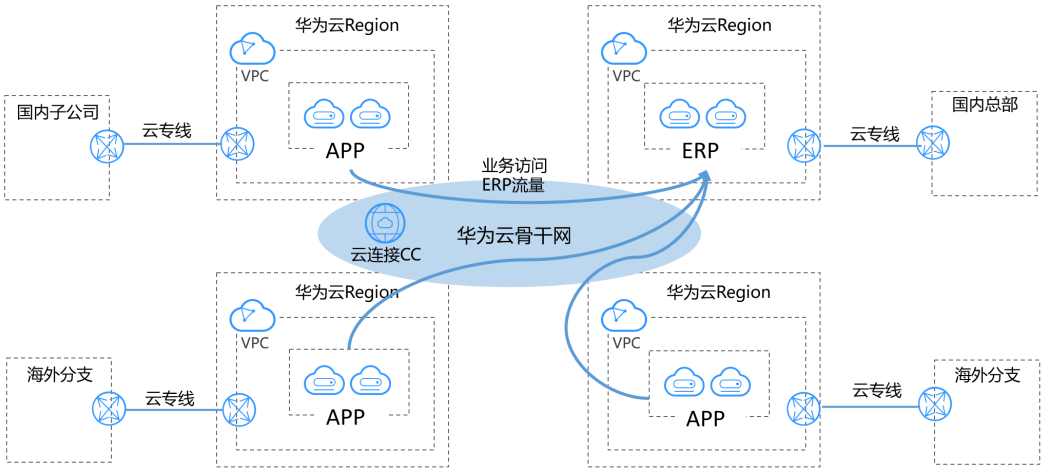
图 1-8 VPC 二层连接网关



云连接 CC

云连接（Cloud Connect）为用户提供一种能够快速构建跨区域VPC之间以及云上多VPC与云下多数据中心之间的高速、优质、稳定的网络能力，帮助用户打造一张具有企业级规模和通信能力的全球云上网络。

图 1-9 云连接组网



VPC 终端节点

VPC终端节点（VPC Endpoint），您能够将VPC私密地连接到云上服务，使VPC中的云资源无需弹性公网IP就能够访问终端节点服务，保证访问服务流量安全。

VPCEP主要用于如下几种场景：

版权所有 © 华为技术有限公司

- 在华为云内网开放服务

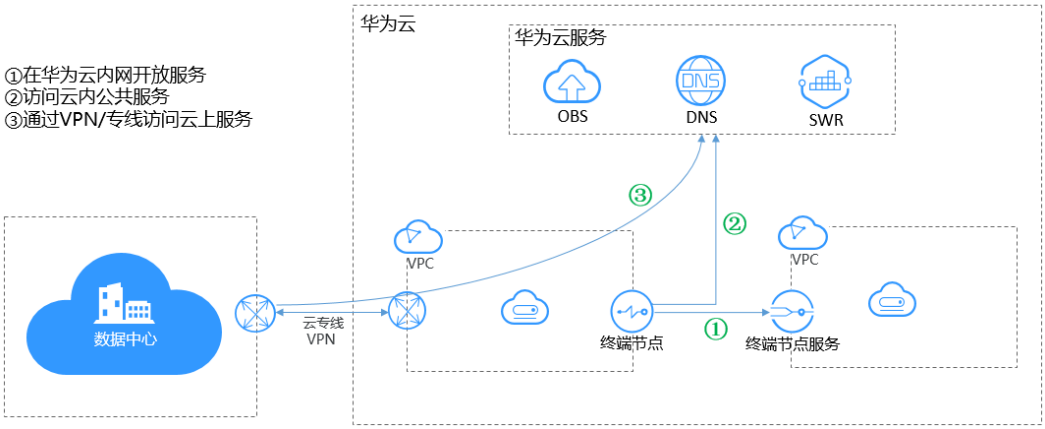
  通过创建VPC Endpoint Service暴露自己的服务。 支持将ELB、弹性云服务器、裸金属服务器上提供的服务开放到VPC。

  客户端通过VPC Endpoint作为接入点访问服务。
- 访问云内公共服务

  云服务注册VPC Endpoint Service，用户可以通过创建相应的VPC Endpoint访问云服务。
- 通过VPN/专线访问云上服务

  购买VPN/专线后，可以通过VPC Endpoint访问云 上的服务，打通云上/云下资源。如访问OBS、DNS、SWR等。

图 1-10 VPC 终端节点



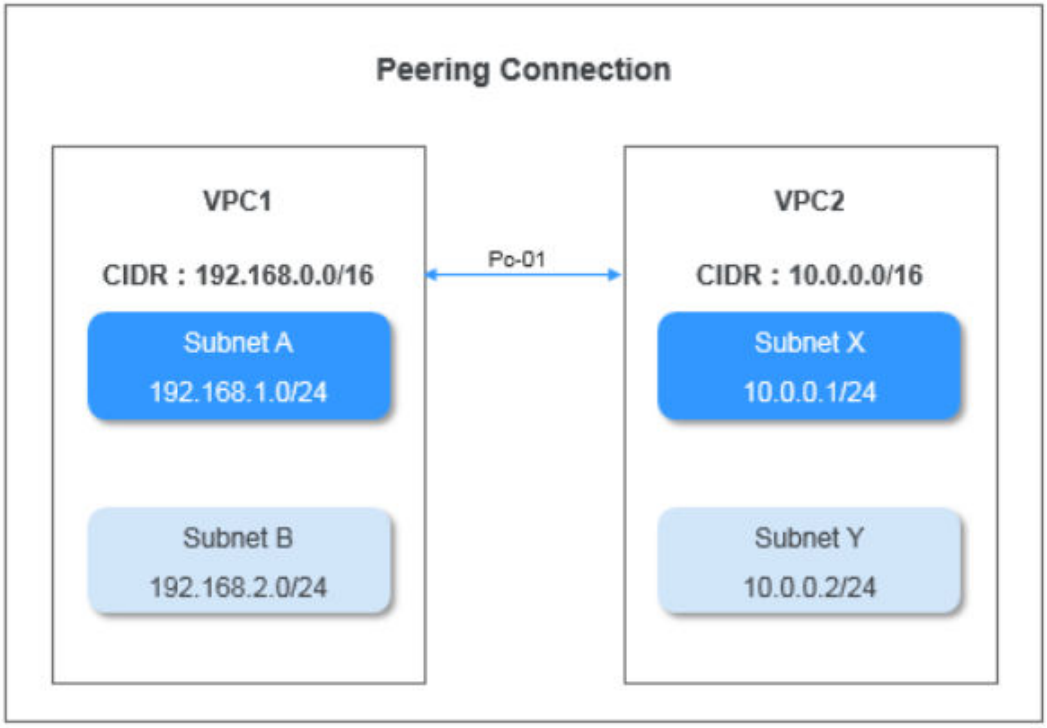
VPC 对等连接

不同VPC之间默认无法互访，可以通过对等连接功能连接VPC，使得VPC之间可以互相访问。您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。同一区域内，您可以在自己的VPC之间创建对等连接，也可以在自己的VPC与其他帐户的VPC之间创建对等连接。不同区域间的VPC之间不能创建对等连接。

详细的介绍与配置请参见**对等连接简介**和**对等连接路由配置方案**。

版权所有 © 华为技术有限公司

图 1-11 VPC 对等连接



对等连接与VPCEP的区别请参见**VPC终端节点和对等连接有什么区别？**。

1.2 网络规划和设计

在云上部署您的业务，不可避免的需要考虑您业务的网络规划和设计，通常网络的规划和设计需要考虑隔离性、扩展性、连接性几个方面的问题。

- **隔离性**

  在规划设计网络的时候，隔离性是最基本的要求。VPC拥有天然的网络隔离功能，默认情况下，不同区域的VPC之间内网不互通，同区域的不同VPC内网不互通。

  通常情况下，将不同业务放在不同VPC，不同部门使用不同VPC，不同环境（如开发、测试、生产）使用不同VPC。

  在VPC内，通过划分子网将IP地址分段，不同业务模块使用不同子网，且子网之间还可以通过网络ACL保证安全性。

- **扩展性**

  业务是不断变化的，在规划网络时，为防止业务快速增长给网络带来冲击，您需要考虑网络的扩展性，通常来说扩展性可从下面两个角度去考虑。

  - 在规划时要为业务预留足够的IP地址，即当需要扩容时要有IP地址可用，不仅要考虑整个业务，也要考虑到单个的业务模块。
  - 在规划时也要考虑如何在不同区域、不同VPC之间扩展，这点也与**连接性**相关。

- **连接性**

  网络的连接性与隔离性、扩展性息息相关，有些连接的需求就是由于隔离性和扩展性引起的，通常连接性需要考虑如下几个方面。

版权所有 © 华为技术有限公司

- VPC与外部互联网的连接。
- VPC之间的连接，包括同区域VPC，不同区域VPC的连接。
- 本地数据中心与云上VPC之间的连接。

上面阐述了网络规划设计的一些基本原则，下面将结合这些基本原则，从VPC规划、子网规划、互联网连接、VPC之间连接、本地数据中心与云上VPC连接几个方面来具体阐述网络规划设计的建议。

VPC 规划

VPC的规划可从如下几点进行考虑：

1. VPC在哪个区域创建通常根据业务靠近用户来决定。VPC具有区域属性，默认情况下，不同区域的VPC之间内网不互通，同区域的不同VPC内网不互通。
2. 决定创建一个VPC还是多个VPC，需要考虑的事项：
   - 业务是否单一，各业务之间没有网络隔离需求？通常会将不同业务部署在不同VPC，避免相互影响；如果只有单一业务，可只创建一个VPC。
   - 业务是否需要多套部署？通常企业会搭建多套环境，比如开发、测试、生产各一套，各有不同用途。
   - 是否对VPC中资源有权限管理的需求？如果有，可将资源分隔到单独的VPC中，从而简化组织中权限分配的管理工作。
3. VPC的网段选择，网段的选择有两点：
   - IP地址数量的考虑，要为业务预留足够的IP地址，防止业务扩展给网络带来冲击。
   - 与其他VPC、本地数据中心连接时，要避免IP地址冲突。

表 1-1 IP 地址数量

VPC网段	IP地址范围	最大IP地址数
10.0.0.0/8~24	10.0.0.0-10.255.255.255	2^24-2=16777214
172.16.0.0/12~24	172.16.0.0-172.31.255.255	2^20-2=1048574
192.168.0.0/16~24	192.168.0.0-192.168.255.255	2^16-2=65534

子网规划

子网是VPC内的IP地址块，VPC中的所有云资源都必须部署在子网内。同一个VPC下，子网网段不可重复。子网创建成功后，网段无法修改。

VPC支持的网段如下，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~29。

- 10.0.0.0/8~24
- 172.16.0.0/12~24
- 192.168.0.0/16~24

版权所有 © 华为技术有限公司

子网规划建议遵循如下原则：

- 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，不涉及和本地数据中心的网络通信，则可以选择上述任何一个网段进行新建子网。
- 如果要通过VPN/云专线与本地数据中心进行互通，本端网段（VPC网段）和对端网段（您的本地数据中心网段）不能重叠，所以在新建VPC及子网的时候务必避开对端网段。
- 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。

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。用户创建VPC时，系统会自动为其生成一个默认路由表，该默认路由表含义为VPC内网互通。

- 如果不需要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。

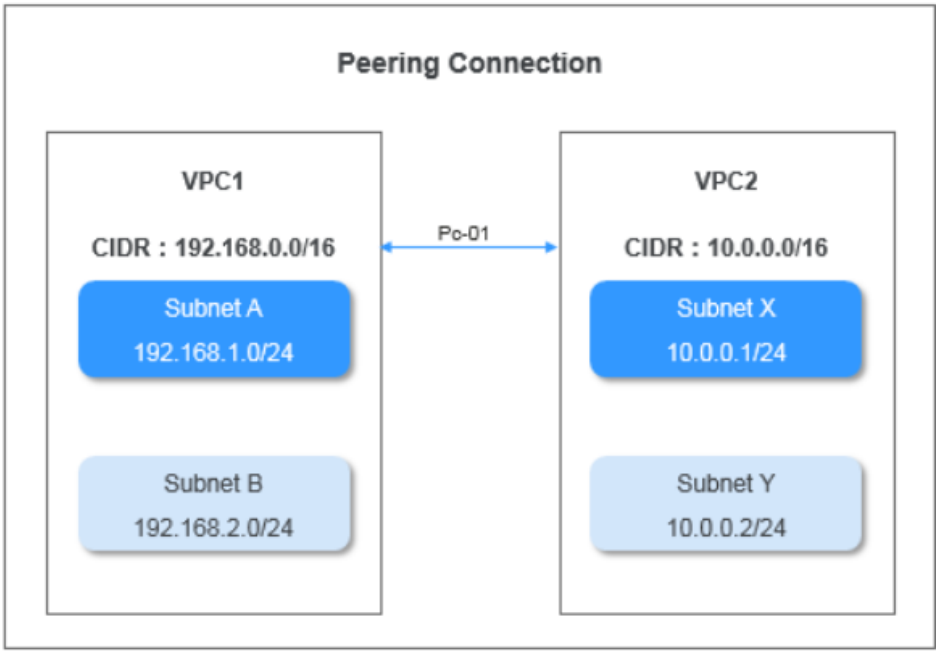
VPC 之间的连接

VPC之间的连接有几种方式可以考虑。

- **VPC对等连接**

  同一个区域之间，可以使用VPC对等连接。对等连接是指两个VPC之间的网络连接，您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。

  对等连接的VPC子网网段不能有重叠，否则连接会不生效。详细信息请参见**对等连接简介**。



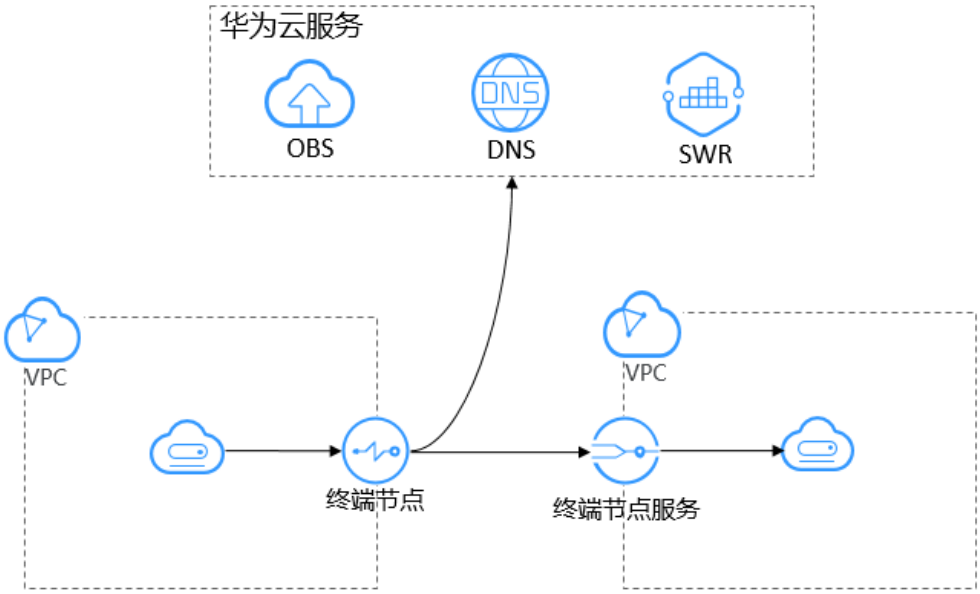
版权所有 © 华为技术有限公司

- **VPC终端节点**

  VPC终端节点服务可以将一个VPC内的资源作为服务开放给其他VPC使用。同时也可以通过VPC终端节点通过内网访问OBS、SWR、DNS等华为云服务。

  通过VPC终端节点访问的是VPC访问提供VPC终端节点的一方，是单向访问，并非双向互通，更加安全私密。详细信息请参见**什么是VPC终端节点?** 。

  图 1-12 通过 VPC 终端节点实现跨 VPC 单向访问

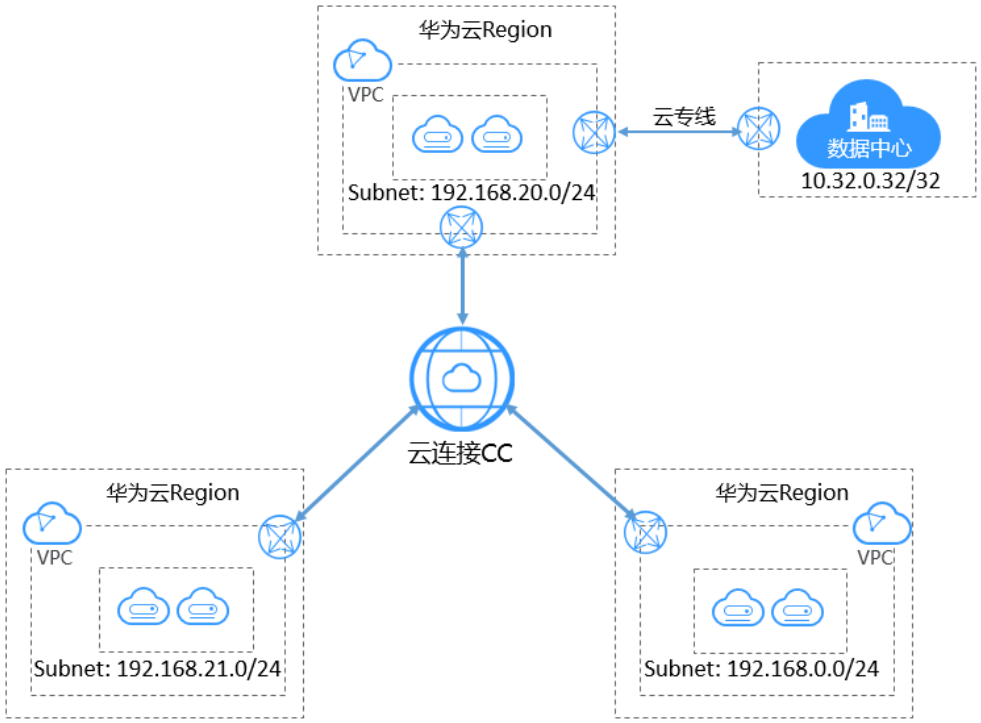
- **云连接CC**

  不同区域之间，可以考虑使用云连接服务将多个VPC连接互通。云连接在华为云不同区域之间提供高速、优质、稳定的网络能力，帮助用户打造一张具有企业级规模和通信能力的全球云上网络。同时配合云专线，能够实现云上多VPC与本地数据中心的连接。

  同一个云连接实例中的VPC子网网段不能重叠，否则会引起互通问题。详细信息请参见**什么是云连接**。

版权所有 © 华为技术有限公司

图 1-13 使用云连接实现跨区域多 VPC 连接

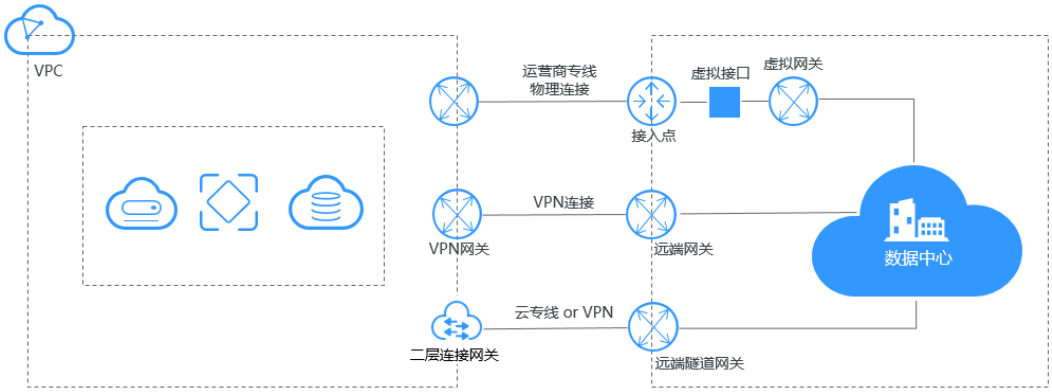


VPC 与本地数据中心之间的连接

当您有VPC与本地数据中心互通的需求时，可以使用云专线或VPN，还可以配合使用VPC二层网关。

- 云专线是专属网络，能实现高速、稳定、安全可靠的混合云部署，流量不经过互联网；
- VPN是在公网上构建的加密隧道网络，其流量经过互联网。
- 同时您还可以使用VPC二层连接网关（Layer 2 Connection Gateway，以下简称L2CG），二层连接网关是一种虚拟隧道网关，可基于云专线/VPN网络建立云上与云下之间的二层网络，解决云上和云下网络二层互通问题，允许您在不改变子网、IP规划的前提下将数据中心或私有云主机业务部分迁移上云。

图 1-14 VPC 与本地数据中心之间的连接



版权所有 © 华为技术有限公司

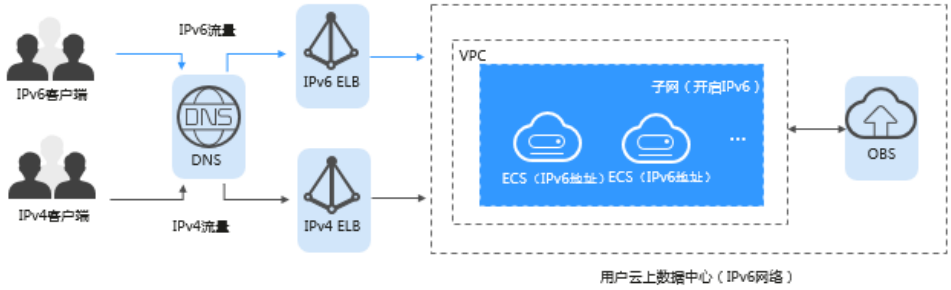
与互联网的连接

- **少量弹性云服务器通过弹性公网IP连接Internet**

  当您仅有少量弹性云服务器访问Internet时，您可将弹性公网IP（EIP）绑定到弹性云服务器上，弹性云服务器即可连接公网。您还可以通过动态解绑它，再绑定到NAT网关、弹性负载均衡上，使这些云产品连接公网，管理非常简单。不同弹性公网IP还可以共享带宽，减少您的带宽成本。

  华为云提供IPv6双栈和IPv6-EIP功能，支持两个不同版本的IP地址：IPv4地址和IPv6地址，这两个IP地址都可以进行内网/公网访问。

  图 1-15 IPv6 双栈

  更多弹性公网IP（EIP）信息，请参见**弹性公网IP简介**。

- **大量弹性云服务器通过NAT网关连接Internet**

  当您有大量弹性云服务器需要访问Internet时，单纯使用弹性公网IP管理成本过高，公有云NAT网关来帮您，它提供SNAT和DNAT两种功能。SNAT可轻松实现同一VPC内的多个弹性云服务器共享一个或多个弹性公网IP主动访问公网，有效降低管理成本，减少了弹性云服务器的弹性公网IP直接暴露的风险。DNAT功能还可以实现端口级别的转发，将弹性公网IP的端口映射到不同弹性云服务器的端口上，使VPC内多个弹性云服务器共享同一弹性公网IP和带宽面向互联网提供服务。

  更多NAT网关信息，请参见**《NAT网关用户指南》**。

- **海量高并发场景通过弹性负载均衡连接Internet**

  对于电商等高并发访问的场景，您可以通过弹性负载均衡（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。弹性负载均衡采用集群化部署，支持多可用区的同城双活容灾。同时，无缝集成了弹性伸缩，能够根据业务流量自动扩容，保证业务稳定可靠。

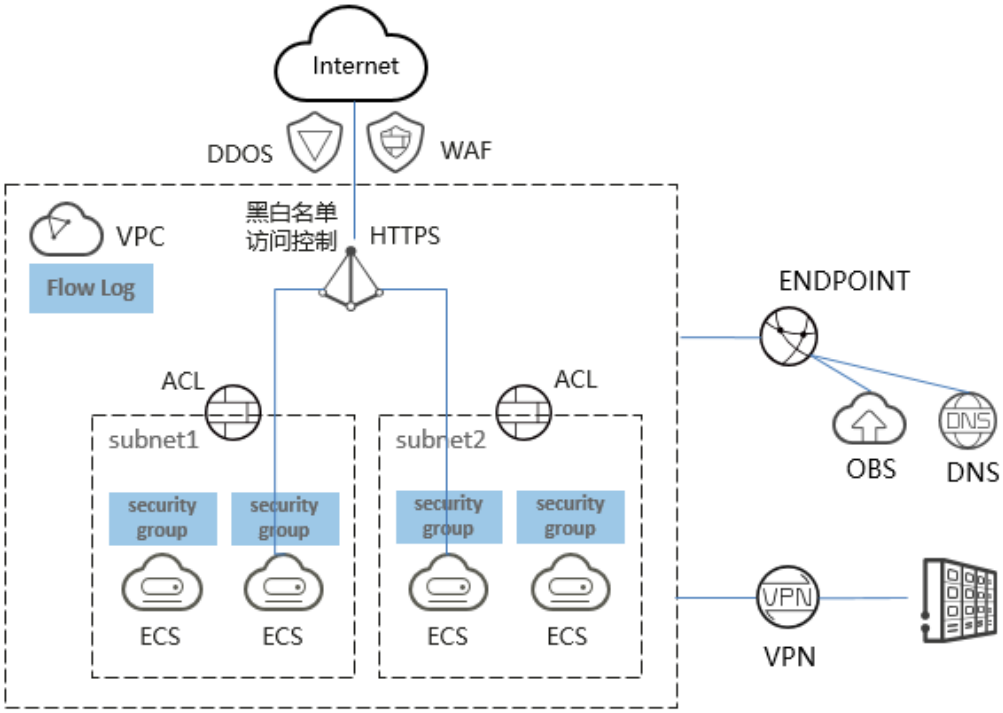
  更多弹性负载均衡信息，请参见**《弹性负载均衡用户指南》**。

1.3 网络安全

华为云提供了丰富的网络安全相关的服务和功能，选取合适的功能组合使用，能够让您的业务更加安全可靠。

本节按照从外部到云内的顺序介绍华为云提供网络安全相关服务和功能，如下是华为云网络安全相关服务及功能示意图。

版权所有 © 华为技术有限公司



DDoS 和 WAF

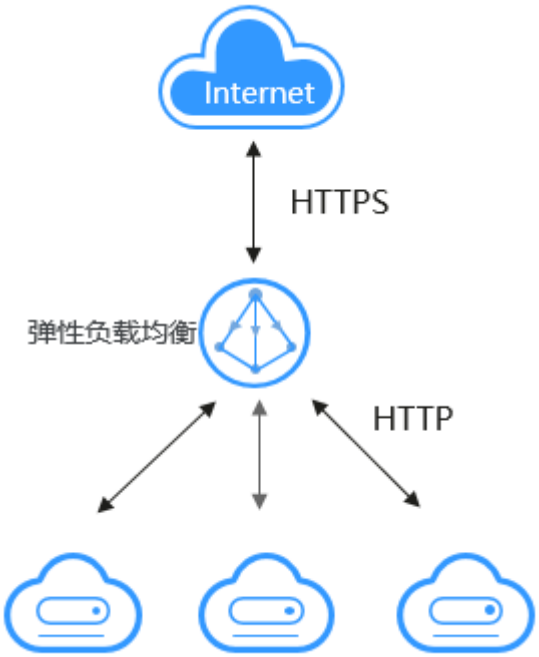
- **DDoS高防**（Advanced Anti-DDoS，AAD）是企业重要业务连续性的有力保障，用户可以通过修改DNS解析或对外服务地址为高防IP，将恶意攻击流量引流到高防IP清洗，确保重要业务不被攻击中断。可服务于华为云、非华为云及本地数据中心的互联网主机。
- **Web应用防火墙**（Web Application Firewall，WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

弹性负载均衡 ELB

ELB提供**HTTPS的协议接入**，可配置SSL证书，记录7层访问日志。同时ELB还提供黑白名单访问权限管理，详细请参见**访问控制策略**。

版权所有 © 华为技术有限公司

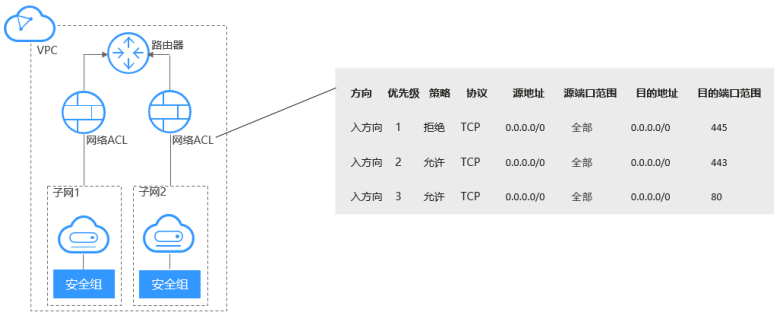
图 1-16 HTTPS 接入



网络 ACL

网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。详细请参见**网络ACL简介**。

图 1-17 网络 ACL



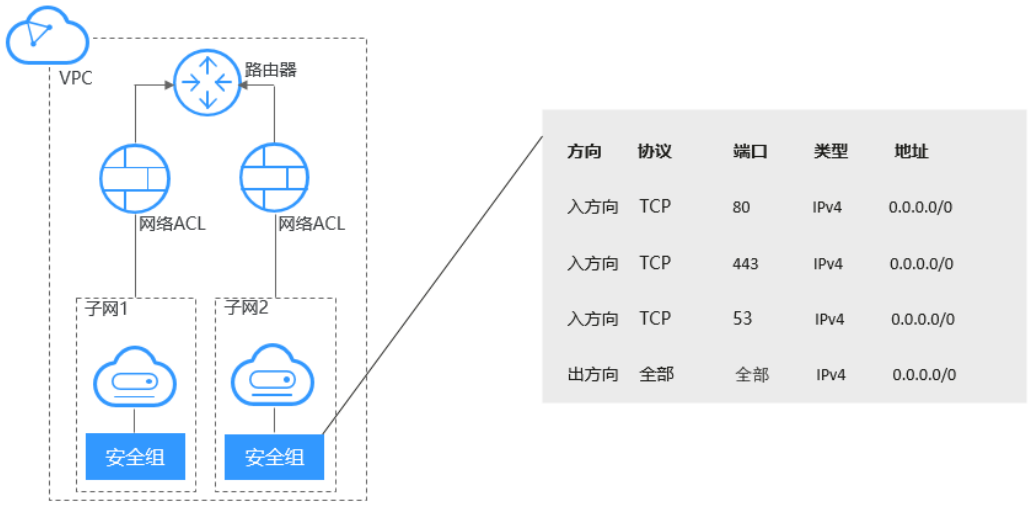
安全组

安全组是一个逻辑上的分组，为同一个VPC内具有相同安全保护需求并相互信任的弹性云服务器提供访问策略。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。详细请参见**安全组简介**。

安全组对弹性云服务器进行防护，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。

版权所有 © 华为技术有限公司

图 1-18 安全组



VPC 流日志

VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。

用户可配置针对VPC/子网/网卡粒度的流日志监控，识别攻击流量，或安全组/ACL误丢弃的流量。流日志可直接在LTS中查看，或转存在OBS中，您可以提取并采用业界通用日志工具分析。详细请参见**VPC流日志简介**。

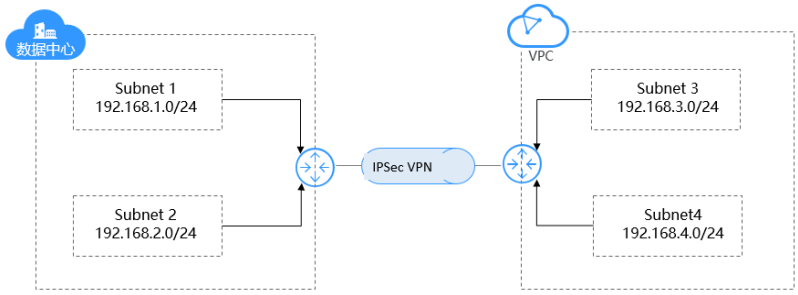
流日志示例如下。

```
<version> <project-id> <interface-id>  <srcaddr>     <dstaddr>      <srcport>  <dstport>  <protocol>
<packets>  <bytes>  <start>     <end>      <action>  <log-status>
1       *          *           192.168.0.59   192.168.0.218   22        39074     6         20        3997
1588743886   1588744486  ACCEPT     OK
1       *          *           192.168.0.59   192.168.0.218   22        39082     6         20        3997
1588743886   1588744486  ACCEPT     OK
1       *          *           192.168.0.218  192.168.0.59    39074     22        6         26        4033
1588743886   1588744486  ACCEPT     OK
1       *          *           192.168.0.218  192.168.0.59    39082     22        6         24        4117
1588743886   1588744486  ACCEPT     OK
```

VPN

在远端用户和VPC之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云上。

图 1-19 使用 VPN 建立安全加密通信隧道



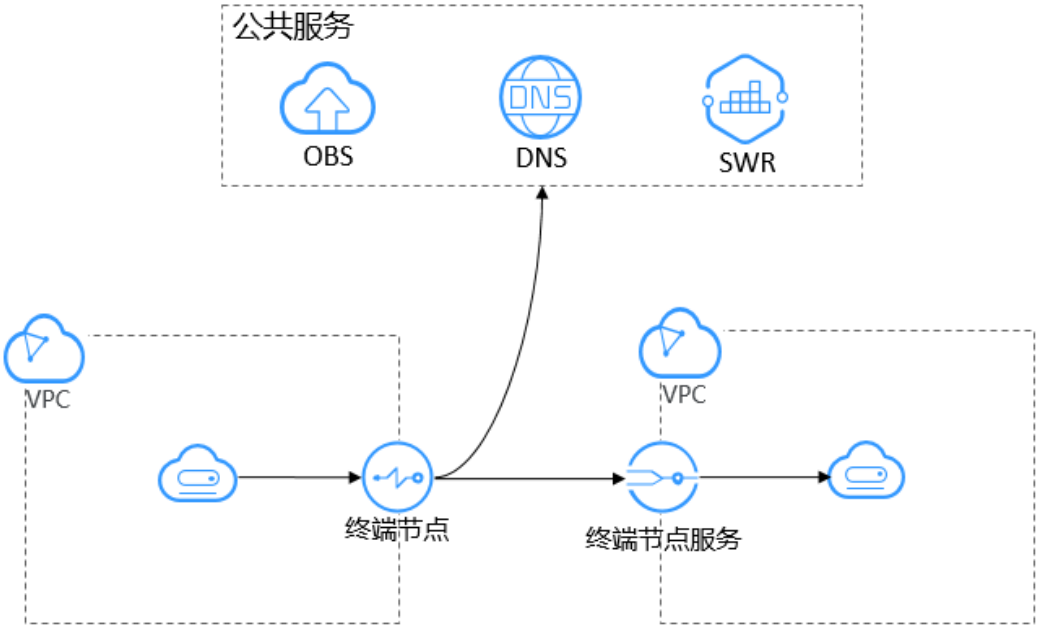
版权所有 © 华为技术有限公司

VPC Endpoint

VPC Endpoint在VPC内提供便捷、安全、私密的通道与终端节点服务（华为云服务、用户私有服务）进行连接，该服务使用华为云内部网络，无需弹性公网IP。

通过VPC Endpoint访问是VPC访问提供VPC终端节点的一方，是单向访问，且只能访问提供终端节点服务VPC中的指定云服务器、ELB等资源。

图 1-20 通过 VPC 终端节点实现私密连接



1.4 网络监控

华为云提供的网络监控主要有两方面。

对弹性公网 IP 和带宽的监控

通过监控入网带宽、出网带宽、带宽使用率，入网流量、出网流量，您可以实时的对弹性网公网IP和带宽的质量进行感知，并且可以设置告警规则，当指标超过某个阈值时自动告警，从而保证网络服务的质量。

详细监控指标和使用方法请参见**支持的监控指标**。

对 VPC 内流量进行监控

使用**VPC流日志**功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。

您可配置针对VPC/子网/网卡粒度的流日志监控，识别攻击流量，或安全组/ACL误丢弃的流量。流日志可直接在LTS中查看，或转存在OBS中，您可以提取并采用业界通用日志工具分析。

流日志示例如下。

```
<version> <project-id> <interface-id>  <srcaddr>     <dstaddr>      <srcport>   <dstport>   <protocol>
<packets>  <bytes>  <start>     <end>      <action>   <log-status>
```


版权所有 © 华为技术有限公司

```
1       *       *       192.168.0.59    192.168.0.218   22      39074   6       20      3997
1588743886      1588744486      ACCEPT      OK
1       *       *       192.168.0.59    192.168.0.218   22      39082   6       20      3997
1588743886      1588744486      ACCEPT      OK
1       *       *       192.168.0.218   192.168.0.59    39074   22      6       26      4033
1588743886      1588744486      ACCEPT      OK
1       *       *       192.168.0.218   192.168.0.59    39082   22      6       24      4117
1588743886      1588744486      ACCEPT      OK
```


版权所有 © 华为技术有限公司

2 什么是虚拟私有云

简介

虚拟私有云（Virtual Private Cloud，以下简称VPC），为云服务器、云容器、云数据库等资源构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。

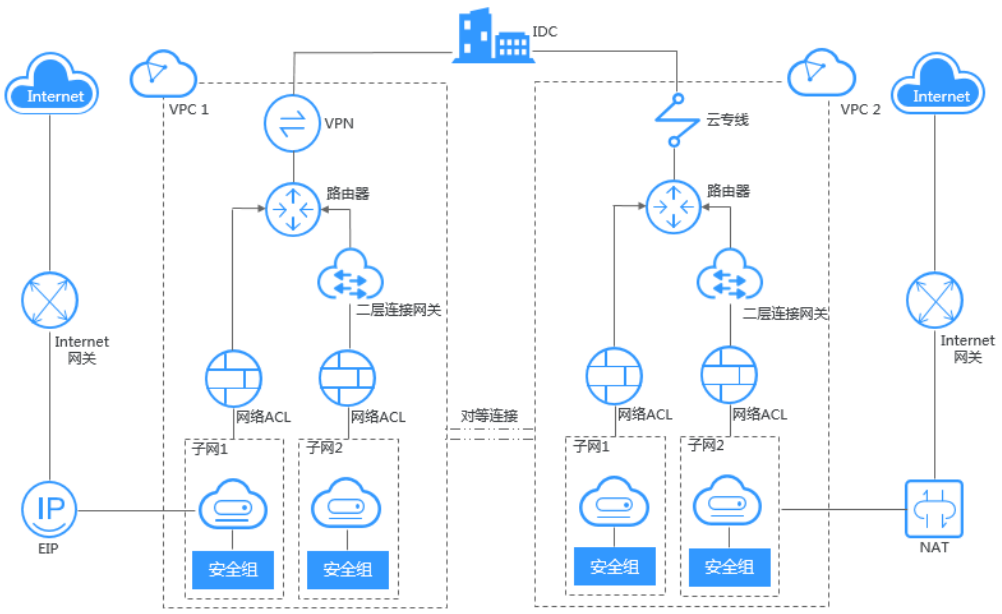
您可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性。用户可以通过VPC方便地管理、配置内部网络，进行安全、快捷的网络变更。同时，用户可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

VPC使用网络虚拟化技术，通过链路冗余，分布式网关集群，多AZ部署等多种技术，保障网络的安全、稳定、高可用。

产品架构

虚拟私有云VPC产品架构可以分为：VPC的组成、安全、VPC连接。

图 2-1 产品架构



VPC组成部分

版权所有 © 华为技术有限公司

每个虚拟私有云VPC由一个私网网段、路由表和至少一个子网组成。

- 私网网段：用户在创建虚拟私有云VPC时，需要指定虚拟私有云VPC使用的私网网段。当前虚拟私有云VPC支持的网段有10.0.0.0/8~24、172.16.0.0/12~24和192.168.0.0/16~24。
- 子网：云资源（例如云服务器、云数据库等）必须部署在子网内。所以，虚拟私有云VPC创建完成后，您需要为虚拟私有云VPC划分一个或多个子网，子网网段必须在私网网段内。更多信息请参考**子网**。
- 路由表：在创建虚拟私有云VPC时，系统会自动生成默认路由表，默认路由表的作用是保证了同一个虚拟私有云VPC下的所有子网互通。当默认路由表中的路由策略无法满足应用（比如未绑定弹性公网IP的云服务器需要访问外网）时，您可以通过创建自定义路由表来解决。更多信息请参考**VPC内自定义路由示例**和**VPC外自定义路由示例**。

安全

安全组与网络ACL（Access Control List）用于保障虚拟私有云VPC内部署的云资源的安全。安全组类似于虚拟防火墙，为同一个VPC内具有相同安全保护需求并相互信任的云资源提供访问策略，更多信息请参考**安全组简介**；您可以为具有相同网络流量控制的子网关联同一个网络ACL，通过设置出方向和入方向规则，对进出子网的流量进行精确控制，更多信息请参考**网络ACL简介**。

VPC连接

华为云提供了多种VPC连接方案，以满足用户不同场景下的诉求。具体应用场景及连接方案请参见**应用场景**。

- 通过VPC对等连接功能，实现同一区域内不同VPC下的私网IP互通。
- 通过EIP或NAT网关，使得VPC内的云服务器可以与公网Internet互通。
- 通过虚拟专用网络VPN、云连接、云专线及VPC二层连接网关功能将VPC和您的数据中心连通。

如何访问虚拟私有云

通过管理控制台、基于HTTPS请求的API（Application Programming Interface）两种方式访问虚拟私有云。

- 管理控制台方式

  管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录**管理控制台**，从主页选择“虚拟私有云”。
- API方式

  如果用户需要将云平台上的虚拟私有云集成到第三方系统，用于二次开发，请使用API方式访问虚拟私有云，具体操作请参见**《虚拟私有云API参考》**。

版权所有 © 华为技术有限公司

3 产品优势

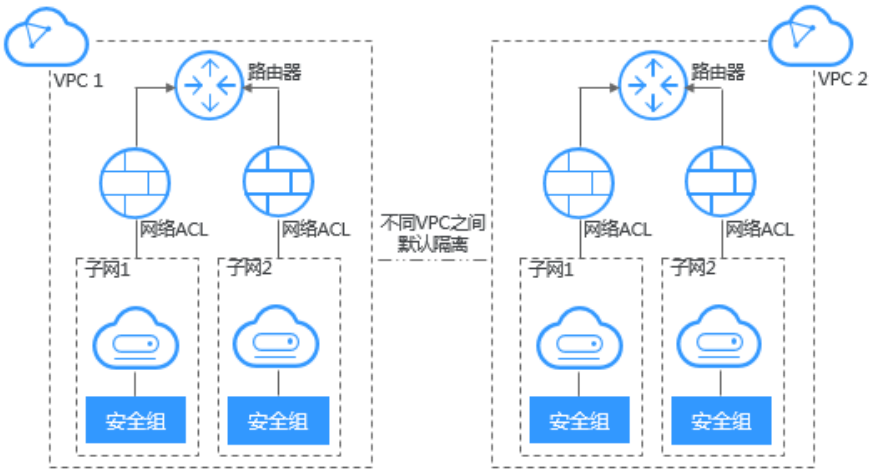
灵活配置

自定义虚拟私有网络，按需划分子网，配置IP地址段，DHCP、路由表等服务。支持跨可用区部署弹性云服务器。

安全可靠

VPC之间通过隧道技术进行100%逻辑隔离，不同VPC之间默认不能通信。网络ACL对子网进行防护，安全组对弹性云服务器进行防护，多重防护您的网络更安全。

图 3-1 安全可靠



互联互通

默认情况下，VPC与公网是不能通信访问的，我们提供了弹性公网IP、弹性负载均衡、NAT网关、虚拟专用网络、云专线等多种方式连接公网。

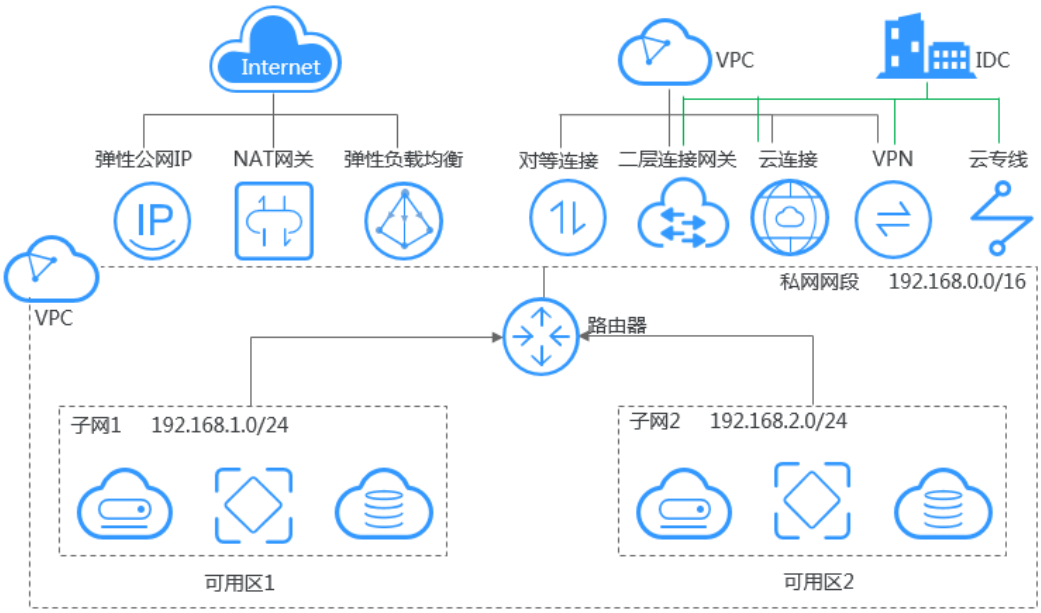
默认情况下，两个VPC之间也是不能通信访问的，我们提供对等连接的方式，使用私有IP地址在两个VPC之间进行通信。

对于云上和云下网络二层互通问题，我们提供二层连接网关功能，允许您在不改变子网、IP规划的前提下将数据中心或私有云主机业务部分迁移上云。

版权所有 © 华为技术有限公司

提供多种连接选择，满足企业云上多业务需求，让您轻松部署企业应用，降低企业IT运维成本。

图 3-2 互联互通



高速访问

使用全动态BGP协议接入多个运营商，支持多达21条线路。可以根据设定的寻路协议实时自动故障切换，保证网络稳定，网络时延低，云上业务访问更流畅。

优势对比

虚拟私有云相比传统IDC的优势如表3-1所示。

表 3-1 虚拟私有云与传统 IDC 对比

对比项	虚拟私有云	传统IDC
部署周期	• 用户无需工程规划，布线等复杂工程部署的工作。 • 用户基于业务需求在华为云上自主规划私有网络、子网和路由。	用户需要自行搭建网络并进行测试，整个周期很长，而且需要专业技术支持。
总成本	华为云网络服务提供了多种灵活的计费方式，加上客户无需前期投入和后期网络运维，整体上降低了TCO。	用户需要机房、供电、施工、硬件物料等固定重资产投入，也需要专业的运维团队来保障网络安全。随着业务变化，资产管理成本也会随之上升。

版权所有 © 华为技术有限公司

对比项	虚拟私有云	传统IDC
灵活性	华为云提供多种网络服务，用户可以根据具体需求搭配服务。当业务发展需要更多的网络资源（如带宽资源）时，可以方便快捷的进行动态扩展。	业务部署需要严格遵守前期网络规划，当业务需求发生变化时，无法便捷的动态调整网络。
安全性	VPC逻辑隔离，结合网络控制ACL、安全组功能和DDoS等安全服务，保障了云上资源的安全使用。	网络很难得到专业维护，安全性较差，需要配置专业的网络安全人员来看护。

版权所有 © 华为技术有限公司

4 应用场景

云端专属网络

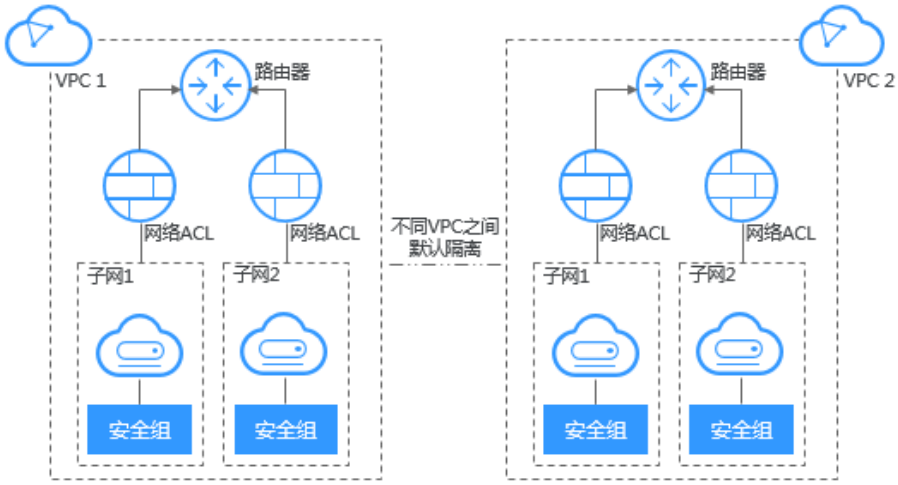
场景描述

每个虚拟私有云VPC代表一个私有网络，与其他VPC逻辑隔离，您可以将业务系统部署在华为云上，构建云上私有网络环境。如果您有多个业务系统例如生产环境和测试环境要严格进行隔离，那么可以使用多个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。

搭配服务

弹性云服务器ECS

图 4-1 云端专属网络



Web 应用或网站托管

场景描述

在VPC中托管Web应用或网站，可以像使用普通网络一样使用VPC。通过弹性公网IP或NAT网关连接弹性云服务器与Internet，运行弹性云服务器上部署的Web应用程序。同时结合弹性负载均衡ELB服务，您可以将来自Internet的流量均衡分配到不同的弹性云服务器上。

版权所有 © 华为技术有限公司

VPC内的云资源连接公网（Internet），可以通过如下云产品实现。

表 4-1 连接公网

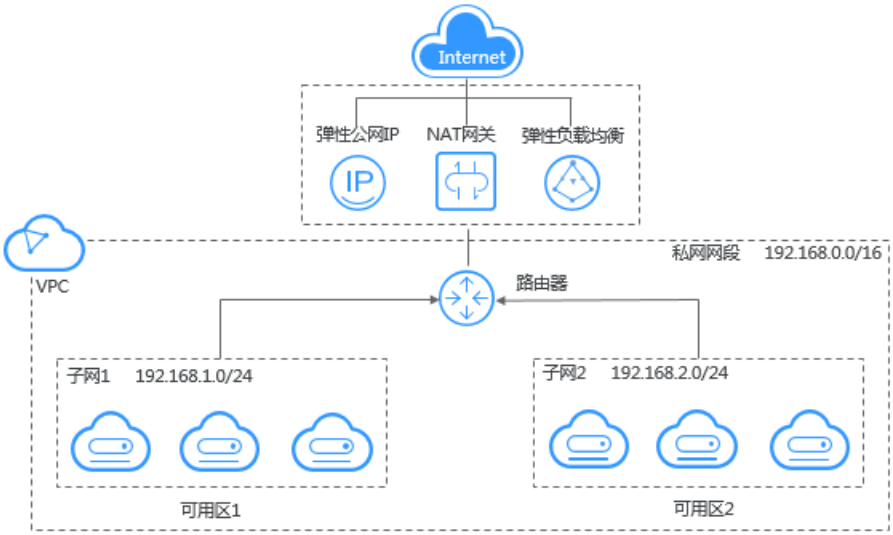
云产品	应用场景	描述	相关操作
弹性公网IP	单个ECS连接公网	申请一个弹性公网IP（EIP）并将其绑定到ECS上，ECS即可连接公网，实现主动访问公网或面向公网提供服务。 支持动态绑定和解绑ECS。 可以使用共享带宽和共享流量包，降低公网成本。	**弹性公网IP介绍**
NAT网关	多个ECS共享弹性公网IP连接公网	NAT网关提供SNAT和DNAT两种功能：SNAT可实现同一VPC内的多个ECS共享一个或多个EIP主动访问公网，有效降低管理成本，同时减少了ECS的EIP直接暴露的风险。DNAT功能还可以实现端口级别的转发，将EIP的端口映射到不同ECS的端口上，使VPC内多个ECS共享同一EIP和带宽面向公网提供服务，但没有均衡流量的功能。	**使用SNAT连接公网** **使用DNAT面向公网提供服务**
弹性负载均衡	通过将访问流量均衡分发到多个ECS的方式对外提供服务，比如电商等高并发访问场景	弹性负载均衡（ELB）可以将访问流量均衡分发（支持4层和7层两种方式）到多个后端ECS上，通过绑定EIP支撑海量用户从公网访问ECS。 通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。	**弹性负载均衡介绍**

搭配服务

弹性云服务器ECS、弹性公网IP、NAT网关、弹性负载均衡

版权所有 © 华为技术有限公司

图 4-2 Web 应用或网站托管



Web 应用访问控制

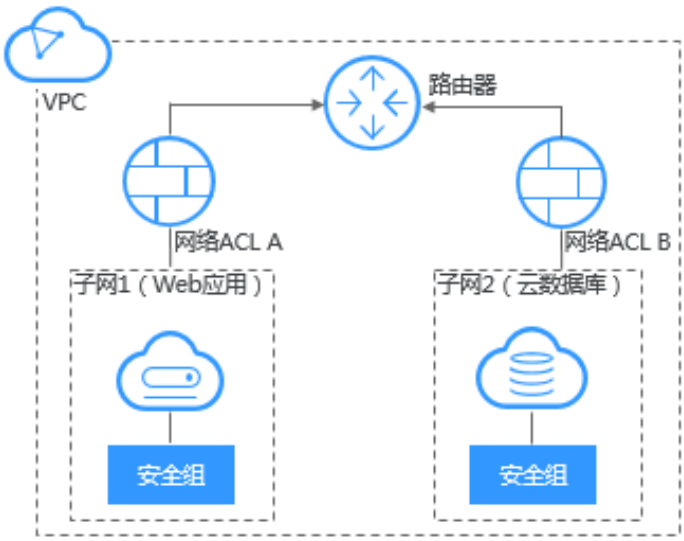
场景描述

将多层Web应用划分到不同的安全域中，按需在各个安全域中设置访问控制策略，可以通过创建一个VPC，将Web服务器和数据库服务器划分到不同的安全组中。Web服务器所在的子网实现互联网访问，而数据库服务器只能通过内网访问，保护数据库服务器的安全，满足高安全场景。

搭配服务

弹性云服务器ECS

图 4-3 Web 应用访问控制



云上 VPC 连接

场景描述

版权所有 © 华为技术有限公司

对于相同或者不同区域下的VPC需要互通连接时，可通过如下云产品实现。

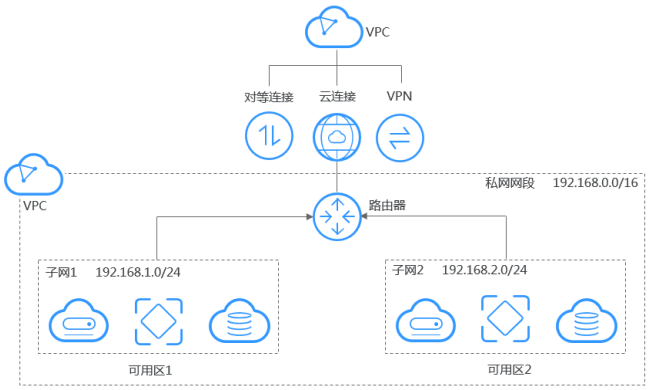
表 4-2 连接 VPC

云产品	应用场景	描述	相关操作
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。对等连接免费。	**创建同一帐户下的对等连接** **创建不同帐户下的对等连接**
云连接	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，跨区域连接实现全球云上网络。	**跨区域VPC互连**
虚拟专用网络VPN	使用公网低成本连接跨区域VPC	基于Internet使用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。但它的网络质量依赖Internet。	**通过VPN连接VPC**

搭配服务

弹性云服务器ECS、云连接CC、虚拟专用网络VPN

图 4-4 云上 VPC 连接



混合云部署

场景描述

对于自建本地数据中心（IDC）的用户，由于利旧和平滑演进的原因，并非所有的业务都能放置在云上，这个时候就可以通过如下产品构建混合云，实现云上VPC与云下IDC之间的互连。

版权所有 © 华为技术有限公司

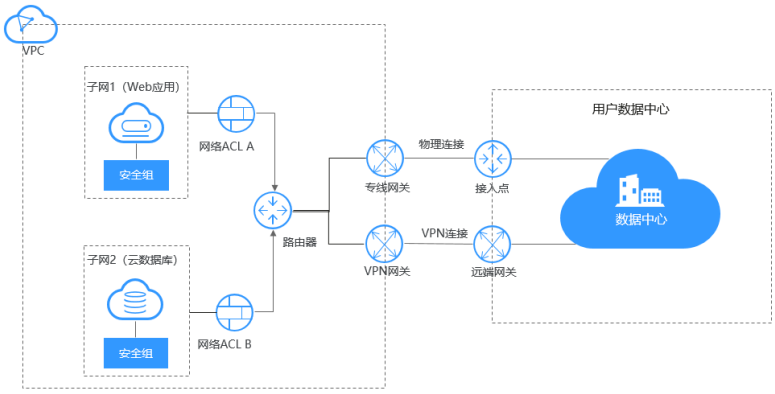
表 4-3 连接 IDC

云产品	应用场景	描述	相关操作
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。	通过VPN连接VPC 二层连接网关
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 。	通过用户专线访问多个VPC 二层连接网关
云连接	跨区域的VPC、IDC互连	将要互通的本地IDC关联的云专线加载到已创建的云连接实例中，实现跨区域的VPC、IDC互连。	跨区域VPC互连 多数据中心与多区域VPC互通

搭配服务

弹性云服务器ECS、云专线DC、云连接CC、虚拟专用网络VPN

图 4-5 混合云部署



版权所有 © 华为技术有限公司

5 功能总览

表5-1列出了虚拟私有云VPC的常用功能。

在使用虚拟私有云VPC之前，建议您先通过基本概念介绍了解子网、路由表、安全组、弹性公网IP等基本概念，以便更好地理解虚拟私有云VPC提供的功能。

表 5-1 虚拟私有云 VPC 常用功能

功能分类	功能名称	功能描述
虚拟私有云和子网	虚拟私有云	虚拟私有云可以为您的云资源构建隔离的、用户自主配置和管理的虚拟网络环境。 华为云提供了管理虚拟私有云的功能：创建虚拟私有云、修改虚拟私有云基本信息、为虚拟私有云添加扩展网段、删除虚拟私有云扩展网段、删除虚拟私有云和导出虚拟私有云列表。 详细内容，请参见**创建虚拟私有云和子网**。
	子网	子网是虚拟私有云内的IP地址块。虚拟私有云中的所有云资源都必须部署在子网内。 华为云提供了管理子网的功能：为虚拟私有云创建新的子网、修改子网网络信息和删除子网。 详细内容，请参见**创建虚拟私有云和子网**。
	路由表	路由表中定义了路由规则，路由规则用于将目标网段的流量路由至指定的目的地。 当您创建虚拟私有云时，系统会自动为您创建一张默认路由表，其路由规则保证了虚拟私有云内的所有子网互通。您也可以添加自定义路由规则，将指定目标网段的流量路由至指定目的地。 华为云提供了管理路由表的功能：添加自定义路由、查询路由、修改路由和删除路由等。 详细内容，请参见**路由表简介**。 当前在部分区域中，路由表与虚拟私有云已解耦，解耦后路由表入口迁移，支持路由表与子网关联功能，已解耦的区域用户请参考**路由表（解耦）**。

版权所有 © 华为技术有限公司

功能分类	功能名称	功能描述
	虚拟IP	虚拟IP是一个未分配给真实弹性云服务器网卡的IP地址。弹性云服务器除了拥有私有IP地址外，还可以拥有虚拟IP地址，用户可以通过其中任意一个IP（私有IP/虚拟IP）访问此弹性云服务器。同时，虚拟IP地址拥有私有IP地址同样的网络接入能力。虚拟IP主要用在弹性云服务器的主备切换，达到高可用性HA的目的。 华为云提供的虚拟IP相关功能包括：申请虚拟IP地址、删除虚拟IP地址、为虚拟IP地址绑定弹性公网IP或弹性云服务器、通过弹性公网IP访问虚拟IP、通过VPN访问虚拟IP、通过云专线访问虚拟IP和通过对等连接访问虚拟IP。 详细内容，请参见**虚拟IP简介**。
	IPv4/IPv6双栈网络	IPv4/IPv6双栈可为您的实例提供两个不同版本的IP地址：IPv4地址和IPv6地址，这两个IP地址都可以进行内网/公网访问。 华为云提供IPv4/IPv6双栈功能，支持新建IPv4/IPv6双栈网络，或在已有虚拟私有云下添加IPv6子网形成双栈网络。 详细内容，请参见**IPv4/IPv6双栈网络**。
	VPC流日志	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。 华为云提供的VPC流日志功能包括：创建VPC流日志、查看VPC流日志、开启/关闭VPC流日志、删除VPC流日志。 详细内容请参见**VPC流日志简介**。
	弹性网卡	弹性网卡即虚拟网卡，您可以通过创建并配置弹性网卡，并将其附加到您的ECS实例上，实现灵活、高可用的网络方案配置。 华为云提供的弹性网卡功能包括：创建弹性网卡、绑定弹性网卡到云服务器实例、绑定弹性网卡到弹性公网IP、绑定弹性网卡到虚拟IP、创建弹性网卡流日志、解绑定弹性云服务器或弹性公网IP、更改弹性网卡所属安全组、删除弹性网卡。 详细内容请参见**弹性网卡简介**。

版权所有 © 华为技术有限公司

功能分类	功能名称	功能描述
访问控制	安全组	安全组是一个逻辑上的分组，为同一个VPC内具有相同安全保护需求并相互信任的弹性云服务器提供访问策略。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。 华为云提供了管理安全组和安全组规则的功能：创建安全组、删除安全组、添加安全组规则、快速添加多条安全组规则、复制安全组规则、修改区安全组规则、删除安全组规则、导入/导出安全组规则、查看弹性云服务器的安全组、变更弹性云服务器的安全组、云资源加入/移出安全组。 详细内容，请参见**安全组简介**。
	网络ACL	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。 华为云提供了管理网络ACL和网络ACL规则的功能：创建网络ACL、查看网络ACL、修改网络ACL、删除网络ACL、开启/关闭网络ACL、关联/解除子网和网络ACL、添加网络ACL规则、修改网络ACL规则、修改网络ACL规则生效顺序、开启/关闭网络ACL规则、删除网络ACL规则。 详细内容，请参见**网络ACL简介**。
	IP地址组	IP地址组是多个IP地址的集合，可被安全组规则引用，可统一管理具有相同安全要求或需要频繁修改的IP地址。通过使用IP地址组，可有效应对需要重复多次编辑安全组规则的场景，方便管理。 华为云提供了管理IP地址组的功能：创建IP地址组、关联IP地址组与安全组规则、修改、删除IP地址组。 详细内容，请参见**IP地址组简介**。
弹性公网IP和带宽	弹性公网IP	弹性公网IP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，可以与云资源灵活绑定及解绑。 华为云提供的弹性公网IP相关功能包括：为云资源申请和绑定弹性公网IP、解绑和释放云资源的弹性公网IP、修改弹性公网IP带宽、静态BGP转换为动态BGP。 详细内容，请参见**弹性公网IP简介**。

版权所有 © 华为技术有限公司

功能分类	功能名称	功能描述
	共享带宽	共享带宽可以实现多个弹性公网IP共同使用一条带宽。提供区域级别的带宽共享及复用能力，同一区域下的所有已绑定弹性公网IP的弹性云服务器、裸金属服务器、弹性负载均衡等实例共用一条带宽资源。 华为云提供的共享带宽相关功能包括：申请共享带宽、修改共享带宽、删除共享带宽、添加弹性公网IP到共享带宽、从共享带宽中移出弹性公网IP。 详细内容，请参见**共享带宽简介**。
	共享流量包	共享流量包是一款带宽流量套餐产品，使用方便，价格实惠。购买共享流量包后立即生效，并自动抵扣按需按流量计费的EIP带宽产生的流量资费，直到流量包用完或到期。 详细内容，请参见**共享流量包简介**。
	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。 华为云提供的带宽加油包相关功能包括：购买带宽加油包、修改带宽加油包和退订带宽加油包。 详细内容，请参见**带宽加油包简介**。
资源互通	VPC对等连接	对等连接是指两个VPC之间的网络连接。您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。同一区域内，您可以在自己的VPC之间创建对等连接，也可以在自己的VPC与其他帐户的VPC之间创建对等连接。不同区域间的VPC之间不能创建对等连接。 华为云提供的VPC对等连接相关功能包括：创建同一帐户下的对等连接、创建不同帐户下的对等连接、查看对等连接、修改对等连接和删除对等连接。 详细内容，请参见**对等连接简介**。
	二层连接网关	二层连接网关是一种虚拟隧道网关，可基于云专线/VPN网络建立云上与云下之间的二层网络，解决云上和云下网络二层互通问题，允许您在不改变子网、IP规划的前提下将数据中心或私有云主机业务部分迁移上云。 华为云提供的二层连接网关相关功能包括：购买二层连接网关、查看二层连接网关、修改二层连接网关、删除二层连接网关、创建二层连接、查看二层连接、删除二层连接。 详细内容，请参见**二层连接网关**。

版权所有 © 华为技术有限公司

功能分类	功能名称	功能描述
监控	查看监控指标	当用户开通了虚拟私有云服务后，无需额外安装其他插件，即可在云监控查看带宽、弹性公网IP的使用情况，也可以创建和设置告警规则，自定义监控目标与通知策略，及时了解虚拟私有云的状况，从而起到预警作用。 详细内容，请参见**支持的监控指标**。
审计	查看审计日志	通过云审计，您可以记录与虚拟私有云相关的操作事件，便于日后的查询、审计和回溯。 华为云提供**查看审计日志**功能，支持在云审计服务管理控制台查看或导出最近7天的操作记录。 详细内容，请参见**支持审计的关键操作**。
标签	标签管理	标签功能方便您识别和管理云资源。华为云支持管理虚拟私有云标签、管理子网标签和管理弹性公网IP标签。
权限	权限管理	您可以使用统一身份认证服务IAM对您所拥有的虚拟私有云进行精细的权限管理，以满足企业基于组织划分、职能划分设置不同的访问权限。 华为云提供的虚拟私有云权限管理功能包括：创建用户并授权使用VPC、创建VPC自定义策略。 详细内容，请参见**权限管理**。

版权所有 © 华为技术有限公司

6 约束与限制

虚拟私有云

虚拟私有云使用限制如表6-1所示。

表 6-1 虚拟私有云使用限制

资源	默认配额（个）	如何提升配额
一个用户创建虚拟私有云的数量	5	提交工单
一个用户创建子网的数量	100	提交工单
一个用户拥有的安全组数量	100	提交工单
一个用户拥有的安全组规则数量	5000	提交工单
一个路由表里拥有的路由数量	200	不能调整
一个虚拟私有云拥有的路由表数量	1	提交工单
一个区域下的对等连接数量	50	不能调整
一个用户拥有网络ACL数量	200	提交工单
一个用户创建二层连接网关的数量	5	提交工单
一个虚拟IP可绑定的ECS数量	10	提交工单

说明

- 以上配额说明针对单租户情况。
- 一个网络ACL单方向拥有的规则数量最好不超过20条，否则可能引起网络ACL性能下降。
- 二层网关连接在公测期间默认只能创建1个二层连接网关。

版权所有 © 华为技术有限公司

安全组的限制

- 默认情况下，一个用户可以创建100个安全组。
- 默认情况下，一个安全组最多只允许拥有50条安全组规则。
- 默认情况下，一个云服务器或扩展网卡建议选择安全组的数量不多于5个。
- 云服务器或扩展网卡绑定多个安全组时，安全组规则先根据绑定安全组的顺序生效，再根据组内规则的优先级生效（安全组规则优先级目前仅在“华东-上海一”、“华南-广州”、“西南-贵阳一”、“华北-北京四”、“中国-香港”、“亚太-新加坡”支持）。
- 安全组添加实例时，一次最多可添加20个实例。
- 一个安全组关联的实例数量建议不超过1000个，否则可能引起安全组性能下降。
- 当安全组规则配置为以下情况时，不支持针对下列类型的云服务器生效。

表 6-2 安全组规则限制

安全组规则	不支持的云服务器类型
策略选择“拒绝”	X86计算型，具体规格请参见**规格清单（X86）** • 通用计算型（S1型、C1型、C2型 ） • 内存优化型（M1型） • 高性能计算型（H1型） • 磁盘增强型（ D1型） • GPU加速型（G1型、G2型） • 超大内存型（E1型、E2型、ET2型）
源/目的地址为“IP地址组”	
协议端口配置为不连续端口号	X86计算型，具体规格请参见**规格清单（X86）** • 通用计算型（S1型、C1型、C2型 ） • 内存优化型（M1型） • 高性能计算型（H1型） • 磁盘增强型（ D1型） • GPU加速型（G1型、G2型） • 超大内存型（E1型、E2型、ET2型）
	鲲鹏计算型，具体规格请参见**规格清单（鲲鹏）**

网络 ACL

- 默认情况下，一个用户可以创建200个网络ACL。
- 网络ACL可以关联多个子网，但一个子网同一时间只能关联一个网络ACL。
- 一个网络ACL单方向拥有的规则数量最好不超过20条，否则可能引起网络ACL性能下降。
- 导入/导出网络ACL规则时，建议您每次导入少于40条的规则，否则可能会影响性能。导入规则是基于已有规则的增量导入，不会删除已有规则。相同规则不允许重复导入。

版权所有 © 华为技术有限公司

弹性网卡

- 云服务器实例与扩展弹性网卡必须在同一VPC，可以分属于不同安全组。
- 主弹性网卡不能解绑服务器。
- 云服务器可附加的扩展弹性网卡数量由云服务器实例规格决定。具体请参见**规格清单**。
- 弹性网卡不支持直接访问华为云内公共云服务，如内网DNS等，推荐使用VPCEP访问华为云公共云服务，具体参见**购买连接“接口”型终端节点服务的终端节点**。

路由表

- 每个虚拟私有云在创建成功后，会自动生成1个路由表，即默认路由表；如果要创建更多自定义路由表，需要申请扩大路由表配额。

  申请扩大配额的操作，请参考**提交工单**。。
- 每个路由表最多添加200个路由。
- 默认路由表不能删除。
- 系统路由不能修改和删除。
- 由VPN、云专线、云连接服务下发到默认路由表中的路由不能修改和删除。
- 云容器引擎类型的路由不支持修改、复制和删除。
- 由VPC终端节点服务下发到默认路由表的网关类型终端节点的路由不能修改、复制和删除，并且自定义路由表中的网关类型终端节点的路由也不能修改和删除。
- 当为默认路由表添加自定义路由时，下一跳类型不支持选择VPN网关与云专线网关。

对等连接

- 有重叠子网网段的VPC建立的对等连接，可能不生效。
- 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。您可以通过使用NAT网关服务或**配置SNAT服务器**，使得VPC2下的弹性云服务器可以通过VPC1下绑定了EIP的弹性云服务器访问Internet。具体实现方式请参见**无公网IP的弹性云服务器访问Internet**。
- 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。
- 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 A与B、C分别建立对等连接，如果B、C两个VPC的网段有重叠，A中无法添加具有相同目的网段的路由。
- 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。
- 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，那么该对等关系不生效。建立对等连接时，请确保两个VPC之间没有重叠的子网。
- VPC对等连接路由存在时，VPC无法被删除。

 版权所有 © 华为技术有限公司

- 支持在华为云中国站和国际站同一区域创建对等连接。

流日志

- 目前支持S2、M2、Hc2、H2、D2、P1、G3、Pi1、fp1、S3、C3、M3、H3、D3、Ir3、I3、Sn3、S6、E3、C3ne、M3ne、G5、P2v、Ai1、M6、D6类型的弹性云服务器。弹性云服务器类型具体信息请参见**实例类型**。
- 默认情况下，一个用户最多允许创建10个VPC流日志。
- 默认情况下，最大支持40万条流日志记录。

虚拟 IP

- 不推荐在弹性云服务器配置多个同子网网卡的场景下，使用虚拟IP功能。若在该场景下使用虚拟IP功能，弹性云服务器内部会存在路由冲突，导致虚拟IP通信异常。
- 虚拟IP仅能绑定到同一个子网下的云服务器。
- 备弹性云服务器需要关闭IP转发功能。请参见**关闭备云主机弹性云服务器IP转发功能**。
- 虚拟IP只能使用默认安全组，不能更新为自定义安全组。
- 建议一个ECS绑定的虚拟IP不要超过8个。
- 建议一个虚拟IP绑定的ECS不要超过10个。
- IPv6的虚拟IP仅支持绑定一个网卡（双栈网卡），如需进行服务器的主备切换，请通过调用API方式。具体请参考**配置云服务器高可用的IPv6虚拟IP功能**。

二层连接网关

- 每个帐号默认可以创建5个L2CG。（公测期间默认只能创建1个L2CG）。
  如需提升配额请提交工单，请参见**提交工单**。
- L2CG依赖专线/VPN，需要提前创建专线/VPN。
- L2CG依赖与IDC侧建立VXLAN隧道，IDC侧交换机要支持VXLAN隧道。
- 一个VPC可绑定多个L2CG，一个L2CG只能绑定一个VPC。
- 一个L2CG支持最多6个二层连接云上云下互通。
- 同个L2CG的多个二层连接对应的远端隧道号和隧道IP组合不允许相同。
- 已被二层连接绑定过的子网不能再被其它二层连接或L2CG使用。
- 在创建中、删除中、规格变更中的资源不允许做修改或删除操作。
- 不支持云下往云上转发未知单播、广播、组播（除VRRP协议外）的IP报文。
- 云上云下IP地址不能冲突（除子网网关IP外）。
- 不支持云下主机访问云上的高级网络特性（ 如VPC对等连接，ELB，路由表，NAT网关等）。
- L2CG的每个二层连接会占用二层子网中的两个IP（接口IP与隧道IP），这两个IP不能与IDC的已有IP相同。
- L2CG网关会占用隧道子网的三个IP，需预留足够IP地址。

弹性公网 IP

关于弹性公网IP的使用，您需要注意以下几点：

 版权所有 © 华为技术有限公司

- 一个弹性公网IP只能绑定一个云资源使用，且弹性公网IP和云资源必须在同一个区域。
- 不同区域用户，可申请的EIP配额不同，如果您需要更多的EIP，请提交工单申请。
- 只有未绑定状态的EIP才能进行绑定操作。
- 按带宽计费的带宽上限为2000Mbit/s（“中国-香港”区域按带宽计费上限为500Mbit/s），如果您需要更大的带宽，请提交工单申请或联系您的客户经理。
- 按流量计费的带宽上限为300Mbit/s。
- 因安全等原因被冻结的EIP无法进行绑定、解绑等操作。
- 申请提升配额，要求该帐户下存在有效订单和持续使用的云服务资源，如您的帐户之前存在多次订购资源后即时释放的情况，拒绝提升配额。
- 未绑定的弹性公网IP地址才可释放，已绑定的弹性公网IP地址需要先解绑定后才能释放。
- 弹性公网IP释放后，如果被其他用户使用，则无法找回。
- 按需计费的弹性公网IP费用包括IP保有费和带宽费用，当与实例解绑且未释放时，仍需支付弹性公网IP的保有费和带宽费用；若绑定实例，则免除保有费。
- 对于长期闲置的EIP资源配额，华为云将降低配额至默认值，如需提升配额，您可通过工单提交申请。
- 如您违反适用法律法规的要求使用华为云EIP资源，华为云有权收回EIP资源，并暂停向您提供服务。
- 弹性公网IP不支持跨帐号转移。

带宽

- 共享带宽只能加入按需计费的EIP。
- 支持按带宽计费、增强型95计费。按带宽计费5Mbit/s起售，增强型95计费300Mbit/s起售。
- 共享带宽可支持加入20个EIP，如果您需要加入更多EIP，请提交工单申请。
- 每个用户最多申请5个共享带宽，如果您需要更多共享带宽，请提交工单申请。
- 对包年包月的带宽，在当前带宽周期内只能提升带宽上限不能降低带宽上限，如果需要降低带宽规格，请在当前带宽周期到期后，重新续费时降低带宽规格。
- 对按流量计费的带宽，仅收取出云方向带宽费用，不收取入云方向带宽费用。

说明

- 入云方向是指Internet流入云内方向，出云方向是指云内流出到Internet方向。
- 2020年7月31日 00:00（北京时间）之后，针对公网带宽进行限速规则调整，调整后的规则如下：
  - 若您购买/修改后的带宽大小小于或等于10Mbit/s，则入云方向带宽为10Mbit/s，出云方向带宽大小为购买/修改后的带宽大小。
  - 若您购买/修改后的带宽大小大于10Mbit/s，则出云方向和入云方向带宽相同，都等于购买/修改后的带宽大小。
- 增强型95计费取入云方向和出云方向中较大的带宽平均值作为采样点的带宽值进行收费。

共享流量包

- 共享流量包只能针对按流量计费的带宽生效，且需要区分静态BGP和动态BGP类型。

 版权所有 © 华为技术有限公司

- 共享流量包不支持退订。

带宽加油包

- 带宽加油包只能针对包年包月带宽生效。
- 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。

说明

工单提交请参见**提交工单**。

版权所有 © 华为技术有限公司

7 与其他服务的关系

虚拟私有云VPC服务与其他服务的关系，如图7-1所示。

图 7-1 与其他服务的关系

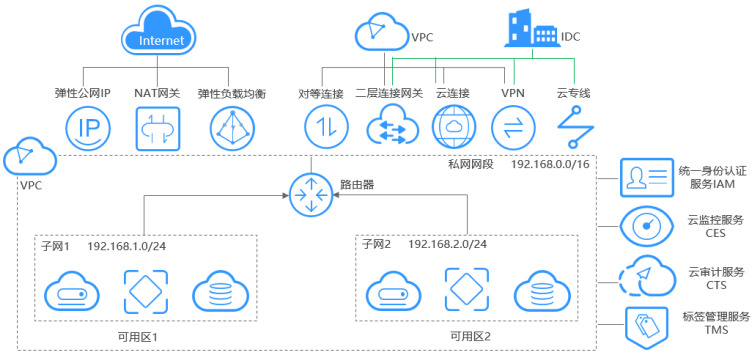


表 7-1 与其他服务的关系

交互功能	相关服务	位置
弹性云服务器的安全防护	弹性云服务器（Elastic Cloud Server，ECS）	添加安全组规则
虚拟私有云内的弹性云服务器与Internet互连	弹性公网IP（Elastic IP，EIP）	使用EIP连接Internet
	NAT网关（NAT Gateway，NAT）	使用SNAT连接Internet
虚拟私有云与本地数据中心互连	虚拟专用网络（Virtual Private Network，VPN）	虚拟专用网络
	云专线（Direct Connect，DC）	云专线
跨区域的虚拟私有云互连	云连接（Cloud Connect，CC）	跨区域VPC互通
访问流量分发到VPC内的多台弹性云服务器	弹性负载均衡（Elastic Load Balance，ELB）	弹性负载均衡

版权所有 © 华为技术有限公司

交互功能	相关服务	位置
如果您需要对华为云上创建的VPC资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。	统一身份认证服务（Identity and Access Management，IAM）	统一身份认证服务
查看带宽和流量使用情况	云监控服务（Cloud Eye Service，CES）	查看监控指标
记录虚拟私有云相关的操作事件，便于日后的查询、审计和回溯	云审计服务（Cloud Trace Service，CTS）	查看审计日志
使用标签标识云资源，实现对虚拟私有云、子网等的分类和搜索。	标签管理服务（Tag Management Service，TMS）	管理虚拟私有云标签

版权所有 © 华为技术有限公司

8 计费说明

计费项

VPC本身不收取费用。

表 8-1 计费项信息

计费项	计费说明
弹性公网IP	如有互联网访问需求，您需要购买弹性公网IP。
二层连接网关	支持按需计费。公测期间免费。

弹性公网IP提供包年包月和按量付费两种计费模式。不同计费方式的弹性公网IP的计费组成不同，您可以根据使用需要选择。下表介绍各种计费方式的弹性公网IP的计费组成。

表 8-2 弹性公网 IP 的计费组成

计费模式	计费方式	IP保有费	带宽费用	公网流量费用
包年包月	按带宽计费	-	√	-
按需计费	按带宽计费	免除IP保有费：当与ECS、BMS、ELB等实例绑定时 收取IP保有费：当与实例解绑且未释放时	√	-
	按流量计费		-	√

说明

- “-”代表不收取该项费用；“√”代表收取该项费用。
- 弹性公网IP的收费标准请参考**产品价格详情**中“弹性公网IP”的内容。

版权所有 © 华为技术有限公司

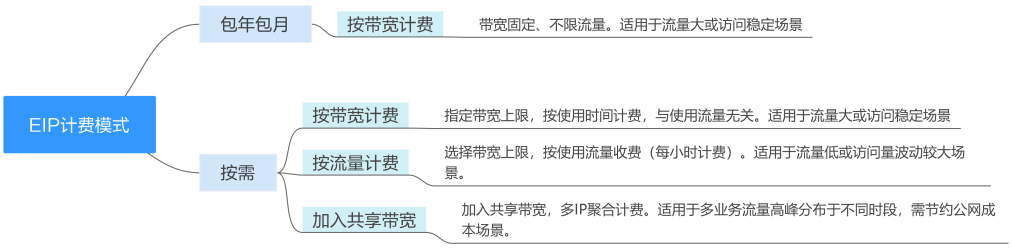
计费模式

公网带宽支持按固定带宽计费和按使用流量计费：

- 按固定带宽计费：是指华为云会按照您指定的带宽收费。使用过程中，您实际的带宽不会高于指定的带宽值。
- 按使用流量计费：是指华为云会按照您实际使用的流量收费，是一种后付费方式。华为云仅收取出网流量费用，不收取入网流量费用。

  为了防止突然爆发的流量产生较高的费用，您可以为出网带宽设置一个峰值。
- 根据带宽利用率可以计算出选择按固定带宽和按使用流量哪种计费方式更划算。按照经验，5M带宽以下时选择带宽包月往往比按流量划算，5M带宽以上时当带宽利用率大于20%一般情况下选择按固定带宽计费更划算。

图 8-1 EIP 计费模式



变更配置

- 修改带宽大小对费用影响如下：

表 8-3 费用影响

当前计费模式	变更场景	对费用的影响
按需	带宽大小变更（升配/降配）	变更成功后，新的计费方式将立即生效。
包年包月	增加带宽大小（补差价升配）	升配后新带宽大小将在原来已有的时间周期内立即生效。需按照与原规格的价格差异，结合已使用的时间周期，补上差价。 例如：（以下价格仅作示例，实际价格以**价格详情**为准） 客户于2018/11/1 购买了1Mbit/s的带宽，购买时长为1个月，此时价格为18.4元/月，客户使用余额支付18.4元，实付金额为18.4元。 客户在2018/11/24 将带宽升级为5Mbit/s，价格为92元/月。 这时，剩余天数为 30 - 24 = 6天，升配费用=92 / 30 * 6 - 18.4 / 30 * 6 = 14.72元。 了解更多变更资源计费信息，请参见**变更资源费用说明**。

版权所有 © 华为技术有限公司

当前计费模式	变更场景	对费用的影响
	降低带宽大小（续费降配）	续费成功后新的带宽大小将在新的计费周期生效。 • 续费降配订单支付成功后不可取消。 • 续费降配后，当前计费周期的剩余时间内不能再对带宽进行任何修改，请谨慎操作。
	临时升配（使用带宽加油包临时升配）	带宽加油包提供包年/包月带宽临时调整带宽使用。您可以在带宽生命周期内选择任意时间段增加临时带宽，带宽加油包到期后带宽自动回落。

- 弹性公网IP计费方式间的变更关系及对费用影响如下：

图 8-2 计费变更

表 8-4 费用影响

当前计费模式	变更场景	对费用的影响
按需	按流量计费与按带宽计费间变更	变更后新的计费方式将立即生效。
	转包年包月	您可以在页面或费用中心转包年包月，变更成功后，新的计费模式将立即生效。 按需按流量计费的不能直接转包年包月，需要先修改为按需按带宽计费，然后再转包年包月。
包年包月	转按需	您可以在费用中心转按需，包年包月资费到期后，新的按需资费才会生效。 包年包月转按需只能变更为按需按带宽计费。如想变更为按需按流量计费，请在包年包月转按需变更成功后，通过修改带宽规格，变更为按流量计费。

续费

如需续费，请在管理控制台**续费管理**页面进行续费操作。详细操作请参考**续费管理**。

到期与欠费

客户欠费后，可以查看欠费详情。为防止相关资源被停止或者释放，需要客户及时进行充值，帐号将进入欠费状态，需要在约定时间内支付欠款，详细操作请参考**欠费还款**。

版权所有 © 华为技术有限公司

9 权限管理

如果您需要对华为云上创建的VPC资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云帐号中给员工创建IAM用户，并授权来控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有VPC的使用权限，但是不希望他们拥有删除VPC等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用VPC，但是不允许删除VPC的权限，控制他们对VPC资源的使用范围。

如果华为云帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用VPC服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

VPC 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

VPC部署时通过物理区域划分。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问VPC时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对VPC服务，管理员能够控制IAM用户仅能对某一类网络资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，虚拟私有云（VPC）支持的API授权项请参见**策略及授权项说明**。

 版权所有 © 华为技术有限公司

如表9-1所示，包括了VPC的所有系统权限。

表 9-1 VPC 系统权限

策略名称	描述	策略类别	依赖关系
VPC FullAccess	对虚拟私有云的所有执行权限。	系统策略	无
VPC ReadOnlyAccess	对虚拟私有云的只读权限。	系统策略	无
VPC Administrator	对虚拟私有云的所有执行权限。拥有该权限的用户必须同时拥有Tenant Guest权限。	系统角色	依赖Tenant Guest策略，在同项目中勾选依赖的策略。

表9-2列出了VPC常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 9-2 常用操作与系统权限的关系

操作	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
创建VPC	x	√	√
修改VPC	x	√	√
删除VPC	x	√	√
查看VPC	√	√	√
创建子网	x	√	√
查看子网	√	√	√
修改子网	x	√	√
删除子网	x	√	√
创建安全组	x	x	√
查看安全组	√	x	√
修改安全组	x	x	√
删除安全组	x	x	√
添加安全组规则	x	x	√
查看安全组规则	√	x	√

版权所有 © 华为技术有限公司

操作	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
修改安全组规则	x	x	√
删除安全组规则	x	x	√
创建网络ACL	x	√	√
查看网络ACL	√	√	√
修改网络ACL	x	√	√
删除网络ACL	x	√	√
添加网络ACL规则	x	√	√
修改网络ACL规则	x	√	√
删除网络ACL规则	x	√	√
创建对等连接	x	√	√
修改对等连接	x	√	√
删除对等连接	x	√	√
创建路由表	x	√	√
删除路由表	x	√	√
添加路由	x	√	√
修改路由	x	√	√
删除路由	x	√	√

相关链接

- IAM产品介绍
- 创建用户并授权使用VPC
- 策略及授权项说明

版权所有 © 华为技术有限公司

10 基本概念

10.1 子网

子网是虚拟私有云内的IP地址块。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，子网网段不可重复。子网创建成功后，网段无法修改。

图 10-1 子网

默认情况下，同一个VPC的所有子网内的弹性云服务器均可以进行通信，不同VPC的弹性云服务器不能进行通信。

不同VPC的弹性云服务器可通过创建对等连接通信，具体参见**对等连接**。

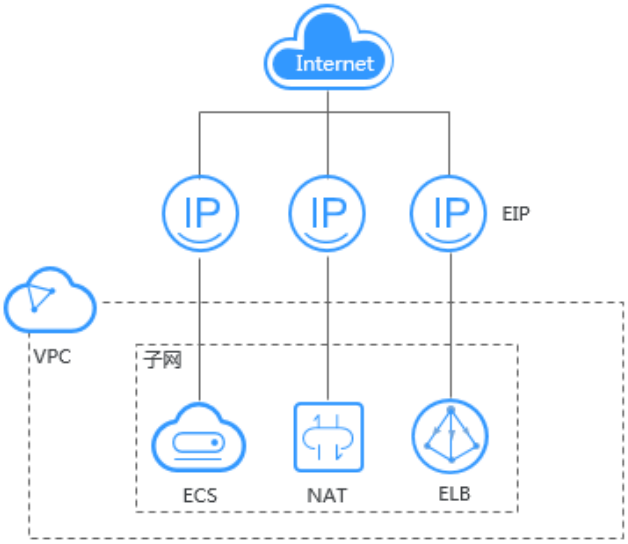
10.2 弹性公网 IP

弹性公网IP（Elastic IP，简称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。

一个弹性公网IP只能绑定一个云资源使用。

版权所有 © 华为技术有限公司

图 10-2 通过 EIP 访问公网



10.3 路由表

相关背景

当前在部分区域中，路由表已从虚拟私有云中解耦，解耦后路由表拥有独立入口，支持路由表与子网关联功能，请以实际界面为准。

- 未解耦：在虚拟私有云详情页的“路由表”页签，可对路由表进行操作。
- 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“路由表”，可对路由表进行操作。

图 10-3 路由表入口

已解耦的区域请参考**路由表(已解耦)**、**默认路由表和自定义路由表**和**路由**的相关描述。

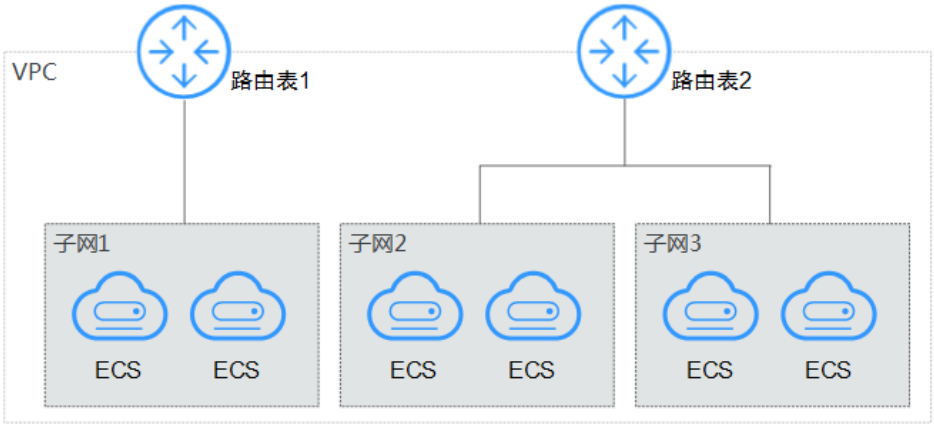
未解耦的区域请参考**路由表(未解耦)**相关描述。

版权所有 © 华为技术有限公司

路由表(已解耦)

路由表由一系列路由规则组成，用于控制虚拟私有云内子网的出流量走向。VPC中的每个子网都必须关联一个路由表，一个子网一次只能关联一个路由表，但一个路由表可以关联多个子网。

图 10-4 路由表



默认路由表和自定义路由表

用户创建虚拟私有云时，系统会自动为其生成一个默认路由表，创建子网后，子网会自动关联默认路由表。您可以在默认路由表中添加、删除和修改路由规则，但不能删除默认路由表。创建VPN、云专线、云连接服务时，默认路由表会自动下发路由，该路由不能删除和修改，您可以将子网关联到自定义路由表或者复制该条路由到自定义路由表中，在自定义路由表中添加、修改和删除路由。

您可以直接使用默认路由表，也可以为具有相同路由规则的子网创建一个自定义路由表，并将自定义路由表与子网关联。自定义路由表可以删除。

说明

当前自定义路由表需提交工单申请，如需使用自定义路由表，请在创建路由表页面单击“申请扩大配额”或在页面右上角单击“更多 > 工单 > 新建工单”申请扩大路由表配额。更多提交工单信息请参考**提交工单**

路由

路由即路由规则，在路由中通过配置目的地址、下一跳类型、下一跳地址等信息，来决定网络流量的走向。路由分为系统路由和自定义路由。

- 系统路由：系统自动添加且无法修改或删除的路由。

  创建路由表后，系统会自动在路由表中添加如下的系统路由，表示VPC内实例互通。

  - 目的地址是100.64.0.0/10、198.19.128.0/20的路由。
  - 目的地址是子网网段的路由。

    说明

    除以上系统路由外，系统还会自动添加目的地址是127.0.0.0/8的路由，表示本地回环地址。

版权所有 © 华为技术有限公司

- 自定义路由：可以修改和删除的路由。自定义路由的目地地址不能与系统路由的目地地址重叠。

  您可以通过添加自定义路由来自定义网络流量的走向，您需要指定目的地址、下一跳类型、下一跳地址。支持的下一跳类型如表10-1所示。

  表 10-1 下一跳类型

下一跳类型	说明
ECS实例	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例。
扩展网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的扩展网卡。
VPN网关	将指向目的地址的流量转发到一个VPN网关。
云连接	将指向目的地址的流量转发到云连接。
云专线网关	将指向目的地址的流量转发到一个云专线网关。
NAT网关	将指向目的地址的流量转发到一个NAT网关。
对等连接	将指向目的地址的流量转发到一个对等连接。
虚拟IP	将指向目的地址的流量转发到一个虚拟IP地址，可以通过该虚拟IP地址将流量转发到主备ECS。
VPC终端节点	将指向目的地址的流量转发到一个VPC终端节点。
云容器引擎	将指向目的地址的流量转发到一个云容器引擎的节点。

  说明

  - 当为默认路由表添加自定义路由时，下一跳类型不支持选择VPN网关。
  - 个别由系统下发的路由可供用户修改和删除，这取决于创建对端服务时是否已设置目的地址。

    例如，创建NAT GateWay时，没有指定目的地址，系统会自动下发一条自定义类型的路由，可供用户自行调整。而创建VPN网关时，可以指定远端子网，也就是路由表的目的地址，系统将下发系统类型的路由。如果在路由表页面更改将会导致与对端数据不一致，您可以前往对端服务页面修改远端子网来调整路由表中的路由规则。

路由表(未解耦)

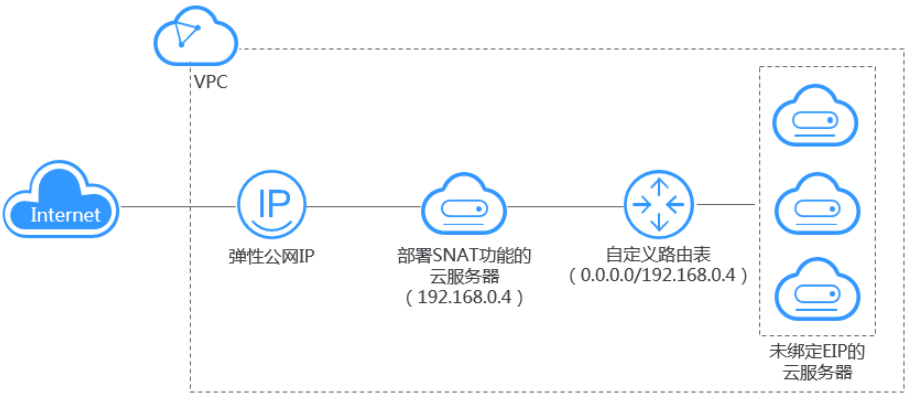
路由表是决定网络流量流向的规则集合。路由表允许用户添加自定义路由，使VPC内其他弹性云服务器通过绑定弹性公网IP的服务器访问Internet网络。

用户可以使用如下单点方式或者主备方式使用路由表功能通过绑定弹性公网IP的服务器访问Internet网络。

- 单点路由表场景如图10-5所示。

 版权所有 © 华为技术有限公司

图 10-5 单点路由表

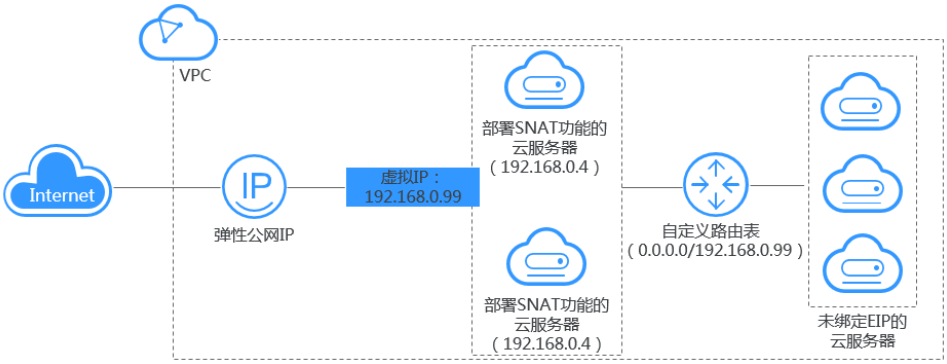


单点方式，VPC内没有绑定弹性公网IP的弹性云服务器通过路由到一台绑定了弹性公网IP且具有SNAT功能的弹性云服务器访问Internet。

单点方式通过为其他弹性云服务器所在的VPC增加路由表，使该VPC下的弹性云服务器可以访问Internet，其中路由表的下一跳地址为绑定了弹性公网IP的弹性云服务器的私有IP地址（即SNAT服务器的私有IP地址）。

- 主备式路由表场景如图10-6所示。

图 10-6 主备路由表



主备方式，VPC内没有绑定弹性公网IP的弹性云服务器通过路由到一组分别绑定了弹性公网IP且具有SNAT功能的弹性云服务器访问Internet。

主备方式通过为其他弹性云服务器所在的VPC增加路由表，使该VPC下的弹性云服务器可以访问Internet，其中路由表的下一跳地址为两台绑定了弹性公网IP的弹性云服务器的虚拟IP地址。

10.4 安全组

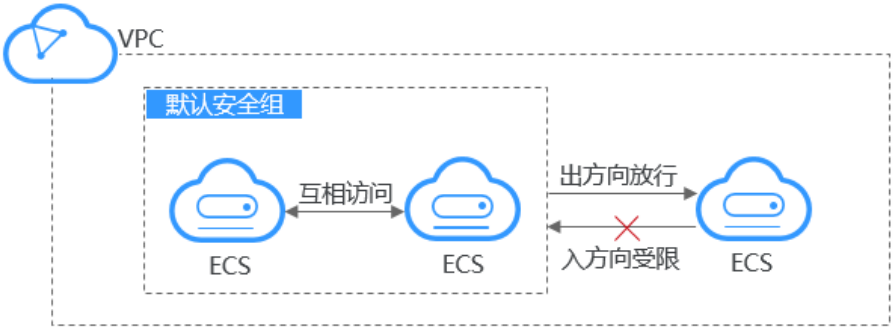
安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。

系统会为每个用户默认创建一个Sys-default安全组，默认安全组的规则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。

默认安全组如图10-7所示。

版权所有 © 华为技术有限公司

图 10-7 默认安全组



默认安全组规则如表10-2所示。

表 10-2 默认安全组 Sys-default 规则

方向	协议	端口范围	目的地址/源地址	说明
出方向	全部	全部	目的地址：0.0.0.0/0	允许所有出站流量的数据报文通过。
入方向	全部	全部	源地址：当前安全组(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	TCP	22	源地址：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	TCP	3389	源地址：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。

默认安全组和规则您可以直接使用，也可以根据需要创建自定义的安全组和规则。

说明

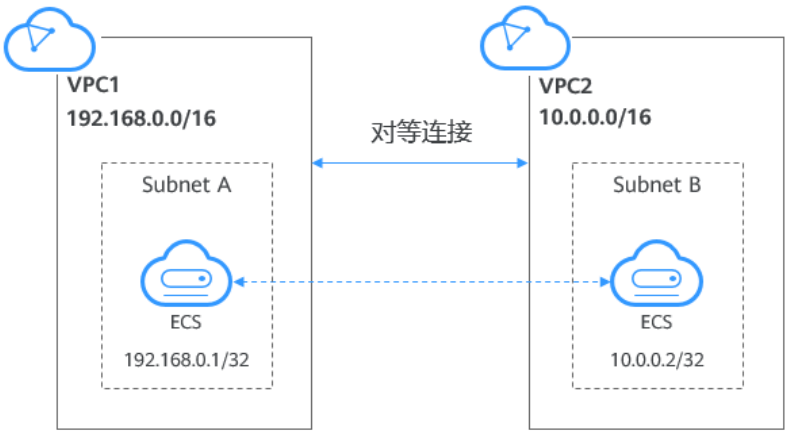
安全组需在网络互通的情况下生效。若实例属于不同VPC，但同属于一个安全组，此时实例不能互通。您可以使用对等连接等产品建立VPC连接互通，安全组才能对不同VPC内实例的流量进行访问控制。VPC连接请参见应用场景。

10.5 对等连接

对等连接是指两个VPC之间的网络连接。您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。同一区域内，您可以在自己的VPC之间创建对等连接，也可以在自己的VPC与其他帐户的VPC之间创建对等连接。不同区域间的VPC之间不能创建对等连接。

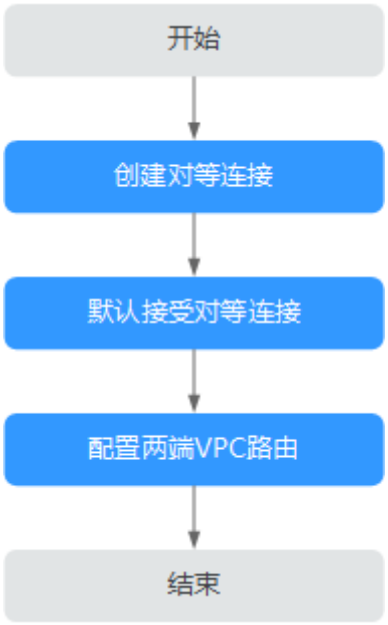
版权所有 © 华为技术有限公司

图 10-8 对等连接



- 同帐户的VPC创建对等连接流程。

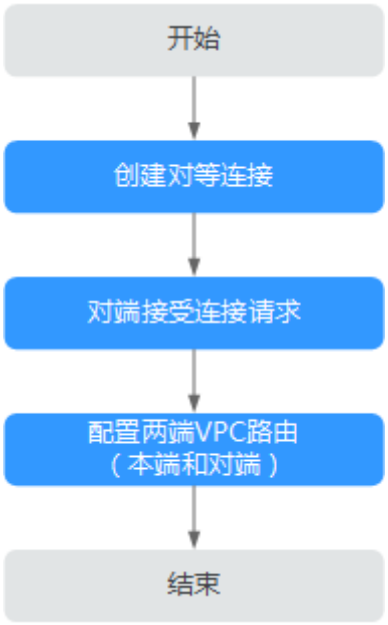
  图 10-9 同帐户的 VPC 创建对等连接流程

  在同一个帐户下，创建对等连接后，状态是已接受。您需要在两端VPC内添加对等连接路由信息，才能使两个VPC互通。
- 跨帐户的VPC创建对等连接流程。

版权所有 © 华为技术有限公司

图 10-10 跨帐户的 VPC 创建对等连接流程



跨帐户创建VPC对等连接时，一端VPC发起创建对等连接请求，对等连接状态为待接受。待对方接受该创建请求后，对等连接状态变为已接受，请求方和接受方须分别配置对等连接路由信息，才能使两个VPC互通。

添加对等连接路由信息时，如果两个VPC网段有重叠，这个对等连接添加的路由将可能会失效。如果要在具有重叠CIDR的VPC间建立对等连接，确保两个VPC下的所有子网CIDR都不重叠，此时，您可以通过VPC对等连接建立子网之间的对等关系。

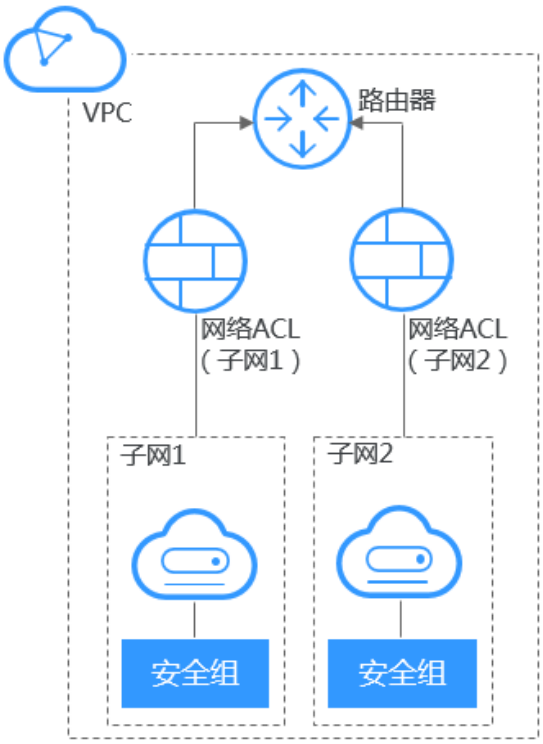
对等连接创建完成后，可以使用“ping”命令检查网络两端网络是否连通。

10.6 网络 ACL

网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。

版权所有 © 华为技术有限公司

图 10-11 安全组与网络 ACL



网络ACL与安全组类似，都是安全防护策略，当您想增加额外的安全防护层时，就可以启用网络ACL。安全组对弹性云服务器进行防护，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。

网络 ACL 基本信息

- 您的VPC默认没有网络ACL。当您需要时，可以创建自定义的网络ACL并将其与子网关联。关联子网后，网络ACL默认拒绝所有出入子网的流量，直至添加放通规则。
- 网络ACL可以关联多个子网，但一个子网同一时间只能关联一个网络ACL。
- 每个新创建的网络ACL最初都为未激活状态，直至您关联子网为止。
- 网络ACL是有状态的。如果您发送一个出站请求，且该网络ACL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，如果您发送一个入站请求，且该网络ACL的入站规则是放通的，那无论出站规则如何，都将允许该入站请求的响应流量可以出站。

  不同协议的连接跟踪老化时间不同，已建立连接状态的TCP协议连接老化时间是600s，ICMP协议老化时间是30s。对于其他协议，如果两个方向都收到了报文，连接老化时间是180s，如果只是单方向收到了一个或多个包，另一个方向没有收到包时，老化时间是30s。对于除TCP、UDP或ICMP以外的协议，仅跟踪IP地址和协议编号。

网络 ACL 默认规则

每个网络ACL都包含一组默认规则，如下所示：

- 默认放通同一子网内的流量。

版权所有 © 华为技术有限公司

- 默认放通目的IP地址为255.255.255.255/32的广播报文。用于配置主机的启动信息。
- 默认放通目的网段为224.0.0.0/24的组播报文。供路由协议使用。
- 默认放通目的IP地址为169.254.169.254/32，TCP端口为80的metadata报文。用于获取元数据。
- 默认放通公共服务预留网段资源的报文，例如目的网段为100.125.0.0/16的报文。
- 除上述默认放通的流量外，其余出入子网的流量全部拒绝，如**表10-3**所示。该规则不能修改和删除。

表 10-3 网络 ACL 默认规则

方向	优先级	动作	协议	源地址	目的地址	说明
入方向	*	拒绝	全部	0.0.0.0/0	0.0.0.0/0	拒绝所有入站流量
出方向	*	拒绝	全部	0.0.0.0/0	0.0.0.0/0	拒绝所有出站流量

规则优先级

- 网络ACL规则的优先级使用“优先级”值来表示，优先级的值越小，优先级越高，最先应用。优先级的值为“*”的是默认规则，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。若某个规则需要优先或落后生效，可在对应规则（需要优先或落后于某个规则生效的规则）前面或后面插入此规则。

应用场景

- 由于应用层需要对外提供服务，因此入方向规则必须放通所有地址，如何防止恶意用户的非正常访问呢?

  解决方案：通过网络ACL添加拒绝规则，拒绝恶意IP的访问。
- 隔离具有漏洞的应用端口，比如Wanna Cry，关闭445端口

  解决方案：通过网络ACL添加拒绝规则，拒绝恶意协议和端口，比如TCP：445端口。
- 子网内的通信无防护诉求，仅有子网间的访问限制。

  解决方案：通过网络ACL设置子网间的访问规则
- 对访问频繁的应用，调整安全规则顺序，提高性能。

  解决方案：网络ACL支持规则编排，可以把访问频繁的规则置顶。

10.7 虚拟 IP

虚拟IP（Virtual IP Address，简称VIP）是一个未分配给真实弹性云服务器网卡的IP地址。弹性云服务器除了拥有私有IP地址外，还可以拥有虚拟IP地址，用户可以通过其中任意一个IP（私有IP/虚拟IP）访问此弹性云服务器。同时，虚拟IP地址拥有私有IP地址

版权所有 © 华为技术有限公司

同样的网络接入能力，包括VPC内二三层通信、VPC之间对等连接访问，以及弹性公网IP、VPN、云专线等网络接入。

多个主备部署的弹性云服务器可以在绑定虚拟IP地址时选择同一个虚拟IP地址。用户可以为该虚拟IP地址绑定一个弹性公网IP地址，从互联网可以访问后端绑定了同一个虚拟IP地址的多个主备部署的弹性云服务器，增强容灾性能。

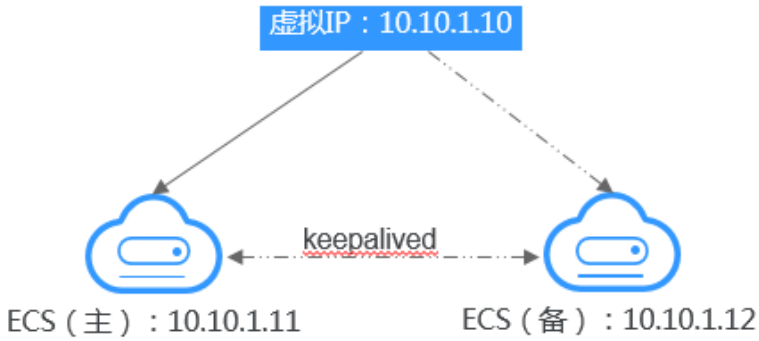
典型组网

虚拟IP主要用在弹性云服务器的主备切换，达到高可用性HA（High Availability）的目的。当主服务器发生故障无法对外提供服务时，动态将虚拟IP切换到备服务器，继续对外提供服务。本节介绍两种典型的组网模式。

- **典型组网1：** HA高可用性模式

  场景举例：如果您想要提高服务的高可用性，避免单点故障，可以用“一主一备”或“一主多备”的方法组合使用弹性云服务器，这些弹性云服务器对外表现为一个虚拟IP。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。

  图 10-12 HA 高可用性模式组网图

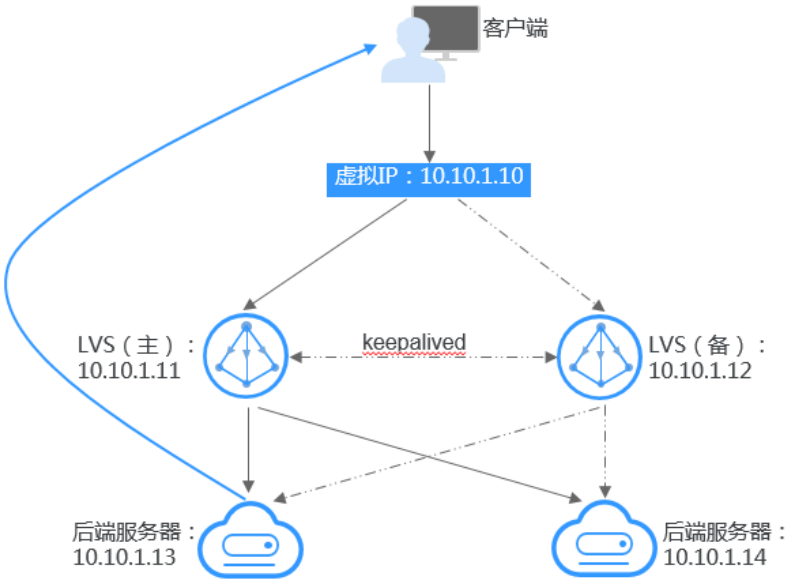
  - 将2台同子网的弹性云服务器绑定同一个虚拟IP。
  - 将这2台弹性云服务器配置Keepalived，实现一台为主服务器，一台为备份服务器。Keepalived可参考业内通用的配置方法，此处不做详细介绍。

- **典型组网2：** 高可用负载均衡集群

  场景举例：如果您想搭建高可用负载均衡集群服务，您可以采用Keepalived + LVS(DR)来实现。

版权所有 © 华为技术有限公司

图 10-13 高可用负载均衡集群



- 将2台弹性云服务器绑定同一个虚拟IP。
- 将绑定了虚拟IP的这2台弹性云服务器配置Keepalived+LVS（DR模式），组成LVS主备服务器。这2台服务器作为分发器将请求均衡地转发到不同的后端服务器上执行。
- 配置另外2台弹性云服务器作为后端RealServer服务器。
- 关闭2台后端RealServer弹性云服务器的源/目的检查。

Keepalived + LVS调度服务端安装配置以及后端RealServer服务器配置可以参考业内通用的配置方法，此处不做详细介绍。

应用场景

- 场景一：通过弹性公网IP访问虚拟IP。

  您的应用需要具备高可用性并通过Internet对外提供服务，推荐使用弹性公网IP绑定虚拟IP功能。
- 场景二：通过VPN/云专线/对等连接访问虚拟IP。

  您的应用需要具备高可用性并且需要通过Internet访问，同时需要具备安全性（VPN），保证稳定的网络性能（云专线），或者需要通过其他VPC访问（对等连接）。

10.8 弹性网卡

弹性网卡（Elastic Network Interfaces，以下简称ENI）即虚拟网卡，您可以通过创建并配置弹性网卡，并将其附加到您的云服务器实例（包括弹性云服务器和裸金属服务器）上，实现灵活、高可用的网络方案配置。

弹性网卡类型

- 主弹性网卡：在创建云服务器实例时，随实例默认创建的弹性网卡称作主弹性网卡。主弹性网卡无法与实例进行解绑。

版权所有 © 华为技术有限公司

- 扩展弹性网卡：您可以创建扩展弹性网卡，将其附加到云服务器实例上，您也可以将其从实例上进行解绑。每台实例可附加的扩展弹性网卡数量由实例规格决定。

应用场景

- 灵活迁移

  通过将弹性网卡从云服务器实例解绑后再绑定到另外一台服务器实例，保留已绑定私网IP、弹性公网IP和安全组策略，无需重新配置关联关系，将故障实例上的业务流量快速迁移到备用实例，实现服务快速恢复。

- 业务分离管理

  可以为服务器实例配置多个分属于同一VPC内不同子网的弹性网卡，特定网卡分别承载云服务器实例的内网、外网、管理网流量。针对子网可独立设置访问安全控制策略与路由策略，弹性网卡也可配置独立安全组策略，从而实现网络隔离与业务流量分离。

约束与限制

- 云服务器实例与扩展弹性网卡必须在同一VPC，可以分属于不同安全组。
- 主弹性网卡不能解绑服务器。
- 云服务器可附加的扩展弹性网卡数量由云服务器实例规格决定。具体请参见**规格清单**。
- 弹性网卡不支持直接访问华为云内公共云服务，如内网DNS等，推荐使用VPCEP访问华为云公共云服务，具体参见**购买连接“接口”型终端节点服务的终端节点**。

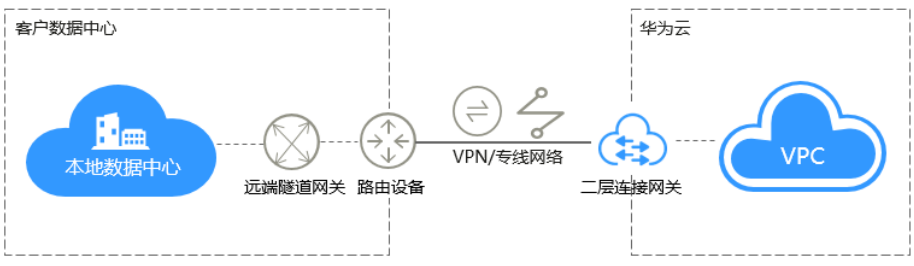
10.9 二层连接网关

二层连接网关（Layer 2 Connection Gateway，以下简称L2CG）是一种虚拟隧道网关，可基于云专线/VPN网络建立云上与云下之间的二层网络，解决云上和云下网络二层互通问题，允许您在不改变子网、IP规划的前提下将数据中心或私有云主机业务部分迁移上云。

通过云专线/VPN，建立的是云上与云下的三层网络通道，要求云上与云下子网网段不重叠。而当数据中心与云上子网网段相同，且需要云上与云下服务器在该相同子网网段互通时，您就可以通过二层连接网关来解决云上与云下二层网络通信问题。

二层连接网关组网图如**图1 L2CG组网图**所示。

图 10-14 二层连接网关组网图



版权所有 © 华为技术有限公司

二层连接网关作为虚拟私有云的隧道网关，与用户本地数据中心侧的隧道网关对应，可基于云专线/VPN网络使虚拟私有云与用户数据中心之间建立二层网络。

二层连接可将虚拟私有云的子网接入到二层连接网关中，并指定二层连接网关与企业数据中心侧的隧道网关建立连接，使虚拟私有云的子网与企业数据中心侧的子网建立二层通信。

10.10 IP 地址组

IP地址组是多个IP地址的集合，可被安全组规则引用，可统一管理具有相同安全要求或需要频繁修改的IP地址。通过使用IP地址组，可有效应对需要重复多次编辑安全组规则的场景，方便管理。

您需要先创建一个IP地址组，添加需要统一管理的IP地址，然后配置安全组规则时，就可以引用该IP地址组，此安全组规则将对IP地址组中所有IP地址生效。

10.11 区域和可用区

什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图10-15阐明了区域和可用区之间的关系。

图 10-15 区域和可用区

目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见华为云全球站点。

版权所有 © 华为技术有限公司

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“南非-约翰内斯堡”区域。
  - 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

    说明

    “拉美-圣地亚哥”区域位于智利。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

版权所有 © 华为技术有限公司