企业路由器

产品介绍

文档版本 01

发布日期 2024-10-28

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 什么是企业路由器

企业路由器（Enterprise Router, ER）可以连接虚拟私有云（Virtual Private Cloud, VPC）或本地网络来构建中心辐射型组网，是云上大规格、高带宽、高性能的集中路由器。企业路由器使用边界网关协议（Border Gateway Protocol, BGP），支持路由学习、动态选路以及链路切换，极大的提升网络的可扩展性及运维效率，从而保证业务的连续性。

- 您可以将虚拟私有云接入企业路由器，快速打通云上网络，具体可参见**通过企业路由器实现同区域VPC互通**。
- 您可以将两个及以上企业路由器接入云连接（Cloud Connect, CC）的中心网络中，构成ER对等连接，实现云上跨区域网络互通，具体请参见**通过企业路由器和云连接中心网络实现跨区域VPC互通**。
- 您可以将云专线（Direct Connect, DC）或者虚拟专用网络（Virtual Private Network, VPN）接入企业路由器，打通线下互联网数据中心（Internet Data Center, IDC）和云上网络，具体可参见**通过企业路由器和云专线构建混合云组网（全域接入网关DGW）**。
- 您可以将企业连接网络（Enterprise Connect Network，ECN）接入企业路由器，帮助企业实现本地网络和云上网络之间的互联互通，具体可参见**通过企业路由器和企业连接实现企业本地网络和云上VPC互通**。
- 您可以通过企业路由器、虚拟私有云VPC和云防火墙（Cloud Firewall，CFW）构建组网，实现云上VPC间的流量防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，具体可参见**通过企业路由器和云防火墙构建组网**。

图1-1和**图1-2**分别展示了不使用和使用企业路由器构建的网络拓扑，详细的对比说明如**表1-1**所示。

图 1-1 不使用企业路由器构建网络

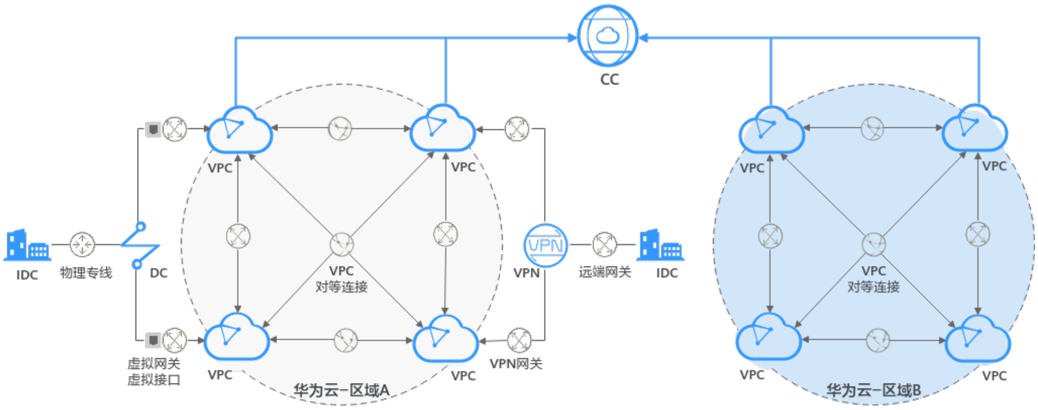


图 1-2 使用企业路由器构建网络

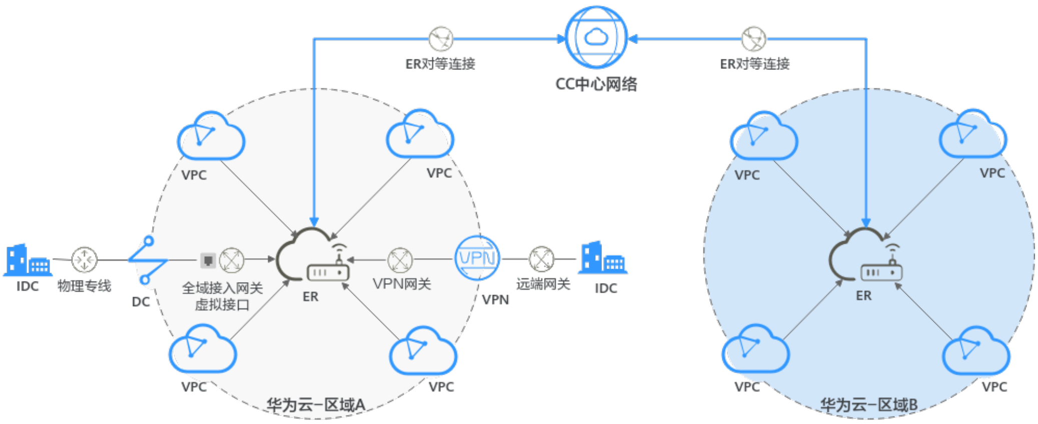


表 1-1 网络拓扑对比说明

对比项	不使用企业路由器	使用企业路由器	企业路由器价值
同区域多个VPC互通	• 同区域4个VPC需要建立6个对等连接实现互通。 • 4个VPC路由表中各需要配置3条对端VPC的路由，共需要配置12条路由。	• 将同区域4个VPC接入ER中，ER可以在接入的所有VPC中转发流量。 • ER可以自动学习VPC网段到路由表中，只需要在4个VPC路由表中配置到ER的路由。	• 免去大量的对等连接配置。 • 减少路由条目配置及维护工作量。
多个VPC跨区域互通	所有区域需要互通的VPC均需要接入云连接中。	只需要将每个区域的ER接入云连接中心网络中。	• 无需在云连接中接入所有网络实例，简化网络拓扑。 • 支持路由学习，无需手工配置路由，快速构建组网。

对比项	不使用企业路由器	使用企业路由器	企业路由器价值
线下IDC和云上多个VPC互通	需要为每个和IDC互通的VPC建立专线或者VPN。	将专线接入ER，多个VPC可以共享专线或者VPN。	• 支持路由学习，免去繁复配置，降低维护难度。 • 多条链路之间联动，实现负载分担或互为主备。

通过对比，可以看出，使用企业路由器构建的网络拓扑更简洁，可扩展性高，同时网络维护工作也更简单。

2 产品优势

企业路由器是一个支持路由学习的高性能集中路由器，本章节为您介绍企业路由器的优势。

高性能

企业路由器采用集群部署，独享资源确保高性能，满足大规模组网的业务负荷。

高可用

企业路由器可同时部署在多个可用区，打造双活或者多活模式，无缝实时切换，确保业务连续性。

管理简单

企业路由器可以在接入的所有网络实例之间路由流量，可以简化网络拓扑，降低网络管理难度，提升网络运维效率。可以减少的工作说明如下：

- 对于VPC互通，不再需要您频繁创建多个VPC对等连接，维护每个VPC路由表。
- 对于VPC和DC/VPN互通，不用接入多条线路，多个VPC可以共享专线/VPN。
- 企业路由器支持路由学习，能够自动进行路由信息的更新和同步，当网络拓扑变更时，能够自动收敛，无需手工配置、变更繁琐的路由条目。

多链路联动

企业路由器使用BGP路由协议，实现多个接入链路之间的联动，多链路可以做负载分担或者互为主备，单链路故障秒级切换，打造高可靠网络，保障业务的连续性。

3 应用场景

企业路由器可以助力客户打造云上、云下、跨云的复杂网络，本章节提供以下典型的应用场景：

- **场景一：多个VPC灵活互通和隔离，共享专线**
- **场景二：多条专线链路动态选路和切换**
- **场景三：专线+VPN双链路主备**
- **场景四：跨区域、跨云高可靠骨干网络**
- **场景五：构建VPC间的边界防火墙**

场景一：多个 VPC 灵活互通和隔离，共享专线

图 3-1 多个 VPC 灵活互通和隔离，共享专线

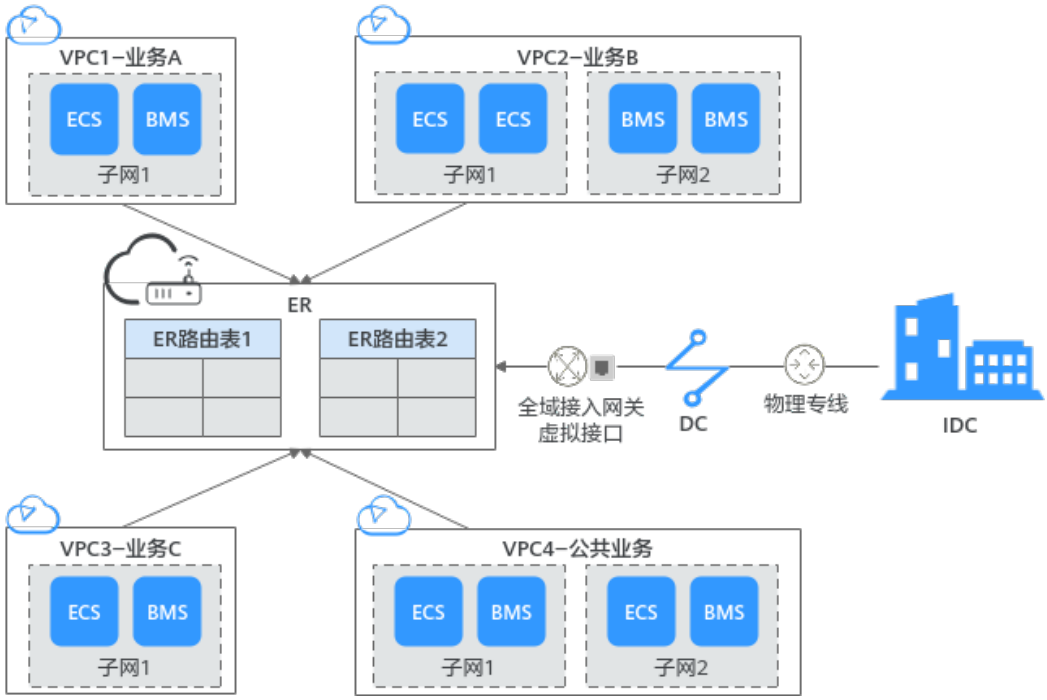


表 3-1 场景一说明

客户场景	企业客户业务上云，多个业务网络之间需要互相访问或者隔离，并且业务网络需要和线下IDC互通。比如X企业的业务部署在公有云内，业务A、业务B、业务C相互独立，因此三个业务所在的VPC网络隔离。同时，业务A、业务B、业务C均需要访问VPC4内的公共业务以及线下IDC。
客户痛点	• VPC之间的网络互通和隔离，通过VPC对等连接来实现。点对点的连接导致网络拓扑复杂，路由配置繁多，管理难度大。 • 公共服务VPC和每个业务VPC互通，需要配置大量的对等连接和路由，对服务规格要求高。VPC对等连接的规格不适用大规模组网，具体如下： – 一个租户在一个区域最多可以配置50个对等连接数量。 – VPC的一个路由表最多支持200条路由。 • VPC访问线下IDC，通过云专线DC，需要为每个VPC都需要配置专线，成本高。
企业路由器价值	• 通过将VPC关联至企业路由器中不同的路由表，灵活实现VPC之间的互通和隔离，网络拓扑简洁，配置简单易管理。 • 企业路由器可以在所有VPC之间路由流量，无需配置大量对等连接，同时企业路由器支持大规格路由条目，适合企业复杂组网场景，具体如下： – 每个企业路由器的路由表最大支持2000条路由。 • 多个VPC可以共享专线访问线下IDC，免去多条专线配置，降低成本。
最佳实践	**通过企业路由器实现同区域VPC隔离**

场景二：多条专线链路动态选路和切换

图 3-2 多条专线链路动态选路和切换

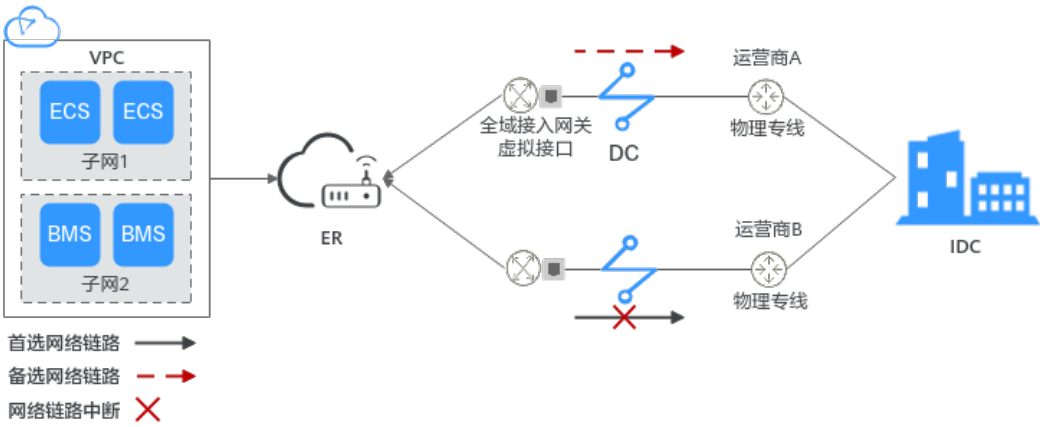


表 3-2 场景二说明

客户场景	客户业务一部分部署在公有云，一部分部署在线下IDC中，云上业务访问线下IDC要求高带宽、高可靠，因此部署了两条DC专线链路，两条专线链路之间相互独立。
客户痛点	部署的两条专线链路之间相互独立，无法联动做负载分担或者互为主备。
企业路由器价值	专线接入企业路由器后，可以实现专线的动态选路和切换： • 多个链路之间进行负载分担实现高带宽，同时保证了高可靠性。 • 多个链路之间互为主备，单链路故障秒级切换，避免了单点故障带来的业务中断。
最佳实践	**通过企业路由器构建DC双链路负载混合云组网（全域接入网关DGW）**

场景三：专线+VPN 双链路主备

图 3-3 专线+VPN 双链路主备

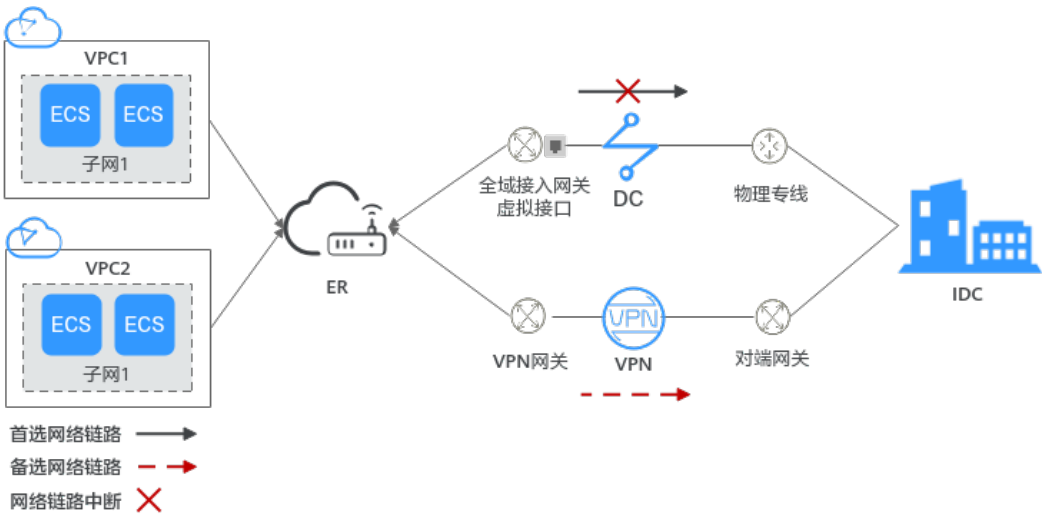
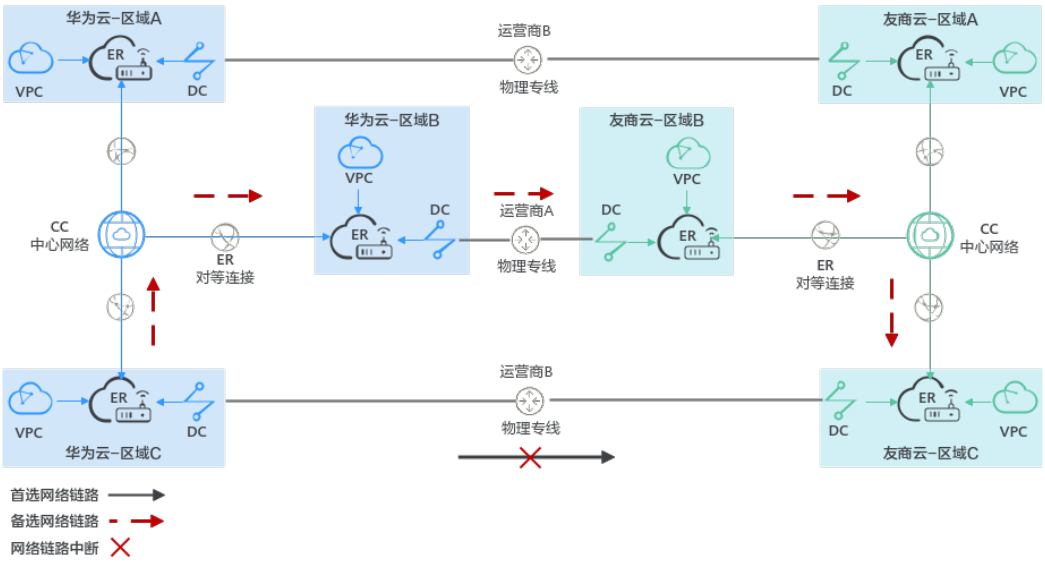


表 3-3 场景三说明

客户场景	企业客户的业务同时部署在公有云和线下IDC中，云上业务访问IDC使用单专线不满足可靠性要求。
客户痛点	为了控制成本，客户无法采用双专线方案。
企业路由器价值	此处部署了一条专线链路和一条VPN链路，通过企业路由器构建专线+VPN主备双链路的混合云组网，当专线链路故障时，可自动切换到VPN链路，降低网络中断对业务造成的影响。
最佳实践	**通过企业路由器构建DC/VPN双链路主备混合云组网（全域接入网关DGW）**

场景四：跨区域、跨云高可靠骨干网络

图 3-4 跨区域、跨云高可靠骨干网络



说明

图3-4中友商云对应的ER、CC、DC、VPC名称仅为示意，实际云服务名称请以友商为准。

表 3-4 场景四说明

客户场景	为了提升业务容灾能力，企业客户业务同时部署在多个公有云上。并且为了业务就近接入，每一个公有云上又横跨多个区域。客户没有自建骨干网，使用公有云的骨干网实现多云多区域网络互通。 比如公司A，其业务涉及多个地区，因此部署在华为云，以及友商云的多个区域内。不同公有云之间通过DC专线链路（不同运营商）互通，同一个公有云不同区域之间通过公有云提供的骨干网（云连接CC的中心网络）互通。
客户痛点	• 多云多区域的VPC实现互通，需要配置管理大量路由条目，维护成本高。 • 专线链路和云连接链路无法联动做负载分担或者主备。

企业路由器价值	在客户的跨云组网中，不同公有云通过专线链路连通，同一个公有云内通过云连接中心网络连通不同区域。 • 企业路由器可以在接入的所有网络实例之间转发流量，精简网络拓扑。同时支持路由学习，网络变化时可以自动收敛，降低维护管理难度。 • 企业路由器可以实现专线和云连接之间的链路联动，用作负载分担或者主备。VPC在不同云之间转发流量，业务优先走运营商专线链路，专线链路故障后，能够动态切换到备份的云连接链路和其他专线链路。 假如华为云-区域C和友商云-区域C之间的专线链路通信故障，则流量可以先由华为云-区域C经过云连接链路转发至华为云-区域B，再经过专线链路转发至友商云-区域B，最后经过云连接链路抵达友商云-区域C，保障了业务的连续性。
最佳实践	**通过企业路由器和云连接中心网络实现跨区域VPC互通** **通过企业路由器和云专线实现线下IDC和云上VPC互通**

场景五：构建 VPC 间的边界防火墙

图 3-5 构建 VPC 间的边界防火墙

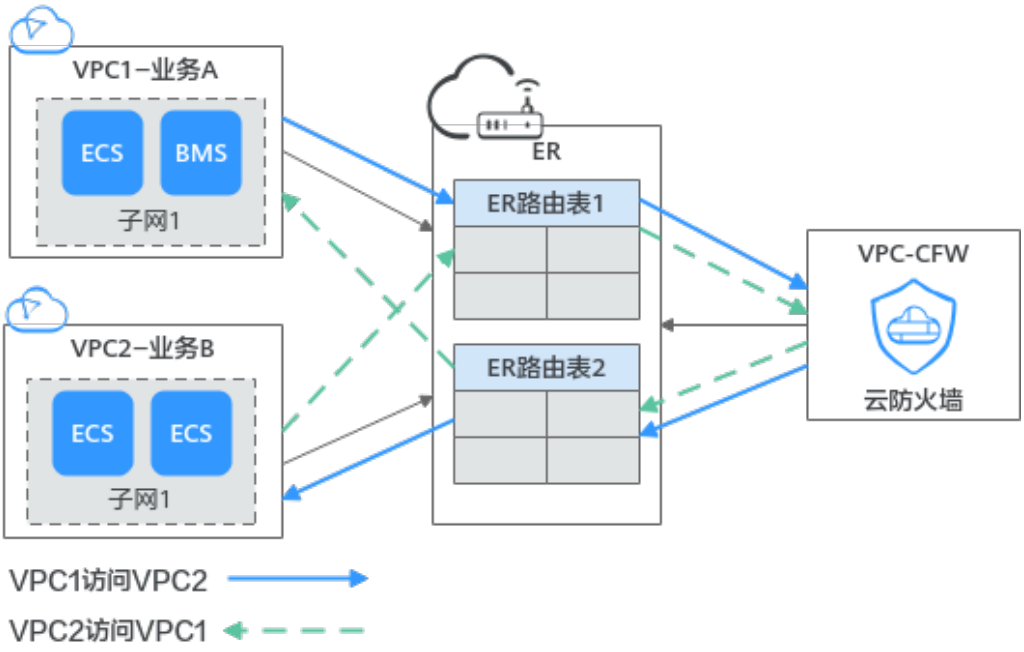


表 3-5 场景五说明

客户场景	企业客户的业务A部署在VPC1内，业务B部署在VPC2内，出于安全考虑，业务A和业务B互访的流量需要经过防火墙过滤清洗。
客户痛点	希望快速搭建满足安全要求的云上组网。

企业路由器价值	客户在组网中部署云防火墙，通过将VPC和云防火墙关联至企业路由器中不同的路由表，控制VPC1和VPC2互访流量经过防火墙。
最佳实践	**通过企业路由器和云防火墙构建组网**

4 产品功能

企业路由器提供丰富的功能供您灵活配置服务，具体说明如表4-1所示。

- 提供添加连接、创建自定义路由表、创建关联、创建传播、添加路由等丰富的网络构建和路由管理功能。
- 提供权限管控、标签管理、配额管理等提升服务使用安全和便捷的多种实用功能。

表 4-1 企业路由器功能概览

功能	功能描述	参考链接
企业路由器	您可以将企业路由器看作一个支持路由学习的高性能集中路由器，创建企业路由器时，您可以设置部署区域、可用区、名称等参数。 企业路由器创建完成后，您可以根据业务使用情况灵活调整部分参数。	创建企业路由器
连接	为企业路由器添加网络实例对应的连接，即表示将网络实例接入企业路由器中。 不同类型连接的添加方法不同： • 虚拟私有云（VPC）：通过企业路由器控制台来添加。 • 虚拟网关（VGW）： 通过云专线控制台来添加。 • VPN网关（VPN）： 通过虚拟专用网络控制台来添加。 • 对等连接（Peering）：通过云连接中心网络控制台加载不同区域的企业路由器来添加。 • 企业连接网（ECN）：通过企业连接控制台来添加。 • 全域接入网关（DGW）：通过云专线控制台来添加。 • 云防火墙（CFW）：通过云防火墙控制台来添加。	连接概述

功能	功能描述	参考链接
路由表	路由表是企业路由器发送报文的依据，包含连接的关联关系、传播关系以及路由信息。 一个企业路由器可以拥有多个路由表，您可以将连接关联至不同的路由表，从而实现网络实例的灵活互通或者隔离。	路由表概述
关联	关联是将连接关联至ER路由表中，您可以通过以下方法创建关联： • 手动创建：选择任意路由表，并在路由表中为连接创建关联。 • 自动创建：开启“默认路由表关联”功能，指定默认路由表，系统会自动为连接在默认路由表中创建关联。	关联概述
传播	传播是企业路由器和连接的路由学习关系，您可以通过以下方法创建传播： • 手动创建：选择任意路由表，并在路由表中为连接创建传播。 • 自动创建：开启“默认路由表传播”功能，指定默认路由表，系统会自动为连接在默认路由表中创建传播。	传播概述
路由	路由是目的地址、下一跳以及路由类型等信息组成。路由分为两种： • 自动学习的传播路由 • 手动添加的静态路由	路由概述
共享	依托于资源访问管理服务（Resource Access Manager，简称RAM），可以实现跨账号共享企业路由器，您可以将账号A所属的企业路由器同时共享给多个其他账号，比如账号B、账号C以及账号D等使用者。 使用者可以在共享企业路由器中添加连接，将自己名下的网络实例加入该企业路由器中，实现多个账号内的网络实例接入同一个企业路由器构建组网的需求。	共享概述
流日志	通过流日志功能可以实时记录企业路由器中连接的流量日志信息。通过这些日志信息，您可以监控连接的网络流量、进行网络攻击分析等，帮助您实现高效的网络运维。 企业路由器流日志功能支持采集以下连接的流日志： • 虚拟私有云（VPC） • 虚拟网关（VGW） • VPN网关（VPN） • 对等连接（Peering） • 全域接入网关（DGW）	流日志概述

功能	功能描述	参考链接
监控	通过云监控服务，您可以监控企业路由器实例以及企业路由器连接的网络情况。	**支持的监控指标**
审计	通过云审计服务，您可以记录与企业路由器相关的操作事件，便于日后的查询、审计和回溯。	**支持审计的关键操作**
权限	针对位于华为云上的企业路由器资源，您可以通过IAM进行精细的权限管理，为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，从而实现资源的安全管控。	**创建用户并授权使用ER**
标签	标签用于标识云资源，可通过标签实现对云资源的分类和搜索。您可以为企业路由器、路由表等资源添加标签。	**标签概述**
配额	为防止资源滥用，平台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企业路由器、每个企业路由器添加多少个连接、每个路由表可以添加多少条路由等。	**配额概述**

5 企业路由器工作原理

您可以在企业路由器中添加多种类型的网络连接，快速构建多元化组网，满足您的多种业务诉求。企业路由的使用方法如图5-1所示：首先，创建您的企业路由器。其次，在企业路由器中添加连接，不同类型的连接添加方法不同。最后，待连接添加完成后，根据网络规划配置路由。

当前企业路由器支持的连接如下：

- “虚拟私有云（VPC）”连接：接入同区域的虚拟私有云VPC。
- “虚拟网关（VGW）”连接：接入同区域云专线DC的虚拟网关。
- “VPN网关（VPN）”连接：接入同区域的虚拟专用网络VPN。
- “对等连接（Peering）”连接：通过云连接中心网络，接入不同区域的其他企业路由器。
- “企业连接网（ECN）”连接：接入同区域或者不同区域的企业连接网络。
- “全域接入网关（DGW）”连接：接入同区域云专线DC的全域接入网关。
- “云防火墙（CFW）”连接：接入同区域的云防火墙。

图 5-1 企业路由器使用方法

当您了解了企业路由器的使用方法后，接下来将为您详细介绍企业路由器的工作原理。工作原理如图5-2所示，详细说明请参见表5-2。

图 5-2 企业路由器工作原理图

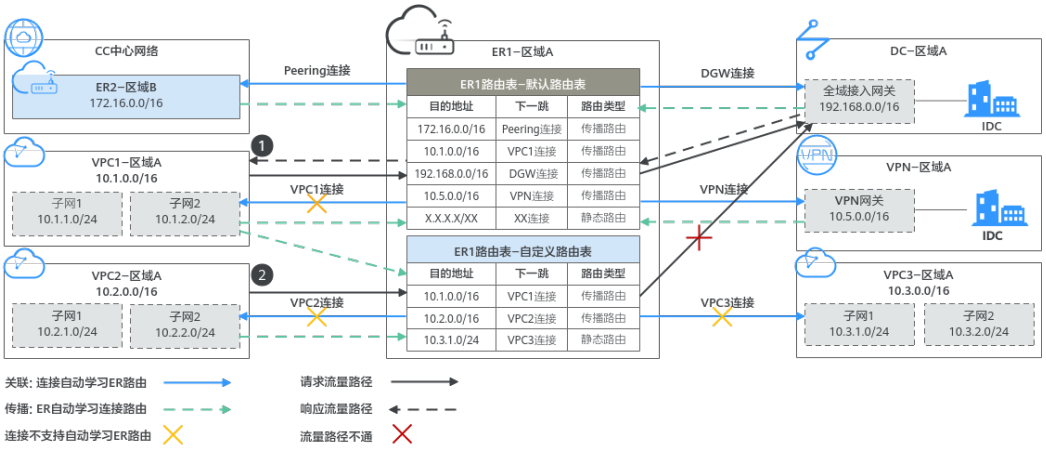


表 5-1 网络流量路径说明

序号	路径	说明
1	请求路径：VPC1→DC全域接入网关	从VPC1去往DC全域接入网关的流量，从VPC1抵达ER1后，会根据ER1默认路由表中DGW连接的传播路由寻址转发。
	响应路径：DC全域接入网关→VPC1	从DC全域接入网关返回VPC1的流量，从全域接入网关抵达ER1后，会根据ER1默认路由表中VPC1连接的传播路由寻址转发。
2	请求路径：VPC2→DC全域接入网关	从VPC2去往DC全域接入网关的流量，从VPC2抵达ER1后，由于VPC2关联的ER1自定义路由表中没有DGW连接的路由信息，因此无法送达。

表 5-2 企业路由器工作原理说明

序号	原理	网络实例说明
1	在企业路由器中添加若干**连接**。	将不同的网络实例接入区域A的ER1中： ● 同区域： – “虚拟私有云（VPC）”连接：VPC1、VPC2、VPC3 – “全域接入网关（DGW）”连接：全域接入网关 – “VPN网关（VPN）”连接：VPN网关 ● 跨区域： “对等连接（Peering）”连接：区域B的ER2

序号	原理	网络实例说明
2	将连接**关联**至ER**路由表**。 一个连接只能关联至一个ER路由表。	• VPC1关联ER1默认路由表，并通过传播关系将路由信息分别传播至ER1默认路由表和ER1自定义路由表，这属于VPC1连接的传播路由。 • VPC2关联ER1自定义路由表，并通过传播关系将路由信息传播至ER1自定义路由表，这属于VPC2连接的传播路由。 • VPC3关联ER1自定义路由表，没有创建传播关系，而是在ER1自定义路由表中直接添加路由，这属于VPC3连接的静态路由。 • DC全域接入网关关联ER1默认路由表，并通过传播关系将路由信息传播至ER1默认路由表，这属于DGW连接的传播路由。 • VPN网关关联ER1的默认路由表，并通过传播关系将路由信息传播至ER1默认路由表，这属于VPN连接的传播路由。 • 区域B的ER2通过CC和区域A的ER1构建Peering连接，该Peering连接关联至ER1默认路由表，并通过传播关系将路由信息传播至ER1默认路由表，即Peering连接的传播路由。
3	为连接创建**传播**，将连接**路由**传播至ER**路由表**。 一个连接可以和多个ER路由表建立传播关系。	

连接

将网络实例接入企业路由器中，则需要为网络实例在企业路由器中添加对应的连接。企业路由器支持接入多种网络实例，不同网络实例对应的连接类型不同，具体说明如**表5-3**所示。

表 5-3 连接说明

连接类型	网络实例
虚拟私有云（VPC）	虚拟私有云VPC。
虚拟网关（VGW）	云专线DC的虚拟网关。
VPN网关（VPN）	虚拟专用网络VPN。
对等连接（Peering）	位于其他区域的另一个企业路由器ER。通过云连接中心网络加载不同区域的企业路由器来创建“对等连接（Peering）”连接。
企业连接网（ECN）	企业连接中的企业连接网络ECN。
全域接入网关（DGW）	云专线DC的全域接入网关。

连接类型	网络实例
云防火墙（CFW）	云防火墙

路由表

路由表是企业路由器发送报文的依据，包含了连接的关联关系、传播关系以及路由信息。路由表分为自定义路由表和默认路由表，具体说明如表5-4所示。

表 5-4 路由表说明

路由表类型	说明
自定义路由表	您可以在企业路由器中创建多个路由表，通过不同的路由策略实现网络实例的灵活互通和隔离。
默认路由表	开启“默认路由表关联”和“默认路由表传播”功能，并指定默认路由表，系统会自动为新接入的连接在默认路由表中创建关联和传播。 默认路由表可以是自定义路由表，不指定的话系统会自动创建一个路由表作为默认路由表，支持修改。

关联

关联是将连接关联至ER路由表中，一个连接只能关联至一个ER路由表，将连接关联至ER路由表后，可以实现以下功能：

- 路由转发：来自连接的报文根据它关联的路由表进行转发。
- 路由学习：将关联路由表中的路由信息自动学习到连接网络中。

对于不同类型的连接，是否支持路由学习，具体如表5-5所示。

表 5-5 关联说明

连接类型	路由学习
虚拟私有云（VPC）	不支持
虚拟网关（VGW）	支持
VPN网关（VPN）	支持
对等连接（Peering）	支持
企业连接网（ECN）	支持

连接类型	路由学习
全域接入网关（DGW）	支持
云防火墙（CFW）	不支持

传播

传播是企业路由器和连接的路由学习关系，一个连接可以和多个ER路由表建立传播关系，为连接创建传播后，可以将连接的路由信息自动学习到ER路由表中。

对于不同类型的连接，传播路由的学习内容有差异，具体如表5-6所示。

表 5-6 传播说明

连接类型	路由学习内容
虚拟私有云（VPC）	VPC的网段
虚拟网关（VGW）	全部路由信息
VPN网关（VPN）	全部路由信息
对等连接（Peering）	全部路由信息
企业连接网（ECN）	全部路由信息
全域接入网关（DGW）	全部路由信息
云防火墙（CFW）	云防火墙承载VPC的网段

路由

路由是网络报文转发的依据，包含目的地址、下一跳以及路由类型等信息。路由说明如表5-7所示。

表 5-7 路由说明

路由类型	路由说明	支持的连接类型
传播路由	通过传播自动学习的路由，创建传播时会自动创建路由，不支持修改和删除。	• 虚拟私有云（VPC） • 虚拟网关（VGW） • VPN网关（VPN） • 对等连接（Peering） • 全域接入网关（DGW） • 企业连接网（ECN） • 云防火墙（CFW）
静态路由	手动创建的路由，支持修改和删除。	• 虚拟私有云（VPC） • 对等连接（Peering） • 云防火墙（CFW）

6 计费说明

企业路由器中可以接入多种连接构建组网，连接类型包括“虚拟私有云（VPC）”连接、“虚拟网关（VGW）”连接、“VPN网关（VPN）”连接以及“对等连接（Peering）”连接等，不同类型连接的计费策略存在差异，具体请您参见**计费说明**。

7 安全

7.1 责任共担

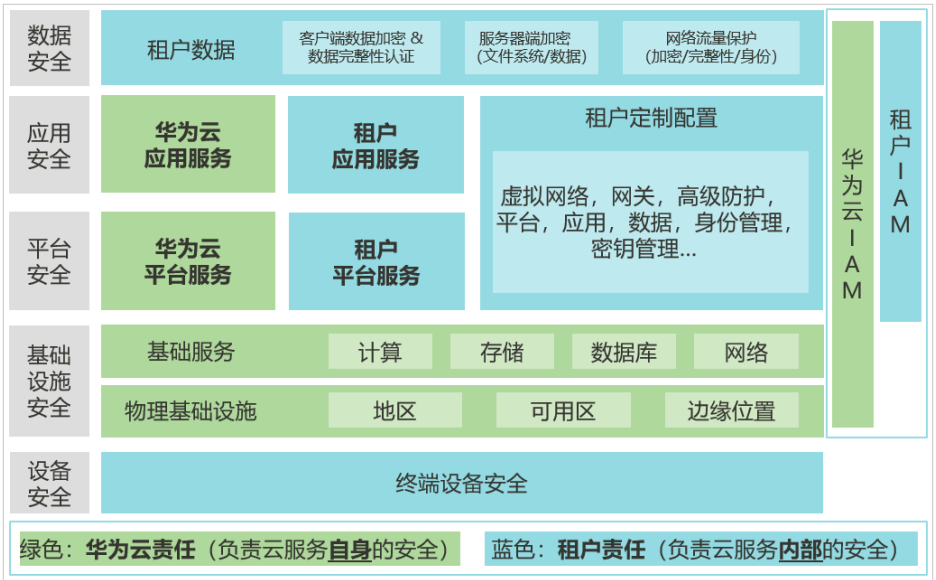
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图7-1**所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 7-1 华为云安全责任共担模型



7.2 身份认证与访问控制

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助用户安全地控制云服务和资源的访问权限。

企业路由器支持通过IAM权限策略进行访问控制。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。

管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予ER所需的权限，组内用户自动继承用户组的所有权限。

- IAM的详细介绍，请参见**IAM功能介绍**。
- ER所需的权限，请参见**权限管理**。

7.3 审计与日志

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务后，CTS可记录企业路由器的操作事件用于审计。

- CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。
- 企业路由器支持审计的操作事件请参见**支持审计的关键动作**。

查看企业路由器的审计日志，请参见**查看审计日志**。

7.4 监控安全风险

企业路由器服务提供基于云监控服务的资源和操作监控能力，帮助用户监控账号下的企业路由器资源，执行自动实时监控、告警和通知操作，帮助您更好地了解企业路由器的各项性能指标。

关于企业路由器服务支持的监控指标，以及如何创建监控告警规则等内容，请参见**监控**。

8 权限管理

如果您需要对华为云上购买的ER资源，为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，您可以在账号中给员工创建IAM用户，并授权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ER的使用权限，但是不希望他们拥有删除ER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ER，但是不允许删除ER的权限，控制他们对ER资源的使用范围。

如果华为账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ER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，您只需要为您华为账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**。

ER 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。

ER部署时通过物理区域划分，为项目级服务。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ER时，需要先切换至授权区域。

权限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ER服务，管理员能够控制IAM用户仅

能对企业路由器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，权限的最小粒度为API授权项（action），ER支持的API授权项请参见**权限及授权项说明**。

如**表1**所示，包括了ER的所有系统权限。

表 8-1 ER 系统权限

系统角色/策略名称	描述	类别	依赖关系
ER FullAccess	企业路由器的管理员权限，拥有该权限的用户可以操作并使用所有企业路由器。	系统策略	无
ER ReadOnlyAccess	企业路由器只读权限，拥有该权限的用户仅能查看企业路由器数据。	系统策略	无

表8-2列出了ER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 8-2 常用操作与系统权限的关系

操作	Tenant Administrator	Tenant Guest	ER FullAccess	ER ReadOnlyAccess
创建企业路由器	√	x	√	x
修改企业路由器配置	√	x	√	x
查看企业路由器	√	√	√	√
删除企业路由器	√	x	√	x
在企业路由器中添加“虚拟私有云（VPC）”连接	√	x	√	x
删除“虚拟私有云（VPC）”连接	√	x	√	x
查看连接（所有类型）	√	√	√	√
创建路由表	√	x	√	x
修改路由表名称	√	x	√	x
查看路由表	√	√	√	√
删除路由表	√	x	√	x

操作	Tenant Administrator	Tenant Guest	ER FullAccess	ER ReadOnlyAccess
创建关联将连接关联至路由表中	√	x	√	x
查看路由表中关联的连接	√	√	√	√
删除路由表中关联的连接	√	x	√	x
在路由表中创建连接的传播	√	x	√	x
查看路由表中连接的传播	√	√	√	√
删除路由表中连接的传播	√	x	√	x
创建静态路由	√	x	√	x
修改静态路由	√	x	√	x
查看路由	√	√	√	√
删除静态路由	√	x	√	x
创建流日志	√	x	√	x
查看流日志	√	√	√	√
关闭流日志	√	x	√	x
开启流日志	√	x	√	x
删除流日志	√	x	√	x
添加资源的标签	√	x	√	x
修改资源的标签	√	x	√	x
查看资源的标签	√	√	√	√
删除资源的标签	√	x	√	x

相关链接

- IAM产品介绍
- 创建用户并授权使用ER
- 权限及授权项说明

9 约束与限制

配额说明

企业路由器的配额说明如表9-1所示，部分默认配额可以提升，您可以根据提示申请扩大配额。

查看每个配额项目支持的默认配额，请参考查看配额，登录控制台查询您的配额详情。

表 9-1 企业路由器的配额说明

配额项目	如何提升配额
每个虚拟私有云支持同时接入的企业路由器数量	不支持修改
每个企业路由器支持接入的“虚拟私有云（VPC）”连接数量	申请更多配额，请参见申请扩大配额
每个企业路由器支持接入的“对等连接（Peering）”连接数量	申请更多配额，请参见申请扩大配额
每个企业路由器支持接入的“虚拟网关（VGW）”连接数量	申请更多配额，请参见申请扩大配额
每个企业路由器支持接入的“VPN网关（VPN）”连接数量	申请更多配额，请参见申请扩大配额
每个企业路由器支持接入的“企业连接网（ECN）”连接数量	不支持修改
每个企业路由器支持创建的路由表数量	不支持修改
每个企业路由器支持的最大路由数量	不支持修改
每个路由表中支持创建的静态路由数量	申请更多配额，请参见申请扩大配额
每个租户支持创建的流日志最大数量	不支持修改

规格说明

企业路由器的规格说明如表9-2所示。

表 9-2 企业路由器的规格说明

规格项目	默认规格	申请提升规格
每个租户支持创建的企业路由器数量	1个	请您提交工单联系华为云客服
每个企业路由器支持的最大转发能力	100 Gbps	请您提交工单联系华为云客服

约束与限制

当前企业路由器服务存在表9-3中列举的使用限制，针对这些限制，请您结合自己的设计业务，参考解决方法建议进行处理。

表 9-3 企业路由器约束与限制说明

约束与限制说明	解决方法建议
当业务VPC下存在共享型弹性负载均衡、VPC终端节点、私网NAT网关、分布式缓存服务、混合云DNS解析时，不建议直接将业务VPC接入ER。 **须知** 若您在弹性负载均衡、VPC终端节点以及分布式缓存服务场景下，直接将业务VPC接入ER，则当ER处于容灾切换、弹性扩缩容、升级等业务可靠性保障过程中，可能造成长连接会话闪断，请您确保业务客户端具有重连机制，在闪断情况下可以自动重连。	针对该限制，请提交工单联系华为云客服，确认服务的兼容性，并优先考虑使用选择企业路由器组网方案中介绍的中转VPC组网方案（方案二）。
当您的VPC和ER组网存在以下情况时，则不建议您在VPC路由表中将下一跳为ER的路由配置成默认路由0.0.0.0/0，那样会导致部分业务流量无法转发至ER。 • VPC内的ECS绑定了EIP。 • VPC被ELB（独享型或者共享型）、NAT网关、VPCEP、DCS服务占用。	• 建议一： 修改路由的目的地址，请您参见如何解决VPC路由表中的0.0.0.0/0路由无法转发至ER的问题？。 • 建议二： 针对该限制，推荐您使用选择企业路由器组网方案中介绍的中转VPC组网方案（方案二），避免将业务VPC直接接入ER。

约束与限制说明	解决方法建议
当接入ER的VPC关联NAT网关，并配置SNAT或者DNAT规则的“使用场景”选择“云专线/云连接”，则网络不通。	针对该限制，推荐您使用**选择企业路由器组网方案**中介绍的中转VPC组网方案（方案二），避免将业务VPC直接接入ER。

10 与其他服务的关系

企业路由器与华为云上多个云服务之间存在交互关系，如图10-1所示。

图 10-1 企业路由器与其他服务的关系

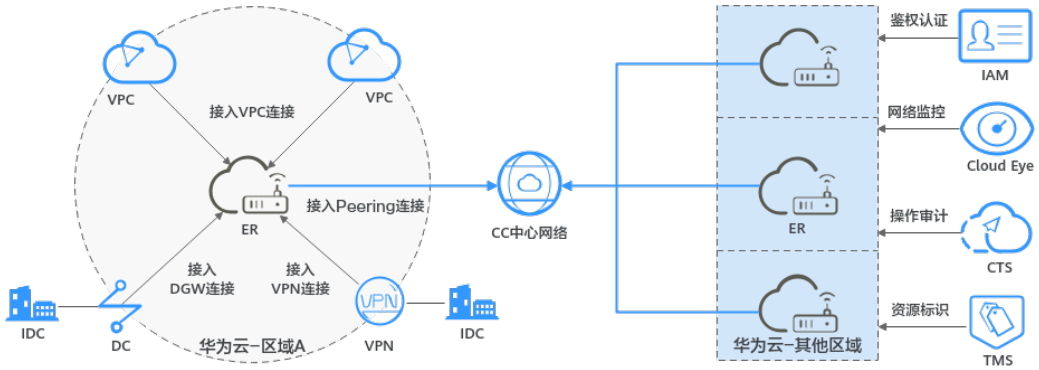


表 10-1 企业路由器与其他服务的关系

服务名称	交互功能
虚拟私有云（Virtual Private Cloud, VPC）	您可以将VPC接入企业路由器，快速打通云上网络，尤其对于多个VPC互通的组网，免去大量的对等连接配置。
云专线（Direct Connect, DC）	您可以将DC接入企业路由器，打通线下IDC和云上网络，多个VPC可以共享专线。
虚拟专用网络（Virtual Private Network，称VPN）	您可以将VPN接入企业路由器，打通线下IDC和云上网络，多个VPC可以共享VPN。
云连接（Cloud Connect, CC）	您可以将两个及以上企业路由器接入云连接中心网络中，构成“对等连接（Peering）”连接，轻松实现云上跨区域网络互通。
企业连接（Enterprise Connect，EC）	您可以将企业连接网络接入企业路由器，帮助企业实现本地网络和云上网络之间的互联互通。
云防火墙（Cloud Firewall，CFW）	您可以通过企业路由器、虚拟私有云VPC和云防火墙构建组网，实现云上VPC间的流量防护。

服务名称	交互功能
统一身份认证服务（Identity and Access Management, IAM）	针对位于华为云上的企业路由器资源，您可以通过IAM进行精细的权限管理，即为不同的用户设置不同的使用权限，权限管理有助于实现资源的安全管控。
云监控（Cloud Eye）	使用云监控可以监控企业路由器实例以及企业路由器连接的网络情况，并对异常进行报警，保证业务的顺畅运行。
云审计服务（Cloud Trace Service, CTS）	使用云审计服务可以记录与企业路由器相关的操作事件，便于日后的查询、审计和回溯。
标签管理服务（Tag Management Service, TMS）	使用标签来标识企业路由器和路由表，便于分类管理和快速搜索。

11 区域和可用区

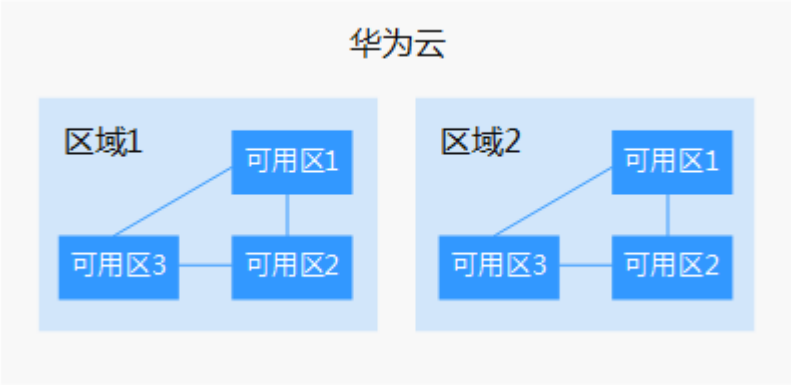
什么是区域、可用区?

区域和可用区用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11-1阐明了区域和可用区之间的关系。

图 11-1 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。

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。

  - 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“非洲-约翰内斯堡”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**。