虚拟专用网络

产品介绍

文档版本	01
发布日期	2025-06-30

华为技术有限公司

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

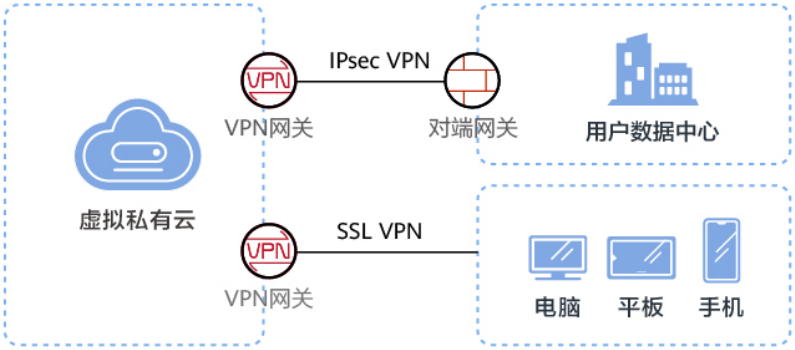
1 图解虚拟专用网络

初识华为云 虚拟专用网络

即开即用的加密连接通道
通信安全 灵活便捷

虚拟专用网络是什么？ 01

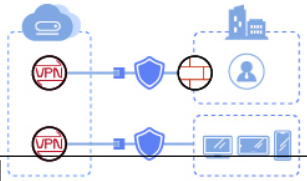
虚拟专用网络（Virtual Private Network）用于在企业的本地网络、数据中心或终端设备与华为云VPC之间搭建安全、可靠、经济的加密连接通道。



为什么选择华为云虚拟专用网络？ 02

更安全

基于IKE/IPsec、SSL对传输数据加密，提供租户级独享网关，保证数据安全。



高可用

2 什么是虚拟专用网络

产品概述

虚拟专用网络（Virtual Private Network，以下简称VPN），用于在企业用户本地网络、数据中心与云上网络之间搭建安全、可靠、高性价比的加密连接通道。

说明

不支持在中国大陆和非中国大陆之间建立VPN跨境连接。在埃及使用VPN时，需要向相关机构申请备案，请**提交工单**申请备案。

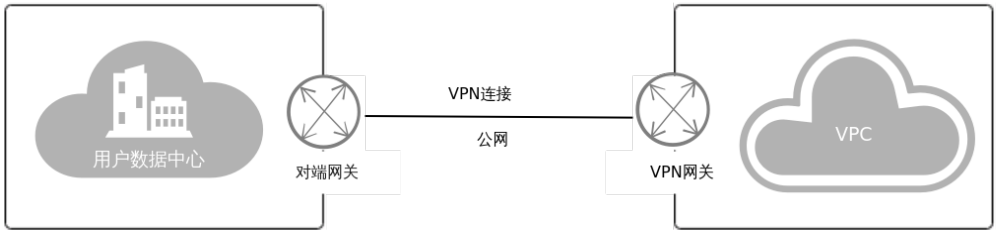
VPN分为站点入云VPN（Site-to-Cloud VPN，以下简称S2C VPN）和终端入云VPN（Point-to-Cloud VPN，以下简称P2C VPN），站点入云VPN基于IPsec协议，终端入云VPN基于SSL协议，两者适用于不同的应用场景。

站点入云VPN由VPN网关、对端网关和VPN连接组成。

- VPN网关提供了VPC的公网出口，与用户数据中心的对端网关对应。
- VPN连接通过加密技术，将VPN网关与对端网关相关联，使数据中心与VPC通信，更快速、更安全地构建混合云环境。

站点入云VPN组网图如**图 站点入云VPN组网图**所示。

图 2-1 站点入云 VPN 组网图

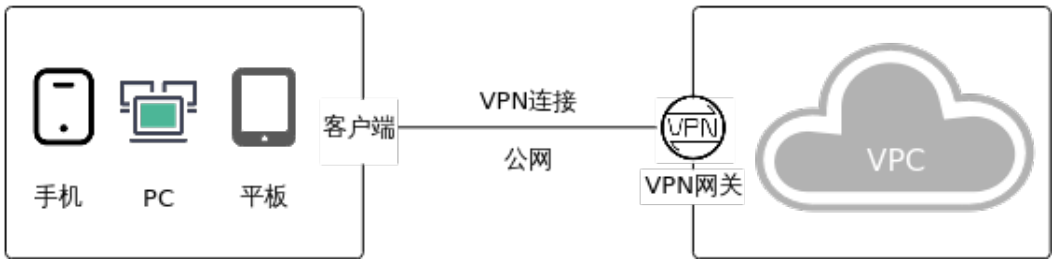


终端入云VPN由VPN网关、服务端和客户端组成。

- VPN网关提供了VPC的公网出口，并绑定对应服务端。
- 服务端实现数据包的封装和解封装，设置和客户端通信的通信端口、加密算法、连通网段。
- 客户端与服务端建立VPN连接，实现对云上资源或服务的远程访问。

终端入云VPN组网图如**图 终端入云VPN组网图**所示。

图 2-2 终端入云 VPN 组网图



组成部分

站点入云VPN

- **VPN网关**：虚拟专用网络在云上的虚拟网关，与用户本地网络、数据中心的对端网关建立安全私有连接。
- **对端网关**：用户数据中心的VPN设备或软件应用程序。控制台上创建的对端网关是云上虚拟对象，用于记录用户数据中心实体设备的配置信息。
- **VPN连接**：VPN网关和对端网关之间的安全通道，使用IKE和IPsec协议对传输数据进行加密。

终端入云VPN

- **VPN网关**：虚拟专用网络在云上的虚拟网关，与客户端建立安全私有连接。
- **服务端**：虚拟网关提供SSL服务的功能模块，用于配置管理及客户端的连接认证。
- **客户端**：用户终端设备上部署的VPN客户端软件。

访问方式

VPN服务提供了Web化的服务管理平台，即管理控制台。用户可以登录管理控制台访问VPN服务。

- 如果用户已注册账户，可直接登录管理控制台，在主页选择“网络 > 虚拟专用网络”。
- 如果未注册，请参见**准备工作**中的“注册账号并开通华为云”。

3 产品优势

企业版虚拟专用网络具有以下几大产品优势：

- **更安全**
  - 基于IKE/IPsec、SSL对传输数据加密，保证用户数据传输安全。
  - VPN支持为每个用户创建独立的VPN网关，提供租户网关隔离防护能力。
  - 支持AES国际、SM国密等加密算法，满足多种安全要求。
  - 支持多种认证模式，包括证书认证、口令认证。
- **高可用**
  - 双连接：网关提供两个接入地址，支持一个对端网关创建两条相互独立的VPN连接，一条连接中断后流量可快速切换到另一条连接。
  - 双活网关：双活网关部署在不同的AZ区域，实现AZ级高可用保障。
  - 主备模式：正常情况下，VPN网关和对端网关通过主连接进行通信；当主连接发生故障时，VPN连接会自动切换到备连接；故障恢复后，VPN连接会自动切回到主连接。
  - HA模式：站点入云VPN支持主备、双活，终端入云VPN支持主备。
- **低成本**
  - 利用Internet构建IPsec加密通道，使用费用相对云专线服务更便宜。
  - 支持绑定同一共享带宽下的EIP实例，从而节省带宽使用成本。
  - 支持在创建EIP实例时，按需配置带宽大小。
  - 支持非固定IP接入，典型场景帮助客户节省接入费用。
- **灵活易用**
  - 支持多种连接模式：一个网关支持配置策略、静态路由和BGP路由多种连接模式，满足不同对端网关的接入需要。
  - 支持分支互访：支持云上VPN网关作为VPN Hub，云下站点通过VPN Hub实现分支互访。
  - 即开即用：部署快速，实时生效，在用户数据中心的VPN设备进行简单配置即可完成对接。
  - 关联企业路由器（Enterprise Router, ER）：企业可以构建更加丰富的云上网络。
  - 专线互备：支持和云专线（DC）互备，故障自动切换。
  - 支持私网类型网关：对专线私有网络进行加密传输，提升数据传输安全。

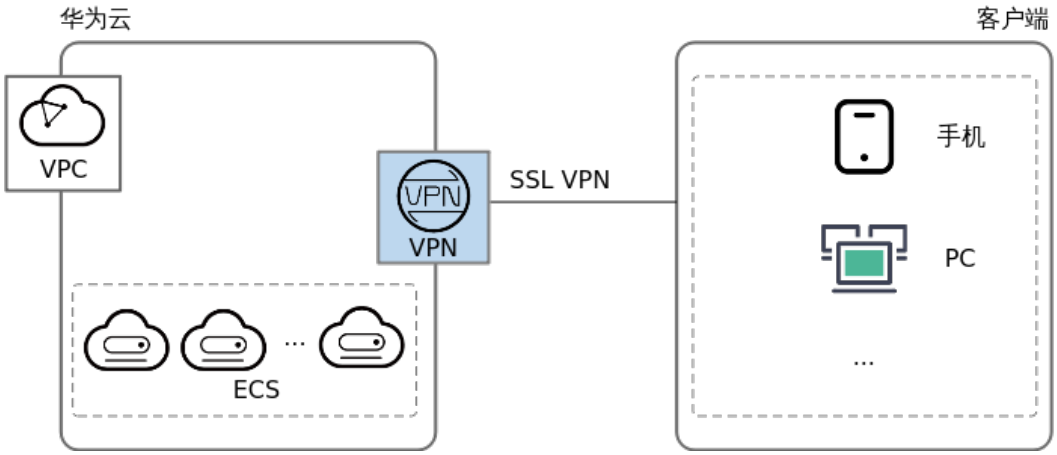
- 支持多平台接入：支持Windows、Mac、Linux、Android、IOS多种终端平台操作系统接入云上网络，实现移动办公。
- 支持DNS域名访问：支持配置DNS，方便用户直接使用域名访问对应的云上业务。
- 支持批量导入用户：支持批量导入和删除用户，方便用户快速添加或删除VPN用户。
- 支持用户连接管理主动断连：终端入云VPN支持用户对连接进行管理，主动断连。
- 支持开启/关闭分支互联功能：站点入云VPN支持用户可以根据需要灵活开启或关闭分支互联，实现对端网关之间互联或隔离。
- 支持一键重置IPsec连接：站点入云VPN支持用户通过重置IPsec连接，实现高效率操作。
- 支持自动生成服务端证书：终端入云VPN支持自动生成服务端证书，方便用户快速使用服务端证书。
- 支持自助升级VPN网关实例：用户根据实际需要自助升级VPN网关实例，方便用户更新网关实例。

4 应用场景

终端设备接入 VPC

用户在PC或手机等终端设备上使用客户端软件远程访问云上VPC，建立与云上资源的连接，如**图 终端设备远程接入VPC**所示。

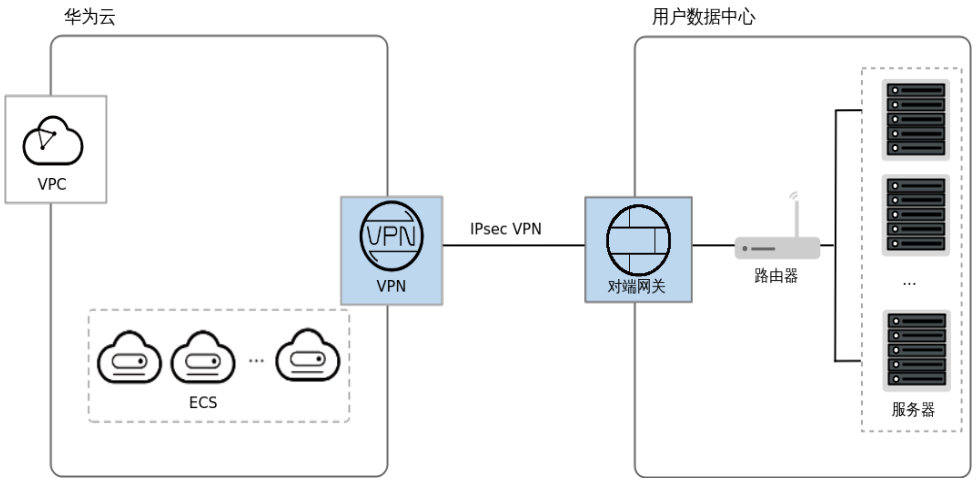
图 4-1 终端设备远程接入 VPC



混合云部署

通过VPN将用户数据中心和云上VPC互联，利用云上弹性和快速伸缩能力，扩展应用计算能力，如**图 混合云部署**所示。

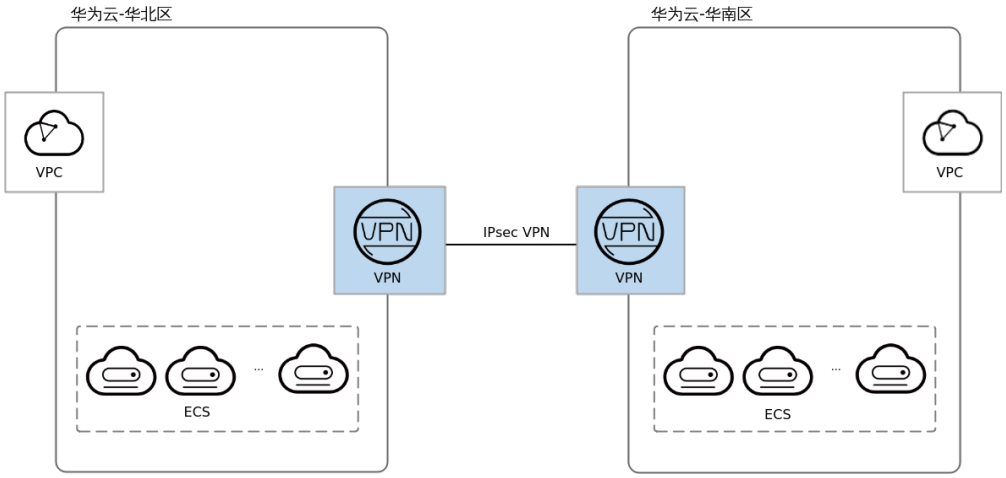
图 4-2 混合云部署



跨地域 VPC 互联

通过VPN将云上的不同region的VPC连接，使得用户的数据和服务在不同地域能够互联互通，如**图 跨地域VPC互联**所示。

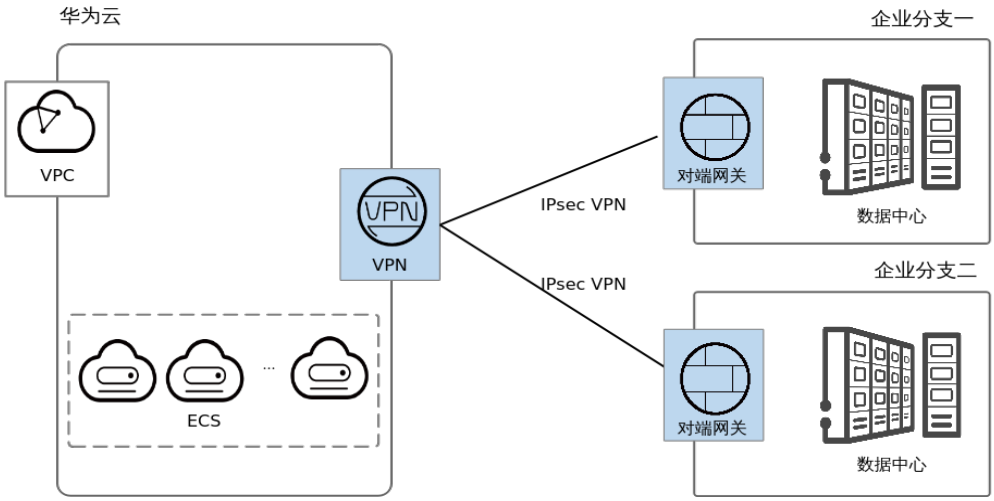
图 4-3 跨地域 VPC 互联



多企业分支互联

通过VPN Hub实现企业分支间互访，避免两两分支之间配置VPN连接，如**图 多企业分支互联**所示。

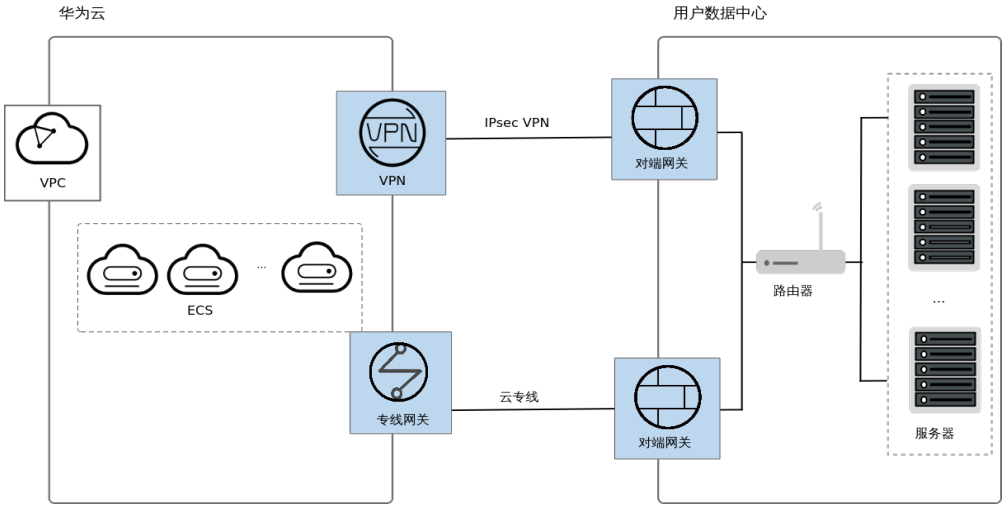
图 4-4 多企业分支互联



VPN 和专线互备

用户数据中心与云上VPC通过专线连接，同时建立VPN连接实现备份，提高可靠性，如**图 VPN和专线互备**所示。

图 4-5 VPN 和专线互备



5 产品规格

5.1 站点入云 VPN

说明

- 本文所述最大转发带宽在以下条件测得，受客户侧及公网等影响因素较多，请以实际测试为准。

  IKE策略版本为v2、认证算法为MD5、加密算法为AES128-GCM、DH算法为group15、本端标识和对端标识为IP Address。

表 5-1 站点入云 VPN 产品规格

对比项	基础型	专业型1	专业型1-非固定IP	专业型2	专业型2-非固定IP	国密型	专业型3	专业型3-非固定IP
独享网关资源	支持	支持	支持	支持	支持	支持	支持	支持
双连接	支持	支持	支持	支持	支持	支持	支持	支持
双活网关	支持	支持	支持	支持	支持	支持	支持	支持
主备网关	支持	支持	支持	支持	支持	支持	支持	支持
策略模式	支持	支持	支持	支持	支持	支持	支持	支持
路由模式-静态路由	支持	支持	支持	支持	支持	支持	支持	支持
路由模式-BGP路由	支持	支持	支持	支持	支持	支持	支持	支持

对比项	基础型	专业型1	专业型1-非固定IP	专业型2	专业型2-非固定IP	国密型	专业型3	专业型3-非固定IP
策略模板模式	不支持	不支持	支持	不支持	支持	不支持	不支持	支持
最大转发带宽	100 Mbps	300Mbps	300Mbps	1Gbps	1Gbps	500Mbps	5Gbps	5Gbps
最大VPN连接组数	10个	100个	100个	100个	100个	100个	200个	200个
对接企业路由器	不支持	支持	支持	支持	支持	支持	支持	支持
对接虚拟私有云	支持	支持	支持	支持	支持	支持	支持	支持
接入公网地址	支持	支持	支持	支持	支持	支持	支持	支持
接入私网地址	不支持	支持	不支持	支持	不支持	支持	支持	不支持
非固定IP接入	不支持	不支持	支持	不支持	支持	不支持	不支持	支持
支持区域	以管理控制台实际上线区域为准。	以管理控制台实际上线区域为准。	以管理控制台实际上线区域为准。	以管理控制台实际上线区域为准。	以管理控制台实际上线区域为准。	以管理控制台实际上线区域为准。	以管理控制台实际上线区域为准。	以管理控制台实际上线区域为准。

5.2 终端入云 VPN

表 5-2 终端入云 VPN 产品规格

对比项	专业型1
独享网关资源	支持
最大转发带宽	300Mbps
最大VPN连接数	500个
支持区域	以管理控制台实际上线区域为准

6 约束与限制

6.1 站点入云 VPN

VPN 网关限制

表 6-1 VPN 网关限制

VPN网关类型	资源	默认限制	如何提升配额
企业版VPN	每租户在每区域支持创建的VPN网关数量	50 • 如果您只有一个VPC，则该VPC最大创建50个VPN网关。 • 如果您有多个VPC，则多个VPC创建的VPN网关数量最大为50个。	申请更多配额，请参见**提交工单**。
	每VPN网关支持配置的VPN连接组数量	100 • 基础型网关支持配置的VPN连接组数量最多为10。 • 专业型3网关支持配置的VPN连接组数量最多为200。 • 其他款型网关支持配置的VPN连接组数量最多为100。	不支持修改。

VPN网关类型	资源	默认限制	如何提升配额
	每VPN网关支持配置的本地子网数量	50	不支持修改。
	不同款型VPN网关支持接收的BGP路由数量	100 • 基础型和国密型网关支持接收的BGP路由数量最多为100。 • 专业型1网关支持接收的BGP路由数量最多为200。 • 专业型2网关支持接收的BGP路由数量最多为300。 • 专业型3网关支持接收的BGP路由数量最多为500。	不支持修改。
	每VPN网关支持最大路由条目数量	10000	不支持修改。
	不同款型VPN网关支持最大ACL规则数量	300 • 专业型3每个IP下支持最大ACL规则数量为1000。 • 其他款型每个IP下支持最大ACL规则数量为300。	不支持修改。
经典版VPN	每租户在每区域支持创建的VPN网关数量	2 每个VPC最多创建1个VPN网关。	申请更多配额，请参见**提交工单**。

- VPN网关TCP协议的最大报文长度默认设置为1300字节。

对端网关限制

表 6-2 对端网关限制

VPN网关类型	资源	默认限制	如何提升配额
企业版VPN	每租户在每区域支持创建的对端网关数量	100	申请更多配额，请参见**提交工单**。

- 请结合组网情况开启对端网关NAT穿越功能。
  - 如果组网为”VPN网关--公网--NAT设备--对端网关”，即对端网关通过NAT设备连接到公网，则对端网关需要开启NAT穿越功能。
  - 如果组网为”VPN网关--公网--对端网关”，即对端网关直接连接到公网，则对端网关无需开启NAT穿越功能。
- 对端网关必须使能DPD（Dead Peer Detection，失效对等体检测）。
- 对端网关必须支持IPsec Tunnel接口，并使能对应的安全策略。
- 静态路由模式连接开启NQA（Network Quality Analysis，网络质量分析）时，对端网关的IPsec Tunnel接口必须配置IP地址，并响应ICMP请求。
- 对端网关TCP协议的最大报文段长度建议设置为小于1399，避免因增加IPsec认证头开销导致分片的问题。

VPN 连接限制

表 6-3 VPN 连接限制

VPN网关类型	资源	默认限制	如何提升配额
企业版VPN	每VPN连接支持配置的策略规则数量	5	不支持修改。
	每VPN连接支持配置的对端子网数量	50	
经典版VPN	每租户在每区域支持创建的VPN连接数量	12	不支持修改。

- 多子网场景下，VPN连接建议使用路由模式。策略模式/策略模板模式下，VPN网关默认为每对本地子网和对端子网创建一个通信隧道，当一条策略模式连接的本地或对端为多子网场景下实际占用了多个通信隧道。

  VPN网关每个网关IP和对端网关建连时，基础型、专业型1、专业型2、国密型的网关最大提供300个通信隧道；专业型3的网关最大提供1000个通信隧道。
  - 路由模式下，每个VPN连接占用网关IP的1个通信隧道。
  - 策略模式/策略模板模式下，每个VPN连接占用网关IP的M*N个通信隧道。M为本端待通信子网数，N为对端待通信子网数。

VPN网关每个网关IP和对端网关建连时，基础型、专业型1、专业型2、国密型的网关最大提供源目的子网对的数量为300个；专业型3的网关最大提供源目的子网对的数量为1000个。

当所有涉及该网关IP的VPN连接模式占用的通信隧道超过100个时，会导致超出部分对应的VPN连接创建失败。

当涉及专业型1、专业型2网关IP的VPN连接模式占用的通信隧道超过300个时，会导致超出部分对应的VPN连接创建失败。

- 使用策略模式创建VPN连接时，若添加多条策略规则，不同策略规则的源、目的网段需要避免出现重叠，以免造成数据流误匹配或IPsec隧道震荡。

6.2 终端入云 VPN

终端入云 VPN 网关限制

表 6-4 终端入云 VPN 网关限制

VPN网关类型	资源	默认限制	如何提升配额
企业版VPN	每租户在每区域支持创建的VPN网关数量	50	不支持修改
	每VPN网关支持关联的服务端数量	1	

终端入云VPN网关的EIP只支持独享带宽，不支持共享带宽。

终端入云 VPN 服务端限制

表 6-5 终端入云 VPN 服务端限制

VPN网关类型	资源	默认限制	如何提升配额
企业版VPN	每服务端支持导入的客户端CA证书数量	10	不支持修改
	每服务端支持添加的本端网段数量	20	

- 修改协议、端口、认证算法、加密算法等，您需要重新下载客户端配置。
- 本端子网的全0配置，暂不开放支持。
- 本端网段的限制网段为0.0.0.0/8，224.0.0.0/4，240.0.0.0/4，127.0.0.0/8，不能与这些特殊网段重叠或冲突。

- 客户端网段和需要访问的VPC中的目标网段不能重叠，且不能包含100.64.0.0/10、100.64.0.0/12和214.0.0.0/8等预留网段。不同region的预留网段不同，实际使用以控制台显示为准。

  如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。
- 每个用户最多建立5个连接。
- 每个VPN网关最多可创建500个用户。
- 用户数最大配置为网关的最大连接数。
- 用户组数量配置最大为50。
- 单策略目的网段数量为10。

  访问策略数量最大规格为100。
- VPN连接只支持VPN网关在正常状态下断连，不支持在非正常状态下断连，比如故障、更新中、删除中或冻结状态。

终端入云 VPN 客户端限制

Windows操作系统环境下，OpenVPN GUI客户端故障重连时间比OpenVPN Connect客户端长，推荐使用OpenVPN Connect客户端。

7 参考标准和协议

与VPN相关的参考标准与协议如下：

- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
- RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2)Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308: Cryptographic Suites for IPsec
- RFC 5282: Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol

- RFC 6989: Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7321: Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 8247: Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 4271: A Border Gateway Protocol 4 (BGP-4)
- RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5116: An Interface and Algorithms for Authenticated Encryption
- GM/T 0022-2014: IPSec VPN技术规范
- GB/T 36968-2018: 信息安全技术 IPSec VPN技术规范

8 站点入云企业版 VPN 和经典版 VPN 的区别

表 8-1 企业版 VPN 和经典版 VPN 的区别

类别	对比项	企业版VPN	经典版VPN
租户隔离	租户独享网关	支持	不支持
功能&特性	策略模式	支持	支持
	路由模式	静态路由/BGP路由	不支持
	VPN Hub	支持	不支持
	企业路由器	支持	不支持
	网络类型	公网/私网	公网
容量&性能	子网数量	• 路由模式：50 • 策略模式：5	策略模式：5
	更多信息，请参见**表 企业版VPN不同规格的区别**。		
可靠性	网关保护方式	主备/双活	-
	网关跨AZ部署	支持	不支持
	双线路双活	支持	不支持
	与专线互备	支持	不支持

9 安全

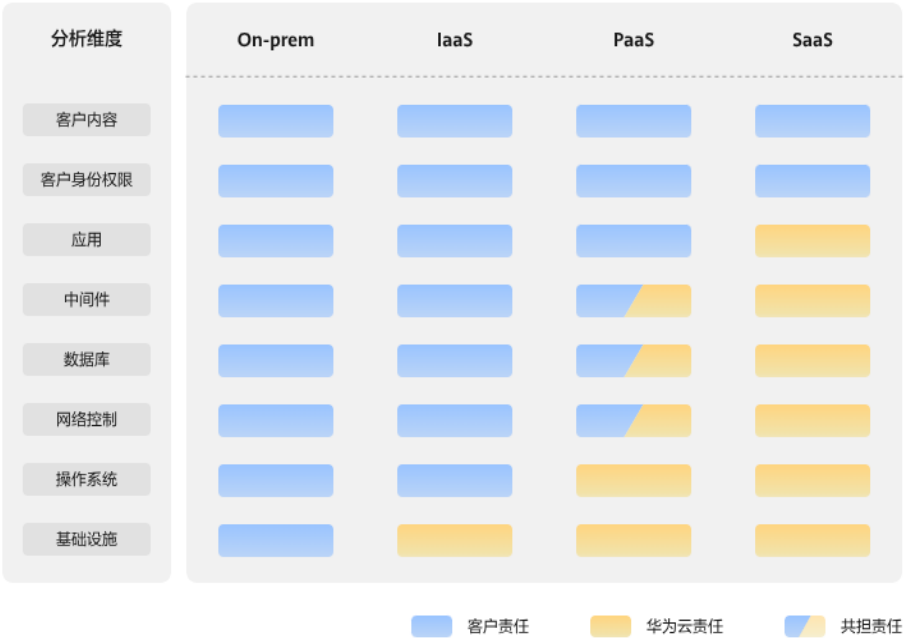
9.1 责任共担

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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如**图 华为云安全责任共担模型**所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 9-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如**图 华为云安全责任共担模型**所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

9.2 身份认证与访问控制

站点入云VPN连接支持通过预共享密钥（PSK）方式对对端网关进行身份验证。

只有对端网关配置的预共享密钥和VPN连接配置的预共享密钥相同时，身份验证才能通过，VPN连接才能成功建立。

图 9-2 身份和访问管理

相关链接：

预共享密钥

9.3 数据保护技术

- 站点入云VPN是基于IKE/IPsec协议族，提供IP层安全的隧道技术，为IP数据包提供机密性和完整性，避免用户数据在不安全网络（如Internet）上被窃取、泄漏和篡改。
- 用户在创建站点入云VPN连接时，可以在策略配置中对数据进行加密和认证算法的配置。

  站点入云VPN推荐使用的算法根据安全性从高到低排序如**表 站点入云VPN策略配置参数说明**所示。

表 9-1 站点入云 VPN 策略配置参数说明

参数		说明
IKE策略	版本	• v2 • v1（版本安全性较低，如果用户设备支持v2版本，建议选择v2。国密型VPN连接，只支持“v1”。） 默认配置为：v2。
	认证算法	认证哈希算法，支持的算法： • SHA2-512 • SHA2-384 • SHA2-256 • MD5（此算法安全性较低，请慎用） • SHA1（此算法安全性较低，请慎用） 默认配置为：SHA2-256。

参数		说明
	加密算法	加密算法，支持的算法： ● AES-256-GCM-16（仅企业版VPN支持） ● AES-128-GCM-16（仅企业版VPN支持） ● AES-256（此算法安全性较低，请慎用） ● AES-192（此算法安全性较低，请慎用） ● AES-128（此算法安全性较低，请慎用） ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。
	DH算法	支持的算法： ● Group 21 ● Group 20 ● Group 19 ● Group 16 ● Group 15 ● Group 14（此算法安全性较低，请慎用） ● Group 5（此算法安全性较低，请慎用） ● Group 2（此算法安全性较低，请慎用） ● Group 1（此算法安全性较低，请慎用） 默认配置为：Group 15。
IPsec策略	认证算法	认证哈希算法，支持的算法： ● SHA2-512 ● SHA2-384 ● SHA2-256 ● MD5（此算法安全性较低，请慎用） ● SHA1（此算法安全性较低，请慎用） 默认配置为：SHA2-256。

参数		说明
	加密算法	加密算法，支持的算法： • AES-256-GCM-16 • AES-128-GCM-16 • AES-256（此算法安全性较低，请慎用） • AES-192（此算法安全性较低，请慎用） • AES-128（此算法安全性较低，请慎用） • 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。

- 终端入云VPN是采用SSL（Security Socket Layer）/TLS（Transport Layer Security）协议加密的方式，保证了数据的机密性和完整性，避免用户数据在不安全网络（如Internet）上被窃取、泄漏和篡改。

  终端入云VPN支持的商用密码算法如**表 终端入云VPN算法配置参数说明**所示。

  表 9-2 终端入云 VPN 算法配置参数说明

参数	说明
认证算法	• SHA2-384 • SHA384
加密算法	• AES-256-GCM-16 • AES-128-GCM-16

完善的前向安全性 PFS

PFS（Perfect Forward Secrecy）指一个IPsec隧道的密钥被破解，不会影响其他隧道的安全性，因为这些隧道的密钥之间没有相关性。站点入云VPN默认开启PFS功能。

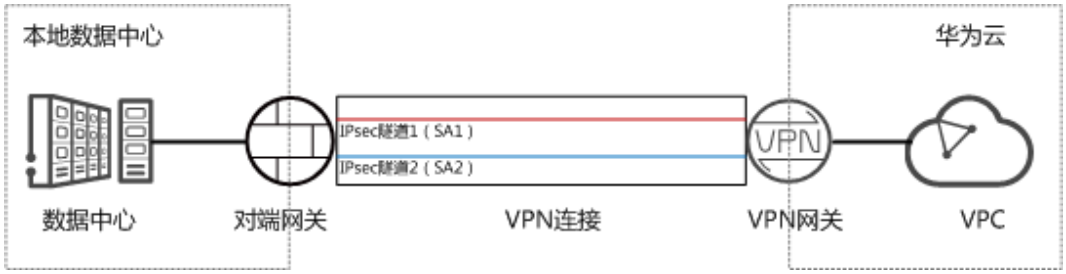
每个IPsec VPN连接由至少一个IPsec隧道组成，每个IPsec隧道使用一套独立的密钥来保护用户流量。

站点入云VPN支持的算法如下：

- DH group 1（此算法安全性较低，请慎用）
- DH group 2（此算法安全性较低，请慎用）
- DH group 5（此算法安全性较低，请慎用）
- DH group 14
- DH group 15
- DH group 16
- DH group 19

- DH group 20
- DH group 21

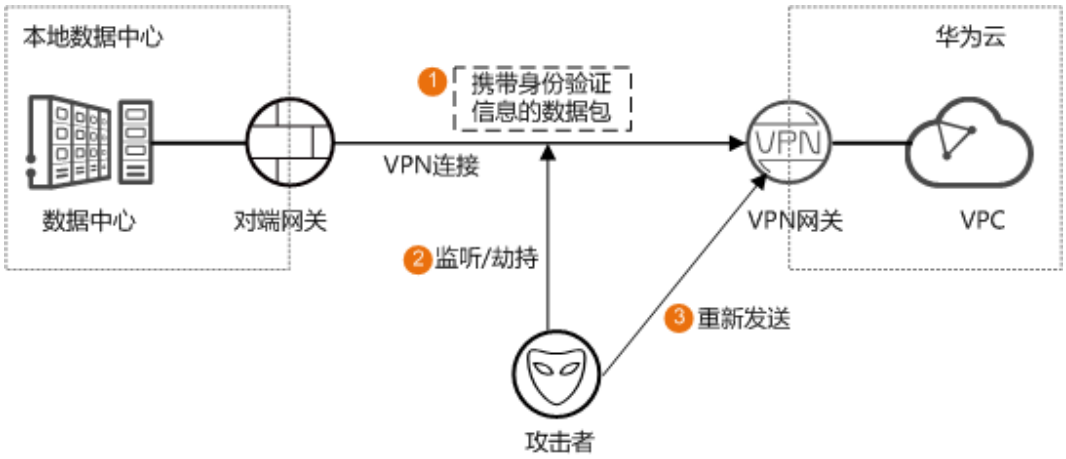
图 9-3 PFS



抗重放

抗重放攻击是针对IPsec加密报文序列号保护的一种方式，防止恶意用户通过重复发送捕获到的数据包进行攻击。VPN服务默认开启抗重放功能。

图 9-4 重放攻击原理

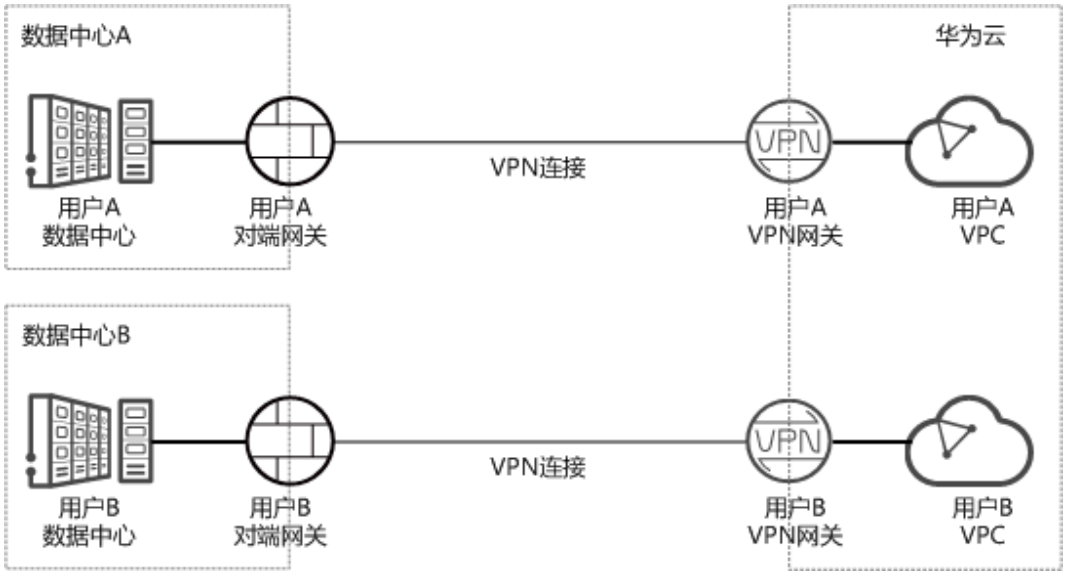


资源隔离

VPN默认为每个用户创建独立的VPN网关，提供租户网关隔离防护能力，确保租户的数据安全。

该特性仅企业版VPN支持，经典版VPN不支持。

图 9-5 数据隔离



如上图示例中，用户A的VPN网关发生故障对用户B的VPN网关不会产生影响。

9.4 审计与日志

VPN支持记录用户账号发出的所有资源创建、删除和修改事件，以日志文件方式发送到云审计服务（CTS），以便用户查询、审计和溯源。

图 9-6 审计与日志

相关链接：

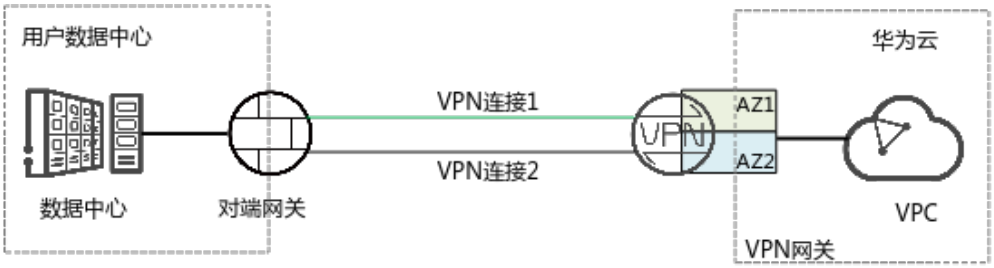
如何查看审计日志，请参见**查看审计日志**。

9.5 服务韧性

VPN提供双AZ容灾能力，即用户创建VPN网关时，支持在当前region下的两个AZ创建VPN网关，并从每个AZ创建一条到对端网关的VPN连接。

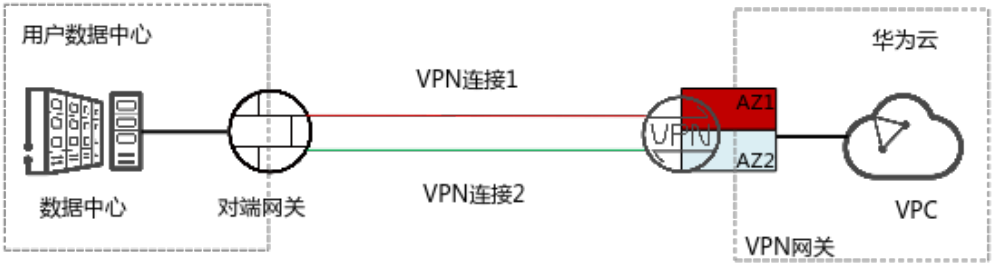
该特性仅企业版VPN支持，经典版VPN不支持。

图 9-7 正常场景



当其中一个AZ下的VPN网关或VPN连接发生故障，系统会自动将流量切换到另一个VPN连接上，保证用户业务正常运行。

图 9-8 故障切换场景



10 权限管理

10.1 基于 IAM 进行权限管理

如果您需要对华为云上购买的VPN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，可以帮助您安全地控制资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制员工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VPN的使用权限，但是不希望他们拥有删除VPN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VPN，但是不允许删除VPN的权限，控制他们对VPN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VPN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**。

VPN 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。

VPN部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，然后在指定区域（如亚太-曼谷）对应的项目（ap-southeast-2）中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问VPN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VPN服务，管理员能够控制IAM用户仅能对某一类VPN资源进行指定的管理操作。

如表10-1所示，包括了VPN的所有系统权限。

表 10-1 VPN 系统权限

系统角色/策略名称	描述	依赖关系
VPN Administrator（不推荐使用）	VPN服务的管理员权限，拥有该权限的用户拥有VPN服务所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、VPC Administrator。** • VPC Administrator：项目级策略，在同项目中勾选。 • Tenant Guest：项目级策略，在同项目中勾选。	-
VPN FullAccess（推荐使用）	VPN服务的所有执行权限。 **说明** 所有查询列表的action不支持企业项目授权，需要在IAM视图下单独配置。	全局服务的action和region级的action不能配置在同一策略，需要补充全局action： • "tms:predefineTags:list" • "scm:cert:list" • "scm:cert:get" • "scm:cert:download" • "iam:identityProviders:getIdentityProvider" • "iam:identityProviders:listProtocols"
VPN ReadOnlyAccess	VPN服务只读权限，拥有该权限的用户仅能查看VPN服务下的资源信息。 **说明** 所有查询列表的action不支持企业项目授权，需要在IAM视图下单独配置。	全局服务的action和region级的action不能配置在同一策略，需要补充全局action： • "tms:predefineTags:list" • "scm:cert:list" • "scm:cert:get"

表 VPN常用操作与系统权限的关系列出了站点入云VPN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 10-2 站点入云 VPN 常用操作与系统权限的关系

操作	VPN Administrator（不推荐使用）	VPN FullAccess（推荐使用）	VPN ReadOnlyAccess
创建VPN网关	√	• 企业版VPN：√ • 经典版VPN：×	×
查询VPN网关	√	√	√
查询VPN网关列表	√	√	√
更新VPN网关	√	• 企业版VPN：√ • 经典版VPN：×	×
删除VPN网关	√	• 企业版VPN：√ • 经典版VPN：×	×
创建VPN连接	√	• 企业版VPN：√ • 经典版VPN：√	×
查询VPN连接	√	√	√
查询VPN连接列表	√	√	√
更新VPN连接	√	• 企业版VPN：√ • 经典版VPN：√	×
删除VPN连接	√	• 企业版VPN：√ • 经典版VPN：√	×
创建对端网关	√	• 企业版VPN：√ • 经典版VPN：不涉及	×
查询对端网关	√	• 企业版VPN：√ • 经典版VPN：不涉及	√
查询对端网关列表	√	• 企业版VPN：√ • 经典版VPN：不涉及	√
更新对端网关	√	• 企业版VPN：√ • 经典版VPN：不涉及	×
删除对端网关	√	• 企业版VPN：√ • 经典版VPN：不涉及	×

操作	VPN Administrator（不推荐使用）	VPN FullAccess（推荐使用）	VPN ReadOnlyAccess
创建连接监控	√	• 企业版VPN：√ • 经典版VPN：×	×
查询连接监控	√	• 企业版VPN：√ • 经典版VPN：×	√
查询连接监控列表	√	• 企业版VPN：√ • 经典版VPN：×	√
删除连接监控	√	• 企业版VPN：√ • 经典版VPN：×	×

列出了终端入云VPN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 10-3 终端入云 VPN 常用操作与系统权限的关系

操作	VPN Administrator（不推荐使用）	VPN FullAccess（推荐使用）	VPN ReadOnlyAccess
订购包周期终端入云VPN网关	√	√	×
变更包周期终端入云VPN网关规格	√	√	×
更新终端入云VPN网关	√	√	×
查询终端入云VPN网关详情	√	√	√
查询终端入云VPN网关列表	√	√	√
查询终端入云VPN连接列表	√	√	√

操作	VPN Administrator（不推荐使用）	VPN FullAccess（推荐使用）	VPN ReadOnlyAccess
创建VPN服务端	√	× 全局服务的action和region级的action不能配置在同一策略，需要补充全局action： scm:cert:get scm:cert:list scm:cert:download	×
查询一个网关下的服务端信息	√	√	√
更新指定网关的服务端	√	× 全局服务的action和region级的action不能配置在同一策略，需要补充全局action： scm:cert:get scm:cert:list scm:cert:download	×
导出服务端对应的客户端配置信息	√	√	×
校验CA证书的合法性	√	√	√
导入客户端CA证书	√	√	×
修改客户端CA证书	√	√	×
查询客户端CA证书	√	√	√
删除客户端CA证书	√	√	×
查询租户下的所有服务端信息	√	√	√
创建VPN用户	√	√	×
查询VPN用户列表	√	√	√
修改VPN用户	√	√	×
查询VPN用户	√	√	√
删除VPN用户	√	√	×

操作	VPN Administrator（不推荐使用）	VPN FullAccess（推荐使用）	VPN ReadOnlyAccess
修改VPN用户密码	√	√	×
重置VPN用户密码	√	√	×
创建VPN用户组	√	√	×
查询VPN用户组列表	√	√	√
修改VPN用户组	√	√	×
查询VPN用户组	√	√	√
删除VPN用户组	√	√	×
添加VPN用户到组	√	√	×
删除组内VPN用户	√	√	×
查询组内VPN用户	√	√	√
创建VPN访问策略	√	√	×
查询VPN访问策略列表	√	√	√
修改VPN访问策略	√	√	×
查询VPN访问策略	√	√	√
删除VPN访问策略	√	√	×
查询P2C VPN网关可用区	√	√	√
批量添加资源标签	√	√	×
批量删除资源标签	√	√	×
通过资源标签查询资源实例列表	√	√	√
查询标签下资源实例数量	√	√	√
通过资源实例查询资源标签列表	√	√	√
查询资源标签列表	√	√	√

相关链接

- IAM产品介绍

- **创建用户组、用户并授予VPN权限**

10.2 站点入云 VPN 授权项列表

10.2.1 VPN 网关

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
创建VPN网关	POST /v5/{project_id}/vpn-gateways	vpn:vpnGateways:create	• er:instances:list • er:instances:get • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list • vpc:subnets:create • vpc:subnets:delete • vpc:subNetworkInterfaces:update • vpc:publicIps:create • vpc:publicIps:delete • vpc:publicIps:update • vpc:publicIps:get • vpc:publicIps:list • vpc:ports:create • vpc:quotas:list • vpc:bandwidths:list • vpc:ports:get • vpc:ports:delete	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
			• vpc:routeTables:update • vpc:routeTables:get • vpc:bandwidths:get		
查询VPN网关	GET /v5/{project_id}/vpn-gateways/{vgw_id}	vpn:vpnGateways:get	• vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • er:instances:list • er:instances:get • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询VPN网关列表	GET /v5/{project_id}/vpn-gateways	vpn:vpnGateways:list	• vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • er:instances:list • er:instances:get • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list	√	×

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
更新VPN网关	PUT /v5/{project_id}/vpn-gateways/{vgw_id}	vpn:vpnGateways:update	• er:instances:list • er:instances:get • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list • vpc:subnets:delete • vpc:subNetworkInterfaces:update • vpc:publicIps:delete • vpc:publicIps:update • vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • vpc:ports:get • vpc:routeTables:update • vpc:routeTables:get	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
删除VPN网关	DELETE /v5/{project_id}/vpn-gateways/{vgw_id}	vpn:vpnGateways:delete	• er:instances:list • er:instances:get • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:delete • vpc:subNetworkInterfaces:update • vpc:publicIps:delete • vpc:publicIps:update • vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • vpc:ports:get • vpc:ports:delete • vpc:routeTables:update • vpc:routeTables:get	√	√
查询VPN网关可用区(V5)	GET /v5/{project_id}/vpn-gateways/availability-zones	vpn:vpnGatewayAvailabilityZone:list	-	√	×

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询VPN网关可用区(V5.1)	GET /v5.1/{project_id}/vpn-gateways/availability-zones	vpn:vpnGatewayAvailabilityZone:list	-	√	×
导入VPN网关证书	POST /v5/{project_id}/vpn-gateways/{vgw_id}/certificate	vpn:vpnGateways:importCertificate	-	√	√
查询VPN网关证书	GET /v5/{project_id}/vpn-gateways/{vgw_id}/certificate	vpn:vpnGateways:getCertificate	-	√	√
更新VPN网关证书	PUT /v5/{project_id}/vpn-gateways/{vgw_id}/certificate/{certificate_id}	vpn:vpnGateways:updateCertificate	-	√	√
查询VPN网关的路由表	GET /v5/{project_id}/vpn-gateways/{vgw_id}/routing-table	vpn:vpnGateways:getRoutingTable	-	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
变更按需VPN网关规格	POST /v5/{project_id}/vpn-gateways/{vgw_id}/update-specification	vpn:vpnGateways:updatePostpaidSpecification	• er:instances:list • er:instances:get • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list • vpc:subnets:delete • vpc:subNetworkInterfaces:update • vpc:publicIps:delete • vpc:publicIps:update • vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • vpc:ports:ge • vpc:routeTables:update • vpc:routeTables:get	√	√
升级站点入云VPN网关	POST /v5/{project_id}/vpn-gateways/{vpn_gateway_id}/upgrade	vpn:vpnGateways:upgrade	-	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询站点入云VPN网关任务列表	GET /v5/{project_id}/vpn-gateways/jobs	vpn:vpnGateways:listResourceJobs	-	√	×
删除站点入云VPN网关任务	DELETE /v5/{project_id}/vpn-gateways/jobs/{job_id}	vpn:vpnGateways:deleteResourceJobs	-	√	×

10.2.2 对端网关

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
创建对端网关	POST /v5/{project_id}/customer-gateways	vpn:customerGateways:create	-	√	×
查询对端网关详情	GET /v5/{project_id}/customer-gateways/{customer_gateway_id}	vpn:customerGateways:get	-	√	×
查询对端网关列表	GET /v5/{project_id}/customer-gateways	vpn:customerGateways:list	-	√	×
更新对端网关	PUT /v5/{project_id}/customer-gateways/{customer_gateway_id}	vpn:customerGateways:update	-	√	×
删除对端网关	DELETE /v5/{project_id}/customer-gateways/{customer_gateway_id}	vpn:customerGateways:delete	-	√	×

10.2.3 VPN 连接

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
创建VPN连接	POST /v5/{project_id}/vpn-connection	vpn:vpnConnections:create	• ces:metricData:list • ces:currentRegionSupportedMetrics:list • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list • vpc:subNetworkInterfaces:update • vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • vpc:ports:get • vpc:routeTables:update • vpc:routeTables:get	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
查询VPN连接列表	GET /v5/{project_id}/vpn-connection	vpn:vpnConnections:list	• vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • er:instances:list • er:instances:get • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list	√	×
查询VPN连接详情	GET /v5/{project_id}/vpn-connection/{vpn_connection_id}	vpn:vpnConnections:get	• vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • er:instances:list • er:instances:get • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
更新VPN连接	PUT /v5/{project_id}/vpn-connection/{vpn_connection_id}	vpn:vpnConnections:update	• vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list • vpc:subNetworkInterfaces:update • vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • vpc:ports:get • vpc:routeTables:update • vpc:routeTables:get	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
删除VPN连接	DELETE /v5/{project_id}/vpn-connection/{vpn_connection_id}	vpn:vpnConnections:delete	• ces:metricData:list • ces:currentRegionSupportedMetrics:list • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subNetworkInterfaces:update • vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • vpc:ports:get • vpc:routeTables:update • vpc:routeTables:get	√	√

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
批量创建VPN连接	POST /v5/{project_id}/vpn-connections/batch-create	vpn:vpnConnections:batchCreate	• ces:metricData:list • ces:currentRegionSupportedMetrics:list • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:subnets:list • vpc:subNetworkInterfaces:update • vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list • vpc:ports:get • vpc:routeTables:update • vpc:routeTables:get	√	√
查询VPN连接日志	GET /v5/{project_id}/vpn-connection/{vpn_connection_id}/log	vpn:vpnConnections:getLog	-	√	√
重置VPN连接	POST /v5/{project_id}/vpn-connection/{vpn_connection_id}/reset	vpn:vpnConnections:reset	-	√	√

10.2.4 VPN 连接监控

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
创建连接监控	POST /v5/{project_id}/connection-monitors	vpn:connectionMonitors:create	-	√	√
查询连接监控列表	GET /v5/{project_id}/connection-monitors	vpn:connectionMonitors:list	-	√	x
删除连接监控	DELETE /v5/{project_id}/connection-monitors/{connection_monitor_id}	vpn:connectionMonitors:delete	-	√	√
查询连接监控	GET /v5/{project_id}/connection-monitors/{connection_monitor_id}	vpn:connectionMonitors:get	-	√	√

10.3 终端入云 VPN 授权项列表

10.3.1 VPN 网关

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
订购包周期终端入云VPN网关	-	vpn:p2cVpnGateway:subscribe	• vpn:system:listAvailabilityZones • vpc:vpcs:list • vpc:subnets:get • vpc:bandwidths:list • vpc:publicIps:create • vpc:publicIps:delete • vpc:publicIps:update • vpc:publicIps:list • vpc:quotas:list	√	×
变更包周期VPN网关规格	-	vpn:p2cVpnGateway:updateSpecification	-	√	×
更新终端入云VPN网关	PUT /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}	vpn:p2cVpnGateway:update	• vpc:publicIps:create • vpc:publicIps:delete • vpc:publicIps:update • vpc:publicIps:get • vpc:publicIps:list • vpc:bandwidths:list	√	×

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询终端入云VPN网关详情	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}	vpn:p2cVpnGateway:get	vpc:publicIps:get	√	×
查询终端入云VPN网关列表	GET /v5/{project_id}/p2c-vpn-gateways	vpn:p2cVpnGateway:list	vpc:publicIps:get	√	×
查询终端入云VPN连接列表	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections	vpn:p2cVpnGateway:listConnections	-	√	×
断开P2C VPN网关连接	POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections/{connection_id}/disconnect	vpn:p2cVpnGateway:disconnectConnection	-	√	×
升级终端入云VPN网关	POST /v5/{project_id}/p2c-vpn-gateways/{vpn_gateway_id}/upgrade	vpn:p2cVpnGateway:upgrade	-	√	×
查询终端入云VPN网关任务列表	GET /v5/{project_id}/p2c-vpn-gateways/jobs	vpn:p2cVpnGateway:listResourceJobs	-	√	×
删除终端入云VPN网关任务	DELETE /v5/{project_id}/p2c-vpn-gateways/jobs/{job_id}	vpn:p2cVpnGateway:deleteResourceJobs	-	√	×

10.3.2 服务端

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
创建终端入云VPN服务端	POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers	vpn:p2cVpnGateway:createServer	• scm:cert:get • scm:cert:list • scm:cert:download • vpc:publicIps:get • vpc:routeTables:update • vpc:subnets:get • vpc:quotas:list	√	x
查询一个网关下的服务端信息	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers	vpn:p2cVpnGateway:listServers	-	√	x
更新指定网关的服务端	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}	vpn:p2cVpnGateway:updateServer	• scm:cert:get • scm:cert:list • scm:cert:download • vpc:publicIps:get • vpc:routeTables:update • vpc:subnets:get	√	x

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
导出服务端对应的客户端配置信息	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-config/export	vpn:p2cVpnGateway:exportClientConfig	-	√	x
校验CA证书的合法性	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/client-ca-certificates/check	vpn:system:checkClientCaCertificate	-	√	x
导入客户端CA证书	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates	vpn:p2cVpnGateway:importClientCa	-	√	x
修改客户端CA证书	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:updateClientCa	-	√	x
查询客户端CA证书	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:getClientCa	-	√	x
删除客户端CA证书	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:deleteClientCa	-	√	x
查询租户下的所有服务端信息	GET /v5/{project_id}/vpn-servers	vpn:p2cVpnGateway:listAllServers	-	√	x

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
断开终端入云VPN网关连接	POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections/{connection_id}/disconnect	vpn:p2cVpnGateway:disconnectConnection	-	√	x
更新终端入云VPN连接日志配置	PUT /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config	vpn:p2cVpnGateway:updateConnectionsLogConfig	• lts:logGroup:listLogGroup • lts:logStream:listLogStream	√	×
查询终端入云VPN连接日志配置	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config	vpn:p2cVpnGateway:getConnectionsLogConfig	-	√	×
删除终端入云VPN连接日志配置	DELETE /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config	vpn:p2cVpnGateway:deleteConnectionsLogConfig	-	√	×

10.3.3 用户管理

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
创建VPN用户	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users	vpn:p2cVpnUser:create	-	√	x
批量创建VPN用户	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/batch-create	vpn:p2cVpnUser:batchCreate	-	√	x
查询VPN用户列表	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users	vpn:p2cVpnUser:list	-	√	x
修改VPN用户	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}	vpn:p2cVpnUser:update	-	√	x
查询VPN用户	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}	vpn:p2cVpnUser:get	-	√	x
删除VPN用户	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}	vpn:p2cVpnUser:delete	-	√	x
批量删除VPN用户	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/batch-delete	vpn:p2cVpnUser:batchDelete	-	√	x

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
修改VPN用户密码	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/password	vpn:p2cVpnUser:updatePassword	-	√	x
重置VPN用户密码	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/reset-password	vpn:p2cVpnUser:resetPassword	-	√	x
创建VPN用户组	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups	vpn:p2cVpnGateway:createUserGroup	-	√	x
查询VPN用户组列表	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups	vpn:p2cVpnGateway:listUserGroup	-	√	x
修改VPN用户组	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpnGateway:updateUserGroup	-	√	x
查询VPN用户组	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpnGateway:getUserGroup	-	√	x
删除VPN用户组	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpnGateway:deleteUserGroup	-	√	x
添加VPN用户到组	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/add-users	vpn:p2cVpnGateway:addUsers	-	√	x

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
删除组内VPN用户	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/remove-users	vpn:p2cVpnGateway:removeUsers	-	√	x
查询组内VPN用户	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/users	vpn:p2cVpnGateway:listUsersInGroup	-	√	x

10.3.4 访问策略

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
创建VPN访问策略	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies	vpn:p2cVpnGateway:createAccessPolicy	-	√	x
查询VPN访问策略列表	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies	vpn:p2cVpnGateway:listAccessPolicies	-	√	x

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
修改VPN访问策略	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:updateAccessPolicy	-	√	x
查询VPN访问策略	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:getAccessPolicy	-	√	x
删除VPN访问策略	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:deleteAccessPolicy	-	√	x

10.4 服务公共接口授权项列表

10.4.1 VPN 配额

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
查询VPN配额	GET /v5/{project_id}/vpn/quotas	vpn:quota:list	-	√	×

10.4.2 VPN 标签

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
创建资源标签	POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create	vpn:resourceInstanceTags:create	-	√	√
删除资源标签	POST /v5/{project_id}/{resource_type}/{resource_id}/tags/delete	vpn:resourceInstanceTags:delete	-	√	√
查询资源类型标签列表	GET /v5/{project_id}/{resource_type}/tags	vpn:resourceTypeTags:list	-	√	×
查询资源实例列表	POST /v5/{project_id}/{resource_type}/resource-instances/filter	vpn:resourceInstances:list	-	√	×

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
查询资源标签列表	GET /v5/{project_id}/{resource_type}/{resource_id}/tags	vpn:resourceInstanceTags:list	-	√	√
查询资源实例数量	POST /v5/{project_id}/{resource_type}/resource-instances/count	vpn:resourceInstances:count	-	√	×

11 与其他服务的关系

VPN服务与其他云服务的关系如图11-1所示。

图 11-1 与其他服务的关系

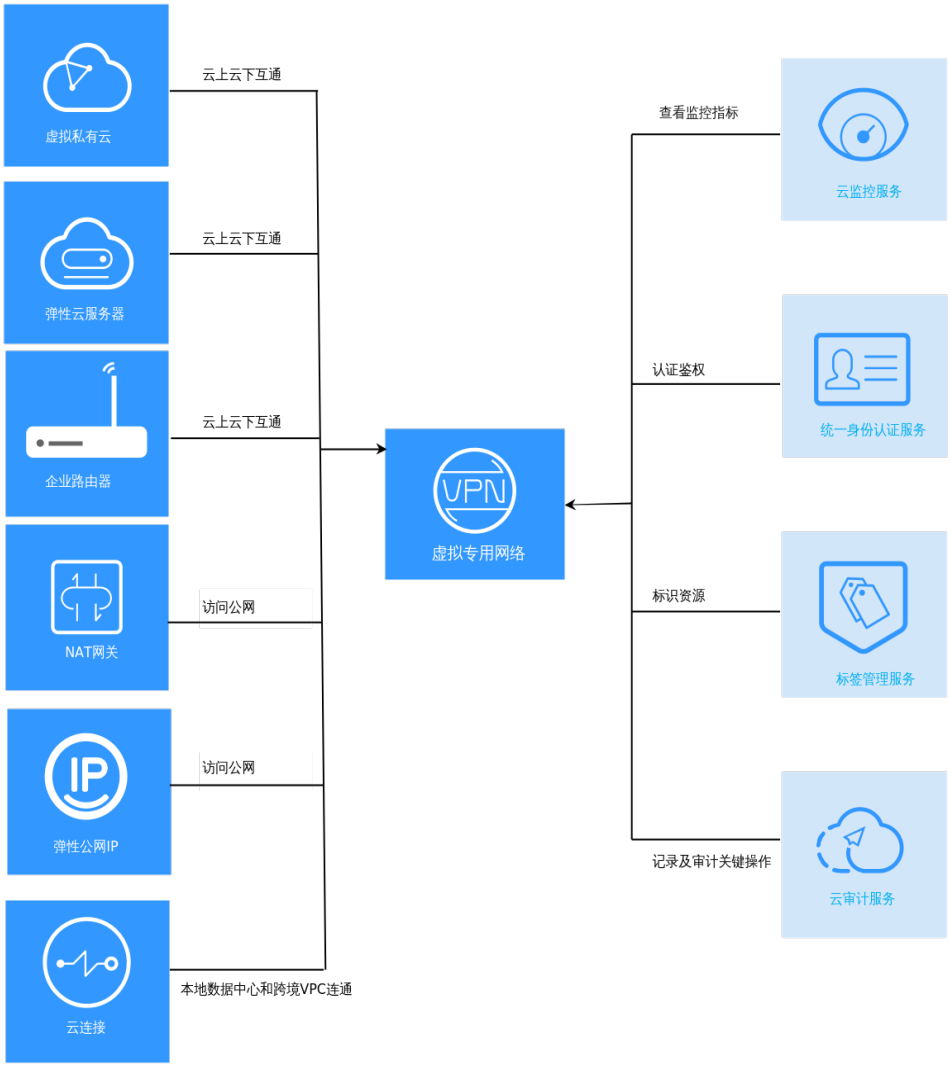


表 11-1 与其他服务的关系

相关服务	交互功能	位置
虚拟私有云（Virtual Private Cloud，VPC）	通过VPC服务，创建VPC，用户数据中心才可以通过VPN上云。	**虚拟私有云**
弹性云服务器（Elastic Cloud Server，ECS）	通过ECS服务，定义安全组中的规则，将VPC中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。	**弹性云服务器**
企业路由器（Enterprise Router，ER）	通过企业路由器ER，用户数据中心上云可以实现VPN和专线双通道互备。 仅企业版VPN网关支持，经典版VPN网关不支持。	**企业路由器**
NAT网关（NAT Gateway）	通过NAT网关服务，可以实现用户数据中心服务器访问公网或为公网提供服务。	**NAT网关**
弹性公网IP（EIP）	通过弹性公网IP，可以实现VPN网关通过公网和对端网关进行网络互通。 仅企业版VPN支持，经典版VPN不支持。	**弹性公网IP**
云连接（Cloud Connect）	通过云连接服务，可以实现用户数据中心和跨境VPC之间的稳定网络连通。	**云连接**
云监控（Cloud Eye）	通过云监控服务，查看VPN资源的监控数据，还可以获取可视化监控图表。	**云监控**
统一身份认证服务（Identity and Access Management，IAM）	通过IAM服务，针对您在华为云上创建的VPN资源，向不同用户设置不同的使用权限，可以帮助您安全地控制华为云VPN资源的访问权限。	**统一身份认证服务**
标签管理服务（Tag Management Service，TMS）	使用标签来标识虚拟专用网络，便于分类和搜索。	**标签管理服务**
云审计服务（Cloud Trace Service，CTS）	记录与VPN服务相关的操作事件。	**云审计服务**

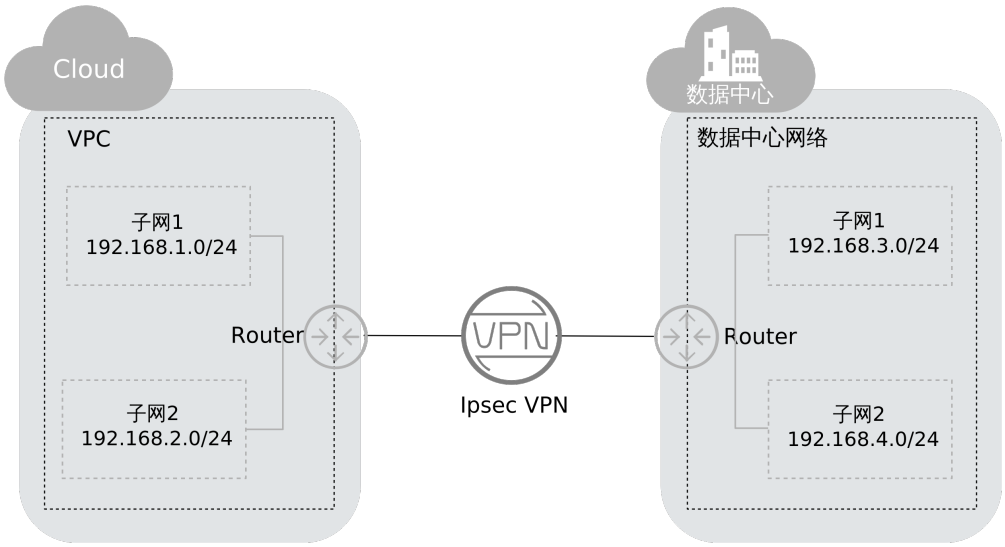
12 基本概念

12.1 IPsec VPN

IPsec VPN是一种加密的隧道技术，通过使用加密的安全服务在不同的网络之间建立保密而安全的通讯隧道。在云上即站点入云VPN，如果需要购买站点入云VPN网关，您可以单击**立即购买**。

如**图12-1**所示，假设您在云上已经申请了VPC，并申请了2个子网（192.168.1.0/24，192.168.2.0/24），同时您在自己的数据中心也有2个子网（192.168.3.0/24，192.168.4.0/24），那么您可以通过VPN使VPC内的子网与数据中心的子网互相通信。

图 12-1 IPsec VPN



支持站点到站点VPN（Site-to-Site VPN），可实现VPC子网和数据中心局域网互访。

相关链接：

站点入云VPN

12.2 SSL VPN

SSL VPN是一种基于SSL协议的虚拟专用网络技术。允许远程用户通过加密的方式安全地访问企业内部网络资源。

在云上即终端入云VPN，如果需要购买终端入云VPN网关，您可以单击**立即购买**。

相关链接：

终端入云VPN

12.3 VPN 网关

VPN网关是虚拟专用网络在云上的虚拟网关，与用户本地网络、数据中心的对端网关建立安全私有连接。VPN网关需要与用户数据中心的对端网关配合使用。

相关链接：

- **创建站点入云VPN网关**
- **创建经典版VPN网关**
- **创建终端入云VPN网关**

12.4 VPN 连接

VPN连接是VPN网关和对端网关之间的安全通道，使用IKE和IPsec协议对传输数据进行加密，保证数据安全可靠。

相关链接：

- **创建企业版VPN连接**
- **创建经典版VPN连接**
- **什么是VPC、VPN网关、VPN连接?**

12.5 VPN 网关带宽

VPN网关带宽指的是出云方向的带宽，即从VPC发往用户侧数据中心的带宽。

- 如果所购带宽 <=10Mbit/s，则入云方向统一限定为10Mbit/s。
- 如果所购带宽 >10Mbit/s，则入云方向与所购买的带宽一致。

按需按流量计费场景下，VPN网关的带宽大小不影响价格，建议您根据实际需求来设置带宽大小，以免因为程序错误或恶意访问导致产生大量计费流量。

12.6 本端子网

本端子网通过VPN与用户侧网络进行互通，有两种输入方式。

- 子网方式：使用下拉列表选择要进行VPN通信的子网。如果要进行VPN通信的子网都在该VPC中，建议采用这种方式。

- 网段方式：用户在输入框中手工输入网段信息，格式为点分十进制加掩码长度，如 192.168.0.0/16； 如果有多个网段，则使用逗号分隔。使用这种方式可以添加不属于该VPC的网段，如通过VPC peering特性连接进来的非该VPN网关关联的VPC内的网段（如0.0.0.0/0等）。

12.7 对端网关

对端网关是用户数据中心的VPN设备或软件应用程序。管理控制台上创建的对端网关是云上虚拟对象，用于记录用户数据中心实体设备的配置信息。

相关链接：

创建对端网关。

12.8 对端子网

对端子网即用户侧数据中心的网段，该网段需要通过VPN与云上VPC网络进行互通。

- 用户需手工输入网段信息，格式为点分十进制加掩码长度，如 192.168.0.0/16；如果有多个网段，则使用逗号分隔。
- 用户在设置完对端子网后，无需在VPC中增加路由信息，VPN服务会自动在VPC中下发到达对端子网的路由。

说明

子网不支持D类组播地址，E类保留地址和127开头的环回地址。

12.9 预共享密钥

预共享密钥（Pre Shared Key），指配置在云上VPN连接的密钥，用于双方VPN设备的IKE协商，需要确保双方配置一致，否则会导致IKE协商失败。

相关链接：

建立IPsec VPN连接需要账户名和密码吗?

12.10 区域和可用区

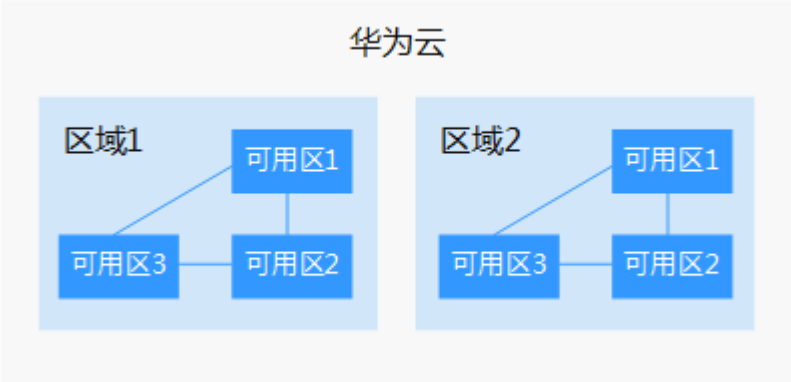
什么是区域、可用区?

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12-2阐明了区域和可用区之间的关系。

图 12-2 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**。