虚拟专用网络

产品介绍

文档版本 01

发布日期 2021-08-30

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。

目 录

1 什么是虚拟专用网络

产品概述

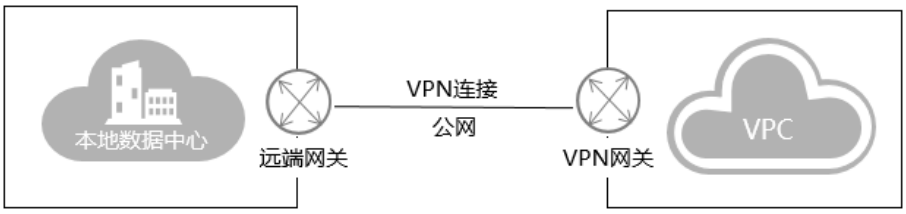
虚拟专用网络（Virtual Private Network，以下简称VPN），用于在远端用户和虚拟私有云（Virtual Private Cloud，以下简称VPC）之间建立一条安全加密的公网通信隧道。当您作为远端用户需要访问VPC的业务资源时，您可以通过VPN连通VPC。

默认情况下，在虚拟私有云（VPC）中的弹性云服务器无法与您自己的数据中心或私有网络进行通信。如果您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，可以启用VPN功能。

VPN由VPN网关和VPN连接组成，VPN网关提供了虚拟私有云的公网出口，与用户本地数据中心侧 的远端网关对应。VPN连接则通过公网加密技术，将VPN网关与远端网关关联，使本地数据中心与虚拟私有云通信，更快速、安全的构建混合云环境。

VPN组网图如图1-1所示。

图 1-1 VPN 组网图



组成部分

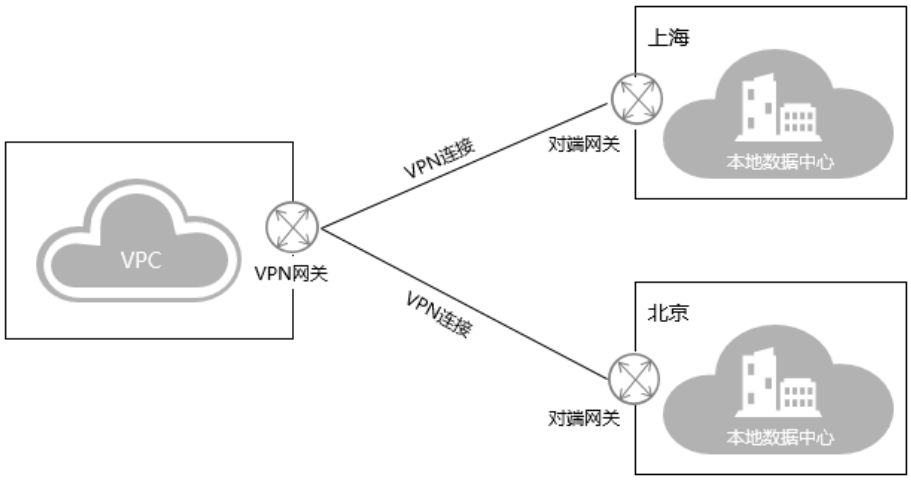
- **VPN网关**

  VPN网关是虚拟私有云中建立的出口网关设备，通过VPN网关可建立虚拟私有云和企业数据中心或其它区域VPC之间的安全可靠的加密通信。

  VPN网关需要与用户本地数据中心的远端网关配合使用，一个本地数据中心绑定一个远端网关，一个虚拟私有云绑定一个VPN网关。VPN支持点到点或点到多点连接，所以，VPN网关与远端网关为一对一或一对多的关系。

  VPN网关如图1-2所示。

图 1-2 组网拓扑



说明

在控制台中创建VPN网关详细请查看**创建VPN网关**。

- **VPN连接**

  VPN连接是一种基于Internet的IPsec加密技术，帮您快速构建VPN网关和用户本地数据中心的远端网关之间的安全、可靠的加密通道。当前VPN连接支持IPsec VPN协议。

  VPN连接使用IKE和IPsec协议对传输数据进行加密，保证数据安全可靠，并且VPN连接使用的是公网技术，更加节约成本。

  说明

  在控制台中创建VPN连接详细请查看**创建VPN连接**。

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。

用户可直接登录管理控制台访问VPN服务。

- 如果用户已注册帐户，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“注册华为云并实名认证”。

2 产品优势

虚拟专用网络具有以下几大产品优势：

- **高安全**

  采用华为专业设备，基于IKE和IPsec对传输数据加密，提供了电信级的高可靠性机制，从硬件、软件、链路三个层面保证VPN服务的稳定运行。
- **无缝扩展资源**

  将用户本地数据中心与云上VPC互联，业务快速扩展上云，实现混合云部署。
- **连通成本低**

  利用Internet构建IPsec加密通道，使用费用相对云专线服务更便宜。
- **即开即用**

  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。

3 应用场景

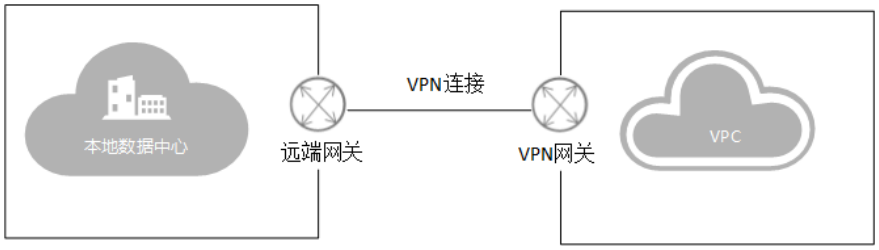
通过VPN在传统数据中心与VPC之间建立通信隧道，您可方便地使用云平台的云服务器、块存储等资源；应用程序转移到云中、启动额外的Web服务器、增加网络的计算容量，从而实现企业的混合云架构，既降低了企业IT运维成本，又不用担心企业核心数据的扩散。

VPN支持站点到站点的连接和多站点连接。

单站点 VPN 连接

您可以通过建立VPN将本地数据中心和VPC快速连接起来，构建混合云。如图3-1所示。

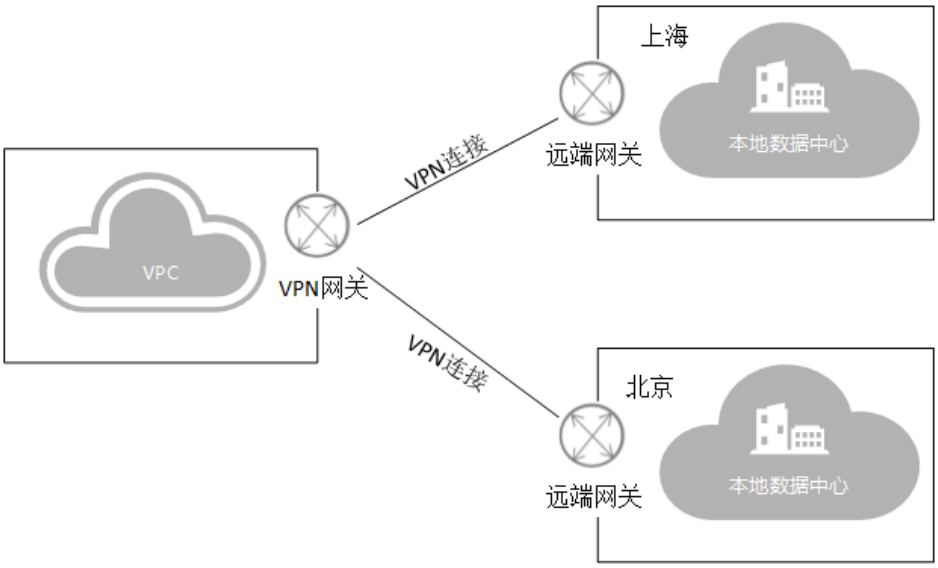
图 3-1 单站点连接



多站点 VPN 连接

您可以通过建立VPN将多个本地数据中心和VPC快速连接起来，构建混合云。如图3-2所示。

图 3-2 多站点连接



说明

建立多站点VPN连接要求各个站点之间的子网网段不能冲突。

4 约束与限制

关于VPN的使用，您需要注意以下几点：

- 每个帐号默认可以创建2个VPN网关。

  说明

  VPN网关需要与用户本地数据中心的远端网关配合使用，一个本地数据中心绑定一个远端网关，一个虚拟私有云绑定一个VPN网关。VPN支持点到点或点到多点连接，所以，VPN网关与远端网关为一对一或一对多的关系。

- 每个帐号默认可以创建12个VPN连接。

  请在购买VPN网关前确认您可用的配额，如果选购信息超出配额可通过**提交工单**申请扩容。

  说明

  VPN连接的数量与VPN连接的本端子网和远端子网的数量无关，仅与用户VPC需要连通的用户本地数据中心（或其它Region的VPC）的数量有关，已创建的VPN连接的数量即VPN连接列表中展示的数量（一个条目即一个VPN连接），也可以在VPN网关中查看当前网关已创建的VPN连接数量。

- 同一区域内的VPN网关之间不能创建VPN连接，详细请参见**VPN支持将两个VPC互连吗？**。

5 参考标准和协议

与IPsec特性相关的参考标准与协议如下：

- RFC 4301：Security Architecture for the Internet Protocol
- RFC 2403：The Use of HMAC-MD5-96 within ESP and AH
- RFC 2409：The Internet Key Exchange (IKE)
- RFC 2857：The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and its use with IPsec
- RFC 3625：More Modular Exponential (MODP)Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3664：The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 3706：A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3748：Extensible Authentication Protocol(EAP)
- RFC 3947：Negotiation of NAT-Traversal in the IKE
- RFC 4109：Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 3948：UDP Encapsulation of IPsec ESP Packets
- 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 4322：Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC 4359：The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4434：The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478：Repeated Authentication in Internet Key Exchange (IKEv2)
- RFC 5996：Internet Key Exchange Protocol Version 2 (IKEv2)

6 计费说明

计费项

表 6-1 VPN 计费项

计费方式	计费项一	计费项二	计费公式
包周期	带宽费用	VPN费用	带宽费用+VPN费用
按带宽计费	VPN网关带宽费用	VPN连接费用	VPN网关带宽费用+VPN连接费用
按流量计费	公网流量费用	VPN连接费用	公网流量费用+VPN连接费用

VPN费用详情请参见**产品价格详情**。

计费模式

包周期（包年/包月）

- **计费方式**：仅支持按带宽，不支持按流量。在创建网关阶段一次性收取带宽费用和VPN费用，用户后续创建VPN连接时不再收取费用。同时包周期付费方式相比按需付费享受更多折扣优惠。
- **计费公式**：带宽费用+VPN费用

  带宽由所有基于该网关创建的VPN连接共享，请用户基于所有VPN连接的传输数据量来评估所需带宽大小。

按需计费

- **按带宽计费**

  计费的周期为1小时，费用也会因带宽大小存在差异。费用包含了网关带宽费用和单条连接费用，您在创建第二条连接时只产生连接的费用。

  计费公式：VPN网关带宽费用+VPN连接费用

  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。

  a. 如果所购带宽 <= 10M， 则入云方向统一限定为10M。

b. 如果所购带宽 >10M， 则入云方向与所购买的带宽一致。

例如，用户选择带宽是50M， 用户使用VPN网关5小时，5小时后删除了资源，则会按照50M带宽收取5小时的使用费。注：按带宽计费与数据传输量没有关系，即使在5小时中，用户实际没有传输数据，也会收取带宽费用。

- **按流量计费**

  统计1小时内产生的流量费用，计费单位为1GByte，不足时按实际量收取（实际收取=实际使用流量/1GByte*单价）。此时，调整带宽大小不产生计费差异，只按出云方向的流量计算，入云方向的不统计。

  计费公式：公网流量费用+VPN连接费用

变更配置

VPN计费方式变更当前支持以下几种情况：

- 按需按带宽转包周期。
- 按需按带宽与按需按流量相互转换。
- 按需按流量转包周期。

说明

- 按需按流量转包周期，需要先将按需按流量转为按需按带宽，再转包周期。
- 包周期资源不支持降配，不可转按需。

按需按带宽转包周期

- **前提条件（按需按带宽转包周期）**
  a. 计费方式选择为按带宽计费。即当前支持按带宽计费的按需计费方式转包周期。
  b. 已创建的VPN连接数量小于10个。
  c. 帐号下可创建VPN连接的配额余量不少于10个。
- **操作步骤**
  a. 登录管理控制台。
  b. 在管理控制台左上角单击 图标，选择区域和项目。
  c. 在系统首页，单击“网络 > 虚拟专用网络”。
  d. 在左侧导航栏选择“虚拟专用网络 > VPN网关”。
  e. 在“VPN网关”界面目标VPN网关所在行，选择“更多>转包年/包月”。
  f. 在“转包年/包月”弹窗界面，单击“确定”。

  说明

  - 包周期模式下，VPN连接数表示基于当前VPN网关可免费创建的VPN连接的数量。
  - 按需转包周期场景下，按需VPN网关只能转为VPN连接数为10个的包周期VPN网关。

  g. 在“按需转包周期”界面，确认需要操作的VPN网关信息，选择续费时长。
  h. 单击“去支付”，进入支付界面。
  i. 在支付界面，确认订单信息，选择优惠和付款方式。
  j. 单击“确认付款”，完成支付。

说明

按需转包周期操作不会影响用户正常业务。

按需按流量转按需按带宽/按需按流量转包周期

1. 在VPN网关列表页面，选择目标VPN网关所在行。
2. 在目标VPN网关所在行的“操作”列，选择“更多 > 修改带宽 ”，进入修改带宽页面。
3. 在修改带宽页面，选择“变更规格 > 按带宽计费”。
4. 单击“提交”，完成按需按流量转按需按带宽。
5. 返回VPN网关列表页面，再次选择目标VPN网关所在行。
6. 在目标VPN网关所在行的“操作”列，选择“更多 > 转包年/包月 ”。
7. 单击“确定”，进入按需转包周期页面。
8. 选择续费时长，单击“去支付”。
9. 选择支付方式，单击“确认付款”。

续费

详细请查看**续费管理**。

到期与欠费

详细请查看**欠费还款**。

更多计费常见问题请参见**VPN常见计费问题**。

7 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**。

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，“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VPN时，需要先切换至授权区域。

如**表7-1**所示，包括了VPN的所有系统角色。

表 7-1 VPN 系统角色

角色名称	描述	依赖关系
VPN Administrator	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。 拥有该权限的用户必须同时拥有Tenant Guest、VPC Administrator权限。	依赖Tenant Guest、VPC Administrator策略。 • 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。

表7-2列出了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 7-2 常用操作与系统权限的关系

操作	VPN Administrator
创建VPN网关	√
查询VPN网关	√
修改VPN网关	√
删除VPN网关	√
创建VPN连接	√
查询VPN连接	√
修改VPN连接	√
删除VPN连接	√

相关链接

- IAM产品介绍
- 创建用户组、用户并授予VPN权限

8 与其他服务的关系

VPN服务与其他云服务的关系如图8-1所示。

图 8-1 与其他服务的关系

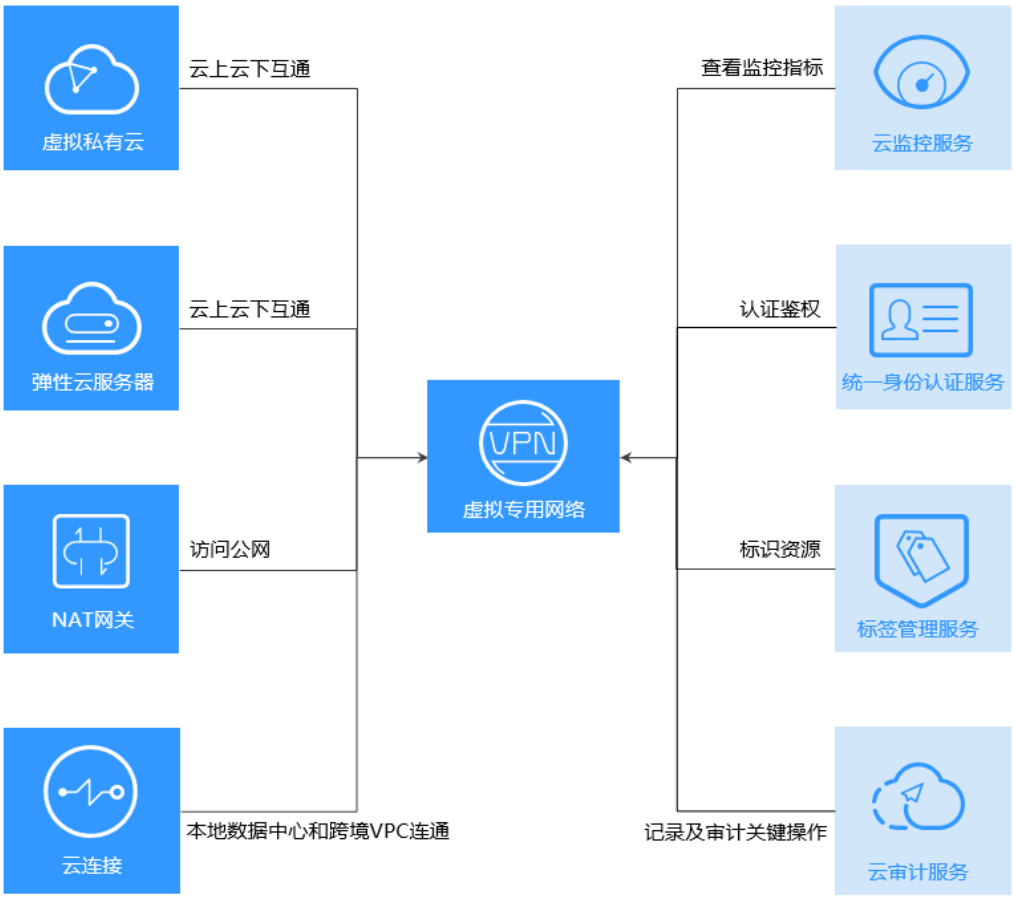


表 8-1 与其他服务的关系

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，本地数据中心才可以通过VPN上云。	**创建虚拟私有云及默认子网**
虚拟私有云（Virtual Private Cloud，VPC）	通过VPC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。	**创建安全组**
云连接（Cloud Connect）	通过云连接服务，可以实现本地数据中心和跨境VPC之间的稳定网络连通。	**构建稳定的跨境网络连接**
NAT网关（NAT Gateway）	通过NAT网关服务，可以实现本地数据中心服务器访问公网或为公网提供服务。	**云间NAT网关高速访问互联网**
弹性云服务器（Elastic Cloud Server，ECS）	通过VPC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。	**添加安全组规则**
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。	**查看监控指标**
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**

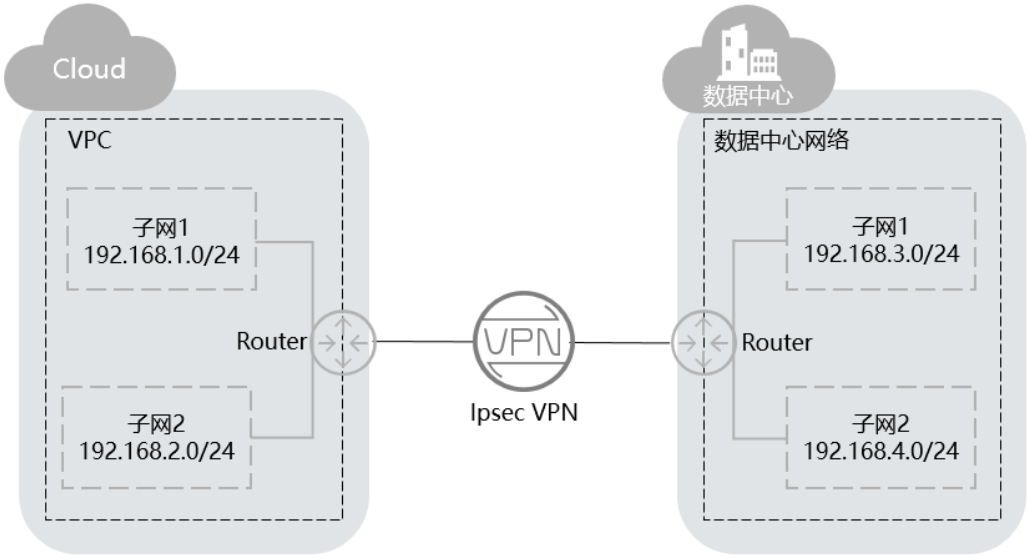
9 基本概念

9.1 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。

如图9-1所示，假设您在云中已经申请了VPC，并申请了2个子网（192.168.1.0/24，192.168.2.0/24），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）。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 9-1 IPsec VPN



目前我们支持点到点VPN（Site-to-Site VPN）和点到多点VPN（Hub-Spoke VPN），需要您在自己的数据中心内也搭建VPN。

VPC内的VPN和您搭建的VPN，需要保证IKE策略以及IPsec策略配置一致。在配置前，请确认您的设备满足IPsec的相关标准协议。

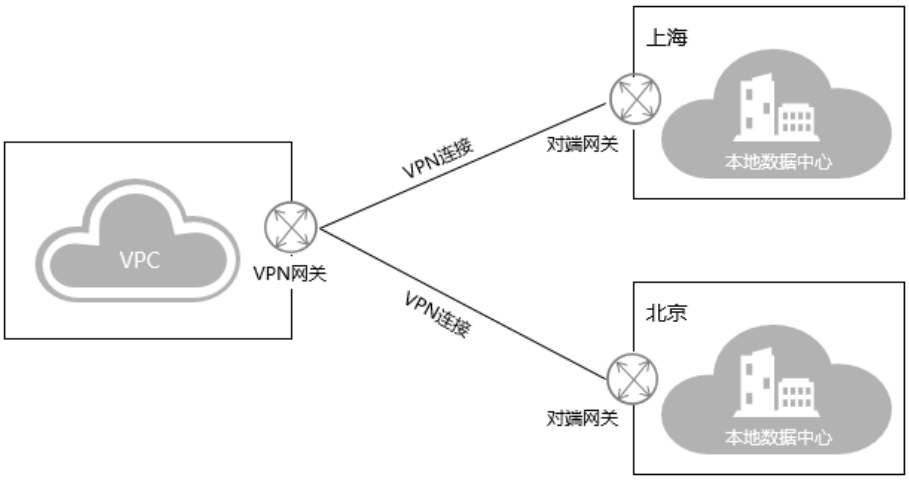
9.2 VPN 网关

VPN网关是虚拟私有云中建立的出口网关设备，通过VPN网关可建立虚拟私有云和企业数据中心或其它区域VPC之间的安全可靠的加密通信。

VPN网关需要与用户本地数据中心的远端网关配合使用，一个本地数据中心绑定一个远端网关，一个虚拟私有云绑定一个VPN网关。VPN支持点到点或点到多点连接，所以，VPN网关与远端网关为一对一或一对多的关系。

VPN网关如**图9-2**所示。

图 9-2 组网拓扑



9.3 VPN 连接

VPN连接是一种基于Internet的IPsec加密技术，帮您快速构建VPN网关和用户本地数据中心的远端网关之间的安全、可靠的加密通道。当前VPN连接支持IPsec VPN协议。

VPN连接使用IKE和IPsec协议对传输数据进行加密，保证数据安全可靠，并且VPN连接使用的是公网技术，更加节约成本。

9.4 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 <= 10M，则入云方向统一限定为10M。
- 如果所购带宽 >10M，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。

9.5 本端子网

本端子网即华为云VPC中的网段，该网段需要通过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特性连接进来的其它VPC的网段。

9.6 远端网关

用户侧数据中心VPN网关需具备固定公网IP，动态拨号公网IP无法与华为云进行IPsec VPN对接。如果用户侧公网IP进行了变更，则需要尽快在华为云上进行同步修改。否则，会导致VPN不通。

相关链接：

哪些设备可以与华为云进行VPN对接?

9.7 远端子网

远端子网即用户侧数据中心的网段，该网段需要通过VPN与华为云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。

用户在设置完远端子网后，无需在VPC中增加路由信息，VPN服务会自动在VPC中下发到达远端子网的路由。

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。

9.8 预共享密钥

预共享密钥（Pre Shared Key），指配置在云上VPN连接的秘钥，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连接需要帐户名和密码吗?

9.9 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9-3阐明了区域和可用区之间的关系。

图 9-3 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。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**。