虚拟专用网络

用户指南

文档版本	01
发布日期	2020-08-30

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 简介

1.1 什么是虚拟专用网络

产品概述

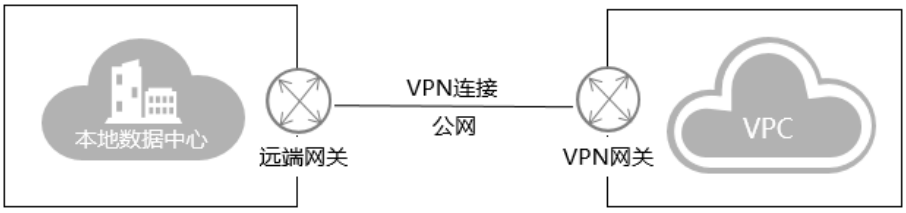
虚拟专用网络（Virtual Private Network，以下简称VPN），用于在远端用户和虚拟私有云（Virtual Private Cloud，以下简称VPC）之间建立一条安全加密的公网通信隧道。当您作为远端用户需要访问VPC的业务资源时，您可以通过VPN连通VPC。

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。

1.2 应用场景

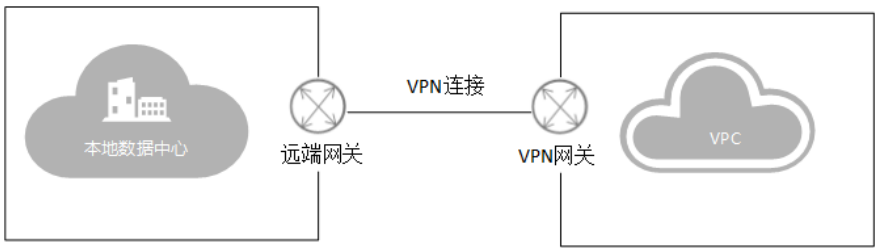
通过VPN在传统数据中心与VPC之间建立通信隧道，您可方便地使用云平台的云服务器、块存储等资源；应用程序转移到云中、启动额外的Web服务器、增加网络的计算容量，从而实现企业的混合云架构，既降低了企业IT运维成本，又不用担心企业核心数据的扩散。

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1-2**所示。

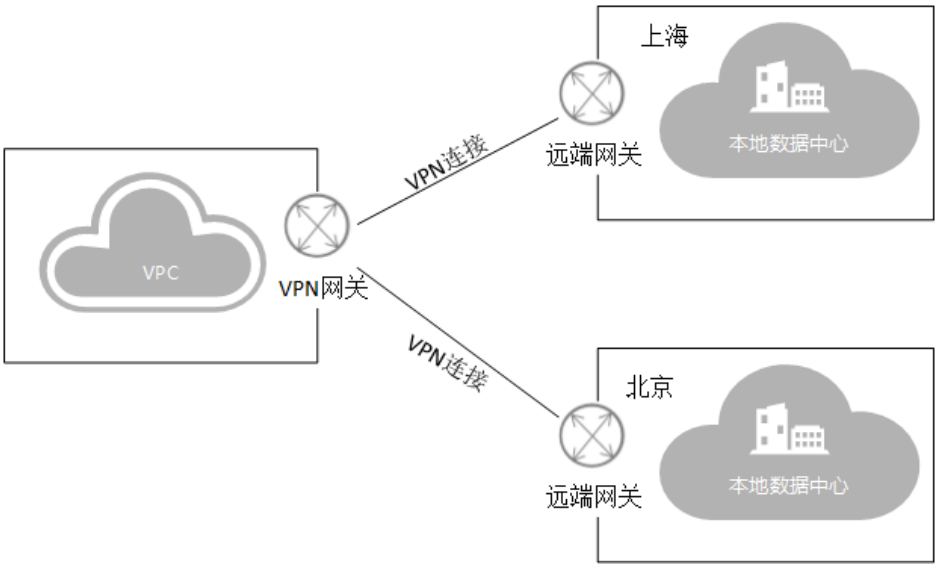
图 1-2 单站点连接



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1-3**所示。

图 1-3 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。

1.3 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)

1.4 权限管理

如果您需要对云服务平台上创建的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云服务资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制他们对云服务资源的访问范围。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，您只需要为您帐号中的资源进行付费。

关于IAM的详细介绍，请参见**IAM产品简介**。

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”，然后在指定区域对应的项目中设置相关权限，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1-1**所示，包括了VPN的所有系统角色。

表 1-1 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1-2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 1-2 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产品简介
- 创建用户并授权使用VPN

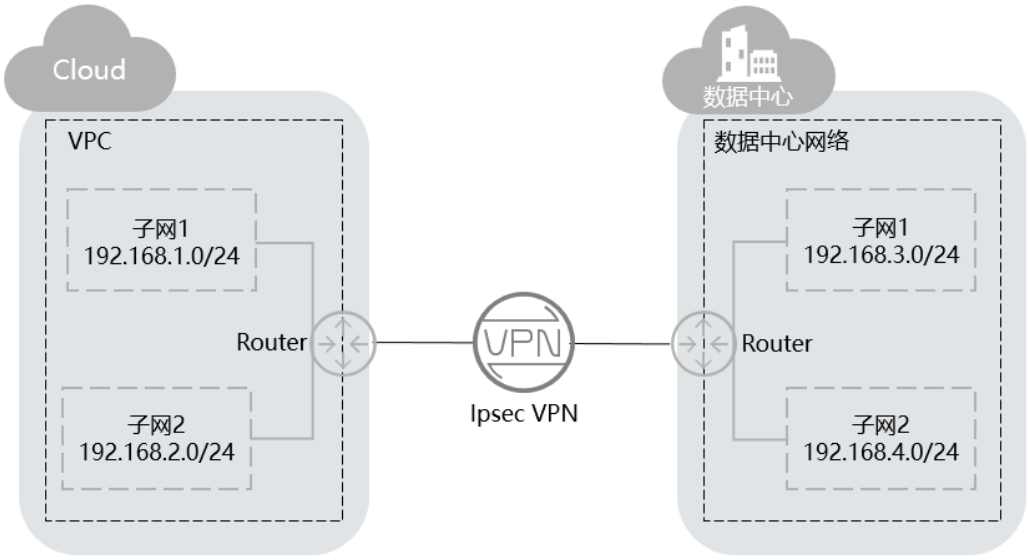
1.5 基本概念

1.5.1 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1-4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Router下也有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 1-4 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。

1.5.2 区域和可用区

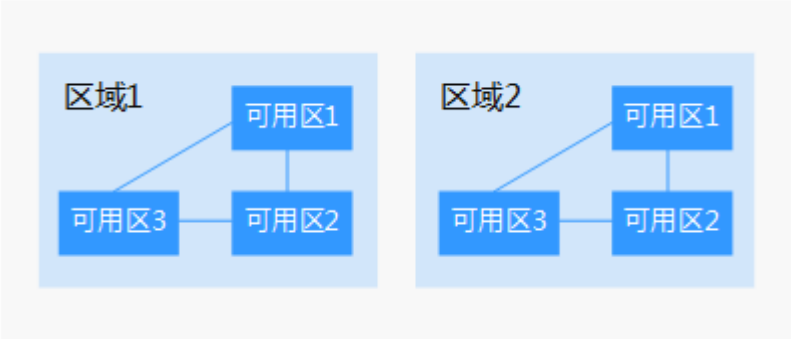
什么是区域、可用区?

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）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。
- 可用区（AZ，Availability Zone）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图1-5阐明了区域和可用区之间的关系。

图 1-5 区域和可用区



如何选择区域?

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。

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

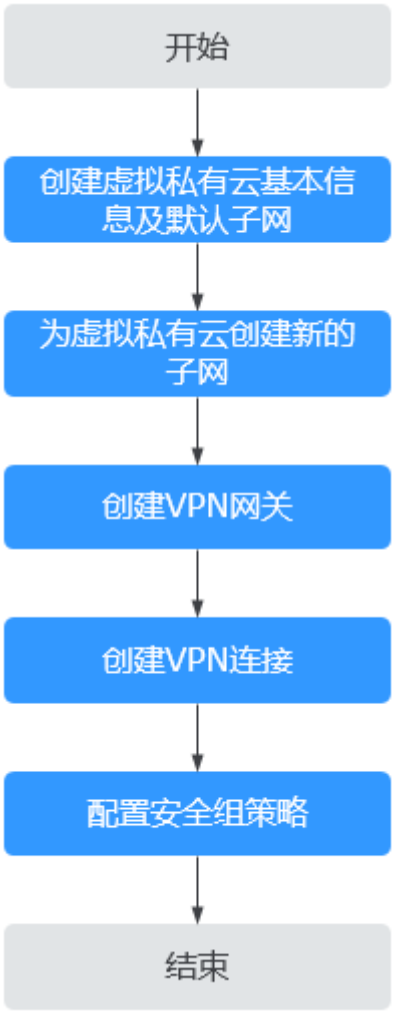
当您通过API使用资源时，您必须指定其区域终端节点。有关公有云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

2 入门

2.1 流程简介

默认情况下，在Virtual Private Cloud (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，可以启用虚拟专用网络（VPN）功能。

图 2-1 虚拟专用网络入门流程图



2.2 创建虚拟私有云基本信息及默认子网（可选）

操作场景

虚拟私有云可以为您的弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。

要拥有一个完整的虚拟私有云，第一步请参考本章节任务创建虚拟私有云的基本信息及默认子网；然后再根据您的实际网络需求，参考后续章节继续创建子网、申请弹性公网IP、安全组等网络资源。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 单击“创建虚拟私有云”。
4. 在“创建虚拟私有云”页面，根据界面提示配置虚拟私有云参数。

创建虚拟私有云时会同时创建一个默认子网，您还可以单击“添加子网”创建多个子网。

单击“自定义配置”，配置子网的高级参数。

表 2-1 虚拟私有云参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	-
名称	VPC名称。 名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	VPC-001
网段	VPC的地址范围，VPC内的子网地址必须在VPC的地址范围内。 目前支持网段范围： 10.0.0.0/8~24 172.16.0.0/12~24 192.168.0.0/16~24	192.168.0.0/16
企业项目	创建VPC时，可以将VPC加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。 关于创建和管理企业项目的详情，请参见《企业项目用户指南》。	default
标签	虚拟私有云的标识，包括键和值。可以为虚拟私有云创建10个标签。	● 键：vpc_key1 ● 值：vpc-01

表 2-2 子网参数说明

参数	说明	取值样例
名称	子网的名称。 名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	Subnet

参数	说明	取值样例
子网网段	子网的地址范围，需要在VPC的地址范围内。	192.168.0.0/24
高级配置	单击下拉箭头，可配置子网的高级参数，包括网关、DNS服务器地址等。	默认配置
网关	子网的网关。 通向其他子网的IP地址，用于实现与其他子网的通信。	192.168.0.1
DNS服务器地址	DNS服务器地址可实现云服务器在VPC子网内直接通过内网域名互相访问。同时，还支持不经公网，直接通过内网DNS访问云上服务。 若您想要使用其他公网DNS进行解析，可以修改默认的DNS服务器地址。	100.125.x.x
DHCP租约时间	DHCP租约时间是指DHCP服务器自动分配给客户端的IP地址的使用期限。超过租约时间，IP地址将被收回，需要重新分配。单位：天/小时。 DHCP租约时间改后，会在一段时间后自动生效（与您的DHCP租约时长有关），如果需要立即生效，请重启ECS或者在实例中主动触发DHCP更新。	365

5. 检查当前配置，单击“立即创建”。

2.3 为虚拟私有云创建新的子网（可选）

操作场景

申请VPC时会创建默认子网，当默认子网不能满足需求时，您可以创建新的子网。

子网默认配置DHCP协议，即使用该VPC的弹性云服务器启动后，会通过DHCP协议自动获取到IP地址。

说明

当前在部分区域中，子网与虚拟私有云已解耦，解耦后子网入口迁移，目前存在以下两种入口。

- 在虚拟私有云详情页的“子网”页签，可对子网进行操作。本小节的操作步骤指导以此入口为例。
- 在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“子网”，可对子网进行操作。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“虚拟私有云”。
5. 在虚拟私有云列表中，单击需要创建子网的虚拟私有云名称。
6. 在“子网”页签中，单击“创建子网”。
7. 根据界面提示配置参数。

表 2-3 参数说明

参数	说明	取值样例
虚拟私有云	选择待创建子网的VPC。 当“子网”独立存在于导航栏时，本参数可见。	-
名称	子网的名称。 名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	Subnet
子网网段	子网的地址范围，需要在VPC的地址范围内。	192.168.0.0/24
子网IPv4网段	子网的地址范围，需要在VPC的地址范围内。 已申请IPv6公测的用户显示此配置项。	192.168.0.0/24
子网IPv6网段	选择是否勾选开启IPv6。 已申请IPv6公测的用户显示此配置项。开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。	-
高级配置	单击下拉箭头，可配置子网的高级参数，包括网关、DNS服务器地址等。	默认配置
网关	子网的网关。 通向其他子网的IP地址，用于实现与其他子网的通信。	192.168.0.1

参数	说明	取值样例
DNS服务器地址	DNS服务器地址可实现云服务器在VPC子网内直接通过内网域名互相访问。同时，还支持不经公网，直接通过内网DNS访问云上服务。 若您想要使用其他公网DNS进行解析，可以修改默认的DNS服务器地址。	100.125.x.x
DHCP租约时间	DHCP租约时间是指DHCP服务器自动分配给客户端的IP地址的使用期限。超过租约时间，IP地址将被收回，需要重新分配。单位：天。 DHCP租约时间改后，会在一段时间后自动生效（与您的DHCP租约时长有关），如果需要立即生效，请重启ECS或者在实例中主动触发DHCP更新。	365

8. 单击“确定”。

注意事项

子网创建成功后，有5个系统保留地址您不能使用。以192.168.0.0/24的子网为例，默认的系统保留地址如下：

- 192.168.0.0：网络标识符，私有IP地址范围开始，不作分配
- 192.168.0.1：网关地址
- 192.168.0.253：系统接口，用于VPC对外通信
- 192.168.0.254：DHCP服务地址
- 192.168.0.255：广播地址

如果您在创建子网时选择了自定义配置，系统保留地址可能与上面默认的不同，系统会根据您的配置进行自动分配。

2.4 创建 VPN 网关

操作场景

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，需要先创建VPN网关。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > VPN网关”。
5. 在“VPN网关”界面，单击“创建VPN网关”。

6. 根据界面提示配置参数，并单击“立即创建”。VPN网关参数请参考表2-4

表 2-4 VPN 网关参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	-
名称	VPN网关名称。	vpngw-001
虚拟私有云	VPN接入的VPC名称。	vpc-001
类型	VPN类型。默认为选择“IPsec”。	IPsec
计费方式	按需计费支持两种计费方式：按带宽计费/按流量计费。 • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 • 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。	按流量计费
带宽大小	本地VPN网关的带宽大小（单位Mbit/s），为所有基于该网关创建的VPN连接共享的带宽，VPN连接带宽总和不超过VPN网关的带宽。	100

表 2-5 VPN 连接参数说明

参数	说明	取值样例
名称	VPN连接名称	vpn-001
VPN网关	VPN连接挂载的VPN网关名称	vpcgw-001
本端子网	本端子网指需要通过VPN访问用户本地网络的VPC子网。 • 选择子网表示本地数据中心或者私有网络与您选择的子网进行互通。 • 选择CIDR表示本地数据中心或者私有网络与您配置的网段之间进行互通。 **说明** 多个本端子网不支持子网网段重叠。	192.168.1.0/24， 192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-

参数	说明	取值样例
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段、专线/云连接的远端子网网段重复。 **说明** 多个远端子网不支持子网网段重叠。	192.168.3.0/24， 192.168.4.0/24
预共享密钥	预共享密钥（Pre Shared Key），取值范围为6～128位。此项配置在VPC的VPN和您的数据中心的VPN中，配置需要一致。	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	• 默认配置 • 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参考**表2-6**和**表2-7**。	自定义配置

表 2-6 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：SHA1、SHA2-256、SHA2-384、SHA2-512、MD5。 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐）。 默认配置为：AES-128。	AES-128
DH算法	Diffie-Hellman密钥交换算法，支持的算法：Group 2、Group 5、Group 14。 默认配置为：Group 14。 协商双方的DH算法必须一致，否则会导致协商失败。	Group 14
版本	IKE密钥交换协议版本，支持的版本：v1、v2。 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Associations）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400

表 2-7 IPsec Policy 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：SHA1、SHA2-256、SHA2-384、SHA2-512、MD5。 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐）。 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置IPsec隧道协商时使用。 PFS组支持的算法：DH group 2、DH group 5、DH group 14。 默认配置为：DH group 14。	DH group 14
传输协议	IPsec传输和封装用户数据时使用的安全协议，目前支持的协议：AH、ESP、AH-ESP。 默认配置为：ESP。	ESP
生命周期（秒）	安全联盟（SA—Security Associations）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：3600。	3600

7. 确认创建的VPN网关规格，单击“确认申请”。

2.5 创建 VPN 连接

操作场景

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，创建VPN网关后需要创建VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > VPN连接”。
5. 在“VPN连接”页面，单击“创建VPN连接”。
6. 根据界面提示配置参数，并单击“立即创建”。VPN连接参数请参考**表2-8**。

表 2-8 VPN 连接参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	-
名称	VPN连接名称。	vpn-001
VPN网关	VPN连接挂载的VPN网关名称。	vpcgw-001
本端子网	本端子网指需要通过VPN访问用户本地网络的VPC子网。支持以下方式设置本端子网： ● 选择子网 ● 手动输入网段 **说明** 多个本端子网不支持子网网段重叠。	192.168.1.0/24， 192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段、专线/云连接的远端子网网段重复。 **说明** 多个远端子网不支持子网网段重叠。	192.168.3.0/24， 192.168.4.0/24
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，需要与本地网络VPN设备配置的密钥一致。此密钥用于VPN连接协商。 取值范围：6~128位。	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	● 默认配置 ● 已有配置 ● 自定义配置：包含IKE策略和IPsec策略，用于指定VPN隧道加密算法。相关配置说明请参考**表2-9**和**表2-10**。	自定义配置

表 2-9 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：SHA1、SHA2-256、SHA2-384、SHA2-512、MD5。 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐）。 默认配置为：AES-128。	AES-128
DH算法	Diffie-Hellman密钥交换算法，支持的算法：Group 2，Group 5，Group 14。 默认配置为：Group 14。	Group 14
版本	IKE密钥交换协议版本，支持的版本：v1、v2。 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Associations）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400

表 2-10 IPsec Policy 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：SHA1、SHA2-256、SHA2-384、SHA2-512、MD5。 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置IPsec隧道协商时使用。 PFS组支持的算法：DH group 2、DH group 5、DH group 14。 默认配置为：DH group 14。	DH group 14

参数	说明	取值样例
传输协议	IPsec传输和封装用户数据时使用的安全协议，目前支持的协议：AH、ESP、AH-ESP。 默认配置为：ESP。	ESP
生命周期（秒）	安全联盟（SA—Security Associations）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：3600。	3600

说明

IKE策略指定了IPsec 隧道在协商阶段的加密和认证算法，IPsec策略指定了IPsec在数据传输阶段所使用的协议，加密以及认证算法；这些参数在VPC上的VPN连接和您数据中心的VPN中需要进行相同的配置，否则会导致VPN无法建立连接。

7. 单击“确认申请”。

2.6 配置安全组策略（可选）

2.6.1 创建安全组

操作场景

您可以创建安全组并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。建议您将不同公网访问策略的弹性云服务器划分到不同的安全组。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航树选择“访问控制 > 安全组”。
5. 在“安全组”界面，单击“创建安全组”。
6. 在“创建安全组”界面，根据界面提示配置参数，参数说明参考**表2-11**。

表 2-11 参数说明

参数	参数说明	取值样例
模板	模板自带安全组规则，方便您快速创建安全组。提供如下几种模板： ● 自定义：用户自定义安全组规则。 ● 通用Web服务器：默认放通22、3389、80、443端口和ICMP协议。 ● 开放全部端口：开放全部端口有一定安全风险，请谨慎选择。	通用Web服务器
名称	安全组的名称，必填项。 安全组的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。 **说明** 安全组名称创建后可以修改，建议不要重名。	sg-318b
描述	安全组的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

7. 单击“确定”。

2.6.2 添加安全组规则

操作场景

安全组创建后，您可以在安全组中设置出方向、入方向规则，这些规则会对安全组内部的云服务器出入方向网络流量进行访问控制，当云服务器加入该安全组后，即受到这些访问规则的保护。

- 入方向：指从外部访问安全组规则下的弹性云服务器。
- 出方向：指安全组规则下的弹性云服务器访问安全组外的实例。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航树选择“访问控制 > 安全组”。
5. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。
6. 在入方向规则页签，单击“添加规则”，添加入方向规则。
   单击“+”可以依次增加多条入方向规则。

表 2-12 入方向参数说明

参数	说明	取值样例
协议端口	网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。	Custom TCP
	端口：允许远端地址访问弹性云服务器指定端口，取值范围为：1～65535。	22或22-30
源地址	源地址：可以是IP地址、安全组。例如： ● xxx.xxx.xxx.xxx/32（IPv4地址） ● xxx.xxx.xxx.0/24（子网） ● 0.0.0.0/0（任意地址） ● sg-abc（安全组）	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

7. 在出方向规则页签，单击“添加规则”，添加出方向规则。
   单击“+”可以依次增加多条出方向规则。

表 2-13 出方向参数说明

参数	说明	取值样例
协议端口	网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。	Custom TCP
	端口：允许弹性云服务器访问远端地址的指定端口，取值范围为：1～65535。	22或22-30
源地址	源地址：可以是IP地址、安全组。例如： ● xxx.xxx.xxx.xxx/32（IPv4地址） ● xxx.xxx.xxx.0/24（子网） ● 0.0.0.0/0（任意地址） ● sg-abc（安全组）	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

8. 单击“确定”。

3 管理

3.1 VPN 连接管理

3.1.1 查看已创建的 VPN 连接

操作场景

用户申请VPN连接后，可以查看已申请的VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络> VPN连接”。
5. 在“VPN连接”页面的VPN连接列表中可以查看VPN连接。
6. 在VPN连接列表中，单击“操作”列的“策略详情”，查看该VPN连接对应的IKE策略和IPsec策略详情。

3.1.2 修改已创建的 VPN 连接

操作场景

VPN连接是建立VPN网关和外部数据中心VPN网关之间的加密通道。当VPN连接的网络参数变化时，可以修改VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > VPN连接”。
5. 在“VPN连接”界面所需修改的VPN连接所在行，单击“修改”。
6. 根据界面提示配置参数。
7. 单击“确定”。

3.1.3 删除 VPN 连接

操作场景

当无需使用VPN网络、需要释放网络资源时，可删除VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > VPN连接”。
5. 在“VPN连接”界面所需删除的VPN连接所在行，单击“删除”。
6. 单击“是”。

3.2 VPN 网关管理

3.2.1 查看已创建的 VPN 网关

操作场景

用户申请VPN网关后，可以查看已申请的VPN网关。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > VPN网关”。
5. 在“VPN网关”页面的VPN网关列表中可以查看VPN网关。

3.2.2 修改已创建的 VPN 网关

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > VPN网关”。

5. 在“VPN网关”界面目标VPN网关所在行，选择“更多 > 修改带宽”。
   也可以选择“更多 > 修改基本信息”。
6. 根据界面参数，修改VPN网关的带宽，或者名称和描述信息。
7. 单击“确定”。

3.2.3 删除 VPN 网关

操作场景

当无需使用VPN网关时，可删除VPN网关。

已被VPN连接使用的VPN网关不可删除，请先删除相关的VPN连接，再删除VPN网关。

操作步骤

1. 在左侧导航栏选择“虚拟专用网络 > VPN网关”。
2. 在“VPN网关”界面所需删除的VPN网关所在行，单击“删除”。
3. 单击“是”。

3.3 监控

3.3.1 监控虚拟专用网络

监控是保持VPN可靠性、可用性和性能的重要部分，通过监控，用户可以观察VPN资源。为使用户更好地掌握自己的VPN运行状态，云平台提供了云监控。您可以使用该服务监控您的VPN，执行自动实时监控、告警和通知操作，帮助您更好地了解VPN的各项性能指标。

通过后续章节，您可以了解以下内容：

- **支持的监控指标**
- **设置告警规则**
- **查看监控指标**

3.3.2 支持的监控指标

功能说明

本节定义了虚拟专用网络服务上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供的管理控制台检索VPN服务产生的监控指标和告警信息。

命名空间

SYS.VPN

监控指标

表 3-1 VPN 连接状态监控

指标	指标名称	含义	取值范围	测量对象	监控周期（原始指标）
connection_status	VPN连接状态	展示VPN连接的通断状态。 0：未连接状态 1：连接状态	0，1	VPN连接	5分钟

表 3-2 弹性公网 IP 和带宽支持的监控指标

指标	指标名称	含义	取值范围	测量对象&维度	监控周期（原始指标）
upstream_bandwidth	出网带宽	该指标用于统计测试对象出云平台的网络速度（原指标为上行带宽）。 单位：比特/秒。	≥ 0 bits/s	测量对象：带宽或弹性公网IP。 测量维度： bandwidth_id, publicip_id	1分钟
downstream_bandwidth	入网带宽	该指标用于统计测试对象入云平台的网络速度（原指标为下行带宽）。 单位：比特/秒。	≥ 0 bits/s	测量对象：带宽或弹性公网IP。 测量维度： bandwidth_id, publicip_id	1分钟

指标	指标名称	含义	取值范围	测量对象&维度	监控周期（原始指标）
upstream_bandwidth_usage	出网带宽使用率	该指标用于统计测量对象出云平台的带宽使用率，以百分比为单位。	0-100%	测量对象：带宽或弹性公网IP。 测量维度： bandwidth_id, publicip_id	1分钟
up_stream	出网流量	该指标用于统计测试对象出云平台的网络流量（原指标为上行流量）。 单位：字节。	≥ 0 bytes	测量对象：带宽或弹性公网IP。 测量维度： bandwidth_id, publicip_id	1分钟
down_stream	入网流量	该指标用于统计测试对象入云平台的网络流量（原指标为下行流量）。 单位：字节。	≥ 0 bytes	测量对象：带宽或弹性公网IP。 测量维度： bandwidth_id, publicip_id	1分钟

维度

key	Value
connection_id	VPN连接

3.3.3 创建告警规则

操作场景

通过设置告警规则，用户可自定义监控目标与通知策略，及时了解虚拟专用网络的状况，从而起到预警作用。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“管理与部署 > 云监控”。
4. 在左侧导航栏，选择“告警 > 告警规则”。
5. 在“告警规则”界面，单击“创建告警规则”进行添加，或者选择已有的告警规则进行修改，设置虚拟专用网络的告警规则。
6. 规则参数设置完成后，单击“立即创建”。

   虚拟专用网络告警规则设置完成后，当符合规则的告警产生时，系统会自动进行通知。

   说明

   更多关于虚拟专用网络监控规则的信息，请参见《云监控用户指南》。

3.3.4 查看监控指标

操作场景

查看VPN连接状态、带宽、弹性公网IP的使用情况。

操作步骤

查看VPN连接状态：

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“管理与部署 > 云监控服务”。
4. 单击页面左侧的“云服务监控”，选择“虚拟专用网络”。
5. 单击“操作”列的“查看监控指标”，查看VPN连接状态。

   支持查看“近1小时”、“近3小时”和“近12小时”的数据。

   说明

   用户也可以在登录管理控制台，选择“虚拟专用网络服务 > VPN连接”，在目标VPN连接所在行选择“操作 > 查看监控”，查看VPN连接状态。

查看带宽或弹性公网IP：

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。

3. 在系统首页，选择“网络 > 虚拟专用网络”。
4. 单击页面左侧的“VPN网关”。
5. 单击“操作”列的“查看监控”，查看带宽或弹性公网IP的监控指标详情。
   支持查看“近1小时”、“近3小时”和“近12小时”的数据。

3.4 权限管理

3.4.1 创建用户并授权使用 VPN

如果您需要对您所拥有的VPN进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用VPN资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将VPN资源委托给更专业、高效的其他账号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

如果账号 已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用VPN服务的其它功能。

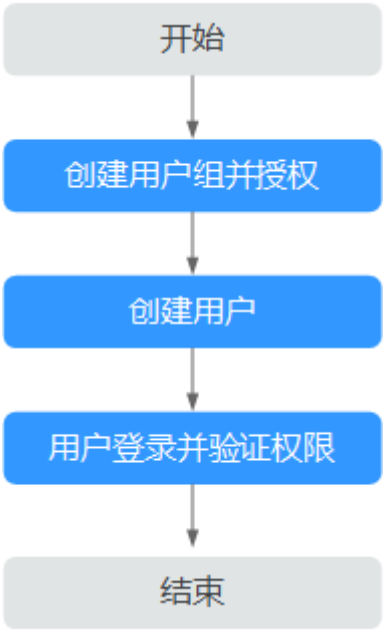
本章节为您介绍对用户授权的方法，操作流程如**图3-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的VPN权限，并结合实际需求进行选择，VPN支持的系统权限，请参见：**权限管理**。如果您需要对除VPN之外的其它服务授权，IAM支持服务的所有权限请参见**权限集**。

示例流程

图 3-1 给用户授予 VPN 权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予消息通知服务权限“VPN Administrator”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，切换至授权区域，验证权限：
   - 在“服务列表”中选择“网络 > 虚拟专用网络”，进入“虚拟专用网络 > VPN网关”页面，单击右上角“创建VPN网关”，尝试创建VPN网关，如果创建成功，表示“VPN Administrator”已生效。
   - 在“服务列表”中选择除VPN服务外（假设当前权限仅包含VPN Administrator）的任一服务，如果提示权限不足，表示“VPN Administrator”已生效。

3.5 关于配额

什么是配额?

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台弹性云服务器、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击页面右上角的“My Quota”图标 。
   系统进入“服务配额”页面。
4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

1. 登录管理控制台。
2. 单击“申请扩大配额”。
3. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。
4. 填写完毕后，勾选协议并单击“提交”。

4 最佳实践

4.1 通过 VPN 连接 VPC

操作场景

默认情况下，在Virtual Private Cloud (VPC) 中的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中的和您的数据中心或私有网络连通，可以启用VPN功能。申请VPN后，用户需要配置安全组并检查本端与对端网络的连通性，以确保VPN功能可用。主要场景分为两类：

- 点对点VPN：本端为处于云服务平台上的一个VPC，对端为一个数据中心，通过VPN建立用户数据中心与VPC之间的通信隧道。
- 点对多点VPN：本端为处于云服务平台上的一个VPC，对端为多个数据中心，通过VPN建立不同用户数据中心与VPC之间的通信隧道。

配置VPN时需要注意以下几点：

- 本端子网与对端子网不能重复。
- 本端子网网段不能重复。
- 本端和对端的IKE策略、IPsec策略、PSK相同。
- 本端和对端子网，网关等参数对称。
- VPC内安全组允许访问对端和被对端访问。
- VPN对接成功后两端的服务器或者虚拟机之间需要进行通信，VPN的状态才会刷新为正常。

前提条件

已创建VPN所需的虚拟私有云和子网。

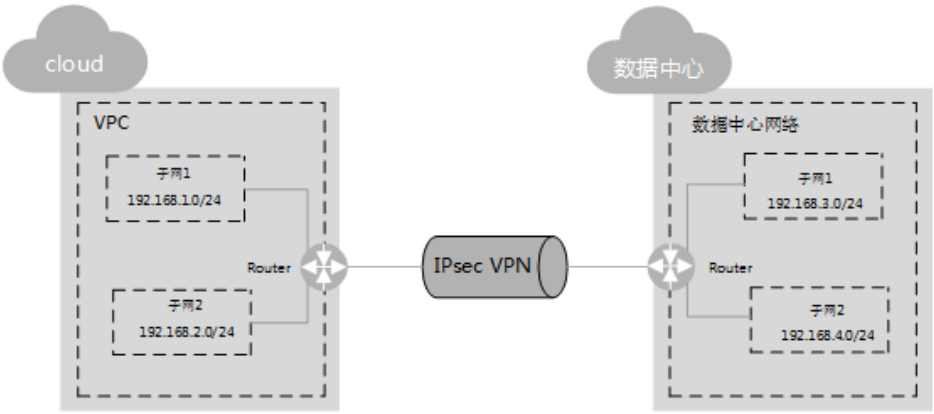
操作步骤

1. 在管理控制台上，选择合适的IKE策略和IPsec策略申请VPN。
2. 检查本端和对端子网的IP地址池。

   如图4-1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Router下也有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 4-1 IPsec VPN



本端和对端子网IP池不能重合。例如，本端VPC有两个子网，分别为：192.168.1.0/24和192.168.2.0/24，那么对端子网的IP地址池不能包含本端VPC的这两个子网。

3. 配置VPC的安全组策略。
4. 检查VPC安全组。

   安全组必须放通来自VPN的报文。可以使用ping方法来检查VPC安全组是否放通。
5. 检查远端LAN配置（即对端数据中心网络配置）。

   在远程LAN（对端数据中心网络）配置中有可以将VPN流量转发到LAN中网络设备的路由。如果VPN流量无法正常通信，请检查远程LAN是否存在拒绝策略。

5 常见问题

5.1 IPsec VPN 是否会自动进行协商?

IPsec VPN隧道为被动模式，只有在本端有流量经过隧道时才会触发自动协商。

5.2 如何解决 VPN 连接无法建立连接问题?

1. 检查云上VPN连接中的IKE策略和IPsec策略中的协商模式和加密算法是否与远端配置一致。
   a. 如果第一阶段IKE策略已经建立，第二阶段的IPsec策略未开启，常见情况为IPsec策略与数据中心远端的配置不一致。
   b. 如果客户本地侧使用的是CISCO的物理设备，建议客户使用MD5算法。同时将云上VPN连接端IPsec策略中的认证算法设置为MD5。
2. 检查ACL是否配置正确。

   假设您的数据中心的子网为192.168.3.0/24和192.168.4.0/24，VPC下的子网为192.168.1.0/24和192.168.2.0/24，则你在数据中心或局域网中的ACL应对你的每一个数据中心子网配置允许VPC下的子网通信的规则，如下例：

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   ```
3. 配置完成后检查VPN是否连接，ping测试两端内网是否正常。

5.3 VPN 建立后您的数据中心或局域网无法访问弹性云服务器?

我们提供的安全组默认不允许任何源访问，请确认您的安全组是否配置允许对端的子网地址访问。

5.4 VPN 连接建立后，弹性云服务器无法访问您的数据中心或局域网?

需要确认是否已做好VPN公网IP到您的数据中心或局域网公网IP的防火墙策略，云上出口未做策略限制。

5.5 VPN 支持将两个 VPC 互连吗?

如果两个VPC位于同一区域内，可以使用VPC对等连接互连。

如果两个VPC位于不同区域，可以通过VPN连接，分别把这两个VPC的CIDR作为本端子网和远端子网。

5.6 VPN 本端子网和远端子网数量有什么限制?

VPN本端子网和远端子网数量乘积最大支持到225的规模。

5.7 为什么 VPN 创建成功后状态显示未连接?

VPN对接成功后两端的服务器或者虚拟机之间需要进行通信，VPN的状态才会刷新为正常。

- IKE v1版本：

  如果VPN连接经历了一段无流量的空闲时间，则需要重新协商。协商时间取决于IPsec Policy策略中的“生命周期（秒）”取值。“生命周期（秒）”取值一般为3600（1小时），会在第54分钟时重新发起协商。若协商成功，则保持则保持连接状态至下一轮协商。若协商失败，则在1小时内将状态设置为未连接，需要VPN两端重新进行通信才能恢复为连接状态。可以使用网络监控工具（例如 IP SLA）生成保持连接的Ping信号来避免这种情况发生。

- IKE v2版本：如果VPN连接经历了一段无流量的空闲时间，VPN保持连接状态。

5.8 VPN 配置下发后，多久能够生效?

VPN配置生效的时间与VPN配置中的本端子网数和对端子网数的乘积呈线性增长关系。

5.9 如何配置 VPN 对端设备？（HUAWEI USG6600 配置示例）

因为隧道的对称性，在云上的VPN参数和您的VPN中需要进行相同的配置，否则会导致VPN无法建立连接。

在您自己数据中心的路由器或者防火墙上需要进行IPsec VPN隧道配置，具体配置方法取决于您使用的网络设备，请查询对应设备厂商的指导书。

本文以Huawei USG6600系列V100R001C30SPC300版本的防火墙的配置过程为例进行说明，供参考。

假设数据中心的子网为192.168.3.0/24和192.168.4.0/24，VPC下的子网为192.168.1.0/24和192.168.2.0/24 ，VPC上IPsec隧道的出口公网IP为XXX.XXX.XX.XX（从VPC上IPsec VPN的本端网关参数上获取）。

操作步骤

1. 登录防火墙设备的命令行配置界面。
2. 查看防火墙版本信息。
   ```
   display version
   17:20:502017/03/09
   Huawei Versatile Security Platform Software
   Software Version: USG6600 V100R001C30SPC300(VRP (R) Software，Version 5.30)
   ```
3. 创建ACL并绑定到对应的vpn-instance。
   ```
   acl number 3065 vpn-instance vpn64
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   q
   ```
4. 创建ike proposal。
   ```
   ike proposal 64
   dh group5
   authentication-algorithm sha1
   integrity-algorithm hmac-sha2-256
   sa duration 3600
   q
   ```
5. 创建ike peer，并引用之前创建的ike proposal，其中对端IP地址是x.x.x.x。
   ```
   ike peer vpnikepeer_64
   pre-shared-key ******** （ ********为您输入的预共享密码 ）
   ike-proposal 64
   undo version 2
   remote-address vpn-instance vpn64 x.x.x.x
   sa binding vpn-instance vpn64
   q
   ```
6. 创建IPsec协议。
   ```
   ipsec proposal ipsecpro64
   encapsulation-mode tunnel
   esp authentication-algorithm sha1
   q
   ```
7. 创建IPsec策略，并引用ike policy和ipsec proposal。
   ```
   ipsec policy vpnipsec64 1 isakmp
   security acl 3065
   pfs dh-group5
   ike-peer vpnikepeer_64
   proposal ipsecpro64
   local-address xx.xx.xx.xx
   q
   ```
8. 将IPsec策略应用到相应的子接口上去。
   ```
   interface GigabitEthernet0/0/2.64
   ipsec policy vpnipsec64
   q
   ```
9. 测试连通性。

   在上述配置完成后，我们可以利用您在云中的主机和您数据中心的主机进行连通性测试，如下图所示：


```
root@i-psiybqhh:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:7c:ba:bf:cc
          inet addr:192.168.3.2  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:7cff:feba:bfcc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2304 (2.3 KB)  TX bytes:3404 (3.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1296 (1.2 KB)  TX bytes:1296 (1.2 KB)

root@i-psiybqhh:/home/ubuntu# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=62 time=4.55 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=62 time=1.27 ms
64 bytes from 192.168.1.2: icmp_req=3 ttl=62 time=1.25 ms
64 bytes from 192.168.1.2: icmp_req=4 ttl=62 time=0.871 ms
64 bytes from 192.168.1.2: icmp_req=5 ttl=62 time=0.886 ms
64 bytes from 192.168.1.2: icmp_req=6 ttl=62 time=0.676 ms
64 bytes from 192.168.1.2: icmp_req=7 ttl=62 time=1.06 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.676/1.510/4.554/1.258 ms
```

5.10 对端 VPN 设备支持列表?

满足IPsec VPN标准和协议的设备，大部分都可以对接VPN。例如：Cisco ASA防火墙、华为USG6系列防火墙、USG9系列防火墙、山石网科防火墙、Cisco ISR路由器等。对于华为USG6系列防火墙、USG9系列防火墙具体设备列表如**表5-1**所示。

表 5-1 华为 VPN 设备列表

对端支持列表	说明
HUAWEI USG6系列	USG6320/6310/6510-SJJ USG6306/6308/6330/6350/6360/6370/6380/6390/6507/6530/6550/6570：2048 USG6620/6630/6650/6660/6670/6680
HUAWEI USG9系列	USG9520/USG9560/USG9580

其他满足**VPN参考标准和协议**的设备，也在支持列表中，但是可能会因为设备对协议的实现方式不一致，导致接入失败。如果发现不能建立连接，请参考**如何解决VPN连接无法建立连接问题?**，进行基本检查或联系技术支持人员。

5.11 VPN 连接无法连接或网速慢如何排查?

排查方法如下：

1. 查看云主机规格，云上VPN的入口流量不限速，与云主机规格有关。
2. 云上VPN的出口流量限速，查看用户的带宽是否已经达到或者超出上限。

3. 排查用户的本地网络，查看是否为用户侧数据中心网络速度的影响。
4. 排查云上与用户侧数据中心是否存在丢包现象。

5.12 虚拟专用网络是否支持 SSL VPN?

目前虚拟专用网络不支持SSL VPN。

A 修订记录

发布日期	修改说明
2020-08-30	第一次正式发布。