

虚拟专用网络

用户指南

文档版本 01
发布日期 2024-11-14



版权所有 © 华为技术有限公司 2024。保留一切权利。

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

商标声明



HUAWEI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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

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 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

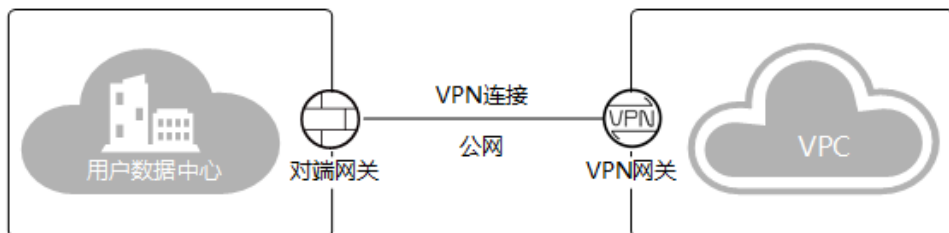
VPN仅支持建立非跨境连接，不支持建立跨境连接。

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。

VPN组网图如[图 VPN组网图](#)所示。

图 1-1 VPN 组网图



组成部分

- **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。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。

- **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。

1.2 产品优势

企业版虚拟专用网络具有以下几大产品优势:

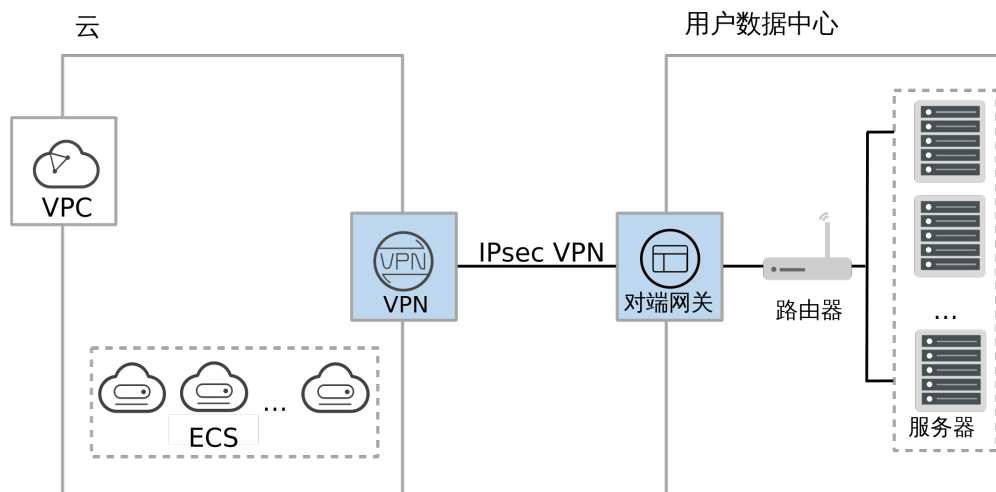
- **更安全**
 - 基于IKE/IPsec对传输数据加密, 保证用户数据传输安全。
 - VPN支持为每个用户创建独立的VPN网关, 提供租户网关隔离防护能力。
 - 支持AES国际、SM国密等加密算法, 满足多种安全要求。
- **高可用**
 - 双连接: 网关提供两个接入地址, 支持一个对端网关创建两条相互独立的VPN连接, 一条连接中断后流量可快速切换到另一条连接。
 - 双活网关: 双活网关部署在不同的AZ区域, 实现AZ级高可用保障。
 - 主备模式: 正常情况下, VPN网关和对端网关通过主连接进行通信; 当主连接发生故障时, VPN连接会自动切换到备连接; 故障恢复后, VPN连接会自动切回到主连接。
- **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。
- **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。
 - 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。

1.3 应用场景

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。

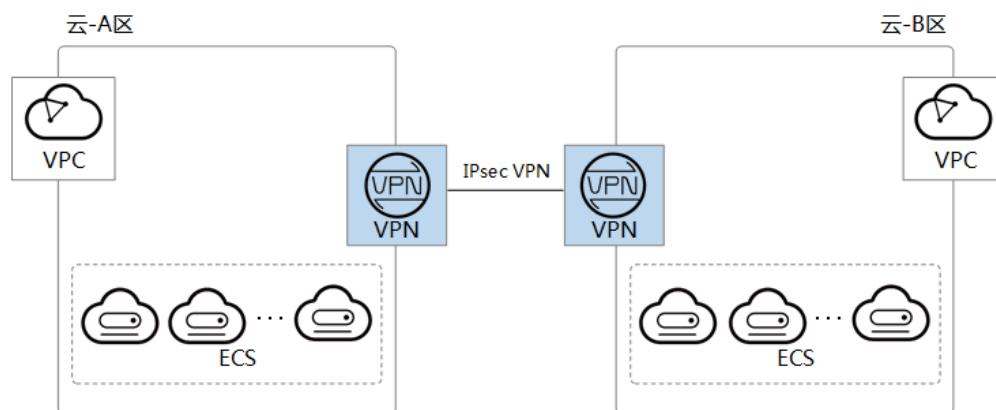
图 1-2 混合云部署



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1-3所示。

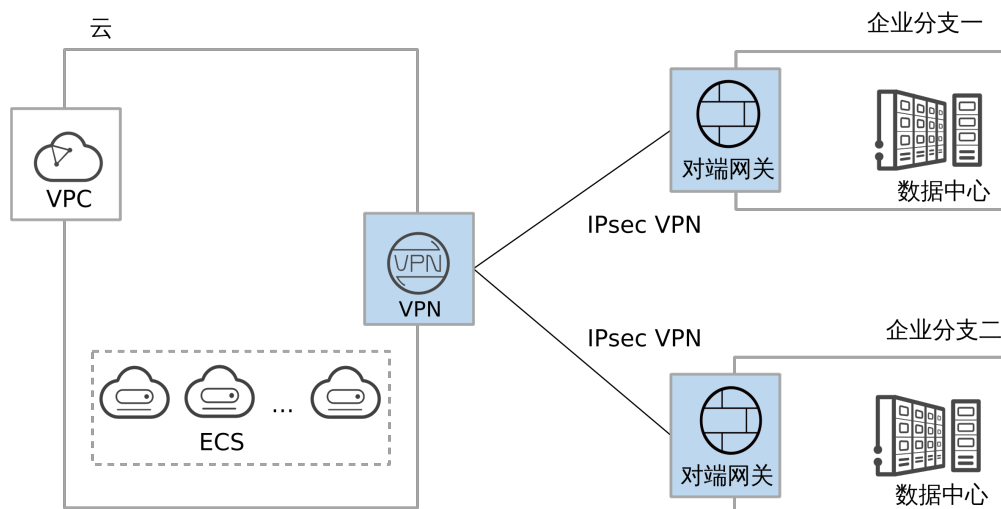
图 1-3 跨地域 VPC 互联



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 1-4 多企业分支互联



1.4 产品规格

说明

- 专业型1、专业型2网关规格，支持相互变更。

表 1-1 VPN 产品规格

对比项	专业型1	专业型2	国密型
独享网关资源	支持	支持	支持
双连接	支持	支持	支持
双活网关	支持	支持	支持
主备网关	支持	支持	支持
策略模式	支持	支持	支持
路由模式-静态路由	支持	支持	支持
路由模式-BGP路由	支持	支持	支持
策略模板模式	不支持	不支持	不支持
最大转发带宽	300Mbps	1Gbps	500Mbps
最大VPN连接组数	100个	100个	100个
接入私网地址	支持	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。

1.5 约束与限制

VPN 网关限制

表 1-2 VPN 网关限制

VPN网关类型	资源	默认限制
企业版VPN	每租户在每区域支持创建的VPN网关数量	50 <ul style="list-style-type: none"> 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。
	每VPN网关支持配置的VPN连接组数量	100
	每VPN网关支持配置的本地子网数量	50
	每VPN网关支持通过每连接接收对端网关发布的BGP路由数量	100

- 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 1-3 对端网关限制

VPN网关类型	资源	默认限制
企业版VPN	每租户在每区域支持创建的对端网关数量	100

- 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 1-4 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	

- 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，最大提供300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。
 当所有涉及该网关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。

1.6 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)

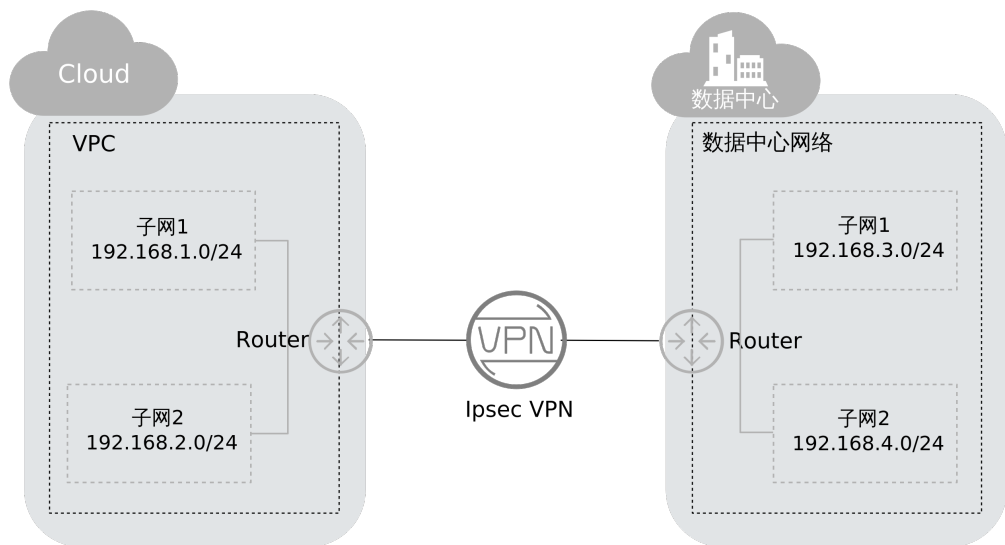
1.7 基本概念

1.7.1 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1-5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 1-5 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。

1.7.2 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。

1.7.3 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。

1.7.4 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。

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。

1.7.5 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 $\leq 10\text{Mbit/s}$ ，则入云方向统一限定为10Mbit/s。
- 如果所购带宽 $> 10\text{Mbit/s}$ ，则入云方向与所购买的带宽一致。

1.7.6 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）。

1.7.7 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。

1.7.8 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。

1.7.9 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：

[6.1.5 建立IPsec VPN连接需要账户名和密码吗？](#)

2 入门

2.1 通过企业版实现数据中心和 VPC 互通

2.1.1 入门指引

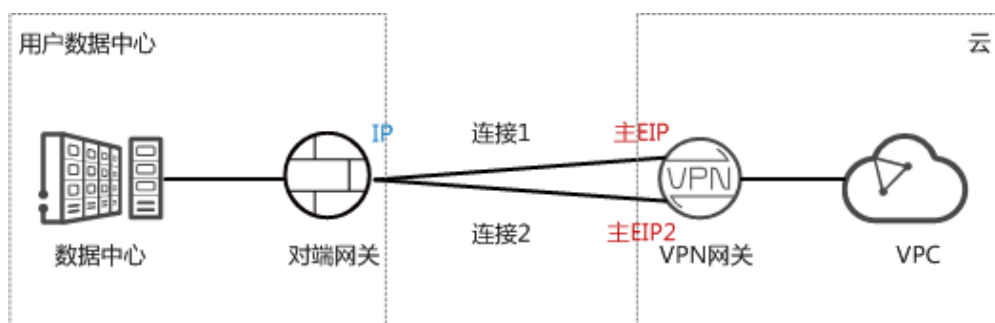
以管理控制台实际上线区域为准。

场景描述

由于业务发展，企业A需要将数据中心和VPC的数据进行互通。此时企业A可以通过VPN服务创建数据中心和VPC的连接，实现云上和云下数据互通。

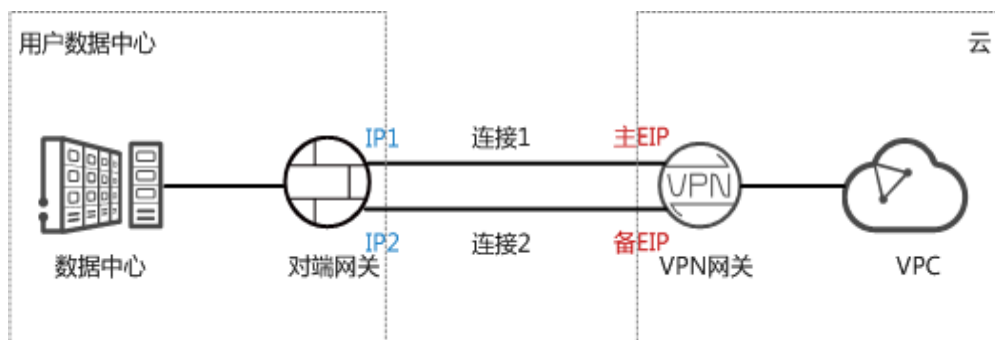
- 如果用户数据中心仅有一个对端网关，且对端网关只能配置一个IP地址，推荐VPN网关使用双活模式，组网如图2-1所示。
双活模式下，如果连接1链路故障，流量自动切换至连接2进行传输，企业业务不受影响；连接1恢复正常后，VPN仍使用连接2进行数据交互。

图 2-1 双活模式



- 如果用户数据中心存在两个对端网关，或一个对端网关可以配置两个IP地址，推荐VPN网关使用主备模式，组网如图2-2所示。
主备模式下，连接1和连接2互为主备，主链路为连接1，备链路为连接2。默认情况下流量仅通过主链路进行传输，如果主链路故障，流量自动切换至备链路进行传输，企业业务不受影响；主链路恢复正常后，VPN回切至主链路进行数据交互。

图 2-2 主备模式



约束与限制

- 对端网关需要支持标准IKE和IPsec协议。
- 本地数据中心和VPC间互通的子网需要没有重叠，且数据中心待互通的子网中不能包含100.64.0.0/10和214.0.0.0/8。
如果VPC使用DC/CC服务和其他VPC互通，则本地数据中心的子网也不能和其他VPC包含的子网存在重叠。

数据规划

表 2-1 规划数据

类别	规划项	规划值
VPC	待互通子网	192.168.0.0/16
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： <ul style="list-style-type: none"> • 主EIP：11.xx.xx.11 • 主EIP2：11.xx.xx.12
VPN连接	Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 <ul style="list-style-type: none"> • VPN连接1：169.254.70.1/30 • VPN连接2：169.254.71.1/30
数据中心	待互通子网	172.16.0.0/16
对端网关	网关IP地址	网关IP地址由运营商统一分配。本示例假设网关IP地址如下： 22.xx.xx.22

类别	规划项	规划值
	Tunnel接口地址	<ul style="list-style-type: none"> VPN连接1: 169.254.70.2/30 VPN连接2: 169.254.71.2/30

操作流程

通过VPN实现数据中心和VPC互通的操作流程如图2-3所示。

图 2-3 操作流程

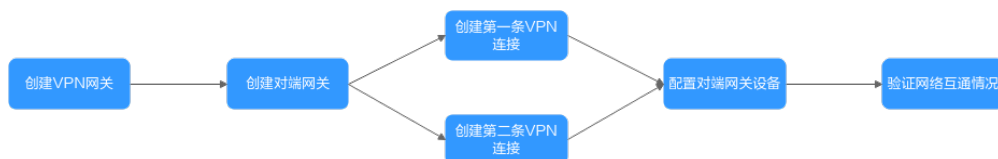


表 2-2 操作流程说明

序号	步骤	说明
1	2.1.2 步骤一：创建VPN网关	VPN网关需要绑定两个EIP作为出口公网IP。如果您已经购买EIP，则此处可以直接绑定使用。
2	2.1.3 步骤二：创建对端网关	添加数据中心的VPN设备为对端网关。
3	2.1.4 步骤三：创建第一条VPN连接	VPN网关的主EIP和对端网关组建第一条VPN连接。
4	2.1.5 步骤四：创建第二条VPN连接	VPN网关的主EIP2和对端网关组建第二条VPN连接。第二条VPN连接的路由模式、预共享密钥、IKE/IPsec策略建议和第一条VPN连接配置保持一致。
5	2.1.6 步骤五：配置对端网关设备	<ul style="list-style-type: none"> 对端网关配置的本端隧道接口地址/对端隧道接口地址需要和VPN连接配置互为镜像配置。 对端网关配置的路由模式、预共享密钥、IKE/IPsec策略需要和VPN连接配置保持一致。
6	2.1.7 步骤六：验证网络互通情况	登录ECS，执行ping命令，验证网络互通情况。

2.1.2 步骤一：创建 VPN 网关


前提条件

- 虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见《虚拟私有云用户指南》。

- 虚拟私有云VPC中ECS的安全组规则已经配置，并确保安全组规则允许数据中心的对端网关可以访问VPC资源。如何配置安全组规则，请参见《虚拟私有云用户指南》。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击图标，选择“网络 > 虚拟专用网络VPN”。

步骤3 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤4 根据界面提示配置参数，单击立即创建并完成支付。

步骤5 本示例仅对关键参数进行说明。

表 2-3 VPN 网关关键参数说明

参数	说明	参数取值
区域	选择靠近您所在地域的区域。	-
名称	输入VPN网关的名称。	vpngw-001
网络类型	<ul style="list-style-type: none"> • 公网：VPN网关通过Internet网络和用户数据中心的对端网关进行通信。 • 私网：VPN网关通过私有网络和用户数据中心的对端网关进行通信。 	公网
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择需要和数据中心互通的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	配置VPC待和数据中心互通的子网。支持“输入网段”和“选择子网”两种方式。	192.168.0.0/24
规格	选择“专业型1”。	专业型1
HA模式	选择“双活”。	双活
主EIP	支持“现在创建”和“使用已有”两种方式。	11.xx.xx.11
主EIP2		11.xx.xx.12

---结束

结果验证

在“VPN网关”页面生成新创建的VPN网关信息，初始状态为“创建中”；当VPN网关状态变为“正常”，表示VPN网关创建完成。

2.1.3 步骤二：创建对端网关

操作步骤

步骤1 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。

步骤2 在“对端网关”界面，单击“创建对端网关”。

步骤3 根据界面提示配置参数，单击“确定”。

本示例仅对关键参数进行说明。

表 2-4 对端网关参数说明

参数	说明	参数取值
名称	输入对端网关的名称。	cgw-001
标识	输入对端网关的IP。	IP Address, 22.xx.xx.22。

----结束

结果验证

在“对端网关”页面生成新创建的对端网关信息。

2.1.4 步骤三：创建第一条 VPN 连接

操作步骤

步骤1 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。

步骤2 在“VPN连接”页面，单击“创建VPN连接”。

步骤3 根据界面提示配置第一条VPN连接参数，单击“提交”。

本示例仅对关键参数进行说明。

表 2-5 第一条 VPN 连接参数说明

参数	说明	参数取值
名称	输入VPN连接的名称。	vpn-001
VPN网关	选择 2.1.2 步骤一：创建VPN网关 创建的VPN网关。	vpngw-001
网关IP	选择VPN网关的 主EIP 。	11.xx.xx.11
对端网关	选择 2.1.3 步骤二：创建对端网关 创建的对端网关。	cgw-001
连接模式	选择“静态路由模式”。	静态路由模式

参数	说明	参数取值
对端子网	<p>输入数据中心待和VPC互通的子网。</p> <p>说明</p> <ul style="list-style-type: none"> 对端子网可以和本端子网重叠，但不能重合。 对端子网不能被VPN网关关联的VPC内已有子网所包含；不能作为被VPN网关关联的VPC自定义路由表的目的地址。 对端子网不能是VPC的预留网段，例如100.64.0.0/10、214.0.0.0/8。 如果互联子网关联了ACL规则，则需要确保ACL规则中已放通所有本端子网到对端子网的TCP协议端口。 VPN不支持对端设备配置策略的源和目的子网时使用地址组配置。 	172.16.0.0/16
接口分配方式	支持“手动分配”和“自动分配”两种方式。	手动分配
本端隧道接口地址	<p>配置在VPN网关上的tunnel接口地址。</p> <p>说明</p> <p>对端网关需要对此处的本端隧道接口地址/对端隧道接口地址做镜像配置。</p>	169.254.70.2/30
对端隧道接口地址	配置在用户侧设备上的tunnel接口地址。	169.254.70.1/30
检测机制	<p>用于多链路场景下路由可靠性检测。</p> <p>说明</p> <p>功能开启前，请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则会导致VPN流量不通。</p>	勾选“使能NQA”
预共享密钥、确认密钥	<p>VPN连接协商密钥。</p> <p>VPN连接和对端网关配置的预共享密钥需要一致。</p>	Test@123
策略配置	<p>包含IKE策略和IPsec策略，用于指定VPN隧道加密算法。</p> <p>VPN连接和对端网关配置的策略信息需要一致。</p>	默认配置

----结束

结果验证

在“VPN连接”页面生成新创建的VPN连接信息，初始状态为“创建中”；由于此时对端网关尚未配置，无法建立有效的连接，所以大约2分钟后，VPN连接状态会变成“未连接”。

2.1.5 步骤四：创建第二条 VPN 连接

操作步骤

步骤1 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。

步骤2 在“VPN连接”页面，单击“创建VPN连接”。

和第一条VPN连接相比，除了名称、网关IP、本端隧道接口地址和对端隧道接口地址不同，其他配置建议保持一致。

表 2-6 第二条 VPN 连接参数说明

参数	说明	参数取值
名称	输入VPN连接的名称。	vpn-002
VPN网关	选择 2.1.2 步骤一：创建VPN网关 创建的VPN网关。	vpngw-001
网关IP	选择VPN网关的 主EIP2 。	11.xx.xx.12
对端网关	选择 2.1.3 步骤二：创建对端网关 创建的对端网关。	cgw-001
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	输入数据中心待和VPC互通的子网。 说明 <ul style="list-style-type: none"> 对端子网可以和本端子网重叠，但不能重合。 对端子网不能被VPN网关关联的VPC内已有子网所包含；不能作为被VPN网关关联的VPC自定义路由表的目的地址。 对端子网不能是VPC的预留网段，例如100.64.0.0/10、214.0.0.0/8。 如果互联网网关关联了ACL规则，则需要确保ACL规则中已放通所有本端子网到对端子网的TCP协议端口。 VPN不支持对端设备配置策略的源和目的子网时使用地址组配置。 	172.16.0.0/16
接口分配方式	支持“手动分配”和“自动分配”两种方式。	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。 说明 对端网关需要对此处的本端隧道接口地址/对端隧道接口地址做镜像配置。	169.254.71.2/30
对端隧道接口地址	配置在用户侧设备上的tunnel接口地址。	169.254.71.1/30

参数	说明	参数取值
检测机制	用于多链路场景下路由可靠性检测。 说明 功能开启前，请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则会导致VPN流量不通。	勾选“使能NQA”
预共享密钥、确认密钥	VPN连接协商密钥。 VPN连接和对端网关配置的预共享密钥需要一致。	Test@123
策略配置	包含IKE策略和IPsec策略，用于指定VPN隧道加密算法。 VPN连接和对端网关配置的策略信息需要一致。	默认配置

----结束

结果验证

在“VPN连接”页面生成新创建的VPN连接信息，初始状态为“创建中”；由于此时对端网关尚未配置，无法建立有效的连接，所以大约2分钟后，VPN连接状态会变成“未连接”。

2.1.6 步骤五：配置对端网关设备

操作步骤

说明

本示例对端网关以AR路由器为例。

步骤1 登录AR路由器配置界面。

步骤2 进入系统视图。

```
<AR651>system-view
```

步骤3 配置公网接口的IP地址。本示例假设AR路由器GigabitEthernet 0/0/8为公网接口。

```
[AR651]interface GigabitEthernet 0/0/8
[AR651-GigabitEthernet0/0/8]ip address 22.xx.xx.22 255.255.255.0
[AR651-GigabitEthernet0/0/8]quit
```

步骤4 配置默认路由。

```
[AR651]ip route-static 0.0.0.0 0.0.0.0 22.xx.xx.1
```

其中，22.xx.xx.1为AR路由器公网IP的网关地址，请根据实际替换。

步骤5 开启SHA-2算法兼容RFC标准算法功能。

```
[AR651]IPsec authentication sha2 compatible enable
```

步骤6 配置IPsec安全提议。

```
[AR651]IPsec proposal hwproposal1
[AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
[AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
[AR651-IPsec-proposal-hwproposal1]quit
```

步骤7 配置IKE安全提议。

```
[AR651]ike proposal 2
[AR651-ike-proposal-2]encryption-algorithm aes-128
[AR651-ike-proposal-2]dh group14
[AR651-ike-proposal-2]authentication-algorithm sha2-256
[AR651-ike-proposal-2]authentication-method pre-share
[AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
[AR651-ike-proposal-2]prf hmac-sha2-256
[AR651-ike-proposal-2]quit
```

步骤8 配置IKE对等体。

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]undo version 1
[AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer1]ike-proposal 2
[AR651-ike-peer-hwpeer1]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer1]remote-address 11.xx.xx.11
[AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer1]rsa signature-padding pss
[AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer1]quit
[AR651]ike peer hwpeer2
[AR651-ike-peer-hwpeer2]undo version 1
[AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer2]ike-proposal 2
[AR651-ike-peer-hwpeer2]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer2]remote-address 11.xx.xx.12
[AR651-ike-peer-hwpeer2]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer2]rsa signature-padding pss
[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer2]quit
```

相关命令说明如下：

- pre-shared-key cipher：预共享密钥，需要和VPN连接配置的预共享密钥保持一致。
- local-address：AR路由器的公网地址。
- remote-address：VPN网关的主EIP/主EIP2。

步骤9 配置IPsec安全框架。

```
[AR651]IPsec profile hwpro1
[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1
[AR651-IPsec-profile-hwpro1]proposal hwproposal1
[AR651-IPsec-profile-hwpro1]pfs dh-group14
[AR651-IPsec-profile-hwpro1]quit
[AR651]IPsec profile hwpro2
[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2
[AR651-IPsec-profile-hwpro2]proposal hwproposal1
[AR651-IPsec-profile-hwpro2]pfs dh-group14
[AR651-IPsec-profile-hwpro2]quit
```

步骤10 配置虚拟隧道接口。

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 22.xx.xx.22
[AR651-Tunnel0/0/1]destination 11.xx.xx.11
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 22.xx.xx.22
[AR651-Tunnel0/0/2]destination 11.xx.xx.12
```

```
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

相关命令说明如下：

- interface Tunnel0/0/1、interface Tunnel0/0/2：两条VPN连接对应的Tunnel隧道。
本示例中，Tunnel0/0/1对应VPN网关主EIP所在的VPN连接；Tunnel0/0/2对应VPN网关主EIP2所在的VPN连接。
- ip address：AR路由器的Tunnel接口地址。
- source：AR路由器的公网地址。
- destination：VPN网关的主EIP/主EIP2。

步骤11 配置NQA。

```
[AR651]nqa test-instance IPsec_nqa1 IPsec_nqa1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]test-type icmp
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit
```

相关命令说明如下：

- nqa test-instance IPsec_nqa1 IPsec_nqa1、nqa test-instance IPsec_nqa2 IPsec_nqa2：NQA名称。
本示例中，IPsec_nqa1对应VPN网关主EIP所在的VPN连接；IPsec_nqa2对应VPN网关主EIP2所在的VPN连接。
- destination-address：VPN网关的Tunnel接口地址。
- source-address：AR路由器的Tunnel接口地址。

步骤12 配置静态路由联动NQA功能。

```
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 track nqa IPsec_nqa2 IPsec_nqa2
```


相关参数说明如下：

- 192.168.0.0：VPC的本端子网。
- 同一条命令中，Tunnelx和IPsec_nqax需要同属于一条VPN连接。

----结束

结果验证

步骤1 登录管理控制台。

步骤2 在页面左上角单击图标，选择“网络 > 虚拟专用网络VPN”。

步骤3 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。


此时可以看到两条VPN连接状态均变为“正常”。

----结束

2.1.7 步骤六：验证网络互通情况

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击  图标，选择区域和项目。

步骤3 单击“服务列表”，选择“计算 > 弹性云服务器”。

步骤4 登录弹性云服务器。

本示例是通过管理控制台远程登录（VNC方式），具体请参见。

步骤5 在弹性云服务器的远程登录窗口，执行以下命令，验证网络互通情况。

```
ping 172.16.0.100
```

其中，172.16.0.100为数据中心服务器的IP地址，请根据实际替换。

回显如下信息，表示网络已通。

```
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245  
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245  
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245  
来自 xx.xx.xx.xx 的回复: 字节=32 时间=27ms TTL=245
```

----结束

2.2 通过站点入云 VPN 经典版实现数据中心和 VPC 互通

2.2.1 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。

前置条件

- 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见《虚拟私有云用户指南》。
- 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见《虚拟私有云用户指南》。

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 > 经典版-VPN网关”。
如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
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网关参数请参见[表 VPN网关参数说明](#)

表 2-7 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
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。	10

表 2-8 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。支持以下方式设置本端子网： <ul style="list-style-type: none"> • 选择子网，表示用户数据中心或者私有网络与您选择的子网进行互通。 • 手动输入网段，表示用户数据中心或者私有网络与您配置的网段之间进行互通。 	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。	192.168.3.0/24, 192.168.4.0/24
预共享密钥	配置在VPC的VPN和您的数据中心的VPN中，配置需要一致。 取值范围： <ul style="list-style-type: none"> 取值长度：6~128个字符。 只能包括以下几种字符： <ul style="list-style-type: none"> 数字 大小写字母 特殊符号：包括“~”、“\`”、“!”、“@”、“#”、“\$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“[”、“]”、“{”、“}”、“ ”、“\”、“;”、“:”、“/”、“.”和“;” 	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	<ul style="list-style-type: none"> 默认配置。 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见表IKE策略和表IPsec策略。 	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： <ul style="list-style-type: none"> MD5（此算法安全性较低，请慎用） SHA1（此算法安全性较低，请慎用） SHA2-256 SHA2-384 SHA2-512 默认配置为：SHA2-256。	SHA2-256

参数	说明	取值样例
加密算法	<p>加密算法，支持的算法：</p> <ul style="list-style-type: none"> • AES-128 • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） <p>默认配置为：AES-128。</p>	AES-128
DH算法	<p>Diffie-Hellman密钥交换算法，支持的算法：</p> <ul style="list-style-type: none"> • Group 1（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 5（此算法安全性较低，请慎用） • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 <p>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。</p>	Group 14
版本	<p>IKE密钥交换协议版本，支持的版本：</p> <ul style="list-style-type: none"> • v1（有安全风险不推荐） • v2 <p>默认配置为：v2。</p>	v2
生命周期（秒）	<p>安全联盟（SA—Security Association）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。</p>	86400

表 2-10 IPsec 策略

参数	说明	取值样例
认证算法	<p>认证哈希算法，支持的算法：</p> <ul style="list-style-type: none"> • SHA1（此算法安全性较低，请慎用） • MD5（此算法安全性较低，请慎用） • SHA2-256 • SHA2-384 • SHA2-512 <p>默认配置为：SHA2-256。</p>	SHA2-256
加密算法	<p>加密算法，支持的算法：</p> <ul style="list-style-type: none"> • AES-128 • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） <p>默认配置为：AES-128。</p>	AES-128
PFS	<p>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。</p> <p>PFS组支持的算法：</p> <ul style="list-style-type: none"> • 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 <p>默认配置为：DH group 14。</p>	DH group 14
传输协议	<p>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：</p> <ul style="list-style-type: none"> • ESP • AH • AH-ESP <p>默认配置为：ESP。</p>	ESP

参数	说明	取值样例
生命周期 (秒)	安全联盟 (SA—Security Association) 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”。

2.2.2 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 > 经典版-VPN连接”。
如果所在region已同步上线企业版VPN, 请选择“虚拟专用网络 > 经典版”。
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连接参数请参见[表 VPN连接参数说明](#)。

表 2-11 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: <ul style="list-style-type: none"> • 选择子网, 表示用户数据中心或者私有网络与您选择的子网进行互通。 • 手动输入网段, 表示用户数据中心或者私有网络与您配置的网段之间进行互通。 	192.168.1.0/24 , 192.168.2.0/24

参数	说明	取值样例
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。	192.168.3.0/24 , 192.168.4.0/24
预共享密钥	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： <ul style="list-style-type: none"> • 取值长度：6~128个字符。 • 只能包括以下几种字符： <ul style="list-style-type: none"> - 数字 - 大小写字母 - 特殊符号：包括“~”、“\`”、“!”、“@”、“#”、“\$”、“%”、“^”、“(”、“)”、“_”、“ ”、“+”、“=”、“[”、“]”、“{”、“}”、“ ”、“\”、“;”、“.”、“/”、“:”和“,” 	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	<ul style="list-style-type: none"> • 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。相关配置说明请参见表 IKE策略和表 IPsec策略。 	自定义配置

表 2-12 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： <ul style="list-style-type: none"> • MD5（此算法安全性较低，请慎用） • SHA1（此算法安全性较低，请慎用） • SHA2-256 • SHA2-384 • SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： <ul style="list-style-type: none"> • AES-128 • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
DH算法	<ul style="list-style-type: none"> • Group 1（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 5（此算法安全性较低，请慎用） • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 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： <ul style="list-style-type: none"> • v1（有安全风险不推荐） • v2 默认配置为：v2。	v2

参数	说明	取值样例
生命周期 (秒)	安全联盟 (SA—Security Association) 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
协商模式	默认配置为: Main。	Main

表 2-13 IPsec 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: <ul style="list-style-type: none"> • SHA1 (此算法安全性较低, 请慎用) • MD5 (此算法安全性较低, 请慎用) • SHA2-256 • SHA2-384 • SHA2-512 默认配置为: SHA2-256。	SHA2-256
加密算法	加密算法, 支持的算法: <ul style="list-style-type: none"> • AES-128 • AES-192 • AES-256 • 3DES (此算法安全性较低, 请慎用) 默认配置为: AES-128。	AES-128

参数	说明	取值样例
PFS	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>默认配置为: DH group 14。</p>	DH group 14
传输协议	<p>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:</p> <ul style="list-style-type: none"> • AH • ESP • AH-ESP <p>默认配置为: ESP。</p>	ESP
生命周期 (秒)	<p>安全联盟 (SA—Security Association) 的生存时间, 单位: 秒。</p> <p>在超过生存时间后, 安全联盟将被重新协商。</p> <p>默认配置为: 3600。</p>	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. 因为隧道的对称性, 还需要在您自己数据中心的路由器或者防火墙上进行IPsec VPN隧道配置。

3 管理

3.1 企业版 VPN 网关管理

3.1.1 创建 VPN 网关

场景描述

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，创建VPN连接之前，需要创建VPN网关。

背景信息

根据对端网关IP地址个数不同，推荐的组网如表3-1所示。

表 3-1 组网关系

对端网关 IP个数	推荐组网	说明
1		VPN网关推荐使用双活模式，该场景占用1个VPN连接组配额。
2		VPN网关推荐使用主备模式，该场景占用2个VPN连接组配额。

- 如果用户数据中心仅有一个对端网关，且对端网关只能配置一个IP地址，VPN网关推荐使用双活模式，主EIP、主EIP2各创建一条VPN连接，对接同一个对端网关的同一个IP地址。该场景下仅占用一个VPN连接组配额。

- 如果用户数据中心存在两个对端网关，或一个对端网关可以配置两个IP地址，VPN网关推荐使用主备模式，主EIP、备EIP各创建一条VPN连接，对接到对端网关的不同IP地址。该场景下占用两个VPN连接组配额。

约束与限制


- 非国密型网关不支持变更为国密型网关。


前提条件

- 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见《虚拟私有云用户指南》。
- 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见《虚拟私有云用户指南》。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击  图标，选择区域和项目。

步骤3 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“创建VPN网关”。

步骤6 根据界面提示配置参数，单击“下一步”。

VPN网关参数请参见[表3-2](#)。

表 3-2 VPN 网关参数说明

参数	说明	取值样例
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	请根据实际需要进行选择
名称	VPN网关的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	vpngw-001
网络类型	<ul style="list-style-type: none"> ● 公网：VPN网关通过公网建立VPN连接。 ● 私网：VPN网关通过私网建立VPN连接。 	公网
关联模式	<ul style="list-style-type: none"> ● 虚拟私有云 通过VPC向对端网关或本端子网内服务器发送通信消息。 	虚拟私有云
虚拟私有云	选择虚拟私有云VPC信息。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.66.0/24

参数	说明	取值样例
本端子网	配置VPC与对端网关对应数据中心互通的子网。 <ul style="list-style-type: none"> 选择子网 选择本VPC子网信息。 输入网段 可以输入本VPC下的子网信息；也可以输入与本VPC建立了对等网络的VPC子网信息。 	192.168.1.0/24,192.168.2.0/24
BGP ASN	VPN网关会根据输入值创建相应的ASN，VPN网关和对端网关的BGP ASN需要不同。	64512
HA模式	<ul style="list-style-type: none"> 双活 <ul style="list-style-type: none"> 关联模式选择“虚拟私有云”时，对端子网和哪个EIP先创建VPN连接1，则VPN网关到该对端子网的出云流量优先走VPN连接1。VPN连接1故障失效后，出云流量会自动切换到该对端子网的另一条VPN连接2；故障失效的VPN连接1恢复后，出云流量会仍然通过VPN连接2，不会切回到VPN连接1。 主备 VPN网关到该对端子网的出云流量优先走该对端子网和主EIP建立的VPN连接1。VPN连接1失效后，出云流量自动切换到该对端子网和备EIP建立的VPN连接2；故障失效的VPN连接1恢复后，出云流量会自动切回到VPN连接1。 	双活
规格	支持专业型1、专业型2、国密型三种类型。	专业型1
带宽名称	EIP对应带宽对象的名称。	Vpngw-bandwidth2
主EIP	用于VPN网关和对端网关进行网络连接。 <ul style="list-style-type: none"> 现在创建：创建新EIP。 使用已有：使用已有EIP，支持与其他网络服务的EIP共享带宽。 	现在创建
带宽大小	EIP对应带宽大小，单位：Mbit/s。 <ul style="list-style-type: none"> 所有使用该EIP创建的VPN连接均会分摊占用该EIP的带宽大小，所有VPN连接的带宽总和不能超过该EIP的带宽大小。当网络流量超过EIP的带宽大小时，有可能造成网络拥塞导致VPN连接中断，请提前做好带宽规划。 支持在云监控中配置告警规则对带宽进行监控。 支持用户在允许的带宽范围内自定义带宽大小。 	10 Mbit/s

参数	说明	取值样例
主EIP2	一个VPN网关需要绑定一组弹性公网IP（即主EIP、主EIP2），每个公网IP可以独立规划带宽，也可以与其他网络服务的EIP共享带宽。	现在创建
备EIP	一个VPN网关需要绑定一组弹性公网IP（即主/备EIP），每个公网IP可以独立规划带宽，也可以与其他网络服务的EIP共享带宽。	现在创建
企业项目	创建VPN时，可以将VPN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。	default
接入虚拟私有云	<ul style="list-style-type: none"> “关联模式”采用“虚拟私有云”、“网络类型”为“私网”时需要配置。 当VPN网关的南北向需要连接不同的虚拟私有云时，设置北向的虚拟私有云为该接入虚拟私有云。VPN网关关联的虚拟私有云为南向业务虚拟私有云。	选择“与网关关联的虚拟私有云一致”
接入子网	<ul style="list-style-type: none"> “关联模式”采用“虚拟私有云”、“网络类型”为“私网”时需要配置。 缺省情况下，VPN网关从关联的虚拟私有云的互联网子网接入。当VPN网关需要从指定子网接入时设置。	选择“与互联网子网一致”

步骤7 确认创建的VPN网关信息，单击“提交”。

步骤8 （可选）对于国密型网关，创建后需要上传VPN网关证书，否则VPN连接将无法建立。

上传VPN网关证书的相关操作请参见[上传VPN网关证书](#)。



----结束

3.1.2 查看已创建的 VPN 网关

场景描述

用户创建VPN网关后，可以查看已创建的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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。



5. 在“VPN网关”页面，查看VPN网关列表信息。
6. 单击VPN网关的名称，查看VPN网关详情。
 - 公网类型网关：可查看基本信息和弹性公网IP。
 - 私网类型网关：可查看基本信息和高级配置。
 - 国密型网关：可查看基本信息和证书信息。


3.1.3 修改已创建的 VPN 网关

场景描述

您可以对VPN网关基本信息进行修改，包括名称、本端子网。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择目标VPN网关所在行，单击操作列的“修改基本信息”。

若仅需修改VPN网关的名称，您也可以直接单击VPN网关名称右侧的  按钮进行修改。

6. 根据界面提示，修改VPN网关的名称、本端子网。
7. 单击“确定”。

VPN网关参数修改请参见[VPN网关参数修改说明](#)。

表 3-3 VPN 网关参数修改说明

参数	说明	是否支持修改
名称	VPN网关的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	支持
本端子网	VPC与对端网关对应数据中心互通的子网。	支持
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	不支持
规格	支持专业型1、专业型2、国密型三种类型。	部分支持，以管理控制台界面为准
关联模式	选择“虚拟私有云”。	不支持



参数	说明	是否支持修改
虚拟私有云	选择需要和用户数据中心通信的VPC。	不支持
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	不支持
BGP ASN	BGP自治系统号码。	不支持
可用区	<p>可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。</p> <ul style="list-style-type: none"> 当存在两个及以上可用区时，必须选择两个可用区。部署在两个可用区的VPN网关具备更高的可用性。建议您根据VPC内资源所在的可用区选择网关的可用区。 当仅存在一个可用区时，可选择此可用区创建VPN网关。 	不支持

3.1.4 绑定弹性公网 IP

场景描述

用户根据需要为已创建的VPN网关绑定EIP。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择目标VPN网关所在行，单击操作列的“绑定EIP”。
 - 如果VPN网关是双活模式，VPN网关支持绑定主EIP/主EIP2。
 - 如果VPN网关是主备模式，VPN网关支持绑定主/备EIP。
6. 根据界面提示，选择需要绑定的EIP，单击“确定”。

3.1.5 解绑弹性公网 IP



场景描述

用户创建VPN网关后，可以解绑已关联的弹性公网IP。

约束与限制

已创建VPN连接的EIP不支持解绑操作。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击  图标，选择区域和项目。
3. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择目标VPN网关所在行，单击操作列的“解绑EIP”，也可以单击操作列的“更多 > 解绑EIP”。
 - 如果VPN网关是双活模式，VPN网关支持解绑主EIP/主EIP2，请根据实际需要进行解绑配置。
 - 如果VPN网关是主备模式，VPN网关支持解绑主/备EIP，请根据实际需要进行解绑配置。
6. 单击“是”。

说明

- 当共享带宽冻结时，EIP的行为以EIP资料为准。请参见。

3.1.6 删除 VPN 网关



场景描述

当无需使用VPN网关时，可以删除VPN网关。

约束与限制

- 在VPN网关状态处于“创建中”、“更新中”、“删除中”三种状态时，不能进行VPN网关删除操作。
- 如果VPN网关绑定了加入共享带宽的EIP，删除VPN网关时会同步释放EIP，保留共享带宽。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

5. 在需要删除的VPN网关所在行，选择操作列的“更多 > 删除”。
6. 单击“是”。

说明



当共享带宽冻结时，EIP的行为以EIP资料为准。请参见。

3.1.7 上传 VPN 网关证书

场景描述

国密型VPN网关，需要上传证书，用于和对端网关建立VPN连接；首次使用国密型网关，用户需要在云监控页面配置云监报告警，详细步骤请参见《云监控服务用户指南》。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在需要上传证书的国密型VPN网关所在行，选择“更多 > 查看/上传证书”。
6. 单击“上传证书”，根据界面提示填写相关信息。

VPN网关证书参数请参见表3-4。

表 3-4 VPN 网关证书参数说明

参数	说明	取值样例
证书名称	用户自定义。	certificate-001
签名证书	<p>签名证书用于对数据进行签名认证，以保证数据的有效性和不可否认性。</p> <p>以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。</p> <p>签名证书需要同时上传签发此签名证书的CA证书。</p>	<pre>-----BEGIN CERTIFICATE----- 签名证书 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- CA证书 -----END CERTIFICATE-----</pre>
签名私钥	<p>签名私钥用于对签名证书加密过的数据进行解密，签名私钥是非公开的，由用户自行保管。</p> <p>以文本编辑器（如Notepad++）打开签名私钥KEY格式的文件，将私钥复制到此处。</p>	<pre>-----BEGIN EC PRIVATE KEY----- 签名私钥 -----END EC PRIVATE KEY-----</pre>

参数	说明	取值样例
加密证书	加密证书用于对VPN连接的传输数据进行加密，以保证数据的保密性和完整性。签发该加密证书的CA机构需和签发签名证书的CA机构保持一致。 以文本编辑器（如Notepad+）打开加密证书PEM格式的文件，将证书内容复制到此处。	-----BEGIN CERTIFICATE----- <i>加密证书</i> -----END CERTIFICATE-----
加密私钥	加密私钥用于对加密证书加密过的数据进行解密，加密私钥是非公开的，由用户自行保管。 以文本编辑器（如Notepad+）打开加密私钥KEY格式的文件，将私钥内容复制到此处。	-----BEGIN EC PRIVATE KEY----- <i>加密私钥</i> -----END EC PRIVATE KEY-----



3.1.8 更换 VPN 网关证书

场景描述

国密型VPN网关证书到期或失效后，需要更换VPN网关证书。

更换VPN网关证书，对端网关需要使用新的配套CA证书与VPN网关进行重协商，否则连接中断。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在需要上传证书的国密型VPN网关所在行，选择“更多 > 查看/上传证书”。
6. 单击“更换”，根据界面提示填写相关信息。

VPN网关证书参数请参见表3-5。

表 3-5 VPN 网关证书参数说明

参数	说明	取值样例
证书名称	不支持修改。	与原证书名称保持一致。

参数	说明	取值样例
新签名证书	<p>签名证书用于对数据进行签名认证，以保证数据的有效性和不可否认性。</p> <p>以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。</p> <p>签名证书需要同时上传签发此签名证书的CA证书。</p>	<pre>-----BEGIN CERTIFICATE----- 签名证书 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- CA证书 -----END CERTIFICATE-----</pre>
新签名私钥	<p>签名私钥用于对签名证书加密过的数据进行解密，签名私钥是非公开的，由用户自行保管。</p> <p>以文本方式打开签名私钥KEY格式的文件，将私钥复制到此处。</p>	<pre>-----BEGIN EC PRIVATE KEY----- 签名私钥 -----END EC PRIVATE KEY-----</pre>
新加密证书	<p>加密证书用于对VPN连接的传输数据进行加密，以保证数据的保密性和完整性。签发该加密证书的CA机构需和签发签名证书的CA机构保持一致。</p> <p>以文本编辑器（如Notepad++）打开加密证书PEM格式的文件，将证书内容复制到此处。</p>	<pre>-----BEGIN CERTIFICATE----- 加密证书 -----END CERTIFICATE-----</pre>
新加密私钥	<p>加密私钥用于对加密证书加密过的数据进行解密，加密私钥是非公开的，由用户自行保管。</p> <p>以文本编辑器（如Notepad++）打开加密私钥KEY格式的文件，将私钥内容复制到此处。</p>	<pre>-----BEGIN EC PRIVATE KEY----- 加密私钥 -----END EC PRIVATE KEY-----</pre>

- 勾选“我已知晓上述内容，确认更换证书”，单击“确定”。

3.2 企业版对端网关管理

3.2.1 创建对端网关

场景描述

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，创建VPN连接之前，需要创建对端网关。

约束与限制

- 国密型对端网关标识仅支持网关IP，且该网关IP地址值必须是静态地址。
- FQDN类型标识的对端网关只支持策略模板模式对接。
- VPN不支持对端设备配置策略的源和目的子网时使用地址组配置。
- 策略模板模式只支持ikev2。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
 4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
 5. 在“对端网关”界面，单击“创建对端网关”。
 6. 根据界面提示配置参数，单击“立即创建”。
- 对端网关参数请参见表3-6。

表 3-6 对端网关参数说明

参数	说明	取值样例
名称	对端网关的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	cgw-001
路由模式	对端网关的网络路由模式。 <ul style="list-style-type: none"> • VPN连接模式使用BGP路由模式时，请选择“动态BGP”。 <ul style="list-style-type: none"> - 配置BGP路由模式前，请确认对端网关支持动态BGP功能。 - 该场景下对端网关最大支持发布100条BGP路由给VPN网关，否则会导致BGP邻居断连，进而导致VPN网关和对端网关之间的流量不通。 • VPN连接模式使用静态路由模式时，请选择“静态路由”。 • VPN连接模式使用策略模式时，建议选择“静态路由”。 	静态路由
BGP ASN	仅“路由模式”选择“动态BGP”时需要配置。 请输入用户数据中心或私有网络的ASN。 对端网关的BGP ASN与VPN网关的BGP ASN不能相同。	65000

参数	说明	取值样例
网关IP	对端网关和VPN网关通信的IP地址，该网关IP地址值必须是静态地址。 请确认数据中心或私有网络中的防火墙规则已经放通UDP端口4500。	1.2.3.4
CA证书（可选）	使用国密型网关时，需要上传对端网关的CA证书，用于和VPN网关建立VPN连接。 <ul style="list-style-type: none"> 上传证书：手动输入，以“-----BEGIN CERTIFICATE-----”作为开头，以“-----END CERTIFICATE-----”作为结尾。 使用已上传证书：查看并勾选已上传证书，请注意证书到期时间。 	-----BEGIN CERTIFICATE- ----- CA证书 -----END CERTIFICATE- -----

- （可选）如果存在两个对端网关，请参见上述步骤添加另一个网关标识对应的对端网关。

相关操作



因为隧道的对称性，还需要在您数据中心的路由器或者防火墙上进行IPsec VPN隧道配置。

3.2.2 查看已创建的对端网关

场景描述

用户创建对端网关后，可以查看已创建的对端网关。

操作步骤

- 登录管理控制台。
- 在管理控制台左上角单击  图标，选择区域和项目。
- 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
- 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
- 在“对端网关”界面，查看对端网关列表信息。
- 单击对端网关名称，查看对端网关详情页面。
 - 基础信息：可查看对端网关的名称、ID、路由模式、BGP ASN、网关接入IP、VPN连接。
 - CA证书：可查看证书序列号、签名算法、到期时间、颁发者、使用者，可添加或更换CA证书（对端网关为国密型时，需要添加CA证书）。




3.2.3 修改已创建的对端网关

场景描述

用户创建对端网关后，可以修改已创建的对端网关名称，国密型对端网关同时支持添加或更换CA证书。

添加或更换CA证书相关操作请参见[3.2.5 上传对端网关证书](#)和[3.2.6 更换对端网关证书](#)。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，选择目标对端网关所在行，单击  。
6. 修改对端网关名称，单击“确定”。

对端网关参数修改请参见[对端网关参数修改说明](#)。

表 3-7 对端网关参数修改说明

参数	说明	是否支持修改
名称	VPN连接的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	支持
BGP ASN	BGP自治系统号码。	不支持
网关IP	对端网关和VPN网关通信的IP地址，该网关IP地址值必须是静态地址。	不支持

3.2.4 删除对端网关



场景描述

用户根据实际需要删除已创建的对端网关。

约束与限制

若对端网关已被VPN连接关联，则无法直接删除该对端网关，需要先将该对端网关在VPN连接中移除。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，选择目标对端网关所在行，单击操作列的“删除”。



6. 确定要删除的对端网关信息，单击“是”。

3.2.5 上传对端网关证书

场景描述

国密型对端网关，需要上传对端网关的CA证书，用于和VPN网关建立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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，单击目标对端网关名称进入详情页面。
6. 在“CA证书”区域，单击“添加”。
7. 根据界面提示填写相关信息，单击“确定”。

对端网关CA证书参数请参见表3-8。

表 3-8 对端网关 CA 证书参数说明

参数	说明	取值样例
上传证书	对端网关的CA证书。	-----BEGIN CERTIFICATE----- <i>CA证书</i> -----END CERTIFICATE-----
使用已上传证书	查看并勾选已上传证书，请注意证书到期时间。	-

3.2.6 更换对端网关证书

场景描述

国密型网关CA证书到期或失效后，需要更换CA证书。

更换CA证书后，该对端网关需要使用新CA签发的国密证书与VPN网关重协商，否则连接断开。

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. 在页面左上角单击图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，单击目标对端网关名称进入详情页面。
6. 在“CA证书”区域，单击“更换”。
7. 根据界面提示填写相关信息。
对端网关CA证书参数请参见表3-9。

表 3-9 对端网关 CA 证书参数说明

参数	说明	取值样例
上传证书	对端网关的CA证书。	-----BEGIN CERTIFICATE----- <i>CA证书</i> -----END CERTIFICATE-----
使用已上传证书	查看并勾选已上传证书，请注意证书到期时间。	-

8. 勾选“我已知晓上述内容，确认更换CA证书”，单击“确定”。

3.3 企业版 VPN 连接管理

3.3.1 创建 VPN 连接

场景描述

如果您需要将VPC中的弹性云服务器和数据中心或私有网络连通，创建VPN网关、对端网关之后，需要继续创建VPN连接。

约束与限制

- 使用静态路由模式创建VPN连接时，使能NQA前请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则可能导致流量不通。

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. 在页面左上角单击图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”页面，单击“创建VPN连接”。

 说明

VPN网关的两个EIP支持分别和对端网关创建一条VPN连接。VPN双连接可以很大程度提升云上云下连接的可靠性，强烈建议配置。

6. 根据界面提示配置参数，单击“立即创建”。

VPN连接参数请参见表3-10。

表 3-10 VPN 连接参数说明

参数	说明	取值样例
名称	VPN连接的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	vpn-001
VPN网关	选择待关联的VPN网关名称。 您也可以单击“创建VPN网关”进行新建，相关参数解释请参见表3-2。 如果您使用国密型VPN网关，且VPN网关没有绑定相关证书，请先单击右侧“上传证书”完成上传证书操作，否则VPN连接将无法建立。	vpngw-001
网关IP	选择VPN网关IP。 VPN网关对接同一对端网关时，不能选择已使用过的地址。	可选的网关IP
对端网关	选择对端网关信息。 您也可以单击“创建对端网关”进行新建，相关参数解释请参见表3-6。 如果您使用国密型网关，且对端网关没有绑定CA证书，请先参见3.2.5 上传对端网关证书上传CA证书，否则VPN连接将无法建立。 说明 如果一个对端网关同时对接多个VPN网关，则VPN网关的BGP ASN和连接模式需要相同。	cgw-001

参数	说明	取值样例
连接模式	<p>IPsec连接的模式，支持路由模式和策略模式。</p> <ul style="list-style-type: none"> 静态路由模式。 根据路由配置（本端子网与对端子网）确定哪些数据进入IPsec VPN隧道。 适用场景：对端网关之间要求互通。 BGP路由模式。 根据BGP动态路由确定哪些数据进入IPsec VPN隧道。 适用场景：对端网关之间要求互通、互通子网数量多或变化频繁、与专线互备等组网场景。 策略模式。 根据策略规则（用户侧到VPC之间通信的数据流信息）确定哪些数据进入IPsec VPN隧道，支持以源网段和目的网段定义策略规则。 适用场景：对端网关之间要求隔离。 	静态路由模式
对端子网	<p>指需要通过VPN连接访问云上VPC的用户侧子网。</p> <p>若存在多个对端子网，请用半角逗号（,）隔开。</p> <p>说明</p> <ul style="list-style-type: none"> 对端子网可以和本端子网重叠，但不能重合。 对端子网不能被VPN网关关联的VPC内已有子网所包含；不能作为被VPN网关关联的VPC自定义路由表的目的地址。 对端子网不能是VPC的预留网段，例如100.64.0.0/10、214.0.0.0/8。 如果互联网网关关联了ACL规则，则需要确保ACL规则中已放通所有本端子网到对端子网的TCP协议端口。 VPN不支持对端设备配置策略的源和目的子网时使用地址组配置。 	172.16.1.0/24,172.16.2.0/24

参数	说明	取值样例
接口分配方式	<p>仅“连接模式”采用“静态路由模式”和“BGP路由模式”时需要配置。</p> <p>说明</p> <ul style="list-style-type: none"> • 接口地址为VPN网关和对端网关通信的tunnel隧道IP地址。 • 如果对端网关的tunnel接口地址固定不可更改，请使用“手动分配”模式，并根据对端网关的tunnel接口地址设置VPN网关的tunnel接口地址。 • 手动分配。 <ul style="list-style-type: none"> - 仅支持在169.254.x.x/30网段（除169.254.195.x/30）范围内，配置VPN网关本端接口地址的tunnel接口地址；对端网关对端接口地址的tunnel接口地址会根据本端接口地址随机生成。 例如：本端接口地址配置为169.254.1.6/30，则对端接口地址自动配置为169.254.1.5/30。 - 当“连接模式”采用“BGP路由模式”的场景下，选择“手动分配”的方式配置隧道接口地址时，对端设备VPN连接的隧道接口地址需要与本端隧道地址配置成镜像地址。 • 自动分配。 <ul style="list-style-type: none"> - VPN网关默认使用169.254.x.x/30网段对tunnel接口分配地址。 - 自动分配的本端接口地址/对端接口地址，可以在VPN连接页面，单击“修改连接信息”进行查看。 - 当“连接模式”采用“BGP路由模式”的场景下，选择“自动分配”的方式，在创建连接后，可查看分配的本端隧道接口地址和对端隧道接口地址，对端设备VPN连接的隧道接口地址需要与本端隧道地址配置成镜像地址。 	自动分配
本端隧道接口地址	<p>仅“接口分配方式”采用“手动分配”时需要配置。</p> <p>配置在VPN网关上的tunnel接口地址。</p>	-

参数	说明	取值样例
对端隧道接口地址	<p>仅“接口分配方式”采用“手动分配”时需要配置。</p> <p>配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。</p>	-
检测机制	<p>仅“连接模式”采用“静态路由模式”时需要配置。</p> <p>说明 功能开启前，请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则可能导致流量不通。 功能开启后，VPN网关会自动对对端接口地址进行NQA探测。</p>	勾选
预共享密钥	<p>VPN网关和对端网关的预共享密钥需要保持一致。</p> <p>取值范围：</p> <ul style="list-style-type: none"> ● 取值长度：8~128个字符。 ● 只能包括以下几种字符，且必须包含三种及以上类型： <ul style="list-style-type: none"> - 数字。 - 大写字母。 - 小写字母。 - 特殊符号：包括“~”、“!”、“@”、“#”、“\$”、“%”、“^”、“(”、“)”、“_”、“”、“+”、“=”、“{”、“}”、“”、“.”、“/”、“.”和“;”。 <p>说明 国密型VPN连接无此参数。</p>	Test@123
确认密钥	<p>再次输入预共享密钥。</p> <p>说明 国密型VPN连接无此参数。</p>	Test@123

参数	说明	取值样例
策略规则	<p>仅“连接模式”采用“策略模式”时需要配置。</p> <p>用于定义本端子网到对端子网之间具体进入VPN连接加密隧道的数据流信息，由源网段与目的网段来定义。系统默认支持配置5条策略规则。</p> <ul style="list-style-type: none"> 源网段。 源网段必须包含部分本端子网。其中，0.0.0.0/0表示任意地址。 目的网段。 目的网段必须完全包含对端子网。一个策略规则最大支持5个目的网段，目的网段之间使用英文逗号(,)进行分隔。 	<ul style="list-style-type: none"> 源网段1: 192.168.1.0/24 目的网段1: 172.16.1.0/24,172.16.2.0/24 源网段2: 192.168.2.0/24 目的网段2: 172.16.1.0/24,172.16.2.0/24
策略配置	<ul style="list-style-type: none"> 默认配置。 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见表3-11和表3-12。 	自定义配置

表 3-11 IKE 策略

参数	说明	取值样例
版本	<p>IKE密钥交换协议版本，支持的版本：</p> <ul style="list-style-type: none"> v1 (v1版本安全性较低，如果用户设备支持v2版本，建议选择v2) 建立国密型VPN连接，IKE密钥交换协议版本只能为“v1”。 v2。 <p>国密型VPN连接默认配置为：v1。 非国密型VPN连接默认配置为：v2。</p>	v2
协商模式	<p>仅“版本”采用“v1”时需要配置。</p> <ul style="list-style-type: none"> Main。 当使用国密型VPN网关创建VPN连接时，“协商模式”仅支持“Main”。 Aggressive。 	Main

参数	说明	取值样例
认证算法	<p>认证哈希算法，支持的算法：</p> <ul style="list-style-type: none"> • SHA1（此算法安全性较低，请慎用）。 • MD5（此算法安全性较低，请慎用）。 • SHA2-256。 • SHA2-384。 • SHA2-512。 • SM3。 <p>仅国密型VPN连接选择该认证算法，此时IKE密钥交换协议版本只能为“v1”。</p> <p>国密型VPN连接默认配置为：SM3。</p> <p>非国密型VPN连接默认配置为：SHA2-256。</p>	SHA2-256
加密算法	<p>加密算法，支持的算法：</p> <ul style="list-style-type: none"> • 3DES（此算法安全性较低，请慎用）。 • AES-128（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-256（此算法安全性较低，请慎用）。 • AES-128-GCM-16。 • AES-256-GCM-16。 <p>选择该加密算法时，IKE密钥交换协议版本只能为“v2”。</p> <ul style="list-style-type: none"> • SM4。 <p>仅国密型VPN连接选择该加密算法，此时IKE密钥交换协议版本只能为“v1”。</p> <p>国密型VPN连接默认配置为：SM4。</p> <p>非国密型VPN连接默认配置为：AES-128。</p>	AES-128

参数	说明	取值样例
DH算法	<p>支持的算法：</p> <ul style="list-style-type: none"> • Group 1（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 5（此算法安全性较低，请慎用）。 • Group 14（此算法安全性较低，请慎用）。 • Group 15。 • Group 16。 • Group 19。 • Group 20。 • Group 21。 <p>默认配置为：Group 15。</p> <p>说明 国密型VPN连接无此参数。</p>	Group 15
生命周期（秒）	<p>安全联盟（Security Association, SA）的生存时间。</p> <p>在超过生存时间后，安全联盟将被重新协商。</p> <ul style="list-style-type: none"> • 单位：秒。 • 取值范围：60~604800。 • 默认配置为：86400。 	86400
本端标识	<p>IPsec连接协商时，VPN网关的鉴权标识。对端网关配置的对端标识需与此处配置的本端标识保持一致，否则协商失败。</p> <ul style="list-style-type: none"> • IP Address（默认）。 系统自动读取VPN网关的EIP作为IP Address，无需用户手动配置。 • FQDN。 全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、?，区分大小写。 <p>说明 国密型VPN连接无此参数。</p>	IP Address

参数	说明	取值样例
对端标识	<p>IPsec连接协商时，对端网关的鉴权标识。在VPN网关配置的对端标识需与对端网关的本端标识保持一致，否则协商失败。</p> <ul style="list-style-type: none"> IP Address（默认）。系统自动读取对端网关的网关IP作为IP Address，无需用户手动配置。 FQDN。全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、?，区分大小写。 <p>说明 国密型VPN连接无此参数。</p>	IP Address

表 3-12 IPsec 策略

参数	说明	取值样例
认证算法	<p>认证哈希算法，支持的算法：</p> <ul style="list-style-type: none"> SHA1（此算法安全性较低，请慎用）。 MD5（此算法安全性较低，请慎用）。 SHA2-256。 SHA2-384。 SHA2-512。 SM3。 <p>仅国密型VPN连接选择该认证算法。 国密型VPN连接默认配置为：SM3。 非国密型VPN连接默认配置为：SHA2-256。</p>	SHA2-256

参数	说明	取值样例
加密算法	<p>加密算法，支持的算法：</p> <ul style="list-style-type: none"> ● 3DES（此算法安全性较低，请慎用）。 ● AES-128（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-256（此算法安全性较低，请慎用）。 ● AES-128-GCM-16。 ● AES-256-GCM-16。 ● SM4。 仅国密型VPN连接选择该加密算法。 <p>国密型VPN连接默认配置为：SM4。 非国密型VPN连接默认配置为：AES-128。</p>	AES-128

参数	说明	取值样例
PFS	<p>PFS (Perfect Forward Secrecy) 即完美前向安全功能, 配置IPsec隧道协商时使用。</p> <p>PFS组支持的算法:</p> <ul style="list-style-type: none"> • Disable (此算法安全性较低, 请慎用)。 • 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 (此算法安全性较低, 请慎用)。 • DH group 15。 • DH group 16。 • DH group 19。 • DH group 20。 • DH group 21。 <p>默认配置为: DH group 15。</p> <p>说明</p> <ul style="list-style-type: none"> • 国密型VPN连接无此参数。 • 国密型VPN网关和国密型对端网关创建VPN连接时, 需要保证国密型对端网关关闭PFS功能, 否则会导致VPN连接无法建立。 	DH group 15
传输协议	<p>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:</p> <ul style="list-style-type: none"> • ESP。 <p>默认配置为: ESP。</p>	ESP
生命周期 (秒)	<p>安全联盟 (Security Association, SA) 的生存时间。</p> <p>在超过生存时间后, 安全联盟将被重新协商。</p> <ul style="list-style-type: none"> • 单位: 秒。 • 取值范围: 30~604800。 • 默认配置: 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隧道在数据传输阶段所使用的协议、加密以及认证算法。VPC和数据中心的VPN连接在策略配置上需要保持一致，否则会导致VPN协商失败，进而导致VPN连接建立失败。

以下算法安全性较低，请慎用：

- **认证算法：**SHA1、MD5。
- **加密算法：**3DES、AES-128、AES-192、AES-256。

出于部分对端设备不支持安全加密算法的考虑，VPN连接的默认加密算法仍为AES-128。在对端设备功能支持的情况下，建议使用更安全的加密算法。

- **DH算法：**Group 1、Group 2、Group 5、Group 14。

7. 确认VPN连接规格，单击“提交”。

8. 参见上述步骤，创建第二条VPN连接。



VPN连接的IP对应关系，请参见[背景信息](#)。

3.3.2 创建健康检查

场景描述

VPN连接创建完成后，添加健康检查可以配置VPN网关向对端网关发送监测报文，统计链路往返时延和丢包率，用于检测连接的质量。云监控服务提供对VPN连接链路往返时延和丢包率的监控指标，详情请参见[支持的监控指标（企业版VPN）](#)。

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”界面，单击目标VPN连接名称，在“基本信息 > 健康检查”区域单击“添加”。
6. 在“添加健康检查”界面，单击“确定”。

3.3.3 查看已创建的 VPN 连接

场景描述

用户创建VPN连接后，可以查看已创建的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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”界面，查看VPN连接列表信息。

- 单击VPN连接的名称，查看VPN连接基本信息、策略配置和标签。
基本信息包括VPN连接信息、健康检查信息和BGP邻居信息。

说明



- 在VPN连接列表中，选择目标VPN连接所在行，单击“修改策略配置”，查看该VPN连接对应的IKE策略和IPsec策略详情。

3.3.4 修改已创建的 VPN 连接

场景描述

VPN连接是建立VPN网关和外部数据中心对端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

- 登录管理控制台。
- 在管理控制台左上角单击  图标，选择区域和项目。
- 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
- 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
- 在“VPN连接”界面，选择目标VPN连接所在行，单击“修改连接信息”或“修改策略配置”。
- 根据界面提示修改VPN连接的配置参数。
- 单击“确定”。

注意

修改预共享密钥和IKE/IPsec策略场景下，请确保VPN连接和对端网关配置的信息一致，否则会导致VPN连接中断。

不同参数修改后的生效机制不同，如表3-13所示。

表 3-13 生效机制

场景	参数	生效机制	操作方法
-	预共享密钥	<ul style="list-style-type: none"> IKE策略为v1时：修改后下个协商周期生效。 IKE策略为v2时：重建VPN连接后生效。 <p>说明 国密型VPN连接无“预共享密钥”参数。</p>	<ul style="list-style-type: none"> IKE策略为v1时 在需要修改的VPN连接所在行，选择“更多 > 重置密钥”，修改VPN连接的预共享密钥。 IKE策略为v2时 <ol style="list-style-type: none"> 删除当前VPN连接。 重新创建VPN连接。

场景	参数	生效机制	操作方法
IKE策略（版本为v1）	加密算法	修改后下个协商周期生效。 说明 <ul style="list-style-type: none"> 国密型VPN连接不支持修改以下参数：“加密算法”、“认证算法”、“协商模式”。 国密型VPN连接无以下参数：“DH算法”、“本端标识”、“对端标识”。 	在需要修改的VPN连接所在行，单击“修改策略配置”。
	认证算法		
	DH算法		
	协商模式		
	本端标识		
	对端标识		
	生命周期		
版本	修改后立即生效。 说明 国密型VPN连接不支持修改“版本”参数。		
IKE策略（版本为v2）	加密算法	修改后下个协商周期生效。	在需要修改的VPN连接所在行，单击“修改策略配置”。
	认证算法		
	DH算法		
	生命周期		
	版本	修改后立即生效。	
	本端标识	重建VPN连接后生效。	1. 删除当前VPN连接。 2. 重新创建VPN连接。
	对端标识		
IPsec策略	加密算法	修改后下个协商周期生效。 说明 <ul style="list-style-type: none"> 国密型VPN连接不支持修改以下参数：加密算法、认证算法。 国密型VPN连接不包含以下参数：PFS。 	在需要修改的VPN连接所在行，单击“修改策略配置”。
	认证算法		
	PFS		
	生命周期		
	传输协议	暂不支持管理控制台修改。	

VPN连接参数修改请参见[VPN连接参数修改说明](#)。

表 3-14 VPN 连接参数修改说明

参数	说明	是否支持修改
名称	VPN连接的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	支持
对端网关	用于与VPC内的VPN互通。	支持
对端子网	用户数据中心的需要和VPC通信的子网。	支持
策略配置	包括IKE策略和IPsec策略。	支持
预共享密钥	VPN网关和对端网关的预共享密钥需要保持一致。	支持
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	支持
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	支持
VPN网关	已创建的VPN网关。	不支持
网关IP	对端网关和VPN网关通信的IP地址，该网关IP地址值必须是静态地址。 请确认数据中心或私有网络中的防火墙规则已经放通UDP端口4500。	不支持
接口分配方式	本端接口和对端接口地址的分配方式。包括手动分配和自动分配。	不支持



3.3.5 删除 VPN 连接

场景描述

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. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”界面所需删除的VPN连接所在行的操作列，选择“更多 > 删除”。
6. 单击“是”。


3.4 经典版 VPN 网关管理

3.4.1 查看已创建的 VPN 网关


操作场景

用户创建VPN网关后，可以查看已创建的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”。
如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在VPN网关列表中可以查看VPN网关。

3.4.2 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”。
如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“经典版”界面，单击“VPN网关”。
 - 在目标VPN网关所在行的操作列选择“更多 > 修改带宽”。
 - 在目标VPN网关所在行的操作列选择“更多 > 修改基本信息”。
 - 在目标VPN网关所在行的操作列选择“更多 > 修改规格”。
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。

3.4.3 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 > 经典版-VPN网关”。
如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
2. 在“经典版-VPN网关”界面所需删除的VPN网关所在行，选择“更多 > 删除”。
如果所在region已同步上线企业版VPN，在“经典版”界面所需删除的VPN网关所在行，选择“更多 > 删除”。
3. 单击“是”。

3.5 经典版 VPN 连接管理

3.5.1 查看已创建的 VPN 连接

操作场景

用户创建VPN连接后，可以查看已创建的VPN连接。

操作步骤

1. 在左侧导航栏选择“虚拟专用网络 > 经典版-VPN连接”。
如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN连接”页签。
2. 在“VPN连接”页面的VPN列表中，查看VPN连接信息，也可以在VPN连接所在行，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。

3.5.2 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。

注意

修改VPN连接高级配置时，有流量中断风险，请谨慎操作。

修改预共享密钥不会删除当前连接，新的预共享密钥在IKE生命周期到期后重协商时生效。

操作步骤

1. 在左侧导航栏选择“虚拟专用网络 > 经典版-VPN连接”。
如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN连接”页签。

2. 在“VPN连接”界面所需修改的VPN连接所在行，单击“修改”。
3. 根据界面提示配置参数。

说明

VPN网关名称只能由中文、英文字母、数字、下划线、中划线、点组成。

4. 单击“确定”。

3.5.3 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. 在左侧导航栏选择“虚拟专用网络 > 经典版-VPN连接”。
如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN连接”页签。
2. 在“VPN连接”界面所需删除的VPN连接所在行，选择“更多 > 删除”。
3. 单击“是”。

3.6 监控

3.6.1 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服务。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，可以帮助您更好地了解VPN的各项性能指标。

3.6.2 支持的监控指标（企业版VPN）

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 3-15 企业版 VPN 网关支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
gateway_sen d_pkt_rate	出云包 速率	该指标用于统计测量对象 平均每秒出云的数据包数 量。	≥ 0 pps	网关	1分钟
gateway_recv _pkt_rate	入云包 速率	该指标用于统计测量对象 平均每秒入云的数据包数 量。	≥ 0 pps	网关	1分钟
gateway_sen d_rate	出云带 宽	该指标用于统计测量对象 平均每秒出云流量。	0-1G bit/s	网关	1分钟
gateway_recv _rate	入云带 宽	该指标用于统计测量对象 平均每秒入云流量。	0-1G bit/s	网关	1分钟
gateway_sen d_rate_usage	出云带 宽使用 率	该指标用于统计测量对象 出云带宽使用率。	0-10 0%	网关	1分钟
gateway_recv _rate_usage	入云带 宽使用 率	该指标用于统计测量对象 入云带宽使用率。	0-10 0%	网关	1分钟
gateway_con nection_num	连接数	该指标用于统计测量对象 关联VPN连接数。	≥ 0	网关	1分钟

表 3-16 企业版 VPN 连接支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
tunnel_aver age_latency	隧道往返 平均时延	VPN网关与对端网关之 间隧道的往返平均时 延。	0~50 00 ms	VPN 连接	1分钟
tunnel_max_ latency	隧道往返 最大时延	VPN网关与对端网关之 间隧道的往返最大时 延。	0~50 00 ms	VPN 连接	1分钟
tunnel_pack et_loss_rate	隧道丢包 率	VPN网关与对端网关之 间隧道的丢包率。	0~10 0 %	VPN 连接	1分钟
link_averag e_latency	链路往返 平均时延	VPN网关与对端网关之 间链路的往返平均时 延。	0~50 00 ms	VPN 连接	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
link_max_latency	链路往返最大时延	VPN网关与对端网关之间链路的往返最大时延。	0~5000 ms	VPN连接	1分钟
link_packet_loss_rate	链路丢包率	VPN网关与对端网关之间链路的丢包率。	0~100 %	VPN连接	1分钟
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 2: 未知状态	0, 1, 2	VPN连接	1分钟
recv_pkt_rate	接收包速率	平均每秒接收的数据包数量。	≥ 0 pps	VPN连接	1分钟
send_pkt_rate	发送包速率	平均每秒发送的数据包数量。	≥ 0 pps	VPN连接	1分钟
recv_rate	接收速率	平均每秒接收流量。	0~1G bit/s	VPN连接	1分钟
send_rate	发送速率	平均每秒发送流量。	0~1G bit/s	VPN连接	1分钟

维度

key	Value
evpn_connection_id	企业版VPN连接
evpn_sa_id	企业版VPN连接sa
evpn_gateway_id	企业版VPN网关

3.6.3 支持的监控指标（经典版 VPN）

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.VPC

监控指标

表 3-17 经典版 VPN 带宽支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	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 bit/s	带宽或弹性公网IP	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 bit/s	带宽或弹性公网IP	1分钟
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。 出网带宽使用率=出网带宽指标/购买的带宽大小	0-100%	带宽或弹性公网IP	1分钟
downstream_bandwidth_usage	入网带宽使用率	该指标用于统计测量对象入云平台的带宽使用率，以百分比为单位。 入网带宽使用率=入网带宽指标/购买的带宽大小 说明 <ul style="list-style-type: none"> 由于在部分站点对10Mbps以下的配置带宽提供10Mbps的入网带宽上限，此时监控的入网带宽使用率会存在大于100%的情况。 EIP使用时修改带宽大小，带宽使用率的指标同步生效会有5~10min的延时。 	0-100%	带宽或弹性公网IP	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	带宽或弹性公网IP	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	带宽或弹性公网IP	1分钟

表 3-18 经典版 VPN 连接支持的监控指标

指标ID	指标名称	指标含义	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

维度





key	Value
vpn_connection_id	经典版VPN连接

3.6.4 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。支持查看“近1小时”、“近3小时”、“近12小时”、“近24小时”和“近7天”的数据。

查看 VPN 网关监控指标



- 通过虚拟专用网络入口
 - a. 登录管理控制台。
 - b. 在管理控制台左上角单击 ，选择区域和项目。
 - c. 在管理控制台左上角单击 ，选择“网络 > 虚拟专用网络”。
 - d. 选择“虚拟专用网络 > 企业版-VPN网关”。
 - e. 在“网关IP”列下单击网关IP后的 ，查看VPN网关IP状态。
支持查看“近1小时”、“近3小时”、“近12小时”、“近24小时”和自定义时间段的数据。
- 通过云监控服务入口
 - a. 登录管理控制台。
 - b. 在管理控制台左上角单击 ，选择区域和项目。
 - c. 在系统首页，选择“管理与监管 > 云监控服务”。
 - d. 选择“云服务监控 > 虚拟专用网络”。
 - e. 在“企业版VPN网关”页签下，找到对应的VPN网关，单击“操作”列的“查看监控指标”，查看对应的VPN网关状态。
支持查看“近1小时”、“近3小时”、“近12小时”、“近24小时”和“近7天”的数据。

3.6.5 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态，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. 在管理控制台左上角单击 ，选择“管理与监管> 云监控服务”。
4. 选择“云服务监控 > 虚拟专用网络”，单击“创建告警规则”，根据不同告警类型在不同页签下配置告警规则。
 - 对应VPN网关告警，请从下拉选项中选择“站点入云VPN网关”，单击“资源详情”页签。在VPN网关“操作”列，选择“更多 > 创建告警规则”进行配置。
 - 对应VPN连接告警，请从下拉选项中选择“站点入云VPN连接”页签，单击“资源详情”页签。在VPN连接“操作”列，选择“更多 > 创建告警规则”进行配置。
 - 经典版VPN对应VPN连接的告警，请从下拉选项中选择“VPN连接”页签，单击“资源详情”页签。在VPN连接“操作”列，选择“更多 > “创建告警规则”进行配置。
5. 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。

3.7 审计

3.7.1 支持审计的关键操作列表

表 3-19 企业版操作列表

操作名称	资源类型	事件名称
创建用户对端网关	customer-gateway	createCgw
更新用户对端网关	customer-gateway	updateCgw
删除用户对端网关	customer-gateway	deleteCgw

操作名称	资源类型	事件名称
创建虚拟专用网络网关	vpn-gateway	createVgw
更新虚拟专用网络网关	vpn-gateway	updateVgw
删除虚拟专用网络网关	vpn-gateway	deleteVgw
更新VPN网关状态	vpn-gateway	updateResourceState
创建虚拟专用网络连接	vpn-connection	createVpnConnection
更新虚拟专用网络连接	vpn-connection	updateVpnConnection
删除虚拟专用网络连接	vpn-connection	deleteVpnConnection
上传网关证书	vgw-certificate	createVgwCertificate
更换网关证书	vgw-certificate	updateVgwCertificate
创建资源标签	instance	batchCreateResourceTags
删除资源标签	instance	batchDeleteResourceTags
查询用户对端网关列表	customer-gateway	listCgws
查询用户对端网关	customer-gateway	showCgw
查询资源标签	instance	showResourceTags
查询项目标签	instance	listProjectTags
按标签查询资源实例列表	instance	listResourcesByTags
按标签查询资源实例数量	instance	countResourcesByTags
查询VPN网关证书	vpn-gateway	showVpnGatewayCertificate
查询VPN网关	vpn-gateway	showVgw
查询VPN网关可用区	vpn-gateway	listExtendedAvailabilityZones
查询VPN连接列表	vpn-connection	listVpnConnections
查询VPN连接	vpn-connection	showVpnConnection
查询VPN网关列表	vpn-connection	listVgws

操作名称	资源类型	事件名称
查询VPN连接监控	vpn-connection	showConnectionMonitor
查询VPN连接监控列表	vpn-connection	listConnectionMonitors
查询指定租户配额	quota	showQuotasInfo

3.8 权限管理

3.8.1 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，这些账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。

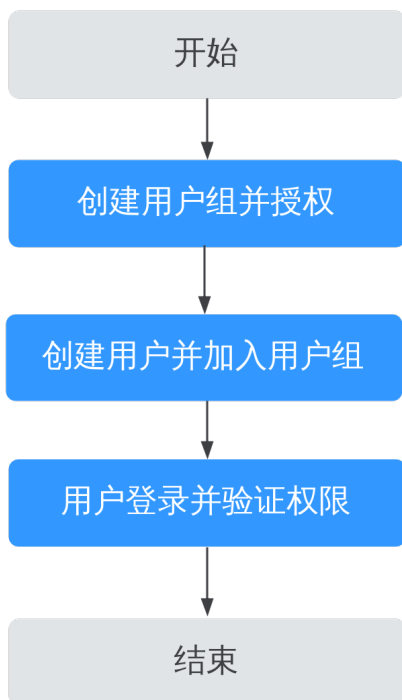
本章节为您介绍对用户授权的方法，操作流程如[图3-1](#)所示。

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。若您需要对除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，并授予虚拟专用网络服务权限“VPN FullAccess”。
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。
新创建的用户登录管理控制台，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 > 企业版-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 FullAccess”已生效。
 - 在“服务列表”中选择“网络 > 虚拟专用网络”，进入“虚拟专用网络 > 经典版”页面，单击“创建VPN网关”，尝试创建VPN网关，如果创建成功，表示“VPN FullAccess”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 FullAccess）的任一服务，若提示权限不足，表示“VPN FullAccess”已生效。

3.8.2 VPN 自定义策略

如果系统预置的VPN权限，不满足您的授权要求，可以创建自定义策略。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：《统一身份认证服务用户指南》的“创建自定义策略”章节。本章为您介绍常用的VPN自定义策略样例。

VPN 自定义策略样例

- 示例1：授权用户删除VPN网关

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpn:vpnGateways:delete"
      ]
    }
  ]
}
```

- 示例2：拒绝用户删除VPN连接

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

如果您给用户授予VPN FullAccess的系统策略，但不希望用户拥有VPN FullAccess中定义的删除VPN连接权限，您可以创建一条拒绝删除VPN连接的自定义策略，然后同时将VPN FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对VPN执行除了删除VPN连接外的所有操作。拒绝策略示例如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "vpn:vpnGateways:delete"
      ]
    }
  ]
}
```

- 示例3：多个授权项策略

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpn:vpnGateways:create",
        "vpn:vpnConnections:create",
        "vpn:customerGateways:create"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "vpn:vpnGateways:delete",
        "vpn:vpnConnections:delete",
        "vpn:customerGateways:create"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "vpc:vpcs:list",

```

```
    "vpc:subnets:get"  
  ]  
}  
]
```

3.9 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。

资源类型

- 经典版VPN的资源类型包括经典版VPN网关和经典版VPN连接。
- 企业版VPN的资源类型包括VPN网关、VPN连接组和对端网关。

资源类型的总配额根据部署Region存在差异，请以实际部署环境为准。

4 最佳实践

4.1 通过 VPN 实现云上云下网络互通（双活模式）

4.1.1 方案概述

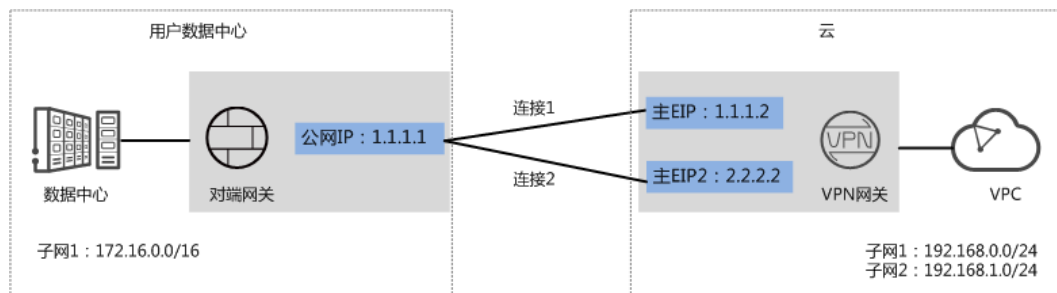
应用场景

当用户数据中心需要和VPC下的ECS资源进行相互访问时，可以通过VPN快速实现云上云下网络互通。

方案架构

本示例中，用户数据中心和VPC之间采用两条VPN连接保证网络可靠性。当其中一条VPN连接故障时，系统可以自动切换到另一条VPN连接，保证网络不中断。

图 4-1 方案架构



方案优势

- 双连接：VPN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：VPN双活网关部署在不同的AZ区域，实现AZ级高可用保障。

约束与限制

- VPN网关的本端子网与对端子网不能相同，即VPC和用户数据中心待互通的子网不能相同。
- VPN网关和对端网关的IKE策略、IPsec策略、预共享密钥需要相同。
- VPN网关和对端网关上配置的本端接口地址和对端接口地址需要互为镜像。
- VPC内弹性云服务器安全组允许访问对端和被对端访问。

4.1.2 组网和资源规划

数据规划

表 4-1 规划数据

类别	规划项	规划值
VPC	待互通子网	<ul style="list-style-type: none"> • 192.168.0.0/24 • 192.168.1.0/24
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： <ul style="list-style-type: none"> • 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
VPN连接	Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 <ul style="list-style-type: none"> • VPN连接1：169.254.70.1/30 • VPN连接2：169.254.71.1/30
用户数据中心	待互通子网	172.16.0.0/16
对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： 1.1.1.1
	Tunnel接口地址	<ul style="list-style-type: none"> • VPN连接1：169.254.70.2/30 • VPN连接2：169.254.71.2/30
IKE/IPsec策略	预共享密钥	Test@123

类别	规划项	规划值
	IKE策略	<ul style="list-style-type: none"> ● 版本: v2 ● 认证算法: SHA2-256 ● 加密算法: AES-128 ● DH算法: Group 15 ● 生命周期 (秒): 86400 ● 本端标识: IP Address ● 对端标识: IP Address
	IPsec策略	<ul style="list-style-type: none"> ● 认证算法: SHA2-256 ● 加密算法: AES-128 ● PFS: DH Group15 ● 传输协议: ESP ● 生命周期 (秒): 3600

4.1.3 操作步骤

前提条件

- 云侧
 - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见《虚拟私有云用户指南》。
 - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见《虚拟私有云用户指南》。
- 数据中心侧
 - 用户数据中心的VPN设备已经完成IPsec连接相关配置。

操作步骤

VPN服务支持静态路由模式、BGP路由模式和策略模式三种连接模式。本示例以静态路由模式进行配置讲解。

步骤1 登录管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建VPN网关”。
2. 根据界面提示配置参数。
VPN网关参数说明如[表4-2](#)所示。

表 4-2 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择用于分配互联网的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	仅关联场景为“虚拟私有云”时需要配置。 - 输入网段 输入需要和用户数据中心通信的子网，该子网可以在关联VPC内，也可以不在关联VPC内。 - 选择子网 选择关联VPC内的子网信息，用于和用户数据中心通信。	192.168.0.0/24, 192.168.1.0/24
BGP ASN	BGP自治系统编号。	64512
HA模式	选择“双活”。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

对端网关参数说明如表4-3所示。

表 4-3 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw
路由模式	选择“静态路由”。	静态路由
网关IP	对端网关和VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	1.1.1.1

步骤5 配置VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置第一条VPN连接参数，单击“提交”。
VPN连接参数说明如表4-4所示。

表 4-4 第一条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-fw
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心的需要和VPC通信的子网。 - 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 - 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	172.16.0.0/16
接口分配方式	- 手动分配 本示例以“手动分配”为例。 - 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.70.2
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认

3. 配置第二条VPN连接参数。

说明

此处仅对和第一条VPN连接配置不同的参数，未提及参数建议和第一条VPN连接配置保持一致。

表 4-5 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2

步骤6 配置对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。

----结束

结果验证

- 大约5分钟后，查看VPN连接状态。
选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
- 用户数据中心内服务器和VPC子网内服务器可以相互Ping通。

4.2 通过 VPN 实现云上云下网络互通（主备模式）

4.2.1 方案概述

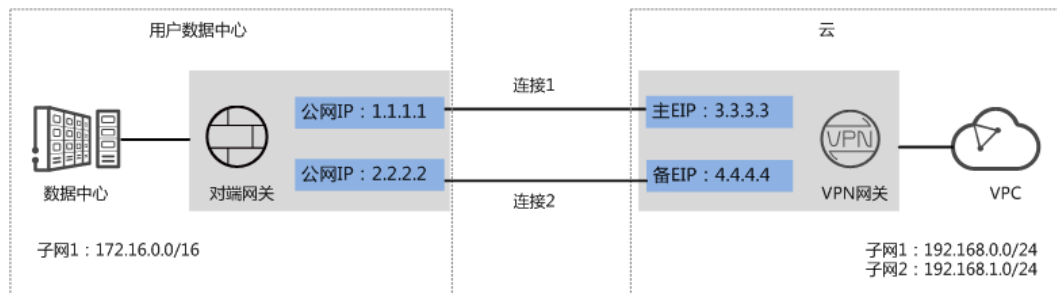
应用场景

当用户数据中心需要和VPC下的ECS资源进行相互访问时，可以通过VPN快速实现云上云下网络互通。

方案架构

本示例中，用户数据中心和VPC之间采用两条VPN连接保证网络可靠性，连接1和连接2互为备用。当其中一条VPN连接故障时，系统可以自动切换到另一条VPN连接，保证网络不中断。

图 4-2 方案架构



方案优势

- 双连接：VPN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。
- 主备网关：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。方便用户确定VPN连接的流量路径，出云流量优先走主EIP。

约束与限制

- VPN网关的本端子网与对端子网不能相同，即VPC和用户数据中心待互通的子网不能相同。
- VPN网关和对端网关的IKE策略、IPsec策略、预共享密钥需要相同。
- VPN网关和对端网关上配置的本端接口地址和对端接口地址需要互为镜像。
- VPC内弹性云服务器安全组允许访问对端和被对端访问。

4.2.2 组网和资源规划

数据规划

表 4-6 规划数据

类别	规划项	规划值
VPC	待互通子网	<ul style="list-style-type: none"> • 192.168.0.0/24 • 192.168.1.0/24
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	主备
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： <ul style="list-style-type: none"> • 主EIP: 3.3.3.3 • 备EIP: 4.4.4.4

类别	规划项	规划值
VPN连接	Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 <ul style="list-style-type: none"> VPN连接1：169.254.70.1/30 VPN连接2：169.254.71.1/30
用户数据中心	待互通子网	172.16.0.0/16
对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： <ul style="list-style-type: none"> 1.1.1.1 2.2.2.2
	Tunnel接口地址	<ul style="list-style-type: none"> VPN连接1：169.254.70.2/30 VPN连接2：169.254.71.2/30
IKE/IPsec策略	预共享密钥	Test@123
	IKE策略	<ul style="list-style-type: none"> 版本：v2 认证算法：SHA2-256 加密算法：AES-128 DH算法：Group 15 生命周期（秒）：86400 本端标识：IP Address 对端标识：IP Address
	IPsec策略	<ul style="list-style-type: none"> 认证算法：SHA2-256 加密算法：AES-128 PFS：DH Group15 传输协议：ESP 生命周期（秒）：3600

4.2.3 操作步骤

前提条件

- 云侧
 - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见《虚拟私有云用户指南》。
 - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见《虚拟私有云用户指南》。
- 数据中心侧
 - 用户数据中心的VPN设备已经完成IPsec连接相关配置。

操作步骤

VPN服务支持静态路由模式、BGP路由模式和策略模式三种连接模式。本示例以静态路由模式进行配置讲解。

步骤1 登录管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建VPN网关”。
2. 根据界面提示配置参数。

VPN网关参数说明如表4-7所示。

表 4-7 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择用于分配互联子网的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	仅关联场景为“虚拟私有云”时需要配置。 - 输入网段 输入需要和用户数据中心通信的子网，该子网可以在关联VPC内，也可以不在关联VPC内。 - 选择子网 选择关联VPC内的子网信息，用于和用户数据中心通信。	192.168.0.0/24, 192.168.1.0/24
BGP ASN	BGP自治系统编号。	64512
HA模式	选择“主备”。	主备
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
备EIP	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

对端网关参数说明如表4-8所示。

表 4-8 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw
路由模式	选择“静态路由”。	静态路由
网关IP	对端网关和VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	1.1.1.1

步骤5 配置VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置第一条VPN连接参数，单击“提交”。

VPN连接参数说明如表4-9所示。

表 4-9 第一条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-fw
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心中需要和VPC通信的子网。 - 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 - 部分网段是VPC预留网段，不能作为对端子网，例如： 100.64.0.0/10, 214.0.0.0/8。	172.16.0.0/16
接口分配方式	- 手动分配 本示例以“手动分配”为例。 - 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.70.2

参数	说明	取值参数
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认

3. 配置第二条VPN连接参数。

说明

此处仅对和第一条VPN连接配置不同的参数，未提及参数建议和第一条VPN连接配置保持一致。

表 4-10 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的备EIP。	2.2.2.2
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2

步骤6 配置对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。

----结束

结果验证

- 大约5分钟后，查看VPN连接状态。
选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
- 用户数据中心内服务器和VPC子网内服务器可以相互Ping通。

4.3 通过 VPN Hub 实现云下多分支网络互通

4.3.1 方案概述

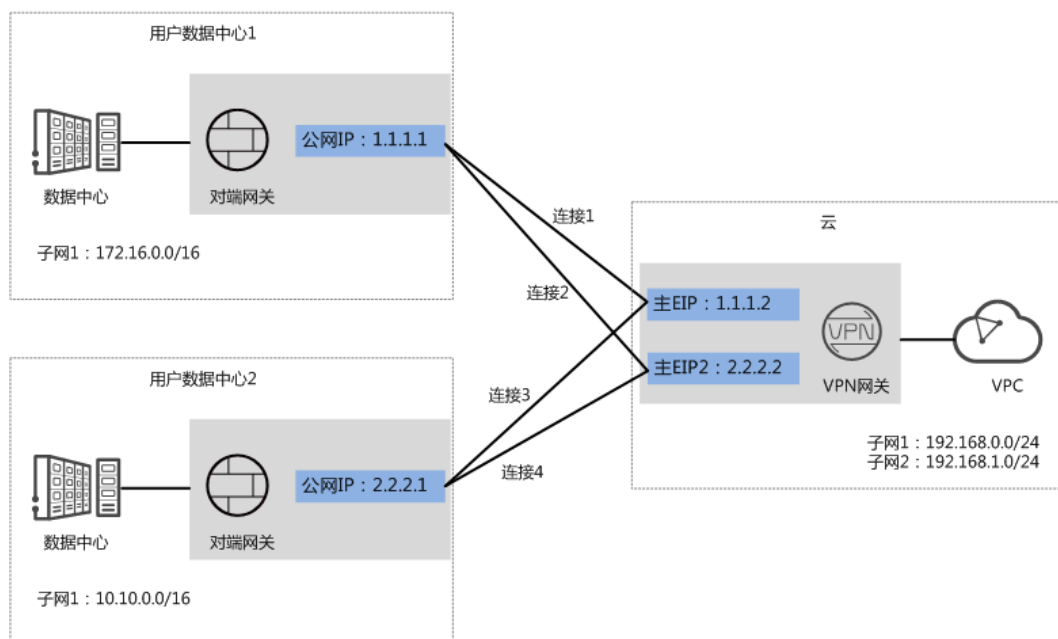
场景描述

由于业务需要，A企业的数据中心1和2需要实现网络互通。

组网方案

VPN服务提供的组网方案如图4-3所示。

图 4-3 组网方案



方案优势

- 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，无需两两站点之间配置VPN连接。
- 双连接：VPN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，保证连接可靠性。

约束与限制

- VPN网关的本端子网与对端子网不能相同，即VPC和用户数据中心待互通的子网不能相同。
- VPN网关和对端网关的IKE策略、IPsec策略、预共享密钥需要相同。
- VPN网关和对端网关上配置的本端接口地址和对端接口地址需要互为镜像。
- VPC内弹性云服务器安全组允许访问对端和被对端访问。

4.3.2 组网和资源规划

数据规划

表 4-11 规划数据

类别	规划项	规划值
VPC	待互通子网	<ul style="list-style-type: none"> 192.168.0.0/24 192.168.1.0/24
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： <ul style="list-style-type: none"> 主EIP：1.1.1.2 主EIP2：2.2.2.2
VPN连接	Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 <ul style="list-style-type: none"> 和用户数据中心1的VPN连接 <ul style="list-style-type: none"> VPN连接1：169.254.70.1/30 VPN连接2：169.254.71.1/30 和用户数据中心2的VPN连接 <ul style="list-style-type: none"> VPN连接3：169.254.72.1/30 VPN连接4：169.254.73.1/30
用户数据中心1	待互通子网	172.16.0.0/16
用户数据中心1对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： 1.1.1.1
	Tunnel接口地址	<ul style="list-style-type: none"> VPN连接1：169.254.70.2/30 VPN连接2：169.254.71.2/30
用户数据中心2	待互通子网	10.10.0.0/16
用户数据中心2对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： 2.2.2.1
	Tunnel接口地址	<ul style="list-style-type: none"> VPN连接3：169.254.72.2/30 VPN连接4：169.254.73.2/30

类别	规划项	规划值
IKE/IPsec策略	预共享密钥	Test@123
	IKE策略	<ul style="list-style-type: none"> ● 认证算法: SHA2-256 ● 加密算法: AES-128 ● DH算法: Group 15 ● 版本: v2 ● 生命周期 (秒): 86400 ● 本端标识: IP Address ● 对端标识: IP Address
	IPsec策略	<ul style="list-style-type: none"> ● 认证算法: SHA2-256 ● 加密算法: AES-128 ● PFS: DH Group15 ● 传输协议: ESP ● 生命周期 (秒): 3600

4.3.3 操作步骤

前提条件

- 云侧
 - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见《虚拟私有云用户指南》。
 - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见《虚拟私有云用户指南》。
- 数据中心侧
 - 用户数据中心1和2的VPN设备已经完成IPsec连接相关配置。
 - 用户数据中心1的VPN设备对端网络中需要包含VPC的本端子网和用户数据中心2的待互通子网；用户数据中心2的VPN设备对端网络中需要包含VPC的本端子网和用户数据中心1的待互通子网。

操作步骤

VPN服务支持静态路由模式、BGP路由模式和策略模式三种连接模式。本示例以静态路由模式进行配置讲解。

步骤1 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建VPN网关”。
2. 根据界面提示配置参数。

VPN网关参数说明如[表4-12](#)所示。

表 4-12 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“虚拟私有云”。	虚拟私有云
虚拟私有云	选择需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
本端子网	VPC需要与用户数据中心互通的子网。	192.168.0.0/24, 192.168.1.0/24
互联子网	用于VPN网关和VPC通信, 请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
BGP ASN	BGP自治系统编号。	64512
HA模式	选择“双活”。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤2 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

对端网关参数说明如表4-13所示。

表 4-13 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw1
路由模式	选择“静态路由”。	静态路由
网关IP	数据中心1下对端网关和VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	1.1.1.1

3. 参见上述步骤，配置数据中心2的对端网关信息（2.2.2.1）。

步骤3 配置云侧和数据中心1的VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置第一条VPN连接参数，单击“提交”。

VPN连接参数说明如表4-14所示。

表 4-14 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
连接模式	选择“静态路由模式”。	静态路由模式
对端网关	选择对端网关。	cgw-fw1
对端子网	用户数据中心1中需要和VPC通信的子网。 - 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 - 部分网段是VPC预留网段，不能作为对端子网，比如100.64.0.0/10，214.0.0.0/8。	172.16.0.0/16
接口分配方式	- 手动分配 本示例以“手动分配”为例。 - 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.70.2
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认

3. 配置第二条VPN连接参数。

说明

此处仅对和第一条VPN连接配置不同的参数，未提及参数建议和第一条VPN连接配置保持一致。

表 4-15 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2

步骤4 配置云侧和数据中心2的VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 根据界面提示配置第一条VPN连接参数，单击“提交”。

VPN连接参数说明如表4-16所示。

表 4-16 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-003
VPN网关	选择VPN网关。	vpngw-001
网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
对端网关	选择对端网关。	cgw-fw2
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心2中需要和VPC通信的子网。 - 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 - 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10，214.0.0.0/8。	10.10.0.0/16
接口分配方式	- 手动分配 本示例以“手动分配”为例。 - 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.72.1

参数	说明	取值参数
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.72.2
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和用户数据中心2对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和用户数据中心2对端网关的策略配置需要保持一致。	保持默认

3. 配置第二条VPN连接参数。

说明

此处仅对和第一条VPN连接配置不同的参数，未提及参数建议和第一条VPN连接配置保持一致。

表 4-17 第二条 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-004
网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.73.1
对端隧道接口地址	用户数据中心2对端网关的Tunnel隧道IP地址。	169.254.73.2

步骤5 配置数据中心1/2的对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。

----结束

结果验证

- 大约5分钟后，查看VPN连接状态。
选择“虚拟专用网络 > 企业版-VPN连接”，四条VPN连接状态显示为正常。
- 用户数据中心1内的服务器和用户数据中心2内的服务器可以相互Ping通。

5 故障排除

5.1 VPN 连接状态显示“未连接”

故障现象

在“虚拟专用网络 > 企业版-VPN连接”页面，VPN连接状态显示为“未连接”。

可能原因

- VPN连接两端的连接配置不正确。
- 安全组和客户设备侧ACL配置不正确。

处理步骤

- 检查VPN连接两端的连接配置
 - 确认两端配置的网关IP参数是否为镜像。
 - VPN网关的主/备EIP可以选择“虚拟专用网络 > 企业版-VPN网关”，在网关IP栏下查看。
 - 客户设备侧网关的公网IP可以选择“虚拟专用网络 > 企业版-对端网关”，在网关IP栏下查看。
 - 确认IKE策略、IPsec策略协商参数是否一致。
 - IKE策略、IPsec策略协商参数可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改策略配置”查看。
 - 确认预共享密钥是否一致。
 - 预共享密钥无法在云上直接查看。如果不确认预共享密钥，建议根据客户设备侧的预共享密钥对VPN连接的预共享密钥进行重置。
可以选择“虚拟专用网络 > 企业版-VPN连接”，选择“更多 > 重置密钥”进行重置。
 - 如果连接模式采用策略模式，请确认两端策略规则中的源网段和目的网段是否为镜像。
策略规则可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改连接信息”查看。

- 如果连接模式采用静态路由模式且云侧开启了NQA功能，请确认客户设备侧是否已经正确配置Tunnel隧道的IP地址。
 - 是否开启NQA功能，可以选择“虚拟专用网络 > 企业版-VPN连接”，单击VPN连接名称，在“基本信息”页签查看“检测机制”。
 - 客户设备侧在VPN连接已设置的Tunnel隧道的IP地址，可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改连接信息”，查看本端接口地址和对端接口地址。VPN连接的本端接口地址和对端接口地址需要和客户设备的本端接口地址和对端接口地址互为镜像配置。
- 如果连接模式采用BGP路由模式，请确认两端的BGP ASN是否为镜像。
 - VPN网关的BGP ASN可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。
 - 客户设备侧网关的BGP ASN可以选择“虚拟专用网络 > 企业版-对端网关”，在BGP ASN栏下查看。
- 检查安全组和客户设备侧ACL配置
 - 确认default安全组已经放通客户设备侧公网IP的UDP协议端口500和4500。default安全组查看步骤如下：
 - i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击关联的VPC名称。
 - ii. 单击VPC对应的路由表。
 - iii. 单击路由表的名称。
 - iv. 找到VPN网关主或备EIP的下一跳，单击下一跳名称。
 - v. 在“关联安全组”页签，检查端口放通情况。
 - 确认客户设备侧安全组已经放通VPN网关主备EIP的UDP协议端口500和4500。

5.2 云上云下无法 Ping 通

故障现象

- 云下数据中心服务器无法Ping通VPC上的ECS服务器。
- VPC上的ECS服务器无法Ping通云下数据中心服务器。

可能原因

- 安全组配置不正确
- 互联子网的ACL规则配置不正确
- 客户设备侧放通策略配置不正确
- 客户设备侧路由配置不正确

处理步骤

- 检查安全组配置
 - 确认default安全组已经放通去往对端子网数据流。default安全组查看步骤如下：

- i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击关联的VPC名称。
 - ii. 单击VPC对应的路由表。
 - iii. 单击路由表的名称。
 - iv. 找到VPN网关主或备EIP的下一跳，单击下一跳名称。
 - v. 在“关联安全组”页签，检查端口放通情况。
 - 确认default安全组已经放通来自对端子网数据流。
 - 确认default安全组已经放通去往本端子网数据流。
 - 确认default安全组已经放通来自本端子网数据流。
 - 确认ECS所在的安全组已经放通去往对端子网数据流。

ECS安全组可以选择“计算 > 虚拟弹性云服务器”，单击ECS名称，选择“安全组”，单击“配置规则”查看。
 - 确认ECS所在的安全组已经放通来自对端子网数据流。
- 互联子网的ACL规则配置不正确
 - 确认互联子网的ACL规则中，是否已放通所有本端子网到对端子网的TCP协议端口。
 - i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称。
 - ii. 在“基本信息”页签，记录互联子网信息。
 - iii. 在“基本信息”页签，单击关联模式对应的VPC名称。
 - iv. 在VPC“基本信息”页签右边“网络互通概览”区域，单击子网个数。
 - v. 根据网段匹配互联子网，并单击“网络ACL”的ACL名称。
 - vi. 放通所有本端子网到对端子网的TCP协议端口。
 - 检查客户设备侧放通策略
 - 确认客户设备侧已经放通去往VPN本端子网的数据流。
 - 确认客户设备侧已经放通来自VPN本端子网的数据流。

本端子网可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。
 - 检查客户设备侧路由配置
 - 确认公网路由配置正确：目的地址为VPN网关EIP地址，下一跳为设备出口地址。
 - 确认私网路由配置正确：目的地址为VPN本端子网，下一跳为设备出口地址。

本端子网可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。

5.3 流量丢包

故障现象

- 云下数据中心服务器对VPC上的ECS服务器执行Ping操作时，存在流量丢包。
- VPC上的ECS服务器对云下数据中心服务器执行Ping操作时，存在流量丢包。

处理步骤

- 检查客户侧组网和带宽情况
 - 确认客户网络的组网是否多出口，是否因为负载分担组网将流量分配到非VPN连接出口导致流量丢包，确保数据流恒定走特定出口访问。
 - 使用客户侧VPN网关地址PingVPN网关IP以及其他公网（例如：114.114.114.114），检查公网时延、丢包率。
如果公网网络质量存在问题，建议向所在网络提供运营商进行求助。
 - 检查客户出口设备带宽是否超限。
- 检查组网和带宽情况
 - 检查VPN网关的带宽是否超限。
如果超限，可以通过扩容VPN网关的带宽进行解决。

6 常见问题

6.1 企业版 VPN

6.1.1 IPsec VPN 适用连接典型组网结构有哪些？

VPN是打通的点到点的网络，实现两点之间的私网互访，不能打通点到端的网络。

- 适用典型场景：
 - 不同region之间创建VPN，实现跨region的VPC间网络互访。
 - VPN HUB功能，结合对等连接和CC实现云下IDC与云上多VPC网络互访。
 - 结合源NAT实现跨云访问特定IP。
- 不适用的典型场景：
 - 相同region的两个VPC不可以使用VPN，推荐使用对等连接打通。
 - 不可与家庭PPPoE拨号网络建立VPN连接。
 - 不可与4G/5G路由器建立VPN连接。
 - 不可与个人终端建立VPN连接。

6.1.2 什么是 VPC、VPN 网关、VPN 连接？

VPC：虚拟私有云是指云上隔离的、私密的虚拟网络环境，用户可通过虚拟专用网络（VPN）服务，安全访问云上虚拟网络内的主机（ECS）。

VPN网关：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连接：是一种基于Internet的IPsec加密技术，帮助用户快速构建VPN网关和用户数据中心的对端网关之间的安全、可靠的加密通道。

云上建立VPN网络分为以下两个步骤：

1. 创建VPN网关：创建VPN网关指明了VPN互联的本地VPC，同时创建连接带宽和网关IP。
2. VPN连接：创建VPN连接指明了与客户侧对接的网关IP、子网和协商策略信息。

6.1.3 VPN 接入 VPC 的网络地址如何规划？

- 云上VPC地址段和客户云下的地址段不能冲突，且不允许存在包含关系。
- 为避免和云服务地址冲突，用户侧网络应尽量避免使用127.0.0.0/8、169.254.0.0/16、224.0.0.0/3、100.64.0.0/10的网段。

6.1.4 IPsec VPN 是否会自动建立连接？

支持自动建立连接。

6.1.5 建立 IPsec VPN 连接需要账户名和密码吗？

常见的使用账户名和密码进行认证的VPN有SSL VPN、PPTP或L2TP，IPsec VPN使用预共享密钥方式进行认证，密钥配置在VPN网关上，在VPN协商完成后即建立通道，VPN网关所保护的主机在进行通信时无需输入账户名和密码。

📖 说明

IPsec XAUTH技术是IPsec VPN的扩展技术，它在VPN协商过程中可以强制接入用户输入账户名和密码。

目前VPN不支持该扩展技术。

6.1.6 VPN 监控可以监控哪些内容？

VPN网关

可以监控网关IP的带宽信息，包含入网流量、入网带宽、出网流量、出网带宽及出网带宽使用率。

VPN连接

可以监控连接的状态信息，包括VPN连接状态、链路往返平均时延、链路往返最大时延、链路丢包率、隧道往返平均时延、隧道往返最大时延、隧道丢包率。

其中，链路往返平均时延、链路往返最大时延、链路丢包率、隧道往返平均时延、隧道往返最大时延、隧道丢包率需要单击VPN连接，在“基本信息”页签通过添加健康检查项进行添加；私网相关指标仅VPN连接使用静态路由模式，且开启NQA检测机制场景下支持配置。

6.1.7 EIP 能作为 VPN 的网关 IP 吗？

可以。

用户可以在创建VPN网关时绑定EIP作为网关IP。

6.1.8 创建 VPN 连接时如何选择 IKE 的版本？

推荐您选择IKEv2进行协商，其原因是IKEv1的版本存在一定的安全风险，且IKEv2在连接的协商建立过程，认证方法支持，DPD超时处理，SA超时处理上都优于IKEv1。

将大力推进IKEv2的使用，逐步停用IKEv1协商策略。

IKEv1 与 IKEv2 的协议介绍

- IKEv1协议是一个混合型协议，其自身的复杂性不可避免地带来一些安全及性能上的缺陷，已经成为目前实现的IPsec系统的瓶颈。

- IKEv2协议保留了IKEv1的基本功能，并针对IKEv1研究过程中发现的问题进行修正，同时兼顾简洁性、高效性、安全性和健壮性的需要，整合了IKEv1的相关文档，由RFC4306单个文档替代。通过核心功能和默认密码算法的最小化规定，新协议极大地提高了不同IPsec VPN系统的互操作性。

IKEv1 存在的安全风险

- IKEv1 支持的密码算法已超过10年未做更新，并不支持诸如AES-GCM、ChaCha20-Poly1305等推荐的强密码算法。IKEv1使用ISALMP头的E比特位来指定该头后跟随的是加密载荷，但是这些加密载荷的数据完整性校验值放在单独的hash载荷中。这种加密和完整性校验的分离阻碍了v1使用认证加密（AES-GCM），从而限制了只能使用初期定义的AES算法。
- 协议本身也无法防止报文放大攻击（属于DOS攻击）初始报文交换，IKEv1容易被半连接攻击，响应方响应初始化报文后维护发起-响应的关系，维护了大量的关系会消耗大量的系统资源。
针对连接的DOS攻击，IKEv2协议上有针对性的解决方案。
- IKEv1野蛮模式安全性低：野蛮模式开始信息报文不加密，存在用户配置信息泄露的风险，当前也存在针对野蛮攻击，如：中间人攻击。

IKEv1 和 IKEv2 的区别

- **协商过程不同。**
 - IKEv1协商安全联盟主要分为两个阶段，其协议相对复杂、带宽占用较多。IKEv1阶段1的目的是建立IKE SA，它支持两种协商模式：主模式和野蛮模式。主模式用6条ISAKMP消息完成协商。野蛮模式用3条ISAKMP消息完成协商。野蛮模式的优点是建立IKE SA的速度较快。但是由于野蛮模式密钥交换与身份认证一起进行无法提供身份保护。IKEv1阶段2的目的就是建立用来传输数据的IPsec SA，通过快速交换模式（3条ISAKMP消息）完成协商。
 - IKEv2简化了安全联盟的协商过程。IKEv2正常情况使用2次交换共4条消息就可以完成一个IKE SA和一对IPsec SA，如果要求建立的IPsec SA大于一对时，每一对SA只需额外增加1次交换，也就是2条消息就可以完成。

说明

IKEv1协商，主模式需要6+3，共9个报文；野蛮模式需要3+3，共6个报文。IKEv2协商，只需要2+2，共4个报文。

- **认证方法不同。**
 - 数字信封认证（hss-de）仅IKEv1支持（需要安装加密卡），IKEv2不支持。
 - IKEv2支持EAP身份认证。IKEv2可以借助AAA服务器对远程接入的PC、手机等进行身份认证、分配私网IP地址。IKEv1无法提供此功能，必须借助L2TP来分配私网地址。
 - IKE SA的完整性算法支持情况不同。IKE SA的完整性算法仅IKEv2支持，IKEv1不支持。
- **DPD中超时重传实现不同。**
 - retry-interval参数仅IKEv1支持。表示发送DPD报文后，如果超过此时间间隔未收到正确的应答报文，DPD记录失败事件1次。当失败事件达到5次时，删除IKE SA和相应的IPsec SA。直到隧道中有流量时，两端重新协商建立IKE SA。
 - 对于IKEv2方式的IPsec SA，超时重传时间间隔从1到64以指数增长的方式增加。在8次尝试后还未收到对端发过来的报文，则认为对端已经下线，删除IKE SA和相应的IPsec SA。

- **IKE SA与IPsec SA超时时间手工调整功能支持不同。**

IKEv2的IKE SA软超时为硬超时的9/10±一个随机数，所以IKEv2一般不存在两端同时发起重协商的情况，故IKEv2不需要配置软超时时间。

IKEv2 相比 IKEv1 的优点

- 简化了安全联盟的协商过程，提高了协商效率。
- 修复了多处公认密码学方面的安全漏洞，提高了安全性能。
- 加入对EAP (Extensible Authentication Protocol) 身份认证方式的支持，提高了认证方式的灵活性和可扩展性。
EAP是一种支持多种认证方法的认证协议，可扩展性是其最大的优点，即如果想加入新的认证方式，可以像组件一样加入，而不用变动原来的认证体系。当前EAP认证已经广泛应用于拨号接入网络中。
- IKEv2使用基于ESP设计的加密载荷，v2加密载荷将加密和数据完整性保护关联起来，即加密和完整性校验放在相同的载荷中。AES-GCM同时具备保密性、完整性和可认证性的加密形式，与v2的配合比较好。

6.1.9 如何解决 VPN 连接无法建立连接问题？

1. 登录管理控制台，进入“虚拟专用网络 > 企业版-VPN连接”页面。
2. 在VPN连接列表中，单击目标VPN连接“操作”列的“修改策略配置”，查看该VPN连接对应的IKE策略和IPsec策略详情。
3. 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。
如果第一阶段IKE SA已经建立，第二阶段IPsec SA未建立，常见情况为IPsec策略与数据中心远端的配置不一致。
4. 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，则您在数据中心或局域网中的ACL应对您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
```
5. 配置完成后检查VPN是否连接，从两侧测试ping是否正常。

6.2 经典版 VPN

6.2.1 IPsec VPN 和 SSL VPN 在使用场景和连接方式上有什么区别？

使用场景

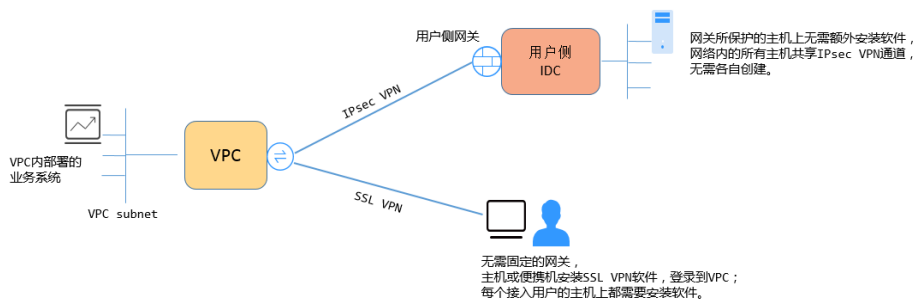
IPsec VPN：连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网；即IPsec VPN是网对网的连接。

SSL VPN：连通的是一个客户端到一个局域网络，如出差员工的便携机访问公司内网。

连接方式

IPsec VPN：要求两端有固定的网关设备，如防火墙或路由器；管理员需要分别配置两端网关完成IPsec VPN协商。

SSL VPN：需要在主机上安装指定的Client软件，通过用户名/密码拨号连接至SSL设备。



说明

VPN目前仅支持IPsec VPN，不支持SSL VPN。

6.2.2 Console 界面在哪添加 VPN 远端路由？

云端在VPN连接创建时会自动下发远端子网路由，无需手动配置。

6.2.3 VPN 连接中断后会通知我吗？

VPN连接的状态监控功能已上线，VPN连接创建后即会向ces上报状态信息，但是并不会自动向用户发送告警通知，需要在服务列表中选择“管理与监管 > 云监控”创建告警规则。

创建VPN连接后，在VPN连接列表页面选择“操作 > 更多 > 查看监控”，可以跳转到VPN连接监控页面。

6.2.4 连接云下的多台服务器需要购买几个连接？

VPN属于IPsec VPN，它是用于打通云上VPC和用户侧数据中心子网的VPN，所以购买VPN连接的个数与服务器的数量无关，而与这些服务器所在的数据中心数量有关。

大部分情况下一个用户侧数据中心会有一个公网出口网关，所有服务器（或用户主机）都通过该网关连接至Internet，因此对于这种情况配置一个VPN连接即可，通过该连接即可打通VPC与用户网络之间的流量。

6.2.5 使用 VPN 会对本地网络造成哪些影响，访问云端主机在路由上会有哪些变化？

配置VPN时，用户需要在用户侧数据中心的网关上增加以下VPN配置信息：

1. IKE/IPsec策略配置。
2. 指定感兴趣流（ACL）。
3. 用户需要审视用户侧数据中心网关的路由配置，确保发往VPC的流量被路由到正确的出接口（即绑定IPsec策略的接口）。

在完成VPN配置后，只有命中感兴趣流的流量会进入VPN隧道，其它网络的访问都不受影响。

例如，云端的ECS绑定的EIP，在未创建VPN前，本地用户访问云端主机都通过EIP访问，创建VPN后，数据流匹配了ACL后会通过VPN隧道访问云端ECS的私网IP。

6.2.6 使用 VPN 替换专线该如何配置？

1. 首先需要确认用户侧数据中心设备支持IPsec VPN。
2. 然后在云上创建一个VPN网关（请注意选择原专线所属的VPC）和VPN连接。

须知

配置VPN连接时需要注意，因为远端子网与专线远端子网一样，不能直接配置，否则会产生路由冲突。可采用以下方案：

- 先删除专线VIF，再配置VPN连接。
- 将远端子网分拆为两个细分子网再配置VPN连接，等专线删除之后，再改为正常的子网配置。

6.2.7 公司网络已通过 VPN 连通了云，我如何在家访问 ECS？

VPN为IPsec VPN，是连接云上VPC和云下局域网的。

家庭网络非公司局域网的组成部分，无法直接和云上VPC实现互联。

居家办公主机需要访问云上VPC资源可以考虑直接访问云服务的EIP，或通过SSL VPN（需公司支持SSL接入）先连接至公司局域网，然后通过公司局域网访问云上VPC资源。

6.2.8 对接云时，如何配置 DPD 信息？

云默认开启DPD配置，且不可关闭该配置。

DPD配置信息如下：

- DPD-type：按需
- DPD idle-time：30s
- DPD retransmit-interval：15s
- DPD retry-limit：3次
- DPD msg：seq-hash-notify。

两端DPD的type、空闲时间、重传间隔、重传次数无需一致，只要能接收和回应DPD探测报文即可，DPD msg格式必须一致。

6.2.9 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。如果协商成功，则保持连接状态至下一轮协商。如果协商失败，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。

A 修订记录

发布日期	修改说明
2024-11-14	第一次正式发布。