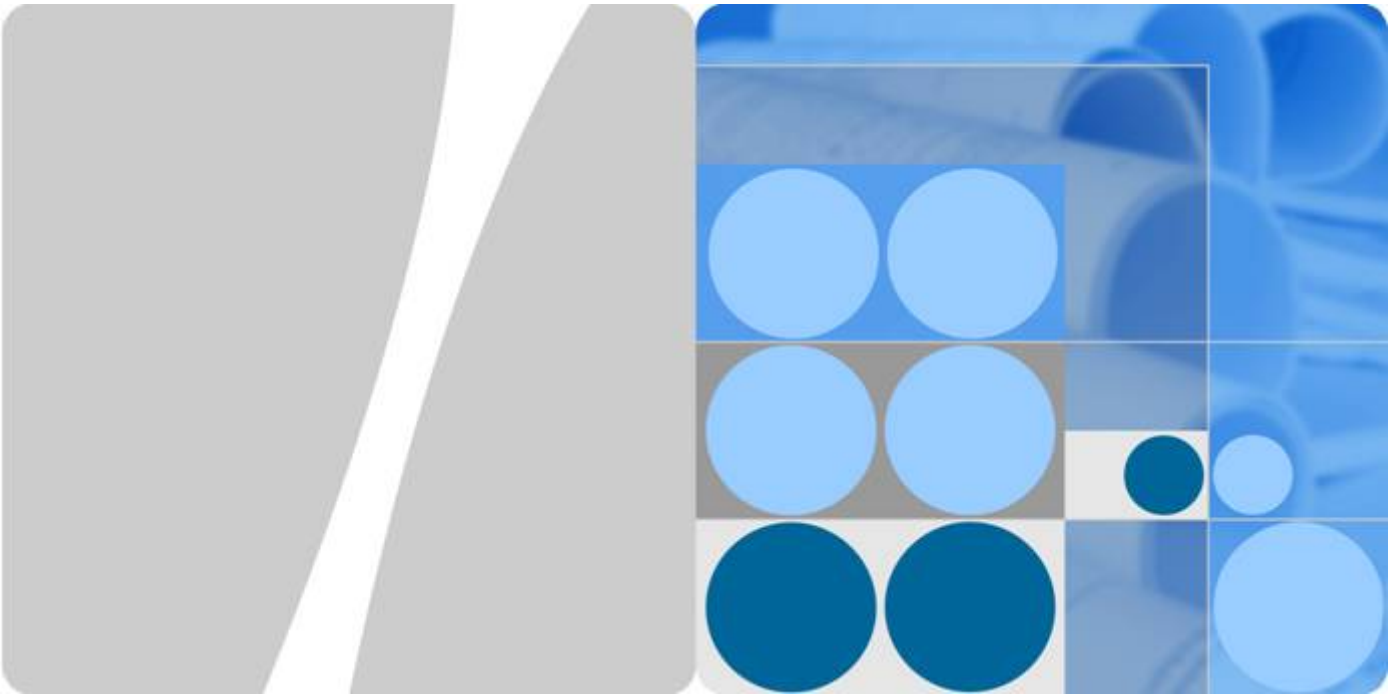


虚拟专用网络

用户指南

发布日期　2025-12-18

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。

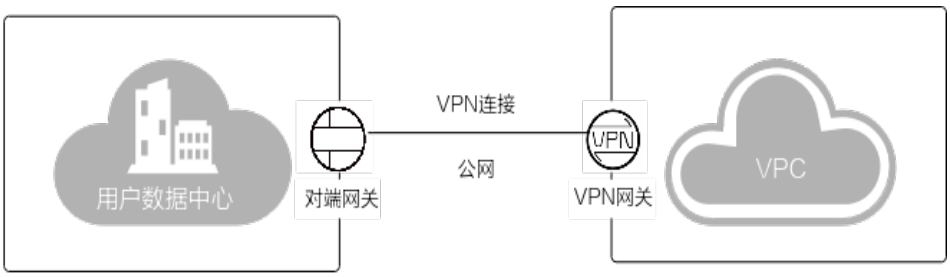
站点入云VPN（Site-to-Cloud VPN，以下简称S2C VPN），站点入云VPN基于IPsec协议，包括企业版VPN和经典版VPN。

站点入云VPN由VPN网关、对端网关和VPN连接组成。

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

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：

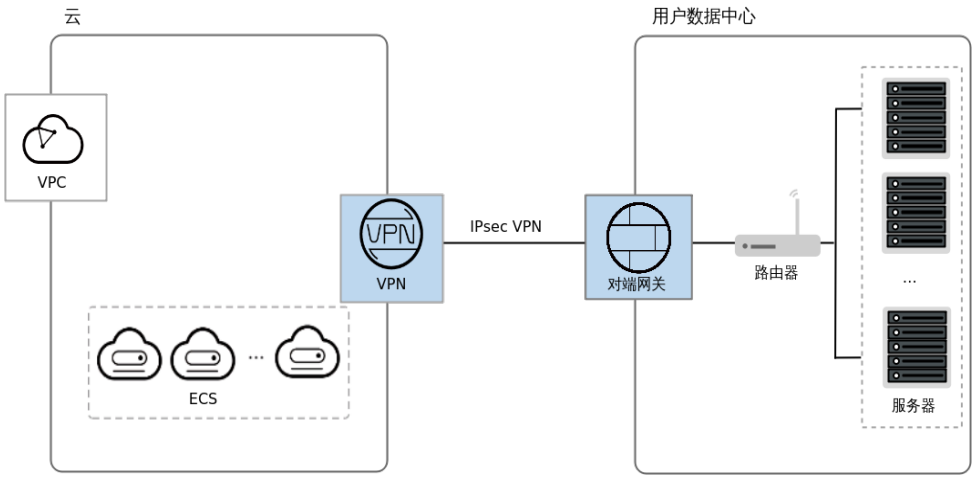
- **更安全**
  - 基于IKE/IPsec、SSL对传输数据加密，保证用户数据传输安全。
  - VPN支持为每个用户创建独立的VPN网关，提供租户网关隔离防护能力。
- **高可用**
  - 双连接：网关提供两个接入地址，支持一个对端网关创建两条相互独立的VPN连接，一条连接中断后流量可快速切换到另一条连接。
  - 双活网关：双活网关部署在不同的AZ区域，实现AZ级高可用保障。
  - 主备模式：正常情况下，VPN网关和对端网关通过主连接进行通信；当主连接发生故障时，VPN连接会自动切换到备连接；故障恢复后，VPN连接会自动切回到主连接。
  - HA模式：站点入云VPN支持主备、双活。
- **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。
  - 关联企业路由器（Enterprise Router, ER）：企业可以构建更加丰富的云上网络。
  - 支持私网类型网关：对专线私有网络进行加密传输，提升数据传输安全。
  - 支持开启/关闭分支互联功能：站点入云VPN支持用户可以根据需要灵活开启或关闭分支互联，实现对端网关之间互联或隔离。

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。

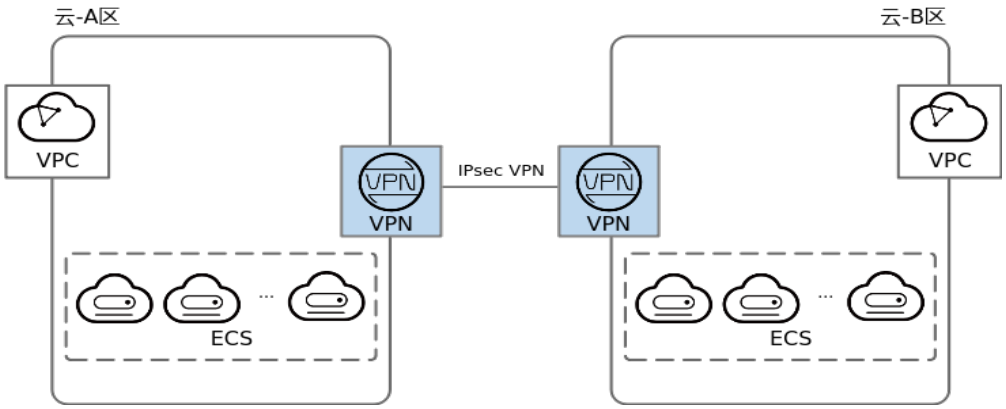
图 1-2 混合云部署



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 跨地域VPC互联**所示。

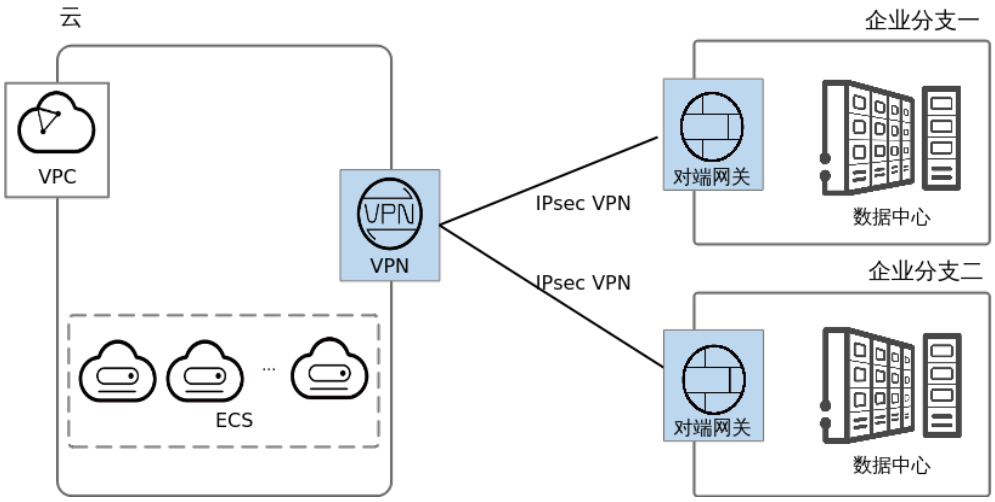
图 1-3 跨地域 VPC 互联



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

1.4.1 站点入云 VPN

说明

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

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

表 1-1 站点入云 VPN 产品规格

对比项	专业型1	专业型2
独享网关资源	支持	支持
双连接	支持	支持
双活网关	支持	支持
主备网关	支持	支持
策略模式	支持	支持
路由模式-静态路由	支持	支持
路由模式-BGP路由	支持	支持
策略模板模式	不支持	不支持
最大转发带宽	300Mbps	1Gbps
最大VPN连接组数	100个	100个
对接企业路由器	支持	支持

对比项	专业型1	专业型2
对接虚拟私有云	支持	支持
接入公网地址	支持	支持
接入私网地址	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。

1.5 约束与限制

1.5.1 站点入云 VPN

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 • 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
	不同款型VPN网关支持接收的BGP路由数量	100 • 专业型1网关支持接收的BGP路由数量最多为200。 • 专业型2网关支持接收的BGP路由数量最多为300。
	每VPN网关支持最大路由条目数量	10000
	不同款型VPN网关支持最大ACL规则数量	300

VPN网关类型	资源	默认限制
经典版VPN	每租户在每区域支持创建的VPN网关数量	2 每个VPC最多创建1个VPN网关。

- 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	
经典版VPN	每租户在每区域支持创建的VPN连接数量	12	不支持修改。

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

  VPN网关每个网关IP和对端网关建连时，专业型1、专业型2的网关最大提供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。

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

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

  当涉及专业型1、专业型2网关IP的VPN连接模式占用的通信隧道超过300个时，会导致超出部分对应的VPN连接创建失败。
- 使用策略模式创建VPN连接时，若添加多条策略规则，不同策略规则的源、目的网段需要避免出现重叠，以免造成数据流误匹配或IPsec隧道震荡。

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 站点入云企业版 VPN 和经典版 VPN 的区别

表 1-5 企业版 VPN 和经典版 VPN 的区别

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

1.8 安全

1.8.1 身份认证与访问控制

站点入云VPN连接支持通过预共享密钥（PSK）方式对对端网关进行身份验证。

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

相关链接：

预共享密钥

1.8.2 数据保护技术

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

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

  表 1-6 站点入云 VPN 策略配置参数说明

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

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

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

完善的前向安全性 PFS

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

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

站点入云VPN支持的算法如下：

- DH group 1（此算法安全性较低，请慎用）
- DH group 2（此算法安全性较低，请慎用）
- DH group 5（此算法安全性较低，请慎用）
- DH group 14
- DH group 15
- DH group 16
- DH group 19
- DH group 20
- DH group 21

抗重放

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

资源隔离

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

1.8.3 审计与日志

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

图 1-5 审计与日志

相关链接：

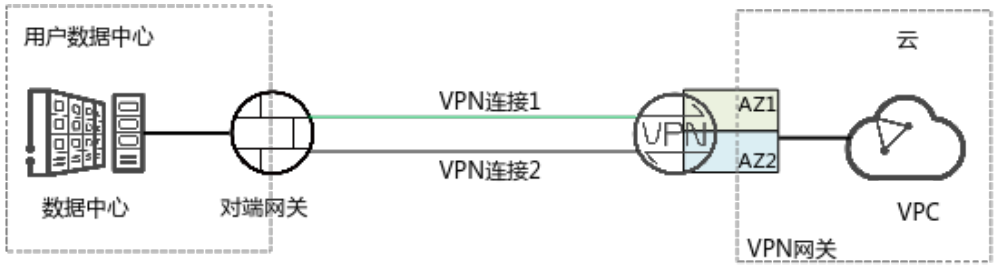
如何查看审计日志，请参见《云审计服务用户指南》。

1.8.4 服务韧性

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

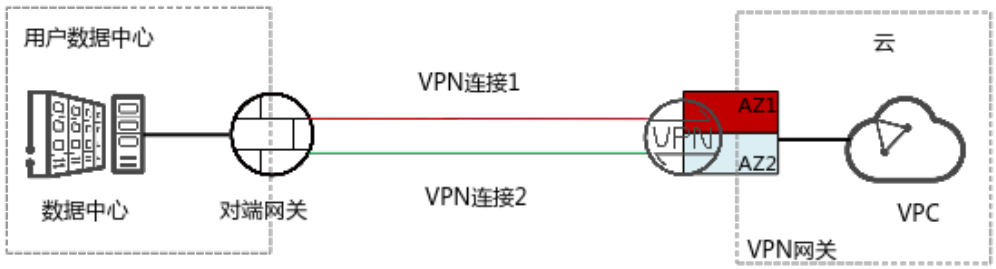
该特性仅企业版VPN支持，经典版VPN不支持。

图 1-6 正常场景



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

图 1-7 故障切换场景



1.9 权限管理

1.9.1 基于 IAM 进行权限管理

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，可以帮助您安全地控制资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制员工对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是云服务平台提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

关于IAM的详细介绍，请参见**IAM产品介绍**。

VPN 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

VPN部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，然后在指定区域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“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问VPN时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对VPN服务，管理员能够控制IAM用户仅能对某一类VPN资源进行指定的管理操作。

如**表1-7**所示，包括了VPN的所有系统权限。

表 1-7 VPN 系统权限

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

表 VPN常用操作与系统权限的关系列出了站点入云VPN常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-8 站点入云 VPN 常用操作与系统权限的关系

操作	VPN Administrator（不推荐使用）	VPN FullAccess（推荐使用）	VPN ReadOnlyAccess
创建VPN网关	√	• 企业版VPN：√ • 经典版VPN：×	×
查询VPN网关	√	√	√

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

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

相关链接

- IAM产品介绍
- 创建用户组、用户并授予VPN权限

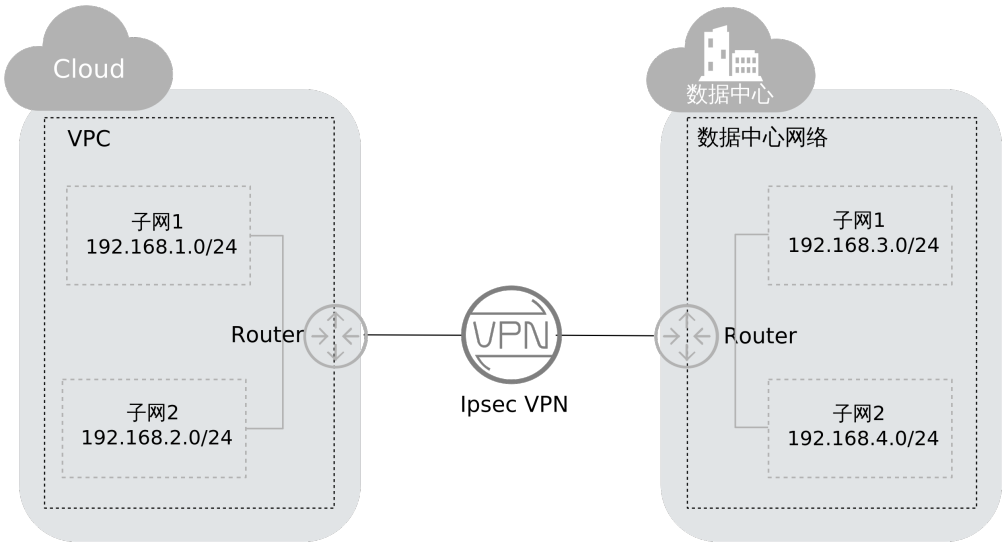
1.10 基本概念

1.10.1 IPsec VPN

IPsec VPN是一种加密的隧道技术，通过使用加密的安全服务在不同的网络之间建立保密而安全的通讯隧道。在云上即站点入云VPN。

如图1-8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 1-8 IPsec VPN



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

相关链接：

站点入云VPN

1.10.2 VPN 网关

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

相关链接：

- **创建站点入云VPN网关**
- **创建经典版VPN网关**

1.10.3 VPN 连接

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

相关链接：

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

1.10.4 VPN 网关带宽

VPN网关带宽指的是出云方向的带宽，即从VPC发往用户侧数据中心的带宽。

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

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

1.10.5 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）。

1.10.6 对端网关

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

相关链接：

创建对端网关。

1.10.7 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。

1.10.8 预共享密钥

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

相关链接：

建立IPsec VPN连接需要账户名和密码吗？

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

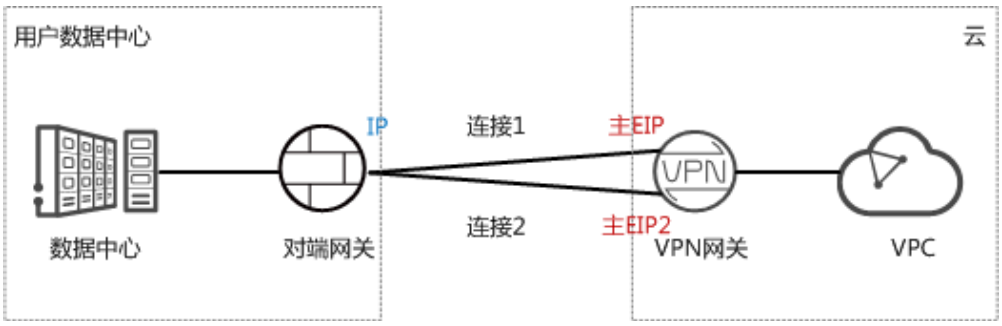
场景描述

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 双活模式**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。

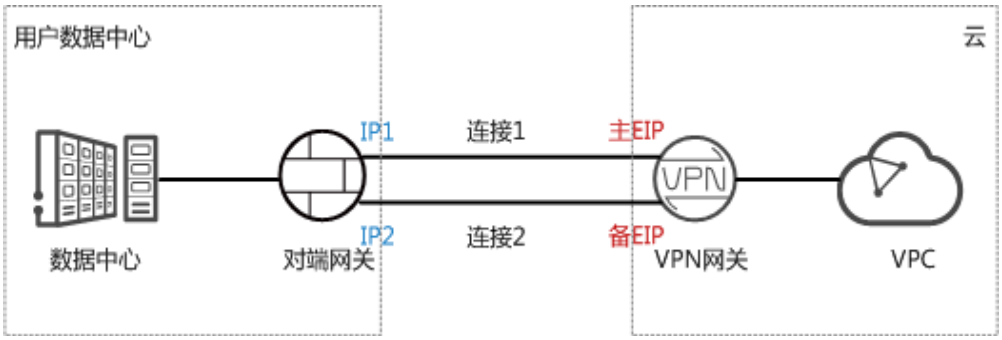
  图 2-1 双活模式

- 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会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、100.64.0.0/12和214.0.0.0/8等预留网段。不同region的预留网段不同，实际使用以控制台显示为准。
  - 如果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： • 主EIP：11.xx.xx.11 • 主EIP2：11.xx.xx.12
VPN连接	“连接1配置”中的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。 • 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30
数据中心	待互通子网	172.16.0.0/16

类别	规划项	规划值
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

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	**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	**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	**步骤三：创建VPN连接**	• VPN网关的主EIP、主EIP2和对端网关组建两条VPN连接。 • 连接2的连接模式、预共享密钥、IKE/IPsec策略需要和连接1的配置保持一致。
4	**步骤四：配置对端网关设备**	• 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。 • 对端网关配置的连接模式、预共享密钥、IKE/IPsec策略需要和VPN连接配置保持一致。
5	**步骤五：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“ > 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 单击“创建站点入云VPN网关”。

步骤5 根据界面提示配置参数，单击“立即购买”并完成支付。

步骤6 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
计费模式	支持“按需计费”。	按需计费
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	• 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	• 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。 • 企业路由器：通过ER向对端网关或ER下所有VPC所在子网发送通信消息。	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“立即创建”。

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
BGP ASN	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

----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 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VPN连接参数，单击“立即购买”。

本示例仅对关键参数进行说明。

表 2-5 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

参数	说明	参数取值
VPN网关	选择**步骤一：创建VPN网关**创建的VPN网关。	vpngw-001
连接1网关IP	VPN网关的主EIP。	11.xx.xx.11
连接1对端网关	选择连接1对端网关。	cgw-001
连接2网关IP	VPN网关的主EIP2。	11.xx.xx.12
连接2对端网关	选择连接2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** • 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、100.64.0.0/12、214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 • 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。 • 当“关联模式”采用“企业路由器”，“连接模式”采用“BGP路由模式”和“策略模式”时，无需配置对端子网。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置等。	请根据实际设置
接口地址分配方式	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。	169.254.70.2/30
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

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
连接2配置	选择是否“与连接1保持一致”。	关闭
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	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

----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：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连接的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，Tunnel*x*和IPsec_nqa*x*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“ > 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

2.1.6 步骤五：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 在页面左上角单击图标，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）。

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. 在页面左上角单击 图标，选择区域，选择“网络 > 虚拟专用网络VPN”。
   进入虚拟专用网络页面。
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“Create Now”。VPN网关参数请参见**表 VPN网关参数说明**

表 2-6 VPN 网关参数说明

参数	说明	取值样例
计费模式	VPN网关支持按需计费计费模式。 按需计费：购买VPN网关时，可以同时购买一条与其相关联的VPN连接。	按需计费
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

表 2-7 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： • 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VPC的VPN和您的数据中心的VPN中，配置需要一致。 取值范围： ● 取值长度：6~128个字符。 ● 只能包括以下几种字符： – 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	● 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 2-8 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： ● 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	加密算法，支持的算法： ● 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	● 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。 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（有安全风险不推荐） ● v2 默认配置为：v2。	v2
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

表 2-9 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： ● 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： ● 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
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。 ● 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 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： ● ESP ● AH ● AH-ESP 默认配置为：ESP。	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. 在页面左上角单击 图标，选择区域，选择“网络 > 虚拟专用网络VPN”。
   进入虚拟专用网络页面。
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“立即购买”。VPN连接参数请参见**表 VPN连接参数说明**。

表 2-10 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

参数	说明	取值样例
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，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。	-
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： ● 取值长度：6~128个字符。 ● 只能包括以下几种字符： – 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	● 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 2-11 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： ● 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： ● 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	● 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： ● 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

表 2-12 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： ● 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： ● 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	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。 ● 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 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 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

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。

3 管理

3.1 站点入云 VPN 企业版

3.1.1 企业版 VPN 网关管理

3.1.1.1 创建 VPN 网关

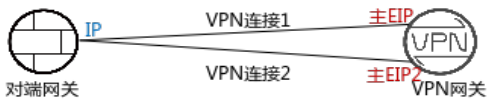
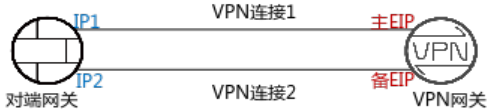
场景描述

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。

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》。
- 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。

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“ > 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 在“站点入云VPN网关”界面，单击“创建站点入云VPN网关”。

步骤6 根据界面提示配置参数，单击“立即创建”。

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

参数	说明	取值样例
关联模式	● 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。 ● 企业路由器 通过ER向对端网关或ER下所有VPC所在子网发送通信消息。 **说明** 该场景下需要关注企业路由器的路由表条数规格限制。如果对端网关和VPN网关发送的路由条数超过企业路由器的规格，则企业路由器将无法学习到超出部分的路由信息，最终导致VPN网关和对端网关之间的流量不通。	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)
企业路由器	选择企业路由器ER信息。	er-001
接入虚拟私有云	“关联模式”采用“企业路由器”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。	vpc-001(192.168.0.0/16)
接入子网	“关联模式”采用“企业路由器”时需要配置。 VPN网关连接公网的子网。	subnet-001(192.168.0.0/24)
网关接入IP	“关联模式”采用“企业路由器”、“网络类型”为“私网”时需要配置。 ● 自动分配IP地址（默认） 使用接入子网对VPN网关分配网关IP。 自动分配的私网网关IP，可以在“VPN网关”页面进行查看。 ● 手动指定IP地址 指定接入子网中的IP地址配置VPN网关IP。	自动分配IP地址
互联子网	仅“关联模式”采用“虚拟私有云”时需要配置。 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
本端子网	仅“关联模式”采用“虚拟私有云”时需要配置。 配置VPC与对端网关对应数据中心互通的子网。 ● 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

参数	说明	取值样例
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。 BGP AS号取值范围为1-4294967295。	64512
HA模式	● 双活 – 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。 – 关联模式选择“企业路由器”时，VPN网关到该对端子网的出云流量由该对端子网对应的所有VPN连接负载分担。 ● 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和专业型2两种类型。	专业型1
带宽名称	EIP对应带宽对象的名称。	Vpngw-bandwidth1
主EIP	用于VPN网关和对端网关进行网络连接。 ● 现在创建：创建新EIP。 ● 使用已有：使用已有EIP。	现在创建
带宽大小	EIP对应带宽大小，单位：Mbit/s。 ● 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。	20 Mbit/s
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

参数	说明	取值样例
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。 **说明** VPN网关“计费模式”为“按需计费”场景下，若备EIP为按流量计费，强烈建议用户在云监控中配置告警规则对备EIP进行监控，避免因VPN连接故障、主链路切换至备链路导致的流量费用超支问题。 如何在云监控中对EIP配置告警规则，请参见《弹性公网IP用户指南》。	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	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	缺省情况下，VPN网关从关联的虚拟私有云的互联子网接入。当VPN网关需要从指定子网接入时设置。	选择“与互联子网一致”

步骤7 确认创建的VPN网关信息，单击“创建”。

----结束

3.1.1.2 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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，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、弹性公网IP、标签。
   - 私网类型网关：可查看基本信息、高级配置。

3.1.1.3 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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，单击目标VPN网关操作列的“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2两种类型。	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”。 包括虚拟私有云和企业路由器。	不支持
企业路由器	仅“关联模式”为“企业路由器”时需要设置。	不支持
虚拟私有云	选择需要和用户数据中心通信的VPC。	不支持

参数	说明	是否支持修改
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	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。	不支持

3.1.1.4 修改 VPN 网关规格

场景描述

VPN网关支持规格升降配，可以在VPN网关页面修改网关规格。以下产品规格升降配，实际情况以控制台显示为准。

- 专业型1和专业型2 VPN网关规格，支持相互变更。

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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，单击目标VPN网关操作列的“更多 > 修改规格”，或者单击操作列的“修改规格”。
6. 根据界面提示，完成修改网关规格操作。

3.1.1.5 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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，单击目标VPN网关操作列的“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”。

3.1.1.6 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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，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“确定”。

3.1.1.7 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EIP，删除VPN网关时会同步释放EIP。

  如果需要保留按需EIP，则您需要先将该EIP解绑，然后再删除VPN网关。如何解绑EIP，请参见**3.1.1.6 解绑弹性公网IP**。

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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，选择需要删除的VPN网关操作列的“更多 > 删除”，或者单击操作列的“删除”。

6. 在“删除VPN网关”的弹窗页，单击“一键输入”。
7. 单击“确定”。

说明

当共享带宽冻结时，EIP的行为以EIP资料为准。

3.1.1.8 按标签搜索 VPN 网关

场景描述

用户在使用VPN服务时，根据使用场景不同，可以将VPN资源按照特定规则进行分类，便于资源管理与费用计算。

VPN支持对接标签管理服务（Tag Management Service，简称TMS），通过给账号下VPN资源添加标签，可以对VPN资源进行自定义标记，实现资源的分类。已添加标签的VPN资源，用户可以在管理控制台对应位置，按照标签进行搜索。

前提条件

已为VPN资源添加标签。

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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，单击搜索框“选择属性筛选，或输入关键字搜索”，选择“资源标签 ”，添加筛选条件标签键值。
   - 此查询功能仅支持选择下拉列表中已存在的键和值。
   - 支持最多20个不同标签的组合搜索。如果输入多个标签，则不同标签之间为“与”的关系。
   - 支持标签和其他条件进行组合搜索。标签和其他搜索条件组合的搜索也是“与”的关系。

3.1.1.9 升级网关实例

升级概述

用户可以在VPN网关列表页，根据是否有升级按钮来判断您的VPN网关是否支持升级。

- 如果VPN网关没有显示升级按钮，则表示您当前的VPN网关不支持升级操作。
- 如果VPN网关有显示升级按钮，则表示您当前的VPN网关支持升级操作。

当升级状态处于“请确认是否完成升级”时，用户可以根据实际需要进行回退操作。

升级影响

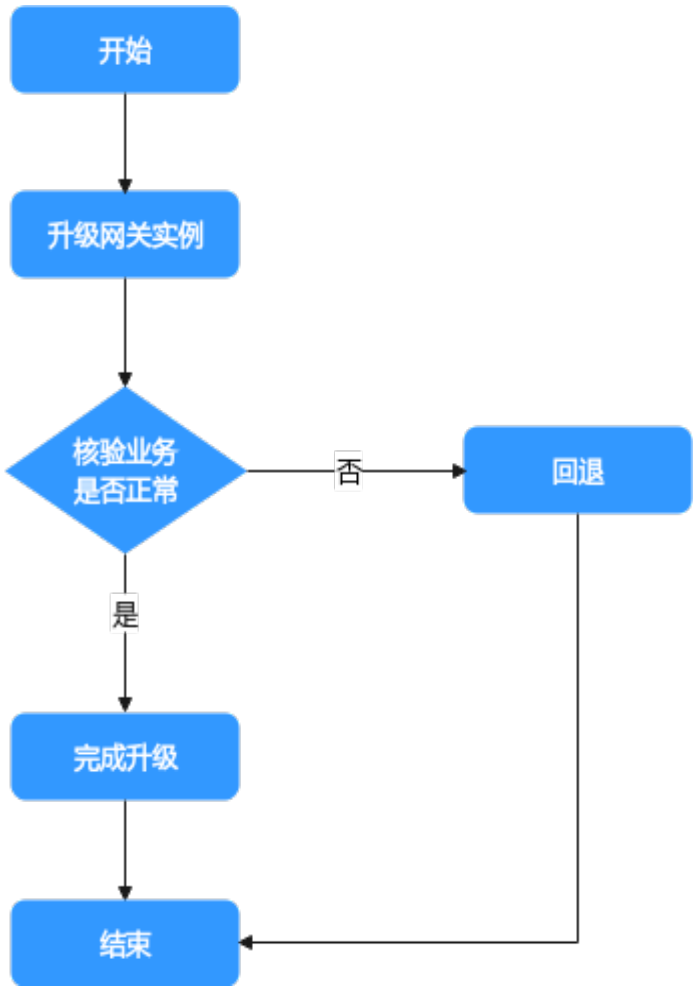
- 升级中VPN连接会出现中断，中断时间大约为10分钟。
- 升级中VPN网关以及其VPN连接均无法操作。

回退机制

升级后需要由您验证业务是否正常：业务有异常时可选择回退；业务正常时可选择完成升级，完成后不支持再回退到低版本。

操作步骤

图 3-1 升级流程示意图



步骤1 升级网关实例。

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“ > VPN”。
4. 在“站点入云VPN网关”界面，选择目标VPN网关，单击操作列的“升级网关实例”。

5. 在弹窗中了解升级影响和回退机制，勾选“我已知晓以上升级须知”后，单击确定。
6. 查看升级状态。实例升级过程中，可以在VPN网关列表页的状态列单击查看任务，查看升级进展。
   - 如果实例升级成功，网关状态会刷新为请确认是否完成升级，进入步骤2。
   - 如果实例升级失败，会自动回滚。可以在VPN网关列表页的右上方，查看失败信息。

步骤2 核验业务。

1. 核验业务正常，单击操作列的“完成升级”。

   须知

   单击“完成升级”后，升级任务无法回退，请谨慎选择。

2. 业务异常，单击操作列的“回退”，请提交工单联系工程师。

----结束

3.1.2 企业版对端网关管理

3.1.2.1 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。

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“ > 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3-4。

表 3-4 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

参数	说明	取值样例
BGP ASN	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
高级配置/标签	VPN服务的资源标签，包括键和值，最大可以创建20对标签。 标签设置时，可以选择预定义标签，也可以自定义创建。 预定义标签可以通过单击“查看预定义标签”进行查看。	-

7. （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。

3.1.2.2 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

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“ > 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，查看对端网关列表信息。
6. 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、标识、ID、BGP ASN、VPN连接。

3.1.2.3 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。

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“ > 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 3-5 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
高级配置/标签	VPN服务的资源标签，包括键和值。	支持
BGP ASN	BGP自治系统号码。	不支持
标识	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

3.1.2.4 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“ > 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“确定”。

3.1.2.5 按标签搜索对端网关

场景描述

用户在使用VPN服务时，根据使用场景不同，可以将VPN资源按照特定规则进行分类，便于资源管理与费用计算。

VPN支持对接标签管理服务（Tag Management Service，简称TMS），通过给账号下VPN资源添加标签，可以对VPN资源进行自定义标记，实现资源的分类。已添加标签的VPN资源，用户可以在管理控制台对应位置，按照标签进行搜索。

前提条件

已为VPN资源添加标签。

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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 单击搜索框“选择属性筛选，或输入关键字搜索”，选择“资源标签 ”，添加筛选条件标签键值。
   - 此查询功能仅支持选择下拉列表中已存在的键和值。
   - 支持最多20个不同标签的组合搜索。如果输入多个标签，则不同标签之间为“与”的关系。
   - 支持标签和其他条件进行组合搜索。标签和其他搜索条件组合的搜索也是“与”的关系。

3.1.3 企业版 VPN 连接管理

3.1.3.1 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“ > 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支持和对端网关创建一组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。

6. 根据界面提示配置参数，单击“立即购买”。

   VPN连接参数请参见表3-6。

表 3-6 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。	vpngw-001
连接1网关IP	• 当“网络类型”采用“公网”时，网关IP为VPN网关的主EIP。 • 当“网络类型”采用“私网”时，网关IP为VPN网关的主IP。 VPN网关对接同一对端网关时，不能选择已使用过的地址。	11.xx.xx.11
连接1对端网关	选择连接1对端网关。 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3-4。 **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
连接2网关IP	• 当“网络类型”采用“公网”、“HA模式”选择“双活”时，网关IP为VPN网关的主EIP2。 • 当“网络类型”采用“私网”、“HA模式”选择“双活”时，网关IP为VPN网关的主IP2。 • 当“网络类型”采用“公网”、“HA模式”选择“主备”时，网关IP为VPN网关的备EIP。 • 当“网络类型”采用“私网”、“HA模式”选择“主备”时，网关IP为VPN网关的备IP。 同一VPN网关和同一对端网关连接使用的网关IP不能相同。	11.xx.xx.12

参数	说明	取值样例
连接2对端网关	选择连接2对端网关。 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3-4。 **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
连接模式	IPsec连接的模式，支持路由模式和策略模式。 • 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。** **说明** 当创建双连接时，默认两个连接的连接模式、对端子网、分支互联开关（BGP路由模式）和策略规则（策略模式）一致。	静态路由模式

参数	说明	取值样例
对端子网	指需要通过VPN连接访问云上VPC的用户侧子网。 若存在多个对端子网，请用半角逗号（,）隔开。 **说明** • 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、100.64.0.0/12、214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 • 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。 • 当“关联模式”采用“企业路由器”，“连接模式”采用“BGP路由模式”和“策略模式”时，无需配置对端子网。	172.16.1.0/24,172.16.2.0/24
分支互联	“连接模式”采用“BGP路由模式”，支持分支互联功能。 • 开启 • 关闭 默认关闭。 **说明** 关闭时只发布本端子网路由。	关闭
策略规则	仅“连接模式”采用“策略模式”时需要配置。 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。 • 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。一个VPN连接最大支持5个源网段。 • 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50个目的网段，目的网段之间使用英文逗号（,）进行分隔。	• 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

参数	说明	取值样例
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥、策略配置和高级配置。	请根据实际设置
接口地址分配方式	仅“连接模式”采用“静态路由模式”和“BGP路由模式”时需要配置。 **说明** • 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 – 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自动生成。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 – 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

参数	说明	取值样例
本端隧道接口地址	仅“接口地址分配方式”采用“手动分配”时需要配置。 配置在VPN网关上的tunnel接口地址。	-
对端隧道接口地址	仅“接口地址分配方式”采用“手动分配”时需要配置。 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。	-
检测机制	仅“连接模式”采用“静态路由模式”时需要配置。 **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。	勾选
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。 取值范围： ● 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： – 数字。 – 大写字母。 – 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
策略配置	● 默认配置。 ● 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见**表3-7**和**表3-8**。 **说明** 当本端标识和对端标识类型为IP Address时，支持配置指定标识值，且本端ID与对端ID不能相同。	自定义配置

参数	说明	取值样例
标签	• VPN服务的资源标签，包括键和值，最大可以创建20对标签。 • 标签设置时，可以选择预定义标签，也可以自定义创建。 • 预定义标签可以通过单击“查看预定义标签”进行查看。	-
连接2配置	选择是否“与连接1保持一致”。 • 开启 • 关闭	开启

表 3-7 IKE 策略

参数	说明	取值样例
版本	IKE密钥交换协议版本，支持的版本： • 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） • v2。 默认配置为：v2。	v2
协商模式	仅“版本”采用“v1”时需要配置。 • Main。 • Aggressive。	Main
认证算法	认证哈希算法，支持的算法： • 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

参数	说明	取值样例
加密算法	加密算法，支持的算法： ● 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。 选择该加密算法时，IKE密钥交换协议版本只能为“v2”。 默认配置为：AES-128。	AES-128
DH算法	支持的算法： ● 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。 默认配置为：Group 15。	Group 15
生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 ● 单位：秒。 ● 取值范围：60~604800。 ● 默认配置为：86400。	86400

参数	说明	取值样例
本端标识	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。 ● IP Address（默认）。 – 系统自动读取VPN网关的网关IP作为IP Address，无需用户手动配置。 – 支持配置指定标识值，且本端ID与对端ID不能相同。 ● 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。	IP Address
对端标识	IPsec连接协商时，对端网关的鉴权标识。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。 ● 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。 – 支持配置指定标识值，且本端ID与对端ID不能相同。 ● 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。	IP Address

表 3-8 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： ● 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

参数	说明	取值样例
加密算法	加密算法，支持的算法： ● 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。 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完善的前向安全功能，配置IPsec隧道协商时使用。 PFS组支持的算法： ● 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。 默认配置为：DH group 15。	DH group 15
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： ESP。 默认配置为：ESP。	ESP

参数	说明	取值样例
生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 ● 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“创建”。

3.1.3.2 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。开启健康检查不会影响隧道连接。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“ > 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”。

3.1.3.3 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“ > 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。
6. 单击VPN连接的名称，查看VPN连接基本信息、策略配置和标签。
   - 当连接模式为静态路由模式时，基本信息包括VPN连接信息、健康检查信息。
   - 当连接模式为BGP路由模式时，基本信息包括VPN连接信息、健康检查信息。
   - 当连接模式为策略模式时，基本信息包括VPN连接信息、策略规则信息和健康检查信息。

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。
- 在VPN连接列表中，选择目标VPN连接所在行，单击“查看监控”，查看该VPN连接的监控信息。

  在监控视图中，“VPN连接状态”显示为“0”，表示VPN连接未连接；“VPN连接状态”显示为“1”，表示VPN连接已连接；“VPN连接状态”显示为“2”，表示VPN连接处于未知状态。
- 在VPN连接列表中，可以查看双连接的标识。名称/ID前的图标 表示一组对端网关相同的VPN连接，如果双连接在分页的边界处，只显示这组连接的一半标识 或 。

  当用户选择根据任意列排序时，不显示双连接标识。当取消排序后恢复双连接标识。
- 在VPN连接列表中，选择目标VPN连接所在行，单击“查看日志”，查看该VPN连接的ipsec协商日志。

  当VPN连接状态显示“未连接”时，可以根据该VPN连接的日志详情来判断VPN未连接的原因。
- 在VPN连接页面，可以看到“导出”和设置按钮。
  - 选择左上方的“导出”，在下拉框中选择需要导出的数据。
  - 单击右上方的 ，根据需要设置自定义显示列。

3.1.3.4 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

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“ > 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，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”。
6. 根据界面提示修改VPN连接的配置参数。
   - BGP路由模式创建的VPN连接支持在“修改连接信息”界面修改“分支互联”的开关。
7. 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3-9所示。

表 3-9 生效机制

场景	参数	生效机制	操作方法
-	预共享密钥	• 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。	• 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 1. 删除当前VPN连接。 2. 重新创建VPN连接。
IKE策略（版本为v1）	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		
	协商模式		
	本端标识		
	对端标识		

场景	参数	生效机制	操作方法
	生命周期		
	版本	修改后立即生效。	
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。	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 3-10 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	用户数据中心中需要和VPC通信的子网。	支持

参数	说明	是否支持修改
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
分支互联	“连接模式”采用“BGP路由模式”，支持分支互联功能。	支持
弹性公网IP	仅“网络类型”采用“公网”时需要配置。	不支持
私网IP	仅“网络类型”采用“私网”时需要配置。	不支持
VPN网关	已创建的VPN网关。	不支持
标识	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
接口地址分配方式	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

3.1.3.5 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“ > 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. 在“删除VPN连接”的弹窗页，单击“一键输入”。
7. 单击“确定”。

3.1.3.6 重置 VPN 连接

场景描述

当用户在使用过程中遇到问题时，可以尝试重置VPN连接以解决该问题。

约束与限制

- 当VPN连接的状态处于“未连接”、“正常”、“未知”时，可以进行重置操作。
- VPN连接是否支持重置操作，以管理控制台实际界面为准。

注意

重置操作会导致该VPN连接中断，请谨慎操作。

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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在目标VPN连接所在行的操作列，单击确定。
6. 查看VPN连接状态。
   在VPN连接页面的状态列，该连接的状态会显示为“重置中”或“未连接”。

注意

重置1分钟后，当VPN连接状态显示为“未连接”时，需要手动刷新页面。
如果刷新后连接状态仍显示为“未连接”，则表示该连接未协商成功，请参见**VPN连接状态显示“未连接”**。

3.1.3.7 查看 VPN 连接日志

场景描述

当VPN连接协商成功或失败时，会生成日志信息，用户可以通过查看连接日志排查VPN连接的故障。

约束与限制

VPN连接的连接日志支持查看最近的200条日志信息。

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“ > 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，找到目标VPN连接，单击“查看日志”，查看相关日志信息。

   在查看日志的弹窗中，可以导出时间和信息的日志数据。

3.1.3.8 按标签搜索 VPN 连接

场景描述

用户在使用VPN服务时，根据使用场景不同，可以将VPN资源按照特定规则进行分类，便于资源管理与费用计算。

VPN支持对接标签管理服务（Tag Management Service，简称TMS），通过给账号下VPN资源添加标签，可以对VPN资源进行自定义标记，实现资源的分类。已添加标签的VPN资源，用户可以在管理控制台对应位置，按照标签进行搜索。

前提条件

已为VPN资源添加标签。

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“ > VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 单击搜索框“选择属性筛选，或输入关键字搜索”，选择“资源标签 ”，添加筛选条件标签键值。
   - 此查询功能仅支持选择下拉列表中已存在的键和值。
   - 支持最多20个不同标签的组合搜索。如果输入多个标签，则不同标签之间为“与”的关系。
   - 支持标签和其他条件进行组合搜索。标签和其他搜索条件组合的搜索也是“与”的关系。

3.2 站点入云 VPN 经典版

3.2.1 经典版 VPN 网关管理

3.2.1.1 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. 在页面左上角单击 图标，选择区域，选择“网络 > 虚拟专用网络VPN”。
   进入虚拟专用网络页面。
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“Create Now”。VPN网关参数请参见**表 VPN网关参数说明**

表 3-11 VPN 网关参数说明

参数	说明	取值样例
计费模式	VPN网关支持按需计费计费模式。 按需计费：购买VPN网关时，可以同时购买一条与其相关联的VPN连接。	按需计费
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

表 3-12 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： ● 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。	-
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： ● 取值长度：6~128个字符。 ● 只能包括以下几种字符： – 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	● 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 3-13 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： ● 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： ● 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	● 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。 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（有安全风险不推荐） ● v2 默认配置为：v2。	v2
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

表 3-14 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： ● 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： ● 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
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。 ● 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 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： ● ESP ● AH ● AH-ESP 默认配置为：ESP。	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”。

3.2.1.2 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. 在页面左上角单击 图标，选择区域，选择“网络 > 虚拟专用网络VPN”。进入虚拟专用网络页面。
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。

3.2.1.3 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. 在页面左上角单击 图标，选择区域，选择“网络 > 虚拟专用网络VPN”。进入虚拟专用网络页面。
5. 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”。
6. 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”。
7. 根据界面参数，修改VPN网关的带宽，或者名称和描述信息。
8. 单击确定。

修改 VPN 网关基本信息

操作场景：

用户根据需要修改VPN网关名称和描述信息。

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，选择区域，选择“网络 > 虚拟专用网络VPN”。进入虚拟专用网络页面。
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”界面目标VPN网关所在行，选择“更多 > 修改基本信息”。
6. 根据界面参数，修改VPN网关的名称和描述信息。

   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。
7. 单击“确定”。

修改 VPN 网关带宽

操作场景：

当VPN网关带宽不能满足需求时，可修改VPN网关带宽。

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. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在页面左上角单击 图标，选择区域，选择“网络 > 虚拟专用网络VPN”。进入虚拟专用网络页面。
5. 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”。
6. 在“VPN网关”界面目标VPN网关所在行，单击“修改带宽”。
7. 根据界面参数，重新选择合适的带宽。
8. 单击“提交”。

修改 VPN 网关规格

操作场景：

当VPN网关所关联的VPN连接数不能满足需求时，可修改VPN网关规格。

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，选择区域，选择“网络 > 虚拟专用网络”。
   进入虚拟专用网络页面。
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“经典版-VPN网关”界面目标VPN网关所在行，选择“更多 > 修改规格”。
6. 根据界面参数，重新输入此VPN网关可以关联的VPN连接数。
7. 单击“提交”。

   说明

   修改VPN网关的规格时，VPN连接数只支持增加连接数。

3.2.1.4 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. 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，选择区域，选择“网络 > 虚拟专用网络VPN”。
   进入虚拟专用网络页面。
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“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”。
6. 单击“是”。

3.2.2 经典版 VPN 连接管理

3.2.2.1 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. 在页面左上角单击 图标，选择区域，选择“网络 > 虚拟专用网络VPN”。
   进入虚拟专用网络页面。
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“立即购买”。VPN连接参数请参见**表 VPN连接参数说明**。

表 3-15 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，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。	-
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

参数	说明	取值样例
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： ● 取值长度：6~128个字符。 ● 只能包括以下几种字符： – 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	● 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 3-16 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： ● 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	加密算法，支持的算法： ● 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	● 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： ● v1（有安全风险不推荐） ● v2 默认配置为：v2。	v2
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

表 3-17 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： ● 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： ● 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
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。 ● 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 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

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

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。

3.2.2.2 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. 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，选择区域，选择“网络 > 虚拟专用网络VPN”。
   进入虚拟专用网络页面。
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”。单击“VPN连接”页签。
5. 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。

3.2.2.3 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. 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，选择区域，选择“网络 > 虚拟专用网络VPN”。
   进入虚拟专用网络页面。
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”。单击“VPN连接”页签。
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。

   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。
7. 单击“确定”。

3.2.2.4 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. 在页面左上角单击 图标，选择区域，选择“网络 > 虚拟专用网络”。
   进入虚拟专用网络页面。
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”。单击“VPN连接”页签。
5. 在“VPN连接”界面所需删除的VPN连接所在行，选择“更多 > 删除”。
6. 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。

相关链接：

更多关于监控的信息，请参见《 云监控用户指南 》。

3.3.2 支持的监控指标（站点入云 VPN 企业版）

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 3-18 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	单位	进制	测量对象（维度）	监控周期（原始指标）
gateway_send_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	不涉及	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	不涉及	网关	1分钟
gateway_send_rate	出云带宽	该指标用于统计测量对象平均每秒出云流量。	0-1	bps	1024(IEC)	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。	0-1	bps	1024(IEC)	网关	1分钟
gateway_send_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。	0-100	percentage(%)	不涉及	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。	0-100	percentage(%)	不涉及	网关	1分钟
gateway_connection_num	连接数	该指标用于统计测量对象关联VPN连接数。	≥ 0	count	不涉及	网关	1分钟

表 3-19 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	单位	进制	测量对象（维度）	监控周期（原始指标）
tunnel_average_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。	0~5000	ms	不涉及	VPN连接	15s
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。	0~5000	ms	不涉及	VPN连接	15s
tunnel_packet_loss_rate	隧道丢包率	VPN网关与对端网关之间隧道的丢包率。	0~100	percentage(%)	不涉及	VPN连接	15s
link_average_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。	0~5000	ms	不涉及	VPN连接	15s
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	不涉及	VPN连接	15s
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	percentage(%)	不涉及	VPN连接	15s
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	不涉及	不涉及	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	不涉及	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	不涉及	VPN连接	1分钟
recv_rate	接收速率	平均每秒接收流量。	0~1	bps	1024(IEC)	VPN连接	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
send_rate	发送速率	平均每秒发送流量。	0~1	bps	1024(IEC)	VPN连接	1分钟
sa_send_pkt_rate	SA发送包速率	平均每秒发送的数据包数量。	≥ 0	pps	不涉及	VPN连接SA	1分钟
sa_recv_pkt_rate	SA接收包速率	平均每秒接收的数据包数量。	≥ 0	pps	不涉及	VPN连接SA	1分钟
sa_recv_rate	SA接收速率	平均每秒接收流量。	0~1	bps	1024(IEC)	VPN连接SA	1分钟
sa_send_rate	SA发送速率	平均每秒发送流量。	0~1	bps	1024(IEC)	VPN连接SA	1分钟

维度

key	Value
evpn_connection_id	企业版**站点入云VPN**连接
evpn_sa_id	企业版**站点入云VPN**连接sa
evpn_gateway_id	企业版**站点入云VPN**网关

3.3.3 支持的监控指标（站点入云 VPN 经典版）

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 3-20 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	单位	进制	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）。	≥ 0	bit/s	1000(SI)	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）。	≥ 0	bit/s	1000(SI)	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。 出网带宽使用率=出网带宽指标/购买的带宽大小。	0-100	%	不涉及	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。 入网带宽使用率=入网带宽指标/购买的带宽大小。 **说明** • 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	%	不涉及	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）。	≥ 0	Byte	1000(SI)	带宽或弹性公网IP	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
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）。	≥ 0	Byte	1000(SI)	带宽或弹性公网IP	1分钟

维度

key	Value
publicip_id	弹性公网IP ID
bandwidth_id	带宽ID

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。支持查看“近15分钟”、“近30分钟”、“近1小时”、“近2小时”、“近3小时”、“近12小时”、“近24小时”、“近7天”、“近30天”或自定义时间段的数据。

背景信息

表 3-21 背景信息

监控指标名称	VPN支持情况	是否默认开启
VPN连接状态	企业版VPN、经典版VPN均支持。	是

监控指标名称	VPN支持情况	是否默认开启
• 链路往返平均时延 • 链路往返最大时延 • 链路丢包率 • 接收包速率 • 发送包速率 • 接收速率 • 发送速率 • SA接收包速率 • SA发送包速率 • SA接收速率 • SA发送速率	仅企业版VPN支持。	否 单击VPN连接名称，在“基本信息”页签添加健康检查项。
• 隧道往返平均时延 • 隧道往返最大时延 • 隧道丢包率	仅企业版VPN支持。	是 仅VPN连接使用静态路由模式，且开启NQA检测机制场景时支持私网相关监控指标。

查看 VPN 网关监控指标

- 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 图标，选择区域和项目。
  c. 在页面左上角单击 图标，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. 单击对应的VPN网关操作列的“查看监控指标”，查看VPN网关状态。
     支持查看“近15分钟”、“近30分钟”、“近1小时”、“近2小时”、“近3小时”、“近12小时”、“近24小时”、“近7天”、“近30天”或自定义时间段的数据。

3.3.5 创建监控告警规则

操作场景

通过设置监控告警规则，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 图标，选择区域和项目。
3. 在页面左上角单击图标，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 VPN”，根据不同告警类型在不同页签下配置告警规则。
   - 站点入云VPN企业版对应的VPN网关告警，单击“企业版站点入云VPN网关”，单击操作列的“创建告警规则”进行配置。
   - 站点入云VPN企业版对应的VPN连接告警，单击“企业版站点入云VPN连接”，单击操作列的“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”。

   虚拟专用网络监控告警规则设置完成后，如果您已启用告警通知，并配置了所需的参数时，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 》。

3.4 审计

3.4.1 支持审计的关键操作列表

表 3-22 站点入云 VPN 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
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
更新按需VPN网关规格	vpn-gateway	updatePostpaidVgwSpecification
创建虚拟专用网络连接	vpn-connection	createVpnConnection

操作名称	资源类型	事件名称
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
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	vpn-gateway	showVgw
查询VPN网关可用区	availability_zone	listAvailabilityZones
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-gateway	listVgws
查询VPN连接监控	connection-monitor	showConnectionMonitor
查询VPN连接监控列表	connection-monitor	listConnectionMonitors
查询指定租户配额	quota	showQuotasInfo
查询VPN连接日志	vpn-connection	showVpnConnectionLog
批量创建VPN连接	vpn-connection	batchCreateVpnConnection
重置VPN连接	vpn-connection	resetVpnConnection
升级站点入云VPN网关	vpn-gateway	upgradeVpnGateway
查询站点入云VPN网关任务列表	job	listVpnGatewayJobs

操作名称	资源类型	事件名称
删除站点入云VPN网关任务	job	deleteVpnGatewayJob
创建VPN连接监控	connection-monitor	createConnectionMonitor
删除VPN连接监控	connection-monitor	deleteConnectionMonitor

3.4.2 查看云审计日志

用户进入云审计服务创建管理类追踪器后，系统开始记录VPN资源的操作。云审计服务管理控制台会保存最近7天的操作记录。

相关链接：

如何查看审计日志，请参见《云审计服务用户指南》。

3.5 权限管理

3.5.1 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。

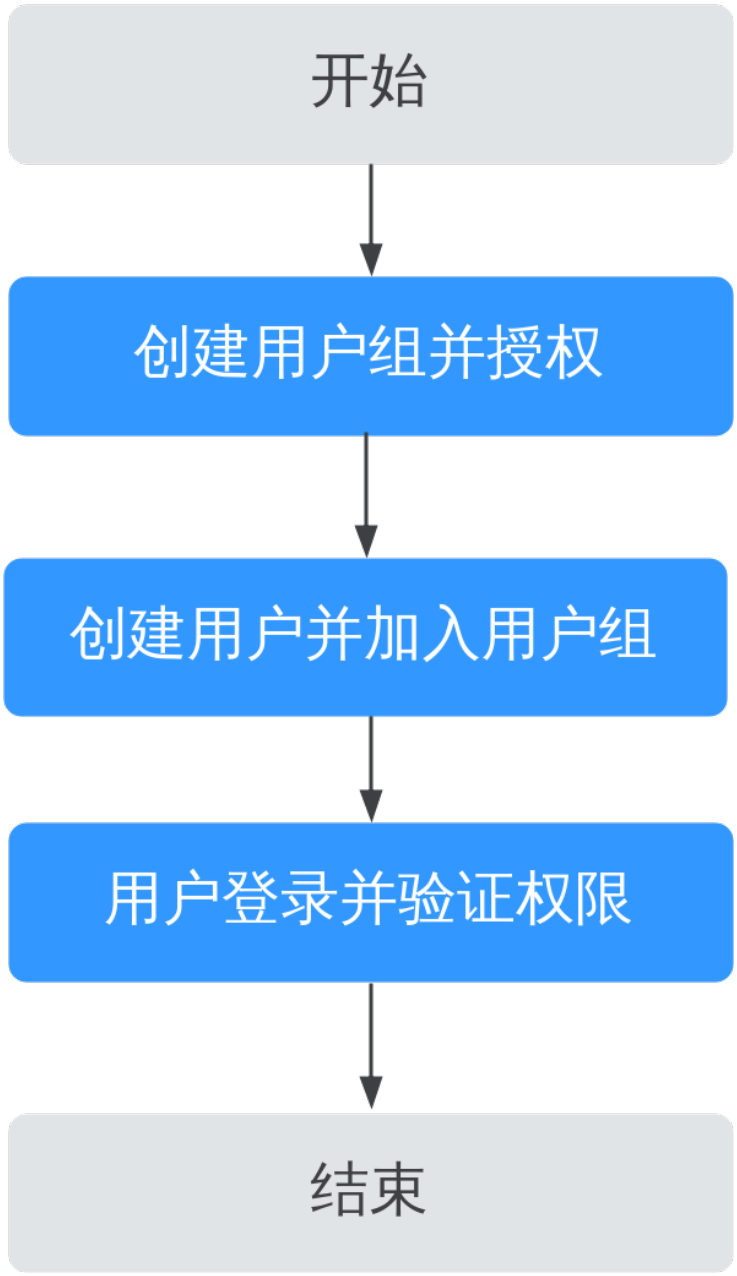
本章节为您介绍对用户授权的方法，操作流程如**图3-2**所示。

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**系统权限**。

示例流程

图 3-2 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：
   - 在页面左上角单击☰图标，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，在“站点入云VPN网关”页签，单击

右上角“创建站点入云VPN网关”，尝试创建VPN网关，如果创建成功，表示“VPN FullAccess”已生效。

- 在页面左上角单击☰图标，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。
- 在页面左上角单击☰图标，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。

3.5.2 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。

目前云服务平台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：**创建自定义策略**。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

  需要添加如下依赖的授权项，如果不添加依赖的授权项，可能会出现异常。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpn:vpnGateways:delete"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "vpc:subNetworkInterfaces:update",
                "vpc:routeTables:update",
                "vpc:subnets:delete",
                "vpc:publicIps:list",
                "vpc:publicIps:delete",
                "vpc:vpcs:get",
                "vpc:routeTables:get",
                "vpc:ports:get",
                "vpc:publicIps:update",
                "vpc:subnets:get",
                "vpc:bandwidths:list",
                "vpc:publicIps:get",
                "vpc:vpcs:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "er:instances:get",
                "er:instances:list"
            ]
        }
```

```
    ]
}
```

- 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:vpnConnections: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"
            ]
        }
    ]
}
```

4 最佳实践

4.1 站点入云 VPN 企业版

4.1.1 通过 VPN 实现云上云下网络互通（双活模式）

4.1.1.1 方案概述

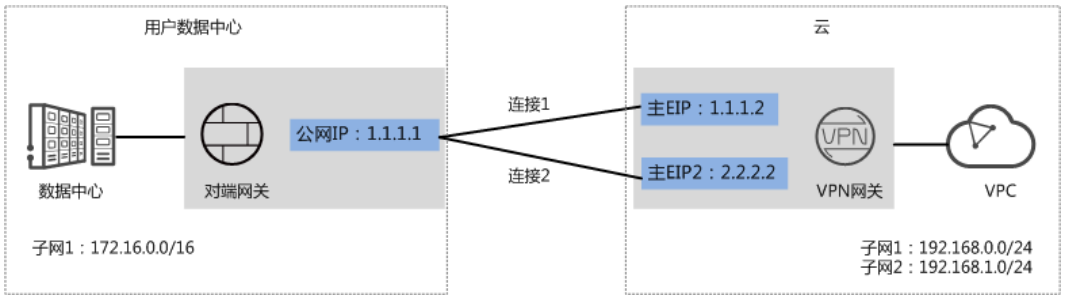
应用场景

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之间采用一组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。

4.1.1.2 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	• 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： • 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
VPN连接	“连接1配置”中的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。 • 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30
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
IKE/IPsec策略	预共享密钥	Test@123

类别	规划项	规划值
	IKE策略	• 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	• 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

4.1.1.3 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》。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 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“创建站点入云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”。 关联ER场景时，请选择“企业路由器”。	虚拟私有云
企业路由器	仅关联场景为“企业路由器”时需要选择。	er-001
虚拟私有云	选择用于分配互联子网的VPC。 关联场景为“企业路由器”时，该VPC可以对接ER，也可以不对接ER。	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
标识	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VPN连接参数，单击“立即购买”。
   VPN连接参数说明如**表 VPN连接参数说明**所示。

表 4-4 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
连接1网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请提交工单申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 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。	169.254.70.1/30

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。	169.254.71.1/30
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
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.70.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

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。

4.1.2 通过 VPN 实现云上云下网络互通（主备模式）

4.1.2.1 方案概述

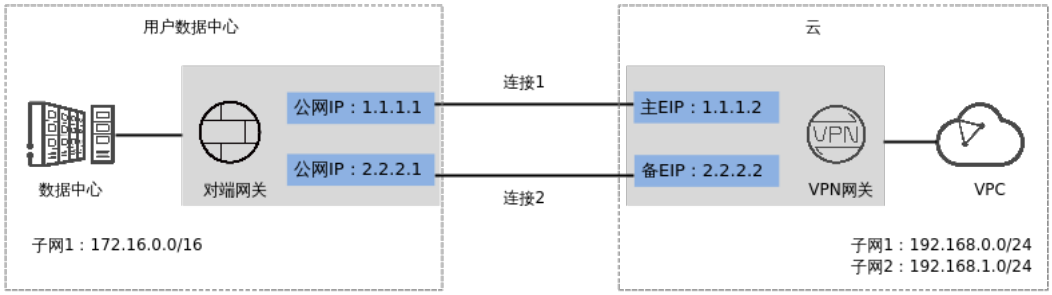
应用场景

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之间采用一组VPN连接保证网络可靠性，连接1和连接2互为主备。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。

4.1.2.2 组网和资源规划

数据规划

表 4-5 规划数据

类别	规划项	规划值
VPC	待互通子网	• 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

类别	规划项	规划值
	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： ● 主EIP：1.1.1.2 ● 备EIP：2.2.2.2
VPN连接	“连接1配置”中的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。 ● 本端隧道接口地址：169.254.70.1/30 ● 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	● 本端隧道接口地址：169.254.71.1/30 ● 对端隧道接口地址：169.254.71.2/30
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 ● 2.2.2.1
IKE/IPsec策略	预共享密钥	Test@123
	IKE策略	● 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	● 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

4.1.2.3 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》。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 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“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如表4-6所示。

表 4-6 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”。 关联ER场景时，请选择“企业路由器”。	虚拟私有云
企业路由器	仅关联场景为“企业路由器”时需要选择。	er-001
虚拟私有云	选择用于分配互联子网的VPC。 关联场景为“企业路由器”时，该VPC可以对接ER，也可以不对接ER。	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

参数	说明	取值参数
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4-7所示。

表 4-7 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
标识	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VPN连接参数，单击“立即购买”。
   VPN连接参数说明如表4-8所示。

表 4-8 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
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2

参数	说明	取值参数
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的备EIP。	2.2.2.2
连接2对端网关	选择连接2对端网关。	2.2.2.1
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请提交工单申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 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。	169.254.70.1/30
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。	169.254.70.2/30
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

参数	说明	取值参数
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

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。

4.1.3 通过 VPN Hub 实现云下多分支网络互通

4.1.3.1 方案概述

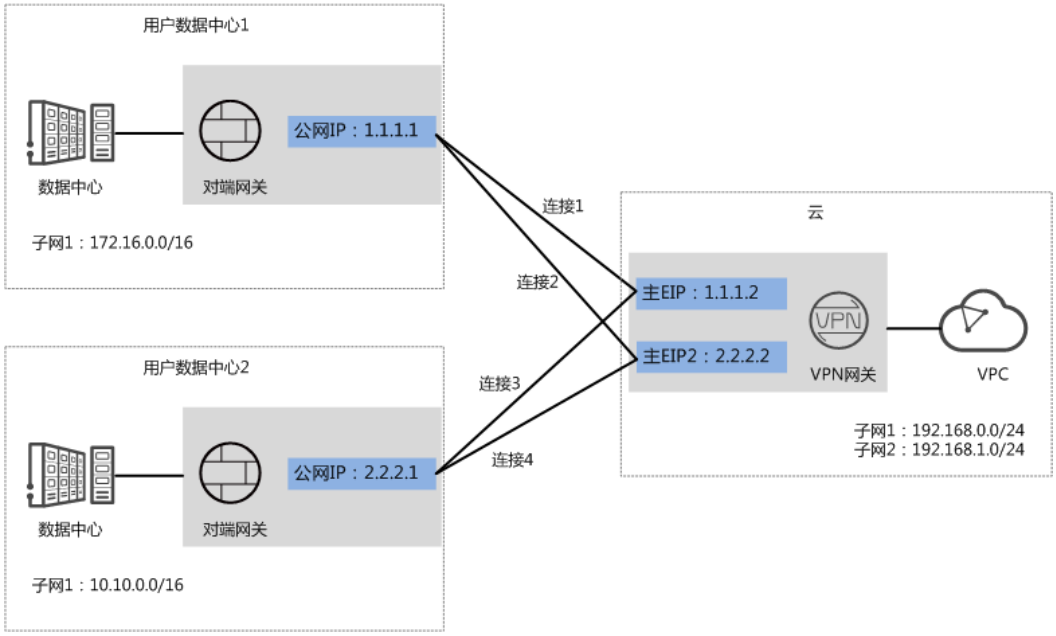
场景描述

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 组网方案**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。

4.1.3.2 组网和资源规划

数据规划

表 4-9 规划数据

类别	规划项	规划值
VPC	待互通子网	• 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

类别	规划项	规划值
	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： ● 主EIP：1.1.1.2 ● 主EIP2：2.2.2.2
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
用户数据中心1VPN连接	“连接1配置”中的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。 ● 本端隧道接口地址：169.254.70.1/30 ● 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	● 本端隧道接口地址：169.254.71.1/30 ● 对端隧道接口地址：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
用户数据中心2VPN连接	“连接1配置”中的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。 ● 本端隧道接口地址：169.254.72.1/30 ● 对端隧道接口地址：169.254.72.2/30
	“连接2配置”中的Tunnel接口地址	● 本端隧道接口地址：169.254.73.1/30 ● 对端隧道接口地址：169.254.73.2/30
IKE/IPsec策略	预共享密钥	Test@123

类别	规划项	规划值
	IKE策略	• 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	• 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

4.1.3.3 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》。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 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“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如**表4-10**所示。

表 4-10 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4-11**所示。

表 4-11 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
标识	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VPN连接参数，单击“立即购买”。
   VPN连接参数说明如**表4-12**所示。

表 4-12 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
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
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，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请提交工单申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 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。	169.254.70.1/30
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。	169.254.70.2/30
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”

参数	说明	取值参数
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
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

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VPN连接参数，单击“立即购买”。
   VPN连接参数说明如表4-13所示。

表 4-13 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
VPN网关	选择VPN网关。	vpngw-001
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	2.2.2.1
连接2网关IP	选择VPN网关的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	2.2.2.1
连接模式	选择“静态路由模式”。	静态路由模式

参数	说明	取值参数
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、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请提交工单申请。	10.10.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 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。	169.254.72.1/30
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。	169.254.72.2/30
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
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.73.1/30

参数	说明	取值参数
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.73.2/30

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。

4.2 站点入云 VPN 经典版

4.2.1 通过 VPN 连接云下数据中心与云上 VPC

操作场景

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VPN功能。申请VPN后，用户需要配置安全组并检查子网的连通性，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内弹性云服务器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。

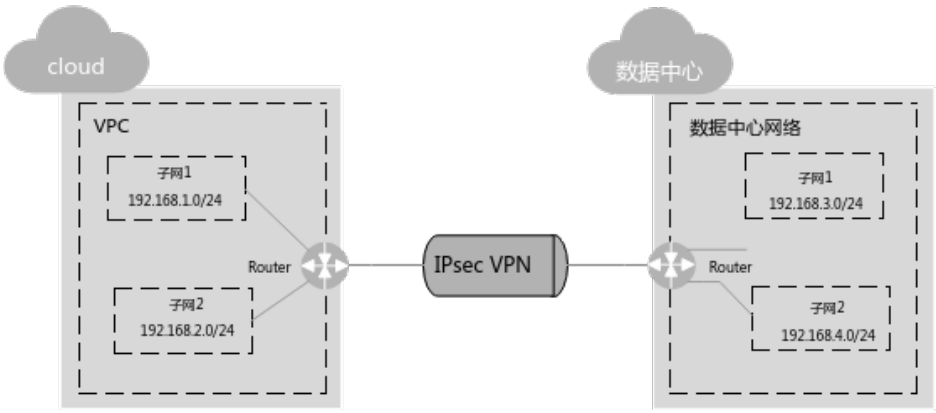
操作步骤

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4-4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 4-4 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. 为弹性云服务器配置安全组规则，允许通过VPN进出用户数据中心的报文。
4. 检查VPC安全组。

   从用户数据中心ping云服务器，验证安全组是否允许通过VPN进出用户数据中心的报文。

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 故障排除

5.1 站点入云 VPN 企业版

5.1.1 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。
- IPsec-VPN连接协商失败或连接断连。

处理步骤

1. 检查VPN连接两端的连接配置。
   a. 确认两端配置的网关IP参数是否为镜像。
      i. 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。
      ii. 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”，在标识栏下查看。
         - 如果两端配置的网关IP参数不是镜像，请修改对应参数。
         - 如果两端配置的网关IP参数是镜像，请继续步骤**b**。
   b. 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。
      如果IKE策略、IPsec策略协商参数不一致，请修改对应策略。
      如果IKE策略、IPsec策略协商参数一致，请继续步骤**c**。
   c. 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。

d. 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。

e. 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。

- 查看是否开启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。

f. 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。

2. 检查安全组和客户设备侧ACL配置。

a. 确认default安全组已经放通客户设备侧公网IP的端口。

b. 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。

c. 确认客户设备侧ACL已经放通VPN网关主备EIP的端口。

3. 查看IPsec连接日志。

a. 登录管理控制台。

b. 在管理控制台左上角单击 图标，选择区域和项目。

c. 在页面左上角单击图标，选择“ > VPN”。

d. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。

e. 在“VPN连接”界面，找到目标VPN连接，单击“查看日志”，查看相关日志信息。

查看IPsec连接日志的过程中，您可以根据日志关键字对照**表 VPN未连接的常见原因**中的错误码自主排查问题。

表 5-1 VPN 未连接的常见原因

分类	错误码	描述
IPsec-VPN连接协商失败	phase1 proposal mismatch	两端IKE安全提议参数不匹配。
	phase2 proposal or pfs mismatch	两端IPSec安全提议参数、PFS算法或Security ACL不匹配。
	responder dh mismatch	响应方的DH算法不匹配。
	initiator dh mismatch	发起方的DH算法不匹配。
	encapsulation mode mismatch	封装模式不匹配。
	flow mismatch	两端Security ACL不匹配。
	version mismatch	两端IKE版本号不匹配。
	peer address mismatch	两端的IKE Peer地址不匹配。
	config ID mismatch	根据ID未找到匹配的IKE Peer。
	exchange mode mismatch	两端的协商模式不匹配。
	authentication fail	身份认证失败。
	construct local ID fail	构造本端ID失败。
	rekey no find old sa	重协商时找不到旧的SA。
	rekey fail	重协商时旧的SA正在下线。
	first packet limited	首包限速。
	unsupported version	不支持的IKE版本号。
	malformed message	畸形消息。
	malformed payload	畸形载荷。
	critical drop	未识别的critical载荷。
	cookie mismatch	Cookie不匹配。
	invalid cookie	无效Cookie。
	invalid length	报文长度非法。
	unknown exchange type	未知的协商模式。
	short packet	超短包。
	unknown exchange type	未知的协商模式。
	uncritical drop	未识别的非critical载荷。

分类	错误码	描述
	route limit	路由注入的数目达到规格。
	ip assigned fail	IP地址分配失败。
	eap authentication timeout	EAP认证超时。
	eap authentication fail	EAP认证失败。
	xauth authentication fail	XAUTH认证失败。
	xauth authentication timeout	XAUTH认证超时。
	license or specification limited	License限制。
	local address mismatch	IKE协商时的本端IP地址和接口IP地址不匹配。
	dynamic peers number reaches limitation	IKE对等体数达到规格。
	ipsec tunnel number reaches limitation	IPSec隧道数达到规格。
	netmask mismatch	开启IPSec掩码过滤功能后，掩码不匹配。
	flow conflict	数据流冲突。
	proposal mismatch or use sm in ikev2	IPSec安全提议不匹配或者IKEv2使用SM算法。
	ikev2 not support sm in ipsec proposal ikev2	IKEv2不支持IPSec安全提议的SM算法。
	no policy applied on interface	没有策略应用到接口上。
	nat detection fail	NAT探测失败。
	fragment packet limit	分片报文超规格。
	fragment packet reassemble timeout	分片报文重组超时。
	peer cert is expired	对端证书过期。
	peer cert is revoked by CRL	对端证书被吊销。
	sa with same user exists	相同用户已存在sa。
	max transmit reached	重传报文达到最大次数。

分类	错误码	描述
IPsec-VPN连接断连	dpd timeout	DPD探测超时。
	peer request	对端发送删除消息。
	config modify or manual offline	修改配置导致SA被删除或者手动清除SA。
	phase1 hard expiry	第一阶段硬超时（没有新的SA协商成功）。
	phase2 hard expiry	第二阶段硬超时。
	heartbeat timeout	heartbeat探测超时。
	re-auth timeout	重认证超时导致SA被删除。
	aaa cut user	AAA模块强制用户下线导致SA被删除。
	ip address syn failed	IP地址同步失败。
	hard expiry triggered by port mismatch	NAT端口不匹配导致硬超时。
	kick old sa with same flow	相同的流接入时删除老的SA。
	cpu table updated	插拔SPU板时删除非本CPU的SA。
	flow overlap	加密流中的IP地址与对端的IP地址冲突。
	spi conflict	SPI冲突。
	admin down	VPN隧道的管理down。
	peer address switch	对端地址变化。
	forward down	fwd群组down。
	sa with same user exists	相同用户已存在sa。
	reset sa by ike user	用户重置sa下线。
	phase1 sa replace	新IKE SA替换老的IKE SA。
	phase2 sa replace	新IPSec SA替换老的IPSec SA。
	manual offline	手动下线。
	nhrp notify	NHRP通知删除SA。
	receive backup delete info	备机收到主机的SA备份删除消息。
	eap delete old sa	对端设备重复进行EAP认证时本端设备删除老的SA。

分类	错误码	描述
	receive invalid spi notify	收到无效SPI通知。
	dns resolution status change	DNS解析状态发生改变。
	ikev1 phase1-phase2 sa dependent offline	设备删除IKEv1 SA时删除其关联的IPSec SA。
	exchange timeout	报文交互超时。
	hash gene adjusted	Hash因子调整导致IPSec隧道被删除。

5.1.2 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

1. 检查安全组配置。
   a. 确认default安全组已经放通去往对端子网数据流。
   b. 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。
   c. 确认default安全组已经放通来自对端子网数据流。
   d. 确认default安全组已经放通去往本端子网数据流。
   e. 确认default安全组已经放通来自本端子网数据流。
   f. 确认ECS所在的安全组已经放通去往对端子网数据流。
   g. 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。
   h. 确认ECS所在的安全组已经放通来自对端子网数据流。

2. 互联子网的ACL规则配置不正确。
   a. 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端口。
3. 检查客户设备侧放通策略。
   a. 确认客户设备侧已经放通去往VPN本端子网的数据流。
   b. 确认客户设备侧已经放通来自VPN本端子网的数据流。
4. 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. 检查客户设备侧路由配置。
   a. 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。
   b. 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。
   c. 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。

5.1.3 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云侧。
  - 使用客户侧VPN网关地址Ping云侧VPN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。
- 检查云侧组网和带宽情况
  - 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 站点入云 VPN 企业版

6.1.1 热点问题

6.1.1.1 VPN 协商参数有哪些？默认值是什么？

表 6-1 VPN 协商参数

协议	配置项	值
IKE	认证算法	• 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（默认） • SHA2-384 • SHA2-512
	加密算法	• 3DES（此算法安全性较低，请慎用） • AES-128（默认） • AES-192 • AES-256 • AES-256-GCM-16

协议	配置项	值
	DH算法	• 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（默认） • Group 16 • Group 19 • Group 20 • Group 21
	版本	• v1（有安全风险不推荐） • v2（默认）
	生命周期	86400（默认） 单位：秒。 取值范围：60-604800。
	本端标识	• IP Address 本端IP地址由系统自动关联显示，无需用户手动配置。 • FQDN 默认的本端标识类型是IP Address，ID值是VPN网关的公网IP。
	对端标识	• IP Address • FQDN 默认的对端标识类型是IP Address，ID值是对端网关的公网IP。
IPsec	认证算法	• 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（默认） • SHA2-384 • SHA2-512

协议	配置项	值
	加密算法	• AES-128（默认） • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） • AES-256-GCM-16
	PFS	• 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（默认） • DH group 16 • DH group 19 • DH group 20 • DH group 21
	传输协议	• ESP（默认）
	生命周期	3600（默认） 单位：秒。 取值范围：30-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

  IKE协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致IPsec VPN受到侵犯。为提升密钥管理的安全性，IKE提供了PFS（完美向前保密）功能。启用PFS后，在进行IPsec SA协商时会进行一次附加的DH交换，重新生成新的IPsec SA密钥，提高了IPsec SA的安全性。
- 为了增强安全性，默认开启PFS，请确认用户侧数据中心网关设备也开启了该功能，且两端配置保持一致，否则会导致协商失败。
- IPsec SA字节生命周期，不是VPN网关服务可配置参数，云侧采用的是默认配置1843200KB。该参数不是协商参数，不影响双方建立IPsec SA。

6.1.1.2 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 网关实现互联?

可以。

VPN连通的是两个子网，即云上VPC网络与用户数据中心网络。

VPN成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是IPsec VPN的典型场景，请用户放心使用。

同时VPN连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通VPN以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行ping，获取网络的丢包和时延情况。

6.1.1.3 是否可以通过 VPN 实现跨境访问网站?

不可以。

VPN实现的是将云上的VPC子网和用户侧数据中心的IDC网络打通的场景，即站点与站点互通（site to site）。

6.1.1.4 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连接创建后即会向云监控服务CES上报状态信息，但是并不会自动向用户发送告警通知，需要在页面左上角单击三图标，选择“管理与监管 > 云监控”创建告警规则。

6.1.1.5 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。

6.1.1.6 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

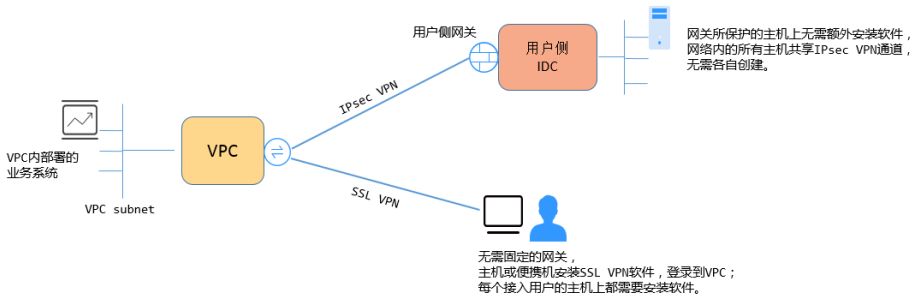
IPsec VPN：连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网；即IPsec VPN是网对网的连接。

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。

6.1.1.7 IPsec VPN 是否会自动建立连接?

支持自动建立连接。

6.1.1.8 VPN 网关删除后公网地址是否可以保留?

按需VPN网关如果绑定了按需EIP，则VPN网关删除后会同步删除绑定的按需EIP。

如果需要保留EIP，请在删除VPN网关前对EIP进行解绑操作。

6.1.1.9 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。

6.1.1.10 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么?

云上用户购买的VPN网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

- 如果所购买的带宽<=10Mbit，则入云方向统一限定为10Mbit。

- 如果所购买的带宽>10Mbit，则入云方向与购买的带宽一致。

按带宽计费度量采用国际统一的带宽单位Mbit，按流量计费的度量单位为GByte。

6.1.1.11 如何测试 VPN 速率情况?

假设测试环境VPN连接已经创建，在VPN连接两端VPC的本端子网下分别创建ECS，并使两个VPC之间的ECS相互能够ping通的情况下，测试VPN的速率情况。

当用户购买的VPN网关的带宽为200Mbit/s时，测试情况如下。

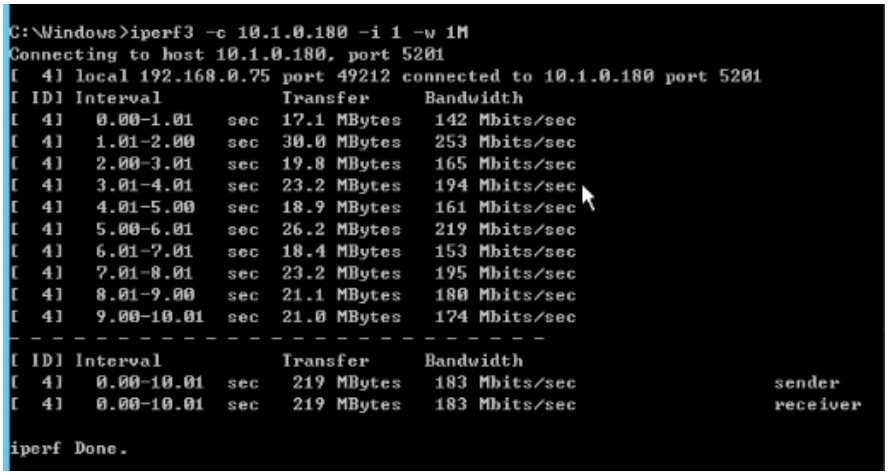
1. 互为对端的ECS都使用Windows系统，测试速率可达180Mbit/s，使用iperf3和filezilla（是一款支持ftp的文件传输工具）测试均满足带宽要求。

   说明

   基于TCP的FTP协议有拥塞控制机制，180Mbit/s为平均速率，且IPsec协议会增加新的IP头，因此10%左右的速率误差在网络领域是正常现象。

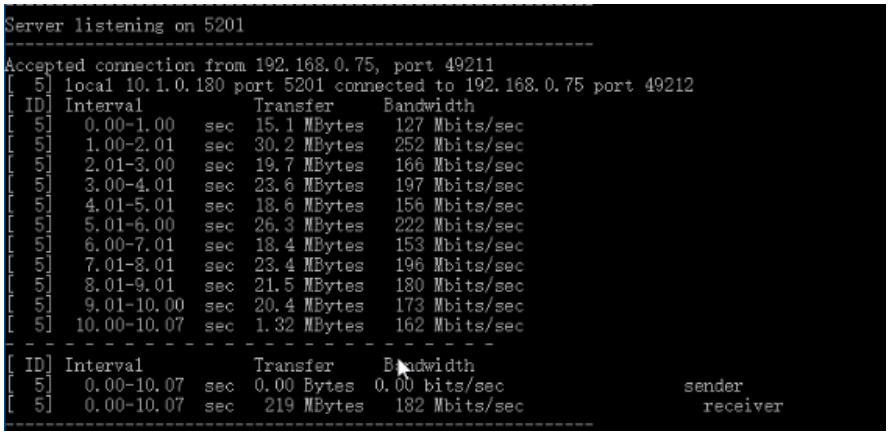
   使用iperf3客户端测试结果截图如图6-1所示。

   图 6-1 200M 带宽客户端 iperf3 测试结果



   使用iperf3服务器端测试结果截图如图6-2所示。

   图 6-2 200M 带宽服务端 iperf3 测试结果

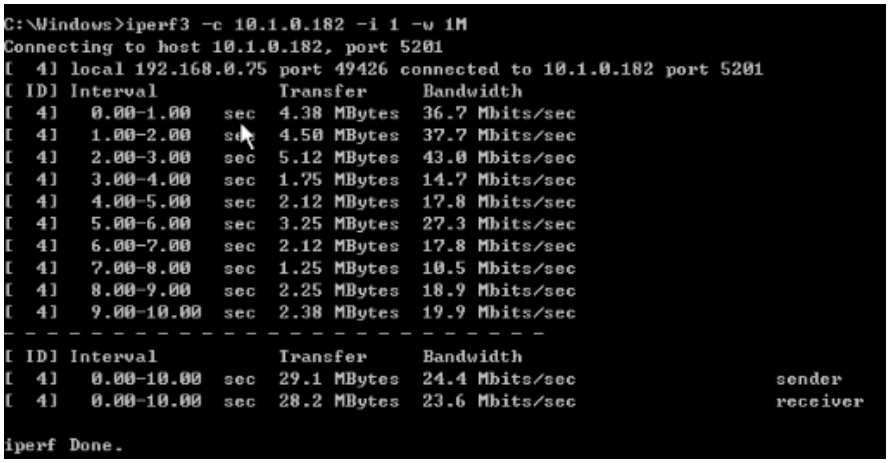


2. 互为对端的ECS都使用Centos7系统，测试速率可达180M，使用iperf3测试满足带宽要求。
3. 服务器端ECS使用Centos7系统，客户端使用Windows系统，测试速率只有20M左右，使用iperf3和filezilla测试均不能满足带宽要求。

   原因在于Windows和Linux对TCP的实现不一致，导致速率慢。所以对端ECS使用不同的系统时，无法满足带宽要求。

   使用iperf3测试结果截图如图6-3所示。

   图 6-3 互为对端的 ECS 系统不同时 iperf3 测试结果



假设用户购买的VPN网关的带宽为1000Mbit/s。

说明

部分区域默认仅支持300M带宽。如果需要更大带宽，您可以先申请300M带宽，然后提交工单进行带宽扩容。

用户购买的VPN网关为网关的整体吞吐能力，即该VPN网关下所有VPN连接的带宽之和。在大带宽场景下，由于主机的转发性能限制，需要使用多台主机构建多条流量才能充分利用网关的带宽。这种场景下对ECS的配置要求也很高，建议ECS的网卡支持2G以上的带宽。

测试总结：综上测试结果，云网关能够满足带宽速率要求，但是建议两端主机使用相同的操作系统，并且网卡要达到配置要求。

6.1.1.12 按流量计费的 VPN 可以使用共享流量包吗?

可以。

VPN服务费用包含弹性公网IP费用，弹性公网IP可以使用共享流量包。

6.1.1.13 VPC、VPN 网关、VPN 连接之间有什么关系?

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

- VPC
  - 即云上私有专用网络，同一Region中可以创建多个VPC，且VPC之间相互隔离。一个VPC内可以划分多个子网网段。

  - 用户可以通过VPN服务，安全访问VPC内的ECS。
- VPN网关
  - 基于VPC创建，是VPN连接的接入点。一个VPC下支持购买多个VPN网关，每个网关可以创建多个VPN连接。
  - 用户可以通过VPN网关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

  基于VPN网关创建，用于连通VPC子网和用户数据中心（或其它Region的VPC）子网，即每个VPN连接连通了一个用户侧数据中心的网关。

  说明

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

6.1.1.14 如何理解 VPN 连接中的对端网关和对端子网?

对端网关和对端子网是个相对的概念，在建立VPN连接时，从云的角度出发，VPC网络就是本地子网，创建的VPN网关就是本地网关，与之对接的用户侧网络就是对端子网， 用户侧的网关就是对端网关。

对端网关IP就是用户侧网关的公网IP，对端子网指需要和VPC子网互联的子网。

6.1.1.15 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。

一个VPN网关支持绑定两个EIP和用户侧网关进行通信：

- 如果用户侧数据中心只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：这种情况需要配置一个VPN连接组，即VPN网关的两个EIP分别配置一条VPN连接和用户侧出口网关通信。
- 如果用户侧数据中心只有两个公网出口网关，所有服务器（或用户主机）通过两个网关连接至Internet：这种情况需要配置两个VPN连接组，即VPN网关的两个EIP分别配置一条VPN连接和两个用户侧出口网关通信。

6.1.1.16 VPN 支持将两个 VPC 互连吗?

- 如果两个VPC位于同一区域内，不支持VPN互连，推荐使用VPC对等连接互连。
- 如果两个VPC位于不同区域，支持VPN互连，具体操作如下：
  a. 为这两个VPC分别创建VPN网关，并为两个VPN网关创建VPN连接。
  b. 将两个VPN连接的对端网关设置为对方VPN网关的网关EIP。
  c. 将两个VPN连接的远端子网设置为对方VPC的网段。
  d. 两个VPN连接的预共享密钥和算法参数需保持一致。

6.1.1.17 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：

- IKE/IPsec策略配置。
- 配置VPN连接模式为路由模式或策略模式。
- 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）。

6.1.1.18 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置?

可以。

6.1.1.19 如何防止 VPN 连接出现中断情况?

VPN连接在正常的使用过程中会存在重协商情况，触发重协商的条件有IPsec SA的生命周期即将到期和VPN传输的流量超过20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的ACL不匹配；
- SA生命周期不匹配；
- 用户侧数据中心未配置DPD；
- VPN使用过程中修改了配置信息；
- 运营商网络抖动。

因此请在配置VPN时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像；
- SA生命周期信息一致；
- 用户侧数据中心网关开启DPD配置，探测次数不少于3次；
- 连接过程中修改参数两侧同步修改；
- 设置用户侧数据中心设备TCP MAX-MSS为1300；
- 确保用户侧数据中心出口有足够的带宽可被VPN使用；
- 确认VPN连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置；

6.1.1.20 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。

6.1.1.21 EIP 能作为 VPN 的网关 IP 吗?

企业版VPN可以。

用户可以在创建VPN网关时绑定EIP作为网关IP。

6.1.1.22 VPN 配置完成了，为什么连接一直处于未连接状态?

可能存在信息配置错误，请从以下方面进行排查：

1. 确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/对端子网、本端网关/对端网关互为镜像。
2. 确认用户侧数据中心设备的路由、NAT和安全策略配置无误。

6.1.1.23 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置?

VPN连接的“连接模式”选择“策略模式”时，才需要在管理控制台上配置策略规则ACL。

6.1.2 产品咨询

6.1.2.1 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。

6.1.2.2 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。

6.1.2.3 VPC、VPN 网关、VPN 连接之间有什么关系?

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

- VPC
  - 即云上私有专用网络，同一Region中可以创建多个VPC，且VPC之间相互隔离。一个VPC内可以划分多个子网网段。
  - 用户可以通过VPN服务，安全访问VPC内的ECS。
- VPN网关
  - 基于VPC创建，是VPN连接的接入点。一个VPC下支持购买多个VPN网关，每个网关可以创建多个VPN连接。
  - 用户可以通过VPN网关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

  基于VPN网关创建，用于连通VPC子网和用户数据中心（或其它Region的VPC）子网，即每个VPN连接连通了一个用户侧数据中心的网关。

  说明

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

6.1.2.4 VPN 连接是什么？用户在购买 VPN 网关时如何选择 VPN 连接数?

VPN连接，指一个VPN网关与用户侧一个独立的公网IP之间建立的IPsec连接，一个连接中可以配置多个本端子网（vpc中的子网）和对端子网（用户侧子网）， 无需配置多个连接。

拟创建VPN连接的数量通常与用户数据中心数量有关，每条VPN连接可打通当前VPC与云下的一个数据中心网络。

说明

当云侧的网段a1、a2与用户侧网段b1、b2分别通信时，仅需创建一条VPN连接并指定云侧多个源网段和多个地址网段即可。

6.1.2.5 如何理解 VPN 连接中的对端网关和对端子网?

对端网关和对端子网是个相对的概念，在建立VPN连接时，从云的角度出发，VPC网络就是本地子网，创建的VPN网关就是本地网关，与之对接的用户侧网络就是对端子网， 用户侧的网关就是对端网关。

对端网关IP就是用户侧网关的公网IP，对端子网指需要和VPC子网互联的子网。

6.1.2.6 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、100.64.0.0/12和214.0.0.0/8的网段。

  如果需要使用100.64.0.0/10或100.64.0.0/12，请提交工单申请。

6.1.2.7 IPsec VPN 是否会自动建立连接?

支持自动建立连接。

6.1.2.8 VPN 工单分类方法有哪些? 如何提交 VPN 工单?

1. 登录管理控制台。
2. 在管理控制台右上角选择“工单 > 新建工单”。
3. 搜索并选择“VPN”。
4. 选择问题类型。

6.1.2.9 VPN 协商参数有哪些? 默认值是什么?

表 6-2 VPN 协商参数

协议	配置项	值
IKE	版本	• 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） • v2（默认）
	协商模式	• Main（默认） • Aggressive
	认证算法	• 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（默认） • SHA2-384 • SHA2-512

协议	配置项	值
	加密算法	• 3DES（此算法安全性较低，请慎用） • AES-128（默认） • 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）
	DH算法	• 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（默认） • Group 15 • Group 16 • Group 19 • Group 20 • Group 21
	生命周期（秒）	86400（默认） 单位：秒。 取值范围：60-604800。
	本端标识	• IP Address 本端IP地址由系统自动关联显示，无需用户手动配置。 • FQDN 默认的本端标识类型是IP Address，ID值是VPN网关的公网IP。
	对端标识	• IP Address • FQDN 默认的对端标识类型是IP Address，ID值是对端网关的公网IP。
IPsec	认证算法	• 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（默认） • SHA2-384 • SHA2-512

协议	配置项	值
	加密算法	• AES-128（默认） • 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） • 3DES（此算法安全性较低，请慎用） • AES-128-GCM-16 • AES-256-GCM-16
	PFS	• 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（默认） • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 • Disable（此算法安全性较低，请慎用）
	传输协议	• ESP（默认）
	生命周期（秒）	3600（默认） 单位：秒。 取值范围：30-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

  IKE协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致IPsec VPN受到侵犯。为提升密钥管理的安全性，IKE提供了PFS（完美向前保密）功能。启用PFS后，在进行IPsec SA协商时会进行一次附加的DH交换，重新生成新的IPsec SA密钥，提高了IPsec SA的安全性。
- 为了增强安全性，默认开启PFS，请确认用户侧数据中心网关设备也开启了该功能，且两端配置保持一致，否则会导致协商失败。
- IPsec SA字节生命周期，不是VPN服务可配置参数，云侧采用的是默认配置1843200KB。该参数不是协商参数，不影响双方建立IPsec SA。

6.1.2.10 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。

6.1.2.11 如何在已创建的 VPN 连接中，限定特定的主机访问云上子网?

云下限制：

- VPN设备按照策略限制访问
- 路由器或交换机上设置ACL限制

云上限制：

- 安全组限制源IP
- ACL限制

说明

不建议通过修改本端子网和对端子网的方式来限定访问。

6.1.2.12 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。

6.1.2.13 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。

6.1.2.14 通过 VPN 互访的主机需要购买 EIP 吗?

如果用户本地的主机通过VPN访问云上的ECS，此时ECS不需要购买EIP。

如果ECS要向公网用户提供服务，需要购买EIP。

6.1.2.15 VPN 配置下发后，多久能够生效?

用户在管理控制台中完成VPN资源创建后，配置1-5分钟下发完成，下发后立即生效。

说明

VPN配置下发成功后，并不表示VPN连接已经建立成功，用户还需要对用户侧网关设备进行配置，完成与VPN网关的隧道协商。

6.1.2.16 VPN 是否支持 IPv6?

不支持。

6.1.2.17 如何选择购买 VPN 带宽的大小?

购买VPN时，选择带宽大小需要考虑以下两个因素：

- VPN隧道中单位时间的数据传输量（需要冗余一定带宽，防止链路拥塞）。
- 考虑两端的出口带宽，云上带宽要小于云下出口带宽。

6.1.2.18 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漏的风险，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。
- 修复了多处公认的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。

6.1.2.19 VPN 使用的 DH group 对应的比特位是多少?

Diffie-Hellman(DH)组确定密钥交换过程中使用的密钥的强度。较高的组号更安全，但需要额外的时间来计算密钥。

VPN使用的DH group对应的比特位如表6-3所示。

表 6-3 DH group 对应比特位

DH group	Modulus
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	ecp256 bits
20	ecp384 bits
21	ecp521 bits

说明

以下DH算法有安全风险，不推荐使用：DH group 1、DH group 2、DH group 5。

6.1.2.20 是否可以通过 VPN 实现跨境访问网站?

不可以。

VPN实现的是将云上的VPC子网和用户侧数据中心的IDC网络打通的场景，即站点与站点互通（site to site）。

6.1.2.21 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联?

可以。

VPN连通的是两个子网，即VPC网络与用户数据中心网络。

VPN成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是IPsec VPN的典型场景，请用户放心使用。

同时VPN连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通VPN以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行ping，获取网络的丢包和时延情况。

6.1.2.22 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

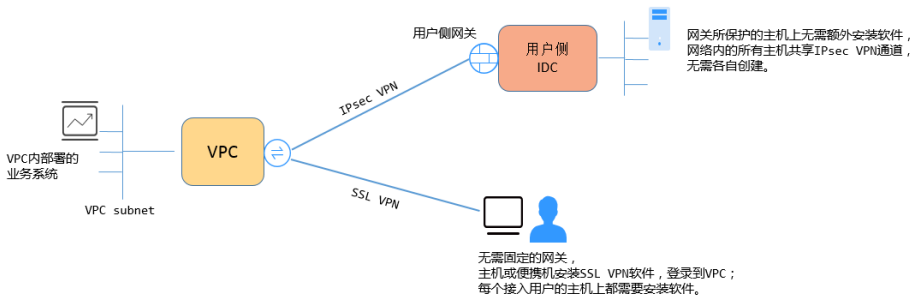
IPsec VPN：连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网；即IPsec VPN是网对网的连接。

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。

6.1.2.23 按流量计费的 VPN 可以使用共享流量包?

可以。

VPN服务费用包含弹性公网IP费用，弹性公网IP可以使用共享流量包。

6.1.2.24 VPN 网关删除后公网地址是否可以保留?

按需VPN网关如果绑定了按需EIP，则VPN网关删除后会同步删除绑定的按需EIP。

如果需要保留EIP，请在删除VPN网关前对EIP进行解绑操作。

6.1.2.25 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对端子网路由，无需手动配置。

6.1.2.26 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连接创建后即会向云监控服务CES上报状态信息，但是并不会自动向用户发送告警通知，需要在页面左上角单击☰图标，选择“管理与监管 > 云监控”创建告警规则。

6.1.2.27 如何解决 VPN 连接无法建立连接问题?

1. 登录控制台，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。

6.1.2.28 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么?

云上用户购买的VPN网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

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

按带宽计费度量采用国际统一的带宽单位Mbit，按流量计费的度量单位为GByte。

6.1.2.29 VPN 网关是否支持规格变更，如从专业型 1 变更到专业型 2

VPN网关支持规格升降配，可以在VPN网关页面修改网关规格。以下产品规格升降配，实际情况以控制台显示为准。

- 专业型1和专业型2 VPN网关规格，支持相互变更。

6.1.2.30 包周期的 VPN 网关是否可以绑定按需 EIP? EIP 共享流量包也适用吗?

支持绑定按需EIP，EIP共享流量包也适用。共享流量包自动抵扣按需计费（按流量计费）的EIP带宽产生的流量资费，直到流量包用完或到期， 需要注意的是EIP会区分动态BGP和静态BGP类型的。

6.1.3 组网与使用场景

6.1.3.1 是否可以通过 VPN 实现跨境访问网站?

不可以。

VPN实现的是将云上的VPC子网和用户侧数据中心的IDC网络打通的场景，即站点与站点互通（site to site）。

6.1.3.2 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联?

可以。

VPN连通的是两个子网，即云上VPC网络与用户数据中心网络。

VPN成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是IPsec VPN的典型场景，请用户放心使用。

同时VPN连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通VPN以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行ping，获取网络的丢包和时延情况。

6.1.3.3 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。

一个VPN网关支持绑定两个EIP和用户侧网关进行通信：

- 如果用户侧数据中心只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：这种情况需要配置一个VPN连接组，即VPN网关的两个EIP分别配置一条VPN连接和用户侧出口网关通信。
- 如果用户侧数据中心只有两个公网出口网关，所有服务器（或用户主机）通过两个网关连接至Internet：这种情况需要配置两个VPN连接组，即VPN网关的两个EIP分别配置一条VPN连接和两个用户侧出口网关通信。

6.1.3.4 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

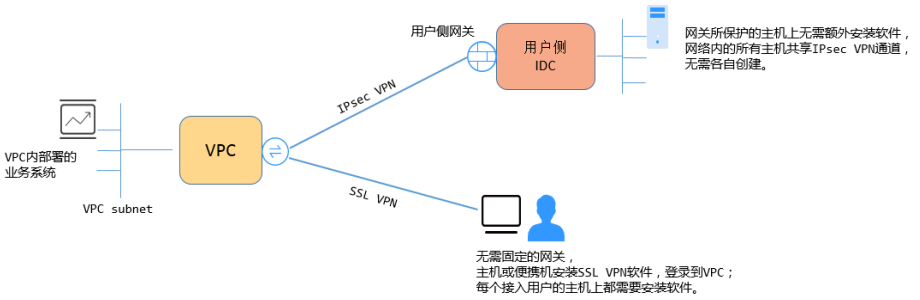
IPsec VPN：连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网；即IPsec VPN是网对网的连接。

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。

6.1.3.5 VPN 支持将两个 VPC 互连吗?

- 如果两个VPC位于同一区域内，不支持VPN互连，推荐使用VPC对等连接互连。
- 如果两个VPC位于不同区域，支持VPN互连，具体操作如下：
  a. 为这两个VPC分别创建VPN网关，并为两个VPN网关创建VPN连接。
  b. 将两个VPN连接的对端网关设置为对方VPN网关的网关EIP。
  c. 将两个VPN连接的对端子网设置为对方VPC的网段。
  d. 两个VPN连接的预共享密钥和算法参数需保持一致。

6.1.3.6 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：

- IKE/IPsec策略配置。
- 配置VPN连接包括静态路由模式、BGP路由模式和策略模式。
- 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）。

6.1.3.7 通过 VPN 来实现云下 IDC 与云端 VPC 的互通，两端分别需要做哪些配置?

VPN对接的工作分为两个部分：云上创建VPN和用户侧数据中心配置VPN设备。

- 云上创建VPN
  - 配置对端网关，配置路由模式等信息。
  - 配置VPN连接，配置两端网关IP，两端子网和协商策略等信息。
- 用户侧数据中心配置VPN设备
  a. 配置用户侧数据中心公网IP，在支持IPsec VPN的设备上完成IPsec协商的一、二阶段配置。

b. 进行网络路由、NAT和安全策略配置。

6.1.3.8 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置?

可以。

6.1.3.9 同一个 Region 的两个 VPC 可以通过 VPN 连通吗?

不可以。

对于同Region的两个VPC，您可以通过对等连接（VPC peering）或者云连接（CC）打通两个VPC。

6.1.3.10 可以通过哪些方式连通同一个 Region 的两个 VPC?

可通过创建对等连接或者云连接的方式打通同Region的两个VPC，对等连接只用同Region的VPC，云连接可连通不同Region的VPC。

6.1.3.11 云端创建了两个 VPC，如何与云下的 IDC 网络互通?

组网拓扑

IDC-VPC1-VPC2。

其中，IDC表示用户数据中心，VPC1与IDC建立VPN连接。

配置步骤

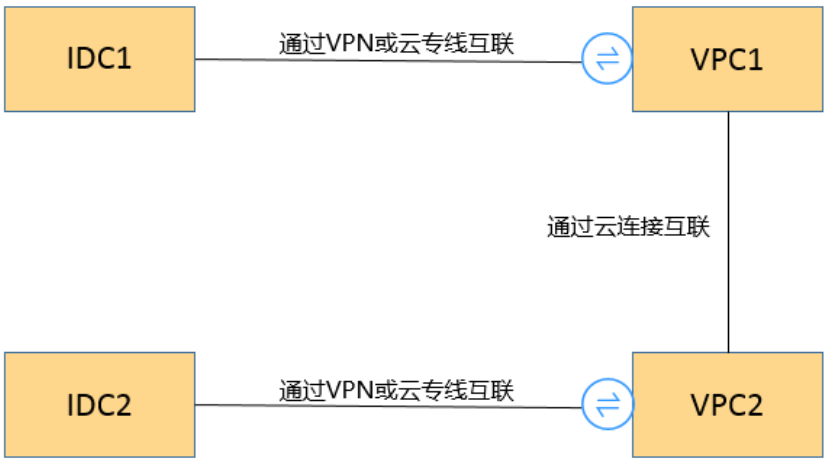
1. 确认云上的两个VPC是否在同一Region。
   - 如果在同一Region可通过对等连接或云连接（CC）将两个VPC连接起来（免费）。
   - 如果两个VPC跨Region，请使用CC进行互联（需支付CC带宽费用）。
2. 用户侧数据中心IDC与其中一个VPC建立VPN连接。

   修改用户侧数据中心设备的对端子网为云上两个VPC子网，VPN对接的VPC1本端子网需要包含通过对等连接或CC连接的子网，对等连接或CC的子网路由包含用户侧数据中心IDC子网。

6.1.3.12 组网拓扑如（IDC1-VPC1-VPC2-IDC2）所示，如何实现四个子网互联?

组网拓扑如图6-4所示。

图 6-4 组网拓扑



1. IDC1可通过VPN或DC与VPC1互联。
2. 两个VPC之间使用CC互联（同Region也可以使用对端连接）。
3. IDC2可通过VPN或DC与VPC2互联。
4. 同时完成VPN子网更新、CC及DC子网路由更新即可实现四个子网相互访问。

6.1.3.13 云端两个 Region，每 Region 有两个子网，是否可以创建两个 VPN 连接，分别连通不同子网?

不可以。

两个Region间只需创建一个VPN连接即可，在VPN连接中将两个子网都加入到VPN中。

针对这种场景，如果用户试图去创建第二条VPN连接，由于两个连接的对端网关地址一样，因此管理控制台界面会提示冲突。

6.1.3.14 VPN 和 OBS 可以直接通信吗?

可以。

1. 用户站点通过VPN访问OBS服务，需要使用VPC终端节点服务。需要为内网DNS和OBS分别申请两个终端节点。
2. 在用户侧配置云的内网DNS和路由

6.1.3.15 用户本地电脑如何连接云上 VPN?

普通家庭宽带路由器、个人的移动终端设备、Windows主机自带的VPN服务（如L2TP）无法与云进行VPN对接。

与云下对接需要对端有支持标准IPsec协议的设备。

6.1.3.16 公司网络已通过 VPN 连通了云，我如何在家访问云 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络的组成部分，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服务对应的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。

6.1.3.17 如何选择在云上的哪个区域创建 VPN 网关?

在云上创建VPN网关，您可以选择任一区域的VPC进行创建。

推荐您选择与IDC同城的区域创建VPN网关，这样可以更大程度降低因公网质量对VPN的影响。

- 同区域的多个VPC，可以通过VPN+DC的方式进行打通。
- 跨区域的多个VPC，可以通过VPN+CC的方式进行打通。

6.1.4 Console 与页面使用

6.1.4.1 VPC、VPN 网关、VPN 连接之间有什么关系?

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

- VPC
  - 即云上私有专用网络，同一Region中可以创建多个VPC，且VPC之间相互隔离。一个VPC内可以划分多个子网网段。
  - 用户可以通过VPN服务，安全访问VPC内的ECS。
- VPN网关
  - 基于VPC创建，是VPN连接的接入点。一个VPC下支持购买多个VPN网关，每个网关可以创建多个VPN连接。
  - 用户可以通过VPN网关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

  基于VPN网关创建，用于连通VPC子网和用户数据中心（或其它Region的VPC）子网，即每个VPN连接连通了一个用户侧数据中心的网关。

  说明

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

6.1.4.2 VPN 配置下发后，多久能够生效?

用户在管理控制台完成VPN资源创建后，配置1-5分钟下发完成，下发后立即生效。

说明

VPN配置下发成功后，并不表示VPN连接已经建立成功，用户还需要对用户侧网关设备进行配置，完成与VPN网关的隧道协商。

6.1.4.3 VPN 配置完成了，为什么连接一直处于未连接状态?

可能存在信息配置错误，请从以下方面进行排查：

1. 确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/对端子网、本端网关/对端网关互为镜像。
2. 确认用户侧数据中心设备的路由、NAT和安全策略配置无误。

6.1.4.4 VPN 网关删除后公网地址是否可以保留?

按需VPN网关如果绑定了按需EIP，则VPN网关删除后会同步删除绑定的按需EIP。

如果需要保留EIP，请在删除VPN网关前对EIP进行解绑操作。

6.1.4.5 已经创建的 VPN 哪些信息可以修改，哪些信息不可以修改?

- VPN网关
  - 可以修改的信息
    - 名称
    - 本端子网
    - 主备EIP
      - 可以通过先解绑EIP，然后绑定EIP的方式对主备EIP进行修改。
        如果EIP已经创建了VPN连接，则无法解绑。
      - EIP的名称、公网IP类型、带宽大小等属性修改。
    - 规格
      部分规格支持，以管理控制台界面为准。
  - 不可以修改的信息
    - 区域
    - 关联模式，包括虚拟私有云和企业路由器。
    - 企业路由器
      仅“关联模式”为“企业路由器”时需要设置。
    - 虚拟私有云
    - 互联子网
    - BGP ASN
    - 可用区
- 对端网关

  - 可以修改的信息
    - 名称
  - 不可以修改的信息
    - BGP ASN
      仅“路由模式”选择“动态BGP”时需要设置。
    - 网关IP
- VPN连接
  - 可以修改的信息
    - 名称
    - 计费模式，只支持按需转包年/包月
    - 本端接口地址
    - 对端网关
    - 对端子网
    - 策略配置，包括IKE策略和IPsec策略
    - 预共享密钥
  - 不可以修改的信息
    - VPN网关
    - 公网IP
    - 连接模式，包括路由模式和策略模式
    - 路由模式，包括静态路由和BGP
      仅“连接模式”选择“路由模式”时需要设置。
    - 策略规则，包括源网段和目的网段
      仅“连接模式”选择“策略模式”时需要设置。

6.1.4.6 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置?

VPN连接的“连接模式”选择“策略模式”时，才需要在管理控制台上配置策略规则ACL。

6.1.4.7 创建 VPN 连接时添加对端子网，提示系统异常，如何处理?

检查VPC内是否存在对等连接、云专线、云连接的子网路由使用了该子网，导致VPN下发子网路由冲突，确认后将其配置的子网路由删除后重新创建即可。

6.1.4.8 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对端子网路由，无需手动配置。

6.1.4.9 如何理解 VPN 连接中的对端网关和对端子网?

对端网关和对端子网是两个相对的概念，在建立VPN连接时，从云的角度出发，VPC网络就是本地子网，创建的VPN网关就是本地网关，与之对接的用户侧网络就是对端子网， 用户侧的网关就是对端网关。

对端网关IP就是用户侧网关的公网IP，对端子网指需要和VPC子网互联的子网。

6.1.4.10 创建 VPN 连接时如何关闭 PFS?

- 云

  请在VPN连接配置参数中，将IPsec策略中PFS的选项选择为Disable。云默认开启PFS。

- 用户数据中心对端网关

  部分设备厂商默认关闭了PFS功能，请查询设备对应用户手册进行操作。

说明

配置过程中，请确认云和对端网关侧PFS配置一致，否则会导致协商失败。

为了增强安全性，建议云和对端网关侧均开启PFS。

6.1.4.11 VPN 本端子网和对端子网的数量有限制吗?

- 每个VPN网关配置的本地子网数量为50。
- 每个VPN连接支持配置的对端子网个数为50。
- 每个VPN连接的策略规则可加的数量为5。

  每条策略规则可以有1个源网段和50个目的网段。

6.1.4.12 配置 VPN 连接的本端子网和对端子网时需要注意什么?

- 子网数量满足规格限制，数量超出规格限制请进行聚合汇总。
  - 每个VPN网关配置的本地子网数量：50
  - 每个VPN连接支持配置的对端子网个数：50
- 本端子网不可以包含对端子网，对端子网可以包含本端子网。
- 推荐配置的本端子网在VPC内有路由可达。
- 同一个VPN网关创建两条连接：若这两条连接的对端子网存在包含关系，在访问的目的网络处于交集网段部分时，按照创建连接的先后顺序匹配VPN连接，且与连接状态无关（策略模式不能按照掩码长度进行匹配）。

6.1.4.13 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接?

VPN连接状态刷新存在一定的延迟，业务已通但是网页上VPN连接状态还是未连接是正常现象。

如果数据面已正常（即业务访问已正常）， 连接就已经完成建立了，短暂等待后VPN连接状态就会更新为“已连接”。

6.1.4.14 修改协商策略后，页面显示资源不存在，如何处理?

此问题为页面刷新周期问题。

在修改连接高级策略时，系统会先删除，再重建VPN连接，如果在页面创建过程中出现短暂的删除中或创建中属于正常现象，切勿重复创建同一连接（本端子网、对端子网、对端网关相同的连接）；

6.1.4.15 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。

云将大力推进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漏的风险，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。
- 修复了多处公认的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。

6.1.4.16 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。

6.1.4.17 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。

6.1.4.18 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连接创建后即会向云监控服务CES上报状态信息，但是并不会自动向用户发送告警通知，需要在页面左上角单击☰图标，选择“管理与监管 > 云监控”创建告警规则。

6.1.5 VPN 协商与对接

6.1.5.1 VPN 协商参数有哪些？默认值是什么?

表 6-4 VPN 协商参数

协议	配置项	值
IKE	认证算法	● 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。
	加密算法	● 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 默认配置为：AES-128。

协议	配置项	值
	DH算法	• 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 默认配置为：Group 15。
	版本	• v1（版本安全性较低，如果用户设备支持v2版本，建议选择v2。） • v2 默认配置为：v2。
	生命周期	86400（默认） 单位：秒。 取值范围：60-604800。
	本端标识	• IP Address 本端IP地址由系统自动关联显示，无需用户手动配置。 • FQDN 默认的本端标识类型是IP Address，ID值是VPN网关的公网IP。
	对端标识	• IP Address • FQDN 默认的对端标识类型是IP Address，ID值是对端网关的公网IP。
IPsec	认证算法	• 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。

协议	配置项	值
	加密算法	● 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 默认配置为：AES-128。
	PFS	● 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 默认配置为：Group 15。
	传输协议	ESP（默认）
	生命周期	3600（默认） 单位：秒。 取值范围：30-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。
  IKE协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致IPsec VPN受到侵犯。为提升密钥管理的安全性，IKE提供了PFS（完美向前保密）功能。启用PFS后，在进行IPsec SA协商时会进行一次附加的DH交换，重新生成新的IPsec SA密钥，提高了IPsec SA的安全性。
- 为了增强安全性，默认开启PFS，请确认用户侧数据中心网关设备也开启了该功能，且两端配置保持一致，否则会导致协商失败。
- IPsec SA字节生命周期，不是VPN服务可配置参数，云侧采用的是默认配置1843200KB。该参数不是协商参数，不影响双方建立IPsec SA。

6.1.5.2 IPsec VPN 是否会自动建立连接?

支持自动建立连接。

6.1.5.3 VPN 支持对端网关域名对接吗?

对端VPN连接需要明确对端的公网IP地址，暂不支持通过域名方式与对端设备进行对接。

6.1.5.4 我创建的 VPN 连接有几个隧道?

VPN连接下的隧道和本端子网/对端子网的数量有关，隧道总数等于本端子网数和对端子网数的乘积。

- 当两个子网间存在数据流时，连接这两个子网的IPsec隧道状态就会变成Active。
- 只要有一个IPsec隧道的状态为Active，对应VPN连接的状态就会显示已连接。

6.1.5.5 如何在已创建的 VPN 连接中，限定特定的主机访问云上子网?

云下限制：

- VPN设备按照策略限制访问
- 路由器或交换机上设置ACL限制

云上限制：

- 安全组限制源IP
- ACL限制

说明

不建议通过修改本端子网和对端子网的方式来限定访问。

6.1.5.6 VPN 是否启动了 DPD 检测机制?

是的。

VPN服务默认开启了DPD探测机制，用于探测用户侧数据中心IKE进程的存活状态。

3次探测失败后即认为用户侧数据中心IKE异常，此时云会删除本端隧道，以保持双方的隧道同步。

DPD协议本身并不要求对端也同步进行配置（但是要求对端可以应答DPD探测），为了保证协商双方隧道状态一致，避免出现单边隧道（一端存在隧道，而另一端已不存

在），建议用户同时启动用户侧网关的DPD探测机制，用于探测云侧VPN服务的IKE状态。

说明

DPD探测失败后会删除隧道，不会导致业务不稳定。

6.1.5.7 如何通过安全组控制使 VPN 不能访问 VPC 上的部分虚拟机，实现安全隔离?

如果用户需要控制VPN站点只能访问VPC的部分网段或者部分主机，可以通过安全组进行控制。

配置示例：不允许客户侧的子网192.168.1.0/24访问VPC内子网10.1.0.0/24下的ECS。

配置方法：

1. 创建两个安全组：安全组1和安全组2。
2. 安全组1的入方向规则配置deny网段192.168.1.0/24。
3. 安全组2允许192.168.1.0/24访问。
4. 网段10.1.0.0/24的ECS选择安全组1，其他的主机选择安全组2。

6.1.5.8 修改 VPN 连接的配置会造成连接重建吗?

VPN连接包含本端子网、对端子网、对端网关、预共享密钥、IKE协商策略、IPsec协商策略。修改VPN连接具体包括以下几种情况：

- 修改本端子网和对端子网，连接ID不发生变化，只是更新了连接两端的子网信息，如果更新的是部分子网信息，已经建立的子网间隧道不会重建。
- 修改对端网关IP，连接ID不发生变化，但连接的对端已改变，连接需要重建。
- 仅修改连接的预共享密钥，连接的ID不发生变化，连接状态当时并不发生改变，重协商会重新校验密钥匹配情况，如果密钥不匹配重协商会失败。
- 修改协商策略（需验证预共享密钥），连接ID发生改变，相当于连接删除重建过程，连接需要重建。

6.1.5.9 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。

6.1.5.10 本地防火墙无法收到 VPN 网关的 IKE 第一阶段的回复包怎么解决?

1. 检查两端公网IP是否可以互访，推荐使用ping命令，VPN网关EIP缺省可以ping通。
2. 云下网关与VPN网关可以互访UDP 500、4500报文。
3. 云下公网IP访问VPN网关IP时，没有发生源端口NAT转换，如果存在NAT穿越，端口号在nat穿越后不得发生改变。
4. 两端的IKE协商参数配置一致。

   NAT穿越场景中，云下ID标识类型选择IP，IP值为NAT转换后的公网IP。

6.1.5.11 本地防火墙无法收到 VPN 子网的回复包怎么解决?

1. 如果二阶段协商中需要检查云下的路由、安全策略、NAT和感兴趣流、协商策略信息。
   - 路由设置：将访问云上子网的数据送入隧道。
   - 安全策略：放行云下子网访问云上子网的流量。
   - NAT策略：云下子网访问云上子网不做源nat。
   - 感兴趣流：两端感兴趣流配置互为镜像，使用IKE v2配置感兴趣流不可使用地址对象名称。
   - 协商信息：协商策略信息云上云下一致，特别注意PFS的配置。
2. 确认一、二阶段协商均已正常后，请检查云上安全组策略，放行入方向的云下子网访问云上子网的ICMP协议。

6.1.5.12 VPN 使用的 DH group 对应的比特位是多少?

Diffie-Hellman(DH)组确定密钥交换过程中使用的密钥的强度。较高的组号更安全，但需要额外的时间来计算密钥。

VPN使用的DH group对应的比特位如表6-5所示。

表 6-5 DH group 对应比特位

DH group	Modulus
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	ecp256 bits
20	ecp384 bits
21	ecp521 bits

说明

以下DH算法有安全风险，不推荐使用：DH group 1、DH group 2、DH group 5。

6.1.6 连接故障或无法 PING 通

6.1.6.1 VPN 配置完成了，为什么连接一直处于未连接状态?

可能存在信息配置错误，请从以下方面进行排查：

1. 确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/对端子网、本端网关/对端网关互为镜像。
2. 确认用户侧数据中心设备的路由、NAT和安全策略配置无误。

6.1.6.2 如何防止 VPN 连接出现中断情况?

VPN连接在正常的使用过程中会存在重协商情况，触发重协商的条件有IPsec SA的生命周期即将到期和VPN传输的流量超过20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的ACL不匹配；
- SA生命周期不匹配；
- 用户侧数据中心未配置DPD；
- VPN使用过程中修改了配置信息；
- 运营商网络抖动。

因此请在配置VPN时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像；
- SA生命周期信息一致；
- 用户侧数据中心网关开启DPD配置，探测次数不少于3次；
- 连接过程中修改参数两侧同步修改；
- 设置用户侧数据中心设备TCP MAX-MSS为1300；
- 确保用户侧数据中心出口有足够的带宽可被VPN使用；
- 确认VPN连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置；

6.1.6.3 使用中 IPsec VPN 连接中断后如何快速恢复?

1. 如果无法正常触发协商，请检查IPsec两侧公网IP的连通性，比如两个公网IP互Ping验证。VPN网关IP默认回应ICMP报文。
2. 如果公网链路正常，需排查是否存在多出口的链路切换，即当前访问云网关IP流量未从协商端口流出。
3. 如果无多出口或出口路径正常，可尝试IPsec隧道两端同时修改一次PSK，重新触发协商。
4. 如果重新触发协商失败，请确认两端配置的协商策略是否一致、感兴趣流是否互为镜像（条目数、子网均相同）。

5. 如果协商策略和感兴趣流配置无误，请关停云下设备的VPN连接，等待云端连接显示为“未连接”后，重启云下设备VPN连接，并进行数据流触发。
6. 如果依然无法触发协商时，请执行以下操作：
   a. 记录VPN连接的协商策略、PSK、本端子网、对端网关、对端子网。
   b. 使用现有网关新建一条连接，协商策略、PSK、本端子网均与原连接相同，对端网关和对端子网先任意填写。
   c. 待新创建连接成功后，删除原连接，之后再修改新建连接的对端网关和对端子网与记录数据一致。
   d. 修改完成后重新触发协商。

6.1.6.4 VPN 网关带宽到达限额时有什么影响?

VPN网关带宽限速限制的出VPC方向的带宽，如果您VPN网关的带宽超过限额使用时，会出现网络卡顿、部分子网间无法访问、甚至出现VPN连接中断现象（无法收到VPN的探测报文）。

因此在出现VPN网关带宽已达到上限时，建议您对VPN网关带宽进行扩容。

说明

VPN网关的带宽最大为1Gbit/s。

6.1.6.5 IPsec VPN 是否会自动建立连接?

支持自动建立连接。

6.1.6.6 两个 Region 创建的 VPN 连接状态正常，为什么不能 ping 通对端 ECS?

安全组默认放行了出方向的所有端口，入方向需要按照实际需要添加放行规则，确认接收ping报文的ECS安全组放行了入方向的ICMP。

6.1.6.7 IDC 与云端对接，VPN 连接正常，子网间业务无法互相访问?

连接状态正常，说明两端的协商参数没有问题，排查项如下：

- 用户侧数据中心设备子网路由是否从网关开始逐跳指向VPN出口设备。
- VPN设备有安全设置放行了子网间的数据互访。
- IDC子网访问云端数据不做NAT。
- 确保两侧公网IP（网关IP）间访问不被阻拦。

6.1.6.8 正在使用 VPN 出现了连接中断，提示数据流不匹配，如何排查?

这通常是由于云上与用户侧数据中心设备配置的ACL不匹配造成的。

1. 首先确认两端VPN连接的子网信息是否配置一致，确保云端生成的ACL与用户侧数据中心ACL配置互为镜像
2. 用户侧数据中心感兴趣流配置推荐使用“子网/掩码”的格式，避免使用网络地址对象模式，即address object模式，address object为非标模式，容易引起不兼容问题。

6.1.6.9 正在使用 VPN 出现了连接中断，提示 DPD 超时，如何排查?

出现DPD超时的连接中断是因为两端网络访问无数据，在SA老化后发送DPD未得到对端响应而删除连接。

解决方法:

1. 开启用户侧数据中心设备的DPD配置，测试两端的数据流均可触发连接建立；
2. 在两端的主机中部署Ping shell脚本，也可在用户侧数据中心的子网的网关设备上配置保活数据，如NQA。

6.1.6.10 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接?

管理控制台界面中VPN连接状态刷新存在一定的延迟，是正常现象。

如果数据面已正常（即业务访问已正常）， 则VPN连接已完成建立。

6.1.6.11 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连接创建后即会向云监控服务CES上报状态信息，但是并不会自动向用户发送告警通知，需要在页面左上角单击☰图标，选择“管理与监管 > 云监控”创建告警规则。

6.1.6.12 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。

6.1.6.13 VPN 建立后您的数据中心或局域网无法访问?

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远端的子网地址访问。

6.1.6.14 为什么 VPN 创建成功后状态显示未连接?

VPN连接状态存在一定延迟，请等待大约2分钟后重新刷新VPN连接状态。

6.1.6.15 VPN 是否启动了 DPD 检测机制?

是的。

VPN服务默认开启了DPD探测机制，用于探测用户侧数据中心IKE进程的存活状态。

3次探测失败后即认为用户侧数据中心IKE异常，此时云会删除本端隧道，以保持双方的隧道同步。

DPD协议本身并不要求对端也同步进行配置（但是要求对端可以应答DPD探测），为了保证协商双方隧道状态一致，避免出现单边隧道（一端存在隧道，而另一端已不存在），建议用户同时启动用户侧网关的DPD探测机制，用于探测云侧VPN服务的IKE状态。

说明

DPD探测失败后会删除隧道，不会导致业务不稳定。

DPD可以及时发现对方IKE进程异常，并通过重置隧道的方法来保持双方隧道同步。在删除隧道后，当有用户流量时，可以重新触发协商并建立隧道。

6.1.7 公网地址

6.1.7.1 VPN 网关删除后公网地址是否可以保留?

按需VPN网关如果绑定了按需EIP，则VPN网关删除后会同步删除绑定的按需EIP。

如果需要保留EIP，请在删除VPN网关前对EIP进行解绑操作。

6.1.7.2 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。

6.1.7.3 通过 VPN 互访的主机需要购买 EIP 吗?

如果用户本地的主机通过VPN访问云上的ECS，此时ECS不需要购买EIP。

如果ECS要向公网用户提供服务，需要购买EIP。

6.1.7.4 为什么我开通 VPN 后，云端 ECS 会有公网 IP 的访问信息?

可能原因：在VPN对接之前，ECS已经绑定了EIP。该场景下，用户除了通过VPN，也可通过公网地址直接访问该ECS。

如果ECS主机只允许VPN内的主机访问，可在完成VPN对接后将ECS的EIP解绑。

6.1.8 路由设置

6.1.8.1 如何理解 VPN 连接中的对端网关和对端子网?

对端网关和对端子网是两个相对的概念，在建立VPN连接时，从云的角度出发，VPC网络就是本地子网，创建的VPN网关就是本地网关，与之对接的用户侧网络就是对端子网， 用户侧的网关就是对端网关。

对端网关IP就是用户侧网关的公网IP，对端子网指需要和VPC子网互联的子网。

6.1.8.2 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到达对端子网的路由，无需手动配置。

6.1.8.3 ECS 主机多网卡是否需要添加去往线下网络的路由?

- 如果客户使用主网卡与线下网络建立了VPN，不需要添加路由。
- 如果客户使用非主网卡与线下网络建立了VPN，需要添加去往线下网段的路由指向非主网卡的网关。

6.1.9 VPN 子网设置

6.1.9.1 配置 VPN 连接的本端子网和对端子网时需要注意什么?

- 子网数量满足规格限制，数量超出规格限制请进行聚合汇总。
  - 每个VPN网关配置的本地子网数量：50。
  - 每个VPN连接支持配置的对端子网个数：50。
- 本端子网不可以包含对端子网，对端子网可以包含本端子网。
- 推荐配置的本端子网在VPC内有路由可达。
- 同一个VPN网关创建两条连接：若这两条连接的对端子网存在包含关系，在访问的目的网络处于交集网段部分时，按照创建连接的先后顺序匹配VPN连接，且与连接状态无关（策略模式不能按照掩码长度进行匹配）。

6.1.9.2 VPN 本端子网和对端子网的数量有限制吗?

- 每个VPN网关配置的本地子网数量：50
- 每个VPN连接支持配置的对端子网个数：50

6.1.9.3 创建 VPN 连接时添加对端子网，提示系统异常，如何处理?

检查VPC内是否存在对等连接、云专线、云连接的子网路由使用了该子网，导致VPN下发子网路由冲突，确认后将其配置的子网路由删除后重新创建即可。

6.1.9.4 VPN 网关删除后公网地址是否可以保留?

按需VPN网关如果绑定了按需EIP，则VPN网关删除后会同步删除绑定的按需EIP。

如果需要保留EIP，请在删除VPN网关前对EIP进行解绑操作。

6.1.9.5 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、100.64.0.0/12和214.0.0.0/8的网段。

  如果需要使用100.64.0.0/10或100.64.0.0/12，请提交工单申请。

6.1.9.6 创建 VPN 网关时 IP 是如何分配的?

VPN网关IP是一组提前规划好的地址组，提前预置了VPN的相关配置。

在用户创建VPN网关时，系统会随机分配一个IP地址和VPC进行绑定，且这个IP地址也只能绑定1个VPC。

因为VPN的网关IP存在预置数据，在创建VPN网关时也不能指定IP地址。删除VPN网关时会释放IP地址与VPC的绑定关系；重新创建VPN网关时系统会重新随机分配网关IP地址。

6.1.10 VPN 感兴趣流

6.1.10.1 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置?

VPN连接的“连接模式”选择“策略模式”时，才需要在管理控制台上配置策略规则ACL。

6.1.10.2 如何配置和修改云上 VPN 的感兴趣流?

感兴趣流由本端子网与对端子网full-mesh生成，例如本端子网有2个，分别为A与B，对端子网有3个，分别为C、D和E，生成感兴趣流时ACL的rule如下：

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

在管理控制台界面修改本端子网和对端子网会自动更新感兴趣流信息，即修改了云上的ACL配置。

6.1.11 VPN 连接保活

6.1.11.1 如何防止 VPN 连接出现中断情况?

VPN连接在正常的使用过程中会存在重协商情况，触发重协商的条件有IPsec SA的生命周期即将到期和VPN传输的流量超过20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的ACL不匹配。
- SA生命周期不匹配。
- 用户侧数据中心未配置DPD。
- VPN使用过程中修改了配置信息。
- 运营商网络抖动。

因此请在配置VPN时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像。

- SA生命周期信息一致。
- 用户侧数据中心网关开启DPD配置，探测次数不少于3次。
- 连接过程中修改参数两侧同步修改。
- 设置用户侧数据中心设备TCP MAX-MSS为1300。
- 确保用户侧数据中心出口有足够的带宽可被VPN使用。
- 确认VPN连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置。

6.1.12 监控类

6.1.12.1 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。

6.1.12.2 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连接创建后即会向云监控服务CES上报状态信息，但是并不会自动向用户发送告警通知，需要在页面左上角单击☰图标，选择“管理与监管 > 云监控”创建告警规则。

6.1.12.3 VPN 监控能不能查看每条连接的流量?

VPN的流量监控是基于VPN网关的，可查看该VPN网关的出入方向的流量、带宽等信息，无法查看单独的某一条连接的流量使用情况。

6.1.13 带宽与网速

6.1.13.1 如何测试 VPN 速率情况?

假设测试环境VPN连接已经创建，在VPN连接两端VPC的本端子网下分别创建ECS，并使两个VPC之间的ECS相互能够ping通的情况下，测试VPN的速率情况。

当用户购买的VPN网关的带宽为200Mbit/s时，测试情况如下。

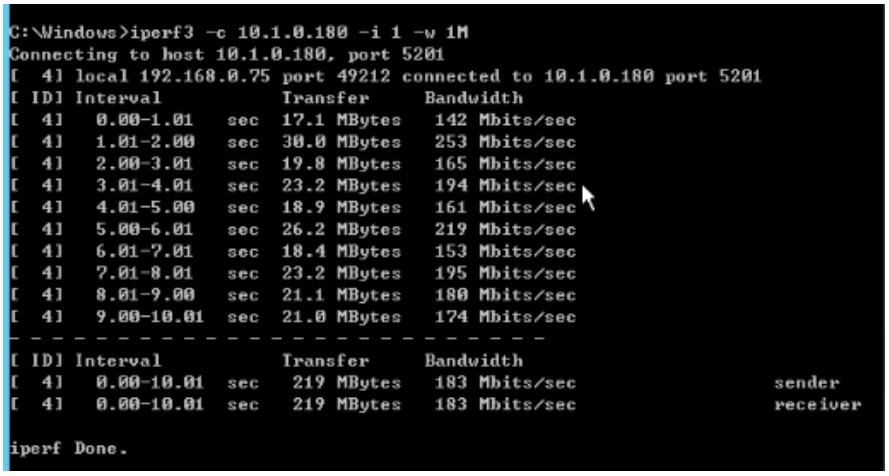
1. 互为对端的ECS都使用Windows系统，测试速率可达180Mbit/s，使用iperf3和filezilla（是一款支持ftp的文件传输工具）测试均满足带宽要求。

说明

基于TCP的FTP协议有拥塞控制机制，180Mbit/s为平均速率，且IPsec协议会增加新的IP头，因此10%左右的速率误差在网络领域是正常现象。

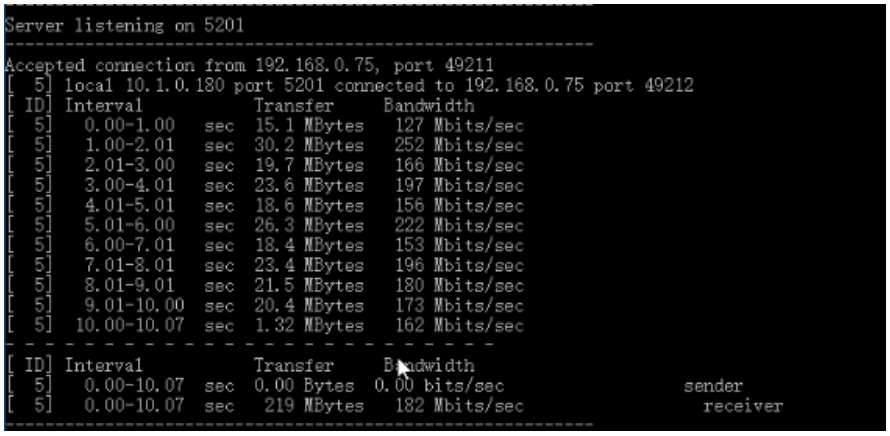
使用iperf3客户端测试结果截图如图6-5所示。

图 6-5 200M 带宽客户端 iperf3 测试结果



使用iperf3服务器端测试结果截图如图6-6所示。

图 6-6 200M 带宽服务端 iperf3 测试结果

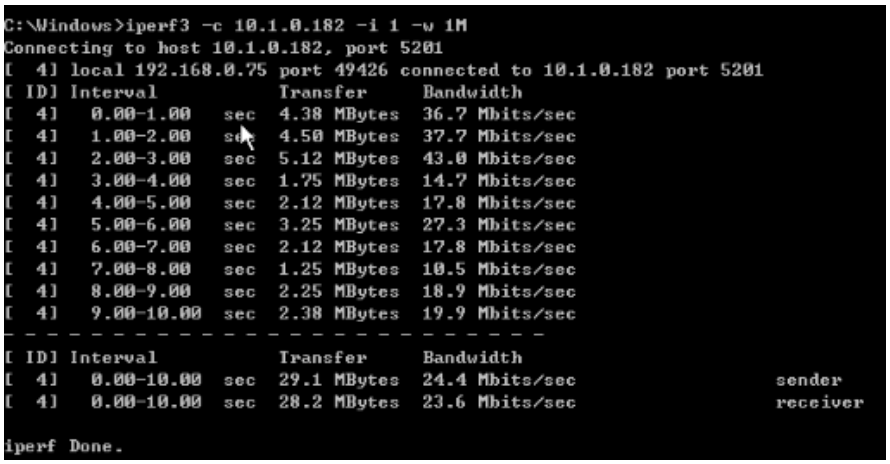


2. 互为对端的ECS都使用Centos7系统，测试速率可达180M，使用iperf3测试满足带宽要求。
3. 服务器端ECS使用Centos7系统，客户端使用Windows系统，测试速率只有20M左右，使用iperf3和filezilla测试均不能满足带宽要求。

   原因在于Windows和Linux对TCP的实现不一致，导致速率慢。所以对端ECS使用不同的系统时，无法满足带宽要求。

   使用iperf3测试结果截图如图6-7所示。

图 6-7 互为对端的 ECS 系统不同时 iperf3 测试结果



假设用户购买的VPN网关的带宽为1000Mbit/s。

用户购买的VPN网关为网关的整体吞吐能力，即该VPN网关下所有VPN连接的带宽之和。在大带宽场景下，由于主机的转发性能限制，需要使用多台主机构建多条流量才能充分利用网关的带宽。这种场景下对ECS的配置要求也很高，建议ECS的网卡支持2G以上的带宽。

测试总结：综上测试结果，云网关能够满足带宽速率要求，但是建议两端主机使用相同的操作系统，并且网卡要达到配置要求。

6.1.13.2 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么?

云上用户购买的VPN网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

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

按带宽计费度量采用国际统一的带宽单位Mbit，按流量计费的度量单位为GByte。

6.1.13.3 VPN 网关带宽到达限额时有什么影响?

VPN网关带宽限速限制的出VPC方向的带宽，如果您VPN网关的带宽超过限额使用时，会出现网络卡顿、部分子网间无法访问、甚至出现VPN连接中断现象（无法收到VPN的探测报文）。

因此在出现VPN网关带宽已达到上限时，建议您对VPN网关带宽进行扩容。

说明

VPN网关的带宽最大为1000(Mbit/s)。

6.1.13.4 修改了 VPN 带宽大小，为什么测试没有生效?

VPN带宽修改到生效会有一定的延迟，是正常现象。

请在修改带宽5分钟后再进行带宽测试。

说明

修改VPN带宽大小，不会导致用户业务和网络中断。

6.1.13.5 VPN 产品中的带宽和云专线的带宽有什么区别?

概念

- 云专线的带宽指用户创建的物理连接的带宽大小。
- VPN的带宽指的是出云方向的带宽。

带宽大小

- 云专线默认最大带宽1000(Mbit/s)，用户在管理控制台创建物理连接界面，“端口类型”参数选择“10GE单模光口”，支持最大带宽10Gbit/s
- VPN的带宽最大为1000(Mbit/s)。

网络质量

- 云专线用户独占一条网络资源，网络质量高。
- VPN是基于VPN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。网络质量依赖公网质量。

6.1.13.6 如何选择购买 VPN 带宽的大小?

购买VPN时，选择带宽大小需要考虑以下两个因素：

- VPN隧道中单位时间的数据传输量（需要冗余一定带宽，防止链路拥塞）。
- 考虑两端的出口带宽，云上带宽要小于云下出口带宽。

6.2 站点入云 VPN 经典版

6.2.1 热点问题

6.2.1.1 VPN 协商参数有哪些? 默认值是什么?

表 6-6 VPN 协商参数

协议	配置项	值
IKE	认证算法	• 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（默认） • SHA2-384 • SHA2-512

协议	配置项	值
	加密算法	• 3DES（此算法安全性较低，请慎用） • AES-256 • AES-192 • AES-128（默认）
	DH算法	• Group 5（此算法安全性较低，请慎用） • Group 2（此算法安全性较低，请慎用） • Group 14（默认） • Group 1（此算法安全性较低，请慎用） • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 **说明** 部分区域仅支持Group 14、Group 2、Group 5。
	版本	• v1（有安全风险不推荐） • v2（默认）
	生命周期	86400（默认） 单位：秒。 取值范围：60-604800。
IPsec	认证算法	• 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（默认） • SHA2-384 • SHA2-512
	加密算法	• AES-128（默认） • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用）

协议	配置项	值
	PFS	• DH group 5（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 14（默认） • DH group 1（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 • Disable **说明** 部分区域仅支持DH group 14、DH group 2、DH group 5。
	传输协议	• ESP（默认） • AH • AH-ESP
	生命周期	3600（默认） 单位：秒。 取值范围：480-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

  IKE协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致IPsec VPN受到侵犯。为提升密钥管理的安全性，IKE提供了PFS（完美向前保密）功能。启用PFS后，在进行IPsec SA协商时会进行一次附加的DH交换，重新生成新的IPsec SA密钥，提高了IPsec SA的安全性。
- 为了增强安全性，云默认开启PFS，请用户在配置用户侧数据中心网关设备时确认也开启了该功能，否则会导致协商失败。
- 用户开启此功能的同时，需要保证两端配置一致。
- IPsec SA字节生命周期，不是VPN服务可配置参数，云侧采用的是默认配置1843200KB。该参数不是协商参数，不影响双方建立IPsec SA。

6.2.1.2 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联?

VPN连通的是两个子网，即云上VPC网络与用户数据中心网络。

VPN成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是IPsec VPN的典型场景，请用户放心使用。

同时VPN连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通VPN以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行ping，获取网络的丢包和时延情况。

6.2.1.3 是否可以通过 VPN 实现跨境访问网站?

您咨询的场景不属于此范畴。

VPN实现的是将云上的VPC子网和用户侧数据中心的IDC网络打通的场景，即站点与站点互通（site to site）。

6.2.1.4 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连接创建后即会向云监控服务上报状态信息，但是并不会自动向用户发送告警通知，需要在页面左上角单击☰图标，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。

6.2.1.5 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，密钥是配置在VPN网关上的，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。

6.2.1.6 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

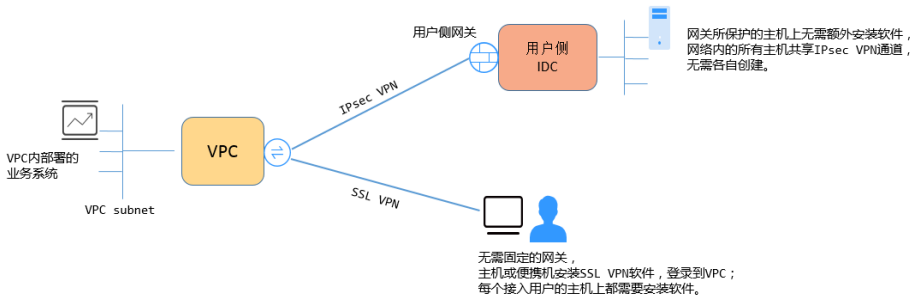
IPsec VPN连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网，即IPsec VPN是网对网的连接。

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，即SSL VPN是点对网的连接。

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。

6.2.1.7 VPN 网关删除后公网地址是否可以保留?

VPN网关删除后不保留网关IP。

通过管理控制台界面删除VPN网关后， VPN网关相关联的资源，如公网IP，配置信息即被释放，不会保留。

须知

在按需计费模式下，删除最后一个连接会同步删除网关，用户如果需要保留公网IP，请确保不要删除最后一个VPN连接。

6.2.1.8 VPN 监控可以监控哪些内容?

VPN网关

可监控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；查询网关监控状态请在VPN网关列表中选择“操作 > 查看监控”即可。

VPN连接

可监控连接的状态，1为正常、0为未连接；查询VPN连接监控请在VPN连接列表中选择“操作 > 更多 > 查看监控”。

6.2.1.9 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么?

云上用户购买的VPN网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

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

按带宽计费度量采用国际统一的带宽单位Mbit，按流量计费的度量单位为GByte。

6.2.1.10 如何测试 VPN 速率情况?

当测试环境为已创建VPN连接，并在VPN连接的本端子网下创建ECS，并使其相互能够ping通的情况下，测试VPN的速率情况。

当用户购买的VPN网关的带宽为200Mbit/s时，测试情况如下。

1. 互为对端的ECS都使用Windows系统，测试速率可达180Mbit/s，使用iperf3和filezilla（是一款支持ftp的文件传输工具）测试均满足带宽要求。

   说明

   基于TCP的FTP协议有拥塞控制机制，180Mbit/s为平均速率，且IPsec协议会增加新的IP头，因此10%左右的速率误差在网络领域是正常现象。

   使用iperf3客户端测试结果截图如图6-8所示。

   图 6-8 200M 带宽客户端 iperf3 测试结果

   ```
   C:\Windows>iperf3 -c 10.1.0.180 -i 1 -w 1M
   Connecting to host 10.1.0.180, port 5201
   [  4] local 192.168.0.75 port 49212 connected to 10.1.0.180 port 5201
   [ ID] Interval           Transfer     Bandwidth
   [  4]   0.00-1.01   sec  17.1 MBytes   142 Mbits/sec
   [  4]   1.01-2.00   sec  30.0 MBytes   253 Mbits/sec
   [  4]   2.00-3.01   sec  19.8 MBytes   165 Mbits/sec
   [  4]   3.01-4.01   sec  23.2 MBytes   194 Mbits/sec
   [  4]   4.01-5.00   sec  18.9 MBytes   161 Mbits/sec
   [  4]   5.00-6.01   sec  26.2 MBytes   219 Mbits/sec
   [  4]   6.01-7.01   sec  18.4 MBytes   153 Mbits/sec
   [  4]   7.01-8.01   sec  23.2 MBytes   195 Mbits/sec
   [  4]   8.01-9.00   sec  21.1 MBytes   180 Mbits/sec
   [  4]   9.00-10.01  sec  21.0 MBytes   174 Mbits/sec
   - - - - - - - - - - - - - - - - - - - - - - - - -
   [ ID] Interval           Transfer     Bandwidth
   [  4]   0.00-10.01  sec   219 MBytes   183 Mbits/sec                  sender
   [  4]   0.00-10.01  sec   219 MBytes   183 Mbits/sec                  receiver

   iperf Done.
   ```

   使用iperf3服务器端测试结果截图如图6-9所示。

   图 6-9 200M 带宽服务端 iperf3 测试结果

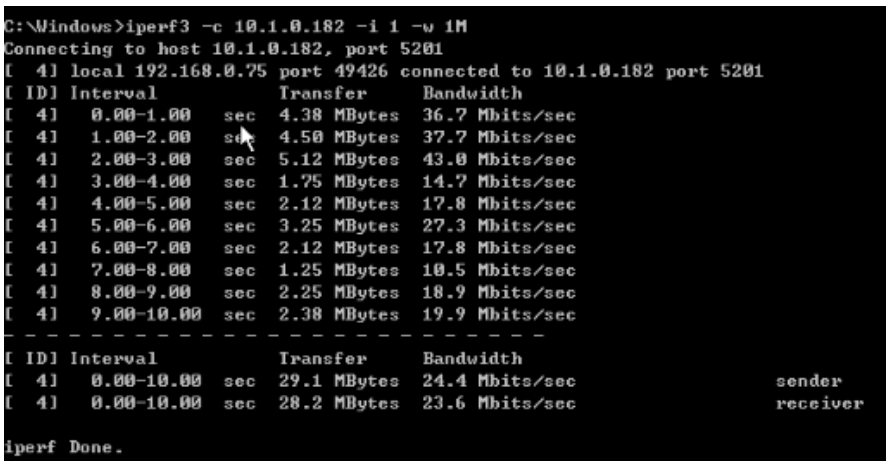
   ```
   -----------------------------------------------------------
   Server listening on 5201
   -----------------------------------------------------------
   Accepted connection from 192.168.0.75, port 49211
   [  5] local 10.1.0.180 port 5201 connected to 192.168.0.75 port 49212
   [ ID] Interval           Transfer     Bandwidth
   [  5]   0.00-1.00   sec  15.1 MBytes   127 Mbits/sec
   [  5]   1.00-2.01   sec  30.2 MBytes   252 Mbits/sec
   [  5]   2.01-3.00   sec  19.7 MBytes   166 Mbits/sec
   [  5]   3.00-4.01   sec  23.6 MBytes   197 Mbits/sec
   [  5]   4.01-5.01   sec  18.6 MBytes   156 Mbits/sec
   [  5]   5.01-6.00   sec  26.3 MBytes   222 Mbits/sec
   [  5]   6.00-7.01   sec  18.4 MBytes   153 Mbits/sec
   [  5]   7.01-8.01   sec  23.4 MBytes   196 Mbits/sec
   [  5]   8.01-9.01   sec  21.5 MBytes   180 Mbits/sec
   [  5]   9.01-10.00  sec  20.4 MBytes   173 Mbits/sec
   [  5]  10.00-10.07  sec  1.32 MBytes   162 Mbits/sec
   - - - - - - - - - - - - - - - - - - - - - - - - -
   [ ID] Interval           Transfer     Bandwidth
   [  5]   0.00-10.07  sec  0.00 Bytes  0.00 bits/sec                  sender
   [  5]   0.00-10.07  sec   219 MBytes   182 Mbits/sec                  receiver
   -----------------------------------------------------------
   ```

2. 互为对端的ECS都使用Centos7系统，测试速率可达180M，使用iperf3测试满足带宽要求。
3. 服务器端ECS使用Centos7系统，客户端使用Windows系统，测试速率只有20M左右，使用iperf3和filezilla测试均不能满足带宽要求。

原因在于Windows和Linux对TCP的实现不一致，导致速率慢。所以对端ECS使用不同的系统时，无法满足带宽要求。

使用iperf3测试结果截图如图6-10所示。

图 6-10 互为对端的 ECS 系统不同时 iperf3 测试结果



假设用户购买的VPN网关的带宽为1000Mbit/s，

用户购买的VPN网关为网关的整体吞吐能力，即该VPN网关下所有VPN连接的带宽之和。在大带宽场景下，由于主机的转发性能限制，需要使用多台主机构建多条流量才能充分利用网关的带宽。这种场景下对ECS的配置要求也很高，建议ECS的网卡支持2G以上的带宽。

测试总结：综上测试结果，云网关能够满足带宽速率要求，但是建议两端主机使用相同的操作系统，并且网卡要达到配置要求。

6.2.1.11 按流量计费的 VPN 可以使用共享流量包?

不可以。

当前VPN服务独立计费，不能使用共享流量包。

6.2.1.12 VPC、VPN 网关、VPN 连接之间有什么关系?

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

- VPC
  - 即云上私有专用网络，同一Region中可以创建多个VPC，且VPC之间相互隔离。一个VPC内可以划分多个子网网段。
  - 用户可以通过VPN服务，安全访问VPC内的ECS。
- VPN网关
  - 基于VPC创建，是VPN连接的接入点。一个VPC仅能购买一个VPN网关，每个网关可以创建多个VPN连接。
  - 用户可以通过VPN网关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

基于VPN网关创建，用于连通VPC子网和用户数据中心（或其它Region的VPC）子网，即每个VPN连接连通了一个用户侧数据中心的网关。

说明

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

6.2.1.13 如何理解 VPN 连接中的远端网关和远端子网?

远端网关和远端子网是个相对的概念，在建立VPN连接时，从云的角度出发，VPC网络就是本地子网，创建的VPN网关就是本地网关，与之对接的用户侧网络就是远端子网， 用户侧的网关就是远端网关。

远端网关IP就是用户侧网关的公网IP，远端子网指需要和VPC子网互联的子网。

6.2.1.14 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。

6.2.1.15 VPN 支持将两个 VPC 互连吗?

- 如果两个VPC位于同一区域内，不支持VPN互连，推荐使用VPC对等连接互连。
- 如果两个VPC位于不同区域，支持VPN互连，具体操作如下：
  a. 为这两个VPC分别创建VPN网关，并为两个VPN网关创建VPN连接。
  b. 将两个VPN连接的远端网关设置为对方VPN网关的网关IP。
  c. 将两个VPN连接的远端子网设置为对方VPC的网段。
  d. 两个VPN连接的预共享密钥和算法参数需保持一致。

6.2.1.16 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。

6.2.1.17 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置?

不可以。

云端创建VPN时，本端子网为VPC内部子网，远端子网为客户用户侧数据中心子网，两条连接使用相同的本端子网和远端子网是无法进行创建的。

6.2.1.18 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。

6.2.1.19 如何解决无法建立连接问题?

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
   ```
3. 配置完成后检查VPN是否连接，ping测试两端内网是否正常。

6.2.1.20 EIP 能作为 VPN 的网关 IP 吗?

企业版VPN可以；经典版VPN不可以。

6.2.1.21 VPN 配置完成了，为什么连接一直处于未连接状态?

首先需要确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/远端子网、本端网关/远端网关互为镜像。

其次确认用户侧数据中心设备的路由、NAT和安全策略配置无误，最后通过两端的子网互PING远端子网主机。

说明

因为VPN是基于数据流触发的，在配置完成后需要从任一端子网主机ping远端子网主机，ping之前请关闭主机防火墙，云上安全组开启入方向ICMP。

ping网关IP无法触发VPN协商，需要ping网关保护的子网中的主机。

6.2.1.22 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6-7所示。

表 6-7 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。

6.2.1.23 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置?

用户侧数据中心配置VPN设备时，是需要独立创建ACL，且该ACL会被IPsec的策略引用。

云上配置VPN服务时，会根据管理控制台界面填入的本端子网和远端子网自动生成ACL，然后下发给VPN网关。其中ACL中的rule数量是两端子网数量的乘积。

6.2.2 产品咨询

6.2.2.1 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SNAT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。

6.2.2.2 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远端网关之间的安全、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。

6.2.2.3 VPC、VPN 网关、VPN 连接之间有什么关系?

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

- VPC
  - 即云上私有专用网络，同一Region中可以创建多个VPC，且VPC之间相互隔离。一个VPC内可以划分多个子网网段。
  - 用户可以通过VPN服务，安全访问VPC内的ECS。
- VPN网关
  - 基于VPC创建，是VPN连接的接入点。一个VPC仅能购买一个VPN网关，每个网关可以创建多个VPN连接。
  - 用户可以通过VPN网关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

  基于VPN网关创建，用于连通VPC子网和用户数据中心（或其它Region的VPC）子网，即每个VPN连接连通了一个用户侧数据中心的网关。

  说明

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

6.2.2.4 如何理解 VPN 连接中的远端网关和远端子网?

远端网关和远端子网是个相对的概念，在建立VPN连接时，从云的角度出发，VPC网络就是本地子网，创建的VPN网关就是本地网关，与之对接的用户侧网络就是远端子网， 用户侧的网关就是远端网关。

远端网关IP就是用户侧网关的公网IP，远端子网指需要和VPC子网互联的子网。

6.2.2.5 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、100.64.0.0/12和214.0.0.0/8的网段。

  如果需要使用100.64.0.0/10或100.64.0.0/12，请提交工单申请。

6.2.2.6 VPN 协商参数有哪些? 默认值是什么?

表 6-8 VPN 协商参数

协议	配置项	值
IKE	认证算法	● 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（默认） ● SHA2-384 ● SHA2-512
	加密算法	● 3DES（此算法安全性较低，请慎用） ● AES-256 ● AES-192 ● AES-128（默认）
	DH算法	● Group 5（此算法安全性较低，请慎用） ● Group 2（此算法安全性较低，请慎用） ● Group 14（默认） ● Group 1（此算法安全性较低，请慎用） ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 **说明** 部分区域仅支持Group 14、Group 2、Group 5。
	版本	● v1（有安全风险不推荐） ● v2（默认）
	生命周期	86400（默认） 单位：秒。 取值范围：60-604800。

协议	配置项	值
IPsec	认证算法	● 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（默认） ● SHA2-384 ● SHA2-512
	加密算法	● AES-128（默认） ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用）
	PFS	● DH group 5（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 14（默认） ● DH group 1（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 ● Disable **说明** 部分区域仅支持DH group 14、DH group 2、DH group 5。
	传输协议	● ESP（默认） ● AH ● AH-ESP
	生命周期	3600（默认） 单位：秒。 取值范围：480-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

  IKE协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致IPsec VPN受到侵犯。为提升密钥管理的安全性，IKE提供了PFS（完美向前保密）功能。启用PFS后，在进行IPsec SA协商时会进行一次附加的DH交换，重新生成新的IPsec SA密钥，提高了IPsec SA的安全性。
- 为了增强安全性，云默认开启PFS，请用户在配置用户侧数据中心网关设备时确认也开启了该功能，否则会导致协商失败。
- 用户开启此功能的同时，需要保证两端配置一致。
- IPsec SA字节生命周期，不是VPN服务可配置参数，云侧采用的是默认配置1843200KB。该参数不是协商参数，不影响双方建立IPsec SA。

6.2.2.7 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。

6.2.2.8 如何在已创建的 VPN 连接中，限定特定的主机访问云上子网?

云下限制：

- VPN设备的按照策略中限制访问
- 路由器或交换机上设置ACL限制

云上限制：

- 安全组限制源IP
- ACL限制

说明

所有的限定规则需要添加在建立VPN隧道之前的设备上。不建议通过修改本端子网和远端子网的方式来限定访问。

6.2.2.9 VPN 监控可以监控哪些内容?

VPN网关

可监控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；查询网关监控状态请在VPN网关列表中选择“操作 > 查看监控”即可。

VPN连接

可监控连接的状态，1为正常、0为未连接；查询VPN连接监控请在VPN连接列表中选择“操作 > 更多 > 查看监控”。

6.2.2.10 EIP 能作为 VPN 的网关 IP 吗?

不可以。

VPN网关IP是在创建VPN网关时分配的，需要和系统内的相关配置信息结合使用，EIP不具备VPN对接服务的功能。

6.2.2.11 通过 VPN 互访的主机需要购买 EIP 吗?

如果用户本地的主机通过VPN访问云上的ECS，此时ECS不需要购买EIP。

如果ECS要向公网用户提供服务，需要购买EIP。

6.2.2.12 VPN 配置下发后，多久能够生效?

用户在管理控制台中完成VPN资源创建后，配置1-5分钟下发完成，下发后立即生效。

说明

VPN配置下发成功后，并不表示VPN连接已经建立成功，用户还需要对用户侧网关设备进行配置，完成与VPN网关的隧道协商。

6.2.2.13 VPN 是否支持 IPv6?

不支持。

当前云只支持IPv4。

6.2.2.14 如何选择购买 VPN 带宽的大小?

购买VPN时，选择带宽大小需要考虑以下两个因素：

- VPN隧道中单位时间的数据传输量（需要冗余一定带宽，防止链路拥塞）。
- 考虑两端的出口带宽，云上带宽要小于云下出口带宽。

6.2.2.15 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。

云将大力推进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漏的风险，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。

- 修复了多处公认的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。

6.2.2.16 VPN 使用的 DH group 对应的比特位是多少?

Diffie-Hellman(DH)组确定密钥交换过程中使用的密钥的强度。较高的组号更安全，但需要额外的时间来计算密钥。

VPN使用的DH group对应的比特位如表6-9所示。

表 6-9 DH group 对应比特位

DH group	Modulus
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	ecp256 bits
20	ecp384 bits
21	ecp521 bits

说明

以下DH算法有安全风险，不推荐使用：DH group 1、DH group 2、DH group 5。

6.2.2.17 是否可以通过 VPN 实现跨境访问网站?

您咨询的场景不属于此范畴。

VPN实现的是将云上的VPC子网和用户侧数据中心的IDC网络打通的场景，即站点与站点互通（site to site）。

6.2.2.18 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联?

VPN连通的是两个子网，即云上VPC网络与用户数据中心网络。

VPN成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是IPsec VPN的典型场景，请用户放心使用。

同时VPN连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通VPN以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行ping，获取网络的丢包和时延情况。

6.2.2.19 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

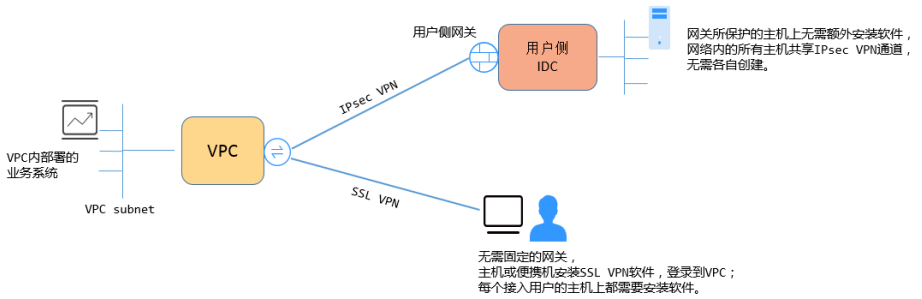
IPsec VPN：连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网；即IPsec VPN是网对网的连接。

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。

6.2.2.20 VPN 网关带宽计费方式在选择按带宽计费和按流量计费时有什么差别?

VPN网关带宽的计费方式是针对VPN网关的。

如果选择按需付费方式（即后付费），可以选择按带宽或按流量计费：

- 按带宽计费，计费的周期为1小时，费用也会因带宽大小存在差异。

- 按流量计费，统计1小时内产生的流量费用，调整带宽大小不产生计费差异，只按产生的出VPC流量进行计费。

6.2.2.21 按流量计费的 VPN 可以使用共享流量包?

不可以。

当前VPN服务独立计费，不能使用共享流量包。

6.2.2.22 VPN 网关删除后公网地址是否可以保留?

VPN网关删除后不保留网关IP。

通过管理控制台界面删除VPN网关后， VPN网关相关联的资源，如公网IP，配置信息即被释放，不会保留。

须知

在按需计费模式下，删除最后一个连接会同步删除网关，用户如果需要保留公网IP，请确保不要删除最后一个VPN连接。

6.2.2.23 通过 VPN 互访的主机需要购买 EIP 吗?

如果用户本地的主机通过VPN访问云上的ECS，此时ECS不需要购买EIP。

如果ECS要向公网用户提供服务，需要购买EIP。

6.2.2.24 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。

6.2.2.25 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，需要在页面左上角单击三图标，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。

6.2.2.26 如何解决无法建立连接问题?

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
```

3. 配置完成后检查VPN是否连接，ping测试两端内网是否正常。

6.2.2.27 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？

云上用户购买的VPN网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

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

按带宽计费度量采用国际统一的带宽单位Mbit，按流量计费的度量单位为GByte。

6.2.3 组网与使用场景

6.2.3.1 是否可以通过 VPN 实现跨境访问网站?

您咨询的场景不属于此范畴。

VPN实现的是将云上的VPC子网和用户侧数据中心的IDC网络打通的场景，即站点与站点互通（site to site）。

6.2.3.2 是否可以将应用部署在云端，数据库放在本地 IDC，然后通过 VPN 实现互联?

VPN连通的是两个子网，即云上VPC网络与用户数据中心网络。

VPN成功建立后，两个子网间可以运行任何类型的业务流量，此时应用服务器访问数据库业务在逻辑上和访问同一局域网的其它主机是相同的，因此该方案可行的。

这种场景是IPsec VPN的典型场景，请用户放心使用。

同时VPN连通以后，并不限定业务的发起方是云上还是用户侧数据中心，即用户可以从云上向用户侧数据中心发起业务，也可以反向。

须知

- 用户在打通VPN以后，需要关注网络延迟和丢包情况，避免影响业务正常运行。
- 建议用户先运行ping，获取网络的丢包和时延情况。

6.2.3.3 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。

6.2.3.4 多人访问 ECS，是否可以给每个客户机安装一套 IPsec 软件和云端建立 VPN 连接?

不可以。

VPN打通的是两个局域网的网络，用户侧数据中心局域网内多台主机都安装IPsec软件，实际情况是用户侧数据中心多个主机使用同一个公网IP与云端对接，云端的VPN网关会收到来自用户侧数据中心不同主机的协商报文，系统会收到大量的重复协商信息，导致连接异常，甚至出现连接不可用的现象。

建议您使用出口的防火墙设备配置VPN与云端进行对接。建立VPN时可以选择多个网段，结合云上安全组或用户侧数据中心安全策略，限定属于开发人员主机才能访问云端ECS。

6.2.3.5 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

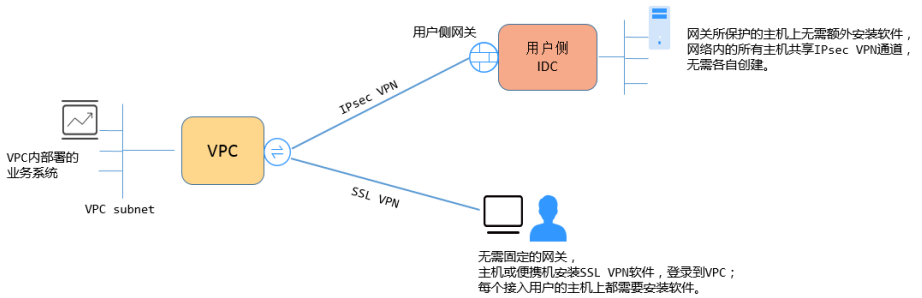
IPsec VPN：连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网；即IPsec VPN是网对网的连接。

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。

6.2.3.6 VPN 支持将两个 VPC 互连吗?

- 如果两个VPC位于同一区域内，不支持VPN互连，推荐使用VPC对等连接互连。

- 如果两个VPC位于不同区域，支持VPN互连，具体操作如下：
  a. 为这两个VPC分别创建VPN网关，并为两个VPN网关创建VPN连接。
  b. 将两个VPN连接的远端网关设置为对方VPN网关的网关IP。
  c. 将两个VPN连接的远端子网设置为对方VPC的网段。
  d. 两个VPN连接的预共享密钥和算法参数需保持一致。

6.2.3.7 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。

6.2.3.8 通过 VPN 来实现云下 IDC 与云端 VPC 的互通，两端分别需要做哪些配置?

VPN对接的工作分为两个部分：云上创建VPN和用户侧数据中心配置VPN设备。

- 云上创建VPN：购买VPN网关，选定计费模式、带宽大小、指定对接的VPC；购买VPN连接，指定两端网关IP，两端子网和协商策略。
- 用户侧数据中心配置VPN设备：选定用户侧数据中心公网IP，在支持IPsec VPN的设备上完成IPsec协商的一、二阶段配置，然后进行网络路由、NAT和安全策略配置。

6.2.3.9 在多出口的网络中，能否使用两个出口分别与同一 VPC 建立 VPN 连接做冗余配置?

不可以。

云端创建VPN时，本端子网为VPC内部子网，远端子网为客户用户侧数据中心子网，两条连接使用相同的本端子网和远端子网是无法进行创建的。

6.2.3.10 同一个 Region 的两个 VPC 可以通过 VPN 连通吗?

不可以。

对于同Region的两个VPC，您可以通过对等连接（VPC peering）或者云连接（CC）打通两个VPC。

6.2.3.11 可以通过哪些方式连通同一个 Region 的两个 VPC?

可通过创建对等连接或者云连接的方式打通同Region的两个VPC，对等连接只用同Region的VPC，云连接可连通不同Region的VPC。

6.2.3.12 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。

6.2.3.13 云端创建了两个 VPC，如何与云下的 IDC 网络互通?

组网拓扑

IDC-VPC1-VPC2。

说明

其中IDC表示用户数据中心，VPC1与IDC建立VPN连接。

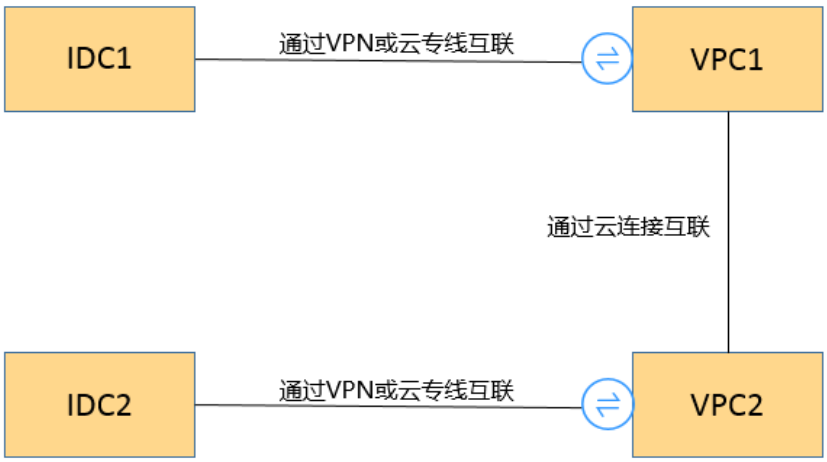
配置步骤

1. 确认云上的两个VPC是否在同一Region。
   - 如果在同一Region可通过对等连接或云连接（CC）将两个VPC连接起来（免费）。
   - 如果两个VPC跨Region，请使用CC进行互联（需支付CC带宽费用）。
2. 用户侧数据中心IDC与其中一个VPC建立VPN连接，修改用户侧数据中心设备的远端子网为云上两个VPC子网，VPN对接的VPC1本端子网需要包含通过对等连接或CC连接的子网，对等连接或CC的子网路由包含用户侧数据中心IDC子网。

6.2.3.14 组网拓扑如（IDC1-VPC1-VPC2-IDC2）所示，如何实现四个子网互联?

组网拓扑如图6-11所示。

图 6-11 组网拓扑



1. IDC1可通过VPN或DC与VPC1互联。
2. 两个VPC之间使用CC互联（同Region也可以使用对端连接）。
3. IDC2可通过VPN或DC与VPC2互联。
4. 同时完成VPN子网更新、CC及DC子网路由更新即可实现四个子网相互访问。

6.2.3.15 云端两个 Region，每 Region 有两个子网，是否可以创建两个 VPN 连接，分别连通不同子网？

不可以。

两个Region间只需创建一个VPN连接即可，在VPN连接中将两个子网都加入到VPN中。

针对这种场景，如果用户试图去创建第二条VPN连接，由于两个连接的远端网关地址一样，因此管理控制台界面会提示冲突。

6.2.3.16 用户本地电脑如何连接 VPN？

普通家庭宽带路由器、个人的移动终端设备、Windows主机自带的VPN服务（如L2TP）无法与云进行VPN对接。

与云下对接需要对端有支持标准IPsec协议的设备。

6.2.3.17 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络的组成部分，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。

6.2.3.18 购买 VPN 网关和连接后，发现云下没有支持 IPsec 的设备，如何临时建立 VPN 连接?

与VPN网关连通时，需要云下有支持标准的IPsec设备和固定公网IP，二者缺一不可。

如果需要临时与云对接，可通过在主机上安装第三方软件完成与云的对接。

第三方IPsec软件推荐：strongSwan、Openswan、TheGreenBow等。

6.2.3.19 如何选择在云上的哪个区域创建 VPN 网关?

在云上创建VPN网关，您可以选择任一区域的VPC进行创建。

推荐您选择与IDC同城的区域创建VPN网关，这样可以更大程度降低因公网质量对VPN的影响。

- 同区域的多个VPC，只需创建一个VPN网关，其它VPC可以通过对等连接（免费）打通。
- 跨区域的多个VPC，可以通过VPN+CC的方式进行打通。

6.2.4 Console 与页面使用

6.2.4.1 VPC、VPN 网关、VPN 连接之间有什么关系?

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

- VPC
  - 即云上私有专用网络，同一Region中可以创建多个VPC，且VPC之间相互隔离。一个VPC内可以划分多个子网网段。
  - 用户可以通过VPN服务，安全访问VPC内的ECS。
- VPN网关
  - 基于VPC创建，是VPN连接的接入点。一个VPC仅能购买一个VPN网关，每个网关可以创建多个VPN连接。
  - 用户可以通过VPN网关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

  基于VPN网关创建，用于连通VPC子网和用户数据中心（或其它Region的VPC）子网，即每个VPN连接连通了一个用户侧数据中心的网关。

  说明

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

6.2.4.2 VPN 配置下发后，多久能够生效?

用户在管理控制台完成VPN资源创建后，配置1-5分钟下发完成，下发后立即生效。

说明

VPN配置下发成功后，并不表示VPN连接已经建立成功，用户还需要对用户侧网关设备进行配置，完成与VPN网关的隧道协商。

6.2.4.3 VPN 配置完成了，为什么连接一直处于未连接状态?

首先需要确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/远端子网、本端网关/远端网关互为镜像。

其次确认用户侧数据中心设备的路由、NAT和安全策略配置无误，最后通过两端的子网互PING远端子网主机。

说明

因为VPN是基于数据流触发的，在配置完成后需要从任一端子网主机ping远端子网主机，ping之前请关闭主机防火墙，云上安全组开启入方向ICMP。

ping网关IP无法触发VPN协商，需要ping网关保护的子网中的主机。

6.2.4.4 VPN 网关删除后公网地址是否可以保留?

VPN网关删除后不保留网关IP。

通过管理控制台界面删除VPN网关后， VPN网关相关联的资源，如公网IP，配置信息即被释放，不会保留。

须知

在按需计费模式下，删除最后一个连接会同步删除网关，用户如果需要保留公网IP，请确保不要删除最后一个VPN连接。

6.2.4.5 本地设备配置 VPN 时需要设置 ACL，为何在控制台上找不到对应的配置?

用户侧数据中心配置VPN设备时，是需要独立创建ACL，且该ACL会被IPsec的策略引用。

云上配置VPN服务时，会根据管理控制台界面填入的本端子网和远端子网自动生成ACL，然后下发给VPN网关。其中ACL中的rule数量是两端子网数量的乘积。

6.2.4.6 创建 VPN 连接时添加远端子网，提示系统异常，如何处理?

检查VPC内是否存在对等连接、云专线、云连接的子网路由使用了该子网，导致VPN下发子网路由冲突，确认后将其配置的子网路由删除后重新创建即可。

6.2.4.7 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。

6.2.4.8 如何理解 VPN 连接中的远端网关和远端子网?

远端网关和远端子网是两个相对的概念，在建立VPN连接时，从云的角度出发，VPC网络就是本地子网，创建的VPN网关就是本地网关，与之对接的用户侧网络就是远端子网， 用户侧的网关就是远端网关。

远端网关IP就是用户侧网关的公网IP，远端子网指需要和VPC子网互联的子网。

6.2.4.9 创建 VPN 连接时如何关闭 PFS 的 Group 配置?

云在部分区域开启了PFS的Disable选项，推荐用户侧数据中心也开启PFS的Group配置。

PFS功能可以增强IKE二阶段协商的安全性，建议用户开启功能。

部分设备厂商默认关闭了PFS功能，请用户查询设备配置手册确保PFS功能打开。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。
  IKE协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致IPsec VPN受到侵犯。为提升密钥管理的安全性，IKE提供了PFS（完美向前保密）功能。启用PFS后，在进行IPsec SA协商时会进行一次附加的DH交换，重新生成新的IPsec SA密钥，提高了IPsec SA的安全性。
- 为了增强安全性，云默认开启PFS，请用户在配置用户侧数据中心网关设备时确认也开启了该功能，否则会导致协商失败。

6.2.4.10 VPN 本端子网和远端子网的数量有限制吗，为什么我选择网段更新本地子网提示报错?

- 本端子网限制数量为5个，VPN本端子网和远端子网数量乘积最大支持到225。
- VPC会根据VPN的远端子网、专线的远端子网、VPC对等连接子网下发VPC子网路由，每个子网网段对应一条子网路由。
- VPC子网路由条目数不得大于200，即VPC中VPN远端子网数、专线的远端子网数、VPC对等连接子网数以及自定义路由条目数的总和不得大于200。

6.2.4.11 配置 VPN 连接的本端子网和远端子网时需要注意什么?

- 子网数量满足规格限制，数量超出规格限制请进行聚合汇总。
- 本端子网不可以包含远端子网，远端子网可以包含本端子网。
- 推荐配置的本端子网在VPC内有路由可达。
- 同一个VPN网关创建两条连接：若这两条连接的远端子网存在包含关系，在访问的目的网络处于交集网段部分时，按照创建连接的先后顺序匹配VPN连接，且与连接状态无关（策略模式不能按照掩码长度进行匹配）。

6.2.4.12 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接?

VPN连接状态刷新存在一定的延迟，业务已通但是网页上VPN连接状态还是未连接是正常现象。

如果数据面已正常（即业务访问已正常）， 连接就已经完成建立了，短暂等待后VPN连接状态就会更新为“已连接”。

6.2.4.13 修改协商策略后，页面显示资源不存在，如何处理?

此问题为页面刷新周期问题。

在修改连接高级策略时，系统会先删除，再重建VPN连接，如果在页面创建过程中出现短暂的删除中或创建中属于正常现象，切勿重复创建同一连接（本端子网、远端子网、远端网关相同的连接）；

6.2.4.14 如何重置已经建立的 VPN 连接?

- 在线下设备上关闭VPN连接，待云上VPN连接状态变为未连接后重新启动线下设备上的VPN连接；
- 更改线上VPN连接的远端网关IP为其它任意IP，待云下连接状态变为inactive后，重新将云上的远端网关IP修改为之前的IP。

6.2.4.15 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。

云将大力推进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漏的风险，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。
- 修复了多处公认的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。

6.2.4.16 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。

6.2.4.17 VPN 监控可以监控哪些内容?

VPN网关

可监控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；查询网关监控状态请在VPN网关列表中选择“操作 > 查看监控”即可。

VPN连接

可监控连接的状态，1为正常、0为未连接；查询VPN连接监控请在VPN连接列表中选择“操作 > 更多 > 查看监控”。

6.2.4.18 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，需要在页面左上角单击☰图标，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。

6.2.5 VPN 协商与对接

6.2.5.1 VPN 协商参数有哪些? 默认值是什么?

表 6-10 VPN 协商参数

协议	配置项	值
IKE	认证算法	• 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（默认） • SHA2-384 • SHA2-512
	加密算法	• 3DES（此算法安全性较低，请慎用） • AES-256 • AES-192 • AES-128（默认）

协议	配置项	值
	DH算法	• Group 5（此算法安全性较低，请慎用） • Group 2（此算法安全性较低，请慎用） • Group 14（默认） • Group 1（此算法安全性较低，请慎用） • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 **说明** 部分区域仅支持Group 14、Group 2、Group 5。
	版本	• v1 • v2（默认）
	生命周期	86400（默认） 单位：秒。 取值范围：60-604800。
IPsec	认证算法	• 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（默认） • SHA2-384 • SHA2-512
	加密算法	• AES-128（默认） • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用）

协议	配置项	值
	PFS	• DH group 5（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 14（默认） • DH group 1（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 • Disable **说明** 部分区域仅支持DH group 14、DH group 2、DH group 5。
	传输协议	• ESP（默认） • AH • AH-ESP
	生命周期	3600（默认） 单位：秒。 取值范围：480-604800。

说明

- PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性。

  IKE协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致IPsec VPN受到侵犯。为提升密钥管理的安全性，IKE提供了PFS（完美向前保密）功能。启用PFS后，在进行IPsec SA协商时会进行一次附加的DH交换，重新生成新的IPsec SA密钥，提高了IPsec SA的安全性。
- 为了增强安全性，云默认开启PFS，请用户在配置用户侧数据中心网关设备时确认也开启了该功能，否则会导致协商失败。
- 用户开启此功能的同时，需要保证两端配置一致。
- IPsec SA字节生命周期，不是VPN服务可配置参数，云侧采用的是默认配置1843200KB。该参数不是协商参数，不影响双方建立IPsec SA。

6.2.5.2 使用 VPN 连通云端 VPC 网络，云下设备如何配置?

首先按照网络的连接规划，明确用户侧数据中心子网、云上子网以及两端的网关公网IP信息。

其次按照云端VPN的协商策略信息完成用户侧数据中心设备的IPsec配置，并开启云上VPC主机关联的安全组的出入方向的ICMP报文。

- 路由设置：用户侧数据中心设备从子网的网关设备开始至VPN对接设备，逐跳添加去往云端子网的路由，下一跳指向连接VPN设备出方向的路由，在VPN设备上的路由指向出接口下一跳公网网关IP。
- NAT设置：在VPN设备上关闭本地子网访问云端子网的NAT，即本端子网访问云端子网不做NAT。最后在安全策略中双向放行本地子网和云端子网互访，双向放行云端VPN网关IP与本地VPN设备对接使用的公网IP的UDP500、UDP4500、ESP(IP protocol 50)、AH(IP protocol 51)报文。

6.2.5.3 VPN 支持远端网关域名对接吗?

云端VPN连接需要明确对端的公网IP地址，暂不支持通过域名方式与对端设备进行对接。

6.2.5.4 我创建的 VPN 连接有几个隧道?

VPN连接下的隧道和本端子网和远端子网的数量有关，隧道总数等于本端子网数和远端子网数的乘积。但在实际建立隧道时，只要有一个隧道的状态Active，连接的状态就会显示正常，如果需要每个隧道都处于Active状态，需要每两个子网间都进行数据流触发。

6.2.5.5 如何在已创建的 VPN 连接中，限定特定的主机访问云上子网?

云下限制：

- VPN设备的按照策略中限制访问
- 路由器或交换机上设置ACL限制

云上限制：

- 安全组限制源IP
- ACL限制

说明

所有的限定规则需要添加在建立VPN隧道之前的设备上。不建议通过修改本端子网和远端子网的方式来限定访问。

6.2.5.6 VPN 是否启动了 DPD 检测机制?

是的。

VPN服务默认开启了DPD探测机制，用于探测用户侧数据中心IKE进程的存活状态。

3次探测失败后即认为用户侧数据中心IKE异常，此时云会删除本端隧道，以保持双方的隧道同步。

DPD协议本身并不要求对端也同步进行配置（但是要求对端可以应答DPD探测），为了保证协商双方隧道状态一致，避免出现单边隧道（一端存在隧道，而另一端已不存在），建议用户同时启动用户侧网关的DPD探测机制，用于探测云侧VPN服务的IKE状态。

说明

DPD探测失败后会删除隧道，不会导致业务不稳定。

DPD可以及时发现对方IKE进程异常，并通过重置隧道的方法来保持双方隧道同步。在删除隧道后，当有用户流量时，可以重新触发协商并建立隧道。

6.2.5.7 如何通过安全组控制使 VPN 不能访问 VPC 上的部分虚拟机，实现安全隔离?

如果用户需要控制VPN站点只能访问VPC的部分网段或者部分主机，可以通过安全组进行控制。

配置示例：VPC内子网10.1.0.0/24下的ECS不允许访问客户侧的子网192.168.1.0/24，

配置方法：

1. 创建两个安全组：安全组1和安全组2。
2. 安全组1的入方向规则配置deny网段192.168.1.0/24。
3. 安全组2允许192.168.1.0/24访问。
4. 网段10.1.0.0/24的ECS选择安全组1，其他的主机选择安全组2。

6.2.5.8 修改 VPN 连接的配置会造成连接重建吗?

VPN连接包含本端子网、远端子网、远端网关、预共享密钥、IKE协商策略、IPsec协商策略。修改VPN连接具体包括以下几种情况：

- 修改本端子网和远端子网，连接ID不发生变化，只是更新了连接两端的子网信息，如果更新的是部分子网信息，已经建立的子网间隧道不会重建。
- 修改远端网关IP，连接ID不发生变化，但连接的对端已改变，连接需要重建。
- 仅修改连接的预共享密钥，连接的ID不发生变化，连接状态当时并不发生改变，重协商会重新校验密码匹配情况，如果密码不匹配重协商会失败。
- 修改协商策略（需验证预共享密钥），连接ID发生改变，相当于连接删除重建过程，连接需要重建。

6.2.5.9 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。

6.2.5.10 本地防火墙无法收到 VPN 网关的 IKE 第一阶段的回复包怎么解决?

1. 检查两端公网IP是否可以互访，推荐使用ping命令，云端网关IP缺省可以ping通。
2. 云下网关与云网关可以互访UDP 500、4500报文。
3. 云下公网IP访问网关IP时，没有发生源端口NAT转换，如果存在nat穿越，端口号在nat穿越后不得发生改变。
4. 两端的ike协商参数配置一致，nat穿越场景中云下ID标识类型选择IP，本地的标识选择NAT转换后的公网IP。

6.2.5.11 本地防火墙无法收到 VPN 子网的回复包怎么解决?

1. 如果二阶段协商中需要检查云下的路由、安全策略、NAT和感兴趣流、协商策略信息。
   - 路由设置：将访问云上子网的数据送入隧道。
   - 安全策略：放行云下子网访问云上子网的流量。
   - NAT策略：云下子网访问云上子网不做源nat。
   - 感兴趣流：两端感兴趣流配置互为镜像，使用IKE v2配置感兴趣流不可使用地址对象名称。
   - 协商信息：协商策略信息云上云下一致，特别注意PFS的配置。
2. 确认一、二阶段协商均已正常后，请检查云上安全组策略，放行入方向的云下子网访问云上子网的ICMP协议。

6.2.5.12 VPN 使用的 DH group 对应的比特位是多少?

Diffie-Hellman(DH)组确定密钥交换过程中使用的密钥的强度。较高的组号更安全，但需要额外的时间来计算密钥。

VPN使用的DH group对应的比特位如表6-11所示。

表 6-11 DH group 对应比特位

DH group	Modulus
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	ecp256 bits
20	ecp384 bits
21	ecp521 bits

说明

以下DH算法有安全风险，不推荐使用：DH group 1、DH group 2、DH group 5。

6.2.5.13 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6-12所示。

表 6-12 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。

6.2.6 连接故障或无法 PING 通

6.2.6.1 VPN 配置完成了，为什么连接一直处于未连接状态?

首先需要确认两端的预共享密钥和协商信息一致，云上与用户侧数据中心的本端子网/远端子网、本端网关/远端网关互为镜像。

其次确认用户侧数据中心设备的路由、NAT和安全策略配置无误，最后通过两端的子网互PING远端子网主机。

说明

因为VPN是基于数据流触发的，在配置完成后需要从任一端子网主机ping远端子网主机，ping之前请关闭主机防火墙，云上安全组开启入方向ICMP。

ping网关IP无法触发VPN协商，需要ping网关保护的子网中的主机。

6.2.6.2 使用中 IPsec VPN 连接中断后如何快速恢复?

1. 通过私网数据流重新触发IPsec协商。比如两端私网间进行互Ping，如果流量触发可正常建立请考虑部署长Ping保活脚本。
2. 如果无法正常触发协商，请检查IPsec两侧公网IP的连通性，比如两个公网IP互Ping验证。VPN网关IP默认回应ICMP报文。
3. 如果公网链路正常，需排查是否存在多出口的链路切换，即当前访问云网关IP流量未从协商端口流出。
4. 如果无多出口或出口路径正常，可尝试隧道两端同时修改一次PSK，重新触发协商。
5. 如果重新触发协商失败，请确认两端配置的协商策略是否一致、感兴趣流是否互为镜像（条目数、掩码均相同）。
6. 如果协商策略和感兴趣流配置无误，请关停云下设备的VPN连接，等待云端连接显示为“未连接”后，重启云下设备VPN连接，并进行数据流触发。
7. 如果依然无法触发协商时，请执行以下操作：
   a. 记录VPN连接的协商策略、PSK、本端子网、远端网关、远端子网。
   b. 使用现有网关新建一条连接，协商策略、PSK、本端子网均与原连接相同，远端网关和远端子网先任意填写。

c. 待新创建连接成功后，删除原连接，之后再修改新建连接的远端网关和远端子网与记录数据一致。

d. 修改完成后重新触发协商。

如果执行以上操作均未触发IPsec隧道状态正常，请向客服寻求帮助。

6.2.6.3 VPN 网关带宽到达限额时有什么影响?

VPN带宽限速限制的出VPC方向的带宽，如果您VPN的带宽超过限额使用时，会出现网络卡顿、部分子网间无法访问、甚至出现VPN连接中断现象（无法收到VPN的探测报文）。

因此在出现VPN带宽已达到上限时，建议您对VPN网关带宽进行扩容。

说明

VPN的带宽最大为300(Mbit/s)。

6.2.6.4 两个 Region 创建的 VPN 连接状态正常，为什么不能 ping 通对端 ECS?

安全组默认放行了出方向的所有端口，入方向需要按照实际需要添加放行规则，确认接收ping报文的ECS安全组放行了入方向的ICMP。

6.2.6.5 IDC 与云端对接，VPN 连接正常，子网间业务无法互相访问?

连接状态正常，说明两端的协商参数没有问题，排查项如下：

- 用户侧数据中心设备子网路由是否从网关开始逐跳指向VPN出口设备。
- VPN设备有安全设置放行了子网间的数据互访。
- IDC子网访问云端数据不做NAT。
- 确保两侧公网IP（网关IP）间访问不被阻拦。

6.2.6.6 正在使用 VPN 出现了连接中断，提示数据流不匹配，如何排查?

这通常是由于云上与用户侧数据中心设备配置的ACL不匹配造成的。

1. 首先确认两端VPN连接的子网信息是否配置一致，确保云端生成的ACL与用户侧数据中心ACL配置互为镜像。
2. 用户侧数据中心感兴趣流配置推荐使用“子网/掩码”的格式，避免使用网络地址对象模式，即address object模式，address object为非标模式，容易引起不兼容问题。

6.2.6.7 正在使用 VPN 出现了连接中断，提示 DPD 超时，如何排查?

出现DPD超时的连接中断是因为两端网络访问无数据，在SA老化后发送DPD未得到对端响应而删除连接。

解决方法：

1. 开启用户侧数据中心设备的DPD配置，测试两端的数据流均可触发连接建立；
2. 在两端的主机中部署Ping shell脚本，也可在用户侧数据中心的子网的网关设备上配置保活数据。

6.2.6.8 创建 VPN 连接后业务已通，但网页上的连接状态还是显示未连接?

管理控制台界面中VPN连接状态刷新存在一定的延迟，是正常现象。

如果数据面已正常（即业务访问已正常）， 则VPN连接已完成建立。

6.2.6.9 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，需要在页面左上角单击☰图标，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。

6.2.6.10 如何解决无法建立连接问题?

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
   ```
3. 配置完成后检查VPN是否连接，ping测试两端内网是否正常。

6.2.6.11 VPN 建立后您的数据中心或局域网无法访问?

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远端的子网地址访问。

6.2.6.12 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。

6.2.6.13 VPN 是否启动了 DPD 检测机制?

是的。

VPN服务默认开启了DPD探测机制，用于探测用户侧数据中心IKE进程的存活状态。

3次探测失败后即认为用户侧数据中心IKE异常，此时云会删除本端隧道，以保持双方的隧道同步。

DPD协议本身并不要求对端也同步进行配置（但是要求对端可以应答DPD探测），为了保证协商双方隧道状态一致，避免出现单边隧道（一端存在隧道，而另一端已不存在），建议用户同时启动用户侧网关的DPD探测机制，用于探测云侧VPN服务的IKE状态。

说明

DPD探测失败后会删除隧道，不会导致业务不稳定。

DPD可以及时发现对方IKE进程异常，并通过重置隧道的方法来保持双方隧道同步。在删除隧道后，当有用户流量时，可以重新触发协商并建立隧道。

6.2.7 公网地址

6.2.7.1 VPN 网关删除后公网地址是否可以保留?

VPN网关删除后不保留网关IP。

通过管理控制台界面删除VPN网关后， VPN网关相关联的资源，如公网IP，配置信息即被释放，不会保留。

须知

在按需计费模式下，删除最后一个连接会同步删除网关，用户如果需要保留公网IP，请确保不要删除最后一个VPN连接。

6.2.7.2 EIP 能作为 VPN 的网关 IP 吗?

不可以。

VPN网关IP是在创建VPN网关时分配的，需要和系统内的相关配置信息结合使用，EIP不具备VPN对接服务的功能。

6.2.7.3 通过 VPN 互访的主机需要购买 EIP 吗?

如果用户本地的主机通过VPN访问云上的ECS，此时ECS不需要购买EIP。

如果ECS要向公网用户提供服务，需要购买EIP。

6.2.7.4 为什么我开通 VPN 后，云端 ECS 会有公网 IP 的访问信息?

此现象多因您在VPN对接之前，ECS绑定了EIP。即用户除了通过VPN，也可通过公网地址直接访问该ECS。

VPN打通后，在感兴趣流内的主机访问云端ECS时会封装在隧道中。

- 如果ECS绑定了EIP，则非VPN网络中的设备仍可通过EIP直接访问该ECS。
- 如果ECS主机只允许VPN内的主机访问，可在完成VPN对接后将ECS的EIP解绑。当ECS需要绑定EIP时，可通过ACL来限定哪些流量可以通过EIP访问该ECS。

说明

用户是否要保留EIP，与业务类型相关。如用户ECS可以通过VPN获取用户侧数据中心的数据，同时该ECS还向互联网用户提供服务（如web server），此时就需要保留EIP。

6.2.7.5 用户侧数据中心的网关设备没有固定的公网 IP 可以吗?

不可以。

用户数据中心与云进行VPN对接时，要求用户侧数据中心有固定的公网IP或者经过NAT映射后的固定公网IP（即NAT穿越，VPN设备在NAT网关后部署）。

说明

普通家庭宽带路由器、个人的移动终端设备、Windows主机自带的VPN服务（如L2TP）无法与云进行VPN对接。

6.2.8 路由设置

6.2.8.1 如何理解 VPN 连接中的远端网关和远端子网?

远端网关和远端子网是两个相对的概念，在建立VPN连接时，从云的角度出发，VPC网络就是本地子网，创建的VPN网关就是本地网关，与之对接的用户侧网络就是远端子网， 用户侧的网关就是远端网关。

远端网关IP就是用户侧网关的公网IP，远端子网指需要和VPC子网互联的子网。

6.2.8.2 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到达远端子网的路由，无需手动配置。

6.2.8.3 ECS 主机多网卡是否需要添加去往线下网络的路由?

- 如果客户使用主网卡与线下网络建立了VPN，不需要添加路由。
- 如果客户使用非主网卡与线下网络建立了VPN，需要添加去往线下网段的路由指向非主网卡的网关。

6.2.9 VPN 子网设置

6.2.9.1 配置 VPN 连接的本端子网和远端子网时需要注意什么?

- 子网数量满足规格限制，数量超出规格限制请进行聚合汇总。
- 本端子网不可以包含远端子网，远端子网可以包含本端子网。
- 推荐配置的本端子网在VPC内有路由可达。
- 同一个VPN网关创建两条连接：若这两条连接的远端子网存在包含关系，在访问的目的网络处于交集网段部分时，按照创建连接的先后顺序匹配VPN连接，且与连接状态无关（策略模式不能按照掩码长度进行匹配）。

6.2.9.2 VPN 本端子网和远端子网的数量有限制吗，为什么我选择网段更新本地子网提示报错?

- 本端子网限制数量为5个，VPN本端子网和远端子网数量乘积最大支持到225。
- VPC会根据VPN连接的远端子网、云专线的远端子网、VPC对等连接子网、云连接的子网下发VPC子网路由，每个子网网段对应一条子网路由。
- VPC子网路由条目数不得大于200，即同一个VPC中所有VPN连接的远端子网数、专线的远端子网数、VPC对等连接子网数、云连接的子网数以及自定义路由条目数的总和不得大于200。

6.2.9.3 创建 VPN 连接时添加远端子网，提示系统异常，如何处理?

检查VPC内是否存在对等连接、云专线、云连接的子网路由使用了该子网，导致VPN下发子网路由冲突，确认后将其配置的子网路由删除后重新创建即可。

6.2.9.4 VPN 网关删除后公网地址是否可以保留?

VPN网关删除后不保留网关IP。

通过管理控制台界面删除VPN网关后， VPN网关相关联的资源，如公网IP，配置信息即被释放，不会保留。

须知

在按需计费模式下，删除最后一个连接会同步删除网关，用户如果需要保留公网IP，请确保不要删除最后一个VPN连接。

6.2.9.5 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、100.64.0.0/12和214.0.0.0/8的网段。

  如果需要使用100.64.0.0/10或100.64.0.0/12，请提交工单申请。

6.2.9.6 创建 VPN 网关时 IP 是如何分配的?

VPN网关IP是一组提前规划好的地址组，提前预置了VPN的相关配置。

在用户创建VPN网关时，系统会随机分配一个IP地址和VPC进行绑定，且这个IP地址也只能绑定1个VPC。

因为VPN的网关IP存在预置数据，所以VPN网关IP和EIP不能转换，在创建VPN网关时也不能指定IP地址。删除VPN网关时会释放IP地址与VPC的绑定关系；重新创建VPN网关时系统会重新随机分配网关IP地址。

6.2.9.7 VPN 本端子网和远端子网数量有什么限制?

- 本端子网限制数量为5个，VPN本端子网和远端子网数量乘积最大支持到的规模。
- VPC会根据VPN连接的远端子网、云专线的远端子网、vpc-peering子网下发VPC子网路由，每个子网网段对应一条子网路由。

- VPC子网路由条目数不得大于200，即同一个VPC中所有VPN连接的远端子网数、专线的远端子网数、vpc-peering子网数以及自定义路由条目数的总和不得大于200。

6.2.10 VPN 感兴趣流

6.2.10.1 本地设备配置 VPN 时需要设置 ACL，为何在 Console 上找不到对应的配置?

用户侧数据中心配置VPN设备时，是需要独立创建ACL，且该ACL会被IPsec的策略引用。

云上配置VPN服务时，会根据管理控制台界面填入的本端子网和远端子网自动生成ACL，然后下发给VPN网关，其中ACL中的rule数量是两端子网数量的乘积。

6.2.10.2 如何配置和修改云上 VPN 的感兴趣流?

感兴趣流由本端子网与远端子网full-mesh生成，例如本端子网有2个，分别为A与B，远端子网有3个，分别为C、D和E，生成感兴趣流时ACL的rule如下：

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

在管理控制台界面修改本端子网和远端子网会自动更新VPN设备的感兴趣流信息，即修改了云上的ACL配置。

6.2.11 VPN 连接保活

6.2.11.1 如何防止 VPN 连接出现中断情况?

VPN连接在正常的使用过程中会存在重协商情况，触发重协商的条件有IPsec SA的生命周期即将到期和VPN传输的流量超过20GB，重协商一般不造成连接中断。

大多数的连接中断都是因为两端的配置信息错误造成的，或公网异常导致重协商失败造成的。

常见的连接中断原因有：

- 两端的ACL不匹配；
- SA生命周期不匹配；
- 用户侧数据中心未配置DPD；
- VPN使用过程中修改了配置信息；
- 数据超过MTU后导致报文分片；
- 运营商网络抖动。

因此请在配置VPN时确保操作和配置，以进行连接状态保活：

- 两端的子网配置互为镜像；

- SA生命周期信息一致；
- 用户侧数据中心设备开启DPD配置，探测次数不少于3次；
- 连接过程中修改参数两侧同步修改；
- 设置用户侧数据中心设备TCP MAX-MSS为1300；
- 确保用户侧数据中心出口有足够的带宽可被VPN使用；
- 确认VPN连接可被两端触发协商，开启用户侧数据中心设备的主动协商配置；
- 两端子网进行长Ping操作（脚本内容如下）。

```
#!/bin/sh
host=$1
if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi
log_name=$host".log"

while :; do
    result=`ping -W 1 -c 1 $host | grep 'bytes from '`
    if [ $? -gt 0 ]; then
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a $log_name
    else
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo $result | cut -d ':' -f 2`"| tee -
a $log_name
    fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

说明

1. 通过VI编辑器将以上脚本粘贴在ping.sh文本中。
2. 给文件授权 chmod 777 ping.sh。
3. 使用文件执行ping命令：

   ./ping.sh x.x.x.x >>/dev/null &

   x.x.x.x是您需要ping的远端目标IP。
4. 执行ping命令后，后台运行并生成x.x.x.x.log文件，执行命令：

   tail -f x.x.x.x.log

   可以实时查看长ping结果。

6.2.12 监控类

6.2.12.1 VPN 监控可以监控哪些内容?

VPN网关

可监控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；查询网关监控状态请在VPN网关列表中选择“操作 > 查看监控”即可。

VPN连接

可监控连接的状态，1为正常、0为未连接；查询VPN连接监控请在VPN连接列表中选择“操作 > 更多 > 查看监控”。

6.2.12.2 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，需要在页面左上角单击☰图标，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。

6.2.12.3 VPN 监控能不能查看每条连接的流量?

VPN的流量监控是基于VPN网关的，可查看该VPN网关的出入方向的流量、带宽等信息，无法查看单独的某一条连接的流量使用情况。

6.2.13 带宽与网速

6.2.13.1 如何测试 VPN 速率情况?

当测试环境为已创建VPN连接，并在VPN连接的本端子网下创建ECS，并使其相互能够ping通的情况下，测试VPN的速率情况。

当用户购买的VPN网关的带宽为200Mbit/s时，测试情况如下。

1. 互为对端的ECS都使用Windows系统，测试速率可达180Mbit/s，使用iperf3和filezilla（是一款支持ftp的文件传输工具）测试均满足带宽要求。

   说明

   基于TCP的FTP协议有拥塞控制机制，180Mbit/s为平均速率，且IPsec协议会增加新的IP头，因此10%左右的速率误差在网络领域是正常现象。

   使用iperf3客户端测试结果截图如图6-12所示。

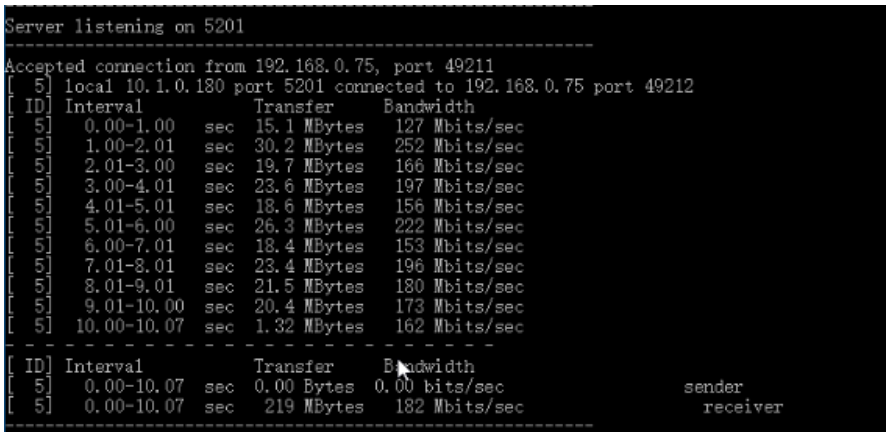
   图 6-12 200M 带宽客户端 iperf3 测试结果

```
C:\Windows>iperf3 -c 10.1.0.180 -i 1 -w 1M
Connecting to host 10.1.0.180, port 5201
[  4] local 192.168.0.75 port 49212 connected to 10.1.0.180 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  17.1 MBytes   142 Mbits/sec
[  4]   1.01-2.00   sec  30.0 MBytes   253 Mbits/sec
[  4]   2.00-3.01   sec  19.8 MBytes   165 Mbits/sec
[  4]   3.01-4.01   sec  23.2 MBytes   194 Mbits/sec
[  4]   4.01-5.00   sec  18.9 MBytes   161 Mbits/sec
[  4]   5.00-6.01   sec  26.2 MBytes   219 Mbits/sec
[  4]   6.01-7.01   sec  18.4 MBytes   153 Mbits/sec
[  4]   7.01-8.01   sec  23.2 MBytes   195 Mbits/sec
[  4]   8.01-9.00   sec  21.1 MBytes   180 Mbits/sec
[  4]   9.00-10.01  sec  21.0 MBytes   174 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec   219 MBytes   183 Mbits/sec                  sender
[  4]   0.00-10.01  sec   219 MBytes   183 Mbits/sec                  receiver

iperf Done.
```

   使用iperf3服务器端测试结果截图如图6-13所示。

图 6-13 200M 带宽服务端 iperf3 测试结果

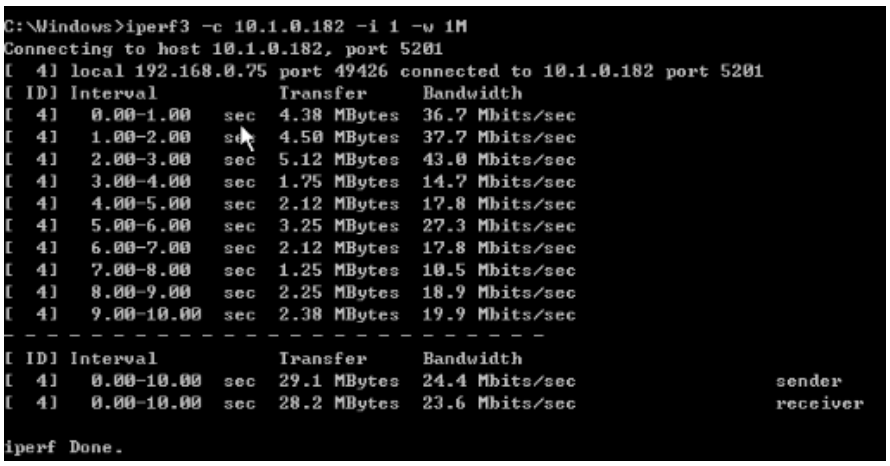


2. 互为对端的ECS都使用Centos7系统，测试速率可达180M，使用iperf3测试满足带宽要求。
3. 服务器端ECS使用Centos7系统，客户端使用Windows系统，测试速率只有20M左右，使用iperf3和filezilla测试均不能满足带宽要求。

   原因在于Windows和Linux对TCP的实现不一致，导致速率慢。所以对端ECS使用不同的系统时，无法满足带宽要求。

   使用iperf3测试结果截图如图6-14所示。

图 6-14 互为对端的 ECS 系统不同时 iperf3 测试结果



假设用户购买的VPN网关的带宽为1000Mbit/s，

用户购买的VPN网关为网关的整体吞吐能力，即该VPN网关下所有VPN连接的带宽之和。在大带宽场景下，由于主机的转发性能限制，需要使用多台主机构建多条流量才能充分利用网关的带宽。这种场景下对ECS的配置要求也很高，建议ECS的网卡支持2G以上的带宽。

测试总结：综上测试结果，云网关能够满足带宽速率要求，但是建议两端主机使用相同的操作系统，并且网卡要达到配置要求。

6.2.13.2 VPN 的带宽限速，是限制的哪个方向的带宽，带宽的单位是什么？

云上用户购买的VPN网关带宽指的是出云方向的，同时为了避免入云方向不限速带来的流量不对称问题。入云方向的带宽策略调整如下两种情况：

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

按带宽计费度量采用国际统一的带宽单位Mbit，按流量计费的度量单位为GByte。

6.2.13.3 VPN 网关带宽到达限额时有什么影响?

VPN带宽限速限制的出VPC方向的带宽，如果您VPN的带宽超过限额使用时，会出现网络卡顿、部分子网间无法访问、甚至出现VPN连接中断现象（无法收到VPN的探测报文）。

因此在出现VPN带宽已达到上限时，建议您对VPN网关带宽进行扩容。

说明

VPN的带宽最大为300(Mbit/s)。

6.2.13.4 修改了 VPN 带宽大小，为什么测试没有生效?

VPN带宽修改到生效会有一定的延迟，是正常现象。

请在修改带宽5分钟后再进行带宽测试。

说明

修改VPN带宽大小，不会导致用户业务和网络中断。

6.2.13.5 VPN 能否共用 EIP 的带宽?

不可以。

目前VPN的公网地址与EIP是各自独立的，用户在创建VPN网关时会自动生成公网地址并设置带宽，无法与EIP共享带宽。

6.2.13.6 VPN 产品中的带宽和云专线的带宽有什么区别?

概念

- 云专线的带宽指用户创建的物理连接的带宽大小。
- VPN的带宽指的是出云方向的带宽。

带宽大小

- 云专线默认最大带宽1000(Mbit/s)，用户在管理控制台创建物理连接界面，“端口类型”参数选择“10GE单模光口”，支持最大带宽10Gbit/s
- VPN的带宽最大为300(Mbit/s)。

网络质量

- 云专线用户独占一条网络资源，网络质量高。
- VPN是基于VPN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。网络质量依赖公网质量。

6.2.13.7 如何选择购买 VPN 带宽的大小?

购买VPN时，选择带宽大小需要考虑以下两个因素：

- VPN隧道中单位时间的数据传输量（需要冗余一定带宽，防止链路拥塞）。
- 考虑两端的出口带宽，云上带宽要小于云下出口带宽。